Institut für Theoretische Informatik

Geometrische Komplexitätstheorie

Bachelorarbeit

Elias L. Kayser

Matrikelnr. 10006908

Erstprüfer:	*PD Dr. Arne Meier*
Zweitprüfer:	*Prof. Dr. Heribert Vollmer*
Betreuer:	*Anselm Haak*

30. März 2021

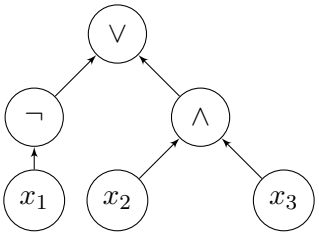
Inhaltsverzeichnis

Einleitung

Seit dem ersten Semester des Informatikstudiums begegnen einem in verschiedenen Vorlesungen aussagenlogische Formeln, etwa

$$\neg x_1 \vee (x_2 \wedge x_3).$$

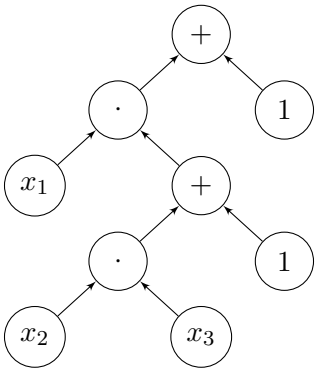
Boolesche Schaltkreise stellen Auswertungsstrategien mittels „$\wedge$“, „$\vee$“ und „$\neg$“-Gattern dar; diese kann man mithilfe eines gerichteten Graphens visualisieren:



Eng verwandt mit boolescher Arithmetik ist die Arithmetik modulo 2, also der Körper $\mathbb{F}_2 = \{0, 1\}$ mit Addition und Multiplikation modulo 2. So lässt sich obiger Schaltkreis auch mittels eines algebraischen Ausdrucks schreiben, etwa

$$((x_1 + 1) + 1) \cdot (x_2 \cdot x_3 + 1) + 1.$$

Dies ist ein Polynom in den drei Variablen $h(x_1, x_2, x_3)$, und eine Auswertungsstrategie kann ebenfalls als Schaltkreis dargestellt werden, hier mit „$+$“ und „$\cdot$“-Gattern



Eine naheliegende Frage für ein Polynom wie h ist, wie effizient es sich mittels eines solchen algebraischen Schaltkreises auswerten lässt. Dies führt zum Komplexitätsmaß $L(h)$, der Größe eines kleinsten Schaltkreises, welcher h berechnet. Ein Polynom mit vielen Variablen, welches in der linearen Algebra auftaucht, ist die Determinante

$$\det \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \cdots & X_{nn} \end{pmatrix} = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)}. \tag{1}$$

Obwohl die Anzahl der Summanden in der Leibnizformel (1) mit wachsendem n mit Größenordnung $O(n!)$ wächst, kennen wir effizientere Algorithmen, um die Determinante auszuwerten. Genauer: Die Folge $L(\det_{n\times n})$ ist polynomiell beschränkt; anschaulich steigt der Berechnungsaufwand von $\det_{n\times n}$ mit wachsendem n beherrschbar. Die Klasse solcher Folgen $(h_n)_n$ wird mit VP bezeichnet, sie ist ein Analogon zur Klasse P.

Lässt man in (1) den Vorfaktor $\operatorname{sign}(\sigma)$ weg, so erhält man die Permanente $\operatorname{perm}_{n\times n}$. Im Kontrast zur Determinante ist bis heute kein effizienter Schaltkreis zur Berechnung der Permanente bekannt. Tatsächlich gehört die Folge $(\operatorname{perm}_{n\times n})_n$ zu den am aufwändigsten zu berechnenden in der Komplexitätsklasse VNP, welche ein algebraisches Analogon zu NP darstellt. Das zentrale Problem der algebraischen Komplexitätstheorie ist *Valiants Hypothese*

$$\mathsf{VP} \overset{?}{\neq} \mathsf{VNP}.$$

Geometrische Komplexitätstheorie

Man kann sich also die Frage stellen, wie man im Raum aller Polynome diejenigen auszeichnen kann, welche geringe Komplexität besitzen, oder sich zumindest durch Polynome geringer Komplexität approximieren lassen.

Hier setzt die geometrische Komplexitätstheorie an: Es stellt sich heraus, dass diese Menge eine geometrische Struktur trägt, sie ist eine sogenannte algebraische Menge. Das mathematische Gebiet der algebraischen Geometrie bietet Methoden, um solche Mengen zu studieren.

Eine Konsequenz dieser Struktur ist zum Beispiel, dass es Funktionen $F_1, \dots, F_k$ auf dem Raum der Polynome gibt, sodass ein Polynom h genau dann durch Polynome kleiner Komplexität approximiert werden kann, wenn

$$F_1(h) = \cdots = F_k(h) = 0.$$

Eine weitere Komponente der GCT ist die Verwendung darstellungstheoretischer Methoden: Polynome wie $\det_{n\times n}$ und $\operatorname{perm}_{n\times n}$ weisen viele Symmetrien auf. Um diese systematisch zu untersuchen und ihre Auswirkungen auf die Komplexität zu beurteilen, werden Methoden aus der Darstellungstheorie verwendet.

Das Ziel dieser Arbeit ist es, eine Einführung in die geometrische Komplexitätstheorie zu geben. Dabei werden die benötigten mathematischen Grundlagen aus der Algebra, Analysis, algebraischer Geometrie und Darstellungstheorie eingeführt und anhand von konkreten Beispielen aus der Komplexitätstheorie illustriert. Weiterhin wird ein Überblick über bisherige Meilensteine der GCT gegeben und bekannte Forschungsergebnisse werden diskutiert.

Notation

In dieser Arbeit werden folgende Notationen und Konventionen verwendet.

- Die Menge der natürlichen Zahlen ohne 0 wird mit $\mathbb{N} = \{1, 2, 3, \dots\}$ bezeichnet, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
- Für eine Funktion $p\colon \mathbb{N} \to \mathbb{N}$ sei

  $$O(p(n)) = \{\, q\colon \mathbb{N} \to \mathbb{N} \mid \text{es gibt } c, n_0 \in \mathbb{N} \text{ mit } q(n) \leq c \cdot p(n)\ \forall n \geq n_0 \,\}.$$

  Ein Ausdruck wie $2^{O(p(n))}$ ist elementeweise zu verstehen. Wir schreiben machmal etwas ungenau $q(n) = O(p(n))$ statt $q(n) \in O(p(n))$.
- $p\colon \mathbb{N} \to \mathbb{N}$ ist *polynomiell beschränkt*, falls es ein $c \in \mathbb{N}$ gibt mit $p(n) \in O(n^c)$.
- Die Matrizen mit m Zeilen und n Spalten und Einträgen aus einer Menge M bezeichnen wir mit $\mathrm{Mat}_{m\times n}(M)$. Für $m = n$ schreiben wir $\mathrm{Mat}_n(M)$.
- Ein Graph $G = (V, E)$ ist ein endlicher *gerichteter* einfacher Graph, d. h. $E \subseteq V \times V$. Der ein-/ausgehende Grad eines Knotens wird mit $\deg_{\text{in}}(v)/\deg_{\text{out}}(v)$ bezeichnet.
  - Ein Zykel ist ein Tupel von Knoten $(v_0, v_1, \dots, v_n)$ $(n \geq 1)$ mit $(v_{i-1}, v_i) \in E$, $v_n = v_0$ und $v_i \neq v_j$ für $0 \leq i < j \leq n - 1$.
  - G ist azyklisch, falls G keine Zykel enthält.
- Es werden in dieser Arbeit Polynome in drei verschiedenen Kontexten auftreten. Um Missverständnisse zu vermeiden, werden verschiedene Buchstaben verwendet:
  - Polynomiell beschränkte Funktionen $\mathbb{N} \to \mathbb{N}$ als Schranke für Komplexität:

    $$p(n), q(n), \dots.$$

  - Polynome, deren Komplexität wir untersuchen wollen:

    $$f, g, \dots \in K[X_1, \dots, X_n].$$

  - Polynome als Funktionen *auf* einem Raum von Polynomen (Kapitel 3):

    $$F, G, \dots \in \mathbb{C}[T_1, \dots, T_m].$$

Kapitel 1

Mathematische Grundlagen

In diesem Kapitel führen wir die benötigten mathematischen Begriffe aus der Algebra und Topologie ein. Wichtig für diese Arbeit sind die Polynomringe in vielen Variablen, sowie Monoidoperationen.

Der Inhalt dieses Abschnittes wird in jedem Lehrbuch zur Algebra behandelt, etwa dem von Lang [Lan02]. Die Grundbegriffe der Topologie werden zum Beispiel im Analysis 2 Buch von Forster eingeführt [For17].

1.1 Algebraische Strukturen

Sei M eine Menge und $*\colon M \times M \to M$ eine Verknüpfung auf M. Wir verwenden die Infixnotation $*(a,b) = a * b$.

- $*$ ist *assoziativ*, falls

$$a * (b * c) = (a * b) * c \qquad \text{für alle } a,b,c \in M.$$

- $*$ ist *kommutativ*, falls

$$a * b = b * a \qquad \text{für alle } a,b \in M.$$

- $e \in M$ ist ein (beidseitig) *neutrales Element* bezüglich $*$, falls

$$a * e = e * a = a \qquad \text{für alle } a \in M.$$

- $*$ besitzt (beidseitige) *inverse Elemente* bezüglich des neutralen Elementes e, falls es zu jedem $a \in M$ ein $a^{-1} \in M$ gibt mit $a * a^{-1} = a^{-1} * a = e$.
- Ist $+$ eine weitere Verknüpfung auf M, so heißt $*$ *distributiv* über $+$, falls

$$a * (b + c) = (a * b) + (a * c), \quad (a + b) * c = (a * c) + (b * c) \qquad \text{für alle } a,b,c \in M.$$

Im Falle der Existenz neutraler bzw. inverser Elemente sind diese durch ihre definierende Eigenschaften eindeutig festgelegt, man kann also von *dem* neutralen Element sprechen.

Definition 1.1.1 (Monoid, Gruppe)**.**
Ein *Monoid* $(G, *, e)$ ist ein Menge G zusammen mit einer zweistelligen Verknüpfung $*$, welche assoziativ ist, und für die e ein neutrales Element ist. Existieren zusätzlich inverse Elemente in G, so ist G eine *Gruppe*.
Ist $*$ kommutativ, so spricht man von einem kommutativen Monoid bzw. einer kommutativen Gruppe. ⌟

Definition 1.1.2 (Ring, Integritätsring, Körper)**.**

(i) Ein *Ring* $(R, +, \cdot, 0, 1)$ ist eine Menge R zusammen mit zwei binären Verknüpfungen $+$, $\cdot$, sodass $(R, +, 0)$ eine kommutative Gruppe, $(R, \cdot, 1)$ ein Monoid und $\cdot$ distributiv über $+$ ist.
Ist $\cdot$ kommutativ, so spricht man von einem kommutativen Ring.

(ii) Ein *Integritätsring* oder nullteilerfreier Ring R ist ein kommutativer Ring mit $1 \neq 0$, sodass für je zwei Elemente $a, b \in R$ gilt

$$a \cdot b = 0 \implies a = 0 \vee b = 0.$$

(iii) Ein *Körper* ist ein kommutativer Ring K, sodass $1 \neq 0$ und jedes Element $a \neq 0$ ein multiplikatives Inverses besitzt. ⌟

Sind die Verknüpfungen aus dem Kontext klar, so sprechen wir auch einfach nur von einem Ring R oder einer Gruppe G.

Beispiel 1.1.3.

- Die bijektiven Abbildungen einer Menge X in sich selbst bilden mit der Verkettung von Abbildungen eine Gruppe

$$\mathrm{Sym}(X) \coloneqq (\{\, \sigma \colon X \to X \mid \sigma \text{ bijektiv} \,\}, \circ, \mathrm{id}_X).$$

  So definieren wir die *symmetrische Gruppe* als $\mathcal{S}_n \coloneqq \mathrm{Sym}(\{1, \ldots, n\})$.
- $\mathbb{Z}$ ist ein Integritätsring, welcher kein Körper ist.
  Die *Moduloarithmetik* der Restklassen $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ mod n bilden einen kommutativen Ring, welcher genau dann ein Körper ist, wenn n eine Primzahl p ist. In diesem Fall schreiben wir auch $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$.
- Die bekannten Zahlbereiche $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ bilden Körper
- Die $n \times n$-Matrizen $\mathrm{Mat}_n(K)$ über einem Grundkörper K bilden mit komponentenweiser Addition und Matrixmultiplikation einen Ring. Das neutrale Element der Multiplikation, die *Einheitsmatrix*, notieren wir mit I_n.
  Die Teilmenge der invertierbaren Matrizen $\mathrm{GL}_n(K)$ bildet eine Gruppe, welche für $n \geq 2$ nicht kommutativ ist.
- Ist X eine Menge und R ein Ring, so bildet die Menge der Abbildungen $\mathrm{Abb}(X, R)$ einen Ring, wenn man für $f, g \in \mathrm{Abb}(X, R)$, $x \in X$ definiert

$$(f \pm g)(x) = f(x) \pm g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$ ⌟

Definition 1.1.4 (Monoid-, Gruppen-, Ringhomomorphismus)**.**

(i) Sind $(G, *_G, e_G)$, $(H, *_H, e_H)$ Monoide, so ist ein *Monoidhomomorphismus* eine Abbildung $\phi \colon G \to H$ mit

$$\phi(e_G) = e_H, \qquad \phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) \qquad \text{für alle } g_1, g_2 \in G.$$

Sind G, H Gruppen, so sprechen wir von einem *Gruppenhomomorphismus*, in diesem Fall ist dann auch $\phi(g)^{-1} = \phi(g^{-1})$ für alle $g \in G$ erfüllt.

(ii) Sind $(R, +_R, \cdot_R, 0_R, 1_R)$, $(S, +_S, \cdot_S, 0_S, 1_S)$ Ringe, so ist ein *Ringhomomorphismus* eine Abbildung $R \to S$, welche zugleich ein Gruppenhomomorphismus $(R, +_R, 0_R) \to (S, +_S, 0_S)$ und ein Monoidhomomorphismus $(R, \cdot_R, 1_R) \to (S, \cdot_S, 1_S)$ ist.

⌟

Definition 1.1.5 (Untergruppe, Ideal)**.**

(i) Es sei G eine Gruppe. Eine *Untergruppe* ist eine Teilmenge $U \subseteq G$, sodass $e_G \in U$ und für $a, b \in U$ auch $a * b^{-1} \in U$ ist. In diesem Fall ist U mit der eingeschränkten Verknüpfung wieder eine Gruppe.

(ii) Ein *Ideal* I in einem kommutativen Ring R ist eine Untergruppe von $(R, +, 0)$, sodass für $r \in R$, $a \in I$ auch $r \cdot a \in I$ gilt. ⌟

Definition 1.1.6 (Quotientenring)**.**
Ist $I \subseteq R$ ein Ideal in einem kommutativen Ring, so ist der *Quotientenring* R/I folgendermaßen definiert:

- $r \sim_I s :\Longleftrightarrow r - s \in I$ definiert eine Äquivalenzrelation auf R. Die Äquivalenzklasse von $r \in R$ hat die Gestalt

$$[r]_\sim = r + I = \{\, r + a \mid a \in I \,\}.$$

- Die Menge der Äquivalenzklassen notieren wir mit R/I. Die Menge R/I wird zu einem kommutativen Ring, in dem Addition und Multiplikation auf den Repräsentanten definiert werden:

$$[r]_\sim \pm [s]_\sim \coloneqq [r \pm s]_\sim, \qquad [r]_\sim \cdot [s]_\sim \coloneqq [r \cdot s]_\sim.$$

  Null- und Einselement sind die Restklassen $[0]_\sim$ und $[1]_\sim$, die Ringaxiome von R vererben sich so auf R/I. ⌟

Beispiel 1.1.7.

- Die geraden Zahlen bilden ein Ideal im Ring der ganzen Zahlen $\mathbb{Z}$. Allgemein ist $n\mathbb{Z} = \{\, kn \mid n \in \mathbb{Z} \,\}$ ein Ideal, der Quotientenring ist gerade $\mathbb{Z}/n\mathbb{Z}$.
- Es sei $M \subseteq \mathbb{R}$ eine Menge und

$$I \coloneqq \{\, f \in \mathrm{Abb}(\mathbb{R}, \mathbb{R}) \mid f(x) = 0 \ \forall x \in M \,\} \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R}).$$

  I ist ein Ideal: Sicher ist $0 \in I$, sind $f_1, f_2 \in I$, $g \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$, so ist

$$(f_1 - f_2)(x) = f_1(x) - f_2(x) = 0, \quad (g \cdot f_1)(x) = g(x) \cdot \underbrace{f_1(x)}_{=0} = 0$$

  für alle $x \in M$. Ideale dieser Form werden uns in Kapitel 3 wiederbegegnen. ⌟

1.2 Polynome

Es sei in diesem Abschnitt K ein Körper (die meisten Aussagen gelten aber auch für kommutative Ringe).

Definition 1.2.1 (Polynom, Polynomring)**.**
Ein Polynom über K ist formal ein Ausdruck der Form

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{i=0}^{n} a_i X^i, \qquad a_0, \ldots, a_n \in K.$$

Die a_i sind die Koeffizenten, wir setzen implizit $a_i = 0$ für $i > n$. Summe und Differenz von Polynomen werden Komponentenweise erklärt, die Multiplikation wird gebildet über die Regel

$$\left(\sum_{i=0}^{m} a_i X^i\right) \cdot \left(\sum_{j=0}^{n} b_j X^j\right) = \sum_{k=0}^{m+n} c_k X^k, \qquad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Mit diesen Verknüpfungen wird die Menge der Polynome zu einem Integritätsring $K[X]$. ⌟

Um Polynome in mehreren Variablen zu definieren, führen wir die Multiindexschreibweise ein. Ein *Multiindex* ist ein Tupel $\boldsymbol{k} = (k_1, \dots, k_n) \in \mathbb{N}_0^n$. Wir definieren für $\boldsymbol{k}, \boldsymbol{\ell} \in \mathbb{N}_0^n$

$$|\boldsymbol{k}| \coloneqq k_1 + \cdots + k_n, \quad \boldsymbol{k} + \boldsymbol{\ell} = (k_1 + \ell_1, \dots, k_n + \ell_n), \quad X^{\boldsymbol{k}} \coloneqq X_1^{k_1} \cdots X_n^{k_n}.$$

Ein Ausdruck der Form $X^{\boldsymbol{k}}$ heißt *Monom* vom Grad $|\boldsymbol{k}|$. Ein Polynom ist nun eine endliche Linearkombination

$$f(X_1, \dots, X_n) = \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} X^{\boldsymbol{k}}, \qquad a_{\boldsymbol{k}} \in K.$$

Die Multiplikation wird analog definiert via

$$\Big(\sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} X^{\boldsymbol{k}} \Big) \cdot \Big(\sum_{|\boldsymbol{\ell}| \le d'} b_{\boldsymbol{\ell}} X^{\boldsymbol{\ell}} \Big) = \sum_{|\boldsymbol{m}| \le d + d'} c_{\boldsymbol{m}} X^{\boldsymbol{m}}, \qquad c_{\boldsymbol{m}} \coloneqq \sum_{\boldsymbol{k} + \boldsymbol{\ell} = \boldsymbol{m}} a_{\boldsymbol{k}} b_{\boldsymbol{\ell}}. \tag{1.1}$$

Wir führen die nützliche Notation

$$\underline{X} \mathrel{\hat{=}} X_1, \dots, X_n$$

ein, wenn die Anzahl der Variablen aus dem Kontext klar oder unerheblich ist.

Definition 1.2.2 (Grad, homogene Polynome)**.**
Für ein Polynom $f \neq 0$ definiert man den Grad durch

$$\deg \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} X^{\boldsymbol{k}} = \max \{\, |\boldsymbol{k}| \mid a_{\boldsymbol{k}} \neq 0 \,\}.$$

Für das Nullpolynom vereinbaren wir $\deg 0 = -\infty$. Ein Polynom ist *homogen* vom Grad $d \in \mathbb{N}_0$, wenn alle vorkommenden Monome Grad d haben. Wir notieren

$$K[\underline{X}]_{\le d} \coloneqq \{\, f \in K[\underline{X}] \mid \deg f \le d \,\}$$
$$K[\underline{X}]_d \coloneqq \{0\} \cup \{\, f \in K[\underline{X}] \mid f \text{ homogen}, \ \deg f = d \,\}. \qquad \lrcorner$$

Die Gradfunktion $\deg\colon K[\underline{X}] \setminus \{0\} \to \mathbb{N}_0$ erfüllt die Eigenschaften

$$\deg(f \pm g) \le \max\{\deg f, \deg g\}, \qquad \deg(f \cdot g) = \deg f + \deg g.$$

Dies zeigt auch, dass $K[\underline{X}]$ keine Nullteiler enthält.

