

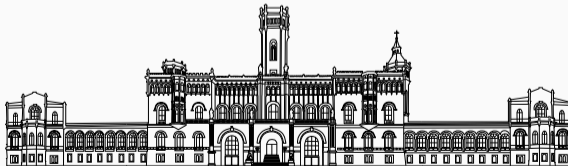


Geometrische Komplexitätstheorie

Vortrag zur Bachelorarbeit

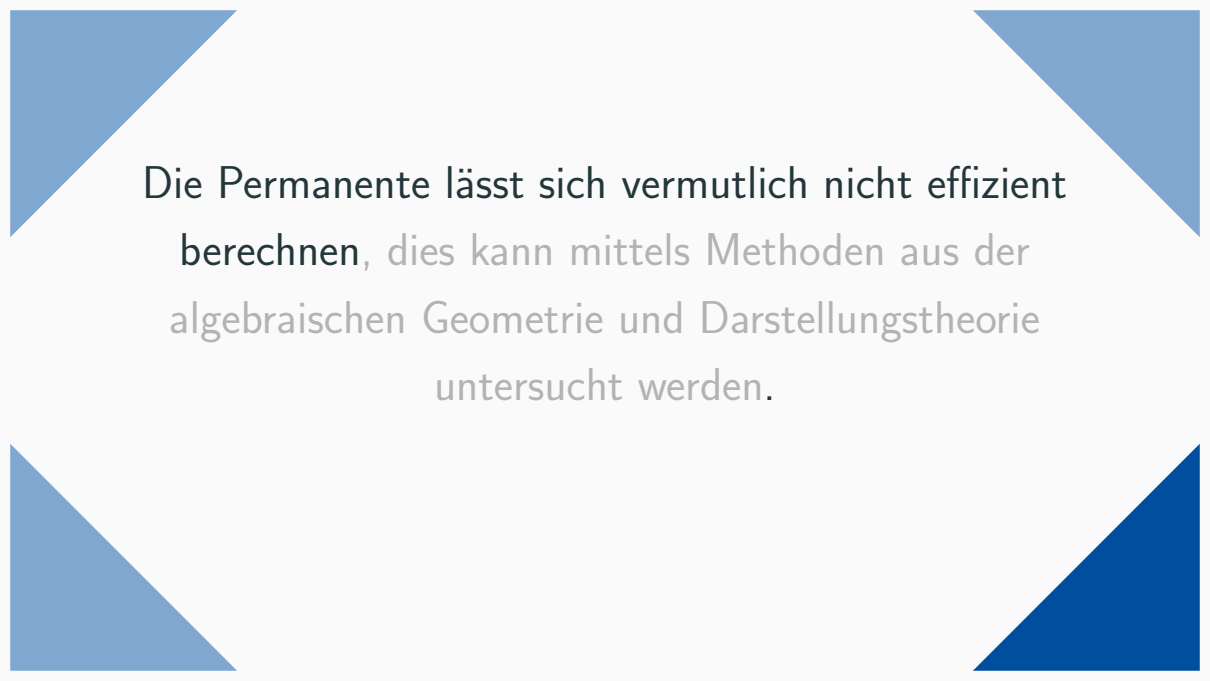
Leo Kayser

Institut für Theoretische Informatik



In einem Satz

Die Permanente lässt sich vermutlich nicht effizient berechnen, dies kann mittels Methoden aus der algebraischen Geometrie und Darstellungstheorie untersucht werden.

The slide features four blue triangles in the corners: a light blue triangle in the top-left, a medium blue triangle in the top-right, a light blue triangle in the bottom-left, and a dark blue triangle in the bottom-right. The text is centered in the white space between them.

Die Permanente lässt sich vermutlich nicht effizient berechnen, dies kann mittels Methoden aus der algebraischen Geometrie und Darstellungstheorie untersucht werden.

Polynome

Es sei K ein Körper und $\{X_1, \dots, X_n\}$ eine Menge von Variablen.

