

Graduate School in Information Engineering: Ph.D. program
Department of Information Engineering
University of Padova

Course Catalogue
2010

Requirements for Ph.D. Students of the Graduate School of Information Engineering:

1. Students are required to take courses from the present catalogue for a *minimum* of 80 hours (20 credits) during the first year of the Ph.D. program.
2. Students are required to take for credit *at least* two out of the following three basic courses “Applied Functional Analysis”, “Applied Linear Algebra”, and “Statistical Methods” during the first year of the Ph.D. program. Moreover, the third course is *strongly recommended* to all students.
3. After the first year, students are *strongly encouraged* to take courses (possibly outside the present catalogue) for at least 10 credits (or equivalent) according to their research interests.

Students have to enroll in the courses they intend to take at least one month before the class starts. To enroll, it is sufficient to send an e-mail message to the secretariat of the school at the address `calore@dei.unipd.it`

Students are expected to attend classes regularly. Punctuality is expected both from instructors and students.

Instructors have to report to the Director of Graduate Studies any case of a student missing classes without proper excuse.

Contents

1	Applied Functional Analysis, Prof. G. Pillonetto	5
2	Applied Linear Algebra, Prof. T. Damm and Prof. H. Wimmer	7
3	Bilinear Control Systems: Theory and Applications, Prof. C. Altafini	8
4	Bioelectromagnetics, Prof. T. A. Minelli	10
5	Design of Radiofrequency Integrated Circuits, Prof. A. Neviani	12
6	Design Patterns in Software Development, Prof. G. Manduchi	13
7	Dose, Effect, Threshold, Prof. A. Trevisan	14
8	Electrostatic Discharge in Integrated Circuits, Prof. G. Meneghesso	15
9	Game Theory for Information Engineering, Prof. L. Badia	16
10	High-frequency techniques in electromagnetism - Antennas and secondary radiation, Prof. G. Pelosi	18
11	Identifiability of Linear and Nonlinear Systems, Prof. M.P. Saccomani	19
12	Information-theoretic Methods in Security, Prof. N. Laurenti	20
13	Introduction to Quantum Optics, Prof. P. Villoresi	22
14	Learning with Structural Kernels: from theory to practice, Prof. A. Moschitti	23
15	Mathematical Modeling, Prof. P. Misra	24
16	Project Management, Prof. L. Vangelista	26

17 Satellite Navigation Systems, Prof. O. Pozzobon and Prof. L. Vangelista	27
18 Statistical Methods, Prof. L. Finesso	29
19 Topics in Quantum Information, Prof. F.Ticozzi	30

1 Applied Functional Analysis

Instructor: Prof. G. Pillonetto, Dept. Information Engineering, University of Padova,
e-mail: giapi@dei.unipd.it

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.

Topics:

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. *Fourier transform and convolution:* The convolution product and its properties. The basic L^1 and L^2 theory of the Fourier transform. The inversion theorem.
4. *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.
5. *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.

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.

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.

Time table: Course of 28 hours (2 two-hours lectures per week): Classes on Tuesday and Thursday, 10:30 - 12:30. First lecture on Tuesday September 21, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Examination and grading: Homework assignments and final test.

2 Applied Linear Algebra

Instructors:

Tobias Damm, TU Kaiserslautern, Germany
e-mail: damm@mathematik.uni-kl.de

Harald Wimmer, University of Würzburg, Germany
e-mail: wimmer@mathematik.uni-wuerzburg.de

Aim: We study concepts and techniques of linear algebra that are important for applications and computational issues. A wide range of exercises and problems will be presented such that a practical knowledge of tools and methods of linear algebra can be acquired.

Topics:

- *Kronecker products*
- *Sylvester and Lyapunov matrix equations*
- *Least squares problems and singular value decomposition*
- *Computational methods*
- *Perturbation theory*

References:

- [1] E. Gregorio and L. Salce. *Algebra Lineare*. Edizioni Libreria Progetto, Padova, 2005.
- [2] A.J. Laub. *Matrix Analysis for Scientists and Engineers*, SIAM, Philadelphia, 2005,
- [3] C.D. Meyer. *Matrix Analysis and Applied Linear Algebra*, SIAM, Philadelphia, 2000.
- [4] L. N. Trefethen and D. Bau *Numerical Linear Algebra*. SIAM, Philadelphia, 2000.

Course requirements: A good working knowledge of basic notions of linear algebra, as e.g. presented in [1].

Time table: Course of 16 hours (2 two-hours lectures per week): Classes on Tuesday and Thursday, 4:30 – 6:30. First lecture on Tuesday, March 9, 2010. **Classroom Oe** (Dept. of Information Engineering, via Gradenigo Building).

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

3 Bilinear Control Systems: Theory and Applications

Instructor: Claudio Altafini, SISSA (Int. School for Advanced Studies), Trieste.
e-mail: altafini@sissa.it

Aim: Bilinear Systems are an important class of nonlinear control systems. The course aims at giving an overview of the main control problems and of some of the mathematical tools (notably differential geometric and Lie algebraic methods) required in the study of bilinear control systems.

