PHD COURSES 2020/2021

- Group-theoretical cryptanalysis of block ciphers and alternative actions

  Lecturer: Roberto Civino, 10 hours

  Program: The course is focused on some group-theoretical techniques for the cryptanalysis of block ciphers. After having introduced the mathematical model describing block ciphers and after having explained the classical attack scenarios, we will study the group-theoretical properties that can be turned into key-recovery attacks. In particular, the main focus will be on two undesirable properties of a group closely related to the set of the encryption functions, i.e. the imprimitivity and the property of being of affine type. In the second case, we also explain a variation of the classical differential attack, one of the most popular attacks against block ciphers, which makes use of alternative actions on the message space coming from different translation groups. Both theoretical and practical aspects will be covered.

  Lect. 1: Introduction to block ciphers, the framework of SPN, differential cryptanalysis;

  Lect. 2: The group generated by the round functions, properties, construction, known attacks: the imprimitive case and the affine case;

  Lect. 3: Differential cryptanalysis using alternative actions: theoretical aspects;

  Lect. 4: Differential cryptanalysis using alternative actions: practical aspects;

  Lect. 5: The study of the translation group and its conjugates as subgroups of the Sylow 2-subgroup of the symmetric group.

- Operator semigroups and applications

  Lecturer: Klaus Engel (`klaus.engel@univaq.it`), 6 hours

  Program: The theory of one-parameter semigroups of bounded linear operators on a Banach space provides a powerful tool to study, in a systematic and unified way, the well-posedness of a wide range of linear evolution equations. Moreover, it allows to obtain detailed information about the qualitative properties of the solutions like long-time behavior or positivity.

  The aim of this short course, consisting of 3 lectures, is to give a brief introduction into this subject and to sketch some application. To this end the first part recalls the necessary notions from functional analysis and operator theory. In the second part the basic results of the abstract theory are presented and illustrated by some standard examples. Finally, these abstract results are applied to study the well-posedness and the qualitative properties of the solutions of some concrete evolution equation.

  References (cf. www.math.uni-tuebingen.de/de/forschung/agfa/members/rana)

  * K.-J. Engel, R. Nagel. One-Parameter Semigroups for Linear Evolution Equations, Graduate Texts in Mathematics, vol. 194. Springer-Verlag, 2000.

  or (short version, less applications)

  * K.-J. Engel, R. Nagel. A Short Course on Operator Semigroups, Universitext. Springer-Verlag, 2006.

- Introduction to Optimal Control

  Lecturer: Teresa Scarinci (`teresa.scarinci@univaq.it`), 6 hours

  Program: The course aims to offer some theoretical concepts in optimal control:

  1. necessary and sufficient conditions for optimality, and various types of constraints

  2. Hamilton-jacobi bellman equations and viscosity solutions

  3. Pontryagin maximum principle

  4. sufficient conditions for local optimality for singular optimal controls: higher order conditions such as the generalized Legendre-Clebsch conditions

  If time permits:

  5. an introduction to optimal control of elliptic PDEs (existence of optimal solutions, necessary optimality conditions and adjoint equations)

- Convex components

  Lecturer: Flavia Giannetti (`giannett@unina.it`), 6 hours

  Program: The aim of the course is to discuss the following question. For a closed bounded set $E \subset \mathbb{R}^2$, it is clear that a decomposition of E of the form

  $$E = \bigcup_{i=1}^{k} E_i,$$

  where $\{E_i\}_{i=1,\dots,k}$ is a family of closed convex sets is not unique. Therefore the problem to estimate from below the minimal number k_{min} of the convex components of E that may exist arises naturally. It will be shown that the following well known monotonicity property of the perimeter

  $$\mathcal{H}^1(\partial A) \leqslant \mathcal{H}^1(\partial B),$$

  for bounded convex sets $A \subset B \subset \mathbb{R}^2$, revealed to be a key tool in the proof of the estimate we are interested to determine.

- Spectral theory on manifolds

  Lecturer: Prof. Gilles Courtois (CNRS, Paris 6), 8 hours

  Program: The goal of this course is to give an introduction to the Laplace operator on manifolds. In the first part of the course, we will focus on relations between the eigenvalues of the Laplace operator on functions and the geometry of the manifold. Among these, classical Theorems illustrate the interplay between the isoperimetric problem and the first positive eigenvalue of the Laplacian on functions, for example the Faber-Krahn inequality or the Cheeger inequality. In the second part of the course, the case of the Hodge de Rham Laplacian acting on differential form will be considered with the perspective of investigating what become the classical Theorems in this context.