Man kann jedem Polynom auf folgende Weise ein homogenes Polynom zuordnen:

Definition 1.2.3 (Homogenisierung)**.**
Es sei $f = \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} \cdot X_1^{k_1} \cdots X_n^{k_n} \in \mathbb{C}[X_1, \dots, X_n]$ ein Polynom vom Grad d. Die Homogenisierung von f ist

$$\tilde{f} = \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} \cdot X_1^{k_1} \cdots X_n^{k_n} Y^{d - |\boldsymbol{k}|} \in \mathbb{C}[X_1, \dots, X_n, Y]_d.$$

Dabei ist Y eine weitere Variable, deren Vorkommen die bestehenden Monome auf den gemeinsamen Grad d ergänzt. $\lrcorner$

Die Homogenisierung als Abbildung $K[\underline{X}]_{\le d} \to K[\underline{X}, Y]_d$ ist eine K-lineare bijektive Abbildung mit Umkehrabbildung $g \mapsto g(X_1, \dots, X_n, 1)$. Insbesondere haben diese Räume die gleiche Dimension, welche man aus der Anzahl der Multiindizes der Länge d kombinatorisch bestimmen kann:

$$\dim_K K[X_1, \dots, X_n]_{\le d} = \dim_K K[X_1, \dots, X_n, Y]_d = \binom{n + d}{d}.$$

Beispiel 1.2.4.
Die Homogenisierung von $f = X_1 + 3 \cdot X_2^2 - X_1^2 X_2 \in \mathbb{Q}[X_1, X_2]$ ist $\tilde{f} = X_1 Y^2 + 3X_2^2 Y - X_1^2 X_2$. ⌟

Definition 1.2.5 (Polynome als Funktionen)**.**
Ist $x = (x_1, \ldots, x_n) \in K^n$, und $f \in K[X_1, \ldots, X_n]$, so können wir x in f einsetzen:

$$x \mapsto f(x) = \sum_{|\boldsymbol{k}| \leq d} a_{\boldsymbol{k}} \cdot x_1^{k_1} \cdots x_n^{k_n} \in K.$$

Dies definiert einen Ringhomomorphismus $K[X_1, \ldots, X_n] \to \mathrm{Abb}(K^n, K)$. Die durch Polynome definierten Funktionen nennen wir auch *Polynomfunktionen*. ⌟

Beispiel 1.2.6 (Polynomfunktionen $\neq$ Polynome)**.**
Im Polynomring $\mathbb{F}_2[X]$ sind $f(X) = X$ und $g(X) = X^2$ zwei verschiedene Polynome, welche jedoch die gleiche Abbildung $\mathbb{F}_2 \to \mathbb{F}_2$ definieren. Die gleiche Polynomfunktion kann also sogar von Polynomen von verschiedenem Grad induziert werden! ⌟

Lemma 1.2.7 (Polynome $\hat{=}$ Polynomfunktionen, falls $|K| = \infty$)**.**
Enthält K unendlich viele Elemente und sind $f, g \in K[X_1, \ldots, X_n]$ mit $f(x) = g(x)$ für alle $x \in K^n$, so gilt bereits $f = g$ als Polynom (alle Koeffizienten sind gleich).

Beweis. [Lan02, Cor. IV.1.7] □

Somit ist die Identifikation von Polynomen und Polynomfunktionen über unendlichen Körpern wie $\mathbb{C}$ unproblematisch.

Definition 1.2.8 (Substitution)**.**
Ein n-Tupel $a = (a_1, \ldots, a_n)$, $a_i \in \{X_1, \ldots, X_n\} \cup K$ definiert eine *Substitition*

$$K[X_1, \ldots, X_n] \ni f \mapsto \mathrm{ev}_a(f) \coloneqq f(a_1, \ldots, a_n) \in K[X_1, \ldots, X_n].$$ ⌟

Für ein festes a definiert ev_a einen Ringhomomorphismus von $K[X_1, \ldots, X_n]$ in sich selbst. Ist $a \in K^n$, so entspricht dies genau der Auswertung von f im Punkt a.

1.3 Monoidoperationen

Um ein mathematisches Objekt zu verstehen, kann es nützlich sein, seine Symmetrien zu untersuchen. Dieses Konzept wird durch den Begriff der Gruppenoperation bzw. Monoidoperation formalisiert.

Definition 1.3.1 (Monoidoperation)**.**
Ist $(G, \cdot, e)$ ein Monoid und X eine Menge, so ist eine *Monoidoperation* eine Abbildung

$$\rho \colon G \times X \to X, \qquad \rho(g, x) = g \triangleright x,$$

sodass für $g_1, g_2 \in G$ und $x \in X$ gilt

$$g_1 \triangleright (g_2 \triangleright x) = (g_1 \cdot g_2) \triangleright x, \qquad e \triangleright x = x.$$ ⌟

Beispiel 1.3.2.

- Die symmetrische Gruppe $\mathcal{S}_n$ operiert durch Permutation auf der Menge $\{1, \ldots, n\}$.
- Der Monoid $(\mathrm{Mat}_n(K), \cdot, I_n)$ operiert auf den Spaltenvektoren K^n durch Matrix-Vektor-Multiplikation:
$$(A, x) \mapsto A \cdot x \in K^n.$$ ⌟

Definition 1.3.3 (Orbit, Fixpunkt, Stabilisator)**.**
Es sei G ein Monoid, welches auf der Menge X operiert. Es sei $x \in X$.

(i) Die *Bahn* oder der *Orbit* von x die Teilmenge

$$G \triangleright x \coloneqq \{\, g \triangleright x \mid g \in G \,\} \subseteq X.$$

(ii) Ist $G \triangleright x = \{x\}$, so ist x ein *Fixpunkt* unter G.
(iii) Die Teilmenge $\mathrm{Stab}_G(x) \coloneqq \{\, g \in G \mid g \triangleright x = x \,\}$ wird der *Stabilisator von* G genannt. ⌟

Ist G eine Gruppe, so sind für $x, y \in X$ die Bahnen $G \triangleright x$, $G \triangleright y$ entweder disjunkt oder gleich. Somit ist X die disjunkte Vereinigung von Bahnen. Der Stabilisator eines Elementes ist eine Untergruppe von G.

Beispiel 1.3.4.

- Die Operation von $\mathrm{GL}_n(K)$ auf K^n hat genau die Bahnen $\{0\}$ und $K^n \setminus \{0\}$.
  Für die Operation von $\mathrm{Mat}_n(K)$ auf K^n hingegen enthält jede Bahn den Nullvektor, da $0 \cdot v = 0$.
- Der Stabilisator von $n \in \{1, \ldots, n\}$ unter der Operation der $\mathcal{S}_n$ sind gerade die Permutationen von $\{1, \ldots, n-1\}$. Daher ist $\mathrm{Stab}_{\mathcal{S}_n}(n) \cong \mathcal{S}_{n-1}$. ⌟

1.4 Topologische Grundbegriffe

Definition 1.4.1 (Topologie, offene Menge, abgeschlossene Menge)**.**
Es sei X eine Menge. Eine *Topologie* auf X ist eine Familie von Teilmengen $\mathcal{T} \subseteq \mathcal{P}(X)$ mit den Eigenschaften

(i) $\emptyset \in \mathcal{T}$, $X \in \mathcal{T}$.
(ii) Sind $U_1, U_2 \in \mathcal{T}$, so ist auch $U_1 \cap U_2 \in \mathcal{T}$.
(iii) Sind $U_i \in \mathcal{T}$ für alle $i \in I$, I eine Indexmenge, so ist $\bigcup_{i \in I} U_i \in \mathcal{T}$.

Die Mengen in $\mathcal{T}$ nennen wir *offene Mengen*, das Paar $(X, \mathcal{T})$ einen *topologischen Raum*. Eine Menge $A \subseteq X$ heißt *abgeschlossen*, falls $X \setminus A$ offen ist. ⌟

Man kann eine Topologie auch durch Angabe der abgeschlossenen Mengen $\mathcal{A}$ definieren, die Axiome lauten dann

(i') $\emptyset \in \mathcal{A}$, $X \in \mathcal{A}$.
(ii') Sind $A_1, A_2 \in \mathcal{A}$, so ist auch $A_1 \cup A_2 \in \mathcal{A}$.
(iii') Sind $A_i \in \mathcal{A}$ für alle $i \in I$, I eine Indexmenge, so ist $\bigcap_{i \in I} A_i \in \mathcal{A}$.

Es sei nun $(X, \mathcal{T})$ ein topologischer Raum mit abgeschlossenen Mengen $\mathcal{A}$

Definition 1.4.2 (Abschluss)**.**
Sei $M \subseteq X$ eine Teilmenge. Der *Abschluss* von M in X ist definiert als die kleinste abgeschlossene Teilmenge von X, welche M enthält.

$$\overline{M} \coloneqq \bigcap_{M \subseteq A \in \mathcal{A}} A. \qquad ⌟$$

So ist etwa A genau dann abgeschlossen, wenn $\overline{A} = A$.

Ein wichtiges Beispiel für eine Topologie aus der Analysis ist die Normtopologie:

Definition 1.4.3 (Normierter Vektorraum)**.**
Es sei $\mathbb{V}$ ein Vektorraum über $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Eine *Norm* ist eine Abbildung $\|\cdot\| \colon \mathbb{V} \to \mathbb{R}_{\geq 0}$ mit folgenden Eigenschaften:

(i) Für $v \in \mathbb{V}$ gilt $\|v\| = 0$ genau dann wenn $v = 0$.
(ii) Für $v \in \mathbb{V}$, $\lambda \in \mathbb{K}$ gilt $\|\lambda v\| = |\lambda| \cdot \|v\|$.
(iii) Für $v, w \in \mathbb{V}$ gilt $\|v + w\| \leq \|v\| + \|w\|$.

Das Paar $(\mathbb{V}, \|\cdot\|)$ ist ein *normierter Vektorraum*. Eine Teilmenge $U \subseteq \mathbb{V}$ ist offen, falls es für jeden Punkt $p \in U$ ein $\varepsilon > 0$ gibt mit

$$B_\varepsilon(p) \coloneqq \{\, x \in \mathbb{V} \mid \|x - p\| < \varepsilon \,\} \subseteq U. \qquad \lrcorner$$

Mit dieser Definition offener Mengen wird jeder normierte Vektorraum $\mathbb{V}$ mit einer Topologie ausgestattet. Durch die Norm lässt sich ein Grenzwertbegriff einführen: Für eine Folge $(v_n)_{n\in\mathbb{N}} \subseteq \mathbb{V}$ ist die Konvergenz gegen $v \in \mathbb{V}$ definiert durch

$$\lim_{n\to\infty} v_n = v \quad :\Longleftrightarrow \quad \lim_{n\to\infty} \|v - v_n\| = 0$$

(Nullfolge in $\mathbb{R}$). Der Abschluss einer Teilmenge $M \subseteq X$ kann charakterisiert werden durch die Menge aller Grenzwerte

$$\overline{M} = \left\{ v \in \mathbb{V} \;\middle|\; \text{Es gibt } (v_n)_{n\in\mathbb{N}} \subseteq M \text{ mit } \lim_{n\to\infty} v_n = v \right\}.$$

Beispiel 1.4.4 (Die Standardtopologie auf $\mathbb{K}^n$)**.**
Der Vektorraum $\mathbb{V} = \mathbb{K}^n$ kann mit verschiedenen Normen ausgestattet werden, etwa

$$\|(x_1, \ldots, x_n)\|_2 \coloneqq \sqrt{|x_1|^2 + \cdots + |x_n|^2}, \qquad \|(x_1, \ldots, x_n)\|_\infty \coloneqq \max\{|x_1|, \ldots, |x_n|\}.$$

Nach einem Satz der Analysis sind auf jedem endlichdimensionalen Vektorraum alle Normen *äquivalent*, d.h. für $\|\cdot\|$, $\|\cdot\|'$ Normen auf $\mathbb{V}$ gibt es Konstanten $c, C > 0$ mit

$$c\|v\| \leq \|v\|' \leq C\|v\| \qquad \text{für alle } v \in \mathbb{V}.$$

Daraus folgt, dass sämtliche Normen die gleiche Topologie definieren und auch Folgenkonvergenz unabhängig von der gewählten Norm ist. Dies rechtfertigt es, von der *Standardtopologie* oder *euklidischen Topologie* auf $\mathbb{V}$ zu sprechen. $\lrcorner$

Kapitel 2

Algebraische Komplexitätsklassen

In diesem Kapitel führen wir grundlegende Konzepte der algebraischen Komplexitätstheorie ein. Wir definieren ein Komplexitätsmaß für Polynome, und ordnen dann Folgen von Polynomen in Komplexitätsklassen ein. Wir führen einen Reduktionsbegriff ein und lernen vollständige Familien kennen.

Die Darstellung folgt in einigen Teilen dem Buch von Bürgisser [Bür00, Kapitel 2], eine knappe Darstellung der Theorie findet sich auch im Buch von Arora und Barak [AB09, Kapitel 16].

2.1 Arithmetische Schaltkreise

Die Definitionen in diesem Abschnitt orientieren sich an [Vol99, Abschnitt 5.1].

Beispiel 2.1.1.
Um das Polynom $X^2 - Y^2 \in \mathbb{R}[X, Y]$ in $(x, y) \in \mathbb{R}^2$ auszuwerten, gibt es (mindestens) die folgenden Möglichkeiten:

(i) Berechne $a \coloneqq x \cdot x$, $b \coloneqq y \cdot y$, $c \coloneqq a - b$, dann ist c das Ergebnis.
(ii) Berechne $a' \coloneqq x + y$, $b' \coloneqq x - y$, $c' \coloneqq a' \cdot b'$, dann ist c' das Ergebnis, da

$$x^2 - y^2 = (x + y)(x - y).$$

Da die Multiplikation von (Gleitkomma)Zahlen im Allgemeinen aufwändiger als die Addition ist, scheint die zweite Methode der ersten zunächst überlegen. Andererseits sind die Multiplikationen $x \cdot x$ und $y \cdot y$ unabhängig voneinander und können parallel berechnet werden. ⌟

Wir definieren nun Schaltkreise, um Komplexitätsmaße für die Auswertung von Polynomen definieren zu können.

Definition 2.1.2 (Basis)**.**
Sei M eine Menge von Werten und $S = \{s_i\}_{i \in I}$ eine Familie von Funktionen $s_i \colon M^{a_i} \to M$, wobei $a_i \in \mathbb{N}_0$ die Stelligkeit von s_i ist. Das Paar (M, S) nennen wir eine *Basis*. ⌟

Beispiel 2.1.3.
Um die Boolesche Arithmetik darzustellen, ist eine mögliche Basis $M = \{0, 1\}$ und $S = \{\vee, \wedge, \neg, 0, 1\}$, wobei $\vee$ und $\wedge$ zweistellig, $\neg$ einstellig und 0, 1 nullstellig (Konstanten) sind. ⌟

Definition 2.1.4 (Schaltkreis)**.**
Ein *Schaltkreis* $C = (G, \alpha, \beta, \omega)$ über der Basis (M, S) mit n Eingängen und m Ausgängen besteht aus folgenden Komponenten;

- Ein gerichteter Graph $G = (V, E)$, welcher keine gerichteten Zyklen enthält.

- Eine injektive Abbildung $\alpha\colon V \to \mathbb{N}$, welche eine topologische Ordnung auf G induziert, d. h. für $(u, v) \in E$ ist $\alpha(u) < \alpha(v)$.
- Eine Abbildung $\beta\colon V \to S \cup \{X_1, \ldots, X_n\}$, welche die *Berechnungsgatter* markiert. Für $v \in V$ mit eingehendem Grad $\deg_{\text{in}}(v)$ erfüllt β:
  - Für $\deg_{\text{in}}(v) = 0$ ist $\beta(v) \in S$ eine nullstellige Funktion oder $\beta(v) = X_i$ eine *Eingangsvariable*. Dabei wird jedes X_i höchstens einmal getroffen.
  - Falls $\deg_{\text{in}}(v) \geq 1$, ist $\beta(v) = s_i \in S$ eine Funktion mit Stelligkeit $a_i = \deg_{\text{in}}(v)$.
- Eine Abbildung $\omega\colon V \to \{*\} \cup \{Y_1, \ldots, Y_m\}$, die die *Ausgabegatter* markiert:
  - Auf die Teilmenge $\{\, v \in V \mid \deg_{\text{out}}(v) = 0 \,\}$ eingeschränkt definiert ω eine Bijektion mit $\{Y_1, \ldots, Y_m\}$.
  - Für alle $v \in V$ mit $\deg_{\text{out}}(v) \geq 1$ ist $\omega(v) = *$.

Die *Größe* $\text{size}(C)$ eines Schaltkreises C sei die Anzahl der Berechnungsgatter. Die *Tiefe* $\text{depth}(C)$ ist die Länge eines längsten gerichteten Pfades in G. ⌟

Definition 2.1.5 (Boolescher Schaltkreis, arithmetischer Schaltkreis)**.**

(i) Ein *Boolescher Schaltkreis* ist ein Schaltkreis über der Basis $(\{0, 1\}, S)$, wobei $S = \{\vee, \wedge, \neg, 0, 1\}$.

(ii) Ein *arithmetischer Schaltkreis* über einem Ring $(R, +, \cdot)$ ist ein Schaltkreis über der Basis (R, S) mit $S = \{+, \cdot\} \cup R$, wobei wir Elemente aus R als nullstellige Funktionen auffassen. ⌟

Wir wollen nun erklären, was die von einem Schaltkreis C berechnete Funktion ist. Seien $x_1, \ldots, x_n \in M$ Eingabewerte. Wir definieren für $v \in V$:

- Falls $\beta(v) = X_i$, so definiere $\text{val}_v(x_1, \ldots, x_n) \coloneqq x_i$.
- Falls $\beta(v) = s_i \in S$ eine nullstellige Funktion, also eine Konstante $c \in M$ ist, so definiere $\text{val}_v(x_1, \ldots, x_n) \coloneqq c$.
- Falls $\beta(v) = s_i \in S$ Stelligkeit $a \geq 1$ hat, so besitzt v genau a Vorgängerknoten $v_1, \ldots, v_a$. Diese seien sortiert nach $\alpha(v_1) < \cdots < \alpha(v_a)$, dann definiere rekursiv

$$\text{val}_v(x_1, \ldots, x_n) \coloneqq s_i(\text{val}_{v_1}(x_1, \ldots, x_n), \ldots, \text{val}_{v_a}(x_1, \ldots, x_n)).$$

Die Rekursion ist wohldefiniert, da die Definition von val_v nur auf $\text{val}_{v'}$ mit $\alpha(v') < \alpha(v)$ zurückgreift.

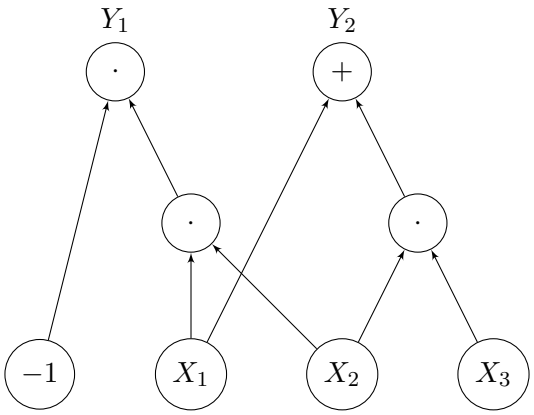
Definition 2.1.6 (Von einem Schaltkreis berechnete Funktion)**.**
Ist C ein Schaltkreis über (M, S) mit n Eingängen und m Ausgängen, so ist die durch C definierte Funktion $f_C\colon M^n \to M^m$ definiert als

$$f_C(x_1, \ldots, x_n) = (\text{val}_{\omega^{-1}(Y_1)}(x_1, \ldots, x_n), \ldots, \text{val}_{\omega^{-1}(Y_m)}(x_1, \ldots, x_n)).$$ ⌟

Bemerkung.
Sind die Funktionen aus S symmetrisch in ihren Eingabewerten, wie etwa bei den angegebenen Basen zu booleschen und arithmetischen Schaltkreisen über *kommutativen* Ringen, so benötigt man zur Auswertung keine konkrete topologische Sortierung. Aus diesem Grund spezifizieren wir im Folgenden keine spezielle Ordnung für diese Schaltkreise. ⌟

Beispiel 2.1.7.
Folgender arithmetischer Schaltkreis über $\mathbb{R}$ berechnet die Funktion

$$f\colon \mathbb{R}^3 \to \mathbb{R}^2, \qquad (x_1, x_2, x_3) \mapsto (-x_1 \cdot x_2, x_1 + x_2 \cdot x_3).$$



Dieser Schaltkreis hat Größe 4 und Tiefe 2. ⌟

2.2 Die Klassen VP und VNP

Die Definitionen in diesem Abschnitt finden sich etwa in [AB09, Abschnitt 16.1] oder [Bür00, Abschnitt 2.1]. Letzterer nutzt ein anderes Berechnungsmodell (*straight-line programs*), welches jedoch zu arithmetischen Schaltkreisen äquivalent ist ([AB09, Lemma 16.6]).

