Doctoral Course in Mathematical Sciences
Department of Mathematics
University of Padova

Doctoral Course in Mathematical Sciences

Catalogue of the courses 2014

Updated July 3, 2014

INTRODUCTION

The courses offered, for the year 2014, to the Graduate Students in Mathematical Sciences include courses taught by internationally recognized external researchers, who have accepted our invitation; such courses will not necessarily be offered again in the future years. Considering the wide impact of the content of theses courses, we emphasize the important for all graduate students to follow them.
The Faculty of the Graduate School could cancel courses with an excessively low number of registered students.

Also next year, beside the courses that our School directly offers, we have selected some courses of the Graduate School in Information Engineering of the University of Padova that we consider relevant also for our School.

REQUIREMENTS FOR GRADUATE STUDENTS

With the advice of some Faculty member, all students are required to select some courses, either because they are linked with the area of their present or planned research, or just to improve their knowledge of specific subject.

This year, considering the fact that courses may vary in duration, we have decided to indicate a mandatory minimum numbers of hour.
Therefore, students are required, within the **first two years**, to follow and **pass the exam** of

- **At least 2 courses of the School**
- other courses, <u>in addition to the two above</u>, in three areas (**Computational Mathematics or Mathematics or Computer Science**) **or of the School**, with total commitment of **at least 64 hours**.

Students are encouraged to register for other courses; although to sit for the exam is not required for these courses, it is strongly advised. In all cases, students must participate with regularity to the activities of the courses they are registered to. At the end of the course the teacher will inform the Coordinators of the Areas on the activities of the course and of the registered students.

<u>Institutional courses for Master of Science in “Mathematics” or “Computer Science”</u>

Students have the possibility to attend, with acquisition of credits, the courses of the Master of Science in Mathematics or Computer Science.
The interest for these courses must be indicated by the Supervisor or a tutor. The Council of the Area the students is enrolled in, will assign the number of hours that will be computed within the mandatory 64 hours.

<u>Courses attended in other Universities</u>

Students are allowed to take Ph.D. courses offered by Doctoral School of other Universities. Acquisition of credits will be subject to approval of the Council of the Area the students is enrolled in.

HOW TO REGISTER TO COURSES

The online registration to courses has changed from last years, and allows students both to register and to cancel.
The registration is required for the attendance to all courses, independently of the intention to sit for the exam. The list of the courses can be found in the website of the School http://dottorato.math.unipd.it/ at the link Courses Registration (or directly at the address http://dottorato.math.unipd.it/registration/), filling the **online registration form** with all required data, and validating with the command "Register".
To acknowledge the registration, an email message will be sent to the address indicated in the registration form; this email message must be saved, since it is necessary for possible cancellation.

Registration for a course implies the agreement of the applicant to the participation.
Requests of **cancellation** to a course must be submitted in a timely manner, and **at least one month before the course** (except those that begin in January and February) using the link indicated in the email message of acknowledgment.

REQUIREMENTS FOR PARTICIPANTS NOT ENROLLED IN THE GRADUATE SCHOOL OF MATHEMATICS

The courses in the catalog, although part of activities in the Graduate School in Mathematics and thus offered to its students, are also open to all students, graduate students and researchers of all Graduate Schools and other universities.
For reasons of organization, external participants are required to **indicate their wish to participate at least two months before the beginning of the course for courses taking place from April 2014 and at least one month before for courses that take place until March 2014, following the procedure described in the preceding paragraph.**
Possible **cancellation** to courses must also be notified.

Courses of the School

Courses of the “Computational Mathematics” area

Courses of the “Mathematics” area

4. Prof. Francesco Maddalena
   Calculus of Variations with applications to Materials Science **M-4**

5. Prof. Francesco Baldassarri, Alessandra Bertapelle and Carla Novelli
   Tropical Geometry **M-5**

6. Prof. Francesco Bottacin
   Differential and Riemannian Geometry **M-6**

Courses of the "Computer Science" area

1. Prof. Mauro Conti
   Privacy and security for mobile cooperative devices **CS-1**

2. Prof. Gilberto Filè
   Definite clauses applied to security **CS-2**

3. Dr. Umberto Grandi
   Logical Frameworks for Multiagent Aggregation **CS-3**

4. Prof. Claudio Palazzi
   Networking issues and solutions in online games **CS-4**

5. Prof. Maria Silvia Pini
   Preference reasoning in computational social choice
   and in Decision Support Systems **CS-5**

6. Prof. Vijay Saraswat
   Resilient, Parallel, Big Data Application Frameworks in X10 **CS-6**

Courses in collaboration with the Doctoral School on "Information Engineering"

1. Prof. Gianluigi Pillonetto
   Applied Functional Analysis **DEI-1**

2. Prof. Giorgio Picci
   Applied Linear Algebra **DEI-2**

3. Prof. Fabio Marcuzzi
   Computational Inverse Problems **DEI-3**

4. Prof. Nicola Laurenti
   Information theoretic Methods in Security **DEI-4**

5. Prof. Morten Gram Pedersen
   Mathematical modeling of cell Biology **DEI-5**

6. Prof. Subhrakanti Dey
   Random Graphs and Stochastic Geometry in Networks **DEI-6**

7. Prof. Lorenzo Finesso
   Statistical methods **DEI-7**

Courses of the School

Random perturbation of differential equations

Dr. D. Barbato[1], Prof. P. Dai Pra[2]

[1] Università di Padova, Dipartimento di Matematica
Email: barbato@math.unipd.it

[1] Università di Padova, Dipartimento di Matematica
Email: daipra@math.unipd.it

Timetable: 24 hrs. First lecture on May 28, 2014, 15:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Standard knowledge of Probability and measure theory.

Examination and grading: Seminar on a subject assigned by the Instructors

SSD: MAT/06

Aim: The course provides an introduction to stochastic evolutions obtained by adding a random term to a differential equation. After an introduction to the finite-dimensional setting, we will deal with some infinite-dimensional problem, where the starting deterministic evolution is described by a partial differential equation.

Course contents:

1. Introduction to Brownian motion and stochastic integration.
2. Stochastic differential equations in finite dimensions.
3. Brownian motion and stochastic integral in infinite dimension.
4. Linear stochastic differential equations in infinite dimension. Example: stochastic heat equation and stochastic wave equation.
5. Nonlinear models of fluid dynamics: stochastic Navier-Stokes equations and related models.

Geometric approaches to optimization

Dott. Marco Di Summa[1], Prof. Samuele Fiorini[2]

[1] *Università degli Studi di Padova*
Dipartimento di Matematica
Email: disumma@math.unipd.it

[2] *Université libre de Bruxelles*
Département de Mathématique
Email: sfiorini@ulb.ac.be

Timetable: 20 hrs. First lecture on April 30, 2014, 16:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Linear algebra. Some knowledge in linear programming and graph theory will be useful, but not strictly necessary.

Examination and grading: Written exam.

SSD:MAT/09.

Aim: In this course we will provide an answer to the following question: what is the best choice of variables to express a given optimization problem? We will focus on reducing the size of optimization problems through reformulations in different spaces. After recalling basics of linear optimization and polyhedra, we will see some cases where it is possible to drastically reduce the number of constraints of linear optimization problems by a reformulation, and prove that this is not always possible. Finally, we will consider more general conic optimization problems.

Course contents:

1. Linear optimization and polyhedra.
2. Reformulations of linear optimization problems: examples, techniques, and size lower bounds.
3. Optimization over other cones (positive semidefinite matrices and completely positive matrices).

Principles of Cloud Computing

Prof. Tullio Vardanega[1]

[1] *University of Padova*
Department of Mathematics
Email: tullio.vardanega@math.unipd.it

Timetable: 20 hours of class lectures, plus 1.5 days of personal study. First lecture on July 14, 2014, 14:30 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: basics in concurrency, networks and distributed systems.

Examination and grading: students will be assigned a practical exercise and will referred to the reference technology to use in carrying that task out. The practical will allow the students to get a taste of the principal architectural characteristics required to take benefit of the Cloud, notably elasticity, multi-level load balancing and transparent dispatching.

SSD: INF01

Aim: to provide the students with some initial yet articulate insight into the architectural principles of the Cloud Computing stack and some hands-on experience on the fundamentals of designing an application for the Cloud.

Course contents:

- a traversal of the Cloud stack with a historical and technological perspective of where its constituents came about
- zooming into the each stack layer in a bottom-up fashion
- an executive review of relevant Cloud technology
- illustration of key principles of *application design for the Cloud*, and hands-on experience with a practical exercise.

