DOCTORAL PROGRAM
DISCRETE MATHEMATICS
TU & KFU GRAZ • MU LEOBEN
AUSTRIA

Graz University of Technology

DK: Doctoral Program in Discrete Mathematics

Univ.-Prof. Dr. W. Woess
Speaker

Univ.-Prof. Dr. A. Geroldinger
Univ.-Prof. Dr. J. Thuswaldner
Deputy Speakers

Steyrergasse 30/III
A-8010 Graz
Austria

Tel. +43(0)316 873-7132
Fax +43(0)316 873-4507

discrete@tugraz.at
www.math.tugraz.at/discrete

DVR: 008 1833 UID: ATU 574 77 929

Graz, Mai 2012

DISCRETE MATHEMATICS DAY 2012

Friday, June 1, 2012, 09:15-16:00
Lecture hall **BE01**, Steyrgasse 30, EG, TU Graz

Program

$09^{15} - 09^{30}$	Opening
$09^{30} - 10^{20}$	Michał Karoński (Poznan, Poland) *Random Web Graphs*
$10^{20} - 10^{40}$	DK Talk: Johannes Cuno (TU Graz) *Either large or small: The Tits alternative for non-spherical Pride groups*
$10^{40} - 11^{10}$	**Coffee break**
$11^{10} - 11^{30}$	DK Talk: Daniel Smertnig (KFU Graz) *Title: Sets of lengths in maximal orders of central simple algebras*
$11^{30} - 12^{20}$	Mihyun Kang (TU Graz) *Phase transition in random discrete structures.*
$12^{30} - 14^{00}$	**Lunch break (buffet in the front of BE01)**
$14^{00} - 14^{20}$	DK Talk: Daniel Krenn (TU Graz) *Counting digits in Non-Adjacent Forms in Conjunction with Hyperelliptic Curve Cryptography*
$14^{20} - 15^{10}$	Karin Baur (KFU Graz) *A frieze (pattern) determinant.*
$15^{10} - 16^{00}$	**Coffee break and poster session** *Posters by: Dijana Kreso, Tetiana Boiko, Alina Bazarova, Marko Raseta*

Abstracts of the talks

- 9:30 - 10:20 **Michał Karoński (Adam Mickiewicz University, Poznan, Poland)**
  Title: Random Web Graphs
  Abstract: Paul Erdős, one of the greatest mathematicians of the twentieth century, was a champion of applications of probabilistic methods in many areas of mathematics, such as graph theory, combinatorics and number theory. He also, almost fifty years ago, jointly with another great Hungarian mathematician Alfred Rényi, laid out foundation of the theory of random graphs: the theory which studies how large and complex systems evolve when randomness of the relations between their elements is incurred. In my talk I'll sketch the long journey of this theory from the pioneering Erdős - Rényi era to modern attempts to model properties of large real-world networks which grow unpredictably, including the Internet, WorldWideWeb (WWW) and social networks.

- 10:20 -10:40 **Johannes Cuno (TU Graz)**
  Title: Either large or small: The Tits alternative for non-spherical Pride groups
  Abstract: In combinatorial group theory one thinks of groups being given in terms of generators and defining relations. After some introductory examples we turn to Pride groups. These are groups with the property that, roughly speaking, each defining relation involves at most two types of generators. We motivate and discuss the question under which conditions non-spherical Pride groups either contain a non-abelian free subgroup or are virtually solvable.

- 11:10 - 11:30 **Daniel Smertnig (KFU Graz)**
  Title: Sets of lengths in maximal orders of central simple algebras
  Abstract: There is a long tradition in studying arithmetical invariants related to the factorization of elements into irreducibles in commutative rings and monoids. However, the same problems arise naturally also in a non-commutative setting: If R is a maximal order in a central simple algebra over a number field (e.g., in a quaternion algebra), and $x \in R^\bullet$, then the set of lengths of x consists of all those natural numbers l for which there exists a factorization $x = u_1 \cdot \ldots \cdot u_l$ into irreducibles. In a large number of cases (including everything but totally definite quaternion algebras), these sets can be studied in the same way as in the commutative setting, while in the remaining cases explicit constructions show very different behaviour.

- 11:30 - 12:20 **Mihyun Kang (TU Graz)**
  Title: Phase transition in random discrete structures
  Abstract: Random discrete structures have been extensively studied during the last few decades and have become one of the central themes of contemporary (discrete) mathematics. This is partly because they are useful for modeling, analysing and solving structural and algorithmic problems arising from mathematics, theoretical computer science and natural sciences, and they provide a wide potential range of applications. The most important and popular example of random discrete structures is random graphs.

  A fascinating phenomenon observed in various contexts is the phase transition and critical behaviour. The phase transition deals with an abrupt change in the properties of an asymptotically large structure by altering critical parameters. The phase transition in random discrete structure has captured the attention of many scientists, and the intense study has brought together different fields such as discrete mathematics, probability theory and theoretical computer science as well as statistical physics. This talk provides a gentle introduction to the phase transition in random discrete structures including Ising model, random walks, random satisfiability problems and random graphs.

- 14:00 - 14:20 **Daniel Krenn (TU Graz)**
  Counting digits in Non-Adjacent Forms in Conjunction with Hyperelliptic Curve Cryptography
  Abstract: One main operation in hyperelliptic curve cryptography is building multiples of a point on a hyperelliptic curve over a finite field. For a class of curves we can use a Frobenius-and-add method. In order to do that efficiently we need to understand digital expansions, where the base is an algebraic integer whose conjugates all have the same absolute value. The talk will be about the existence of "good" expansions (non-adjacent forms) and about the number of occurrences of digits in such expansions.

- 14:20 - 15:10 **Karin Baur (KFU Graz)**: *Title: A frieze (pattern) determinant*
  Abstract: Frieze patterns are designs on a two-dimensional surface which are repetitive in one direction (as opposed to tilings). The term frieze is used in architecture. Many examples of friezes can be found in the Alhambra in Spain. Frieze patterns exhibit different types of symmetries, the simplest being a translation. We are interested in frieze patterns of numbers which are invariant under a glide reflection. They have been studied by Conway and Coxeter in the 70's who showed that such frieze patterns arise from triangulations of polygons.

  Broline, Crow and Isaacs have computed the determinant of a matrix associated to a frieze pattern. In joint work with R. Marsh we generalize their result to the corresponding frieze pattern of cluster variables arising from a cluster algebra of type A. Time permitted we will give a representation-theoretic interpretation of this result in terms of configurations of indecomposable objects in the root category of type A.