Fixiere einen Körper K. Ist C ein algebraischer Schaltkreis über K mit n Eingängen und einem Ausgang, so folgt aus der Konstruktion von f_C, dass $f_C \colon K^n \to K$ eine *Polynomfunktion* berechnet.

Definition 2.2.1 (Schaltkreiskomplexität eines Polynoms)**.**
Ist $f \in K[X_1, \ldots, X_n]$ ein Polynom, so definiere die *Komplexität*

$$L(f) \coloneqq \min \{ \operatorname{size}(C) \mid C \text{ ist arith. Schaltkreis über } K,\ f_C = f \text{ (als Funktion)} \}. \qquad ⌟$$

Definition 2.2.2 (p-Familie)**.**
Eine *p-Familie* ist eine Folge von Polynomen $(f_n)_{n\in\mathbb{N}}$, sodass es polynomiell beschränkte Funktionen $p, q \colon \mathbb{N} \to \mathbb{N}$ gibt mit $f_n \in K[X_1, \ldots, X_{p(n)}]$ und $\deg f_n \leq q(n)$. ⌟

Beispiel 2.2.3.

- Die Folge $f_n \coloneqq X_1 \cdots X_n \in K[X_1, \ldots, X_n]$ ist eine p-Familie ($p(n) = q(n) = n$ genügen). Offenbar ist $L(f_n) \in O(n)$.
- Die Determinante einer $n \times n$-Matrix, definiert über die Leibnizformel

$$\det \begin{pmatrix} X_{11} & \ldots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \ldots & X_{nn} \end{pmatrix} = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)} \tag{2.1}$$

  definiert eine p-Famile von Polynomen $(\det_n)_{n\in\mathbb{N}}$ ($p(n) = n^2$, $q(n) = n$).
  Streng genommen müssten wir noch eine Anordnung der Variablen $X_{ij} \leftrightarrow \tilde{X}_k$ wählen, es ist jedoch praktischer, die Variablen wie gewohnt mit zwei Indizes zu indizieren.
- Lässt man in Gleichung (2.1) das Signum der Permutation weg, so erhält man die *Permanente*

$$\operatorname{perm} \begin{pmatrix} X_{11} & \ldots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \ldots & X_{nn} \end{pmatrix} = \sum_{\sigma \in \mathcal{S}_n} X_{1\sigma(1)} \cdots X_{n\sigma(n)}, \tag{2.2}$$

  welche ebenfalls eine p-Familie $(\operatorname{perm}_n)_{n\in\mathbb{N}}$ definiert. ⌟

Wir führen nun Klassen von p-Familien ein, welche wir im Folgenden untersuchen wollen.

Definition 2.2.4 (VP, VNP)**.**

(i) Die Klasse VP_K besteht aus den p-Familien $(f_n)_n$, sodass $L(f_n) = O(n^c)$ für ein $c \in \mathbb{N}$.

(ii) Die Klasse VNP_K besteht aus den p-Familien $(f_n)_n$, sodass es polynomiell beschränkte Funktionen $p\colon \mathbb{N} \to \mathbb{N}$, $p'\colon \mathbb{N} \to \mathbb{N}_0$ und eine Familie von Polynomen $\tilde{f}_n \in K[X_1, \ldots, X_{p(n)}, Y_1, \ldots, Y_{p'(n)}]$ gibt mit $(\tilde{f}_n)_n \in \mathsf{VP}_K$ und

$$f_n(X_1, \ldots, X_{p(n)}) = \sum_{e \in \{0,1\}^{p'(n)}} \tilde{f}_n(X_1, \ldots, X_{p(n)}, e_1, \ldots, e_{p'(n)}).$$

Ist der Grundkörper aus dem Kontext klar, so schreiben wir einfach VP und VNP. ⌟

Ist $p'(n) = 0$, so ist $\tilde{f}_n \in K[X_1, \ldots, X_{p(n)}]$ und die Summe ist definiert als

$$\sum_{e \in \{0,1\}^0} \tilde{f}_n(X_1, \ldots, X_{p(n)}) = \tilde{f}_n(X_1, \ldots, X_{p(n)}).$$

Insbesondere ist $\mathsf{VP} \subseteq \mathsf{VNP}$ ($p'(n)$ kann immer konstant 0 gesetzt werden). Die Namen VP und VNP sind zu Ehren Valiants gewählt worden, welcher diese Klassen in der Arbeit *Completeness Classes in Algebra* eingeführt hat [Val79]. In Abschnitt 2.6 gehen wir auf die Analogie zu P und NP genauer ein.

Beispiel 2.2.5 ($(\mathrm{imm}_n)_n \in \mathsf{VP}$)**.**
Wir wollen iterierte Matrixmultiplikation (IMM) durch eine Familie von Polynomen beschreiben.

Seien $X_{ij}^{(\ell)}$ Variablen für $1 \le i, j, \ell \le n$ und $A_\ell = (X_{ij}^{(\ell)})_{i,j=1}^n$ Matrizen. Definiere imm_n als die erste Komponente des Matrixprodukts

$$\mathrm{imm}_n := (A_1 \cdot A_2 \cdots A_n)_{11} \in K[X_{11}^{(1)}, \ldots, X_{nn}^{(n)}]$$

(ein Polynom in n^3 Variablen). An der Definition des Matrixprodukts sieht man, dass sämtliche Einträge von $A_1 \cdot A_2$ homogene Polynome vom Grad 2 sind. Setzt man dies iterativ fort, erhält man, dass die Einträge von $A_1 \cdots A_n$ homogene Polynome vom Grad n sind. Dies zeigt, dass $(\mathrm{imm}_n)_n$ eine p-Familie ist.

Das Produkt $A_1 \cdot A_2$ hat n^2 Einträge, wobei jeder Eintrag von der Form

$$X_{i1}^{(1)} X_{1k}^{(2)} + X_{i2}^{(1)} X_{2k}^{(2)} + \cdots + X_{in}^{(1)} X_{nk}^{(2)}$$

ist. Der Schaltkreis mit $n^2 + n^2$ Eingängen und n^2 Ausgängen, welcher zunächst alle Produkte $X_{ij}^{(1)} X_{jk}^{(2)}$ berechnet, und dann die Terme in jeder der n^2 Komponenten zusammenaddiert, beinhaltet $n^2 \cdot n = n^3$ Multiplikationsgatter und $n^2 \cdot (n-1)$ Additionsgatter.

Nutzt man $n-1$ dieser Schaltkreise, um nacheinander

$$A_1 \cdot A_2, \quad (A_1 A_2) \cdot A_3, \quad \ldots \quad (A_1 \cdots A_{n-1}) \cdot A_n$$

zu berechnen, so erhält man einen Schaltkreis C_n mit $\mathrm{size}(C_n) = O(n^4)$, welcher alle Einträge von $A_1 \cdots A_n$ berechnet. Insgesamt sehen wir, dass $(\mathrm{imm}_n)_n \in \mathsf{VP}$. ⌟

Das Verfahren zeigt auch, dass Familien von passenden rechteckigen Matrizen $A_1, \ldots, A_n$ mit polynomiellem Aufwand in der Gesamtzahl der Einträge berechnet werden können.

Wir wenden uns nun den Familien $(\det_n)_n$ und $(\mathrm{perm}_n)_n$ zu. Die Leibnizformel (2.1) ist zur effizienten Berechnung ungeeignet, da sie $O(n!)$ Additionen und $O(n \cdot n!)$ Multiplikationen beinhaltet. Dennoch können wir die Determinante mittels polynomiellem Aufwand evaluieren.

Satz 2.2.6.
$(\det_n)_n \in \mathsf{VP}$.

Beweis. Wir nutzen den *Samuelson-Berkowitz-Algorithmus*, um das charakteristische Polynom $\det(T \cdot I_n - A)$ von $A = (X_{ij})_{i,j=1}^n$ mittels Matrixmultiplikation auszurechnen. Die Determinante erhält man dann als den konstanten Term dieses Polynoms.
Es sei $A_r := (X_{ij})_{i,j=1}^r$ die Untermatrix der ersten r Zeilen und Spalten; zerlege dann diese Matrizen in folgende Blöcke:

$$A_r = \left(\begin{array}{c|c} A_{r-1} & S_{r-1} \\ \hline R_{r-1} & X_{rr} \end{array}\right), \qquad r = 1, \ldots, n.$$

Da R_r ein Zeilenvektor und S_r ein Spaltenvektor ist, ergibt das Matrixprodukt $R_r \cdot A_r^k \cdot S_r$ ($k \in \mathbb{N}_0$) eine 1×1-Matrix, also einen Eintrag aus $K[\underline{X}]$. Definiere die Matrizen

$$T^{(r)} = (T_{ij}^{(r)}) \in \mathrm{Mat}_{(r+1)\times r}(K[\underline{X}]), \qquad T_{i,j}^{(r+1)} = \begin{cases} 0 & \text{falls } i < j \\ 1 & \text{falls } i = j \\ -X_{r+1,r+1} & \text{falls } i = j+1 \\ -R_r A_r^{i-j-2} S_r & \text{falls } i \geq j+2. \end{cases}$$

Dann ist $P := T^{(n)} \cdot T^{(n-1)} \cdots T^{(1)} \in (K[\underline{X}])^{r+1}$ ein Vektor, welcher die Koeffizienten des charakteristischen Polynoms von A beinhaltet:

$$\chi_A(T) = P_1 T^n + P_2 T^{n-1} + \cdots + P_{n+1}.$$

Für den konstanten Term erhält man nun $\det(A) = (-1)^n P_{n+1}$. Diese Berechnungsvorschrift können wir mittels eines Schaltkreises polynomieller Größe realisieren:

- Für festes $r \in \{1, \ldots, r\}$ kann man jeden einzelnen Eintrag von $T^{(r)}$ als Matrixprodukt mit einem Schaltkreis der Größe $O(r^4)$ berechnen (Beispiel 2.2.5).
- Fügt man diese $(r+1)\times r$ Schaltkreise zusammen, kann man die vollständige Matrix $T^{(r)}$ mit einem Schaltkreis der Größe $O(r^6)$ berechnen.
- Fügt man diese n Schaltkreise für $T^{(1)}, \ldots, T^{(n)}$ zusammen, und berechnet dann das Matrixprodukt $T^{(n)} \cdots T^{(1)}$, so liefert dies einen Schaltkreis für den Koeffizientenvektor P der Größe $O(n^7)$.

Eine Herleitung und Analyse dieses Verfahrens findet sich in dem Artikel von Abdeljaoued [Abd97, S. 21-32] (insbesondere wird dort auch auf die Korrektheit eingegangen). □

Satz 2.2.7.
$(\mathrm{perm}_n)_n \in \mathsf{VNP}$.

Beweis. Es sei $f_n = \mathrm{perm}_n(X_{11}, \ldots, X_{nn})$ und $(Y_{ij})_{i,j=1}^n$ eine weitere Matrix mit Unbestimmten als Einträge. Definiere

$$g_n := \underbrace{\left(\prod_{\substack{i,j,i',j'=1 \\ i=i' \text{ xor } j=j'}}^{n} (1 - Y_{ij}Y_{i'j'})\right)}_{=:\alpha_n(\underline{Y})} \underbrace{\left(\prod_{i=1}^n \sum_{j=1}^n Y_{ij}\right)}_{=:\beta_n(\underline{Y})} \underbrace{\left(\prod_{i=1}^n \sum_{j=1}^n Y_{ij}X_{ij}\right)}_{=:\gamma_n(\underline{X},\underline{Y})} \in K[\underline{X}, \underline{Y}].$$

Ist nun $e = (e_{ij}) \in \{0,1\}^{n\times n}$ eine Belegung der Y_{ij}, so ist $\alpha(e) \in \{0,1\}$. Genauer ist $\alpha(e) = 1$ genau dann wenn $e_{ij}e_{i'j'} = 0$ für alle Indizes mit $i = i', j \neq j'$ oder umgekehrt, d.h. jede Zeile/Spalte von e enthält *höchstens* eine 1. Ist $\alpha(e) = 1$, so beinhaltet die Summe in β höchstens einen Eintrag $\neq 0$, d. h. $\alpha(e) \cdot \beta(e) = 1$ genau dann, wenn e eine *Permutationsmatrix* ist. In diesem Fall ist dann

$$g_n(X_{11}, \ldots, X_{nn}, e_{11}, \ldots, e_{nn}) = 1 \cdot \prod_{i=1}^{n} \sum_{j=1}^{n} e_{ij}X_{ij} = \prod_{i=1}^{n} X_{i\sigma(i)},$$

wobei σ die durch die Matrix e dargestellte Permutation ist. Ist e keine Permutationsmatrix, so verschwindet $\alpha(e)\beta(e)$ und $g_n(X, e)$ ist das Nullpolynom. Insgesamt erhalten wir

$$\sum_{e\in\{0,1\}^{n\times n}} g_n(X_{11}, \ldots, X_{nn}, e_{11}, \ldots, e_{nn}) = \sum_{\sigma\in\mathcal{S}_n} \prod_{i=1}^{n} X_{i\sigma(i)} = \operatorname{perm}_n .$$

Schließlich schätzen

$$L(g_n) \leq L(\alpha_n) + L(\beta_n) + L(\gamma_n) + 2 = O(n^3) + O(n^2) + O(n^2),$$

also $(g_n)_n \in \mathsf{VP}$. Damit ist $(\operatorname{perm}_n)_n \in \mathsf{VNP}$ gezeigt. □

Analog zum P versus NP Problem lautet nun *Valiants Hypothese*

$$\mathsf{VP} \neq \mathsf{VNP}.$$

2.3 Projektionen und Vollständigkeit

Um die schwierigsten Probleme in NP auszuzeichnen, führt man den Begriff der Polynomialzeitreduktion ein. Für die hier betrachteten algebraischen Komplexitätsklassen definieren wir ein analoges Konzept, welches jedoch deutlich restriktiver ist.

Definition 2.3.1 (Projektion, $\leq_{\mathrm{p}}$, abgeschlossen unter Projektionen)**.**

(i) $f \in K[X_1, \ldots, X_n]$ ist eine *Projektion* von $g \in K[X_1, \ldots, X_m]$, wenn es eine Substitution $a = (a_1, \ldots, a_m)$, $a_i \in \{X_1, \ldots, X_n\} \cup K$ gibt mit

$$f(X_1, \ldots, X_n) = g(a_1, \ldots, a_m).$$

In diesem Fall schreiben wir $f \leq g$.

(ii) Sind $(f_n)_n$, $(g_n)_n$ p-Familien, so schreiben wir $(f_n)_n \leq_{\mathrm{p}} (g_n)_n$, falls es eine polynomiell beschränkte Funktion $t\colon \mathbb{N} \to \mathbb{N}$ gibt mit $f_n \leq g_{t(n)}$ für alle $n \in \mathbb{N}$.

(iii) Eine Menge von p-Familien $\mathcal{C}$ nennen wir *unter Projektionen abgeschlossen*, falls für p-Familien $(f_n)_n \leq_{\mathrm{p}} (g_n)_n$ mit $(g_n)_n \in \mathcal{C}$ stets auch $(f_n)_n \in \mathcal{C}$ gilt. ⌟

Beispiel 2.3.2.
Sei $f_n = X_1 \cdots X_n$, dann ist $f_n \leq \det_n$, denn die Substitution

$$X_{ij} \mapsto \begin{cases} X_i & \text{falls } i = j \\ 0 & \text{falls } i \neq j. \end{cases}$$

realisiert f_n als Projektion der Determinante:

$$\det \begin{pmatrix} X_1 & & 0 \\ & \ddots & \\ 0 & & X_n \end{pmatrix} = X_1 \cdots X_n = f_n.$$

Tatsächlich ist $(\det_n)_n$ sogar eine sogenannte *universelle* Familie, d.h. für *jedes* Polynom $f \in K[X_1, \ldots, X_n]$ gibt es ein $m \in \mathbb{N}$ mit $f \leq \det_m$. ⌟

Lemma 2.3.3 (VP, VNP sind abgeschlossen unter Projektionen)**.**
Sind $(f_n)_n \leq_\mathrm{p} (g_n)_n$ p-Familien, so haben wir die Implikationen

(i) $(g_n)_n \in \mathsf{VP} \implies (f_n)_n \in \mathsf{VP}$.
(ii) $(g_n)_n \in \mathsf{VNP} \implies (f_n)_n \in \mathsf{VNP}$.

Beweis. (i) Es sei zunächst f eine Projektion von g mittels der Substitution $X_i \mapsto a_i$. Ist C ein Schaltkreis, welcher g berechnet, so erhält man durch Ersetzen der Eingangsvariablen durch die a_i einen Schaltkreis gleicher Größe, welcher f berechnet. Dies zeigt $L(f) \leq L(g)$. Ist nun $f_n \leq g_{t(n)}$ für eine polynomiell beschränkte Funktion $t(n) = O(n^b)$ und $L(g_n) = p(n)$, so folgt

$$L(f_n) \leq L(g_{t(n)}) = p(t(n)).$$

Ist $(g_n)_n \in \mathsf{VP}$, so ist p polynomiell beschränkt, und damit auch $p \circ t$, d. h. $(f_n)_n \in \mathsf{VP}$.

(ii) Es sei $f_n(X_1, \ldots, X_{p(n)}) \leq g_{t(n)}(X_1, \ldots, X_{q(t(n))})$ durch Substitutionen $X_i \mapsto a_i^{(n)}$. Haben wir eine Darstellung

$$g_n(X_1, \ldots, X_{q(n)}) = \sum_{e \in \{0,1\}^{q'(n)}} \tilde{g}_n(X_1, \ldots, X_{q(n)}, e_1, \ldots, e_{q'(n)}),$$

wie in Definition 2.2.4, so ist

$$f_n(X_1, \ldots, X_{p(n)}) = g_n(a_1, \ldots, a_{q(t(n))}) = \sum_{e \in \{0,1\}^{q'(n)}} \tilde{g}_n(a_1, \ldots, a_{q(t(n))}, e_1, \ldots, e_{q'(n)}).$$

Nach (i) ist $(\tilde{g}_n(a_1, \ldots, a_{q(t(n))}, e_1, \ldots, e_{q'(n)}))_n \in \mathsf{VP}$, daher ist die definierende Eigenschaft für $(f_n)_n \in \mathsf{VNP}$ gezeigt. □

Nachdem wir nun einen Reduktionsbegriff eingeführt haben, definieren wir einen analogen Begriff zu NP-Schwere und NP-Vollständigkeit. Im Folgenden sei $\mathcal{C}$ eine Klasse von p-Familien, welche unter p-Projektionen abgeschlossen ist, etwa VP oder VNP.

Definition 2.3.4 ($\mathcal{C}$-Schwere, $\mathcal{C}$-Vollständigkeit)**.**
Es sei $(g_n)_n$ eine p-Familie.

(i) $(g_n)_n$ ist *$\mathcal{C}$-schwer*, falls $(f_n)_n \leq_p (g_n)_n$ für alle $(f_n)_n \in \mathcal{C}$.
(ii) $(g_n)_n$ ist *$\mathcal{C}$-vollständig*, falls $(g_n)_n$ $\mathcal{C}$-schwer ist und selbst in $\mathcal{C}$ liegt. ⌟

Diese Begriffe wenden wir nun auf die Klasse VNP an. Tatsächlich existieren über jedem Grundkörper VNP-vollständige Familien, zum Beispiel

$$\mathrm{HC}_n := \sum_{\substack{\sigma \in \mathcal{S}_n \text{ Zykel} \\ \text{der Länge } n}} X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in K[X_{11}, \ldots, X_{nn}]$$

(vergleiche die Arbeit von Valiant [Val79, Theorem 3]). Vollständige Familien repräsentieren die schwierigsten Probleme einer Klasse, wie folgendes Lemma zeigt.

Lemma 2.3.5 (Vollständige Familien charakterisieren ihre Klasse)**.**
Es sei $(g_n)_n$ eine $\mathcal{C}$-vollständige Familie.

