Besprechungen zu Büchern der Computeralgebra

Erschienen im Computeralgebra Rundbrief 23, Oktober 1998.

- **L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation**. Mit einem Vorwort von R.M. Karp.

  Springer-Verlag New York, 1998, ISBN 0-387-98281-7, pp. 453, DM 79.

  In den letzten Jahren sind in der Computeralgebra zunehmend Bemühungen zu verzeichnen, Brücken hin zur numerischen Mathematik zu schlagen und auf diese Weise dem Begriff des "wissenschaftlichen Rechnens" eine umfassendere Bedeutung als heute gemeinhin üblich zu geben (und so auf längere Sicht eine "Computermathematik" als gemeinsamen Oberbegriff zu etablieren – [Grabmeier; it + ti, Heft 6/95]). Dabei stoßen paradigmatisch unterschiedliche Welten aufeinander: Während die symbolischen Methoden der Computeralgebra, wenigstens im Prinzip, streng mathematisch deduktiver Natur sind, haben numerische Verfahren meist approximativen Charakter und sind damit zunächst auf ein quantitatives Bild der Realität ausgerichtet.

  Entsprechend unterscheiden sich auch die Möglichkeiten einer detaillierten Analyse der jeweiligen Algorithmen auf einer exakten komplexitätstheoretischen Grundlage; während symbolische Verfahren ob der potentiellen Endlichkeit der vorkommenden Strukturen gut mit dem theoretischen Bild vom Computer etwa als Turingmaschine zusammenspielen, wird es in numerischen Verfahren durch die Abbildung der Überabzählbarkeit der reellen Welt auf die Endlichkeit des Computers im Detail oftmals schwierig, die Ergebnisse von Rechnungen mit ebendieser Realität in Verbindung zu bringen. Obwohl dabei Werkzeuge der Analysis an vielen Stellen hilfreich sind, schreibt S. Smale (SIAM Review 32 (1990), 211-220): "The numerical analysis is highly successful but with no foundation".

  Das hier zu referierende Buch leistet einen Beitrag in Richtung einer solchen Fundierung von Rechnungen mit reellen Zahlen aus einer komplexitätstheoretischen Sicht, indem es die von den Autoren in den letzten $10 \cdots 15$ Jahren entwickelten Ansätze und Ergebnisse, die in ihrer Mehrzahl bereits in verschiedenen Zeitschriftenaufsätzen publiziert worden sind, in monographischer Form zusammenfaßt. Im Mittelpunkt steht dabei das Konzept einer uniformen algebraischen Maschine für Rechnungen über einem Ring oder Körper R, das sich an der Idee der Berechnungsbäume orientiert und bereits an anderer Stelle ausführlich dargestellt wurde, vgl. etwa den Artikel von drei der Autoren im *Bull. AMS 21 (1989), 1-46* oder L. Blums Vortrag auf dem ICM 1990 in Kyoto.

  Das Buch untergliedert sich in drei voneinander relativ unabhängige Teile. Als Ausgangspunkt dient eine Fragestellung von Penrose, der in seinem Buch "The Emperor's New Mind" (dt. erschienen als "Computerdenken" im Spektrum-Verlag Heidelberg 1991) an einer Stelle danach fragt, ob die Mandelbrot-Menge rekursiv ist. Mit Blick auf deren unendlich vielfältige Struktur lautet seine intuitive Antwort "nein", doch fehlt es zur Begründung an einem für algorithmische Zwecke brauchbaren Begriff einer reellen Zahl. Nach ausführlicher Erörterung dieses Problems aus unterschiedlicher Perspektive stellt Penrose abschließend, ganz im Sinne von Smale, fest: "Insgesamt gewinnt man deutlich den Eindruck, daß der richtige Ansatz erst noch gefunden werden muß." (Computerdenken, S. 125)

  Im ersten Teil **"Basic Developments"** (Kap. 1 bis 7) wird das von den Autoren vorgeschlagene uniforme Berechnungsmodell für eine Theorie reeller Zahlen, in dem man derartige Fragen zufriedenstellend beantworten kann, entwickelt und analysiert und Begriffe der klassischen Komplexitätstheorie wie Entscheidbarkeit, rekursive Funktionen, Laufzeit usw. verallgemeinert. Als Grundringe sind dabei neben den reellen Zahlen auch andere geordnete und ungeordnete Ringe und Körper, insbesondere $\mathbf{C}$, $\mathbf{Q}$, $\mathbf{Z}$ und $\mathbf{Z}_2$, von Interesse.

