Seminararbeit

Arithmetische Komplexität

Polynome & Schaltkreise

Author:
Julian Lorenz
Mtr.: 3383863

Betreuer:
Prof. Dr. Holger Dell

2021 – 03 – 01

Inhaltsverzeichnis

1 Einleitung

Das Thema dieser Ausarbeitung ist die *arithmetische Komplexität*, vorgestellt im Kapitel 12 des Buches *Mathematics & Computation* von Avi Wigderson [4], das sich mit Polynomen und diese berechnende arithmetische Schaltkreise beschäftigt.
Zunächst werden notwendige Definitionen eingeführt, allen voran die Definition und Größe von Schaltkreisen. Im Anschluß werden ein paar für das Thema historisch relevante Beispiele präsentiert, namentlich die Matrix Multiplikation, die Determinante und die Permanente. Der Fokus der Betrachtung liegt hierbei auf oberen und den komplexeren unteren Schranken entsprechender arithmetischer Schaltkreise.
Im Folgenden bezieht sich der Autor auf das Paper *Completness Classes in Algebra* [3] von Leslie Valiant. Dort werden die Komplexitätsklassen $\mathcal{VP}$ und $\mathcal{VNP}$ sowie die (affine) Projektion eingeführt und die bisherigen Beispiele entsprechend eingeordnet.
Abschließend werden kurz verschiedene eingeschränkte Modelle angeschnitten, die stärkere Aussagen und einen Ausblick in aktuelle Forschungsgebiete liefern.

2 Arithmetische Schaltkreise & univariate Polynome

Arithmetische Komplexität beschäftigt sich mit der Berechnung von Polynomen $\mathbb{F}[x_1, x_2, \cdots]$ über beliebigen Körpern $\mathbb{F}$ durch arithmetische Schaltkreise.
Allgemein sind in der Berechnung eines Polynoms stets mehr Informationen enthalten als in der Berechnung der resultierenden Funktion. Beispielweise wird das Polynom $b(x) = x^2 + x$ über $\mathbb{F}_2$ stets zu 0 ausgewertet, entspricht jedoch nicht dem Nullpolynom $n(x) = 0$. Obgleich das Resultat identisch ist enthält die Berechnung von $p(x)$ mehr Informationen als die von $n(x)$. Um jedoch inherente Zusammenhänge dieser Art zu vermeiden werden im Verlauf dieser Ausarbeitung nur Körper mit einer Charakteristik von 0 betrachtet, bei denen im Gegensatz zu Primrestklassenkörpern kein ganzzahliges Vielfaches des multiplikativen neutralen Elements das additive neutrale Element ergibt.

Ein *arithmetischer Schaltkreis* entspricht einem gerichteten kreisfreien Graphen. Knoten mit Eingangsgrad 0 entsprechen der Eingabe und bestehen aus Polynomen.
Alle weiteren Knoten haben einen Eingangsgrad von 2 und sind durch die arithmetischen Operationen + und × gekennzeichnet. Eine spezielle Form von arithmetischen Schaltkreisen sind sogenannte *arithmetische Formeln*, bei denen der Ausgangsgrad jedes Knoten durch 1 begrenzt ist. Der Graph ist in diesem Fall ein Baum, womit das Ergebnis einer arithmetischen Operation nicht mehrfach verwendet werden kann und entsprechend oft separat neu berechnet werden muss.

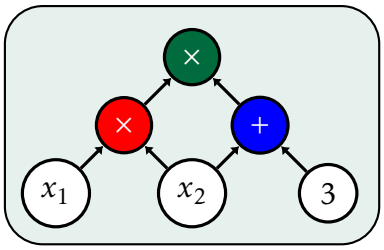

Abbildung 1

Die Komplexitäts eines Schaltkreises ist direkt von dessen *Größe* abhängig, die durch die Anzahl der Kanten bzw Knoten festgelegt ist. Es gelte die folgende Bezeichnung:

Definition. Sei $\mathrm{S}(f)$ die minimale Größe eines arithmetischen Schaltkreises der ein Polynom f berechnet, sowie $\mathrm{L}(f)$ eine entsprechende arithmetische Formel.

