Schulmathematik und Algorithmen der Computeralgebra

Prof. Dr. Wolfram Koepf

Universität Kassel
http://www.mathematik.uni-kassel.de/~koepf

Tag der Mathematik
13. Dezember 2008
Universität Passau

Überblick

- Computeralgebrasysteme
- Algorithmen
- Übungsaufgaben im Tutorium

Vorführung

Fähigkeiten von Computeralgebrasystemen

„General Purpose“ Computeralgebrasysteme wie Axiom, Derive, Maxima, Maple, *Mathematica*, MuPAD oder Reduce

- führen numerische Rechnungen durch wie Taschenrechner bzw. Programmiersprachen wie Pascal,
- rechnen auch mit rationalen Zahlen exakt,
- enthalten eine höhere Programmiersprache mit mathematiknahen Hochsprachenkonstrukten,
- sind im Gegensatz zu numerischen Programmiersprachen dialogorientiert,
- können Funktionen graphisch darstellen,
- und können auch symbolisch rechnen.

Symbolische Rechnungen

Was können Computeralgebrasysteme?

- Lineare Algebra,
- Polynome und rationale Funktionen,
- Faktorisierung von Zahlen und Polynomen,
- Modulare Arithmetik,
- Rechnen mit algebraischen Zahlen,
- Lösen polynomialer Gleichungssysteme,
- Differentiation,
- Integration,
- Lösen von Differentialgleichungen,
- Taylorpolynome und Potenzreihen.

Online-Demonstrationen mit Computeralgebra

Computeralgebrasysteme

- Zur Vorführung verwende ich das Computeralgebrasystem DERIVE, da es an deutschen Schulen weit verbreitet und den Handhelds von TI ähnlich ist. Auch wenn DERIVE von TI leider nicht mehr produziert wird.
- Genauso gut könnte aber auch jedes anderes General Purpose Computeralgebrasystem wie Maple, *Mathematica*, MuPAD oder Reduce verwendet werden.
- Start der Vorführung

Berechnung des ggT

Euklidischer Algorithmus

Den größten gemeinsamen Teiler von $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ berechnet man beispielsweise so:

- $\text{ggT}(a, b) := \text{ggT}(|a|, |b|)$, falls $a < 0$ oder $b < 0$
- $\text{ggT}(a, b) := \text{ggT}(b, a)$, falls $a < b$
- $\text{ggT}(a, 0) := a$
- $\text{ggT}(a, b) = \text{ggT}(b, a \mod b)$

Test mit DERIVE

Faktorisierung und Effizienz

Der euklidische Algorithmus ist viel effizienter als Faktorisierung, die in der Schule zur Bestimmung des ggT benutzt wird.

Modulare Potenzen

Kleiner Satz von Fermat

- Für eine Primzahl $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ gilt
$$a^p = a \mod p\,.$$
- Ist ggT$(a, p) = 1$, dann gilt ferner
$$a^{p-1} = 1 \mod p\,.$$
- Unter Benutzung der binomischen Formel
$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$
ist ein schultauglicher Beweis verfügbar.
- Fermattest: Ist der Satz von Fermat für eine Zahl $a \in \mathbb{Z}$ nicht erfüllt, so ist p keine Primzahl!
- Test mit DERIVE

Modulare Potenzen

Effiziente Berechnung von Potenzen

Die modulare Potenz $a^n \mod p$ berechnet man am besten durch Zurückführen auf Exponenten der Größe $\frac{n}{2}$ (Teile-und-Herrsche-Algorithmus):

- $a^0 \mod p := 1$
- $a^n \mod p := \left(a^{\frac{n}{2}} \mod p\right)^2 \mod p$ für gerade n
- $a^n \mod p := \left(a^{n-1} \mod p\right) \cdot a \mod p$ für ungerade n

Test mit DERIVE

Anwendung: Verschlüsselungsverfahren

Verschlüsselungsverfahren

- Bei einem Verschlüsselungsverfahren wird eine Nachricht N mit Hilfe einer Funktion E und eines Schlüssels e verschlüsselt
$$K = E_e(N) \ .$$
- Die Dekodierung erfolgt mit der (zugehörigen) Funktion D und dem Schlüssel d:
$$D_d(K) = D_d(E_e(N)) = N \ .$$
- Die Funktionen E und D sollten effizient berechnet werden können.
- Ein Problem ist die Schlüsselübergabe.