Numerical methods for Ordinary Differential Equations

Prof. Marino Zennaro[1], Prof. Rossana Vermiglio[2]

[1] *University of Trieste, Department of Mathematics and Geosciences*
Email: zennaro@units.it

[2] *University of Udine, Department of Mathematics and Computer Science*
Email: Rossana.Vermiglio@uniud.it

Timetable: 12 hrs. (Part I, Prof. Zennaro), First lecture on January 23, 2014, 15:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.
12 hours (Part II, Prof. Vermiglio), First lecture on February 27, 2014, 14:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: it is advisable to have attended a basic course in Numerical Analysis.

Examination and grading: A unique written exam for both Part I and Part II.

SSD: MAT/08 Numerical Analysis
Aim: We present basic numerical methods for initial value problems in ordinary differential equations and we analyse their convergence and stability properties.

Course contents:
Part I
Existence and uniqueness of the solution and continuous dependence on the data for the initial value problem $y'(x) = f(x, y(x)), y(x_0) = y_0$.
Classical Lipschitz constant and right hand side Lipschitz constant.
General one-step methods; explicit and implicit Runge-Kutta methods.
Definition of local truncation and discretization error for one-step methods and definition of consistency of order p.
Convergence theorem with order p for one-step methods. Order conditions for Runge-Kutta methods. Order barriers for explicit and implicit methods.
Variable stepsize implementation. Embedded pairs of methods of Runge-Kutta-Fehlberg type.

Part II
Introduction to the stability of numerical methods. Stiff problems.
Definition of A-stability, AN-stability and BN-stability of a numerical method.
Analysis of A-stability for Runge-Kutta methods: A-stability regions. L-stability.
Analysis of AN-stability and BN-stability for Runge-Kutta methods. Algebraic stability.
The phenomenon of the order reduction: an example. B-convergence.
Introduction to Linear Multistep (LM) methods. Zero-stability and convergence. A-stability, A(α)-stability and stiff-stability. Backward differentiation formulas.

References:

- E. Hairer, S.P. Norsett, G. Wanner: Solving Ordinary Differential Equations I, Nonstiff Problems, Springer-Verlag, Berlin, 1993.
- E. Hairer, G. Wanner: Solving Ordinary Differential Equations II, Stiff Problems, Springer-Verlag, Berlin, 1993.
- J.C. Butcher: Numerical methods for ordinary differential equations. Second edition, John Wiley & Sons, Ltd., Chichester, 2008.
- J.D. Lambert: Numerical methods for ordinary differential systems. John Wiley & Sons, Ltd., Chichester, 1991.

Introduction to Hamilton-Jacobi equations.

Prof. Martino Bardi[1]

[1] University of Padua
Department of Mathematics
Email: bardi@math.unipd.it

Timetable: 24 hrs. First Lecture on March 6, 2014, 09:30 (dates already fixed, see the calendar), Torre Archimede, Room 2AB/45.

Course requirements: Standard knowledge of Advanced Calculus.

Examination and grading: Seminar on a subject assigned by the Instructors.

SSD: MAT/05

Aim: The course provides an introduction to nonlinear first order partial differential equations of Hamilton-Jacobi type and to some of their numerous applications.

Course contents:

- Models and motivations.
- The method of characteristics for Hamilton-Jacobi (HJ) equations.
- Links of HJ equations with analytical mechanics and calculus of variations; Hopf-Lax formulas.
- Viscosity solutions: well-posedness of the Dirichlet and Cauchy problems.
- Applications to optimal control theory and differential games.

Courses of the “Computational Mathematics” area

Introduction to Delay Differential Equations

Prof. Stefano Maset[1]

[1] University of Trieste
Department of Mathematics and Computer Science
Email: maset@units.it

Timetable: 16 hrs. Lectures May 2014 (to be defined), Torre Archimede, Room 2BC/30.

Course requirements: Numerical methods for ordinary differential equations.

Examination and grading: written examination.

SSD: MAT/08 Numerical Analysis.

Aim: to introduce students to delay differential equations and their numerical solution.

Course contents:

1. Functional Differential Equations (FDEs). Retarded Functional Differential Equations (RFDEs). Particular types of RFDEs: Delay Differential Equations (DDEs), Integro-Differential Equations (IDEs), State-Dependent DDEs (SDDDEs), State-Dependent IDEs (SDIDEs). Neutral Functional Differential Equations (NFDEs). Mathematical models based on such equations.
2. Existence and uniqueness of the solution and continuous dependence on the data for an initial problem of RFDEs.
3. Continuous Runge-Kutta (CRK) methods for RFDEs. Discrete order, uniform order and global order of a CRK method for RFDEs. Order conditions.

Computational Methods for Inverse Problems and Applications in Image Processing

Prof. James Nagy[1]

[1] Emory University, Atlanta, USA
Department of Mathematics and Computer Science
Email: nagy@mathcs.emory.edu

Timetable: 14 hrs (lectures and laboratories). First lecture on February 17, 2014, 09:00 (dates already fixed, see calendar), Torre Archimede, Laboratory LabTA on 2nd floor except on February 19, Room 2BC/30.

Course requirements: Background in numerical linear algebra and some experience using MATLAB.

Examination and grading: final project.

SSD: MAT/08

Aim: Students will learn computational techniques to solve ill-posed inverse problems that arise in scientific and engineering applications.

Course contents:

One of the most difficult challenges in scientific computing is the development of algorithms and software for large scale ill-posed inverse problems. Such problems are extremely sensitive to perturbations (e.g. noise) in the data. To compute a physically reliable approximation from given noisy data, it is necessary to incorporate appropriate regularization (i.e., stabilization) into the mathematical model. Numerical methods to solve the regularized problem require effective numerical optimization strategies and efficient large scale matrix computations.

In these lectures we describe how the challenges of solving linear inverse problems can be analyzed using the singular and spectral value decomposition (SVD), and how to efficiently implement the ideas with iterative methods on realistic large scale problems. We also discuss how the approaches can be adapted for use on nonlinear inverse problems. Examples from image processing will be used to illustrate the performance of various methods.

Topics in Stochastic Analysis

Prof. Tiziano Vargiolu[1]

[1] Università di Padova
Dipartimento di Matematica Pura ed Applicata
Email: vargiolu@math.unipd.it

Calendario: 10 ore. First lecture on March 4, 2014, 14:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Prerequisiti: A previous knowledge of the basics of continuous time stochastic analysis with standard Brownian motion, i.e. stochastic integrals, Itô formula and stochastic differential equations, as given for example in the master course "Analisi Stocastica".

Tipologia di esame: Seminar

SSD: MAT/06

Programma: The program will be fixed with the audience according to its interests. Some examples could be:

- continuous time stochastic control;
- Levy processes;
- numerical methods.

Numerical stability of dynamical systems described by delay differential equations

Proff. Rossana Vermiglio, Dimitri Breda[1]

[1]University of Udine
Department of Mathematics and Informatics
Email: {rossana.vermiglio,dimitri.breda}@uniud.it

Timetable: 12 hrs (6+6). Lectures in the first semester 2014 (to be defined), Room 2BC/30, Torre Archimede.

Course requirements: basic course on Numerical Analysis.

Examination and grading: exercises and/or computer experiments or brief essay on an argument treated during the course.

SSD: MAT/08 Numerical Analysis

Course contents:

The study of the dynamical systems that are encountered in diverse natural evolutive phenomena is focused on the possibility of foreseeing the time behavior by varying either some control parameters or initial conditions. The stability of the solutions represents a key aspect and the numerical analysis, through the development of efficient and accurate algorithms, can furnish an important contribution in the comprehension and description of the dynamics over the long period (equilibria, cycles, chaos).

Object of this course are the dynamical systems described by differential equations with delay(s), characterized by a future evolution depending on the past history. Interesting applications can be found in control theory, where the delay can be used to stabilize the system, or in population models, where it acts, e.g., as gestation time.

The basic concepts of stability, asymptotic stability and the relevant conditions will be defined by generalizing the same concepts for linear and autonomous systems of ordinary differential equations. Then, the most recent numerical approaches for the study of the stability of equilibria and limit cycles in the retarded case will be presented, based on the discretization with pseudospectral methods of the solution operators or their infinitesimal generator. Eventually, example of applications will be given, relevant to the bifurcation analysis and the stability maps following the variation of the parameters.

With regards to nonautonomous problems, finally, the concepts of Lyapunov exponents and spetrum will be introduced, always starting from the ordinary case, passing then to the theory and numerical methods recently developed for delay differential equations.

