
Pro-Seminar Mathematik im Alltag

Daten: 24.4, 8.5, 15.5, 29.5, 5.6, 12.6, 19.6, 26.6, 3.7, 10.7, 17.7 (12 Termine)

Ziel dieses Proseminars ist es in jedem Vortrag die Mathematik einer Technik oder einem Problem des täglichen Lebens zu verstehen.

Dabei sollen Sie zunächst erklären, worum es geht, und was die zugehörige Mathematik ist und wie diese das Thema beschreibt und ggf. löst. Dazu sind oft neue mathematische Begriffe zu definieren oder Sätze zu beweisen. Ziel ist es, am Ende eines Vortrages das Thema aus mathematischer Sicht zu verstehen.

Die angegebene Literatur ist immer nur als Ausgangspunkt gedacht; die Vortragenden sollen (und müssen) zusätzliche Quellen suchen, um den Vortragsgegenstand oder die dafür benötigte Mathematik besser zu verstehen oder verwandte Teilaspekte mit aufzugreifen.

Vorträge mit \diamond sind geeignet, um eine Zulassungsarbeit zu schreiben.

Programm:

1. **Additions- und Schiebe-Algorithmen.** Taschenrechner, vor allem ältere Modelle, verfügen über eine sehr einfache Hardware. In diesem Vortrag sollen daher Algorithmen vorgestellt werden, die die Exponentialfunktion, Winkel- und Hyperbelfunktionen und ihre Inversen mit möglichst einfachen Mitteln vergleichsweise schnell und vor allem zuverlässig ausrechnen. [6] Stichworte: CORDIC, BKM.
2. **SRT-Division** ist ein schnelles Divisionsverfahren in der Computerarithmetik. Es ist vor allem wegen des Pentium-FDIV-Bug bekannt, der in den ersten Versionen von Intels Pentium-Prozessoren zu vereinzelt fehlerhaften Divisionen führte. [6] Weiteres Stichwort: Modifizierte SRT-Algorithmen
3. **Der Satz vom Diktator.** Nach Wahlen oder Abstimmungen entsteht bei den Beteiligten manchmal das Gefühl, dass das Abstimmungsverfahren zu einem "ungerechten" Ergebnis geführt hat. Verschiedene mathematische Kriterien für "Gerechtigkeit" an ein solches Verfahren können unvereinbar sein.
Der Satz von Arrow, umgangssprachlich auch Satz vom Diktator, ist ein Beispiel dafür. Der Vortrag soll diesen Satz erklären und beweisen und eventuell verwandte Sätze vorstellen. [6], Stichwort Arrow's impossibility theorem
4. **Sitzzuteilungsverfahren.** Nach einer Bundestagswahl wird anhand der abgegeben Stimmen und mit Hilfe eines Auszählverfahrens eine Sitzverteilung für das Parlament festgelegt. Mittlerweile ist seit Gründung der Bundesrepublik das dritte solche Verfahren in Kraft. In diesem Vortrag soll auf den Unterschied zwischen Divisor- und Quotenverfahren eingegangen werden, sowie auf den Unmöglichkeitssatz von Balinski und Young. [6], Stichworte Sitzzuteilungsverfahren, Unmöglichkeitssatz von Balinski und Young.
5. **Risk-limiting audits** sind eine Form der Wahlprüfung. Es basiert auf statistischen Stichproben von Papierwahlzählungen, um zu überprüfen, ob das Wahlergebnis die richtigen Gewinner ermittelt hat. [6, 4]
6. **Fehlerfortpflanzung** Oft ist eine Größe nicht direkt messbar, sondern sie wird aus anderen gemessenen Größen berechnet. Jedoch hat jeder Messwert einen Fehler. Bei Einsetzen in eine Formel 'pflanzen sich diese Fehler fort'. [6]
7. \diamond **Lokalisierung** Möchte man den Standort von einem Objekt bestimmen, kann man z.B. seinen Abstand zu verschiedenen anderen Objekten, deren Standort man kennt bestimmen und daraus den gesuchten Standort bestimmen. Das führt mathematisch auf die Berechnung des Schnittes von Kreisen (in der Ebene) oder Kugeln (im Raum). Misst man allerdings Abstandsdifferenzen (z.B. als Unterschied in

Lichtlaufzeiten), führt das analoge Problem auf den Schnitt von Hyperbeln und Hyperboloiden. Analog kann man sich fragen, worauf führt das Problem der Winkel(differenz)messung. Komplizierter wird es, wenn man mit einberechnen will, dass alle Messergebnisse fehlerbehaftet ist und sich fragt, wieviele feste Vergleichobjekte man haben sollte.[6] Stichworte: GPS, Hyperbolic navigation.

