Positivität symmetrischer Polynome

Diplomarbeit

Universität Konstanz
Fachbereich Mathematik und Statistik
Betreuer: Prof. Dr. A. Prestel

David Grimm

September 2005

Inhaltsverzeichnis

Einleitung

Ausgangspunkt dieser Arbeit war eine Veröffentlichung von Dr. Vlad Timofte in [Ti], in welcher er unter anderem zu folgendem bemerkenswerten Resultat kommt: Die Positivität (oder auch Nichtnegativität) eines gegebenen unter Variablenpermutation invarianten Polynoms f in n Unbestimmten und vom Grad $d \geq 4$, kann auf einer Teilmenge des $\mathbb{R}^n$ getestet werden, die ich hier plakativ als die "*Diagonalflächen der Dimension* $\lfloor \frac{d}{2} \rfloor$" bezeichnen will. Besonders bemerkenswert ist dabei, daß die "Dimension" der Testmenge nur vom Grad, und überhaupt nicht von der Anzahl der Unbestimmten des Polynoms abhängt. Den Beweis für dieses Resultat von Timofte habe ich im ersten Teil des 2.Kapitels ausgearbeitet.

Die Motivation für den zweiten Teil des 2.Kapitels war die Fragestellung, ob sich nicht eine ähnliche Testmenge für eine etwas allgemeinere Klasse von invarianten Polynomen finden läßt (etwa alternierende Polynome). Ich konnte dies zwar bejahen, allerdings haben die von mir gefundenen Diagonalflächen-Testmengen den Schönheitsmakel, daß ihre "Dimension" noch (logarithmisch) von der Anzahl der Unbestimmten des zu testenden Polynoms abhängt.

Der Beweis des Resultats von Timofte beruht wesentlich auf der Tatsache, daß die Algebra der symmetrischen Polynome (so nennen wir die unter Variablenpermutation invarianten Polynome) von bestimmten algebraisch unabhängigen symmetrischen Polynomen erzeugt wird. Dies ist im allgemeinen Fall invarianter Polynome nicht mehr der Fall. Es ist also nur natürlich, daß der von mir eingeschlagene Weg im allgemeineren Fall sich sehr von Timoftes Beweis unterscheidet. Dabei kann man die Grundidee beider Beweise noch gemeinsam formulieren: Man betrachtet zu jedem Wert, den ein Polynom f annimmt, die Zusammenhangskomponenten der zugehörigen Faser um zu zeigen, daß der Schnitt mindestens *einer* dieser Zusammenhangskomponenten mit der betrachteten Testmenge nichtleer ist. Timofte konstruiert dazu mittels Differentialgleichungen eine Kurve, ausgehend von einem *beliebigen* Punkt außerhalb der Testmenge, die in den Fasern aller in der Darstellung von f benötigten algebraisch unabängigen symmetrischen Erzeugern verläuft, und die den gegebenen Punkt mit der Testmenge verbindet. Insbesondere verläuft die Kurve dann auch in einer Faser von f.

In meinem Beweis für den allgemeineren symmetrischen Fall, würde eine ähnliche Konstruktion einer Kurve in den Erzeugerfasern nichts bringen. Zwar folgt aus dem Invariantensatz von Hilbert-Noether, daß der Ring der invarianten Polynome von endlich vielen invarianten Polynomen erzeugt wird, man kann auf Grund der fehlenden algebraischen Unabhängigkeit der Erzeuger jedoch nicht mehr aus dem Wissen über den Grad von f auf die in der Darstellung von f verwendeten Erzeuger schließen. Ich ziehe mich deshalb in meinem Beweis auf eine rein kombinatorische Überlegung zurück. Ein Resultat aus der reellen algebraischen Geometrie liefert eine obere Schranke für die mögliche Anzahl der Zusammenhangskomponenten einer algebraischen Menge. Aufgrund der verallgemeinerten Symmetrie (ich spreche dann von der Teilsymmetrie) des Polynoms f, liegt mit jedem Punkt aus dem $\mathbb{R}^n$ gleich die ganze zugehörige Bahn (unter Wirkung der entsprechenden Gruppe) innerhalb einer Faser von f. Die Mächtigkeit der Bahn hängt von der Anzahl der *verschiedenen* Komponenten des Punktes ab. Bei 'zu vielen' verschiedenen Komponenten übersteigt diese Mächtigkeit die Anzahl der Zusammenhangskomponenten der Faser, und nach dem Schubfachprinzip liegen dann zwei Punkte der Bahn in ein und derselben Zusammenhangskomponente der Faser. Gewisse Wegzusammenhangsbetrachtungen zeigen dann, daß in der Faser dann irgendwo ein Punkt liegen muss, der weniger als die ursprünglich Anzahl an verschiedenen Komponenten hat. Durch trickreiches iterieren dieser Betrachtung, erhält man dann eine "diagonale" Testmenge, deren Dimension logarithmisch in n ist.

Der dritte Teil des zweiten Kapitels beruht auf Überlegungen von Dr. Markus Schweighofer. Er zeigte mir einen Weg, einen schönen Zusammenhang zwischen der Existenz "diagonaler" Nichtnegativitätstestmengen für homogene symmetrische Polynome und einer bestimmten Darstellbarkeit gewisser homogener symmetrischer Polynome herzustellen. Seine Hoffnung war dabei, daß ich mittels elementarer kombinatorischer Überlegungen diese Darstellbarkeit beweisen könnte und dadurch gleichzeitig die Existenz "diagonaler" Testmengen für homogene symmetrische Polynome gewinnen könnte. Ein elementarer Beweis der Darstellbarkeit gelang mir leider nicht für alle betrachteten homogenen Polynome. Es zeigte sich sogar, daß sich einfache Beispiel finden lassen, für die ein rein kombinatorischer Beweis nicht funktionieren kann. Gerade für diese Fälle aber fand sich eine gänzlich andere Möglichkeit die gewünschte Darstellung zu zeigen.

Zu guter Letzt habe ich mir im 3.Kapitel dann noch Gedanken zu einer algorithmischen Anwendung der von Timofte gefundenen Diagonaltestmengen gemacht (auf die auch Dr. Vlad Timofte bereits hingewiesen hat). Es geht dabei um die Existenz eines effizienten Algorithmus, der bei fixierter Gradschranke ein beliebiges (insbesondere mit beliebiger Anzahl an Unbestimmten) gegebenes symmetrisches Polynom auf Nichtnegativität (oder auch Positivität) testet. Der Schlüssel zu diesem Algorithmus ist die Tatsache, daß die "Dimension" $\lfloor\frac{d}{2}\rfloor$ der gefundenen Testmengen *nicht* von der Anzahl der Unbestimmten abhängt. Dies führt das Nichtnegativitättesten *eines* Polynoms in n Unbestimmten auf das Testen *mehrerer* Polynome in $\lfloor\frac{d}{2}\rfloor$ Unbestimmten zurück. Das Effiziente daran ist, daß es für eine feste Gradschranke d und feste Anzahl an Unbestimmten (hier $\frac{d}{2}$) für Polynome g, es gewisse polynomiale Ungleichungssysteme gibt, von denen mindestens eines nach Einsetzen der Koeffizienten von g genau dann erfüllt ist, wenn g überall nichtnegativ (positiv) ist (Stichwort: Quantorenelimination). Dies auf alle durch Unbestimmtengleichsetzung erhaltenen Polynome anzuwenden, ist wesentlich effizienter, als für variable Anzahl n der Unbestimmten, besagte Ungleichungssysteme erst zu generieren und dann auf die das ursprüngliche Polynom anzuwenden.

Ich möchte mich an dieser Stelle bei Prof. Dr. Alexander Prestel dafür bedanken, daß er mir ermöglichte an seinem Lehrstuhl die Diplomarbeit zu schreiben. Ebenso möchte ich mich bei seinem Mitarbeiter Dr. Markus Schweighofer bedanken, nicht nur für den schon erwähnten inhaltlichen Beitrag, sondern auch für einige für ihn sicherlich mühsame aber für mich sehr hilfreiche Stunden des Korrekturlesens und gemeinsamen Überarbeitens.

1. Grundlagen

1.1 Theorie der reell abgeschlossenen Körper

In dieser Arbeit werden an zwei Stellen modelltheoretische Ergebnisse der Theorie reell abgeschlossener Körper benutzt. Es ist dies einerseits die Tatsache, daß die Theorie der reell abgeschlossenen Körper die sogenannte *Quantorenelimination* zuläßt und andererseits, als Folgerung, die *Vollständigkeit* dieser Theorie.

Leser, denen diese Ergebnisse bekannt sind, können diesen Teil überspringen. Ich werde an dieser Stelle grundlegende Definitionen, wie zum Beispiel die einer formalen Sprache, einer Theorie oder auch eines Modells für eine Theorie, als bekannt voraussetzen. Auch werde ich die hier aufgeschriebenen Resultate nur zitieren. All dies läßt sich in [Pr] sehr gut nachlesen.

Folgendes allgemeines Vollständigkeitsresultat geht auf Gödel zurück.

Satz 1.1.1 (Gödels Vollständigkeitssatz). *Sei Σ ein Axiomensystem einer formalen Sprache L der Logik erster Stufe. Sei φ eine Aussage in der formalen Sprache L, dann ist φ aus Σ deduzierbar genau dann, wenn φ in jedem Modell von Σ gilt.*

siehe [Pr, Seite 60]

Definition 1.1.2. Sei mit $\mathrm{Aus}(L)$ die Menge aller Aussagen in der formalen Sprache L bezeichnet. Eine Theorie $\Sigma \subset \mathrm{Aus}(L)$ heißt *vollständig*, wenn für jedes $\varphi \in \mathrm{Aus}(L)$ gilt $\varphi \in \Sigma$ oder $\neg\varphi \in \Sigma$.

Definition 1.1.3. Einer Formel δ in einer formalen Sprachen L heißt *quantorenfrei*, wenn in δ die Zeichen $\forall, \exists$ nicht auftauchen, also wenn alle vorkommenden

Variablen frei sind.

Definition 1.1.4 (Quantorenelimination). Eine Theorie $\Sigma \subset \mathrm{Aus}(L)$ *erlaubt Quantorenelimination*, falls jede Formel φ in dieser Theorie äquivalent zu einer quantorenfreien Formel δ ist, deren Variablen in φ *frei* vorkommen.

Definition 1.1.5. Einen angeordneten Körper $(R, \leq)$, dessen echte algebraische Erweiterungen allesamt keine Anordnung besitzen, nennt man *reell abgeschlossen*

Wir betrachten hier die formale Sprache der angeordneten Ringe, und über dieser die Theorie RCF, welche der deduktive Abschluß des Axiomensystems der angeordneten Körper zusammen mit den unendlich vielen Axiomen für $d \in \mathbb{N}$:

$$RC_0 : \forall x \exists y (x < 0 \vee x = y^2)$$
$$RC_d : \forall a_0 ... \forall a_{2d} \exists x (x^{2d+1} + a_{2d} x^{2d} + ... + a_0 = 0)$$

ist. Artin und Schreier bewiesen im Jahr 1926, daß die reell abgeschlossenen Körper *genau* die Modelle dieser Theorie sind.

Satz 1.1.6 (RCF erlaubt QE). *Es gibt einen Algorithmus, der zu jeder Formel $\phi(X_1, ..., X_n)$ eine in RCF äquivalente quantorenfreie Formel $\delta(X_1, ..., X_n)$ generiert.*

Beweis. Der Beweis vollzieht sich in zwei Schritten. Zunächst kann man mit modelltheoretischen Methoden zu jeder Formel $\phi(X_1, ..., X_n)$, die Existenz einer quantorenfreien Formel $\delta(X_1, ..., X_n)$ zeigen, welche in jedem reell abgeschlossenen Körper äquivalent zu ϕ ist [Pr2, Theorem 2.1.6 und Seite 41 ff]. Mit Gödels Vollständigkeitssatz ist also die Aussage

$$(\star) \quad \forall X_1, ..., \forall X_n \big(\phi(X_1, ..., X_n) \leftrightarrow \delta(X_1, ..., X_n)\big)$$

aus der Theorie RCF.

Im zweiten Schritt überlegt man sich, daß man δ auch effektiv generieren kann. Man schreibt einfach nacheinander für jedes $l \in \mathbb{N}$ alle möglichen (endlich vielen) Beweise der Länge l, welche die obigen Axiome von RCF benutzt, auf. Irgendwann muß in irgendeiner dieser Beweisketten am Ende die Aussage $(\star)$ stehen für ein quantorenfreie Formel δ. Dieses δ ist die gesuchte quantorenfreie Formel. $\square$

Daraus kann die Vollständigkeit der Theorie RCF gefolgert werden, da quantorenfreie Aussagen in dieser Sprache boolesche Kombinationen von Relationen ($<$) und Gleichungen von Termen in $\mathbb{Z}$ sind, und diese in jedem reell abgeschlossenen Körper simultan wahr oder simultan falsch sind, und also mit Gödels Vollständigkeitssatz 1.1.1 die Aussage oder die negierte Aussage aus den Axiomen der Theorie RCF deduzierbar ist.

Satz 1.1.7. *RCF ist eine vollständige Theorie.*

1.2 Teilsymmetrische Polynome

Es bezeichne $K[X_1, ..., X_n]$ den Polynomring in n Unbestimmten über einem Körper K, sei S_n die symmetrische Gruppe von $\{1, ..., n\}$.

Sei für $k \leq n \in \mathbb{N}$

$$e : \{1, ..., k\} \hookrightarrow \{1, , ..., n\}$$

eine injektive Abbildung. Dann definiert e eine Einbettung

$$\hat{e} : S_k \hookrightarrow S_n \text{ mit } \hat{e}(\sigma)(i) = \begin{cases} e \circ \sigma \circ e^{-1}(i) & \text{falls } i \in e(\{1, ..., k\}) \\ i & \text{sonst} \end{cases}$$

Diese Einbettungen wollen wir in Zukunft *kanonische* Einbettungen von S_k in S_n nennen.

Definition 1.2.1. Sei für jedes $n \in \mathbb{N}$ eine Untergruppe H_n von S_n mit den Eigenschaften

(1) Es gibt ein minimales $l \in \mathbb{N}$, so daß $\#S_n/H_n \leq l$ ist für jedes $n \in \mathbb{N}$.

(2) für jede kanonische Einbettung $\hat{e} : S_k \hookrightarrow S_n$ gilt $\hat{e}(H_k) \subset H_n$.

Die Familie $H := (H_n)_{n \in \mathbb{N}}$ nennen wir dann eine *teilsymmetrische* Familie vom Index l.

Definition 1.2.2. Sei $H := (H_n)_{n \in \mathbb{N}}$ eine teilsymmetrische Familie. Ein Polynom $f \in K[X_1, ..., X_n]$ nennen wir dann H-teilsymmetrisch, falls für alle $\sigma \in H_n$

$$f(X_{\sigma(1)}, ..., X_{\sigma(n)}) = f$$

gilt. Wir bezeichnen mit $\Sigma_H^{(n)}(K)$ die K-Unteralgebra von $K[X_1, ..., X_n]$ der H-teilsymmetrischen Polynome.

Beispiel 1.2.3. Die Familie $A = (A_n)_{n\in\mathbb{N}}$ der alternierenden Gruppen ist eine teilsymmetrische Familie. Die 'alternierenden' Polynome sind die A-teilsymmetrischen Polynome. Die Familie $S = (S_n)_{n\in\mathbb{N}}$ ist eine teilsymmetrische Familie. Die 'symmetrischen Polynome' sind die S-teilsymmetrischen Polynome

Definition 1.2.4. Wir bezeichnen mit $\Sigma^{[n]}(K)$ die K-Unteralgebra der symmetrischen Polynome von $K[X_1, ..., X_n]$.

1.2.1 Erzeuger der symmetrischen Polynome

Nach dem Satz von Hilbert-Noether [Be, Theorem 1.3.1] ist für jede endliche Gruppe G, welche auf einer endlich erzeugten K-Algebra operiert, die Unteralgebra der G-Invarianten ebenfalls endlich erzeugt. Eine Besonderheit der Algebra der symmetrischen Polynome ist allerdings, daß sie von algebraisch unabhängigen Elementen über dem Grundkörper K erzeugt wird. *Eine* solche Algebrabasis sind die sogenannten *elementarsymetrischen* Funktionen

$$s_i = \sum_{1\leq j_1<...<j_i\leq n} X_{j_1}\cdots X_{j_i} \quad \text{für } 1 \leq i \leq n.$$

Diese Tatsache ist besser bekannt als der...

Satz 1.2.5 (Fundamentalsatz der symmetrischen Funktionen). *Für jedes symmetrische Polynom $f(X_1, ..., X_n) \in \Sigma^{(n)}(K)$ gibt es ein eindeutiges $g \in K[T_1, ..., T_n]$ (wobei $T_1, ..., T_n$ Unbestimmte sind), so daß $f = g(s_1, ..., s_n)$.*

Siehe etwa [Ar, Seite 548]. Die Eindeutigkeit des darstellenden Polynoms g besagt die algebraische Unabhängigkeit der elementarsymmetrischen Funktionen. Ausgehend davon werden wir ein für unsere Zwecke geeigneteres algebraisch unabhängiges Algebraerzeugendensystem für $\Sigma^{[n]}(K)$ über K finden (für $\mathrm{char}(K) = 0$).

Die Potenzsymmetrischen Funktionen

Definition 1.2.6. Fur $j \in \mathbb{N}$ nennen wir

$$P_j^{[n]} := X_1^j + ... + X_n^j \in K[X_1, ..., X_n]$$

die *potenzsymmetrische* Funktion vom Grad j in n Unbestimmten.

Falls die Anzahl der Unbestimmten aus dem Zusammenhang klar ist, schreiben wir P_j statt $P_j^{[n]}$.

Satz 1.2.7. *Sei* $\operatorname{char} K > n$ *oder* $\operatorname{char} K = 0$. *Dann ist*

$$\Sigma^{[n]}(K) = K[P_1, ..., P_n],$$

und $P_1, ..., P_n$ *sind* K*-algebraisch unabhängig.*

Beweis. Es genügt zu zeigen, daß sich die *elementarsymmetrischen* Funktionen s_i als Polynome in den P_j darstellen lassen, für $1 \leq j \leq n$. Die algebraische Unabhängigkeit folgt dann einfach aus dem Transzendenzgrad n von $\operatorname{Quot}(\Sigma^{[n]}(K)) = K(s_1, ..., s_n)$ über K. Dazu beweisen wir (mit $s_0 := 1$) zunächst die sogenannten *Newtonrelationen*:
für $n \in \mathbb{N}$ und für $1 \leq k \leq n$ ist in $K[X_1, ..., X_n]$

$$\sum_{j=0}^{k-1} (-1)^j s_j P_{k-j} + (-1)^k k s_k = 0.$$

Wir zeigen dies durch Induktion über n, die Anzahl der Unbestimmten:

Im Fall $n = 1$ ist $s_0 P_1 + (-1)s_1 = 0$ offensichtlich. Gelten also die Newtonrelationen für $n - 1$ Unbestimmte und betrachten wir diese nun in $K[X_1, ..., X_n]$, dann sind zwei Fälle zu unterscheiden:

Falls $k < n$, so betrachten wir das Polynom

$$F := \sum_{j=0}^{k-1} (-1)^j s_j P_{k-j} + (-1)^k k s_k \in K[X_1, ...X_n]$$

Es ist leicht nachzurechnen, daß $\deg F \leq k < n$ ist. Für $i < k$ setzen wir $(X_1, ..., X_{n-1}, 0)$ zunächst in die s_i, P_i ein:

$$\begin{aligned} s_i(X_1, ..., X_{n-1}, 0) &= \sum_{1 \leq j_1 < ... < j_i \leq n-1} X_{j_1} \cdots X_{j_i} = s_i^{[n-1]} \in \Sigma^{[n-1]}(K) \\ P_i(X_1, ..., X_{n-1}, 0) &= \quad X_1^i + ... + X_{n-1}^i \quad = P_i^{[n-1]} \in \Sigma^{[n-1]}(K). \end{aligned}$$

Also erhalten wir bei Auswertung in F mit der Induktionsvoraussetzung:

$$F(X_1, ..., X_{n-1}, 0) = \sum_{j=0}^{k-1} (-1)^j s_j^{[n-1]} P_{k-j}^{[n-1]} + (-1)^k k s_k^{[n-1]} = 0,$$

woraus wir schließen können, daß F in $K[X_1, ..., X_n]$ von X_n geteilt wird. Da F offensichtlich symmetrisch ist, wird F sogar von allen X_j geteilt. Nun sind aber die verschiedenen X_j im faktoriellen Ring $K[X_1, ..., X_n]$ irreduzibel und paarweise nichtassoziiert, was dazu führt, daß F auch vom Produkt $X_1 \cdots X_n$ geteilt wird. Damit ist entweder $F = 0$ oder $\deg F \geq n$. Wir hatten letzteres aber schon am Anfang dieses Falles ausschliessen können.

Falls $k = n$, betrachten wir folgendes normiertes Polynom h in einer Unbestimmten T über $\Sigma^{[n]}(K)$:

$$h(T) := (T - X_1) \cdots (T - X_n) = \sum_{j=0}^{n-1} (-1)^j s_j T^{n-j} + (-1)^n s_n$$

Die X_i sind die Nullstellen dieses Polynoms, also gilt

$$h(X_i) = 0 = \sum_{j=0}^{n-1} (-1)^j s_j X_i^{n-j} + (-1)^n s_n$$

für $i = 1, ..., n$. Durch Aufsummieren dieser n Gleichungen, erhalten wir die Newtonrelation im Fall $k = n$:

$$0 = \sum_{j=0}^{n-1} (-1)^j s_j P_{n-j} + (-1)^n n s_n.$$

Da ja $\operatorname{char} K = 0$ oder $\operatorname{char} K > n$ ist, können wir die Newtonrelationen für jedes $1 \leq k \leq n$ nach s_k auflösen,

$$s_k = \frac{1}{k} \sum_{j=0}^{k-1} (-1)^{j+k-1} s_j P_{k-j},$$

und erhalten iterativ eine Darstellung der s_k als Polynom in den P_j. Dies ist möglich, da im Term für s_k nur s_j mit $j \leq k-1$ auftauchen, und $s_1 = P_1$ ist. $\square$

Im Folgenden verwenden wir die abkürzende Schreibweise $X = (X_1, ..., X_n)$ und $T = (T_1, ..., T_n)$.