Recent advances in Finance and Stochastics

Nicole El Karoui & Monique Jeanblanc

Univ. Pierre et Marie Curie & Univ. d'Évry Val d'Essonne)

Lecture schedule: 18h, in May 2014, room 1BC45[1], unless explicitly mentioned.

PART A) May 22 (15 − 18, room 2BC30), May 26 (10 − 13), May 27 (10 − 13);

PART B) May 26 (14.30 − 17.30), May 27 (14.30 − 17.30), May 28 (10 − 13).

Course requirements: Probability and Stochastic Calculus.
Examination: written.
SSD: MAT/06.

Contents

PART A) Enlargement of filtrations

The course is devoted to enlargement of filtration with Finance in view. Two filtrations $\mathbb{F}$ and $\mathbb{G}$ are given, such that $\mathbb{F} \subset \mathbb{G}$. The goal is to study the behavior of $\mathbb{F}$-martingales and to give conditions so that these martingales are $\mathbb{G}$ semi-martingales. In that case, the decomposition of any $\mathbb{F}$-martingale as a $\mathbb{G}$ semimartingale will be provided. The two main examples of such filtrations $\mathbb{G}$ are the case of initial enlargement, where $\mathbb{G} = \mathbb{F} \vee \sigma(L)$, where L is a random variable, and the case of progressive enlargement, where $\mathbb{G}$ is the smallest filtration which contains $\mathbb{F}$ and makes a given positive random variable τ a stopping time. The case where $\mathbb{F}$ is a Brownian filtration will be studied with more details. Applications to arbitrage opportunities in finance will be given.

We will provide answers to the above questions and see some recent applications of this theory to Finance.

Lecture I

The basic model of credit risk modelling involves a specific case of progressive enlargement of filtration, namely the case where any $\mathbb{F}$-martingale is a $\mathbb{G}$-martingale. If the filtration $\mathbb{F}$ enjoys a predictable representation theorem (for example, if $\mathbb{F}$ is the filtration generated by a Brownian motion), then a predictable representation theorem is valid in the enlarged filtration. The case where there are discontinuous $\mathbb{F}$-martingales is more involved, and we shall study some examples.

Lecture II

[1]Dipartimento di Matematica, Torre Archimede, Via Trieste 63, 35121 Padova.

If τ is a random time with a positive conditional density, i.e. if $\mathbb{P}(\tau > u | \mathcal{F}_t) = \int_u^\infty p_t(\theta) f(\theta) d\theta$ for some $\mathbb{F}$ adapted positive process $p(\theta)$, where f is the density of τ, it is easy to prove that any $\mathbb{F}$-martingale is a semi-martingale for the initially enlarged filtration $\mathbb{G} = \mathbb{F} \vee \sigma(\tau)$ and for the progressive enlarged filtration. In that case, there are no arbitrages opportunities induced by the enlargement, however, the more informed agent makes a profit, characterized by the drift information (in the logarithm case).

Lecture III

In a general case, any $\mathbb{F}$-martingale stopped at τ is a $\mathbb{G}$-semi martingale, with an explicit decocmposition. For a specific case of random times τ (called honest times), and in a complete financial market, there are classical arbitrages before τ which can be given in an explicit form. For the general case of random times, under some weak condition, there are no arbitrages of the first kind, meaning more or less that there exists a positive $\mathbb{G}$-local martingale L so that $S^\tau L$ is a $\mathbb{G}$-local martingale , where S^τ is the stopped process associated with the price of the assets in an $\mathbb{F}$-arbitrage free financial market.

The case after τ is more difficult, and we shall pay attention only to honest times. In this last lecture, we shall restrict our attention to the case where the filtration $\mathbb{F}$ will be a Brownian filtration, even if the results can be extended to any filtration.

References

[1] Aksamit, A., Choulli, T., Deng, J., and Jeanblanc, M.: *Non-Arbitrage under Random Horizon for Semimartingale Models*, Preprint of University of Alberta and Evry-Val d'Essonne University, 2014.

[2] Aksamit, A., Choulli, T., Deng, J., and Jeanblanc, M.:*Arbitrages in a progressive enlargement setting*, Arbitrage, Credit and Informational Risks, Peking University Series in Mathematics, Vol. 6, 55-88, World Scientific (2014)

[3] Barlow M. T., *Study of a filtration expanded to include an honest time,* Z. Wahrscheinlichkeitstheorie verw, Gebiete, 44, 307-323, 1978.

[4] Dellacherie, M., Maisonneuve, B. and Meyer, P-A. (1992), *Probabilités et Potentiel, chapitres XVII-XXIV: Processus de Markov (fin), Compléments de calcul stochastique*, Hermann, Paris.

[5] Fontana, C. and Jeanblanc, M. and Song, S. (2013) *On arbitrages arising with honest times*. To appear in Finance and Stochastics

[6] Imkeller, P. (2002), *Random times at which insiders can have free lunches*, Stochastics and Stochastic Reports , 74(1-2): 465–487.

[7] J. Jacod. *Grossissement initial, hypothèse (H') et théorème de Girsanov.* Lecture Notes in Mathematics, 1118, 15–35, Springer-Verlag, 1985.

[8] T. Jeulin. *Semi-martingales et grossissement d'une filtration.* Lecture Notes in Mathematics, Vol 833, Springer-Verlag, 1980.

[9] Jeulin, T. (1980), *Semi-martingales et Grossissement d'une Filtration*, Lecture Notes in Mathematics, vol. 833, Springer, Berlin - Heidelberg - New York.

[10] R. Mansuy, M. Yor. *Random times and enlargements of filtrations in a Brownian setting.* Lecture Notes in Mathematics, Vol 1873, Springer-Verlag, 2006.

PART B) Microsimulation and population dynamics
Most countries are experiencing a reduction in mortality over time, which is a new phenomenon, without any historical reference. In this context, societies are facing new challenges, in particular concerning generation equilibrium, the role of ageing populations and the viability of shared collective systems, in particular pension systems. In so-called structured populations, individuals differ according to variables that influence their survival and/or reproduction abilities. These variables are from different types, depending of the specificities of the population in consideration. For instance, in human population, key characters are gender, socioeconomic level, spacial location, marital status and age. For example, the "population" of firms interacting in the counterparty risk of a bank may be characterized by sector, countries, rating, "age" and other specificities. In the study of the order book in HFT by Hawkes process, the main factor is the age of the order. We are concerned with the dynamics of populations with trait and age structures.

Lecture I - Introduction and description of the classical methodology
Introduction to basic life insurance and to some mortality models for annual death probabilities. Example: Life insurance products, called "Variable Annuities".

Introduction to Marked Point processes, and Birth and Death processes.

Lecture III - Individual-based model and population dynamics
Introduction of a dynamic population model, inspired by [5] and [4] in the field of ecology, and the work of [1] for demographic purposes, that allows to take into account individual characteristics (called "traits" as gender, socio-economic characteristics...) which have a real impact on demographic behavior and age. Example: a new simulation method of Hawkes processes used in credit modeling or HFTrading.

Lecture III - Applications to longevity risk dynamics using empirical data Back to longevity risk modelisation, utilization of the population dynamics model to simulate some stylized fact as the cohort effect, and more generally the importance of the composition of the underlying population.

References

[1] H. Bensusan. *Risques de taux et de longévité: Modélisation dynamique et applications aux produits dérivés et à l'assurance vie.* PhD thesis, École Polytechnique, 2010.

[2] A. J. G. Cairns, D. Blake and K. Dowd. *Monte Carlo Algorithms for Default Timing Problems.* Journal of Risk and Insurance, 73: 687–718.

[3] A. Dassios, H. Zhao *Exact simulation of Hawkes process with exponentially decaying intensity* Electron. Commun. Probab. 18 (2013), no. 62, 1–13.

[4] R. Ferriere and V.C. Tran. *Stochastic and deterministic models for age-structured populations with genetically variable traits.* In *ESAIM: Proceedings*, volume 27, pages 289–310, 2009.

[5] N. Fournier and S. Méléard. A microscopic probabilistic description of a locally regulated population and macroscopic approximations. *Annals of applied probability*, 14(4):1880–1919, 2004.

[6] K. Giesecke, B. Kim, S. Zhu. *Monte Carlo Algorithms for Default Timing Problem.* Management Science: Vol 57, No.12, Dec 2011.

[7] R. Lee and L. Carter. Modeling and forecasting US mortality. *Journal of the American Statistical Association*, 87(419):659–671, 1992.

