Leopold-Franzens Universität Innsbruck
Fakultät für Mathematik, Informatik und Physik

Institut für Mathematik

Arbeitsgruppe Algebra

Bachelorarbeit

zur Erreichung des akademischen Grades

Bachelor of Science

Numerische irreduzible Zerlegung Algebraischer Varietäten

von
Noah Kleinschmidt
(Matr.-Nr.: 11924534)

Submission Date: 14. Juni 2023
Supervisor: Tim Netzer

Eidestattliche Erklärung

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht. Die vorliegende Arbeit wurde bisher in gleicher oder ähnlicher Form noch nicht als Magister-/Master-/Diplomarbeit/Dissertation eingereicht.

Ort und Datum: Innsbruck 14.06.2023

Unterschrift:

Einleitung

Das Teilgebiet der algebraischen Geometrie beschäftigt sich mit der Analyse und Beschreibung von Nullstellenmengen polynomialer Gleichungssysteme, den sogenannten Varietäten. Um solche Varietäten besser studieren zu können, ist es oft von Vorteil die Varietät in kleinere Untervarietäten zu zerlegen. Dabei ist die Irreduzible Zerlegung von besonderer Wichtigkeit, da sie gewissermaßen eine Zerlegung in kleinstmögliche Untervarietäten liefert.
In [1] und [2] wird ein numerischen Algorithmus vorgestellt, der zu einem gegebenen polynomialen Gleichungssystem über den komplexen Zahlen, wesentliche Informationen über die irreduzible Zerlegung bereitstellt, wie Anzahl der Komponenten, Dimension und Grad der Komponenten sowie Zugehörigkeit eines Punktes zu einer Komponente. Im Gegensatz zu vielen der bekannteren Algorithmen aus dem Feld der algorithmischen Algebra verzichtet dieser Algorithmus komplett auf die Berechnung von Gröbnerbasen, die numerisch instabil ist. Stattdessen basiert der Algorithmus auf Wahrscheinlichkeit 1 Überlegungen, Homotopie-Verfahren, sowie sogenannte Witness-Sets, die Sample der zugehörigen irreduziblen Komponenten enthalten. Das Ziel dieser Arbeit ist es, die wesentlichen Resultate dieser Werke zusammenzufassen und eine einfach verständliche Beschreibung der Funktionsweise des besagten Algorithmus zu liefern. Dazu werde ich wie folgt Vorgehen:
Im ersten Abschnitt werde ich einige grundlegende Definitionen und Sätze der algebraischen Geometrie vorstellen. Wir werden affine und projektive algebraische Varietäten kennenlernen, den Begriff einer generischen Eigenschaft definieren und uns mit der Dimension sowie dem Grad algebraischer Varietäten beschäftigen.
Im zweiten Abschnitt werde ich Homotopie-Verfahren zunächst allgemein vorstellen und anschließend näher auf zwei konkrete Homotopie-Verfahren eingehen, die gewissermaßen das Fundament des Algorithmus bilden.
Der dritte Abschnitt beschäftigt sich mit dem Herzstück des Algorithmus. Ich erkläre wie wir unsere sogenannten Witness-Sets in drei Schritten unter Verwendung von Homotopie-Verfahren konstruieren können. Witness-Sets sind Mengen bestimmter Sample Punkte jeder Komponente, und wir können aus diesen alle Informationen über die irreduzible Zerlegung unserer Varietät , die uns der Algorithmus liefert, konstruieren. Im vierten und letzten Abschnitt beschreibe ich, wie man aus den Witness-Sets diese Informationen über die Irreduzible Zerlegung der Varietät konstruieren kann.

Inhaltsverzeichnis

1 Grundlagen

Im Folgenden bezeichnet K einen algebraisch abgeschlossenen Körper mit Charakteristik 0, wir können uns stets einfach $K = \mathbb{C}$ denken, da wir in folgenden Abschnitten sowieso stets nur die komplexen Zahlen betrachten.

1.1 Algebraische Varietäten

Der folgende Abschnitt fasst einige Grundlagen der algebraischen Geometrie zusammen, dabei orientiert sich dieser Abschnitt an [3] und [4, Kapitel 2 und 3].

Definition 1.1.1 (Affine algebraische Varietät)**.** *Sei $V \subseteq K^n$, so dass $V = \{a \in K^n : \forall p \in M : p(a) = 0\}$ für ein $M \subseteq K[x]$ und $x = (x_1, ..., x_n)$, so heißt V eine affine algebraische Varietät*
Zu einer gegebenen Menge $M \subseteq K[x]$ definieren wir $\mathcal{V}(M) := \{a \in K^n : \forall p \in M : p(a) = 0\}$
Für endliche Mengen $\{p_1, ..., p_n\}$ lassen wir in der Regel die Mengenklammern weg und schreiben $\mathcal{V}(p_1, ..., p_n)$ für $\mathcal{V}(\{p_1, ..., p_n\})$

Bemerkung 1.1.2. *Sei $I = (M) \subseteq K[x]$ das von M erzeugte Ideal dann gilt offensichtlich: $\mathcal{V}(M) = \mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, wobei $\sqrt{I}$ das Radikal von I bezeichnet*
Da $K[x]$ noethersch ist, ist jedes Ideal endlich erzeugt und für jedes Ideal I ist $\mathcal{V}(I) = \mathcal{V}(p_1, ..., p_m)$ mit $p_1, ..., p_n \in K[x]$. Somit kann M stets endlich gewählt werden

Definition 1.1.3 (Verschwindeideal)**.** *Sei $V \subseteq K^n$, dann heißt $\mathcal{I}(V) := \{p \in K[x] : \forall a \in V : p(a) = 0\}$ das Verschwindeideal von V. Offensichtlich ist dies tatsächlich ein Ideal in $K[x]$*

Satz 1.1.4. *Sei $V \subseteq K^n$, dann ist V eine Varietät, genau dann wenn $V = \mathcal{V}(\mathcal{I}(V))$.*

Beweis. "$\Leftarrow$": ist klar
"$\Rightarrow$": Offensichtlich gilt für eine Varietät $V \subseteq K^n$, dass $V \subseteq \mathcal{V}(\mathcal{I}(V))$, weiter existiert ein Ideal $I \subseteq K[x]$ mit $V = \mathcal{V}(I)$, nun gilt offensichtlich $I \subseteq \mathcal{I}(V)$, damit gilt dann auch $V = \mathcal{V}(I) \supseteq \mathcal{V}(\mathcal{I}(V))$ □

Satz 1.1.5 (Hilberts Nullstellensatz, idealtheoretisch)**.** *Sei $I \subseteq K[x]$ ein Ideal, dann gilt: $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$*

Beweis. Offensichtlich gilt $\mathcal{I}(\mathcal{V}(I)) \supseteq \sqrt{I}$. Für $0 \neq p \in \mathcal{I}(\mathcal{V}(I))$ betrachten wir nun das Ideal $J = (I, tp-1) \subseteq K[t, x]$. Nun gilt $p \equiv 0$ auf I und daher $\mathcal{V}(J) = \varnothing$. Nach der geometrischen Form des Hilbertschen Nullstellensatzes gilt somit $J = K[t, x]$. Daher existieren $a, b_i \in K[t, x]$ und $p_i \in I$, so dass

$$1 = a(tp - 1) + \sum_i b_i p_i.$$

Substituieren wir nun p^{-1} für t und multiplizieren oft genug mit p dass alle Nenner verschwinden, so fällt der erste Summand weg, und wir erhalten

$$p^k = \sum_i \left(b_i p^{k_i}\right) p_i \in I,$$

also $p \in \sqrt{I}$. □

Satz 1.1.6 (Schnitte von Varietäten)**.** *Beliebige Schnitte von Varietäten sind Varietäten*

Beweis. Sei I eine Indexmenge und $(X_i)_{i\in I}$ eine Menge von Varietäten, und $(J_i)_{i\in I}$ eine Menge von Idealen mit $\forall i \in I : X_i = \mathcal{V}(J_i)$ dann gilt

$$\bigcap_{i\in I} X_i = \mathcal{V}\left(\bigcup_{i\in I} J_i\right)$$

ist eine Varietät □

Satz 1.1.7 (Vereinigung von Varietäten)**.** *Seien $X, Y \subseteq K^n$ Varietäten und $I, J \subseteq K[x]$ Ideale, so dass $X = \mathcal{V}(I)$ und $Y = \mathcal{V}(J)$ dann gilt $X \cup Y = \mathcal{V}(IJ)$*

Beweis. "$\subseteq$": sei $x \in X = \mathcal{V}(I)$, dann gilt $\forall p \in I : p(x) = 0$. Sei nun $q \in IJ$ dann gilt $q = \sum_{i=1}^{k} p_i q_i$ mit $p_i \in I, q_i \in J$. Damit gilt

$$q(x) = \sum_{i=1}^{k} p_i(x)q_i(x) = \sum_{i=1}^{k} 0 q_i(x) = 0, \text{ also } x \in \mathcal{V}(IJ).$$

Für $x \in Y = \mathcal{V}(J)$ analog.
"$\supseteq$": sei $x \in \mathcal{V}(IJ)$ und o.B.d.A $x \notin X = V(I)$. Nun gilt für $p \in I$ und $q \in J : pq \in IJ$ und somit $pq(x) = p(x)q(x) = 0$ und somit $q(x) = 0$. Also ist $x \in Y = \mathcal{V}(J)$ □

Satz 1.1.8. *Die Abbildung $\mathcal{I} : V \mapsto \mathcal{I}(V)$ ist eine inklusionsumkehrende Bijektion zwischen der Menge der affinen Varietäten und der Menge der Radikalideale in $K[x]$. Die Umkehrabbildung ist gegeben durch $\mathcal{V} : I \mapsto \mathcal{V}(I)$*

Beweis. Dass die Abbildung inklusionsumkehrend ist, ist klar. Um zu zeigen das die Abbildung bijektiv ist zeigen wir das $\mathcal{V}$ tatsächlich eine Umkehrabbildung ist. Dies folgt jedoch direkt aus Satz 1.1.4 und Satz 1.1.5 □

Bemerkung 1.1.9. *Insbesondere entsprechen minimale Varietäten den maximalen Idealen und maximale Varietäten minimalen Idealen*

Definition 1.1.10 (Zariski-Topologie)**.** *Die Zariski-Topologie auf K^n ist definiert durch die Bedingung, dass die abgeschlossenen Mengen genau den algebraischen Varietäten entsprechen.*

Satz 1.1.11. *Die Zariski-Topologie ist tatsächlich eine Topologie.*

Beweis.
- z.z. $\varnothing$ ist offen: $\varnothing = (K^n)^c$ und $K^n = \mathcal{V}(0)$ ist Varietät, also ist $\varnothing$ offen
- z.z. Beliebige Vereinigung offener Mengen ist offen: Folgt nach De Morgan und Satz 1.1.6
- z.z. endlicher Schnitt offener Mengen ist offen: Folgt nach De Morgan und Satz 1.1.7

□

Definition 1.1.12 (irreduzibel)**.** *Sei $T \neq \varnothing$ ein topologischer Raum. Dann heißt T irreduzibel, falls für $A, B \subseteq T$ abgeschlossen gilt: $A \cup B = T \Rightarrow A = T \vee B = T$. Ansonsten nennt man T reduzibel.*
Eine Teilmenge $M \subseteq T$ heißt irreduzibel, wenn sie irreduzibel mit der Teilraumtopologie ist.

Bemerkung 1.1.13. *Wenn wir von Irreduzibilität in bezug auf Varietäten sprechen, beziehen wir uns stets auf die Zariski-Topologie. Eine Varietät heißt genau dann irreduzibel, wenn sie keine echte Vereinigung zweier Varietäten ist.*

In der Literatur werden Varietäten oft algebraische Mengen genannt, während Varietäten dann irreduzible algebraische Mengen sind.

Satz 1.1.14 (Irreduzible Zerlegung)**.** *Jede Varietät in K^n besitzt Darstellung als Vereinigung endlich vieler irreduzibler Varietäten. Diese Darstellung ist eindeutig, da wir zusätzlich voraussetzten, dass die irreduziblen Varietäten paarweise nicht in einander enthalten sind.*

Beweis. Wir zeigen zunächst die Existenz einer solchen Zerlegung. Eine Varietät $X \subseteq K^n$ ist entweder irreduzibel oder es gibt Varietäten $Y, Z \subsetneq X$ mit $X = Y \cup Z$. Wir können nun dieses Argument induktiv auf die Komponenten anwenden und erhalten entweder das X Vereinigung endlich vieler irreduzibler Varietäten ist, oder dass eine unendliche Kette von Varietäten $X \supsetneq X_1 \supsetneq X_2 \supsetneq ...$ existiert. Nun gilt jedoch dass für Varietäten $X, Y \subseteq K^n$ gilt $X \subsetneq Y \Rightarrow \mathcal{I}(X) \supsetneq \mathcal{I}(Y)$. Somit ist die Existenz einer solchen Kette $X \supsetneq X_1 \supsetneq X_2 \supsetneq ...$ ein Widerspruch zu $K[x]$ ist noethersch.
Für die Eindeutigkeit nehmen wir an, wir hätten zwei irreduzible Zerlegungen der selben Varietät: $V_1 \cup ... \cup V_k = W_1 \cup ... \cup W_s$ wobei die Komponenten jeweils nicht paarweise ineinander enthalten sind. Wir fixieren nun einen beliebigen Index $i_0 \in [s]$. Nun gilt:

$$W_{i_0} = \left(\bigcup_{j=1}^{k} V_j \right) \cap W_{i_0} = \bigcup_{j=1}^{k} (V_j \cap W_{i_0})$$

Da W_{i_0} irreduzibel ist, existiert ein Index $j_0 \in [k]$ so dass $W_{i_0} = V_{j_0} \cap W_{i_0}$. Somit gilt $W_{i_0} \subseteq V_{j_0}$.Analog können wir ein $i_1 \in [s]$ finden, so dass $V_{j_0} \subseteq W_{i_1}$, und somit $W_{i_0} \subseteq W_{i_1}$. Da die W_i nicht paarweise ineinander enthalten sein dürfen, gilt somit $W_{i_0} = W_{i_1} = V_{j_0}$. Somit gilt für jedes $i \in [s] : \exists j \in [k] : W_i = V_j$ und wir haben die Eindeutigkeit der Zerlegung gezeigt. □

Definition 1.1.15 (Komponenten)**.** *Die irreduziblen Untervarietäten in der irreduziblen Zerlegung einer Varietät nennen wir die Komponenten dieser Varietät.*

Lemma 1.1.16. *$\mathbb{C}^n$ ist irreduzibel bezüglich der Zariski-Topologie*

Beweis. Wir beweisen die Aussage per Widerspruch. Seien also $V, W \subsetneq \mathbb{C}^n$ Varietäten mit $V \cup W = \mathbb{C}^n$
Nun besitzen V, W Darstellungen $V = \mathcal{V}(p_1, ..., p_r)$, $W = \mathcal{V}(q_1, ..., q_s)$ mit $0 \neq p_1, ..., p_r, q_1, ..., q_s \in \mathbb{C}[x]$. Nun gilt für $0 \neq P := p_1 \cdots p_r$, $0 \neq Q = q_1 \cdots q_s$, dass $V \subseteq \mathcal{V}(P)$, $W \subseteq \mathcal{V}(Q)$ und $\mathbb{C}^n = \mathcal{V}(P) \cup \mathcal{V}(Q) = \mathcal{V}(PQ)$. Nun ist $PQ \neq 0$ und wir erhalten unseren Widerspruch, wenn wir zeigen, dass für ein Polynom $f \neq 0$ es stets ein $a \in \mathbb{C}^n$ gibt mit $f(a) \neq 0$. Wir zeigen das per Induktion über die Dimension m:
IA: $m = 1$: ein Nicht-Nullpolynom in einer Variablen hat bekanntlich nur endlich viele Nullstellen, somit unendlich viele Punkte, wo es nicht Null ist.
IS: $m \to m+1$: Wir schreiben f als $f = \sum_{i=0}^{\deg(f)} \tilde{f}_i(x_1, ..., x_m) x_{m+1}^i$, wobei mindestens eines der $\tilde{f}_i \neq 0$. Nach Induktionsvorraussetzung gibt es nun ein $a \in \mathbb{C}^n$ und ein $i \in [\deg(f)]$ mit $\tilde{f}_i(a) \neq 0$. Somit ist $f(a, x_{m+1})$ ein nicht Nullpolynom in einer Variablen. Somit gibt es ein $b \in \mathbb{C}$ so dass $f(a, b) \neq 0$ □

Satz 1.1.17. *Sei $V \subsetneq K^n$ eine affine Varietät, dann gilt V irreduzibel $\Leftrightarrow \mathcal{I}(V) \subseteq K[x]$ prim*

Beweis. „⇒“: Sei V eine irreduzible Varietät. Dann gilt wegen $V \neq \varnothing$, dass $\mathcal{I}(V) \neq K[x]$ und wegen $V \neq K^n$, dass $\mathcal{I}(V) \neq \{0\}$. Sei nun $p, q \in K[x]$ mit $pq \in \mathcal{I}(V)$, dann gilt $\forall a \in V : pq(a) = 0$ und somit $\forall a \in V : p(a) = 0 \vee q(a) = 0$. Damit gilt $V \subseteq \mathcal{V}(p) \cup \mathcal{V}(q)$, wegen der Irreduzibilität von V gilt nun o.B.d.A. (sonst Rollen von p und q tauschen) $V \subseteq \mathcal{V}(p)$ und somit $p \in \mathcal{I}(V)$. Also ist $\mathcal{I}(V)$ prim
„⇐“: Sei nun $\mathcal{I}(V)$ ein Primideal und $V = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$ mit $I_1, I_2 \subseteq K[x]$ sind Ideale. Nun gilt nach Satz

1.1.7 $V = \mathcal{V}(I_1 I_2)$ und somit $I_1 I_2 \subseteq \mathcal{I}(V)$. Da $\mathcal{I}(V)$ prim gilt nun o.B.d.A. $I_1 \subseteq \mathcal{I}(V)$ damit gilt weiter $V \subseteq \mathcal{V}(I_1)$ bzw. $V = \mathcal{V}(I_1)$. Somit ist V irreduzibel. □

Bemerkung 1.1.18. *Zusammen mit Satz 1.1.8 haben wir damit eine Entsprechung von irreduziblen Varietäten und Primidealen. Insbesondere entsprechen die irreduziblen Komponenten einer Varietät V den minimalen Primidealen über $\mathcal{I}(V)$.*

Definition 1.1.19 (Koordinatenring)**.** *Sei V eine affine Varietät, dann nennen wir $K[V] := K[x]/\mathcal{I}(V)$ den affinen Koordinatenring von V.*

Bemerkung 1.1.20. *Wir können die Elemente von $K[V]$ als polynomiale Funktionen auf V betrachten, denn für zwei Polynome $p, q \in K[x]$ gilt $p|_V = q|_V \Leftrightarrow (p-q)|_V = 0 \Leftrightarrow p - q \in \mathcal{I}(V)$.*
Weiter entsprechen die Ideale in $K[V]$ den Idealen in $K[x]$, die $\mathcal{I}(V)$ enthalten. Selbiges gilt für Radikal- und Primideale. Somit erhalten wir analog zu Satz 1.1.8 und Bemerkung 1.1.18 eine Zuordnung von Radikalidealen in $K[V]$ und Untervarietäten von V bzw. von Primidealen in $K[V]$ und irreduziblen Untervarietäten von V. Insbesondere entsprechen die irreduziblen Komponenten von V den minimalen Primidealen von $K[V]$.