Topics:

1. Introductory material
 - manifolds, vector fields, tangent spaces;
 - orbits of vector fields and Frobenius Theorem;
 - controllability and Chow Theorem;
 - drift versus driftless systems, accessibility versus controllability;
2. Bilinear control systems
 - bilinear systems and matrix transition Lie groups;
 - structure of matrix Lie groups (homogeneous spaces, transitivity, exponential map and canonical coordinates);
 - Lie algebras (Levi decomposition, semisimplicity, solvability, nilpotency, Cartan criteria);
 - controllability properties for bilinear control systems on matrix Lie groups;
3. Control methods
 - feedback linearization;
 - system inversion and differential flatness;
 - feedback stabilization;
4. Applications
 - rigid body motion (rigid bodies on $SO(3)$ and $SE(3)$; system on a sphere);
 - nonholonomic systems (trailer systems, chained form);
 - switching systems (simultaneous stability);
 - quantum control systems (Shrodinger equation, Liouville equation).

References: There is no book specific for the geometric aspect of bilinear control systems that will be treated in the course. Some parts can be found in

[1] V. Jurdjevic. *Geometric Control Theory*, Cambridge Univ. Press. 1997.

Reading material will be provided during the course.

Time table: Course of 16 hours. Lectures (2 hours) on Monday and Wednesday 2:30 – 4:30. First lecture on Monday, May 3, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic courses of automatic control and linear systems theory.

Examination and grading: The grading will be based on homeworks.

4 Bioelectromagnetics

Instructor: Prof. Tullio A. Minelli, CIRMANMEC University of Padova, e-mail: minelli@pd.infn.it.

Aim: Comprehension of bio-physics and bio-mathematical instruments underlying cell and tissue electromagnetic stimulation. A phenomena survey.

Topics:

1. Basics of bioelectromagnetics.
2. Neuroelectrical phenomena.
3. Chaos, fractals, solitons and neuroelectrical signals.
4. Mobile phone radiation and neuroelectrical phenomena.
5. Neurodegeneration: Bio-physical and bio-mathematical phenomenology.
6. Mathematical models of cell membrane dynamics.

References:

- [1] C. Polk and E. Postow. CRC handbook of biological effects of electromagnetic fields. Boca Raton, CRC Press 1986.
- [2] C.H. Durney and D.A. Christensen. Basic introduction to bioelectromagnetics. Boca Raton, CRC Press, 2000.
- [3] S. Deutsch and A. Deutsch. Understanding the nervous system. An Engineering perspective. New York: IEEE, 1993.
- [4] S.S. Nagarajan. A generalized cable equation for magnetic stimulation of axons. IEEE Transactions on biomedical Engineering, 43, 304-312, 1996.
- [5] M. Balduzzo, F. Ferro Milone, T.A. Minelli, I. Pittaro Cadore and L. Turicchia: Mathematical phenomenology of neural synchronization by periodic fields, Nonlinear Dynamics, Psychology and Life Sciences 7, pp.115-137, 2003.
- [6] A. Vulpiani. Determinismo e caos. La nuova Italia Scientifica, Roma, 1994.
- [7] T.A. Minelli, M. Balduzzo, F. Ferro Milone and V. Nofrate: Modeling cell dynamics under mobile phone radiation. Nonlinear Dynamics, Psychology and Life Sciences, to appear.
- [8] Report on the potential health risk of Radiofrequency Fields (the Royal Society of Canada, 2001-2003).
- [9] C.P. Fall. Computational Cell Biology. Berlin, Springer, 2002.
- [10] J.D. Murray. Mathematical Biology. Berlin: Springer-Verlag, 1993.
- [11] Bioinitiative Report, 2007 in <http://www.bioinitiative.org/report/index.htm>

Time table: Course of 12 hours plus a visit to an electro-physiology laboratory. Lectures (2 hours) on Friday 11:00 – 13:00. First lecture on Friday, January 8, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: None.

Examination and grading: Production of simple pedagogical circuits or measures and simulations of biophysical interest.

5 Design of Radiofrequency Integrated Circuits

Instructor: Prof. Andrea Neviani, Department of Information Engineering, Univ. of Padova, e-mail: nevigiani@dei.unipd.it

Aim: to study the architecture and the basic building blocks of integrated radiofrequency (RF) transceivers used in today's and future wireless communication systems.

Topics: Main performance metrics of RF transceivers. Impedance matching. Passive components in modern CMOS technologies. Design techniques for integrated low-noise amplifiers and mixers. Noise analysis in mixers. Sinusoidal oscillators. Phase noise in oscillators.

References:

- [1] T.H. Lee, "The Design of CMOS Radio-Frequency Integrated Circuits", Cambridge University Press, 2004.
- [2] B. Razavi, "RF Microelectronics", Prentice Hall, 1998.

Time table: Course of 20 hours (2 two-hour lectures per week). Classes on Tuesday and Thursday 10:30 – 12:30. First class on Tuesday, April 20, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic knowledge of analog circuit design.

Examination and grading: Homeworks (40%) and final project (60%).

6 Design Patterns in Software Development

Instructor: Gabriele Manduchi, Istituto Gas Ionizzati del CNR,
e-mail: gabriele.manduchi@igi.cnr.it

Aim: Introduction of Design Patterns in software development. The course is centered around a case study in software development in "e-Science". A graphical front-end for browsing and visualizing scientific data is progressively refactored using important design patterns for object-oriented software. The use of design patterns is introduced by presenting some Java programs in order to highlight recurrent problems and solutions in software development. An introduction to UML and the Unified Process is presented at the beginning of the course.