- Ein *Multiindex* ist ein Tupel $\mathbf{k} = (k_1, \dots, k_n) \in \mathbb{N}_0^n$. Kurzschreibweisen:

$$|\mathbf{k}| := k_1 + \dots + k_n, \quad \mathbf{k} + \mathbf{l} = (k_1 + l_1, \dots, k_n + l_n), \quad X^{\mathbf{k}} := X_1^{k_1} \dots X_n^{k_n}.$$

- Ein Ausdruck der Form $X^{\mathbf{k}}$ heißt *Monom* vom Grad $|\mathbf{k}|$.
- Ein *Polynom* ist eine endliche K -Linearkombination von Monomen

$$f(X_1, \dots, X_n) = \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} X^{\mathbf{k}}, \quad a_{\mathbf{k}} \in K.$$

- Addition und Multiplikation „wie gewohnt“, etwa

$$\left(\sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} X^{\mathbf{k}} \right) \cdot \left(\sum_{|\mathbf{l}| \leq d'} b_{\mathbf{l}} X^{\mathbf{l}} \right) = \sum_{|\mathbf{k}| \leq d} \sum_{|\mathbf{l}| \leq d'} (a_{\mathbf{m}} b_{\mathbf{l}}) X^{\mathbf{k} + \mathbf{l}}.$$

Der Ring der Polynome

↷ Polynomring über K in n Variablen $K[\underline{X}] = K[X_1, \dots, X_n]$.

- Für ein Polynom $f \neq 0$ definiert man den Grad durch

$$\deg \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} X^{\mathbf{k}} = \max\{|\mathbf{k}| \mid a_{\mathbf{k}} \neq 0\}, \quad \deg(0) = -\infty.$$

- Ein Polynom ist *homogen* vom Grad $d \in \mathbb{N}_0$, wenn alle vorkommenden Monome Grad d haben.
- Teilräume der Polynome von beschränktem Grad

$$K[\underline{X}]_{\leq d} := \{f \in K[\underline{X}] \mid \deg f \leq d\}$$

$$K[\underline{X}]_d := \{0\} \cup \{f \in K[\underline{X}] \mid f \text{ homogen, } \deg f = d\}.$$

Beispiele für Polynome

- (Affin-)lineare Polynome $a_0 + a_1X_1 + \dots + a_nX_n \in K[X_1, \dots, X_n]_{\leq 1}$
- *Determinante* einer Matrix $A = (X_{ij})_{i,j=1}^n \in \text{Mat}_n(K)$

$$\det_n(X_{11}, \dots, X_{nn}) = \sum_{\sigma \in \mathcal{S}_n} \text{sign}(\sigma) \cdot X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in K[X_{11}, \dots, X_{nn}]$$

- *Permanente* einer Matrix $A = (X_{ij})_{i,j=1}^n \in \text{Mat}_n(K)$

$$\text{perm}_n(X_{11}, \dots, X_{nn}) = \sum_{\sigma \in \mathcal{S}_n} X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in K[X_{11}, \dots, X_{nn}]$$

Gesucht: Ein Berechnungsmodell für Polynomfunktionen $K^n \rightarrow K$

$$(x_1, \dots, x_n) \mapsto \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} x_1^{k_1} \cdots x_n^{k_n}.$$

Arithmetische Schaltkreise

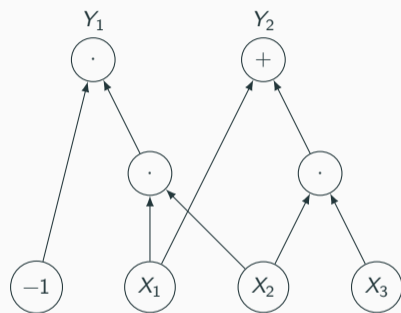


Abbildung. Darstellung eines arithmetischen Schaltkreises.

