Effiziente Lösung reeller Polynomialer Gleichungssysteme

D I S S E R T A T I O N

zur Erlangung des akademischen Grades
doctor rerum naturalium
(dr. rer. nat.)
im Fach Mathematik

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät II
Humboldt-Universität zu Berlin

von
Herr Dipl.-Math. Mbakop Guy Merlin
geborem am 09.08.1966 in Bangoua (Kamerun)

Präsident der Humboldt-Universität zu Berlin:
Prof. Dr. Hans Meyer

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät II:
Prof. Dr. Bodo Krause

Gutachter:

1. Prof. Dr. B. Bank
2. Priv.-Doz. Dr. W. Kleinert
3. Prof. Dr. Luis Miguel Pardo

eingereicht am:	12. Juli 1999
Tag der mündlichen Prüfung:	24. September 1999

Abstract

This dissertation deals with *geometric algorithms* for solving real multivariate polynomial equation systems, that define a reduced regular sequence (cf. subsection 2.2). Real solving means that one has to find at least one real point in each connected component of a real compact and smooth variety $V := W \cap \mathbb{R}^n$.

The main point of this thesis is the use of a complex symbolic geometric algorithm, which is designed for an algebraically closed field and was published in the papers [GHM$^+$98] and [GHH$^+$97]. The models of computation are *straight–line programms* and *arithmetic Networks* with parameters in $\mathbb{Q}$. Let the polynomials be given by a division–free straight–line programm of size L. A geometric solution for the system of equations given by the regular sequence consists in a *primitiv element* of the ring extension associated with the system, a minimal polynomial of this primitive element and a parametrization of the coordinates. This representation has a long history going back to *Leopold Kronecker* [Kro82]. The time–complexity of our algorithms turns out to be linear in L and polynomial with respect to n, d, δ or δ', respectively. Here n denotes the number of variables, d is an upper bound of the degrees of the polynomials involved in the system, δ and δ' are geometric invariants representing the maximum of the *affine (geometric) degree* of the system under consideration and the affine (geometric) degree of suitable *polar varieties* (cf. [Hei83] for the (*geometric*) degree).

The application of an algorithm running in the complex numbers to solve polynomial equations in the real case becomes possible by the introduction of polar varieties (cf. [BGHM97]). The polar varieties introduced for this purpose prove to be the corner–stone and the preliminary tool for the efficient use of the geometric algorithm mentioned above. An incremental algorithm is designed to find at least one real point on each connected component of the zero set defined by the input under the assumption that the given semialgebraic set $V = W \cap \mathbb{R}^n$ is a bounded, smooth (local) complete intersection manifold in $\mathbb{R}^n$. The increment of the new algorithm is the codimension of the polar varieties under consideration. The main theorems are Theorem 17 on page 39 for the hypersurface case, and Theorem 27 on page 69 for the complete intersection as well as the statement in the introduction of this thesis on page 6.

Keywords:

affine (geometric) degree, geometric algorithm, straight–line program and arithmetic network, polar variety.

Zusammenfassung

Diese Arbeit beinhaltet *geometrische Algorithmen* zur Lösung reeller polynomialer Gleichungssysteme mit rationalen Koeffizienten, wobei die Polynome eine reduzierte reguläre Folge bilden (vgl. Abschnitt 2.2). Unter reellem Lösen verstehen wir hier die Bestimmung eines Punktes in jeder Zusammenhangskomponente einer kompakten glatten reellen Varietät $V := W \cap \mathbb{R}^n$.
Im Mittelpunkt steht die Anwendung des für den algebraisch abgeschlossenen Fall veröffentlichten symbolischen geometrischen Algorithmus nach [GHM$^+$98] und [GHH$^+$97]. Die Berechenungsmodelle sind *Straight–Line Programme* und arithmetische Netzwerke mit Parametern in $\mathbb{Q}$. Die Input–Polynome sind durch ein Straight–Line Programm der Größe L gegeben. Eine geometrische Lösung des Input–Gleichungssystems besteht aus einem primitiven Element der Ringerweiterung, welche durch die Nullstellen des Systems beschrieben ist, aus einem mininalen Polynom dieses primitiven Elements, und aus den Parametrisierungen der Koordinaten. Diese Darstellung der Lösung hat eine lange Geschichte und geht mindestens auf Leopold Kronecker [Kro82] zurück. Die Komplexität des in dieser Arbeit begründeten Algorithmus erweist sich als linear in L und polynomial bezüglich n, d, δ bzw. $\delta\,'$, wobei n die Anzahl der Variablen und d eine Gradschranke der Polynome im System ist. Die Größen δ und $\delta\,'$ sind geometrische Invarianten, die das Maximum der *Grade des Inputsystems* und geeigneter *polarer Varietäten* repräsentieren (bzgl. des (*geometrischen*) Grades vgl. [Hei83]).
Die Anwendung eines Algorithmus über den komplexen Zahlen auf das Lösen von polynomialen Gleichungen im Reellen wird durch die Einfürung polarer Varietäten möglich (vgl. [BGHM97]). Die polaren Varietäten sind das Kernstück und das vorbereitende Werzeug zur effizienten Nutzung des oben erwähnten geometrischen Algorithmus. Es wird ein inkrementelles Verfahren zur Auffindung reeller Punkte in jeder Zusammenhangskomponente der Nullstellenmenge des Inputsystems abgeleitet, welches einen beschränkten glatten (lokalen) vollständigen Durchschnitt in $\mathbb{R}^n$ beschreibt. Das Inkrement des Algorithmus ist die Kodimension der polaren Varietäten. Die Hauptsätze sind Satz 17 auf Seite 39 für den Hyperflächenfall, und Satz 27 auf Seite 69, sowie die Aussage in der Einführung dieser Arbeit, Seite 6 für den vollständigen Durchschnitt.

Schlagwörter:
affiner (geometrischer) Grad, geometrischer Algorithmus, Straight–Line Programm und arithmetisches Netzwerk, polare Varietät.

How to Solve It

> “ *It would be a mistake to think that solving problems is a purely* “ *intellectual affair* ”*; determination and emotions play an important role. Lukewarm determination and sleepy consent to do a little something may be enough for a routine problem in classroom. But, to solve a serious scientific problem, will power is needed that can outlast years of toil and bitter disappointments.* ”

G. Polya A New Aspect of Mathematical Method, Princeton University Press

Je dédie ce Document à ma Famille, ma tante *Ernestine Nnemele Zombou*, ma grande mère *Anne Ngamga*, ma maman *Jacqueline Ngahane Nguele* mon Papa *Pierre Lebel Nguele* et mon oncle *Charles Zombou.* Ils m'ont soutenu pendant mon long séjour à Berlin.

À *Michel Emmanuel Abata*, *Marie-Solange Oyama* et à tous ceux des miens qui m'ont quitté pendant la rédaction de ce chef d'oeuvres.

Blues On The Bayou

> “ *In the case you're interested, my favorite is* “ *I'll Survive*, ” a Song I wrote back in the Fifties. I sang it then, but I'm not sure I understood it.
>
> Now I know the meaning of survival. ”

B. B. King as told to David Ritz

Inhaltsverzeichnis

1 Einführung **1**

2 Zeitpolynomiale Algorithmen zur geometrischen Lösung **10**
2.1 Bezeichnungen und Grundbegriffe 10
2.2 Geometrische Lösung eines affinen vollständigen Durchschnittes . . . 13
2.3 Kodierung der Polynome 15
2.4 Der geometrische Lösungsalgorithmus 17

3 Reelle Lösungen, der Hyperflächenfall **20**
3.1 Polare Varietäten 20
3.2 Der algorithmische und komplexitätstheoretische Aspekt des Hyperflächenfalls 27
3.3 Generische Koordinatenwahl 40
3.3.1 Die Resultante eines Polynoms und eines homogenen Ideals . . 42
3.3.2 Die Diskriminante einer Abbildung 43

4 Der vollständige Durchschnitt **46**
4.1 Lokale Beschreibung der Determinantenvarietäten 48
4.2 Lokale Beschreibung der Varietäten 51
4.3 Die Existenz glatter reeller Punkte in den polaren Varietäten 59
4.4 Ein Algorithmus für den vollständigen Durchschnitt 62

5 Generische Koordinaten **70**

Literaturverzeichnis **81**

Symbole **i**

Danksagung **iii**

Curriculum Vitae **iv**

Kapitel 1

Einführung

Im Mittelpunkt dieser Dissertation stehen die *reellen Lösungen* eines multivariaten polynomialen Gleichungssystems mit rationalen Koeffizienten. Die Lösungsmenge eines Systems polynomialer Gleichungen wird eine affine algebraische Varietät genannt. Wir benutzen die kurze Form Varietät, da wir stets in affinen Räumen $\mathbb{R}^n$ oder $\mathbb{C}^n$ und ausschließlich mit Polynomen arbeiten.

Entscheidend zur Bestimmung reeller Lösungen von Gleichungen und Ungleichungen war das von *Sturm* 1829 in *l'Academie Royale des Sciences* formulierte Theorem, [Stu35]. Das Theorem gibt ein auf dem euklidischen Algorithmus basierendes Verfahren zur Aufzählung reeller Nullstellen eines univariaten Polynoms in einem vorgegebenen Intervall an. Das Sturm'sche Verfahren generierte seiner Zeit einen von *Sylvester* genannten „*Zyklus von Sturm'schen Ideen* “. Das sind Folgen auf dem Sturm'schen Theorem basierender Arbeiten, die von berühmten Gelehrten, wie Sylvester, Cayley, Hermite und später Kronecker verfaßt wurden. Die algebraische Deutung des Beweises von Sturm hat sich historisch gesehen auf drei verschiedenen Wegen vollzogen. In erster Linie zeigten *Hermite*, [Her53] und *Sylvester*, [Syl53] eine Verallgemeinerung des Sturm'schen Theorems auf multivariate Gleichungen, indem sie die Beziehung zwischen der algebraischen Eliminationstheorie und der Theorie der quadratischen Formen zeigten. In zweiter Linie gab die durch *Artin* und *Schreier*, [AS26] dargestellte Konstruktion reeller Körper eine allgemeine algebraische Grundlage der Theorie der Gleichungen und Ungleichungen. Drittens verallgemeinerte *Tarski* das Sturm'sche Theorem auf ein gemischtes System von Gleichungen und Ungleichungen und definierte die Methode der Quantorenelimination für die elementare Theorie geordneter Körper reeller Zahlen und reeller abgeschlossener Körper. Erst nach dem Resultat von A. Robinson konnte der Parallelismus zwischen reell abgeschlossenen Körpern und algebraisch abgeschlossenen Körpern gezeigt werden. Das Sturm'sche Theorem im reell abgeschlossenen Körper wurde mit diesem Resultat das Analogon des Hilbert'schen Nullstellensatzes in algebraisch abgeschlossenen Körpern. Dieser mehr als ein Jahrhundert bestehende Parallelismus zeigt, daß sich Methoden zum Lösen algebraischer Gleichungen in algebraisch abgeschlossenen

Körpern nur mit erheblichen Schwierigkeiten auf das Reelle anwenden lassen.

Mit dieser Arbeit wird versucht eine direkte Anwendung eines im algebraisch abgeschlossenen Fall aufgebauten geometrischen Lösungsalgorithmus auf die Bestimmung von reellen Nullstellen eines polynomialen Gleichungssystems zu begründen. Die Grundidee für diese Anwendung ist in der Arbeit in [GHM+98] gelegt worden.

Unter geeigneten Voraussetzungen, die später erklärt werden, bauen wir einen inkrementellen Algorithmus auf, welcher ausgehend von einem System gegeben durch eine reduzierte reguläre Folge (vgl. Abschnitt 2.2)

$$f_1, \dots, f_p \in \mathbb{Q}[X_1, \dots, X_n],\ p \leq n \tag{1.1}$$

einen reellen repräsentativen Punkt in jeder Zusammenhangskomponente der Varietät

$$V(f_1, \dots, f_p) \cap \mathbb{R}^n := \{x \in \mathbb{R}^n | f_1(x) = \dots = f_p(x) = 0\} \tag{1.2}$$

findet.

Unser Verfahren besteht aus zwei Hauptschritten: einem Vorbereitungsschritt und einem symbolisch geometrischen Lösungsalgorithmus.

1. Der Vorbereitungsschritt besteht aus dem Aufbau gewisser *polarer Varietäten*, welche das Hinzufügen gewisser Polynome, $p-$Minoren $M_p \dots M_{n-1}$ der Jacobimatrix $J(f_1, \dots, f_p)$, zu dem System $f_1, \dots, f_p$ ermöglichen, so daß die entstehende Folge
$$f_1, \dots, f_p, M_p, \dots, M_{n-1} \tag{1.3}$$
eine transversale Folge außerhalb der Vereinigung
$$V(m) \cup Sing\, V(f_1, \dots, f_p) \tag{1.4}$$
der Hyperfläche $V(m) := \{x \in \mathbb{C}^n |\ m(x) = 0\}$ mit der Menge der singulären Punkten $SingV(f_1, \dots, f_p)$ in $V(f_1, \dots, f_p)$ ist, wobei $m \in \mathbb{Q}[X_1, \dots, X_n]$ ein gewisser $(p-1)-$Minor der Jacobimatrix $J(f_1, \dots, f_p)$ ist (vgl. Definition 4).

2. Eine geometrische Lösung des Systems (1.3) außerhalb
$$V(m) \cup Sing\, V(f_1, \dots, f_p)$$
bestimmt die Parametrisierung von mindestens einem Punkt in jeder Zusammenhangskomponenten der Varietät
$$\overline{V(f_1, \dots, f_p) \setminus (V(m) \cup Sing\, V(f_1, \dots, f_p)}\quad \text{(vgl. Satz10).}$$

Dieser Vorbereitungsschritt ermöglicht dann die Anpassung der in den Arbeiten [GHMP95], [GHM+98], [GHH+97] veröffentlichten Algorithmen an den reellen Fall. Der resultierende Algorithmus ist dann von *wesentlichem Typ*, was heißen soll, daß die Methode zwischen semantischen und syntaktischen Eigenschaften des Eingangssystems unterscheiden kann und dadurch eine Verbesserung der Komplexitätsabschätzungen gegenüber „*klassischen*“Verfahren möglich wird (vgl. z.B. [Her26], [Sei74], [Buc70], [HW75], [Hei83], [Laz77], [Laz81], [CG83], [CGH89], [DFGS91], [Can88], [GH93], [KP94], [KP96], [Chi95]). Die Semantik beinhaltet die Deutung (den Sinn) der Lösung des Problems und die Syntax die Darstellung und die Handhabung der mathematischen Objekte (das Bild): das Sinnbild und das symbolische Rechnen entsprechen einander.

Im Fall einer Hyperfläche (vgl. Kapitel 3) besteht der Vorbereitungsschritt aus einem schrittweisen Aufbau einer transversalen reduzierten Folge außerhalb einer Hyperfläche

$$V(\Delta) := \{x \in \mathbb{C}^n \mid \Delta(x) = 0\}; \tag{1.5}$$

die Folge besteht dann aus einem Polynom f mit rationalen Koeffizienten und seinen partiellen Ableitungen (vgl.[BGH+95], [BGHM97]). Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ quadratfrei und vom Grad d. Das Polynom f sei eine reguläre Gleichung der reellen Varietät $V(f) \cap \mathbb{R}^n$, d.h. der Gradient von f verschwindet nicht auf $V(f) \cap \mathbb{R}^n$. Die reelle Varietät $V(f) \cap \mathbb{R}^n$ ist mit dieser Annahme, eine Hyperfläche. Seien weiterhin die Variablen $X_1, \ldots, X_n$ generisch gewählt. Dann ergänzen wir das aus f bestehende System Schritt für Schritt mit den partiellen Ableitungen $\frac{\partial f}{\partial X_i},\ 0 \le i \le n-1$. Sei

$$\Delta(x) := \sum_{j=1}^{n} \left(\frac{\partial f(x)}{\partial X_j} \right)^2 . \tag{1.6}$$

Wir bestimmen in jedem Schritt $i,\ 0 \le i \le n-1$, eine geometrische Lösung des Systems (vgl. Abschnitt 2.2)

$$f,\ \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}, \tag{1.7}$$

außerhalb der Hyperfläche

$$V(\Delta) := \{x \in \mathbb{C}^n | \Delta(x) = 0\}. \tag{1.8}$$

Diese Lösung wird mit den Methoden in [GHMP95], [GHM+98], [GHH+97] beschrieben und ist eine parametrische Darstellung der positiv dimensionalen $i-$ten polaren Varietät, die mit dem $\mathbb{Q}$–Zariski–Abschluß

$$\overline{\left\{ x \in \mathbb{C}^n \mid f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0,\ \Delta(x) \neq 0 \right\}} \tag{1.9}$$

übereinstimmt. Die geometrische Lösung des zur $(n-1)-$ten polaren Varietät gehörenden Gleichungssystems gestattet es für jede Zusammenhangskomponente der reellen Varietät $\{x \in \mathbb{R}^n \mid f(x) = 0\}$ einen repräsentativen reellen Punkt anzugeben.

Die Vorgehenweise im Hyperflächenfall läßt sich auf den Fall eines vollständigen Durchschnittes verallgemeinern. Seien $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$, $p \leq n$ Polynome, die eine reduzierte Folge bilden (vgl. (1.1)). Wir wählen einen beliebigen $(p-1)-$Minor $\tilde{m} \in \mathbb{Q}[X_1, \ldots, X_n]$ der Jacobimatrix $J(f_1, \ldots, f_p)$. Zu diesem $(p-1)-$Minor können wir eine aus $n-p$ vielen Polynomen, das sind maximale Minoren von $J(f_1, \ldots, f_p)$, bestehende Folge konstruieren, die das Startsystem $f_1, \ldots, f_p$ zu einer transversalen regulären Folge außerhalb $V(\tilde{m}) \cup Sing\ V(f_1, \ldots, f_p)$ ergänzen (wie es z.B. in (1.3) der Fall ist für den Minor m). Das neu entstehende System beschreibt einen lokalen null–dimensionalen vollständigen Durchschnitt, auf welchen die geometrische Eliminationsmethode angewendet werden kann. Es gibt $p\binom{n}{p-1}$ viele Möglichkeiten, einen $(p-1)-$Minor in $J(f_1, \ldots, f_p)$ festzulegen, mit welchem eine lokaler vollständiger Durchschnitt generiert wird.

Unter der Voraussetzung, daß die reelle Varietät $V := V(f_1, \ldots, f_p) \cap \mathbb{R}^n$ beschränkt und nur aus $(f_1, \ldots, f_p)-$glatten Punkte besteht (vgl. Definition 2), lassen sich repräsentative Punkte in der Varietät V mit der geometrischen Lösungen aller entstehenden, null–dimensional lokalen vollständigen Durchschnitte parametrisieren. Diese Parametrisierung wurde neuerlich von den Autoren in [GHH⁺97], [Mat97], [Mor97] und [Häg98] als eine Variante des im Jahre 1882 von Kronecker entworfenen Eliminationsverfahrens erkannt (vgl. [Kro82] [Zar95]).

Seien $X_1, \ldots, X_n$ generische Koordinaten im affinen Raum $\mathbb{C}^n$. Wir setzen ohne Einschränkung der Allgemeinheit voraus, daß die Polynome $f_1, \ldots, f_p$, $p \leq n$, wie in (1.1) gegeben sind. Das Kronecker'sche Eliminationsverfahren generiert eine parametrische Darstellung der Varietät

$$V(f_1, \ldots, f_p) := \{x \in \mathbb{C}^n |\ f_1(x) = \ldots = f_p(x) = 0\}$$

und definiert die Dimension der im Verfahren auftretenden Varietäten, (vgl. [Bou84], [Sev47], [Zar95]). Das Eliminationsverfahren läßt sich folgendermaßen zusammenfassen (vgl. [Kro82], [Bou84]): zur Lösung des Systems $f_1 = 0, \ldots, f_p = 0, 1 \leq p \leq n$, können wir durch einen linearen Koordinatenwechsel die Polynome $f_1, \ldots, f_p$ so darstellen, daß in jedem Polynom $f_i, 1 \leq i \leq p$, der Term mit höchstem Grad in X_1 die Form $c_i X_1^{m_i}$ hat, wobei $c_i \neq 0$ eine Konstante ist. Indem wir alle Polynome durch ihren größten gemeinsamen Teiler dividieren, können wir weiterhin voraussetzen, daß die Polynome $f_1, \ldots, f_p$ keinen gemeinsamen Faktor besitzen. Wir betrachten nun für die neuen $2p$ Unbestimmten $A_i, B_i, 1 \leq i \leq p$, die Polynome

$$\sum_{i=1}^{p} A_i f_i \text{ und } \sum_{i=1}^{p} B_i f_i \qquad (1.10)$$

als Polynome in X_1. Wir bilden die Sylvester–Resultante bezüglich der Variable X_1, welche ein Polynom in A_i und B_i mit Koeffizienten in $\mathbb{Q}[X_2, \ldots, X_n]$ ist. Indem wir diese Koeffizienten zu Null setzen, erhalten wir ein System von Gleichungen, dessen Lösungen $(x_2, \ldots, x_n)$ genau die Projektion der gemeinsamen Nullstellen $(x_1, \ldots, x_n)$

der Polynome $f_1, \ldots, f_p$ ist. Wir setzen diesen Schritt induktiv fort, bis die Variable X_n eliminiert ist.

Das Verfahren geht von einer reduzierten regulären Folge $f_1, \ldots, f_p$ aus und generiert eine endliche Anzahl von irreduziblen algebraischen Varietäten, die jeweils so parametrisiert sind, daß gewisse Koordinaten frei, und andere algebraische Funktionen dieser freien Variablen sind. Die Anzahl der freien Koordinaten in der Parametrisierung einer irreduziblen Komponente heißt dann die Dimension der irreduziblen Komponente. Die Methode von Kronecker ist in dieser Form nicht effizient, und nahezu unpraktisch. Diese Tatsache hat viele Autoren in der Algebraischen Geometrie [Wei46], [Bou84], [Van58] und in der Computeralgebra dazu geführt, diese Methode in Vergessenheit geraten zu lassen und was das Eliminieren eines ideenreichen Eliminationsverfahrens zur Folge hatte. Francesco Severi (1879–1961) zeigte in [Sev47], anhand von Beispielen einer Raumkubik, die auf Oskar Perron (1880–1975) zurückgeht, wie die Kronecker'sche Eliminationstheorie in der Schnitttheorie und damit auch auf dem Gebiet der Singularitätstheorie leistungstark sein kann. Seien die Polynome

$$f_1(X_1, X_2, X_3, X_4) := X_1X_3 - X_2^2 \tag{1.11}$$

und

$$f_2(X_1, X_2, X_3, X_4) := X_1X_4^2 - 2X_2X_3X_4 + X_3^3 \tag{1.12}$$

gegeben. Die Kubik C_3 sei in homogenen Koordinaten $[x_1, x_2, x_3, x_4]$ parametrisiert:

$$C_3 := \{[x_1, x_2, x_3, x_4] \in \mathbb{P}\mathbb{C}^3 |\ x_1 = \varrho^3, x_2 = \varrho^2\sigma, x_3 = \varrho\sigma^2, x_4 = \sigma^3,\ \varrho, \sigma \in \mathbb{C}\} \tag{1.13}$$

Severi zeigte mit Hilfe der Kronecker'schen Eliminationstheorie, daß die einfach gezählte Kurve nicht der vollständige Schnitt der zwei Flächen

$$\{[x_1, x_2, x_3, x_4] \in \mathbb{P}\mathbb{C}^3 | f_1(x_1, x_2, x_3, x_4) = 0\} \tag{1.14}$$

und

$$\{[x_1, x_2, x_3, x_4] \in \mathbb{P}\mathbb{C}^3 | f_2(x_1, x_2, x_3, x_4) = 0\} \tag{1.15}$$

ist. Der Schnitt dieser Flächen ergibt genau zwei mal die Kubik C_3: Der Schnitt ist von der Vielfachheit 2.

$$2C_3 = \{[x_1, x_2, x_3, x_4] \in \mathbb{P}\mathbb{C}^3 |\ x_1x_3 - x_2^2 = x_1x_4^2 - 2x_2x_3x_4 + x_3^3 = 0\}. \tag{1.16}$$

Er beantwortete damit die Frage positiv, ob *die allgemeine Eliminationstheorie (hiermit ist die Kronecker'sche gemeint) die Hilfsmittel zur Feststellung der Vielfachheit der Lösungen in allgemeinen Schnittproblemen liefert.* Severi's Antwort auf diese Frage in [Sev47] ist die folgende: „*In der Tat liefert die von Kronecker begründete Eliminationstheorie*, **wenn sie aufmerksam angewandt wird**, *von selbst alle Lösungen mit der ihnen zukommenden Vielfachheit.* “

Diese Aufmerksamkeit findet sich den Publikationen [KP96], [GHMP95], [GHM+98], [GHH+97], [Mat97], [Mor97], [Häg98], [BGH+95] und [BGHM97], welche die Kronecker'sche Eliminationstheorie erst recht so entwickeln haben, daß sie heutzutage ein effizientes Verfahren zum Lösen von Systemen polynomialer Gleichungen ist. Wovon Severi damals fest überzeugt war, ist heute mit dieser Reihe von Veröffentlichungen Wirklichkeit geworden (vgl. [Sev47], Seite 100 & 101): „*Die algebraische Geometrie ist ganz auf dem Vielfachheitsbegriff der Lösungen aufgebaut. Wenn man es unterläßt nachzuprüfen, wie dieser Begriff in die Probleme, die sich von Fall zu Fall in der algebraischen Geometrie ergeben, hineinspielt, so verkennt man seine Bedeutung für unsere Erkenntnis. Denn nur auf Grund einer strengen Fassung des Multiplizitätsbegriffes hat unsere Geometrie Allgemeingültigkeit und Durchschlagskraft und verläuft sich nicht in der Unterscheidung einer Unzahl von Fällen und Unterfällen. ... Ich glaube, daß in der algebraischen Eliminationstheorie die Ausschaltung des Multiplizitätsbegriffes bei den Lösungen, deren Ermittlung ja doch der Hauptzweck ist, dem Verzicht auf eine vollständige Lösung des Problems gleichkommt.*"Eine weitere Darstellung des Kronecker'schen Eliminationsverfahren zur Lösung polynomialer Gleichungssysteme findet man in der Arbeit [GLS99].

Die Rechenmodelle in unserem Algorithmus sind Straight–Line Programme und arithmetische Netzwerke mit Parametern in $\mathbb{Q}$ (vgl. Definition 5). Unser Hauptalgorithmus basiert auf einem symbolisch geometrischen Verfahren, das vollständige Durchschnitte im komplexen Raum effizient parametrisiert. Bei der Aufzählung arithmetischer Operationen in $\mathbb{Q}$ mit einheitlichen Kosten waren die besten bekannten Komplexitätsschranken zur Lösung eines Gleichungssystems in $\mathbb{R}^n$, proportional zu $d^{O(n)}$ (see [GV88], [Gri88], [Sol89], [HRS89b], [HRS89a], [HRS90], [Can88], [Ren88a], [Ren88b], [BPR94]). Diese Schranke wurde zum ersten Mal in [BGH+95] und [BGHM97] für den Hyperflächenfall, unter Berücksichtigung geometrischer Invarianten verbessert.

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ mit Gradschranke d, eine durch ein Straight–Line Programm β der Größe L und nichtskalaren Tiefe ℓ gegebene reduzierte reguläre Folge. Sei die reelle Varietät $V := V(f_1, \ldots, f_p) \cap \mathbb{R}^n$ nichtleer, beschränkt und $(f_1, \ldots, f_p)$–glatt, d.h. $J(f_1, \ldots, f_p)$ hat den maximalen Rang p in jedem Punkt von V (vgl. Definition 2). Dann läßt sich das Hauptergebnisse dieser Arbeit folgendermaßen formulieren:
Es gibt ein arithmetisches Netzwerk auf $\mathbb{Q}$, mit der Größe $\binom{n}{p-1} L(nd\delta\,')^{O(1)}$, welches startend mit β ein Straight–Line Programm erzeugt, das mindestens einen repräsentativen Punkt in jeder Zusammenhangskomponente von V kodiert. Die Invariante $\delta\,'$ ist das Maximum aller geometrischen Grade der im Verfahren erzeugten polaren Varietäten, die zu $f_1, \ldots, f_p$ assoziiert sind.

Die Größe des Netzwerks $\binom{n}{p-1} L(nd\delta\,')^{O(1)}$ beinhaltet den maximalen geometrischen Grad $\delta\,'$ gewisser zum polynomialen System $f_1, \ldots, f_p$ assoziierten *komplexen* polaren Varietäten, (vgl. [Hei83], [GHM+98], und [GHH+97]). Die Kombinatorische Zahl $p\binom{n}{p-1} < n\binom{n}{p-1}$ drückt die verschiedenen Möglichkeiten zur Wahl eines $(p-1)$–Minores m der Jacobimatrix $J(f_1, \ldots, f_p)$ aus, der eine lokal Beschreibung der Determinantenvarietät W_{n-p} ermöglicht.

Die Antwort auf das algorithmische Problem ist hiermit vollständig gegeben. Was die Größe des Netzwerks angeht, so ist das nicht der Fall, da diese Größe, außer n, d, und L noch die Invariante $\delta\ '$ beinhaltet, die nicht nur die reellen, sondern auch die komplexen Lösungen reflektiert. Im Fall einer Hyperfläche kann man eine Schranke angeben, die polynomial bezüglich eines geeignet definierten *reellen* Grades der assoziierten polaren Varietäten ist, und somit die reellen Lösungen reflektiert. Das ist der Inhalt eines weiteren Komplexitätsergebnisses.

Diese Komplexitätsresultat ist mit zwei algorithmischen Voraussetzungen verknüpft, die sehr stark in der Theorie sind, aber keine Einschränkung der Allgemeinheit bedeuten. Wir setzen dazu voraus, daß eine Prozedur zur Faktorisierung univariater Polynome mit rationalen Koeffizienten vorhanden ist, die eine polynomiale Zeitkomplexität in einem bestimmten Sinn hat (z.B. die arithmetischen Operationen in $\mathbb{Q}$ werden mit einheitlichen Kosten gezählt). Wir setzen weiterhin voraus, daß wir mittels eines zeitpolynomialen Verfahrens Regionen lokalisieren können, in denen ein gegebenes multivariates Polynom *endlich viele* reelle Lösungen besitzt, wenn es solche Lösungen überhaupt gibt. Die zweite Prozedur läßt sich durch die folgende ersetzen, die zwar theoretisch, aber leicht formulierbar ist: Wir nehmen an, daß wir in polynomialer Zeit entscheiden können, ob ein multivariates polynomiales System eine reelle Nullstelle besitzt, ohne diese Nullstelle auszurechnen. Wir nennen ein Netzwerk *erweitert*, wenn es von den eben beschriebenen zwei Subroutinen Gebrauch macht.

Seien die Bezeichnungen und Voraussetzungen wie vorhin. Wir setzen weiterhin voraus, daß das Polynome f quadratfrei und eine reguläre Gleichung der nicht–leeren glatten und beschränkten reellen Varietät $V := V(f) \cap \mathbb{R}^n$ beschreibt. Sei f durch ein Straight–Line Programm β der Größe L gegeben. Dann existiert ein erweitertes arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$, welches die Größe $L(nd\delta^*)^{O(1)}$ hat, und ein Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_n]$ erzeugt, welches mindestens einen repräsentativen Punkt in jeder Zusammenhangskomponente von V kodiert. Die Größe dieses Straight–Line Programms ist $L(nd\delta^*)^{O(1)}$, wobei δ^* der geeignet definierte, maximale reelle Grad gewisser zu f assozierter polarer Varietäten ist.

Vergleichbare Komplexitätsergebnisse wurden ausgehend von den Arbeiten [SS93a], [SS93b], [SS93c], [SS96] (siehe auch [Ded97], [Ded95]), vom numerischen Standpunkt zur Lösung polynomialer Gleichungssysteme in [SS94] erzielt. Der Fall der dünnen Besetzheit ist in [CE95] und [Emi96] geschildert. Wir verweisen auf [Par95] und [GHH$^+$97] und die dort zitierte Literatur für einen Vergleich zwischen den drei Modellen.

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ durch ein Straigth–Line Programm gegeben, welches den Platzbedarf $\mathcal{S}$ und die Zeitkomplexität $\mathcal{T}$ hat.

Unter Berücksichtigung der neuen Resultate in [HMW99] und in [GLS99] kann man einen Algorithmus mit Platzbedarf

$$\binom{n}{p-1} O(\mathcal{S}dn(\delta\,')^2) \tag{1.17}$$

und Zeitkomplexität

$$\binom{n}{p-1} O((\mathcal{T}dn^2 + n^5)(\delta\,')^3 \log^3(\delta\,') \log^2 \log(\delta\,')) \tag{1.18}$$

aufbauen, welcher eine geometrische Lösung der algebraischen Varietät

$$V(f_1, \ldots, f_p) \cap \mathbb{R}^n$$

liefert. Die während des Algorithmus entstehenden Polynome werde mit einem Vorgang der Spezialisierung freier Variablen gespeichert (vgl. [GLS99]).

Da in den relevanten praktischen Fällen der geometrische Grad $\delta\,'$ größer als $\mathcal{S}$, $\mathcal{T}$ und n ist, besitzt das neue Verfahren einen quadratischen Raumbedarf und eine kubische Zeitkomplexität.

Unter den Name „*Kronecker* "(vgl. [GLS99]) wird von *Grégoire Lecerf* im Laboratorium GAGE der École Polytechnique, Paris–Palaiseau unter Leitung von *Marc Giusti* ein geometrischer, Gröbner– Basis–freier Lösungsalgorithmus mit dieser Komplexität entwickelt. Der Prototyp läuft unter *MAGMA* $2.4-6$.

Der Aufbau von reduzierten transvervalen Folgen im Vorsschritt unseres Lösungsalgorithmus setzt voraus, daß die Variablen $X_1, \ldots, X_n$ in generischer Position sind. Seien $X = (X_1, \ldots, X_n)$ und $Y = (Y_1, \ldots, Y_n)$ Vektoren von Variablen. Wir beschreiben für den Fall einer Hyperfläche, ein Verfahren, welches den Parametervektor $z \in \mathbb{Q}^{\frac{n(n-1)}{2}}$ außerhalb einer gewissen Diskriminante Ω in $\mathbb{C}^{\frac{n(n-1)}{2}}$ bestimmt, so daß die neuen Variablen $Y_1, \ldots, Y_n$ nach dem Koordinatenwechsel $X = A(z)Y$ eine transversale Folge

$$f^{A(z)}, \frac{\partial f^{A(z)}}{\partial Y_1}, \ldots, \frac{\partial f^{A(z)}}{\partial Y_{n-1}} \tag{1.19}$$

bilden, dabei ist $f^{A(z)}(y) := f(A(z)(y)) = f(x)$. Die Diskriminante läßt sich lokal durch eine Hyperfläche beschreiben, und die Wahl des Vektors $z \in \mathbb{Q}^{\frac{n(n-1)}{2}}$ muß außerhalb dieser Hyperfläche erfolgen. Man erhält dann das Ergebnis:

Seien n, d, D, L nichtnegative ganze Zahlen. Sei ein nichtkonstantes quadratfreies Polynom $f \in \mathbb{Q}[X_1, \ldots, X_n]$ vom Grad $d \geq 2$ durch ein Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe L und nichtskalaren Tiefe ℓ gegeben. Dann gibt es ein arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$, welches die Größe $(ndDL)^{O(1)}$ und die nichtskalaren Tiefe $O(n(log(dD) + \ell))$ hat, und aus β, ein Netzwerk erzeugt, das *eine durch ihre Koeffizienten gegebene reguläre Matrix $A(z)$ generiert. Die Variablen $(X_1, \ldots, X_n)$ werden mit der Transformation $X = A(z)Y$ in die neuen Variablen $(Y_1, \ldots, Y_n)$ überführt, so daß die Folge*

$$f^{A(z)}, \frac{\partial f^{A(z)}}{\partial Y_1}, \ldots, \frac{\partial f^{A(z)}}{\partial Y_{n-1}} \tag{1.20}$$

eine reduzierte transversale Folge ist.
Zur Noether–Normalisierung verweisen wir auf [Mor97], [GHH$^+$97], [KP96]. Eine Realisierung in *Maple* der Noether–Normalisierung wurde zum ersten Mal in [GHL$^+$98] unter einem Noether–Paket zur Berechnung der Dimension einer projektiven Varietät veröffentlicht. Hieraus folgte die Implementierung in *Magma* vom Prototyp „*Kronecker*“(siehe [GLS99]).