1.2 Projektive Varietäten

Projektive Räume und Varietäten werden im Rest dieser Arbeit eine große Rolle spielen, da sie viele Beweise immens vereinfachen.
Ich werde im folgenden Grundwissen über projektive Räume vorraussetzen und nur kurz auf die Notation eingehen bevor ich mit dem Thema der projektiven Varietäten beginne.
Die folgenden Ausführungen orientieren sich an [3].

Bemerkung 1.2.1 (Notation)**.** *Für den n-dimensionalen projektiven Raum über K schreiben wir $\mathbb{P}^n(K) := \mathbb{P}(K^{n+1})$, falls klar ist welcher Körper gemeint ist. Beispielsweise im zweiten Teil dieser Arbeit wenn $K = \mathbb{C}$ fixiert ist, schreiben wir häufig auch bloß $\mathbb{P}^n$ für $\mathbb{P}^n(K)$.*
Elemente von $\mathbb{P}^n(K)$ schreiben wir in homogenen Koordinaten, für $0 \neq (a_0, ..., a_n) \in K^{n+1}$ schreiben wir $(a_0 : ... : a_n) = [(a_0, ...a_n)] = K(a_0, ..., a_n) \in \mathbb{P}^n(K)$.
Weiter sei $\underline{x} = (x_0, ..., x_n)$ und somit $K[\underline{x}]$ der Polynomring über K in $n+1$ Variablen

Definition 1.2.2 (Homogenes Polynom)**.** *Ein Polynom $p \in K[\underline{x}]$ heißt homogen (vom grad g) falls p Summe von Monomen des Grades g ist.*

Bemerkung 1.2.3. *Homogene Polynome vertragen sich gut mit projektiven Räumen, da für ein homogenes Polynom $p \in K[\underline{x}]$ sowie $a \in K^{n+1}, \lambda \in K$ gilt:*

$$\big(p(\lambda a) = \lambda^{\deg(p)} p(a)\big) \text{ und deshalb } (p(a) = 0 \Leftrightarrow p(Ka) = 0)$$

Somit können wir sinnvoll definieren, wann ein homogenes Polynom für ein Element des n-dimensionalen projektiven Raumes Null ist. Für $[a] \in \mathbb{P}^n(K)$ und $p \in K[\underline{x}]$ homogen gilt:

$$p([a]) = 0 :\Leftrightarrow p(a) = 0.$$

Ein allgemeines $p \in K[\underline{x}]$ von Grad d besitzt eine Zerlegung $p = p_0 + ... + p_d$ mit für alle $i \in \{0, ..., d\}$ gilt p_i ist homogen und $\deg(p_i) = i$. Somit können wir sinnvoll Nullstellen im projektiven Raum definieren: für

$[a] \in \mathbb{P}^n(K)$*:*

$$p([a]) = 0 :\Leftrightarrow p_0(a) = ... = p_d(a) = 0.$$

Hiermit können wir nun projektive Varietäten definieren.

Definition 1.2.4 (Projektive Varietäten, Verschwindungsideal)**.** *Sei $M \subseteq K[\underline{x}]$ und $\varnothing \neq V \subseteq \mathbb{P}^n(K)$, dann heißt eine Menge der Form $\mathcal{V}_+(M) := \{a \in \mathbb{P}^n(K) : \forall p \in M : p(a) = 0\}$ projektive Varietät.*
Weiter heißt eine Menge der Form $\mathcal{I}_+(V) := \{p \in K[\underline{x}] : \forall a \in V : p(a) = 0\}$ Verschwindungsideal von V.

Bemerkung 1.2.5. *Offensichtlich können wir eine projektive Varietät stets durch homogene Polynome in $K[\underline{x}]$ definieren.*

Definition 1.2.6 (homogene Ideale)**.** *Ein Ideal $I \subseteq K[\underline{x}]$ heißt homogen genau dann, wenn I von homogenen Polynomen erzeugt ist*

Bemerkung 1.2.7. *Wir sehen leicht, dass das Verschwindungsideal einer projektiven Varietät homogen ist.*

Bemerkung 1.2.8. *Viele Sätze lassen sich analog zum affinen Fall beweisen, so gilt für eine Indexmenge I und homogene Ideale $(J_i)_{i\in I}$:*

$$\forall i,j \in I : \mathcal{V}_+(J_i) \cup \mathcal{V}_+(J_j) = \mathcal{V}_+(J_iJ_j) \qquad \wedge \qquad \bigcap_{i\in I} \mathcal{V}_+(J_i) = \mathcal{V}_+\left(\bigcup_{i\in I} J_i\right) = \mathcal{V}_+\left(\sum_{i\in I} J_i\right).$$

Damit folgt, dass wir analog zum affinen Fall die Zariski-Topologie auf $\mathbb{P}^n(K)$ definieren können.
Weiter gilt offensichtlich, dass für eine projektive Varietät $V \subseteq \mathbb{P}^n(K)$ gilt $\mathcal{V}_+(\mathcal{I}_+(V)) = V$.

Definition 1.2.9 (Zariski-Topologie)**.** *Die Zariski-Topoogie ist eine Topologie auf $\mathbb{P}^n(K)$ die dadurch definiert ist dass die abgeschlossenen Mengen den projektiven Varietäten entsprechen.*

Satz 1.2.10. *Die Zariski-Topologie ist eine Topologie auf $\mathbb{P}^n(K)$.*

Beweis. Analog zum affinen Fall (Satz 1.1.11). □

Konstruktion 1.2.11. *für $i \in \{0,...,n\}$ betrachten wir die Menge $\mathcal{D}_i = \mathbb{P}^n(K)\backslash\mathcal{V}_+(\{x_i\})$ dann ist*

$$\phi_i : \mathcal{D}_i \to K^n : (a_0 : ... : a_n) \mapsto \left(\frac{a_0}{a_i}, ..., \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, ... \frac{a_n}{a_i}\right)$$
$$(b_0 : ... : b_{i-1} : 1 : b_i : ... : b_n) \leftarrow\!\shortmid (b_0, ..., b_{i-1}, b_i, ..., b_n)$$

eine Bijektion.
Nun möchten wir vergleichbares auf algebraischer Ebene mit den Polynomen tun, die unsere Varietäten definieren.
Sei $0 \neq p \in k[x]$, dann definieren wir die Homogensierung von p mittels x_0 als:

$$p^h := x_0^{\deg(p)} p\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right) \in K[\underline{x}].$$

Das ist offensichtlich ein homogenes Polynom.
Umgekehrt ist die Dehomogenisierung eine Polynomes $q \in K[\underline{x}]$ mittels x_0 definiert als:

$$\tilde{q} := q(1, x_1, ..., x_n) \in K[x]$$

Bemerkung 1.2.12. *Natürlich können wir auch bezüglich einer anderen Variable (de-)homogenisieren. Wir werden sehen, dass sich die Wahl, mit x_0 zu (de-)homogenisieren gut mit ϕ_0 verträgt, was wir im Folgenden meist betrachten werden.*
Offensichtlich gilt für $p \in K[x]$ das $\tilde{p^h} = p$ und für $q \in K[\underline{x}] : x_0^m \left(\tilde{q}\right)^h = q$ für ein $m \in \mathbb{N}$, diese m ist $\neq 0$ genau dann, wenn der Grad von q beim Homogenisieren sinkt bzw. wenn in jedem Monom höchsten Grades, welches in q vorkommt, x_0 auftritt.

Definition 1.2.13. *Sei $I \subseteq K[x]$ ein Ideal, dann heißt $I^h := \left(\{p^h : p \in I\}\right) \subseteq K[\underline{x}]$ die Homogenisierung von I.*

Bemerkung 1.2.14. *Offensichtlich ist I^h ein homogenes Ideal.*

Satz 1.2.15. *Sei $I \subseteq K[x]$ ein Ideal und $q \in I^h$, dann gilt $\tilde{q} \in I$.*

Beweis. Da $q \in I^h$ ist q endliche Idealkombination homogenisierter Polynome aus I, und da die Dehomogenisierung linear ist und für $p \in K[x]$ stets $\tilde{p^h} = p$ gilt, ist $\tilde{q} \in I$. □

Satz 1.2.16. *Sei $p \in K[x]$ und $q \in K[\underline{x}]$ homogen, dann gilt:*

$$\phi_0^{-1}(\mathcal{V}(p)) = \mathcal{V}_+(p^h) \cap \mathcal{D}_0 \ \wedge \ \phi_0(\mathcal{V}_+(q) \cap \mathcal{D}_0) = \mathcal{V}(\tilde{q}).$$

Beweis.

$$\begin{aligned}
\phi_0^{-1}(\mathcal{V}(p)) &= \left\{(a_0 : ... : a_n) \in \mathbb{P}^n(K) : a_0 \neq 0,\, p\left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) = 0\right\} \\
&= \left\{(a_0 : ... : a_n) \in \mathbb{P}^n(K) : a_0 \neq 0,\, a_0^{\deg(p)} p\left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) = 0\right\} \\
&= \left\{(a_0 : ... : a_n) \in \mathbb{P}^n(K) : a_0 \neq 0,\, p^h\left(a_0, a_1, ..., a_n\right) = 0\right\} = \mathcal{V}_+(p^h) \cap \mathcal{D}_0 \\
\phi_0(\mathcal{V}_+(q) \cap \mathcal{D}_0) &= \left\{\left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) \in K^n : a_0 \neq 0,\, q(a_0, a_1, ..., a_n) = 0\right\} \\
&= \left\{\left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) \in K^n : a_0 \neq 0,\, a_0^{\deg(p)} q\left(1, \frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) = 0\right\} \\
&= \{(b1, ..., b_n) \in K^n : \tilde{q}(b_1, ..., b_n) = 0) = \mathcal{V}(\tilde{q})
\end{aligned}$$

□

Lemma 1.2.17. *sei $I \subseteq K[x]$ ein Ideal, dann gilt:*

$$\phi_0^{-1}(\mathcal{V}(I)) = \mathcal{V}_+(I^h) \cap \mathcal{D}_0.$$

Beweis. Mit 1.2.16 gilt:

$$\phi_0^{-1}(\mathcal{V}(I)) = \phi_0^{-1}\left(\bigcap_{p \in I} \mathcal{V}(p)\right) = \bigcap_{p \in I} \phi_0^{-1}(\mathcal{V}(p)) = \mathcal{D}_0 \cap \bigcap_{p \in I} \mathcal{V}_+(p^h) = \mathcal{D}_0 \cap \mathcal{V}_+(\{p^h : p \in I\}) = \mathcal{D}_0 \cap \mathcal{V}_+(I^h).$$

□

Satz 1.2.18. *ϕ_0 ein Homöomorphismus bezüglich der Zariski-Topologien.*

Beweis. Wir wissen, dass ϕ_0 bijektiv ist. Da $K[x], K[x]$ noethersch sind, ist jede Varietät endlicher Schnitt von Nullstellenmengen von Polynomen, im projektiven Fall sogar von homogenen Polynomen. Somit folgt aus Satz 1.2.16, dass Bilder und Urbilder abgeschlossener Mengen abgeschlossen sind, somit ist ϕ_0 ein Homöomorphismus. □

Bemerkung 1.2.19. *Selbiges gilt natürlich für alle ϕ_i mit $i \in \{0, ..., n\}$*

Satz 1.2.20. *Sei $I \subseteq K[x]$ ein Ideal dann gilt $\sqrt{I^h} = \sqrt{I}^h$.*

Beweis. "$\subseteq$": sei $p \in \sqrt{I^h}$, dann existiert ein $r \in \mathbb{N}$, so dass:

$$p^r \in I^h \overset{1.2.15}{\Longrightarrow} (\tilde{p})^r = \tilde{p^r} \in I \Rightarrow \tilde{p} \in \sqrt{I} \Rightarrow \tilde{p}^h \in \sqrt{I}^h \Rightarrow p \in \sqrt{I}^h.$$

"$\supseteq$": sei nun $p \in \sqrt{I}^h$, dann existiert ein $r \in \mathbb{N}$, so dass:

$$\tilde{p} \in \sqrt{I} \Rightarrow \tilde{p}^r \in I \Rightarrow (\tilde{p}^r)^h = \left(\tilde{p}^h\right)^r \in I^h \Rightarrow \tilde{p}^h \in \sqrt{I^h} \Rightarrow p \in \sqrt{I^h}.$$

□

Definition 1.2.21 (Projektiver Abschluss)**.** *Sei $V \subseteq K^n$ eine Varietät, dann heißt die projektive Varietät $\overline{V} := \overline{\phi_o^{-1}(V)} \subseteq \mathbb{P}^n$ der projektive Abschluss von V. Dabei ist der Abschluss der Abschluss bezüglich der Zariski-Topologie.*

Bemerkung 1.2.22. *Nach Konstruktion 1.2.11 können wir K^n mit $\mathcal{D}_0$ identifizieren. Somit ist K^n in $\mathbb{P}^n$ eingebettet, und wir tun im Weiteren einfach so, als wäre $K^n \subseteq \mathbb{P}^n$. Weiter induziert die Zariski-Topologie auf $\mathbb{P}^n$, nach Satz 1.2.18, genau die Zariski-Topologie auf K^n, somit gilt für eine Varietät $V \subseteq K^n$, dass $\overline{V} \cap K^n = V$.*
Wir nennen die Punkte von $\mathbb{P}^n \backslash K^n$ auch die unendlich fernen Punkte von $\mathbb{P}^n$.