Korollar 1.2.8. *Sei $f \in \Sigma^{[n]}(K)$ mit $\deg f \leq d$. Sei $\bar{d} := min\{n, d\}$, dann gibt es Polynome $g_1, g_{\lfloor \frac{d}{2} \rfloor + 1}, ..., g_{\bar{d}}$, so daß*

$$f = g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{\bar{d}} g_i(P_1, ..., P_{d-i}) P_i \tag{1.1}$$

geschrieben werden kann.

Beweis. Mit dem letzten Satz wissen wir, daß $f = g(P_1, ..., P_n)$ ist, für ein Polynom

$$g = \sum_{\mu \in \mathbb{N}_0^n} \alpha_\mu T_1^{\mu_1} \cdots T_n^{\mu_n} \in K[T_1, ..., T_n].$$

Es sei $\mathcal{M}(g) := \left\{ \alpha_\mu T_1^{\mu_1} \cdots T_n^{\mu_n} \mid \alpha_\mu \neq 0 \right\}$ die Menge aller in g vorkommenden Monome. Wir zeigen

$$m := \max\left\{ \deg_{T_1} M + 2 \deg_{T_2} M + ... + n \deg_{T_n} M \mid M \in \mathcal{M}(g) \right\} \stackrel{!}{=} \deg f. \tag{1.2}$$

Seien also $M_1, ..., M_r \in \mathcal{M}(g)$ diejenigen Monome, für die der Ausdruck

$$\deg_{T_1} M_i + 2 \deg_{T_2} M_i + ... + n \deg_{T_n} M_i$$

das Maximum m annimmt. Wir schreiben $g = M_1 + ... + M_r + h$, wobei h die Summe über die restlichen in g vorkommenden Monome ist.

Es ist $\deg_X h(P_1, ..., P_n) < m$, da dies ja nach Wahl von h bereits für jedes in h vorkommende Monom gilt. Da die P_j algebraisch unabhängig sind, gilt $(M_1 + ... + M_r)(P_1, ..., P_n) \neq 0$. Die M_i waren so gewählt, daß jedes $M_i(P_1, ..., P_n)$ homogen vom Grad m ist, also ist auch

$$\deg_X(M_1(P_1, ..., P_n) + ... + M_r(P_1, ..., P_n)) = m,$$

und somit $m = \deg_X g(P_1, ..., P_n) = \deg_X f \leq d$.

Wir wissen nun, daß in jedem Monom M von g die Unbestimmte T_i höchstens in erster Potenz vorkommen kann, falls $i > \lfloor \frac{d}{2} \rfloor$. Außer T_i können in einem solchen Monom nur Unbestimmte T_l vorkommen, für die $l + i \leq d$, also $l \leq d - i$. Sortieren wir nun die Monome von g nach dem höchsten vorkommenden Index i der Unbestimmten T_i, so erhalten wir die Darstellung (1.1). $\square$

2. Positivität teilsymmetrischer Polynome

2.1 Spezielle Testmengen für symmetrische Polynome

2.1.1 Der Satz von Timofte

Satz 2.1.1 (Timofte). *Sei R ein reell angeschlossener Körper, sei $f \in \Sigma^{[n]}(R)$ mit* $\deg f = d$. *Sei* $A := \{x \in R^n \mid \#\{x_1, ..., x_n\} \leq \max\{\frac{d}{2}, 2\}\}$. *Dann gilt*

$$f(x) \overset{(\geq)}{>} 0 \textit{ für alle } x \in R^n \Leftrightarrow f(x) \overset{(\geq)}{>} 0 \textit{ für alle } x \in A \tag{2.1}$$

Den Beweis des Satzes werden wir nur für $R = \mathbb{R}$ führen, werden jedoch im Anschluß sehen, wie man mit Hilfe *modelltheoretischer* Methoden die Aussage auf jeden reell abgeschlossenen Körper übertragen kann.

Im Beweis werden Sphären (Fasern der potenzsymmetrischen Funktion vom Grad 2) aus dem $\mathbb{R}^n$ betrachtet, und die Aussage '*f nimmt das Minimum auf einer Sphäre auch in einem Punkt an, der weniger als* $\max\{\frac{d}{2}, 2\}$ *verschiedene Komponenteneinträge hat*' gezeigt. Um das zu zeigen, konstruiert man mit Hilfe passend gewählter Differentialgleichungen zu jedem Punkt ξ einer Sphäre, für den $f(\xi)$ minimal unter allen Punkten der Sphäre ist, eine parametrisierte Kurve auf der Sphäre, auf welcher f konstant ist, und deren Endpunkt höchstens $\max\{\lfloor\frac{d}{2}\rfloor, 2\}$ verschiedene Komponenten hat. Damit ist dann gezeigt, daß das

Minimum von f auf dieser Sphäre auch in A angenommen wird. Da sich der $\mathbb{R}^n$ durch Sphären überdecken lässt, zeigt dies dann insbesondere den Satz.

Existenz komponentenreduzierender Kurven

Wir wollen hier ein grundlegendes technisches Lemma beweisen, mit welchem wir dann die Existenz besagter Verbindungskurven zeigen können. Wir werden für letzteres die Darstellbarkeit eines symmetrischen Polynoms f in den Potenzsymmetrischen Funktionen verwenden (Korollar 1.2.8). Im folgenden Lemma 'konstruieren' wir zu einem gegebenen Punkt $\xi \in \mathbb{R}^m$ mit s verschiedenen Komponenteneinträgen eine Verbindungskurve zu einem Punkt ξ' mit weniger als s verschiedenen Komponenteneinträgen, welche zudem noch insbesondere die Eigenschaft hat, in den Fasern $P_i = P_i(\xi)$ der potenzsymmetrischen Funktionen für $1 \leq i \leq s-1$ zu verlaufen. Dies garantiert dann nicht nur, daß für $s > 3$ die Kurve in einer Sphäre verläuft (Faser von P_2), sondern zeigt bereits eine abgeschwächte Version des Satzes von Timofte (mit d statt $\frac{d}{2}$). Denn nach Korollar 1.2.8 benötigt man zur Darstellung des symmetrischen Polynoms f mit $\deg f = d$ höchstens die Potenzsymmetrischen Funktionen $P_1, ..., P_d$. Man kann also einen Punkt ξ mit $s \geq d+1$ verschiedenen Komponenteneinträgen iterativ innerhalb einer Faser von f mit einem Punkt mit weniger oder gleich d verschiedenen Komponenteneinträgen verbinden. Also wird jeder mögliche Wert, den f *irgendwo* annimmt bereits in einem Punkt mit weniger oder gleich d verschiedenen Komponenteneinträge angenommen, insbesondere läßt sich die Nichtnegativität von f auf all diesen Punkten testen.

Definition 2.1.2. Sei $D \subset \mathbb{R}^n$. Dann heißt

$$\mathcal{F} : D \longrightarrow \mathbb{R}^m$$

lokal Lipschitzstetig, falls es zu jedem $y \in D$ eine Umgebung U von y und eine positive Konstante L gibt, sodaß

$$\|\mathcal{F}(x) - \mathcal{F}(y)\| \leq L\|x - y\|,$$

für alle $x \in U$.

Satz 2.1.3. *(Picard-Lindelöf) Sei $D \subset \mathbb{R}^n$ offen. Sei $\mathcal{F} : D \longrightarrow R^n$ eine lokal Lipschitzstetige Funktion. Dann gibt ein offenes Intervall I mit $t_0 \in I$ und eine Lösung $u : I \to D$ des Anfangswertproblems*

$$\begin{aligned} u'(t) &= \mathcal{F}(u(t)) \\ u(t_0) &= u_0, \end{aligned}$$

welche auf kein offenes Intervall $\tilde{I} \supset I$ fortgesetzt werden kann, und welche zudem auf jedem Teilintervall $J \subset I$ mit $t_0 \in J$ eindeutig ist.

Siehe dazu [AE, Seite 242 ff].

Proposition 2.1.4. *Seien $a < b \in \mathbb{R}$. Sei $\psi : [a, b] \longrightarrow \mathbb{R}^m$ eine stetige Funktion, stetig differenizierbar auf (a, b). Sei weiter ψ' stetig fortsetzbar auf $[a, b)$, dann existiert die rechtsseitige Ableitung von ψ an der Stelle a und stimmt mit der Fortsetzung von ψ' an der Stelle a überein.*

Beweis. Wir betrachten für $1 \leq j \leq m$ jede Komponentenfunktion ψ_j gesondert. Wähle eine positive Folge (h_n), die gegen 0 konvergiert. Zu jedem n wählen wir ein $\varepsilon_n > 0$, so daß

$$\varepsilon_n < \frac{h_n}{n} \text{ und } |\psi_j(a + \varepsilon_n) - \psi_j(a)| < \frac{h_n}{n}$$

Mit Hilfe des *Mittelwertsatzes* finden wir zu jedem n ein $t_n \in (a + \varepsilon_n, a + h_n)$, so daß

$$\begin{aligned} \frac{\psi_j(a + h_n) - \psi_j(a)}{h_n} &= \frac{\psi_j(a + h_n) - \psi_j(a + \varepsilon_n)}{h_n} + \frac{\psi_j(a + \varepsilon_n) - \psi_j(a)}{h_n} \\ &= \frac{h_n - \varepsilon_n}{h_n} \psi_j'(t_n) + \frac{\psi_j(a + \varepsilon_n) - \psi_j(a)}{h_n}. \end{aligned}$$

Offensichtlich konvergiert t_n gegen a und $\frac{h_n - \varepsilon_n}{h_n}$ gegen 1 und $\frac{\psi_j(a+\varepsilon_n) - \psi_j(a)}{h_n}$ konvergiert gegen 0. $\square$

Lemma 2.1.5. *Sei $m \in \mathbb{N}$, $\xi \in \mathbb{R}^m$ mit $\#\{\xi_1, ..., \xi_m\} =: s \geq 3$. Dann gibt es $a < b \in \mathbb{R}$, sowie eine stetig differenzierbare Abbildung $\varphi : [a, b] \longrightarrow \mathbb{R}^m$, die folgende Eigenschaften erfüllt:*

(i) Es ist $t_0 := P_s(\xi) \in (a,b)$ *und* $\varphi(t_0) = \xi$.

(ii) für $i = 1, ..., s-1$ *ist* $P_i \circ \varphi$ *konstant und* $P_s \circ \varphi = \mathrm{id}_{[a,b]}$.

(iii) $\#\{\varphi_1(a), ..., \varphi_m(a)\} < s$ *und* $\#\{\varphi_1(b), ..., \varphi_m(b)\} < s$.

(iv) Falls $s = m$, *so ist* $(P_k \circ \varphi)'$ *konstant für* $k = m, ..., 2m-1$.

(v) Die $\varphi_1, ..., \varphi_m$ *sind streng monotone Funktionen.*

Beweis. Da Koordinatenvertauschung eine lineare und damit C^∞-Abbildung auf dem $\mathbb{R}^m$ ist, und die P_k darunter invariant sind, genügt es das Lemma für solche ξ zu zeigen, für die

$$\xi = (\underbrace{\zeta_1, ..., \zeta_1}_{m_1\text{-mal}}, ..., \underbrace{\zeta_s, ..., \zeta_s}_{m_s\text{-mal}}) \text{ mit } \zeta_1 < ... < \zeta_s$$

gilt. Setzen wir nun $\zeta := (\zeta_1, ..., \zeta_s) \in \mathbb{R}^s$ und definieren auf der offenen Menge $D := \{z \in \mathbb{R}^s \mid z_1 < ... < z_s\}$ im $\mathbb{R}^s$ die stetig differenzierbare Funktion

$$\begin{array}{rcl} \mathcal{F} : D & \longrightarrow & \mathbb{R}^s \\ z & \mapsto & \big(\mathcal{F}_1(z), ..., \mathcal{F}_s(z)\big) \end{array}$$

$$\text{mit } \mathcal{F}_j(z) := \frac{1}{m_j s} \prod_{k \neq j} \frac{1}{z_j - z_k} \text{ für } 1 \leq j \leq s$$

und betrachten für $t_0 := P_s(\xi)$ das folgende *Anfangswertproblem*:

$$\begin{array}{rcl} u(t_0) & = & \zeta \in D \\ u'(t) & = & \mathcal{F}(u(t)) \end{array} \tag{2.2}$$

Wegen $\mathcal{F} \in C^1(D)$, ist $\mathcal{F}'$ auf jeder kompakten Teilmenge K von D beschränkt, und daher ist $\mathcal{F}$ lokal *Lipschitzstetig* auf D, denn es gibt um jedes $x \in D$ eine beschränkte Umgebung $U_x \subset D$ mit $\overline{U_x} \subset D$ und somit ein $L = \sup_{\xi \in U_x} \|\mathcal{F}'(\xi)\| \in \mathbb{R}$, so daß

$$\|\mathcal{F}(x) - \mathcal{F}(y)\| \leq L\|x-y\| \text{ für alle } y \in U_x$$

ist. Also gibt es mit *Picard-Lindelöf* 2.1.3 ein maximales Lösungsintervall I und eine Lösung

$$\psi : I \longrightarrow D$$

des Anfangswertproblems, welche sogar auf jedem offenen Teilintervall von I eindeutig ist. Aus dieser Lösung konstruieren wir nun eine Kurve im $\mathbb{R}^m$:

$$\begin{array}{rcl} \varphi : I & \longrightarrow & \mathbb{R}^m \\ t & \mapsto & (\underbrace{\psi_1(t), ..., \psi_1(t)}_{m_1\text{-mal}}, ..., \underbrace{\psi_s(t), ..., \psi_s(t)}_{m_s\text{-mal}}) \end{array}$$

Die stetige Differenzierbarkeit von ψ überträgt sich natürlich auf φ. Da ψ der Differentialgleichung des Anfangswertproblems (2.2) genügt, ist

$$\psi_l'(t) = \frac{1}{n_l} \prod_{k \neq l} \frac{1}{\psi_l - \psi_k} \neq 0 \text{ für } 1 \leq l \leq s,$$

also sind die φ_j streng monotone Funktionen. Dies zeigt bereits den Punkt (v).

Um die anderen im Lemma behaupteten Eigenschaften zu zeigen, ist es nützlich, sich noch eine weitere Differentialgleichung anzuschauen, die von ψ gelöst wird:

$$\underbrace{\begin{pmatrix} m_1 & m_2 & \cdots & m_s \\ m_1\psi_1 & m_2\psi_2 & \cdots & m_s\psi_s \\ \vdots & \vdots & \ddots & \vdots \\ m_1\psi_1^{s-2} & m_2\psi_2^{s-2} & \cdots & m_s\psi_s^{s-2} \\ m_1\psi_1^{s-1} & m_2\psi_2^{s-1} & \cdots & m_s\psi_s^{s-1} \end{pmatrix}}_{=:A} \begin{pmatrix} \psi_1' \\ \psi_2' \\ \vdots \\ \psi_{s-1}' \\ \psi_s' \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \frac{1}{s} \end{pmatrix}}_{=:b} \tag{2.3}$$

Um zu sehen, daß ψ tatsächlich diese Differentialgleichung (2.3) löst, ersetzen wir einfach den Ausdruck $\psi'(t)$ durch $\mathcal{F}(\psi(t))$ aus (2.2), und zeigen, daß dies punktweise, das heißt für jedes $t \in I$ mit der Lösung x des linearen Gleichungssytems

$$A(t) \cdot x = b$$

übereinstimmt. Die i-te Komponente der Lösung erhält man mit der *Cramer-*

schen Regel:

$$
\begin{aligned}
x_i(t) &= \frac{\det\big(A^{(1)}(t),...,A^{(i-1)}(t),b,A^{(i+1)}(t),...,A^{(s)}(t)\big)}{\det A(t)} \\
&= (-1)^i \frac{\frac{1}{s}\begin{vmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 \\ \psi_1(t) & \cdots & \psi_{i-1}(t) & \psi_{i+1}(t) & \cdots & \psi_s(t) \\ \vdots & . & \vdots & \vdots & . & \vdots \\ \psi_1(t)^{s-2} & \cdots & \psi_{i-1}(t)^{s-2} & \psi_{i+1}(t)^{s-2} & \cdots & \psi_s(t)^{s-2} \end{vmatrix}}{m_i \begin{vmatrix} 1 & \cdots & 1 \\ \psi_1(t) & \cdots & \psi_s(t) \\ \vdots & . & \vdots \\ \psi_1(t)^{s-1} & \cdots & \psi_s(t)^{s-1} \end{vmatrix}} \\
&= (-1)^i \frac{\prod\limits_{l,k\neq i;l>k}(\psi_l-\psi_k)}{m_i s \prod\limits_{l>k}(\psi_l-\psi_k)} \\
&= \frac{1}{m_i s \prod_{k\neq i}\psi_i-\psi_k} \\
&\overset{(2.2)}{=} \psi_i'
\end{aligned}
$$

Mit (2.3) folgt nun Punkt (ii) des Lemmas recht schnell:

$$
\begin{aligned}
(P_i\circ\varphi)' &= i\big(m_1\psi_1^{i-1}+...+m_s\psi_s^{i-1}\big) \overset{(2.3)}{=} 0 \text{ für } 1\leq i\leq s-1 \\
(P_s\circ\varphi)' &= s\big(m_1\psi_1^{s-1}+...+m_s\psi_s^{s-1}\big) \overset{(2.3)}{=} 1
\end{aligned}
$$

Folglich ist $(P_i\circ\varphi)(t)$ konstant für $1\leq i\leq s-1$, und $(P_s\circ\varphi)(t)=t$, da $(P_s\circ\varphi)(t_0)=P_s(\xi)=t_0$.

Wir müssen noch zeigen, daß das Lösungsintervall I beschränkt ist. Wir können jedes $t\in I$ nun wie folgt durch eine Konstante abschätzen (wegen $s>2$ und (ii)):

$$
\begin{aligned}
|t| &= |P_s(\varphi(t))| = |\varphi_1(t)^s+...+\varphi_n(t)^s| \\
&\leq |\varphi_1(t)|^s+...+|\varphi_n(t)|^s = \big(\varphi_1(t)^2\big)^{\frac{s}{2}}+...+\big(\varphi_s(t)^2\big)^{\frac{s}{2}} \\
&\leq s\big(\varphi_1^2(t)+...+\varphi_s^2(t)\big)^{\frac{s}{2}} = s\big((P_2\circ\varphi)(t)\big)^{\frac{s}{2}} = sP_2(\xi)^{\frac{s}{2}}
\end{aligned}
$$

Also ist $I = (a, b)$ für gewisse $a < t_0 < b$.

Die ψ_j sind strikt monoton (mit Punkt(v)) und auf (a, b) beschränkt, da

$$\psi_j^2 \leq \sum_{i=1}^{s} n_i \psi_i^2 = P_2 \circ \varphi = P_2(\xi) \quad (s > 2).$$

Diese beiden Eigenschafte erlauben uns ψ stetig auf $[a, b]$ fortzusetzen.

(iii): Es ist sicherlich

$$\#\{\varphi_1(t), ..., \varphi_m(t)\} = \#\{\psi_1(t), ..., \psi_s(t)\} \leq s$$

für alle $t \in [a, b]$.

Angenommen $\#\{\psi_1(a), ..., \psi_s(a)\} = s$, das heißt $\psi(a) \in D$. Dann gibt es wegen der Differentialgleichung (2.2) eine stetige Fortsetzung von ψ' auf $[a, b)$. Die rechtsseitige Ableitung von ψ an der Stelle a ist gleich der Fortsetzung von ψ' an der Stelle a mit Proposition (2.1.4). Betrachten wir nun das modifizierte Anfangswertproblem (vgl. (2.2))

$$\begin{aligned} u(a) &= \psi(a) \\ u'(t) &= \mathcal{F}(u(t)). \end{aligned}$$

Wir finden wiederum mit *Picard-Lindelöf* 2.1.3 ein maximales Lösungsintervall J und eine Lösung χ auf J. Da aber die rechtsseitige Ableitung von ψ und die stetige Fortsetzung von ψ' an der Stelle a übereinstimmen, können wir eine Lösung des ursprünglichen Angfangswertproblems (2.2) auf $J \cup (a, b)$ konstruieren:

$$u(t) := \begin{cases} \chi(t), & t \in J \setminus (a, b) \\ \psi(t), & t \in (a, b) \end{cases}$$

Die vorherigen Überlegungen zeigen, daß u stetig ist, und somit auch an der Stelle a sowohl die linksseitige als auch die rechtsseitige Ableitung der Differentialgleichung (2.2) genügen (und damit auch insbesondere übereinstimmen). Somit ist also u eine Lösung des urspünglichen Anfangswertproblems (2.2). Es ist aber $J \cup (a, b) \supsetneq (a, b)$, was der Maximalität von (a, b) als Lösungsintervall des ursprünglichen Anfangswertproblems widerspricht. Ergo ist $\#\{\psi_1(a), ..., \psi_s(a)\} < s$ und ganz analog zeigt man $\#\{\psi_1(b), ..., \psi_s(b)\} < s$.