(i) *Eine p-Familie $(f_n)_n$ liegt in $\mathcal{C}$ genau dann, wenn $(f_n)_n \leq_\mathrm{p} (g_n)_n$.*
(ii) *Ist $(g_n)_n$ VNP-vollständig, so gilt $\mathsf{VP} = \mathsf{VNP}$ genau dann, wenn $(g_n)_n \in \mathsf{VP}$.*

Beweis. (i) Ist $(f_n)_n \in \mathcal{C}$, so ist $(f_n)_n \leq_\mathrm{p} (g_n)_n$, da $(g_n)_n$ $\mathcal{C}$-schwer ist.
Ist umgekehrt $(f_n)_n \leq_\mathrm{p} (g_n)_n$, so folgt aus der Abgeschlossenheit von $\mathcal{C}$ unter Projektionen aus $(g_n)_n \in \mathcal{C}$ auch $(f_n)_n \in \mathcal{C}$.

(ii) Falls $\mathsf{VNP} = \mathsf{VP}$, so ist sicher $(g_n)_n \in \mathsf{VP}$.
Es sei umgekehrt $(g_n)_n \in \mathsf{VP}$. Für jedes $(f_n)_n \in \mathsf{VNP}$, ist $(f_n)_n \leq_\mathrm{p} (g_n)_n$. Da VP unter Projektionen abgeschlossen ist, ist also auch $(f_n)_n \in \mathsf{VP}$. □

2.4 Die Vollständigkeit der Permanente

Satz 2.4.1 ($(\mathrm{perm}_n)_n$ ist VNP-vollständig)**.**
$(\mathrm{perm}_n)_n$ *ist* VNP*-vollständig über jedem Körper der Charakteristik* $\neq 2$.

Bevor wir eine Beweisidee dieses Satzes geben, gehen wir noch auf eine eingeschränkte Familie von Schaltkreisen ein.

Definition 2.4.2 (Formeln, $L_\mathrm{e}(f)$, VP_e, VNP_e)**.**

(i) Ein algebraischer Schaltkreis ist eine *Formel*, falls der zugrundeliegende Graph G ein (gerichteter) Baum ist. Die Größe der kleinsten Formel, welche ein Polynom f berechnet, bezeichnen wir mit $L_\mathrm{e}(f)$.

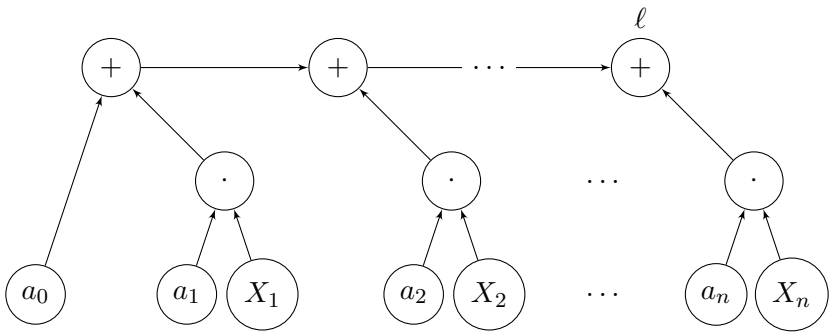
(ii) Die Klasse VP_e besteht aus den p-Familien $(f_n)_n$, sodass $L_\mathrm{e}(f_n) = O(n^c)$ für ein $c \in \mathbb{N}$.

(iii) Die Klasse VNP_e besteht aus den p-Familien (f_n), sodass es polynomiell beschränkte Funktionen $p, q\colon \mathbb{N} \to \mathbb{N}$ und Polynome $\tilde{f}_n \in K[X_1, \ldots, X_{p(n)}, Y_1, \ldots, Y_{q(n)}]$ gibt mit $(\tilde{f})_n \in \mathsf{VP}_\mathrm{e}$ und

$$f_n(X_1, \ldots, X_{p(n)}) = \sum_{e \in \{0,1\}^{q(n)}} \tilde{f}_n(X_1, \ldots, X_{p(n)}, e_1, \ldots, e_{q(n)}). \qquad \lrcorner$$

Das „e“ in VP_e steht für „expression“. Offenbar ist $L(f) \leq L_\mathrm{e}(f)$ und damit $\mathsf{VP}_\mathrm{e} \subseteq \mathsf{VP}$ und $\mathsf{VNP}_\mathrm{e} \subseteq \mathsf{VNP}$. Die Forderung, dass der Graph ein Baum ist, besagt anschaulich, dass der Algorithmus kein Zwischenergebnis mehrfach verwenden darf.

Beispiel 2.4.3.
Ein lineares Polynom $\ell_n(\underline{X}) = a_0 + a_1X_1 + \cdots + a_nX_n$ lässt sich durch eine Formel der Größe $O(n)$ berechnen:



Somit ist $(\ell_n)_n \in \mathsf{VP}_\mathrm{e}$. $\lrcorner$

Es ist unbekannt, ob das Berechnungsmodell der Formeln genauso mächtig ist wie jenes der beliebigen Schaltkreise, also ob $\mathsf{VP}_\mathrm{e} \stackrel{?}{=} \mathsf{VP}$. Andererseits gilt folgendes überraschendes Resultat.

Satz 2.4.4 ($\mathsf{VNP} = \mathsf{VNP}_\mathrm{e}$)**.**
Wir haben die Inklusion $\mathsf{VNP} \subseteq \mathsf{VNP}_\mathrm{e}$*. Insbesondere ist damit* $\mathsf{VNP} = \mathsf{VNP}_\mathrm{e}$*.*

Beweis. [Bür00, Theorem 2.13]. □

Der Beweis nutzt nun folgende kombinatorische Interpretation der Permanente:
Es sei $G = (V, E)$ ein gerichteter Graph mit einer Gewichtsfunktion $w\colon E \to K \cup \underline{X}$. Es sei $A = (a_{ij}) \in \mathrm{Mat}_{|V|}(K \cup \underline{X})$ die Gewichtsmatrix mit

$$a_{ij} = \begin{cases} w((v_i, v_j)) & \text{falls } (v_i, v_j) \in E, \\ 0 & \text{sonst.} \end{cases}$$

Definiere dann $\operatorname{perm}(G) \coloneqq \operatorname{perm}(A) \in K[\underline{X}]$. Da die Permanente invariant unter Permutation der Zeilen und Spalten ist, hängt dies nicht von der Nummerierung der Knoten ab. Eine *Zyklenüberdeckung* $(\pi_1, \dots, \pi_k)$ von G ist eine Überdeckung von V mit disjunkten Zyklen $\pi_1, \dots, \pi_k$. Ist $\pi_i = (v_0^{(i)}, \dots, v_{l_i}^{(i)})$, so definieren wir

$$w(\pi_i) \coloneqq \prod_{j=1}^{l_i} w((v_{j-1}^{(i)}, v_j^{(i)})) \qquad w(\pi) \coloneqq w(\pi_1) \cdots w(\pi_k).$$

Dann rechnet man nach

$$\operatorname{perm}(G) = \sum_{\substack{\pi \text{ Zyklen-} \\ \text{überdeckung}}} w(\pi).$$

Beweis von Satz 2.4.1. Wir haben bereits in Satz 2.2.7 gesehen, dass $(\operatorname{perm}_n)_n \in \mathsf{VNP}$. Der Beweis der VNP-Schwere ist aufwändiger und wird im Buch von Bürgisser ausführlich dargestellt [Bür00, Abschnitt 2.2]. Wir geben hier nur die wesentlichen Schritte an.
Schritt 1: Sei $(f_n)_n \in \mathsf{VNP}$. Nach Satz 2.4.4 ist $(f_n)_n \in \mathsf{VNP}_\mathrm{e}$, wir können also annehmen, dass

$$f_n(\underline{X}) = \sum_{e \in \{0,1\}^{q(n)}} \tilde{f}_n(\underline{X}, e), \qquad (\tilde{f}_n)_n \in \mathsf{VP}_\mathrm{e}.$$

Schritt 2: Es sei nun $E_n \coloneqq L_\mathrm{e}(\tilde{f}_n)$ und C eine Formel mit E_n Gattern, welche $\tilde{f}_n$ berechnet. Dann konstruiert man aus C explizit einen gewichteten Graphen G_n mit $E_n + 1$ Knoten, sodass $\operatorname{perm}(G_n) = \tilde{f}_n$ [Bür00, Proposition 2.16].
Schritt 3: Aus dem Graphen G_n konstruiert man nun einen gewichteten Graphen F_n' mit höchstens $6(E_n + 1)$ Knoten, sodass

$$f_n(\underline{X}) = \sum_{e \in \{0,1\}^{q(n)}} \tilde{f}_n(\underline{X}, e) = \operatorname{perm}(F_n') \tag{2.3}$$

[Bür00, Proposition 2.17]. In dieser Konstruktion werden dem gewichteten Graphen G_n geschickt konstruierte Teilgraphen hinzugefügt, um die Summation über $e \in \{0,1\}$ als Summe über die Zyklenüberdeckungen zu erreichen.
Schritt 4: Die Gleichung (2.3) zeigt, dass $f_n \leq \operatorname{perm}_{6E_n}$ (wobei die Substitution der Einträge gerade die Gewichtematrix von F ist). Somit ist schließlich $(f_n)_n \leq_\mathrm{p} (\operatorname{perm}_n)_n$ gezeigt. □

Einer dieser „Bausteine“ besitzt Kantengewichte der Größe $\pm\frac{1}{2}$; an dieser Stelle des Beweises wird verwendet, dass $\operatorname{char}(K) \neq 2$, also $2 \neq 0$ ist. Im Falle $\operatorname{char}(K) = 2$ ist $-1 = 1$, daher stimmen dort die Definitionen von $\det_n$ und perm_n überein. Es wird nicht erwartet, das in diesem Fall $(\operatorname{perm}_n)_n$ VNP-schwer ist, da dies $\mathsf{VNP} = \mathsf{VP}$ zur Folge hätte (siehe auch Satz 2.6.2).

Dieses Resultat zusammen mit Lemma 2.3.5 zeigt, dass Valiants Hypothese (über einem Körper der Charakteristik $\neq 2$) äquivalent ist zu

$$(\operatorname{perm}_n)_n \notin \mathsf{VP}.$$

2.5 Die Komplexität der Determinante

Ist $(f_n)_n \in \mathsf{VP}$ eine VP-vollständige p-Famile, so ist nach Lemma 2.3.5(i) $\mathsf{VP} = \mathsf{VNP}$ genau dann, wenn $(\operatorname{perm}_n)_n \leq_\mathrm{p} (f_n)_n$. Es ist bislang nicht bekannt, ob $(\det_n)_n$ VP-vollständig ist, zumindest ist $(\det_n)_n$ vollständig für eine Teilklasse von VP.

Definition 2.5.1 (Schwach-schiefe Schaltkreise, $L_{\mathrm{ws}}(f)$, $\mathsf{VP}_{\mathrm{ws}}$)**.**

(i) Ein Schaltkreis C ist *schwach-schief* (engl. *weakly skew*), falls der zugrundeliegende Graph G folgende Eigenschaft erfüllt:

($*$) Ist v ein Multiplikationsgatter mit eingehenden Kanten $\alpha, \beta \in E$, so führt das Entfernen von α oder β dazu, dass G (ungerichtet) unzusammenhängend wird.

Die Größe des kleinsten schwach-schiefen Schaltkreises, welcher ein Polynom f berechnet, bezeichnen wir mit $L_{\mathrm{ws}}(f)$.

(ii) Die Klasse $\mathsf{VP}_{\mathrm{ws}}$ besteht aus den p-Familien $(f_n)_n$, sodass $L_{\mathrm{ws}}(f_n) = O(n^c)$ für ein $c \in \mathbb{N}$. ⌟

Die Forderung, dass die berechnenden Schaltkreise schwach-schief seien, bewirkt, dass für jede Multiplikation mindestens einer der Faktoren *ausschließlich* für dieses Produkt berechnet wurde. Offenbar liegt $\mathsf{VP}_{\mathrm{ws}}$ zwischen VP_{e} (noch restriktivere Schaltkreise) und VP (keine Restriktionen außer polynomielle Größe). Wie in Lemma 2.3.3 sieht man, dass $\mathsf{VP}_{\mathrm{ws}}$ unter Projektionen abgeschlossen ist.

Beispiel 2.5.2.

- Der Schaltkreis aus Beispiel 2.1.7 ist nicht schwach-schief, da die Bedingung ($*$) für das mittlere Multiplikationsgatter verletzt ist.
- Der Schaltkreis für imm_n aus Beispiel 2.2.5 lässt sich leicht zu einem schwach-schiefen Schaltkreis umbauen:
  Es sei o. B. d. A. $n \geq 2$. Aus der Konstruktion ist ersichtlich, dass jedes Multiplikationsgatter mindestens eine Eingangsvariable $X_{ij}^{(l)}$ ($l \geq 2$) unmittelbar als Eingang besitzt. Gibt man jedem einzelnen Multiplikationsgatter sein „eigenes“ Eingangsgatter $X_{ij}^{(l)}$, so ist der resultierende Schaltkreis sicher schwach-schief. Dabei wird die Größe des Schaltkreises höchstens verdoppelt (es kommen höchstens so viele Knoten hinzu, wie es Multiplikationsgatter gibt).
- In Satz 2.2.6 haben wir die Determinante mithilfe iterierter Matrixmultiplikation berechnet. Realisiert man im dortigen Schaltkreis die Multiplikation durch schwach-schiefe Schaltkreise, so liefert dies $(\det_n)_n \in \mathsf{VP}_{\mathrm{ws}}$. Ähnlich wie bei der Matrixmultiplikation müssen Kopien der Schaltkreise für $T_{ij}^{(r)}$ genutzt werden, da die Ergebnisse nicht wiederverwendet werden können. ⌟

Satz 2.5.3 ($(\det_n)_n$ ist $\mathsf{VP}_{\mathrm{ws}}$-vollständig)**.**
Jedes Polynom $f \in K[\underline{X}]$ ist eine Projektion von $\det_{m+1}$, $m = L_{\mathrm{ws}}(f)$. Insbesondere ist $(\det_n)_n$ $\mathsf{VP}_{\mathrm{ws}}$-vollständig.

Beweis. [MP08, Theorem 7]. □

Wir haben also die Äquivalenz

$$\mathsf{VP}_{\mathrm{ws}} = \mathsf{VNP} \qquad \Longleftrightarrow \qquad (\mathrm{perm}_n)_n \leq_{\mathrm{p}} (\det_n)_n,$$

sodass $(\mathrm{perm}_n)_n \not\leq_{\mathrm{p}} (\det_n)_n$ zwar notwendig, aber nicht hinreichend für Valiants Hypothese ist. Interessanterweise ist $(\det_n)_n$ vollständig für VP, wenn man zur Berechnung Schaltkreise *quasipolynomieller* Größe zulässt:

Definition 2.5.4 (Quasipolynomiell, VQP, $\leq_{\mathrm{qp}}$)**.**

(i) Eine Funktion $p\colon \mathbb{N} \to \mathbb{N}$ wächst *quasipolynomiell*, falls es ein $c > 0$ gibt mit $p(n) \in 2^{O(\log^c(n))}$.

(ii) Eine p-Familie $(f_n)_n$ liegt in VQP, falls $L(f_n)$ quasipolynomiell beschränkt ist.

(iii) Sind $(f_n)_n$, $(g_n)_n$ p-Familien, so schreiben wir $(f_n)_n \leq_{\mathrm{qp}} (g_n)_n$, falls es eine quasipolynomiell beschränkte Funktion $t\colon \mathbb{N} \to \mathbb{N}$ gibt mit $f_n \leq g_{t(n)}$ für alle $n \in \mathbb{N}$. ⌟

Sicher ist $\mathsf{VP} \subseteq \mathsf{VQP}$, tatsächlich ist sogar $\mathsf{VQP} \not\subseteq \mathsf{VNP}$ [Bür00, Corollary 8.9]. Es gilt nun folgendes Resultat.

Satz 2.5.5 ($(\det_n)_n$ ist VQP-Vollständig)**.**
$(\det_n)_n$ *ist qp-vollständig für die Klasse* VQP*, d.h.* $(f_n)_n \leq_{\mathrm{qp}} (\det_n)_n$ *für jede Familie* $(f_n)_n \in \mathsf{VQP}$*.*

Beweis. [Bür00, Corollary 2.29] oder [MP08, Theorem 4]. □

Auf diese Weise erhält man die Äquivalenz

$$\mathsf{VNP} \subseteq \mathsf{VQP} \qquad \Longleftrightarrow \qquad (\mathrm{perm}_n)_n \leq_{\mathrm{qp}} (\det_n)_n.$$

Die Hypothese $\mathsf{VNP} \not\subseteq \mathsf{VQP}$ ist also eine *stärkere* Aussage als Valiants Hypothese, und wird auch als *Valiants erweiterte Hypothese* bezeichnet.

2.6 Ein Vergleich mit P und NP

In diesem Abschnitt wollen wir uns kurz der Analogie von VP vs. VNP und P vs. NP widmen. Die Darstellung folgt *Computational Complexity: A Modern Approach* [AB09, insbesondere Abschnitt 16.1].

Definition 2.6.1 (P/poly)**.**
Eine Sprache $A \subseteq \{0,1\}^*$ liegt in P/poly, falls es eine Familie von Booleschen Schaltkreisen $(C_n)_{n\in\mathbb{N}}$ mit folgenden Eigenschaften gibt:

- C_n hat Eingangsvariablen $X_1, \ldots, X_n$ und berechnet genau ein Ausgabegatter.
- $\mathrm{size}(C_n)$ ist polynomiell beschränkt.
- Für alle $n \in \mathbb{N}$ und $x \in \{0,1\}^2$ gilt $x \in A$ genau dann wenn $f_{C_n}(x) = 1$. ⌟

Eine äquivalente Charakterisierung für $A \in \mathsf{P/poly}$ ist, dass es eine deterministische Turingmaschine polynomieller Laufzeit M und Wörter $(\alpha_n)_{n\in\mathbb{N}_0} \subseteq \{0,1\}^*$ polynomieller Länge gibt, sodass für $x \in \{0,1\}^n$ gilt: $x \in A$ genau dann wenn $M(x, \alpha_n)$ akzeptiert [AB09, Theorem 6.18]. Ersetzt man hier deterministisch durch nichtdeterministisch, so erhält man die Klasse NP/poly.

Ein Vergleich von Definition 2.6.1 und 2.2.4 zeigt, dass VP ein algebraisches Analogon von P/poly ist: Eine Sprache A ist in P/poly, wenn die charakteristische Funktion von $A \cap \{0,1\}^n$ von Booleschen Schaltkreisen polynomieller Größe berechnet werden kann.

Um eine Analogie von VNP und NP zu ziehen, erinnern wir an die Charakterisierung von NP durch Zertifikate: $A \in \mathsf{NP}$, falls es eine Sprache $B \in \mathsf{P}$ gibt, sodass für $x \in \{0,1\}^*$ gilt

$$x \in A \quad \Longleftrightarrow \quad \exists e \in \{0,1\}^{\mathrm{poly}(|x|)} : (x,e) \in B.$$

Dem Quantor $\exists e \in \{0,1\}^p$ entspricht der Ausdruck $\bigvee_{e\in\{0,1\}^p}$. Das algebraische Analogon des logischen Oders ist die Summe, also $\sum_{e\in\{0,1\}^p}$.

Wir zitieren noch folgendes Resultat, welches Valiants Hypothese mit P vs. NP in Zusammenhang bringt.

Satz 2.6.2.
Angenommen $\mathsf{VP} = \mathsf{VNP}$ *über einem Körper* K*, sodass entweder*

(i) K *ein endlicher Körper ist, oder*
(ii) $\mathrm{char}(K) = 0$ *und die verallgemeinerte Riemann-Hypothese wahr ist.*

Dann ist $\mathsf{P/poly} = \mathsf{NP/poly}$ *und die Polynomialzeithierarchie kollabiert auf die zweite Stufe.*

Beweis. [Bür00, Corollary 4.6]. □

Kapitel 3

Das Orbitabschlussproblem

In diesem Kapitel übersetzen wir Valiants Hypothese aus dem Kontext der algebraischen Komplexitätstheorie in ein geometrisches Problem über Gruppenoperationen. Um dieses Problem untersuchen zu können, werden grundlegende Konzepte der algebraischen Geometrie eingeführt. Die Situation wird am Beispiel des Waringranges illustriert.