Da eine arithmetische Formel immer auch ein Schaltkreis ist, gilt $\mathrm{S}(f) \leq \mathrm{L}(f)$. Ein weiterer relevanter Parameter ist der Grad eines Polynoms, der nach Voraussetzung polynomiell in n

beschränkt sein soll. Im Folgenden werden weitestgehend multilineare Polynome betrachtet, so dass der Grad eines Polynoms durch die Anzahl der Variablen beschränkt ist.
Zunächst ein paar grundlegende Überlegungen bezüglich der Frage nach der Anzahl benötigter Additionen und Multiplikationen, um ein Polynom zu berechnen. Nach *Horner-Schema* lässt sich jedes univariate Polynom $f(x)$ von Grad d wie folgt beschreiben:

$$f(x) = \sum_{i=0}^{d} a_i x^i = a_0 + x(a_1 + x(a_2 + \cdots + x(a_{d-1} + xa_d)\cdots))$$

Dies liefert unmittelbar eine obere Schranke von $\mathrm{S}(f) = \mathcal{O}(d)$ für alle univariaten Polynome und wirft indirekt die Frage auf, ob es spezielle Polynome mit schärferen Schranken gibt. Ein erstes Beispiel hierfür sind Polynome der Form $g(x) = x^d$. Auch hier ist die Problematik von $x = x^d$ des $\mathbb{F}_2$ zu erkennen. Für die aktuelle Betrachtung ist es leicht zu sehen, dass sowohl die obere als auch die untere Schranke der Berechnung von $g(x)$ durch $\mathrm{S}(g) = \Theta(\log(d))$ logarithmisch beschränkt ist. Die Berechnung gestaltet sich durch eine vielfache Nullstelle als trivial und die entsprechende untere Schranke gilt für alle univariaten Polynome.
Das Gegenstück hierzu bilden Polynome der Form $h(x) = (x-1)\cdot(x-2)\cdot\cdots\cdot(x-(d-1))\cdot(x-d)$ mit d unterschiedlichen Nullstellen. Doch bereits hier zeigen sich die Grenzen der aktuellen Forschung auf, da außer den bereits erwähnten Schranken für alle Polynome aktuell keine weiteren Aussagen getroffen werden können.

3 *Multivariate Polynome*

Das einführende Beispiel dieses Kapitels sind *Symmetrische Polynome*, die bei Vertauschung zweier beliebiger unterschiedlicher Variablen das gleiche Polynom ergeben.
Eine besondere Form stellen hierbei elementarsymmetrische Polynome dar, aus denen sich alle symmetrischen Polynome zusammensetzen lassen. Formell ergibt sich:

$$\mathrm{SYM}_n^k(x_1, \cdots, x_n) = \sum_{\substack{S \subset [n] \\ |S|=k}} \prod_{i \in S} x_i, \quad \forall k : 0 \leq k \leq n, \quad n, k \in \mathbb{N}$$

Jedes elementarsymmetrische Polynom ist einzigartig für Grad d in n Variablen. Die Anzahl der entstehenden Monome ist durch den Binomialkoeffizienten beschränkt, dessen Komplexität sich über die Stirling Approximation als $\mathcal{O}(2^n/\sqrt{n})$ und somit exponentiell bestimmen lässt.

Die bisherige Darstellung der elementarsymmetrischen Polynome geschah über eine Summe von Produkten. Da elementarsymmetrische Polynome den Koeffizienten des univariaten Polynoms $g(t) = \sum_{i=1}^{n}(t - x_i)$ in einer neuer Variablen t entsprechen, kann $g(t)$ nun für $n+1$ unterschiedliche Werte von t ausgewertet und die Resultate linear interpoliert werden.
Im Folgenden eine kurze Darstellung für ein Polynom von Grad 3:

$$\begin{aligned} g(t) &= t^3 + a_2 t^2 + a_1 t + a_0 \\ &\Leftrightarrow (t - x_1)\cdot(t - x_2)\cdot(t - x_3) \end{aligned}$$

$$\begin{aligned} a_2 &= -x_1 - x_2 - x_3 \\ a_1 &= x_1 x_2 + x_1 x_3 + x_2 x_3 \\ a_0 &= -x_1 x_2 x_3 \end{aligned}$$