Die vorliegende Arbeit ist in fünf Kapitel unterteilt. Das erste Kapitel ist diese Einführung und faßt die erzielten Hauptergebnisse zusammen. Im zweiten Kapitel präzisieren wir den Begriff des Algorithmus und beschreiben das Rechenmodell. In diesem Kapitel werden die Grundbegriffe zusammengefaßt, welche zum Aufbau unseres Verfahrens von Bedeutung sein werden. Anhand der Arbeiten [GHMP95] und [GHH$^+$97] erörtern wir, was wir unter einer geometrischen Lösung, einer (simultanen) Noether–Normalisierung, einem Lifting–Punkt sowie einer Lifting–Faser verstehen. Das dritte Kapitel basiert auf dem in [BGH$^+$95], [BGHM97] veröffentlichten Algorithmen zur Auffindung reeller Punkte in jeder Zusammenhangskomponente einer reellen beschränkten glatten Hyperfläche. Das vierte Kapitel behandelt den Fall eines vollständigen Durchschnittes und ist eine Verallgemeinerung des Hyperflächenfalls. Im letzten fünften Kapitel geben wir eine effiziente Methode zur Darstellung der Koordinaten in generischer Position. Dieses Verfahren läßt sich auch für den Fall eines vollständigen Durchschnittes anwenden.

Kapitel 2

Zeitpolynomiale Algorithmen zur geometrischen Lösung

In diesem Kapitel sollen die in den letzten 5 Jahren entwickelten Algorithmen ([GHMP95], [GHM+98], [GHH+97]) zur geometrischen Lösung affiner algebraischer Varietäten in ihren Grundzügen beschrieben werden, welche wir bei den zu entwickenden Methoden für das Auffinden *reeller Lösungen* algebraischer Gleichungen systematisch anwenden.

Ein Merkmal von zentraler Bedeutung für diese Algorithmen ist der konsequente Gebrauch *problemangepaßter Datenstrukturen*, nämlich *arithmetische Netzwerke* und *Straight–Line Programme.*
Die Zeitkomplexität dieser Algorithmen hängt polynomial von der *Länge* des Inputs (gegeben durch ein Straight–Line Programm) und einer *wesentlichen geometrischen Invarianten*, dem adäquat definierten *geometrischen Grad des Gleichungssystems* ab.

Auf die Beweise der Sätze, die die Algorithmen begründen, verzichten wir, da sie u.a. in den Arbeiten [GHM+98], [GHH+97] und [Mor97] zu finden sind. Die Darstellung in diesem Kapitel folgt im wesentlichen der Beschreibung der Sachverhalte in [Mor97] und [GS99].

Im Hinblick auf die Anwendung auf das reelle Lösen algebraischer Gleichungen können wir uns auf Polynome mit rationalen Koeffizienten beschränken.

2.1 Bezeichnungen und Grundbegriffe

Mit $\mathbb{N}$ und $\mathbb{Z}$ werden die Mengen der natürlichen und ganzen Zahlen bezeichnet. Die Symbole $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ stehen für die Körper der rationalen, reellen und komplexen Zahlen. Die affinen Räume über diesen Körpern werden entsprechend mit $\mathbb{Q}^n, \mathbb{R}^n$ und $\mathbb{C}^n$ bezeichnet. Den Raum $\mathbb{C}^n$ versehen wir mit der $\mathbb{Q}-$Zariski–Topologie, in welcher abgeschlossene Mengen die gemeinsamen Nullstellen endlicher polynomialer Systeme mit rationalen Koeffizienten sind. Sei $W \subset \mathbb{C}^n$ eine abgeschlossene Menge bezüglich dieser Topologie und $W = C_1 \cup \ldots \cup C_s$ ihre Zerlegung in irreduzible Komponenten bezüglich dieser Topologie. Die Mengen $W, C_1, \ldots, C_s$ sind dann $\mathbb{Q}-$definierbare algebraische Teilmengen von $\mathbb{C}^n$.

Wir betrachten einige spezifische geometrische Invariante der Varietät W. Dann bezeichnen wir mit $\dim C$ die *Krull–Dimension* des Koordinatenringes einer irreduziblen Komponente $C = C_k$, von W, für ein k, $1 \leq k \leq s$. Der Grad von C, den wir mit $\deg C$ bezeichnen, ist die Anzahl der Schnitte von C mit $\dim C$ vielen generischen affinen Hyperebene in $\mathbb{C}^n$. Wir definieren nun die Dimension der Varietät W durch

$$\dim W := \max\{\dim C_k \mid 1 \leq k \leq s\} \tag{2.1}$$

Man nennt die abgeschlossene Menge W äquidimensional, falls alle ihre irreduziblen Komponenten $C_1, \ldots, C_s$ von der gleichen Dimension sind.

Der geometrische Grad von W ist durch

$$\deg W := \sum_{k=1}^{s} \deg C_k \tag{2.2}$$

definiert. Dieser ehe unkonventionelle Begriff des Grades erfüllt die *Bézout–Ungleichung* und ist unabhängig vom Typ des Durchschnittes, den in W auftritt (vgl. [Hei83]).

Sei ein System $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ gegeben. Unter dem *geometrischen Grad dieses Systems* verstehen wir das Maximum aller geometrischen Grade der Varietäten $V(f_1, \ldots, f_i)$, $1 \leq i \leq p$.

Variable (Unbestimmte) bezeichnen wir mit $X_1, \ldots, X_n$ bzw. $Y_1, \ldots, Y_n$. Seien von nun an die Zahlen $p \leq n \in \mathbb{N}$ beliebig fixiert.

Definition 1
Eine Folge $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ heißt eine reguläre Folge *in $\mathbb{Q}[X_1, \ldots, X_n]$, wenn die folgenden Bedingungen erfüllt sind:*

- $(f_1, \ldots, f_p)\mathbb{Q}[X_1, \ldots, X_n] \neq \mathbb{Q}[X_1, \ldots, X_n]$;
- *für jeden Index i, $2 \leq i \leq n$, ist das Bild von f_i im Faktorring*

$$B_{i-1} := \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_{i-1})$$

kein Nullteiler.

Mit dieser Definition ist die Homothetie $\eta_{f_i} : B_{i-1} \to B_{i-1}$, $h \mapsto f_i h$, welche eine Restklasse $h \in B_{i-1}$ der Restklasse $f_i h$ in B_{i-1} zuordnet eine injektive Abbildung.
Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$, $1 \leq p \leq n$, mit beschränktem Grad $\deg f_k \leq d$, $d \geq 2$, $\forall k$, $1 \leq k \leq p$. Wir setzen voraus, daß die Folge

$f_1, \ldots, f_p$ eine reguläre Folge in $\mathbb{Q}[X_1, \ldots, X_n]$ ist, und daß das von den Polynomen $f_1, \ldots, f_i,\ 1 \leq i \leq p$ erzeugte Ideal $(f_1, \ldots, f_i)$ radikal ist. Dieses Ideal läßt sich folgendermaßen beschreiben:

$$(f_1, \ldots, f_i) = \sqrt{(f_1, \ldots, f_i)} := \{f \in \mathbb{Q}[X_1, \ldots, X_n] |\ \exists s \in \mathbb{N}, f^s \in (f_1, \ldots, f_i)\}.$$

Aus dem Hilbert'schen Nullstellensatz erhalten wir die Gleichung $(f_1, \ldots, f_i) =$

$$= I(V((f_1, \ldots, f_i))) := \{f \in \mathbb{Q}[X_1, \ldots, X_n] |\ f(x) = 0\ \forall x \in V((f_1, \ldots, f_i))\}$$

Mit $X := (X_1, \ldots, X_n)$ wird der Variablenvektor und $x := (x_1, \ldots, x_n) \in \mathbb{C}^n$ ein Punkt im affinen Raum $\mathbb{C}^n$ bezeichnet.

sei $V(f_1, \ldots, f_p)$ die von den gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_p$ definierte affine Varietät, d.h.

$$V(f_1, \ldots, f_p) := \{x \in \mathbb{C}^n | f_1(x) = \ldots = f_p(x) = 0\}.$$

Die entsprechende Jacobimatrix ist durch

$$J(f_1, \ldots, f_p) := \left(\frac{\partial f_k}{\partial X_j}\right)_{\substack{1 \leq k \leq p \\ 1 \leq j \leq n}}$$

gegeben und

$$J(f_1, \ldots, f_p)(\tilde{x}) := \left(\frac{\partial f_k}{\partial X_j}(\tilde{x})\right)_{\substack{1 \leq k \leq p \\ 1 \leq j \leq n}}$$

bezeichnet die Jacobimatrix an der Stelle $\tilde{x} \in \mathbb{C}^n$.

Definition 2
Sei der Index $i,\ 1 \leq i \leq p$ beliebig aber fest. Ein Punkt $\tilde{x} \in V(f_1, \ldots, f_i)$ heißt $(f_1, \ldots, f_i)-$glatt, falls die Jacobimatrix $J(f_1, \ldots, f_i)(\tilde{x})$ maximalen Rang hat, d.h. die durch die Polynome $f_1, \ldots, f_i$ beschriebenen Hyperflächen schneiden sich in $\tilde{x}$ transversal.

Falls keine Mißverstänisse entstehen, wird ein $(f_1, \ldots, f_i)-$glatter Punkt einfachheitshalber nur glatt genannt.

Bemerkung 1
Die Definition eines glatten Punktes *einer Komponente C_r ist folgendermaßen zu interpretieren: Ein Punkt ist glatt in C_r, wenn der Tangentialraum von C_r in diesem Punkt die Dimension $(n - i)$ hat, oder, genauer gesagt, wenn die durch die Polynome $f_1, \ldots, f_i$ beschriebenen Hyperflächen sich in diesem Punkt in $\mathbb{C}^n$ transversal schneiden.*

Definition 3
Ein System von Polynomen $f_1, \ldots, f_i \in \mathbb{Q}[X_1, \ldots, X_n],\ i \leq n$ heißt ein reguläres Gleichungssystem der algebraische Menge $V(f_1, \ldots, f_i) \cap \mathbb{R}^n$, wenn der Jacobimatrix $J(f_1, \ldots, f_i)(x)$ maximaler Rang in jedem Punkt in $V(f_1, \ldots, f_i) \cap \mathbb{R}^n$ hat.

2.2 Geometrische Lösung eines affinen vollständigen Durchschnittes

Zunächst soll die Definition einer geometrischen Lösung einer affinen, äquidimensionalen Varietät in Erinnerung gerufen werden. Es sei hier bemerkt, daß der Begriff der geometrischen Lösung eine lange Geschichte hat. Bei Komplexitätsüberlegungen wurde er wohl zuerst in [CG83] und [GM89] benutzt, doch geht die Definition mindestens auf Kronecker zurück, (vgl. [Kro82]).

Im Hinblick auf die Betrachtung von Varietäten, die einen vollständigen Durchschnitt darstellen, können wir uns darauf beschränken, daß die Polynome $f_1, \dots, f_p$, die die Varietät $V(f_1, \dots, f_p)$ beschreiben, eine reguläre Folge in $\mathbb{Q}[X_1, \dots, X_n]$ bilden und die Dimension von $V(f_1, \dots, f_p)$ daher $r := n - p$ ist.

Man sagt, daß die Variablen $X_1, \dots, X_r$ in *Noether–Position bezüglich* V sind, falls die Abbildung $\mathbb{Q}[X_1, \dots, X_r] \to \mathbb{Q}[X_1, \dots, X_n]/(f_1, \dots, f_p)$ injektiv ist und eine ganze Ringerweiterung beschreibt. Vom geometrischen Standpunkt heißt das, daß die Projektion $\pi_p : V \longrightarrow \mathbb{C}^r$ auf die ersten r Variablen $X_1, \dots, X_r$, die *freien* Variablen , surjektiv und endlich ist. Die Variablen $X_{r+1}, \dots, X_n$ werden *abhängig* genannt.

Eine Folge $f_1, \dots, f_p$ wird *reduziert* genannt, falls es einen linearen Koordinatenwechsel $(X_1, \dots, X_n) \mapsto (Y_1, \dots, Y_n)$ gibt, so daß für jedes i, $1 \le i \le p$, die Variablen $Y_1, \dots, Y_{n-i}$ in Noether–Position bezüglich der Varietät $V(f_1, \dots, f_i)$ sind, und die Determinante der Jacobimatrix $J(f_1, \dots, f_i)$ kein Nullteiler modulo $(f_1, \dots, f_i)$ ist.

Die Reduziertheit einer regulären Folge $f_1, \dots, f_p$ in $\mathbb{Q}[X_1, \dots, X_n]$ ist äquivalent zu der Forderung, daß alle *Zwischenideale* $(f_1, \dots, f_i)$, $1 \le i \le p$, radikal sind.

Für lokale Betrachtungen, d.h. außerhalb einer Hyperfläche in $\mathbb{C}^n$, wollen wir die folgende Definition treffen.

Definition 4 (Transversale Folge (suite sécante))
Sei $V(g) := \{x \in \mathbb{C}^n | g(x) = 0\}$ eine Hyperfläche in $\mathbb{C}^n$, die durch ein Polynom $g \in \mathbb{Q}[X_1, \dots, X_n]$ definiert ist. Wir nennen eine reduzierte Folge $f_1, \dots, f_p$ in $\mathbb{Q}[X_1, \dots, X_n]$ eine transversale Folge (suite sécante) außerhalb von $V(g)$*, falls für jedes i, $1 \le i \le p$, alle irreduziblen Komponenten der affinen Varietät $V(f_1, \dots, f_i)$, welche nicht vollständig in der Hyperfläche $V(g)$ enthalten sind, die Dimension $n-i$ haben.*

Wir werden auch hier annehmen, daß die Folge $f_1, \dots, f_p$ regulär ist, obwohl die resultierenden Cohen–Macaulay–Eigenschaften für unsere Überlegungen nicht entscheidend sind.

Geometrisch beinhaltet die Definition einer transversalen Folge dann, daß sich für jedes i, $1 \le i \le p$ die Hyperflächen $V(f_1), \dots, V(f_i)$ außerhalb der Hyperfläche

$V(g)$ transversal schneiden, oder anders gesagt, die Polynome $f_1, \ldots, f_i$ definieren für jedes i, $1 \leq i \leq p$, außerhalb von $V(g)$ einen reduzierten lokalen vollständigen Durchschnitt der Kodimension i.

Unter diesen Begriffsbildungen und Voraussetzungen besteht eine geometrische Lösung in folgendem:

- Einem linearer Koordinatenwechsel $(X_1, \ldots, X_n) \mapsto (Y_1, \ldots, Y_n)$ derart, daß die Polynome in Noether–Position bezüglich der neuen Variablen sind.

- Einer Linearform $U = \lambda_{r+1}X_{r+1} + \ldots + \lambda_n X_n$ mit Koeffizienten $\lambda_{r+1}, \ldots, \lambda_n$ in $\mathbb{Z}$, welche ein *primitives* Element u von

$$\mathbb{Q}[Y_1, \ldots, Y_r] \to \mathbb{Q}[Y_1, \ldots, Y_n]/(f_1, \ldots, f_p)$$

  mit einem Minimalpolynom $q_u \in \mathbb{Z}[U]$ erzeugt. Im null-dimensionalen Fall ist u dann und nur dann ein primitives Element, wenn $U(P) \neq U(Q)$ für alle verschiedenen Punkte P und Q von V gilt. Mit dieser Eigenschaft heißt u *separierend*. Der Grad von q_u ist gleich dem Rang von $\mathbb{Q}[Y_1, \ldots, Y_n]/(f_1, \ldots, f_p)$ als freier $\mathbb{Q}[Y_1, \ldots, Y_r]$–Modul.

- Einer Menge von Parametrisierungen $\rho_i y_i - v_i(u)$ für $i = r+1, \ldots, n$, wobei ρ_i bzw. $v_i(u)$ Polynome in $\mathbb{Z}[Y_1, \ldots, Y_r]$ bzw. $\mathbb{Z}[Y_1, \ldots, Y_r][U]$ sind. Sie hängen von der Wahl von u ab. Mit $\rho = \Pi\rho_i$ ist die Menge der Punkte x von V außerhalb von $\rho^{-1}(0)$ durch $q_u(u) = 0, \rho_i y_i - v_i(u) = 0$ gegeben.

Dieses so definierte Objekt, *geometrische Lösung*, ist unseren Bedürfnissen wohl angepaßt. Das Minimalpolynom q_u des primitiven Elements ist unser fragliches Eliminationsobjekt.

In einem Punkt v, der keine Nullstelle dieses Polynoms ist, liefert die Parametrisierung die Werte der gebundenen Variablen. Grob gesagt,bedeutet das: wenn man annimmt, daß sich v auf einem Wege außerhalb der Diskriminantenvarietät $\rho^{-1}(0)$ einem v_0 mit $q_u(v_0) = 0$ annähert, so nähern sich die Werte der Parametrisierung den Koordinaten der Lösung v_0 an. Diese Werte lassen sich dann als Approximationen einer gewissen Lösung ansehen.

Eine geometrische Lösung läßt sich vermöge eines Gröbner–Basis–Algorithmus berechnen (den Zusammenhang liefert das sogenannte Shape Lemma), jedoch die Methode, welche in den Arbeiten [GH93], [KP96], [GHMP95], [GHM$^+$98], [GHH$^+$97] entwickelt wurde, liefert weitaus effektivere Algorithmen zur Berechnung einer geometrischen Lösung.

Die dieser Methode zugrunde liegende Idee besteht darin, anstelle der üblichen Rewriting–Verfahren einem iterativen Schnitt–Prozeß zu folgen. Die entsprechenden Algorithmen haben eine Zeitkomplexität, die sowohl in der *Berechnungskomplexität* der Input–Polynome als auch in *wesentlichen geometrischen Invarianten* der durch die Input–Polynome definierten Varietät polynomial ist.

Wir beschreiben jetzt die Merkmale dieser Algorithmen.

2.3 Kodierung der Polynome

Wenn Polynome „gute Berechnungseigenschaften“ besitzen, so kann man auch relativ leicht eine geometrische Lösung finden. Was damit gemeint sein soll, zeigt das folgende Beispiel.

Die Determinante einer quadratischen Matrix $A = [a_{ij}]$ der Ordnung n ist nach der Leibniz–Formel ein Polynom in den Elementen a_{ij} mit $n!$ Monomen. Jedoch, gibt es Polynomialzeitalgorithmen, welche den Wert der Determinante für eine beliebige Wahl der a_{ij} berechnen, ohne die Entwicklungsformel zu benutzen. Die Determinante als Polynom besitzt, so sagt man, *gute Berechnungseigenschaften.*

Der entscheidende Punkt besteht darin, ein Polynom als *Funktion* von $\mathbb{C}^n$ nach $\mathbb{C}$ anzusehen, anstatt es als ein Element des Vektorraumes $\mathbb{C}[X_1, \ldots, X_n]$ zu betrachten.
Vom praktischen Standpunkt bedeutet das, ein Polynom nicht als Liste seiner Koeffizienten gemäß der Monombasis in $\mathbb{C}[X_1, \ldots, X_n]$ zu speichern sondern als eine Funktion mittels eines Auswertungsverfahrens. Als solche werden *Straight-Line Programme* benutzt. Grob gesagt, berechnet ein Straight-Line Programm Werte von Polynomen in beliebigen Punkten eines Grundraumes, d.h. einer Potenz eines effektiven Körpers, z.B. in Punkten aus $\mathbb{Q}^n$.

Wir geben die Definitionen sowie kurze Beschreibungen von einem arithmetischen Netzwerk und einem Straight-Line Programm an.

Definition 5 (Arithmetisches Netzwerk)
Ein gerichteter azyklischer Graph mit ausschließlich arithmetischen und booleschen Operationen sowie Auswahlen auf Grund von Tests auf Gleichheit mit Null (ggf auch Positivitätstests) an inneren Knoten sowie Ein– und Ausgängen (Input/Output) in einem effektiven Körper (z.B. $\mathbb{Q}$) an externen Knoten wird ein arithmetisches Netzwerk *genannt.*

Eine besondere Rolle spielen solche arithmetischen Netzwerke, die weder Verzweigungen noch Divisionen aufweisen, d.h. an internen Knoten werden nur Additionen und Multiplikationen ausgeführt. Derartige Netzwerke sind gut geeignet zur Kodierung von Polynomen.

Definition 6 (Straight-Line Programm (SLP))
Ein Straight-Line Programm *ist eine Computer–Prozedur, welche die Werte eines arithmetischen Netzwerkes ohne Verzweigungen und Divisionen berechnet.*

Der Übergang von einem arithmetischen Netzwerk ohne Verzweigungen und Divisionen zu einem Straight-Line Programm ist einer Kompilation ähnlich. Auf Einzelheiten soll hier jedoch nicht eingegangen werden.

Der Umfang eines Straight-Line Programms wird in zwei Größen gemessen: seiner *Länge* L und seiner *nicht–skalaren Tiefe* ℓ. Die Länge ist nichts weiter als die Anzahl der Knoten, und die nicht–skalare Tiefe bezeichnet die Länge des längsten Weges im Graphen, wobei nur nicht–skalare Operationen gezählt werden.

Unter nicht–skalaren Operationen versteht man Multiplikationen von Polynomen positiven Grades. Lineare arithmetische Operationen haben auf die nicht–skalare Tiefe keinen Einfluß.

Während die Länge die sequentielle Berechnungszeit des SLP bestimmt, ist die nicht–skalare Tiefe eine wesentliche Größe für die Abschätzungen von Graden und Höhen, d.h. für die Bitkomplexität, und sie bestimmt andererseits auch die parallele Berechnungszeit des SLP.

Da man SLPs als Funktionen ansehen kann, lassen sich die üblichen Operationen der Addition, Multiplikation und Zusammensetzung von Polynomen leicht durch SLPs ausführen. Bei anderen Operationen ist das weniger offensichtlich.

Eine natürliche Frage ist die nach dem Test, ob eine Größe gleich Null ist, d.h. Gleichheitstest. Wenn z.B. zwei SLPs auf einer hinreichend großen Menge von Punkten dieselben Werte berechnen, so kodieren sie die gleichen Polynome. Dieses Faktum läßt sich im Begriff der *korrekten Testfolgen* formalisieren.

Definition 7 (Korrekte Testfolge)
Sei $W(n, D, L)$ eine Menge von Polynomen aus $\mathbb{Q}[X_1, \ldots, X_n]$ von einem Grade höchstens D, die sich durch ein Straight-Line Programm mit einer Länge höchstens L kodieren lassen. Eine Menge von Punkten $G = \{\gamma_1, \ldots, \gamma_m\}$ in $(\mathbb{Q}^n)^m$ heißt eine korrekte Testfolge *für $W(n, D, L)$ falls jedes Polynom, welches auf G verschwindet, identisch Null ist.*

Der Grad D der Polynome in $W(n, D, L)$ in vorstehender Definition ist beschränkt durch 2^ℓ, wobei ℓ die nicht–skalare Tiefe des SLP ist:

$$D \leq 2^\ell \leq 2^L \tag{2.3}$$

Der folgende Satz gibt eine Schranke für die Anzahl korrekter Testfolgen in einer gegebenen Menge aus $\mathbb{Q}^n$ (vgl. [HS82]).

Satz 8 (Heintz-Schnorr)
Sei Γ eine Teilmenge von $\mathbb{Q}$ mit $2L(D+1)^2$ Elementen, und sei $m = 6(L+n)(L+n+1)$. Die Anzahl τ von Teilmengen korrekter Testfolgen in $(\Gamma^n)^m$ genügt der folgenden Ungleichung

$$\tau \geq |\Gamma|^{nm}(1 - |\Gamma|^{-\frac{m}{6}}).$$

Dieser Satz besagt, daß die Wahrscheinlichkeit dafür, daß eine Folge in Γ^{nm} keine korrekte Testfolge ist, kleiner als 1/262144 ist.

Die nächste Behauptung drückt die Existenz einer korrekten Testfolge für $\mathcal{W}(n, L, \ell)$ aus, die eine angemessene Länge besitzt [KP96], [GHH+97].

Behauptung 9 (Krick-Pardo) *Seien natürliche Zahlen n, L, ℓ, mit $L \geq n+1$ gegeben.*
Seien $r := (2^{\ell+1}-2)(2^{\ell}+1)^2$ und $t := 6(\ell L)^2$ definiert.
Dann enthält die endliche Menge $\{1, \ldots, r\}^{nt} \subset \mathbb{Z}^{nt}$ mindestens $r^{nt}(1-r^{-t/6})$ korrekte Testfolgen der Länge t für $\mathcal{W}(n, L, \ell)$. Insbesondere ist die Menge der korrekten Testfolgen für $\mathcal{W}(n, L, \ell)$ mit der Länge t, die nur Punkte aus $\{1, \ldots, r\}^n$ enthalten, nicht–leer.

Es ist kein deterministischer Algorithmus bekannt, der korrekte Testfolgen in einer Zeit finden kann, die polynomial in (n, D, L) ist. Die Algorithmen dieser Arbeit benutzen Nulltests und werden daher von nichtuniformer Komplexität sein, für die man vorbestimmte korrekte Testfolgen benötigt. Mit anderen Worten, wir werden es mit probabilistischen Algorithmen zu tun haben, die zufällig gewählte korrekte Testfolgen benutzen.

2.4 Der geometrische Lösungsalgorithmus

Wir rekapitulieren einen Satz von *Giusti, Heintz, Morais, Morgenstern, Pardo* (1995) [GHM+98], der einen Algorithmus zur lokalen geometrischen Lösung charakterisiert und dessen Zeitkomplexität ein Polynom in der Länge der SLP–Kodierung des Input–Gleichungssystems und seines (affinen) geometrischen Grades ist.

Satz 10 ([GHM+98])
Seien $f_1, \ldots, f_p$ eine reguläre Folge und g ein weiteres Polynom in $\mathbb{Q}[X_1, \ldots, X_n]$ mit der Eigenschaft, daß $f_1, \ldots, f_p$ eine reduzierte transversale Folge außerhalb der Hyperfläche $V(g)$ bilden. Ferner sei d eine Gradschranke der Polynome. Die Polynome $f_1, \ldots, f_p, g$ seien durch ein Straight–Line Programm der Länge L und der nicht–skalaren Tiefe ℓ gegeben. Ferner sei mit δ der geometrische Grad des Gleichungssystems $f_1 = \ldots = f_p = 0$ bezeichnet.
Dann gibt es ein arithmetisches Netzwerk, welches eine geometrische Lösung derjenigen affinen Varietät berechnet, die durch den Zariski–Abschluß

$$\overline{V(f_1, \ldots, f_p) \setminus V(g)}$$

darstellbar ist. Die Zeitkomplexität der Berechnung ist $L(nd\delta)^{O(1)}$.

Bemerkung 2 (Bemerkungen zum Algorithmus)

- *Der Algorithmus berechnet sukzessiv geometrische Lösungen der Varietäten $V(f_1, \ldots, f_i)$, $1 \leq i \leq p$, außerhalb der Hyperfläche $V(g)$.*

- *Der Algorithmus arbeitet mit vorher bestimmten korrekten Testfolgen.*
- *In jedem Schritt läßt sich testen, ob das System reduziert ist. Daher wird kein falsches Ergebnis ausgegeben, falls das nicht der Fall ist.*
- *Für die lokale Berechnung außerhalb einer Hyperfläche kann der affine Grad kleiner sein als δ, (Komponenten im Unendlichen beeinflussen nicht die Komplexität der affinen Lösung).*
- *Die Output Polynome, welche die geometrischen Lösungen beschreiben, sind durch ein Straight-Line Programm gegeben.*
- *Im Fall $p = n$ läßt sich der Algorithmus gemäß [HMW99] effektiver gestalten und es lassen sich explizite Schranken angeben.*

Um den induktiven Schritt des Algorithmus zu erklären, benötigen wir noch den Begriff des *Lifting–Punktes* für $V(f_1, \ldots, f_i)$ Mit seiner Hilfe wird der Übergang von einer geometrischen Lösung einer null-dimensionalen Varietät zu einer von einer Varietät positiver Dimension vorgenommen. Wir beschränken uns hier auf den globalen Fall; für den lokalen Fall (d.h. außerhalb einer Hyperfläche) erhält man analoge Sachverhalte.

Auf Grund der Voraussetzungen sind die Zwischenvarietäten $V(f_1, \ldots, f_i)$, $1 \leq i \leq p$ alle vollständige Durchschnitte außerhalb von $V(g)$, und der Algorithmus berechnet für jede der Varietäten $V(f_1, \ldots, f_i)$ eine geometrische Lösung.

Wir nehmen an, daß wir im Schritt i angelangt sind, eine geometrische Lösung der Varietät V_{i-1} vorliegt, und daß die Variablen bezüglich $V(f_1, \ldots, f_i)$ in Noether–Position sind.
Sei $\pi_i \ : V(f_1, \ldots, f_i) \rightarrow \ \mathbb{C}^{n-i}$ die Projektion auf die ersten $n - i$ (die freien) Koordinaten. Ein Punkt $P_i \in \mathbb{Q}^{n-i}$ wird *Lifting–Punkt* für $V(f_1, \ldots, f_i)$ bezüglich der Projektion π_i genannt, falls

- die 0–dimensionale Faser $V_{P_i} := \pi_i^{-1}(P_i)$ genau D_i Punkte enthält, wobei die Größe $D_i :=$ Rang $\ \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_i)$ definiert ist, und
- diese alle $(f_1, \ldots, f_i)$–glatte Punkte von $V(f_1, \ldots, f_i)$ sind.

Die Faser V_{P_i} wird *Lifting–Faser* für $V(f_1, \ldots, f_i)$ genannt.

Die Bedingung, daß alle Punkte der Lifting–Faser V_{P_i} glatt sind, bedeutet, daß die Jacobimatrix (bezüglich der gebundenen Variablen) der Polynome $f_1, \ldots, f_i$ in allen Punkten der Faser V_{P_i} regulär ist. Das ist äquivalent dazu, daß das absolute Glied des charakteristischen Polynoms der Homothetie, welche durch diese Jacobimatrix in $\mathbb{Q}[V(f_1, \ldots, f_i)]$ definiert ist, in P_i nicht Null wird (vgl. z.B. [Mor97], Proposition 28]).

Lifting–Punkte haben die Eigenschaft, daß die Kenntnis der geometrischen Lösung von V_{P_i} ausreicht, um eine geometrische Lösung der ganzen Varietät $V(f_1, \ldots, f_i)$ zu gewinnen, was über eine kohärente Anwendung einer symbolischen Newton-Hensel Iteration erreicht wird. In diesem Kontext besteht der iterative Schritt des Algorithmus in folgenden zwei Teilen:

- Bestimme eine geometrische Lösung von $V(f_1, \ldots, f_i)$ ausgehend von P_i, die Noether–Normalisierung von $V(f_1, \ldots, f_i)$ und die geometrische Lösung der Faser V_{P_i}, dieser Teil benutzt eine symbolische Newton-Hensel Iteration.

- Bestimme eine Noether–Normalisierung von V_{i+1}, bestimme einen neuen Lifting–Punkt P_{i+1} und berechne eine geometrische Lösung der Faser $V_{P_{i+1}}$ zu diesem Punkt, was ein null-dimensionales Problem ist.

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ durch ein Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_n]$ gegeben, welches den Raumbedarf $\mathcal{S}$ und Zeitkomplexität $\mathcal{T}$ benötigt. Unter Berücksichtigung der neuen Resultaten in [HMW99] und die in [GLS99] ausgehende Implementierung können wir einen Algorithmus mit einer Raumkomplexität

$$\binom{n}{p-1} O(\mathcal{S} dn\delta^2)$$

und einer Zeitkomplexität

$$\binom{n}{p-1} O((\mathcal{T} dn^2 + n^5)\delta^3 \log^3 \delta \log^2 \log \delta)$$

aufbauen, welcher eine geometrische Lösung der algebraischen Varietät $V(f_1, \ldots, f_p)$ liefert. Da in den relevanten praktischen Fällen der geometrische Grad wesentlich größer als $\mathcal{S}$, $\mathcal{T}$ und n ist, besitzt das verbesserte Verfahren einen quadratischen Raumbedarf und eine kubische Zeitkomplexität.

Kapitel 3

Reelle Lösungen, der Hyperflächenfall

3.1 Polare Varietäten

Die Betrachtung gewisser polarer Varietäten einer gegebenen affinen Varietät bekannter Kodimension ermöglicht unter der Benutzung von Algorithmen im komplexen Bereich in [GHM+98], [GHH+97], den Aufbau eines induktiven Verfahrens zur Auffindung reeller Lösungen eines gegebenen Gleichungssystems, [BGH+95], [BGHM97]. Das Inkrement in diesem Verfahren wird die Kodimension der polaren Varietäten sein.

Lemma 11 (Hauptemma)
Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein nichtkonstantes und quadratfreies Polynom und sei $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ die Menge aller komplexen Nullstellen der Gleichung $f(x) = 0$. Wir betrachten für jeden festen Index $i, 0 \leq i < n$, die komplexe Varietät

$$\widetilde{W}_i := \left\{ x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0 \right\}.$$

(Unter $\widetilde{W}_0$ verstehen wir W.) Seien die Variablen generisch bezüglich des Polynoms f gewählt. Dann ist jeder Punkt in $\widetilde{W}_i$, der in W glatt ist, auch ein glatter Punkt von $\widetilde{W}_i$. In so einem Punkt hat die Jacobimatrix des Systems $f = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0$ einen maximalen Rang, und die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$, definierten Hyperflächen schneiden sich transversal in diesem Punkt.

Beweis:
Sei $i \in \mathbb{N}, 1 \leq i < n$, fest gewählt, und seien durch

$$Z_{i+1,1}, \ldots, Z_{n,1}, \ldots, Z_{i+1,i}, \ldots, Z_{n,i}$$

$(n-1)i$ Unbestimmte betrachtet, die wir in Matrixform

$$Z := \begin{pmatrix} Z_{i+1,1} & \dots & Z_{i+1,i} \\ \vdots & \dots & \vdots \\ Z_{n,1} & \dots & Z_{n,i} \end{pmatrix} \tag{3.1}$$

darstellen. Ferner erklären wir eine folgendermaßen strukturierte, reguläre Matrix

$$A^{(i)} := A^{(i)}(Z) := \begin{pmatrix} I_i & 0_{i,n-i} \\ Z & I_{n-i} \end{pmatrix}, \tag{3.2}$$

wobei I_k die entsprechende $k \times k$ Einheitsmatrix für $k = i, n-i$, und $0_{i,n-i}$ die $i \times (n-i)$ Nullmatrix ist. Wenn wir Z zu a spezialisieren, d.h.

$$a := \begin{pmatrix} a_{i+1,1} & \dots & a_{i+1,i} \\ \vdots & \dots & \vdots \\ a_{n,1} & \dots & a_{n,i} \end{pmatrix}, \tag{3.3}$$

so schreiben wir für die reguläre Matrix $A^{(i)}(a)$. Für einen festen Index $k \in \mathbb{N}, 1 \leq k \leq i < n$, definieren wir das Polynom

$$F_k := \frac{\partial f}{\partial X_k} + \sum_{j=i+1}^{n} Z_{jk} \frac{\partial f(x)}{\partial X_j} \in \mathbb{Q}[X, Z].$$

Die Jacobimatrix von $F_1, \dots, F_i$ bezüglich der Variablen Z sei mit

$$J_Z(F_k) = \left(\frac{\partial F_k}{\partial Z_{r,s}} \right)_{1 \leq k \leq i,\, i+1 \leq r \leq n,\, 1 \leq s \leq i}$$

bezeichnet und für ihre Einträge erhält man die Gleichheit

$$\frac{\partial F_k}{\partial Z_{r,s}} = \frac{\partial f}{\partial X_r}.$$

Wir betrachten die folgende Koordinatentransformation $X = A^{(i)}(a)Y$. Die Darstellung des Polynoms $f \in \mathbb{Q}[X_1, \dots, X_n]$ in den neuen Koordinaten $Y_1, \dots, Y_n$ ergibt ein neues Polynom $g(Y_1, \dots, Y_n) := f(A^{(i)}(a)Y)$. Damit läßt sich die Hyperfäche $W := \{x \in \mathbb{C}^n | \ f(x) = 0\}$ in den neuen Koordinaten $Y_1, \dots, Y_n$ ausdrücken: $W := \{y \in \mathbb{C}^n | \ f(A^{(i)}(a)y) = 0\}$.