  Zunächst werden endlich-dimensionale Maschinen mit polynomialen oder rationalen Berechnungs- und Verzweigungsknoten eingeführt, mit denen Probleme vorgegebener Größe bearbeiten werden können. Aus den Eigenschaften der Haltemengen solcher Maschinen, die stets abzählbare Vereinigungen von semi- oder quasi-algebraischen Mengen sind, folgt bereits, daß das Enthaltenseinsproblem für interessante Mengen aus der Chaostheorie, wie Mandelbrot- oder Juliamengen, ja selbst für den Konvergenzbereich des Newton-Verfahrens, in diesem Modell unentscheidbar ist.

  Universelle Maschinen entstehen aus endlich-dimensionalen durch die Hinzunahme einer Shift-Operation, womit man in einem potentiell unendlichdimensionalen Zustandsraum operieren und damit entsprechende

Problemklassen durch Hinzunahme der Größe als Eingabeparameter als universelle Probleme formulieren sowie Komplexitätsklassen P und NP definieren kann. Wie in der klassischen Komplexitätstheorie wird danach der Begriff der Polynomialzeit-Reduzierbarkeit eingeführt und eine Hierarchie von Problemen über verschiedenen Grundbereichen entwickelt, die von der Lösbarkeit von semialgebraischen Systemen über geordneten Körpern (SA-FEAS) über den effektiven Hilbertschen Nullstellensatz (HN), das lineare und ganzzahlige Optimierungsproblem (LPF, IPF) und das Rucksack-Problem (KP) bis hin zum klassischen 3-SAT-Problem reichen, um eine kleine Auswahl der betrachteten Probleme aufzuführen. Die meisten der Probleme erweisen sich im weiteren als NP-vollständig, wobei mit dem 3-SAT-Problem die Äquivalenz der eingeführten Begriffswelt für $R = \mathbf{Z}_2$ zur klassischen NP-Vollständigkeit gezeigt wird. Für die Frage $P = NP\,?$ über verschiedenen Grundringen spielt (HN) eine zentrale Rolle, da es bei Einheitskosten in NP liegt, aber etwa über $R = \mathbf{Z}$ nicht einmal entscheidbar ist. Damit wird zugleich die neue argumentative Dimension gegenüber der klassischen Komplexitätstheorie deutlich.

Der erste Teil des Buches schließt mit dem Beweis der polynomialen Äquivalenz von Maschinen über $\mathbf{Z}_2$ mit Einheitskosten und über $\mathbf{Z}$ mit Bitkosten sowie einer eingehenderen Betrachtung der Frage $P = NP\,?$ über algebraisch abgeschlossenen Körpern der Charakteristik 0.

Der zweite Teil **"Some Geometry of Numerical Algorithms"** (Kap. 8 bis 15), der von den anderen beiden Teilen relativ unabhängig ist, widmet sich dem für numerische Rechnungen typischen Phänomen des Präzisionsverlusts. Dazu wird zunächst als primum mobile das Newton-Verfahren und der Begriff der approximativen Nullstelle untersucht und die Existenz universeller Konstanten bewiesen, die Gebiete um fixierte Nullstellen beschreiben, innerhalb derer das Newton-Verfahren genügend rasch konvergiert. Am Beispiel des Fundamentalsatzes der Algebra wird gezeigt, wie es auf dieser Basis entwickelte Pfadverfolgungs-Verfahren gestatten, universelle Komplexitätsschranken herzuleiten. Es schließt sich ein Beweis des Satzes von Bezout mit ähnlichen Methoden an.

Der Präzisionsverlust numerischer Rechnungen wächst gewöhnlich in der Nähe von Ausnahmemengen, was sich oft durch Konditionszahlen beschreiben läßt. Diesem Thema sind die Kapitel 11-14 gewidmet. Die Ausführungen beginnen mit Konditionszahlen für lineare Probleme, dem Eckart-Young-Theorem und einem Satz über den durchschnittlichen Präzisionsverlust für lineare Systeme. Danach werden Konditionszahlen für nichtlineare homogene polynomiale Gleichungssysteme definiert, deren Zusammenhang mit dem Abstand von der Diskriminanten-Varietät untersucht und die Verteilungsfunktion solcher Gleichungssysteme bei vorgegebenem Gradvektor bzgl. dieser Konditionszahl bestimmt. Daraus ergibt sich (u.a.) die durchschnittliche Anzahl reeller Nullstellen eines solchen Gleichungssystems mit reellen Koeffizienten als die Wurzel aus der Bezout-Zahl. Schließlich werden die Ergebnisse auf projektive Nullstellen erweitert und ein Zusammenhang zwischen der Konditionszahl eines Pfades und der Anzahl der notwendigen Newton-Iterationsschritte bei der Pfad-Verfolgung hergeleitet.

Diesen Teil beschließt Kapitel 15, in dem bewiesen wird, daß (LPF) über $\mathbf{Q}$ mit Bitkosten in Polynomialzeit entscheidbar ist.