Nonlinear optimization: Derivative-free methods

Dott. Francesco Rinaldi[1], Dott. Giovanni Fasano[2]

[1] Università degli Studi di Padova
Dipartimento di Matematica
Email: disumma@math.unipd.it

[2] University of Venice "Ca' Foscari"
Department of Management
Email: fasano@unive.it

Timetable: 12 hrs. First lecture on June 6, 2014, 10:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Basic knowledge of calculus in $\mathbb{R}^n$, including some introductory elements of optimization methods and numerical analysis.

Examination and grading: Oral exam with a final mark.

SSD:MAT/09.

Aim: We describe some basics of optimization methods, where both the objective function and the constraints are possibly unavailable. We compare different approaches from the literature, analyzing their convergence properties.

Course contents: This course will be divided into three parts, so that it will correspondingly introduce the student to different levels of investigation for Derivative-Free Optimization (DFO).

The introductory part will provide some basics of DFO, so that clear motivations and some preliminary results on the subject will be detailed. This part will partially review the literature and emphasize the relation between DFO approaches and exact methods for nonlinear continuous optimization, where derivatives are available. We will also clarify the importance of addressing methods which do not use derivatives , for the solution of nonsmooth real applications.

The second part of this course will focus on specific successful DFO approaches from the literature. In particular, Direct-Search methods and Model-based methods will be considered, along with their relation and their impact on the literature. Since the course is entirely devoted to exact techniques, convergence properties for the described schemes will be analyzed.

Finally, in the third part of the course we will try to give an overview on additional current topics for DFO, with a glimpse to constrained real problems and some suggestions on dedicated software.

References:

- Kolda T.G., Lewis R.M. and Torczon V. Optimization by direct search: new perspectives on some classical and modern methods. SIAM Review 45(3), pp. 385-482, 2003.
- Conn A.R., Scheinberg K. and Vicente L.N. Introduction to Derivative-Free Optimization, MPS-SIAM Series on Optimization, SIAM, Philadelphia, 2009.

Courses of the “Mathematics” area

On the O'Nan-Scott theorem in its applications

Prof. Pablo Spiga[1]

[1] *Universitá di Milano-Bicocca*
Dipartimento di Matematica e Applicazioni
Email: pablo.spiga@unimib.it

Timetable: 14 hrs. First Lecture on April 10, 2014, 11:30 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Only some basic and elementary facts on the Theory of Groups are needed.

Examination and grading: Short presentation on a mutually agreeable subject related to the content of the course.

SSD: MAT/02

Aim: We aim to show how the pivotal O'Nan-Scott theorem on finite primitive groups has been (and is) used to study some problems on finite permutation groups or finite combinatorial structures.

Course contents:

In the first part of this course, we present one of the fundamental theorems for analysing finite primitive groups: the O'Nan-Scott theorem. Loosely speaking, this result gives a satisfactory classification of the algebraic structure of finite primitive groups together with some information on the group actions.

The O'Nan-Scott theorem combined with the Classification of the Finite Simple Groups turned out to be an invaluable tool for analysing and studying some combinatorial objects.

In the second part of the course, we present some of these applications, mostly on the theory of group actions on graphs.

A soft introduction to algebraic entropy

Prof. Luigi Salce[1]

[1] *University of Padova*
Department of Mathematics
Email: salce@math.unipd.it

Timetable: 10 hrs. First lecture on February 18, 2014 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Linear Algebra, Basic Algebra.

Examination and grading: Seminar on a subject assigned by the Instructor.

SSD: MAT/02, MAT/03

Aim: The course is an introduction to the theory of algebraic entropy of endomorphisms of algebraic structures in the basic setting of vector spaces over a field K. The two main results on this topic are presented: the Addition Theorem and the characterization of the algebraic entropy as the unique additive invariant extending the dimension invariant via the Bernoulli functor from the category of K-vector spaces to the category of $K[X]$-modules.

Course contents:

1. Preliminaries on vector spaces, modules over PID's and the Fekete Lemma.
2. The category of flows of a linear transformation. The Bernoulli shift and the Bernoulli functor.
3. Definition, existence and properties of the algebraic entropy.
4. Algebraic entropy as rank of $K[X]$-modules. Addition and Uniqueness Theorems.
5. Adjoint algebraic entropy.

Nonlinear wave equations and applications

Prof. Dario Bambusi

Università degli Studi di Milano
Dipartimento di Matematica "F. Enriques"
Email: dario.bambusi@unimi.it

Duration: 12 hours.
Location: Mathematics Department (Torre Archimede), Room 2BC/30.
Timetable:

- Tuesday, 27 May 2014, 14.30-17.30
- Wednesday, 28 May 2014, 09.30-12-30
- Thursday, 29 May 2014, 09.30-12.30
- Friday, 30 May 2014, 09.30-12.30

Course requirements: no prerequisite knowledge of the subject is required.

Examination and grading: to be decided by the Lecturer.

SSD: MAT/07 (Mathematical Physics)

Course contents:
Deduction of the Euler equations for fluids and of the surface water wave equations. Lagrangian and Hamiltonian formulation of the problem: Lagrangian of the water wave equations, Dirichlet-Neumann operator, and Hamiltonian setting of the problem. Averaging principle and its application to the shallow water wave problem. Deduction of the Korteweg-de Vries equation as an effective equation. Applications to Tsunami propagation.

Calculus of Variations with applications to Materials Science

Prof. Francesco Maddalena[1]

[1] Politecnico di Bari
Department of Mechanics, Mathematics and Management
Email: f.maddalena@poliba.it

Timetable: 12 hrs. First lecture on June 23, 2014, 16:30 (dates already fixed, see the calendar) Torre Archimede, Room 2BC/30.

Course requirements: Calculus, Basic functional analysis

Examination and grading: a brief discussion

SSD: MAT/05

Aim: An introduction to the field of the Calculus of Variations, keeping an eye to applications

Course contents:

1. Some classical problems of the Calculus of Variations
2. Preliminaries: Sobolev spaces, convex Analysis, weak topologies...
3. Classical methods: the first variation and the Euler-Lagrange equation
4. Direct methods: Scalar and vectorial case, quasi–convexity, polyconvexity
5. Relaxation: non convex functionals
6. Gamma - convergence: Cahn-Hilliard's method for the phase transition
7. Continuum mechanics and elasticity: finite and linear elasticity theory, existence problems and deduction of the Gamma convergence.
8. Thin structures: Biological membranes and adhesion problems

Tropical Geometry

Prof. Francesco Baldassarri[1], Prof. Alessandra Bertapelle[2], Prof. Carla Novelli[3]

[1] University of Padova
Department of Mathematics
Email: baldassa@math.unipd.it

[2] University of Padova
Department of Mathematics
Email: bertapel@math.unipd.it

[3] University of Padova
Department of Mathematics
Email: novelli@math.unipd.it

Timetable: 16 hrs. Regularly, Thursday 14:30-16:00. Torre Archimede, Room 1BC/45. First meeting of the course: Thursday, Jan. 16, at 13:00, room 1C/150

Course requirements: As prerequisites, some familiarity with p-adic numbers and functions, and with (complex) Riemann surfaces. Some knowledge of cohomology (simplicial, De Rham, coherent,..) will be helpful.

Examination and grading: To be arranged with the organizers.

SSD: MAT/03

Aim: To acquire new instruments to understand the geometry of algebraic curves (and perhaps of surfaces) and of their moduli spaces.

Course contents: We will discuss some non-archimedean (especially p-adic) analytic geometry in the Berkovich style, with emphasis to smooth curves and their semistable models. We will discuss tropical geometry, again with emphasis to tropical curves, under various viewpoints. We will review the classical origin of tropicalization, via limits of log-maps, the abstract definite as algebraic geometry over the tropical real semiring. We will describe the connection between the Berkovich analytification and tropicalization of complex algebraic curves.

Differential and Riemannian Geometry

Prof. Francesco Bottacin[1]

[1] *Università degli Studi di Padova*
Dipartimento di Matematica
Email: bottacin@math.unipd.it

Timetable: 16 hrs. First lecture on March 21, 2014, 14:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: basic notions of Topology and Real Analysis

Examination and grading: Oral examination.

SSD:MAT/03.

Aim: The course will provide an introduction to the basic notions and results of differential and Riemannian geometry.

Course contents: Manifolds, vector bundles, tensor bundles, differential forms, de Rham cohomology, integration on manifolds. Distributions, Lie derivative, flows. Connections on vector bundles, curvature. (Pseudo)Riemannian metrics on manifolds.

