Herbsttagung 2010

der

MATHEMATISCHEN GESELLSCHAFT IN HAMBURG

GEGRÜNDET 1690

zusammen mit dem
Fachbereich Mathematik
der Universität Hamburg

Endliche Strukturen und Algorithmen

Freitag und Samstag, 12. und 13. November 2010
Geomatikum, Hörsäle H4 und H1
Bundesstraße 55, 20146 Hamburg

*****

Herbsttagung 2010

Endliche Strukturen und Algorithmen

Freitag, 12. November 2010, Hörsaal 4 (Geomatikum)

15:00 h	Begrüßung und Einführung
15:05 – 15:55 h	Albrecht Beutelspacher *Die Erfindung der Public-Key-Kryptographie*
16:00 – 16:30 h	Kaffeepause

Freitag, 12. November 2010, Hörsaal 1 (Geomatikum)

16:30 –17:20 h	Hubert Kiechle *Können Sie ein Geheimnis für sich behalten?*
17:30 – 18:20 h	Gerhard Tischel *Endliche algebraische Strukturen im Mathematikunterricht*
ab ca. 19:30 h	Nachsitzung im Hotel „Hafen Hamburg“, Seewartenstraße 9, 20459 Hamburg. Für das Essen wird ein Unkostenbeitrag von EUR 27,00 erhoben

Samstag, 13. November 2010, Hörsaal 1

10:00 – 10:50 h	Stephan Hußmann *„Gut – besser – am besten“ – Ein studierenden- und problemorientierter Zugang zur kombinatorischen Optimierung*
10:50 – 11:20 h	Kaffeepause
11:20 – 12:05 h	Walther Parson *Die mitochondriale Datenbank EMPOP im Schnittpunkt von Genetik, Mathematik und Informatik und ihre Rolle in der Gerichtsmedizin*
12:05 – 12:50 h	Hans-Jürgen Bandelt *Das algebraische Dual einer Sequenzdatentabelle und seine Realisierung als Graph*

Albrecht Beutelspacher
Universität Gießen

Die Erfindung der Public-Key-Kryptographie

Die Erfindung der Public-Key-Kryptographie in den 70er Jahren des 20. Jahrhunderts stellt eine Revolution dar, die weit über die Mathematik hinausreicht. Mit Hilfe der Public-Key-Kryptographie sind Verfahren möglich, an die man vorher nicht zu denken gewagt hat: Sicherheit im Internet, elektronisches Bezahlen, elektronische Wahlen usw. Diese Erfindung hat ebenfalls eine Fülle von Anwendungen möglich gemacht und nicht zuletzt scheinbar „reinste“ Mathematik (nämlich Primzahlen) ins Zentrum der Anwendungen katapultiert. Die Grundzüge dieser Entwicklungen lassen sich auf Schulniveau behandeln, das soll in diesem Vortrag dargestellt werden.

*****

Hubert Kiechle
Universität Hamburg

Können Sie ein Geheimnis für sich behalten?

Können Sie? Hier sind natürlich nicht die kleinen Geheimnisse des täglichen Lebens gemeint; sondern Geheimnisse wie sie in der Kryptographie vorkommen, etwa Passwörter, PINs usw.
Eine alltägliche Situation: Sie stehen vor dem Geldautomaten, stecken Ihre Karte in den Schlitz und geben dann die PIN ein. Um die Maschine zu nutzen, müssen Sie Ihr Geheimnis der Maschine preisgeben! Kann man das vermeiden? Etwas schärfer und präziser gefragt: Kann man eine Instanz davon überzeugen, ein Geheimnis zu besitzen, ohne es preisgeben zu müssen, ohne überhaupt Information preisgeben zu müssen? Mit dieser Frage beschäftigt sich der Vortrag.

*****

Gerhard Tischel
Hamburg

Endliche algebraische Strukturen im Mathematikunterricht

Die sehr starke Betonung von Modellierungen im Mathematikunterricht hat dazu geführt, dass algebraische Strukturen im Mathematikunterricht an der Schule gar nicht mehr vorkommen. Damit wird ein wesentlicher Aspekt der Mathematik aus dem Schulunterricht ganz ausgeblendet. Der Vortrag möchte Möglichkeiten aufzeigen, einfache algebraische Begriffe wie Gruppe und Körper im MU zu behandeln. Ausgangspunkt sind folgende Überlegungen: Im sogenannten Algebra-Unterricht in den Klassen 7 bis 10 lernen die Schüler u.a. lineare Gleichungen, lineare Gleichungssysteme und quadratische Gleichungen zu lösen. Das intensive Einüben von Lösungsverfahren verschüttet dabei oft die algebraischen Grundlagen der Lösungsverfahren. Das Lösen der genannten Gleichungstypen in endlichen Körpern erfordert eine Besinnung auf diese Grundlagen und ist eine gute Möglichkeit für eine vertiefende Wiederholung. Zugleich werden dabei neue mathematische Fenster aufgestoßen. Der Unterricht kann sich dabei an sinnstiftenden Aufgaben orientieren. Im Vortrag werden additive, multiplikative und exponentielle Verschlüsselung von Texten und ihre geometrische Deutung behandelt.