(iv): Sei $s = m$, insbesondere $\psi = \varphi$. Für k mit $m \leq k \leq 2m-1$ gilt dann

$$P_k \circ \varphi = \sum_{j=1}^{m} \psi_j^k \text{ , also } \frac{1}{k}(P_k \circ \varphi)' = \sum_{j=1}^{m} \psi_j^{k-1} \psi_j'$$

Zusammen mit der Differentialgleichung (2.3) im Fall $s = m$, erhalten wir

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 0 \\ \psi_1 & \psi_2 & \cdots & \psi_m & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \psi_1^{m-2} & \psi_2^{m-2} & \cdots & \psi_m^{m-2} & 0 \\ \psi_1^{m-1} & \psi_2^{m-1} & \cdots & \psi_m^{m-1} & \frac{1}{m} \\ \psi_1^{k-1} & \psi_2^{k-1} & \cdots & \psi_m^{k-1} & \frac{1}{k}(P_k \circ \varphi)' \end{vmatrix} = 0,$$

da $(\psi_1', ..., \psi_m', -1)$ im Kern der Matrix aus obiger Determinante liegt. Durch Entwicklung dieser Determinante nach der letzten Spalte, erhalten wir:

$$\frac{1}{k}(P_k \circ \varphi)' \prod_{1 \leq i < j \leq m} (\psi_j - \psi_i) - \frac{1}{m} \underbrace{\begin{vmatrix} 1 & \cdots & 1 \\ \psi_1 & \cdots & \psi_m \\ \vdots & & \vdots \\ \psi_1^{m-2} & \cdots & \psi_m^{m-2} \\ \psi_1^{k-1} & \cdots & \psi_m^{k-1} \end{vmatrix}}_{=:D(\psi_1, ..., \psi_m)} = 0 \qquad (2.4)$$

Wir wollen zunächst zeigen, daß

$$D(\psi_1, ..., \psi_m) = g(\psi_1, ..., \psi_m) \prod_{1 \leq i < j \leq m} (\psi_j - \psi_i)$$

ist für ein $g \in \Sigma^{[m]}(\mathbb{R})$ mit $\deg g = k - m$. Indem wir in die Definition von D die Unbestimmten $T_1, ..., T_m$ an Stelle der $\psi_1, ..., \psi_m$ einsetzen, sehen wir, daß

$$D(\bar{T_1}, ..., \bar{T_m}) = \begin{vmatrix} 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\ \bar{T_1} & \cdots & \bar{T_{l_1}} & \cdots & \bar{T_{l_2}} & \cdots & \bar{T_m} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \bar{T_1}^{m-2} & \cdots & \bar{T_{l_1}}^{m-2} & \cdots & \bar{T_{l_2}}^{m-2} & \cdots & \bar{T_m}^{m-2} \\ \bar{T_1}^{k-1} & \cdots & \bar{T_{l_1}}^{k-1} & \cdots & \bar{T_{l_2}}^{k-1} & \cdots & \bar{T_m}^{k-1} \end{vmatrix} = \bar{0}$$

im Integritätsring $\mathbb{R}[T_1, ...T_m]/(T_{l_2} - T_{l_1})$ gilt, und zwar für beliebige $1 \leq l_1 < l_2 \leq m$, da ja die l_1-te Spalte mit der l_2-ten Spalte übereinstimmen.

Damit wissen wir, daß $D(T_1, ..., T_m)$ von $(T_{l_2} - T_{l_1})$ in $\mathbb{R}[T_1, ..., T_m]$ geteilt wird, und da die $(T_{l_2} - T_{l_1})$ für verschiedene $l_1 < l_2$ jeweils irreduzibel und paarweise nichtassoziiert im faktoriellen Ring $\mathbb{R}[T_1, ..., T_m]$ sind, folgt auch

$$\prod_{1 \leq i < j \leq m} (T_j - T_i) \text{ teilt } D(T_1, ..., T_m),$$

also ist

$$D(T_1, ..., T_m) = g \prod_{1 \leq i < j \leq m} (T_j - T_i)$$

für ein $g \in \mathbb{R}[T_1, ..., T_m]$.

Die Symmetrie von g ist relativ einfach zu sehen: Sei $\tau = (l_1, l_2) \in S_m$ eine beliebige Transposition. Wenn wir uns die Determinante in (2.4) betrachten, die D definiert hat, stellt man fest, daß

$$D(T_{\tau(1)}, ..., T_{\tau(m)}) = (-1)D(T_1, ..., T_m)$$

gelten muss, da das Transponieren der Unbestimmten einer Spaltenvertauschung in der Matrix der Determinante entspricht. Also erhalten wir

$$\begin{aligned}(-1)g(T_1, ..., T_m) \prod_{1 \leq i < j \leq m} (T_j - T_i) &= g(T_{\tau(1)}, ..., T_{\tau(m)}) \prod_{1 \leq i < j \leq m} (T_{\tau(j)} - T_{\tau(i)}) \\ &= g(T_{\tau(1)}, ..., T_{\tau(m)})(-1) \prod_{1 \leq i < j \leq m} (T_j - T_i),\end{aligned}$$

und daher $g(T_1, ..., T_m) = g(T_{\tau(1)}, ..., T_{\tau(m)})$, was die Symmetrie von g zeigt.

Mit der *Leibnitz'schen Regel* für Determinanten erhält man

$$\begin{aligned}\deg D(T_1, ..., T_m) &= (k-1) + (m-2) + ... + 1, \\ \deg \prod_{1 \leq i < j \leq m} (T_j - T_i) &= (m-1) + (m-2) + ... + 1\end{aligned}$$

und somit $\deg g(T_1, ...T_m) = k - m$. Mit Korollar (1.2.8) finden wir also ein Polynom $\tilde{g}$, so daß $g = \tilde{g}(P_1, ..., P_{k-m})$ ist.

Mit diesem Wissen erhalten wir aus (2.4)

$$\frac{m}{k}\big(P_k \circ \varphi\big)' \prod_{1\leq i<j\leq m} (\psi_j - \psi_i) = \tilde{g}\big(P_1(\varphi), ..., P_{k-m}(\varphi)\big) \prod_{1\leq i<j\leq m} (\psi_j - \psi_i),$$

und da

$$\prod_{1\leq i<j\leq m} (\psi_j(t) - \psi_i(t)) \neq 0$$

ist für alle $t \in I$, ist auch

$$(P_k \circ \varphi)' = \frac{k}{m}\tilde{g}(P_1, ..., P_{k-m}) \circ \varphi.$$

Nun ist $k - m < m$ und mit Punkt (iii) dieses Lemmas ist $P_i \circ \varphi$ konstant für jedes $i < s = m$. Damit ist dann auch $(P_k \circ \varphi)'$ konstant. □

Satz 2.1.6 (Zwischenergebnis). *Sei $f \in \Sigma^{[n]}(\mathbb{R})$ mit $\deg f = d$. Sei $a \in \mathbb{R}$ mit $a = f(y)$ für ein $y \in \mathbb{R}^n$. Dann gibt es ein $x \in \mathbb{R}^n$ mit $\#\{x_1, ..., x_n\} \leq d$ und $a = f(x)$.*

Beweis. Nach Korollar 1.2.8 kommen in der Darstellung von f in den potenzsymmetrischen Funktionen höchstens diejenigen bis zum Grad d vor $(P_1, ..., P_d)$. Falls nun $\#\{y_1, ..., y_n\} \geq d+1$ ist, dann gibt es nach dem letzten Lemma 2.1.5(ii) (für $m = n$) eine stetige, kompakte Kurvenparametrisierung φ im $\mathbb{R}^n$, für die $P_1 \circ \varphi, ..., P_d \circ \varphi$ konstant ist. Insbesondere ist dann $f \circ \varphi = a$ konstant. Die Kurve verbindet y mit eine Punkt y', für den $\#\{y'_1, ..., y'_n\} < \#\{y_1, ..., y_n\}$ ist. So kommen wir iterativ auf einen Punkt x mit der behaupteten Eigenschaft. □

Weitergehende Komponentenreduzierung bei sphärisch minimalwertigen Startpunkten

Definition 2.1.7. Zu $r \in \mathbb{R}_{>0}$, $f \in \mathbb{R}[X_1, ..., X_n]$ ist

$$rS^{n-1} := \{x \in \mathbb{R}^n \mid P_2(x) = r^2\}$$

die Sphäre vom Radius r um den Nullpunkt, wobei P_2 die potenzsymmetrische Funktion vom Grad 2 ist, und

$$M_{r,f} := \{x \in rS^{n-1} \mid f(x) \leq f(y) \text{ für alle } y \in rS^{n-1}\}$$

ist die Minimalvarietät von f auf der Sphäre rS^{n-1}.

Das vorige Lemma 2.1.5 bringt uns unserem Ziel schon entscheidend näher, es garantiert uns nämlich für einen beliebigen Punkt ξ mit $\|\xi\| = r$ und $\#\{\xi_1, ..., \xi_n\} = s > \max\{\frac{d}{2}, 2\}$ die Existenz einer stetigen, kompakten Kurvenparametrisierung φ auf der Sphäre rS^{n-1} (nach Lemma 2.1.5 (ii) ist $P_2 \circ \varphi$ konstant), deren Endpunkt *weniger* als s verschiedene Komponenteneinträge hat. Für $s > d$ ist ein symmetrisches Polynom f vom Grad d, wie gesehen, konstant auf der Kurve. Wir wollen nun zeigen, daß letzteres sogar im Fall $s > \max\{\frac{d}{2}, 2\}$ gilt, sofern $\xi \in M_{r,f}$ ist (für $r = \|\xi\|$).

Da ja $f \in \Sigma^{[n]}(\mathbb{R})$ ist, haben wir mit Korollar 1.2.8 eine Darstellung

$$f = g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{\bar{d}} g_i(P_1, ..., P_{d-i})P_i \tag{2.5}$$

mit den potenzsymmetrischen Funktionen P_j. Wegen $s > \frac{d}{2}$ folgt wiederum mit Lemma 2.1.5(ii) für die zugehörige Kurvenparametrisierung φ, daß

$$f \circ \varphi(t) = \underbrace{g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor})(\varphi(t))}_{\text{konstant}} + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{\bar{d}} \underbrace{g_i(P_1, ..., P_{d-i})(\varphi(t))}_{\text{konstant}} P_i(\varphi(t)).$$

Wir wollen ja zeigen, daß dies eine konstante Funktion in t ist. Um das zu erreichen, werden wir zeigen, daß die Koeffizienten

$$g_i(P_1, ..., P_{d-i})(\varphi(t)) = g_i(P_1, ..., P_{d-i})(\xi) = 0$$

sind, für alle i mit $\lfloor \frac{d}{2} \rfloor + 1 \leq i \leq \bar{d}$. Dies werden wir zunächst nur für solche $\xi \in M_{r,f}$ zeigen, die n verschiedene Komponenteneinträge haben:

Lemma 2.1.8. *Sei $d \in \mathbb{N}$ mit $3 < d < 2n$, sei*

$$f(X_1, ..., X_n) = g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{\bar{d}} g_i(P_1, ..., P_{d-i})P_i$$

für gewisse Polynome g_j in den potenzsymmetrischen Funktionen $P_l(X_1, ..., X_n)$ vom Grad l und $\bar{d} = \min\{n, d\}$. Sei $r \in \mathbb{R}_{>0}$ und $\eta \in M_{r,f}$ mit $\#\{\eta_1, ..., \eta_n\} = n$, dann ist

$$g_i(P_1, ..., P_{d-i})(\eta) = 0$$

für alle i mit $\lfloor \frac{d}{2} \rfloor + 1 \leq i \leq \bar{d}$.

Beweis. Dazu betrachten wir die folgende affine Abbildung

$$\begin{aligned}\mathcal{A}:\mathbb{R}^{\bar{d}-\lfloor\frac{d}{2}\rfloor} &\longrightarrow \mathbb{R}\\ (z_{\lfloor\frac{d}{2}\rfloor+1},...,z_{\bar{d}}) &\mapsto g_1(P_1,...,P_{\lfloor\frac{d}{2}\rfloor})(\eta)+\sum_{i=\lfloor\frac{d}{2}\rfloor+1}^{\bar{d}} g_i(P_1,...,P_{d-i})(\eta)z_i.\end{aligned}$$

Wir werden zeigen, daß $\mathcal{A}$ ein lokales Minimum an der Stelle

$$z:=(P_{\lfloor\frac{d}{2}\rfloor+1}(\eta),...,P_{\bar{d}}(\eta))$$

besitzt. Eine affine Abbildung, die ein lokales Minimum besitzt, ist aber konstant, woraus sofort die Behauptung folgt.

Wir zeigen zunächst, daß die (stetig differenzierbare) Abbildung

$$\begin{aligned}\mathcal{P}:\mathbb{R}^n &\longrightarrow \mathbb{R}^n\\ x &\mapsto \big(P_1(x),...,P_n(x)\big)\end{aligned}$$

im Punkt η lokal umkehrbar ist. Die Jacobi-Determinante an der Stelle η ist

$$\det\big(\partial_i P_j(\eta)\big)_{(1\le i,j\le n)}=\begin{vmatrix}1 & \cdots & 1\\ 2\eta_1 & \cdots & 2\eta_n\\ \vdots & & \vdots\\ n\eta_1^{n-1} & \cdots & n\eta_n^{n-1}\end{vmatrix}=n!\prod_{i<j}(\eta_j-\eta_i)\neq 0,$$

wonach mit dem Satz über *lokale Umkehrbarkeit* eine Umgebung U von η und eine Umgebung V von $(P_1(\eta),...,P_n(\eta))$ existieren, welche durch $\mathcal{P}$ bijektiv (sogar diffeomorph) ineinander überführt werden.

Sei $\varepsilon>0$ so, daß die offene Kugel $B(v,\varepsilon)$ mit Mittelpunkt

$$v:=\big(P_1(\eta),...,P_n(\eta)\big)$$

noch vollständig in V liegt. Sei $y\in\mathbb{R}^{\bar{d}-\lfloor\frac{d}{2}\rfloor}$ mit $\|y\|<\varepsilon$, dann ist

$$w:=\Big(v_1,...,v_{\lfloor\frac{d}{2}\rfloor},\ v_{\lfloor\frac{d}{2}\rfloor+1}+y_{\lfloor\frac{d}{2}\rfloor+1}\ ,...,\ v_{\bar{d}}+y_{\bar{d}}\ ,\ v_{\bar{d}+1},...,v_n\Big)\in V,$$

also gibt es ein $x\in U$ mit $\mathcal{P}(x)=w$. Da nach Voraussetzung $\frac{d}{2}\geq 2$ ist, gilt $P_2(x)=P_2(\eta)$, das heißt $x\in rS^{n-1}$. Dann gilt aber wegen $\eta\in M_{r,f}$

$$\mathcal{A}\big(P_{\lfloor\frac{d}{2}\rfloor+1}(\eta),...,P_{\bar{d}}(\eta)\big)=f(\eta)\le f(x)=\mathcal{A}\big(P_{\lfloor\frac{d}{2}\rfloor+1}(\eta)+y_{\lfloor\frac{d}{2}\rfloor+1},...,P_{\bar{d}}(\eta)+y_{\bar{d}}\big)$$

Somit hat die betrachtete affine Funktion also tatsächlich ein lokales Minimum an der Stelle $(P_{\lfloor \frac{d}{2} \rfloor+1}(\eta), ..., P_{\bar{d}}(\eta))$. □

Wenn wir nun noch zeigen, daß jeder Punkt $\xi \in M_{r,f}$ mit mehr als $\frac{d}{2}$ Komponenteneinträge durch Punkte, die n verschiedene Komponeneteneinträge haben *in* $M_{r,f}$ approximiert werden kann, so haben wir die Aussage des vorigen Lemmas auf ξ erweitert, und somit also nachgewiesen, daß die betrachtete Kurve, welche ξ mit einem Punkt mit geringerer Anzahl an Komponenteneinträgen verbindet, tatsächlich in $M_{r,f}$ verläuft. Diese Approximation wollen wir im Folgenden zeigen. Dazu werden wir abermals das Lemma 2.1.5 verwenden, wobei an dieser Stelle Punkt (i) und (v) des Lemmas eingehen wird.

Lemma 2.1.9. *Sei $d \in \mathbb{N}$ mit $3 < d < 2n$, sei $f \in \Sigma^{(n)}\mathbb{R}$ mit $\deg f \leq d$. Sei $r \in \mathbb{R}_{>0}$ und $\xi \in M_{r,f}$ mit $\#\{\xi_1, ..., \xi_n\} > \frac{d}{2}$. Dann gibt es eine gegen ξ konvergente Folge $(\eta^{(k)})_{k\in\mathbb{N}}$ in $M_{r,f}$ mit $\#\{\eta_1^{(k)}, ..., \eta_n^{(k)}\} = n$ für jedes $k \in \mathbb{N}$.*

Beweis. Sei also $\#\{\xi_1, ..., \xi_n\} = m > \frac{d}{2}$.

Falls $m = n$ ist, gibt es nichts zu zeigen. Andernfalls können wir ohne Einschränkung der Allgemeinheit davon ausgehen, daß $\xi = (\zeta_1, ..., \zeta_m, \rho)$ mit $\zeta_1 < ... < \zeta_m$. Dabei ist ρ die mit entsprechenden Vielfachheiten vorkommende Wiederholung der ersten m Einträge ζ_j. Dies ist wiederum auf Grund der Stetigkeit der Koordinatenvertauschung im $\mathbb{R}^n$ und der Invarianz von f bezüglich selbiger möglich.

Mit Lemma (2.1.5) erhalten wir zu $\zeta \in \mathbb{R}^m$ ein kompaktes Intervall $[a, b]$ und eine stetige Kurve

$$\varphi : [a, b] \longrightarrow \mathbb{R}^m$$

welche den Eigenschaften (i)-(v) des Lemmas genügen. Ausgehend davon konstruieren wir die stetige Kurve

$$\begin{array}{rcl} \psi : [a, b] & \longrightarrow & \mathbb{R}^n \\ t & \mapsto & (\varphi(t), \rho). \end{array}$$

Mit $t_0 := P_m^{[m]}(\zeta) \in (a, b)$ ist $\psi(t_0) = \xi$ (wegen Lemma 2.1.5 (i)), und für $1 \leq i \leq m - 1$ gilt

$$P_i \circ \psi = P_i^{[m]} \circ \varphi + P_i^{[n-m]}(\rho) = P_i^{[m]}(\zeta) + P_i^{[n-m]}(\rho) = P_i(\xi)$$

sowie

$$(P_m \circ \psi)(t) = P_m^{[m]} \circ \varphi + P_m^{[n-m]}(\rho) = t + P_m^{[n-m]}(\rho)$$

für alle $t \in [a,b]$ (wegen Punkt(ii) von Lemma 2.1.5). Insbesondere ist $P_2 \circ \psi$ konstant, was bedeutet, daß $\psi([a,b])$ auf der Sphäre rS^{n-1} liegt.

Mit Lemma 2.1.5 (iv) ist $P_i^{[m]} \circ \varphi$ eine affine Funktion für $m \leq i \leq 2m$, somit ist auch $P_i \circ \psi = P_i^{[m]} \circ \varphi + P_i^{[n-m]}(\rho)$ eine affine Funktion. Nach Punkt (ii) des selben Lemmas, ist $P_i \circ \psi$ für $1 \leq i < m$ sogar eine konstante Funktion, folglich ist

$$(f \circ \psi)(t) = \beta_1 + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{\bar{d}} \alpha_i t + \beta_i,$$

für einige Konstanten $\alpha_i, \beta_i \in \mathbb{R}$. Darum ist $(f \circ \psi)' = \sum_{i=\lfloor \frac{d}{2} \rfloor + 1} \alpha_i = c$ konstant. Dabei ist die Konstante

$$c = (f \circ \psi)'(t_0) = 0,$$

da $\psi(t_0) = \xi$ eine Minimalstelle von f auf der Sphäre rS^{n-1} ist, und da die Kurve $\psi([a,b])$ auf dieser Sphäre liegt, ist $t_0 \in (a,b)$ ein lokale Minimalstelle vom $f \circ \psi$, also $(f \circ \psi)'(t_0) = 0$.

Für f gibt es die Darstellung (2.5) in den potenzsymmetrischen Funktionen, dann wissen wir, daß $f \circ \psi$ eine *konstante* Funktion ist. Das Bild von ψ verläuft also auf der Sphäre rS^{n-1} und ist unter Auswertung in f konstant. Da ξ im Bild von ψ liegt ($\psi(t_0) = \xi$), ist also

$$\psi([a,b]) \subset M_{r,f}.$$

Es ist ja $\psi(t) = (\varphi_1(t), ..., \varphi_m(t), \rho)$. Mit Punkt (v) vom Lemma (2.1.5) sind alle φ_j strikt monotone Funktionen. Damit aber ist für jedes $t \in (a,b)$ mit $t \neq t_0$ und $|t - t_0|$ klein genug

$$\#\{\varphi_1(t), ..., \varphi_m(t), \rho\} = \#\{\psi_1(t), ..., \psi_m(t)\} + \#\{\rho_1, ..., \rho_{n-m}\} \geq m + 1.$$

Der Punkt $\tilde{\xi} = \#\{\varphi_1(t), ..., \varphi_m(t), \rho\} \in M_{r,f}$ hat also mindestens einen Komponenteneintrag mehr als das ursprüngliche ξ. Dabei konnte t genügend aber beliebig nahe an t_0 (jedoch ungleich t_0) gewählt werden. Da die Kurvenparametrisierung ψ stetig war, findet man einen solchen Punkt $\tilde{\xi}$ in jeder ε-Umgebung von ξ.

Ausgehend von $\tilde{\xi}$ müssen wir diesen Approximationsschritt höchstens $(n-\frac{d}{2})$-mal wiederholen, um einen Punkt $\eta \in M_{r,f}$ mit n verschiedenen Komponenteneinträgen in einer vorgegebenen ε-Umgebung von ξ zu erhalten. $\square$

Satz 2.1.10. *Sei $f \in \Sigma^{[n]}(\mathbb{R})$ mit $\deg f \leq d$ für $3 < d < 2n$. Sei $r \in \mathbb{R}^+$ und $\xi \in M_{r,f}$ mit $\#\{\xi_1, ..., \xi_n\} > \frac{d}{2}$. Dann gibt es ein kompaktes Intervall $[a, b] \subset \mathbb{R}$, sowie eine stetige Abbildung $\varphi : [a, b] \longrightarrow M_{r,f}$ mit $\varphi(t_0) = \xi$ für ein $t_0 \in (a, b)$, sowie $\#\{\varphi_1(a), ..., \varphi_n(a)\} < \#\{\xi_1, ..., \xi_n\}$*

Beweis. Sei $s := \#\{\xi_1, ..., \xi_n\}$. Lemma (2.1.5) liefert dann die gewünschte Kurve. Man setze $t_0 := P_s(\xi)$. Es ist nur noch zu zeigen, daß $\varphi([a, b]) \subset M_{r,f}$.