Courses of the “Computer science” area

Privacy and Security for Mobile Cooperative Devices

Prof. Mauro Conti[1]

[1] *University of Padua*
Department of Mathematics
Email: conti@math.unipd.it

Timetable: 12 hrs. First Lecture on June 24, 2014, 09:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: Basic notions of Networking and Security are desirable.

Examination and grading: Final project.

SSD: INF/01 - Computer Science

Aim: the course will provide an introduction to a selection of research topics in privacy and security, with a focus on wireless networks.

Course contents: the course will be based mainly on the content of the book by Buttyan et al. [1]:

Part I Introduction
1. Existing Wireless Neworks
2. New Wireless Networks and New Challenges
3. Trust

Part II Thwarting Malicious Behavior

4. Naming and Addressing
5. Establishment of Security Associations
6. Securing Neighbor Discovery
7. Secure Routing in Multi-Hop Wireless Networks
8. Privacy Protection

Part III Thwarting Selfish Behavior

9. Selfish Behaviour at the MAC layer of CSMA/CA
10. Selfishness in Packet Forwarding
11. Cooperation among Operators
12. Secure Protocols for Behavior Enforcement

Additional material (recently published research papers on the topic) will be provided during the lectures, and selected also according to students' interest.

[1] *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. Levente Buttyán and Jean-Pierre Hubaux. Cambridge University Press New York, NY, USA, 2007. ISBN:0521873711 9780521873710.*

Definite clauses applied to security

Prof. G.Filè[1]

[1] University of Padova
Department of Mathematics
Email: gilberto@math.unipd.it

Timetable: 12 hrs. Lectures on May 2014, Torre Archimede, Room 2BC/30.

Course requirements: some logic

Examination and grading: oral examination

SSD: MAT and INF/01

Aim: Show that definite clauses are a powerful tool for modelling communication protocols at different levels of complexity (with and without a notion of state)

Course contents: Preliminaries: definite clauses, unification and resolution, clauses for modelling communication protocols. Proverif study and use in laboratory. Limits of Proverif and a way to overcome them. Definite clauses used for modelling state sensitive protocols.

Logical Frameworks for Multiagent Aggregation

Umberto Grandi[1]

[1] *University of Padova*
Department of Mathematics
Email: umberto@math.unipd.it

Timetable: 10 hrs. Lectures in May or June or July or in Autumn.

Course requirements: No strict requirement for attending this course. A good mastery of mathematical proofs and formal modelling will be expected. Familiarity with basic notions in computational complexity (polynomial reductions, NP-completeness) and propositional logic (basic definitions, conjunctive normal form) will be useful.

Examination and grading: Final paper.

SSD: INF/01

Abstract: In this course I will provide an introduction to the various frameworks developed for the study of aggregation of individual expressions, with a focus on judgment aggregation, and explore in depth the main research questions arising in this field. Logic will be our travel companion: we will see that it is a natural tool to model individual views and rationality assumptions, and proves very useful in characterising domains in which aggregation can be performed in a safe way.

Course content: After introducing various aggregation frameworks in the first lecture, and exploring translations from one setting to the other, we will touch upon the most common problem in aggregation theory: paradoxes. We will show that most paradoxical situations, such as the Condorcet paradox in preference aggregation and the discursive dilemma in judgment aggregation, share a common structure. This will allow us to introduce the problem of collective rationality as a central research question in the study of aggregation. In the second lecture we will already show a characterisation result identifying all paradoxes that can be obtained using the majority rule. The third and fourth lectures will contain the central topics of the course, in which we will learn the two most important techniques used in proving characterisation, possibility and impossibility results in judgment aggregation and Social Choice Theory in general. First, we will focus on non-independent aggregation procedures and prove characterisation results that identify syntactically those domains in which aggregation can be performed safely. We will also show that recognising such domains is a hard computational problem (it sits in the second layer of the polynomial hierarchy). Second, we will show how to study the set of winning coalitions (i.e., sets of individuals that can force certain collective outcomes) in independent rules to obtain impossibility results. The course is ended with an overview of practical aggregation procedures for judgment aggregation recently proposed in the literature.

I will provide lecture notes at the beginning of the course.

Networking Issues and Solutions in Online Games

Prof. Claudio E. Palazzi[1]

[1] *University of Padova*
Department of Mathematics
Email: cpalazzi@math.unipd.it

Timetable: 12 hrs. Lectures in November/December 2014, Torre Archimede.

Course requirements: Background knowledge of Computer Networks

Examination and grading: Seminar and paper on a subject assigned by the Instructor

SSD: INF/01 Computer Science

Aim: To introduce students to issues and solutions related to online game networking

Course contents:

1. Introduction to online games
2. Online game architectures
3. Online game traffic characteristics
4. Interactivity, scalability, fairness and consistency
5. Network coexistence with other applications
6. Online gaming over ad-hoc networks
7. Cloud-based online gaming
8. Performance measurement

Preference Reasoning in Computational Social Choice and in Decision Support Systems

Dott.ssa Maria Silvia Pini[1]

[1] University of Padova
Department of Information Engineering
Email: pini@dei.unipd.it

Timetable: 12 hrs. First Lecture on September 16, 2014, 11:00 (dates already fixed, see the calendar), Torre Archimede, Room 2BC/30.

Course requirements: None

Examination and grading: The students' performance will be assessed for each course via an academic paper where the student will relate his research area with some of the topics presented in the course. Failure to submit papers within a required deadline, without prior endorsement by the lecturer, will be considered as an insufficient result.

SSD: ING-INF/05

Aim: I want to show the crucial role of preference reasoning in Computational Social Choice and in Decision Support Systems. Computational Social Choice is an interdisciplinary field of study at the interface of social choice theory and computer science, promoting an exchange of ideas in both directions. On the one hand, it is concerned with the application of techniques developed in computer science, such as complexity analysis or algorithm design, to the study of social choice mechanisms, such as voting procedures. On the other hand, computational social choice is concerned with importing concepts from social choice theory into computing, such as fairness and non-manipulability. In this course, I will show how preference reasoning is crucial in voting rules and in multiagent preference aggregation with uncertainty, where some agents reveal incomplete preferences. Also, I will also show two compact preference formalisms (soft constraints and CP-nets) to express preferences over combinatorial domains. Moreover, I will show how preference reasoning is central in stable matching problems, that have many practical applications in two-sided markets, like those that assign doctors to hospitals and students to schools. Finally, I will show how preference reasoning is central in two specific decision support systems: recommender systems (e.g., Amazon) and reputation systems (e.g., Tripadvisor).

Course contents: Computational social choice, preferences, voting rules, preference aggregation with uncertainty, compact preference formalisms, stable matching problems, recommender systems, and reputation systems.

Resilient, Parallel, Big Data Application Frameworks in X10

Vijay Saraswat[1]

[1] IBM T. J. Watson research center
Email: vijay@saraswat.org

Timetable: 12 hrs., First lecture on June 3, 2014, 11:00 (dates already fixed, see calendar) Torre Archimede, Room 2BC/30.

Course requirements: Java and/or C++, programming experience, introduction to concurrency

Examination and grading: Two in-class quizzes, one two-week programming assignment (code to be run on cluster)

SSD: INF/01

Aim: To introduce students to programming with large data sets using application frameworks developed in (Resilient) X10.

Course contents:

This course will introduce students to the use and design of resilient parallel application frameworks in X10, such as Map Reduce, Bulk Synchronous Parallel (BSP) programming, Streaming, Global Load Balancing etc. These frameworks are characterized by offering a very simple programming model for the user – basically, sequential programming – while taking care of distribution, scale-out, synchronization and parallelism. Hitherto such frameworks have typically been developed from the ground up in languages such as Java or C++. We show how these frameworks can be built in a small amount of code (often just a few hundred lines of code) in X10, a programming language built explicitly for productivity and performance at scale. We will also discuss programming in Resilient X10, an extension of X10 that permits programs to continue executing even when nodes fail.

Topics covered: Introduction to Big Data and data analysis problems. Introduction to X10 and the APGAS (Asynchronous, Partitioned Global Address Space model), and basic multi-place programming idioms. Map Reduce programming – Hadoop and the X10 Map Reduce engine. Graph analytics – between-ness centrality, k-clique, using Bulk Synchronous Parallelism. State-space search – unbalanced tree search problem. Global Matrix Library – sparse, distributed matrix computations.