Satz 1.2.23. *Seien X, Y affine Varietäten dann gilt $\overline{X} \cup \overline{Y} = \overline{X \cup Y}$.*

Beweis. Offensichtlich gilt $\overline{X \cup Y} \subseteq \overline{X} \cup \overline{Y}$, nun gilt jedoch auch $\overline{X} \subseteq \overline{X \cup Y}$ und $\overline{Y} \subseteq \overline{X \cup Y}$, und somit gilt:

$$\overline{X} \cup \overline{Y} = (\overline{X} \cap \overline{X \cup Y}) \cup (\overline{Y} \cap \overline{X \cup Y}) \subseteq \overline{X \cup Y}.$$

□

Satz 1.2.24 (Eigenschaften des projektiven Abschluss)**.** *Sei $I \subseteq K[x]$ ein Ideal dann gilt:*

$$\overline{\mathcal{V}(I)} = \mathcal{V}_+(I^h) \wedge \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right) = \sqrt{I^h} = \sqrt{I}^h = \mathcal{I}(\mathcal{V}(I))^h.$$

Beweis. Wir beweisen die zweite Aussage, die erste folgt mit Bemerkung 1.2.8 unmittelbar aus der zweiten. Wir betrachten ein $p \in \sqrt{I} = \mathcal{I}(\mathcal{V}(I))$, dann gilt nach Lemma 1.2.17 $p^h \equiv 0$ auf $\phi_0^{-1}(\mathcal{V}(I))$. Damit muss nun auch $p^h \equiv 0$ auf $\overline{\phi_o^{-1}(\mathcal{V}(I))} = \overline{\mathcal{V}(I)}$, da andernfalls $\overline{\mathcal{V}(I)} \cap \mathcal{V}_+(p^h)$ eine projektive Varietät wäre, die echt in $\overline{\phi_o^{-1}(\mathcal{V}(I))}$ enthalten ist, und die selber $\phi_o^{-1}(\mathcal{V}(I))$ enthält. Somit gilt $p^h \in \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right)$, und da $\sqrt{I}^h$ von homogenisierten Polynomen aus I erzeugt wird, gilt somit auch $\sqrt{I}^h \subseteq \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right)$.
Für die andere Richtung betrachten wir ein $g \in \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right)$. Wir können nun o.B.d.A. g homogen annehmen (falls g nicht homogen ist, so ist es Linearkombination endlich vieler homogener Elemente, und wir

betrachten diese). Wir heben nun möglichst viele x_0 aus g heraus, schreiben also $g = x_0^m g_1$ mit $m \in \mathbb{N}$ und $x_0 \nmid g_1$. Nun gilt $g_1 \equiv 0$ auf $\overline{\mathcal{V}(I)} \cap \mathcal{D}_0$ und somit nach Satz 1.2.16 $\tilde{g_1} \equiv 0$ auf $\mathcal{V}(I)$ und daher wiederum $\tilde{g_1} \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. Wegen $x_0 \nmid g_1$ gilt $g_1 = \tilde{g_1}^h$. Also $g_1 \in \sqrt{I}^h$ und somit auch $g \in \sqrt{I}^h$, und da g beliebig war, auch $\sqrt{I}^h \supseteq \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right)$. Die anderen Gleichungen haben wir bereits bewiesen. □

Satz 1.2.25. *Sei $I, J \subseteq K[x]$ Radikalideale mit $I \subsetneq J$, dann gilt auch $I^h \subsetneq J^h$.*

Beweis. Da $I \subsetneq J$, existiert ein $p \in J \backslash I$. Wir zeigen $p^h \notin I^h$ per Widerspruch. Wir nehmen also an, $p^h \in I^h$, dann existieren $f_i \in K[\underline{x}], q_i \in I$, so dass

$$p^h = \sum_{i=1}^{k} f_i q_i^h \Rightarrow p = \tilde{p^h} = \widetilde{\sum_{i=1}^{k} f_i q_i^h} = \sum_{i=1}^{k} \widetilde{f_i q_i^h} = \sum_{i=1}^{k} \tilde{f}_i q_i.$$

Da nun für alle i gilt $\tilde{f}_i \in K[x], q_i \in I$, folgt $p \in I$, und wir haben unseren Widerspruch. □

Bemerkung 1.2.26. *Aus dem Satz folgt unmittelbar, dass die Inklusionseigenschaften von Varietäten unter dem Bilden des projektiven Abschlusses erhalten bleiben.*

Satz 1.2.27. *Sei $V \subseteq K^n$ eine irreduzible Varietät. Dann ist auch $\overline{V} \subseteq \mathbb{P}^n$ irreduzibel .*

Beweis. Wir können K^n in $\mathbb{P}^n$ einbetten, dabei ist die Zariski-Topologie auf K^n nach Satz 1.2.18 die von der Zariski-Topologie auf $\mathbb{P}^n$ induzierte Topologie.
Seien nun $A, B \subseteq \mathbb{P}^n$ abgeschlossen mit $A \cup B = \overline{V}$, dann gilt $V \subseteq A \cup B$ und daraus folgt wegen der Irreduzibilität von V in K^n und der Verträglichkeit der Topologien, dass o.B.d.A. $V \subseteq A$ (ansonsten Rollen von A und B tauschen). Da nun A bereits abgeschlossen ist, gilt auch $\overline{V} \subseteq A$ und somit $\overline{V} = A$ also $\overline{V}$ irreduzibel. □

Bemerkung 1.2.28. *Somit kriegen wir nach Satz 1.2.23 durch Homogenisieren der Komponenten einer Varietät eine irreduzible Zerlegung ihres projektiven Abschlusses.*

1.3 Stochastische Algorithmen und generische Eigenschaften

Ein stochastischer Algorithmus ist ein Algorithmus, bei dem mindestens einmal etwas zufällig gewählt wird, und der nur für eine Nullmenge unter den Auswahlmöglichkeiten nicht das richtige Ergebniss liefert. Ein einfaches Beispiel ist: wir wollen überprüfen ob ein komplexes Polynom in einer Variablen dem 0-Polynom entspricht. Dazu können wir einfach eine zufällige Stelle hernehmen und überprüfen, ob das Polynom an dieser Stelle 0 ist. Falls es Null ist schließen wir, dass das Polynom das 0-Polynom ist, andernfalls, dass es ungleich 0 ist. Dieser Algorithmus gibt mit Wahrscheinlichkeit 1 ein richtiges Ergebnis, da ein Nicht-Nullpolynom nur endlich viele Nullstellen hat und somit die Wahrscheinlichkeit, genau eine von diesen zu wählen, 0 ist. Nun ist dies jedoch die einzige Möglichkeit, wie der Algorithmus ein falsches Ergebniss liefert.
Dabei haben wir unterschlagen, dass durch Rundungsfehler eine Reihe von Problemen auftauchen können, weswegen ein stochastischer Algorithmus nicht mehr mit Wahrscheinlichkeit 1 konvergiert. Denken wir an das Beispiel zurück, zum Einen wählt der Computer nicht aus unendlich vielen Punkten, sondern aufgrund der endlichen Maschinengenauigkeit bloß aus sehr vielen aus. Weiter müssen wir eine Schranke bestimmen, ab wann der Wert der Funktionsauswertung als 0 gewertet werden soll. Es werden also durch die endliche Maschinengenauigkeit aus endlich vielen „Problempunkten“in einer unendlichen Grundmenge,

kleine Problembereiche in einer diskreten Grundmenge. Uns wird im Verlauf dieser Arbeit nichts anderes übrigbleiben, als zu hoffen, dass die Wahrscheinlichkeit, dass der stochastische Algorithmus das falsche Ergebnis liefert, trotzdem klein bleibt. Eine genauere Analyse mit welcher Wahrscheinlichkeit unser Algorithmus ein falsches Ergebnis liefert, werden wir nicht durchführen.
Nun möchten wir den Begriff der generischen Eigenschaft definieren und motivieren, welchen man häufig in diesem Kontext hört.

Definition 1.3.1 (generisch)**.** *Sei X eine affine oder projektive Varietät. Dann gilt eine Eigenschaft generisch auf X genau dann, wenn sie auf einer nicht leeren, offenen (bezüglich der Zariski-Topologie auf X) Teilmenge von X gilt. Die Punkte in dieser offenen Menge heißen generische Punkte.*

Satz 1.3.2. *Eine affine Varietät $X \subsetneq \mathbb{C}^n$ ist eine Lebesque Nullmenge.*

Beweis. Wir beweisen den Satz per Induktion über n:
$n = 1$: Ein Polynom in einer Variable hat nur endlich viele Nullstellen, somit ist X endlich und somit eine Lebesque Nullmenge.
$n \to n+1$:X ist Nullstellenmenge eines polynomialen Gleichungssystems $F : \mathbb{C}^{n+1} \to \mathbb{C}^m$. Nun besitzt F eine Darstellung:

$$F(x) = \sum_{i=0}^{g} \tilde{F}_i(x_1, ..., , x_n) x_{n+1}^i, \qquad g = \max_{j=1,...,m} \deg(F_j),$$

mit $\tilde{F}_1, ..., \tilde{F}_g : \mathbb{C}^n \to \mathbb{C}^m$ polynomial. Wir teilen nun $\mathbb{C}^n$ auf in $A = \mathcal{V}(\tilde{F}_1, ..., \tilde{F}_g) := \mathcal{V}(\tilde{F_{1,1}}, ..., \tilde{F_{1,m}}, ..., \tilde{F_{g,1}}, ..., \tilde{F_{g,m}}) \subseteq \mathbb{C}^n$ und A^c. Nun gilt

$$X = A \times \mathbb{C} \cup \underbrace{\{(x, y) \in \mathbb{C}^n \times \mathbb{C} : x \in A^c, y \in \mathcal{V}(F(x, \cdot)\}}_{=:B}.$$

Nach Induktionsannahme gilt $\lambda^n(A) = 0$, und mit dem Satz von Fubini $\lambda^{n+1}(A \times \mathbb{C}) = 0$. Wir zeigen nun das auch $\lambda^{n+1}(B) = 0$ gilt. Dafür verwenden wir erneut den Satz von Fubini, sowie das $\mathcal{V}(F(x, \cdot)$ endlich ist.

$$\lambda^{n+1}(B) = \int_{\mathbb{C}^{n+1}} \mathbb{1}_B \, \mathrm{d}\, \lambda^{n+1} = \int_{\mathbb{C}^n} \int_{\mathbb{C}} \mathbb{1}_B(x, y) \, \mathrm{d}\, \lambda(y) \, \mathrm{d}\, \lambda^n(x) = \int_{\mathbb{C}^n} 0 \, \mathrm{d}\, \lambda^n = 0.$$

□

Bemerkung 1.3.3. *Dieser Satz zeigt, dass ein Algorithmus, bei dem an einer Stelle etwas zufällig aus einer Menge, die mit dem $\mathbb{C}^n$ für ein $n \in \mathbb{N}$ identifiziert werden kann, gewählt wird und der für generische Wahl das richtige Ergebnis liefert ,ein Wahrscheinlichkeit 1 Algorithmus ist.*
Mit etwas mehr Aufwand können wir ein analoges Resultat für generische Teilmengen des Projektiven Raumes beweisen.

1.4 Dimension und Grad von Varietäten

Die grundlegenden Definitionen und Sätze in diesem Kapitel orientieren sich an [3, Abschnitt 5.3] sowie [5][Abschnitt 1.1].

Definition 1.4.1. *Für einen topologischen Raum T definieren wir die Dimension* $\dim(T)$ *von T als Supremum der Längen n von Ketten der Form:*

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_n \subseteq T,$$

wobei Z_i abgeschlossen und irreduzibel für alle i.
Für eine Teilmenge eines topologischen Raumes ist die Dimension als die Dimension der Teilmenge als topologischer Raum mit der induzierten Topologie definiert.
Weiter setzen wir $\dim(\varnothing) = -1$.
Für einen Ring R definieren wir $\dim(R)$ *als Supremum der Längen n von Ketten der Form:*

$$\mathbf{p}_0 \subsetneq \mathbf{p}_1 \subsetneq ... \subsetneq \mathbf{p}_n \subseteq R$$

wobei $\mathbf{p}_i$ ein Primideal von R ist für alle i.
Genauso definieren wir die Höhe $\text{height}(\mathbf{p})$ *eines Primideals $\mathbf{p}$ als Supremum der Längen von Ketten von Primidealen die in $\mathbf{p}$ enthalten sind.*

Bemerkung 1.4.2. *Die Dimension von Varietäten bezieht sich stets auf die Zariski-Topologie.*
Offensichtlich ist die Dimension einer Varietät gleich dem Maximum der Dimensionen der irreduziblen Komponenten.

Satz 1.4.3. *Sei V eine affine Varietät, dann gilt* $\dim(V) = \dim(K[V])$.

Beweis. Die irreduziblen Untervarietäten von V entsprechen den Primidealen von $K[V]$, somit liefert uns jede Kette von irreduziblen Untervarietäten von V eine Kette von Primidealen von $K[V]$ und andersrum. □

Satz 1.4.4. *Die Dimension von $\mathbb{C}^n$ als Untervarietät von $\mathbb{C}^n$ ist n.*

Beweis. [3, Korollar 5.3.10] □

Satz 1.4.5. *Die Dimension einer Varietät $V \subseteq K^n$ ist gleich der Dimension ihres projektiven Abschlusses.*

Beweis. Da die projektive Zariski-Topologie auf der Einbettung des K^n in den $\mathbb{P}^n$ nach 1.2.18 genau die Zariski-Topologie auf K^n induziert, entspricht die Dimension von V als Teilmenge des K^n genau der Dimension von V, eingebettet in den $\mathbb{P}^n$. Somit folgt wegen $V \subseteq \overline{V}$ unmittelbar, dass $\dim(V) \leq \dim\left(\overline{V}\right)$.
Für die andere Richtung betrachten wir eine Kette für $\overline{V}$:

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_n \subseteq \overline{V}$$

mit Z_i abgeschlossen und irreduzibel in $\mathbb{P}^n$ für alle i.
Nun gilt für jedes i, dass $Z_i \cap V$ abgeschlossen und irreduzibel in V ist. Abgeschlossen ist klar, die Irreduzibilität zeigen wir per Widerspruch. Seien also $A, B \subseteq \mathbb{P}^n$ mit $(A \cap V) \cup (B \cap V) = Z_i \cap V$, dann wäre $Z_i \subseteq A \cup B \cup (Z_i \cap \mathcal{V}_+(x_0))$ und somit o.B.d.A, da Z_i irreduzibel ist $Z_i \subseteq A \cup (Z_i \cap \mathcal{V}_+(x_0))$, woraus $A \cap V = Z_i \cap V$ folgt.
Da V dicht in $\overline{V}$ ist, müssen auch die Inklusionen echt bleiben, da

$$Z_i \cap V = Z_j \cap V \Rightarrow Z_i = Z_i \cap \overline{V} = \overline{Z_i \cap V} = \overline{Z_j \cap V} = Z_j \cap \overline{V} = Z_j.$$

Insgesamt kriegen wir so aus der oberen Kette die Kette:

$$\varnothing \neq Z_0 \cap V \subsetneq Z_1 \cap V \subsetneq ... \subsetneq Z_n \cap V \subseteq V$$

mit $Z_i \cap V$ abgeschlossen und irreduzibel in V für alle i, und somit $\dim(V) \geq \dim\left(\overline{V}\right)$. □

Satz 1.4.6. *Sei $V \subseteq K^n$ eine Varietät mit $\dim(V) = 0$. Dann besteht V nur aus endlich vielen Punkten.*

Beweis. Wir wissen, dass V aus endlich vielen irreduziblen Varietäten $X_1, ..., X_k$ besteht, und dass $\forall i \in [k] : 0 \leq \dim(X_i) \leq \dim(V) = 0 \Rightarrow \forall i \in [k] : \dim(X_i) = 0$. Wir zeigen als nächstes per Widerspruch, dass X_i nur einen Punkt enthält.
Wir nehmen also an, dass X_i mehr als einen Punkt enthält, nun wählen wir ein $a \in X_i$ dann ist $\varnothing \neq \{a\} \subsetneq X_i$ und somit $\dim(X_i) \geq 1$, womit wir den gewünschten Widerspruch haben. □

Definition 1.4.7 (Isolierte Lösung)**.** *Eine isolierte Lösung eines Gleichungssystems ist eine Lösung für die es eine offene Umgebung (bezüglich der Standardtopologie) gibt, in der keine anderen Lösungen des Gleichungssystems liegen.*

Bemerkung 1.4.8. *Sei $\dim(\mathcal{V}(p_1, ..., p_r)) = 0$, dann besteht die Varietät nach Satz 1.4.6 nur aus endlich vielen Punkten, somit sind offensichtlich alle Lösungen des Gleichungssystems*

$$\begin{pmatrix} p_1(x) \\ \vdots \\ p_r(x) \end{pmatrix} = 0$$

isoliert.