Mit Korollar 1.2.8 haben wir wieder die Darstellung

$$f(X_1, ..., X_n) = g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor+1}^{\bar{d}} g_i(P_1, ..., P_{d-i})P_i$$

für gewisse Polynome g_j und den potenzsymmetrischen Funktionen P_l. Mit Punkt (ii) von Lemma 2.1.5 ist

$$f \circ \varphi(t) = \underbrace{g_1(P_1, ..., P_{\lfloor \frac{d}{2} \rfloor})(\varphi(t))}_{\text{konstant}} + \sum_{i=\lfloor \frac{d}{2} \rfloor+1}^{\bar{d}} \underbrace{g_i(P_1, ..., P_{d-i})(\varphi(t))}_{\text{konstant}} P_i(\varphi(t)).$$

Es ist also

$$g_i(P_1, ..., P_{d-i})(\varphi(t)) = g_i(P_1, ..., P_{d-i})(\xi)$$

für $\lfloor \frac{d}{2} \rfloor + 1 \leq i \leq \bar{d}$. Mit dem Lemma 2.1.9 erhalten wir eine Folge $\eta^{[k]}$, die gegen ξ konvergiert, und für die $\#\{\eta_1^{(k)}, ..., \eta_n^{(k)}\} = n$ für jedes k ist.

Mit Lemma 2.1.8 ist dann $g_i(P_1, ..., P_{d-i})(\eta^{[k]}) = 0$ für jedes k, und aus Gründen der Stetigkeit dann auch $g_i(P_1, ..., P_{d-i})(\xi) = 0$. Es ist also $f \circ \varphi$ konstant, also ist $\varphi([a, b]) \subset M_{r,f}$. $\square$

Nun folgt der zentrale Satz dieses Kapitels als Korollar.

Korollar 2.1.11 (Satz von Timofte). *Sei $f \in \Sigma^{[n]}(\mathbb{R})$. Dann ist $f(x) \geq 0$ (bzw. $f(x) > 0$) für alle $x \in \mathbb{R}^n$ genau dann, wenn $f(x) \geq 0$ (bzw. $f(x) > 0$) ist für alle $x \in \mathbb{R}^n$ mit $\#\{x_1, ..., x_n\} \leq \max\{\frac{\deg f}{2}, 2\}$.*

Beweis. $'' \Rightarrow$ " : trivial

$'' \Leftarrow$ " : Sei also $f(x) \geq 0$ (bzw. $f(x) > 0$) für alle $x \in \mathbb{R}^n$ mit

$$\#\{x_1, ..., x_n\} \leq \max\{\frac{\deg f}{2}, 2\}.$$

Angenommen es gibt ein $x \in \mathbb{R}^n$ mit $f(x) < 0$ (bzw. $f(x) \leq 0$). Setze $r := \|x\|$. Sei $\xi \in M_{r,f}$, dann ist $f(\xi) \leq f(x) < 0$ (bzw.≤ 0). Setze $d := \max\{\deg f, 4\}$. Es ist dann $\#\{\xi_1, ..., \xi_n\} > \frac{d}{2}$. Mit dem Satz 2.1.10 gibt es dann ein $\tilde{\xi} \in M_{r,f}$ mit

$$\#\{\tilde{\xi}_1, ..., \tilde{\xi}_n\} < \#\{\xi_1, ..., \xi_n\}.$$

Entweder es ist dann bereits $\#\{\tilde{\xi}_1, ..., \tilde{\xi}_n\} \leq \frac{d}{2}$ und wir haben eine Widerspruch, oder man kann mit Satz 2.1.10 die Überlegung solange iterieren (höchstens n-mal), bis man ein $\tilde{\xi} \in M_{r,f}$ hat, mit $\#\{\tilde{\xi}_1, ..., \tilde{\xi}_n\} \leq \frac{d}{2}$ und erhält dann den Widerspruch. □

Man bemerke noch einmal, daß hier eigentlich noch etwas mehr gezeigt wurde, als im Korollar formuliert war. Nicht nur kann man die globale Nichtnegativität (Positivität) eines symmetrischen Polynoms f auf den Punkten mit weniger oder gleich $\max\{\frac{d}{2}, 2\}$ verschiedenen Komponenteneinträgen testen, sondern es kann eben auch die Nichtnegativität (Positivität) auf einer Sphäre auf eben all solchen Punkten, die *auf* der Sphäre liegen, getestet werden.

2.1.2 Übertragung des Resultats auf alle reell abgeschlossenen Körper

Im Beweis des Satzes gingen einige analytische Eigenschaften der reellen Zahlen ein, wie zum Beispiel Zusammenhangs- und Kompaktheitseigenschaften beschränkter und abgeschlossener Intervalle beim Satz von *Picard-Lindelöf* und der stetigen Fortsetzung der mit diesem Satz gewonnenen Kurven.

Im Allgemeinen gelten diese Eigenschaften nicht in reell abgeschlossenen Körpern. Deshalb wird es nicht möglich sein den Beweis zu verallgemeinern. Die Aussage selbst lässt sich jedoch in der formalen Sprache der angeordneten

Ringe formulieren, allerdings nur als Konjunktion unendlich vieler Aussagen in dieser Sprache. Dazu betrachten wir für jedes $d, n \in \mathbb{N}$ die Aussage:

'*Falls f ein symmetrisches Polynom über $\mathbb{R}$ in n Unbestimmten vom Grad $\leq d$ ist, und $f(x_1, ..., x_n) \geq 0$ ist für alle $x_1, ..., x_n \in \mathbb{R}$ mit $\#\{x_1, ..., x_n\} \leq \max\{\frac{d}{2}, 2\}$, so ist f nichtnegativ*'.

Wir zeigen, daß für jedes $d, n \in \mathbb{N}$ diese Aussage in der formalen Sprache der angeordneten Ringe formuliert werden kann: Ein Polynom f vom Grad $\leq d$ ist ein Term der Form

$$f = \sum_{\mu \in \mathbb{N}_0^n, |\mu| \leq d} \alpha_\mu X_1^{\mu_1} \cdots X_n^{\mu_n},$$

mit insgesamt $N := \binom{n+d}{d}$ Koeffizienten $\alpha_\mu \in R$. Die Tatsache, daß dieses Polynom symmetrisch ist, läßt sich durch eine Konjunktion sehr einfacher algebraischer Gleichheiten der Koeffizienten über $\mathbb{Z}$ codieren, nämlich einfach

$$\alpha_\mu - \alpha_\nu = 0,$$

für all diejenigen μ, ν, für die es eine Permutation $\sigma \in S_n$ gibt mit $\big(\mu_1, ..., \mu_n\big) = \big(\sigma(\nu_1), ..., \sigma(\nu_n)\big)$. Die Konjunktion dieser Gleichungen entspricht einer (quantorenfreien) Formel $\delta_1(\alpha_{\mu^1}, ..., \alpha_{\mu^N})$.

Auch die Tatsache,daß $\#\{x_1, ..., x_n\} \leq \max\{\frac{d}{2}, 2\}$ ist für gewisse $x_1, ..., x_n \in R$, läßt sich formal aufschreiben: Es gibt ja nur endlich viele Möglichkeiten dafür, daß $\#\{x_1, ..., x_n\} \leq g = \max\{\frac{d}{2}, 2\}$ ist. Jede dieser Möglichkeiten läßt sich wiederum als Konjunktion von (Polynom-)Gleichungen über $\mathbb{Z}$ hinschreiben, etwa $x_1 = ... = x_{m_1}$ und $x_{m_1+1} = ... = x_{m_2}$ und ... und $x_{m_{g-1}+1} = ... = x_n$. Die Disjunktion all dieser möglichen formalen Gleichungssyteme ist eine (quantorenfreie) Formel $\delta_2(x_1, ..., x_n)$.

Somit lautet also die Formulierung der eigentlichen Aussage für festes d und n in der Sprache der angeordneten Ringe:

$$\forall \alpha_{\mu^1}, ..., \forall \alpha_{\mu^N} \Bigg(\delta_1(\alpha_{\mu^1}, ..., \alpha_{\mu^N}) \rightarrow \Bigg(\forall y_1, ..., \forall y_n \Big(\sum_{i=1}^{N} \alpha_{\mu^i} y^{\mu^i} \geq 0 \Big) \vee \exists x_1, ..., \exists x_n \Big(\delta_2(x_1, ..., x_n) \wedge \sum_{i=1}^{N} \alpha_{\mu^i} x^{\mu^i} < 0 \Big) \Bigg) \Bigg). \tag{2.6}$$

Jede dieser Aussagen (d.h. für jedes feste d und n) gilt in den reellen Zahlen $\mathbb{R}$. Aufgrund der Vollständigkeit von der Theorie RCF (Satz 1.1.7) gilt jede dieser Aussagen also in *jedem* reell abgeschlossenen Körper R. Die Gesamtheit dieser unendlich vielen formalen Aussagen können wir nun wieder zu dem Satz von Timofte zusammenfassen, indem wir die formale Sprache wieder verlassen und eine Aussage über alle möglichen Polynome f treffen (also alle möglichen Anzahlen n an Unbestimmten und alle möglichen Grade des Polynoms).

Damit ist der Satz von Timofte 2.1 des Kapitels in seiner vollen Allgemeinheit gezeigt.

Bemerkung 2.1.12. Für festes $n \in \mathbb{N}$ und festes $d \in \mathbb{N}$ gilt ja, wie eben überlegt, die formale Aussage (2.6) in jedem reell abgeschlossenen Körper R, also in jedem Modell der Theorie der reell abgeschlossenen Körper. Mit *Gödels Vollständigkeitssatz* 1.1.1 folgt dann, daß diese Aussage schon in der Logik erster Stufe aus den Axiomen von RCF hergeleitet werden kann.
Leider kann diese Herleitung für jeden Fall n, d völlig anders aussehen, so daß es nicht unbedingt einen elementaren Beweis geben muß, der uniform für alle $n, d \in \mathbb{N}$ funktioniert.

2.2 Testmengen für teilsymmetrische Polynome

Es bezeichne immer R einen reell abgeschlossenen Körper.

Die Stärke des Satzes von Timofte ergibt sich, wie wir in der Anwendung sehen werden, daraus, daß die obere Schranke $\max\{\frac{d}{2}, 2\}$ für die Anzahl der verschiedenen Komponenteneinträge der Testpunkte im R^n, nur vom Grad d der zu testenden symmetrischen Polynomfunktion, und *nicht* von der Anzahl der Unbestimmten n abhängt. Timofte benutzt in seinem Beweis, wie gesehen, wesentliche analytische Eigenschaften der reellen Zahlen. In diesem Kapitel werden wir einen ganz anderen Weg gehen, um ähnliche Testmengen zu erhalten. Es wird sich dabei um Testmengen handeln, die für *jeden* Wert, der von einem symmetrischen Polynom f irgendwo angenommen wird, einen Punkt enthalten, auf dem f genau diesen Wert annimmt. Leider führt der hier gewählte Zugang zu einer schlechteren oberen Schranke für die Anzahl der verschiedenen Komponenteneinträge, als der von Timofte gewählte. Andererseits brauchen wir uns bei diesem Zugang nicht auf die symmetrischen Polynome beschränken, sondern erhalten entsprechend gute Resultate auch für Polynome die invariant unter gewissen Untergruppen der symmetrischen Gruppe sind (etwa invariant unter der alternierenden Gruppe A_n).

Wir werden die Fasern des Polynoms f einerseits unter geometrischen Gesichtspunkten (Symmetrie) untersuchen, andererseits unter Gesichtspunkten der semialgebraischen Topologie. Genauer gesagt werden wir mit Hilfe eines Resultats aus der reellen algebraischen Geometrie (Oleinik-Petrovski/Thom/Milnor - Schranke) die Anzahl der semialgebraischen Zusammenhangskomponenten einer Faser abschätzen und mit kombinatorischer Analyse der Geometrie der Faser schlußfolgern, daß diese einen nichtleeren Schnitt mit unserer Testmenge hat.

Zunächst aber soll an dieser Stelle eine kurze Einführung in die semialgebraische Topologie und Homologie gegeben werden, damit nachvollzogen werden kann, daß wir die aus der Literatur [BPR] entnommene Oleinik-Petrovski-

/Thom/Milnor-Schranke in unserem Kontext korrekt anwenden. Wem die hier gegebene Einführung nicht ausführlich genug erscheint, kann das alles sehr viel genauer in [BPR] nachlesen.

2.2.1 Semialgebraische Topologie

Definition 2.2.1. $M \subset R^n$ heißt *semialgebraische* Menge, falls es ein $m \in \mathbb{N}$, eine Formel $\delta(Y_1, ..., Y_m, X_1, ..., X_n)$ in der Sprache der angeordneten Ringe und gewisse $a_1, ..., a_m \in R$ gibt, so daß

$$M = \{x \in R^n \mid \delta(a_1, ..., a_m, x) \text{ gilt in } R\}.$$

Bemerkung 2.2.2. Semialgebraische Mengen sind genau die endlichen Kombinationen von Schnitten, Vereinigungen und Komplementbildungen von Mengen der Form

$$U(g) := \{x \in R^n \mid g(x) > 0\}$$

für Polynome $g \in R[X_1, ..., X_n]$. Dies ist eine Folgerung aus Satz 1.1.6 über die Quantorenelimination.

Algebraische Mengen sind insbesondere semialgebraische Mengen.

Definition 2.2.3. Seien $S \subset R^k$ und $T \subset R^l$ semialgebraische Mengen. Eine Abbildung

$$f : S \longrightarrow T$$

heißt *semialgebraisch*, falls der Graph $\{(x, f(x)) \mid x \in S\}$ semialgebraisch ist.

Bemerkung 2.2.4. Falls $f : A \longrightarrow B$ und $g : B \longrightarrow C$ semialgebraisch sind, so ist auch $g \circ f$ semialgebraisch.

Definition 2.2.5. Die *semialgebraische Topologie* des R^n ist diejenige Topologie, welche von den Mengen der Form $U(g)$ für ein Polynom $g \in R[X_1, ..., X_n]$ erzeugt wird.

Die semialgebraische Topologie von R ist die Intervalltopologie. Im Fall $R = \mathbb{R}$ ist dies gerade die übliche Topologie des $\mathbb{R}^n$.

Definition 2.2.6. Sei $M \subset R^n$ eine semialgebraische Menge. Diese heißt *semialgebraisch zusammenhängend*, falls es keine nichttriviale disjunkte Zerlegung $M = F_1 \dot{\cup} F_2$ in semialgebraische Mengen F_1, F_2 gibt, welche in M offen sind.

Falls eine semialgebraische Menge M zusammenhängend in der semialgebraischen Topologie ist, so ist sie insbesondere semialgebraisch zusammenhängend. Umgekehrt gilt das nicht. Man betrachte etwa $M = \mathbb{R}_{\text{alg}}$ in $R := \mathbb{R}_{\text{alg}}$, dem reellen Abschluß von $\mathbb{Q}$. M ist in der semialgebraischen Topologie nicht zusammenhängend. Betrachte dazu die in $\mathbb{R}$ offenen Intervalle $(-\infty, \pi), (\pi, \infty)$. Da $\mathbb{R}_{\text{alg}}$ dicht in $\mathbb{R}$ ist, lassen sich $M_1 := (-\infty, \Pi) \cap \mathbb{R}_{\text{alg}}$ und $M_2 := (\Pi, \infty) \cap \mathbb{R}_{\text{alg}}$ als unendliche Vereinigung offener Intervalle in $\mathbb{R}_{\text{alg}}$ schreiben. Also ist $\mathbb{R}_{\text{alg}} = M_1 \dot{\cup} M_2$ nicht zusammenhängend, jedoch sicherlich semialgebraisch zusammenhängend.

Definition 2.2.7. Eine semialgebraische Menge $M \subset R^n$ heißt *semialgebraisch wegzusammenhängend*, falls es zu je zwei $x, y \in M$ eine stetige semialgebraische Abbildung $\varphi : [0,1] \longrightarrow M$ vom inheitsintervall $[0,1] \subset R$ nach M gibt, mit $\varphi(0) = x$ und $\varphi(1) = y$.

Proposition 2.2.8. *Eine semialgebraische Menge ist semialgebraisch zusammenhängend genau dann, wenn sie semialgebraisch wegzusammenhängend ist.*

Beweis siehe [BPR, Seite 148].

Satz 2.2.9. *Jede semialgebraische Menge $S \subset R^n$ ist eindeutige disjunkte Vereinigung von endlich vielen semialgebraisch zusammenhängenden, in S offenen semialgebraischen Mengen $C_1, ..., C_l$.*

Diese $C_1, ..., C_l$ nennen wir die semialgebraischen Zusammenhangskomponenten von S. Für den Beweis siehe [BPR, Seite 147].

Proposition 2.2.10. *Das Bild einer semialgebraisch zusammenhängenden semialgebraischen Menge S unter einer semialgebraischen stetigen Abbildung ist semialgebraisch zusammenhängend. Insbesondere induziert ein semialgebraischer Homöomorphismus $F : S \longrightarrow S'$ eine Bijektion zwischen den semialgebraischen Zusammenhangskomponenten.*

Beweis. Angenommen $f(S)$ ist nicht semialgebraisch zusammenhängend für eine stetige semialgebraische Abbildung f. Es zerfalle etwa $f(S)$ nichttrivial in die beiden offenen semialgebraischen disjunkten Teilmengen U, V. Dann ist

$$f^{-1}(U)\dot{\cup}f^{-1}(V) = S,$$

wobei die Urbilder von U und V nichtleer, offen und semialgebraisch sind. (Letzteres folgt aus Anwendung des Projektionssatzes [Pr2, Theorem 2.1.5] für den Graphen von f.) Der zweite Teil der Behauptung folgt aus der Eindeutigen Zerlegbarkeit in semialgebraische Zusammenhangskomponenten (Proposition 2.2.10). $\square$

2.2.2 Semialgebraische Homologie und Bettizahlen

Wir wollen nun für eine beschränkte algebraische Menge eine obere Schranke für die Anzahl der semialgebraischen Zusammenhangskomponenten angeben. In der Literatur findet man eine obere Schranke für die Summe der Homologiedimensionen einer semialgebraischen abgeschlossenen und beschränkten Menge. Die zu diesen Mengen definierte semialgebraische Homologie verhält sich zur Kategorie der semialgebraischen abgeschlossenen Mengen mit den stetigen semialgebraischen Abbildungen ähnlich wie die übliche Homologie über $\mathbb{R}$ zur Kategorie der topologischen Räume mit den stetigen Abbildungen. Insbesondere entspricht die $\mathbb{Q}$-Dimension der nullten Homologiegruppe der Anzahl der semialgebraischen Zusammenhangskomponenten. Dies wollen wir nachvollziehen. Den Beweis für die obere Schranke für die Summe der Homologiedimensionen werden wir an dieser Stelle dann aber nicht mehr nachvollziehen, sondern auf die entsprechende Stelle in der Literatur verweisen.

Homologie simplizialer Komplexe

Definition 2.2.11. Seien $p \in \mathbb{N}_0$, $a_0, ..., a_p \in R^k$ so, daß sie nicht in einem gemeinsamen $p-1$ dimensionalen affinen Unterraum liegen, dann nennen wir die formale Folge $[a_0, ..., a_p]$ einen *geordneten* p-Simplex. Auf der Menge der geordneten Simplizes definieren wir die kleinste Äquivalenzrelation, für die

$$[a_0, ..., a_p] \sim [a_{\pi(0)}, ..., a_{\pi(p)}] \text{ ist für } \pi \in S_{p+1} \text{ mit } \operatorname{sgn}(\pi) = 1$$

Wir schreiben ab jetzt $[a_0, ..., a_p]$ für die zugehörigen Äquivalenzklassen. Diese nennen wir die *orientierten* p-Simplizes. Wir nennen den p-Simplex

$$|[a_0, ..., a_p]| := \{\lambda_0 a_0 + ... + \lambda_p a_p \mid \lambda_i \geq 0, \sum \lambda_i = 1\}$$

dann die Realisierung eines solchen orientierten Simplex.

Definition 2.2.12. Für $e \leq p$ nennen wir einen e-Simplex s eine *e-Seite* eines p-Simplex $|[a_0, ..., a_p]|$, falls $s = |[a_{i_1}, ..., a_{i_e}]|$ für gewisse $0 \leq i_1 < ... < i_e \leq p$.

Ein *simplizialer Komplex* K im R^k ist eine endliche Menge von Simplizes im R^k, so daß für $s, s' \in K$ gilt: Jede Seite von s ist in K und $s \cap s'$ ist leer oder eine Seite sowohl von s als auch von s'.

Wir nennen $|K| = \bigcup_{s \in K} s$ die Realisierung von K.

Man betrachte nun zunächst den von den orientierten p-Simplizes frei erzeugten $\mathbb{Q}$-Vektorraum V_p. Darin betrachten wir den Unterraum U_p, der von allen Elementen der Form

$$[a_0, ..., a_p] + [a_{\pi(0)}, ..., a_{\pi(p)}] \text{ für } \pi \in S_{p+1} \text{ mit } \operatorname{sgn}(\pi) = -1$$

erzeugt wird.

Definition 2.2.13. Sei K ein simplizialer Komplex. Wir nennen

$$C_p(K) := V_p / U_p$$

den $\mathbb{Q}$-Vektorraum der *p-Ketten* in K. Im Fall $p = -1$ ist es der Nullvektorraum (erzeugt von der leeren Menge).

Wir übernehmen abermals die Bezeichnung $[a_0, ..., a_p]$ diesmal für die zugehörige Restklasse der freien Erzeuger von V_p (welche dann Erzeuger von $C_p(K)$ sind).

Sei

$$\partial_p : C_p(K) \longrightarrow C_{p-1}(K)$$

derjenige $\mathbb{Q}$-Vektorraumhomomorphismus, der auf den erzeugenden orientierten Simplizes $[a_0, ..., a_p]$ wie folgt definiert ist:

$$\partial_p([a_0, ..., a_p]) = \sum_{0 \le i \le p} (-1)^i [a_0, ..., \hat{a}_i, ..., a_p].$$

Wir bezeichnen diesen als *p-Randabbildung* von K.

Dabei bedeutet $\hat{}$, daß die darunterliegende Komponente aus der Folge herausgestrichen wird. Die Abbildung ∂_p ist wohldefiniert.

Es gilt

$$[a_0, ..., a_p] = -[a_{\pi(0)}, ..., a_{\pi(p)}],$$

falls $\operatorname{sgn}(\pi) = -1$ ist. Anschaulich gesprochen hat man paarweise die orientierten p-Simplizes als 'gegengleich' orientierte Simplizes identifiziert. C_p ist also *frei* erzeugt von den orientierten p-Simplizes mit Vorzugsorientierung.

