



Forschung an der Fakultät für Technische Mathematik und Technische Physik

Nationales Forschungsnetzwerk: Analytische Kombinatorik und Probabilistische Zahlentheorie *National Research Network: Analytic Combinatorics and Probabilistic Number Theory*

Kombinatorik und Zahlentheorie sind klassische Gebiete der Mathematik, die immer aktuell waren und sind. In jüngerer Zeit hat etwa die Entwicklung der Computerwissenschaften für diese Gebiete einerseits neue Anwendungsfelder erschlossen (wie die Kryptographie), andererseits aber auch neue theoretische Fragen aufgeworfen (z.B. die Komplexität von Algorithmen). Dabei wird der klassische methodische Rahmen mehr und mehr gesprengt. So spielen etwa wahrscheinlichkeitstheoretische Ansätze, analytische Verfahren und

dynamische Systeme eine immer wichtiger werdende Rolle, um kombinatorische und zahlentheoretische Objekte zu quantifizieren. Dieses vom FWF geförderte Forschungsnetzwerk bündelt mehrere dieser in Österreich stark verankerten Gebiete: Enumerative Kombinatorik, diskrete Wahrscheinlichkeitstheorie, probabilistische Analyse von Algorithmen, dynamische Systeme und Diskrepanztheorie. Dabei spannt sich der Bogen von theoretischen Fragestellungen, wie etwa wahrscheinlichkeitstheoretische Untersuchungen von speziellen Folgen

und deren Zusammenhang mit diophantischen Gleichungen, bis zu anwendungsorientierten Problemen, wie zum Beispiel die Konstruktion gleichverteilter Folgen zur numerischen Integration.

Die zehn Forschungsgruppen des Netzwerks verteilen sich auf die Universitäten von Graz (TU), Leoben, Linz, Salzburg, Wien (Univ. und TU). Die Koordination der Aktivitäten erfolgt durch M. Drmota (TU Wien) und P. Grabner (TU Graz).

Vier der Gruppen sind an der TU Graz situiert:

- Probabilistic Discrepancy Theory and Diophantine Equations (I. Berkes am Institut für Statistik; R. Tichy am Institut für Analysis und Computational Number Theory). Bei der genauen Untersuchung der Verteilungseigenschaften von Teilfolgen der $n\alpha$ -Folgen ist der Fall subexponentiellen Wachstums eine der letzten Herausforderungen: Hier spielen diophantische Eigenschaften der Teilfolge eine entscheidende Rolle. *Number Theory meets Probability*.
- Combinatorics and Dynamics of Numeration Systems (P. Grabner am Institut für Analysis und Computational Number Theory). Kombinatorische Eigenschaften von allgemeinen Ziffernentwicklungen werden in probabilistische und dynamische Eigenschaften eines geeignet konstruierten dynamischen Systems (Odometer) übersetzt. Dabei auch entsprechende Kompaktifizierungen der natürlichen Zahlen studiert, deren klassische Analoga bei der Untersuchung arithmetischer Funktionen verwendet wurden.
- Analysis of Digital Expansions with Applications in Cryptography (C. Heuberger am Institut für Optimierung und Diskrete Mathematik; P. Grabner). Einige moderne kryptographische

Verfahren beruhen auf effizienter Arithmetik in der Punktgruppe einer elliptischen Kurve. Dies kann unter anderem durch Einsatz redundanter Ziffernentwicklungen beschleunigt werden. Deren Design und präzise probabilistische Analyse bilden den Schwerpunkt dieses Teilprojekts.

- The Hardy-Littlewood Method in the Analysis of Digit Problems and Enumerative Combinatorics (R. Tichy, J. Thuswaldner an der Montanuniversität Leoben). Es werden zahlentheoretische Eigenschaften von Mengen, die durch Zifferneigenschaften charakterisiert sind, und die Kombinatorik von graphentheoretischen Indizes, die in der theoretischen Chemie von Interesse sind, untersucht. Erstaunlicherweise können diese völlig verschiedenen Fragestellungen mit ähnlichen Methoden behandelt werden.

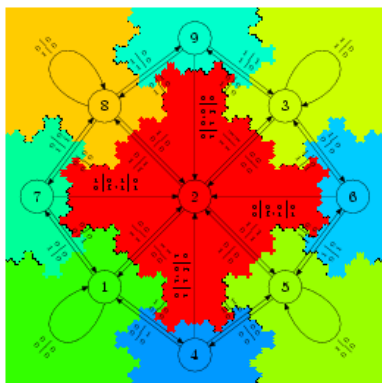
Über die aktive Forschungstätigkeit hinaus hat das Netzwerk auch eine starke Ausbildungskomponente: Die Teilprojekte beschäftigen Doktoranden und junge Post-Docs, die international rekrutiert wurden. Die Kooperation mit führenden internationalen Experten wird durch ein gut ausgestattetes Gästeprogramm ermöglicht. Jedes der drei Jahre der ersten Antragsphase steht unter einem Generalthema, zu dem jeweils eine Summer School und ein oder mehrere Workshops veranstaltet werden: Probabilistische Methoden in der Kombinatorik (2006: Summer School und Workshop in Mariatrost), Dynamische Systeme und Zahlentheorie (2007: Journées de Numération, Graz sowie ein Workshop in Strobl und eine Summer School in Graz), Enumerative Kombinatorik (2008: Programm Combinatorics and Statistical Physics in Zusammenarbeit mit dem Erwin-Schrödinger-Institut in Wien).

National Research Network: Analytic Combinatorics and Probabilistic Number Theory

This National Research Network funded by the FWF comprises ten groups in active research areas ranging from enumerative combinatorics, discrete probability and probabilistic analysis of algorithms to dynamical systems and discrepancy theory. The groups are situated in Vienna, Linz, Leoben, Salzburg, and Graz.

Four of these research groups are based at TU Graz: Probabilistic Discrepancy Theory and Diophantine Equations (I. Berkes, R. Tichy), Combinatorics and Dynamics of Numeration Systems (P. Grabner), Analysis of Digital Expansions with Applications in Cryptography (C. Heuberger, P. Grabner), The Hardy-Littlewood Method in the Analysis of Digit Problems and Enumerative Combinatorics (R. Tichy, J. Thuswaldner).

The network has a strong educational component: The research projects offer positions for doctorands and young post-docs, recruited internationally. A generous guest program allows cooperations with leading international experts. Each of the three years of the program is focussed on one major aspect, which serves as a theme for a summer school and one or more workshops: Probabilistic Methods in Combinatorics (2006), Dynamical Systems and Number Theory (2007), Enumerative Combinatorics (2008).



Charakteristische Mengen der Simple Joint Sparse Form und zugehöriger Transducer.