Bergische Universität Wuppertal Wintersemester 2019/20
Fakultät 4, Mathematik und Informatik
Dr. Matthias Wendt, Dr. Sean Tilson

Seminar: Mathematik im Alltag

Der Alltag ist voller Mathematik. Von Kodierung in der elektronischen Kommunikation oder in Audio- bzw. Videoformaten, Navigationssysteme zur Routenplanung über bildgebende Verfahren in der Medizintechnik bis hin zur mathematischen Analyse von Wahlverfahren gibt es viele Beispiele, wie Mathematik bei der Lösung alltäglicher Probleme weiterhilft. Ziel des Seminars ist, anhand verschiedener Beispiele die relevante Mathematik hinter alltäglichen Gegenständen oder Vorgängen kennenzulernen. In jedem Vortrag soll ein Gegenstand, Verfahren, Problem, Phänomen des Alltags erklärt werden, von der Formulierung über die mathematische Modellierung bis zur Lösung des Problems. Ziel am Ende des Vortrags ist, das Thema aus mathematischer Sicht zu verstehen. (Insbesondere sind die Vorträge des Seminars weitgehend unabhängig voneinander, bauen nicht aufeinander auf und können so unabhängiger vorbereitet werden.)
Das Seminar richtet sich an B.Sc.-Studierende ab dem dritten Fachsemester; für die meisten Vorträge sind nur Vorkenntnisse aus den Vorlesungen Lineare Algebra I-II und Analysis I-II notwendig. (Meistens werden aber die konkreten mathematischen Objekte oder Sätze nicht notwendig aus Vorlesungen bekannt sein.) Für manche Themen sind weitere Kenntnisse nötig oder wünschenswert; dies ist dann jeweils in der Vortragsbeschreibung angegeben.
Die angegebene Literatur ist ein Ansatzpunkt für eine selbständige Suche nach weiteren Quellen; eine Auseinandersetzung mit dem Thema, eigene Schwerpunktsetzungen, Aufgreifen verwandter Teilaspekte etc. sind ausdrücklich erwünscht. (Dabei bleibt aber die *mathematische* Auseinandersetzung mit dem Thema der zentrale Aspekt.) Die unten angeführte Liste ist nur eine Auswahl möglicher Themen. Gerne können Sie (nach Absprache) auch eigene Themenvorschläge einbringen.

Liste der Vorträge.

(1) **Additions- und Schiebealgorithmen**
Es gibt einfache und zuverlässige Algorithmen, die Exponentialfunktion, Winkel- und Hyperbelfunktionen schnell berechnen können. Die Algorithmen sollen im Vortrag vorgestellt werden. [Wikipedia, CORBIC, BKM]

(2) **Kreiszahl π**
Es gibt viele verschiedene Möglichkeiten, gute Näherungen für die Kreiszahl π zu berechnen. Einige davon sollen im Vortrag vorgestellt werden. [Wikipedia, Approximations of π, Kreiszahl]. (Eine interessante Variante, π näherungsweise zu ermitteln ist das Buffonsche Nadelproblem.)

(3) **RSA-Code**
Eines der einfachsten asymmetrischen Verschlüsselungsverfahren ist das von Rivest, Shamir und Adleman entwickelte RSA-Verfahren. Kodierung und Dekodierung erfolgt durch modulare Arithmetik, und die Sicherheit des Verfahrens beruht auf der angenommenen Schwierigkeit der Primfaktorzerlegung großer Zahlen. Literatur: [Wikipedia, RSA], aber RSA wird in jedem Buch zu Kodierungstheorie und Kryptographie behandelt. (Hier sind Vorkenntnisse in der Algebra hilfreich.)