Bemerkung 2.2.14. Man rechnet nach, daß $\partial_p \circ \partial_{p+1} = 0$ gilt, also daß

$$\operatorname{im}(\partial_{p+1}) \subset \ker(\partial_p).$$

Definition 2.2.15. Für $p \in \mathbb{N}_0$ und einen simplizialen Komplex K, sei

$$H_p(K) := \ker(\partial_p) / \operatorname{im}(\partial_{p+1})$$

die p-te Homologiegruppe von K

simpliziale Homologie von beschränkten abgeschlossenen semialgebraischen Mengen

Definition 2.2.16. Sei K ein simplizialer Komplex im R^k, sei S eine beschränkte und abgeschlossene semialgebraische Menge, dann nennen wir einen semialgebraischen Homöomorphismus

$$f : |K| \longrightarrow S$$

eine *Triangulation* von S. Falls die 0-Seiten (Eckpunkte) von K rational sind, sprechen wir von einer *rationalen Triangulation.*

Satz 2.2.17 (rationale Triangulation). *Sei $S \subset R^k$ abgeschlossen und beschränkt, dann hat S eine rationale Triangulation*

Dies ist ein Spezialfall von [BPR, Theorem 5.41].

Nachdem man Homologiegruppen für simpliziale Komplexe definiert hat, kann man mit einigem Aufwand (vgl. [BPR, Seiten 189/190]) zeigen, daß zwei simpliziale Komplexe L, K im R^k, deren 0-Seiten (Eckpunkte) rational sind und welche semialgebraisch homöomorph zueinander sind, isomorphe Homologiegruppen definieren.

Damit ist folgende Definition möglich:

Definition 2.2.18. Sei S eine abgeschlossene beschränkte semialgebraische Menge, $f : |K| \longrightarrow S$ eine rationale Triangulation von S, dann setze $H_p(S) := H_p(K)$ für $p \in \mathbb{N}_0$.

Die p-te *Bettizahl* von S ist $\beta_p := \dim_{\mathbb{Q}} H_p(S)$

Proposition 2.2.19. *Die nullte Bettizahl β_0 einer abgeschlossenen beschränkten semialgebraischen Menge S ist die Anzahl der semialgebraischen Zusammenhangskomponenten von S.*

Beweis. Sei $f : |K| \longrightarrow S$ eine rationale Triangulation von S. Mit Proposition 2.2.10 genügt es, die semialgebraischen Zusammenhangskomponenten von $|K|$ zu zählen. Man kann sich überlegen, daß die Realisierung eines simplizialen Komplexes genau dann semialgebraisch zusammenhängend ist, wenn die Realisierung seines simplizialen Teilkomplexes, welcher nur aus den 0-Seiten und 1-Seiten besteht, semialgebraisch wegzusammenhängend ist. Es genügt also die Wegzusammenhangskomponenten von $|K_1| \subset |K|$ zu untersuchen, wobei K_1 eben besagter simpliziale Teilkomplex von K ist.

Betrachte nun $H_0(K) = \ker(\partial_0)/\operatorname{im}(\partial_1)$. Es ist $\partial_0 = 0$, also $\ker(\partial_0) = C_0(K)$ der von den 0-Seiten (Eckpunkten) frei erzeugte $\mathbb{Q}$-Vektorraum. Seien $a_1, ..., a_m$ Vertreter für die 0-Seiten aus jeweils einer Zusammenhangskomponente von $|K_1|$.

Wir zeigen, daß die Restklassen dieser Vertreter eine Vektorraumbasis von $H_0(K)$ sind. Dazu zeigen wir zunächst, daß die Restklassen eines beliebigen Eckpunktes gleich der Restklasse des Vertreters aus der selben Zusammenhangskomponente ist. Seien etwa a und b aus der selben Zusammenhangskomponente. Dann gibt es eine Folge von 1-Seiten $[a, c_1], [c_1, c_2], ..., [c_m, b]$ in K_1. Betrachte $[a, c_1] + [c_1, c_2] + ... + [c_m, b] \in C_1(K)$. Es ist dann

$$[b] - [a] = \partial_1\big([a, c_1] + [c_1, c_2] + ... + [c_m, b]\big) \in \mathrm{im}(\partial_1),$$

also haben $[b]$ und $[a]$ die selbe Restklasse in $H_0(K)$. Damit sind also die Restklassen der Zusammenhangskomponentenvertreter $[a_1], ..., [a_m]$ ein Erzeugendensystem von $H_0(K)$. Wir überzeugen uns nun von der linearen Unabhängigkeit. Seien

$$\alpha_1[a_1] + ... + \alpha_m[a_m] = \partial_1\left(\sum \beta_i[c_i, d_i]\right) \in \mathrm{im}(\partial_1),$$

für gewisse $\alpha_j, \beta_i \in \mathbb{Q}$. Für die 1-Seiten $[c_i, d_i]$ gilt, daß c_i und d_i in der selben Zusammenhangskomponente liegen müssen. Dann kann man die von diesen 1-Seiten erzeugte Summe nach Zugehörigkeit zu den Zusammenhangskomponenten ordnen, und wir erhalten

$$\alpha_1[a_1] + ... + \alpha_m[a_m] = \partial_1\left(\sum_i \beta_i^{(1)}[c_i^{(1)}, d_i^{(1)}]\right) + ... + \partial_1\left(\sum_i \beta_i^{(m)}[c_i^{(m)}, d_i^{(m)}]\right).$$

Da die $a_1, ..., a_m$ alle aus verschiedenen Zusammenhangskomponenten sind, ist dann nach allfälliger Umnumerierung

$$\alpha_l[a_l] = \partial_1\left(\sum_i \beta_i^{(l)}[c_i^{(l)}, d_i^{(l)}]\right) = \sum_i \left(\beta_i^{(l)}[d_i^{(l)}] - \beta_i^{(l)}[c_i^{(l)}]\right)$$

für alle $1 \leq l \leq m$. Betrachte nun die $\mathbb{Q}$-lineare Abbildung, definiert auf der kanonischen Basis von $C_0(K)$

$$\begin{aligned} Z : \mathbb{C}_0(K) &\longrightarrow \mathbb{Q} \\ [a] &\mapsto 1. \end{aligned}$$

Es folgt $\alpha_l = Z\big(\alpha_l[a_l]\big) = \sum Z\big(\beta_i^{(l)}[d_i^{(l)}] - \beta_i^{(l)}[c_i^{(l)}]\big) = 0$ für alle $1 \leq l \leq m$, was die $\mathbb{Q}$-lineare Unabhängigkeit der Restklassen von $[a_1], ..., [a_m]$ zeigt. Also ist $\dim_{\mathbb{Q}} H_0(K) = m$ die Anzahl der semialgebraische Zusammenhangskomponenten. $\square$

Nach dieser kurzen Wiedergabe der Einführung in die semialgebraische Homolgie aus [BPR], können wir nun ein tiefliegendes Resultat über eine Schranke für die Summe der Bettizahlen einer beschränkten algebraischen Menge (insbesondere abgeschlossen und semialgebraisch) verwenden, um die Anzahl der semialgebraischen Zusammenhangskomponenten dieser Menge nach oben abzuschätzen:

Satz 2.2.20 (Oleinik-Petrovski/Thom/Milnor -Schranke). *Für die Bettizahlen $\beta_0, ..., \beta_k$ einer beschränkten algebraischen Varietät im R^k, die von Polynomen vom Grad kleiner oder gleich d definiert wird, gilt*

$$\sum_{i=0}^{k} \beta_i \leq d(2d-1)^{k-1}.$$

Dem Beweis dieses Satzes wird in [BPR] beinahe ein ganzes Unterkapitel (Seiten 220-225) gewidmet. Dabei wird die Aussage zunächst im Fall $R = \mathbb{R}$ gezeigt, unter Verwendung der sogenannten *Morse*-Theorie, welcher ihrerseits das gesamte vorangehende Unterkapitel (Seiten 201-220) gewidmet wird. Auf eine Wiedergabe des Beweises wird an dieser Stelle verzichtet.

Korollar 2.2.21. *Eine beschränkte algebraische Varietät im R^k, die von Polynomen vom Grad kleiner oder gleich d definiert wird, hat nicht mehr als $d(2d-1)^{k-1}$ semialbegraische Zusammenhangskomponenten.*

2.2.3 Testmengensatz für teilsymmetrische Polynome

Proposition 2.2.22. *Sei $M \subset R^n$ eine semialgebraisch zusammenhängende Menge. Seien $\xi, \eta \in M$. Seien $1 \leq i < j \leq n$ und $\xi_i < \xi_j$, sowie $\eta_i > \eta_j$, dann gibt es ein $\zeta \in M$ mit $\zeta_i = \zeta_j$*

Beweis. Angenommen, es gäbe kein solches $\zeta \in M$. Setze dann

$$F_1 := M \cap \{x \in R^n \mid x_i < x_j\}$$
$$F_2 := M \cap \{x \in R^n \mid x_j < x_i\}$$

Es ist dann $F_1 \cap F_2 = \emptyset$ und $F_1 \cup F_2 = M$. Man sieht leicht, daß F_1 und F_2 semialgebraische Mengen sind, die relativ M offen sind.
Zudem ist $F_1 \neq \emptyset$, sowie $F_2 \neq \emptyset$, da $\xi \in F_1$ und $\eta \in F_2$. Somit ist M nicht semialgebraisch zusammenhängend. Widerspruch. $\square$

Definition 2.2.23. Zu $x \in R^n$ heißt für passendes $m \in \mathbb{N}$ eine Partition $(I_1, ..., I_m)$ ($I_i = \emptyset$ möglich) von $\{1, ..., n\}$ *eine Partition von* x, falls für alle $i \in \{1, ..., m\}$ und alle $l, k \in I_i$ gilt $x_l = x_k$.

Behauptung 2.2.24. *Zu jedem $c, k, l \in \mathbb{N}$ gibt es ein $g \in \mathbb{N}$ mit*

$$\frac{g!}{l} \geq ck^{g-1}.$$

Für ein solches g ist $\frac{m!}{l} > ck^{m-1}$ für alle $m > g$.

Beweis. Die Existenz ist einfach. Den zweiten Teil der Aussage zeigen wir induktiv über m. Sei also die schwache Ungleichung erfüllt für ein $m \geq g$, dann folgt für $m+1$, daß $(m+1)m! > lck^{m-1}k$ ist, da $m \geq k$ (sonst $m! < k^{m-1}$). $\square$

Definition 2.2.25. Seien $f_1, ..., f_m \in R[X_1, ..., X_n]$, dann notiere $V(f_1, ..., f_m) \subset R^n$ die *reelle* algebraische Varietät, also die gemeisame reelle Nullstellenmenge der Polynome.

Das folgende Lemma besagt nichts anderes, als daß wir in einer nichtleeren Varietät eines H-teilsymmetrischen Polynoms einen Punkt finden, dessen Komponenten wir fast alle in lauter Paare zusammenfassen können, deren Einträge gleich sind, und das höchstens g viele Komponenten übrigbleiben, die man nicht derart "verkuppeln" kann. Dabei ist g eine von n unabhängige Konstante.

Lemma 2.2.26. *Sei $l \in \mathbb{N}$ und H eine teilsymmetrische Familie vom Index l. Sei $f \in \Sigma_H^{(n)}(R)$ mit $\deg f \leq d \geq 2$, sei $V(f) \neq \emptyset$. Sei $g \in \mathbb{N}$ mit $\frac{g!}{l} \geq d(2d-1)^{g-1}$. Dann gibt es ein $x \in V(f)$ und eine Partition $(I_1, ..., I_m)$ von x, so daß gilt:*

$$\#I_j \text{ ist ungerade für höchstens } g \text{ verschiedene } j \in \{1, ..., m\}.$$

Beweis. Angenommen es ist nicht so. Sei dann h minimal, so daß es ein $\xi \in V(f)$ und eine Partition $(I_1, ..., I_m)$ von ξ gibt, mit

$$\#I_j \text{ ungerade für genau } h \text{ verschiedene } j.$$

Nach Annahme gilt dann $h > g$. Wir können ohne Einschränkung annehmen, daß $\#I_j$ ungerade ist für $j = 1, ..., h$. Wähle für jedes $1 \leq j \leq h$ ein $i_j \in I_j$. Um nicht in einer Indexflut unterzugehen, nummerieren wir die Komponenten so um, daß $i_1 = 1, ..., i_h = h$ gewählt werden können. Es sind dann die $\xi_1, ..., \xi_h$ paarweise verschieden, da sonst die Teil-Partition $(I_1, ..., I_h)$ vergröbert werden könnte, was der Minimalität von h widerspräche. Ohne Einschränkung können wir wieder davon ausgehen, daß $\xi_1 < ... < \xi_h$ (sonst nummerieren wir anfangs passend um). Betrachte dann das Polynom vom Grad $\leq d$ in h Unbestimmten

$$\tilde{f}(X_1, ..., X_h),$$

welches dadurch entstehe, daß man für alle $i \notin \{1, ..., h\}$ in die i-te Unbestimmte X_i den Wert ξ_i einsetzen. Dieses Polynom ist wiederum H-teilsymmetrisch, wegen Eigenschaft (2) von Definition 1.2.1 der teilsymmetrischen Familie. Nun ist ja

$$y := (\xi_1, ..., \xi_h) \in V(\tilde{f}),$$

da $\tilde{f}(\xi_1, ..., \xi_h) = f(\xi) = 0$. Betrachte $P_2^{[h]} := X_1^2 + ... + X_h^2$. Setze $a := P_2^{[h]}(y)$ und $g := P_2^{[h]} - a$, dann liegt y sogar in der *beschränkten* algebraischen Menge $V(\tilde{f}, g)$, und auf Grund der H-Teilsymmetrie von $\tilde{f}$ und g, ist dann auch $y_\sigma := (\xi_{\sigma(1)}, ..., \xi_{\sigma(h)}) \in V(\tilde{f}, g)$, für jedes $\sigma \in H_h$. Da für $1 \leq i \leq h$ die ξ_i alle paarweise verschieden sind, sind die y_σ ebenso alle paarweise verschieden.

Nun zerfällt nach Korollar 2.2.21 die algebraische Varietät $V(\tilde{f}, g)$ in nicht mehr als $d(2d-1)^{h-1}$ semialgebraische Zusammenhangskomponenten. Nach Wahl von g gilt wegen Behauptung 2.2.24 die Ungleichung $\frac{h!}{l} > d(2d-1)^{h-1}$, und mit dem Schubfachprinzip folgt, daß zwei der mindestens $\frac{h!}{l}$ vielen Punkte von $\{y_\sigma \mid \sigma \in H_h\}$ in derselben semialgebraischen Zusammenhangskomponente liegen müssen. Etwa y_{σ_1} und y_{σ_2} liegen in der selben semialgebraischen Zusammenhangskomponente von $V(\tilde{f}, g)$. Es liegen dann auch y und y_τ in der selben

semialgebraischen Zusammenhangskomponente, für $\tau = \sigma_1 \circ \sigma_2^{-1}$. Finde nun Zahlen $l < k \in \{1, ..., h\}$ mit $\tau(l) > \tau(k)$ (einen solchen '*Fehlstand*' muss es geben, da $\tau \neq \mathrm{id}$). Aus $l < k$ folgt $y_l = \xi_l < \xi_k = y_k$, und aus $\tau(l) > \tau(k)$ folgt $(y_\tau)_l = \xi_{\tau(l)} > \xi_{\tau(k)} = (y_\tau)_k$. Nach Proposition 2.2.22 gibt es dann ein $\zeta \in R^h$ in dieser Zusammenhangskomponente von $V(\tilde{f}, g)$ mit $\zeta_l = \zeta_k$.
Setze $x_i := \xi_i$, falls $i \notin \{1, ..., h\}$, sowie $x_j := \zeta_j$ für $j = 1, ..., h$. Aus der ursprünglichen Partition von ξ konstruieren wir eine Partition von x, in welcher möglichst viele Partitionsmengen gerade Kardinalität haben. Dazu setzen wir

$$\begin{aligned} I'_j &:= I_j \setminus \{j\} \text{ für } 1 \leq j \leq h \\ I'_j &:= I_j \text{ für } h+1 \leq j \leq m \\ I'_{m+1} &:= \{l, k\} \\ I'_{m+1+j} &:= \begin{cases} \{j\} & \text{für } j \neq l, k \\ \emptyset & \text{sonst} \end{cases} \quad \text{für } 1 \leq j \leq h \end{aligned}$$

Man sieht, daß $(I'_1, ..., I'_{m+1+h})$ eine Partition von $x = (x_1, ..., x_n) \in V(f)$ ist. Ebenso sieht man, daß $\#I'_j$ gerade für $1 \leq j \leq m+1$ ist. Auch ist $\#I'_{m+1+k} = \#I'_{m+1+l} = 0$. Demnach gibt es also ein $x \in V(f)$ und eine Partition $(I'_1, ..., I'_{m'})$ von x, bei der höchstens $h-2$ verschiedene $\#I'_j$ ungerade sind. Widerspruch zur angenommenen Minimalität von h. $\square$

Definition 2.2.27. Für $g, n \in \mathbb{N}$ setze

$$A_g(n) := \left\{x \in R^n \mid \#\{x_1, ..., x_n\} \leq g \log_2(n)\right\}$$

Satz 2.2.28. *Sei $l \in \mathbb{N}$ und H eine teilsymmetrische Familie vom Index l. Sei $f \in \Sigma_H^{(n)}(R)$ mit $\deg f \leq d \geq 2$, sei $g \in \mathbb{N}$ mit $\frac{g!}{l} \geq d(2d-1)^{g-1}$, sei $V(f) \neq \emptyset$, dann ist $V(f) \cap A_g(n) \neq \emptyset$ für $n \geq 2$.*

Beweis. Wir beweisen die Behauptung durch Induktion über n. Im Fall $n = 2, 3$ ist die Aussage trivial, da $(2d-1) \geq 3$ und also $g \geq 3$. Sei nun $n > 3$ und gelte die Aussage für alle $n' < n$. Nach Lemma 2.2.26 gibt es ein $x \in V(f)$ und dazu eine Partition $(I'_1, ..., I'_{m'})$ von x, für welche nur weniger oder gleich g Stück der Partitionsmengen I'_j eine ungerade Kardinalität haben. Indem wir nötigenfalls *leere* Partitionsmengen entfernen, und die übrigen Partitionsmengen verfeinern, das heißt indem wir jedes I'_j zerteilen in möglichst viele Paarmengen (im ungeraden Fall bleibt eine Einsermenge übrig), erhalten wir also für ein passendes $g' \leq g$ eine Partition $(I_1, ..., I_m)$ von x, so daß $\#I_i = 1$ für $m - g' + 1 \leq i \leq m$ und $\#I_i = 2$ für $1 \leq i \leq m - g'$.

Wir setzen dann für diejenigen Unbestimmten X_i mit $i \in I_{m-g'+1} \cup ... \cup I_m$ den Wert x_i ein, und ersetzen diejenigen Unbestimmten X_i, für die $i \in I_j$ ist für ein $1 \leq j \leq m - g'$, durch die neue Unbestimmte Y_j. So erhalten wir ein neues Polynom

$$\tilde{f}(Y_1, ..., Y_{m-g'}).$$

Dieses Polynom ist wieder H-teilsymmetrisch, nach Wahl der Partition, da jede Permutation der Y_j einer Permutation der entsprechenden Partitionsmengen I_j entspricht, was aufgrund der gleichen Mächtigkeit derselben auf zwei 'disjunkte' Indexpermutationen im ursprünglichen Polynom f zurückgeführt werden kann (wegen Eigenschaft (2) der Definition 1.2.1 ist dies möglich). Wir setzen für $1 \leq j \leq m - g'$:

$$\tilde{x}_j := x_l \text{ für ein (und damit jedes) } l \in I_j$$

Dann ist $\tilde{x} \in V(\tilde{f})$, da $0 = f(x) = \tilde{f}(\tilde{x})$. Es ist $\tilde{n} := m - g' \leq \lfloor \frac{n}{2} \rfloor$. Nach Induktionsvoraussetzung, gibt es nun ein $\zeta \in A_g(m - g') \cap V(\tilde{f})$. Setze nun für $1 \leq l \leq n$

$$y_l := \begin{cases} \zeta_j, & \text{falls } l \in I_j \text{ für ein } 1 \leq j \leq m - g' \\ x_l, & \text{sonst} \end{cases}$$

Dann ist $y \in V(f)$ und

$$\#\{y_1, ..., y_n\} \leq g' + g \log_2(\lfloor \frac{n}{2} \rfloor) \leq g \log_2(2) + g \log_2(\lfloor \frac{n}{2} \rfloor) \leq g \log_2(n).$$

Damit ist $y \in A_g(n)$. □

Korollar 2.2.29. *Sei $l \in \mathbb{N}$ und H eine teilsymmetrische Familie vom Index l. Sei $n \geq 2$, $f \in \Sigma_H^{(n)}(R)$ mit $\deg f \leq d \geq 2$. Sei $g \in \mathbb{N}$ mit $\frac{g!}{l} \geq d(2d-1)^{g-1}$. Dann gibt es für jedes $a \in f(R^n)$ ein $x \in A_g(n)$ mit $f(x) = a$. Insbesondere ist f nichtnegativ (positiv), wenn f nichtnegativ (positiv) auf $A_g(n)$ ist.*

Beweis. Es ist $f - a \in \Sigma_H^{(n)}(R)$. Der Rest folgt mit Satz 2.2.28 für $V(f - a)$. □

2.3 Dualer Standpunkt

Es gibt eine interessante Schlußfolgerung aus dem Satz von Timofte. Man findet für symmetrische Summen $2k$-ter Linearformpotenzen

$$\sum_i (a_{i1}X_1 + ... + a_{in}X_n)^{2k}$$

immer Darstellungen, bei denen für die Koeffizienten jeder einzelnen Linearform gilt:

$$\#\{a_{i1}, ..., a_{in}\} \leq k.$$

Man erhält dieses Resultat aus dem Satz 2.1 von Timofte durch Dualisierung, indem man den reellen Vektorraum der symmetrischen $2k$-Formen in n Unbestimmten $\mathcal{H}_{2k,n}^{S_n}$ mit einem geeigneten Skalarprodukt versieht. Umgekehrt erhielte man den Satz von Timofte (aber nur die Formulierung für Nichtnegativität) für den Spezialfall *homogener* symmetrischer Polynome, wenn man obige Darstellung der symmetrischen Summen $2k$-ter Linearformpotenzen direkt zeigen könnte. Im Abschnitt 2.3.2 zeigen wir, ohne den Satz von Timofte zu benutzen, eine solche Darstellbarkeit (mit $2k$ bzw. $k+1$ statt k) für gewisse Spezialfälle von Summen von Linearformpotenzen. Könnte man noch zeigen, daß die betrachteten Spezialfälle *dicht* im Kegel der symmetrischen Summen von Linearformpotenzen liegen, so erhielte man mit einem weiteren Resultat dieses Abschnitts (Lemma 2.3.5), welcher die Abgeschlossenheit des Teilkegels der Summen von Linearformpotenzen mit obiger Einschränkung an die Koeffizienten besagt, die gewünschte Gleichheit der Kegel. Leider ist mir dies nicht gelungen, nichts desto trotz schien es mir wert, die Resultate für die Spezialfälle mit in diese Arbeit aufzunehmen.