*****

Stephan Hußmann
Universität Dortmund

„Gut – besser – am besten“ –
Ein studierenden- und problemorientierter Zugang zur kombinatorischen Optimierung

Wie kann man eine Vorlesung so gestalten, dass Studierende am eigenen Leib erleben, was es bedeutet, mathematisch tätig zu sein? Das ist sicher keine kleine Herausforderung, da viele Errungenschaft der Mathematik nicht individuell nacherfunden werden können und auch die Stofffülle nicht unbedingt gestattet, lange Phasen der Eigenaktivität an die Studierenden abzugeben. Doch ist es andererseits insbesondere für Lehramtsstudierende wichtig, Mathematik als aktiven Prozess zu erleben, d.h. insbesondere: Wie findet man ein mathematisches Modell, wie formuliert man eine geeignete Definition, die präzise genug ist, welche Bedeutung haben mathematische Sätze und wie beweist man sie? Und alles vor dem Hintergrund,

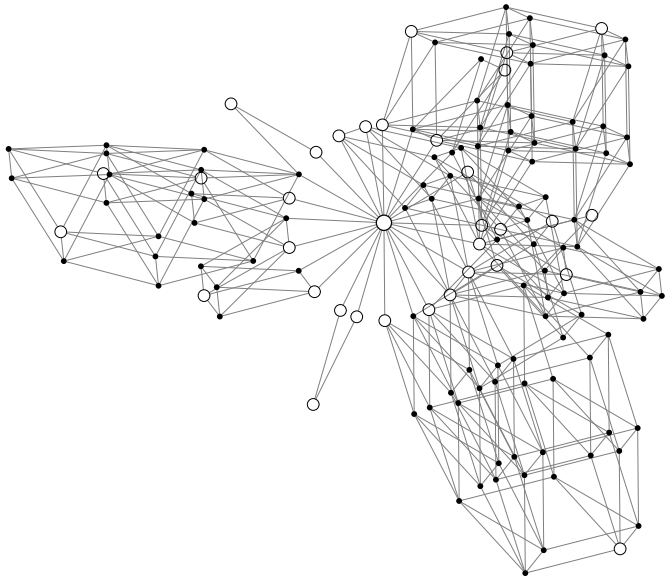
dass Mathematik Antworten auf reale Probleme geben kann. Am Beispiel einer Vorlesung für Lehramtsstudierende wird ein problemorientierter Zugang zur diskreten Mathematik vorgestellt, der wesentlich auf Aktivitäten der Studierenden aufbaut.

*****

Walther Parson
Universität Innsbruck

Die mitochondriale Datenbank EMPOP im Schnittpunkt von Genetik, Mathematik und Informatik und ihre Rolle in der Gerichtsmedizin

Die gerichtsmedizinische Untersuchung der so genannten mitochondrialen DNA (mtDNA) spielt bei schwierigen bzw. sehr kleinen biologischen Proben eine Rolle, wie zum Beispiel bei menschlichen Haarschaftanteilen. Die mtDNA wird ausschließlich über die mütterliche Linie vererbt, weshalb ihre relative Häufigkeit in der Bevölkerung für die Würdigung des Beweiswertes vor Gericht durch eine mtDNA Datenbankabfrage bestimmt wird. MtDNA Datenbanken erwiesen sich in der Vergangenheit als sehr fehleranfällig, da sie meist ohne Einhaltung der erforderlichen Qualitätsmaßstäbe erstellt und später bei Erkennen der Fehler nicht korrigiert wurden. Häufigkeitsrecherchen in mangelhaften mtDNA Datenbanken reduzieren artifiziell die relative Häufigkeit einer mtDNA Sequenz, erhöhen damit den Hinweischarakter einer biologischen Spur in einem Kriminaldelikt und wirken sich damit nachteilig für den Angeklagten aus. Mit dem internationalen Projekt EMPOP wird ein neuer Weg beschritten. Neben der Einführung eines verbesserten Labormanagementsystems werden als zusätzliche Qualitätskontrolle der Labordaten mathematische Methoden angewandt. Besonders effektiv ist die grafische Darstellung von Teilen der mtDNA Sequenzen durch quasi-mediane Netzwerke, die bei Vorliegen qualitativ hochwertiger Daten fast sternhaft sind. Fehlerhafte Datensätze erhöhen in der Regel die Komplexität des Netzwerkes erheblich, womit Fehler entlarvt werden können.



*****

Hans-Jürgen Bandelt
Universität Hamburg

Das algebraische Dual einer Sequenzdatentabelle und seine Realisierung als Graph

Sequenzdaten über einem Alphabet (wie z.B. alignierte DNA Sequenzen) erzeugen mittels einer gewissen ternären Operation eine Struktur, die man sowohl als algebraisches Dual als auch als Graph (bzw. Netzwerk) interpretieren kann. Biologisch relevante Eigenschaften der Daten werden so in algebraische bzw. kombinatorische Eigenschaften des Graphen übersetzt. Für eine Spezialklasse läßt sich diese Dualität auch geometrisch in der hyperbolischen Ebene realisieren, was algorithmisch für das automatische Zeichnen solcher Graphen relevant ist. Die von Sequenzdaten erzeugten ternären Algebren bilden eine sogenannte reine Dual-Diskriminator-Varietät, bei der die Teilalphabete versehen mit dem dualen Diskriminator die einzigen subdirekt Irreduziblen sind. Setzte man statt des dualen Diskriminators den Diskriminator auf dem Alphabet ein, so wäre die zugehörige Varietät zwar nicht mehr biologisch von Interesse, korrespondierte aber zur sogenannten schiefen Booleschen Logik über diesem Alphabet (wenn man zusätzlich eine Konstante auszeichnet).