Inhaltlich folgen wir dem Buch von Landsberg [Lan17, Kapitel 1] und der Arbeit von Ikenmeyer [Ike12, Kapitel 2 und 3]. Bei Verständnis hat mir das Vorlesungsskript zur geometrischen Komplexitätstheorie von Bläser und Ikenmeyer sehr geholfen [BI18].

3.1 Algebraische Komplexitätsmaße

Definition 3.1.1 (Affine/lineare Projektion, determinantielle Komplexität dc)**.**
Es seien $f \in K[X_1, \dots, X_n]$, $g \in K[Y_1, \dots, Y_m]$ Polynome.

(i) f ist eine *affine Projektion* von g, falls es lineare Polynome $\ell_1, \dots, \ell_m \in K[\underline{X}]_{\leq 1}$ gibt mit
$$f(\underline{X}) = g(\ell_1(\underline{X}), \dots, \ell_m(\underline{X})).$$
f ist eine *lineare* Projektion von g, falls die ℓ_i homogen (also aus $K[\underline{X}]_1$) gewählt werden können.

(ii) Die *determinantielle Komplexität* $\mathrm{dc}(f)$ ist definiert als das kleinste $k \in \mathbb{N}$, sodass f eine affine Projektion von $\det_k$ ist. Konkret ist $\mathrm{dc}(f)$ die minimale Größe einer Matrix linearer Polynome $A(\underline{X}) = (\ell_{ij}(\underline{X}))_{i,j=1}^{k} \in \mathrm{Mat}_k(K[\underline{X}]_{\leq 1})$ mit
$$f(\underline{X}) = \det \begin{pmatrix} \ell_{11}(\underline{X}) & \dots & \ell_{1k}(\underline{X}) \\ \vdots & \ddots & \vdots \\ \ell_{k1}(\underline{X}) & \dots & \ell_{kk}(\underline{X}) \end{pmatrix}.$$

⌟

$\mathrm{dc}(f)$ ist für jedes Polynom definiert, da $(\det_n)_n$ wie in 2.5.3 gesehen eine universelle Familie ist.

Lemma 3.1.2.
Eine p-Familie $(f_n)_n$ liegt in $\mathsf{VP}_{\mathrm{ws}}$ genau dann, wenn $\mathrm{dc}(f_n)$ polynomiell beschränkt ist.

Beweis. Falls $(f_n)_n \in \mathsf{VP}_{\mathrm{ws}}$, so ist $(f_n)_n \leq_{\mathrm{p}} (\det_n)_n$, also $f_n \leq \det_{p(n)}$ für eine polynomiell beschränkte Funktion p. Nach Definition der determinantiellen Komplexität ist dann $\mathrm{dc}(f_n) \leq p(n)$, also polynomiell beschränkt.

Es sei umgekehrt $\mathrm{dc}(f_n) = p(n) \in O(n^c)$. Seien ℓ_{ij} lineare Polynome, sodass f_n eine affine Projektion von $\det_{p(n)}$ ist. Wir wissen, dass lineare Polynome $a_0 + a_1X_1 + \dots + a_nX_n$

Formeln linearer Größe besitzen (Beispiel 2.4.3). Ist C_n ein schwach-schiefer Schaltkreis, welcher $\det_n$ berechnet, so können die Eingänge, welche mit der Eingangsvariablen X_{ij} belegt werden, durch die Formeln für ℓ_{ij} ersetzt werden. Der so resultierende Schaltkreis C'_n berechnet f_n, ist selbst schwach-schief, und ist höchstens $O(n)$-Mal größer als C_n. Dies zeigt, dass $L_{\mathrm{ws}}(f_n)$ polynomiell beschränkt ist. □

Interessanterweise lässt sich also die Aussage „$\mathsf{VNP} \neq \mathsf{VP}_{\mathrm{ws}}$“ (für $\mathrm{char}(K) \neq 2$) äquivalent ausdrücken als

„Zu jedem $c \in \mathbb{N}$ gibt es ein $n_0 \in \mathbb{N}$ mit $\mathrm{dc}(\mathrm{perm}_n) > n^c$ für $n \geq n_0$.“

Eine analoge Aussage lässt sich auch für $\mathsf{VNP} \not\subseteq \mathsf{VQP}$ treffen. In dieser Formulierung kommt nun unser Berechnungsmodell der arithmetischen Schaltkreise gar nicht vor; die Definition für dc lässt sich lediglich mit Mitteln der (linearen) Algebra ausdrücken!

Ein Beispiel für ein anderes algebraisches Komplexitätsmaß ist der Waringrang.

Definition 3.1.3 (Waringrang WRank, Waringzerlegung)**.**
Es sei $f \in K[\underline{X}]_d$ ein homogenes Polynom. Der *Waringrang* oder auch *symmetrischer Rang* $\mathrm{WRank}(f) \in \mathbb{N}_0$ ist die kleinste Zahl $r \in \mathbb{N}$, sodass es Linearformen $\ell_1, \ldots, \ell_r \in K[\underline{X}]_1$ gibt mit

$$f = \ell_1^d + \cdots + \ell_r^d.$$

Eine solche Darstellung als Summe von Potenzen von Linearformen heißt *Waringzerlegung* von f. ⌟

Der Waringrang $\mathrm{WRank}(f)$ von $f \in K[\underline{X}]_d$ ist also das kleinste $r \in \mathbb{N}$, sodass f eine lineare Projektion von $X_1^d + X_2^d + \cdots + X_r^d$ ist.

Beispiel 3.1.4.
Das Polynom $f = XY \in \mathbb{C}[X, Y]_2$ ist kein Quadrat einer Linearform, da

$$\ell^2 = (a_1 X + a_2 Y)^2 = a_1^2 X^2 + 2a_1 a_2 XY + a_2^2 Y^2 \stackrel{!}{=} XY$$

durch Koeffizientenvergleich $a_1^2 = a_2^2 = 0$, also $\ell = 0$ liefert, im Widerspruch zu $f \neq 0$. Somit ist $\mathrm{WRank}(f) \geq 2$, und es herrscht Gleichheit, da

$$\begin{aligned} XY &= \frac{1}{4}X^2 + \frac{1}{2}XY + \frac{1}{4}Y^2 - \frac{1}{4}X^2 + \frac{1}{2}XY - \frac{1}{4}Y^2 \\ &= \frac{1}{2}(X+Y)^2 - \frac{1}{2}(X-Y)^2 = \left(\frac{1}{2}X + \frac{1}{2}Y\right)^2 + \left(\frac{i}{2}X - \frac{i}{2}Y\right)^2. \end{aligned}$$ ⌟

Es stellt sich die Frage, ob jedes Polynom eine Waringzerlegung besitzt. Über den komplexen Zahlen können wir diese Frage positiv beantworten:

Lemma 3.1.5 (Erste Eigenschaften des Waringrangs)**.**

(i) *Jedes Polynom $f \in \mathbb{C}[X_1, \ldots, X_n]_d$ besitzt eine Waringzerlegung.*

(ii) $\mathrm{WRank}(f)$ *ist das kleinste $r \in \mathbb{N}$, sodass es $\ell_1, \ldots, \ell_r \in \mathbb{C}[\underline{X}]_1$, $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ gibt mit*

$$f = \lambda_1 \ell_1^d + \cdots + \lambda_r \ell_r^d.$$

(iii) *Ist $\lambda \in \mathbb{C} \setminus \{0\}$, so ist* $\mathrm{WRank}(\lambda f) = \mathrm{WRank}(f)$.

Beweis. (ii) Eine Waringzerlegung ist von der Gestalt des Lemmas ($\lambda_1 = \cdots = \lambda_r = 1$). Umgekehrt kann man in jede Potenz einer Linearform einen Skalar hineinziehen, da in $\mathbb{C}$ jede Zahl eine d-te Wurzel besitzt:

$$\lambda \cdot (a_1 X_1 + \cdots + a_n X_n)^d = \left((\sqrt[d]{\lambda} a_1) X_1 + \cdots + (\sqrt[d]{\lambda} a_n X_n)\right)^d.$$

Dies zeigt, dass jede Darstellung aus dem Lemma zu einer Waringzerlegung der gleichen Länge umgeformt werden kann:

$$f = \sum_{i=1}^{r} \lambda_i \ell_i(X_1, \dots, X_n)^d = \sum_{i=1}^{r} \ell_i(\sqrt[d]{\lambda_i} X_1, \dots, \sqrt[d]{\lambda_i} X_n)^d$$

(iii) Ist $f = \sum_{i=1}^{r} \ell_i^d$, so ist $\lambda f = \sum_{i=1}^{r} \lambda \ell_i^d$. Nach (ii) ist also $\mathrm{WRank}(\lambda f) \leq \mathrm{WRank}(f)$. Wendet man die Argumentation auf $f = \frac{1}{\lambda} \cdot \lambda f$ an, so erhält man die umgekehrte Ungleichung $\mathrm{WRank}(f) = \mathrm{WRank}(\frac{1}{\lambda} \cdot \lambda f) \leq \mathrm{WRank}(\lambda f)$.

(i) Für das Polynom $X_1 \cdots X_d$ kann man eine explizite Formel angeben:

$$X_1 \cdots X_d = \frac{1}{2^d d!} \sum_{\varepsilon \in \{-1,1\}^d} \varepsilon_1 \cdots \varepsilon_d \cdot \left(\sum_{j=1}^{d} \varepsilon_j X_j \right)^d.$$

Eine Analyse des Waringranges dieses Monoms findet sich im Buch von Landsberg [Lan17, Abschnitt 7.1.2 und 10.1.4], tatsächlich ist $\mathrm{WRank}(X_1 \cdots X_d) = 2^{d-1}$ (ohne Beweis). Durch eine Substitution $\{X_1, \dots, X_d\} \to \{\tilde{X}_1, \dots, \tilde{X}_n\}$,

$$X_1, \dots, X_{d_1} \mapsto \tilde{X}_1, \quad X_{d_1+1} = \cdots = X_{d_1+d_2} = \tilde{X}_2, \quad \dots$$

gewinnt man daraus eine Waringzerlegung für jedes beliebige Monom $\tilde{X}_1^{d_1} \cdots \tilde{X}_n^{d_n}$. Da jedes $f \in \mathbb{C}[\underline{X}]_d$ eine Linearkombination von Monomen vom Grad d ist, ist die Aussage gezeigt. □

Korollar 3.1.6 (Globale Abschätzung für WRank)**.**
Für jedes $f \in \mathbb{C}[X_1, \dots, X_n]_d$ *ist* $\mathrm{WRank}(f) \leq \dim_{\mathbb{C}} \mathbb{C}[X_1, \dots, X_n]_d = \binom{d+n-1}{d}$.

Beweis. Da jedes Polynom eine Waringzerlegung besitzt, spannen die Polynome der Form ℓ^d, $\ell \in \mathbb{C}[X_1, \dots, X_n]_1$ den Raum $\mathbb{V} = \mathbb{C}[X_1, \dots, X_n]_d$ auf. Da jedes Erzeugendensystem eine Basis enthält, zeigt dies, dass es eine Basis von $\mathbb{V}$ der Form $\{\ell_1^d, \dots, \ell_m^d\}$ gibt ($m = \dim \mathbb{V}$). Jedes $f \in \mathbb{V}$ lässt sich als Linearkombination der ℓ_i^d schreiben, nach vorigem Lemma ist $\mathrm{WRank}(f) \leq \dim \mathbb{V}$. □

Waringzerlegungen können als eingeschränktes Maschinenmodell für die Auswertung von Polynomen angesehen werden: Das Polynom $w = X_1^d + \cdots + X_r^d$ hat Formelkomplexität

$$L_{\mathrm{e}}(w) \leq \underbrace{r \cdot (d-1)}_{r \times (d\text{-Potenz})} + \underbrace{r-1}_{\text{Summe}} = rd - 1.$$

Nach Satz 2.5.3 ist $X_1^d + \cdots + X_r^d$ somit eine Projektion von $\det_{dr}$. Wir folgern daraus:

Lemma 3.1.7.
Für $f \in \mathbb{C}[X_1, \dots, X_n]_d$ *ist* $\mathrm{dc}(f) \leq d \cdot \mathrm{WRank}(f)$.

Beweis. Ist $f = \ell_1^d + \cdots + \ell_r^d$, so ersetze in einer Projektion $w \leq \det_{dr}$ die X_j durch ℓ_j, um f als affine Projektion von $\det_{dr}$ zu realisieren. Dies zeigt $\mathrm{dc}(f) \leq d \cdot \mathrm{WRank}(f)$. □

3.2 Umformulierung als Orbitproblem

Wie im ersten Kapitel gesehen, operiert das Monoid $\mathrm{Mat}_n(\mathbb{C})$ auf dem Raum $\mathbb{C}^n$. Wir wollen diese Operation auf den Ring $\mathbb{C}[X_1, \dots, X_n]$ übertragen:

Es bezeichne B^T die transponierte Matrix, dann definiere für $B = (b_{ij})_{i,j=1}^n \in \mathrm{Mat}_n(\mathbb{C})$, $f \in \mathbb{C}[X_1, \dots, X_n]$ und $x \in \mathbb{C}^n$

$$(B \triangleright f)(x) \coloneqq f(B^\mathsf{T} x).$$

Fasst man die Koordinaten $x = (x_1, \dots, x_n)$ als Variablen auf, so sieht man sofort, dass auch $B \triangleright f$ ein Polynom definiert:

$$\begin{aligned} f &= \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} \cdot X_1^{k_1} \cdots X_n^{k_n} \in \mathbb{C}[X_1, \dots, X_n], \\ B \triangleright f &= \sum_{|\boldsymbol{k}| \le d} a_{\boldsymbol{k}} \cdot (b_{11}X_1 + \cdots + b_{n1}X_n)^{k_1} \cdots (b_{n1}X_1 + \cdots + b_{nn}X_n)^{k_n}. \end{aligned} \tag{3.1}$$

Lemma 3.2.1 ($\mathrm{Mat}_n(\mathbb{C})$ operiert linear auf $\mathbb{C}[X_1, \dots, X_n]$)**.**

(i) *Diese Abbildung* $\mathrm{Mat}_n(\mathbb{C}) \times \mathbb{C}[X_1, \dots, X_n] \to \mathbb{C}[X_1, \dots, X_n]$ *erfüllt die Axiome einer Monoidoperation.*

(ii) *Die Operation schränkt sich zu einer Operation auf* $\mathbb{C}[X_1, \dots, X_n]_d$ *ein.*

(iii) *Sind* $f, g \in \mathbb{C}[X_1, \dots, X_n]$, $\lambda \in \mathbb{C} = \mathbb{C}[X_1, \dots, X_n]_0$ *und* $A \in \mathrm{Mat}_n(\mathbb{C})$*, so ist*

$$A \triangleright (f + g) = (A \triangleright f) + (A \triangleright g), \quad A \triangleright (f \cdot g) = (A \triangleright f) \cdot (A \triangleright g), \quad A \triangleright \lambda = \lambda.$$

Beweis. (i) Zunächst ist $I_n \triangleright f = f$. Für $A, B \in \mathrm{Mat}_n(K)$ rechnen wir unter Verwendung von $(AB)^\mathsf{T} = B^\mathsf{T} A^\mathsf{T}$ nach

$$(A \triangleright (B \triangleright f))(x) = (B \triangleright f)(A^\mathsf{T} x) = f(B^\mathsf{T} A^\mathsf{T} x) = f((AB)^\mathsf{T} x) = (AB \triangleright f)(x).$$

(ii) Ist $f \in \mathbb{C}[X_1, \dots, X_n]_d$ homogen, so steht in (3.1) eine Summe von Produkten von Linearformen. Da das Produkt von $k_1 + \cdots + k_n = d$ Linearformen homogen vom Grad d ist, liegt $B \triangleright f$ wieder in $\mathbb{C}[X_1, \dots, X_n]_d$.

(iii) Es seien A, f, g wie oben gegeben, so ist

$$(A \triangleright (f + g))(x) = (f + g)(A^\mathsf{T} x) = f(A^\mathsf{T} x) + g(A^\mathsf{T} x) = (A \triangleright f + A \triangleright g)(x).$$

Die Rechnung verläuft völlig analog für die Multiplikation. Ist λ ein konstantes Polynom, so kommt in (3.1) kein Monom von positivem Grad vor, daher wird λ invariant gelassen. □

Der letzte Punkt impliziert, dass die Zuordnung $f \mapsto A \triangleright f$ für ein festes $A \in \mathrm{Mat}_n(\mathbb{C})$ einen Ringhomomorphismus $\mathbb{C}[\underline{X}] \to \mathbb{C}[\underline{X}]$ definiert ($A \triangleright 1 = 1$ ist hier klar).

Nun sehen wir, dass sich der Waringrang ausdrücken lässt als Eigenschaft des Orbits dieser Operation:

Satz 3.2.2 (Waringrang als Orbitproblem)**.**
Es sei nun $f \in \mathbb{C}[X_1, \dots, X_n]_d$ *homogen vom Grad* d, $N = \dim \mathbb{C}[X_1, \dots, X_n]_d$*. Dann gilt für* $r \le N$

$$\mathrm{WRank}(f) \le r \quad \Longleftrightarrow \quad f \in \mathrm{Mat}_N(\mathbb{C}) \triangleright (X_1^d + \cdots + X_r^d).$$

Dabei ist die Operation von $\mathrm{Mat}_N(\mathbb{C})$ auf dem Raum $\mathbb{C}[X_1, \dots, X_N]_d$ zu verstehen, um sicherzustellen, dass $X_1^d, \dots, X_r^{\mathrm{WRank}(f)}$ in diesem Raum enthalten ist.

Beweis. Es sei zunächst

$$f = \ell_1^d + \cdots + \ell_r^d, \quad \text{mit} \quad \ell_j = a_{1j}X_1 + \cdots + a_{nj}X_n. \tag{3.2}$$

Setze $a_{ij} \coloneqq 0$ für $i > n$ oder $j > r$, so erhalten wir eine $N \times N$-Matrix $A = (a_{ij})_{i,j=1}^{N} \in \mathrm{Mat}_N(\mathbb{C})$. Einsetzen liefert

$$\ell_1^d + \cdots + \ell_r^d = \begin{pmatrix} a_{11} & \dots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \dots & a_{NN} \end{pmatrix} \triangleright (X_1^d + \cdots + X_r^d) \in \mathrm{Mat}_n(\mathbb{C}) \triangleright (X_1^d + \cdots + X_r^d).$$

Ist umgekehrt $f = A \triangleright (X_1^d + \cdots + X_r^d)$ für ein $A \in \mathrm{Mat}_n(\mathbb{C})$, zeigt selbige Rechnung, dass f eine Waringzerlegung der Länge $\leq r$ besitzt:

$$f = A \triangleright (X_1^d + \cdots + X_r^d) = \sum_{j=1}^{r} \left(\sum_{i=1}^{N} a_{ij} X_i \right)^d.$$

Dabei können grundsätzlich Variablen X_i, $i > n$ auftauchen, da diese jedoch nicht in f vorkommen, können wir für all diese Variablen $X_i = 0$ substituieren und erhalten eine Summe, in denen nur $X_1, \dots, X_n$ auftaucht. □

Um eine analoge Aussage für die determinantielle Komplexität treffen zu können, machen wir zunächst folgende Beobachtung: Es sei f ein Polynom vom Grad d mit $\mathrm{dc}(f) \leq r$, also $f = \det(A(X_1, \dots, X_n))$, wobei

$$A = (A_{ij})_{i,j=1}^{r} \in \mathrm{Mat}_r(\mathbb{C}[\underline{X}]_{\leq 1}), \qquad A_{ij} = a_{ij}^{(0)} + \sum_{k=1}^{n} a_{ij}^{(k)} X_k.$$

Homogenisiert man die linearen Polynome A_{ij} mittels der Variablen Y, so erhält man eine Matrix $\tilde{A} \in \mathrm{Mat}_n(\mathbb{C}[X_1, \dots, X_n, Y]_1)$ mit

$$\det \tilde{A} = \sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) \cdot \prod_{i=1}^{r} \tilde{A}_{i\sigma(i)}(X_1, \dots, X_n, Y) = Y^{r-d} \tilde{f},$$

wobei $\tilde{f}$ die Homogenisierung von f ist. Die Ursprüngliche affine Projektion kann man durch $Y = 1$ wieder zurückgewinnen. Dies zeigt, dass f genau dann eine affine Projektion von $\det_r$ ist, wenn $Y^{r-d}\tilde{f}$ eine lineare Projektion von $\det_r$ ist.

Mit dieser Modifikation von f erreichen wir genau die Situation wie beim Waringrang, sodass der Beweis völlig analog funktioniert. Nach Lemma 3.1.7 können wir ein N abhängig von n und d wählen, sodass $\mathrm{dc}(f) \leq N(n, d)$ für alle $f \in \mathbb{C}[X_1, \dots, X_n]_d$.