Die durch $A^{(i)}(a)$ gegebene Koordinatentransformation induziert einen Morphismus affiner Räume $\Phi_i : \mathbb{C}^n \times \mathbb{C}^{(n-i)i} \longrightarrow \mathbb{C}^{i+1}$ definiert durch

$$\Phi_i(X_1, \dots, X_n, a) = \left(f, \frac{\partial f}{\partial X_1} + \sum_{j=i+1}^{n} a_{j1} \frac{\partial f}{\partial X_j}, \dots, \frac{\partial f}{\partial X_i} + \sum_{j=i+1}^{n} a_{ji} \frac{\partial f}{\partial X_j} \right).$$

Sei

$$\alpha := (\alpha_1, \ldots, \alpha_{n+(n-i)i}) := (X_1, \ldots, X_n, a_{i+1,1}, \ldots, a_{n,i}) \in \mathbb{C}^n \times \mathbb{C}^{(n-i)i}$$

gegeben. Dann hat die Jacobimatrix $J(\Phi_i)(\alpha)$ von Φ_i in α die folgende Gestalt:

$$J(\Phi_i)(\alpha) = \begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \frac{\partial f}{\partial X_n} & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ * & \cdots & * & \frac{\partial f}{\partial X_{i+1}} & \cdots & \frac{\partial f}{\partial X_n} & 0 \cdots & \vdots & 0 \\ \vdots & & \vdots & \ddots & \ddots & 0 & \cdots & \ddots & 0 \\ * & \cdots & * & 0 \cdots & 0 \cdots & \cdots & \frac{\partial f}{\partial X_{i+1}} & \cdots & \frac{\partial f}{\partial X_n} \end{pmatrix} (\alpha).$$

Sei ein Punkt $\alpha^0 = (X_1^0, \ldots, X_n^0, a_{i+1,1}^0, \ldots, a_{n,i}^0)$ der Faser $\Phi_i^{-1}(0)$ gegeben und sei $(X_1^0, \ldots, X_n^0)$ ein Punkt der Hyperfläche W, in welchem das Polynom f regulär ist (d.h. wir setzen voraus, daß mindestens eine partielle Ableitung von f in diesem Punkt nicht verschwindet). Sei $\mathcal{U}$ die Zariski–offene Umgebung von $(X_1^0, \ldots, X_n^0)$ mit folgender Eigenschaft: Ein Punkt von $\mathbb{C}^n$ ist genau dann in $\mathcal{U}$, wenn mindestens eine partielle Ableitung von f in diesem Punkt nicht verschwindet. Wir behaupten nun, daß die Restriktion der Abbildung Φ_i auf $\mathcal{U} \times \mathbb{C}^{(n-i)i}$

$$\Phi_i : \mathcal{U} \times \mathbb{C}^{(n-i)i} \longrightarrow \mathbb{C}^{i+1}$$

transversal zum Ursprung $0 = (0, \ldots, 0)$ von $\mathbb{C}^{i+1}$ ist. Zum Beweis dieser Behauptung betrachten wir einen beliebigen Punkt $\alpha = (X_1, \ldots, X_n, a_{i+1,1}, \ldots, a_{n,i})$ in $\mathcal{U} \times \mathbb{C}^{(n-i)i}$, der der Gleichung $\Phi_i(\alpha) = 0$ genügt. Da der Punkt $(X_1, \ldots, X_n)$ in der Zariski–offenen Menge $\mathcal{U} \cap W$ liegt, befindet er sich auf der Hyperfläche W und seine reguläre Gleichung ist durch f gegeben. Wir zeigen indirekt, daß die Jacobimatrix von Φ_i den maximalen Rang $i+1$ in α hat. Ist das nicht der Fall, so verschwinden die partiellen Ableitungen $\frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}$ im Punkt $(X_1, \ldots, X_n)$. Die Beziehung $\Phi_i(\alpha) = 0$ impliziert auch das Verschwinden der partiellen Ableitungen $\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ in $(X_1, \ldots, X_n)$.

Das steht aber im Widerspruch zur Tatsache, daß das Polynom f eine reguläre Gleichung in diesem Punkt ist. Damit hat die Jacobimatrix von Φ_i den maximalen Rang in α, d.h. daß der Punkt α ein regulärer Punkt von Φ_i ist. Da aber der Punkt α beliebig auf dem Durchschnitt $\Phi_i^{-1}(0) \cap (\mathcal{U} \times \mathbb{C}^{(n-i)i})$ gewählt war, folgt unsere Behauptung. Die Anwendung einer algebraisch–geometrischen Form des *schwachen Thom-Sard's Theorems* (vgl. [Dem89], [GG86]) auf das Diagramm

$$\begin{array}{ccc} \Phi_i^{-1}(0) \cap (\mathcal{U} \times \mathbb{C}^{(n-i)i}) & \overset{\imath}{\hookrightarrow} & \mathbb{C}^n \times \mathbb{C}^{(n-i)i} \\ & \pi_i \searrow & \downarrow \mathrm{pr}_2 \\ & & \mathbb{C}^{(n-i)i} \end{array}$$

führt zu der Schlußfolgerung, daß die Menge der Matrizen $(a_{kl})_{n-i,i} \in \mathbb{R}^{(n-i)i}$, für die die Transversalität gilt, Zariski–dicht in $\mathbb{C}^{(n-i)i}$ ist. Genauer gesagt: Der affine Raum $\mathbb{Q}^{(n-i)i}$ enthält eine nicht–leere Zariski–offene Menge von Matrizen $A^{(i)}$, deren entsprechende Koordinatentransformation $X = A^{(i)}(a)Y$ zu der gewünschten Glattheitseigenschaft von $\widetilde{W}_i$ in glatten Punkten von W führt. ∎

Der Beweis von Lemma 11 kann auch mit einer generisch nichtsingulären $n \times n$ Matrix an Stelle einer triangulären Matrix erzielt werden. Die hier benutzte Transformation hat den Vorteil, daß sie die für den Algorithmus wünschenswerte dünn–besetzte Gleichungen ergibt, und genügend generisch für den Beweis von Lemma 11 ist.

Sei das Polynom $f \in \mathbb{Q}[X_1, \ldots, X_n]$ nichtkonstant, quadratfrei und sei $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ die durch f definierte Hyperfläche. Sei $\Delta \in \mathbb{Q}[X_1, \ldots, X_n]$ das Polynom $\Delta := \sum\limits_{j=1}^{n} \left(\frac{\partial f}{\partial X_j}\right)^2$. Wir betrachten die reelle Varietät $V := W \cap \mathbb{R}^n$ und setzen voraus, daß

- *die Varietät V nicht–leer und beschränkt ist, und somit kompakt ist;*
- *der Gradient von f in jedem Punkt von V von null verschieden ist (d.h., V ist eine glatte Hyperfläche in $\mathbb{R}^n$, und $f = 0$ ist ihre reguläre Gleichung);*
- *die Variablen $X_1, \ldots, X_n$ bezüglich f generisch gewählt sind.*

Wir können mit diesen Voraussetzungen die folgende angepaßte Definition einer *polaren Varietät*, die konsistent mit der allgemeinen Definition ist, einführen (vgl. [LT81]).

Definition 12
Sei $0 \leq i < n$. Wir betrachten den linearen Unterraum X^i in $\mathbb{C}^n$ definiert durch die linearen Formen $X_{i+1}, \ldots, X_n$, d.h.,

$$X^i := \{x \in \mathbb{C}^n | X_{i+1}(x) = \ldots = X_n(x) = 0\} = \{x \in \mathbb{C}^n | x_{i+1} = \ldots = x_n = 0\}.$$

Dann heißt die algebraische Varietät W_i von $\mathbb{C}^n$, die durch den Zariski–Abschluß der Menge

$$\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0, \Delta(x) \neq 0\}$$

gegeben ist, die zum linearen Unterraum X^i von $\mathbb{C}^n$ assoziierte (komplexe) polare Varietät von W. Die entsprechende reelle Varietät $V_i := W_i \cap \mathbb{R}^n$ heißt die zum linearen Unterraum $X^i \cap \mathbb{R}^n$ von $\mathbb{R}^n$ assoziierte reelle polare Varietät *von V. Die Varietät W_0 ist der Zariski–Abschluß der Menge $\{x \in \mathbb{C}^n |\ f(x) = 0, \Delta(x) \neq 0\}$, und V_0 entspricht V.*

Bemerkung 3
Da nach Voraussetzung die relle Varietät V eine nicht–leere und kompakte Hyperfläche des $\mathbb{R}^n$ ist, und die Variablen $X_1, \ldots, X_n$ generisch gewählt sind, können wir aus der Morse Theorie (wie in [Mil64]) sicherstellen, daß die reelle polare Varietät V_i nicht–leer und glatt für jeden Index $0 \leq i < n$ ist. Insbesondere ist die komplexe Varietät W_i nicht–leer und die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ definierten Hyperflächen in $\mathbb{C}^n$ schneiden sich transversal in einer Zariski–offenen und dichten Teilmenge von W_i (man bemerke hierzu, daß jedes Element in $\{x \in \mathbb{C}^n | \ f(x) = 0, \Delta(x) \neq 0\}$ ein glatter Punkt von W ist, und man wende Lemma 11 *an).*

Wir wollen den Begriff des *reellen Grades* eines äquidimensionalen Varietät einführen. Diese geometrische Invariante ist ein Verfahren zur Auffindung reeller Lösungen eines Gleichungssystem besser als der geometrische Grad angepaßt. da sie nicht nur kleiner als dieser ist, sondern auch die reelle Lösungen des Systems widerspiegeln. Sei eine Zariski–abgeschlossene Teilmenge des $\mathbb{C}^n$ Z der Dimension $n-i$, $i \leq n$ druch ihre reguläre Gleichungen $f_1, \ldots, f_i \in \mathbb{Q}[X_1, \ldots, X_n]$ gegeben, und sei $Z := \bigcup_{i=1}^{s} C_i$ die Darstellung von Z in irreduziblen Komponenten.

Definition 13
Für jeden Index j, $1 \leq j \leq s$, heißt die irreduzible Komponente C_j eine reelle Komponente von Z, falls die reelle Varietät $C_j \cap \mathbb{R}^n$ einen glatten Punkt in C_j enthält. Sei

$$I := \{j \in \mathbb{N} | 1 \leq j \leq s, \ C_j \ \text{ ist eine reelle Komponente von } Z\}.$$

Dann heißt die (komplexe) affine Varietät $Z^* := \bigcup_{j \in I} C_j$ der reelle Teil *von Z. Wir bezeichnen mit $\deg^* Z := \deg Z^* = \sum_{j \in I} \deg C_j$ den reellen Grad der algebraischen Menge Z.*

Bemerkung 4
Der reelle Grad $\deg^* Z$ der Varietät Z ist stets kleiner als der geometrische Grad von Z. $\deg^* Z$ ist genau dann null, wenn der reelle Teil Z^* von Z leer ist.

Mit der Glattheitsvoraussetzung an die reelle Varietät V erhalten wir die folgende mengentheoretische Darstellung der reellen polaren Varietät

$$V_i = \{x \in \mathbb{R}^n | \ f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots \frac{\partial f(x)}{\partial X_i} = 0\}$$

für jeden Index $0 \leq i \leq n$.

Satz 14
Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein nichtkonstantes quadratfreies Polynom und sei $\Delta :=$

$\sum\limits_{j=1}^{n} \left(\frac{\partial f}{\partial X_j}\right)^2$. *Sei* $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ *die durch das Polynom* f *gegebene Hyperfläche von* $\mathbb{C}^n$. *Wir setzen weiterhin voraus, daß die reelle Varietät* $V := W \cap \mathbb{R}^n$ *nicht–leer ist und eine glatte und beschränkte Hyperfläche des* $\mathbb{R}^n$ *mit regulärer Gleichung* f *darstellt. Seien die Variablen* $X_1, \ldots, X_n$ *generisch bezüglich* f. *Für jeden Index* i, $0 \leq i < n$, *sei die komplexe polare Varietät* W_i *von* W *mit ihrer reellen polaren Varietät* V_i *von* V *wie oben definiert. Mit dieser Schreibweise erhalten wir:*

(i) $V_0 \subset W_0 \subset W$, *mit* $W_0 = W$ *genau dann, wenn* f *und* Δ *teilerfremd sind;*

(ii) W_i *ist eine nicht–leere äquidimensionale affine Varietät der Dimension* $n - (i+1)$, *die glatt in allen Punkten ist, die glatte Punkte von* W *sind;*

(iii) der reelle Teil W_i^* *der komplexen polaren Varietät* W_i *stimmt mit dem Zariski–Abschluß in* $\mathbb{C}^n$ *der reellen polaren Varietät*

$$V_i = \left\{ x \in \mathbb{R}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0 \right\},$$

überein;

(iv) das Ideal $\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}\right)_\Delta$ *ist radikal.*

Beweis:
Die erste Behauptung ist klar, da sich die Varietät W_0 als Vereinigung über alle irreduziblen Komponenten von W, in denen Δ nicht identisch verschwindet, darstellen läßt.

Wir zeigen nun die zweite Behauptung. Sei ein Index i, $0 \leq i < n$, fixiert. Dann ist nach Bemerkung 3 die polare Varietät W_i nicht–leer. Die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}}$ definierten Hyperflächen von $\mathbb{C}^n$ schneiden jede irreduzible Komponente von W_i transversal in einer Zariski–offenen Menge. Diese Tatsache hat zur Folge, daß die Varietät W_i eine nicht–leere äquidimensionale Varietät der Dimension $n-(i+1)$ ist, und die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}}$ eine reguläre Folge im lokalen Ring bilden, der durch Lokalisierung von $\mathbb{Q}[X_1, \ldots, X_n]$ mit dem Polynom Δ entsteht. Das Polynom Δ verschwindet nicht identisch auf jeder irreduziblen Komponente von W_i, d.h. $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$, ist eine reguläre Folge in $\mathbb{Q}[X_1, \ldots, X_n]_\Delta$. Mit Lemma 11 schlußfolgern wir, daß die Varietät W_i glatt in allen ihren Punkten ist, die glatt in der Hyperfläche W sind, und somit auch, daß sich die von den Polynomen $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$, definierten Hyperflächen transversal in diesen Punkten schneiden.

Wir gehen nun zum Beweis der Aussage *(iii)* über. Der Zariski–Abschluß von V_i in $\mathbb{C}^n$ ist in W_i^* enthalten (dies ist eine Folge der Glattheit von V_i). Die umgekehrte Inklusion erhalten wir folgendermaßen: Sei $x^* \in W_i^*$ ein beliebiger Punkt, und sei C eine irreduzible Komponente von W_i^*, die x^* enthält. Da C eine reelle Komponente von W_i ist, ist der Durchschnitt $C \cap \mathbb{R}^n$ nicht–leer und in W_i enthalten. Die polare Varietät W_i ist in der algebraischen Menge

$$\widetilde{W}_i := \left\{ x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0 \right\}$$

enthalten. Wir haben demzufolge $C \cap V_i \neq \emptyset$. Weiterhin schneiden die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ definierten Hyperflächen von $\mathbb{R}^n$ eine dichte Teilmenge des Durchschnittes $C \cap V_i$ transversal. Somit erhalten wir

$$\begin{aligned} n-(i+1) \quad &= dim_{\mathbb{R}}(C \cap V_i) = dim_{\mathbb{R}} R(C \cap V_i) = \\ &= dim_{\mathbb{C}} R((C \cap V_i)') \leq dim_{\mathbb{C}} C = n-(i+1). \end{aligned}$$

($R(C \cap V_i)$ steht für die Menge der glatten Punkte in $C \cap V_i$ und $(C \cap V_i)'$ für die Komplexifizierung von $C \cap V_i$.) Nach diesen Gleichungen gilt $dim_{\mathbb{C}}(C \cap V_i)' = dim_{\mathbb{C}} C = n-(i+1)$, und somit auch $C = (C \cap V_i)'$. Weiterhin ist die Komplexifizierung $(C \cap V_i)'$ im Zariski–Abschluß von V_i in $\mathbb{C}^n$ enthalten. Dies impliziert, daß C im Zariski–Abschluß von V_i enthalten ist, und somit auch x^*.

Zum Schluß beweisen wir die letzte Aussage. Wir betrachten wiederum die algebraische Menge

$$\widetilde{W}_i := \left\{ x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0 \right\},$$

die die polare Varietät W_i enthält. Sei C' eine beliebige irreduzible Komponente von W_i. Dann ist C' auch eine irreduzible Komponente von $\widetilde{W}_i$. Weiterhin verschwindet das Polynom Δ nicht identisch auf C'. Nach Bemerkung 3 existiert ein glatter Punkt x^* in $\widetilde{W}_i$, der in C' enthalten ist, und in welchem sich die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ definierten Hyperflächen transversal schneiden.

Sei $x^* = (x_1^*, \ldots, x_n^*) \in \mathbb{C}^n$ auf diese Weise fixiert. Wir betrachten den lokalen Ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ des Punktes x^* in der Varietät $\widetilde{W}_i$ (d.h., $\mathcal{O}_{\widetilde{W}_i, x^*}$ ist der Ring der Keime rationaler Funktionen auf $\widetilde{W}_i$, die im Punkt x^* definiert sind). Wir erhalten den lokalen Ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ algebraisch, indem wir den polynomialen Ring $\mathbb{C}[X_1, \ldots, X_n]$ mit dem Ideal $(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i})$, das die algebraische Menge $\widetilde{W}_i$ definiert, faktorisieren und dann in dem durch $x^* = (x_1^*, \ldots, x_n^*)$ induzierten maximalen Ideal $(X_1 - x_1^*, \ldots, X_n - x_n^*)$ lokalisieren. Die Anwendung von Standard–Argumenten der kommutativen Algebra und algebraischen Geometrie (vgl. [Kun80]) impliziert unter Benutzung der Tatsache, daß sich die durch die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ beschriebenen Hyperflächen in x^* transversal schneiden, daß der Ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ ein regulärer lokaler Ring, somit auch ein Integritätsbereich, ist. Da der Ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ ein Integritätsbereich ist, gibt es genau eine irreduzible Komponente von $\widetilde{W}_i$, die den glatten Punkt x^* enthält (dies gilt sowohl für die $\mathbb{C}$–Zariski–Topologie, als auch für die in dieser Arbeit betrachtete $\mathbb{Q}$–Zariski–Topologie). Der Punkt x^* ist folglich in genau einer irreduziblen Komponente C' von $\widetilde{W}_i$ (und von W_i) enthalten.

Da der lokale Ring $\mathcal{O}_{\widetilde{W}_i,x^*}$ einen Intergritätsbereich definiert, ist sein Verschwindungsideal ein Primideal. Damit erzeugen die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ ein Primideal im lokalen Ring $\mathbb{C}[X_1, \ldots, X_n]_{(X_1-x_1^*,\ldots,X_n-x_n^*)}$. Die isolierte Primärkomponente des Ideals $(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i})$ in $\mathbb{Q}[X_1, \ldots, X_n]$, welche der irreduziblen Komponente C' entspricht, ist selbst ein Primideal. Da dies aber für jede irreduzible Komponente von W_i gilt, ensteht die Varietät W_i aus der Varietät $\widetilde{W}_i$ durch Streichung aller in der Hyperfläche $\{x \in \mathbb{C}^n | \Delta(x) = 0\}$ eingebetteten irreduziblen Komponenten. Wir schließen daraus, daß das Ideal $(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i})_\Delta$ in $\mathbb{Q}[X_1, \ldots, X_n]_\Delta$ ein Durchschnitt von Primidealen ist und somit radikal sein muß.

■

Bemerkung 5
Unter den Voraussetzungen von Theorem 14 *gelten für jeden Index* i, $0 \leq i < n$, *die folgenden Inklusionen zwischen den bis jetzt eingeführten verschiedenen nicht–leeren Varietäten,*

$$V_i \subset V \text{ und } V_i \subset W_i^* \subset W_i \subset \widetilde{W}_i.$$

Die reelle Varietät V beschreibt eine beschränkte und glatte reelle Hyperfläche. Die Varietäten W_i und V_i sind die in Definition 12 *eingeführten polaren Varietäten, W_i^* ist der reelle Teil von W_i wie in der Definition* 13, *und $\widetilde{W}_i$ ist die im Lemma* 11 *eingeführte komplexe affine Varietät. Die Voraussetzungen und Theorem* 14 *implizieren die folgenden Gleichungen $n - (i+1) = dim_{\mathbb{C}} W_i = dim_{\mathbb{C}} W_i^* = dim_{\mathbb{R}} V_i$. Unter der Glattheitannahme und der generischen Wahl der Koordinaten erhalten wir die folgenden Inklusionen zwischen den entsprechenden Mengen glatter Punkte:*

$$V_i = R(V_i) \subset R(W_i) \subset R(\widetilde{W}_i) \subset R(W), \tag{3.4}$$

wobei $R(V_i)$, $R(W_i)$, $R(\widetilde{W}_i)$, und $R(W)$ in der aufsteigenden Kette (3.4) *die Menge der entsprechenden regulären Punkte in V_i, W_i, $\widetilde{W}_i$ und W sind, und die Varietät W die affine Hyperfläche $W = \{x \in \mathbb{C}^n | f(x) = 0\}$ in $\mathbb{C}^n$ ist.*

3.2 Der algorithmische und komplexitätstheoretische Aspekt des Hyperflächenfalls

Die Betrachtung von polaren Varietäten erlaubt nun die Formulierung eines ersten Komplexitätsresultats:
Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein quadratfreies Polynom vom Grad $d \geq 2$, welches eine reguläre Gleichung der reellen beschränkten algebraischen Menge

$$V := W \cap \mathbb{R}^n = \{x \in \mathbb{R}^n |\ f(x) = 0\}$$

definiert, d.h. der Gradient von f verschwindet nicht in jedem Punkt der kompakten reellen Hyperfläche V. Seien die Koordinaten $X_1, \ldots, X_n$ generisch bezüglich f gewählt. Sei mit Δ das Polynom $\sum_{j=1}^n \left(\frac{\partial f}{\partial X_j}\right)^2$ bezeichnet.

Für jeden Index $i,\ 0 \leq i < n$ sei W_i der Zariski–Abschluß der Menge

$$\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_j} = 0, \Delta(x) \neq 0\}.$$

W_i ist die zum linearen Unterraum $X^i := \{x \in \mathbb{C}^n | x_{i+1} = \ldots = x_n = 0\}$ assoziierte polare Varietät der Hyperfläche W.
Unter diesen Voraussetzungen haben wir im Theorem 14 gezeigt, daß

$$f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$$

eine transversale Folge außerhalb der Hyperfläche $\{x \in \mathbb{C}^n |\ \Delta(x) = 0\}$ im Sinne der Definition 4 ist.
Sei δ_i der geometrische Grad der polaren Varietät $W_i,\ 0 \leq i < n$. Dann besteht eine geometrische Lösung des Systems

$$f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}} \tag{3.5}$$

im Sinne von Abschnitt 2.2 aus:

- einem linearer Koordinatenwechsel $(X_1, \ldots, X_n) \mapsto (Y_1, \ldots, Y_n)$ derart, daß die Polynome in Noether–Position bezüglich der neuen Variablen sind;
- einer Linearform $U = \lambda_1 X_1 + \ldots + \lambda_n X_n$ mit Koeffizienten $\lambda_1, \ldots, \lambda_n$ in $\mathbb{Z}$, welche ein *primitives* Element u von

  $$\mathbb{Q} \to \mathbb{Q}[Y_1, \ldots, Y_n]/(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}})$$

  mit einem Minimalpolynom $q \in \mathbb{Q}[U]$ erzeugt;
- einer Menge von Parametrisierungen $\rho_i y_i - p_i(u)$ für $i = 1, \ldots, n$. Die ρ_i bzw. $p_i(u)$ sind Polynome in $\mathbb{Z}[Y_1, \ldots, Y_r]$ bzw. $\mathbb{Z}[Y_1, \ldots, Y_r][U]$, und hängen von der Wahl von u ab.

$$W_{n-1} := \{(\frac{p_1(u)}{\rho_1}, \ldots, \frac{p_n(u)}{\rho_n}) \in \mathbb{C}^n |\ q(u) = 0, \rho := \Pi \rho_i \neq 0\}. \tag{3.6}$$

Satz 15
Seien n, d, δ, L nichtnegative ganze Zahlen. Unter den obigen Voraussetzungen gibt es ein arithmetisches Netzwerk $\mathcal{N}$ auf $\mathbb{Q}$ im Sinne der Definition 5, mit der Größe $(nd\delta L)^{O(1)}$ und nichtskalaren Tiefe $O(n(log(d\delta) + \ell))$, so daß folgendes gilt:

Sei das Polynom $f \in \mathbb{Q}[X_1, \ldots, X_n]$ durch ein divisionsfreien Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe L und nichtskalaren Tiefe ℓ gegeben. Dann erzeugt das Netzwerk $\mathcal{N}$ aus dem Schaltkreis β die Koeffizienten einer regulären

Matrix, die die Koordinaten $X = (X_1, \ldots, X_n)$ *in die neuen Koordinaten* $Y = (Y_1, \ldots, Y_n)$ *überführt, so daß die gewünschte Noether–Position und Transversalität in jedem Iterationsschritt* i, $0 \leq i < n-1$, *erfüllt ist.*
Der durch das arithmetische Netz $\mathcal{N}$ *erzeugte Algorithmus testet, startend mit* β, *ob die komplexe algebraische Menge* W_{n-1} *null–dimensional ist. Wenn dies der Fall ist, so erzeugt das arithmetische Netzwerk* $\mathcal{N}$ *ein Straight–Line Programm der Größe* $(nd\delta L)^{O(1)}$ *und nichtskalarer Tiefe* $O(n(log(d\delta) + \ell))$ *mit Parametern in* $\mathbb{Q}$, *welches die Koeffizienten der* $n+1$ *univariaten Polynome* $q, p_1, \ldots, p_n \in \mathbb{Q}[U]$ *berechnet. Die Polynome haben die folgenden Eigenschaften:*

(1) $\deg(q) = \delta_{n-1} = \deg W_{n-1}$

(2) $\max\{\deg(p_j) | 1 \leq j \leq n\} < \delta_{n-1}$

(3) $W_{n-1} = \{(\frac{p_1(u)}{\rho_1}, \ldots, \frac{p_n(u)}{\rho_n}) | \ u \in \mathbb{C}, q(u) = 0\}$.

Der dem arithmetischen Netzwerk $\mathcal{N}$ *unterliegende Algorithmus testet, ob die semi–algebraische Menge* $W_{n-1} \cap \mathbb{R}^n$ *nicht–leer ist. Wenn dieser Fall eintritt, erzeugt das Netz* $\mathcal{N}$ *höchstens* δ_{n-1} *Vorzeichenbedingungen in* $\{-1, 0, 1\}^{\delta_{n-1}}$, *die die reellen Nullstellen des Polynoms* q à la Thom *kodieren, [CR88]. Das Netz* $\mathcal{N}$ *beschreibt mit dieser Kodierung die Parametrisierung der nicht–leeren Menge* $W_{n-1} \cap \mathbb{R}^n$.

Wir erhalten mit dem Output dieses Algorithmus folgende Informationen:

- Wenn die komplexe Varietät W_{n-1} keine null–dimensionale Varietät ist, oder wenn W_{n-1} null–dimensional aber $W_{n-1} \cap \mathbb{R}^n$ leer ist, so können wir schlußfolgern, daß die reelle Varietät V keine kompakte glatte Hyperfläche in $\mathbb{R}^n$ mit einer regulären Gleichung f ist.

- Falls die Varietät V eine kompakte glatte Hyperfläche in $\mathbb{R}^n$ mit einer regulären Gleichung f ist, so ist der Durchschnitt $W_{n-1} \cap \mathbb{R}^n$ nicht–leer und enthält für jede Zusammenhangskomponente in V mindestens einen Punkt, den das Netzwerk $\mathcal{N}$ im Sinne von Thom durch eine reelle Nullstelle des minimalen Polynoms q parametrisiert.

Bemerkung 6
Wir leiten aus dem Satz von Bézout die folgende Abschätzung über den geometrischen Grad (vgl. [Hei83], nämlich $\max\{\delta_i | 0 \leq i < n\} \leq d(d-1)^{n-1} < d^n$ *ab. Das Polynom* f *läßt sich durch ein divisionsfreies Straight–Line Programm in* $\mathbb{Q}[X_1, \ldots, X_n]$ *evaluieren. Bei fixiertem* $\delta := d(d-1)^{n-1}$ *und* $L := d^n$ *erhalten wir im obigen Satz, für den Fall einer kompakten, durch ein reguläres Polynom von Grad* d *gegebenen, glatten Hyperfläche in* R^n, *eine worst case Abschätzung, welche die Hauptkomplexitätsresultate in [GV88], [Gri88], [HRS89b], [HRS89a], [HRS90], [Can88], [Ren88a], [Ren88b], und [BPR94] beinhaltet. Die Bedeutung von Theorem*

15 *besteht darin, daß zu erwarten ist, daß in vielen praktisch relevanten Fällen der geometrische Grad δ wesentlich kleiner als die Bézout Zahl $d(d-1)^{n-1}$, und die Größe L kleiner als d^n sein werden.*

Beweis des Satzes:
Sei das Polynom f durch ein Straight–Line Programm β der Länge L und Tiefe ℓ gegeben. Unter einer einfachen Anwendung der Leibniz Regel, zur Differentiation eines Produkts können wir ein Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_n]$, der Länge $(2n+1)L$ und nichtskalaren Tiefe $\ell + 1$ ableiten, welches alle partiellen Ableitungen von f evaluiert. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß das Straight–Line Programm β, welches das Polynom f evaluiert, auch das Polynom Δ repräsentiert, da sich die partiellen Ableitungen von f aus dem Straight–Line Programm β in einer in n und L linearen Komplexitätszeit auswerten lassen (vgl. [BS82] und [Mor84]).
Eine Anwendung der simultanen Noether–Normalisierung im Theorem 5, [KP96] finden wir eine reguläre $(n \times n)-$Matrix, die die Koordinaten $X_1, \ldots, X_n$ in Noether–Position bezüglich den polaren Varietäten $W_0,\ W_1, \ldots, W_{n-1}$ darstellt. Wir finden unter Benutzung des der Proposition 18, [GHM$^+$98], zugrunde liegenden Algorithmus mit der im Theorem 31, [GHH$^+$97], eingeführten Modifizierung (siehe auch Theorem 19 und dessen Beweis) ein arithmetisches Netzwerk $\mathcal{N}'$ mit Parametern in $\mathbb{Q}$ von der Größe $(nd\delta L)^{O(1)}$, welches entscheidet, ob die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}}$ transversal außerhalb der durch Δ definierte Hyperfläche sind. Dies ist genau dann der Fall, wenn die Varietät W_{n-1} eine null–dimensionale Varietät ist.

Wir setzen nun voraus, daß die Polynome $(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}})$ transversal außerhalb der durch Δ definierte Hyperfläche sind. Unter Anwendung der Proposition 18 in [GHM$^+$98] und des Theorems 31 in [GHH$^+$97] auf die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}}$ und Δ erhalten wir ein arithmetisches Netzwerk $\mathcal{N}'$. Dieses Netzwerk $\mathcal{N}'$ erzeugt ein die Koeffizienten der Polynome $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ repräsentierendes Straight–Line Programm in $\mathbb{Q}$. Die Polynome $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ charakterisieren den Teil W_{n-1} der komplexen Varietät $\widetilde{W}_{n-1} := \left\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_{n-1}} = 0\right\}$, der die Hyperfläche $\{x \in \mathbb{C}^n | \Delta(x) = 0\}$ meidet. Die Ausgabe $q, p_1, \ldots, p_n$ des Netzwerks $\mathcal{N}'$ erfüllt dann die Bedingungen $(1), (2), (3)$ im Theorem 15.

Das Netzwerk $\mathcal{N}'$ läßt sich durch die Anwendung des korrekten Algorithmus in [BOKR86] (vgl. auch [RS90] für eine Verfeinerung) erweitern, indem geeignete komprimierte Knoten addiert werden, die testen, ob eine rationale Zahl positiv ist. Das resultierende Netzwerk $\mathcal{N}$ entscheidet nun, ob das Polynom q irgendeine reelle Lösung besitzt und es hat eine Größe, die asymptotisch gleich $(nd\delta L)^{O(1)}$ ist. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß das Netzwerk $\mathcal{N}$ jede existierende Nullstelle des Polynoms q im Sinne von Thom (vgl. [CR88], [RS90]) kodiert. Die Einschränkung der letzten Koordinate X_n auf eine irreduzible Komponente der kompakten reellen Varietät $V := W \cap \mathbb{R}^n$ nimmt das Maximum auf dieser Komponente an, welches in $V_{n-1} := W_{n-1} \cap \mathbb{R}^n$ liegt. Damit kodiert das arithmetische Netzwerk $\mathcal{N}$ mindestens einen Punkt in jeder irreduziblen Komponente von V. Der Beweis folgt. ■

Das arithmetische Netzwerk $\mathcal{N}$ im Beweis des obigen Satzes startet mit der Ausgabe von β und berechnet in jeder Zusammenhangskomponente von V mindestens einen repräsentativen Punkt, falls $f \in \mathbb{Q}[X_1, \ldots, X_n]$ eine reguläre Gleichung einer beschränkten glatten Hyperfläche V in $\mathbb{R}^n$ ist. Die Größe des Netzwerks $\mathcal{N}$ hängt polynomial von der Anzahl n der Variablen, vom Grad d des Polynoms f, von der Länge L des f auswertenden Straight–Line Programms, und vom Grad δ gewisser zu f assoziierter komplexer polarer Varietäten $W_i, 0 \leq i < n$, ab.
Das Netzwerk $\mathcal{N}$ gibt somit eine Antwort auf das algorithmische Problem, repräsentative Punkte auf irreduziblen Komponenten einer kompakten glatten reellen Varietät zu kodieren. Die Komplexität des zugrunde liegenden Algorithmus hängt vom geometrischen Grad δ abhängt, welcher mehr komplexen Lösungen als den reellen von f assoziiert ist.

Es ist wünschenswert, ein Netzwerk aufzubauen, dessen Größe direkt von einer geometrischen Invarianten abhängt, die reelle Wurzeln vom Polynom f entspricht. Als eine solche Invariante erweist der in Definition 13 eingeführte reelle Grad der betrachteten polaren Varietäten W_i ist $0 \leq i < n$. Wir werden durch einen zweiten Algorithmus zeigen, daß es ein Netzwerk gibt, dessen Größe polynomial vom reellen Grad abhängt. Der Preis, den wir dafür in Kauf nehmen müssen, ist relativ hoch:

- Die zweite Prozedur ist nicht mehr in der Lage zu entscheiden, ob ein Polynom f eine reguläre Gleichung einer beschränkten glatten Hyperfläche V des $\mathbb{R}^n$ ist, sondern wir müssen das voraussetzen. Weiterhin setzen wir voraus, daß die reelle Gleichung $f = 0$ konsistent ist, d.h. es gibt mindestens eine reelle Lösung. Wir benutzen dann diese Prozedur, um die reelle Gleichung $f = 0$ zu lösen, wobei wir mit *Lösen* meinen, daß der Algorithmus mindestens einen repräsentativen Punkt in jeder irreduziblen Komponente von V erzeugt.

- Für unseren neuen Algorithmus benötigen wir zwei „ äußere Subroutinen, deren theoretische Komplexitätsschranken nicht direkt ins Kalkül gezogen werden, obwohl ihre praktische Komplexität als polynomial anzusehen ist:

  - Die erste benötigte Subroutine ist ein Faktorisierungsalgorithmus für univariate Polynome in $\mathbb{Q}$. Während die Komplexität der Faktorisierung eines Polynoms über $\mathbb{Q}$ im Bitkomplexitätsmodell polynomial ist ([LLL82]), ist sie im hier betrachteten arithmetischen Modellen komplizierter (vgl. [vzGS91]). Im erweiterten Komplexitätsmodell werden wir die Kosten der Faktorisierung eines univariaten Polynoms vom Grad D über $\mathbb{Q}$ mit $D^{O(1)}$ ansetzen.
  - Die zweite Subroutine verwirft die komplexen irreduziblen Komponenten der polaren Varietät, die keinen glatten reellen Punkt enthalten. Diese

zweite Subroutine startet mit einem Straight–Line Programm β für ein einziges Polynom in $\mathbb{Q}[X_1, \ldots, X_n]$ als Eingabe und entscheidet, ob das Polynom eine glatte reelle Nullstelle besitzt (ohne diese Nullstelle zu finden, falls eine solche existiert). Die Kosten dieses Verfahrens werden in unserer Methode polynomial ansetzen.

- Wir nennen ein arithmetisches Netzwerk über $\mathbb{Q}$ *erweitert*, falls es neue Knoten enthält, welche der ersten und zweiten Subroutine entsprechen.

Wir fassen jetzt Voraussetzungen und Bezeichnungen, die wir im folgenden, den zuvor beschriebenen Sachverhalt betreffenden Lemma 16 benutzen.
Seien die natürliche Zahlen n, d, δ^* und L fixiert. Wir setzen voraus, daß ein divisionsfreies Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ mit Größe L derart gegeben ist, so daß β ein nichtkonstantes Polynom $f \in \mathbb{Q}[X_1, \ldots, X_n]$ mit Gradschranke d auswertet. Seien wieder $\Delta := \sum_{j=1}^{n} \left(\frac{\partial f}{\partial X_j}\right)^2$ und das Polynom f eine reguläre Gleichung der nicht–leeren beschränkten glatten Hyperfläche V in $\mathbb{R}^n$. Ferner sei $W := \{x \in \mathbb{C}^n; f(x) = 0\}$ die durch f in $\mathbb{C}^n$ definierte komplexe Hyperfläche, und es seien die Variablen $X_1, \ldots, X_n$ in generischer Position bezüglich f. Ein Index i, $0 \leq i < n$, sei beliebig fixiert. Die zum linearen Unterraum $X^i := \{x \in \mathbb{C}^n | x_{i+1} = 0, \ldots, x_n = 0\}$ assoziierte polare Varietät W_i ist der Zariski–Abschluß in $\mathbb{C}^n$ der Menge

$$\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0, \Delta(x) \neq 0\}.$$

Sei $V_i := W_i \cap \mathbb{R}^n$ die zur reellen Hyperfläche V assoziierte polare Varietät. Sei δ_i^* der reelle Grad der polaren Varietät W_i, d.h., der geometrische Grad von W_i^* (vgl. Definition 13). Nach Theorem 14 ist die Größe δ_i^* auch den geometrischen Grad des Zariski–Abschlusses der reellen polaren Varietät V_i in $\mathbb{C}^n$, d.h., der Komplexifizierung von V_i. Sei $r := n - (i + 1)$. Da die Variablen $X_1, \ldots, X_n$ generisch bezüglich unserer geometrischen Daten gewählt sind, sind sie auch in Noether–Position bezüglich der komplexen Varietät W_i, wobei die Koordinaten $X_1, \ldots, X_r$ frei sind (vgl. [GHMP95], [GHM+98]). Ferner sei $\delta^* \geq \max\{\delta_i^* | 0 \leq i < n\}$.