Ein *arithmetischer Schaltkreis* $C = (G, \beta, \omega)$ mit n Eingängen und m Ausgängen besteht aus

- einem gerichtet azyklischen Graph $G = (V, E)$,
- einer Zuordnung $\beta: V \rightarrow K \cup \{X_1, \dots, X_n, +, \cdot\}$, welche die Knoten als *Eingabegatter* bzw. *Berechnungsgatter* kennzeichnet,
- einer Zuordnung $\omega: V \rightarrow \{*\} \cup \{Y_1, \dots, Y_m\}$, welche die Knoten mit $\deg_{\text{out}}(v) = 0$ bijektiv den *Ausgabevariablen* zuweist.

Ein Schaltkreis berechnet komponentenweise ein Polynomfunktion $f: K^n \rightarrow K^m$.

Die Schaltkreiskomplexität eines Polynoms

- Die *Größe* $\text{size}(C)$ eines arithmetischen Schaltkreises ist die Anzahl der Berechnungsgatter.
- Die *Schaltkreiskomplexität* eines Polynoms $f \in K[X_1, \dots, X_n]$ ist

$$L(f) = \min \{ \text{size}(C) \mid C \text{ ist arith. Schaltkreis und berechnet } f \}$$

- Eine *p-Familie* ist eine Folge von Polynomen $(f_n)_{n \in \mathbb{N}}$, sodass Grad und Anzahl der Variablen $f_n \in K[X_1, \dots, X_{p(n)}]_{\leq q(n)}$ polynomiell beschränkt sind.
- Beispiel: $(\det_n)_n$ und $(\text{perm}_n)_n$ sind p-Familien

↪ Ordne p-Familien nach dem *Wachstum* ihrer Schaltkreiskomplexität in Klassen ein.

Die Klassen VP und VNP

Definition 1: (VP, VNP)

Es sei $f_n \in K[X_1, \dots, X_{p(n)}]_{\leq q(n)}$ eine p -Familie.

- $(f_n)_n \in \text{VP}$, falls $L(f_n)$ polynomiell beschränkt ist ($L(f_n) \in O(n^c)$, $c \in \mathbb{N}$).
- $(f_n)_n \in \text{VNP}$, falls es eine p -Familie $\tilde{f}_n \in K[X_1, \dots, X_{p(n)}, Y_1, \dots, Y_{p'(n)}]$ gibt, sodass $(\tilde{f}_n)_n \in \text{VP}$ und für alle $n \in \mathbb{N}$ gilt

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

- $\text{VP} \subseteq \text{VNP}$ (wähle $\tilde{f}_n = f_n$)
- $(\text{perm}_n)_n \in \text{VNP}$ und $(\text{det}_n)_n \in \text{VP}$

Valiants Hypothese

Ein zentrales offenes Problem der algebraischen Komplexitätstheorie ist *Valiants Hypothese*:

$$VP \stackrel{?}{\neq} VNP$$

Zusammenhang zu P vs. NP?

Satz 2: ([Bür00, Corollary 4.6])

Angenommen $VP = VNP$ über einem Körper K , sodass entweder

- (i) K ein endlicher Körper ist, oder
- (ii) $\mathbb{Q} \subseteq K$ und die verallgemeinerte Riemann-Hypothese wahr ist.

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

Projektionen und Vollständigkeit

- $f \in K[X_1, \dots, X_n]$ ist eine *Projektion* von $g \in K[X_1, \dots, X_m]$, falls es $a_1, \dots, a_m \in \{X_1, \dots, X_n\} \cup K$ gibt mit

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

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

- Sind $(f_n)_n, (g_n)_n$ p-Familien, so schreiben wir $(f_n)_n \leq_p (g_n)_n$, falls es eine polynomiell beschränkte Funktion $t: \mathbb{N} \rightarrow \mathbb{N}$ gibt mit $f_n \leq g_{t(n)}$ für alle $n \in \mathbb{N}$.
- Eine p-Familie $(g_n)_n$ heißt *vollständig* für eine Klasse von p-Familien \mathcal{C} , falls $(g_n)_n \in \mathcal{C}$ und $(f_n)_n \leq_p (g_n)_n$ für alle $(g_n)_n \in \mathcal{C}$.