Topics:

1. **Advanced Java Programming:** the case study refers to a graphical waveform browser for networked scientific data.
2. **Design Patterns definition:** design patterns are introduced step by step during the refactoring stages. Finally an overview of the most useful design patterns which have not been encountered in the case study is provided.
3. **UML Modelling:** a subset of UML will be used thorough the course to represent class organization and component relationships.
4. **Unified Process:** The steps in the case study are presented in the more general framework of the Unified Process, by first analyzing Use Cases and then introducing the basic architecture.

References:

1. E. Gamma, R. Helm, R. Jonson, J. Vlissides: Design Patterns: Elements of Reusable Object Oriented Software, Addison Wesley 1995
2. Henry Gardner, Gabriele Manduchi: Design Patterns for e-Science Springer, 2007.
3. John Hunt: Guide to the Unified Process, Springer 2003.

Time table: Course of 20 hours. Lectures (two hours) on Monday and Thursday 8:30 – 10:30. First lecture on Monday, November 8, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic Java programming, Object-Oriented terminology and methods

Examination and grading: A project will be assigned to students, and will represent the base of the final discussion

7 Dose, effect, threshold

Instructor: Prof. Andrea Trevisan, Dipartimento di Medicina Ambientale e Sanità Pubblica, Univ. di Padova, e-mail: andrea.trevisan@unipd.it

Aim: understanding of biological mechanisms that are the basis of the effect of chemical, physical and biological agents in humans. To supply a critical evaluation of the reference data on biological effects of electromagnetic fields.

Topics: General introduction to cell biology and mechanisms of pharmacokinetics. The dose and the significance of threshold. The effect (response) of the dose. Methods to define the threshold. The significance of cancer and the threshold problem. Electromagnetic fields and general aspects related to the dose and the effect.

References: Handouts provided by the instructor.

Time table: Course of 12 hours. Lectures (2 hours) on Thursday 10:30 – 12:30. First lecture on Thursday, Jan. 14, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: None.

Examination and grading: Oral exam.

8 Electrostatic Discharge in Integrated Circuits

Instructor: Gaudenzio Meneghesso, Dept. Ingegneria dell'Informazione (DEI), University of Padova, e-mail: gaudenzio.meneghesso@unipd.it

Aim: This course is intended to provide an introduction coverage of the Electrostatic Discharge (ESD) problem in modern Integrated Circuits (ICs). There are several reasons that indicate the ESD problem as one of the most critical issues in modern ICs to be faced, among others: a) with the continuous technology scaling down, in the deca-nanometer dimension, devices can not sustain voltages larger than 1 V, hence these devices are extremely sensitive to electrostatic discharge and an adequate ESD protection becomes quite difficult to provide; b) very high speed RF circuits need ESD protection devices that do not affect their RF performances by altering the input/output matching, so suitable ESD protection elements must be developed; c) automotive industry is making very comfortable and secure cars by filling them with as much electronics as possible working in a very hostile ambient, a suitable ESD protection of these devices is not trivial. These are only a few examples that however give an impression of how much critical will be the ESD aspect in the future ICs.

Topics:

1. Basics of the Electrostatic Discharge phenomena;
2. Test Methods;
3. Active and passive ESD protection;
4. Device Physics of the most common ESD protection elements;
5. Characterization of ESD protection elements;
6. Failure Modes, Reliability Issues and Case Studies;
7. Circuit Simulation basics: approaches and applications.

References:

- [1] Amerasekera, C. Duvvury, ESD in Silicon Integrated Circuits, Wiley 2002 (Second Edition).
- [2] Z. H. Wang, On Chip ESD Protection for Integrated Circuits, Kluwer Academic Publisher, 2002.
- [3] S. Dabral, T. J. Maloney, Basic ESD and I/O Design, Wiley Interscience, 1998.

Time table: Course of 20 hours (2 two-hours lectures per week): Classes on Monday 2:30 – 4:30 and Thursday, 2:30 – 4:30. First lecture on October 25, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Introductory course of device physics: Microelectronics

Examination and grading: Design and SPICE verification of an ESD protection network.

9 Game Theory for Information Engineering

Instructor: Leonardo Badia, e-mail: leonardo.badia@gmail.com

Aim: Nowadays, micro-economics instruments have exited their traditional scope and have penetrated into many other research areas. The introduction of such concepts and techniques within scientific reasoning is becoming more and more common, and this especially applies to subjects related to technology and applications, such as information engineering, which are impacted by business models and customer choices. Game-theory has since long represented one of the most interesting branches of micro-economics, particularly due to its wide range of applications and its ability of giving a mathematical formulation to a plethora of problems. Even though the convergence of game-theory and information engineering problems looks very promising, several issues are still open and it is reasonable to think of them as main research directions in the immediate future.

For these reasons, it is important for an information engineer to be aware of game-theoretical concepts and instruments, while at the same time, whenever possible, being capable to bring them into use. The knowledge of game-theory fundamentals enables not only the understanding of several contributions recently appeared in the scientific literature, but also to identify possible developments of this pioneering work and solutions to the problems they have found.