8. **Algorithmen zur Routenplanung.** Bei der Routenplanung geht es darum, einen optimalen Weg zwischen einem Start und einem Zielort zu finden. Dabei hängt der Begriff 'optimal' im Allgemeinen von verschiedenen Parametern ab, z.B. versucht man einen Weg unter Zeitminimierung, Kostenminimierung sowie über bestimmte Zwischenorte zu realisieren. Mathematisch wird dieses Problem mit Hilfe der Graphentheorie betrachtet. Eine optimale Lösung kann man dann mit Hilfe des Dijkstra-Algorithmus bestimmen. [1]
9. **Die RSA Verschlüsselung** ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann. Es beruht darauf, dass die Multiplikation zweier Primzahlen einfach ist, aber die Zerlegung in Primfaktoren schnell die Kapazitäten von Rechnern sprengt. [6, 3] (Vorkenntnisse: Algebra)
10. **Der Diffie-Hellmann-Schlüsselaustausch** ist ein Protokoll zur Schlüsselvereinbarung. Es beruht auf diskrete Logarithmen: In machen endlichen zyklischen Gruppen mit gegebenem Erzeuger g lässt sich die Potenz $h = g^n$ für gegebenes n schnell berechnen, während kein effizientes Verfahren bekannt ist, dass den n .ten Logarithmus bei gegebenem h bestimmt. [3] Weiteres Stichwort: Elgamal-Verschlüsselungsverfahren (Vorkenntnisse: Algebra)
11. **Quantencomputer** Ersetzt man klassische Bits durch quantenmechanisch verschränkte“ Qubits, so kann man viele Rechnungen parallel durchführen. Beispielsweise gibt es einen effizienten Algorithmus zur Primfaktorzerlegung mittels eines Quantencomputers, den Shor-Algorithmus. Der Vortrag sollte sich auf theoretische Aspekte konzentrieren, aber durchaus auch auf den Stand der Technik eingehen. [6] (Vorkenntnisse: Algebra. Auch Quantenmechanik I ist hilfreich.)
12. **Benford's Gesetz.** Bei den Zahlen einer Steuererklärung treten typischerweise die ersten Ziffern nicht alle mit derselben Häufigkeit auf. Ähnliches gilt auch in anderen Zusammenhängen. Diese Erfahrung soll diskutiert und begründet werden. Sie wird eingesetzt, um Betrügereien auf die Spur zu kommen. [5]
13. **Temperierte Stimmung.** J. S. Bach veröffentlichte 1722 und 1740/42 zwei Sammlungen von Präludien und Fugen in allen Dur- und Molltonarten unter dem Titel: Das wohltemperierte Klavier. Der Vortrag soll sich mit dem Begriff wohltemperiert beschäftigen und auf die mathematische Beschreibung von Tonstrukturen eingehen. [6] (Stichworte: Tonstruktur)
14. **Kaffeetassen-Katakaustik.** Durch Lichtbrechung und -reflexion können sich interessante Muster ergeben. Dieser Vortrag soll erklären, wie sie zustandekommen. [2]

Literatur

- [1] M. Aigner, E. Behrends (Hrsg.), Alles Mathematik – von Pythagoras zum CD-Player, Vieweg, 2000.
- [2] C. Ucke, C. Engelhardt, Kaustik in der Kaffeetasse, Physik in unserer Zeit 29 (1998) 120–122, <http://www.ucke.de/christian/physik/ftp/lectures/kaustik3.pdf>
- [3] R.-H. Schulze, Codierungstheorie, Vieweg 2003
- [4] <https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>
- [5] <http://www.educ.ethz.ch/unt/um/mathe/ana/benford>
- [6] Wikipedia: The free Encyclopedia, Wikimedia foundation, <http://en.wikipedia.org/> oder <http://de.wikipedia.org/>