2.3.1 Darstellungen von Summen $2k$-ter Linearformpotenzen

Definition 2.3.1. Sei V ein reeller Vektorraum, wir nennen $\emptyset \neq C \subset V$ einen *konvexen Kegel*, falls $\mathbb{R}_{\geq 0}C + \mathbb{R}_{\geq 0}C = C$. Zu einem reellen Skalarprodukt $\langle , \rangle$ auf V heißt

$$C^* := \{x \in V \mid \langle x, y \rangle \geq 0 \text{ für alle } y \in C\}$$

der *duale* Kegel von C.

Bemerkung 2.3.2. Für einen konvexen Kegel C ist C^* abgeschlossen und ebenfalls ein konvexer Kegel. Es ist $(C^*)^* = \bar{C}$, falls $\dim_{\mathbb{R}} V < \infty$

Beweis. Es ist $C^* = \bigcap_{y \in C} \langle \cdot, y \rangle^{-1}(\mathbb{R}_{\geq 0})$ als Schnitt von Urbildern abgeschlossener Mengen unter stetigen Abbildungen abgeschlossen. Die Kegeleigenschaften sind trivial.

" $\supset$": Sei $x \in \bar{C}$. Dann gibt es eine Folge $(x_n) \to x$ in C. Es ist $\langle x_n, y \rangle \geq 0$ für alle $y \in C^*$. Wegen der Stetigkeit von $\langle \cdot, y \rangle$ gilt dies dann auch für x und jedes $y \in C^*$.

" $\subset$": Angenommen es gibt ein $x \in (C^*)^* \setminus \bar{C}$. Der Abstand von x zu C ist dann $m = \inf\{\|x - y\| \mid y \in C\} > 0$. Es gibt also eine Folge (y_n) in C, für welche $\|x - y_n\|$ gegen m konvergiert. Diese ist beschränkt, und da V endlichdimensional ist, findet man mit *Bolzano-Weierstrass* eine konvergente Teilfolge. Also gibt es ein $y \in \bar{C}$, mit minimalem Abstand zu x, d.h. $\|x - y\| = m$. Wir betrachten nun die zu $(y - x)$ orthogonale Hyperebene E durch den Ursprung. Diese Hyperebene teilt V in zwei Halbräume:

$$E^+ := \{x \in V \mid \langle x, (y - x) \rangle \geq 0\} \qquad E^- := \{x \in V \mid \langle x, (y - x) \rangle < 0\}.$$

Es ist $C \subseteq E^+$, denn falls es ein $c \in C$ gäbe mit $\langle c, (y - x) \rangle < 0$, dann wäre auf Grund der Konvexität von C auch $(y + \alpha(c - y)) \in C$ für beliebiges $\alpha \in [0, 1]$, und somit würde

$$\|x - y - \alpha(c - y))\|^2 = \|x - y\|^2 + \alpha^2 \|c - y\| + 2\alpha \underbrace{\langle (y - x), (c - y) \rangle}_{<0}$$

nicht minimal sein für $\alpha = 0$.

Offenbar ist dann $(y - x) \in C^*$, jedoch

$$\langle x, (y - x) \rangle = \langle (x - y), (y - x) \rangle + \underbrace{\langle y, (y - x) \rangle}_{=0} < 0,$$

also ist $x \notin (C^*)^*$. Widerspruch. $\square$

Definition 2.3.3. Wir werden mit $\mathcal{H}_{2k,n}$ den reellen Vektorraum der $2k$-Formen in n Unbestimmten bezeichnen; mit $N(n, 2k)$ werden wir dessen Dimension $\binom{n+2k-1}{2k}$ (siehe [Ba, Seite 12]) bezeichnen. Der konvexe Kegel

$$\mathcal{P}_{2k,n} := \{p \in \mathcal{H}_{2k,n} \mid p(x) \geq 0 \text{ für alle } x \in \mathbb{R}^n\}$$

ist die Menge der positiv semidefiniten $2k$-Formen. Der konvexe Kegel

$$\mathcal{L}_{2k,n} := \left\{ \sum_{i=1}^{m} (a_{i1}X_1 + ... + a_{in}X_n)^{2k} \mid m \in \mathbb{N}, a_{ij} \in \mathbb{R} \right\}$$

ist die Menge der Summen von $2k$-ten Linearformpotenzen. Es bezeichne $\mathcal{H}_{2k,n}^{S_n}$ den Unterraum der *symmetrischen* $2k - Formen$, und für jedes $C \subset \mathcal{H}_{2k,n}$ definieren wir

$$C^{S_n} := C \cap \mathcal{H}_{2k,n}^{S_n}.$$

Falls C ein konvexer Kegel im $\mathcal{H}_{2k,n}$ ist, so ist auch C^{S_n} konvexer Kegel im $\mathcal{H}_{2k,n}^{S_n}$. Für ein $g \in \mathbb{N}$, nennen wir den konvexen Kegel

$$\mathcal{T}_{2k,n}^{g} := \left\{ \sum_{i=1}^{m} (a_{i1}X_1 + ... + a_{in}X_n)^{2k} \in \mathcal{L}_{2k,n}^{S_n} \;\middle|\; m \in \mathbb{N}, a_{ij} \in \mathbb{R} \text{ mit } \#\{a_{i1}, ..., a_{in}\} \leq g \right\}$$

die *Timofte-Formen* der Güte g. Die entsprechenden Darstellungen nennen wir Timofte-Darstellungen der Güte g.

Wir werden nach Einführung eines passenden Skalarprodukts speziell die konvexen Kegel $\mathcal{P}_{2k,n}^{S_n}$, $\mathcal{L}_{2k,n}^{S_n}$ und $\mathcal{T}_{2k,n}^{g}$ in Hinblick auf gegenseitige Dualität untersuchen. Doch zunächst sei an dieser Stelle noch ein sehr nützlicher Satz notiert, auf den wir noch einigemale zurückgreifen werden. Er liefert eine Summenlängenbeschränkung in reellen Vektorräumen.

Satz 2.3.4 (Carathéodory). *Sei V ein reeller Vektorraum mit* $\dim V = n$. *Seien $v_1, ..., v_s \in V$ für ein $s \in \mathbb{N}$. Dann gibt es $i_1, ..., i_n \in \{1, ..., s\}$, sowie $\alpha_{i_1}, ..., \alpha_{i_n} \in \mathbb{R}_{\geq 0}$, so daß*

$$\sum_{i=1}^{s} v_i = \sum_{j=1}^{n} \alpha_{i_j} v_{i_j}.$$

Einen Beweis dieser Version des Satzes findet man in [Re, Seite 27].

Als eine erste Anwendung beweisen wir gleich ein Resultat, das eine wichtige Rolle im Beweis der Gleichheit von $\mathcal{L}_{2k,n}^{S_n}$ und $T_{2k,n}^{k}$ spielen wird. Der Beweis dazu ist eine Verallgemeinerung eines Beweises aus [Re, Seite 36], welcher die Abgeschlossenheit von $\mathcal{L}_{2k,n}$ in $\mathcal{H}_{2k,n}$ zeigt.

Lemma 2.3.5. *Für $g \in \mathbb{N}$ ist $\mathcal{T}_{2k,n}^{g} \subset \mathcal{H}_{2k,n}^{S_n}$ abgeschlossen bezüglich der Normtopologie.*

Wir werden etwas mehr zeigen, als im Lemma behauptet wird. Wir werden zeigen, daß

$$\mathcal{L}_{2k,n}^{g} := \left\{ \sum_{i=1}^{m} (a_{i1}X_1 + ... + a_{in}X_n)^{2k} \in \mathcal{L}_{2k,n} \;\middle|\; m \in \mathbb{N}, a_{ij} \in \mathbb{R} \text{ mit } \#\{a_{i1}, ..., a_{in}\} \leq g \right\}$$

abgeschlossen ist im $\mathcal{H}_{2k,n}$. Daraus folgt dann sofort, daß der Schnitt mit $\mathcal{H}_{2k,n}^{S_n}$ in $\mathcal{H}_{2k,n}^{S_n}$ abgeschlossen ist. Da $g \in \mathbb{N}$ beliebig ist, zeigt der Beweis aber insbesondere für $g = n$ auch die Abgeschlossenenheit von $\mathcal{L}_{2k,n}$ in $\mathcal{H}_{2k,n}$.

Beweis. Sei $(p_m)_{m\in\mathbb{N}} \subset \mathcal{L}_{2k,n}^{g}$ eine in $\mathcal{H}_{2k,n}$ konvergente Folge. Mit dem Satz von Carathéodory 2.3.4 haben die p_m eine Darstellung gleichbeschränkter Summenlänge:

$$(\star)\ p_m = \sum_{i=1}^{N(n,2k)} (a_{i1}^{(m)}X_1 + ... + a_{in}^{(m)}X_n)^{2k},$$

und es ist nachwievor $\#\{a_{i1}^{(m)}, ..., a_{in}^{(m)}\} \leq g$ für jedes $1 \leq i \leq N(n, 2k)$.

Wir finden also für jedes m und jedes i eine Partition (siehe Definition 2.2.23) $\big(I_1, ..., I_g\big)(i, m)$ von $\big(a_{i1}^{(m)}, ..., a_{in}^{(m)}\big) \in \mathbb{R}^n$. Da es aber nur *endlich viele* Möglichkeiten gibt $\{1, ..., n\}$ in g Teilmengen zu partitionieren, muß es also nach dem Schubfachprinzip für festes i unendlich viele m geben, für welche die Partition $(I_1, ..., I_g)(i, m)$ dieselbe ist. Schreibe $(I_1(i), ..., I_g(i)) := (I_1, ..., I_g)(i, m)$ für all diese m. Es muß sogar unendlich viele m geben, für welche dies für jedes

$1 \leq i \leq n$ simultan erfüllt ist. Wählen wir nun die zu diesen m gehörende Teilfolge von $(p_m)_m$. Der Einfachheit halber bezeichnen wir diese wieder mit $(p_m)_m$. wir können also für diese Teilfolge die Darstellung $(\star)$ uniform zusammenfassend umschreiben zu

$$p_m = \sum_{i=1}^{N(n,2k)} \Big(b_{i1}^{(m)} \big(\sum_{j \in I_1(i)} X_j \big) + ... + b_{ig}^{(m)} \big(\sum_{j \in I_g(i)} X_j \big) \Big)^{2k}.$$

Da die Folge (p_m) konvergent im Raum $\mathcal{H}_{2k,n}$ ist, konvergiert sie insbesondere unter punktweiser Auswertung. Betrachten wir die Folge der Auswertungen des j-ten Standardbasisvektors $e_j \in \mathbb{R}^n$. Für $1 \leq i \leq n$ sei l_i so, daß $j \in I_{l_i}(i)$ ist. Dann ist

$$p_m(e_j) = \sum_{i=1}^{N(n,2k)} (b_{il_i}^{(m)})^{2k},$$

beschränkt auf Grund der Konvergenz für $m \to \infty$. Da

$$(b_{rl_r}^{(m)})^{2k} \leq \sum_{i=1}^{N(n,2k)} (b_{il_i}^{(m)})^{2k}$$

ist für jedes einzelne $1 \leq r \leq N(n, 2k) = N$, ist die Folge

$$(b_{1l_1}^{(m)}, ..., b_{Nl_N}^{(m)})_m \subset \mathbb{R}^N$$

beschränkt und somit hat sie eine konvergente Teilfolge nach *Bolzano-Weierstrass*. Betrachten wir die zugehörige Teilfolge von (p_m), welche wir wiederum mit (p_m) bezeichnen. Wir haben dann die Darstellung

$$(\star\star)\ p_m = \sum_{i=1}^{N(n,2k)} \Big(b_{i1}^{(m)} \big(\sum_{j \in I_1(i)} X_j \big) + ... + b_{ig}^{(m)} \big(\sum_{j \in I_g(i)} X_j \big) \Big)^{2k},$$

in welcher für jedes i (jeden Summanden) es eine Koeffizientenfolge $(b_{il_i}^{(m)})_m$ gibt, welche für $m \to \infty$ konvergiert. Indem wir dieselbe Vorgehensweise nacheinander für alle Standardbasisvektoren e_j iterieren, finden wir schließlich eine Teilfolge $(p_m)_m$, in welcher die Darstellung $(\star\star)$ koeffizientenweise konvergiert. Sei $p \in \mathcal{L}_{2k,n}^g$ definiert durch die Darstellung $(\star\star)$, in welcher für die jeweiligen Koeffizienten $b_{il}^{(m)}$ deren Grenzwert für $m \to \infty$ eingesetzt ist. Man überlegt sich schnell, daß dann (p_m) gegen p in $\mathcal{H}_{2k,n}$ konvergiert. Damit ist alles gezeigt. $\square$

Definition 2.3.6. Wir definieren nun ein Skalarprodukt auf $\mathcal{H}_{2k,n}$:
für $f = \sum_{|\mu|=2k} \alpha_\mu X^\mu$ und $g = \sum_{|\mu|=2k} \beta_\mu X^\mu$ definieren wir

$$\langle f, g\rangle := \sum_{|\mu|=2k} \frac{\mu_1! \cdots \mu_n!}{(2k)!} \alpha_\mu \beta_\mu.$$

Man sieht einfach, daß dies eine positiv definite symmetrische Bilinearform ist.

Bemerkung 2.3.7. Sei $g = (a_{i1}X_1 + ... + a_{in}X_n)^{2k} \in \mathcal{L}_{2k,n}$, dann ist $\langle f, g\rangle = f(a_{i1}, ..., a_{in})$ für jedes $f \in \mathcal{H}_{2k,n}$.

Diese Eigenschaft des Skalarprodukts ist der Schlüssel, um die symmetrischen positiv semidefiniten $2k$-Formen als dualen Kegel der symmetrischen Summen von $2k$-ten Linearformpotenzen auffassen zu können. Dazu schränken wir das Skalarprodukt auf den Raum $\mathcal{H}_{2k,n}^{S_n}$ ein. Dann können wir die symmetrischen positiv semidefiniten Formen $\mathcal{P}_{2k,n}^{S_n}$ wie folgt schreiben:

$$\begin{aligned}
P_{2k,n}^{S_n} &= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid p(a_1, ..., a_n) \geq 0 \text{ für alle } a \in \mathbb{R}^n\right\} \\
&= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid \sum_{i=1}^{m} p(a_{i1}, ..., a_{in}) \geq 0 \text{ für alle } m \in \mathbb{N}, a_{ij} \in \mathbb{R}\right\} \\
&= \left\{p \in \mathcal{H}_{2k,n}^{S_n}\right. \\
&\qquad \left. \mid \sum_{i=1}^{m} \Big(\sum_{\sigma \in S_n} p(a_{i\sigma(1)}, ..., a_{i\sigma(n)}) \Big) \geq 0 \text{ für alle } \ m \in \mathbb{N}, a_{ij} \in \mathbb{R}\right\} \\
&= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid \langle p, h\rangle \geq 0 \text{ für alle } h \in \mathcal{L}_{2k,n}^{S_n}\right\} \\
&= {\mathcal{L}_{2k,n}^{S_n}}^*
\end{aligned}$$

Andererseits wissen wir mit dem Satz von Timofte 2.1, daß

$$\begin{aligned}
\mathcal{P}_{2k,n}^{S_n} &= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid p(a_1, ..., a_n) \geq 0 \text{ für alle } a \in \mathbb{R}^n \text{ mit } \#\{a_1, ..., a_n\} \leq k\right\} \\
&= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid \sum_{\sigma \in S_n} p(a_{\sigma(1)}, ..., a_{\sigma(n)}) \geq 0 \text{ für } a \in \mathbb{R}^n \text{ mit } \#\{a_1, ..., a_n\} \leq k\right\} \\
&\ \vdots \\
&= \left\{p \in \mathcal{H}_{2k,n}^{S_n} \mid \langle p, h\rangle \geq 0 \text{ für alle } h \in \mathcal{T}_{2k,n}^{k}\right\} \\
&= {\mathcal{T}_{2k,n}^{k}}^*
\end{aligned}$$

In beiden Gleichungsketten ist nicht jede Gleichheit völlig trivial. Man muß sich beispielsweise klarmachen, daß für jedes $a \in \mathbb{R}^n$

$$\frac{1}{n!} \sum_{\sigma \in S_n} p(a_{\sigma(1)}, ..., a_{\sigma(n)}) = p(a_1, ..., a_n)$$

gilt, wegen der Symmetrie von p.

Da ja $\mathcal{T}_{2k,n}^k \subset \mathcal{L}_{2k,n}^{S_n}$ abgeschlossene konvexe Kegel in $\mathcal{H}_{2k,n}^{S_n}$ sind, folgt das Hauptresultat dieses Kapitels nun leicht.

Satz 2.3.8 (Darstellungssatz).

$$\mathcal{T}_{2k,n}^k = \mathcal{L}_{2k,n}^{S_n}$$

Beweis. $\mathcal{T}_{2k,n}^k = (\mathcal{T}_{2k,n}^k{}^*)^* = \mathcal{P}_{2k,n}^{S_n}{}^* = (\mathcal{L}_{2k,n}^{S_n}{}^*)^* = \mathcal{L}_{2k,n}^{S_n}$ Die erste und die letzte Gleichheit folgt aus der in Lemma 2.3.5 bewiesene Abgeschlossenheit der konvexen Kegel $\mathcal{T}_{2k,n}^k$ und $\mathcal{L}_{2k,n}^{S_n}$ zusammen mit Bemerkung 2.3.2, die zweite und dritte Gleichheit folgt direkt aus der eben festgestellte Dualität $\mathcal{P}_{2k,n}^{S_n} = \mathcal{T}_{2k,n}^k{}^*$ sowie $\mathcal{P}_{2k,n}^{S_n} = \mathcal{L}_{2k,n}^{S_n}{}^*$, wobei für die zweite Gleichheit der nichttriviale Satz von Timofte ausgenutzt wurde. □

2.3.2 Elementarer Beweis der Timofte-Darstellung für Spezialfälle

Wie schon erwähnt, wäre ein elementarer Beweis des Darstellungssatzes 2.3.8 auch ein Beweis für einen Spezialfall des Satzes von Timofte 2.1 (nämlich die Aussage über Nichtnegativität für *homogene* symmetrische Polynome f). Leider gelang es mir nicht den Darstellungssatz in seiner vollen Allgemeinheit ohne Verwendung des Satzes von Timofte zu zeigen, sondern nur für ganz spezielle symmetrische Summen von Linearformpotenzen, nämlichen einerseits solchen, deren Darstellung in minimaler Summenlänge eindeutig ist, und andererseits solchen, die sogar invariant unter orthogonaler Koordinatentransformation sind.

Summen von Linearformpotenzen mit eindeutiger minimaler Summen-Darstellung

Definition 2.3.9. Wir nennen eine Darstellung $f = \sum_{i=1}^{s}(a_{i1}X_1 + ... + a_{in}X_n)^{2k}$ von $f \in \mathcal{L}_{2k,n}^{S_n}$ *minimal*, falls die Summenlänge s minimal ist unter allen Darstellungen f.

Wir nennen die minimale Darstellung $f = \sum_{i=1}^{s}(a_{i1}X_1 + ... + a_{in}X_n)^{2k}$ eine *eindeutige minimale* Dastellung falls es für jede weitere minimale Darstellung $f = \sum_{i=1}^{s}(b_{i1}X_1 + ... + b_{in}X_n)^{2k}$ eine Permutation τ der Summanden gibt, so daß

$$(a_{i1}, .., a_{in}) = (b_{\tau(i)1}, ..., b_{\tau(i)n}) \text{ oder } (a_{i1}, .., a_{in}) = -(b_{\tau(i)1}, ..., b_{\tau(i)n})$$

ist für jedes $1 \leq i \leq s$.

Mit dem Satz von Carathéodory 2.3.4 für $\mathcal{H}_{2k,n}$ gilt für die minimale Summenlänge immer $s \leq N(n, 2k)$.