Satz 3.2.3 (Determinantielle Komplexität als Orbitproblem).
Es sei $f \in \mathbb{C}[X_1, \dots, X_n]_{\leq d}$ vom Grad d und $\tilde{f}$ seine Homogenisierung. Es sei $N \geq \mathrm{dc}(f)$ und wähle eine beliebige Inklusion von $\{X_1, \dots, X_n, Y\} \hookrightarrow \{X_{11}, \dots, X_{NN}\}$. Dann gilt für $r \leq N$

$$\mathrm{dc}(f) \leq r \quad \iff \quad Y^{r-d}\tilde{f} \in \mathrm{Mat}_{N^2}(\mathbb{C}) \triangleright \det_r .$$

3.3 Grenzkomplexität

Unser Ziel ist es nun, unter den Polynomen in $\mathbb{C}[X_1, \dots, X_n]$ jene mit beschränkter Komplexität bezüglich eines Komplexitätsmaßes $\mathcal{L}\colon \mathbb{C}[\underline{X}] \to \mathbb{N}$ wie dc oder WRank auszuzeichnen. Wir beschränken uns dabei auf homogene Polynome vom Grad d, welche einen endlichdimensionalen $\mathbb{C}$-Vektorraum bilden:

$$\mathbb{V} \coloneqq \mathbb{C}[X_1, \dots, X_n]_d.$$

Es sei nun $U \subseteq V$ die Teilmenge der Polynome mit Komplexität $\leq c$:

$$U = \{ f \in \mathbb{V} \mid \mathcal{L}(f) \leq c \}.$$

Da der Vektorraum $\mathbb{V}$ nach Beispiel 1.4.4 ein topologischer Raum ist, kann man der Frage nachgehen, ob sich Polynome größerer Komplexität nicht zumindest durch Polynome kleinerer Komplexität *approximieren* lassen . Formalisiert wird dies durch folgenden Begriff.

Definition 3.3.1 (Grenzkomplexität $\overline{\mathcal{L}}(f)$, $\overline{\mathrm{WRank}}$, $\overline{\mathrm{dc}}$)**.**
Es sei $f \in \mathbb{C}[X_1, \ldots, X_n]_d$. Die *Grenzkomplexität* $\overline{\mathcal{L}}(f)$ ist das kleinste $r \in \mathbb{N}$, sodass es eine Folge $(f_n)_{n\in\mathbb{N}}$ in $\mathbb{V}$ gibt, welche gegen f konvergiert, und deren Elemente Komplexität $\mathcal{L}(f_n) \leq r$ haben.

Insbesondere definiert dies $\overline{\mathrm{WRank}}$ und $\overline{\mathrm{dc}}$ für homogene Polynome. ⌟

Es ist also $\overline{\mathcal{L}}(f) \leq c$, falls sich f beliebig gut durch Polynome von Komplexität $\leq c$ approximieren lässt.

Beispiel 3.3.2 ($\overline{\mathrm{WRank}}(XY^2) < \mathrm{WRank}(XY^2)$)**.**
Es sei $f(X, Y) = XY^2$. Nach Lemma 3.1.5 ist $\mathrm{WRank}(XY^2) \leq 3$, da

$$6XY^2 = (X + Y)^3 + (X - Y)^3 - 2X^3.$$

Man kann zeigen, dass tatsächlich $\mathrm{WRank}(XY^2) = 3$. Allgemein haben Carlini, Catalisano und Geramita eine geschlossene Formel für $\mathrm{WRank}(X_1^{d_1} \cdots X_n^{d_n})$ gefunden [CCG12]. Andererseits lässt sich f als Grenzwert von Polynomen mit Waringrang 2 schreiben:

$$\lim_{\varepsilon\to 0} \left(\frac{1}{3\varepsilon}(\varepsilon X - Y)^3 + \frac{1}{3\varepsilon} Y^3 \right) = \lim_{\varepsilon\to 0} \frac{\varepsilon^3 X^3 - 3\varepsilon^2 X^2 Y + 3\varepsilon X Y^2 - Y^3 + Y^3}{3\varepsilon} = XY^3.$$

Dies zeigt $\overline{\mathrm{WRank}}(f) \leq 2 < 3 = \mathrm{WRank}(f)$. ⌟

Wir können nun Satz 3.2.3 auf die Grenzkomplexität übertragen:

Satz 3.3.3 (Das Orbitabschlussproblem der Determinante)**.**
Es sei $f \in \mathbb{V} = \mathbb{C}[X_1, \ldots, X_n]_d$. Es sei $m \in \mathbb{N}$ mit $m^2 \geq n + 1$ und $m \geq d$ und wähle eine beliebige Inklusion von $\{X_1, \ldots, X_n, Y\} \hookrightarrow \{X_{11}, \ldots, X_{mm}\}$.

$$\overline{\mathrm{dc}}(f) \leq m \quad \Longleftrightarrow \quad Y^{m-n} f \in \overline{\mathrm{Mat}_{m^2}(\mathbb{C}) \triangleright \det_m}.$$

Beweis. Eine Folge $(f_n)_n \subseteq \mathbb{V}$ konvergiert gegen f genau dann, wenn $(Y^{m-d} f_n)_n$ in $\mathbb{C}[X_{11}, \ldots, X_{mm}]_m$ gegen $Y^{m-d} f$ konvergiert (da die Koeffizientenvektoren bis auf Nulleinträge gleich bleiben). Nach Satz 3.2.3 ist $\mathrm{dc}(f_n) \leq m$ genau dann wenn $Y^{m-d} f_n$ im Orbit von $\det_m$ liegt. Somit ist $\overline{\mathrm{dc}}(f) \leq m$ genau dann, wenn $Y^{m-d} f$ im Orbitabschluss von $\det_m$ liegt. □

Ein Vorteil der Grenzkomplexität ist es, dass wir die Monoidoperation von $\mathrm{Mat}_n(\mathbb{C})$ durch die Gruppenoperation von $\mathrm{GL}_n(\mathbb{C})$ ersetzen können.

Lemma 3.3.4 (Die Orbiten unter $\mathrm{Mat}_n(\mathbb{C})$ und $\mathrm{GL}_n(\mathbb{C})$ haben denselben Abschluss)**.**
Ist $g \in \mathbb{C}[X_1, \ldots, X_N]_d$ ein Polynom, so ist

$$\overline{\mathrm{Mat}_N(\mathbb{C}) \triangleright g} = \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g}$$

Insbesondere trifft dies auf $g = X_1^d + \cdots + X_N^d$ und $g = \det_n$ (für $n^2 = N$) zu.

Wir verwenden die Tatsache, dass die Operation von $\mathrm{GL}_N(\mathbb{C})$ auf $\mathbb{V}$ stetig ist; dies wird später im Beweis von Satz 3.5.3 klar werden.

Beweis. Wir zeigen zunächst, dass es zu $A \in \mathrm{Mat}_N(\mathbb{C})$ eine Folge $(A_n)_{n\in\mathbb{N}} \subset \mathrm{GL}_N(\mathbb{C})$ mit $\lim_{n\to\infty} A_n = A$ (im Vektorraum $\mathrm{Mat}_N(\mathbb{C})$) gibt. Betrachte dazu

$$\chi_A(1/m) = \det(\tfrac{1}{m} \cdot I_n - A), \qquad m \in \mathbb{N}$$

Da das charakteristische Polynom nur endlich viele Nullstellen hat, gibt es ein $n_0 \in \mathbb{N}$ mit

$$\det(\tfrac{1}{m} I_n - A) \neq 0 \qquad \text{für } m \geq n_0$$

Daher ist $A_n \coloneqq A - \frac{1}{n+n_0} I_n$ eine Folge invertierbarer Matrizen, welche gegen A konvergiert.

Die Inklusion $\overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g} \subseteq \overline{\mathrm{Mat}_N(\mathbb{C}) \triangleright g}$ ist klar. Es sei nun $f = A \triangleright g$ für ein $A \in \mathrm{Mat}_N(\mathbb{C})$. Es sei A_n eine Folge aus $\mathrm{GL}_N(\mathbb{C})$, welche gegen A konvergiert, dann ist wegen der Stetigkeit

$$f = A \triangleright g = (\lim_{n\to\infty} A_n) \triangleright g \overset{\text{stetig}}{=} \lim_{n\to\infty} (A_n \triangleright g) \in \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g}.$$

Somit ist $\mathrm{Mat}_N(\mathbb{C}) \triangleright g \subseteq \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g}$. Da die rechte Menge abgeschlossen ist, folgt damit auch $\overline{\mathrm{Mat}_N(\mathbb{C}) \triangleright g} \subseteq \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g}$ □

Um die Struktur dieses Orbitabschlusses besser zu verstehen, führen wir einige Grundbegriffe der algebraischen Geometrie ein.

3.4 Grundlagen algebraischer Geometrie

Die algebraische Geometrie beschäftigt sich klassischerweise mit den Nullstellenmengen von Polynomen, und untersucht diese mit algebraischen und geometrischen Methoden. Eine gute Einführung bietet das Buch von Hulek [Hul12], wir benötigen hier nur einige Begriffe aus dem ersten Kapitel.

Definition 3.4.1 (Algebraische Menge, affine Varietät)**.**
Sei $S \subseteq K[X_1, \ldots, X_n]$ eine Menge von Polynomen. Die *Nullstellenmenge* von S ist

$$\mathcal{V}(S) \coloneqq \{\, x \in \mathbb{C}^n \mid f(x) = 0 \text{ für alle } f \in S \,\} \subseteq \mathbb{C}^n.$$

Eine Teilmenge $V \subseteq \mathbb{C}^n$ ist *algebraisch* oder eine *affine Varietät*, falls $V = \mathcal{V}(S)$ für eine Menge von Polynomen S. ⌟

Lemma 3.4.2 (Algebraische Mengen bilden eine Topologie)**.**
Es bezeiche $\mathcal{A} \subseteq \mathcal{P}(\mathbb{C}^n)$ die Menge der algebraischen Mengen in $\mathbb{C}^n$. Dann erfüllt $\mathcal{A}$ die Axiome für abgeschlossene Mengen einer Topologie auf $\mathbb{C}^n$.

Beweis. Wir weisen die Axiome nach.

(i') $\emptyset = \mathcal{V}(\{1\})$, $\mathbb{C}^n = \mathcal{V}(\{0\})$.

(ii') Es seien $V_1 = \mathcal{V}(S_1)$, $V_2 = \mathcal{V}(S_2)$ algebraische Mengen, zeigen wir $V_1 \cup V_2 = \mathcal{V}(S)$, wobei $S = \{\, f_1 \cdot f_2 \mid f_1 \in S_1,\ f_2 \in S_2 \,\}$.
Die Inklusion $V_1 \cup V_2 \subseteq \mathcal{V}(S)$ ist klar. Es sei $x \in \mathbb{C}^n \setminus V_1 \cup V_2$, d.h. es gibt ein $f_1 \in S_1$ mit $f_1(x) \neq 0$ und ein $f_2 \in S_2$ mit $f_2(x) \neq 0$. Da $\mathbb{C}$ nullteilerfrei ist, ist $f_1(x) \cdot f_2(x) \neq 0$ und $x \notin \mathcal{V}(S)$.

(iii') Sind $V_i = \mathcal{V}(S_i)$ für $i \in I$, wobei $S_i \subseteq \mathbb{C}[\underline{X}]$, so ist

$$\bigcap_{i\in I} V_i = \{\, x \in \mathbb{C}^n \mid f(x) = 0 \text{ für alle } i \in I,\ f \in S_i \,\} = \mathcal{V}\big(\textstyle\bigcup_{i\in I} S_i\big). \qquad \square$$

Diese Topologie wird die *Zariskitopologie* auf $\mathbb{C}^n$ genannt

Beispiel 3.4.3.

- Endliche Mengen sind algebraisch: Ist $P = (a_1, \dots, a_n) \in \mathbb{C}^n$, so ist

$$\mathcal{V}(X_1 - a_1, \dots, X_n - a_n) = \{\, x \in \mathbb{C}^n \mid x_1 = a_1, \dots, x_n = a_n \,\} = \{P\}.$$

  Für $V = \{P_1, \dots, P_m\}$ folgt die Aussage, da die Vereinigung endlich vieler algebraischer Mengen wieder algebraisch ist.
- $V(X^2 + Y^2)$ ist die Vereinigung zweier eindimensionaler $\mathbb{C}$-Vektorräume von $\mathbb{C}^2$, da

$$X^2 + Y^2 = (X + iY) \cdot (X - iY) \quad \Longrightarrow \quad \mathcal{V}(X^2 + Y^2) = \mathcal{V}(X + iY) \cup \mathcal{V}(X - iY).$$

- Wir fassen die Menge der komplexen $n \times n$-Matrizen $\mathrm{Mat}_n(\mathbb{C})$ als n^2-dimensionalen Raum $\mathbb{C}^{n^2}$ auf. Die Teilmenge

$$\mathrm{SL}_n(\mathbb{C}) \coloneqq \{\, A \in \mathrm{Mat}_n(\mathbb{C}) \mid \det(A) = 1 \,\}$$

  ist eine algebraische Menge, da die Bedingung $\det(A) = 1$ eine polynomielle Gleichung ist:

$$\mathrm{SL}_n(\mathbb{C}) = \left\{ x = (x_{ij})_{i,j=1}^n \in \mathbb{C}^{n^2} \;\middle|\; \det(x) = \textstyle\sum_{\sigma \in \mathcal{S}_n} \mathrm{sign}(\sigma) \cdot \prod_{i=1}^n x_{i\sigma(i)} = 1 \right\}. \qquad \lrcorner$$

Definition 3.4.4 (Definierendes Ideal, Koordinatenring)**.**
Es sei $V \subseteq \mathbb{C}^n$ eine algebraische Teilmenge.

(i) Das *definierende Ideal* von V ist das Ideal

$$\mathcal{I}(V) \coloneqq \{\, f \in \mathbb{C}[\underline{X}] \mid f(x) = 0 \text{ für alle } x \in V \,\}.$$

(ii) Der Quotient $\mathbb{C}[V] \coloneqq \mathbb{C}[\underline{X}]/\mathcal{I}(V)$ heißt *Koordinatenring* von V. $\lrcorner$

Dass $\mathcal{I}(V)$ ein Ideal ist, rechnet man genau wie in Beispiel 1.1.7 nach. Das Ideal hat die Eigenschaft, dass für $f \in \mathbb{C}[\underline{X}]$ stets gilt

$$f^m \in \mathcal{I}(V) \text{ für ein } m \in \mathbb{N} \quad \Longrightarrow \quad f \in \mathcal{I}(V).$$

Ideale mit dieser Eigenschaft werden *Radikalideale* genannt. Nach Konstruktion des Quotientenringes in Definition 1.1.6 sind dies Polynomfunktionen, welche als gleich angesehen werden, wenn sie auf V dieselbe Funktion definieren.

Die Zuordnungen $\mathcal{I}(-)$ und $\mathcal{V}(-)$ sind invers zueinander, wenn man sie auf geeignete Teilmengen von $\mathbb{C}^n$ bzw $\mathbb{C}[\underline{X}]$ einschränkt.

Satz 3.4.5 (Hilberts Nullstellensatz)**.**
Wir haben eine Bijektion

$$\{\, I \subseteq \mathbb{C}[X_1, \dots, X_n] \mid I \text{ Radikalideal} \,\} \underset{\mathcal{I}(V) \hookleftarrow V}{\overset{I \mapsto \mathcal{V}(I)}{\rightleftarrows}} \{\, V \subseteq \mathbb{C}^n \mid V \text{ algebraisch} \,\}$$

Genauer ist $\mathcal{V}(\mathcal{I}(V)) = V$ für jede algebraische Menge V und $\mathcal{I}(\mathcal{V}(I)) = I$ für jedes Radikalideal I. Diese Bijektion ist inklusionsumkehrend: Für algebraische Mengen V_1, V_2 gilt

$$V_1 \subseteq V_2 \quad \Longleftrightarrow \quad \mathcal{I}(V_1) \supseteq \mathcal{I}(V_2).$$

Beweis. [Hul12, Korollar 1.12] $\square$

Man kann sich bei der Definition der Zariskitopologie auf Nullstellenmengen endlich vieler Polynome beschränken:

Satz 3.4.6 (Hilberts Basissatz)**.**
Ist $I \subseteq \mathbb{C}[X_1, \dots, X_n]$ ein Ideal, so gibt es $f_1, \dots, f_m \in I$ mit

$$I = (f_1, \dots, f_m)_{\mathbb{C}[\underline{X}]} \coloneqq \{\, g_1 f_1 + \cdots + g_m f_m \mid g_1, \dots, g_m \in \mathbb{C}[\underline{X}] \,\}.$$

Jede algebraische Menge $V \subseteq \mathbb{C}^n$ ist die Nullstellenmenge endlich vieler *Polynome.*

Beweis. [Lan02, Corollary 4.4.2] bzw. [Hul12, Lemma 0.1]. □

Definition 3.4.7 (Polynomielle Abbildung)**.**
Eine Abbildung $f\colon \mathbb{C}^n \to \mathbb{C}^m$ ist *polynomiell*, falls es Polynome $f_1, \dots, f_m \in \mathbb{C}[X_1, \dots, X_n]$ gibt, sodass

$$f(x) = (f_1(x), \dots, f_m(x)) \qquad \forall x \in \mathbb{C}^n. \qquad \lrcorner$$

Polynomielle Abbildungen sind stetig in der Standardtopologie und Zariskitopologie.

3.5 Polynomielle Obstruktionen

Es sei nun wieder $\mathbb{V} = \mathbb{C}[X_1, \dots, X_n]_d \cong \mathbb{C}^N$, wobei wir als Basis die Monome $X^{\boldsymbol{k}}$ wählen. Diesen N-dimensionalen Raum fassen wir nun als affinen Raum auf; die Polynome auf diesem Raum bezeichnen wir mit $\mathbb{C}[\mathbb{V}] \coloneqq \mathbb{C}[T_1, \dots, T_N]$.

Um den Abschluss des Orbits der Gruppenoperation besser zu verstehen, benötigen wir folgende Begriffe.

Definition 3.5.1 (Lokalabgeschlossene Menge, konstruierbare Menge)**.**
Wir betrachten $\mathbb{C}^n$ mit der Zariskitopologie.

(i) Eine Menge $M \subseteq \mathbb{C}^n$ heißt *lokalabgeschlossen*, falls es eine offene Menge $U \subseteq \mathbb{C}^n$ und eine abgeschlossene Menge $A \subseteq \mathbb{C}^n$ gibt, sodass $M = A \cap U$.
(ii) Eine Menge $M \subseteq \mathbb{C}^n$ heißt *konstruierbar*, falls $M = M_1 \cup \cdots \cup M_k$ für geeignete lokalabgeschlossene Mengen $M_1, \dots, M_k$. $\lrcorner$

Satz 3.5.2 (Eigenschaften konstruierbarer Mengen, Satz von Chevalley)**.**
Es sei $M \subseteq \mathbb{C}^n$ eine konstruierbare Menge.

(i) *Ist $f\colon \mathbb{C}^n \to \mathbb{C}^m$ eine polynomielle Abbildung, so ist $f(M) \subseteq \mathbb{C}^m$ ebenfalls konstruierbar.*
(ii) *Der Abschluss von M in der Standardtopologie ist gleich dem Abschluss in der Zariskitopologie, insbesondere also eine algebraische Menge.*

Beweis. [Kra84, Abschnitt AI.3.3 Folgerung 2] und [Kra84, Abschnitt AI.7.2 Folgerung]. □

Satz 3.5.3.
Es sei $g \in \mathbb{V} = \mathbb{C}[X_1, \dots, X_n]_d$, $N = \dim \mathbb{V}$.

(i) *Die Menge $M = \mathrm{Mat}_N(\mathbb{C}) \triangleright g$ ist konstruierbar.*
(ii) *Die Menge $\overline{M} \subseteq \mathbb{V}$ ist ein algebraische Menge.*

Beweis. Betrachte die Abbildung

$$\psi\colon \mathrm{Mat}_N(\mathbb{C}) \to \mathbb{V}, \qquad A \mapsto A \triangleright g.$$

Wir weisen nach, dass ψ eine polynomielle Abbildung ist. Es sei $B = (b_{ij})_{i,j=1}^N \in \mathrm{Mat}_N(\mathbb{C})$.