Mit diesen Bezeichnungen und Annahmen erhalten wir im folgenden Lemma eine *reelle* Version von Proposition 17 in [GHM+98]:

Lemma 16
Sei i ein fest gewählter Index mit $0 \leq i < n$ und sei $r := n - (i + 1)$. Dann existiert ein erweitertes arithmetisches Netzwerk $\mathcal{N}$ mit Parametern in $\mathbb{Q}$ von der Größe $(id\delta^* L)^{O(1)}$, welches aus dem Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ ein divisionsfreies Straight–Line Programm β_i in $\mathbb{Q}[X_1, \ldots, X_r]$ erzeugt. Dieses Straight–Line Programm β_i repräsentiert ein Polynom $\varrho \in \mathbb{Q}[X_1, \ldots, X_r]$, welches nicht identisch Null ist, sowie die Koeffizienten gewisser Polynome

$$q, p_{r+1}, \ldots, p_n \in \mathbb{Q}[X_1, \ldots, X_r, X_{r+1}]$$

bezüglich X_{r+1}. Die Polynome $\varrho, q, p_{r+1}, \ldots, p_n$ haben die folgenden Eigenschaften:

(i) Das Polynom q hat den Leitkoeffizienten eins und ist in X_{r+1}, vom Grade $\deg q = \deg_{X_{r+1}} q = \delta_i^* = \deg W_i^* \leq \delta^*$.

(ii) Das Polynom ϱ ist die Diskriminante von q bezüglich der Variablen X_{r+1} und sein Grad läßt sich durch $\deg \varrho \leq 2(\delta_i^*)^3$ abschätzen.

(iii) Die Grade der Polynome $p_1, \ldots, p_n$ genügen den Ungleichungen

$$\max\{\deg_{X_{r+1}} p_k | 1 \leq k \leq n\} < \delta_i^*,$$

$$\max\{\deg p_k | 1 \leq k \leq n\} = 2(\delta_i^*)^3.$$

(iv) Das Ideal

$$(q, \varrho X_{r+1} - p_{r+1}, \ldots, \varrho X_n - p_n)_\varrho,$$

das in der Lokalisierung

$$\mathbb{Q}[X_1, \ldots, X_n]_\varrho$$

durch die Polynome $q, \varrho X_{r+1} - p_{r+1}, \ldots, \varrho X_n - p_n$ erzeugt wird, beschreibt das Verschwindungsideal der affinen Varietät $(W_i^*)_\varrho := \{x \in W_i^* | \varrho(x) \neq 0\}$. Ferner ist $(W_i^*)_\varrho$ eine dichte Zariski–offene Teilmenge der komplexen Varietät W_i^*.

(v) Die Straight–Line Programms β_i ist von der Größe $(id\delta^* L)^{O(1)}$.

Beweis:
Der Beweis dieses Lemma folgt den allgemeinen Linien des Beweises von Theorem 14 und basiert wiederum auf Algorithmen, die der Proposition 18 [GHM⁺98] und dem Theorem 31 in [GHH⁺97] zugrunde liegen. Wir wissen aus Theorem 14, daß die Polynome $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_{n-1}}$, außerhalb der in $\mathbb{C}^n$ durch Δ definierte Hyperfläche eine transversale Folge bilden. Somit läßt sich der auf dem Theorem 10 basierende Algorithmus zur geometrischen Lösung (vgl. [GHM⁺98], Abschnitt 3, anwenden.

Zunächst können wir mit dem Ergebnissen aus den Arbeiten [BS82] und [Mor84] das Straight–Line Programm β, welches das Eingangspolynom f evaluiert, so modifizieren, daß auch entsprechende partielle Ableitungen von f evaluiert werden. Die entstehenden Kosten sind linear in L. Wir können also ohne Einschränkung der Allgemeinheit voraussetzen, daß das Straight–Line Programm β sowohl f als auch Δ repräsentiert.

Wir zeigen Lemma 16, indem wir unter der Voraussetzung, daß die beiden ein erweitertes Netzwerk definierenden Subroutinen zur Verfügung stehen, eine in i, $0 \leq i \leq n$, rekursive Prozedur aufbauen.

Sei zuerst der Index $i := 0$, und sei β_0 das Straight–Line Programm β, das die Polynome f und Δ darstellt. Da die Variablen $X_1, \ldots, X_n$ in generischer Position sind, lassen sich die Polynome f und Δ mit Leitkoeffizienten eins in X_n darstellen, und diese Polynome genügen den Bedingungen $d \geq \deg f = \deg_{X_n} f$ und $2d \geq \deg \Delta = \deg_{X_n} \Delta$.

Sei $R_0 := \mathbb{Q}[X_1, \ldots, X_{n-1}]$, und wir betrachten die Polynome f und Δ mit Leitkoeffizienten eins und Koeffizienten in R_0. Durch Interpolation in $2d+1$ beliebigen, voneinander verschiedenen rationalen Punkten erhalten wir ein divisionsfreies Straight–Line Programm in $R_0 = \mathbb{Q}[X_1, \ldots, X_{n-1}]$, das die Koeffizienten von f und Δ bezüglich X_n darstellt. Dieses Straight–Line Programm hat die Länge $Ld^{O(1)}$.

Wir erhalten den größten gemeinsamen Teiler von f und Δ in $R_0[X_n]$ durch die Anwendung vom Lemma 8 in [GHM$^+$98]. Dieser größte gemeinsame Teiler hat den Leitkoeffizienten eins in $R_0[X_n]$, und seine Koeffizienten bezüglich X_n lassen sich durch ein divisionsfreies Straight–Line Programm in $R_0 = \mathbb{Q}[X_1, \ldots, X_{n-1}]$ darstellen. Sei $\bar{q} \in R_0[X_n] = \mathbb{Q}[X_1, \ldots, X_n]$ der Quotient von f und dem größten gemeinsamen Teiler von f und Δ. Dann lassen sich die Koeffizienten von $\bar{q}$ bezüglich X_n durch ein divisionsfreies Straight–Line Programm $\bar{\beta}_1$ in R_0 darstellen. Das Polynom $\bar{q}$ ist quadratfrei, da f quadratfrei ist, den Leitkoeffizienten eins bezüglich X_n hat und f teilt. Wir haben weiterhin eine Beschreibung der Varietät $W_0 = \{x \in \mathbb{C}^n | \bar{q}(x) = 0\}$. Das Polynom $\bar{q}$ ist das minimale Polynom der Hyperfläche W_0 in $\mathbb{C}^n$. Der Grad des Polynoms $\bar{q}$ genügt den Gleichungen $\deg \bar{q} = \deg_{X_n} \bar{q} = \deg W_0$.

Das Straight–Line Programm $\bar{\beta}_1$, welches die Koeffizienten des Polynoms $\bar{q}$ bezüglich der Variablen X_n darstellt, hat die Länge $(dL)^{O(1)}$. Um die Beschreibung der Rekursion für $i = 0$ zu beenden, genügt es, den Faktor q des minimalen Polynoms $\bar{q}$ zu finden, welcher den reellen Teil W_0^* der Varietät W_0 beschreibt. Dazu betrachten wir die Projektionsabbildung $\mathbb{C}^n \to \mathbb{C}^{n-1}$, die jedem Punkt in $\mathbb{C}^n$ seine ersten $n-1$ Koordinaten zuordnet. Da die Variablen $X_1, \ldots, X_n$ generisch gegeben sind, induziert diese Projektion einen endlichen surjektive Morphismus $\pi : W_0 \to \mathbb{C}^{n-1}$. Wir wählen einen generischen *Lifting Punkt* $t = (t_1, \ldots, t_{n-1}) \in \mathbb{Q}^{n-1}$ mit rationalen Koordinaten $t_1, \ldots, t_{n-1}$. Der Punkt t ist ein generischer Punkt in $\mathbb{Q}^{n-1}$ für die Hyperfläche W_0 vom Morphismus π. Die null–dimensionale Faser $\pi^{-1}(t)$, *die Lifting Faser*, besteht nur aus in W_0 glatten Punkten.

Die irreduziblen Komponenten von W_0 sind die Hyperflächen in $\mathbb{C}^n$, die durch die $\mathbb{Q}$–irreduziblen Faktoren $q_1, \ldots, q_s$ von $\bar{q}$ beschrieben sind.

Ohne Einschränkung der Allgemeinheit können wir annehmen, daß für Indizes $1 \leq m \leq s$ die irreduziblen Polynome $q_1, \ldots, q_m$ die reellen irreduziblen Komponenten von W_0 definieren. Hieraus folgt, daß der gesuchte Faktor q des minimalen Polynoms $\bar{q}$ durch $q := q_1 \ldots q_m$ darstellbar ist. Dann müssen alle irreduziblen Faktoren $q_1, \ldots, q_s$ von $\bar{q}$ gefunden und die Faktoren $q_{m+1}, \ldots, q_s$ gestrichen werden.

Wir geben im folgenden eine Methode zur Auffindung aller irreduziblen Polynome $q_1, \ldots, q_s$ von $\bar{q}$ an. Wir spezialisieren in $\bar{q}$ die Variablen $X_1, \ldots, X_{n-1}$ durch die Koordinaten $t_1, \ldots, t_{n-1}$ des rationalen Lifting Punktes $t \in \mathbb{Q}^{n-1}$ und erhalten ein univariates Polynom $\bar{q}(t, X_n) := \bar{q}(t_1, \ldots, t_{n-1}, X_n) \in \mathbb{Q}[X_n]$, das sich in $\bar{q}(t, X_n) = q_1(t, X_n) \ldots q_s(t, X_n)$ in $\mathbb{Q}[X_n]$ zerlegen läßt. Da der Lifting Punkt t generisch in $\mathbb{Q}^{n-1}$ gewählt war, impliziert der Hilbertsche Irreduzibilitätssatz (vgl. [Lan62]), daß die Polynome $q_1(t, X_n)$,...,$q_s(t, X_n)$ irreduzibel in $\mathbb{Q}$ sind. Eine Spezialisierung der Variablen $X_1, \ldots, X_{n-1}$ im Straight–Line Programm $\bar{\beta}_1$ auf die Werte $t_1, \ldots, t_{n-1}$ ergibt ein arithmetisches Netzwerk in $\mathbb{Q}$, das die Koeffizienten des univariaten Polynoms $\bar{q}(t, X_n)$ darstellt. Die Anwendung der erste Subroutine liefert die Koeffizienten der Polynome $q_1(t, X_n), \ldots, q_s(t, X_n)$. Die Anwendung der Lifting Prozedur (aus dem Algorithmus zur geometrischen Lösung) auf diese Polynome liefert ein divisionsfreies Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ mit der Größe $(dL)^{O(1)}$, welches die Koeffizienten der Polynome $q_1, \ldots, q_s$ bezüglich der Variable X_n darstellt (vgl. [GHH+97]).

Um den Schritt $i = 0$ zu beenden, muß eine algorithmische Identifizierung der Polynome $q_1, \ldots, q_m$, die die irreduziblen reellen Komponenten von W_0 und somit auch W^* definieren erfolgen. Das Produkt $q = q_1 \ldots q_m$ ist dann leicht zu erhalten. Wir bemerken nochmals, daß $\bar{q}$ das minimale Polynom der Hyperfläche W_0 ist. Wir erhalten die Gleichung $V_0 = W_0^* \cap \mathbb{R}^n = W_0 \cap \mathbb{R}^n$ aus der Glattheit der Varietät $V = W \cap \mathbb{R}^n$. Die Polynome $\bar{q}$ und q sind auch reguläre Gleichungen der reellen Hyperfläche V, denn nach Voraussetzung gilt das für f und die Polynome $\bar{q}$ und q sind Faktoren von f. Damit muß jedes Polynom in der Folge $q_1, \ldots, q_s$, welches eine reelle Nullstelle $x \in \mathbb{R}^n$ hat, einen im Punkt x nichtverschwindenden Gradient haben. Dies hat zur Folge, daß jede der Polynom $q_1, \ldots, q_s$ mit reellen Nullstellen in der Folge $q_1, \ldots, q_m$ vorkommen muß. Durch Aufruf der zweiten Subroutine findet man Polynome $q_1, \ldots, q_m$, und somit auch das Produkt $q = q_1 \ldots q_m$.

Wir erweitern nun das divisionsfreie Straight–Line Programm, das die Polynome $q_1, \ldots, q_s$ darstellt, zu einem Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe $(dL)^{O(1)}$, welches das Polynom $q = q_1 \ldots q_m$ ausrechnet. Wir interpolieren das Polynom q in der Variablen X_n wie oben beschrieben, und erhalten ein Straight–Line Programm β_1 in $\mathbb{Q}[X_1, \ldots, X_n]$ mit der Größe $(dL)^{O(1)}$, welches die Koeffizienten des Polynoms q bezüglich der Variable X_n darstellt. Das Straight–Line Programm β_1 läßt sich ohne Änderung in der Komplexität zu einen divisionsfreien Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ erweitern, welches die Diskriminante ϱ von q bezüglich der Variablen X_n und die Polynome $\varrho X_1, \ldots, \varrho X_{n-1}$ berechnet.
Sei das Polynom $p_n := \varrho X_n \in \mathbb{Q}[X_1, \ldots, X_{n-1}, X_n]$ definiert. Dann erfüllen die Polynome $\varrho \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$ und $q, p_n \in \mathbb{Q}[X_1, \ldots, X_{n-1}, X_n]$ die Bedingungen (i) - (iv) im Lemma 16 für $i = 0$. Weiterhin ist β_1 ein divisionsfreies Straight–Line Programm in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ der Größe $(dL)^{O(1)}$, welches ϱ und die Koeffizienten der Polynome q, p_n bezüglich der Variablen X_n berechnet. Die Ausgabe des Straight–Line Programms β_1 läßt sich aus dem Straight–Line Programm β durch ein erweitertes arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$ der Größe $(dL)^{O(1)}$ erzeugen. Damit ist der Beweis des ersten Schrittes unserer rekursiven Prozedur erbracht.

Wir betrachten nun den Fall $0 < i < n$ und setzen $r := n-(i+1)$. Wir nehmen an, daß ein divisionsfreies Straight–Line Programm β_{i-1} in $\mathbb{Q}[X_1,\ldots,X_{r+1}]$ der Größe Λ_{i-1} gegeben ist, welches das von Null verschiedene Polynom $\varrho\,' \in \mathbb{Q}[X_1,\ldots,X_{r+1}]$ und die Koeffizienten gewisser Polynome $q\,', p_{r+2}\,', \ldots, p_n\,' \in \mathbb{Q}[X_1,\ldots,X_{r+1},X_{r+2}]$ bezüglich der Variablen X_{r+2} darstellt. Diese Polynome haben die folgenden Eigenschaften: $q\,'$ hat den Leitkoeffizienten eins, ist bezüglich X_{r+2} separiert und erfüllt die Gradbedingung $\deg q\,' = \deg_{X_{r+2}} q\,' = \delta^*_{i-1}$. $\varrho\,'$ ist die Diskriminante von $q\,'$ bezüglich X_{r+2}, und die Polynome $p_{r+2}\,', \ldots, p_n\,'$ haben die Gradsschranke $\max\{\deg_{X_{r+2}} p_k\,' | r+2 \leq k \leq n\} < \delta^*_{i-1}$. Das Ideal $(q\,', \varrho\,'X_{r+2} - p_{r+2}\,', \ldots, \varrho\,'X_n - p_n\,')_{\varrho\,'}$ der Lokalisierung $\mathbb{Q}[X_1,\ldots,X_n]_{\varrho}$ ist das Verschwindungsideal der affinen Varietät $(W^*_{i-1})_{\varrho\,'}$. Wir bemerken, daß $(W^*_{i-1})_{\varrho\,'}$ eine Zariski–offene und dichte Teilmenge von (W^*_{i-1}) ist. Sei Z der Zariski–Abschluß in $\mathbb{C}^n$ von $\{x \in W^*_{i-1} | \frac{\partial f(x)}{\partial X_i} = 0, \Delta(x) \neq 0\}$. Wir haben $W_i^* \subset Z \subset W_i$ und Z enthält die Vereinigung aller reellen irreduziblen Komponenten von W_i. Insbesondere sind alle irreduziblen Komponenten von Z auch irreduzible Komponenten von W_i. Außerdem gilt die Ungleichung $\deg Z \leq d\delta^*_{i-1}$.

Um eine explizite Beschreibung der algebraischen Menge

$$\{x \in W^*_{i-1} | \frac{\partial f(x)}{\partial X_i} = 0\}$$

erzeugen zu können, wenden wir auf die Straight–Line Programme β_{i-1} und β, welche $\varrho\,', q\,', p_{r+2}\,', \ldots, p_n\,'$ und $\frac{\partial f(x)}{\partial X_i}$ repräsentieren, eine Prozedur an, welche die Aussage von Proposition 18 in [GHM+98] zugrunde liegt.
Vermögen dieses Algorithmus sind wir in der Lage, irreduzible Komponenten von $\{x \in W^*_{i-1} | \frac{\partial f(x)}{\partial X_i} = 0\}$, die in der Hyperfläche $\{x \in \mathbb{C}^n | \Delta(x) = 0\}$ liegen, zu eliminieren. Wir erhalten dadurch ein divisionsfreies Straight–Line Programm $\bar{\mu}$ in $\mathbb{Q}[X_1,\ldots,X_r]$ der Größe $i(L+\Lambda_{i-1})(d\delta^*_{i-1})$, welches das von Null verschiedene Polynom $\bar{\varrho} \in \mathbb{Q}[X_1,\ldots,X_r]$ und die Koeffizienten gewisser Polynome $\bar{q}, \bar{p}_{r+1}, \ldots, \bar{p}_n \in \mathbb{Q}[X_1,\ldots,X_{r+1}]$ bezüglich der Variablen X_{r+1} darstellt.

Letztere Polynome haben die folgenden Eigenschaften: $\bar{q}$ hat den Leitkoeffizienten eins, ist bezüglich X_{r+1} separiert und erfüllt die Gradbedingung $\deg \bar{q} = \deg_{X_{r+1}} \bar{q} = \deg Z$. Das Polynom $\bar{\varrho}$ ist die Diskriminante von $\bar{q}$ bezüglich X_{r+1}, und die Polynome $\bar{p}_{r+1}, \ldots, \bar{p}_n$ genügen der Gradsschranke

$$\max\{\deg_{X_{r+1}} \bar{p}_k | r+1 \leq k \leq n\} < \deg Z.$$

Das Ideal $(\bar{q}, \bar{\varrho}X_{r+1} - \bar{p}_{r+1}, \ldots, \bar{\varrho}X_n - \bar{p}_n)_{\bar{\varrho}}$ ist in der Lokalisierung $\mathbb{Q}[X_1,\ldots,X_n]_{\bar{\varrho}}$ das Verschwindungsideal der affinen Varietät $Z_{\bar{\varrho}}$. Wir bemerken weiterhin, daß $Z_{\bar{\varrho}}$ eine Zariski–offene und dichte Teilmenge von Z beschreibt.

Man findet nun (vgl. [GHM+98], insbesondere Proposition 15) ein arithmetisches Netzwerk $\mathcal{N}_i$ mit Parametern in $\mathbb{Q}$ der Größe $i(d\delta^*_{i-1}L\Lambda_{i-1})^{O(1)}$, welches aus β_{i-1} und β das oben angeführte Straight–Line Programm $\bar{\mu}$ erzeugt.

Seien $q_1, \ldots, q_s \in \mathbb{Q}[X_1, \ldots, X_{r+1}]$ die $\mathbb{Q}$-irreduziblen Faktoren von $\bar{q}$. Da das Polynom $\bar{q}$ den Leitkoeffizienten eins hat und bezüglich X_{r+1} separiert ist, gilt $\bar{q} = q_1 \ldots q_s$. Da die Variablen $X_1, \ldots, X_n$ generisch gewählt sind, können wir schlußfolgern, daß jede irreduzible Komponente der algebraischen Varietät Z durch exakt eines der irreduziblen Polynome $q_1, \ldots, q_s$ dargestellt wird. Dies bedeutet, daß die Varietät Z aus s irreduziblen Komponenten hat, seien es $C_1, \ldots, C_s$, so daß für jeden Index $1 \leq l \leq s$, die irreduzible Komponente C_l identisch mit dem Zariski–Abschluß in $\mathbb{C}^n$ der folgenden Menge ist:

$$\begin{aligned}\{x = (X_1, \ldots, X_n) \in \mathbb{C}^n | \quad & \bar{\varrho}(X_1, \ldots, X_r)X_{r+1} - \bar{p}_{r+1}(X_1, \ldots, X_{r+1}) = 0, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \bar{\varrho}(X_1, \ldots, X_r)X_n - \bar{p}_n(X_1, \ldots, X_{r+1}) = 0, \\ & q_l(X_1, \ldots, X_r) = 0, \bar{\varrho}(X_1, \ldots, X_r) \neq 0\}.\end{aligned}$$

Wir nehmen an, daß die reellen irreduziblen Komponenten von Z (und folglich auch die von W_i) auf diese Weise durch die Polynome $q_1, \ldots, q_m$ gegeben sind, und es sei $q := q_1 \ldots q_m$. Das Polynom q hat den Leitkoeffizienten eins, ist in X_{r+1} separiert und genügt der Gradsschranke $\deg q = \deg_{X_{r+1}} q = \delta_i^*$. Wir haben ferner $W_i^* = C_1 \cup \ldots \cup C_m$.

Wir suchen nun nach einem Straight–Line Programm μ, dessen Länge von der Ordnung $(id\delta_i^* L)^{O(1)}$ ist (und somit unabhängig von Größe Λ_{i-1} des Straight–Line Programms β_{i-1} ist), welches die Koeffizienten der Polynome $q_1, \ldots, q_s$, und damit das Polynom q darstellt. Wir erweitern das arithmetische Netzwerk $\mathcal{N}_i$ um $(id\delta_i^* L\Lambda_{i-1})^{O(1)}$ viele zusätzliche Knoten und finden (wie im Beweis von der Proposition 33 in [GHH+97]), einen *„genügend generischen "Lifting–Punkt* $t = (t_1, \ldots, t_r) \in \mathbb{Q}^r$ für die algebraische Varietät Z. Durch die generische Wahl des Punktes t können wir mit dem Hilbertschen Irreduzibilitätstheorem schlußfolgern, daß die Polynome $q_1(t, X_{r+1}), \ldots, q_s(t, X_{r+1})$ irreduzible Polynome in $\mathbb{Q}[X_{r+1}]$ sind. Damit stellt die Identität $\bar{q}(t, X_{r+1}) = q_1(t, X_{r+1}) \ldots q_s(t, X_{r+1})$ eine Zerlegung des Polynoms $\bar{q}(t, X_{r+1}) \in \mathbb{Q}[X_{r+1}]$ in seine irreduziblen Faktoren dar.
Wenn wir nun im Straight–Line Programm $\bar{\mu}$ die Variablen $X_1, \ldots, X_r$ auf die Werte $t_1, \ldots, t_r$ spezialisieren, so erhalten wir ein arithmetisches Netzwerk in $\mathbb{Q}$, das die Koeffizienten des univariaten Polynoms $\bar{q}(t, X_{r+1})$ darstellt. Wir fügen dem Netzwerk einige Sonderknoten hinzu, ohne seine Größe asymptotisch zu verändern, und können dann ohne Einschränkung der Allgemeinheit voraussetzen, daß $\mathcal{N}_i$ die von Null verschiedene rationale Zahl $\bar{\varrho}(t)$ und die Koeffizienten der univariaten Polynome $\bar{q}(t, X_{r+1}), \bar{p}_{r+1}(t, X_{r+1}), \ldots, \bar{p}_n(t, X_{r+1})$ darstellt. Wir bemerken weiterhin, daß $\deg \bar{q}(t, X_{r+1}) = \deg_{X_{r+1}} \bar{q} = \deg \bar{q} \leq d\delta_{i-1}^*$ gilt. Damit sind wir in der Lage, die irreduziblen Faktoren $q_1(t, X_{r+1}), \ldots, q_s(t, X_{r+1})$ von $\bar{q}(t, X_{r+1})$ durch einen Aufruf der erste Subroutine zu finden. Dieser Aufruf bringt Kosten $(d\delta_{i-1}^*)^{O(1)}$ mit sich.

Eine solche Erweiterung des Netzwerks $\mathcal{N}_i$ um Sonderknoten ohne Änderung seiner asymptotischen Größe, versetzt uns in die Lage vorauszusetzen, daß $\mathcal{N}_i$ für jeden Index $1 \leq l \leq s$ die rationale Zahl $\bar{\varrho}(t)$ und die Koeffizienten der Polynome $q_l(t, X_{r+1}), \bar{p}_{r+1}(t, X_{r+1}), \dots, \bar{p}_n(t, X_{r+1})$ darstellt.

Man beachte, daß $\mathcal{N}_i$ nun ein *erweitertes* arithmetisches Netzwerk ist.

Für einen fixierten Index l, $1 \leq l \leq s$, ist die Menge $C_l \cap (\{t\} \times \mathbb{C}^{n-r})$ die Lifting Faser des Punktes t in der irreduziblen Komponente C_l von Z. Die Polynome $q_l(t, X_{r+1})$, $\frac{1}{\bar{\varrho}(t)}\bar{p}_{r+1}(t, X_{r+1}), \dots, \frac{1}{\bar{\varrho}(t)}\bar{p}_n(t, X_{r+1})$ stellen eine geometrische Lösung der Lifting Faser dar. Dies bedeutet, daß die folgende Identität gilt:

$$C_l \cap (\{t\} \times \mathbb{C}^{n-r}) = \left\{ \left(t_1, \dots, t_r, \frac{\bar{p}_{r+1}(t,u)}{\bar{\varrho}(t)}, \dots, \frac{\bar{p}_n(t,u)}{\bar{\varrho}(t)} \right) | u \in \mathbb{C},\ q_l(t,u) = 0 \right\}$$

Wendet man jetzt den Algorithmus, den das Theorem 31, [GHH$^+$97] liefert auf den Input

$$\beta,\ t = (t_1, \dots t_r),\ \bar{\varrho}(t),\ q_l(t, X_{r+1}), \bar{p}_{r+1}(t, X_{r+1}), \dots, \bar{p}_n(t, X_{r+1})$$

an, so erhält man ein divisionsfreies Straight–Line Programm in $\mathbb{Q}[X_1, \dots, X_r]$ der Größe $(id \deg C_l L)^{O(1)}$, welches die Koeffizienten des Polynoms q_l bezüglich der Variablen X_{r+1} darstellt. Wir wiederholen dieses Vorgehen für jeden Index l, $1 \leq l \leq s$, und müssen stets einige Sonderknoten zum arithmetischen Netzwerk $\mathcal{N}_i$ hinzufügen, ohne jedoch seine asymptotische Größe zu ändern. Damit können wir annehmen, daß $\mathcal{N}_i$ ein divisionsfreies Straight–Line Programm in $\mathbb{Q}[X_1, \dots, X_r]$ erzeugt, welches die Koeffizienten der Polynome $q_1, \dots q_s$ bezüglich der Variablen X_r darstellt. Wie im Fall $i = 0$ können wir durch Aufruf der zweiten Subroutine Polynome $q_{m+1}, \dots, q_s$ streichen, die keine Nullstelle in $\mathbb{R}^n$ haben. Aus den übriggebliebenen Polynomen $q_1, \dots, q_m$ erzeugen wir das Polynom $q = q_1 \dots q_m$. Die durch das Streichen von $q_{m+1}, \dots, q_s$ und die Erzeugung von q hinzugekommenen Kosten sind von der Ordnung $(\sum_{l=1}^{s} id \deg C_l L)^{O(1)} = (id \deg Z L)^{O(1)} = (id\delta_{i-1}^* L)^{O(1)}$. Damit können wir ohne Einschränkung der Allgemeinheit annehmen, daß das erweiterte arithmetische Netzwerk $\mathcal{N}_i$ ein divisionsfreies Straight–Line Programm in $\mathbb{Q}[X_1, \dots, X_r]$ der Größe

$$\left(\sum_{l=1}^{s} id \deg C_l L \right)^{O(1)} = (id\delta_{i-1}^* L)^{O(1)}$$

erzeugt, welches die Koeffizienten des Polynoms q bezüglich der Variablen X_r darstellt. Wir bemerken, daß der Punkt $t \in \mathbb{Q}^r$ auch Lifting Punkt der algebraischen Varietät $W_i^* = \cup_{l=1}^{s} C_l$ ist. Damit ist die Lifting Faser von t in W_i^* durch die rationale Zahl $\bar{\varrho}(t)$ und die Koeffizienten folgender Polynome

$$q(t, X_{r+1}) \quad \text{und} \quad \bar{p}_{r+1}(t, X_{r+1}), \dots, \bar{p}_n(t, X_{r+1})$$

charakterisiert, die prinzipiell schon vom arithmetischen Netzwerk $\mathcal{N}_i$ ausgerechnet wurden. Eine erneute Anwendung obiger Methode auf den Input

$$\beta, t = (t_1, \dots, t_r), \bar{\varrho}(t), q(t, X_{r+1}), \bar{p}_{r+1}(t, X_{r+1}), \dots, \bar{p}_n(t, X_{r+1})$$

ergibt ein divisionsfreies Straight–Line Programm β_i in $\mathbb{Q}[X_1, \ldots, X_r]$ von der Größe $\Lambda_i = (id\delta_i^* L)^{O(1)}$. Dieses Straight–Line Programm β_i repräsentiert ein von Null verschiedenes Polynom $\varrho \in \mathbb{Q}[X_1, \ldots, X_r]$ und die Koeffizienten des Polynoms q bezüglich der Variablen X_{r+1}, sowie gewisse Polynome $p_{r+1}, \ldots, p_n$ im polynomialen Ring $\mathbb{Q}[X_1, \ldots, X_r, X_{r+1}]$, welche die Eigenschaften (i) - (iv) im Lemma 16 erfüllen.

Das erweiterte arithmetische Netzwerk $\mathcal{N}_i$ in $\mathbb{Q}$, das diese Ausgabe β_i aus dem Input β_{i-1} und β erzeugt, hat die Größe $(id\delta_{i-1}^* L\Lambda_{i-1})^{O(1)}$.
Man bemerke, daß die Länge Λ_i des Straight–Line Programms β_i unabhängig von der Länge Λ_{i-1} von β_{i-1} ist. Genauer gesagt, haben wir $\Lambda_i = (id\delta_i^* L)^{O(1)}$. Wegen der Ungleichung $\delta_i^* \leq d\delta_{i-1}^*$ und der Gleichung $\Lambda_{i-1} = ((i-1)d\delta_{i-1}^* L)^{O(1)}$ können wir schlußfolgern, daß die Größe des erweiterten arithmetischen Netzwerks $\mathcal{N}_i$, das aus den Input β_{i-1} und β den Output β_i erzeugt, von der Ordnung $(id\delta_i^* L)^{O(1)}$ ist. Indem wir die Netzwerke $\mathcal{N}_1, \ldots, \mathcal{N}_i$ nacheinander in dieser Reihenfolge verknüpfen, erhalten wir ein erweitertes arithmetisches Netzwerk $\mathcal{N}$ in $\mathbb{Q}$, welches das Straight–Line Programm β_i aus dem Input β erzeugt. Das Netzwerk $\mathcal{N}$ hat die Größe $(id\delta^* L)^{O(1)}$.

■

Mit Lemma 16 erhält man das folgende eigentliche Hauptergebnis für den Fall einer beschränkten reellen glatten Hyperfläche. Es präzisiert die Komplexitätsschranke des Theorem 15 in dem Sinne, daß anstelle des komplexes Grades δ des jeweiligen Gleichungssystems der reelle Grad δ^* der assoziierten polaren Varietäten tritt ($\delta^* \leq \delta$).

Satz 17
Seien n, d, δ^*, L ganzzahlige Größen. Dann gibt es ein erweitert arithmetisches Netzwerk $\mathcal{N}$ in $\mathbb{Q}$ der Größe $(nd\delta^* L)^{O(1)}$, das die folgenden Eigenschaften besitzt:
Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein nichtkonstantes Polynom mit einer Gradschranke d, welches durch ein divisionsfreies Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe L gegeben ist. Seien

$$\Delta := \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i} \right)^2, \quad W := \{x \in \mathbb{C}^n | f(x) = 0\}, \quad V := W \cap \mathbb{R}^n,$$

und seien die Variablen $X_1, \ldots, X_n$ generisch gewählt.
Wir setzen weiterhin voraus, daß die reelle Varietät V eine nicht–leere, beschränkte und glatte Hyperfläche des $\mathbb{R}^n$ mit regulärer Gleichung f darstellt.
Für $0 \leq i < n$ sei die Varietät W_i der Zariski–Abschluß der Menge

$$\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0, \Delta(x) \neq 0\} \quad \textit{und} \quad W_i^* := W_i \cap \mathbb{R}^n.$$

Sei $\delta_i^* := \deg^* W_i := \deg W_i^*$ der reelle Grad der komplexen Varietät W_i und wir setzen voraus, daß die Ungleichung $\delta^* \geq \max\{\delta_i^* | 0 \leq i < n\}$ gilt.

Der durch das erweiterte arithmetische Netzwerk $\mathcal{N}$ dargestellte Algorithmus startet mit dem Straight–Line Programm β als Input und erzeugt ein Straight–Line Programm in $\mathbb{Q}$ der Größe $(nd\delta^* L)^{O(1)}$. Dieses Straight–Line Programm stellt die Koeffizienten der $n+1$ univariaten Polynome $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ dar, welche die folgenden Bedingungen erfüllen:

(i) $\deg q = \delta^*_{n-1}$

(ii) $\max\{\deg p_i | 1 \leq i \leq n\} < \delta^*_{n-1}$

(iii) Jede Zusammenhangskomponente der reellen Hyperfläche V besitzt mindestens einen Punkt in der Menge

$$S := \{(p_1(u), \ldots, p_n(u)) | u \in \mathbb{R}, q(u) = 0\}.$$

Das erweiterte algorithmische Netzwerk $\mathcal{N}$ kodiert jede reelle Nullstelle u des Polynoms q (und somit auch die Elemente der null–dimensionalen reellen Varietät S) à la Thom.

Beweis:
Wir wenden das Lemma 16 auf den Schritt $i := n-1$ an. Damit ergibt sich der Beweis des Theorems 17, denn die restlichen Aussagen erhält man analog zum Beweis des Theorems 15 sind. ∎

3.3 Generische Koordinatenwahl

Der Algorithmus im vorstehenden Abschnitt benutzt zwei generischen Koordinatentransformationen, eine zur Auffindung transversaler Richtungen zu den betrachteten polaren Varietäten, und eine andere zur Darstellung der Koordinaten in Noether–Position. Wir verfahren Schritt für Schritt mit wachsendem Index $i, 0 \leq i \leq n-1$, und erzeugen reguläre rationale $(n \times n)-$Matrizen, die im Sinne des Algorithmus

1. die Noether–Normalisierung und
2. die Glattheit der polaren Varietäten

sichern.

Sei $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein nichtkonstantes quadratfreies Polynom. Wir betrachten die Hyperfläche $\{x \in \mathbb{C}^n | f(x) = 0\}$. Im Vektorraum $\mathbb{C}^n$ betrachten wir zwei Basen $\{e^1, \ldots, e^n)$ mit $e^i := (0, \ldots, \overset{i}{1}, \ldots, 0)$ und $\{v^1, \cdots, v^n\}$ mit $v^i,\ 1 \leq i \leq n$ lineare unabhängige Vektoren in $\mathbb{C}^n$. Für einen Punkt $x \in \mathbb{C}^n$ gilt

$$X = \sum_{i=1}^{n} X_j e^i = \sum_{k=1}^{n} Y_k v^k. \tag{3.7}$$

Der Übergang von der kanonischen Basis $\{e^1, \ldots, e^n\}$ zu einer Basis $\{v^1, \ldots, v^n\}$ wird durch die linearen Abbildung $\phi : \mathbb{C}^n \longrightarrow \mathbb{C}^n$, mit $\phi(e^i) = v^i$, realisiert.