Wie zu sehen entsprechen die Parameter a_0, a_1, a_2 jeweils einem entsprechenden elementarsymmetrischen Polynom. Eine solche Darstellung als $\sum\prod\sum$ liefert sogar für arithmetische Formeln eine quadratische obere Schranke.
Alle folgenden Polynome haben einen starken Bezug zu Matrizen und auch außerhalb dieser Ausarbeitung eine große Bedeutung in vielen Teilgebieten der Naturwissenschaften.
Für zwei Matrizen $A \in \mathbb{K}^{m\times n}$, $B \in \mathbb{K}^{n\times p}$ ist die Matrixmultiplikation wie folgt definiert:

$$\mathrm{MM}(AB) = C \; C \in \mathbb{K}^{m\times p} \text{ mit } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

In diesem Abschnitt werden nur quadratische Matrizen der Form $M \in \mathbb{K}^{n\times n}$, $n \in \mathbb{N}$ mit entsprechend n^2 vielen Einträgen betrachtet. Da stets alle Einträge jeder Matrix betrachtet werden müssen liefert dies somit eine klare untere Schranke von $\Omega(n^2)$. Für den naiven Algorithmus ergibt sich als obere Schranke für die größe des Schaltkreises $S(MM) = \mathcal{O}(n^3)$. Diese Erkenntnis kann auf verschiedene Arten erlangt werden. Zum einen durch die Berechnung des inneren Produkts, wofür über die Anzahl der Zeilen bzw Spalten der entsprechenden Matrizen iteriert werden muss. Zum anderen kann für quadratische Matrizen der Größe $n = 2^k$, $k \in \mathbb{N}$ ein *Divide & Conquer* Algorithmus zur Berechnung angewandt werden. Für die Rekursion werden die Matrizen wie folgt in jeweils 4 gleichgroße quadratische Matrizen der Größe $n/2$ unterteilt:

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}$$

Die Anzahl der benötigten Additionen ist hierbei durch die Anzahl n^2 der Elemente beschränkt. Somit ergibt sich für den naiven Algorithmus die Rekursionsgleichung:

$$T(n) = 8 \cdot T(n/2) + \Theta(n^2) \text{ mit Basisfall } T(1) = \Theta(1)$$

Für das Master Theorem ergeben sich somit die Werte $a = 8$, $b = 2$ sowie $f(n) = n^2$, womit man sich im Fall $f(n) \in \mathcal{O}(n^{\log_b(a-\varepsilon)})$ befindet und sich eine Komplexität von
$T(n) \in \Theta(n^{\log_b(a)}) = \Theta(n^3)$ ergibt.
Hervorzuheben ist hierbei, dass $b = 2$ fest ist und man sich für $4 \leq a < 8$ immer in diesem Fall des Master Theorems befindet, was zu der ersten offenen Frage bezüglich der Matrix Multiplikation führt:

Offene Frage: Gilt für alle $\varepsilon > 0$, dass $S(MM) = \mathcal{O}(n^{2+\varepsilon})$?