- Die komponentenweise Summe polynomieller Funktionen

$$\psi + \psi' = (\psi_1 + \psi'_1, \ldots, \psi_N + \psi'_N)$$

ist offenbar wieder eine polynomielle Funktion. Da nach Lemma 3.2.1 die Operation linear ist, genügt es, die Aussage für ein Monom $g = X_1^{d_1} \cdots X_n^{d_n}$ zu zeigen.
- Aus der Gleichung 1.1 sieht man, dass sich die Koeffizienten $c_{\boldsymbol{k}}$ des Produktes zweier Polynome als Polynom in den Koeffizienten $a_{\boldsymbol{k}}$ und $b_{\boldsymbol{\ell}}$ ausdrücken lassen. Induktiv gilt dies auch für n-fache Produkte, also lassen sich die Koeffizienten von

$$B \triangleright g = (b_{11}X_1 + \cdots + b_{n1}X_n)^{k_1} \cdots (b_{n1}X_1 + \cdots + b_{nn}X_n)^{k_n}.$$

als Polynom in den a_{ij} ausdrücken.

Nach Satz 3.5.2(i) ist die Menge $M = \mathrm{Mat}_N(\mathbb{C}) \triangleright g = \psi(\mathrm{Mat}_N(\mathbb{C}))$ als Bild der polynomiellen Abbildung ψ konstruierbar, die zweite Aussage folgt dann ebenfalls aus Satz 3.5.2(ii). □

Dies zeigt, dass $\left\{ f \in \mathbb{V} \;\middle|\; \overline{\mathrm{dc}(f)} \leq r \right\} = \mathcal{V}(F_1, \ldots, F_k)$ für endlich viele Polynome $F_1, \ldots, F_k \in \mathbb{C}[T_1, \ldots, T_N]$. Falls man solche Polynome konkret konstruieren kann, ist es leicht, untere Schranken für die Grenzkomplexität zu erhalten:

$$\overline{\mathrm{dc}}(f) > r \qquad \Longleftrightarrow \qquad F_i(f) \neq 0 \text{ für ein } i \in \{1, \ldots, k\}.$$

Untere Schranken sind in diesem Sinne *äquivalent* sind zur Existenz von sogenannten polynomiellen Obstruktionen:

Definition 3.5.4 (Polynomielle Obstruktion)**.**
Eine *polynomielle Obstruktion* für ein Orbitabschlussproblem

$$f \overset{?}{\in} \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g}, \qquad f, g \in \mathbb{C}[X_1, \ldots, X_n]_d \cong \mathbb{C}^N,$$

ist ein Polynom $F \in \mathbb{C}[T_1, \ldots, T_N]$ mit $F(\mathrm{GL}_n(\mathbb{C}) \triangleright g) = \{0\}$ und $F(f) \neq 0$. ⌟

Beispiel 3.5.5 ($\mathrm{WRank}(f) \leq 1$)**.**
Eine quadratische Form in zwei Variablen

$$f(X, Y) = a_2X^2 + a_1XY + a_0Y^2 \in \mathbb{C}[X, Y]_2$$

hat genau dann Waringrang 1, wenn es sich als Quadrat $f = (\alpha X + \beta Y)^2$ schreiben lässt ($\alpha, \beta \in \mathbb{C}$). Dies ist nach Dehomogenisieren äquivalent zu

$$f(X, 1) = a_2X^2 + a_1X + a_0 = (\alpha X + \beta)^d.$$

Dies ist also genau dann der Fall, wenn das quadratische Polynom $f(X, 1)$ eine *doppelte* Nullstelle hat. Dies ist genau dann der Fall, wenn die Diskrimiante

$$\Delta(a_0, a_1, a_2) = a_1^2 - 4a_0a_2$$

verschwindet (vergleiche mit der Lösungsformel für quadratische Gleichungen). Somit können wir hier explizit ein Polynom angeben, welches die Orbitmenge ausschneidet:

$$\left\{ f = a_2X^2 + a_1XY + a_0Y^2 \in \mathbb{C}[X, Y]_2 \;\middle|\; \mathrm{WRank}(f) \leq 1 \right\} = \mathcal{V}(\Delta(a_0, a_1, a_2)).$$ ⌟

Wir wenden uns nun wieder der Permanente zu. In Satz 3.3.3 hatten wir den Zusammenhang der determinantiellen Grenzkomplexität mit dem Orbitabschlussproblem dargestellt.

Definition 3.5.6 ($\mathcal{D}et_n$, $\mathcal{P}erm_n^m$)**.**
Für $m, n \in \mathbb{N}$, $n > m$ definieren wir folgende Teilmengen von $\mathbb{C}[X_{11}, \ldots, X_{nn}]_n$

$$\mathcal{D}et_n \coloneqq \overline{\mathrm{GL}_{n^2}(\mathbb{C}) \triangleright \det_n(X_{11}, \ldots, X_{nn})},$$
$$\mathcal{P}erm_n^m \coloneqq \overline{\mathrm{GL}_{n^2}(\mathbb{C}) \triangleright X_{nn}^{n-m} \operatorname{perm}_m(X_{11}, \ldots, X_{mm})}.$$ ⌟

Satz 3.5.7.
$\overline{\mathrm{dc}}(\operatorname{perm}_m) \geq n$ *genau dann, wenn* $\mathcal{P}erm_n^m \not\subseteq \mathcal{D}et_n$.

Beweis. Dies ist lediglich eine Umformulierung von Satz 3.3.3, wenn man beachtet, dass $X_{nn}^{m-n} \operatorname{perm}_m \in \overline{\mathrm{GL}_{n^2} \triangleright \det_n}$ genau dann wenn $\overline{\mathrm{GL}_{n^2} \triangleright X_{nn}^{m-n} \operatorname{perm}_m} \subseteq \overline{\mathrm{GL}_{n^2} \triangleright \det_n}$. □

Wir können uns bei der Suche nach polynomiellen Obstruktionen sogar auf homogene Polynome beschränkten: Ist $f = \lim_{n\to\infty}(A_n \triangleright g) \in \overline{\mathrm{Mat}_N(\mathbb{C}) \triangleright g}$ und $\lambda \in \mathbb{C}$, so ist

$$\lambda \cdot f = \lim_{n\to\infty} \lambda \cdot (A_n \triangleright g) = \lim_{n\to\infty} \left((\sqrt[d]{\lambda} \cdot A_n) \triangleright g \right) \in \overline{\mathrm{Mat}_N(\mathbb{C}) \triangleright g}.$$

Dies zeigt, dass unsere Orbitenabschlüsse sogenannte affine Kegel sind:

Definition 3.5.8 (Koordinatenring, affiner Kegel)**.**
Eine algebraische Menge$V \subseteq \mathbb{C}^N$ ist ein *affiner Kegel*, falls für $x \in V$ und $\lambda \in \mathbb{C}$ auch $\lambda \cdot x \in V$ ist. Dies ist äquivalent dazu, dass $V = \mathcal{V}(S)$ für homogene Polynome $S \subseteq \mathbb{C}[T_1, \ldots, T_N]$. ⌟

In diesem Fall ist $\mathcal{I}(V) = \bigoplus_{d\in\mathbb{N}_0} \mathcal{I}(V)_d$ mit Untervektorräumen $\mathcal{I}(V)_d \subseteq \mathbb{C}[\underline{X}]_d$. Der Koordinatenring hat ebenfalls eine Zerlegung

$$\mathbb{C}[V] = \bigoplus_{d\in\mathbb{N}_0} \mathbb{C}[V]_d = \bigoplus_{d\in\mathbb{N}_0} \mathbb{C}[X_1, \ldots, X_n]_d / \mathcal{I}(V)_d.$$

Kapitel 4

Geometrische Komplexitätstheorie

Geometrische Komplexitätstheorie hat zwei verschiedene Bedeutungen:

- Einerseits das Programm der geometrischen Komplexitätstheorie, wie es von Mulmuley und Sohoni vorgeschlagen und in einer Reihe von Papern ausgearbeitet wurde, hier kurz *GCT-Programm* gennannt.
- Und andererseits allgemein der Einsatz von Geometrie und Darstellungstheorie, um Resultate in der Komplexitätstheorie wie untere Schranken zu finden.

In diesem Kapitel führen wir die darstellungstheoretischen Grundlagen ein, um dann die wichtigsten Ideen des ursprünglichen GCT-Programms nachzuvollziehen. Neben dem Negativresultat, dass das Programm in seiner ursprünglichen Form *nicht* gelingen kann, präsentieren wir einige weitere Resultate der letzten Jahre.

Inhaltlich folgen wir dem Buch von Landsberg [Lan17, Kapitel 6 und 8], sowie der Darstellung im Artikel von Mulmuley [Mul12]. Eine sehr schöne Darstellung findet sich in der Doktorarbeit von Grochow, welche mir beim Einordnen der Themen ebenfalls sehr hilfreich war [Gro12, Kapitel 3].

4.1 Grundlagen der Darstellungstheorie

Es sei in diesem Abschnitt G eine Gruppe, für uns wird der Fall $G = \mathrm{GL}_n(\mathbb{C})$ besonders relevant sein. Die klassische Darstellungstheorie beschäftigt sich mit der Realisierung von G als Untergruppe von Automorphismengruppen wie $\mathrm{GL}_n(\mathbb{C})$. Eine Referenz ist das Buch [FH04].

Definition 4.1.1 (Darstellung, G-lineare Abbildung)**.**
Eine (endlichdimensionale) *Darstellung* $(\rho, \mathbb{V})$ von G ist ein endlichdim. $\mathbb{C}$-Vektorraum $\mathbb{V} \neq \{0\}$ mit einer Gruppenoperation $\rho\colon G \times \mathbb{V} \to \mathbb{V}$, sodass für jedes $g \in G$ die Zuordnung

$$\rho(g, -)\colon \mathbb{V} \to \mathbb{V}, \qquad v \mapsto g \triangleright v$$

eine lineare Abbildung definiert. Eine Isomorphismus von Darstellungen $(\rho, \mathbb{V})$ und $(\pi, \mathbb{W})$ ist ein Vektorraumisomorphismus $f\colon \mathbb{V} \to \mathbb{W}$ mit

$$\pi(g, f(v)) = f(\rho(g, v)) \qquad \forall g \in G,\ v \in \mathbb{V}. \qquad \lrcorner$$

Nach den Axiomen der Gruppenoperation ist

$$\rho(g_1, -) \circ \rho(g_2, -) = \rho(g_1, \rho(g_2, -)) = \rho(g_1 \cdot g_2, -).$$

Für $g_2 = g_1^{-1}$ ist dies die Identität $\rho(1, v) = v$, d. h. die Abbildung ist invertierbar. Die Zuordnung $g \mapsto \rho(g, -)$ definiert also einen Gruppenhomomorphismus $G \to \mathrm{GL}(\mathbb{V})$. Umgekehrt definiert ein Gruppenhomomorphismus $\phi\colon G \to \mathrm{GL}(\mathbb{V})$ eine Darstellung via

$$\rho(g, v) \coloneqq (\phi(g))(v).$$

Diese Konstruktionen sind zueinander invers, die Begriffe Darstellung und Homomorphismus $G \to \mathrm{GL}(\mathbb{V})$ können also synonym verwendet werden.

Beispiel 4.1.2.

- Die Gruppe $\mathcal{S}_n$ operiert auf $\mathbb{C}^n$ durch Permutation der Komponenten:

  $$\sigma \triangleright (x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

  Dies liefert die *reguläre* Darstellung der $\mathcal{S}_n$.
- Die Operation von $\mathrm{GL}_n(\mathbb{C})$ auf $\mathbb{C}^n$ ist die *Standarddarstellung*; sie entspricht dem Identitätshomomorphismus $\mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$. Ein interessanteres Beispiel ist die Darstellung von $\mathrm{GL}_n(\mathbb{C})$ auf $\mathbb{V} = \mathbb{C}[X_1, \ldots, X_n]_d$ aus Lemma 3.2.1.
- Die Determinante selbst ist eine Darstellung; sie ist ein Gruppenhomomorphismus $\det\colon \mathrm{GL}_n(\mathbb{C}) \to (\mathbb{C} \setminus \{0\}, \cdot) \cong \mathrm{GL}_1(\mathbb{C})$. ⌟

Sind $(\rho_1, \mathbb{V}_1), \ldots, (\rho_k, \mathbb{V}_k)$ Darstellungen von G, so wird die direkte Summe $\mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_k$ zu einer Darstellung durch

$$\rho(g, (v_1, \ldots, v_k)) \coloneqq (\rho(g, v_1), \ldots, \rho(g, v_k)).$$

Man kann umgekehrt fragen, ob sich Darstellungen als Summe einfacherer Darstellungen schreiben lassen.

Definition 4.1.3 (G-Invarianz, irreduzibel, (un)zerlegbar)**.**
Es sei $(\rho, \mathbb{V})$ eine Darstellung von G.

(i) Ein Untervektorraum $U \subseteq \mathbb{V}$ heißt *G-invariant*, falls $\rho(g, U) \subseteq U$ für alle $g \in G$. In diesem Fall ist die Einschränkung von ρ auf U wieder eine Darstellung.
(ii) $\mathbb{V}$ heißt *irreduzibel*, falls $\{0\}$ und $\mathbb{V}$ die einzigen G-invarianten Unterräume von $\mathbb{V}$ sind.
(iii) $\mathbb{V}$ heißt *zerlegbar*, falls es G-invariante Unterräume $U_1, U_2 \neq \{0\}$ gibt mit $\mathbb{V} = U \oplus U'$; ansonsten ist $\mathbb{V}$ *unzerlegbar*. ⌟

Beispiel 4.1.4.

- Die Standarddarstellung von $\mathrm{GL}_n(\mathbb{C})$ auf $\mathbb{C}^n$ ist irreduzibel: Es sei $U \neq \{0\}$ ein $\mathrm{GL}_n(\mathbb{C})$-invarianter Unterraum und $0 \neq v \in U$. Zu jedem Vektor $v' \in \mathbb{C}^n \setminus \{0\}$ gibt es eine invertierbare Matrix $A \in \mathrm{GL}_n(\mathbb{C})$ mit $Av = v'$, da U ein invarianter Unterraum ist, folgt $v' \in U$, also $U = \mathbb{C}^n$.
- Die reguläre Darstellung von $\mathcal{S}_n$ auf $\mathbb{C}^n$ besitzt den invarianten Unterraum $U = \{ (x, \ldots, x) \mid x \in \mathbb{C} \}$. Dieser besitzt ein G-invariantes Komplement

  $$U' = \{ (x_1, \ldots, x_n) \mid \textstyle\sum_{i=1}^n x_i = 0 \}.$$

  Somit ist die reguläre Darstellung reduzibel. ⌟

Der Satz von Maschke zeigt allgemein, dass für eine endliche Gruppe G und eine Darstellung $(\rho, \mathbb{V})$ jeder G-invariante Unterraum $U \subseteq \mathbb{V}$ ein G-invariantes Komplement besitzt [FH04, Proposition 1.5]. Wiederholtes Anwenden dieses Resultates zeigt, dass sich jede Darstellung als direkte Summe endlich vieler irreduzibler Darstellungen schreiben lässt.

Für uns ist von Bedeutung, dass es solche Zerlegungen auch für $G = \mathrm{GL}_n(\mathbb{C})$ gibt. Wir notieren $\mathbb{V}^{\oplus a} \coloneqq \bigoplus_{i=1}^a \mathbb{V}$.

Satz 4.1.5 (Satz von Weyl, Lemma von Schur).
Es sei $(\rho, \mathbb{V})$ eine Darstellung von $G = \mathrm{GL}_n(\mathbb{C})$.

(i) *Jeder G-invariante Unterraum $U \subseteq \mathbb{V}$ besitzt ein invariantes Komplement $U \oplus U' = \mathbb{V}$.*
(ii) *Es gibt irreduzible Darstellungen $\mathbb{V}_1, \dots, \mathbb{V}_k$ und $a_1, \dots, a_k \in \mathbb{N}$, sodass wir eine Isomorphie von Darstellungen*

$$\mathbb{V} \cong \mathbb{V}_1^{\oplus a_1} \oplus \cdots \oplus \mathbb{V}_k^{\oplus a_k}$$

haben. Die irreduziblen Darstellungen $\mathbb{V}_i$ sind bis auf Isomorphie eindeutig bestimmt, ebenso die Vielfachheiten $\mathrm{mult}_{\mathbb{V}_i}(\mathbb{V}) \coloneqq a_i \in \mathbb{N}$.

Beweis. [FH04, Theorem 9.19] und [FH04, Proposition 1.8]. □

Da also jede Darstellung von $\mathrm{GL}_n(\mathbb{C})$ sich als Summe irreduzibler Darstellungen schreiben lässt, stellt sich die Frage nach der Klassifikation der irreduziblen Darstellungen.

Satz 4.1.6 (Irreduzible Darstellungen von $\mathrm{GL}_n(\mathbb{C})$).
Jeder Partition

$$\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k) \in \mathbb{N}^k, \qquad r \in \mathbb{N},\ \lambda_1 \geq \cdots \geq \lambda_k \geq 1$$

kann man eine irreduzible Darstellung von $\mathrm{GL}_n(\mathbb{C})$

$$\boldsymbol{\lambda} \ \mapsto\ S_{\boldsymbol{\lambda}}\mathbb{C}^n$$

zuordnen. Diese Abbildung definiert eine Bijektion zwischen der Menge der Partitionen und der Menge der Isomorphieklassen irreduziblen Darstellungen von $\mathrm{GL}_n(\mathbb{C})$.

Beweis. [FH04, Proposition 5.47] oder [Lan17, Theorem 8.7.1.2] □

Ohne auf die Konstruktion genauer einzugehen, seien folgende Beispiele erwähnt:

- $S_{(1)}\mathbb{C}^n$ entspricht der Standarddarstellung,
- $S_{(d)}\mathbb{C}^n$ entspricht der Darstellung auf $\mathbb{C}[X_1, \dots, X_n]_d$,
- $S_{(1,\dots,1)}\mathbb{C}^n$ (n Einträge) enspricht der Determinante.

4.2 Geometrische Obstruktionen

Wir betrachten nun wieder ein Orbitabschluss $V = \overline{\mathrm{GL}_N(\mathbb{C}) \triangleright g} \subseteq \mathbb{V} \coloneqq \mathbb{C}[X_1, \dots, X_n]_d$ für ein homogenes Polynom $g \in \mathbb{V}$. Es sei wieder $\mathbb{C}[\mathbb{V}] = \mathbb{C}[T_1, \dots, T_N]$ der Polynomring auf dem Raum $\mathbb{V} \cong \mathbb{C}^N$.

Lemma 4.2.1 ($\mathcal{I}(V)_\delta$ und $\mathbb{C}[V]_\delta$ sind Darstellungen).
Für jedes $\delta \in \mathbb{N}$ induziert die Operation von $G = \mathrm{GL}_N(\mathbb{C})$ auf $\mathbb{V}$ eine lineare Operation auf den homogenen Komponenten $\mathbb{C}[\underline{T}]_\delta$, $\mathcal{I}(V)_\delta$ und $\mathbb{C}[V]_\delta$.

Beweis. Die Operation von G auf $\mathbb{V}$ war definiert als $(A \triangleright f)(x) = f(A^\mathsf{T} x)$. Ist nun F ein Polynom auf $\mathbb{V}$, so definieren wir wieder $(A \triangleright F)(f) \coloneqq F(A^\mathsf{T} \triangleright f)$. Der Nachweis der Operationseigenschaften funktioniert analog, ebenfalls die Linearität, und dass sich diese Operation auf $\mathbb{C}[T_1, \dots, T_N]_\delta$ einschränkt.