Asymmetrische Kryptographie

Asymmetrische Kryptographie

- Das RSA-Verfahren (Rivest, Shamir und Adleman (1978)) ist ein Beispiel eines *asymmetrischen* Verschlüsselungsverfahrens.
- Solche Verfahren wurden 1976 von Diffie und Hellman eingeführt.
- Hierbei verwenden Sender und Empfänger *jeweils eigene* Schlüssel e und d.
- Der Schlüssel e wird jeweils öffentlich bekannt gegeben, während der Schlüssel d geheim bleibt.
- Ein Schlüsselaustausch des jeweils persönlichen Dekodierungsschlüssels d ist demnach nicht erforderlich.

Das RSA-Verfahren

Wo wird das RSA-Verfahren eingesetzt?

- Das RSA-Verfahren wird bei der sicheren Anmeldung auf einem entfernten Computer benutzt (secure shell (`ssh`)).
- Es verbirgt sich hinter sicherer E-Mail mit dem Verfahren PGP (Pretty Good Privacy).
- Es wird verwendet beim sicheren Datentransfer auf *sicheren Webseiten* (`https`), beispielsweise beim Online-Banking.
- Also: Interneteinkauf und Online-Banking (mit `https`!) können wirklich sicher sein.

Das RSA-Verfahren

Kryptographisches Protokoll des RSA-Verfahrens

- Die Empfängerin Barbara bestimmt
  1. zwei mindestens (dezimal) 100-stellige zufällig ausgewählte Primzahlen $p \in \mathbb{P}$ und $q \in \mathbb{P}$.
  2. $n = p \cdot q$.
  3. $\varphi = (p-1) \cdot (q-1)$.
  4. eine zufällige natürliche Zahl $e < \varphi$ mit $\text{ggT}(e, \varphi) = 1$. Das Paar $e_B = (e, n)$ ist Barbaras öffentlicher Schlüssel und wird publiziert.
  5. $d = e^{-1} \pmod{\varphi}$. Die Zahl $d_B = d$ konstituiert Barbaras privaten Schlüssel, der unbedingt geheim gehalten werden muss.
- Barbara löscht (aus Sicherheitsgründen) p, q und φ.

Das RSA-Verfahren

Kryptographisches Protokoll des RSA-Verfahrens

- Die Senderin Anna verschlüsselt ihre Nachricht $N \in \mathbb{Z}_n$ mit der Rechnung

$$K = E_{e_B}(N) = N^e \mod n \in \mathbb{Z}_n \, .$$

- Barbara entschlüsselt (gegebenenfalls die einzelnen Blöcke) gemäß

$$D_{d_B}(K) = K^d \mod n \in \mathbb{Z}_n \, .$$

- Als Folge des kleinen Satzes von Fermat ist das RSA-Verfahren korrekt:

$$D_{d_B}(E_{e_B}(N) = N \, .$$

- Test mit DERIVE

Algorithmische Faktorisierung

Faktorisierung von Polynomen

- Polynome mit rationalen Koeffizienten können algorithmisch faktorisiert werden!
- Dies funktioniert sogar, wenn mehrere Variablen im Spiel sind.
- Algorithmische Faktorisierungen über $\mathbb{R}$ dagegen sind nur unter Verwendung algebraischer Zahlen möglich, z. B. $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
- Moderne schnelle Algorithmen gibt es nicht in DERIVE, aber in Maple, Mathematica, ...
- Test mit DERIVE