Satz 1.4.9. *Sei $V \subseteq \mathbb{C}^n$ eine Varietät und $d \in \mathbb{N}$, dann gilt für ein generisches Polynom vom Grad kleiner gleich d, genannt p, dass $\dim(V \cap \mathcal{V}(p)) < \dim(V)$*

Beweis. Zunächst zeigen wir, dass generisch $V \cap \mathcal{V}(p) \subsetneq V$. Sei dazu $a \in V$, betrachten wir nun für ein Polynom p die Gleichung $0 = p(a) = p_0 + p_1 a_1 + ... p_l a_n^d$ wobei $l = \binom{n+d}{d}$ so sehen wir, dass wir die Bedingung, dass ein Polynom mit beschränktem Grad eine Nullstelle in a hat, als Polynomiale Gleichung in den Koeffizienten des Polynoms formulieren können. Somit hat ein generisches Polynom p vom Grad $\leq d$ in a keine Nullstelle und $p|_V \not\equiv 0$ also $V \cap \mathcal{V}(p) \subsetneq V$
Nun können wir o.B.d.A v irreduzibel annehmen (sonst betrachten wir die Komponenten von V einzeln). Und wir betrachten eine Kette irreduzibler Varietäten $Z_0, ..., Z_k$ mit

$$\varnothing \neq Z_0 \subsetneq ... \subsetneq Z_k \subseteq V \cap \mathcal{V}(p),$$

so erhalten wir, da für generisches p gilt, dass $V \cap \mathcal{V}(p) \subsetneq V$, unmittelbar eine Kette irreduzibler Varietäten $Z_0, ..., Z_{k+1}$ mit

$$\varnothing \neq Z_0 \subsetneq ... \subsetneq Z_k \subsetneq Z_{k+1} = V$$

Somit gilt $\dim(V) \geq \dim(V \cap \mathcal{V}(p)) + 1$ und die Aussage ist gezeigt. □

Satz 1.4.10 (Krulls Hauptidealsatz)**.** *Sei $p \in \mathbb{C}[x]$ nicht konstant, so gilt für jedes minimale Primideal $\mathbf{p}$ mit $p \in \mathbf{p}$, dass $\text{height}(\mathbf{p}) = 1$.*

Beweis. [5, Kapitel I: 1.11A] □

Satz 1.4.11. *Sei R ein Integritätsring, und als $\mathbb{C}$-Algebra endlich erzeugt. Dann gilt für jedes Primideal $\mathbf{p} \subseteq R$:*

$$\dim(R/\mathbf{p}) = \dim(R) - \text{height}(\mathbf{p}).$$

Beweis. [5, Kapitel I: 1.8A] □

Satz 1.4.12. *Sei $V \subseteq \mathbb{C}^n$ eine Varietät der Dimension d und $p \in K[x]$. Dann gilt* $\dim(V \cap \mathcal{V}(p)) \geq d-1$ *oder $V \cap \mathcal{V}(p) = \varnothing$*
Falls V irreduzibel ist, gilt für jede irreduzible Komponente $W \subseteq V \cap \mathcal{V}(p)$, dass $\dim(W) \geq d-1$. *Insbesondere gilt für $p_1, ..., p_r \in \mathbb{C}[x]$, dass für jede irreduzible Komponente $W \subseteq \mathcal{V}(p_1, ..., p_r)$ gilt, dass* $\dim(W) \geq n - r$.

Beweis. Die erste Aussage folgt aus der zweiten durch Betrachtung aller irreduziblen Komponenten von V. Für die zweite Aussage nehmen wir o.b.d.A. $p \notin \mathcal{I}(V)$ an, sonst ist $V \cap \mathcal{V}(p) = V$ und die Aussage trivial. Falls nun $V \cap \mathcal{V}(p) \neq \varnothing$ so gibt es eine irreduzible Komponente W von $V \cap \mathcal{V}(p)$. Weiter gilt dann $\dim(W) = \dim(\mathbb{C}[W])$. Nun entspricht W einem minimalen Primideal $\mathbf{p}$ über (p) in $\mathbb{C}[V]$, also $\mathbb{C}[W] = \mathbb{C}[V]/\mathbf{p}$. Nun ist nach Krulls Hauptidealsatz (1.4.10) $\text{height}(\mathbf{p}) = 1$ und somit nach Satz 1.4.11 $\dim(W) = \dim(\mathbb{C}[W]) = \dim(\mathbb{C}[V]) - 1 = \dim(V) - 1$.
Der dritte Teil folgt unmittelbar aus mehrfacher Anwendung des zweiten Teils auf $V = \mathbb{C}^n$ zusammen mit Satz 1.4.4. □

Satz 1.4.13. *Sei $V \subseteq \mathbb{C}^n$ eine Varietät mit* $\dim(V) \geq 1$, *dann gilt für eine generische affine Hyperebene $H \subseteq \mathbb{C}^n$, dass $V \cap H \neq \varnothing$.*

Beweis. Nach [3, Satz 5.3.15] gilt die Aussage für projektive Varietäten positiver Dimension und beliebige Hyperebenen. Also gilt für eine beliebige affine Hyperebene H dass $\overline{V} \cap \overline{H} \neq \varnothing$. Wir zeigen nun, für eine generische Hyperebene H, dass $\overline{V} \cap \overline{H} = \overline{V \cap H}$:
Dazu überlegen wir uns zunächst für den Spezialfall $H = \mathcal{V}(x_n)$, was es bedeutet, dass $\overline{V \cap H} = \overline{V} \cap \overline{H}$ bzw., da die eine Inklusion immer erfüllt ist, dass $\overline{V \cap H} \supseteq \overline{V} \cap \overline{H}$. Den allgemeinen Fall können wir anschließend durch Koordinatenwechsel auf diesen zurückführen.
Ist nun $V = \mathcal{V}(p_1, ..., p_r)$, so gilt o.B.d.A., dass

$$\begin{aligned} V \cap H &= \mathcal{V}(p_1, ..., p_r, x_n) \subseteq \mathbb{C}^n \\ V \cap H &= \mathcal{V}(p_1(x_1, ..., x_{n-1}, 0), ..., p_r(x_1, ..., x_{n-1}, 0)) \subseteq \mathbb{C}^{n-1} \\ \overline{V \cap H} &= \mathcal{V}_+(p_1^h(x_0, x_1, ..., x_{n-1}, 0), ..., p_r^h(x_0, x_1, ..., x_{n-1}, 0)) \subseteq \mathbb{P}^{n-1}. \end{aligned}$$

Dass dies tatsächlich o.B.d.A. gilt, sehen wir wie folgt: Sei $I = (p_1(x_1, ..., x_{n-1}, 0), ..., p_r(x_1, ..., x_{n-1}, 0)) \subseteq \mathbb{C}[x_1, ...x_{n-1}]$, dann gilt nach dem Hilbertschen-Basissatz, dass $\exists q_1, ...q_{\tilde{r}} \in I^h$, so dass $I^h = (q^h : q \in I) = (q_1, ...q_{\tilde{r}})$. Weiter gilt:

$$\forall i \in [\tilde{r}] : q_i = \sum_{j=1}^{m_i} h_j f_{i,j}^h(x_0, ..., x_{n-1}, 0)$$

mit $h_j \in \mathbb{C}[x_0, ...x_{n-1}]$ und $f_{i,j}(x_1, ...x_{n-1}, 0) \in I$, dann ist

$$I^h = (f^h_{1,1}(x_0, ...x_{n-1}, 0), ..., f^h_{1,m_1}(x_0, ...x_{n-1}, 0), f^h_{2,1}(x_0, ...x_{n-1}, 0), ..., f^h_{\tilde{r},m_{\tilde{r}}}(x_0, ...x_{n-1}, 0)),$$

und wir erweitern, falls $p_1, ..., p_r$ die obigen Bedingungen nicht erfüllt, den Erzeuger um $f_{1,1}(x_1, ...x_n), ..., f_{1,m_1}(x_1, ...x_n)$, $f_{2,1}(x_1, ...x_n), ..., f_{\tilde{r},m_{\tilde{r}}}(x_1, ...x_n)$.
Genauso können wir o.B.d.A. $\overline{V} = \mathcal{V}_+(p^h_1, ..., p^h_r) \subset \mathbb{P}^n$ annehmen.
Nun überlegen wir uns, wann in dieser Situation $\overline{H} \cap \overline{V} \subseteq \overline{H \cap V}$. Offensichtlich gilt das im Affinen immer, wir betrachten also nur noch die unendlich fernen Punkte.
Sei also $a \in \overline{H} \cap \overline{V} \cap \mathcal{V}_+(x_0)$ dann gilt wegen $a \in \overline{H}$, dass $a_n = 0$. Da a unendlich ferner Punkt ist bzw. $a \in \mathcal{V}_+(x_0)$, gilt $a_0 = 0$ und wegen $a \in \overline{V} = \mathcal{V}_+(p^h_1, ..., p^h_r)$ gilt

$$\forall i \in [r] : p^h_i(a) = p^h_i(0 : a_1 : ... : a_{n-1} : 0) = 0.$$

Weiter gilt

$$a = (0 : a_1 : ... : a_{n-1} : 0) \in \overline{V \cap H} \Leftrightarrow \forall i \in [r] : (p_i(\cdot, 0))^h (0 : a_1 : ... : a_{n-1}) = 0.$$

Somit gilt also

$$\overline{H} \cap \overline{V} \subseteq \overline{H \cap V} \Leftrightarrow \Big(\big(\forall i \in [r] : p^h_i(0 : a_1 : ...a_{n-1} : 0) = 0 \big) \Rightarrow \big(\forall i \in [r] : (p_i(\cdot, 0))^h (0 : a_1 : ... : a_{n-1}) = 0 \big) \Big).$$

Nun bleiben in $(p_i(\cdot, 0))$ nur jene Monome über, in denen x_n nicht vorkommt. Homogenisieren wir nun und setzen dann $(0 : x_1 : ...x_{n-1})$ ein, so bleiben von diesen Monomen die höchsten Grades über.
Andersrum gilt, wenn wir in p^h_i $(0 : a_1 : ...a_{n-1} : 0)$ einsetzen, bleiben die Monome höchsten Grades über, und von denen auch nur die, in denen x_n nicht vorkommt. Somit gilt:

$$\begin{aligned} \overline{H} \cap \overline{V} \subseteq \overline{H \cap V} &\Leftrightarrow \forall i \in [r] : \text{es gibt in } p_i \text{ ein Monom höchsten Grades, in dem kein } x_n \text{ vorkommt} \\ &\Leftrightarrow \forall i \in [r] : 0 \not\equiv p^h_i(0 : x_1 : ...x_{n-1} : 0) = (p_i)_d(x_1 : ... : x_{n-1} : 0), \end{aligned}$$

wobei $(p_i)_d$ den Anteil von p_i höchsten Grades bezeichnet, und somit offensichlich homogen ist.
Sei nun H eine beliebige Hyperebene, dann gibt es eine invertierbare Matrix A und ein $b \in \mathbb{C}^n$, so dass $H = A\mathcal{V}(x_n) + b$. Wir betrachten nun den Koordinatenwechsel $x \mapsto A^{-1}(x - b)$, um diese Situation auf den zuvor betrachteten Fall zurückzuführen. Dadurch werden die Polynome p_i zu $\hat{p_i} = p_i(A \cdot + b)$ nach obigen Überlegungen gilt nun

$$\begin{aligned} \overline{V \cap H} \neq \overline{V} \cap \overline{H} \Leftrightarrow \forall i \in [r] : 0 &= \hat{p_i}^h (0 : x_1 : ... : x_{n-1} : 0) \\ &= (\hat{p_i})_d (x_1 : ... : x_{n-1} : 0) \\ &= (p_i)_d(A(x_1 : ... : x_{n-1} : 0)) = (p_i)_d\big|_{H_l} \end{aligned}$$

wobei H_l die lineare Hyperebene parallel zu H ist. Nun ist $(p_i)_d \neq 0$, und somit gilt, da $\mathcal{V}((p_i)_d)$ echte Untervarietät von $\mathbb{C}^n$ ist, nach Satz 1.4.4 und Satz 1.1.16, dass $\dim(\mathcal{V}((p_i)_d)) \leq n-1$. Analog zum Beweis von Satz 1.4.9 lässt sich zeigen, dass für eine generische lineare Hyperebene H_l das $\dim(\mathcal{V}((p_i)_d \cap H_l) \leq \dim(\mathcal{V}((p_i)_d)) - 1 \leq n-2$ und somit $H_l \notin \mathcal{V}((p_i)_d)$. Und nach obigen Überlegungen gilt somit für generische affine Hyperebenen $\overline{V \cap H} = \overline{V} \cap \overline{H}$. Somit ist für H eine generische affine Hyperebene $\overline{V \cap H} = \overline{V} \cap \overline{H}$. $\square$

Korollar 1.4.14. *Sei $V \subseteq \mathbb{C}^n$ eine Varietät mit $\dim(V) = d$ und $g \in \mathbb{N}$. Dann gilt für generische Polynome mit Grad kleiner gleich g, welche ich mit $p_1, ..., p_d$ bezeichne, dass $\dim(V \cap \mathcal{V}(p_1) \cap ... \cap \mathcal{V}(p_d)) = 0$. Insbesondere besteht $V \cap \mathcal{V}(p_1) \cap ... \cap \mathcal{V}(p_d)$ aus endlich vielen isolierten Punkten.*

Beweis. Wir zeigen zunächst, dass $\dim(V \cap \mathcal{V}(p_1)) = d - 1$. Aus Satz 1.4.9 folgt $\dim(V \cap /V(p_1)) \leq d - 1$. Wegen Satz 1.4.12 und Satz 1.4.13 gilt $\dim(V \cap \mathcal{V}(p_1)) \geq d - 1$, somit haben wir $\dim(V \cap \mathcal{V}(p_1)) = d - 1$. Wir iterieren diese Argumentation d mal und erhalten $\dim(V \cap \mathcal{V}(p_1) \cap ... \cap \mathcal{V}(p_d)) = 0$. Die zweite Aussage folgt unmittelbar aus Satz 1.4.6. □

Bemerkung 1.4.15. *Die Aussage gilt genauso für projektive Varietäten und homogene Polynome. Allerdings können wir Satz 1.4.12 nicht analog beweisen, da wir keine Entsprechung des Koordinatenrings für projektive Varietäten haben. Einen Beweis der projektiven Version dieses Satzes ist hier angegeben: [3, Korollar 5.3.18] der Rest des Beweises geht analog. Ebenso stimmt der Satz auch, wenn wir, statt generische affine bzw. projektive Hyperebenen zu betrachten, uns auf generische affine bzw. projektive Hyperebenen, die einen bestimmten Punkt enthalten, beschränken. Für den Beweis dieser Aussage, müssen wir lediglich den Beweis der Sätze 1.4.9 und 1.4.13, auf unsere Situation anpassen. Die Beweise funktionieren allerdings komplett analog.*

Definition 1.4.16 (Grad)**.** *Sei V eine affine oder projektive irreduzible Varietät der Dimension d, dann ist $\deg(V)$ der Grad von V, definiert als Anzahl der Punkte im Schnitt von V mit d generischen Hyperebenen.*

Satz 1.4.17. *Der Grad einer irreduziblen Varietät ist wohldefiniert.*

Beweis. Die Aussage ist für projektive Varietäten als klassisches Resultat bekannt. Siehe bspw. [6, Ex. 18.2].
Wir beweisen den affinen Fall davon ausgehend. Sei $V \subseteq \mathbb{C}^n$ irreduzible Varietät mit $\dim(V) = d$ nach Satz 1.4.5, ist somit auch $\dim(\overline{V}) = d$. Nach Satz 1.2.27 ist $\overline{V}$ darüber hinaus auch irreduzibel. Nun gilt offensichtlich, dass $\dim(\overline{V} \cap \mathcal{V}_+(x_0)) < d$, und somit gilt für d generische Hyperebenenen $H_1, ..., H_d \subseteq \mathbb{P}^n$, dass $\overline{V} \cap H_1 \cap ... \cap H_d \cap \mathcal{V}_+(x_0) = \varnothing$. Alle Punkte von $\overline{V} \cap H_1 \cap ... \cap H_d$ liegen also im Affinen. Unter der Annahme, dass die Menge $\{\overline{E} \subseteq \mathbb{P}^n \,|E \subseteq \mathbb{C}^n \text{ Hyperebene}\}$ Zariski-offen in der Menge der Hyperebenen im $\mathbb{P}^n$ ist, folgt die Aussage unmittelbar aus den vorherigen Überlegungen, da wir so statt generische Hyperebenen in $\mathbb{P}^n$ zu wählen, einfach generische Hyperebenen in $\mathbb{C}^n$ wählen können und diese homogenisieren. Nach vorherigen Überlegungen kommen durch einen solchen Wechsel ins Projektive keine Punkte zu dem Schnitt hinzu. Das die Annahme stimmt, sieht man wie folgt: wir können jede Hyperebene in $\mathbb{P}^n$ mit einem homogenen Grad-1-Polynom p in $K[\underline{x}]$ identifizieren. Wir können p als $c_0x_0 + ... + c_1x_1$ darstellen. Dies ist für $p \neq c_0x_0$ die Homogenisierung des Polynoms $c_0 + c_1x_1 + ... + c_nx_n \in K[x]$. Somit gilt unsere Annahme generisch. □

Bemerkung 1.4.18. *Aus dem Beweis sehen wir unmittelbar, dass für eine affine irreduzible Varietät V gilt, dass $\deg(V) = \deg(\overline{V})$.*
Weiter lässt sich im projektiven Fall die Einschränkung auf generische Hyperebenen abschwächen zu der Bedingung, dass der Schnitt der Varietät mit den Hyperebenen Dimension 0 haben muss. Indem wir die isolierten Lösungen mit Multiplizitäten zählen, siehe [7]. Betrachten wir die Multiplizitäten nicht, so erhalten wir immmer noch, dass der Grad eine obere Schranke für die Kardinalität des Schnitts ist.