Sei $i \in \mathbb{N}, 1 \leq i < n$, fest gewählt, und seien durch

$$Z_{i+1,1}, \ldots, Z_{n,1}, \ldots, Z_{i+1,i}, \ldots, Z_{n,i} \tag{3.8}$$

$(n-i)i$ Unbestimmte bezeichnet, die wir in Matrixform

$$Z^{(i)} := \begin{pmatrix} Z_{i+1,1} & \ldots & Z_{i+1,i} \\ \vdots & \ldots & \vdots \\ Z_{n,1} & \ldots & Z_{n,i} \end{pmatrix} \tag{3.9}$$

darstellen. Wir betrachten reguläre Matrizen der Gestalt

$$A^{(i)} := A^{(i)}(Z^{(i)}) := \begin{pmatrix} I_i & 0_{i,n-i} \\ Z^{(i)} & I_{n-i} \end{pmatrix}, \tag{3.10}$$

wobei I_k die entsprechende $k \times k$ Einheitsmatrix für $k = i, n-i$ und $0_{i,n-i}$ die $i \times (n-i)$ Nullmatrix ist.

Sei das Polynom $g(y) := f(A^{(i)}y) \in \mathbb{Q}[X_1, \ldots, X_n, Z_{i+1,1}, \ldots, Z_{n,i}]$ gegeben. Dann wird die Hyperfläche $W = \{x \in \mathbb{C}^n | \ f(x) = 0\}$ in $\mathbb{C}^n$ mittels der Koordinatentransformation $X = A^{(i)}Y$ in die Hyperfläche $W(Z) = \{y \in \mathbb{C}^n | \ g(y) = 0\}$ transformiert. Da $A^{(i)}$ eine reguläre Matrix ist, sind durch diese Transformation die irreduziblen Komponenten der Hyperflächen eineindeutig zugeordnet. Das Polynom g ist linear in den Variablen $Z_{i+1,1}, \ldots, Z_{n,i}$ und hat den gleichen Grad in den Variablen $Y_1, \ldots, Y_n$ wie f in $X_1, \ldots, X_n$. Ein Punkt $x \in \mathbb{C}^n$ liegt genau dann in der Hyperfläche W, wenn sein Urbild $(A^{(i)})^{-1}x$ in $W(Z)$ liegt.

Die zum linearen Unterraum $Y^i := \{y \in \mathbb{C}^n | \ y_{i+1} = \ldots = y_n = 0\}$ assoziierte polare Varietät W_i ist der Zariski–Abschluß der Menge

$$\left\{ y \in \mathbb{C}^n | \ g(y) = \frac{\partial g(y)}{\partial Y_1} = \cdots = \frac{\partial g(y)}{\partial Y_i} = 0, \ \sum_{k=1}^{n} \left(\frac{\partial g(y)}{\partial Y_k} \right)^2 \neq 0 \right\}. \tag{3.11}$$

Sei $F_0(x) := f(x)$ gegeben. Für Indizes $k \in \mathbb{N}, 1 \leq k \leq i \leq n-1$, definieren wir die Polynome

$$F_k := \frac{\partial f}{\partial X_k} + \sum_{j=i+1}^{n} Z_{jk} \frac{\partial f}{\partial X_j} \in \mathbb{Q}[X, Z]. \tag{3.12}$$

Die polare Varietät W_i ist eine Teilmenge der durch die Polynome $F_0, \ F_1, \ldots, F_i$ definierten Varietät.

Bemerkung 7
Falls die Polynome $F_0, \ldots, F_i, 0 \leq i < n$, eine transversale Folge außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | \ \Delta(x) = 0\}$ bildet, so läßt sich die simultane Noether–Normalisierung in [KP96] anwenden.

Wir können unsere Betrachtungen daher auf die Erzeugung solcher Parameter Z_{rs}, $i+1 \leq r \leq n$, $1 \leq s \leq i+1$, in der Matrix $A^{(i)}$ (i ist der Schrittindex $0 \leq i < n-1$) beschränken, so daß die zum linearen Raum $X^{i+1} = \{x \in \mathbb{C}^n | \, x_{i+2} = \ldots = x_n = 0\}$ assoziierte polare Varietät

$$W_i := \overline{\{x \in \mathbb{C}^n | F_0(x) = F_1(x) = \cdots = F_i(x) = 0, \Delta(x) \neq 0\}} \tag{3.13}$$

den linearen Raum $X^{i+1} = \{x \in \mathbb{C}^n | \, x_{i+2} = \ldots = x_n = 0\}$ transversal schneidet.

3.3.1 Die Resultante eines Polynoms und eines homogenen Ideals

Die Resultante eines homogenen Polynoms $g \in \mathbb{Q}[X_0, X_1, \ldots, X_n]$ mit einem ungemischten homogenen radikalen Ideal $J \subset \mathbb{Q}[X_0, X_1, \ldots, X_n]$ wird durch das folgende Lemma gegeben

Lemma 18 ([GHM+98], Lemma 16)
Sei J ein ungemischtes homogenes radikales Ideal in $\mathbb{Q}[X_0, X_1, \ldots, X_n]$, und sei der kanonische Morphismus

$$\phi : \mathbb{Q}[X_0, X_1, \ldots, X_{n-i}] \to Q[X_0, X_1, \ldots, X_n]/J$$

eine ganze Ringerweiterung. Dann hat das minimale Polynom

$$m_g \in Q[X_0, X_1, \ldots, X_{n-i}, T]$$

eines homogenen Polynoms $g \in \mathbb{Q}[X_0, X_1, \ldots, X_n]$ die Form

$$T^d + a_{d-1}T^{d-1} + \ldots + a_0,$$

wobei $d \leq \deg J$ ist, und die Koeffizienten $a_j, \in \mathbb{Q}[X_0, \ldots, X_{n-i}], 0 \leq j \leq d-1$ entweder Null, oder ein homogenes Polynom vom Grad $(d-j)\deg(g)$ ist.
Die gleiche Schlußfolgerung gilt, wenn wir das minimale Polynom m_g durch das charakteristische Polynom χ_g vom Polynom g ersetzen. Weiterhin ist das minimale Polynom quadratfrei, falls der Morphismus ϕ generisch unramifiziert ist, d.h. die zu ϕ assoziierte endliche Körpererweiterung separabel ist. In diesem Fall haben wir die Ungleichung $d \leq \deg V(J)$.

Bemerkung 8
Falls das Polynom $g \in Q[X_0, X_1, \ldots, X_n]$ kein Nullteiler modulo dem Ideal J ist, so ist sein konstantes Glied $a_0 \in \mathbb{Q}[X_0, X_1, \ldots, X_{n-i}]$ ein homogenes Polynom vom Grad $d\deg(g)$.

3.3.2 Die Diskriminante einer Abbildung

Sei $i, 0 \leq i < n$ fest gewählt. Wir betrachten die Koordinatentransformation $X = A^{(i)}Y$ mit $A^{(i)}$ nach (3.10). Die zur Varietät

$$\{x \in \mathbb{C}^n : F_0(x) \ = \ F_1(x) \ = \ldots = \ F_i(x) = 0\},$$

wobei die Polynome $F_1, \ldots, F_i$ gemäß (3.12) und $F_0(x) = g(A^{(i)}x) = f(x)$ definiert sind assoziierte Abbildung Φ_i ist gegeben durch $\Phi_i : \mathbb{C}^n \times \mathbb{C}^{i(n-i)} \longrightarrow \mathbb{C}^{i+1}$ $\Phi_i\,(X_1, \ldots, X_n, Z_{i+1,1}, \ldots, Z_{n,1}, \ldots, Z_{i+1,i}, \ldots, Z_{n,i}) =$

$$(F_0(X_1, \ldots, X_n),\ F_1(X_1, \ldots, X_n),\ \ldots, F_i(X_1, \ldots, X_n)),$$

wobei die Polynome $F_1, \ldots, F_i$ gemäß (3.12) und $F_0(x) = g((A^{(i)})^{-1}x) = f(x)$ definiert sind Das zur Faser $\Phi_i^{-1}(0)$ assoziierte kommutative Diagramm hat die Gestalt

$$\begin{tikzcd} \Phi_i^{-1}(0) \cap (R(W) \times \mathbb{C}^{i(n-i)}) \arrow[r, hook, "\imath_i"] \arrow[dr, "\pi_i"'] & \mathbb{C}^n \times \mathbb{C}^{i(n-i)} \arrow[d, "\mathrm{pr}_2"] \\ & \mathbb{C}^{i(n-i)} \end{tikzcd} , \tag{3.14}$$

wobei $\pi_i = \mathrm{pr}_2 \circ \imath_i$ ist. Sei zuerst

$$\alpha := (\alpha_1, \ldots, \alpha_{n+i(n-i)}) := (X_1, \ldots, X_n, Z_{i+1,1}, \ldots, Z_{n,i}) \in \mathbb{C}^n \times \mathbb{C}^{i(n-i)}.$$

Die tangentiale Abbildung von Φ_i ist genau dann eine Submersion, wenn die Parameter $Z_{i+1,1}, \ldots, Z_{n,i}$ nicht in der Diskriminante Ω_i von Φ_i liegen. Damit ist Φ_i transversal zu $\{0\}_{\mathbb{C}^{i+1}}$, und die Jacobimatrix $J_{X,A^{(i)}}\Phi_i(\alpha)$ in den Koordinaten $(X_1, \ldots, X_n, A^{(i)})$ hat maximalen Rang, nämlich $i+1$. Nach der algebraischen Version des impliziten Funktionentheorems ist $\Phi_i^{-1}(0)$ eine Untervarietät in $\mathbb{C}^n \times \mathbb{C}^{i(n-i)}$ und die Diskriminante Ω_i, die eine strikt positive Kodimension besitzt, ist vom Maß null, (vgl. [GG86], [Dem89]). Die Jacobimatrix $J_{X,A^{(i)}}(\Phi_i)(\alpha)$ der Abbildung Φ_i in α hat die Form

$$J_{X,A^{(i)}}(\Phi_i)(\alpha) = \begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \frac{\partial f}{\partial X_n} & 0 & & \cdots & 0 & & \cdots & \cdots & 0 \\ *_{11} & \cdots & *_{1n} & \frac{\partial f}{\partial X_{i+1}} & \cdots & \frac{\partial f}{\partial X_n} & 0 \cdots & & \vdots & 0 & \\ \vdots & & \vdots & \ddots & & \ddots & 0 & & \cdots & \ddots & 0 \\ *_{(i)1} & \cdots & *_{(i)n} & 0 \cdots & & 0 \cdots & \cdots & & \frac{\partial f}{\partial X_{i+1}} & \cdots & \frac{\partial f}{\partial X_n} \end{pmatrix} (\alpha),$$

wobei die Sterne in den Einträgen $*_{r,s}$, $1 \leq r \leq i$, $1 \leq s \leq n$, dieser Matrix die folgende Gestalt haben:

$$*_{r,s} := \frac{\partial^2 f}{\partial X_r \partial X_s} + \sum_{j=i+1}^{n} Z_{jr} \frac{\partial^2 f}{\partial X_j \partial X_s}.$$

Die Jacobimatrix $J_{X,A^{(i)}}(\Phi_i)(\alpha)$ von Φ_i ist eine Matrix mit $i+1$ Zeilen und $n+i(n-i)$ Spalten.

Wir betrachten die folgende $((i+1)\times n)-$Teilmatrix der Jacobimatrix $J_{X,A^{(i)}}(\Phi_i)$:

$$J_X(\Phi_i) := \begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \frac{\partial f}{\partial X_n} \\ *_{11} & \cdots & *_{1n} \\ \vdots & \ddots & \vdots \\ *_{(i)1} & \cdots & *_{(i)n} \end{pmatrix} \tag{3.15}$$

Sei Σ_i der kritische Ort von Φ_i. Σ_i ist der Durchschnitt der Faser $\Phi_i^{-1}(0)$ und der Determinantenvarietät

$$\{(x,a^{(i)}) \in \mathbb{C}^n \times \mathbb{C}^{i(n-i)} |\ M(k_1,\ldots,k_{i+1})(x,a^{(i)}) = 0,\ 1 \leq k_1 < \ldots < k_{i+1} \leq n\}, \tag{3.16}$$

wobei $M(k_1,\ldots,k_{i+1})(x,a^{(i)})$ der aus den Spalten $k_1,\ldots,k_{i+1}$ bestehende $(i+1)-$ Minor der Matrix $J_X(\Phi_i)(x,a^{(i)})$ ist. Die *Diskriminante* der Abbildung Φ_i ist durch die Menge

$$\Omega_i := \pi_i(\Sigma_i) = \Big\{a^{(i)} \in \mathbb{C}^{i(n-i)} | M(k_1,\ldots,k_{i+1})(x,a^{(i)}) = 0,$$

$$1 \leq k_1 < \ldots < k_{i+1} \leq n \text{ für alle } (x,a^{(i)}) \in \Phi_i^{-1}(0)\Big\} \tag{3.17}$$

definiert. Sie ist die Projektion von Σ_i auf den Parameterraum $\mathbb{C}^{i(n-i)}$. Der kritische Ort Σ_i von Φ_i wird auf der Faser $\Phi_i^{-1}(0)$ durch alle $(i+1)-$Minoren in $J_X(\Phi_i)$ definiert, und hat in der Faser $\Phi_i^{-1}(0)$ die Kodimension

$$\operatorname{codim}_{\Phi_i^{-1}(0)}(\Sigma_i) = (i+1-(i+1)+1)(n-(i+1)+1) = n-i. \tag{3.18}$$

Der kritische Ort Σ_i ist eine Determinantenvarietät und wird lokal durch $i+1+n-i = n+1$ Polynomiale Gleichungen in $\mathbb{Q}[X_1,\ldots,X_n,Z_{i+1,1},\ldots,Z_{n,i}]$ definiert.

Unter Benutzung eines effektiven Bertini–Verfahrens (vgl. [KP96]) finden wir eine $((n-i)\times \binom{n}{i+1})-$Matrix von Parametern

$$\Lambda := \begin{pmatrix} \lambda_{1,1} & \ldots & \lambda_{1,\binom{n}{i+1}} \\ \ldots & \ldots & \ldots \\ \lambda_{n-i,1} & \ldots & \lambda_{n-i,\binom{n}{i+1}} \end{pmatrix}, \tag{3.19}$$

so daß die Gleichungen

$$F_0,\ldots,F_i,G_1,\ldots,G_{n-i} \tag{3.20}$$

die Diskriminante Σ_i definieren, wobei

$$G_k := \sum_{j=1}^{\binom{n}{i+1}} \lambda_{k,j} M_j \tag{3.21}$$

gilt, und $M_j,\ 1 \leq j \leq \binom{n}{i+1}$ die verschiedenen $(i+1)-$Minoren der Matrix $J_X(\Phi_i)$ sind. Die n ersten Gleichungen

$$F_0, \dots, F_i, G_1, \dots, G_{n-(i+1)} \tag{3.22}$$

bilden ein null–dimensionalen System.

Sei D_i der Grad des Systems 3.22. Aus der Bézout–Ungleichung erhalten wir, (vgl. [Hei83]):

$$D_i \leq d(d-1)^i[(d-1)+i(d-2)]^{n-(i+1)} \leq (i+1)^{n-(i+1)}d^n \tag{3.23}$$

Ein Verfahren zur Darstellung der Variablen $X_1, \dots, X_n$ in generischer Position bezüglich $\widetilde{W}_i$ ist dadurch gegeben, indem wir eine geometrische Lösung des Systems (3.22) bestimmen, und damit die Parameter in der Matrix $A^{(i)}$ so wählen, daß die Resultante $Res_U(J_n(i), G_{n-i})$ des Ideals

$$J_n(i) := (F_0, \dots, F_i, G_1, \dots, G_{n-(i+1)})$$

und des Polynoms G_{n-i} nicht verschwindet.

Wir verzichten auf dieses Verfahren und verweisen auf [KP96] für eine effektive Wahl der neuen Parametermatrix Λ. Die Komplexitätsschranke eines solchen Verfahrens erweist sich als polynomial in $(i+1)^{n-i-1}d^{n+1}$ und somit die worst–case des Algorithmus im Kapitel 3 ergibt.

Der Nachteil dieser Methode ist die Einführung einer kombinatorischen Anzahl von Parametern

$$\lambda_{k,l},\ 1 \leq k \leq i+1,\ 1 \leq l \leq \binom{n}{i+1},$$

deren Höhe von der Ordnung $d^{O(n)}$ ist.

Wir geben im Kapitel 5 eine effektivere Methode zur Bestimmung generischer Koordinaten an, welche die Beschreibung der Determinantenvarietäten im Abschnitt 4.1 des Kapitels 4 benutzen wird. Dieses Verfahren vermeidet die Einführung neuer Parameter wie im obigen Verfahren à la *Bertini*.

Kapitel 4

Der vollständige Durchschnitt

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n],\ 1 \leq p \leq n$, mit beschränktem Grad $\deg f_k \leq d,\ \ d \geq 2,\ \forall k,\ 1 \leq k \leq p$. Wir setzen voraus, daß die Variablen $X_1, \ldots, X_n$ in generischer Position sind, und daß die Folge $f_1, \ldots, f_p$ eine reduzierte reguläre Folge in $\mathbb{Q}[X_1, \ldots, X_n]$ bildet.
Sei $X := (X_1, \ldots, X_n)$ der Variablenvektor.

Sei W die von den gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_p$ definierte affine Varietät, d.h.

$$W := V(f_1, \ldots, f_p) := \{x \in \mathbb{C}^n | f_1(x) = \ldots = f_p(x) = 0\} \tag{4.1}$$

ist nach Voraussetzung eine reduzierte vollständige Durchschnittsvarietät, insbesondere bedeutet, daß die Varietät $V(f_1, \ldots, f_i),\ \ 1 \leq i \leq p$ durch radikale Ideale $(f_1, \ldots, f_i)$ beschrieben werden.

Die entsprechende Jacobimatrix sei durch

$$J(f_1, \ldots, f_p) := \left(\frac{\partial f_k}{\partial X_j} \right)_{\substack{1 \leq k \leq p \\ 1 \leq j \leq n}}$$

gegeben und

$$J(f_1, \ldots, f_p)(x) := \left(\frac{\partial f_k}{\partial X_j}(x) \right)_{\substack{1 \leq k \leq p \\ 1 \leq j \leq n}}$$

bezeichnet die Jacobimatrix an der Stelle $x \in \mathbb{C}^n$.

Wie schon im Falle einer reellen Hyperfläche soll in diesem Kapitel gezeigt werden, daß sich die Algorithmen zur geometrischen Lösung polynomialer Gleichungssysteme zur Auffindung eines repräsentativen reellen Punktes in jeder Zusammenhangskomponenten einer affinen vollständigen Durchschnittsvarietät anwenden lassen.

Bindenglied zwischen dem komplexen und dem reellen Fall wird wiederum die Definition geeigneter polarer Varietäten sein.

Den Algorithmus, den wir ableiten wollen, wird wiederum seine Polynomialität in der Größe des die Polynome kodierenden Straight–Line Programms und dem affinen geometrischen Grad des mittels der polaren Varietät erhaltenen Gleichungssystems sein.

Definition 19
Für jeden Index i, $1 \leq i \leq n-p$, bezeichne Δ_i die Determinantenvarietät der gemeinsamen Nullstellen aller bis zur Spalte $\{1, \ldots, i+p-1\}$ aufgebauten $p-$Minoren der Jacobimatrix $J(f_1, \ldots, f_p)$, d.h. Δ_i ist durch alle $p-$Minoren der Untermatrix $J_1^{i+p-1}(f_1, \ldots, f_p)$ definiert, die durch die Spalten $\{1, \ldots, i+p-1\}$ der Jacobimatrix $J(f_1, \ldots, f_p)$ gebildet werden können.

Die gemeinsamen Nullstellen aller $p-$Minoren der Jacobimatrix $J(f_1, \ldots, f_p)$ sei die durch Δ_{n-p+1} bezeichnete Determinantenvarietät.

Wir definieren die affine Varietät

$$\widetilde{W}_i := W \cap \Delta_i. \tag{4.2}$$

Bemerkung 9 *Die affinen Varietäten $\widetilde{W}_i$, $1 \leq i \leq n-p$ werden hier eine ähnliche Rolle spielen, wie die gleichbezeichneten Varietät im Fall einer Hyperpläche ($p = 1$).*

Der Index i entpricht der zu erwartenden Kodimension der affinen Varietät $\widetilde{W}_i$ in W, d.h. codim $\widetilde{W}_i = p + i$.

Wie schon früher wollen wir Glattheit im folgenden Sinne verwenden.

Ein Punkt $x \in W = V(f_1, \ldots, f_p)$ heißt $(f_1, \ldots, f_p)$*–glatt*, wenn der Rang der Jacobimatrix in x maximal ist. Andernfalls ist der Punkt x ein $(f_1, \ldots, f_p)$*–singulärer* Punkt. Wenn es nicht zu Mißverständnissen führt, sprechen wir einfach von *glatten* bzw. *singulären* Punkten.

Bemerkung 10

- *Wenn $x \in W$ ein $(f_1, \ldots, f_p)$-glatter Punkt ist, schneiden die Hyperflächen*

  $$\{x \in \mathbb{C}^n \mid f_1(x) = 0\}, \ldots, \{x \in \mathbb{C}^n \mid f_p(x) = 0\}$$

  den Punkt x transversal.

- *Die algebraischen Mengen W_i, $0 \leq i \leq n-p$, bilden eine absteigende Folge*

  $$W \supset \widetilde{W}_1 \supset \cdots \supset \widetilde{W}_i \supset \cdots \supset \widetilde{W}_{n-p} \supset Sing\ W, \tag{4.3}$$

  wobei $Sing\ W$ die Menge der $(f_1, \ldots, f_p)$-singulären Punkte in W repräsentiert. Es gilt die Gleichung $Sing\ W = \widetilde{W}_{n-p+1} := W \cap \Delta_{n-p+1}$.

- *Die algebraischen Mengen Sing W und $\widetilde{W}_i$, $1 \leq i \leq n-p$, hängen von der Beschreibung durch die Polynome $f_1, \ldots, f_p$ und von der Lage der Variable $X_1, \ldots, X_n$ ab. Unter der Voraussetzung , daß das Ideal $(f_1, \ldots, f_p)$ radikal ist, stimmt Sing W mit der Menge der singulären Punkte von W im Sinne der Geometrie überein.*

In Analogie zum Hyperflächenfall definieren wir polare Varietäten W_i, $1 \leq i \leq n-p$, zum vollständigen Durchschnitt W.

Definition 20 *Sei $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ eine reduzierte reguläre Folge. Sei i beliebig fest, $1 \leq i \leq n-p$, und sei $\widetilde{W}_i$ die oben eingeführte affine Varietät, dann heißt*

$$W_i := \overline{\widetilde{W}_i \setminus Sing\ W} \tag{4.4}$$

die zum linearen Unterraum $X^{p+i-1} := \{x \in \mathbb{C}^n |\ x_{p+i} = \ldots = x_n = 0\}$ assoziierte <u>i–te polare Varietät.</u>

Wir werden in den nächsten zwei Abschnitten zeigen, daß die polaren Varietäten W_i außerhalb gewisser, angebbarer Hyperflächen entweder leer sind oder einen lokal vollständigen glatten Durchschnitt der Kodimension $p+i$ darstellen, für welchen wir eine lokal reguläre transversale Folge angeben können.

4.1 Lokale Beschreibung der Determinantenvarietäten

Wir benutzen im folgenden Abschnitt ein Lemma, das bestimmte Beziehungen zwischen den Minoren einer Matrix darstellt (vgl. [GH80]).

Sei A eine $(p \times n)$-Matrix mit Einträgen a_{ij} aus einem kommutativen Ring. Seien l und k natürliche Zahlen, mit $l \leq n$ und $k \leq min\{p,\ l\}$. Ferner sei $I_k := (i_1, \ldots, i_k)$ eine geordnete Folge von k verschiedenen Elementen einer endlichen Menge natürlicher Zahlen $\{1, \ldots, l\}$, die wir auch als eine geordnete Indexmenge $\{i_1, \ldots, i_k\}$ auffassen kann. Sei $C(l, k)$ die Menge der geordneten $k-$Tupel in $\{1, \cdots, l\}$. Sei $M_A\,(I_k) := M_A(i_1, \ldots, i_k)$ der aus den ersten k Zeilen und Spalten $i_1, \ldots, i_k$ bestehende k-Minor der Matrix A. Falls kein Mißverständnis auftritt, so schreiben wir $M_A\,(I_k) = M(i_1, \ldots, i_k)$.

Lemma 21 (Wechsellemma)
Seien die Indizes l und k wie oben gewählt. Für jede Matrix A und für je zwei Indexmengen $I_k = (i_1, \ldots, i_k)$ und $I_{k-1} = (j_1, \ldots, j_{k-1})$ mit nichtleerem Durchschnitt gilt die Gleichung

$$M\,(I_{k-1})\,M\,(I_k) = \sum_{j \in I_k \setminus I_{k-1}} \varepsilon_j\ \ M\,(I_k \setminus \{j\})\,M\,(I_{k-1} \cup \{j\})\,, \tag{4.5}$$

wobei ε_j die Werte $\{-1, 1\}$ annimmt.

Beweis:
Wir betrachten die folgende aus A aufgebaute $((2k-1)\times(2k-1))$-Matrix

$$L(I) := \left(\begin{array}{c|c} & L_1(I_k) \\ O & \vdots \\ & L_{k-1}(I_k) \\ \hline & \\ L_1(I_{k-1}) & L_1(I_k) \\ \vdots & \vdots \\ L_k(I_{k-1}) & L_k(I_k) \end{array}\right),$$

wobei für jeden Index $j,\ 1 \leq j \leq k,\ L_j\ (I_k)$ und $L_j\ (I_{k-1})$ Vektoren mit Einträgen in der $j-$ten Zeile der Matrix A bezeichnen, deren Elementen in den Spalten $i_1, \ldots, i_k$ bzw. $j_1, \ldots, j_{k-1}$ von A liegen.
Wir erhalten die gewünschte Gleichung, indem wir die Determinante der obige Matrix $((2k-1)\times(2k-1))$–Matrix auf zwei verschiedene Weisen nach Laplace entwickeln.

Sei $\sigma = (i_1, \cdots, i_{k-1}) \in C(2k-1, k-1)$ eine Permutation von $k-1$ Elementen in $\{k, \cdots, 2k-1\}$, wobei $k \leq i_1 < \cdots < i_{k-1} \leq 2k-1$. Das Komplement von σ in $\{1, \ldots, 2k-1\}$ ist $\bar{\sigma} := \{1, \ldots, 2k-1\} \setminus \sigma \in C(2k-1, k)$.

Unter Berücksichtigung der Permutation $(k, \cdots, 2k-1)$ und ihres Komplements $(1, \cdots, k-1)$, erhalten wir nach Laplace:

$$det(L(I)) = \sum_{\tau \in C(2k-1,k)} \varepsilon(\tau\bar{\tau}) M(L(I)_\tau) M(L(I)_{\bar{\tau}}) = \varepsilon M_A(I_k) M_A(I_{k-1}), \tag{4.6}$$

wobei die Permutation $\tau \in C(2k-1, k)$ in der Formel die Zeilen in $L(I)$ angibt, die zum Aufbau der Matrix $L(I)_\tau$ dienen: Sei z. B. $\tau_0 = (k, \ldots, 2k-1) \in C(2k-1, k)$. Dann gilt

$$L(I)_{\tau_0} = \begin{vmatrix} L_k(I_k) \\ \ddots \\ L_{2k-1}(I_k) \end{vmatrix}.$$

Andererseits gilt:

$$\begin{aligned} det(L(I)) &= \sum_{\sigma \in C(k,k-1)} \varepsilon(\sigma) M_A(I_k \setminus \{i \notin \sigma\}) M_A(I_{m-1} \cup \{i\}) \ = \\ &= \sum_{i \in I_k \setminus I_q} \varepsilon_i M_A(I_k \setminus \{i\}) \times M_A(I_{k-1} \cup \{i\}). \end{aligned}$$

■

Wir bezeichnen mit $m \in \mathbb{Q}[X_1, \ldots, X_n]$ den aus den ersten $(p-1)$ Zeilen und Spalten bestehenden $(p-1)$–Minor der Jacobimatrix $J(f_1, \ldots, f_p)$, d.h.

$$m := det \left(\frac{\partial f_k}{\partial X_j} \right)_{\substack{1 \leq k \leq p-1 \\ 1 \leq j \leq p-1}} . \tag{4.7}$$

Da $m \in \mathbb{Q}[X_1, \ldots, X_n]$, ist $\{x \in \mathbb{C}^n \mid m(x) = 0\}$ eine Hyperfläche in $\mathbb{C}^n$. Wir betrachten die Determinantenvarietät Δ_i außerhalb dieser Hyperfläche und bezeichnet mit $(\Delta_i)_m$ die Lokalisierung der Determinantenvarietät Δ_i außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | m(x) = 0\}$, d.h.

$$(\Delta_i)_m := \{x \in C^n | x \in \Delta_i, \ m(x) \neq 0\}.$$

Sei

$$M(f_1, \ldots, f_p)(i_1, \ldots, i_p) := M(i_1, \ldots, i_p)$$

der durch alle p Zeilen und die Spalten $i_1, \ldots, i_p$ der Jacobimatrix $J(f_1, \ldots, f_p)$ definierte $p-$Minor in $\mathbb{Q}[X_1, \ldots, X_n]$ und sei

$$M(f_1, \ldots, f_p)(i_1, \ldots, i_p)(x) = M(i_1, \ldots, i_p)(x)$$

die Spezialisierung dieses $p-$Minors im Punkt $x \in \mathbb{C}^n$.

Behauptung 22
Sei i, $1 \leq i \leq n-p$, beliebig fixiert, und sei m der oben definierte $(p-1)$–Minor. Dann ist die Determinantenvarietät Δ_i lokal, außerhalb der Hyperfläche $\{x \in \mathbb{C}^n \mid m(x) = 0\}$, durch die folgenden i polynomialen Gleichungen beschrieben

$$M_p = M_{p+1} = \ldots = M_{p+i-1} = 0, \tag{4.8}$$

d.h.

$$(\Delta_i)_m := \{x \in \mathbb{C}^n \mid m(x) \neq 0, M_s(x) = 0, s \in \{p, \ldots, p+i-1\}\},$$

wobei

$$M_s := M(1, \ldots, p-1, s) \tag{4.9}$$

den aus den ersten $(p-1)$ Spalten und der Spalte s, $(s \leq p+i-1)$ bestehenden $p-$Minor der Jacobimatrix $J(f_1, \ldots, f_p)$ bezeichnet.

Beweis.

Wir zeigen nur die Inklusion

$$(\Delta_i)_m \supset \{x \in \mathbb{C}^n \mid m(x) \neq 0, M(1, \ldots, p-1, s) = 0, s \in \{p, \ldots, i+p-1\}\},$$

da die andere Inklusion aus der Definition von Δ_i folgt. Sei ein Punkt $x^* \in \mathbb{C}^n$ so gewählt, daß $m(x^*) \neq 0$ und $M(1,\ldots,p-1,s)(x^*) = 0, s \in \{p,\ldots,i+p-1\}$ gelten. Wir zeigen, daß die Gleichungen

$$M(i_1,\ldots,i_p)(x^*) = 0 \text{ für alle } (i_1,\ldots,i_p) \text{ in } \{1,\ldots,i+p-1\}$$

gelten. Wir erhalten die Gleichung

$$m(x^*)M(i_1,\ldots,i_p)(x^*) =$$

$$= \sum_{j\in\{i_1,\ldots,i_p\}\setminus\{1,\ldots,p-1\}} \varepsilon_j \;\; M\left(\{i_1,\ldots,i_p\}\setminus\{j\}\right)(x^*)M(1,\ldots,p-1,j)(x^*),$$

indem wir die Polynome $M\left(I_{k-1}\right) = m = M(1,\ldots,p-1)$ und $M\left(I_k\right) = M(i_1,\ldots,i_p)$ auf der rechten Seite der Gleichung (4.5) des Wechsellemmas 21 substituieren und die daraus entstehende Gleichung im Punkt x^* berücksichtigen. Der Punkt x^* liegt dann in $(\Delta_i)_m$, da die Ungleichung $m(x^*) \neq 0$ gilt und die Gleichungen $M(1,\ldots,p-1,j)(x^*) = 0$ für alle $j \in \{p,\ldots,i+p-1\}$ realisiert sind.

■

Bemerkung 11

- *Behauptung 22 hat zur Folge, daß die Kodimension der Varietät Δ_i außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | \; m(x) = 0\}$ höchstens i sein kann.*
- *Behauptung 22 ist auch für den Index $i = n-p+1$ richtig. Die Determinantenvarietät Δ_{n-p+1}, läßt sich außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | \; m(x) = 0\}$, durch die folgenden $n-p+1$ polynomialen Gleichungen beschreiben*

$$(\Delta_{n-p+1})_m := \{x \in \mathbb{C}^n | \; M(1,\ldots,p-1,s)(x) = 0, \; s \in \{p,\ldots,n\}\}. \quad (4.10)$$

- *Die Argumentation über die Lokalisierung bezüglich des $(p-1)-$Minors m bleibt bei entsprechender Notation für jeden beliebigen $(p-1)-$Minor der Jacobimatrix $J(f_1,\ldots,f_p)$ gültig, so daß die Behauptung 22 sinngemäß für einen beliebigen $(p-1)-$Minor von $J(f_1,\ldots,f_p)$ gilt.*

4.2 Lokale Beschreibung der Varietäten

Das Ziel dieses Abschnittes besteht darin, zu zeigen daß die folgende Aussage gilt:

Falls die Variablen $X_1,\ldots,X_n$ in generischer Position bezüglich der Folge $f_1,\ldots,f_p$ sind, und $\widetilde{m}$ ein beliebiger $(p-1)$–Minor der Jacobimatrix $J(f_1,\ldots,f_p)$ ist, dann bildet jede polare Varietät W_i, $1 \le i \le n-p$, außerhalb der abgeschlossenen Menge $(Sing\ W) \cup \{x \in \mathbb{C}^n \mid \widetilde{m}(x) = 0\}$ einen lokal glatten vollständigen Durchschnitt.

Wir können eine lokal reguläre transversale Folge angeben, welche die polare Varietät W_i, $1 \le i \le n-p$, außerhalb von

$$(Sing\ W) \cup \{x \in \mathbb{C}^n \mid \widetilde{m}(x) = 0\}$$

beschreibt.
Sei $m \in \mathbb{Q}[X_1, \ldots, X_n]$ der aus den ersten $(p-1)$ Zeilen und Spalten der Jacobimatrix $J(f_1, \ldots, f_p)$ bestehende $(p-1)-$Minor.

Sei A eine reguläre $(n \times n)-$Matrix. Wir betrachten den Koordinatenwechsel $X = AY$, wobei $Y := (Y_1, \ldots, Y_n)$ der aus den neuen Variablen bestehende Vektor ist. Wir führen neue Polynome

$$g_1(Y) := f_1(AY), \ldots, g_p(Y) := f_p(AY),$$

ein. Ihre Jacobimatrix bezüglich den neuen Koordinaten ist

$$J(g_1, \ldots, g_p) := \left[\frac{\partial g_k}{\partial Y_j}\right]_{\substack{1 \le k \le p \\ 1 \le j \le n}} = J(f_1, \ldots, f_p)A.$$

Wir bezeichnen mit

$$\widetilde{M}(i_1, \ldots, i_p) := \widetilde{M}(g_1, \ldots, g_p)(i_1, \ldots, i_p)$$

den p–Minor der transformierten Jacobimatrix $J(g_1, \ldots, g_p)$, und schreiben $\widetilde{M}_j$ für den aus den ersten $p-1$ Spalten der Jacobimatrix $J(g_1, \ldots, g_p)$ und der Spalte $j \in \{p, \ldots, n\}$, bestehenden $p-$Minor $\widetilde{M}(1, \ldots, p-1, j)$.

Sei

$$Z := \begin{bmatrix} 1 & 0 & & 0 & & & \cdots & 0 \\ Z_{p+1,p} & 1 & & & & & & \\ \vdots & \vdots & \ddots & & \mathrm{O} & & & \vdots \\ Z_{p+i-1,p} & Z_{p+i-1,p+1} & \cdots & 1 & & & & \\ Z_{p+i,p} & Z_{p+i,p+1} & \cdots & Z_{p+i,p+i-1} & 1 & & & \\ \vdots & \vdots & & \vdots & \vdots & \ddots & & 0 \\ Z_{n,p} & Z_{n,p+1} & \cdots & Z_{n,p+i-1} & Z_{n,p+i} & Z_{n,p+i+1} & \cdots & 1 \end{bmatrix}, \quad (4.11)$$

eine $(n-p+1) \times (n-p+1)$–Matrix von Parametern $Z_{r,t}$. Wir bilden nun eine von Z abhängige reguläre $(n \times n)-$Matrix $A := A(Z)$, die zum Beweis unsere Behauptung geeignet ist.