Algorithmische Differentiation

Differentiationsregeln

Ableiten ist algorithmisch, wenn wir die üblichen Ableitungsregeln verwenden:

- Konstantenregel: $c' = 0$, falls c konstant ist
- Potenzregel: $(x^n)' = n\,x^{n-1}$
- Linearität: $(f+g)' = f' + g'$ und $(c \cdot f)' = c \cdot f'$
- Produktregel: $(f \cdot g)' = f' \cdot g + g' \cdot f$
- Quotientenregel: $\left(\frac{f}{g}\right)' = \frac{f' \cdot g - g' \cdot f}{g^2}$
- Kettenregel: $f(g)' = f'(g) \cdot g'$
- Ableitungen transzendenter Funktionen

Test mit Mathematica

Algorithmische Integration

Stammfunktionen

Integration ist bekanntlich viel schwieriger. Dennoch:

- Auch für die Integration gibt es Algorithmen, welche entscheiden, ob ein Integral eine elementare Funktion ist.
- Die übliche Methode zur rationalen Integration benötigt eine reelle Faktorisierung des Nenners und ist daher kein guter Algorithmus. Aber rationale Integration kann algorithmisch durchgeführt werden und verwendet dann nur quadratfreie Faktorisierungen.
- Der Risch-Algorithmus und seine Verwandten zur elementaren Integration sind erheblich komplizierter und verallgemeinern den rationalen Fall.

Test mit Maple

Integration durch Summation

Flächenberechnung

Mit Computeralgebra kann man Integration didaktisch günstig durch Flächenberechnung einführen.

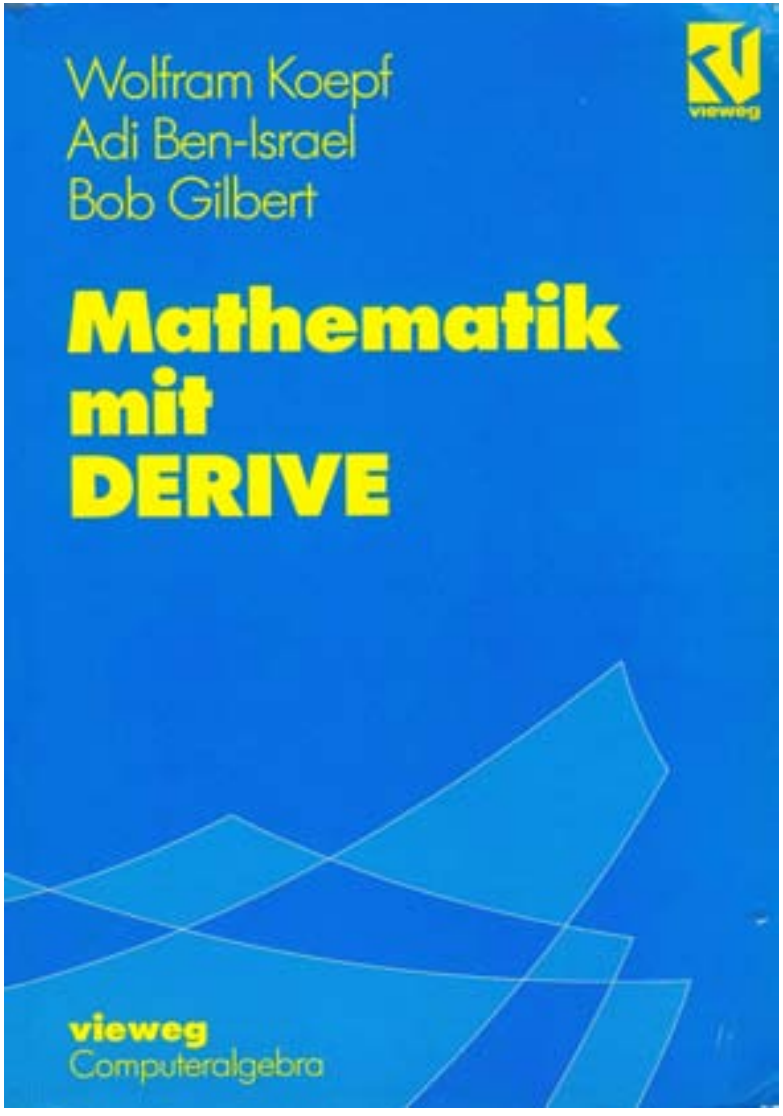
- Wählt man bei einer im Intervall $[a, b]$ positiven Funktion $f(x)$ und einer äquidistanten Zerlegung von $[a, b]$ eine Rechteckzerlegung des Flächeninhalts, so ergibt sich