(4) **Diskrete Logarithmen**
Ein ähnliches schwieriges Problem, das für Kryptoverfahren benutzt wird ist das diskrete Logarithmusproblem. Während potenzieren in modularer Arithmetik (in den Gruppen $\mathbb{Z}/n\mathbb{Z}$) relativ einfach ist, ist es typischerweise schwer, die Gleichung $a^x \equiv m \bmod p$ für gegebene a, m und p zu lösen. Diffie–Hellman-Schlüsselaustausch, Elgamal-Signatur und DSA-Verfahren basieren auf dem diskreten Logarithmusproblem. [Wikipedia, Diskreter Logarithmus, Diffie–Hellman, Elgamal, DSA] (Auch hier sind Vorkenntnisse in Algebra hilfreich.)

(5) **Quantencomputer**
Im Quantencomputer werden klassische Bits (die nur binäre Werte 0 und 1 annehmen) durch Qubits ersetzt, die quantenmechanische Effekte wie Superposition und Verschränkung benutzen, um Berechnungen durchzuführen. Dadurch können für klassische Computer schwierige Probleme auf einem Quantencomputer viel schneller gelöst werden; allerdings sind derzeit trotz intensiver Forschung die derzeitigen Umsetzungen des Konzepts noch weit von praktischer Anwendbarkeit entfernt. Ein Beispiel für einen Quantenalgorithmus ist der Algorithmus von Shor zur Primfaktorzerlegung großer Zahlen. [Wikipedia, Quantencomputer, Shor-Algorithmus] (Auch hier sind Vorkenntnisse in Algebra und eventuell Quantenmechanik hilfreich.)

(6) **Schwingungen und Abtasttheorem**

Das Abtasttheorem ist eine für die Signalverarbeitung und Informationstheorie zentrale Aussage, die Schranken für die Rekonstruierbarkeit von Signalen aus diskreten Abtastwerten beschreibt. Der Vortrag soll das Abtasttheorem beweisen und Anwendungen z.B. in der Audio-Signalverarbeitung erklären. [AB16, pp. 193–202], [Wikipedia, Nyquist–Shannon-Abtasttheorem] und Literaturreferenzen dort.

(7) **Audio-Kompression**

Kompressionsalgorithmen komprimieren Audio-Daten insbesondere durch Weglassen derjenigen Teile des Signalspektrums, die in psycho-akustischen Modellen als unwesentlich angesehen werden. Der Übergang vom Audio-Signal zum Spektrum wird dabei durch die modifizierte diskrete Kosinustransformation (MDCT) realisiert. Der Vortrag soll die Transformation erklären und die resultierenden Artefaktprobleme diskutieren. (In der Bildverarbeitung wird die diskrete Kosinustransformation z.B. beim JPEG-Format eingesetzt.)

[Wikipedia, MP3, MDCT] und Literaturreferenzen dort.

(8) **Fehlerkorrigierende Codes**

Zur Übertragung von Informationen über fehleranfällige Kanäle oder auch zur Speicherung von Information werden fehlererkennende und fehlerkorrigierende Codes eingesetzt. Solche Codes können in begrenztem Maße Übertragungsfehler erkennen oder sogar korrigieren. Bei sogenannten linearen Codes kann Codierung, Decodierung und Fehlerkorrektur mit den Methoden der linearen Algebra durchgeführt werden. Im Vortrag sollen verschiedene lineare Codes und ihre Eigenschaften vorgestellt werden. [AB16], [Wikipedia, Hamming-Code, BCH-Code, Reed–Solomon-Codes] und dortige Literaturreferenzen.

(9) **Matrixvervollständigung**

Audio- und Videostreamingdienste versuchen, Nutzerbewertungen vorherzusagen ("Nutzer, die Produkt A kaufen, sind auch interessiert an Produkt B"). Nutzerbewertungen können als Einträge einer unvollständigen Matrix gesehen werden, deren Zeilen die Nutzer und deren Spalten die Produkte sind. Matrixvervollständigung versucht, die fehlenden Einträge der Matrix zu ergänzen (unter der Annahme, dass der Rang der Matrix klein, oder die Matrix dünn besetzt ist). Ähnliche Probleme gibt es bei der Positionierung in Sensornetzwerken und anderen Situationen, der allgemeinere Überbegriff hierbei ist "compressed sensing". Der Vortrag soll die grundlegenden Techniken erläutern. [Wikipedia, matrix completion] und Literaturreferenzen dort.