Als nächstes zeigen wir, dass $\mathcal{I}(V)_\delta$ G-invariant ist. Es sei $A \in G$, $F \in \mathcal{I}(V)_\delta$, dann gilt für alle $f \in V$, da V abgeschlossen unter der Operation von G ist,

$$(A \triangleright F)(f) = F(\underbrace{A^\mathsf{T} \triangleright f}_{\in V}) = 0 \quad \Longrightarrow \quad A \triangleright F \in \mathcal{I}(V) \cap \mathbb{C}[\mathbb{V}]_\delta = \mathcal{I}(V)_\delta.$$

Die Operation von G auf $\mathbb{C}[T_1, \ldots, T_N]_\delta$ wird vererbt zu einer Operation auf $\mathbb{C}[V]_\delta = \mathbb{C}[\underline{T}]_\delta/\mathcal{I}_\delta$ durch Definition auf Repräsentanten

$$A \triangleright [F]_\sim := [A \triangleright F]_\sim.$$

Dies ist wohldefiniert: Falls $F_1 \sim F_2$, also $F_1 = F_2 + G$ für, $G \in \mathcal{I}(V)$, $F_1, F_2 \in \mathbb{C}[\underline{T}]$, so gilt

$$A \triangleright F_1 = A \triangleright (F_2 + G) = A \triangleright F_2 + \underbrace{A \triangleright G}_{\in \mathcal{I}(V)} \quad \Longrightarrow \quad A \triangleright F_1 \sim A \triangleright F_2.$$

Somit sind $\mathcal{I}(V)_\delta$ und $\mathbb{C}[V]_\delta$ auf natürliche Weise Darstellungen von G. □

Somit sind $\mathbb{C}[\mathcal{D}et_n]$ und $\mathbb{C}[\mathcal{P}erm_n^m]$ Darstellungen der Gruppe $\mathrm{GL}_{n^2}(\mathbb{C})$. Wir notieren $\mathrm{mult}_{\boldsymbol{\lambda}}$ für die Vielfachheit der irreduziblen Komponente $S_{\boldsymbol{\lambda}}\mathbb{C}^n$ in einer Darstellung von $\mathrm{GL}_n(\mathbb{C})$. Wir haben nun das folgende wesentliche Resultat:

Satz 4.2.2 ($\mathcal{P}erm \subseteq \mathcal{D}et$ impliziert Abschätzung der Vielfachheiten $\mathrm{mult}_{\boldsymbol{\lambda}}$)**.**
Falls für $m, n \in \mathbb{N}$ $\mathcal{P}erm_n^m \subseteq \mathcal{D}et_m$, so ist für $\delta \in \mathbb{N}$ und irreduzible Darstellung $S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2}$ von $\mathrm{GL}_{n^2}(\mathbb{C})$

$$\mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{D}et_n]_\delta \geq \mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{P}erm_n^m]_\delta.$$

Im Beweis nutzen wir folgende Aussage, welche aus dem Lemma von Schur folgt:
Das Bild einer irreduziblen Darstellung $\mathbb{V}_1 \subseteq \mathbb{V}$ unter einer surjektiven Abbildung $\mathbb{V} \twoheadrightarrow \mathbb{W}$ von Darstellungen ist $\{0\}$ oder wieder eine irreduzible Darstellung.

Beweis. Nach der Korrespondenz des Hilbertschen Nullstellensatzes ist

$$\mathcal{P}erm_n^m \subseteq \mathcal{D}et_n \quad \Longleftrightarrow \quad \mathcal{I}(\mathcal{D}et_n) \subseteq \mathcal{I}(\mathcal{P}erm_n^m).$$

Für die homogenen Komponenten bedeutet dies $\mathcal{I}(\mathcal{D}et_n)_\delta \subseteq \mathcal{I}(\mathcal{P}erm_n^m)_\delta$, nach Übergang zum Koordinatenring erhalten wir eine surjektive Abbildung durch Einschränkung

$$\phi\colon \mathbb{C}[\mathcal{D}et_n]_\delta \twoheadrightarrow \mathbb{C}[\mathcal{P}erm_n^m]_\delta, \qquad F + \mathcal{I}(\mathcal{D}et_m) \mapsto F + \mathcal{I}(\mathcal{P}erm_n^m).$$

Nimmt man nun eine Zerlegung in irreduzible Darstellungen

$$\mathbb{C}[\mathcal{D}et_n]_\delta \cong \bigoplus_{\boldsymbol{\lambda}} (S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2})^{\oplus \mathrm{mult}_{\boldsymbol{\lambda}}(\mathbb{C}[\mathcal{D}et_n])}$$

vor, so sind die Bilder dieser irreduziblen Komponenten unter ϕ nach der vorangegangenen Bemerkung $\{0\}$ oder irreduzible Komponenten von $\mathbb{C}[\mathcal{P}erm_n^m]_\delta$ sind.
Wir erhalten also eine Zerlegung in irreduzible Darstellungen von $\mathbb{C}[\mathcal{P}erm_n^m]_\delta$ durch das Weglassen endlich vieler Komponenten von $\mathbb{C}[\mathcal{D}et_n]_\delta$. Für die Vielfachheiten einer beliebigen Komponente $S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2}$ bedeutet dies

$$\mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{D}et_n]_\delta \geq \mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{P}erm_n^m]_\delta.$$ □

Die Kontraposition dieses Resultats ist der Angriffspunkt des GCT-Programms von Mulmuley und Sohoni.

Definition 4.2.3 (Ocurrence Obstruction, Multiplicity Obstruction)**.**
Es seien $m, n \in \mathbb{N}$ mit $m > n$.

(i) Eine Partition $\boldsymbol{\lambda}$, sodass $S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2}$ für ein $\delta \in \mathbb{N}$ als irreduzible Komponente in $\mathbb{C}[\mathcal{P}erm_n^m]_\delta$, aber nicht in $\mathbb{C}[\mathcal{D}et_n]_\delta$ auftaucht, wird *Ocurrence Obstruction* genannt.
(ii) Eine Partition $\boldsymbol{\lambda}$, sodass $\mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{D}et_n]_\delta < \mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{P}erm_n^m]_\delta$ für ein $\delta \in \mathbb{N}$, wird *Multiplicity Obstruction* genannt. ⌟

Dabei sind Ocurrence Obstructions der Spezialfall von Multiplicity Obstructions für

$$\mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{D}et_n]_\delta = 0 < 1 \leq \mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{P}erm_n^m]_\delta.$$

Eine solche Obstruktion $\boldsymbol{\lambda}$ ist also ein *Beweis* für

$$\overline{\mathrm{dc}}(\mathrm{perm}_m) > n.$$

4.3 Das GCT-Programm nach Mulmuley und Sohoni

Die Kernidee der Geometrischen Komplexitätstheorie nach Mulmuley und Sohoni ist die Hypothese, dass es für m (quasi)polyniell in n Ocurrence Obstructions gibt, welche dann untere Schranken für $\overline{dc}(\mathrm{perm}_m)$ beweisen.

Vermutung 4.3.1 (VNP $\not\subseteq$ VQP durch Ocurrence Obstructions)**.**
Ist $n(m) = 2^{O(\log^a(m))}$ *quasipolynomiell in* m*, so gibt es ein* $n \in \mathbb{N}$ *und eine Ocurrence Obstuction für* $n(m)$*,* m*.*
Insbesonder wächst $\mathrm{dc}(\mathrm{perm}_m)$ *nicht quasipolynomiell und* VNP $\not\subseteq$ VQP*.*

Vergleiche [Mul, GCTII - Conjecture 4.2] für die ursprüngliche genaue Formulierung.

Das Programm, Algebraische Geometrie und Darstellungstheorie für die Trennung von VP und VNP zu nutzen, wurde von Mulmuley und Sohoni in einer Reihe von Papern seit 2001 ausgearbeitet. Die Arbeiten, Übersichtsartikel und Vorlesungsskripten zum GCT-Programm werden auf der Homepage von Mulmuley gesammelt [Mul].

Ein zentraler Punkt ist der konzeptuelle „Flip“ für Valiants erweiterte Hypothese:

Existenz von Obstruktionen $\boldsymbol{\lambda}$ für $m(n)$ quasipolynomiell

$\Downarrow$

Nichtexistenz von Schaltkreisen quasipolynomieller Größe für perm_m

Beispiel 4.3.2 (Ein „flip“ in der Berechenbarkeitstheorie)**.**
Dies ist vergleichbar mit dem Beweis der Unentscheidbarkeit des Halteproblems: Es gibt einen Algorithmus A, welche auf Eingabe einer Maschine M, welche behauptet, das Halteproblem zu entscheiden, eine Maschine M' ausgibt, sodass M auf Eingabe M' das falsche Ergebnis produziert.

Existenz des Algorithmus A

$\Downarrow$

Nichtexistenz von Maschinen M, welche das Halteproblem entscheiden.

Dieses Analogie stammt aus [Gro12, Abschnitt 3.4.2] ⌟

Für allgemeine Orbitabschlussprobleme wird nicht erwartet, dass man sie durch Obstructions trennen kann. Die besondere Situation bei der Frage nach det vs. perm ist, dass diese Polynome durch ihre Symmetrien charakterisiert sind:

Definition 4.3.3 (Durch Symmetrien charakterisiert)**.**
Es sei $f \in \mathbb{C}[X_1, \ldots, X_n]_d$ und $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{C})}(f) = \{\, A \in \mathrm{GL}_n(\mathbb{C}) \mid A \triangleright f = f \,\}$ der Stabilisator. Das Polynom f ist *durch seine Symmetrien charakterisiert*, falls für jedes Polynom $g \in \mathbb{C}[\underline{X}]_d$ mit $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{C})}(f) \subseteq \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{C})}(g)$ bereits $g = a \cdot f$ für $a \in \mathbb{C}$ gilt. ⌟

Durch Symmetrien charakterisiert zu sein, bedeutet also in gewissem Sinne, bis auf Skalare eindeutig durch den Stabilisator charakterisiert zu werden. In unserer Situation ist dies der Fall:

Lemma 4.3.4.
$\det_n, \mathrm{perm}_n \in \mathbb{C}[X_{11}, \ldots, X_{nn}]_n$ *sind durch ihre Symmetrien charakteriert.*

Beweis. [Gro12, Proposition 3.4.3] und [Gro12, Proposition 3.4.5]. □

Diese Symmetrien ermöglichen es, den Suchraum für Ocurrence Obtructions weiter einzuschränken, da a prori mehr darstellungstheoretische Werkzeuge zur Verfügung stehen (Satz von Peter-Weyl), dies wird im Buch von Landsberg genauer ausgeführt [Lan17, Abschnitt 8.6].

Die *flip strategy* versucht sich an der Konstruktion von Polynomialzeitalgorithmen für folgende Probleme [Mul, GCT VI], [Mul12, Abschnitt 3]:

Vermutung 4.3.5 (Flip Hypothese)**.**

- FH[Short]: *Falls n polynomiell in m ist, so existiert eine Ocurrence Obstruction $\boldsymbol{\lambda}$, deren Bitlänge polynomiell in m und n ist.*
- FH[Verification]: *Bei Eingabe von $m, n, \boldsymbol{\lambda}$ kann in polynomieller Zeit (in m, n und der Bitlänge von $\boldsymbol{\lambda}$) verifiziert werden, dass $\boldsymbol{\lambda}$ eine Ocurrence Obstruction ist.*
- FH[Discovery and Construction]: *Bei Eingabe von m, n kann die Existenz einer Ocurrence Obstruction in polynomieller Zeit in m und n entschieden werden. Falls eine Obstruktion existiert, kann diese ebenfalls in Polynomialzeit konstruiert werden.*
- FH[Det, Perm]: *Für gegebenes $m, n, \boldsymbol{\lambda}$ kann in polynomieller Zeit (in m, n und der Bitlänge von λ) entschieden werden, ob $S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2}$ eine irreduzible Komponente von $\mathbb{C}[\mathcal{D}et_n]$ bzw. $\mathbb{C}[\mathcal{D}et_n^m]$ ist.*

Bürgisser, Ikenmeyer und Panova haben allerdings 2016 gezeigt, dass schon Hypothese 4.3.1 *falsch* ist!

Satz 4.3.6 („No ocurrence obstructions exists“)**.**
Für $n, m, \delta \in \mathbb{N}$ mit $n \geq m^{25}$ taucht jede irreduzible Komponente $S_{\boldsymbol{\lambda}}\mathbb{C}^{n^2}$ von $\mathbb{C}[\mathcal{P}erm_n^m]_\delta$ auch in $\mathbb{C}[\mathcal{D}et_n]_\delta$ auf.

Beweis. [BIP16], der Beweis wird auch im Buch von Landsberg vorgestellt [Lan17, Abschnitt 8.10]. □

Die Existenz von Multiplicity Obstructions wird durch dieses Resultat allerdings nicht ausgeschlossen.

4.4 Einige Resultate

Es stellt sich die Frage, ob der Ansatz über die Vielfachheit von irreduziblen Darstellungen überhaupt geeignet ist, untere Schranken zu zeigen. Als „proof-of-concept“ haben Dörfler, Ikenmeyer und Panova gezeigt, dass es Orbitabschlussprobleme gibt, welche sich durch Multiplicity Obstructions, aber nicht durch Ocurrence Obstructions trennen lassen.

Satz 4.4.1.
Betrachte folgende affinen Varietäten $\mathbb{C}[X_1, \ldots, X_m]_n$ definiert als Orbitabschlüsse

$$\mathcal{C}h_m^n := \overline{\mathrm{Mat}_m(\mathbb{C}) \triangleright (X_1 \cdots X_n)}$$
$$\mathcal{P}ow_{m,k}^n := \overline{\mathrm{Mat}_m(\mathbb{C}) \triangleright (X_1^n + \cdots + X_k^n)}.$$

Für $m \geq 3$, $n \geq 2$, $k = \delta = n + 1$ und $\boldsymbol{\lambda} = (n^2 - 2, n, 2)$ ist

$$\mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{C}h_m^n]_\delta < \mathrm{mult}_{\boldsymbol{\lambda}} \mathbb{C}[\mathcal{P}ow_{m,k}^n]_\delta,$$

es liegt also eine Multiplicity Obstruction vor, welche $\mathcal{P}ow_{m,k}^n \not\subseteq \mathcal{C}h_m^n$ zeigt.

Beweis. [DIP19, Theorem 2.1]. □

Für konkrete Werte von m, n, δ, k wurde zudem gezeigt, dass eine Trennung durch Multiplicity Obstructions möglich ist, obwohl keine Ocurrence Obstructions vorliegen.

Was konkrete untere Schranken für die determinantielle Komplexität angeht, ist man noch weit von nicht-polynomiellen Schranken entfernt. Die bislang beste Schranke wurde von Mignon und Ressayre 2004 bewiesen:

Satz 4.4.2 (Untere Schranken für $\mathrm{dc}(\mathrm{perm}_n)$)**.**
Für alle $n \in \mathbb{N}$ *ist* $\mathrm{dc}(\mathrm{perm}_n) \geq \frac{1}{2}n^2$.

Beweis. [Lan17, Theorem 6.4.6.4]. □

Dieses Resultat wurde 2013 von Landsberg, Manivel und Ressayre auf die Grenzkomplexität ausgeweitet:

Satz 4.4.3 (Untere Schranken für $\overline{\mathrm{dc}}(\mathrm{perm}_n)$)**.**
Für alle $n \in \mathbb{N}$ *ist* $\overline{\mathrm{dc}}(\mathrm{perm}_n) \geq \frac{1}{2}n^2$.

Beweis. [Lan17, Theorem 6.5.2.3]. □

Ein anderer Ansatz von Landsberg und Ressayre fragt, ob man leichter untere Schranken für $\mathrm{dc}(\mathrm{perm}_n)$ erhält, wenn man fordert, dass die affinen Projektionen $\mathrm{perm}_n(\underline{X}) = \det_m(A(\underline{X}))$ selbst einen gewissen Grad an Symmetrie aufweisen.

Dazu wird für eine affinen Projektion A definiert, wann sie eine äquivariante determinantielle Darstellung ist, die *äquivarianten determinantiellen Komplexität* $\mathrm{edc}(f)$ ist dann wieder das kleinste r, sodass f eine äquivariante determinantielle Darstellung der Größe $r \times r$ besitzt. Die genaue Definition wird in der Arbeit [LR17] gegeben.

Für diese restriktive Art der affinen Projektion konnte nun die Komplexität der Permanente bestimmt werden:

Satz 4.4.4.
$\mathrm{edc}(\mathrm{perm}_m) = \binom{2m}{m} - 1 \sim 4^m$.

Beweis. [LR17, Theorem 2.1], dies wird auch im Buch von Landsberg dargestellt [Lan17, Abschnitt 8.11]. □

Literatur

[AB09] Sanjeev Arora und Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge: Cambridge University Press, 2009. ISBN: 9780521424264. DOI: 10.1017/CBO9780511804090.

[Abd97] Jounaidi Abdeljaoued. „The Berkowitz Algorithm, Maple and Computing the Characteristic Polynomial in an Arbitrary Commutative Ring“. In: *MapleTech* Vol. 4, No. 3 (1997).

[BI18] Markus Bläser und Christian Ikenmeyer. *Introduction to geometric complexity theory*. 2018.

[BIP16] Peter Bürgisser, Christian Ikenmeyer und Greta Panova. „No occurrence obstructions in geometric complexity theory“. In: *Journal of the American Mathematical Society* 32 (Apr. 2016). DOI: 10.1090/jams/908.

[Bür00] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. en. Algorithms and Computation in Mathematics. Berlin Heidelberg: Springer-Verlag, 2000. ISBN: 9783540667520. DOI: 10.1007/978-3-662-04179-6.

[CCG12] Enrico Carlini, Maria Virginia Catalisano und Anthony V. Geramita. „The solution to the Waring problem for monomials and the sum of coprime monomials“. In: *Journal of Algebra* 370 (2012), S. 5–14. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2012.07.028.

[DIP19] Julian Dörfler, Christian Ikenmeyer und Greta Panova. „On Geometric Complexity Theory: Multiplicity Obstructions Are Stronger Than Occurrence Obstructions“. In: *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*. Bd. 132. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019. ISBN: 9783959771092. DOI: 10.4230/LIPIcs.ICALP.2019.51.

[FH04] William Fulton und Joe Harris. *Representation Theory: A First Course*. en. Readings in Mathematics. New York: Springer-Verlag, 2004. ISBN: 9780387975276. DOI: 10.1007/978-1-4612-0979-9.

[For17] Otto Forster. *Analysis 2: Differentialrechnung im $\mathbb{R}^n$, gewöhnliche Differentialgleichungen*. de. 11. Aufl. Grundkurs Mathematik. Springer Spektrum, 2017. ISBN: 9783658194109. DOI: 10.1007/978-3-658-19411-6.

[Gro12] Joshua A. Grochow. „Symmetry and equivalence relations in classical and geometric complexity theory“. Diss. Chicago, IL: University of Chicago, 2012.

[Hul12] Klaus Hulek. *Elementare Algebraische Geometrie: Grundlegende Begriffe und Techniken mit zahlreichen Beispielen und Anwendungen*. de. 2. Aufl. Aufbaukurs Mathematik. Vieweg+Teubner Verlag, 2012. ISBN: 9783834819642. DOI: 10.1007/978-3-8348-2348-9.

[Ike12] Christian Ikenmeyer. „Geometric complexity theory, tensor rank, and Littlewood-Richardson coefficients“. de. Diss. Universität Paderborn, 2012.

[Kra84] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. de. Aspects of Mathematics. Vieweg+Teubner Verlag, 1984. ISBN: 9783528085254. DOI: 10.1007/978-3-322-83813-1.

[Lan02] Serge Lang. *Algebra*. en. 3. Aufl. Graduate Texts in Mathematics. New York: Springer-Verlag, 2002. ISBN: 9780387953854. DOI: 10.1007/978-1-4613-0041-0.

[Lan17] Joseph M. Landsberg. *Geometry and Complexity Theory*. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 2017. ISBN: 9781107199231. DOI: 10.1017/9781108183192.

[LR17] J. M. Landsberg und Nicolas Ressayre. „Permanent v. determinant: An exponential lower bound assuming symmetry and a potential path towards Valiant's conjecture". en. In: *Differential Geometry and its Applications*. Geometry and complexity theory 55 (Dez. 2017), S. 146–166. ISSN: 0926-2245. DOI: 10.1016/j.difgeo.2017.03.017.

[MP08] Guillaume Malod und Natacha Portier. „Characterizing Valiant's algebraic complexity classes". In: *Journal of Complexity* 24.1 (2008). Computational Algebraic Geometry Workshop, S. 16–38. ISSN: 0885-064X. DOI: https://doi.org/10.1016/j.jco.2006.09.006.

[Mul] Ketan Mulmuley. *GCT publications*. http://ramakrishnadas.cs.uchicago.edu/.

[Mul12] Ketan D. Mulmuley. „The GCT Program toward the P vs. NP Problem". In: *Commun. ACM* 55.6 (Juni 2012), S. 98–107. ISSN: 0001-0782. DOI: 10.1145/2184319.2184341.

[Val79] Leslie G. Valiant. „Completeness Classes in Algebra". In: *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*. STOC '79. Atlanta, Georgia, USA: Association for Computing Machinery, 1979, S. 249–261. ISBN: 9781450374385. DOI: 10.1145/800135.804419.

[Vol99] Heribert Vollmer. *Introduction to Circuit Complexity: A Uniform Approach*. en. Texts in Theoretical Computer Science. An EATCS Series. Berlin Heidelberg: Springer-Verlag, 1999. ISBN: 9783540643104. DOI: 10.1007/978-3-662-03927-4.

Erklärung der Selbstständigkeit

Hiermit versichere ich, die vorliegende Bachelorarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet zu haben. Die Arbeit hat in gleicher oder ähnlicher Form noch keinem anderen Prüfungsamt vorgelegen.

Ort, Datum	Unterschrift