Sei der Index i, $1 \le i \le n-p$, fixiert. Wir betrachten die Varietät $\widetilde{W}_i$ außerhalb der Hyperfläche $\{x \in \mathbb{C}^n \mid m(x) = 0\}$. In bezug auf den Index i zerlegen wir die Matrix Z in (4.11) folgendermaßen

$$Z = \begin{bmatrix} Z_1^{(i)} & O_{i,n-p-i+1} \\ Z^{(i)} & Z_2^{(i)} \end{bmatrix}, \tag{4.12}$$

wobei $Z^{(i)}$ in (4.12) durch

$$Z^{(i)} := \begin{bmatrix} Z_{p+i,p} & \dots & Z_{p+i,p+i-1} \\ \dots & \dots & \dots \\ Z_{np} & \dots & Z_{n,p+i-1} \end{bmatrix},$$

definiert ist, und $Z_1^{(i)}$ und $Z_2^{(i)}$ untere Dreiecksmatrizen sind.O ist eine Null–Matrix entsprechender Größe ist. Wir definieren die folgende reguläre $(n \times n)-$Matrix

$$A := A(Z) := \begin{bmatrix} I_{p-1} & O_{p-1,i} & O_{p-1,n-p-i+1} \\ O_{i,p-1} & Z_1^{(i)} & O_{i,n-p-i+1} \\ O_{n-p-i+1,p-1} & Z^{(i)} & Z_2^{(i)} \end{bmatrix}, \tag{4.13}$$

wobei I und O in (4.13) entsprechende Einheits– und Null–Matrizen sind, $Z^{(i)}, Z_1^{(i)}$, und $Z_2^{(i)}$ bilden die in (4.12) eingeführten Matrix von Parametern Z. Wie die Matrix Z enthält die Matrix A in (4.13)

$$s := \frac{(n-p)(n-p+1)}{2}$$

Parameter $Z_{r,t}$. Die Spezialisierung dieser Parameter ergibt einen Punkt z im affinen Raum $\mathbb{C}^s$.

Wir betrachten den durch $X = AY$ gegebenen Koordinatenwechsel, wobei $A := A(Z)$ gilt. Wir berechnen die Jacobimatrix $J(g_1, \dots, g_p)$ der neuen Polynome $g_1, \dots, g_p$ bezüglich der neuen Variablen $Y_1, \dots, Y_n$.

In bezug auf die Struktur der Matrix $A = A(Z)$ für einen festen Index $i, 1 \le i \le n-p$, zerlegen wir die Jacobimatrix $J(f_1, \dots, f_p)$ in drei Teilmatrizen

$$J(f_1, \dots, f_p) = \begin{bmatrix} U & V & W \end{bmatrix}, \tag{4.14}$$

wobei

$$U := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1 \le k \le p \\ 1 \le j \le p-1}}, \; V := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1 \le k \le p \\ p \le j \le p+i-1}}, \; W := \left[\frac{\partial f_k}{\partial X_j}\right]_{\substack{1 \le k \le p \\ p+i \le j \le n}},$$

in (4.14) gelten. Da $J(g_1,\dots,g_p) = J(f_1,\dots,f_p)\ A$ ist, hat die neue Jacobimatrix die Form

$$J(g_1,\dots,g_p) := \left[\frac{\partial g_k}{\partial Y_j}\right]_{\substack{1\le k\le p\\ 1\le j\le n}} = \left[\begin{array}{ccc} U & VZ_1^{(i)} + WZ^{(i)} & WZ_2^{(i)} \end{array}\right]. \tag{4.15}$$

Wir sind an der lokalen Beschreibung der Varietät $\widetilde{W}_i = W \cap \Delta_i$ außerhalb der Hyperfläche $\{x \in \mathbb{C}^n \mid m(x) = 0\}$ interessiert, wobei der fixierte $(p-1)-$Minor m aus der Teilmatrix U durch Streichen der letzten Zeile entsteht. Da die Teilmatrix U konstant bleibt bei der Koordinatentransformation $X = AY$, bleibt der Minor m unter dieser Transformation auch unverändert. Durch die Behauptung 22 weißt man, daß die Lokalisierung $(\Delta_i)_m$ durch die folgenden i Gleichungen beschrieben ist:

$$M_p(x) = \cdots = M_{p+i-1}(x) = 0; \tag{4.16}$$

Wir haben hier

$$M_j(x) := M(1,\dots,p-1,j)(x),\ j = p,\dots,p+i-1$$

gesetzt. Die $p-$Minoren $M_p,\dots,M_{p+i-1}$, die diese Gleichungen definieren, sind aus dem Teil $[\,U\ \ V]$ der Jacobimatrix $J(f_1,\dots,f_p)$ aufgebaut. Da dieser Teil in die Teilmatrix

$$\left[U\ \ VZ_1^{(i)} + WZ^{(i)}\right], \tag{4.17}$$

von $J(g_1,\dots,g_p)$ transformiert wird, sind die $p-$Minoren $M_p,\dots,M_{p+i-1}$ in die $p-$Minoren

$$\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1},$$

aus der Matrix in (4.17) transformiert, daß die folgende Matrizenidentität gilt:

$$\left[\widetilde{M}_p,\dots,\widetilde{M}_{p+i-1}\right] = [M_p,\dots,M_{p+i-1}]\ Z_1^{(i)} + [M_{p+i},\dots,M_n]\ Z^{(i)} \tag{4.18}$$

Die Koordinatentransformation $X = A(Z)Y$ induziert für jeden gewählten Index i, $1 \le i \le n-p$, einen Morphismus affiner Räume

$$\Phi_i :\ \mathbb{C}^n \times \mathbb{C}^s \to \mathbb{C}^p \times \mathbb{C}^i,$$

definiert durch

$$(x,z) \longmapsto \Phi_i(x,z) := \left(\, f_1(x),\dots,f_p(x), \widetilde{M}_p(x,z),\dots,\widetilde{M}_{p+i-1}(x,z)\,\right).$$

Die Nullfaser $\Phi_i^{-1}(0)$ dieses Morphismus enthält die Menge

$$(W_i^z)_m := W \cap (\Delta_i^z)_m\,, \tag{4.19}$$

wobei Δ_i^z die durch alle $p-$Minoren der Teilmatrix $\left[U\ \ VZ_1^{(i)}(z) + WZ^{(i)}(z)\right]$ der Jacobimatrix $J(g_1,\dots,g_p)$ spezialisiert in einem beliebig gewähltem $z \in \mathbb{C}^s$ ist.

Anders gesagt, für ein beliebiges gewähltes $z \in \mathbb{C}^s$ enthält die Nullfaser $\Phi_i^{-1}(0)$ des Morphismus Φ_i die transformierte Varietät W_i^z ausgedrückt in den alten Koordinaten außerhalb der Hyperfläche $\{x \in \mathbb{C}^n \mid m(x) = 0\}$.

Wir müssen nun den Rang der Jacobimatrix des Morphismus Φ_i untersuchen. Unter Benutzung der Zerlegung der Parametermatrix Z in die drei Teile $Z^{(i)}$, $Z_1^{(i)}$ und $Z_2^{(i)}$ können wir die Jacobimatrix $J(\Phi_i)$ des Morphismus Φ_i symbolisch in der Form

$$J(\Phi_i) = \begin{bmatrix} \dfrac{\partial \Phi_i}{\partial X} & \dfrac{\partial \Phi_i}{\partial Z^{(i)}} & \dfrac{\partial \Phi_i}{\partial Z_1^{(i)}} & \dfrac{\partial \Phi_i}{\partial Z_2^{(i)}} \end{bmatrix} \tag{4.20}$$

schreiben, und es gilt

$$\begin{bmatrix} \dfrac{\partial \Phi_i}{\partial X} & \dfrac{\partial \Phi_i}{\partial Z^{(i)}} \end{bmatrix} = \begin{bmatrix} J(f_1, \ldots, f_p) & O_{p,n-p-i+1} & \cdots & O_{p,n-p-i+1} \\ * & \left[\frac{\partial \widetilde{M}_p}{\partial Z_{p+i,p}}, \ldots, \frac{\partial \widetilde{M}_p}{\partial Z_{np}}\right] & \cdots & O_{1,n-p-i+1} \\ \vdots & \vdots & \ddots & \vdots \\ * & O_{1,n-p-i+1} & \cdots & \left[\frac{\partial \widetilde{M}_{p+i-1}}{\partial Z_{p+i,p+i-1}}, \ldots, \frac{\partial \widetilde{M}_{p+i-1}}{\partial Z_{n,p+i-1}}\right] \end{bmatrix},$$

wobei die Spalten dieser Teilmatrix durch die partiellen Ableitungen von Φ_i bezüglich der Variablen

$$X_1, \ldots, X_n, Z_{p+i,p}, \ldots, Z_{n,p}, \ldots, Z_{p+i,p+i-1}, \ldots, Z_{n,p+i-1}$$

in dieser Reihenfolge gegeben sind. Die Einträge $O_{r,t}$ bezeichnen Null–Matrizen entsprechender Größe. Die durch „ $*$ “ bezeichneten Zeilenmatrizen stellen die partiellen Ableitungen der Minoren $\widetilde{M}_p, \ldots, \widetilde{M}_{p+i-1}$ bezüglich der Variablen $X_1, \ldots, X_n$ dar, welche für unsere Untersuchungen irrelevant sind.

Wir haben weiterhin

$$\begin{bmatrix} \dfrac{\partial \Phi_i}{\partial Z_1^{(i)}} \end{bmatrix} = \begin{bmatrix} O_{p,i-1} & O_{p,i-2} & \cdots & 0 \\ \left[\frac{\partial \widetilde{M}_p}{\partial Z_{p+1,p}}, \ldots, \frac{\partial \widetilde{M}_p}{\partial Z_{p+i-1,p}}\right] & O_{1,i-2} & \cdots & 0 \\ O_{1,i-1} & \left[\frac{\partial \widetilde{M}_{p+1}}{\partial Z_{p+2,p+1}}, \ldots, \frac{\partial \widetilde{M}_p}{\partial Z_{p+i-1,p+1}}\right] & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ O_{1,i-1} & O_{1,i-2} & \cdots & \left[\frac{\partial \widetilde{M}_{p+i-1}}{\partial Z_{p+i-1,p+i-2}}\right] \\ O_{1,i-1} & O_{1,i-2} & \cdots & 0 \end{bmatrix},$$

und die letzte Teilmatrix $\begin{bmatrix} \dfrac{\partial \Phi_i}{\partial Z_2^{(i)}} \end{bmatrix}$ von $J(\Phi_i)$ in der Zerlegung (4.20) dieser Jacobimatrix ist eine Null–Matrix, da die $p-$Minoren $\widetilde{M}_p, \ldots, \widetilde{M}_{p+i-1}$ unabhängig von den Parametern $Z_{r,t}$ sind, die in der Teilmatrix $Z_2^{(i)}$ zusammengefaßt sind.

Wir können nun schlußfolgern, daß die Jacobimatrix $J(\Phi_i)$ von vollem Rang $p+i$ ist, wenn die Teilmatrix

$$\widetilde{J}(\Phi_i) := \left[\frac{\partial \Phi_i}{\partial X} \; \frac{\partial \Phi_i}{\partial Z^{(i)}}\right] \tag{4.21}$$

in (4.20) den maximalen Rang $p+i$ hat.

Für die i Zeilenmatrizen in $\widetilde{J}(\Phi_i)$ erhalten wir mit (4.18) die Identität

$$\left[\frac{\partial \widetilde{M}_j}{\partial Z_{p+i,j}}, \ldots, \frac{\partial \widetilde{M}_j}{\partial Z_{n,j}}\right] = [\, M_{p+i}, \ldots, M_n] \,. \tag{4.22}$$

Hiermit haben wir die Darstellung

$$\widetilde{J}(\Phi_i) = \begin{bmatrix} J(f_1,\ldots,f_p) & O_{p,n-p-i+1} & \cdots & O_{p,n-p-i+1} \\ * & [M_{p+i},\ldots,M_n] & \cdots & O_{1,n-p-i+1} \\ \vdots & \vdots & \ddots & \vdots \\ * & O_{1,n-p-i+1} & \cdots & [M_{p+i},\ldots,M_n] \end{bmatrix}. \tag{4.23}$$

Da alle Einträge in (4.23) der Teilmatrix $\widetilde{J}(\Phi_i)$ von $J(\Phi_i)$ zu $\mathbb{Q}[X_1,\ldots,X_n]$ gehören, hängt der Rang von $J(\Phi_i)$ im Punkt $(x,z) \in \mathbb{C}^n \times \mathbb{C}^s$ tatsächlich nur von der Wahl von $x \in \mathbb{C}^n$ ab.

Gemäß unserer Lokalisierung außerhalb von $\{x \in \mathbb{C}^n | \; m(x) = 0\}$ betrachten wir einen $(f_1,\ldots,f_p)-$glatten Punkt $\widetilde{x} \in W = V(f_1,\ldots,f_p)$, so daß $m(x) \neq 0$ ist.

Angenommen, die Matrix $\widetilde{J}(\Phi_i)(\widetilde{x})$ ist nicht von vollem Rang, d.h.

$$\mathrm{rk}\; \widetilde{J}(\Phi_i)(\widetilde{x}) < p+i. \tag{4.24}$$

Diese Ungleichung in (4.24) ist dann und nur dann richtig, falls alle $p-$Minoren $M_{p+i},\ldots,M_n$ der Jacobimatrix $J(f_1,\ldots,f_p)$ in $\tilde{x}$ verschwinden. Sei $\tilde{z} \in \mathbb{C}^s$ beliebig gewählt, so daß das Paar $(\tilde{x},\tilde{z})$ in der Faser $\Phi_i^{-1}(0)$ des Morphismus Φ_i liegt. Dann müssen die $p-$Minoren $\widetilde{M}_p,\ldots,\widetilde{M}_{p+i-1}$ der transformierten Jacobimatrix $J(g_1,\ldots,g_p)$ alle in $(\tilde{x},\tilde{z})$ verschwinden und mit der Gleichung (4.18) heißt das

$$[0,\ldots,0] = [M_p(\tilde{x}),\ldots,M_{p+i-1}(\tilde{x})] \; Z_1^{(i)}(\tilde{z}), \tag{4.25}$$

wobei $Z_1^{(i)}(\tilde{z})$ besagt, daß die Matrix $Z_1^{(i)}$ im Punkt $(\tilde{z}) \in \mathbb{C}^s$ spezialisiert ist. Da die Teilmatrix $Z_1^{(i)}$ eine untere Dreiecksmatrix mit lauter Eins auf der Diagonal ist (vgl. 4.12), gilt die letztere Matrizenidentität genau dann, wenn die folgenden Gleichungen gelten

$$M_{p+i-1}(\tilde{x}) = \cdots = M_p(\tilde{x}) = 0.$$

Damit implizieren unsere Voraussetzungen an $\tilde{x}$ und $\tilde{z}$

$$m(\tilde{x}) \neq 0, M_p(\tilde{x}) = \cdots = M_n(\tilde{x}) = 0. \tag{4.26}$$

Mit der Gleichung (4.10) in der Bemerkung 11 heißt dies, daß die Jacobimatrix $J(f_1, \ldots, f_p)(\tilde{x})$ singulär ist. Damit kann der Punkt $\tilde{x}$ kein glatter Punkt in der Varietät W sein, d.h., $\tilde{x} \in Sing\ W$, was unserer Annahme widerspricht.

Sei nun ein Punkt $(\bar{x}, z) \in \mathbb{C}^n \times \mathbb{C}^s$ in der Faser $\Phi_i^{-1}(0)$ gegeben. Dann liegt der Punkt $\bar{x}$ in W. Wir setzen weiterhin voraus, daß $\bar{x}$ ein glatter Punkt von W außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | m(x) = 0\}$ ist. Sei $\tilde{U}$ eine Zariski–offene Umgebung von $\bar{x}$, welche aus allen glatten Punkten von W besteht, die nicht in der Hyperfläche $\{x \in \mathbb{C}^n |\ m(x) = 0\}$ liegen, d.h.,

$$\widetilde{U} := \mathbb{C}^n \setminus (Sing\ W \cup \{x \in \mathbb{C}^n |\ m(x) = 0\})\,. \tag{4.27}$$

Wir zeigen, daß die Einschränkung des Morphismus

$$\Phi_i :\ \mathbb{C}^n \times \mathbb{C}^s \to \mathbb{C}^p \times \mathbb{C}^i$$

auf $\tilde{U} \times \mathbb{C}^s$ transversal zum Ursprung $0 \in \mathbb{C}^p \times \mathbb{C}^i$ ist.

Sei also (x, z) ein beliebiger Punkt in $\tilde{U} \times \mathbb{C}^s$, der die Gleichung $\Phi_i(x, z) = 0$ erfüllt. Nach Definition der Umgebung $\widetilde{U}$ in (4.27) liegt der Punkt x in $\widetilde{U} \cap W$, und ist somit ein glatter Punkt in W, der außerhalb der Hyperfläche $\{x \in \mathbb{C}^n |\ m(x) = 0\}$ liegt. Unsere Untersuchung über den Rang der Jacobimatrix $J(\Phi_i)$ zeigt, daß der Rang dieser Matrix in (x, z) maximal ist, also der Punkt (x, z) ein regulärer Punkt von Φ_i ist. Da aber der Punkt (x, z) beliebig in der Faser $\Phi_i^{-1}(0) \cap\ (\tilde{U} \times \mathbb{C}^s)$ gewählt war, ist die gewünschte Transversalitätseigenschaft bewiesen.

Wir wenden nun das schwache Transversalitätstheorem von Thom–Sard (vgl. [Dem89], [GG86]) auf das Diagramm

$$\begin{array}{ccc} \Phi_i^{-1}(0) \cap (\tilde{U} \times \mathbb{C}^s) & \hookrightarrow & \mathbb{C}^n \times \mathbb{C}^s \\ & \searrow & \downarrow \\ & & \mathbb{C}^s \end{array},$$

an und finden eine residuelle dichte Menge Ω_i von Parametern $z \in \mathbb{C}^s$, in welcher die Transversalität erhalten bleibt. Dies impliziert, daß für jedes $z \in \Omega_i$ die Menge der glatten Punkte der transformierten lokalisierten $i-$ten Varietät

$$\widetilde{W}_i^z \setminus ((Sing\ W) \cup \{x \in \mathbb{C}^n \mid m(x) = 0\}) \tag{4.28}$$

entweder leer oder ein lokal glatter vollständiger Durchschnitt der Kodimension $p+i$ ist, der durch die Gleichungen

$$\left(f_1, \ldots, f_p, \widetilde{M}_p(., z), \ldots, \widetilde{M}_{p+i-1}(., z)\right) \tag{4.29}$$

beschrieben ist, wobei die Varietät $\widetilde{W}_i^z$ in (4.28) durch

$$W_i^z := W \cap \{x \in \mathbb{C}^n | \ \widetilde{M}(i_1, \ldots, i_p)(x, z) = 0 \quad \text{für} \quad 1 \leq i_1 < \ldots < i_p \leq p + i - 1\}.$$

gegeben ist. Unsere Betrachtungen wurden bis jetzt nur für einen Koordinatenwechsel bei beliebig *festem* Index i, $1 \leq i \leq n-p$ geprüft. Wenn wir jedoch $\Omega := \bigcap_{i=1}^{n-p} \Omega_i$ betrachten, finden wir eine residuelle dichte Menge von Parametern in $\mathbb{C}^s$, aus welcher wir einen Koordinatenwechsel für alle i, $1 \leq i \leq n-p$ wählen können. Für jede Wahl des Parameters $z \in \Omega$ ist die transformierte Varietät $\widetilde{W}_i^z$ außerhalb der abgeschlossenen Menge

$$(Sing\ W) \cup \{x \in \mathbb{C}^n \mid m(x) = 0\}$$

entweder leer oder ein lokal vollständiger Durchschnitt, welcher durch die in (4.29) angegebene reguläre Folge beschrieben ist. Genauer gesagt, der affine Raum $\mathbb{R}^s$ enthält eine nicht–leere residuelle dichte Menge von Parametern z, so daß die Koordinatentransformation $X = A(z)Y$ zur gewünschten Transversalität führt. Da die rationalen Zahlen in $\mathbb{R}$ dicht liegen, können wir ohne Beschränkung der Allgemeinheit die Parameter z in $\mathbb{Q}^s$ wählen.

Damit haben wir das folgende Theorem bewiesen:

Satz 23
Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ so gegeben, daß die affine Varietät $W = V(f_1, \ldots, f_p)$ ein reduzierter vollständiger Durchschnitt ist. Seien weiterhin die Variablen $X_1, \ldots, X_n$ in generischer Position bezüglich dem Ideal $(f_1, \ldots, f_p)$ und sei m der $(p-1)$–Minor der Jacobimatrix $J(f_1, \ldots, f_p)$, welcher aus den ersten $(p-1)$ Zeilen und Spalten dieser Matrix besteht. Dann ist jede Varietät $\widetilde{W}_i$, $1 \leq i \leq n-p$, entweder leer oder ein lokal glatter vollständiger Durchschnitt der Kodimension $p+i$. Falls sie nicht leer ist, so läßt sich diese Varietät durch die folgende lokal (außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | \ m(x) = 0\}$) glatte reguläre Folge beschreiben

$$f_1, \ldots, f_p, M_p, \ldots, M_{p+i-1},$$

wobei M_j, $p \leq j \leq p+i-1$, der p–Minor der Jacobimatrix $J(f_1, \ldots, f_p)$ ist, der aus den Spalten $1, \ldots, p-1, j$ besteht.

Bemerkung 12
Da die Argumentation über die Lokalisierung bezüglich eines festen $(p-1)$–Minor m mutatis mutandis für jeden beliebegen $(p-1)$–Minor der Jacobimatrix $J(f_1, \ldots, f_p)$ angewendet werden kann, läßt sich Theorem 23 bis auf Umordnung von Zeilen und Spalten der Jacobimatrix $J(f_1, \ldots, f_p)$, für jeden beliebigen $(p-1)$–Minor formulieren.

Wir sind jetzt in der Lage den Hauptsatz dieses Kapitel zu formulieren:

Satz 24 (Hauptsatz)
Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ so gegeben, daß die affine Varietät $W = V(f_1, \ldots, f_p)$ ein reduzierter vollständiger Durchschnitt ist. Seien die Variablen $X_1, \ldots, X_n$ in generischer Position bezüglich W und die reelle Varietät $W \cap \mathbb{R}^n$ nichtleer, beschränkt und $(f_1, \ldots, f_p)-$glatt. Sei weiterhin m der $(p-1)-$Minor der Jacobimatrix $J(f_1, \ldots, f_p)$, welcher aus den ersten $(p-1)$ Zeilen und Spalten dieser Matrix besteht. Sei $V(m)$ die durch m beschriebene Hyperfläche, d.h. $V(m) := \{x \in \mathbb{C}^n | m(x) = 0\}$.

Dann ist für jeden Index i, $1 \leq i \leq n-p$, die polare Varietät

$$W_i = \overline{\widetilde{W_i} \setminus ((Sing\ W) \cup V(m))} \tag{4.30}$$

ein lokal glatter vollständiger Durchschnitt der Kodimension $p+i$, welcher sich durch die glatte reguläre Folge

$$f_1, \ldots, f_p, M_p, \ldots, M_{p+i-1},$$

außerhalb der Varietät $(Sing\ W) \cup V(m)$ beschreiben läßt, wobei M_j, $p \leq j \leq p+i-1$, der $p-$Minor der Jacobimatrix $J(f_1, \ldots, f_p)$ ist, der aus den Spalten $1, \ldots, p-1, j$ besteht.

Der Beweis des Hauptsatzes läßt sich aus dem vom Theorem 23 ableiten, da die polaren Varietäten W_i, $0 \leq i < n$, unter den Voraussetzungen vom Hauptsatz nichtleer sind.

4.3 Die Existenz glatter reeller Punkte in den polaren Varietäten

Wir setzen wieder voraus, daß die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ eine reduzierte reguläre Folge bilden. W sei $V(f_1, \ldots, f_p)$ und wir betrachten die Teilvarietät

$$V := W \cap \mathbb{R}^n,$$

von der wir voraussetzen, daß sie nichtleer und beschränkt ist. Darüberhinaus soll V nur $(f_1, \ldots, f_p)-$glatte Punkte enthalten (d.h. V wird als glatte Teilvarietät von $\mathbb{R}^n$ vorausgesetzt). Die Variablen $X_1, \ldots, X_n$ sollen bezüglich $f_1, \ldots, f_p$ in generischer Position sein. Mit $\widetilde{W_i}$, $1 \leq i \leq n-p$, bezeichnen wir dieselben affinen Varietäten wie zuvor. Dann gilt der folgende

Satz 25
Falls die reelle Varietät $V = W \cap \mathbb{R}^n$ nichtleer, beschränkt und $(f_1, \ldots, f_p)-$glatt ist, und falls die Variablen $X_1, \ldots, X_n$ in generischer Position sind, dann ist jede

affine Varietät $\widetilde{W}_i$ nichtleer, lokal $(f_1, \dots, f_p)$−glatt und von der Dimension $n-p-i$. Jede Varietät $\widetilde{W}_i$ enthält einen reellen Punkt. Ferner ist $\overline{W_i \setminus Sing\, W}$ ein nichtleerer lokaler vollständiger Durchschnitt, der einen reellen Punkt enthält.

Beweis des Satzes 25:

Sei C eine Zusammenhangskomponente von $V = W \cap \mathbb{R}^n$ und sei

$$b := (a_1, \dots, a_{p-1}, a_p, \dots, a_{n-1}, a_n) \in W \cap \mathbb{R}^n$$

ein lokal maximaler Punkt in C bezüglich der letzten Koordinate X_n. Die Existenz eines Maximums in jeder Zusammenhangskomponente einer kompakter Varietät V ist gewährleistet, da die Komponenten kompakt sind. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß der $(p-1)$−Minor m, gebildet aus den ersten $p-1$ Zeilen und Spalten der Jacobimatrix $J(f_1, \dots, f_p)$ in b nicht verschwindet. Nach unseren Voraussetzungen muß ein solcher Minor existieren, da b ein $(f_1, \dots, f_p)$−glatter Punkt ist. In jeder lokalen Parametrisierung von V im Punkt b kann die Variable X_n nur eine abhängige Variable sein, da X_n einen lokal maximalen Wert in b annimmt (a_n ist dieses Maximum). Wir können daher ohne Einschränkung der Allgemeinheit annehmen, daß sich im Punkt b die Varietät V folgendermaßen parametrisieren läßt.

Es gibt eine den Punkt $a := (a_p, \dots, a_{n-1})$ enthaltende offene Menge $\mathcal{U} \subset \mathbb{R}^{n-p}$ und eine stetig differenzierbare Abbildung

$$\varphi : \mathcal{U} \to \mathbb{R}^p \ , \varphi := (\varphi_1, \dots, \varphi_{p-1}, \varphi_n), \tag{4.31}$$

so daß in jedem Punkt $(x_p, \dots, x_{n-1})$ in $\mathcal{U}$ gilt:

$$x_1 = \varphi_1(x_p, \dots, x_{n-1}), \dots, x_{p-1} = \varphi_{p-1}(x_p, \dots, x_{n-1}),$$

$$x_n = \varphi_n(x_p, \dots, x_{n-1}).$$

Diese Parametrisierung der Polynome $f_k,\ 1 \leq k \leq p$, erzeugt die reell− wertigen Funktionen

$$\tilde{f}_k(x_p, \dots, x_{n-1}) :=$$

$$f_k(\varphi_1(x_p, \dots, x_{n-1}), \dots, \varphi_{p-1}(x_p, \dots, x_{n-1}), x_p, \dots, x_{n-1}, \varphi_n(x_p, \dots, x_{n-1})).$$

Für jeden Index $k,\ 1 \leq k \leq p$, und jeden Index $j,\ p \leq j \leq n-1$, gilt in der offenen Menge $\mathcal{U}$

$$\frac{\partial \tilde{f}_k}{\partial X_j} = \frac{\partial f_k}{\partial X_j} + \frac{\partial f_k}{\partial X_1}\frac{\partial \varphi_1}{\partial X_j} + \cdots + \frac{\partial f_k}{\partial X_{p-1}}\frac{\partial \varphi_{p-1}}{\partial X_j} + \frac{\partial f_k}{\partial X_n}\frac{\partial \varphi_n}{\partial X_j} = 0. \tag{4.32}$$

Wir definieren die folgende $(p \times p)$−Matrix

$$B := \begin{pmatrix} \dfrac{\partial f_1}{\partial X_1} & \cdots & \dfrac{\partial f_1}{\partial X_{p-1}} & \dfrac{\partial f_1}{\partial X_n} \\ \ldots\ldots\ldots & & \ldots\ldots\ldots\ldots & \\ \dfrac{\partial f_p}{\partial X_1} & \cdots & \dfrac{\partial f_p}{\partial X_{p-1}} & \dfrac{\partial f_p}{\partial X_n} \end{pmatrix},$$

welche regulär in $\mathcal{U}$ ist, und erhalten aus der Gleichung (4.32) die Gültigkeit der Gleichung

$$-\det B(x) \begin{pmatrix} \dfrac{\partial \varphi_1}{\partial X_j}(x_p, \ldots, x_{n-1}) \\ \vdots \\ \dfrac{\partial \varphi_{p-1}}{\partial X_j}(x_p, \ldots, x_{n-1}) \\ \dfrac{\partial \varphi_n}{\partial X_j}(x_p, \ldots, x_{n-1}) \end{pmatrix} = (Adj\ B)(x) \begin{pmatrix} \dfrac{\partial f_1}{\partial X_j}(x) \\ \vdots \\ \dfrac{\partial f_{p-1}}{\partial X_j}(x) \\ \dfrac{\partial f_p}{\partial X_j}(x) \end{pmatrix} \tag{4.33}$$

in $\mathcal{U}$, wobei $(Adj\ B)$ die adjungierte Matrix der Matrix B ist. Da b ein lokal maximaler Punkt der Funktion X_n ist, gilt

$$\frac{\partial \varphi_n}{\partial X_j}\ (a) = 0$$

gilt für jeden Index $j,\ p \leq j \leq n-1$. Damit impliziert die Gleichung (4.33) die Gleichheit

$$B(n,1)\ (b)\ \frac{\partial f_1}{\partial X_j}\ (b) + \cdots + B(n,p)\ (b)\ \frac{\partial f_p}{\partial X_j}\ (b) = 0 \tag{4.34}$$

für jeden Index $j,\ p \leq j \leq n-1$, wobei $B(n,k),\ 1 \leq k \leq p$, der Eintrag der adjungierten Matrix $(Adj\ B)$ im „ Kreuzpunkt " der $k-$ten Spalte und letzten Zeile ist. Unter Beachtung der Struktur der Matrix B erhalten wir aus der Gleichung (4.34), daß

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(b) & \ldots & \frac{\partial f_1}{\partial X_{p-1}}(b) & \frac{\partial f_1}{\partial X_j}(b) \\ \ldots\ldots\ldots\ldots & & \ldots\ldots\ldots\ldots\ldots\ldots & \\ \frac{\partial f_p}{\partial X_1}(b) & \ldots & \frac{\partial f_p}{\partial X_{p-1}}(b) & \frac{\partial f_p}{\partial X_j}(b) \end{pmatrix} = 0 \qquad (4.35)$$

für jeden Index $j,\ p \leq j \leq n-1$ gelten muß. Die Gleichung (4.35) hat zur Folgerung, daß die folgenden $p-$Minoren der Jacobimatrix $J(f_1, \ldots, f_p)$ im Punkt b verschwinden:

$$M(1, \ldots, p-1, p)\ (b) = \ldots = M(1, \ldots, p-1, n-1)\ (b) = 0,$$

diese Minoren haben wir im vorstehenden Abschnitt mit $M_p, \ldots, M_{n-1}$ bezeichnen. Da wir $m(b) \neq 0$ annehmen konnten, leiten wir aus Behauptung 22 die Folgerung ab, daß b in der Lokalisierung $(\Delta_{n-p})_m$ der Determinanten Varietät Δ_{n-p} außerhalb von $\{x \in \mathbb{C}^n |\ m(x) = 0\}$ liegt. Also gehört der reelle Punkt b zu $W \cap (\Delta_{n-p})_m$. Was aber mit den Bezeichnungen aus dem Abschnitt 4.1 heißt $b \in \widetilde{W}_{n-p}$. Die Varietät W_{n-p} ist somit nichtleer und enthält den reellen Punkt b.

■

Bemerkung 13 *Der Beweis des Satzes* 25 *beinhaltet die folgende Aussage:*
Sei C eine Zusammenhangskomponente von $V = W \cap \mathbb{R}^n$ und b ein lokal maximaler Punkt der linearen Form X_n in C, so daß der $(p-1)-$Minor m in b nicht Null ist. Dann liegt b in W_{n-p}. Mit anderen Worten, jede Zusammenhangskomponente von V enthält mindestens einen Punkt von $W_{n-p} \cap \mathbb{R}^n \setminus (Sing\, W \cup V(m))$.

4.4 Ein Algorithmus für den vollständigen Durchschnitt

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n], p < n$ so gegeben, daß sie eine reduzierte reguläre Folge bilden. Sei $W := V(f_1, \ldots, f_p)$. Sei m der wie bisher fixierte $(p-1)-$Minor der Jacobimatrix $J(f_1, \ldots, f_p)$. Wir finden zu $m,\ n-p$ viele $p-$Minoren

$$M_p, \ldots, M_{n-1} \in \mathbb{Q}[X_1, \ldots, X_n], \qquad (4.36)$$

so daß die Folge

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1} \qquad (4.37)$$

entweder die leere Menge beschreibt, oder transversal außerhalb $(Sing\ W) \cup V(m)$ ist (vgl. Theorem 23). Sei $\Delta_i,\ 1 \leq i \leq n-p+1$, wieder die Determinantenvarietät, die durch alle $p-$Minoren der Untermatrix der Jacobimatrix $J(f_1,\ldots,f_p)$ beschrieben ist, welche aus den ersten Spalten $\{1,\ldots,p+i-1\}$ gebildet wird.

Seien die Variablen $X_1,\ldots,X_n$ generisch bezüglich W.

In der Lokalisierung außerhalb der Hyperfläche $V(m)=\{x\in \mathbb{C}^n|\ m(x)=0\}$, hat die Menge der singuläre Punkte von W die folgende Beschreibung, (vgl. Bemerkung 11, Abschnitt 4.1):
$(Sing\ W)\setminus V(m)=\widetilde{W}_{n-p+1}\setminus V(m)=$

$$=\{x\in \mathbb{C}^n|f_1(x)=\ldots=f_p(x)=M_p(x)=\ldots=M_n(x)=0,m(x)\neq 0\}. \quad (4.38)$$

- Der Algorithmus in [GHM+98] und [GHH+97] kann entscheiden, ob die Varietät $W_{n-1}\setminus((Sing\ W)\cup V(m))$ null–dimensional ist, und somit auch enscheiden, ob die Folge
$$f_1,\ldots,f_p,M_p,\ldots,M_{n-1}, \quad (4.39)$$
außerhalb der Varietät $(Sing\ W)\cup V(m)$ eine reduzierte reguläre Folge ist.
- Ein Verfahren zur Darstellung der Variablen in generischer Position bezüglich W geben wir im Kapitel 5.

Wir wissen, daß vorstehende Bemerkungen mutatis mutandis richtig sind für jeden $(p-1)-$Minor aus der Jacobimatrix $J(f_1,\ldots,f_p)$. Unter den Voraussetzungen des Satzes 25 gibt es einen $(p-1)-$Minor $m\in\mathbb{Q}[X_1,\ldots,X_n]$, für welchen die Folge aus den ersten $p-1$ Zeilen und Spalten der Jacobimatrix $J(f_1,\ldots,f_p)$ besteht, sei nun so gewählt, daß die Folge

$$f_1,\ldots,f_p,M_p,\ldots,M_{n-1},$$

eine transversale reduzierte Folge außerhalb von $(Sing\ W)\cup V(m)$ ist, dabei ist $V(m)$ die durch m beschriebene Hyperfläche.

Sei $\delta'_{n-1}(m)$ der geometrische Grad des Gleichungssystems (4.39) außerhalb der Hyperfläche $V(mM_n)$. Mit $V(mM_n)$ sei das Produkt der Polynome m und $M_n:=M(1,\ldots,p-1,n)$ bezeichnet.
$V(mM_n):=V(m)\cup V(M_n)=$

$$\{x\in \mathbb{C}^n|\ m(x)\}\cup\{x\in \mathbb{C}^n|\ M(1,\ldots,p-1n)(x)=0\}. \quad (4.40)$$

Dann ist

$$\delta'_{n-1}(m)=\max\left(\max_{1\leq j\leq p}\delta'_j\quad,\max_{1\leq i\leq n-p}\delta_{p+i-1}\right), \quad (4.41)$$

wobei

$$\delta'_j:=\deg\overline{V(f_1,\ldots,f_j)\setminus V(mM_n)}, \quad (4.42)$$

und

$$\delta_{p+i-1} := \max_{1 \leq i \leq n-p} \deg \overline{W_{p+i-1} \setminus V(mM_n)}. \tag{4.43}$$

δ'_{n-1} ist der geometrische Grad des Systems (4.39) außerhalb $V(mM_n)$.