Topics The list of topics covered in the course is as follows.

First part (game-theory):

- Equilibrium concepts. Pareto dominance.
- Choices and utilities. Rationality. Indifference.
- Games. Non-cooperation. Strategies.
- Nash equilibrium. The Prisoner's dilemma.
- Pure and mixed strategies. Dominance of strategies. Multiple equilibria.
- Dynamic games. Repeated games.
- Cooperation. Pricing. Imperfect/incomplete information. Bayesian equilibrium.
- Signaling. Beliefs.

Second part (application to information engineering):

- Resource sharing, cooperation versus competition.
- Game-theoretic power control and admission control.
- ALOHA as a non cooperative game.
- The price of selfish routing. The Forwarder's dilemma.
- Cooperation enforcement in communication networks.

- Optimization problems in game-theory. How to solve them, and how complex it is.
- Future developments and applications.

References:

[1] R. Gibbons, "Game theory for applied economists."

[2] H. R. Varian, "Microeconomic Analysis."

Further material presented during the course (basically, up-to-date articles recently appeared in the literature).

Time table: Course of 20 hours (2 two-hours lectures per week): Classes on Wednesday 10:30 – 12:30 and Friday, 10:30 – 12:30. First lecture on Wednesday March 3, 2010.

Course requirements: Very basic principles of calculus (typically, already available after two math undergraduate courses).

Basic principles of optimization (a dedicated course on optimization theory might help, although it is not strictly necessary, if some optimization principles are presented in basic math courses).

A basic course in Computer Networks and/or Communication Networks is required. The students should master for example concepts like: Ad Hoc Networks, Routing Protocol, ALOHA, Collision Detection. Expertise in the field of Cognitive Networks is useful, but not mandatory.

Examination and grading: The examination may consist of two parts (to harmonize the course with the rest of the PhD program, one of them can be avoided if needed). Neither part is necessarily to be performed before the other.

Part one: a written proposal (in the form of an extended abstract limited to about 3 pages including references) on a possible development and application of the topics explored by the course. The student is free to relate it to its own research goals.

Part two: a presentation in front of the class of a recent research paper on course-related subjects. The students are free to present a paper of their choice, if compatible with the course's scope. This should be in any case related to the written proposal. The presentation is limited to a 20-minute conference-like (aided with slides) setup, plus questions from the teacher and the audience (if present).

Grading: it is determined by the numerical average of the two parts, with equal weights.

10 High-frequency techniques in electromagnetism - Antennas and secondary radiation

Instructor: Giuseppe Pelosi, Department of Electronics and Telecommunications, University of Florence, Italy. e-mail: giuseppe.pelosi@unifi.it

Aim: The purpose of the course is to bridge the gap between the usual approach to antenna theory and design, where the source is supposed to be alone in an unbounded homogeneous medium, and the real world, where any antenna is installed in the proximity of many other perturbing objects.

Topics: The course deals with three main topics:

- a. Antennas in their operational environment;
- b. Radar cross section of complex targets;
- c. Radiating systems: advanced studies of reflector antennas.

References:

1. E.F. Knott et al., Radar Cross Section, Artech House, Boston, MA, 1993
2. P. Ya. Ufimtsev, Theory of edge diffraction in electromagnetics, Tech Science Press, Encino, CA, 2003
3. C.A. Balanis, Advanced engineering electromagnetic techniques: recent advances and applications, J. Wiley & Sons, New York, 1995.

Time table: Course of 12 hours (2 two-hours lectures per week): Classes on Thursday 2:30 – 4:30 and Friday, 10:30 – 12:30. First lecture on Thursday February 18, 2010. Last lecture will be on Friday, March 5, 2010, **8:30 – 10:30**.

Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: The student background must include at least one course on basic electromagnetic fields and waves.

Examination and grading: Homework assignment and final project.

11 Identifiability of Linear and Nonlinear Systems

Maria Pia Saccomani: Dept. of Information Engineering, University of Padova,
e-mail: pia@dei.unipd.it

Aim: The course is intended to give a survey of the methods to check a priori identifiability of linear and nonlinear dynamical systems. In particular, the course is intended to provide a deep comprehension of the modern differential algebra tools which have been applied to the study of a priori identifiability of dynamic systems described by polynomial or rational equations [1, 2, 3]. Emphasis will be given to systems describing biological phenomena.

Topics: State space linear and nonlinear dynamical models. Global and local parameter identifiability. Basic concepts of differential algebra. Software tool implementations. Case studies.

References:

- [1] F. Ollivier. *Le problème de l'identifiabilité structurelle globale: étude théorique, méthodes effectives et bornes de complexité*. Thèse de Doctorat en Science, École Polytechnique, Paris, France (1990).
- [2] L. Ljung, and S.T. Glad. On global identifiability for arbitrary model parameterizations, *Automatica*, 30, 2, 265–276 (1994).
- [3] M.P. Saccomani, S. Audoly, and L. D'Angiò. Parameter identifiability of nonlinear systems: the role of initial conditions, *Automatica*, 39, 619–632 (2004).

Time table: Course of 12 hours. Classes (2 hours) on Tuesday and Friday 10:30–12:30. First lecture on Tuesday November 9, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Examination and grading: Homework and a final written examination.