Courses in collaboration with the Doctoral School on “Information Engineering”

Applied Functional Analysis

Prof. Gianluigi Pillonetto[1]

[1] *Dept. of Information Engineering*
University of Padova
Email: giapi@dei.unipd.it

Timetable: 28 hrs. (2 two-hours lectures per week): Classes on Tuesday and Thursday, 10:30 12:30. First lecture on Tuesday September 23rd, 2014. Room 318 DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements:

1. The classical theory of functions of real variable: limits and continuity, differentiation and Riemann integration, infinite series and uniform convergence.
2. The arithmetic of complex numbers and the basic properties of the complex exponential function.
3. Some elementary set theory.
4. A bit of linear algebra.

Examination and grading: Homework assignments and final test.

Aim: The course is intended to give a survey of the basic aspects of functional analysis, operator theory in Hilbert spaces, regularization theory and inverse problems.

Course contents:

1. *Review of some notions on metric spaces and Lebesgue integration*: Metric spaces. Open sets, closed sets, neighborhoods. Convergence, Cauchy sequences, completeness. Completion of metric spaces. Review of the Lebesgue integration theory. Lebesgue spaces.
2. *Banach and Hilbert spaces*: Normed spaces and Banach spaces. Finite dimensional normed spaces and subspaces. Compactness and finite dimension. Bounded linear operators. Linear functionals. The finite dimensional case. Normed spaces of operators and the dual space. Weak topologies. Inner product spaces and Hilbert spaces. Orthogonal complements and direct sums. Orthonormal sets and sequences. Representation of functionals on Hilbert spaces. Hilbert adjoint operator. Self-adjoint operators, unitary operators.
3. *Compact linear operators on normed spaces and their spectrum*: Spectral properties of bounded linear operators. Compact linear operators on normed spaces. Spectral properties of compact linear operators. Spectral properties of bounded self-adjoint operators, positive operators, operators defined by a kernel. Mercer Kernels and Mercer's theorem.
4. *Reproducing kernel Hilbert spaces, inverse problems and regularization theory*: Reproducing Kernel Hilbert Spaces (RKHS): definition and basic properties. Examples of RKHS. Function estimation problems in RKHS. Tikhonov regularization. Support vector regression and regularization networks. Representer theorem.

All the necessary material can be found in W. Rudin's book Principles of Mathematical Analysis (3rd ed., McGraw-Hill, 1976). A summary of the relevant facts will be given in the first lecture.

References:

[1] E. Kreyszig, Introductory Functional Analysis with Applications, John Wiley and Sons, 1978.

[2] M. Reed and B. Simon, Methods of Modern Mathematical Physics, vol. I, Functional Analysis, Academic Press, 1980.
[3] G. Wahba. Spline models for observational data. SIAM, 1990.
[4] C.E. Rasmussen and C.K.I. Williams. Gaussian Processes for Machine Learning. The MIT Press, 2006.
[5] R.T. Rockafellar. Convex analysis. Princeton University Press, 1996.

Applied Linear Algebra

Prof. Giorgio Picci[1]

[1] *University of Padova*
Email: picci@dei.unipd.it

Timetable: 20 hrs. Class meets everyWednesday and Friday, 10:30 12:30. First lecture on Wednesday, March 5th, 2014. Room DEI/G, 3-rd floor, Dept. of Information Engineering, via Gradenigo Building.

Course requirements: A good working knowledge of basic notions of linear algebra as for example in [1]. Some proficiency in MATLAB.

Examination and grading: Grading is based on homeworks or a written examination or both.

Aim: TWe study concepts and techniques of linear algebra that are important for applications with a special emphasis on linear Least Squares problems, their numerical treatment and their statistical interpretation. A wide range of exercises and problems will be an essential part of the course and constitute homework required to the student.

Course contents:

1. Review of some basic concepts of L.A. and matrix theory
2. Deterministic Least Squares and the projection theorem
3. Statistical Least squares
4. Numerical treatment of Least Squares problems and regularization techniques

References:

[1] Gilbert Strang's linear algebra lectures, from M.I.T. on You Tube
[2] Notes from the instructor

Computational Inverse Problems

Prof. Fabio Marcuzzi[1]

[1] *Dept. of Mathematics*
University of Padova
Email: marcuzzi@math.unipd.it

Timetable: 16 hrs. (2 two-hours lectures per week): Classes on Tuesday and Thursday, 10:30 - 12:30. First lecture on Tuesday February 25th, 2014. Room DEI/G, 3-rd floor, Dept. of Information Engineering, via Gradenigo Building.

Course requirements:

1. basic notions of linear algebra and, possibly, numerical linear algebra.
2. the examples and homework will be in Python (the transition from Matlab to Python is effortless).

Examination and grading: Homework assignments and final test.

Aim: We study numerical methods that are of fundamental importance in computational inverse problems. Real application examples will be given for distributed parameter systems. Computer implementation performance issues will be considered also.

Course contents:

1. definition of inverse problems, basic examples and numerical difficulties.
2. numerical methods for QR and SVD and their application to the square-root implementation in PCA, least-squares, model reduction and Kalman filtering; recursive least-squares;
3. regularization methods;
4. numerical algorithms for nonlinear parameter estimation: Gauss-Newton, Levenberg-Marquardt, back-propagation (neural networks), adjoint model (VDA);
5. examples with distributed parameter systems;
6. HPC implementations and parallel implementations on GPUs;

References:

[1] F.Marcuzzi "Analisi dei dati mediante modelli matematici", http://www.math.unipd.it/ marcuzzi/MNAD.html

[2] CUDA programming guide, http://docs.nvidia.com/cuda/index.html

Information theoretic Methods in Security

Prof. Nicola Laurenti[1]

[1] University of Padova
Department of Information Engineering
Email: nil@dei.unipd.it

Timetable: 20 hrs. (two lectures of two hours each per week). Class meets every Wednesday and Friday from 10:30 to 12:30, starting on Wednesday, October 1-st and ending on Wednesday, October 31-st, 2014. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic notions of Information Theory

Examination and grading: Each student must submit a project, and grading will be based on its evaluation. I encourage students to work from an information theoretic point of view on a security problem related to their research activities.

Aim: Provide the students with an information theoretic framework that will allow formal modeling, and understanding fundamental performance limits, in several security-related problems

Course contents: Topics will be chosen, according to the students' interests from the following

Measuring information. Review of basic notions and results in information theory: entropy, equivocation, mutual information, channel capacity.

The Holy Grail of perfect secrecy. Shannon's cipher system. Perfect secrecy. Ideal secrecy. Practical secrecy. The guessing attack.

Secrecy without cryptography. The wiretap channel model. Rate-equivocation pairs. Secrecy capacity for binary, Gaussian and fading channel models.

Security from uncertainty. Secret key agreement from common randomness on noisy channels. Information theoretic models and performance limits of quantum cryptography.

A different approach. Secrecy capacity from channel resolvability. Secret-key capacity from channel intrinsic randomness.

The gossip game. Broadcast and secrecy models in multiple access channels. The role of trusted and untrusted relays.

Secrets in a crowd. Information theoretic secrecy in a random network with random eavesdroppers. Secrecy graphs and large networks secrecy rates.

A cipher for free? Information theoretic security of random network coding.

Who's who? An information theoretic model for authentication in noisy channels. Signatures and fingerprinting.

Writing in sympathetic ink. Information theoretic models of steganography, watermarking and other information hiding techniques.

The jamming game. Optimal strategies for transmitters, receivers and jammers in Gaussian, fading and MIMO channels.

Leaky buckets and pipes. Information leaking and covert channels. Timing channels.

The dining cryptographers. Privacy and anonymity. Secure multiparty computation.

Information theoretic democracy. Privacy, reliability and verifiability in electronic voting systems.

References:

1. Y. Liang, H.V. Poor, and S. Shamai (Shitz), Information Theoretic Security, Now, 2007.
2. M. Bloch, J. Barros, Physical-Layer Security: from Information Theory to Security Engineering Cambridge University Press, 2011.

Mathematical modeling of cell Biology

Prof. Morten Gram Pedersen[1]

[1] Dept. of Information Engineering
University of Padova
Email: pedersen@dei.unipd.it

Timetable: 20 hrs.(2 two-hours lectures per week). Class meets every Monday from 10:30 to 12:30 and Wednesday from 1:30 to 3:30. First lecture on Monday, October 20, 2014. Room DEI/G, 3-rd floor, Dept. of Information Engineering, via Gradenigo Building.

Course requirements: Basic courses of linear algebra and ODEs. Basic experience with computer programming. Knowledge of cellular biology is not required.

Examination and grading: Homeworks and/or final project.