Satz 1.4.19. *Seien $X \neq Y \subseteq \mathbb{C}^n$ irreduzible Komponenten einer Varietät und $\dim(X) = d$, dann gilt für generische affine Hyperebenen $H_1, ..., H_d$ und $a \in X \cap H_1 \cap ... \cap H_d$, dass $a \notin Y$. Weiter gibt es sogar eine Umgebung U (bezüglich der standarttopologie) von a mit $U \cap Y = \varnothing$.*

Beweis. Wir beweisen die erste Aussage per Widerspruch, sei dazu $a \in X \cap Y$.
Wir zeigen $\dim(X \cap Y) < d$, dann gilt $a \in X \cap Y \cap H_1 \cap ... \cap H_d = \varnothing$ und wir haben einen Widerspruch.
Sei $r = dim(X \cap Y)$ dann existieren irreduzible Varietäten $Z_0, ..., Z_r$ so dass:

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_r \subseteq X \cap Y.$$

Es gilt aber $X \cap Y \subsetneq X$ und somit kriegen wir eine Kette

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_r \subsetneq X$$

für X, womit folgt das $d \geq r + 1$.
Für den zweiten Teil betrachten wir $p_1, ..., p_r$, so dass $Y = \mathcal{V}(p_1, ..., p_r)$, da $a \notin Y$ gibt es ein $i \in [r]$ mit $p_i(a) \neq 0$. Da p_i als Polynom insbesondere stetig ist, gibt es somit eine Umgebung U von a mit $\forall b \in U : p_i(b) \neq 0$, also $\forall b \in U : b \notin Y$. □

Bemerkung 1.4.20. *Dieser Satz zusammen mit Satz 1.4.14 garantiert, dass wir, wenn wir eine Varietät haben, die Komponenten verschiedener Dimensionen besitzt, wir wenn wir mit d generischen Hyperebenen schneiden, die Anzahl der Isolierten Punkte der Summe der Grade der Komponenten der Dimension d entsprechen.*

2 Homotopie-Verfahren

In diesem Abschnitt werden wir eine Klasse von numerischen Verfahren, die sogennanten Homotopie-Verfahren, kennen lernen, mit denen wir alle isolierten Lösungen eines polynomialen Gleichungssystems finden können. Diese Verfahren bilden einen fundamentalen Baustein unseres Algorithmus.
Wir werden uns zunächst anhand eines einfachen Beispiels die Funktionsweise dieser Verfahren sowie die möglichen Probleme, die es zu vermeiden gilt, vor Augen führen, dabei gehen wir analog zu [1, Kapitel 2] vor. Anschließend möchten wir die so gewonnenen Erkenntnisse verallgemeinern. Der Fokus dieser Arbeit soll jedoch weiterhin auf unserem Algorithmus zur Berechnung einer irreduziblen Zerlegung liegen, daher werden wir in erster Linie jene Homotopie-Verfahren behandeln, die wir im weiteren Verlauf dieser Arbeit benutzen werden.
Die Grundidee hinter Homotopie-Verfahren ist es, ein zu lösendes Problem in eine Familie von Problemen einzubetten, die stetig von bestimmten Parametern abhängt. Kennt man nun die Lösungen eines der Probleme aus der Familie, so möchten wir nun stetig die Parameter so verändern, dass wir zu unserem eigentlichen Problem kommen und dabei das ebenfalls stetige Verhalten der Lösungen verfolgen, so dass wir schließlich die Lösungen unseres eigentlichen Problems erhalten.

2.1 Motivation/Einfaches Beispiel

Als einfaches Beispiel werden wir ein Polynom in einer Variable betrachten und schauen, wie wir durch Homotopie-Verfahren die Lösungen dieses Polynoms finden können. Anhand dieses Beispiels werden wir

schnell sehen, was die problematischen Stellen bei den Homotopie-Verfahren sind und wie wir diese umgehen können, so dass die Verfahren trotzdem gut funktionieren.
Wir betrachten nun also das Polynom

$$p = -x^3 + 5x^2 - x + 3.$$

Nun brauchen wir für unser Homotopie-Verfahren ein Startsystem, von dem wir die Nullstellen kennen sowie eine Familie von Problemen bzw. eine Familie von Polynomen, in die wir p einbetten. Als Startsystem wählen wir das Polynom $s = x^3 - 1$, von dem wir wissen, dass es genauso viele Nullstellen hat wie p, und von dem wir diese Nullstellen bereits kennen: $\mathcal{V}(s) = \{e^{\frac{k2\pi i}{3}} | k \in \{0,1,2\}\}$. Wir betrachten nun die parametrisierte Familie von Polynomen

$$H : \mathbb{C}^2 \to \mathbb{C} : \ (x,y) \mapsto ys(x) + (1-y)p(x).$$

Dabei ist $p(x) = H(x,0)$ und $s(x) = H(x,1)$.
Wir möchten nun einen Weg $\phi : [0,1] \to \mathbb{C}$ mit $\phi(0) = 0$ und $\phi(1) = 1$ wählen und anschließend den Lösungen von $H(x,\phi(t))$ folgen, während wir t von 1 nach 0 laufen lassen. Die entscheidene Frage ist dabei wie wir den Weg ϕ wählen, so dass unser Verfahren funktioniert. Dazu überlegen wir zunächst, was die Probleme, die wir vermeiden müssen, sind. Dass wir t von 1 nach 0 laufen lassen, anstatt andersrum, wie es intuiv einleuchtender erscheint, liegt daran, dass wir für unsere numerische Berechnung mehr Zahlen nahe 0 zur Verfügung haben, als nahe 1, wodurch die Berechnung der Lösungen von $p(x) = 0$ genauer wird. Da unser Startpolynom s sowie auch p 3 Nullstellen besitzt, wird unser Verfahren funktionieren, so lange diese Pfade, die bei den Lösungen von s starten, sich brav genug verhalten, d.h. keiner der drei Pfade Richtung unendlich divergiert, und keiner der drei Pfade mit einem der anderen zusammenläuft, bzw. einen der anderen schneidet.
Dass einer der Pfade divergiert, ist gleichbedeutend damit, dass für ein $t \in [0,1]$ der Grad von $H(x,\phi(t))$ fällt. So ein Verhalten haben wir hier genau dann, wenn $\phi(t) = 1 - \phi(t)$, also für $\phi(t) = \frac{1}{2}$. Somit wäre ein Weg entlang der reellen Achse schlecht geeignet. Die Abbildung 1 veranschaulicht genau dieses unerwünschte Verhalten für einen Weg entlang der reellen Achse, wir sehen die Nullstellen von $H(x,\phi(t))$ für $\phi(t) = t$ und $t \in (0.5, 0.7]$

Betrachten wir das Problem, dass $H(x,y)$ für bestimmte Werte von y doppelte Nullstellen haben kann. An diesen Stellen muss dann zusätzlich zu $H(x,y) = 0$ auch noch $\partial_x H(x,y) = 0$ gelten. Die Punkte (x,y) an denen mehrfache Nullstellen auftreten bilden also die durch

$$0 = \begin{pmatrix} H(x,y) \\ \partial_x H(x,y) \end{pmatrix} = \begin{pmatrix} ys(x) + (1-y)p(x) \\ ys'(x) + (1-y)p'(x) \end{pmatrix}$$

definierte Varietät V in $\mathbb{C}^2$. Aus der ersten Zeile erhalten wir, dass für $(x,y) \in V$ gilt, dass $y = \frac{-p(x)}{s(x)-p(x)}$. Aus der zweiten Zeile ergibt sich $y = \frac{-p'(x)}{s'(x)-p'(x)}$, und somit gilt für $(x,y) \in V$, dass $p(x)(s'(x) - p'(x)) - p'(x)(s(x) - p(x)) = 0$. Da dies ein Polynom vom Grad 4 ist (die Terme höherer Ordnung kürzen sich) haben wir höchstens 4 Nullstellen und da nach obigen Überlegungen wir die Werte für y direkt durch $y = \frac{-p(x)}{s(x)-p(x)}$ aus den Lösungen für x bekommen, gibt es höchstens 4 Werte für y, an denen wir doppelte Wurzeln haben und die unser ϕ vermeiden muss. Rechnen wir diese Nullstellen aus, so zeigt sich, dass

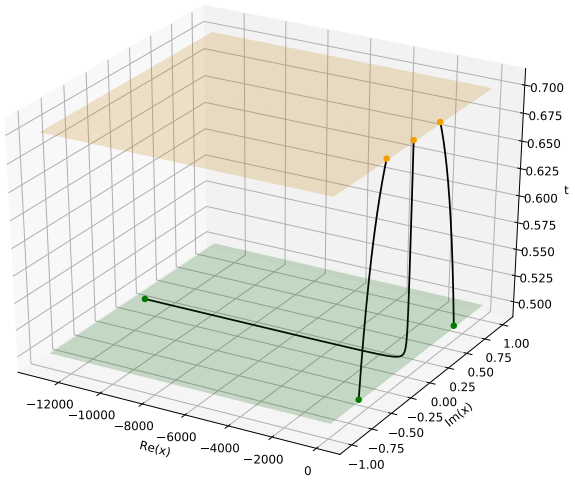

Abbildung 1: Divergierende Nullstelle nahe $t = 0.5$

$H(x, y)$ für $y \approx 0.833913$ eine doppelte Nullstelle besitzt. Die Abbildung 2 soll dies veranschaulichen und zeigt die Nullstellen von $H(x, \phi(t))$, wobei $\phi(t) = t$ die Reelle-Achse von $t = 0.8$ bis $t = 1$ Parametrisiert.

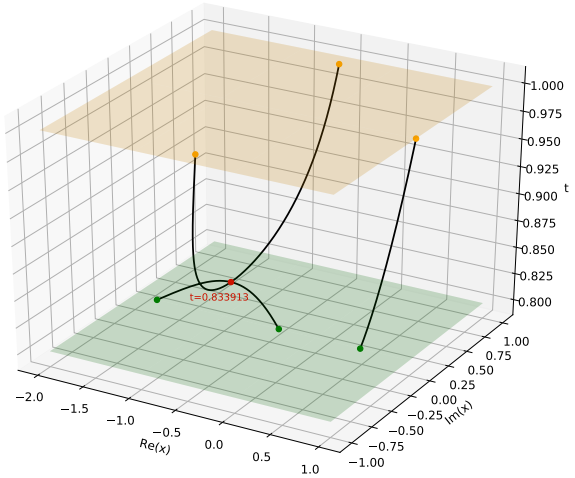

Abbildung 2: Doppelte Nullstelle bei $t \approx 0.833913$

Nun wirkt dieses Verhalten auf den ersten Blick nicht allzu schlimm. Wenn wir uns jedoch überlegen dass wir diesen Lösungspfaden folgen möchten, indem wir einen numerischen Differenzialgleichungslöser verwenden, siehe Bemerkung 2.2.7, so haben wir offensichtlich an dem Punkt bzw. nahe des Punktes, wo die Lösungspfade sich schneiden, das Problem, dass dieser Löser, unabhängig von dem zuvor zurückgelegten Pfad, von nun an beide Pfade gleich berechnet. Dies hat zur Folge, dass wir eine Lösung von p doppelt finden, während wir eine andere überhaupt nicht finden.
Um einen Weg zu erhalten der diese Punkte meidet, wählen wir ein zufälliges $\gamma \in \mathbb{C}$ mit $|\gamma| = 1$ und betrachten

$$\phi(t) = \frac{\gamma t}{1 + (\gamma - 1)t}.$$

Wir werden im nächsten Abschnitt einen Beweis dafür sehen, dass so ein Weg mit Wahrscheinlichkeit 1 die Problemstellen meidet, der entscheidene Punkt wird sein, dass für verschiedene Wahl von γ die so parametrisierten Wege sich nur in 0 und 1 schneiden und somit nur auf endlich vielen Wegen die endlich vielen „Problemstellen“liegen können.
Abbildung 3 zeigt das generische brave Verhalten der Lösungspfade für die Wahl $\gamma = \frac{1+i}{\sqrt{2}}$

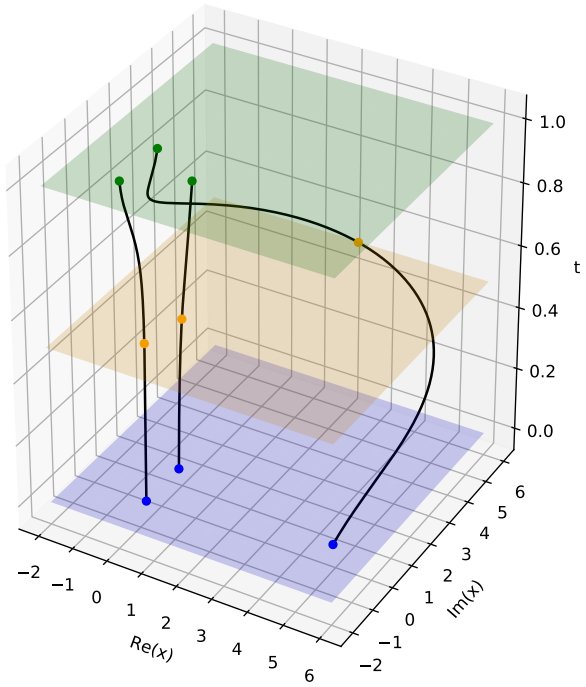

Abbildung 3: Generisches Verhalten der Nullstellen am Beispiel $\gamma = \frac{1+i}{\sqrt{2}}$

2.2 Allgemeine Homotopie-Verfahren

Definition 2.2.1 (Homotopie)**.** *Sei $X \subseteq \mathbb{C}^m$. Als Homotopie bezeichen wir eine Gleichung $H(x, \phi(t)) = 0$ wobei*

$$H(x, z) : \mathbb{C}^n \times X \to \mathbb{C}^r$$

polynomial in den Unbekannten x und stetig in den Parametern z ist und

$$\phi : [0, 1] \to X$$

stetig.
Wir nennen $H(x, z) = 0$ ein parametrisiertes System von Problemen und für ein festes $z \in X$ nennen wir $H(x, z) = 0$ ein Problem
Für einen Weg $\phi : [0, 1] \to X$ nennen wir $H(\cdot, \phi(1))$ das Startsystem und $H(\cdot, \phi(0))$ das Zielsystem der Homotopie.
Eine Homotopie heißt quadratisch falls $r = n$.
Eine Homotopie heißt polynomial falls H auch in den Parametern polynomial ist.

Bemerkung 2.2.2. *Alle Homotopien die uns im Folgenden beschäftigen werden, sind sowohl quadratisch als auch polynomial. Die Einschränkung auf polynomiale Homotopien ist natürlich, während wir noch etwas Arbeit leisten müssen um zu sehen, warum auch die Einschränkung auf quadratische Homotopien in der Praxis problemlos möglich ist. Diese Frage klären wir im Abschnitt „Randomization“.*

Definition 2.2.3 (Lösungspfad)**.** *Sei $H(x, \phi(t)) = 0$ eine Homotopie, dann nennen wir eine Funktion $l : [0, 1] \to \mathbb{C}^n$ einen Lösungspfad der Homotopie, falls $H(l(t), \phi(t)) = 0$ für alle $t \in [0, 1]$.*
Wir nennen einen Lösungspfad $l(t)$ isolierte-Lösung-Pfad, wenn für jedes $t \in [0, 1]$ gilt, dass $l(t)$ isolierte Lösung von $H(x, \phi(t)) = 0$ ist.

Die nächsten Sätze zeigen, dass Homotopie-Verfahren, analog zu unserem Beispiel aus dem letzten Abschnitt, auch in höheren Dimensionen den kritischen Stellen ausweichen und mit Wahrscheinlichkeit 1 funktionieren.
In den nächsten Abschnitten werden wir für die Homotopie-Verfahren, die wir verwenden werden, also für spezielle Wahl von H und X, den folgenden Satz beweisen:

Satz 2.2.4. *Wir betrachten das Polynom*

$$H(x, z) : \mathbb{C}^n \times X \to \mathbb{C}^n$$

Für $z \in X$ bezeichne nun $\mathcal{N}(z)$ die Anzahl der isolierten Lösungen von $H(\cdot, z)$ Dann gilt:

1. *Es gibt eine Zariski-offene Menge $\varnothing \neq U \subseteq X$ und ein $\mathcal{N} \in \mathbb{N}$ so dass $\forall z \in X : \mathcal{N}(z) \leq \mathcal{N}$ und $\forall z \in U : \mathcal{N}(z) = \mathcal{N}$*
2. *Die Homotopie $H(x, \phi(t)) = 0$ mit $\phi : [0, 1] \to U$ hat $\mathcal{N}$ stetige Isolierte-Lösung-Pfade $l(t)$*
3. *Betrachte die Homotopie $H(x, \phi(t)) = 0$ mit $\phi : [0, 1] \to X$ und $\forall t \in (0, 1] : \phi(t) \in U$ dann sind alle isolierten Lösungen von $H(\cdot, \phi(0)) = 0$ unter den Grenzwerten der Isolierte-Lösung-Pfade für $t \to 0$*

Beweis. Der schwierige Teil des Beweises ist der erste Punkt, diesen werden wir später beweisen, wenn wir die Homotopie-Verfahren, für die wir den Satz beweisen wollen, kennengelernt haben. Der zweite und dritte Punkt folgen aus dem ersten unter Verwendung des klassischen Resultates, dass Nullstellen von Polynomen stetig von den Koeffizienten abhängen. Dass nicht nur der Pfad einer Lösung stetig ist, sondern eine isolierte Lösung auch isoliert bleibt, sehen wir wie folgt: Sei $a(t)$ ein Lösungspfad und nehmen wir an, dass $a(t)$ für $t \in (\tau, 1]$ isolierte Lösung ist, aber für $t = \tau$ nicht isolierte Lösung, dann muss es, da die Anzahl der isolierten Lösungen konstant ist, einen anderen Lösungspfad $b(t)$ geben, so dass $b(t)$ für $t \in (\tau, 1]$ nicht isoliert ist, aber für $t = \tau$ schon. Aufgrund der stetigen Abhängigkeit der Lösungen von den Koeffizienten ist nun jedoch $b(t)$ in einer Umgebung von τ isoliert, womit wir einen Widerspruch haben. □

Wir wollen uns nun überlegen wie wir einen Weg $\phi : [0,1] \to \mathbb{C}^m$ finden, der den Bedingungen aus Satz 2.2.4 3. genügt. Die Antwort auf diese Frage liefert der "Gamma-Trick".