- Perturbative Methods for the Stability Analysis of Dynamical Systems

  Lecturer: Prof. Simona Di Nino (Univaq), 8 hours

  Program: The course introduces the basics of the perturbation analysis for weakly nonlinear dynamical systems, with special reference to the multiple scale method for ordinary differential systems. The following topics are addressed: eigenvalue and eigenvector sensitivity analysis; initial value problems: straightforward expansions; the multiple scale method: basic aspects and advanced topics; Duffing oscillator under external excitation: primary, super-harmonic and sub-harmonic resonances; Duffing oscillator under parametric excitation; multi-d.o.f. quasi-Hamiltonian systems under external/parametric/internal resonances.

- On Kubo's derivation of the fluctuation-dissipation theorem

  Lecturer: Prof. Matteo Colangeli (Univaq), 6 hours

  Program: We review the original Kubo?s derivation of the celebrated fluctuation-dissipation theorem, that stands as a cornerstone of nonequilibrium statistical mechanics. The theorem expresses the linear response of a system to an external stimulus in terms of the fluctuation properties of the system in thermal equilibrium. By studying a generalized Langevin equation, we shall highlight the connection between the dynamical susceptibility and the power spectrum of fluctuations, and shall also discuss the density response for a system of interacting particles.

- From microscopic dynamics to macroscopic equations: scaling limits for the Lorentz Gas.

  Lecturer: Prof. Alessia Nota (Univaq), 6 hours

  Program: Many interesting systems in physics are constituted by a large number of identical components so that they are difficult to analyze from a mathematical point of view. At the same time we are not interested in a detailed description of the system but rather in its collective (statistical) behavior. Therefore, it is necessary to look for all the procedures leading to simplified models which preserve all the interesting physical informations of the original system, cutting away redundant information. The central point is to outline the limiting procedures which lead from the microscopic description based on the fundamental laws of mechanics to a kinetic picture described by integro-differential equations depending on a small number of degrees of freedom. In this course, we will focus on a simple microscopic model, the Lorentz gas, which is a gas of non-interacting particles in a random configuration of scatterers. This model is paradigmatic since it provides a rare source of exact results in kinetic theory. Indeed one can prove, under suitable scaling limits, a rigorous validation of linear kinetic equations as well as hydrodynamic equations. In order to accomplish this goal we will rely on an interplay of analysis, probability, and statistical mechanics.

- Mathematical Models For Economic Equilibria

  Lecturer: Prof. Massimiliano Giuli (Univaq), 10 hours

  Program: In science the term "equilibrium" has been widely used in physics, chemistry, biology, engineering and economics, among others, within different frameworks. It generally refers to conditions or states of a system in which all competing influences are balanced. For instance, the

economic equilibrium which studies the dynamics of supply, demand, and prices in an economy within several markets, can be modeled as a variational inequality problem.

In non-cooperative game involving two or more players, Nash proposed an equilibrium solution in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only their own strategy. This problem can be reformulated as a fixed point problem.

These mathematical models share an underlying common structure that allows to conveniently formulate them in a unique format of equilibrium. The course is devoted to describe this format and it focuses on the main mathematical tools which are crucial for studying the existence and the stability of the solutions.

- Numerics for stochastic differential equations

  Lecturer: Prof. Raffaele D'Ambrosio (Univaq), 10 hours

  Program: TBA

- Variational derivation of continuum mechanics equations

  Lecturer: Proff. Emilio Barchiesi (MeMoCS), Francesco dell'Isola (Univaq), Luca Placidi (Uninettuno), 10 hours

  Program: The aim of this short course is to introduce the students to the variational methods, and their epistemological assumptions, that are used in continuum mechanics. Static and dynamic cases will be analyzed. The mathematical derivations will be done on the basis of assumptions that are formulated under the action formalism. In the static case, the action is reduced to the total energy functional and a method to derive its form from a discrete model is also sketched.

- Quantum Computing

  Lecturer: Prof. Guidoni+ IBM lecturer, 14 hours

  Program: The present short course is a joint PhD course between the PhD in Mathematics and Models and the PhD in Informatics. The aim of the short course is to provide to students with background in mathematics and informatics the foundation of quantum computation. The course will consist of theoretical lectures as well as hands-on tutorial lead by the Quantum Computing experts from IBM-Italia.

  Arguments: General overview on quantum computation. Introduction to Quantum Mechanics and Qubits. Quantum circuits and algorithms. Single and double Qubit gates with examples. Present and future applications. Perspective of quantum computation and practical implementation of algorithms on the IBM-Q quantum computer and simulator.