Lemma 2.3.10. *Habe $f \in \mathcal{L}_{2k,n}^{S_n}$ eine eindeutige minimale Darstellung $f = \sum_{i=1}^{s}(a_{i1}X_1 + ... + a_{in}X_n)^{2k}$, dann läßt sich für jedes $1 \leq i \leq s$ die Ordnung der Gruppe*

$$U_i := \left\{\sigma \in S_n \mid (a_{i1}X_1 + ... + a_{in}X_n)^{2k} = (a_{i1}X_{\sigma(1)} + ... + a_{in}X_{\sigma(n)})^{2k}\right\}$$

wie folgt nach unten abschätzen:

$$\#U_i \geq \frac{n!}{s}.$$

Beweis. U_i ist eine Untergruppe der S_n. Wir betrachten nun die Menge der Linksnebenklassen in S_n/U. Diese korrespondieren eineindeutig mit einigen Summanden der minimalen Darstellung von f, denn falls für $\tau_1, \tau_2 \in S_n$ gilt, daß

$$(a_{i1}X_{\tau_1(1)} + ... + a_{in}X_{\tau_1(n)})^{2k} = (a_{i1}X_{\tau_2(1)} + ... + a_{in}X_{\tau_2(n)})^{2k},$$

dann ist wohl $\tau_2^{-1}\tau_1 \in U_i$ und somit $\tau_1 U_i = \tau_2 U_i$. Dies führt uns zu der Abschätzung $\#S_n/U_i \leq s$, und somit zu $|U_i| \geq \frac{n!}{s}$. $\square$

Lemma 2.3.11. *Habe $f \in \mathcal{L}_{2k,n}^{S_n}$ eine eindeutige minimale Darstellung $f = \sum_{i=1}^{s}(a_{i1}X_1 + ... + a_{in}X_n)^{2k}$, dann läßt sich für jedes $1 \leq i \leq s$ die Ordnung der Gruppe*

$$H_i := \left\{\sigma \in S_n \mid (a_{i1}X_1 + ... + a_{in}X_n) = (a_{i1}X_{\sigma(1)} + ... + a_{in}X_{\sigma(n)})\right\}$$

wie folgt nach unten abschätzen:

$$\#H_i \geq \frac{n!}{2s}.$$

Beweis. H_i ist eine Untergruppe der Gruppe U_i aus dem vorigen Lemma. Wir schätzen nun den Index von H_i in U_i ab. Für jedes $\sigma \in U_i$ gilt ja

$$(a_{i1}X_1 + ... + a_{in}X_n)^{2k} = (a_{i1}X_{\sigma(1)} + ... + a_{in}X_{\sigma(n)})^{2k}.$$

Aufgrund der Irreduzibilität von linearen Polynomen im faktoriellen Ring $\mathbb{R}[X_1, ..., X_n]$ ist dann

$$a_{i1}X_1 + ... + a_{in}X_n = \alpha(a_{i1}X_{\sigma(1)} + ... + a_{in}X_{\sigma(n)})$$

für passendes $\alpha \in \mathbb{R}[X_1, ..., X_n]^* = \mathbb{R} \setminus \{0\}$. Es muß dann $\alpha^{2k} = 1$ sein, also $\alpha = 1$ oder $\alpha = -1$. Die Zuordnung $\sigma \mapsto \alpha$ ist offensichtlich ein Gruppenhomomorphismus von U_i nach $(\{1, -1\}, \cdot)$ mit Kern H_i. Mit dem Homomorphiesatz ist dann $\#U_i/H_i \leq 2$. Damit ist alles gezeigt. $\square$

Mit diesen Abschätzungen wollen wir nun zeigen, daß eine eindeutige minimale Darstellung von $f \in \mathcal{L}_{2k,n}^{S_n}$ schon notwendig eine Timofte-Darstellung der Güte $2k$ ist. Wir benutzen dabei, daß sich die Anzahl der verschiedenen Koeffizienten einer Linearform $(a_{i1}X_1 + ... + a_{in}X_n)$ der Darstellung nach oben abschätzen läßt durch die Anzahl der Bahnen in $\{1, ..., n\}$ unter der Wirkung der Gruppe H_i. Wir werden die Gruppenordnung der H_i abhängig von der Anzahl der Bahnen nach oben abschätzen. Da wir andererseits aber bereits eine untere Schranke für die Gruppenordnung gefunden haben, werden wir dann umgekehrt die Anzahl der Bahnen nach oben abschätzen können.

Lemma 2.3.12. *Sei $G \subset S_n$ eine Untergruppe und sei $\{1, ..., n\} = I_1 \dot{\cup} \cdots \dot{\cup} I_m$ die Zerlegung in die m Bahnen von G. Dann ist $\#G \leq (n - m + 1)!$*

Beweis. Wir überlegen uns zuerst, daß $G \hookrightarrow S_{I_1} \times \cdots \times S_{I_m}$. Da die I_j Bahnen von G sind, ist für jedes $g \in G$ die Einschränkung der Gruppenoperation $g|_{I_j} \in S_{I_j}$ wohldefiniert, da ja $g(x) \in I_j$ ist für alle $x \in I_j$. Also ist $g = g|_{I_1} \circ \cdots \circ g|_{I_m}$. Betrachten wir nun die Abbildung

$$\begin{array}{ccc} G & \longrightarrow & S_{I_1} \times \cdots \times S_{I_m} \\ g & \mapsto & (g|_{I_1}, ..., g|_{I_m}). \end{array}$$

Sie ist ein Gruppenhomomorphismus, da $g \circ f = g|_{I_1} \circ \cdots \circ g|_{I_m} \circ f|_{I_1} \circ \cdots \circ f|_{I_m} = (g \circ f)|_{I_1} \circ \cdots (g \circ f)|_{I_m}$ (die I_j sind disjunkt!), deren Kern trivial ist.

Somit haben wir also $\#G \leq \#I_1! \cdots \#I_m!$. Wir haben noch die Bedingung $\#I_1 + ... + \#I_m = n$, woraus folgt, daß $\#I_1! \cdots \#I_m! \leq (n - m + 1)!$. (Man kann zeigen, daß etwa für $\#I_1 = n - (m - 1)$ und $|I_j| = 1$ für $j \neq 1$ dieses Produkt maximal wird). $\square$

Bevor wir nun das angestrebte Resultat dieses Abschnitts beweisen, wollen wir noch eine kleine dazu benötigte Eigenschaft natürlicher Zahlen in einer Behauptung auslagern.

Behauptung 2.3.13. *Seien $n, m \in \mathbb{N}$ mit $3 \leq m \leq n - 3$, dann ist*

$$m(n - m) \geq n + m.$$

Beweis. Wir zeigen die Behauptung induktiv nach n. Für $n = 6$ ist $m = 3$ ist die Ungleichung erfüllt. Sein nun die Behauptung war für ein $n \in \mathbb{N}$. Im Fall $3 \leq m \leq n - 3$ ist $m(n + 1 - m) = m(n - m) + m \geq n + 2m \geq (n + 1) + m$. Im Fall $m = (n + 1) - 3$ ist $m(n + 1 - m) = (n - 2)3 = 3n - 6 \geq 2n - 2 = n + m$ (da $n \geq 6$). $\square$

Satz 2.3.14. *Habe $f \in \mathcal{L}_{2k,n}^{S_n}$ eine eindeutige minimale Darstellung. Dann gilt für diese Darstellung $f = \sum_{i=1}^{s} (a_{i1}X_1 + ... + a_{in}X_n)^{2k}$, daß*

$$\#\{a_{i1}, ..., a_{in}\} \leq \max\{2k, 4\}$$

für alle $1 \leq i \leq s$.

Beweis. Offensichtlichtlich müssen wir nur den Fall $\max\{2k, 4\} + 1 < n$ betrachten.
Mit dem Satz von Carathéodory 2.3.4 angewandt auf $\mathcal{H}_{2k,n}$ wissen wir, daß $s \leq \binom{n+2k-1}{n-1}$. Sei H_i die wie in Lemma 2.3.11 definierte Untergruppe der S_n. Für $\sigma \in S_n$ gilt dann

$$(a_{i1}, ..., a_{in}) = (a_{i\sigma(1)}, ..., a_{i\sigma(n)}) \Leftrightarrow \sigma \in H_i.$$

Die Anzahl der Bahnen von H_i in $\{1, ..., n\}$ ist eine obere Schranke für die Anzahl der *verschiedenen* Koeffizienten unter den $a_{i1}, ..., a_{in}$. Nach Lemma 2.3.11 ist $\#H_i \geq \frac{n!}{2\binom{n+2k-1}{n-1}}$. Wir werden nun zeigen, daß im Fall $m = \max\{2k, 4\} + 1$ die Ungleichung $\frac{n!}{2\binom{n+2k-1}{n-1}} > (n - m + 1)!$ gilt, woraus dann mit Lemma 2.3.12 folgt, daß es weniger als m Bahnen von H_i in $\{1, ..., n\}$ geben muß. Wir werden für $k \geq 2$ dazu die Ungleichung $\frac{n!(n-1)!(2k)!}{2(n+2k-1)!(n-2k+1)!} > 1$ zeigen, bzw. nach offensichtlichem Kürzen die Ungleichung

$$\frac{(2k)!n \cdots (n - 2k + 1)}{2(n + 2k - 1) \cdots n} > 1.$$

Durch passendes sortieren der Faktoren, erhalten wir

$$\frac{(2k-1)(n-(2k-1))}{n+2k-1} \cdot \frac{(2k-2)(n-(2k-2))}{n+2k-2} \cdots \frac{3(n-3)}{n+3} \cdot \frac{2(n-2)}{n+2} \cdot \frac{k(n-1)}{n+1} \cdot \frac{2n}{2n} > 1,$$

da mit Behauptung 2.3.13 die "ersten $2k - 3$ Faktoren" größer als 1 sind (wegen $3 \leq 2k - (2k - 3) \leq ... \leq 2k - 1 \leq n - 3$), und die "letzten 3 Faktoren" sind größer oder gleich 1, denn wegen $k \geq 2$ muß $n > 5$ sein.

Falls $k = 1$ ist, überlegen wir uns, daß $\frac{n!}{2\binom{n+1}{n-1}} > (n - 4)!$, oder $\frac{n(n-1)(n-3)}{(n+1)n} > 1$ ist. Da wir in diesem Fall aber nur $n > 5$ betrachten, ist das nicht schwer zu sehen. $\square$

Orthogonal invariante $2k$-Formen

Wir haben im letzten Unterabschnitt gezeigt, daß eine symmetrische Summe $2k$-ter Linearformpotenzen, deren Darstellung minimaler Summenlänge "eindeutig" ist, eine Timofteform der Güte $2k$ ist. Der Beweis dazu ließe sich problemlos verallgemeinern für solche Fälle, die nicht mehr als $m(n)$ verschiedene minimale Darstellungen haben (dann aber mit einer schlechteren Güte), solange $m(n)$ "genügend klein" im Vergleich zu $n!$ ist. Dies würde uns aber auch keinen allgemeinen Darstellungssatz liefern, da es sogar Beispiele gibt, die jeweils unendlich viele minimale Darstellungen haben.

Wir werden in diesem Abschnitt einerseits zeigen, daß es sich bei orthogonal invarianten $2k$-Formen um solche Beispiele handelt. Andererseits werden wir aber gerade für diese Fälle einen völlig anderen Beweis (der ebensowenig den Satz von Timofte verwendet) dafür liefern, daß es Timofte-Darstellungen der Güte $k+1$ gibt.

Definition 2.3.15. $f \in \mathcal{H}_{2k,n}$ heißt *orthogonal invariant*, falls für $x \in \mathbb{R}^n$ gilt

$$f(x) = f(Ax) \text{ für alle } A \in O_n(\mathbb{R}).$$

(Insbesondere ist dann $f \in \mathcal{H}_{2k,n}^{S_n}$.)

Bemerkung 2.3.16. Reelle homogene Polynome (Formen) sind eindeutig bestimmt durch ihre Werte auf der Einheitssphäre S^{n-1}. Deshalb gibt es für jedes orthogonal invariante $f \in \mathcal{H}_{2k,n}$ ein $r \in \mathbb{R}$, so daß

$$f = r(X_1^2 + ... + X_n^2)^k.$$

Das nächste Lemma zeigt, daß es sich bei orthogonal invarianten $2k$-Formen um Summen $2k$-ter Linearformpotenzen handelt. Deren Symmetrie ist sowieso klar. Der Beweis lehnt sich an einen Beweis aus [Ba, Seite 13/14].

Lemma 2.3.17 (Hilbertidentitäten). *Für $(X_1^2 + ...X_n^2)^k \in \mathcal{H}_{2k,n}^{S_n}$ gibt es $N \in \mathbb{N}$ sowie $(a_{i1}, ..., a_{in}) \in \mathbb{R}^n$ für $i \leq N$, so daß*

$$(X_1^2 + ...X_n^2)^k = \sum_{i=1}^{N} (a_{i1}X_1 + ... + a_{in}X_n)^{2k}.$$

Beweis. Betrachte die Abbildung

$$\begin{aligned} \mathbb{R}^n &\longrightarrow \mathcal{H}_{2k,n} \\ a &\mapsto (a_1X_1 + ... + a_nX_n)^{2k}. \end{aligned}$$

Diese ist stetig. Wir wählen uns auf der Einheitssphäre $S^{n-1} \subset \mathbb{R}^n$ ein Borelmaß μ, das unter orthogonaler Transformation invariant ist (bekannt aus der Maßtheorie), dann existiert aufgrund der Stetigkeit (also Borelmessbarkeit) obiger Abbildung das Integral

$$I := \int_{S^{n-1}} (a_1X_1 + ... + a_nX_n)^{2k} \mathrm{d}a \in \mathcal{H}_{2k,n}.$$

Es ist I der Grenzwert einer Folge von Integralen von Treppenfunktionen

$$\sum_i \mu(A_i)(a_{i1}X_1 + ... + a_{in}X_n)^{2k} \in \mathcal{L}_{2k,n},$$

wobei die $A_i \subset S^{n-1}$ borelmessbar sind mit $S^{n-1} = \dot{\bigcup}_i A_i$. Aufgrund der Abgeschlossenheit von $\mathcal{L}_{2k,n}$, ist $I \in \mathcal{L}_{2k,n}$.

Wir zeigen nun, daß I orthogonal invariant und positiv definit ist. Wir wissen, daß I Grenzwert von Integralen von Treppenfunktionen im Polynomraum $\mathcal{H}_{2k,n}$ ist. Insbesondere ist die Polynomfunktion $I(x)$ *punktweise* Grenzwert dieser Integrale (also nach Einsetzen von $x \in \mathbb{R}^n$). Aufgrund der orthogonalen Invarianz des Borelmaßes gilt dann punktweise und für jede orthogonale Transformation T:

$$\begin{aligned} I(Tx) = \quad & \textstyle\int_{S^{n-1}} \langle a, Tx\rangle^{2k} \mathrm{d}a & = \int_{S^{n-1}} \langle T^{-1}a, x\rangle^{2k} \mathrm{d}a & \\ = \quad & \textstyle\int_{T^{-1}S^{n-1}} \langle T^{-1}a, x\rangle^{2k} \mathrm{d}T^{-1}a & = \int_{S^{n-1}} \langle a, x\rangle^{2k} \mathrm{d}a & = I(x) \end{aligned}$$

Dies zeigt die orthogonale Invarianz von I. Da für festes x der Integrand eine positiv semidefinite stetige Funktion in a ist, welche nicht überall 0 ist, hat I mit Bemerkung 2.3.16 dann die Gestallt $I = r(X_1^2 + ... + X_n^2)^k$ für ein $r \in \mathbb{R}_{>0}$. Damit ist alles gezeigt, da man $(\frac{1}{r})^{\frac{1}{2k}}$ in die Koeffizienten der Linearformen hineinziehen kann. □

Dies zeigt unmittelbar folgendes Korollar.

Korollar 2.3.18. *Es gibt orthogonal invariante $f \in \mathcal{L}_{2k,n}^{S_n}$. Diese haben unendlich viele minimale Darstellungen als Summen $2k$-ter Linearformpotenzen. Unter diesen gibt es solche, die keine Timofte-Darstellungen sind.*

Beweis. Mit Lemma (2.3.17) wissen wir, daß

$$(X_1^2 + ...X_n^2)^k = \sum_{i=1}^{N} (a_{i1}X_1 + ... + a_{in}X_n)^{2k} \in \mathcal{L}_{2k,n}^{S_n}$$

ist. Sei dabei die Summenlänge N minimal unter all solchen Darstellungen. Betrachten wir die obige Gleichung als Gleichheit von Funktionen auf dem $\mathbb{R}^n$:

$$(x_1^2 + ... + x_n^2)^k = \sum_{i=1}^{N} \langle a_i, x\rangle^{2k}$$

Die linke Seite der Gleichung ist ganz offensichtlich invariant unter jeder orthogonalen Variablentransformation T, also ist

$$(x_1^2 + ... + x_n^2)^k = \sum_{i=1}^{N} \langle a_i, Tx\rangle^{2k} = \sum_{i=1}^{N} \langle T^{-1}a_i, x\rangle^{2k}.$$

Die orthogonale Gruppe hat unendliche Kardinalität, so daß es unendlich viele verschieden Darstellungen $(X_1^2 + ...X_n^2)^k = \sum_{i=1}^{N} (a_{i1}X_1 + ... + a_{in}X_n)^{2k}$ geben muß, die paarweise nicht durch Vertauschung der Summanden auseinander hervorgehen (oder durch passendes Wechseln der Koeffizientenvorzeichen). Außerdem gibt es für jedes $b \in \mathbb{R}^n$ mit $\|b\| = \|a_1\|$ eine orthogonale Transformation T, für die $T^{-1}a_1 = b$ ist. Also gibt es immer eine Darstellung von f, in welcher a_1 sogar n verschiedene Komponenteneinträge hat. Insbesondere ist dies keine Timofte-Darstellung. $\square$

Nachdem wir nun gezeigt haben, daß die kombinatorische Überlegung aus dem vorigen Unterabschnitt für minimale Darstellungen im orthogonal invarianten Fall nicht greifen kann, werden wir für diesen Fall einen anderen Weg gehen, um eine Timofte-Darstellung der Güte $k+1$ zu erhalten. Wir werden dazu die Hilbertidentitäten aus Lemma 2.3.17 präzisieren, indem wir uns an einem beinahe konstruktiven Beweis von *Haussdorff* für selbige orientieren.

Die von Hausdorff präzisierten Identitäten wurden von *Hilbert* schon früher (etwas komplizierter) bewiesen und benutzt, um das aus der Zahlentheorie bekannte *Waringsche Problem* zu lösen. Das Waringsche Problem stellt die Frage, ob es zu jeder natürlichen Zahl k eine natürliche Zahl s gibt, so daß jede natürliche Zahl n als Summe von höchstens s k-ten Potenzen natürlicher Zahlen geschrieben werden kann. Hilbert zeigte, daß dem so ist. Dazu benutzte er die von ihm gefundenen Identitäten, in denen die Koeffizienten der Linearformen sogar *rational* gewählt werden konnten. (Dies und den Beweisweg von Hausdorff findet man in [Na, Seiten 77-93].) Wir werden in unserem modifizierten Beweis darauf verzichten die Koeffizienten der Darstellung rational zu wählen und als Belohnung für diesen Verzicht eine Timofte-Darstellung der Güte $k+1$ erhalten.

Lemma 2.3.19. *Für jedes $n \in \mathbb{N}_0$ gilt für das n-te Moment*

$$\mathcal{M}_n = \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} x^n \exp(-x^2)\, dx$$

des Gaußmaßes auf dem $\mathbb{R}^1$:

$$\mathcal{M}_n = \begin{cases} \dfrac{n!}{2^n (\frac{n}{2})!}, & n \text{ gerade} \\ 0, & n \text{ ungerade} \end{cases}$$

Beweis. Wir zeigen die Aussage zunächst für gerade n induktiv. Für $n = 0$ ist mit $\mathcal{M}_0 = 1 = 2^0 0!$ die Aussage wahr. Sei $\mathcal{M}_n = \dfrac{n!}{2^n(\frac{n}{2})!}$ für ein beliebiges gerades $n \in \mathbb{N}$, dann ist

$$\begin{aligned}
\mathcal{M}_{n+2} &= \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} x \exp(-x^2) x^{n+1} \mathrm{d}x \\
&= \frac{-1}{2\sqrt{\pi}} [\exp(-x^2) x^{n+1}]_{-\infty}^{\infty} - \frac{-(n+1)}{2\sqrt{\pi}} \int_{\mathbb{R}} x^n \exp(-x^2) \mathrm{d}x \\
&= \frac{n+1}{2} \mathcal{M}_n = \frac{(n+1)(n+2)}{2^2 \frac{n+2}{2}} \mathcal{M}_n \\
&= \frac{(n+2)!}{2^{n+2} (\frac{n+2}{2})!}
\end{aligned}$$

Falls n ungerade ist, stimmt die Behauptung offensichtlich, da $\exp(-x^2)$ eine gerade Funktion ist. $\square$

Um das nächste wichtige Lemma beweisen zu können, müssen wir uns zunächst von Eigenschaften einiger spezieller reellen Polynome überzeugen.

Definition 2.3.20. $H_n(x) := (\frac{-1}{2})^n \exp(x^2) \left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^n (\exp(-x^2))$ definiert für jedes $n \in \mathbb{N}_0$ eine Polynomfunktion auf $\mathbb{R}$, daß sogenannte *Hermite*-Polynom vom Grad n.

Behauptung 2.3.21. *Für jedes $n \in \mathbb{N}_0$ ist H_n ein Polynom vom Grad n, für das gilt:*

(i) $H_{n+1}(x) = xH_n(x) - \frac{1}{2}H_n'(x)$ für $n \neq 0$ und $H_0 = 1$.

(ii) H_n hat n verschiedene reelle Nullstellen.

Beweis. (i):Wegen

$$\begin{aligned} H_n'(x) = \quad & (\frac{-1}{2})^n 2x \exp(x^2) \left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^n \left(\exp(-x^2)\right) \\ + & (\frac{-1}{2})^n \quad \exp(x^2) \left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^{n+1} \left(\exp(-x^2)\right) \end{aligned}$$

erhalten wir die (polynomial) rekursive Darstellung $\frac{1}{2}H_n' = XH_n - H_{n+1}$. Da zudem $H_0 = 1$ ist, ist insbesondere H_n ein Polynom.

(ii): Wir zeigen dies durch Induktion nach n. H_0 hat keine Nullstelle. Habe H_n nun n verschiedene reelle Nullstellen $\alpha_1 < ... < \alpha_n$. Da diese dann einfache Vielfachheit haben, ist $H_n'(\alpha_i) \neq 0$. Es muß dann $H_n'(\alpha_n) > 0$ sein, da $H_n(x) \to \infty$ für $x \to \infty$, da nach (i), das Polynom H_n den Leitkoeffizienten 1 hat. Für die Nullstellen hat $H_n'(\alpha_i)$ notwendigerweise wechselnde Vorzeichen, insbesondere ist $(-1)^{n-1}H_n'(\alpha_1) > 0$. Nach (i) hat dann $H_{n+1}(\alpha_i)$ gegenläufig wechselndes Vorzeichen, und nach dem Zwischenwertsatz hat dann H_{n+1} die $n-1$ verschiedenen Nullstellen $\beta_{i+1} \in (\alpha_i, \alpha_{i+1})$, für $1 \leq i \leq n$. Doch es gibt noch zwei weitere reelle Nullstellen: Einmal gibt es eine Nullstelle $\beta_{n+1} > \alpha_n$, da $H_{n+1}(\alpha_n) < 0$ aber $H_{n+1}(x)$ positiv ist für groß genuge x. Dann gibt es auch noch eine Nullstelle $\beta_1 < \alpha_1$, da im Fall n ungerade, $H_{n+1}(\alpha_1) < 0$ ist, aber H_{n+1} geraden Grad hat, und im Fall n gerade es entsprechend umgekehrt ist. $\square$

Lemma 2.3.22. *Für $k \in \mathbb{N}$ gibt es eine Quadraturformel für das Gaußmaß im $\mathbb{R}^1$ von Präzission $2k-1$ mit k Stützstellen, das heißt es gibt $\beta_1, ..., \beta_k \in \mathbb{R}$ und positive Gewichte $\rho_1, ..., \rho_k \in \mathbb{R}_{>0}$, so daß für jedes Polynom $f \in \mathbb{R}[X]$ mit $\deg(f) \leq 2k-1$ gilt*

$$\frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} f(x) \exp(-x^2) dx = \sum_{i=1}^{k} \rho_i f(\beta_i). \tag{2.7}$$

Insbesondere gilt für das j-te Moment $\mathcal{M}_j = \sum_{i=1}^{k} \rho_i \beta_i^j$, für $0 \leq j \leq 2k-1$.