12 Information-theoretic Methods in Security

Instructor: Nicola Laurenti, Department of Information Engineering, Univ. of Padova, e-mail: `nil@dei.unipd.it`

Aim: To provide the students with an information theoretic framework to formalize modeling and understand fundamental performance limits in several security-related problems

Topics:

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

The Holy Grail of perfect secrecy. Shannon's cipher system. Different definitions of perfect secrecy. Practical secrecy.

Security from uncertainty. Information theoretic models and limits of quantum cryptography and quantum key distribution.

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

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

A different approach. Secret key agreement from common randomness on fading channels. The secrecy capacity and resolvability of fading channels.

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 (and information theoretic democracy). Privacy and anonymity. Secure multiparty computation. Electronic voting.

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, 2010.

A list of reference papers for each lecture will be provided during class meetings.

Time table: Course of 20 hours (2 two-hour lectures per week). Class meets every Wednesday and Friday from 10:30 to 12:30, starting on Wednesday, October 6 and ending on Friday, November 5. 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.

13 Introduction to Quantum Optics

Instructor: Paolo Villorosi, Dept. Information Engineering, University of Padova,
e-mail: paolo.villoresi@unipd.it

Aim: The course is intended to provide the basic concepts of current Quantum Communications in the optical domain. The initial part will review the underlying physical concepts, while in the second part the topics of entanglement, quantum interference, teleportation, quantum computation and quantum key distribution will be addressed. The experimental implementations of these topics will be discussed.

The course is organized in the Framework of the projects QuantumFuture ("Progetto Strategico di Ateneo") and QUINTET.

Topics:

1. Review of Quantum Mechanics;
2. quantization of EM field;
3. statistics of radiation;
4. entanglement;
5. quantum interferometry.
6. Applications: teleportation, quantum computation and quantum key distribution.

Laboratory: The Course include a Laboratory session on single photon generation and detection, and statistics of radiation.

References: Gerry C, Knight P, Introductory Quantum Optics (Cambridge 2005)

Time table: Course of 20 hours (2 two-hour lectures per week). Class meets every Monday and Wednesday from 10:30 to 12:30, starting on Monday, March 15, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic concept of Quantum Physics.

Examination and grading: Homework and final exam.

14 Learning with Structural Kernels: from theory to practice

Instructor: Alessandro Moschitti, e-mail: moschitti@disi.unitn.it

Aim: to provide the attendees with basic principles and techniques of machine learning as well as with the latest tools of statistical learning theory for fast and effective application design, i.e. structural kernels and Support Vector Machines. The practical examples focused on Natural Language Processing and Information Retrieval also provide some insights in these fields.

Topics: Basic machine learning concepts: concept learning, Decision Trees, Naive B  yes classifiers, parameterization and feature selection. Performance measurements: empirical error estimation, n-fold cross validation, learning and testing computational complexity. Introduction to PAC Learning: formal PAC definition, examples of PAC learnable functions and VC-dimension. Advanced Statistical Learning: Perceptron, Support Vector Machines (classification, regression and ranking), Kernel Methods for structured data. Application examples on Natural Language Processing and Information Retrieval fields: text categorization, question and answer categorization and semantic role labeling.

References:

- [1] Roberto Basili and Alessandro Moschitti. Automatic Text Categorization: from Information Retrieval to Support Vector Learning. Aracne Publisher, 2005.
- [2] Nello Cristianini and John Shawe-Taylor. An introduction to Support Vector Machines. Cambridge University Press, 2000.
- [3] T. M. Mitchell. Machine Learning. McGraw-Hill, 1997.
- [4] J. Shawe-Taylor and N. Cristianini. Kernel Methods for Pattern Analysis. Cambridge University Press, 2004.

Time table: Course of 12 hours. Lectures (two hours) on Thursday 2:30 – 4:30 and Friday 10:30 – 12:30. First lecture on Thursday, May 27, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic algebraic, geometric and analysis concepts: Vector Spaces, Matrices and Probability Theory;

Examination and grading: A practical project on the course topics with the related technical questions.

15 Mathematical Modeling

Instructor: Pradeep Misra, Wright State University, USA, e-mail: `pradeep.misra@wright.edu`

Aim: The aim of this course is to expose the student to a wide array of modeling techniques encompassing single and multiple variable optimization models, dynamic models and probability models. Through projects and exercise, students will be able to get hands on experience in modeling and simulating complex systems.

Topics:

- Week 1. *Optimization Models*
 1. Single-Variable Optimization
 2. Multivariable Optimization
 3. Computational Methods for Optimization
- Week 2. *Dynamic Models*
 4. Introduction to Dynamic Models
 5. Analysis of Dynamic Models
 6. Simulation of Dynamic Models
- Week 3. *Probability Models*
 7. Introduction to Probability Models
 8. Stochastic Models
 9. Simulation of Probability Models

References:

1. M. M. Meerschaert , *Mathematical Modeling*, Academic Press, 2007
2. W. Press, B. Flannery, S. Teukolsky and W. Vetterlin, *Numerical Recipes*, Cambridge University Press, 1987.
3. E. Beltrami, *Mathematics for Dynamic Modeling*, Academic Press, 1987

Time table: Course of 12 hours (2 two-hours lectures per week): Classes on Tuesday and Thursday, 10:30 – 12:30. First lecture on Tuesday, July 13, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Working knowledge of single-variable calculus, multivariable calculus, linear algebra, and differential equations. Prior exposure to computing and probability and statistics is useful, but is not required.