Die Vollständigkeit der Permanente

Es sei nun K ein Körper der Charakteristik $\text{char}(K) \neq 2$, d.h. $1 + 1 \neq 0$ in K .

Satz 3

$(\text{perm}_n)_n$ ist vollständig für VNP.

Valiants Hypothese ist äquivalent zur Aussage

$$(\text{perm}_n) \notin \text{VP}.$$

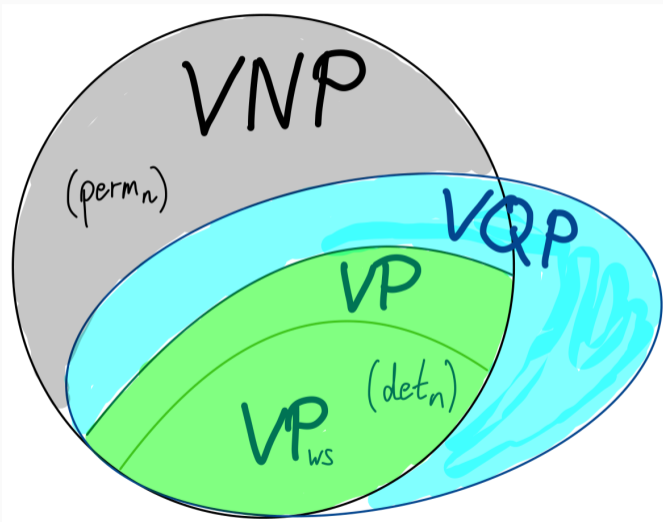
Die Vollständigkeit der Determinante

- Ein algebraischer Schaltkreis C heißt *schwach-schief*, falls für jedes Multiplikationsgatter v das Entfernen eines der beiden eingehenden Kanten den Graphen unzusammenhängend werden lässt.
- $L_{ws}(f) = \min \{ \text{size}(C) \mid C \text{ ist schwach-schiefer Schaltkreis und berechnet } f \}$.
- $(f_n)_n \in \text{VP}_{ws}$, falls $L_{ws}(f_n) \in O(n^c)$.
- $(f_n)_n \in \text{VQP}$, falls $L(f_n) \in 2^{O(\log^c(n))}$ (*quasipolynomielles Wachstum*).

Satz 4

- $(\det_n)_n$ ist vollständig für VP_{ws} .
- $(\det_n)_n$ ist vollständig für VQP unter Projektionen quasipolynomieller Wachstumsordnung ($f_n \leq \det_{t(n)}$, t quasipolynomiell).