Beweis. Seien zunächst $\beta_1 < ... < \beta_k \in \mathbb{R}$ beliebige k verschiedene reelle Zahlen. Dann gibt es eine Lösungen $\rho_1, ..., \rho_k \in \mathbb{R}$ für das Gleichungssystem

$$\begin{pmatrix} 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_k \\ \vdots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} \end{pmatrix} \begin{pmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_k \end{pmatrix} = \begin{pmatrix} \mathcal{M}_0 \\ \mathcal{M}_1 \\ \vdots \\ \mathcal{M}_{k-1} \end{pmatrix}, \tag{2.8}$$

da die (van-der-Monde) Determinante der Abbildungsmatrix $\neq 0$ ist. Wir suchen nun solche $\beta_1, ..., \beta_k$ für welche die ρ_i alle positiv sind.

Wählen wir uns dazu die k *verschiedenen* Nullstellen $\beta_1 < ... < \beta_k$ des Hermite-Polynoms H_k vom Grad k. Wir wissen noch nicht, ob die zugehörigen $\rho_1, ..., \rho_k$ alle positiv sind, aber wir können bereits sagen, daß für diese β_i als Stützstellen und ρ_i als (eventuell negative) Gewichte, Gleichung (2.7) für Polynome wegen (2.8) bis zum Grad $k-1$ gilt (wegen der Linearität des Integrals folgt dies aus der Gültigkeit für die Momente). Sei f ein Polynom mit $\deg(f) \leq 2k-1$. Da $\mathbb{R}[X]$ bezüglich der Gradabbildung ein euklidischer Wertebereich ist, schreiben wir $f = H_k q + r$ für Polynome q, r, wobei $\deg(r) \leq k-1$ und $\deg(q) \leq k-1$ ist. Es gilt

$$\begin{aligned} & \int_{\mathbb{R}} H_n(x) q(x) \exp(-x^2) \mathrm{d}x \\ = & \int_{\mathbb{R}} \left(\frac{-1}{2}\right)^n \underbrace{\exp(x^2)\exp(-x^2)}_{=1} \left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^k (\exp(-x^2)) q(x) \mathrm{d}x = 0, \end{aligned}$$

denn nach k-fach iterierter partieller Integration verschwindet im Integranden die k-te Ableitung von q, und die beim partiellen Integrieren entstandenen Randterme verschwinden sowieso. So erhalten wir Gleichung (2.7) für Polynome f bis zum Grad $2k-1$:

$$\sum_{i=1}^{k} \rho_i f(\beta_i) = \sum_{i=1}^{k} \rho_i r(\beta_i) = \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} r(x) \exp(-x^2) \mathrm{d}x = \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} f(x) \exp(-x^2) \mathrm{d}x.$$

Die Positivität der $\rho_1, ..., \rho_k$ kann man nun nachträglich zeigen. Für $1 \leq i \leq k$ setzen wir $f_i := \prod_{j \neq i} (x - \beta_j)^2$. Dann ist f_i vom Grad $2k-2$ positiv semidefinit und es ist $f_i(\beta_i) > 0$. Wir dürfen also Gleichung (2.7) darauf anwenden und erhalten

$$0 < \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} f_i(x) \exp(-x^2) \mathrm{d}x = \sum_{j=1}^{k} f_i(\beta_j) \rho_j = f_i(\beta_i) \rho_i.$$

Schließlich ist dann $\rho_i > 0$. $\square$

Satz 2.3.23. *Seien $n, k \in \mathbb{N}$, dann gibt es $\beta_1, ..., \beta_{k+1} \in \mathbb{R}$ sowie $\rho_1, ..., \rho_{k+1} \in \mathbb{R}_{>0}$, so daß*

$$(X_1^2 + ... + X_n^2)^k = \frac{4^k k!}{(2k)!} \sum_{j_1=1}^{k+1} ... \sum_{j_n=1}^{k+1} \rho_{j_1} \cdots \rho_{j_n} (\beta_{j_1} X_1 + ... + \beta_{j_n} X_n)^{2k}.$$

Insbesondere haben orthogonal invariante $f \in \mathcal{L}_{2k,n}$ eine Timofte-Darstellung der Güte $k+1$.

Beweis. Seien $\beta_1, ..., \beta_{k+1}$ die Stützstellen und $\rho_1, ..., \rho_{k+1}$ die positiven Gewichte der Quadraturformel (2.7) des letzten Lemmas (für $k+1$ statt k). Dann ist

$$\begin{aligned}
& \sum_{j_1=1}^{k+1} ... \sum_{j_n=1}^{k+1} \rho_{j_1} \cdots \rho_{j_n} (\beta_{j_1} X_1 + ... + \beta_{j_n} X_n)^{2k} \\
= \quad & \sum_{j_1=1}^{k+1} ... \sum_{j_n=1}^{k+1} \left(\rho_{j_1} \cdots \rho_{j_n} \sum_{|\alpha|=2k} \frac{(2k)!}{\alpha_1! \cdots \alpha_n!} \beta_{j_1}^{\alpha_1} \cdots \beta_{j_n}^{\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \right) \\
= \quad & (2k)! \sum_{|\alpha|=2k} \sum_{j_1=1}^{k+1} ... \sum_{j_n=1}^{k+1} \prod_{i=1}^{n} \left(\frac{X_i^{\alpha_i}}{\alpha_i!} \rho_{j_i} \beta_{j_i}^{\alpha_i} \right)
\end{aligned}$$

$$
\begin{aligned}
&= && (2k)! \sum_{|\alpha|=2k} \prod_{i=1}^{n} \left(\frac{X_i^{\alpha_i}}{\alpha_i!} \sum_{j=1}^{k+1} \beta_j^{\alpha_i} \rho_j \right) \\
&\overset{\text{Lemma 2.3.22}}{=} && (2k)! \sum_{|\alpha|=2k} \prod_{i=1}^{n} \left(\frac{X_i^{\alpha_i}}{\alpha_i!} \mathcal{M}_{\alpha_i} \right) \\
&\overset{\text{Lemma 2.3.19}}{=} && (2k)! \sum_{|\mu|=k} \prod_{i=1}^{n} \left(\frac{X_i^{2\mu_i}}{(2\mu_i)!} \frac{(2\mu_i)!}{2^{2\mu_i} \mu_i!} \right) \\
&= && \frac{(2k)!}{4^k} \sum_{|\mu|=k} \prod_{i=1}^{n} \frac{X_i^{2\mu_i}}{\mu_i!} \\
&= && \frac{(2k)!}{4^k k!} \sum_{|\mu|=k} \frac{k!}{\mu_1! \cdots \mu_n!} (X_1^2)^{\mu_1} \cdots (X_n^2)^{\mu_n} \\
&= && \frac{(2k)!}{4^k k!} (X_1^2 + ... + X_n^2)^k.
\end{aligned}
$$

□

Wie schon gesagt, folgt aus dem Satz von Timofte, daß es eine Timofte-Darstellung sogar der Güte k geben muß.

3. Anwendung

3.1 Effizienzgewinn für Positivitätstests bei festem Grad

Im Abschnitt *Modelltheorie reell abgeschlossener Körper* wurde bereits erwähnt, daß für jedes $N \in \mathbb{N}$ und für jede Formel $\phi(X_1, ..., X_N)$ in der Sprache der angeordneten Ringe, eine in der Theorie der reell abgeschlossenen Körper äquivalente *quantorenfreie* Formel $\delta(X_1, ..., X_N)$ effektiv erzeugt werden kann (Satz 1.1.6).

Dies impliziert insbesondere, daß es einen Algorithmus gibt, der zu gegebenen $N \in \mathbb{N}$, Formel $\phi(X_1, ..., X_N)$ und $a \in \mathbb{R}^N$ entscheidet, ob a die Formel ϕ erfüllt.

Für jede Anzahl an Unbestimmten n und jede Gradbeschränkung d gibt es also *eine* quantorenfreie Formel, welche für ein gegebenes Polynom $f(X_1, ..., X_n) = \sum \alpha_\mu X^\mu$ mit $\deg f \leq d$ anhand seiner Koeffizienten entscheidet, ob die Aussage

$$\forall x\big(f(x) \geq 0\big)$$

in den reell abgeschlossenen Körpern, die die Koeffizienten von f enthalten, gültig ist oder nicht.

Obwohl es effektiv möglich ist, zu jedem $n, d \in \mathbb{N}$ die entsprechende quantorenfreie Formel zu generieren, ist dieses Vorgehen keinesweg *effizient* (es muß mit mindestens exponentieller Abhängigkeit von n gerechnet werden, siehe [BPR, Seite 510]). Folglich ist die Generierung von quantorenfreien Formeln eine denkbar ungeeignete Grundlage für einen Algorithmus, der allgemeine reelle Polynome f auf Positivität (Nichtnegativität) testen soll.

Anders sieht es aus, wenn man die Fragestellung einschränkt, etwa wenn man

Positivität (Nichtnegativität) nicht für ganz allgemeine reelle Polynome testen will, sondern nur für eine ganz bestimmte Klasse von Polynomen.

Wir wollen die Ergebnisse für Positivitätstestmengen symmetrischer Polynome, die in dieser Arbeit dargelegt wurden, nun benutzen, um für *symmetrische* Polynome mit fester Gradschranke d (aber nicht beschränkter Anzahl von Unbestimmten) zu zeigen, daß die Quantorenelimination eben doch Grundlage eines effizienten Algorithmus sein kann. Der Satz von Timofte 2.1 wird es uns erlauben, bei fester Gradschranke d mit *einer einzigen* quantorenfreien Formel arbeiten zu können, was bedeutet, daß die "kostspielige" Generierung dieser Formel aus der Effizienzbetrachtung herausfällt.

Betrachten wir zunächst für feste $n, d \in \mathbb{N}$ diejenige Formel, welche nach Einsetzen der Koeffizienten eines Polynoms

$$f = \sum_{|\mu| \leq d} \alpha_\mu X_1^{\mu_1} \cdots X_n^{\mu_n}$$

(vom Grad $\leq d$ in weniger oder gleich n Unbestimmten) in die freien Variablen der Formel, dessen Positivität (Nichtnegativität) ausdrückt. Die Anzahl deren freien Variablen $N(n,d) = \binom{n+d}{n}$ entspricht der Anzahl der Monome vom Grad $\leq d$. Um beim Einsetzen der Koeffizienten eines gegebenen Polynoms in die Formel konsistent zu bleiben, wählen wir uns für die betrachteten Multiindizes eine uns genehme Nummerierung $\mu^{(1)}, ..., \mu^{(N)}$, etwa indem wir sie lexikographisch anordnen. Dann sieht die gesuchte Formel wie folgt aus:

$$\phi_{n,d}(Y_1, ..., Y_N) = \forall x_1, ..., x_n \Big(\sum_{i=1}^{N} Y_i x_1^{\mu_1^{(i)}} \cdots x_n^{\mu_n^{(i)}} \overset{(\geq)}{>} 0 \Big).$$

Die Anzahl $N = N(n,d)$ der freien Variablen Y_i in der Formel hängt sowohl von n als auch d ab.

Definition 3.1.1. Für $n \in \mathbb{N}$ nennen wir $m_1 \leq ... \leq m_g \in \mathbb{N}$ mit $m_1 + ... + m_g = n$ eine g-Partition von n.

Bemerkung 3.1.2. Sei $g = \max\{\lfloor \frac{d}{2} \rfloor, 2\}$. Für $f \in \Sigma^{[n]}(R)$ mit $\deg f \leq d$, ist

$f(X_1, ..., X_n)$ positiv (oder nichtnegativ) genau dann, wenn

$$f(\underbrace{X_1, ..., X_1}_{m_1 \text{ Stellen}}, X_2, ..., \underbrace{X_g, ..., X_g}_{m_g \text{ Stellen}})$$

nichtnegativ (oder positiv) im R^g ist für jede g-Partition von n.

Lemma 3.1.3. *Sei $g \in \mathbb{N}$. Dann gibt es für $n > g$ weniger als $(n+g)^g$ g-Partitionen von n.*

Beweis. Die Anzahl dieser Partitionen ist die Anzahl an Möglichkeiten n als Summe von g *von Null verschiedenen* Summanden zu schreiben. Wir bezeichnen diese mit $P(n, g)$, in Anlehnung an die aus der Kombinatorik bekannte *Partitionsfunktion* $P(n)$.

Es läßt sich nun $P(n, g)$ leicht nach oben abschätzen, durch die Anzahl an Möglichkeiten n als Summe von g *nicht notwendig von Null verschiedenen* Summanden *mit* Berücksichtigung der Reihenfolge der Summanden, zu schreiben. Diese Möglichkeiten wiederum können leicht mit der kanonischen Basis des Vektorraums der homogenen Polynome vom Grad n in g Variablen $\mathcal{H}_{n,g}$ identifiziert werden. Die Dimension dieses Vektorraums ist $\dim \mathcal{H}_{n,g} = \binom{g+n-1}{n}$. Es gilt also

$$P(n, g) \leq \binom{g+n-1}{n} = \frac{(n+g-1)\cdots(n+1)}{(g-1)!} \leq (n+g)^g.$$

$\square$

Wenn wir uns nun einen Algorithmus konstruieren für das Entscheidungsproblem, ob ein gegebenes symmetrisches (gradbeschränktes) Polynom nichtnegativ ist, und dessen Komplexität in Abhängigkeit von den Inputdaten abschätzen wollen, so brauchen wir eine Vorstellung davon, was eigentlich die Datengröße eines solchen Polynoms ist. Es gibt verschiedene (vernünftige gängige) Möglichkeiten, ein Polynom zu speichern. Wir werden nun aber nicht die Komplexitätsanalyse für jede dieser Möglichkeiten extra betreiben. Wir werden vielmehr eine obere Schranke für die Komplexität angeben, die von gewissen *Kenngrößen* (Anzahl an Unbestimmten, maximale Bitgröße) eines Polynoms abhängen. Von diesen Kenngrößen werden wir uns überlegen, daß sie kleiner sind als die Datengröße eines

Polynoms, egal wie man dieses nun gespeichert haben mag. Aufgrund der Monotonie der Komplexitätsschrankenfunktion in den Kenngrößen, ist diese dann auch eine für alle möglichen Speicherarten des Inputpolynoms gültige Komplexitätsschrankenfunktion in der Datengröße des Polynoms.

Bemerkung 3.1.4. Die *Datengröße* eines durch d gradbeschränkten symmetrischen Polynoms f in n Unbestimmten ist nach unten beschränkt durch die maximal vorkommende Datengröße der einzelnen Koeffizienten (klar). Sie ist ebenso nach unten beschränkt durch die Anzahl n der Unbestimmten.

Satz 3.1.5. *Für jedes feste $d \in \mathbb{N}$ gibt es einen Algorithmus von polynomialer Komplexität, welcher entscheidet ob ein gegebenes symmetrisches Polynom vom Grad $\leq d$ positiv (oder auch nichtnegativ) ist.*

Beweis. Nach dem Satz von Timofte 2.1 gibt es zu $d \in \mathbb{N}$ ein $g = \max\{\frac{d}{2}, 2\} \in \mathbb{N}$, so daß für ein beliebiges (also in der Anzahl n der Unbestimmten nicht eingeschränktes) symmetrisches Polynom f mit $\deg f \leq d$ die Positivität (oder Nichtnegativität) auf allen Punkten mit nicht mehr als g verschiedenen Komponenten getestet werden kann. Das Polynom $f(X_1, ..., X_n)$ auf diesen Punkten auf Positivität (Nichtnegativität) zu testen, ist (wegen der Symmetrie von f) gleichbedeutend damitfür jede g-Partition $P = \{m_1 \leq ... \leq m_g\}$ von n,

$$f_P := f(\underbrace{X_1, ..., X_1}_{m_1 \text{ Stellen}}, \underbrace{X_2, ..., X_2}_{m_2 \text{ Stellen}}, ..., \underbrace{X_g, ..., X_g}_{m_g \text{ Stellen}})$$

auf Positivität (Nichtnegativität) im $\mathbb{R}^g$ zu testen.

Die Daten des Polynoms f, sind durch seine Koeffizienten gegeben. Wir sollten uns zunächst davon überzeugen, daß die Berechnung der Koeffizienten des Polynoms

$$f_P = \sum_{|\nu| \leq d} \beta_\nu X_1^{\nu_1} \cdots X_g^{\nu_g}$$

aus den Koeffizienten von f jeweils von polynomialer Komplexität ist. Schreibt man

$$f(X_1, ..., X_n) = \sum_{|\mu| \leq d} \alpha_\mu X^\mu,$$

so erhält man die Koeffizienten β_ν des Polynoms f_P als

$$\beta_\nu = \sum_{\substack{\mu_1+\ldots+\mu_{m_1}=\nu_1,\ldots \\ \mu_{g-1}+1+\ldots+\mu_g=\nu_g}} \alpha_\mu.$$

Addition ist aber polynomial realisierbar. Da die Anzahl der in einer Summation vorkommenden Koeffizienten α_μ beschränkt ist durch die Anzahl der insgesamt in f vorkommenden Koeffizienten, und da diese Anzahl kleiner ist, als die Datengröße des Polynoms f, ist also jeder Koeffizient β_ν in polynomialer Komplexität aus den Daten (Koeffizienten) von f berechenbar. Die Anzahl der Koeffizienten β_ν ist eine vom Polynom f unabhängige Konstante, so daß also das Polynom f_P insgesamt in polynomialer Komplexität in den Daten des Polynoms f berechnet werden kann. Insbesondere ist die Datengröße des Polynoms f_P polynomial in der Datengröße des Polynoms f.
Bei f_P handelt es sich um ein Polynom vom Grad $\leq d$ in g Unbestimmten. Es gibt nach Satz 1.1.6 eine quantorenfreie Formel, welche für ein beliebiges Polynom h vom Grad $\leq d$ in g Unbestimmten anhand der Koeffizienten von h entscheidet, ob h positiv (oder nichtnegativ) ist. Eine quantorenfreie Formel ist eine endliche boolesche Kombination von polynomialen Ungleichungen und Gleichungen (in den Koeffizienten von h). Jede dieser polynomialen Terme läßt sich in polynomialer Komplexität in den Daten von g berechenen. Also ist auch der Aufwand, die Positivität (Nichtnegativität) von f_P zu testen polynomial in dessen Daten und folglich auch in der Datengröße von f.

Jetzt muß man sich nur noch überlegen, daß die Anzahl der möglichen Partitionen $P_g(n)$ polynomial von der Datenmengen von f abhängt. Wir haben uns bereits in Lemma 3.1.3 überlegt, daß $P_g(n) \leq (n+g)^g$ ist. Es ist also $P_g(n)$ beschränkt durch ein Polynom in n. Die Datengröße von f übersteigt die Anzahl n der vorkommenden Unbestimmten. Die bisher für feste Partition P von n überlegten Rechenschritte müssen $P_g(n)$ mal auf f angewendet werden. Der Aufwand ist also insgesamt polynomial in den Daten von f. $\square$

Literaturverzeichnis

[AE] H.Amann und J.Escher, *Analysis II*, Birkhäuser 1999 , 1.Auflage

[Ar] M.Artin, *Algebra*, Englewood Cliffs, NJ: Prentice-Hall (1991)

[Ba] A.Barvinok, *A Course in Convexity*, Graduate Studies in Mathematics. 54. Providence, RI: American Mathematical Society (AMS) (2002)

[Be] D.J.Benson , *Polynomial Invariants of Finite Groups*, London Mathematical Society Lecture Note Series. 190. Cambridge: Cambridge University Press (1993)

[BPR] S.Basu, R.Pollack, M.-F.Roy, *Algorithms in Real Algebraic Geometry*, Algorithms and Computation in Mathematics. 10. Berlin: Springer (2003)

[Na] M.Nathanson, *Additive Number Theory, The Classical Basis*, Graduate Texts in Mathematics. 164. New York, NY: Springer (1996)

[Pr] A.Prestel, *Einführung in die Mathematische Logik und Modelltheorie*, Vieweg Studium, 60. Aufbaukurs Mathematik. Braunschweig/Wiesbaden: Friedr. Vieweg & Sohn (1986)

[Pr2] A.Prestel,C.Delzell, *Positive Polynomials. From Hilbert's 17th problem to real algebra* Springer Monographs in Mathematics. Berlin: Springer(2001)

[Re] B.Reznick, *Sums of Even Powers of Real Linear Forms*,Mem. Am. Math. Soc. 463, (1992)

[Ti] V.Timofte, *On the positivity of symmetric polynomial functions. I: General results* J. Math. Anal. Appl. 284, No.1, 174-190 (2003)

Erklärung

1. Ich versichere hiermit, dass ich die vorliegende Arbeit mit dem Thema:

   Positivität symmetrischer Polynome

   selbstständig verfasst und keine anderen Hilfsmittel als die angegebenen benutzt habe. Die Stellen, die anderen Werken dem Wortlaut oder dem Sinne nach entnommen sind, habe ich in jedem einzelnen Falle durch Angaben der Quelle, auch der benutzten Sekundärliteratur, als Entlehnung kenntlich gemacht.

   Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

2. Diese Arbeit wird nach Abschluss des Prüfungsverfahrens der Universitätsbibliothek Konstanz übergeben und ist durch Einsicht und Ausleihe somit der Öffentlichkeit zugänglich. Als Urheber der anliegenden Arbeit stimme ich diesem Verfahren zu/~~nicht zu~~*.

Konstanz, den

(Unterschrift)

*Nichtzutreffendes bitte streichen.