Satz 2.2.5 (Gamma-Trick)**.** *Sei $z_0 \in U, U \subseteq X$ und U Zariski-offen in $\mathbb{C}^m$. Dann gilt für alle bis auf endlich viele $\gamma \in \mathbb{C}$ mit $|\gamma| = 1$, dass der durch*

$$\phi_\gamma(t) := \left(\frac{\gamma t}{1+(\gamma-1)t}\right) z_1 + \left(1 - \left(\frac{\gamma t}{1+(\gamma-1)t}\right)\right) z_0, \quad t \in (0,1]$$

parametrisierte Bogen in U liegt

Beweis. Bezeichne A das Komplement von U in $\mathbb{C}^m$. Wir betrachten die Menge

$$T := \{t \in \mathbb{C} | (tz_1 + (1-t)z_o) \in A\}.$$

Nun ist A eine Varietät und somit existieren Polynome $p_1, ..., p_r$, so dass $A = \mathcal{V}(p_1, ..., p_r)$. Nun ist offensichtlich $T = \mathcal{V}(p_1(\cdot z_1 + (1-\cdot)z_0), ...p_r(\cdot z_1 + (1-\cdot)z_0)) \subseteq \mathbb{C}$ und somit T ebenfalls eine Varietät. Da $z_1 \notin A$ gilt $1 \notin T$, und somit besteht T als Untervarietät von $\mathbb{C}$ nur aus endlich vielen Punkten.
Wir zeigen nun, dass die Bilder von

$$\Phi_\gamma : (0,1) \to \mathbb{C} : \ t \mapsto \frac{\gamma t}{1+(\gamma-1)t}$$

für verschiedene $\gamma \in \mathbb{C}$ mit $|\gamma| = 1$ disjunkt sind. Wenn wir dies gezeigt haben, folgt die Aussage unmittelbar, da nur für endlich viele γ einer der endlich vielen Punkte aus T in $\Phi_\gamma((0,1])$ liegen kann.
Um zu zeigen, dass die Kurven disjunkt sind, wählen wir $\gamma_1 \neq \gamma_2 \in \mathbb{C}$ mit $|\gamma_1| = |\gamma_2| = 1$. Nun gilt:

$$\begin{aligned} &\frac{\gamma_1 t_1}{1+(\gamma_1-1)t_1} = \frac{\gamma_2 t_2}{1+(\gamma_2-1)t_2} \\ \Leftrightarrow\ &\gamma_1 t_1 + \cancel{\gamma_1 t_1 \gamma_2 t_2} - \gamma_1 t_1 t_2 = \gamma_2 t_2 + \cancel{\gamma_2 t_2 \gamma_1 t_1} - \gamma_2 t_2 t_1 \\ \Leftrightarrow\ &\gamma_1 t_1 (1-t_2) = \gamma_2 t_2 (1-t_1). \end{aligned}$$

Da $t_1(1-t_2), t_2(1-t_1) \in \mathbb{R}_{\geq 0}$ und wegen $|\gamma_1| = |\gamma_2| = 1$ gilt, dass γ_1 und γ_2 nicht auf dem selben Halbstrahl in der komplexen Ebene liegen. Somit gibt es keine $t_1, t_2 \in (0,1)$, so dass die Gleichung oben erfüllt ist. □

Bemerkung 2.2.6. *Dieser Satz zeigt, dass um mit Wahrscheinlichkeit 1 einen geeigneten Weg für unser Homotopie-Verfahren zu finden, es genügt, ein Startsystem mit der generischen Anzahl an Lösungen zu finden und zu lösen.*

An dieser Stelle möchte ich kurz etwas genauer darauf eingehen, wie wir in der Praxis unseren Lösungswegen folgen.

Bemerkung 2.2.7. *Wir haben eine Homotopie $h(x,\phi(t)) = 0$ gegeben zusammen mit $p_0,...,p_r$ den Isolierten Lösungen von $h(x,\phi(1)) = 0$ dann definiert die gewöhnliche Differenzialgleichung:*

$$\partial_t h(x_i(t),\phi(t)) = 0, \quad x_i(1) = p_i$$

für jedes $i \in [r]$ den Lösungspfad $x_i : [0,1] \to \mathbb{C}^n$
Nun sind numerische Methoden fürs Lösen von Differentialgleichungen weit fortgeschritten und wir nutzen, wie in der Einleitung bereits angedeutet, ein solches numerisches Verfahren.

Nun stellt sich noch die Frage, wie wir ein geeignetes Startsystem finden und vor allem lösen können. Wir bekommen zwar durch zufällige Wahl der Parameter mit Wahrscheinlichkeit 1 ein geeignetes Startsystem allerdings stehen wir dann vor dem Problem die Lösungen dieses Startsystems zu finden, was im Allgemeinen nicht leichter ist, als die Lösungen unseres Zielsystems zu finden. Trotzdem ist dieses Vorgehen häufig sinnvoll, da wir häufig nicht nur eines der in der Homotopie enthaltenden Probleme lösen wollen, sondern mehrere, und dann, sobald man die Lösung des generischen Startsystems hat, das Lösen jedlicher anderer in der Homotopie enthaltenden Probleme vergleichsweise einfach ist.
Im folgenden Abschnitt werden wir uns mit zwei Klassen von Homotopie-Verfahren beschäftigen, den „Slice "-Homotopie-Verfahren die wir in unserem Algorithmus hauptsächlich verwenden werden, sowie den „Total degree "-Homotopien, die wir benutzen, um die Lösungen der Startsysteme für unsere „Slice "-Homotopie-Verfahren zu finden.

2.3 „Total degree "-Homotopie-Verfahren

In diesem Abschnitt sei $X = \mathbb{C}^m$.

Definition 2.3.1 („Total degree "-Homotopie-Verfahren)**.** *Seien $d_1,...,d_n \in \mathbb{N}, \phi : [0,1] \to \mathbb{C}^m$ stetig und $H_{d_1,...,d_n}(x,z) = (h_1(x,z),...,h_n(x,z))^T : \mathbb{C}^n \times \mathbb{C}^m \to \mathbb{C}^n$ mit*

$$h_i(x,z) = \sum_{|\alpha| \le d_i} z_{i,\alpha} x^\alpha,$$

wobei $\alpha \in \mathbb{N}_0^n$, dann nennen wir die Homotopie $H(x,\phi(t)) = 0$ „Total degree "-Homotopie zu den Graden $d_1,...,d_n$. Diese Homotopie enthält alle polynomialen Gleichungssysteme der Länge n in n Variablen, wobei der Grad des i-ten Polynoms kleiner gleich d_i ist. Da $\#\{\alpha \in \mathbb{N}_0^n : |\alpha| \le d_i\} = \binom{n+d_i}{n}$ ist $m = \sum_{i=1}^n \binom{n+d_i}{n}$.

Punkt eins von Satz 2.2.4 ist für den Spezialfall der „Total degree "-Homotopie-Verfahren bekannt als Satz von Bezout.

Satz 2.3.2 (Satz von Bezout)**.** *Sei $V = \mathcal{V}(p_1,...,p_n) \subseteq \mathbb{C}^n$ mit $\forall i \in [n] : \deg(p_i) = d_i$ dann besitzt V höchstens $B = \prod_{i=1}^n d_i$ isolierte Lösungen. Weiter ist für generische Wahl an Polynomen $q_1,...,q_n$ mit $\forall i \in [n] : \deg(q_i) \le d_i$ die Anzahl der isolierten Lösungen von $\mathcal{V}(q_1,...,q_n)$ genau B*

Beweis. Wir beweisen zunächst den Ersten Teil der Aussage: Einen Beweis dafür, dass die Kardinalität der Vereinigung der Komponenten der Dimension 0 durch B beschränkt ist, findet man in [8]. Nun wissen wir aus dem Beweis von Satz 1.4.6, dass eine Komponente der Dimension 0 aus genau einem isolierten

Punkt besteht. Dass Komponenten positiver Dimension keine isolierten Punkte enthalten können, folgt unmittelbar aus dem Connectedness-Theorem [9, Satz 4.16].
Für den zweiten Teil des Beweises überlegen wir uns zunächst, dass ein generisches Polynom vom Grad $\leq d$ Grad d hat. Dazu überlegen wir uns, dass die Menge der Polynome vom Grad $\leq d$ einen endlich dimensionalen Vektorraum bilden und die Polynome vom Grad $< d$ einen echten Unterraum. Somit ist die Menge der Polynome vom Grad $\leq d$ isomorph zum $\mathbb{C}^l$ für ein $l \in \mathbb{N}$ und die Menge der Polynome vom Grad $< d$ ein echter Unterraum des $\mathbb{C}^l$. Somit hat ein generisches Polynom vom Grad $\leq d$ Grad d und wir können von nun an o.B.d.A $\forall i \in [n] : \deg(q_i) = d_i$ annehmen.
Als Nächstes zeigen wir, dass für generische Polynome $q_1, ..., q_n \in \mathbb{C}[\underline{x}]$ mit $\forall i \in [n] : \deg(q_i) = d_i$ die Anzahl der isolierten Lösungen B ist. Dabei folgen wir der Idee von [10]. Nach [11, Satz 8.4] gilt $\deg(\mathcal{V}_+(q_1, ..., q_n)) = \prod_{i=1}^n d_i = B$. Nach einer Verallgemeinerung des Satzes von Bertini ([12]) durch Anwendung der Veronese-Abbildung ([3, Abschnitt 4.2]) ist der Schnitt einer glatten projektiven Varietät mit $\mathcal{V}_+(p)$ für generische Wahl von $p \in \mathbb{C}[\underline{x}]$ glatt, somit ist für generische Wahl von $q_1, ..., q_n$ die projektive Varietät $\mathcal{V}_+(q_1, ..., q_n)$ glatt. So wie in [11] der Grad einer Varietät definiert ist, folgt unmittelbar, dass die Kardinalität einer glatten projektiven Varietät der Dimension 0 gleich ihrem Grad ist. Somit verbleibt noch zu zeigen, dass für generische $q_1, ..., q_n$ die projektive Varietät $\mathcal{V}_+(q_1, ..., q_n)$ Dimension 0 hat, dies folgt jedoch unmittelbar aus Bemerkung 1.4.15
Nun können wir dieses Resultat verwenden, um unser Resultat für affine Varietäten zu beweisen.
Wir betrachten nun n generische Polynome $p_1, ..., p_n \in \mathbb{C}[x]$ dann ist nach Satz 1.4.14 $\dim(\mathcal{V}(p_1, ..., p_n)) = 0$. Genauso gilt dies für generische homogene Polynome $q_1, ..., q_n \in \mathbb{C}[\underline{x}]$, und insbesondere gilt generisch dass $\mathcal{V}_+(q_1, ..., q_n) \cap \mathcal{V}_+(x_0) = \varnothing$, also alle Punkte aus $\mathcal{V}_+(q_1, ..., q_n)$ im Affinen liegen, und somit $\mathcal{V}_+(q_1, ..., q_n) = \mathcal{V}(\tilde{q_1}, ..., \tilde{q_n})$. Wir zeigen nun, dass ein generisches homogenes Polynom $q \in \mathbb{C}[\underline{x}]$ vom Grad d Homogenisierung eines Polynoms vom Grad d in $\mathbb{C}[x]$ ist. Damit können wir nach den vorherigen Überlegungen die affine Version dieses Satzes einfach durch Homogenisieren unserer ursprünglicher Polynome bekommen. Offensichlich ist ein homogenes Polynom in $\mathbb{C}[\underline{x}]$ Homogenisierung eines Polynoms in $\mathbb{C}[x]$ ist genau dann, wenn nicht jedes Monom in dem Polynom x_0 enthält. Wenn also nicht alle Koeffizienten vor den Monomen, die x_0 nicht enthalten, 0 sind. Dies ist offensichtlich eine Zariski-offene Bedingung. Somit können wir ein bezüglich einer Eigenschaft generisches homogenes Polynom vom Grad d in $\mathbb{C}[\underline{x}]$ bekommen, indem wir ein generisches Polynom vom Grad d in $\mathbb{C}[x]$ homogenisieren. □

Nun sehen wir leicht, dass

$$f(x) = \begin{pmatrix} x_1^{d_1} - 1 \\ \vdots \\ x_n^{d_n} - 1 \end{pmatrix} = 0$$

die nach dem Satz von Bezout generische Anzahl an Lösungen einer „Total degree"-Homotopie besitzt. Die Lösungen sind nämlich genau jene $a \in \mathbb{C}^n$ mit $\forall i \in [n] : a_i^{d_i} = 1$ somit haben wir für jede Komponente unabhängig von den anderen Komponenten d_i Möglichkeiten und somit insgesamt $\prod_{i=1}^n d_i$ Lösungen. Insbesondere kennen wir diese Lösungen also bereits. Somit haben wir ein perfekt geeignetes Startsystem für unser „Total degree"-Homotopie-Verfahren gefunden. Und können somit nach Satz 2.2.4 unter verwendung de Gamma-Tricks (Satz 2.2.5) alle isolierten Lösungen eines beliebigen quadratischen polynomialen Gleichungssystems bestimmen.

Lemma 2.3.3 („Gamma Trick"und lineare Homotopien)**.** *Sei $H(x, \phi(t)) = 0$ eine Homotopie die linear in*

den Parametern ist und

$$\phi(t) = \left(\frac{\gamma t}{1+(\gamma-1)t}\right) z_1 + \left(1 - \left(\frac{\gamma t}{1+(\gamma-1)t}\right)\right) z_0 = \left(\frac{\gamma t}{1+(\gamma-1)t}\right) z_1 + \left(\frac{1-t}{1+(\gamma-1)t}\right) z_0,$$

dann gilt

$$H(x, \phi(t)) = 0 \Leftrightarrow \gamma t H(x, z_1) + (1-t) H(x, z_0) = 0.$$

Beweis. Die Aussage folgt unmittelbar durch Ausnutzen der Linearität und Multiplikation mit dem Nenner. □

Bemerkung 2.3.4. *Die „Total degree"-Homotopie-Verfahren sind linear in den Parametern. Wir können also das Lemma verwenden, was zu einfacherer numerischer berechnung der Lösungspfade beitragen kann.*

2.4 „Slice "-Homotopie-Verfahren

Die „Slice"-Homotopie-Verfahren sind um einiges spezieller als die „Total Degree"-Verfahren, so haben die Probleme, die in dieser Homotopie enthalten sind mehr Gemeinsamkeiten als beim „Total Degree"-Verfahren.
Beim „Total Degree"-Verfahren haben wir nur die Grade der Polynome in unserem Zielsystem betrachtet und alle Komponenten unserer Homotopie verändert, bei den „Slice"-Verfahren hingegen halten wir eine Varietät fest und variieren die Hyperebenen, mit denen wir diese Varietät schneiden entsprechend unserer Parameter. Dies liefert den „Slice"-Verfahren zusätzliche Struktur, die wie wir im Abschnitt zum Membership Testing sehen werden, für die Funktion unseres Algorithmus notwendig ist.