Ein Überblick

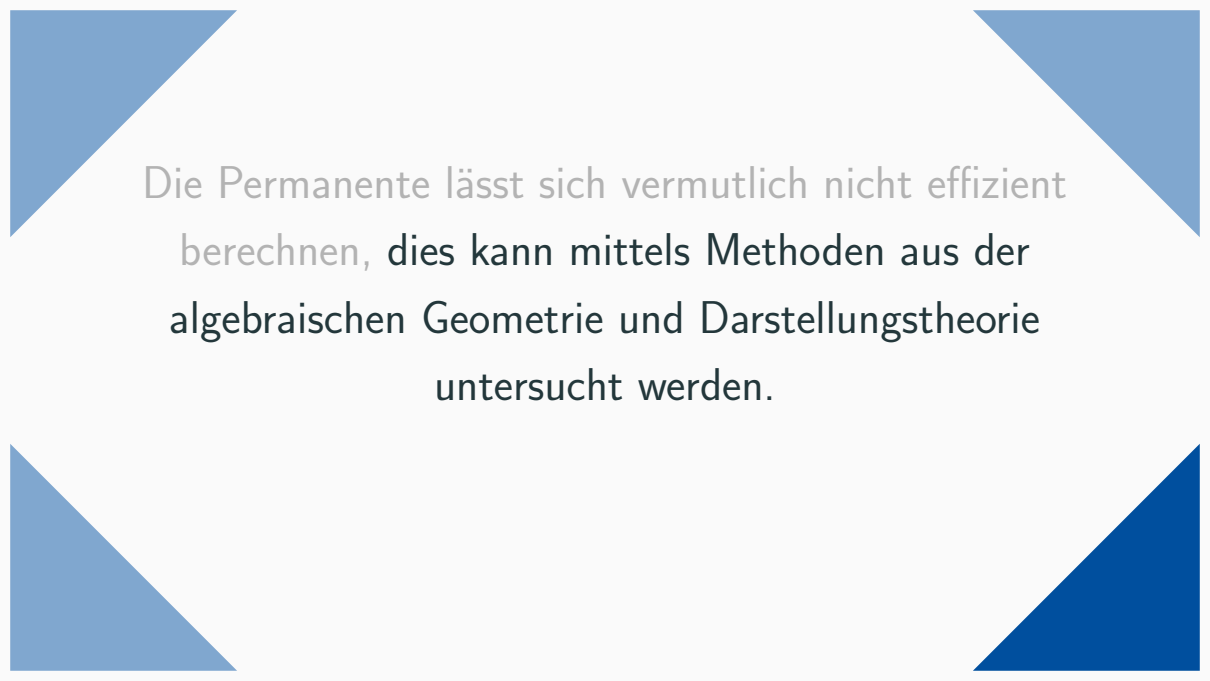


Valiants Hypothese:

$$VP \neq VNP$$

Valiants erweiterte Hypothese:

$$VNP \not\subseteq VQP$$

The slide features four blue triangles in the corners: a light blue triangle in the top-left, a medium blue triangle in the top-right, a light blue triangle in the bottom-left, and a dark blue triangle in the bottom-right. The text is centered in the white space between them.

Die Permanente lässt sich vermutlich nicht effizient berechnen, dies kann mittels Methoden aus der algebraischen Geometrie und Darstellungstheorie untersucht werden.

Determinantielle Komplexität

Ab jetzt sei der Grundkörper stets $K = \mathbb{C}$.

Die *determinantielle Komplexität* $dc(f)$ von $f \in \mathbb{C}[X_1, \dots, X_n]$ ist das kleinste $r \in \mathbb{N}$, sodass es lineare Polynome $l_{ij}(X_1, \dots, X_n) \in \mathbb{C}[\underline{X}]_{\leq 1}$ ($1 \leq i, j \leq r$) gibt mit

$$f(\underline{X}) = \det_r \begin{pmatrix} l_{11}(\underline{X}) & \dots & l_{1r}(\underline{X}) \\ \vdots & \ddots & \vdots \\ l_{r1}(\underline{X}) & \dots & l_{rr}(\underline{X}) \end{pmatrix}.$$

Lemma 5

- $(f_n)_n \in \text{VP}_{ws}$ genau dann, wenn $dc(f_n)$ polynomiell beschränkt wächst.
- $(f_n)_n \in \text{VQP}$ genau dann, wenn $dc(f_n)$ quasipolynomiell beschränkt wächst.

Valiants erweiterte Hypothese: $dc(\text{perm}_n)$ wächst nicht quasipolynomiell.

Die Operation von $\text{Mat}_n(\mathbb{C})$ auf $\mathbb{C}[X_1, \dots, X_n]_d$

- Für ein Polynom $f \in \mathbb{C}[X]$ und eine Matrix $B = (b_{ij}) \in \text{Mat}_n(\mathbb{C})$ definiere $B \triangleright f \in \mathbb{C}[X]$ für $x = (x_1, \dots, x_n)^T$

$$(A \triangleright f)(x) = f(B^T x) = f(b_{11}x_1 + \dots + b_{n1}x_n, \dots, b_{1n}x_1 + \dots + b_{nn}x_n).$$

- \triangleright erfüllt die Eigenschaften einer *Monoidoperation*:

$$I_n \triangleright f = f, \quad (B \cdot C) \triangleright f = (B \triangleright f) \cdot (C \triangleright f)$$

- Ist f homogen, so auch $B \triangleright f$, die Operation lässt sich auf $\mathbb{C}[X]_d$ einschränken.
- Die *Bahn* von f ist die Menge $\text{Mat}_n(\mathbb{C}) \triangleright f := \{ B \triangleright f \mid B \in \text{Mat}_n(\mathbb{C}) \} \subseteq \mathbb{C}[X]$.