Im dritten Teil **"Complexity Classes over the Reals"** (Kap. 16 bis 23) wird das im ersten Teil entwickelte Berechnungs-Modell im Verhältnis zu anderen Ansätzen betrachtet, die sich ebenfalls eignen, Aspekte der Komplexität des Rechnens mit reellen Zahlen widerzuspiegeln. Dieser Teil des Buches enthält eine Fülle verschiedensten Materials über die Beziehungen zwischen solchen Komplexitätsklassen. Dabei wird auch ein Schwachpunkt des gewählten Ansatzes mehrfach verdeutlicht, der darin besteht, daß man in der Ziffernfolge einer einzigen reellen Zahl kompliziert zu berechnende Information speichern und als Konstante einer Maschine zur Verfügung stellen kann.

Kap. 16 beginnt mit der Betrachtung algebraischer Berechnungsbäume. Für die Tiefe solcher Bäume wird eine logarithmische untere Schranke in der Zahl der reellen Zusammenhangskomponenten einer zu erkennenden Menge hergeleitet. Kap. 17 widmet sich probabilistischen Maschinen. Es wird gezeigt, daß über $\mathbf{R}$ die Klasse der fehlerbeschränkten probabilistischen Polynomialzeit-Maschinen mit der Klasse der deterministischen Polynomialzeit-Maschinen zusammenfällt, wobei die in einer einzigen reellen Konstanten kodierbare "richtige" Zufallswahl eine Rolle spielt.

Kap. 18 erweitert das bisherige uniforme Modell zu dem einer uniformen parallelen Maschine, in der eine abzählbare Anzahl bisheriger Maschinen über eine Aktivierungsfunktion, Kommunikationsknoten und einen gemeinsamen Takt zusammenwirken. In dem Zusammenhang werden neue Komplexitätsklassen PL

(parallele polylogarithmische Zeit) und PAR (parallele polynomiale Zeit) untersucht, $NP_{\mathbf{R}} \subseteq PAR_{\mathbf{R}}$ gezeigt sowie der Zusammenhang mit algebraischen Schaltkreisfamilien und den Klassen NC beschrieben.

Kap. 19 widmet sich der genaueren Abgrenzung zwischen diesen verschiedenen Klassen. Die entscheidenden Beispiele ergeben sich dabei wieder aus unteren Abschätzungen von Parametern verschiedener reeller Nullstellengebilde. Schließlich wird der Begriff der $P_{\mathbf{R}}$-Vollständigkeit (bzgl. polylogarithmischer Reduzierbarkeit) untersucht, um genauere Aussagen über $P_{\mathbf{R}}$-Probleme, die nicht in $NC_{\mathbf{R}}$ liegen, zu erhalten. Insbesondere ist (KP) ein solches Problem.

Kap. 20 untersucht Maschinen, in deren Kostenfunktion Multiplikationen besonders berücksichtigt werden (weak machines). Für diese gilt $P_W \neq NP_W = NP_{\mathbf{R}}$, womit sie für die Frage $P_{\mathbf{R}} = NP_{\mathbf{R}}$? interessant sind. Kap. 21 ist additiven Maschinen gewidmet, d.h. solchen, die keine Multiplikationen/Divisionen enthalten. Die Möglichkeit, in einzelnen reellen Zahlen umfangreiche Information zu kodieren, erlaubt es, derartige Maschinen durch solche mit konstantem Speicher zu simulieren. Weiter wird die polynomiale Hierarchie und ihr digitales Gegenbild untersucht und in Beziehung zueinander gestellt. Im Kap. 22 werden schließlich nichtuniforme Komplexitätsklassen, die durch algebraische Schaltkreisfamilien mit polynomial wachsender Größe beschrieben werden, untersucht, während Kap. 23 dem Begriff der deskriptiven Komplexität gewidmet ist.

"Real Computation" wird in diesem Buch also im doppelten Sinne des Wortes entwickelt, nämlich zum einen im Kontext einer Komplexitätstheorie, die reelle Zahlen (und allgemeiner Elemente eines Rings oder Körpers) nicht als dezimale Approximation, sondern als begriffliche Grundeinheit betrachtet, und zum anderen im Sinne von numerischen, also auf das Rechnen mit "wirklichen" reellen Zahlen gerichteten Methoden. Beides unter einen Hut zu bringen ist aus den eingangs dargelegten Gründen außerordentlich schwierig. Das vorliegende Buch arbeitet die wichtigsten Ansätze, die dabei im Rahmen der Übertragung von Ideen der klassischen und algebraischen Komplexitätstheorie bisher entwickelt wurden, monographisch auf. Der Klappentext schließt mit den Worten: "All those interested in questions of complexity and decidability will find this to be a path-breaking monograph into one of the most active areas of current research. It is written, however, so that it can be used as a textbook at the advanced undergraduate or graduate level in either a mathematics or a computer science department." Dem ist nichts hinzuzufügen.

Hans-Gert Gräbe (Leipzig)