Sei

$$\delta' := \max\{\delta'_{n-1}(\widetilde{m})| \quad \text{alle} \quad (p-1)-\text{Minor} \quad \widetilde{m} \quad \text{in} \quad J(f_1, \ldots, f_p)\} \tag{4.44}$$

Aus der Bezout–Ungleichung folgt die Ungleichungen (vgl. [Hei83])

$$\delta'_{n-1}(m) \leq \delta' \leq d^p[p(d-1)]^{n-p} \leq p^{n-p}d^n. \tag{4.45}$$

Unter dieser Voraussetzungen von Satz 25 sind wir in der Lage, ein Komplexitätsresultat bezüglich der geometrischen Lösung der transversalen glatten Folge in (4.39) zu formulieren.

Satz 26

Seien die Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ mit maximalem Grad $d \geq 2$ gegeben, so daß sie eine reduzierte reguläre Folge in $\mathbb{Q}[X_1, \ldots, X_n]$ bilden. Seien die Variablen $X_1, \ldots, X_n$ generisch bezüglich der Varietät $W = V(f_1, \ldots, f_p)$. Wir setzen weiterhin voraus, daß die reelle Teilvarietät $V := W \cap \mathbb{R}^n$ nichtleer, beschränkt und $(f_1, \ldots, f_p)$–glatt ist.

Seien n, d, δ', L, ℓ nichtnegative ganze Zahlen, mit $d \geq 2$. Sei m wie zuvor gewählt, $\delta'_{n-1}(m)$ der geometrische Grad der transversale Folgen

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1},$$

außerhalb $(Sing\ W) \cup V(m)$, mit $\delta'_{n-1}(m) \leq \delta'$. Ferner seien die Polynome $f_1, \ldots, f_p$ durch ein Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe L und nichtskalaren Tiefe ℓ gegeben.

Dann gibt es ein arithmetisches Netzwerk $\mathcal{N}$ mit Parametern in $\mathbb{Q}$, welches die Größe $L(nd\delta')^{O(1)}$ hat, das Straight–Line Programm β auswertet und die geometrischen Lösungen der null–dimensionalen transversalen Folge

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1}$$

außerhalb der Hyperfläche $V(mM_n)$ generiert.

Der dem arithmetischen Netzwerk unterliegende Algorithmus testet, ob die polare Varietät Varietät

$$W_{n-1} \setminus ((Sing\ W) \cup V(m))$$

null–dimensional ist. Wenn das der Fall ist, so erzeugt das arithmetische Netzwerk $\mathcal{N}$ ein Straight–Line Programm der Größe $L(nd\delta')^{O(1)}$ und nichtskalaren Tiefe

$O(n(log(d\delta') + \ell))$ mit Parametern in $\mathbb{Q}$, welches die Koeffizienten der $n+1$ univariaten Polynome $q^{(m)}, p_1^{(m)}, \ldots, p_n^{(m)} \in \mathbb{Q}[X_n]$ darstellt. Diese Polynome beschreiben die geometrischen Lösung der Lokalisierung der null-dimensionalen polaren Varietät

$$(W_{n-1})_{mM_n} := V(f_1, \ldots, f_p, M_p, \ldots, M_{n-1}) \setminus (V(m) \cup V(M_n)) \tag{4.46}$$

und haben die folgenden Eigenschaften:

(1) $deg(q^{(m)}) = \delta'_{n-1}(m) = \deg(W_{n-1})_{mM_n}$

(2) $max\{deg(p_j^{(m)}) | 1 \leq j \leq n\} < \delta'_{n-1}(m)$

(3) $(W_{n-1})_{mM_n} = \{(p_1^{(m)}(u), \ldots, p_n^{(m)}(u)) | u \in \mathbb{C}, q^{(m)}(u) = 0\}.$

Der dem arithmetischen Netzwerk $\mathcal{N}$ unterliegende Algorithmus erzeugt höchstens $\delta'_{n-1}(m)$ Vorzeichenbedingungen in $\{-1, 0, 1\}^{\delta'(m)}$, die die reellen Nullstellen des Polynoms q à la Thom *kodieren, [CR88]. (Andernfalls wären die Punkte der kompakten reellen Varietät V nicht $(f_1, \ldots, f_p)-$glatt.)*

Das Netz $\mathcal{N}$ beschreibt mit dieser Codierung die Parametrisierung der nicht–leeren reellen polaren Varietät $(W_{n-1})_{mM_n} \cap \mathbb{R}^n$.

Beweis des satzes:
Seien die Polynome $f_1, \ldots, f_p$ durch ein Straight–Line Program der Länge L und Tiefe ℓ gegeben. Unter einer einfachen Anwendung der Leibniz Regel, zur Differentiation eines Produkts, leiten wir aus β ein Straight–Line Program β_1 der Länge $(2n+1)L$ und nichtskalaren Tiefe $\ell + 1$ in $\mathbb{Q}[X_1, \ldots, X_n]$ ab, das die partiellen Ableitungen der Polynome $f_1, \ldots, f_p$ evaluiert (vgl. Lemma 25, [GHH+97]). Da die Determinante einer Matrix im konstanten Glied ihres charakteristischen Polynoms auftritt, wenden wir die verbesserte Variante des (gut–parallelisierbaren) Algorithmus von Berkowitz [Abd97] zur Berechnung der Koeffizienten des charakteristischen Polynoms einer $(n \times n)-$Matrix an, um startend mit β_1, ein Straight–Line Program β_2 in $\mathbb{Q}[X_1, \ldots, X_n]$ der Größe $O(n^4 \log_2 n)L$ und nichtskalaren Tiefe $O(\log_2(n) + \log_2 \log_2 n) + \ell$ abzuleiten, das alle partiellen Ableitungen der Polynome $f_1, \ldots, f_p$, sowie alle $(p-1)-$ und $p-$Minoren der Jacobimatrix $J(f_1, \ldots, f_p)$ auswertet.

Die Varietät *Sing W* wird in der Lokalisierung außerhalb der Hyperfläche $V(m)$ durch die Varietät W_{n-p+1} beschrieben.

$$(Sing\ W) \setminus V(m) = W_{n-p+1} \setminus V(m) \tag{4.47}$$

Unter Benutzung des der Behauptung 18 [GHM+98] zugrunde liegenden Algorithmus mit der im Theorem 31, [GHH+97], eingeführten Modifizierung (siehe auch

Theorem 19, [GHH+97] und dem Beweis davon), finden wir ein arithmetisches Netzwerk $\mathcal{N}_1^{(m)}$ mit Parametern in $\mathbb{Q}$ von der Größe $L(nd\delta')^{O(1)}$, welches entscheidet, ob die Folge

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1}, mM_n \tag{4.48}$$

eine transversale Folge außerhalb der Hyperfläche $V(mM_n)$ beschreibt, wobei die Polynome

$$M_l := M(1, \ldots, p-1, l), \; p \leq l \leq n \tag{4.49}$$

jeweils aus den Spalten $1, \ldots, p-1, l$ der Jacobimatrix $J(f_1, \ldots, f_p)$ bestehende p–Minoren sind. Die Folge (4.48) ist genau dann eine transversale Folge außerhalb der Hyperfläche $V(mM_n)$, wenn die Varietät

$$(W_{n-1})_{mM_n} := V(f_1, \ldots, f_p, M_p, \ldots, M_{n-1}) \setminus V(mM_n) \tag{4.50}$$

eine null–dimensionale Varietät beschreibt.

Da wir mit den Algorithmen in [GHM+98], und [GHH+97] die Dimension der Varietät $(W_{n-1})_{mM_n}$ berechnen können, setzen wir nun voraus, daß die Polynome in (4.48),

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1}$$

transversal außerhalb der Hyperfläche $V(mM_n)$ sind.

Sei

$$R_0 := \mathbb{Q}[X_1, \ldots, X_{n-1}]. \tag{4.51}$$

Wir betrachten die Polynome f_1 und $m = M(1, \ldots, p-1)$ mit dem Leitkoeffizienten eins und Koeffizienten in R_0. Durch Interpolation in $pd + 1$ beliebigen, voneinander verschiedenen rationalen Punkten erhalten wir ein divisionsfreies Straight–Line Programm in $R_0 = \mathbb{Q}[X_1, \ldots, X_{n-1}]$, das die Koeffizienten von f_1 und m bezüglich X_n darstellt. Dieses Straight–Line Programm hat die Länge $L(nd)^{O(1)}$.

Wir erhalten den größten gemeinsamen Teiler von f_1 und mM_n in $R_0[X_n]$ durch Anwendung vom Lemma 8 in [GHM+98]. Dieser größte gemeinsame Teiler hat den Leitkoeffizienten eins in $R_0[X_n]$, und seine Koeffizienten bezüglich X_n lassen sich durch ein divisionsfreies Straight–Line Programm in R_0 darstellen. Sei

$$\bar{q}_0^{(m)} \in R_0[X_n] = \mathbb{Q}[X_1, \ldots, X_n] \tag{4.52}$$

der analog zur Noether–Normalisierung in [GHM+98] erhaltene Quotient von f_1 und dem größten gemeinsamen Teiler von f_1 und mM_n. Die Koeffizienten bezüglich X_n lassen sich durch ein divisionsfreies Straight–Line Programm $\bar{\beta}_2$ in R_0 darstellen. Das Polynom $\bar{q}_0^{(m)}$ ist quadratfrei, da wir ausschließlich mit dem quadratfreien Teil des Polynoms f_1 rechnen. $\bar{q}_0^{(m)}$ hat den Leitkoeffizienten eins bezüglich X_n und es teilt f_1. Wir haben weiterhin eine Beschreibung der Varietät

$$W^{(0)} := \{x \in \mathbb{C}^n | \bar{q}_0^{(m)}(x) = 0\}. \tag{4.53}$$

Da die Koordinaten $X_1, \ldots, X_n$ generisch gewählt sind, sind sie auch in Noether–Position bezüglich der Varietät $V(f_1)$ und das Polynom $q_0^{(m)}$ ist das zur Ringerweiterung

$$R_0 \to R_0[X_n]/(f_1) \tag{4.54}$$

assozierte minimale Polynom mit primitivem Element u_n, welches das Bild eines trennbaren Elements

$$U_n := \lambda_n X_n \tag{4.55}$$

ist. Da das minimale Polynom $\bar{q}_0^{(m)}$ auf $V(f_1)$ verschwindet, erhalten wir die vollständige Parametrisierung der Varietät $W^{(0)}$, indem wir die Gleichung $\bar{q}_0^{(m)}(\lambda_n, T)$ nach dem Parameter λ_n ableiten (vgl. [Mac16], [GLS99]):

$$\frac{\partial \bar{q}_0^{(m)}(\lambda_n, T)}{\partial \lambda_n} = \frac{\partial \bar{q}_0^{(m)}(\lambda_n, T)}{\partial U_n} X_n. \tag{4.56}$$

Wir erhalten die Identität

$$W^{(0)} := \left\{ \left(x_1, \ldots, x_{n-1}, \frac{v_n(u_n)}{\varrho_n} \right) \in \mathbb{C}^n | \bar{q}_0^{(m)}(u_n) = 0 \right\}, \tag{4.57}$$

wobei $\varrho_n \in R_0$ die Diskriminante des minimalen Polynoms $\bar{q}_0^{(m)}$ ist. Der Grad des Polynoms $\bar{q}_0^{(m)}$ genügt den Gleichungen

$$\deg \bar{q}_0^{(m)} = \deg_{X_n} \bar{q}_0^{(m)} = \deg \widetilde{W}^{(0)}. \tag{4.58}$$

Das Straight–Line Programm $\bar{\beta}_2$, welches die Koeffizienten des Polynoms $\bar{q}_0^{(m)}$ bezüglich der Variablen X_n darstellt, hat die Länge $L(nd)^{O(1)}$.

Damit ist der Schritt $i = 0$ bewiesen, welcher aus der Elimination der Variable X_n besteht. Es handelt sich um die Beschreibung einer Projektion $\pi_n : V(f_1) \to \mathbb{C}^{n-1}$, die durch die Gleichung

$$\pi(x) = (x_1, \ldots, x_{n-1}), \quad \text{für} \quad x \in V(f_1) \tag{4.59}$$

definiert ist.

Wir setzen unter Benutzung der Proposition 18 in [GHM+98], sowie der Proposition 33 in [GHH+97], die Rekursion für die Elimination der Variablen $X_{n-1}, \ldots, X_1$ fort. Im Schritt $i = n-1$ angelangt, finden wir ein Netzwerk $\mathcal{N}_2^{(m)}$, welches ein die Koeffizienten der Polynome

$$\bar{q}_{n-1}^{(m)} =: q^{(m)}, p_{n-1,1}^{(m)} =: p_1^{(m)}, \ldots, p_{n-1,n}^{(m)} =: p_n^{(m)} \in \mathbb{Q}[T] \tag{4.60}$$

repräsentierendes, Straight–Line Programm in $\mathbb{Q}$ erzeugt. Diese Polynome charakterisieren den Teil $(W_{n-1})_{mM_n}$ der null–dimensionalen komplexen polaren Varietät

$$(W_{n-1})_{mM_n} := W_{n-1} \setminus V(mM_n), \tag{4.61}$$

deren Komponenten außerhalb der Hyperfläche $\{x \in \mathbb{C}^n | m(x)M_n(x) = 0\}$ liegen. Die Ausgabe $q^{(m)}, p_1^{(m)}, \ldots, p_n^{(m)}$ des Netzwerks $\mathcal{N}_2^{(m)}$ erfüllt dann die Bedingungen $(1), (2), (3)$ im Theorem 26.

Das Netzwerk $\mathcal{N}_2^{(m)}$ läßt sich durch Anwendung des in [BOKR86] veröffentlichen korrekten Algorithmus erweitern, indem geeignete komprimierte Knoten addiert werden, die testen, ob eine rationale Zahl positiv ist oder nicht (vgl. auch [RS90] für eine Verfeinerung). Das resultierende Netzwerk $\mathcal{N}^{(m)}$ entscheidet nun, ob das Polynom $q^{(m)}$ eine reelle Lösung besitzt. Es hat eine Größe, die asymptotisch gleich $L(nd\delta')^{O(1)}$ ist. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß das Netzwerk $\mathcal{N}^{(m)}$ jede existierende Nullstelle des Polynoms $q^{(m)}$ im Sinne von Thom (vgl. [CR88], [RS90]) kodiert. Für jede Zusammenhangskomponente $K \subset (W_{n-1})_{mM_n}$ finden wir einen Punkt $\zeta \in K$ und einen Parameter $\tau \in \mathbb{R}$, so daß

$$q^{(m)}(\tau) = 0 \quad \text{und} \quad \zeta = (p_1(\tau), \ldots, p_n(\tau)). \tag{4.62}$$

Der Punkt ζ ist ein isolierter kritischer Punkt der auf die Komponente K eingeschränkten Projektion der letzten Koordinate

$$X_n : K \to \mathbb{R}. \tag{4.63}$$

Diese Einschränkung auf eine irreduzible Komponente einer kompakten reellen Teilvarietät $K \subset V := W \cap \mathbb{R}^n$ nimmt das Maximum auf dieser an, welches in $(V_{n-1})_{mM_n} := (W_{n-1})_{mM_n} \cap \mathbb{R}^n$ liegt.

■

Bemerkung 14
Die allgemeine Aufgabe besteht darin für eine reduzierte Folge von p Polynome $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n], p \leq n$ durch $n-p$ Polynome,die $p-$Minoren der Jacobimatrix $J(f_1, \ldots, f_p)$ sind, so zu ergänzen, daß die entstehende Folge transversal außerhalb einer gewissen abgeschlossenen Menge ist.

Wir wollen diese Bemerkung kommentieren.
Man wähle wirkürlich einen $(p-1)-$Minor $\tilde{m}$ aus

$$p\binom{n}{p-1} \quad \text{vielen aus} \quad J(f_1, \ldots, f_p) \tag{4.64}$$

Sei $\widetilde{m}$ ohne Einschränkung der Allgemeinheit aus den $(p-1)$ ersten Zeilen und Spalten der Jacobimatrix $J(f_1, \ldots, f_p)$. Dann hat man zu entscheiden, ob die Folge

$$f_1, \ldots, f_p, M_1, \ldots, M_{n-1} \tag{4.65}$$

eine transversale Folge außerhalb der Hyperfläche $V(\widetilde{m}M(1, \ldots, p-1, n))$ ist. Falls dies der Fall ist, so wendet man das im Satz 26 beschriebene Verfahren an. Im andern Fall wählt man einen anderen $(p-1)-$Minor aus $J(f_1, \ldots, f_p)$ neu aus und wiederholt die Prozedur.

Wir erzeugen durch eine Vorrechnung lokale Beschreibungen von polaren Varietäten, indem wir zu jedem festen gewählten $(p-1)-$Minor $m \in \mathbb{Q}[X_1, \ldots, X_n]$ der Jacobimatrix $J(f_1, \ldots, f_p)$, zuerst eine transversale reguläre Folge

$$f_1, \ldots, f_p, M_p, \ldots, M_{n-1}$$

außerhalb der Hyperfläche $V(mM_n) := \{x \in \mathbb{C}^n \mid m(x)M_n(x) = 0\}$ aufbauen, wenn dies möglich ist. Für einen solchen $(p-1)-$Minor m können wir mit dem Satz 26, ein Netzwerk $\mathcal{N}^{(m)}$ konstruieren, welches entscheidet, ob die polare Varietät $(W_{n-1})_{mM_n}$ null–dimensional ist. Wenn dies der Fall ist, wird diese Varietät $(W_{n-1})_{mM_n}$ durch eine transversale null–dimensionale Folge außerhalb der Hyperfläche $V(mM_n)$ beschrieben. Das arithmetische Netzwerk $\mathcal{N}^{(m)}$ im Beweis des Satzes 26 kodiert die Punkte dieser Varietät. Wir vervollständigen diese Methode, indem wir das Verfahren im Satz 26 für jeden $(p-1)-$Minoren in der Jacobimatrix $J(f_1, \ldots, f_p)$ laufen lassen. Die entstehenden Netzwerke $\mathcal{N}^{(\tilde{m})}$ hintereinander verknupfen: Wir erhalten damit ein Netzwerk $\mathcal{N}$, welche mindestens einen Punkt in jeder irreduziblen Komponente von $V := W \cap \mathbb{R}^n$ kodiert. Die Größe dieses Netzwerkes ist

$$\binom{n}{p-1} L(nd\delta')^{O(1)}. \tag{4.66}$$

Wir haben nun das folgende Theorem bewiesen

Satz 27
Seien die Bezeichnungen und Voraussetzungen wie vorhin. Wir setzen weiterhin voraus, daß die Polynome $f_1, \ldots, f_p$ ein reduzierte Folge bilden und die reelle Varietät $V := W \cap \mathbb{R}^n$ beschränkt und $(f_1, \ldots, f_p)-$glatt ist. Dann existiert ein arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$, welches mindestens einen repräsentativen Punkt in jeder Zusammenhangskomponente der reellen Varietät V findet. Die Größe dieses Netzes ist $\binom{n}{p-1} L(nd\delta')^{O(1)}$, wobei δ' der geeignet definierte, maximale Grad aller im Verfahren auftretenden transversalen Folge ist.

Bemerkung 15 *Offensichtlich erhält man das erste Komplexitätsergebnis für den Hyperflächenfall, indem man $p = 1$ setzt.*

Kapitel 5

Generische Koordinaten

Im Abschnitt 3.3 hatten wir ein auf dem Satz von *Bertini* beruhendes Verfahren zur Transformation der Variablen in generische Position bezüglich einer Hyperfläche beschrieben. Wir wollen jetzt eine von der Komplexität her effektivere Methode dafür beschreiben.

Wir werden hier eine Methode ableiten, die auch auf der geometrischen Lösung einer affinen Varietät außerhalb einer gewissen Hyperfläche beruht. Die Komplexität dieser Methode wird von gleicher Struktur sein wie die der Algorithmen im Kapitel 3, die Gesamtkosten der Algorithmen nicht vergrößert.

Wir entwickeln die Methode für den Hyperflächenfall, für den vollständigen Durchschnitt kann man eine analoge Methode beschreiben.

Wir setzen zunächst voraus, daß $f \in \mathbb{Q}[X_1, \ldots, X_n]$ ein quadratfreies Polynom ist, das eine reguläre Gleichung einer reellen Hyperfläche beschreibt. Gesucht ist ein Koordinatenwechsel $X = AY$, so daß sich die Hyperflächen definiert durch

$$f^A, \frac{\partial f^A}{\partial Y_1}, \ldots, \frac{\partial f^A}{\partial Y_i} \tag{5.1}$$

für jedes $i,\ 1 \leq i \leq n-1$ transversal schneiden. Dabei ist

$$f(X_1, \ldots, X_n) = f(AY) =: f^A(Y_1, \ldots, Y_n). \tag{5.2}$$

Wir betrachten einen Koordinatenwechsel $X = A(Z)Y$, wobei die Transformationsmatrix $A(Z)$ für jedes $i,\ 1 \leq i \leq n-1$, dieselbe Parametermatrix ist, und zwar wählen wir $A(Z)$ nach (4.11), d.h.

$$A(Z) := \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & 0 \\ Z_{2,1} & 1 & 0 & \ldots & \ldots & 0 \\ Z_{3,1} & Z_{3,2} & 1 & 0 & \ldots & \vdots \\ \vdots & \ldots & \ddots & 1 & \ddots & \vdots \\ Z_{n-1,1} & \ldots & \ldots & Z_{n-1,n-2} & 1 & 0 \\ Z_{n,1} & \ldots & \ldots & \ldots & Z_{n,n-1} & 1 \end{pmatrix}, \tag{5.3}$$

Dabei haben wir die Bezeichnung $Z := (Z_{2,1}, \ldots, Z_{n,n-1})$ für die Parameter benutzt.

$$\frac{\partial f^{A(Z)}}{\partial Y_k} = \frac{\partial f}{\partial X_k} + \sum_{j=k+1}^{n} Z_{j,k} \frac{\partial f}{\partial X_j},\ 1 \leq k \leq i,\ 1 \leq i \leq n-1. \tag{5.4}$$

Sei die Bezeichnung

$$F_0 := f, \quad F_1 := \frac{\partial f^{A(Z)}}{\partial Y_1}, \ldots, \frac{\partial f^{A(Z)}}{\partial Y_i} \tag{5.5}$$

eingeführt.

Dann interessiert uns der Morphismus

$$\begin{array}{cccccc} \Phi_i : & \mathbb{C}^n & \times & \mathbb{C}^{\frac{n(n-1)}{2}} & \to & \mathbb{C}^{i+1} \\ & & (x, z) & & \longmapsto & \Phi_i(x, z), \end{array} \tag{5.6}$$

wobei

$$\Phi_i(x, z) := (F_0(x),\ F_1(x), \ldots, F_i(x))\,.$$

Die Jacobimatrix $J_{X,Z}(\Phi_i)$ von Φ_i ist durch

$$J_{X,Z}(\Phi_i) = \begin{pmatrix} \frac{\partial \Phi_i}{\partial X} & \frac{\partial \Phi_i}{\partial Z} \end{pmatrix} = \begin{pmatrix} \frac{\partial F_0}{\partial X_1} & \cdots & \frac{\partial F_0}{\partial X_n} & \frac{\partial F_0}{\partial Z_{2,1}} & \cdots & \frac{\partial F_0}{\partial Z_{n,n-1}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial F_i}{\partial X_1} & \cdots & \frac{\partial F_i}{\partial X_n} & \frac{\partial F_i}{\partial Z_{2,1}} & \cdots & \frac{\partial F_i}{\partial Z_{n,n-1}} \end{pmatrix}$$

gegeben.

Mit der Definition der F_k sowie obiger Ableitungen erhalten wir

$$\begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \frac{\partial f}{\partial X_n} & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ *_{11} & \cdots & *_{1n} & \frac{\partial f}{\partial X_2} & \cdots & \frac{\partial f}{\partial X_n} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & 0 & 0 & \cdots & 0 \\ *_{(i)1} & \cdots & *_{(i)n} & 0\cdots & 0\cdots & 0\cdots & \frac{\partial f}{\partial X_{i+1}} & \cdots & \frac{\partial f}{\partial X_n} & 0 & \cdots & 0 \end{pmatrix}, \tag{5.7}$$

wobei die Sterne $*_{r,s},\ 1 \leq r \leq i,\ 1 \leq s \leq n$, in (5.7) die folgende Gestalt haben:

$$*_{r,s} := \frac{\partial^2 f}{\partial X_r \partial X_s} + \sum_{j=r+1}^{n} Z_{jr} \frac{\partial^2 f}{\partial X_j \partial X_s}.$$

Die Jacobimatrix $J_{X,Z}(\Phi_i)$ ist eine $(i+1) \times (n + \frac{n(n-1)}{2})-$Matrix.

Mit $J_X(\Phi_i)$ bezeichnen wir die $((i+1) \times n)-$Teilmatrix der Jacobimatrix $J_{X,Z}(\Phi_i)$), welche aus den ersten partiellen Ableitungen der Polynome $F_0, \ldots, F_i$ nach $X_1, \ldots, X_n$ besteht, d.h.

$$J_X(\Phi_i) := \begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \cdots & \frac{\partial f}{\partial X_n} \\ *_{11} & \ddots & \cdots & *_{1n} \\ \vdots & \cdots & \cdots & \vdots \\ *_{(i)1} & \cdots & \cdots & *_{(i)n} \end{pmatrix}. \tag{5.8}$$

Sei $\Delta(\Phi_i)$ die gemeinsamen Nullstellen aller nicht identisch verschwindenden $(i+1)-$Minoren der Teilmatrix $J_X(\Phi_i)$. Das aus aller $(i+1)-$Minoren der Teilmatrix $J_X(\Phi_i)$ erzeugende Ideal $J_1^n(Z)$ ist das Verschwindungsideal von $\Delta(\Phi_i)$:

$$\Delta(\Phi_i) = V(J_1^n(Z)) \tag{5.9}$$

Sei $\mathcal{P} \subset J_1^n(Z)$ ein mininales Primideal mit der Komponenten $C \subset \Delta(\Phi_i)$. Dann ist die Höhe von $\mathcal{P}$ kleiner oder gleich $n-(i+1)+1 = n-i$ (vgl. [Mat94]). Damit gilt

$$\dim W - \dim C \leq n - i. \tag{5.10}$$

Hieraus folgt

$$\dim C \geq \dim W - n + i. \tag{5.11}$$

Die Kodimension des Ideals $J_1^n(\Phi_i)$ ist höchstens $n-i$ und das Ideal wird von höchstens $n-i$ Polynomen erzeugt, welche eine reguläre Folge bilden. Mit Σ_i sei der Durchschnitt in $\mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}}$ der Phaser $\Phi_i^{-1}(0)$ mit $\Delta(\Phi_i)$, d.h.

$$\Sigma_i := \{(x,z) \in \Phi_i^{-1}(0) |\ M(j_1,\ldots,j_{i+1})(x,z) = 0,\ 1 \leq j_1 < \ldots < j_{i+1} \leq n\}, \tag{5.12}$$

wobei $M(j_1,\ldots,j_{i+1})$ der aus den Spalten $j_1 \ldots j_{i+1}$ bestehende $(i+1)-$Minor von $J_X(\Phi_i)$ ist. Dann ist die *Diskriminante* Ω_i des Morphismus Φ_i die Projektion von Σ_i in den Parameterraum $\mathbb{C}^{\frac{n(n-1)}{2}}$:

$$\Omega_i := \{z \in \mathbb{C}^{\frac{n(n-1)}{2}} | (x,z) \in \Sigma_i, \quad \text{für ein} \quad x \in \mathbb{C}^n\} \tag{5.13}$$

Bezeichnet man mit m denjenigen $i-$Minor von $J_{X,Z}(\Phi_i)$, der aus den ersten i Zeilen und Spalten von $J_{X,Z}(\Phi_i)$ gebildet ist, so soll Σ_i außerhalb der Hyperfläche

$$V(m) := \{(x,z) \in \mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}} |\ m(x,z) = 0\} \tag{5.14}$$

mit

$$(\Sigma_i)_m := \Sigma_i \setminus V(m) = \Phi^{-1}(0) \cap (\Delta(\Phi_i))_m \tag{5.15}$$

bezeichnet werden.

Analog wie beim Beweis von Behauptung 22 erhalten wir mit dem Wechsellemma 21 $(\Sigma_i)_m =$

$$\{(x,\overline{a}) \in \Phi^{-1}(0) |\ m(x,\overline{a}) \neq 0, M(1,\ldots,i,l)(x,\overline{a}) = 0, l \in \{i+1,\ldots,n\}\}, \tag{5.16}$$

wobei $M(1,\ldots,i,l)$ den aus den ersten i Spalten und der Spalte l bestehenden $(i+1)-$Minor der Teilmatrix $J_X(\Phi)$ der Jacobimatrix $J(\Phi)$ bezeichnet.

Die Varietät Σ_i ist außerhalb der Hyperfläche

$$\{(x,z) \in \mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}} \mid m(x,z) = 0\},$$

durch die Polynome

$$F_0 = f, F_1 = \frac{\partial f}{\partial X_1} + \sum_{l=i+1}^{n} Z_{l,1}\frac{\partial f}{\partial X_l}, \ldots, F_i = \frac{\partial f}{\partial X_i} + \sum_{l=i+1}^{n} Z_{l,i}\frac{\partial f}{\partial X_l}$$

und

$$M(1,\ldots,i,i+1) = M(1,\ldots,i,i+2) = \ldots = M(1,\ldots,i,n) = 0,$$

beschrieben.

Unter der Voraussetzung, daß die reelle Varietät $V := W \cap \mathbb{R}^n$ beschränkt ist, ist die Projektion

$$\pi : V \times \mathbb{R}^{n(n-1)/2} \to \mathbb{R}^{n(n-1)/2} \tag{5.17}$$

echt , d.h. das Urbild $\pi^{-1}(K)$ einer kompakten Menge K von Parametern in $\mathbb{R}^{n(n-1)/2}$ ist in $V \times \mathbb{R}^{n(n-1)/2}$ kompakt. Wir finden nach dem Hauptlemma 11 im Kapitel 3, eine offene und dichte Menge $\mathcal{U}_i \subset \mathbb{R}^{n(n-1)/2}$ von Parametern, so daß die Einschränkung des Morphismus in (5.17) auf $V \times \mathcal{U}_i$ den maximalen Rang $n(n-1)/2$ hat. Die Einschränkung des Morphismus π auf $V \times \mathcal{U}_i$ bestimmt also eine Fibration, (vgl. *Ehreshman's Lemma* [BR90])

$$\begin{array}{ccccc} \pi^{-1}(\mathcal{U}_i) & \to & V & \times & \mathcal{U}_i \\ & \searrow & & \downarrow & \\ & & & \mathcal{U}_i & \end{array} . \tag{5.18}$$

Die Diskriminante

$$\Omega_i = \pi(\Sigma_i) \tag{5.19}$$

ist abgeschlossen.

Da der Index i beliebig fest gewählt war, können wir für die Indizes $1,\ldots,n-1$ offene und dichte Menge von Parametern

$$\mathcal{U}_1,\ldots,\mathcal{U}_{n-1} \subset \mathbb{R}^{\frac{n(n-1)}{2}} \tag{5.20}$$

finden, so daß die Einschränkung des Morphismus π auf

$$V \times (\mathcal{U}_1 \cap \mathcal{U}_2 \cap \ldots \cap \mathcal{U}_{n-1}) \tag{5.21}$$

den maximalen Rang $n(n-1)/2$ hat und eine Fibration induziert

$$\begin{array}{ccccc} \pi^{-1}(\mathcal{U}) & \to & V & \times & \mathcal{U} \\ & \searrow & & \downarrow & \\ & & & \mathcal{U} & \end{array} . \tag{5.22}$$

wobei $\mathcal{U} := \mathcal{U}_1 \cap \ldots \cap \mathcal{U}_{n-1}$ gesetzt ist.

Sei

$$\overline{\pi} : V \times \mathcal{U} \to I\!R^{\frac{n(n-1)}{2}} \tag{5.23}$$

die Einschränkung des Morphismus π auf $V \times \mathcal{U}$, wobei

$$\mathcal{U} := (\mathcal{U}_1 \cap \mathcal{U}_2 \cap \ldots \cap \mathcal{U}_{n-1})$$

ist.

Seien der Index $1 \leq i \leq n-1$ fixiert und $F_k := M(1, \ldots, i, k)$ für $k = i+1, \ldots, n$ gesetzt.

Bemerkung 16
Unter den Voraussetzungen, daß die reelle Varietät

$$V = W \cap I\!R^n = \{x \in I\!R^n |\; f(x) = 0\}$$

nichtleer und glatt ist, können wir ohne Einschränkung der Allgemeinheit nach dem Hauptlemma 11 *schlußfolgern, daß wir eine residuelle Menge von Parametern $z \in \mathbb{C}^{\frac{n(n-1)}{2}}$ finden können, so daß aus der Koordinatentransformation $X = A(z)Y$ nichtleere komplexe polare Varietäten*

$$W_i = \overline{\{x \in \mathbb{C}^n |\; F_0(x) = \ldots = F_i(x, z) = 0, \quad rk\; J_X(F_0, \ldots, F_i) = i+1\}} \tag{5.24}$$

aufgebaut werden.

Die Koordinatentransformation $X = AY$ impliziert die folgende Gleichung der Jacobimatrizen

$$J_Y\left(f^{A(z)}, \frac{\partial f^{A(z)}}{\partial Y_1}, \ldots, \frac{\partial f^{A(z)}}{\partial Y_i}\right) = J_X\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial x_i}\right)\; A(z) \tag{5.25}$$

Eine Deutung des Hauptlemmas 11 im Kapitel 3 auf (5.25) lautet nun
Für eine generische Wahl der Parameter $z \in \mathbb{C}^{\frac{n(n-1)}{2}}$ ist der Rang der Matrix

$$J_Y\left(f^{A(z)}, \frac{\partial f^{A(z)}}{\partial Y_1}, \ldots, \frac{\partial f^{A(z)}}{\partial Y_i}\right)$$

maximal und gleich $i+1$. Unter Beachtung der Gleichung (5.25) ist demzufolge der Rang der Jacobimatrix

$$J_X\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}\right)$$

maximal gleich $i+1$.

Die Bestimmung einer residuelle Menge wie in Bemerkung 16 wird durch die Vermeidung einer Hyperfläche in $\mathbb{C}^{\frac{n(n-1)}{2}}$ erfolgen, welche die Diskriminante Ω_i des

Morphismus Φ_i beschreibt. Diese Diskriminante läßt sich unter den Voraussetzungen in der Bemerkung 16 mit den symbolisch geometrischen Algorithmus in [GHH+97] parametrisieren (vgl. [GS99] zur Lösung parametrischer überbestimmter Systeme).

Wir finden mit dem Hauptlemma 11 in Kapitel 3 eine residuelle Menge $\mathcal{U}_i$ von Parametern in $\mathbb{C}^{\frac{n(n-1)}{2}}$, so daß der singuläre Ort des Morphismus Φ_i eingeschränkt auf $\mathbb{C}^n \times \mathcal{U}_i$, durch die transversale Folge

$$F_0, \ldots, F_i, F_{i+1}, \ldots, F_n \tag{5.26}$$

außerhalb der Hyperfläche

$$V(m) = \{(x,z) \in \mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}} \mid m(x,z) = 0\}$$

beschrieben wird.

Sei

$$\mathcal{U} := \cap_{i=1}^{n-1} \mathcal{U}_i. \tag{5.27}$$

Wir betrachten von nun an nur die Einschränkung des Morphismus Φ_i auf $\mathbb{C}^n \times \mathcal{U}$.

Die Folge $F_0, \ldots, F_i, F_{i+1}, \ldots, F_n$ bildet also eine transversale Folge von Polynomen in $\mathbb{Q}[X_1, \ldots, X_n, Z_{2,1}, \ldots, Z_{n,n-1}]$ außerhalb der Hyperfläche

$$V(m) := \{(x,z) \in \mathbb{C}^{n+\frac{n(n-1)}{2}} \mid m(x,z) = 0\}.$$

Mit $D_j^{(i)}$ bezeichnen wir den affinen Grad der transversalen Folge

$$F_0, \ldots, F_j$$

außerhalb der Hyperfläche $V(m)$, für $0 \leq j \leq i$.