Beobachtung: $\{ f \in \mathbb{C}[X_{11}, \dots, X_{nn}]_n \mid \text{dc}(f) \leq n \} = \text{Mat}_n(\mathbb{C}) \triangleright \det_n$.

Das Padding der Permanente

Problem: perm_n und det_r haben für $r > n$ unterschiedlichen Grad.

- Ist $f = \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} X^{\mathbf{k}} \in \mathbb{C}[X_1, \dots, X_n]$, $d = \deg(f)$, so ist die *Homogenisierung*

$$\tilde{f}(X_1, \dots, X_n, Y) = \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} X^{\mathbf{k}} Y^{d-|\mathbf{k}|} \in \mathbb{C}[X_1, \dots, X_n, Y]_d.$$

- Ist $f = \text{det}_r(\ell_{11}(\underline{X}), \dots, \ell_{rr}(\underline{X}))$ mit $\ell_{ij}(\underline{X}) = a_{ij}^{(0)} + \sum_{k=1}^n a_{ij}^{(k)} X_k$, so ist

$$Y^{r-d} \tilde{f}(\underline{X}, Y) = \text{det}_n(a_{11}^{(0)} Y + \sum_{k=1}^n a_{11}^{(k)} X_k, \dots, a_{rr}^{(0)} Y + \sum_{k=1}^n a_{rr}^{(k)} X_k).$$

Lemma 6 Für $n > m$ haben wir die Äquivalenz

$$\text{dc}(\text{perm}_m) \leq n \iff X_{nn}^{n-m} \text{perm}_m \in \text{Mat}_n(\mathbb{C}) \triangleright \text{det}_n.$$

Grenzkomplexität

Von nun an sei $\mathbb{V} := \mathbb{C}[X_1, \dots, X_n]_d \cong \mathbb{C}^N$.

- Wir können über Abgeschlossenheit, Folgenkonvergenz, ... in \mathbb{V} sprechen.
- Möglicherweise gilt zwar $f \notin X = \text{Mat}_n(\mathbb{C}) \triangleright \det_n$, aber eine Folge von Polynomen aus X konvergiert gegen f , d.h. $f \in \overline{X}$ (Abschluss).
- Die determinantielle *Grenzkomplexität* $\overline{\text{dc}}(f)$ ist das kleinste r , sodass f Grenzwert einer Folge $(f_j)_{j \in \mathbb{N}} \in \mathbb{V}$ mit $\text{dc}(f_j) \leq r$ ist.
- *Noch stärkere Vermutung*: $\overline{\text{dc}}(\text{perm}_n)$ wächst nicht quasipolynomiell, also

$$X_{nn}^{n-m} \text{perm}_m \notin \mathcal{DET}_n := \overline{\text{Mat}_n(\mathbb{C}) \triangleright \det_n}$$

für $n = n(m)$ quasipolynomiell und $m \gg 0$.

- Mit der Notation $\mathcal{PERM}_n^m := \overline{\text{Mat}_n(\mathbb{C}) \triangleright X_{nn}^{n-m} \text{perm}_m}$ äquivalent zu

$$\mathcal{PERM}_n^m \not\subseteq \mathcal{DET}_n.$$

Polynomielle Obstruktionen

Eine Teilmenge $V \subseteq \mathbb{C}^N$ ist *algebraisch*, falls es Polynome $F_1, \dots, F_k \in \mathbb{C}[T_1, \dots, T_N]$ gibt, sodass $V = \{ x \in \mathbb{C}^N \mid F_1(x) = \dots = F_k(x) = 0 \}$.