Ein erster Schritt in diese Richtung und somit eine bedeutende Verbesserung des naiven Algorithmus wurde 1969 von Volker Strassen [2] erreicht. Das Strassen-Algorithmus getaufte Verfahren macht sich die Tatsache zu Nutze, dass eine konstante Erhöhung der benötigten Additionen pro Rekursionsschritt keinerlei Auswirkungen auf die Komplexität der Rekursion hat. Durch geschickte Kombination einzelner Teilmatrizen konnte die Anzahl der benötigten Multiplikationen jedoch auf 7 reduziert werden.
Im Folgenden sind die multiplikativen Blöcke sowie ihre Zusammensetzung aufgeführt:

S_1	=	$(A_{11} + A_{22}) \cdot (A_{22} + B_{22})$	S_5	=	$(A_{11} + A_{12})B_{22}$	C_{11}	=	$S_1 + S_4 - S_5 + S_7$
S_2	=	$(A_{21} + A_{22})B_{11}$	S_6	=	$(A_{21} - A_{11}) \cdot (B_{11} + B_{12})$	C_{12}	=	$S_3 + S_5$
S_3	=	$A_{11} \cdot (B_{12} - B_{22})$	S_7	=	$(A_{12} - A_{22}) \cdot (B_{21} + B_{22})$	C_{21}	=	$S_2 + S_4$
S_4	=	$A_{22} \cdot (B_{21} - B_{11})$				C_{22}	=	$S_1 - S_2 + S_3 + S_6$

Die Komposition von C_{11} ist in Abbildung 2 beispielhaft illustriert.

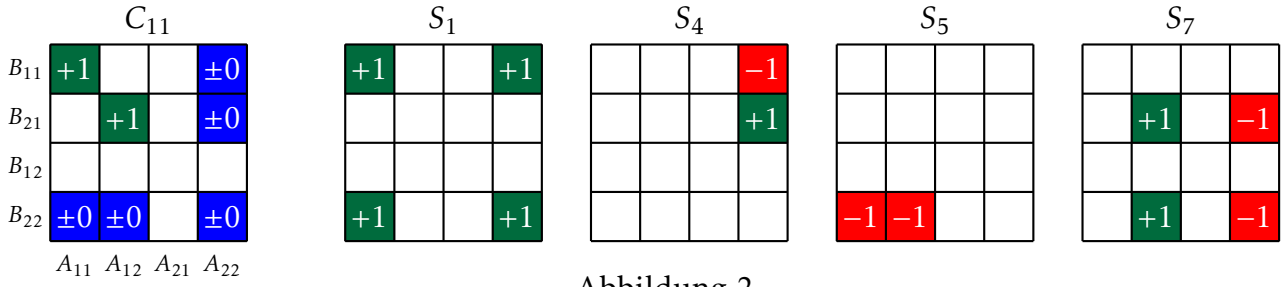

Abbildung 2

Die Komplexität des Strassen-Algorithmus kann wie zuvor durch das Master-Theorem bestimmt werden und es folgt $\Theta(n^{\log_2(7)}) \approx \Theta(n^{2.8074\ldots})$.

Im Laufe der letzten 50 Jahre kam es kontinuierlich zu Verbesserungen, die jedoch weitestgehend auf Strassens Laser Methode aufbauen. Für solche Algorithmen wurde eine Schranke von $\mathcal{O}(n^{2.3078})$ nachgewiesen, was den Traum einer quadratischen Komplexität vorerst einen Dämpfer versetzt. Das aktuell beste Ergebnis liegt seit 2020 bei Alman und Williams mit einer Komplexität von $\mathcal{O}(n^{2.3728\ldots})$.

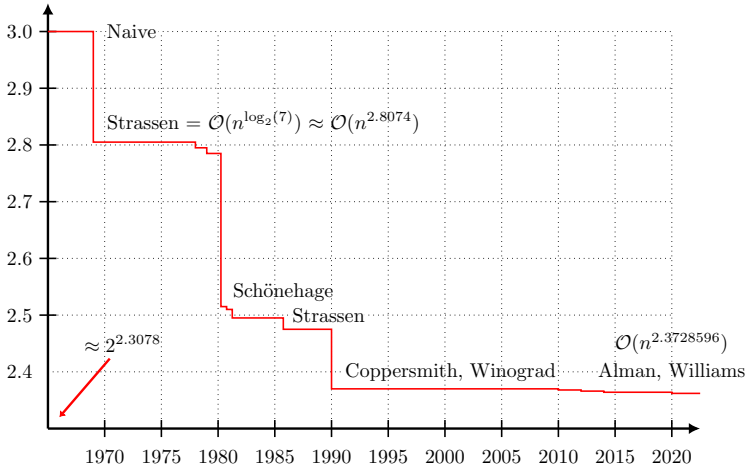

Abbildung 3

Ein weiteres Polynom mit direktem Bezug zu quadratischen Matrizen ist die durch die Leibniz-Formel bestimmte Determinante:

$$DET(A) = \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i} \right), A \in \mathbb{K}^{n \times n}, n \in \mathbb{N}$$