Definition 2.4.1 („Slice "-Homotopie-Verfahren)**.** *Seien $p_1, ..., p_k \in \mathbb{C}[x]$, $r \in \mathbb{N}$, $\phi : [0,1] \to X_r \subseteq \mathbb{C}^{(n+1)r}$ stetig und*

$$H_r(x, z) = \begin{pmatrix} p_1(x) \\ \vdots \\ p_k(x) \\ z_{1,0} + z_{1,1}x_1 + ...z_{1,n}x_n \\ \vdots \\ z_{r,0} + z_{r,1}x_1 + ...z_{r,n}x_n \end{pmatrix},$$

dann ist $H_r(x, \phi(t)) = 0$ eine Homotopie

Für ein $z \in \mathbb{C}^{(n+1)r}$ sind die Nullstellen von $H_{p_1,...,p_k}(\cdot, z)$ der Schnitt der Varietät $\mathcal{V}(p_1, ..., p_k)$ mit r affinen Hyperebene, die durch den Parameter z bestimmt sind. Generisch entspricht die Anzahl der isolierten Lösungen also genau der Summe der Grade der Komponenten der Dimension r von $\mathcal{V}(p_1, ..., p_k)$. Für den Beweis von Punkt eins von Satz 2.2.4 fehlt nun bloß noch, dass für kein $z \in X_r$ die Anzahl der isolierten Lösungen von $H_r(\cdot, z)$ größer sein kann als der Grad von $\mathcal{V}(p_1, ..., p_k)$.
Dazu bestimmen wir zunächst wie, X_r aussieht. Zunächst bezeichnen wir mit V_i die Vereinigung der Komponenten von V der Dimension i. Sei nun

$$Y_r = \{(H_1, ..., H_r) | \forall i \in [r] : H_i \subset \mathbb{P}^{(n+1)} \text{ Hyperebene} \wedge \dim((\overline{V})_r \cap H_1 \cap ... \cap H_r) = 0 \wedge \forall i < r : (\overline{V})_i \cap H_1 \cap ... \cap H_r = \varnothing\}.$$

Nach Satz 1.4.14 enthält Y_r Zariski-offene Mengen. Wir definieren nun X_r als jene Koeffizienten, die Tupel von affinen Hyperebenen definieren, die Dehomogenisierungen von Tupeln von Hyperebenen aus Y_r entsprechen. Also

$$X_r = \{(z_1, ..., z_r) \in \mathbb{C}^{(n+1)r} | \exists (H_1, ..., H_r) \in Y_r : \forall i \in [r] : \mathcal{V}(z_{i,0} + z_{i,1}x_1 + ... + z_{i,n}x_n) = \tilde{H}_i\}.$$

Sei nun $z \in X$, so definiert z die Hyperebenen $\tilde{H}_1, ..., \tilde{H}_r \subseteq \mathbb{C}^{(n+1)d}$, wobei $H_1, ..., H_r \in Y_r$. Aufgrund der speziellen Wahl von Y_r bleiben von den Komponenten der Dimension kleiner r von $\overline{V}$ nach Schnitt mit den Hyperebenen keine Punkte mehr übrig, von den Komponenten der Dimension r bleiben nur Isolierte Punkte übrig und nach Bemerkung 1.4.18 höchstens so viele, wie die Summe der Grade der Komponenten der Dimension r, und nach dem Connectedness-Theorem ([9, Satz 4.16]) und Satz 1.4.12 kommen von den Komponenten mit Dimension größer r keine weiteren isolierten Punkte dazu. Also ist die Anzahl der Isolierten Punkte in $\overline{V} \cap H - 1 \cap ... \cap H_r$ durch die Summe der Grade der r-dimensionalen Komponenten von $\overline{V}$ beschränkt. Dies entspricht jedoch der Summe der Grade der r-dimensionalen Komponenten von V. Da weiter $V \cap \tilde{H}_1 \cap ... \cap \tilde{H}_r \subseteq \overline{V} \cap H_1 \cap ... \cap H_r$, gilt diese Abschätzung nun auch für $V \cap \tilde{H}_1 \cap ... \cap \tilde{H}_r$.

Bemerkung 2.4.2. *Diese umständliche Einschränkung des Parameterraumes auf X ist notwendig, wie man an dem folgenden Beispiel sieht.*
Seien $V, W \subseteq \mathbb{C}^n$ Irreduzible Varietäten mit $\dim(V) = d = \dim(W) + 1$ und $\deg(V) = 1$, $\deg(W) = 10$. Wir betrachten nun die Varietät $U = V \cup W$ für generische Hyperebenen $H_1, ..., H_d$ besteht nun $U \cap H_1 \cap ... \cap H_d$ offensichtlich aus genau einem Punkt. Für generische Wahl von Hyperebenen $H_1, ..., H_{d-1}$ besteht jedoch $U \cap H_1 \cap ... \cap H_{d-1} \cap H_{d-1}$ aus 10 isolierten Punkten, die aus dem Schnitt von W mit den Hyperebenen hervorgehen, sowie aus Komponenten der Dimension 1, die aus dem Schnitt von V mit den Hyperebenen entstehen. Somit kann es für sehr ungeschickte Wahl der Parameter passieren, dass ein Problem mehr isolierte Lösungen hat als ein generisches Problem.

Bemerkung 2.4.3. *Auch für diese Homotopie-Verfahren können wir etwas ähnliches wie Lemma 2.3.3 verwenden. Zwar ist die Homotopie nicht linear, sie ist jedoch linear in den letzten r Komponenten und konstant (bezüglich den Parametern) in den Ersten Komponenten. Nun gilt $H_r(x, az_1 + bz_2) = aH_r(x, z_1) + bH_r(x, z_2) - (a+b-1)H_r(x, 0)$. Nun gilt jedoch weiter $(\exists y \in \mathbb{C}^m : H_r(x, y) = 0) \Rightarrow H_r(x, 0) = 0$. Multiplikation mit Konstanten ändert nichts an den Lösungen eines Gleichungssystems, somit können wir die Homotopie $H_r(x, \phi(t))$ mit ϕ wie beim Gamma Trick in folgender Form schreiben:*

$$H_r(x, t) = 0 \Leftrightarrow H_r(x, \gamma t z_0 + (1-t)z_1) = 0 \Leftrightarrow H_r(x, \gamma t z_0) + H_r(x, (1-t)z_1) = 0.$$

2.5 Randomization

In diesem Abschnitt lernen wir einige Resultate kennen, die uns ermöglichen in Situationen, in denen wir Homotopie-Verfahren für nicht-quadratische Gleichungssysteme anwenden wollen, unsere Gleichungssyteme so abzuändern, das sie quadratisch sind und alle für uns entscheidenden Informationen erhalten bleiben. Dabei können wir uns auf Situationen, in denen unser Gleichungssystem überbestimmt ist, einschränken. Der Grund dafür ist, dass wir stets Systeme betrachten, wo wir mit mit eben so vielen Hyperebenen schneiden bzw. soviele affine Gleichungen zu unserem System hinzunehmen wie die Dimension einer irreduziblen Komponente unserer Varietät. Und nach Satz 1.4.12 ist die Anzahl der Polynome, die zur Definition der Varietät benutzt wurden, addiert zu der Dimension einer irreduziblen Komponente der Varietät stets $\geq n$

Wir gehen also davon aus, dass wir ein System $F(x) = 0$ mit $F : \mathbb{C}^n \to \mathbb{C}^m$ polynomial mit $n \leq m$ gegeben haben. Die Idee wird nun sein, eine Zufallsmatrix $M \in \mathbb{C}^{s \times m}$ herzunehmen und dann das System $MF(x) = 0$ bestehend aus s Gleichungen in n Unbekannten zu lösen. offensichtlich ist die von $F(x) = 0$ definierte Varietät $\mathcal{V}(F)$ in der von $MF(x) = 0$ definierten Varietät $\mathcal{V}(MF)$ enthalten. Der folgende Satz zeigt das $\mathcal{V}(MF)$ für generische Wahl von M „klein"genug bleibt.

Satz 2.5.1. *Sei $F = (f_1, ..., f_m)^T : \mathbb{C}^n \to \mathbb{C}^m$ mit $\forall i \in [m] : f_i \in \mathbb{C}[x]$ dann gibt es für jedes $s \in \mathbb{N}$ eine Zariski-offene Teilmenge $U \subseteq \mathbb{C}^{s \times m}$, so dass $\forall M \in U : \mathcal{V}(MF) \backslash \mathcal{V}(F)$ ist leer oder hat Dimension $n - s$*

Beweis. Der Satz ist ein Spezialfall von [2, Satz A.8.7] für den Beweis möchte ich dorthin verweisen. □

Bemerkung 2.5.2. *Der Schnitt einer affinen algebraischen Varietät mit dem Komplement einer affinen algebraischen Varietät nennt man quasiaffine Varietät. Sind die beiden Varietäten projektiv sprechen wir von quasiprojektiven Varietäten.*

Satz 2.5.3. *Seien $A, B \subseteq \mathbb{C}^n$ algebraische Varietäten, dann gilt $\dim(A \backslash B) = \dim(\overline{A \backslash B})$, wobei hier der Abschluss in der Zariski-Topologie gemeint ist, und die Dimension der quasiaffinen Varietät $A \backslash B$ der Dimension als topologischer Raum mit der induzierten Zariski-Topologie entspricht.*

Beweis. [5, Kapitel I: 1.10] □

Korollar 2.5.4. *Seien $A, B \subseteq \mathbb{C}^n$ algebraische Varietäten mit $\dim(A \backslash B) = 0$, dann besteht $A \backslash B$ nur aus endlich vielen punkten.*

Beweis. Nach Satz 2.5.3 gilt $0 = \dim(A \backslash B) = \dim(\overline{A \backslash B})$ und nach Satz 1.4.6 besteht somit $\overline{A \backslash B}$ nur aus endlich vielen Punkten also auch $A \backslash B$ □

Konstruktion 2.5.5 („Total-Degree"-Homotopie-Verfahren mit Randomization)**.** *Gehen wir nun davon aus das wir ein überbestimmtes Gleichungssystem (m Gleichungen in n Variablen mit $m > n$) haben, von dem wir mit einem „Total-Degree"-Homotopie-Verfahren die isolierten Lösungen bestimmen wollen. Dann randomizieren wir mithilfe einer zufälligen $n \times m$ Matrix. Nach Satz 2.5.1 und Satz 2.5.4 kommen durch das randomizieren nur endlich viele Punkte hinzu, die isolierten Lösungen des ursprünglichen Systems bleiben also isoliert, und es kommen schlimmstenfalls endlich viele Lösungen hinzu, die nicht in der ursprünglichen Varietät enthalten sind. Diese unerwünschten Punkte können wir jedoch leicht durch Einsetzen in das ursprüngliche Gleichungssystem ausmachen und aussortieren.*

Bemerkung 2.5.6. *Da die Determinante eine polynomiale Funktion der Koeffizienten einer Matrix ist, sehen wir schnell, dass eine generische Matrix invertierbar ist. Wählen wir nun $M \in \mathbb{C}^{n \times m}$ generisch wobei $m > n$, so können wir M darstellen als $M = (M'|A)$ mit $M' \in \mathbb{C}^{n \times n}$ invertierbar und $A \in \mathbb{C}^{n \times m-n}$. Nun ändert Multiplikation mit einer invertierbaren Matrix die Lösungsmenge unseres Gleichungssystems F nicht. Die Probleme $MF = 0$ und $(M')^{-1}MF = 0$ sind somit äquivalent, und statt $M \in \mathbb{C}^{n \times m}$ generisch zu wählen, brauchen wir nur ein $A \in \mathbb{C}^{n \times m-n}$ generisch zu wählen und betrachten dann $M = (I_n|A)$. Weiter können wir die Reihenfolge unserer Komponenten von F frei wählen und wir ordnen sie nach absteigendem Grad. Dies hat zusammen mit der speziellen Wahl von M zur Folge, dass der Grad der Komponenten von MF möglichst gering bleibt, da zu den ersten n Komponenten stets nur Linearkombinationen von Komponenten mit niedrigerem oder gleichem Grad addiert werden. Durch dieses Vorgehen können wir die Anzahl von Pfaden, denen wir beim „Total-Degree"Homotopie-Verfahren folgen müssen, minimieren.*

Der Nächste Satz wird fürs Membership-Testing mit dem „Slice “-Homotopie-Verfahren entscheident sein.

Satz 2.5.7. *Sei A eine irreduzible Komponente von $V := \mathcal{V}(p_1, ..., p_m)$ mit $\dim(A) = n - k$, dann ist für eine generische Matrix $M \in \mathbb{C}^{k \times m}$ A auch eine irreduzible Komponente von $VM := \mathcal{V}(M(p_1, ..., p_m)^T)$*

Beweis. Offensichtlich ist A irreduzible Untervarietät von VM. Damit A nun auch irreduzible Komponente von VM ist, bleibt zu zeigen, dass es keine irreduzible Varietät $B \subseteq VM$ mit $A \subsetneq B$ gibt.
Sei nun B irreduzibel mit $A \subseteq B \subseteq VM$. Wir zeigen $A = B$.
Es gilt:

$$B = (B \cap V) \cup (B \cap (VM \backslash V)) = (B \cap V) \cup (B \cap (\overline{VM \backslash V})).$$

Da B irreduzibel ist, ist nun $B \subseteq V$ oder $B \subseteq \overline{VM \backslash V}$. Wir betrachten nun diese zwei Fälle:
Sei $B \subseteq \overline{VM \backslash V}$ dann gilt nach Satz 2.5.3 und Satz 2.5.1 $\dim(B) \leq \dim(\overline{VM \backslash V}) = \dim(VM \backslash V) = n - k = dim(A)$ und somit $B = A$.
Falls $B \subseteq V$ gilt $B = A$ da A als irreduzible Komponente von V in keiner anderen Irreduziblen Untervarietät von V echt enthalten ist. □

3 Algorithmus

Nun haben wir alle Vorarbeit geleistet und können uns anschauen wie unser Algorithmus funktioniert, dabei folgen wir [1, Kapitel 9 und 10]. Führen wir uns nochmal vor Augen was unsere Ausgangssituation ist: Wir haben eine endliche Menge von Polynomen gegeben und wollen Informationen über die Irreduzible Zerlegung der von diesen Polynomen definierten Varietät gewinnen. Um den Algorithmus zu verstehen ist es sinnvol ihn in mehrere Phasen aufzuteilen.
In der ersten Phase wollen wir für jede Dimension alle Komponenten einer gegebenen Dimension durch Schnitte mit affinen Hyperebenen so manipulieren, dass bloß noch endlich viele isolierte Punkte aus den ursprünglichen Komponenten über bleiben. Diese Punkte können wir anschließend mit unserem Homotopie-Verfahren bestimmen, leider können wir nicht ausschließen, dass auch Punkte aus höherdimensionalen Komponenten von unserem Homotopie-Verfahren gefunden werden. Die Menge der gefundenden Punkte speichern wir und nennen diese Mengen Witness-Supersets.
Im zweiten Schritt wollen wir überprüfen, welche der im letzten Schritt gefundenen Punkte nicht zu einer Komponente der Richtigen Dimension gehört und diese aussortieren. Damit haben wir unsere sogenannten reduzierten Witness-Supersets gefunden, die endlich viele Sample-Punkte aller irreduzibler Komponenten einer gegebenen Dimension enthalten.
Als letztes gilt es die Witness-Supersets entsprechend der irreduziblen Komponenten zu partitionieren so dass wir die sogenannten Witness-Sets erhalten. Das Witness-Set zu einer irreduziblen Komponente enthält eine Anzahl zufälliger Sample von Punkten aus der entsprechenden Komponente. Nun können wir alle wichtigen informationen über die Komponente entweder direkt aus dem Witness-Set oder durch erneute Anwendung eines „Slice“-Homotopie-Verfahrens bekommen. Die Punkte des Witness-Sets verwenden wir dabei als Startpunkte.

3.1 Phase 1: Slicing

Die Grundlage dieses Abschnitts ist der Umstand, dass die Wohldefiniertheit des Grades zusammen mit Satz 1.4.19, garantiert, dass wir, wenn wir eine gegebene Varietät mit d zufälligen Hyperebenen schneiden, mit Wahrscheinlichkeit 1 eine Menge isolierter Punkte bekommen, die zu Komponenten der Dimension d gehören und deren Anzahl nicht von der Wahl der Hyperebenen abhängt.
Dabei brauchen wir Satz 1.4.19 um zu garantieren, dass die isolierten Punkte die aus dem Schnitt einer d-dimensionalen Komponente mit d generischen Hyperebenen entstehen, nicht auch zusätzlich in einer Komponente anderer Dimension liegen und somit, wenn wir die ganze Varietät (statt nur der Komponente) mit den Hyperebenen schneiden es nicht passieren kann, dass diese Punkte tatsächlich nicht isoliert sind.
Wir verwenden nun ein „Total-Degree"-Homotopie-Verfahren, um all diese isolierten Lösungen zu finden. So gehen wir nun Dimension für Dimension durch, schneiden stets mit entsprechend vielen Hyperebenen und bestimmen die isolierten Punkte. Wir müssen allerdings nicht jede Dimension durchtesten, so wissen wir, dass jede irreduzible Komponente mindestens Dimension $n - m$ hat, wobei m die Anzahl der Gleichungen in dem definierenden System angibt, wir brauchen also keine niedrigeren Dimensionen betrachten. Dimension n müssen wir ebenfalls nicht überprüfen da $\mathbb{C}^n$ die einzige Varietät in $\mathbb{C}^n$ ist, die Dimension n hat, und sobald eines der definierenden Polynome nicht das 0-Polynom ist, dies ausgeschlossen ist.

Da im Allgemeinen das von uns betrachtete System nach, Schneiden mit den Hyperebenen überbestimmt ist, gehen wir wie im Kapitel über "Randomization"vor, um eine quadratische Homotopie zu finden und die isolierten Lösungen zu bestimmen.
Die so gefundenen Sample-Points speichern wir als sogenannte Witness-Supersets $\hat{W}_i$ wobei i die entsprechende Dimension angibt. Zusätzlich speichern wir auch zu jeder Dimension die affine Hyperebene, die wir benutzt haben bzw. die Grad 1 Polynome, mit denen wir sie definiert haben.
$\hat{W}_i$ enthält nun Punkte aus den i-dimensionalen Komponenten, jedoch können wir nicht ausschließen, dass $\hat{W}_i$ auch Punkte aus höherdimensionalen Komponenten enthält. Im nächsten Abschnitt überlegen wir uns, wie wir diese Punkte aus $\hat{W}_i$ entfernen können um unsere sogenannten reduzierten Witness-Supersets zu erhalten. Diese teilen wir dann im letzten Schritt entsprechend der Komponenten auf.