(10) **PageRank-Algorithmus**

Suchmaschinen versuchen, die Wichtigkeit von Webseiten abzuschätzen. Wenn man die Wichtigkeit von Webseiten anhand der eingehenden Links schätzen will, hat man ein typisches Henne–Ei-Problem, wenn man die Wichtigkeit der verlinkenden Webseiten nicht kennt. Die Lösung ist, die Eigenvektoren zum größten Eigenwert der Link-Matrix zu finden. Das ist die Basis des PageRank-Algorithmus. [Wikipedia, PageRank] und Literaturreferenzen dort.

(11) **Logistische Differentialgleichung**

Eines der einfachsten Wachstumsmodelle der Biologie ist die logistische Differentialgleichung, eine nichtlineare gewöhnliche Differentialgleichung erster Ordnung, die mit den Mitteln der Analysis-Vorlesung gelöst werden kann. Etwas komplizierter sind die Lotka–Volterra-Gleichungen im Räuber-Beute-Modell, ein System von zwei nichtlinearen DGL erster Ordnung.

[Wikipedia, logistic function, Lotka–Volterra equations]

(12) **Spieltheorie und Nash-Gleichgewicht**

Spieltheorie kann helfen, Konfliktsituationen mathematisch zu formulieren und Lösungsstrategien zu untersuchen. Im Vortrag sollen die Grundbegriffe Spiel und reine bzw. gemischte Strategien definiert werden, und die Existenz von Nash-Gleichgewichten für gemischte Strategien soll gezeigt werden. Eines der bekanntesten Beispiele ist das Gefangenendilemma. [Wikipedia, Gefangenendilemma, Nash-Gleichgewicht] (Hier ist eventuell Topologie hilfreich, Fixpunktsatz von Brouwer.)

(13) **Satz vom Diktator**

Wahlverfahren kann man mathematisch analysieren. Verschiedene Kriterien an Abstimmungsverfahren können unvereinbar sein. In der Sozialwahltheorie (social choice and welfare) gibt es eine ganze Reihe solcher Sätze, deren bekanntester das Unmöglichkeitstheorem von Arrow ist. Im Vortrag soll der Satz erklärt und bewiesen werden. [Wikipedia, Arrow's impossibility theorem] und Literaturreferenzen dort.

Variante: Der Unmöglichkeitssatz von Balinski und Young ist ein Satz, der sagt, dass kein Sitzzuteilungsverfahren, existiert, dass verschiedene Paradoxien (wie z.B. negatives Stimmgewicht) vermeidet.

Variante: Analyse approval voting vs plurality voting, Gibbard's theorem

[AB16, Die Qual der Wahl – die Mathematik des Wählens]

(14) **Algorithmen zur Routenplanung**

Bei der Routenplanung geht es darum, den besten/schnellsten/kürzesten Weg zwischen zwei Orten A und B zu finden. Das Problem kann mit Graphentheorie formuliert werden, und der Algorithmus von Dijkstra ist eine Lösungsvariante.

[AB16, Der schnellste Weg zum Ziel] oder [Wikipedia, Dijkstra-Algorithmus]

(15) **Ebene Gelenke**

Das Ziel mechanischer Gelenkmechanismen ist die Transformation einer Kreisbewegung oder Pendelbewegung in eine lineare; allgemeiner kann man fragen, welche Bewegungen in der Ebene durch Gelenkmechanismen ausgeführt werden können. Die Transformation von Pendelbewegung in lineare Bewegung wird durch das Peaucellier–Lipkin-Gelenk bewerkstelligt. Allgemein besagt der Universalitätssatz von Kempe, dass jede beschränkte Teilmenge einer algebraischen Kurve (d.h. beschrieben durch Polynome) durch ein ebenes Gelenk modelliert werden kann. Am Beispiel der Ellipse kann man sehen, dass diese Gelenke unter Umständen sehr kompliziert werden können.