Sie beschreibt die Änderung des Volumens der durch die Matrix beschriebene lineare Abbildung und liefert konkrete Aussagen über die eindeutige Lösbarkeit linearer Gleichungssysteme. Durch ihre praktische Relevanz besteht großes Interesse an effizienter Berechenbarkeit, da in ihrer naiven Form $n!$ Summanden entstehen. Eine praktischere Alternative hierzu ist die auf dem gaußschen Eliminationsverfahren basierende LU Dekomposition, die eine Matrix als das Produkt eine unteren sowie einer oberen Dreiecksmatrix realisiert. Hierfür wird jedoch Division genutzt, die in der Welt der arithmetischen Schaltkreise so nicht gestattet ist. Stattdessen ist es jedoch möglich, die Determinante als Produkt von Matrizen auszudrücken und es folgt:

Theorem. $S(DET) \leq \mathcal{O}(S(MM)\log(n)) = \mathcal{O}(n^{2.3728\ldots})$.

Nach aktuellem Stand steht die Komplexität der Determinante somit in direktem Bezug zu der Komplexität der Matrixmultiplikation. Die Berechnung der Determinante durch arithmetische Formeln gestaltet sich jedoch als merklich komplexer und es gilt:

Theorem. *Es gilt* $L(DET) = \mathcal{O}(n^{\log(n)})$ *sowie* $L(DET) = \Omega(n^3)$.

Im direkten Vergleich zur Determinante steht ihre große Schwester, die Permanente.

$$PER(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma_i},\ A \in \mathbb{K}^{n \times n}, n \in \mathbb{N}$$

Auch wenn die Formel durch das Fehlen des Signums zunächst vereinfacht wirkt, gestaltet sich ihre Berechnung als deutlich komplexer. Eine Ausnahme hierzu bildet wieder der Körper $\mathbb{F}_2$, wo die Permanente der Determinante entspricht.

Die Permanente hat einen direkten Bezug zu *perfekten Matchings* in bipartiten Graphen, da jedes Monom ungleich null einem Matching entspricht. Das beste Ergebnis für die Berechnung liefert aktuell die 1963 von H.J. Ryser [1] entwickelte Formel:

$$\text{RYSER}(A) = (-1)^n \sum_{S \subseteq \{1,\cdots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} a_{ij}$$

Wie bereits bei der Berechnung symmetrischer Polynome werden auch hier $\sum\prod\sum$ - Schaltkreise genutzt. In ihrer klassischen Form ergibt sich als obere Schranke für arithmetische Formeln eine Komplexität von $\text{L}(PER) = \mathcal{O}(n^2 2^{n-1})$. Für arithmetische Schaltkreise können weitere arithmetische Operationen eingespart werden, indem die Mengen S in Gray code Reihenfolge durchgegangen werden, also pro Schritt nur ein Bitwechsel vorliegt. Dies liefert eine Komplexität von $\mathcal{O}(n2^{n-1})$. Nach aktuellem Stand der Forschung ist davon auszugehen, dass die Berechnung der Permanente nicht in polynomieller Zeit möglich ist.