Definition 3.1.1 (Reduziertes Witness-Superset, Witness-Set)**.** *Sei $\hat{W}_i$ ein Witness-Superset der Varietät V zur Dimension i und $X \subseteq V$ die Vereinigung aller Komponenten von V, die Dimension i haben. Dann nennen wir $W_i = \hat{W}_i \cap X$ ein reduziertes Witness-Superset der Varietät V zur Dimension i.*
Sei W_i ein reduziertes Witness-Superset der Varietät V zur Dimension i und $X \subseteq V$ eine Komponente von V mit $\dim(X) = i$. Dann nennen wir $W_{i,j} = W_i \cap X$ Witness-Set von V zur i-dimensionalen Komponente $X \subseteq V$.

3.2 Phase 2: Junk-Removal und Membership-Testing

Der zentrale Punkt beim Entfernen der ungewünschten Punkte aus den Witness-Supersets ist das Membership-Testing, was darüber hinaus auch eine wichtige Anwendung unseres Fertigen Algorithmus sein wird. Beim Membership-Testing hat man ein reduziertes Witness-Superset oder später ein Witness-Set gegeben und kann damit überprüfen, ob ein weiterer gegebener Punkt in einer der zu dem Witness-Superset gehörigen Komponenten bzw. in der zu dem Witness-Set gehörigen Komponente liegt.
Die Idee beim Junk-Removal ist, vorausgesetzt man hat ein solches Membership-Testing Verfahren, sehr simpel. Wir fangen mit dem nichtleeren Witness-Superset zu den Komponenten höchster Dimension an,

von diesem wissen wir, dass es keine überflüssigen Punkte enthält, einfach da es keine höherdimensionalen Komponenten gibt. Betrachten wir nun das Superset zu den Komponenten mit der zweitgrößten Dimension. So können wir mit unserer Membership-Testing Routine für jeden der Punkte aus dem Superset überprüfen, ob diese in einer Komponente höheren Grades enthalten sind, und sie gegebenenfalls entfernen. So können wir uns Dimension für Dimension vorwärtsarbeiten, wobei der Aufwand immer größer wird da wir nun für jeden Punkt nicht mehr nur für eine Dimension überprüfen müssen, ob er in einer Komponente dieser Dimension liegt, sondern für alle höheren Dimensionen. Durch das Entfernen aller Punkte, die in höherdimensionalen Komponenten liegen, wird unser Witness-Superset zu einem reduzierten Witness-Superset.

Konstruktion 3.2.1 (Membership-Testing Routine)**.** *Wir haben ein $a \in \mathbb{C}^n$ gegeben und möchten herausfinden, ob a in einer Komponente der Dimension d liegt. Dann konstruieren wir zunächst einen zufälligen affinen Unterraum der Codimension d, der a enthält, bzw. ein linear affines Gleichungssystem L', welches diesen Raum definiert. Dies können wir zum Beispiel einfach tun, indem wir eine zufällige Matrix $A \in \mathbb{C}^{d\times n}$ mit vollem Rang wählen und $L'(x) = A(x-a)$ setzen. Da eine generische Matrix bekanntlich vollen Rang hat, reicht es eine beliebige Zufallsmatrix zu wählen. Sei weiter L das linear affine Gleichungssystem das wir zur Konstruktion unseres Witness-Supersets W_d verwendet haben. Wir verwenden nun eine „Slice"-Homotopie um dieses Problem zu lösen. Dazu verwenden wir den „Gamma Trick", um einen Weg zu erhalten, der unseren Anforderungen entspricht und wenden die Vereinfachung aus Bemerkung 2.4.3 an. Damit erhalten wir die folgende Homotopie:*

$$H_d(x,t) = \begin{pmatrix} f(x) \\ (\gamma)tL(x) + (1-t)L'(x) \end{pmatrix} = 0$$

Das γ können wir dabei auch weglassen, da wir durch die zufällige Wahl von L' bereits eine zufällige Richtung für den Weg gewählt haben. Dabei ist f ein polynomiales Gleichungssystem, das unsere Varietät definiert, falls f nun aus $r > d$ Polynomen besteht, ist diese Homotopie nicht quadratisch und wir müssen randomizieren, dies tun wir indem wir f durch Mf ersetzen, wobei $M \in \mathbb{C}^{n-d\times r}$ zufällig gewählt, also mit Wahrscheinlichkeit 1 generisch ist. Nach Satz 2.5.7 sind die irreduziblen Komponenten der Dimension d auch irreduzible d-dimensionale Komponenten von $\mathcal{V}(Mf)$.
Wir folgen nun den Lösungspfaden dieser Homotopie, angefangen mit den Punkten aus unserem reduziertem Witness-Superset. Da der Grad einer irreduziblen Varietät wohldefiniert ist, die Lösungspfade stetig sind und nach Satz 1.4.19 an jedem Punkt unserer Lösungspfade in einer Umgebung dieser Lösungspfade keine Punkte aus anderen irreduziblen Komponenten liegen, können die Lösungspfade nicht zwischen Komponenten wechseln und unser Homotopie-Verfahren liefert, falls L' ein zulässiges Zielsystem ist also falls wir L' mit einem $z \in X_d$ identifizieren können, genau die Punkte im Schnitt der irreduziblen Komponenten mit $\mathcal{V}(L')$ und somit insbesondere auch a genau dann, wenn a in einer der Komponenten liegt.

Bemerkung 3.2.2. *An dieser Stelle sehen wir, warum wir sowohl das „total degree"-Homotopie-Verfahren brauchen als auch das „Slice"-Homotopie-Verfahren. Das „total degree"-Verfahren brauchen wir um unsere Witness-Supersets und somit die Startpunkte für unsere „Slice"-Verfahren zu finden. Allerdings könnten wir fürs Membership-Testing nicht auch diese Verfahren verwenden, da wir dann nicht mehr gewährleisten könnten, dass die Endpunkte auf den selben Komponenten liegen wie die Startpunkte, was hier aber unbedingt notwendig ist.*
Wir können, sobald wir unsere Witness-set gefunden haben, genauso vorgehen um zu einer gegebenen

Komponente zu überprüfen, ob ein Punkt in dieser liegt. Wir müssen bloß, statt alle Punkte aus dem reduzierten Witness-Superset als Startpunkte für unser Homotopie-Verfahren zu benutzen, nur die aus dem Witness-Set der Komponente nehmen.

Noch offen ist die Frage wie wir garantieren, dass L' mit Wahrscheinlichkeit 1 ein zulässiges Zielsystem ist. Dies folgt jedoch aus Satz 1.4.14 und Bemerkung 1.4.15, da d generische projektive Hyperebenen die a enthalten in Y liegen, und da die Menge der homogenisierten affinen Hyperebenen die a enthalten Zariski-offen in der Menge der projektiven Hyperebenen, die a enthalten ist. Der Beweis dieser letzten Aussage geht analog zum Beweis der Aussage ohne die Einschränkung auf Hyperebenen, die a enthalten, diesen Beweis findet man als Teil des Beweises von Satz 1.4.17

3.3 Phase 3: Trace Test und Partitionierung

In diesem Schritt wollen wir die sogenannten Witness-Sets konstruieren, indem wir unsere reduzierten Witness-Supersets entsprechend der Zugehörigkeit zu den irreduziblen Komponenten aufteilen, dabei gehen wir vor wie in [1, Abschnitt 10.2], der theoretische Hintergrund wird in [2, Abschnitt 15.5] behandelt.
Entscheidend für diesen Abschnitt ist das folgende Resultat.

Satz 3.3.1. *Sei $V \subseteq \mathbb{C}^n$ eine irreduzible Varietät der Dimension d, sei weiter L ein generischer affiner Unterraum mit Kodimension d und $L(t)$ für $t \in \mathbb{C}$ ein affiner Unterraum der aus L durch Parallelverschiebung um t in eine vorher definierte Richtung entsteht. Für generisches $L(t)$ besteht $V \cap L(t)$ aus $\deg(V)$ vielen Punkten. Bezeichne weiter $C(t)$ den geometrischen Schwerpunkt der Punkte aus $V \cap L(t)$ (mit Vielfachheit), dann ist $C(t)$ eine affine Funktion. Weiter gilt dies für keine echte Teilmenge der Punkte aus $V \cap L(t)$.*

Beweis. [2, Abschnitt 15.5] □

Da der Durchschnitt affiner Funktionen affin ist, gilt auch für eine Varietät, die Vereinigung von irreduziblen Varietäten gleicher Dimension ist, dass der geometrische Schwerpunkt dieser Varietät geschnitten mit einem affinen Unterraum dessen Kodimension der Dimension der Varietät entspricht, affin ist bezüglich parallelverschiebung des Unterraums.
Wir werden nun Teilmengen unserer reduzierten Witness-Supersets suchen und überprüfen, ob ihr geometrischer Schwerpunkt dieses Verhalten besitzt, was bedeutet, dass sie alle Punkte einer Menge von irreduziblen Komponenten geschnitten mit dem affinen Unterraum enthalten. Anschließend werden wir überprüfen, ob eine Teilmenge von ihnen sich ebenfalls so verhält. Falls nicht, haben wir ein Witness-Set für eine irreduzible Komponente gefunden.

Konstruktion 3.3.2 (Trace Test)**.** *Sei $\hat{W}_d$ das reduzierte Witness-Superset für die d dimensionalen Komponenten einer Varietät $V \subseteq \mathbb{C}^n$, sei weiter L der affine Unterraum, der zur Berechnung von $\hat{W}_d$ verwendet wurde, nun wähle ich zufällig $c_1, c_2 \in \mathbb{C}$, $v, \in \mathbb{C}^n$. Für ein $a \in \hat{W}_d$ folgen wir nun der Homotopie aus Konstruktion 3.2.1 zu den Punkten a_1, a_2 in $V \cap (L + c_1 v)$ bzw. $V \cap (L + c_2 v)$ und berechnen $\sigma_a := \frac{a_1 - a}{c_1} - \frac{a_2 - a}{c_2}$. Nach Satz 3.3.1 ist nun, falls $W_{d,i}$ ein Witness-Set ist ,*

$$\sum_{a \in W_{d,i}} \sigma_a = 0 \quad \wedge \quad \forall \varnothing \neq S \subsetneq W_{d,i} : \sum_{a \in S} \sigma_a \neq 0.$$

Wir wollen nun zeigen, dsas mit Wahrscheinlichkeit 1 auch die Umkehrung gilt.
Nun ist nach [2, Abschnitt 15.5] der Pfad eines Punktes unter Verschiebung des affinen Unterraums eine

holomorphe Funktion und somit auch die Linearkombination dieser Funktionen. Wir betrachten nun drei Punkte auf dem Graph dieser Funktion und überprüfen, ob diese kolinear sind. Dabei ist der erste Punkt gegeben, der zweite wird zufällig ausgewählt. Wir gehen nun davon aus, dass die Funktion nicht linear affin ist, dann gibt es nach dem Identitätssatz für holomorphe Funktionen, da eine überabzählbare Teilmenge der komplexen Zahlen stets einen Häufungspunkt besitzt, höchstens abzählbar viele Punkte auf dem Graphen, so dass die drei Punkte kolinear sind. Somit gilt die Umkehrung mit Wahrscheinlichkeit 1.
Dass jede überabzählbare Teilmenge der komplexen Zahlen einen Häufungspunkt besitzt, beweist man per Widerspruch, indem man $\mathbb{C}$ *mit abzählbar vielen kompakten Mengen überdeckt, nun muss der Schnitt der ursprünglichen Menge, falls diee überabzählbar ist, mit einer der kompakten Mengen auch überabzählbar sein, auf diese Menge können wir nun den Satz von Bolzano-Weierstraß anwenden, was uns den gewünschten Widerspruch liefert.*

Mit dem Trace Test Teilen wir nun also unser reduziertes Witness-Superset$\hat{W}_d$ auf in die Witness-Sets $W_{d,1}, ..., W_{d,l_d}$.
Insgesamt haben wir nun zu jeder irreduziblen Komponente unserer Varietät ein Witness-Set bestehend aus Punkten, die in dieser Komponente liegen.

4 Anwendung

Nun, da wir wissen, wie wir unsere Witness-Sets konstruieren können, was den Hauptteil unseres Algorithmus ausmacht, werden wir uns in diesem letzten Abschnitt noch anschauen, was wir anhand unserer Witness-Sets über unsere Varietät aussagen können.

4.1 Dimension und Grad

Diese beiden Informationen bekommen wir direkt aus dem Witness-Set selber, so ist die Dimension der irreduziblen Komponente, die durch das Witness-Set $W_{d,i}$ repräsentiert wird, gleich d. Interessiert uns die Dimension der ganzen Varietät, brauchen wir bloß das Maximum der Dimensionen der irreduziblen Komponenten betrachten.
Der Grad einer irreduziblen Komponente entspricht genau der Mächtigkeit des dazugehörigen Witness-Sets.

4.2 Zugehörigkeit von Punkten

Ob ein gegebener Punkt zu einer irreduziblen Komponente gehört, lässt sich mit der Membership-Testing-Routine (Bemerkung 3.2.2) überprüfen. Überprüfen wir die Zugehörigkeit für jede Komponente, können wir eine Liste aller Komponenten, zu denen der gegebene Punkt gehört, bekommen.

4.3 Sample Punkte

Mit der Membership-Testing Routine (Bemerkung 3.2.2)können wir zu jeder Komponente Punkte im Schnitt dieser Komponente mit einem beliebigen affinen Unterraum der richtigen Dimension generieren.

4.4 Lokale Dimension

Definition 4.4.1 (lokale Dimension)**.** *Sei $V \subseteq \mathbb{C}^n$ eine Varietät, $a \in V$. Dann ist die lokale Dimension von V in a definiert als das Maximum der Dimensionen der irreduziblen Komponenten von V die a enthalten .*

Wir können die lokale Dimension der Varietät V in $a \in V$ berechnen, indem wir für alle Komponenten überprüfen, ob a in ihr liegt und anschließend einfach das Maximum über die Dimensionen dieser Komponenten bilden.
Da sobald wir eine Komponente gefunden haben, in der a liegt, es irrelevant ist ob a auch in Komponenten der selben oder niedrigerer Dimension enthalten ist, ist es sinnvoll die Komponenten nach absteigender Dimension durchzugehen, wir sind dann fertig, sobald wir eine Komponente gefunden haben, in der a liegt.

5 Anmerkungen und Ausblick

In dieser Arbeit haben wir die Funktionsweise eines Algorithmus zur numerischen Berechnung der irreduziblen Zerlegung algebraischer Varietäten erklärt und bewiesen, dass dieser Algorithmus ein Wahrscheinlichkeit-1-Algorithmus ist. Nicht genauer betrachtet haben wir die Auswirkungen von numerischen Fehlern auf die Performance des Algorithmus, sowie die zahlreichen Tricks, die man verwenden kann, um diese Fehler zu minimieren. Beispielsweise benutzt man im Fall von Homotopie-Verfahren spezielle Methoden, wie im einfachsten Fall z.B. ein Newtonverfahren, um die Genauigkeit der gefundenden Lösungen weiter zu verbessern.
Auch die Komplexität unseres Algorithmus haben wir nicht weiter behandelt und auch bezüglich diesem Aspekt gibt es zahlreiche interessante Verfeinerungen des Algorithmus.
Wer sich für diese Fragen interessiert, den möchte ich auf [2] und [1] verweisen. Das Software-Paket „Bertini “das eine Implementierung des hier behandelten Algorithmus enthält, kann man unter https://bertini.nd.edu/download.html kostenlos downloaden.

6 Literaturverzeichniss

Literatur

[1] Daniel J. Bates, Andrew J. Sommese, Jonathan D. Hauenstein, and Charles W. Wampler. *Numerically Solving Polynomial Systems with Bertini*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 2013.

[2] Andrew Sommese and Charles Wampler. *The Numerical Solution of Systems of Polynomial Arising in Engineering and Science*, volume 2005. 01 2005.

[3] Tim Netzer. *Einführung in die Algebraische Geometrie*.

[4] Mateusz Michałek and Bernd Sturmfels. *Invitation to nonlinear algebra*, volume 211. American Mathematical Soc., 2021.

[5] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[6] Joe Harris. *Algebraic geometry: a first course*, volume 133. Springer Science & Business Media, 2013.

[7] Wikipedia contributors. Degree of an algebraic variety — Wikipedia, the free encyclopedia, 2022. URL: https://en.wikipedia.org/wiki/Degree_of_an_algebraic_variety (Version: 10.05.2023).

[8] Terence Tao. Bezout's inequality, 2011. URL:https://terrytao.wordpress.com/2011/03/23/bezouts-inequality/ (Version: 15.05.2023).

[9] David Mumford. *Algebraic geometry I: complex projective varieties*, volume 221. Springer, 1976.

[10] ronno (https://math.stackexchange.com/users/32766/ronno). Bezouts theorem generalization to n dimensions proof reference. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/4682812 (Version: 19.05.2023.

[11] William Fulton. *Intersection theory*, volume 2. Springer Science & Business Media, 2013.

[12] Wikipedia contributors. Theorem of bertini — Wikipedia, the free encyclopedia, 2021. URL:https://en.wikipedia.org/wiki/Theorem_of_Bertini (Version: 19.05.2023).