Lemma 7: Der Abschluss unserer Bahnen ist algebraisch

$\overline{\text{Mat}_n(\mathbb{C}) \triangleright f} \subseteq \mathbb{V} \cong \mathbb{C}^N$ ist eine algebraische Menge. Insbesondere trifft dies auf \mathcal{DET}_n und \mathcal{PERM}_n^m zu.

Satz 8: (Polynomielle Obstruktionen zeigen untere Schranken)

Es sei $\mathcal{DET}_n = \{ x \in \mathbb{C}^N \mid F_1(x) = \dots = F_k(x) = 0 \}$, $x \hat{=} X_{nn}^{n-m} \text{perm}_m \in \mathbb{C}^N$.
Dann ist $\overline{\text{dc}(\text{perm}_m)} > n$ genau dann wenn $F_j(x) \neq 0$ für ein $j = 1, \dots, k$.

Exkurs: Darstellungstheorie

Es sei $G = \mathrm{GL}_n(\mathbb{C})$.

- Eine *Darstellung* von G ist ein endl. dim. Vektorraum \mathbb{W} und eine Operation $\triangleright: G \times \mathbb{W} \rightarrow \mathbb{W}$, sodass $w \mapsto A \triangleright w$ eine \mathbb{C} -lineare Abbildung für alle $A \in G$ ist.
- Beispiele: Matrixmultiplikation operiert auf \mathbb{C}^n , vorige Operation auf $\mathbb{C}[X_1, \dots, X_n]_d$.
- Ein Unterraum $U \subset \mathbb{W}$ ist *G-invariant*, falls sich die Operation auf U einschränken lässt. Dann existiert ein G -invariantes Komplement $U \oplus U' = \mathbb{W}$.
- Falls es einen G -invarianten Unterraum $0 \neq U \subsetneq \mathbb{W}$ gibt, heißt die Darstellung *reduzibel*, andernfalls *irreduzibel*.
- Jede Darstellung lässt sich als direkte Summe irreduzibler Darstellungen schreiben:

$$\mathbb{W} \cong \mathbb{W}_1^{\oplus a_1} \oplus \dots \oplus \mathbb{W}_k^{\oplus a_k},$$

die \mathbb{W}_i sind bis auf Isomorphie eindeutig bestimmt, a_i ist die *Vielfachheit* von \mathbb{W}_i . 17

Geometrische Obstruktionen

$f \in \mathbb{V} = \mathbb{C}[X_1, \dots, X_n]_d$, $V = \overline{\text{Mat}_n(\mathbb{C}) \triangleright f}$.

- Sei $\mathbb{C}[V] := \mathbb{C}[T_1, \dots, T_N] / \sim_V$ der *Koordinatenring*, wobei $F \sim_V G \Leftrightarrow F|_V = G|_V$.
- Für $\delta \in \mathbb{N}_0$ sei $\mathbb{C}[V]_\delta = \mathbb{C}[T_1, \dots, T_N]_\delta / \sim_V$.
- Die Darstellung von G auf $\mathbb{V} = \mathbb{C}[T_1, \dots, T_N]_\delta$ vermöge $(A \triangleright F)(f) = F(A^T \triangleright f)$ lässt sich zu einer Darstellung auf $\mathbb{C}[V]_\delta$ einschränken.
- Für eine irreduzible Darstellung $S_\lambda \mathbb{C}^{n^2}$ sei $\text{mult}_\lambda \mathbb{W}$ die *Vielfachheit* in \mathbb{W} .