Mit

$$D^{(i)} := \max\{D_j^{(i)} \mid 1 \leq j \leq n\} \tag{5.28}$$

bezeichnen wir den affinen Grad der transversalen Folge

$$F_0, \ldots, F_i, F_{i+1}, \ldots, F_n$$

außerhalb der Hyperfläche $V(m)$. Sei

$$D := \max\{D^{(i)} \mid 1 \leq i \leq n\}. \tag{5.29}$$

Aus der Bezout–Ungleichung erhalten wir eine Schranke für $D^{(i)}$ und D:

$$D^{(i)} \leq d^{i+1}[(i+1)(d-1)]^{n-i} \leq (i+1)^{n-i} d^{n+1}; \tag{5.30}$$

$$D := \max\{D^{(i)} \mid 1 \leq i \leq n-1\} \leq \max_{1 \leq k \leq n} (k^{n-k+1}) d^{n+1}. \tag{5.31}$$

Sei der Index i beliebig und fest $1 \leq i \leq n-1$. Mit m bezeichnen wir wie oben den aus den ersten i Zeilen und Spalten der Jacobimatrix $J_X(F_0, \ldots, F_i)$ bestehenden $(i)-$Minor. Unter den Voraussetzungen in Bemerkung 16 bilden die Polynome

$$F_0, \ldots, F_i, F_{i+1}, \ldots, F_n \in \mathbb{Q}[X_1, \ldots, X_n, Z_{2,1}, \ldots, Z_{n,n-1}]$$

eine transversale Folge außerhalb der Hyperfläche $V(m)$, und beschreiben den singulären Ort $\Sigma_i := Sing\ \Phi_i$.

Wir fassen im folgenden Theorem das Ergebnis über die generische Darstellung der Koordinaten $X_1, \ldots, X_n$ bezüglich einer Hyperfläche $\{x \in \mathbb{C}^n | f(x) = 0\}$ zusammen. Dieses Verfahren ist eine Anpassung des in [GS99] veröffentlichten Algorithmus zur Lösung überbestimmter polynomialer Systeme.

Satz 28 (Generische Koordinaten)
Seien n, d, L nichtnegative ganze Zahlen. Wir setzen voraus, daß ein divisionsfreies Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ mit Größe L derart gegeben ist, daß β ein nichtkonstantes quadratfreies Polynom $f \in \mathbb{Q}[X_1, \ldots, X_n]$ von der Gradschranke d darstellt. Dann gibt es ein arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$, und der Größe $(ndDL)^{O(1)}$, welches aus dem Straight–Line Programm β ein arithmetisches γ Netzwerk erzeugt. Das Netzwerk γ hat eine Größe $(ndDL)^{O(1)}$ und erzeugt eine reguläre untere $(n \times n)-$Dreiecksmatrix

$$A(z) := \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & 0 \\ z_{2,1} & 1 & 0 & \ldots & \ldots & 0 \\ z_{3,1} & z_{3,2} & 1 & 0 & \ldots & \vdots \\ \vdots & \ldots & \ddots & 1 & \ddots & \vdots \\ z_{n-1,1} & \ldots & \ldots & z_{n-1,n-2} & 1 & 0 \\ z_{n,1} & \ldots & \ldots & \ldots & z_{n,n-1} & 1 \end{pmatrix}. \tag{5.32}$$

Die Koordinatentransformation $X = A(z)Y$ mit $A(z)$ nach 5.32 bewirkt, daß die Variablen $Y_1, \ldots, Y_n$ in generischer Position bezüglich der Varietät

$$\widetilde{W}_i = \{y \in \mathbb{C}^n |\ f^{A(z)}(y) = \frac{\partial f^{A(z)}(y)}{\partial Y_1} = \ldots = \frac{\partial f^{A(z)}(y)}{\partial Y_i} = 0\} \tag{5.33}$$

sind.

Beweis:

Sei der Index $i,\ 1 \leq i \leq n-1$ beliebig aber fest. Da der Morphismus Φ_i eingeschränkt auf $\mathbb{C}^n \times \mathcal{U}$ ist, bildet die Folge

$$F_0, \ldots, F_i, F_{i+1}, \ldots, F_n$$

eine transversale Folge außerhalb der Hyperfläche $V(m)$.

Wir wollen die Parameter der regulär Matrix $A(z)$ außerhalb der Diskriminante Ω_i, der Abbildung Φ_i bestimmen.

1. Im ersten Schritt des Beweises geben wir eine geometrische Lösung der transversalen Folge von Polynomen
$$F_0, \ldots, F_i, F_{i+1}, \ldots, F_n, \tag{5.34}$$
außerhalb der Hyperfläche $V(m) = \{(x,z) \in \mathbb{C}^{n+n(n-1)/2} | \ m(x,z) = 0\}$ an. Der singuläre Ort $SingW_i$ läßt sich als eine Hyperfläche in $\mathbb{C}^{\frac{n(n-1)}{2}}$ parametrisieren.

2. Im zweiten Schritt bestimmen wir die Parameter $Z_{2,1}, \ldots, Z_{n,n-1}$ außerhalb der Vereinigung $\cup_{i=1}^{n-1} \Omega_i$.

Die auf diese Weise gewählten Parameter $z \in \mathbb{C}^{n(n-1)/2}$ liegen nicht in der Diskriminante Ω_i, da für jedes $x \in \mathbb{C}^n$ mit $\Phi_i(x,z) = 0$ der Punkt (x,z) keine Lösung des Systems
$$F_0(x,z) = \ldots = F_i(x,z) = F_{i+1}(x,z) = \ldots = F_n(x,z) = 0$$
ist, welches Σ_i außerhalb der Hyperfläche $\{(x,z) \in \mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}} | \ m(x,z) = 0\}$ beschreibt.

Sei
$$\overline{\pi} : V \times \mathcal{U} \to \mathbb{C}^{\frac{n(n-1)}{2}} \tag{5.35}$$
die Einschränkung des Morphismus π auf $\mathbb{C}^n \times \mathcal{U}$, wobei
$$\mathcal{U} := (\mathcal{U}_1 \cap \mathcal{U}_2 \cap \ldots \cap \mathcal{U}_{n-1})$$
ist. Wir wollen diese Projektion mit einer Eliminationsprozedur beschreiben und damit auch eine Prozedur zur Vermeidung der Diskriminante Ω_i aufbauen:

Bemerkung 17
Der Morphismus $\pi : \mathbb{C}^n \times \mathbb{C}^{n(n-1)/2} \to \mathbb{C}^{n(n-1)/2}$ ist allgemein nicht echt, und die Diskriminante Ω allgemein nicht abgeschlossen. Wenn wir in diesem Fall von den definierenden Gleichungen der Diskriminanten sprechen, so meinen wir die Gleichungen, die den Zariski–Abschluß von Ω definieren.

Da nach Bemerkung 16 die komplexe polare Varietät W_i für jeden Index $i, 1 \leq i \leq n-1$ nichtleer ist und die Projektion $\overline{\pi} : \mathbb{C}^n \times \mathcal{U} \to \mathbb{C}^{\frac{n(n-1)}{2}}$ die Einschränkung von π auf $\mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}}$ beschreibt, können wir die ersten Variablen $X_1, \ldots, X_n$ eliminieren, indem wir das System
$$F_0, \ldots, F_{n-1} \tag{5.36}$$

außerhalb der Hyperfläche $\{(x,z) \in \mathbb{C}^n \times \mathbb{C}^{\frac{n(n-1)}{2}} \mid m(x,z) = 0\}$ lösen (vgl. Satz 26).

Wir finden ein arithmetisches Netzwerk mit Parametern in $\mathbb{Q}(Z)$, welches die Größe $(ndLD)^{O(1)}$ hat. Das Netzwerk erzeugt ein Straight–Line Programm, welches eine geometrische Lösung der transversalen Folge in (5.36) kodiert. Diese Lösung besteht aus

- dem primitiv minimalen Polynom des primitiven Elementes X_n,
$$q \in \mathbb{Q}[X_n, Z_{2,1}, \ldots, Z_{n,n-1}];$$
- der Diskriminante $\varrho \in \mathbb{Q}[Z_{2,1}, \ldots, Z_{n,n-1}]$ von q
- den Polynomen $v_1, \ldots, v_n \in \mathbb{Q}[X_n, Z_{2,1}, \ldots, Z_{n,n-1}]$.

Diese Polynome haben die folgenden Eigenschaften:

1. Der Grad des minimalen Polynoms q in der Variable X_n ist
$$\deg_{X_n} q = D^{(i)}.$$
2. Die Grade der Polynome $v_1, \ldots, v_n$ in der Variable X_n sind nach oben durch $D^{(i)}$ beschränkt: $\max\{\deg_{X_n} v_j \mid 1 \le j \le n\} \le D^{(i)}$.
3. $(F_0, \ldots, F_i, F_{i+1}, \ldots, F_{n-1})_{m\varrho} = (q(x_n), v_1(x_n), \ldots, v_n(x_n))_{m\varrho}$.

Eine Anwendung des Lemmas 18 zur Bestimmung der Resultante des Ideals

$$(F_0, \ldots, F_i, F_{i+1}, \ldots, F_{n-1})_m$$

und des Polynoms F_n ergibt die gewünschte Wahl der Parameter außerhalb der Diskriminante Ω_i. Das Polynom

$$\overline{F}_n := F_n\left(\frac{v_1(T)}{\varrho_1}, \ldots, \frac{v_n(T)}{\varrho_n}\right) \tag{5.37}$$

liegt in $\mathbb{Q}[T, Z_{2,1}, \ldots, Z_{n,n-1}]$ und ist Nichtnullteiler in der Algebra

$$B_n := R_0[Z_{2,1}, \ldots, Z_{n,n-1}]/(F_0, \ldots, F_i, F_{i+1}, \ldots, F_{n-1}), \tag{5.38}$$

wobei R_0 als $R_0 := \mathbb{Q}[X_1, \ldots, X_n]$ definiert ist. Das Konstantenglied

$$C_0^{(i)} \in Q[Z_2, \ldots, Z_{n,n-1}] \tag{5.39}$$

der Homothetie $\eta_{\overline{F}_n}$, welche durch die Multiplikation mit $\overline{F}_n$ in B_n definiert ist, hat den Grad

$$\deg C_0^{(i)} = D^{(i)} \le d^{i+1}[(i+1)(d-1)]^{n-i} \le (i+1)^{n-i} d^{n+1}. \tag{5.40}$$

Unter Benutzung der Behauptung 9 finden wir Parameter

$$a_{2,1},\ldots,a_{n,n-1}\in\mathbb{Q}$$

mit der Eigenschaft, daß der Wert von $C_0^{(i)}$ in diesen Parametern von Null verschieden ist.

$$C_0^{(i)}(a_{2,1},\ldots,a_{n,n-1})\neq 0. \tag{5.41}$$

Eine Schranke der Höhe dieser Parameter ist durch die Zahl

$$\max\{ht(a_{k,l})|i+1\leq k\leq n,\ 1\leq l\leq i\}\leq(2^{\ell'+1}-2)(2^{\ell'}+1)^2 \tag{5.42}$$

gegeben, wobei die Ungleichung

$$\ell'\leq(n+1)\log_2 d+(n-i)\log_2(i+1) \tag{5.43}$$

gilt.

Eine lokale Beschreibung der Diskriminante des Morphismus Φ_i erreichen wir, indem wir zuerst eine reguläre untere $(\frac{n(n-1)}{2}\times\frac{n(n-1)}{2})$–Dreieckmatrix B mit rationalen Koeffizienten finden, welche die Parameter

$$\overline{Z}^t:=\begin{pmatrix}\overline{Z}_{2,1}\\ \vdots\\ \overline{Z}_{n,n-1}\end{pmatrix}=B\begin{pmatrix}Z_{2,1}\\ \vdots\\ Z_{n,n-1}\end{pmatrix}=:BZ^t \tag{5.44}$$

in Noether–Position bzgl. des Zariski–Abschlußes

$$\overline{V(F_0,\ldots,F_{n-1})\setminus V(m)\cup Sing\,W}=$$

$$\left\{\left(\frac{v_1(t,\bar z)}{\varrho},\ldots,\frac{v_n(t,\bar z)}{\varrho},\overline{Z}_{2,1},\ldots,\overline{Z}_{n,n-1}\right)\in\mathbb{C}^n\times\mathbb{C}^{\frac{n(n-1)}{2}}\mid q(t,\bar z)=0\right\} \tag{5.45}$$

darstellen, und eine geometrische Lösung des Systems (5.34) außerhalb der Hyperfläche $V(m)$ bestimmen (vgl. [GS99]). Diese geometrische Lösung besteht aus

- dem primitiv minimalen Polynom des primitiven Elementes $\overline{Z}_{2,1}$,

$$q'(\overline{Z}_{2,1})\in\mathbb{Q}[\overline{Z}_{3,1},\ldots,\overline{Z}_{n,n-1}][T];$$

- der Diskriminante $\varrho\in\mathbb{Q}[\overline{Z}_{3,1},\ldots,\overline{Z}_{n,n-1}]$ von q
- den Polynomen $v_1',\ldots,v_n'\in\mathbb{Q}[\overline{Z}_{3,1},\ldots,\overline{Z}_{n,n-1}][T]$.

Diese Polynome haben die folgenden Eigenschaften:

1. Der Grad des minimalen Polynoms q in der Variable X_n ist

$$\deg_{\overline{Z}_{2,1}}q'=(i+1)(d-1)D^{(i)}.$$

2. Die Grade der Polynome $v_1{}', \ldots, v_n{}'$ in der Variable $\overline{Z}_{2,1}$ sind nach oben durch $(i+1)(d-1)D^{(i)}$ beschränkt: $\max\{\deg_{\overline{Z}_{2,1}} v_j{}' \mid 1 \leq j \leq n\} \leq (i+1)(d-1)D^{(i)}$.

3. $(F_0, \ldots, F_i, F_{i+1}, \ldots, F_n)_{m\varrho} = (q'(\overline{Z}_{2,1}), v_1{}'(\overline{Z}_{2,1}), \ldots, v_n{}'(\overline{Z}_{2,1}))_{m\varrho}$.

Bemerkung 18 *Die Parameter $Z_{2,1}, \ldots, Z_{n,n-1}$ lassen sich mit der inverse Matrix B^{-1} berechnen $Z^t = B^{-1}\overline{Z}$.*

Da der Grad des minimalen Polynoms q' in $Z_{2,1}$ kleiner als D ist, finden wir unendlich viele Punkte $z_{2,1} \in \mathbb{Q}$ mit $q'(z_{2,1}) \neq 0$, und somit auch unendlich viele Punkte $z = (z_{2,1}, \ldots, z_{n-1,n}) \in \mathbb{Q}^{\frac{n(n-1)}{2}}$ außerhalb $\cup_{i=1}^{n-1}\Omega_i$. ∎

Satz 29 (generische Koordinaten)
Sei der Index $i, 0 \leq i \leq n-1$ fest gegeben. Seien $n, d, D^{(i)}, L$ nichtnegative ganze Zahlen. Wir setzen voraus, daß ein divisionsfreies Straight–Line Programm β in $\mathbb{Q}[X_1, \ldots, X_n]$ mit Größe L und Tiefe ℓ gegeben ist, welches die reduzierte Folge von Polynomen $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ mit der Gradschranke d auswertet. Dann gibt es ein arithmetisches Netzwerk mit Parametern in $\mathbb{Q}$, und der Größe $L(ndD^{(i)})^{O(1)}$, welches die Koordinaten $X_1, \ldots, X_n$ in generischer Position bezüglich

$$W_i := W \cap \Delta_i,\ 1 \leq i \leq n-p$$

darstellt, wobei Δ_i die durch alle $p-$Minoren der Untermatrix der Jacobimatrix $J(f_1, \ldots, f_p)$ definiert ist, die aus den Spalten $\{1, \ldots, i+p-1\}$ dieser Matrix besteht. Das Netzwerk wertet das Straight–Line Programm β aus und erzeugt ein Straight–Line Programm der Größe $L(ndD^{(i)})^{O(1)}$, welcher eine reguläre $(n \times n)-$Unterdreiecksmatrix

$$A(\overline{a}) := \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & 0 \\ a_{2,1} & 1 & 0 & \ddots & \ldots & 0 \\ a_{3,1} & a_{3,2} & 1 & 0 & \ldots & \vdots \\ \vdots & \ldots & \ddots & 1 & \ddots & \vdots \\ a_{n-1,1} & \ldots & \ldots & a_{n-1,n-2} & 1 & 0 \\ a_{n,1} & \ldots & \ldots & \ldots & a_{n,n-1} & 1 \end{pmatrix}, \tag{5.46}$$

generiert. Diese Matrix ist zur koordinaten Transformation $X = A(\overline{a})Y$ assoziert, und die Variablen $X_1, \ldots, X_n$ sind in generischer Position bezüglich der algebraischen Menge $W_i,\ 1 \leq i \leq n-p$ dargestellt.

Dieser Satz ist die Verallgemeinerung des im Kapitel 5 bewiesenen Satzes 28 für den Hyperflächenfall. Sein Beweis läßt sich bis auf einigen technischen Umformungen, wie den des Satzes 28 durchführen.

Literaturverzeichnis

[Abd97] J. Abdeljaoued. The Berkowitz Algorithm, Maple and Computing the Characteristic Polynomial in an Arbitrary Commutative Ring. *Computer Algebra MapleTech*, 4(3):21–32, 1997.

[AS26] E. Artin and O. Schreier. Algebraische Konstruktion reeller Körper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 5, pages 85–99, 1926.

[BGH+95] B. Bank, M. Giusti, J. Heintz, R. Mandel, and G. Mbakop. Polar varieties and efficient real equation solving: The hypersurface case. In B. Bank, J. Guddat, M. A. Jimenez, H. Th. Jongen, and W. Römisch, editors, *Proceedings of the 3rd International Conference on Approximation and Optimization in the Caribbean.* Universidad de las Américas Puebla, 1995.

[BGHM97] B. Bank, M. Giusti, J. Heintz, and G. Mbakop. Polar varieties, real equation solving, and data structures: The hypersurface case. *J. of Complexity*, 13(1):5–27, 1997.

[BOKR86] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci.*, pages 251–264, 1986.

[Bou84] N. Bourbaki. *Éléments d'histoire des mathématiques.* Masson, Paris Milan Barcelone, 1984.

[BPR94] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 632–641, Los Alamitos, CA, USA, nov 1994. IEEE Computer Society Press.

[BR90] R. Benedetti and J-J. Risler. *Real algebraic Geometry and semi–algebraic sets.* Hermann, Éditeur des Sciences et des Arts, 1990. Actualité Mathematiques.

[BS82] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comp. Sci.*, 22:317–330, 1982.

[Buc70] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes math.*, 4:371–383, 1970.

[Can88] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings 20. ACM STOC*, pages 460–467, 1988.

[CE95] J. Canny and I. Z. Emiris. Efficient incremental algorithms for the sparse resultant and the mixed volume. preprint, 1995.

[CG83] A. L. Chistov and D. Y. Grigoriev. Subexponential time solving systems of algebraic equations. LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[CGH89] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora, editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-6*, volume 357 of *LNCS*, pages 131–152. Springer, 1989.

[Chi95] A. L. Chistov. Polynomial time computation of the dimension of components of algebraic varieties in zero-characteristic. Preprint Université Paris Val de Marne, 1995.

[CR88] M. Coste and M.-F. Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets, 1988.

[Ded95] J.-P. Dedieu. Approximate solutions of numerical problems, condition number analysis and condition number theorems. *Preprint*, 1995.

[Ded97] J.-P. Dedieu. Estimations for the separation number of a polynomial system. *Journal of Symbolic Computation*, 24(6):683–693, dec 1997.

[Dem89] M. Demazure. *Catastrophes et Bifurcations.* X École Polytechnique. ellipses, Paris, 1989. Édition Marketing.

[DFGS91] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33:73–94, 1991.

[Emi96] I. Z. Emiris. On the complexity of sparse elimination. *J. Complexity*, 12:134–166, 1996.

[GG86] M. Golubitsky and V. Guillemin. *Stable Mappings and their Singularities.* Springer-Verlag, 1986.

[GH80] M. Giusti and J.-P.-G. Henry. Les minorations de nombres de milnor. *Bulletin de la Société de Mathématiques de France*, 108:17–45, 1980.

[GH93] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, number XXXIV in Symposia Matematica, pages 216–256. Cambridge University Press, 1993.

[GHH+97] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for diophantine approximation. In *Proceedings of MEGA'96*, volume 117,118, pages 277–317. Journal of Pure and Applied Algebra, 1997.

[GHL+98] M. Giusti, K. Hägele, G. Lecerf, J. Marchand, and B. Salvy. The Projective Noether Maple Package: Computing the Dimension of a Projective Variety. *Journal of Symbolic Computation*, 11:1–000, 1998.

[GHM+98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–line programs in geometric elimination theory. *J. of Pure and App. Algebra*, 124:101–146, 1998.

[GHMP95] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be solved fast? In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[GLS99] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner Free Alternative for Polynomial System Solving. Technical report, Laboratoire GAGE, Polytechnique, Palaiseau, Paris, 1999.

[GM89] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using gröbner bases. In *Proc. 5th Internat. Symp. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-5*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257. Springer Verlag Berlin, 1989.

[Gri88] D. Grigoriev. Complexity of deciding Tarski algebra. *J. Symbolic Comput.*, 3:65–108, February 1988.

[GS99] M. Giusti and E. Schost. Solving overdetermined polynomial systems. Preprint, UMS MEDICIS, Laboratoire GAGE, École Polytechnique, 1999.

[GV88] D. Yu. Grigoriev and N. N. Vorobjov, Jr. Solving systems of polynomial inequalities in sub-exponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, February 1988.

[Häg98] K. Hägele. *Intrinsic Height estimates for the Nullstellensatz.* PhD thesis, Universidad de Cantabria, Spain, 1998.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, 24(3):239–277, 1983.

[Her53] Ch. Hermite. Remarques sur le théorème de M. Sturm. *Comptes rendus de l'Académie des sciences*, 36, 1853.

[Her26] G. Hermann. Die frage der endlich vielen schritte in der theorie de polynomideale. *Math. Ann.*, 95:736–788, 1926.

[HMW99] J. Heintz, G. Matera, and A. Waissbein. On the time–space complexity of geometric elimination procedures. Technical report, Departamento de Matemática, Universidad de Buenos Aires, 1999.

[HRS89a] J. Heintz, M.-F. Roy, and P. Solernó. Complexité du principe de tarski-seidenberg. *C. R. Acad. Sci. Paris*, 309(I):825–830, 1989.

[HRS89b] J. Heintz, M.-F. Roy, and P. Solernó. On the complexity of semialgebraic sets. In G.X.Ritter, editor, *Proc. Information Processing*, volume 89, pages 293–298. North-Holland, 1989.

[HRS90] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de tarski-seidenberg. *Bull. Soc. Math. de France*, 118:101–126, 1990.

[HS82] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *Logic and Algorithmic*, volume 30 of *Monographie de l'Enseignement Mathématique*, pages 237–254, 1982.

[HW75] J. Heintz and R. Wüthrich. An efficient quantifier elimination algorithm for algebraically closed fields of any characteristic. *SIGSAM Bull.*, 9(4), 1975.

[KP94] T. Krick and L. M. Pardo. Une approche informatique pour l' approximation diophantienne. *C. R. Acad. Sci. Paris*, 318(1):407–412, 1994.

[KP96] T. Krick and L. M. Pardo. A computational method for diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254. Birkhäuser Verlag, 1996.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. reine angew. Math.*, 92:1–122, 1882.

[Kun80] E. Kunz. *Einführung in die kommutative Algebra und Algebraische Geometrie*, volume 46 of *Aufbaukurs Mathematik.* Vieweg Studium, 1980.

[Lan62] S. Lang. *Diophantine Geometry.* Interscience Publishers John Wiley & Sons, 1962.

[Laz77] D. Lazard. Algèbre linéaire sur $k[x_1, \ldots, x_n]$ et élimination. *Bull. Soc. Math. France*, 105:165–190, 1977.

[Laz81] D. Lazard. Résolution des systèmes d'équations algébriques. *Theor. Comp. Sci.*, 15:77–110, 1981.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:534–543, 1982.

[LT81] D. T. Lê and B. Teissier. Variétés polaires locales et classes de chern des variétés singuliéres. *Ann. of Math.*, 114:457–491, 1981.

[Mac16] F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[Mat94] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1994.

[Mat97] G. Matera. *Sobre la complejidad en espacio y tiempo de la eliminación geométrica.* PhD thesis, Universidad de Buenos Aires, Argentina, 1997.

[Mil64] John Milnor. On the betti numbers of real algebraic varieties. *Proc. Amer. Math. Soc.*, 15:275–280, 1964.

[Mor84] J. Morgenstern. How to compute fast a function an all its derivatives. Prepublication No. 49, Université de Nice, 1984.

[Mor97] J. E. Morais. *Resolución eficaz de sistemas de ecuaciones polinomiales.* PhD thesis, Universidad de Cantabria, Santander, Spain, 1997.

[Par95] L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, editors, *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69. Springer, Berlin, 1995.

[Ren88a] J. Renegar. A faster PSPACE algorithm for the existential theory of the reals. In *29th Annual Symposium on the Foundation of Computer Science, FOCS*, pages 291–295, White Plains, New York, oct 1988. IEEE.

[Ren88b] J. Renegar. On the computational complexity and geometry of the first–order theory of the reals. part I: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of Symbolic Computation*, 13(3):255–299, March 1988.

[RS90] M.-F. Roy and A. Szpirglas. Complexity of computation with real algebraic numbers. *J. Symbolic Computat.*, 10:39–51, 1990.

[Sei74] A. Seidenberg. Constructions in algebra. *Transactions Amer. Math. Soc.*, 197:273–313, 1974.

[Sev47] F. Severi. Über die Darstellung algebraischer Mannigfaltigkeiten als Durchschnitte von Formen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, pages 97–119, 1943- 47.

[Sol89] P. Solernó. *Complejidad de conjuntos semialgebraicos*. PhD thesis, Universidad de Buenos Aires, Argentina, 1989.

[SS93a] M. Shub and S. Smale. Complexity of Bézout's theorem I: Geometric aspects. *J. of the AMS*, 6(2):459–501, 1993.

[SS93b] M. Shub and S. Smale. Complexity of Bézout's theorem II: Volumes and probabilities. In *Proceeding effective methods in Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 267–285. MEGA '92, Niece, Birkhäuser, 1993.

[SS93c] M. Shub and S. Smale. Complexity of Bézout's theorem III: Condition number and packing. *J. of Complexity*, 9:4–14, 1993.

[SS94] M. Shub and S. Smale. Complexity of Bézout's theorem V: Polynomial time. *Theor. Comp. Sci.*, 133:141–164, 1994.

[SS96] M. Shub and S. Smale. Complexity of Bezout's theorem. IV. probability of success and extensions. *SIAM Journal on Numerical Analysis*, 33(1):128–148, February 1996.

[Stu35] Ch. F. Sturm. Mémoire sur la résolution des équations numériques. *Mémoires présentés par divers savants étrangers à l'Academie Royale des Sciences, sections sciences mathématiques et physiques*, pages 273–318, 1835.

[Syl53] J. J. Sylvester. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. In *Philosophical transactions of the Royal Society of London*, volume 143, pages 407–548, 1853.

[Van58] B. L. Van der Waerden. Ueber André Weil Neubegründung der algebraischen Geometrie. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg: Emil Artin zum 60. Geburtstag*, volume 22, 1958.

[vzGS91] J. von zur Gathen and G. Seroussi. Boolean circuits versus arithmetic circuits. *Information and Computation*, 91:142–154, 1991.

[Wei46] A. Weil. *Foundations of algebraic geometry*, volume 29. Amer. Math. Soc. Coll. Publ., New York, 1946.

[Zar95] O. Zariski. *Algebraic Surfaces.* Classics in Mathematics. Springer, 1995.

Symbole

bzgl.	bezüglich
d.h.	das heißt
vgl.	vergleich[e]
z.B.	zum Beispiel
$\emptyset$	leere Menge
$\mathbb{N}$	Menge der nicht negativen ganzen Zahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{R}^n$	n-dimensionaler Euklidischer Raum
$\mathbb{C}$	Menge der komplexen Zahlen
$\mathbb{C}^n$	n-dimensionaler komplexer Raum
$X_1, \ldots, X_n$	Koordinaten
$\mathbb{Z}[X_1, \ldots, X_n]$	Polynomialer Ring mit ganzen Koeffizienten
$\mathbb{Q}[X_1, \ldots, X_n]$	Polynomialer Ring mit rationalen Koeffizienten
$\mathbb{R}[X_1, \ldots, X_n]$	Polynomialer Ring mit reellen Koeffizienten
$\mathbb{C}[X_1, \ldots, X_n]$	Polynomialer Ring mit komplexen Koeffizienten.
$f_1, \ldots, f_p$	Polynome in $\mathbb{Q}[X_1, \ldots, X_n]$
d	maximaler Grad der Polynome $f_1, \ldots, f_p$
δ	geometrischer Grad
δ^*	reeller Grad
$J(f_1, \ldots, f_p)$	Jacobimatrix von $f_1, \ldots, f_p$
$m, \tilde{m}$	$(p-1)-$Minoren in $J(f_1, \ldots, f_p)$
$M(i_1, \ldots, i_p)$	der aus den Spalten $i_1, \ldots, i_p)$ bestehende $p-$Minor von $J(f_1, \ldots, f_p)$
$V(m)$	die durch m beschriebene Hyperfläche
$W := V(f_1, \ldots, f_p)$	die von $f_1, \ldots, f_p$ definierte Varietät
$(f_1, \ldots, f_p)$	das von $f_1, \ldots, f_p$ erzeugte Ideal
$\sqrt{(f_1, \ldots, f_p)}$	das radikale Ideal von $(f_1, \ldots, f_p)$
$Sing\ W$	die Menge der singulären Punkte in W
$[X^i$	der lineare Raum $\{x \in \mathbb{C}^n \mid x_{i+1} = \ldots = x_n = 0\}$

Δ_i	die Determinanten Varietät, welche durch $p-$Minoren der Spalten $1,\ldots,p+i-1$ in $J(f_1,\ldots,f_p)$ beschrieben ist
$(\Delta_i)_m$	$(\Delta_i)\setminus V(m) \quad 1\leq i\leq n-p$
$\widetilde{W}_i$	$W\cap\Delta_i \quad 1\leq i\leq n-p$
W_i	die zum linearen Raum X^i assoziierte polare Varietät $\overline{\widetilde{W}_i\setminus Sing\, W}$
V_i	die zum linearen Raum X^i assoziierte reelle polare Varietät $W_i\cap\mathbb{R}^n$
U,u	primitives Element einer polynomialen Ringerweiterung
q	minimales Polynom des primitiven Elementes u
$\varrho:=\prod_{i=1}^n\varrho_i$	Diskriminante des minimalen Polynoms q
$v_1,\ldots,v_n$	Polynome in $\mathbb{Q}[T]$
β	arithmetischer Schaltkreis
L	Größe von β
ℓ	nichtskalare Tiefe von β
$\mathcal{N}$	arithmetisches Netzwerk
$\frac{\partial f}{\partial X_i}$	partiellen Ableitung nach $X_i,\ 1\leq i\leq n$

Danksagung

Ein herzliches Dankeschön für ihre wertvolle Hilfe an die Professoren *Bernd Bank, Marc Giusti* und *Joos Heintz*, die mich im Laufe der Arbeit unterstützten. Der Weg, den ich mit dieser Arbeit verfolgt habe, geht in das Jahr 1995 zurück, als ich Stipendiat des Graduiertenkollegs Geometrie und Angewandte Analysis an der Humboldt–Universität war. Ich bin Herrn Professor *Jürgen Guddat* sowie meinen Kommilitonen für die gute Zeit im Gaduiertenkolleg zu Dank verpflichtet. Diese Dissertation nahm ihren Wendepunkt durch intensives Zusammenwirken der oben genannten Professoren während der Publikation [BGHM97], die mich auf Vorschlag meines Betreuers, Professor *Bernd Bank*, nach Santander führte. Mein Aufenthalt vom 25.3. bis 20.4.'96 an der Universidad de Cantabria war fruchtbar und ich lernte dort die Professoren *Joos Heintz* und *Luis–Miguel Pardo* sowie *Klemens Hägele* und *Enrique Morais* kennen. Ich danke diesen hochgeschätzten Freunden, die mir die Methode der Elimination bis in die Details vermittelten. In Santander traf ich Professor *Marc Giusti* während der TERA'96 Tagung (Turbo Evaluation and Rapid Algorithms). Diese Begegnung hat mich bewegt, mehr über die polaren Varietäten zu lernen. Mein Aufenthalt vom 27.1. bis 7.2.'97 an der École Polytechnique in Paris hat meine Arbeit sehr positiv beeinflußt. Viele Menschen haben mir bei diesem Unterfangen geholfen. Ich bin ihnen allen für ihre Freundschaft und Ratschläge zu Dank verpflichtet. Namentlich bedanke ich mich bei Herrn Professor Pablo Solernó für die guten Ratschläge und Hinweise. Für ihre Bemerkungen und Richtigstellungen meines schwer verständlichen Deutsches danke ich Frau *Jutta Kerger* und Herrn *Lutz Lehman*. Ein besonderer Dank gilt der Familie *Frömer* für ihre anregenden Ratschläge und ihre Sympathie. Ich bin der Gruppe Optimierung des Instituts für Mathematik der Humboldt–Universität sehr dankbar für die guten Arbeitsbedingungen, die mir über Jahre hinweg zur Verfügung standen. Meine zwei jährige Tätigkeit als wissenschaftlicher Mitarbeiter bei Herrn Professor *Bernd Bank* hat dazu beigetragen, diese Arbeit zu Ende zu schreiben. Zu guter Letzt gebührt mein Dank meiner Familie für ihre motivierenden Unterstützungen aller Form, wie auch ihr Verständnis.

Curriculum Vitae

Name:	Mbakop Guy Merlin
Geboren am:	9. August 1966
in:	Bangoua (Kamerun)
Vater:	Nguele Pierre Lebel
Mutter:	Ngahane Jacqueline

Ausbildung und wissenschaftlischer Werdegang

1970 – 1972:	Besuch des Kindergartens *Saint Kisito* in Nkongsamba.
1972 – 1978:	Schulbesuch in der *École Saint Martin* in Nkongsamba.
1978 – 1983:	Ausbildung im *Colège Saint Michel* in Melong, mit dem Abschluß Brevet d'Étude du Premier Cycle B.E.P.C.
1983 – 1985:	Ausbildung im Gymnasium *Lycée de Manengoumba,* Nkongsamba Zeugnisse: Probatoire série C und Baccalauréat série C.
1985 – 1986:	Ausbildung in Mathematik und Informatik an der Universität zu Jaunde (Kamerun).
1986 – 1987:	Sprachausbildung in Glauchau bei Chemnitz (DDR).
1987 – 1993:	Studium der Mathematik an der Humboldt–Universität zu Berlin mit dem Abschluß–Zeugnis Diplom–Mathematiker Diplomarbeit: Komplexität von Wortsproblemen in der Theorie der verbandsgeordneten abelschen Gruppen.
1993 – 1996:	Stipendiat des Graduiertenkollegs Analysis und Geometrie des Instituts für Mathematik der Humboldt–Universität.
01.10. – 30.11.96:	Wissenschaftlicher Mitarbeiter am Weierstraß Institut für Angewandte Analysis und Stochastik (WIAS Berlin).
22.04.97 – 22.04.99:	Wissenschaftlicher Mitarbeiter am Institut für Mathematik der Humboldt–Universität zu Berlin.

Wichtige Forschungsaufenthalte

17.07. – 11.08.95:	Teilnahme am AMS-SIAM Summer Seminar in Applied Mathematics, Park City (Utah, USA).
25.03. – 20.04.96:	Aufenthalt an der Universidad de Cantabria Santander. Teilnahme am TERA – Workshop *Geometry and Computation*.
27.01. – 07.02.97	Aufenthalt an der École Polytechnique de Paris, Palaiseau.
01.12. – 05. 12.97:	École Polytechnique de Paris, Palaiseau.
08.06 – 12.06.98:	Teilnahme an der Tagung Meeting of young researchers: Real Algebraic and Analytic Geometry in Pisa, Italien.
18.08 – 27.08.98:	Teilnahme und Mitarbeit am International Congress of Mathematicians ICM'98, in Berlin.

Öffentlichkeitsarbeit und Publikationen

- 09.'94: Mitbegründer des Projekts *Exchange* zur Bereitsstellung und Sendung von Bücher an die Universitäten in Kamerun.

- '95: Verantwortlicher für Politik und Auswärtiges bei der *Afrikanischen Studentenunion* in Berlin.

- B. Bank, M. Giusti, J. Heintz, R. Mandel, and G. Mbakop. Polar varieties and efficient real equation solving: The hypersurface case. Proceedings of the 3rd International Conference on Approximation and Optimization in the Caribbean. Universidad de las Américas Puebla, 1995.

- B. Bank, M. Giusti, J. Heintz, and G. Mbakop. Polar varieties, real equation solving, and data structures: The hypersurface case. J. of Complexity, 13(1):5–27, 1997. Selected Co–winner: Best Paper Award'97 of J. of Complexity, awarded at FoCM'99.