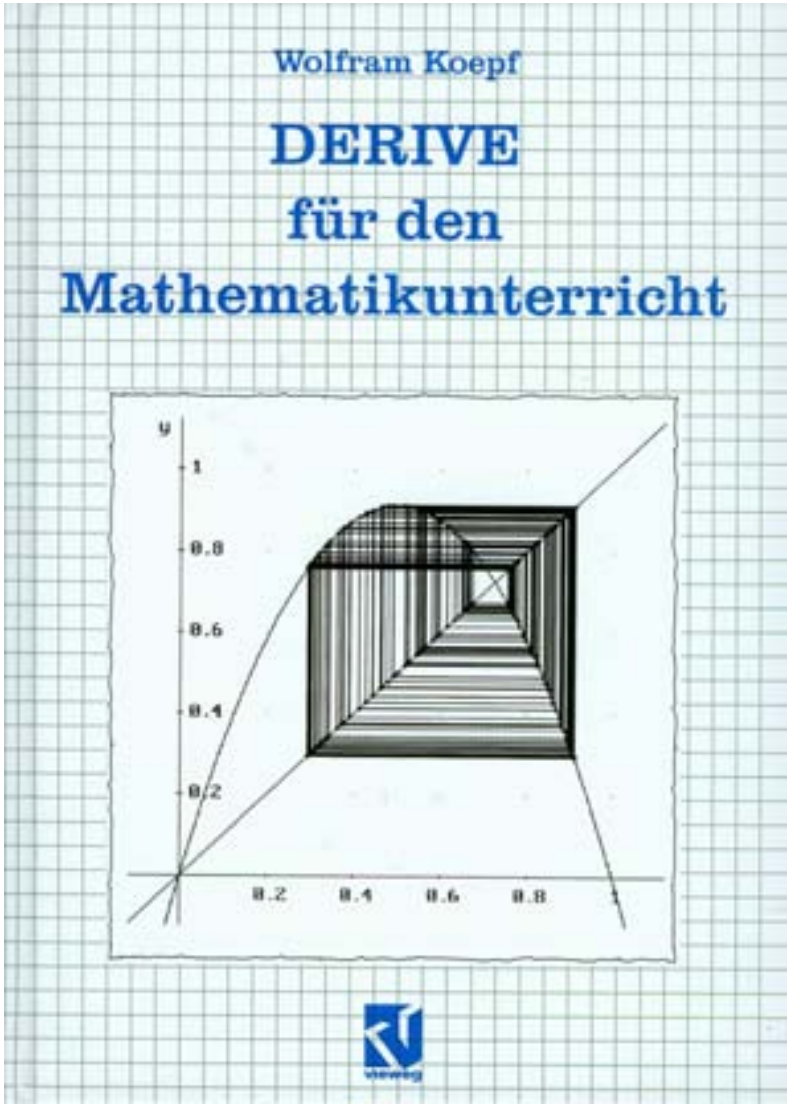
$$\int_a^b f(x)\,dx = \lim_{n\to\infty} \frac{b-a}{n} \sum_{k=1}^{n} f\left(a + k\,\frac{b-a}{n}\right) .$$

- Mit dieser Formel kann man viele Stammfunktionen mit DERIVE direkt aus der Definition bestimmen.
- Für weitere Funktionen klappt es mit einer geometrischen Zerlegung.