Aim: The aim of this course is to provide an introduction to commonly used mathematical models of cellular biology. At the end of the course, the students should be able to build models of biological processes within the cell, to simulate and analyze them, and to relate the results back to biology. The focus will be on electrical activity and calcium dynamics in neurons and hormone-secreting cells.

Course contents: Biochemical reactions; Ion channels, excitablity and electrical activity; Calcium dynamics; Intercellular communication; Spatial and stochastic phenomena (if time allows); Qualitative analysis of nonlinear differential equations.

References: The following books will provide the core material, which will be supplemented by research articles:

[1] C.P. Fall, E.S. Marland, J.M. Wagner, J.J. Tyson. Computational Cell Biology. Springer, NY, USA (2002).

[2] J. Keener, J. Sneyd: Mathematical Physiology. Springer, NY, USA (2004).

Random Graphs and Stochastic Geometry in Networks

Prof. Subhrakanti Dey[1]

[1] Signals and Systems
Uppsala University, Sweden
Email: Subhra.Dey@signal.uu.se

Timetable: 20 hrs. Class meets every Tuesday and Thursday from 2:30 to 4:30. First lecture on Tuesday, June 10-th, 2014. Room 318 DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Advanced calculus, and probability theory and random processes

Examination and grading: A project assignment for students in groups of 2 requiring about 20 hours of work.

Aim: To provide graduate students with some basic concepts of random graphs and stochastic geometry and illustrate their applications to relevant engineering problems involving networks, such as multiagent control networks, wireless communication networks etc.

Course contents:

- *Introduction to random graphs*: basic models and properties, random regular graphs, giant component, connectivity, degree sequence (2 lectures)
- *Basic Percolation Theory*: Tree percolation, lattice bond percolation (1 lecture)
- *Small world and scale free networks* (1 lecture)
- *Consensus and Gossip algorithms*: a short survey for distributed averaging, consensus over random switching graphs, consensus and gossip algorithms for distributed estimation (2 lectures)
- *Connectivity and capacity in wireless multihop networks* (1 lecture)
- *Stochastic Geometry and its applications*: Basic Point Process theory and properties, hard-core and Gibbs processes, Applications to characterizing interference and outage in networks (2 lecture)
- *Applications of Stochastic Geometry to wireless networks* (1 lecture)

References:

[1] Bella Bollobas, Random Graphs, Second Edition, Cambridge Studies in Advanced Mathematics, Cambridge University Press, UK, 2001.
[2] M. Haenggi, Stochastic Geometry for Wireless Networks, Cambridge University Press, New York, 2013.
[3] M. Grossglauser and P. Thiran, "Networks out of Control: Models and Methods for Random networks", Lecture notes, EPFL, 2012.
[4] M. Franceschetti and R. Meester, Random Networks for Communication: From Statistical Physics to Information Systems, Cambridge University Press, UK, 2007.

Various articles and papers will be referenced during the course for further reading.

Statistical methods

Prof. Lorenzo Finesso[1]

[1] *Istituto di Ingegneria Biomedica, ISIB-CNR, Padova*
Email: lorenzo.finesso@isib.cnr.it

Timetable: 24 hrs. (two lectures of two hours each, per week). Class meets every Monday and Wednesday from 10:30 to 12:30. First lecture on Monday, June 16, 2014. Room DEI/G (3-rd floor, Dept. of Information Engineering, Via Gradenigo 6/a, Padova).

Course requirements: Basics of Probability Theory and Linear Algebra.

Examination and grading: homework assignments and take-home exam.

Aim: The course will present a survey of statistical techniques which are important in applications. The unifying power of the information theoretic point of view will be stressed.

Course contents:

Background material. The noiseless source coding theorem will be quickly reviewed in order to introduce the basic notions of entropy and informational divergence (Kullback-Leibler distance) of probability measures. The analytical and geometrical properties of the divergence will be presented.

Divergence minimization problems. Three basic minimization problems will be posed and, on simple examples, it will be shown that they produce the main methods of statistical inference: hypothesis testing, maximum likelihood, maximum entropy.

Multivariate analysis methods. Study of the probabilistic and statistical aspects of the three main methods: Principal Component Analysis (PCA), Canonical Correlations (CC) and Factor Analysis (FA). In the spirit of the course these methods will be derived also via divergence minimization. Time permitting there will be a short introduction to the Nonnegative Matrix Factorization method as an alternative to PCA to deal with problems with positivity constraints.

EM methods. The Expectation-Maximization method was introduced as an algorithm for the computation of the Maximum Likelihood (ML) estimator with partial observations (incomplete data). We will derive the EM method for the classic mixture decomposition problem and also interpret it as an alternating divergence minimization algorithm (à la Csiszár Tusnády).

Hidden Markov models. We will introduce the simple yet powerful class of Hidden Markov models (HMM) and discuss parameter estimation for HMMs via the EM method.

The MDL method. The Minimum Description Length method of Rissanen will be presented as a general tool for model complexity estimation.

References: A set of lecture notes and a list of references will be posted on the web site of the course.

Calendar

The calendar is not completely filled in. Updated July 3, 2014

gennaio 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15 * Seminari Dottorato 14:30-16:00	16 * Seminario Geometria 13:00-14:30	17	18
19	20	21	22	23 * Seminario Geometria 14:30-16:00 * Zennaro-Vermiglio 15:00-17:00	24 * Zennaro-Vermiglio 10:00-12:00	25
26	27	28	29 * Seminari Dottorato 14:30-16:00	30 * Seminario Geometria 14:30-16:00 * Zennaro-Vermiglio 15:00-17:00	31 * Zennaro-Vermiglio 10:00-12:00	1
2	3	4	5	6	7	8

febbraio 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
26	27	28	29	30	31	1
2	3	4	5	6 * Zennaro-Vermiglio 15:00-17:00 * Seminario Geometria 14:30-16:00	7 * Zennaro-Vermiglio 10:00-12:00	8
9	10	11	12 * Seminari Dottorato 14:30-16:00	13 * Seminario Geometria 14:30-16:00	14	15
16	17 * Nagy 09:00-11:00	18 * Nagy 09:00-11:00	19 * Nagy 09:00-11:00	20 * Nagy 09:00-11:00 * Seminario Geometria 14:30-16:00	21 * Nagy 09:00-11:00	22
23	24 * Nagy 09:00-11:00	25 * Marcuzzi 10:30-12:30	26 * Seminari Dottorato 14:30-16:00 * Nagy 09:00-11:00	27 * Zennaro-Vermiglio 14:00-16:00 * Marcuzzi 10:30-12:30	28 * Zennaro-Vermiglio 10:00-12:00	1
2	3	4	5	6	7	8

marzo 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
23	24	25	26	27	28	1
2	3	4 * Vargiolu 14:00-16:00 * Marcuzzi 10:30-12:30	5 * Vargiolu 15:00-17:00 * Picci 10:30-12:30	6 * Zennaro-Vermiglio 13:30-15:30 * Bardi 09:30-11:15 * Zennaro-Vermiglio 16:00-18:00 * Marcuzzi 10:30-12:30	7 * Zennaro-Vermiglio 09:00-10:30 * Bardi 09:30-11:15 * Picci 10:30-12:30	8
9	10	11 * Vargiolu 14:00-16:00 * Marcuzzi 10:30-12:30	12 * Seminari Dottorato 14:30-16:00 * Picci 10:30-12:30	13 * Zennaro-Vermiglio 13:00-15:30 * Bardi 09:30-11:15 * Marcuzzi 10:30-12:30	14 * Bardi 09:30-11:15 * Picci 10:30-12:30	15
16	17	18 * Vargiolu 14:00-16:00 * Marcuzzi 10:30-12:30	19 * Vargiolu 15:00-17:00 * Picci 10:30-12:30	20 * Bardi 09:30-11:15 * Marcuzzi 10:30-12:30	21 * Bottacin 14:00-16:00 * Bardi 09:30-11:15 * Picci 10:30-12:30	22
23	24	25 * Bottacin 11:00-13:00	26 * Seminari Dottorato 14:30-16:00 * Picci 10:30-12:30	27 * Bardi 09:30-11:15	28 * Bardi 09:30-11:15 * Picci 10:30-12:30	29
30	31	1	2	3	4	5