Satz 9: (Multiplicity/Ocurrence Obstructions zeigen untere Schranken)

Falls $\mathcal{P}ERM_n^m \subseteq \mathcal{D}ET_n$, so gilt für jede irreduzible Darstellung $S_\lambda \mathbb{C}^{n^2}$

$$\text{mult}_\lambda \mathbb{C}[\mathcal{D}ET_n]_\delta \geq \text{mult}_\lambda \mathbb{C}[\mathcal{P}ERM_n^m]_\delta.$$

Geometrische Komplexitätstheorie nach Mulmuley & Sohoni

- Komplexitätstheoretische Fragen wie $VP \neq VNP$ mittels Geometrischer und Darstellungstheoretischer Methoden beantworten
- Reihe von „GCT papers“ seit 2001
- **Zentrales Ziel:** Ist $n(m) = 2^{O(\log^a(m))}$ quasipolynomiell in m , so gibt es $n \gg 0$, $\delta \in \mathbb{N}$ und eine Occurrence Obstruction für $n(m)$, m , δ liegt vor.
 $\implies VNP \not\subseteq VQP.$
- GCT = „the string theory of computer science“ [Scott Aaronson, $P \stackrel{?}{=} NP$]

Satz 10: (Bürgisser, Ikenmeyer, Panova: *No occurrence obstructions exist*)

Für $n, m, \delta \in \mathbb{N}$ mit $n \geq m^{25}$ taucht jede irreduzible Komponente von $\mathbb{C}[\mathcal{P}ERM_n^m]_\delta$ auch in $\mathbb{C}[\mathcal{D}ET_n]_\delta$ auf.

Positive Resultate

Satz 11: (Dörfler, Ikenmeyer und Panova)

Folgende Orbitabschlüsse in $\mathbb{C}[X_1, \dots, X_m]_n$ lassen sich durch Multiplicity Obstructions trennen, aber nicht immer durch Occurrence Obstructions:

$$\begin{aligned}\mathcal{C}H_m^n &:= \overline{\text{Mat}_m(\mathbb{C}) \triangleright (X_1 \cdots X_n)} \\ \mathcal{P}OW_{m,k}^n &:= \overline{\text{Mat}_m(\mathbb{C}) \triangleright (X_1^n + \cdots + X_k^n)}.\end{aligned}$$

Satz 12: (Bekannte Schranken für die Komplexität der Permanente)

- $\text{dc}(\text{perm}_n) \geq \frac{1}{2}n^2$ (Mignon und Ressayre, 2004)
- $\overline{\text{dc}}(\text{perm}_n) \geq \frac{1}{2}n^2$ (Landsberg, Manivel und Ressayre, 2013)
- $\text{edc}(\text{perm}_n) = \binom{2n}{n} - 1 \sim 4^n$ (Landsberg und Ressayre, 2017)

Auf einen Blick

$VP \neq VNP$ \Leftarrow $VNP \neq VQP$ \Leftrightarrow $dc(\text{perm}) \neq$ ^{quasi-} ~~polynomiell~~
Valiants Hypothese Erweiterte VH. Determinantielle Komplexität

$\exists \lambda$ in $\mathbb{C}[\text{PERM}]$ \Rightarrow $\exists F \in \mathbb{C}[I]:$ $F|_{\text{DET}}=0$ \Leftrightarrow $dc(\text{perm}) \neq$ ^{quasi-} ~~polynomiell~~
nicht in $\mathbb{C}[\text{DET}]$ $F(\text{perm}) \neq 0$ Grenzkomplexität
Occurrence Obstructions polynomielle Obstruktionen

$\exists \lambda$ mit $\uparrow \uparrow$
 $\text{mult}_\lambda \mathbb{C}[\text{DET}] < \text{mult}_\lambda \mathbb{C}[\text{PERM}]$
Multiplicity obstructions

Danke!

Fragen?

Quellenverweise

- [Bür00] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Springer-Verlag, 2000. DOI: [10.1007/978-3-662-04179-6](https://doi.org/10.1007/978-3-662-04179-6).
- [Lan17] Joseph M. Landsberg. *Geometry and Complexity Theory*. Cambridge University Press, 2017. DOI: [10.1017/9781108183192](https://doi.org/10.1017/9781108183192).
- [Mul12] Ketan D. Mulmuley. „The GCT Program toward the P vs. NP Problem“. In: *Communications of the ACM* (2012). DOI: [10.1145/2184319.2184341](https://doi.org/10.1145/2184319.2184341).