Examination and grading: Each topic will result in a computer project. The final grade will be based 50% on projects and 50% on a cumulative final examination.

16 Project Management

Instructor: Prof. Lorenzo Vangelista, Department of Information Engineering, Univ. of Padova, e-mail: lorenzo.vangelista@unipd.it

Aim: Understanding the fundamentals of R&D and product project management

Topics:

1. system design;
2. project definition, life-cycle, the project in an organization;
3. economics: quantitative methods to evaluate projects feasibility;
4. planning, programming and controlling projects: inputs and outputs, processes, tools and techniques, knowledge areas;
5. risk management, including FMEA; quality management;
6. multi-project management, project office.

References:

- Handouts provided by the instructor.
- “A Guide to the Project Management Body of Knowledge”, *The Program Management Institute*, 3rd Revised edition edition, Oct. 2004 (or 4th edition), ISBN-13: 978-1930699458, ISBN-10: 193069945X

Time table: Course of 16 hours. Lectures (2 hours) on Monday 10:30 – 12:30 and Wednesday 10:30 – 12:30. First lecture on Monday, Jan. 11, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: None.

Examination and grading: Oral exam on Friday February 12, 2010

17 Satellite Navigation Systems

Instructor: Prof. Oscar Pozzobon, Prof. Lorenzo Vangelista
e-mail: o.pozzobon@qascom.com, lorenzo.vangelista@unipd.it

Aim: The course has the objective to provide the student with a basic knowledge of the Global Satellite Navigation System (GNSS) technologies, including system, signal, receiver and augmentation systems. The course has a particular focus to the upcoming Galileo system.

Topics:

1. Global Satellite Navigation System (GNSS) Introduction: GPS, Galileo and their evolution program, Glonass, QZSS (Japan), IRNSS (India) , Beidou (China). positioning concept, from the Time of arrival (TOA), position solution.
2. System Overview: System components including the ground, space and user segments. GPS and Galileo frequencies allocation.
3. GPS signal: modulation schemes, Doppler effect, data encoding schemes, errors affecting the ranging and the mechanism of ephemeris and almanac data broadcast.
4. Galileo signal: The Binary Offset Carrier (BOC) modulation scheme, data encoding schemes, errors affecting the ranging and the mechanism of ephemeris and almanac data broadcast. The Open Service (OS) signal, the Safety of Life Service (SoL) signal, the Commercial Service (CS) and Public Regulated Service (PRS) signals.
5. Galileo Integrity: Galileo Integrity Concept, building blocks of the system, effects to the navigation parameters.
6. GNSS receiver architecture: RF front ends, based-band processing, correlation block. Overview of ASIC, software based with HW correlator, software based with software correlator and GNSS system on chips architectures. Dual frequency receivers and RAIM receivers.
7. GNSS Software receiver: wideband analog-to-digital (A/D) conversion. Software based extraction, down-conversion and demodulation of channels. GNSS operations of acquisition, tracking (code and phase) and navigation data extraction, position solution. GNSS SDR receiver in Matlab example.
8. GNSS Security: GNSS vulnerabilities and attacks. Signal jamming and spoofing . Galileo security services: signal and navigation messages authentication. Cryptographic applications for GNSS.
9. Precise positioning: Carrier phase tracking, Relative Kinematic Positioning (RKP) and real-time kinematic positioning (RTK).
10. Augmentation Systems: Error correction techniques. Satellite Based Augmentation systems (SBAS) as (European geostationary navigation overlay system) EGNOS or Wide Area Augmentation System (WAAS)

References:

- [1] Global Positioning System: Theory and Applications, Bradford W. Parkinson (Editor), James J. Spilker (Editor), James J. Spilker (Editor), Penina Axelrad (Editor), Per Enge (Editor), January 1996.
- [2] A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach Di Kai Borre, Dennis M. Akos, Nicolaj Bertelsen, Peter Rinder, Soren Holdt Jensen.
- [3] GPS Interface Control Document (ICD 200c), navigation center, U.S department of homeland security.
- [4] European Space Agency (ESA) - Navigation technical documents.

Time table: Course of 20 hours. Lectures (two hours) on Tuesday and Thursday 2:30 – 4:30 P.M. First lecture on Tuesday, January 12, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basics on telecommunication systems;

Examination and grading: Homework assignments and Final test.

18 Statistical Methods

Instructor: Lorenzo Finesso, Istituto di Ingegneria Biomedica, ISIB-CNR, Padova
e-mail: lorenzo.finesso@isib.cnr.it

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.

Topics:

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 Maximum Likelihood (ML) estimator with partial observations (incomplete data). We will present the EM method as an alternating divergence minimization algorithm (à la Csiszár Tusnády) and show its application to the ML estimation of Hidden Markov Models.

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.

Time table: Course of 24 hours (2 two-hours lectures per week): Classes on Monday and Wednesday, 10:30 – 12:30. First lecture on Monday, June 7, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basics of Probability Theory and Linear Algebra.