[Wikipedia, Planar linkages, Peaucellier–Lipkin linkage, Kempe universality] und Literaturverweise dort.

s. auch A practical implementation of Kempe's universality theorem.
`https://courses.csail.mit.edu/6.849/fall12/kempe-sim/project.pdf`

(16) **Origami**

Die japanische Papierfalttechnik kann für geometrische Konstruktionen benutzt werden, die nicht mit Zirkel und Lineal durchführbar sind. Der Vortrag sollte die Würfelverdopplung und die Winkeldreiteilung durch Origami erklären. [Henn]

(17) **Polygone mit einem Schnitt**

Man kann jedes Polygon erhalten, indem ein Stück Papier gefaltet wird und *einmal* gerade durchgeschnitten wird. Der Vortrag sollte diesen Satz erklären, gern an Beispielen verdeutlichen (`erikdemaine.org/foldcut/`) und soweit möglich beweisen. [DO07]. (Alternativ hat das Buch von Demaine und O'Rourke natürlich auch noch viele andere interessante Sachen zu bieten.)

(18) **Knoten**

Im Vortrag soll eine kurze Einführung in die Mathematik der Knoten gegeben werden, wie Knoten mathematisch modelliert werden, und wie man verschiedene Knoten voneinander unterscheiden kann. [AB16, Die Mathematik der Knoten]

(19) **Computer-Tomographie oder Kernspin-Tomographie**

Für die Computer-Tomographie wird ein Körper aus verschiedenen Richtungen mit Röntgenstrahlen durchleuchtet (Einsatz in der Medizin und der Materialprüfung). Die gemessenen Strahlungsverluste nach Durchlaufen des Körpers können als Radon-Transformierte der Dichtefunktion des Körpers interpretiert werden. Das Invertieren der Radon-Transformation erlaubt, die Dichtefunktion des Körpers zu rekonstruieren.

alternatives Thema: Kernspin-Tomographie. Im Kernspin-Tomographen werden Wasserstoffatomkerne durch Magnetfelder angeregt. Mit Fouriertransformation kann aus den gemessenen elektromagnetischen Felder der angeregten Atome eine Dichtefunktion der Wasserstoffkerne im Körper ermittelt werden.

[Wikipedia, Computertomographie, CT scan, Radon transform bzw. nuclear magnetic resonance, magnetic resonance imaging], [Dea93, Kapitel 1.7, 2.2, 5.3], benötigt Vorkenntnisse aus Analysis III. [AB16, Diskrete Tomographie]

(20) **Newcomb–Benford-Gesetz**

In empirischen Datensätzen (insbesondere Steuererklärung oder allgemeiner Buchhaltungsdaten) treten Anfangsziffern der Zahlensätze nicht gleich häufig auf. Das Newcomb–Benford-Gesetz, das diese Erfahrung formuliert, wird benutzt, um Steuerhinterziehung, Wirtschaftskriminalität oder allgemeinere Datenmanipulation zu identifizieren. [Wikipedia, Benfordsches Gesetz/Benford's law] und Literaturverweise dort.

Literatur

[AB16] M. Aigner, E. Behrends (Hrsg.). Alles Mathematik – von Pythagoras zu Big Data, Springer 2016.

[Dea93] S. Deans. The Radon transform and some of its applications. Krieger 1993.

[DO07] E. Demaine and J. O'Rourke. Geometric folding algorithms: linkages, origami, polyhedra. Cambridge University Press, 2007.

[Henn] H.-W. Henn. Origamics. Papierfalten mit mathematischem Spürsinn.
`http://www.mathematik.uni-dortmund.de/ieem/_personelles/people/henn/origa_hd.pdf`

[Wikipedia] Wikipedia: The free encyclopedia, Wikimedia foundation.
`http://en.wikipedia.org/` oder `http://de.wikipedia.org/`