aprile 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
30	31	1 * Bottacin 11:00-13:00	2 * Picci 10:30-12:30	3 * Bardi 09:30-11:15	4 * Bardi 09:30-11:15 * Picci 10:30-12:30	5
6	7	8 * Bottacin 11:00-13:00	9 * Seminari Dottorato 14:30-16:00	10 * Spiga 11:30-13:30 * Bardi 09:30-11:15	11 * Spiga 11:30-13:30 * Bardi 09:30-11:15	12
13	14	15 * Bottacin 11:00-13:00	16	17 * Spiga 11:00-13:00	18	19
20	21	22	23	24	25	26
27	28	29 * Bottacin 11:00-13:00 * Seminari Dottorato 14:30-15:30 (?!)	30 * Seminari Dottorato 14:30-16:00 (forse anticipa al 29/04) * Fiorini 16:00-18:00	1	2	3
4	5	6	7	8	9	10

maggio 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
27	28	29	30	1 * Holiday	2	3
4	5	6 * Bottacin 11:00-13:00	7 * Fiorini 16:00-18:00 * Seminari Dottorato 14:30-16:00	8 * Spiga 11:00-13:00	9 * Spiga 11:00-13:00 * Fiorini 14:00-16:00	10
11	12	13 * Bottacin 11:00-13:00	14	15 * Spiga 11:00-13:00	16 * Spiga 11:00-13:00	17
18	19	20	21 * Seminari Dottorato 14:30-16:00 * Fiorini 16:00-18:00	22 * Jeanblanc-ElKaroui 15:00-18:00 * Spiga 11:00-13:00	23 * Spiga 11:00-13:00 * Fiorini 14:00-16:00	24
25	26 * Jeanblanc-ElKaroui 10:00-13:00 * Jeanblanc-ElKaroui 14:30-17:30	27 * Jeanblanc-ElKaroui 10:00-13:00 * Bambusi 14:30-17:30 * Jeanblanc-ElKaroui 14:30-17:30	28 * Jeanblanc-ElKaroui 10:00-13:00 * Bambusi 09:30-12:30 * Barbato-Dai Pra 15:00-17:00	29 * Barbato-Dai Pra 15:00-17:00 * Bambusi 09:30-12:30	30 * Fiorini 14:00-16:00 * Bambusi 09:30-12:30	31
1	2	3	4	5	6	7

giugno 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
1	2	3 * Barbato-Dai Pra 15:00-17:00 * Saraswat 11:00-13:00	4 * Seminari Dottorato 14:30-16:00 * Fiorini 16:00-18:00 * Saraswat 11:00-13:00	5 * Barbato-Dai Pra 15:00-17:00 * Saraswat 11:00-13:00	6 * Fiorini 14:00-16:00 * Rinaldi-Fasano 10:00-13:00	7
8	9 * Rinaldi-Fasano 10:00-13:00 * Barbato-Dai Pra 15:00-17:00	10 * Barbato-Dai Pra 16:30-18:30 * Saraswat 11:00-13:00 * Dey 14:30-16:30	11 * Fiorini 16:00-18:00 * Saraswat 11:00-13:00 * Rinaldi-Fasano 14:00-16:00	12 * Saraswat 11:00-13:00 * Rinaldi-Fasano 14:00-16:00 * Dey 14:30-16:30	13	14
15	16 * Finesso 10:30-12:30	17 * Barbato-Dai Pra 10:30-12:30 * Dey 14:30-16:30	18 * Seminari Dottorato 14:30-16:00 * Fiorini 16:00-18:00 * Finesso 10:30-12:30	19 * Rinaldi-Fasano 11:00-13:00 * Dey 14:30-16:30	20 * Barbato-Dai Pra 10:30-12:30	21
22	23 * Maddalena 16:30-18:30 * Finesso 10:30-12:30	24 * Conti 09:00-13:00 * Dey 14:30-16:30	25 * Barbato-Dai Pra 15:00-17:00 * Finesso 10:30-12:30	26 * Conti 09:00-13:00 * Conti 14:00-16:00 * Maddalena 16:30-18:30 * Dey 14:30-16:30	27 * Maddalena 16:30-18:30 * Barbato-Dai Pra 11:00-13:00 * Conti 11:00-13:00	28
29	30 * Finesso 10:30-12:30	1	2	**3**	4	5
6	7	8	9	10	11	12

luglio 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
29	30	1 * Maddalena 14:30-16:30 * Dey 14:30-16:30	2 * Finesso 10:30-12:30	**3** * Maddalena 16:30-18:30 * Dey 14:30-16:30	4 * Maddalena 09:00-11:00	5
6	7 * Finesso 10:30-12:30	8 * Dey 14:30-16:30	9 * Barbato-Dai Pra 10:30-12:30 * Finesso 10:30-12:30	10 * Dey 14:30-16:30	11 * Barbato-Dai Pra 10:30-12:30	12
13	14 * Vardanega 14:30-17:30 * Finesso 10:30-12:30	15 * Vardanega 09:30-12:30 * Dey 14:30-16:30	16 * Vardanega 14:30-17:30 * Finesso 10:30-12:30	17 * Vardanega 09:30-12:30 * Dey 14:30-16:30	18 * Vardanega 09:30-12:30	19
20	21 * Finesso 10:30-12:30	22 * Vardanega 09:30-12:30 * Dey 14:30-16:30	23 * Finesso 10:30-12:30	24 * Dey 14:30-16:30	25 * Vardanega 09:30-12:30	26
27	28	29 * Dey 14:30-16:30	30	31 * Dey 14:30-16:30	1	2
3	4	5	6	7	8	9

agosto 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
27	28	29	30	31	1	2
3	4	5 * Dey 14:30-16:30	6	7 * Dey 14:30-16:30	8	9
10	11	12 * Dey 14:30-16:30	13	14 * Dey 14:30-16:30	15	16
17	18	19 * Dey 14:30-16:30	20	21 * Dey 14:30-16:30	22	23
24	25	26 * Dey 14:30-16:30	27	28 * Dey 14:30-16:30	29	30
31	1	2	3	4	5	6

settembre 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
31	1	2 * Dey 14:30-16:30	3	4 * Dey 14:30-16:30	5	6
7	8	9 * Dey 14:30-16:30	10	11 * Dey 14:30-16:30	12	13
14	15	16 * Pini 11:00-13:00 * Dey 14:30-16:30	17	18 * Pini 11:00-13:00 * Dey 14:30-16:30	19 * Pini 11:00-13:00 * Pini 14:00-16:00	20
21	22 * Pini 14:00-16:00	23 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	24	25 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	26 * Pini 11:00-13:00	27
28	29	30 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	1	2	3	4
5	6	7	8	9	10	11

ottobre 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
28	29	30	1 * Laurenti 10:30-12:30	2 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	3 * Laurenti 10:30-12:30	4
5	6	7 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	8 * Laurenti 10:30-12:30	9 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	10 * Laurenti 10:30-12:30	11
12	13	14 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	15 * Laurenti 10:30-12:30	16 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	17 * Laurenti 10:30-12:30	18
19	20 * Pedersen 10:30-12:30	21 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	22 * Laurenti 10:30-12:30 * Pedersen 13:00-15:00	23 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	24 * Laurenti 10:30-12:30	25
26	27 * Pedersen 10:30-12:30	28 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	29 * Laurenti 10:30-12:30 * Pedersen 13:00-15:00	30 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	31 * Laurenti 10:30-12:30	1
2	3	4	5	6	7	8

novembre 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
26	27	28	29	30	31	1
2	3 * Pedersen 10:30-12:30	4 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	5 * Pedersen 13:00-15:00	6 * Dey 14:30-16:30 * Pillonetto 10:00-12:00	7	8
9	10 * Pedersen 10:30-12:30	11 * Dey 14:30-16:30	12 * Pedersen 13:00-15:00	13 * Dey 14:30-16:30	14	15
16	17 * Pedersen 10:30-12:30	18 * Dey 14:30-16:30	19 * Pedersen 13:00-15:00	20 * Dey 14:30-16:30	21	22
23	24	25 * Dey 14:30-16:30	26	27 * Dey 14:30-16:30	28	29
30	1	2	3	4	5	6

dicembre 2014

domenica	lunedì	martedì	mercoledì	giovedì	venerdì	sabato
30	1	2 * Dey 14:30-16:30	3	4 * Dey 14:30-16:30	5	6
7	8	9 * Dey 14:30-16:30	10	11 * Dey 14:30-16:30	12	13
14	15	16 * Dey 14:30-16:30	17	18 * Dey 14:30-16:30	19	20
21	22	23 * Dey 14:30-16:30	24	25 * Christmas * Dey 14:30-16:30	26	27
28	29	30 * Dey 14:30-16:30	31	1	2	3
4	5	6	7	8	9	10