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

19 Topics in Quantum Information

Instructor: Prof. Francesco Ticozzi, Department of Information Engineering, Univ. of Padova, e-mail: ticozzi@dei.unipd.it

Aim: The Course aims to serve as an introduction to a selection of topics of interest in quantum information theory, with a focus on the role of uncertainty and noise. A mathematically consistent approach will be developed, in order to tackle problems of information encoding, communication and error-correction for finite-dimensional systems.

The course is organized in the framework of the projects QuantumFuture (Progetto Strategico di Ateneo) and QUINTET.

Topics:

1. **Quantum Theory as a Probability Theory;** Densities, observable quantities, measurements in a non-commutative setting. Unitary dynamics. Composite systems and entanglement. Partial trace and marginal densities.
2. **Quantum Information Distances, Uncertainty and Distinguishability;** Entropy, relative entropy, trace norm, their interpretation and basic properties. Fidelity and related quantities.
3. **Quantum Dynamical Systems and Noise;** Open quantum systems and quantum operations. Kraus representation theorem. Errors and Markov noise models. Examples for two-level systems.
4. **Encoding Information in Quantum Systems;** The logical qubit. Encoding qubits in physical systems, operational requirements and "good codes". Quick overview of the network model.
5. **Classical and Quantum Information over Quantum Channels;** No-cloning theorem. Schumacher's quantum noiseless coding theorem. The Holevo-Schumacher-Westmoreland theorem.
6. **Introduction to Quantum Error-Correction;** Classical and quantum error correction. Stabilizer codes. Concatenation and threshold theorem. Notes on subsystem codes.

References: The main reference is M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum information (Cambridge, 2000). Other relevant references, on-line notes and research papers will be provided during the course.

Time table: Course of 16 hours. Lectures (2 hours) on Tuesday and Thursday 10:30 – 12:30. First lecture on Tuesday, June 8, 2010. Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Standard linear algebra and probability theory.

Examination and grading: Homeworks and final project.

January 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
28	29	30	31	1	2	3
4	5	6	7	8 ■ 11:00 Minelli	9	10
11 ■ 10:30 Vangelista	12 ■ 14:30 Pozzobon	13 ■ 10:30 Vangelista	14 ■ 10:30 Trevisan ■ 14:30 Pozzobon	15 ■ 11:00 Minelli	16	17
18 ■ 10:30 Vangelista	19 ■ 14:30 Pozzobon	20 ■ 10:30 Vangelista	21 ■ 10:30 Trevisan ■ 14:30 Pozzobon	22 ■ 11:00 Minelli	23	24
25 ■ 10:30 Vangelista	26 ■ 14:30 Pozzobon	27 ■ 10:30 Vangelista	28 ■ 10:30 Trevisan ■ 14:30 Pozzobon	29 ■ 11:00 Minelli	30	31

February 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1 ■ 10:30 Vangelista	2 ■ 14:30 Pozzobon	3 ■ 10:30 Vangelista	4 ■ 10:30 Trevisan ■ 14:30 Pozzobon	5 ■ 11:00 Minelli	6	7
8	9 ■ 14:30 Pozzobon	10	11 ■ 10:30 Trevisan ■ 14:30 Pozzobon	12 ■ 11:00 Minelli	13	14
15	16	17 ■ 10:30 Trevisan ■ 14:30 Pelosi	18	19 ■ 10:30 Pelosi	20	21
22	23	24 ■ 14:30 Pelosi	25	26 ■ 10:30 Pelosi	27	28

March 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1	2	3 ■ 10:30 Badia	4 ■ 14:30 Pelosi	5 ■ 08:30 Pelosi ■ 10:30 Badia	6	7
8	9 ■ 16:30 ROOM Oe: Damm – Wimmer	10 ■ 10:30 Badia	11 ■ 16:30 ROOM Oe: Damm – Wimmer	12 ■ 10:30 Badia	13	14
15 ■ 10:30 Villorosi	16 ■ 16:30 ROOM Oe: Damm – Wimmer	17 ■ 10:30 Badia	18 ■ 10:30 Villorosi ■ 16:30 ROOM Oe: Damm – Wimmer	19 ■ 10:30 Badia	20	21
22 ■ 10:30 Villorosi	23 ■ 16:30 ROOM Oe: Damm – Wimmer	24 ■ 10:30 Badia	25 ■ 10:30 Villorosi ■ 16:30 ROOM Oe: Damm – Wimmer	26 ■ 10:30 Badia	27	28
29 ■ 10:30 Villorosi	30 ■ 16:30 ROOM Oe: Damm – Wimmer	31 ■ 10:30 Badia	1 ■ 10:30 Villorosi ■ 16:30 ROOM Oe: Damm – Wimmer	2 ■ 10:30 Badia	3	4

April 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
29 ■ 10:30 Villoresi	30 ■ 16:30 ROOM Oe: Damm - Wimmer	31 ■ 10:30 Badia	1 ■ 10:30 Villoresi ■ 16:30 ROOM Oe: Damm - Wimmer	2 ■ 10:30 Badia	3	4
5 ■ 10:30 Villoresi	6	7	8 ■ 10:30 Villoresi	9	10	11
12 ■ 10:30 Villoresi	13	14	15 ■ 10:30 Villoresi	16	17	18
19	20 ■ 10:30 Neviani	21	22 ■ 10:30 Neviani	23	24	25 Holiday
26	27 ■ 10:30 Neviani	28	29 ■ 10:30 Neviani	30	1 Holiday	2