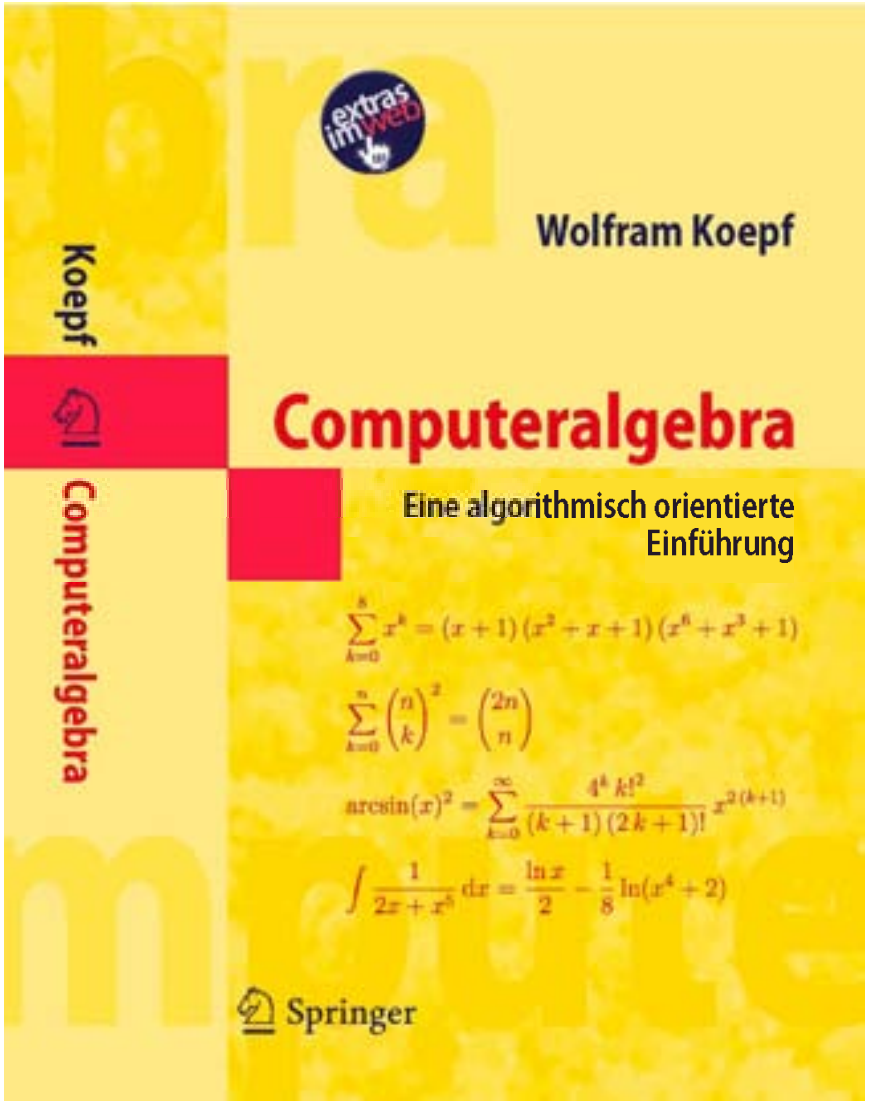
Test mit DERIVE

Wo kann man diese Themen nachlesen?





Wo kann man diese Themen nachlesen?



Vielen Dank für Ihr Interesse!