4 *Valiant's Komplexitätsklassen*

Leslie Valiant leistete mit seinem 1979 veröffentlichten Paper *Completness Classes in Algebra* [3] einen bedeutenden Beitrag zur Komplexitätstheorie. Die erste relevante Klasse ist $\#\mathcal{P}$ der Funktionen, die durch das Zählen von Turing Maschinen polynomieller Komplexität berechnet werden können. Sie entspricht somit der Menge aller Zählprobleme der zugehörigen Entscheidungsprobleme der Klasse $\mathcal{NP}$. Außerdem führte Valiant die an $\mathcal{P}$ und $\mathcal{NP}$ angelehnten und seinen Namen tragenden Klassen $\mathcal{VP}$ und $\mathcal{VNP}$ ein. Des weiteren entwickelte er mit der (affinen) Projektion ein Verfahren für die Reduzierbarkeit von Polynomen. Abschließend werden die im vorherigen Kapitel besprochenen Beispiele in die eingeführten Klassen eingeordnet.

Definition. Eine Sequenz von Polynomen $f = \{f_n\}$ ist in $\mathcal{VP}$ wenn $\text{S}(f) \leq n^{\mathcal{O}(1)}$.

Die Klasse $\mathcal{VP}$ entspricht somit allen Polynomen, die von arithmetischen Schaltkreisen polynomieller Größe berechnet werden können. Dementsprechend lassen sich die Probleme SYM, MM und DET alle in die Klasse $\mathcal{VP}$ einordnen. PER hingegen liegt wie diskutiert nicht in der Klasse.
Eine Unterklasse von $\mathcal{VP}$ ist die Klase $\mathcal{VL}$ aller Polynome mit polynomiellen Formeln.

Analog der bekannten Reduzierbarkeit von Entscheidungsproblemen führt Valiant die Projektion zwischen Polynomen ein.

Definition. Seien $f \in \mathbb{F}[x_1, \cdots, x_n]$ und $g \in \mathbb{F}[y_1, \cdots, y_m]$, dann ist f eine **affine Projektion** $f \leq g$ von g, wenn m affine Funktionen $l_i : \mathbb{F}^n \to \mathbb{F}$ existieren, so dass $f(x) = g(l_1(x), \cdots, l_m(x))$. f ist eine **Projektion** von g, wenn alle affinen Funktionen l_i von maximal einer Variablen abhängig sind.

Die Projektion erlaubt es für die Eingaben von g jeweils eine der Variablen aus x zu wählen und diese zu skalieren bzw translatieren. Insbesondere erlaubt dieses Verfahren die wiederholte Verwendung einzelner Variablen, womit es vielen Schaltkreisen möglich ist weniger komplexe Schaltkreise zu simulieren. Nutzt ein Polynom analog dazu explizit all seine Variablen, so kann es keine Projektion mit weniger Variablen geben.
Existiert eine Projektion $f \leq g$, so gilt entsprechend $S(f) \leq S(g) + \mathcal{O}(m \cdot n)$. Relationen dieser Form zwischen Polynomen sind stets transitiv, so dass sie als partielle Ordnung der Komplexität von Polynomen aufgefasst werden können. Valiant zeigte in seinem Paper, dass DET $\mathcal{VP}$-schwer ist. Dies bedeutet, dass jede Sequenz von Polynomen aus $\mathcal{VL}$ die Projektion der Determinante einer Matrix polynomieller Größe ist. Final führt Valiant die Klasse $\mathcal{VNP}$ ein:

Definition. Eine Sequenz von Polynomen $f = \{f_n\} \in \mathbb{F}[x_1, \cdots, x_n]$ ist in $\mathcal{VNP}$ wenn es ein $g = \{g_n\} \in \mathbb{F}[x_1, \cdots, x_n, y_1, \cdots, y_n] \in \mathcal{VP}$ gibt, so dass $f_n(x) = \sum_{\alpha \in \{0,1\}^n} g_n(x, \alpha)$.