May 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
26 ■ 10:30 Neviani	27	28 ■ 10:30 Neviani	29	30	1 Holiday	2
3 ■ 14:30 Altafini	4 ■ 10:30 Neviani	5 ■ 14:30 Altafini	6 ■ 10:30 Neviani	7	8	9
10 ■ 14:30 Altafini	11 ■ 10:30 Neviani	12 ■ 14:30 Altafini	13 ■ 10:30 Neviani	14	15	16
17 ■ 14:30 Altafini	18 ■ 10:30 Neviani	19 ■ 14:30 Altafini	20 ■ 10:30 Neviani	21	22	23
24 ■ 14:30 Altafini	25	26 ■ 14:30 Altafini	27 ■ 14:30 Moschitti	28 ■ 10:30 Moschitti	29	30
31	1 Holiday	2 ■ 14:30 Moschitti	3 ■ 10:30 Moschitti	4	5	6

June 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
31	1	2 Holiday	3 ■ 14:30 Moschitti	4 ■ 10:30 Moschitti	5	6
7 ■ 10:30 Finesso	8 ■ 10:30 Ticozzi	9 ■ 10:30 Finesso	10 ■ 10:30 Ticozzi ■ 14:30 Moschitti	11 ■ 10:30 Moschitti	12	13 Holiday
14 ■ 10:30 Finesso	15 ■ 10:30 Ticozzi	16 ■ 10:30 Finesso	17 ■ 10:30 Ticozzi	18	19	20
21 ■ 10:30 Finesso	22 ■ 10:30 Ticozzi	23 ■ 10:30 Finesso	24 ■ 10:30 Ticozzi	25	26	27
28 ■ 10:30 Finesso	29 ■ 10:30 Ticozzi	30 ■ 10:30 Finesso	1 ■ 10:30 Ticozzi	2	3	4

July 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
28 ■ 10:30 Finesso	29 ■ 10:30 Ticozzi	30 ■ 10:30 Finesso	1 ■ 10:30 Ticozzi	2	3	4
5 ■ 10:30 Finesso	6	7 ■ 10:30 Finesso	8	9	10	11
12 ■ 10:30 Finesso	13 ■ 10:30 Misra	14 ■ 10:30 Finesso	15 ■ 10:30 Misra	16	17	18
19	20 ■ 10:30 Misra	21	22 ■ 10:30 Misra	23	24	25
26	27 ■ 10:30 Misra	28	29 ■ 10:30 Misra	30	31	1

August 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
26	27	28	29	30	31	1
	■ 10:30 Misra		■ 10:30 Misra			
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

September 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20 ■ 10:30 Pilonetto	21	22 ■ 10:30 Pilonetto	23	24	25	26
27 ■ 10:30 Pilonetto	28	29 ■ 10:30 Pilonetto	30	1	2	3

October 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
27	28	29	30	1	2	3
	■ 10:30 Pillonetto		■ 10:30 Pillonetto			
4	5	6	7	8	9	10
	■ 10:30 Pillonetto	■ 10:30 Laurenti	■ 10:30 Pillonetto	■ 10:30 Laurenti		
11	12	13	14	15	16	17
	■ 10:30 Pillonetto	■ 10:30 Laurenti	■ 10:30 Pillonetto	■ 10:30 Laurenti		
18	19	20	21	22	23	24
	■ 10:30 Pillonetto	■ 10:30 Laurenti	■ 10:30 Pillonetto	■ 10:30 Laurenti		
25	26	27	28	29	30	31
■ 14:30 Meneghesso	■ 10:30 Pillonetto	■ 10:30 Laurenti	■ 10:30 Pillonetto ■ 14:30 Meneghesso	■ 10:30 Laurenti		

November 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1 Holiday	2 ■ 10:30 Pillonetto	3 ■ 10:30 Laurenti	4 ■ 10:30 Pillonetto ■ 14:30 Meneghesso	5 ■ 10:30 Laurenti	6	7
8 ■ 08:30 Manduchi ■ 14:30 Meneghesso	9 ■ 10:30 Saccomani	10	11 ■ 08:30 Manduchi ■ 14:30 Meneghesso	12 ■ 10:30 Saccomani	13	14
15 ■ 08:30 Manduchi ■ 14:30 Meneghesso	16 ■ 10:30 Saccomani	17	18 ■ 08:30 Manduchi ■ 14:30 Meneghesso	19 ■ 10:30 Saccomani	20	21
22 ■ 08:30 Manduchi ■ 14:30 Meneghesso	23 ■ 10:30 Saccomani	24	25 ■ 08:30 Manduchi ■ 14:30 Meneghesso	26 ■ 10:30 Saccomani	27	28
29 ■ 08:30 Manduchi ■ 14:30 Meneghesso	30	1	2 ■ 08:30 Manduchi	3	4	5

December 2010

■ Ph.D. Courses: Room DEI/G

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
29 ■ 08:30 Manduchi ■ 14:30 Meneghesso	30	1	2 ■ 08:30 Manduchi	3	4	5
6 ■ 08:30 Manduchi	7	8 Holiday	9 ■ 08:30 Manduchi	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2