Übungsaufgabe 1

Reihenentwicklungen: Klassische und relativistische Energie

- In der speziellen Relativitätstheorie ergibt sich die Energie aus der Formel

$$E(v) = \frac{m\,c^2}{\sqrt{1 - \frac{v^2}{c^2}}}$$

- Wir erhält man mit DERIVE hieraus die berühmte Einsteinsche Formel für die Ruhemasse

$$E = m\,c^2$$

und die klassische Formel für die kinetische Energie

$$E_{\text{kin}} = \frac{1}{2} m\,v^2 \ ?$$

Übungsaufgabe 2

Das Hofstadterproblem

- Douglas Hofstadter (Gödel, Escher, Bach) kam bei der Verallgemeinerung des Morleyschen Dreiecks auf eine geometrische Vermutung.
- Hofstadters geometrische Vermutung ist richtig, wenn die Determinante der Matrix

$$\begin{pmatrix} \frac{\sin(r\alpha)}{\sin((1-r)\alpha)} & \frac{\sin(2\alpha)}{\sin(-\alpha)} & \frac{\sin((2-r)\alpha)}{\sin((r-1)\alpha)} \\ \frac{\sin(r\beta)}{\sin((1-r)\beta)} & \frac{\sin(2\beta)}{\sin(-\beta)} & \frac{\sin((2-r)\beta)}{\sin((r-1)\beta)} \\ \frac{\sin(r\gamma)}{\sin((1-r)\gamma)} & \frac{\sin(2\gamma)}{\sin(-\gamma)} & \frac{\sin((2-r)\gamma)}{\sin((r-1)\gamma)} \end{pmatrix}$$

  für alle $r \in (0,1)$ gleich 0 ist, sofern $\alpha + \beta + \gamma = \pi$ ist.
- Versuchen Sie dies mit DERIVE nachzuweisen.

Übungsaufgabe 3

Wo ist der zweite Pol?

- Während graphische Taschenrechner und Computeralgebrasysteme im Allgemeinen auf Anhieb Funktionsgraphen darstellen, gibt es auch Fälle, wo hierzu Kurvenuntersuchungen nötig sind.
- Stellen Sie folgende Funktion graphisch dar:

$$f(x) = \frac{100(x-1)}{(101x-100)(100x-99)}$$

- Wo ist der zweite Pol? Finden Sie durch eine Kurvendiskussion heraus, wo wichtige Punkte des Graphen liegen und stellen Sie schließlich den Graphen mit DERIVE in einem geeigneten Intervall so dar, „dass man alles sieht“.

Übungsaufgabe 4

Schlecht-konditionierte Probleme

- Wir wollen das Integral

$$I_n := \int_0^1 x^n \, e^{x-1} \, dx$$

für großes n bestimmen, sagen wir $I_{1.000.000}$.

- Versuchen Sie mit DERIVE den exakten bzw. den approximativen Wert von $I_{1.000.000}$ zu finden.
- DERIVE liefert die Approximation

$$I_{1.000.000} \approx 9.999978605\,10^{-7} \, .$$

Dies ist leider falsch.

Übungsaufgabe 4

Schlecht-konditionierte Probleme

- Wegen $ex < e^x < e$ für $x \in [0, 1]$ gilt

$$\int_0^1 x^{n+1}\,dx < I_n < \int_0^1 x^n\,dx\ ,$$

also

$$\frac{1}{n+2} < I_n < \frac{1}{n+1}\ .$$

Überprüfen Sie, ob DERIVEs Resultat dieser Bedingung genügt.

- Berechnen Sie I_{20} mit DERIVE exakt und erklären Sie, warum eine symbolische Berechnung ebenfalls scheitert.

Übungsaufgabe 4

Schlecht-konditionierte Probleme

- Partielle Integration liefert die Rekursion

$$I_n = 1 - n\, I_{n-1}$$

und den Anfangswert

$$I_0 = 1 - \frac{1}{e} \approx 0{,}63212\,05588\,28557\,6784\ldots\,.$$

- Benutzen Sie die DERIVE-Funktion `I(n):=IF(n=0,1-1/EXP(1),1-n*I(n-1))`, um `VECTOR(I(n),n,1,20)` zu approximieren.
- Erklären Sie!
- Haben Sie eine Idee, wie man das Dilemma auflösen kann?