

# Besprechungen zu Büchern der Computeralgebra

Erschienen im Computeralgebra Rundbrief 21, Oktober 1997.

- **P. Bürgisser, M. Clausen, M.A. Shokrollahi, Algebraic Complexity Theory**

Volume 315 der *Grundlehren der mathematischen Wissenschaften*, Springer-Verlag Berlin, Heidelberg, New York 1997, ISBN 3-540-60582-7, pp. 618, DM 188.

Gegenstand des vorliegenden Buches ist die algebraische Komplexitätstheorie, d.h. “the study of the intrinsic algorithmic difficulty of algebraic problems within an algebraic model of computation”. Dies ist ein recht junges Gebiet der Mathematik, dessen Etablierung als eigenständiges Wissenschaftsgebiet gewöhnlich in die 50er und 60er Jahre datiert wird. Wie die Komplexitätstheorie insgesamt hat es seine Wurzeln einerseits im Bereich des Designs effektiver Algorithmen und andererseits in der Suche nach Invarianten, die die inhärente Schwierigkeit gewisser Probleme widerspiegeln. Es greift dazu anspruchsvolle Argumente aus vielen Bereichen der Mathematik auf, was eine einigermaßen umfassende monographische Darstellung ebenso wünschenswert wie schwierig macht.

Hier besteht in der vorhandenen Literatur noch eine Lücke, wie die Autoren unter Verweis auf eine Reihe von Übersichtsbeiträgen vermerken: “However, with the exception of the now classic monograph by Borodin and Munro (American Elsevier, 1975) a systematic treatment of this theory is not available.” Das vorliegende Buch leistet einen wesentlichen Beitrag, diese Lücke auszufüllen. Es besteht aus 5 Teilen sowie einem informellen Einführungskapitel in die Fragestellungen der algebraischen Komplexitätstheorie.

Die 5 Teile behandeln im einzelnen folgende Aspekte:

**Teil 1: Grundlegende Algorithmen** (78 S.), führt asymptotisch schnelle Algorithmen zur Polynom-Multiplikation, zum Rechnen mit Potenzreihen (Algorithmen von Sieveking, Kung, Brent und Brent-Kung), zur GCD-Berechnung von univariaten Polynomen (Knuth-Schönhage) und zur Mehrfachevaluierung (Horowitz) ein und diskutiert Meyer auf der Heides Ergebnis zum Rucksackproblem.

**Teil 2: Elementare untere Schranken** (66 S.), führt das im Weiteren verwendete algebraische Berechnungsmodell (straight line programs und Berechnungsbäume) ein und beschreibt verschiedene Techniken zur Herleitung elementarer (d.h. linearer) unterer Komplexitäts-Schranken (Transzendenzgrad, Substitutionsmethode, Strassens Vermeidung von Divisionen, Derivationen).

**Teil 3: High Degree** (132 S.), zeigt, wie Konzepte der algebraischen Geometrie und der algebraischen Topologie eingesetzt werden können, um nichtlineare untere Schranken herzuleiten.

Einen großen Teil des Buches nimmt **Teil 4: Low Degree** (236 S.) ein, in dem sehr detailliert Fragen der Matrixmultiplikation und der bilinearen Komplexität behandelt werden und der von den Autoren als “book within the book” bezeichnet wird.

Das Buch beschließt ein kurzer **Teil 5: Vollständigkeitsprobleme** (32 S.), in dem Valiants nicht-uniformes algebraisches Analogon zur Problematik P vs. NP diskutiert wird.

Das Buch ist sehr ausführlich in der Argumentation und mit einer Vielzahl von Übungsaufgaben unterschiedlichen Schwierigkeitsgrads untermsetzt. Es ist damit sowohl als Referenz als auch als Lehrbuch vorzüglich geeignet.

Vergleicht man es mit den in der Einleitung genannten Übersichtsbeiträgen, so fällt die starke Affinität zu Strassens Kap. 11 im *Handbook of Theoretical Computer Science*, Elsevier 1990, ins Auge, dessen Einfluß die Autoren auch dankend vermerken. Damit bleiben trotz der Dicke des Buches eine Reihe wichtiger Entwicklungen, wie sie etwa in v.z.Gathens Beitrag in *Ann. Rev. Comp.*

*Sci.* **3** (1988), 317-344, für andere algebraische Teilgebiete (Polynomfaktorisierung, Permutationsgruppen) aufgerissen werden, außer Betracht.

Man mag eine solche Beschränkung mit Hinweis auf eben diese Dicke des Buches hinnehmen. Besonders bedauert es der Referent allerdings, daß dabei auch das ganze Thema der parallelen algebraischen Komplexität ausgeklammert wurde, die ebenfalls auf wichtige Ergebnisse verweisen kann. Eine wünschenswerte monographische Aufarbeitung dieser Ergebnisse, die bereits im Buch von Borodin/Munro begonnen wurde, könnte nahtlos an den entwickelten Begriffsapparat anschließen und hätte kaum einer Aufstockung des verwendeten mathematischen Apparats bedurft.

Hans-Gert Gräbe (Leipzig)