Proseminar: Mathematik der Kommunikation

Dr. Alexandr Polujan

Kurze Beschreibung des Inhalts

In der modernen Gesellschaft ist ein Großteil unserer Kommunikation digital: Jeden Tag nutzen wir intelligente Geräte, um Nachrichten zu senden und zu empfangen, QR-Codes zu scannen oder Transaktionen mit Debit- und Kreditkarten durchzuführen. Möglich wird dieser Fortschritt nicht nur durch jahrzehntelange Entwicklungen in Technik, Ingenieurwesen und Software, sondern auch durch die Mathematik. In diesem Proseminar werden einige dieser Verfahren vorgestellt, die häufig auf "einfachen" Ideen aus Algebra, Kombinatorik und diskreter Mathematik beruhen.

Blockstruktur und vorläufiger Zeitplan

Das Proseminar ist als Blockveranstaltung geplant. In jedem Block werden ausgewählte Themen aus der Mathematik der Kommunikation behandelt. Jeder Block umfasst zwei oder drei spezifische Themen. Ein vorläufiger Plan ist wie folgt:

Block I: Fehlerkorrigierende Codes (Freitag, 24. April)

1. Fehlerkorrigierende Codes und das zentrale Problem der Codierungstheorie
2. Endliche Körper und Vektorräume über endlichen Körpern
3. Lineare Codes, Reed-Muller-Codes und Hadamard-Matrizen

Block II: Codes, Kodierung und Dekodierung (Freitag, 29. Mai)

4. Kodierung und Dekodierung mit einem linearen Code
5. Der duale Code, die Prüfmatrix und Syndromdekodierung
6. Anwendungen im Alltag

Block III: Kryptographie – Symmetrische Kryptographie I (Freitag, 5. Juni)

7. Kryptographie und Sicherheit: Grundbegriffe und historische Chiffren
8. Symmetrische Kryptographie – AES-Verschlüsselung
9. Was ist eine kryptographische Boolesche Funktion?

Block IV: Kryptographie – Asymmetrische (Public-Key-)Kryptographie (Freitag, 26. Juni)

10. Asymmetrische vs. symmetrische Kryptographie und Grundprinzipien der Public-Key-Kryptographie
11. Das RSA-Kryptosystem
12. Public-Key-Kryptosysteme auf Basis des diskreten Logarithmusproblems

Block V: Abschließende Themen (Freitag, 3. Juli)

13. Elliptische Kurven
14. ENIGMA, Turing und COLOSSUS

Literatur

Die genannten Themen entsprechen hauptsächlich ausgewählten Kapiteln aus den folgenden Büchern, Artikeln und Skripten. Die überwiegende Mehrheit dieser Referenzen (mit möglicher Ausnahme von [3]) ist frei im Internet verfügbar oder über einen Universitätszugang zugänglich:

1. Martin Aigner, *Diskrete Mathematik*, 6. Auflage, Vieweg+Teubner Verlag Wiesbaden, 2006, XI, 356 Seiten. Link.
2. Raymond Hill, *A First Course in Coding Theory*, Oxford University Press, Oxford, 1986, xii, 251 pages. Link
3. F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977, xv+762 pages.
4. Wolfgang Willems, *Codierungstheorie und Kryptographie*, Birkhäuser Basel, 2008, XII, 152 Seiten. Link
5. Franck Jeannot. QR Code Model 2 Structure and Algorithms. 18 Seiten Link
6. Christof Paar, Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer Berlin, Heidelberg, 2010, XVIII, 372 pages. Link
7. Joachim von zur Gathen, *CryptoSchool*, Springer Berlin, Heidelberg, 2015, XII, 876 pages. Link
8. Lilya Budaghyan, Pantelimon Stănică, *What is ... a Cryptographic Boolean function?*, Notices of the American Mathematical Society 66 (1), 2019, 60–63. Link
9. Anne Canteaut, *Lecture Notes on Cryptographic Boolean Functions*, Lecture notes, 2016, approx. 48 pages. Link
10. J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, 2nd edition, Cambridge University Press, Cambridge, 2001, xvi+602 pages. Link

Voraussetzungen

Die einzelnen Themen sind in sich abgeschlossen, und es werden keine speziellen Lehrveranstaltungen im Vorfeld vorausgesetzt. Der vorherige Besuch einer Veranstaltung zur diskreten Mathematik und Algebra ist jedoch hilfreich.

Veranstaltungsformat und Anforderungen

Eine Motivation für die Organisation des Proseminars als Blockveranstaltung – neben der Konzentration auf spezifische Themen an festgelegten Terminen – ist die Simulation eines typischen Tages auf einer (mathematischen) Konferenz. Ein solcher Tag gilt in der Regel als gelungen, wenn alle Beteiligten aktiv eingebunden sind: die Vortragenden durch einen guten Vortrag und das Publikum durch aufmerksames Zuhören und das Stellen von Fragen.

Um das Proseminar erfolgreich zu bestehen, gelten die folgenden Anforderungen:

1. Ein Vortrag (60 Minuten) zu einem der ausgewählten Themen mit anschließender Beantwortung von mindestens 3 Fragen aus dem Publikum (Diskussionsrunde von 15 Minuten).
2. Teilnahme an mindestens 10 von 14 Vorträgen, die nicht der eigene sind. Bei Teilnahme an weniger als 10 Vorträgen ist ein schriftlicher Bericht über die versäumten Vorträge zu verfassen (mindestens 5 Seiten pro versäumtem Vortrag bei angemessener Schriftgröße und Seitenrändern). Berichte, die als KI-generiert identifiziert werden, werden nicht akzeptiert.
3. Stellen von mindestens 3 Fragen im Laufe des Semesters; dabei wird jedoch höchstens 1 Frage pro Block gezählt, was die Teilnahme an mindestens 3 verschiedenen Blöcken voraussetzt.

Die erforderliche Anzahl an Fragen sowie die Anzahl der zu besuchenden Vorträge kann abhängig von der Zahl der angemeldeten Teilnehmer:innen angepasst werden.

Anmeldung

- Die Anzahl der verfügbaren Seminarplätze ist auf 14 begrenzt.
- Etwa am 16. Februar werden weitere Details zu den Themen bekannt gegeben, einschließlich Hinweisen zu relevanten Abschnitten der Literatur und zu den Schwerpunkten der Vorträge.
- Die Anmeldung ist vom 23. Februar bis zum 24. März möglich. Sobald bei der Anmeldung ein Thema ausgewählt wird, ist dieses für andere nicht mehr verfügbar.
- Details zum Anmeldeformat (per E-Mail oder über ein Formular auf ovgu.cloud) werden ebenfalls etwa am 16. Februar mitgeteilt.