Es ist leicht zu sehen, dass für jedes Polynom $f \in \mathcal{VP}$ g identisch zu f gewählt werden kann. Somit liegen alle Polynome aus $\mathcal{VP}$ auch in $\mathcal{VNP}$. Für alle Polynome f in $\mathcal{VNP}$ gilt insbesondere, dass alle Koeffizienten von Monomen in f in polynomieller Zeit berechnet werden können. Da alle Monome der Permanente polynomiell in n sind gilt $PER \in \mathcal{VNP}$. Valiant gelang es außerdem zu zeigen, dass die Permanente sogar $\mathcal{VNP}$-vollständig ist und somit hohe Relevanz für weitere Forschung und Beweise durch Projektionen besitzt. Eine weitere wichtige Rolle spielt die Permanente auch für die Klasse $\#\mathcal{P}$, da t bereits die die 0/1-Permanente erstaunlicherweise $\#\mathcal{P}$-vollständig und somit auch implizit mindestens so schwer wie alle Probleme in $\mathcal{NP}$ ist.

Bisher sind nur wenige direkte Zusammenhänge bekannt. Wie besprochen gilt $\mathcal{VP} \subseteq \mathcal{VNP}$, jedoch wird wie auch bei $\mathcal{P}$ und $\mathcal{NP}$ eine echte Teilmengenrelation vermutet. Sollte sich $\mathcal{P} \neq \mathcal{NP}$ zeigen lassen, so würde sofort $\mathcal{VP} \neq \mathcal{VNP}$ folgen. Gilt hingegen $\mathcal{VP} \neq \mathcal{VNP}$, so gilt direkt $\mathcal{P}/poly \neq \mathcal{NP}/poly$. Nichtsdestotrotz erlaubt Valiants Ansatz tiefe Einblicke in das Verständnis von Polynomen und arithmetischen Schaltkreisen.

5 *Ausblick*

Arithmetische Komplexität ist im Kontext der Wissenschaftsgeschichte mit ihren 50 Jahren ein noch junges Themengebiet. Wie zu sehen wurden zwar einige Schranken aufgezeigt, jedoch gestaltet es sich als schwierig diesbezüglich allgemeingültige Aussagen zu treffen. Aus diesem Grund beschäftigt man sich verstärkt mit der Betrachtung von eingeschränkten Schaltkreisen. Diese erlauben stärkere, dafür jedoch spezifischere Aussagen.

Ein Beispiel hierfür sind *monotone Schaltkreise*, die nur positive Koeffizienten des Körpers nutzen. Sie sind vergleichbar mit Boolschen Schaltkreisen, die nur aus $\wedge$ und $\vee$ Gattern bestehen und berechnen entsprechend monotone Funktionen. Eine Boolsche Funktion $f : \{0,1\}^n \to \{0,1\}$ heißt monoton genau dann, wenn für zwei beliebige Eingaben $x, y \in \{0,1\}^n$ mit $x_i = 1 \Rightarrow y_i$ für alle $i \leq n$ gilt, dass $f(x) \leq f(y)$. Für monotone Schaltkreise konnte bereits

gezeigt werden, dass die Berechnung der Permanente arithmetische Schaltkreise exponentieller Größe benötigt.

Das abschließende Beispiel sind *nicht-kommutative Schaltkreise*. Diese untersagen die Permutation verschiedener Variablen in einem Monom. Als direkte Konsequenz erschweren sich gewisse Rechnungen. Die Berechnung des Polynoms x^2-y^2 hat bisher durch die Umformung zu $(x-y)\cdot(x+y)$ nur eine Multiplikation benötigt. Nicht-kommutative Schaltkreise können dies nicht leisten und benötigen entsprechend zwei Multiplikationen. Interessanterweise sind die Determinante und die Permanente für nicht-kommutative Schaltkreise äquivalent schwer und es gilt $DET \leq PER$ sowie $PER \leq DET$. Für beide konnte bisher gezeigt werden, dass sie nicht-kommutative Formeln exponentieller Größe benötigen.

Literatur

[1] Herbert John Ryser. *Combinatorial mathematics*, volume 14. American Mathematical Soc., 1963.

[2] Volker Strassen. Gaussian elimination is not optimal. *Numerische mathematik*, 13(4):354–356, 1969.

[3] Leslie G Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[4] Avi Wigderson. *Mathematics and Computation: A Theory Revolutionizing Technology and Science*. Princeton University Press, 2019.