UNIVERSITÀ DEGLI STUDI DI TORINO

MASTER MATHEMATICAL AND PHYSICAL METHODS FOR AVIATION SCIENCES

Academic year 2021-2022

Courses

Foundations
Analytical methods
Numerical methods for engineering modeling
Physics of fluids with elements of aeronautical applications

Core topics
Basic lean and six-sigma knowledge
Cybersecurity
Introduction to (semi)automated certification

Data analysis
Data analysis
Machine learning
Advanced machine learning
Advanced deep learning

Note: the names of teachers of the course are tentative.

https://www.dipmatematica.unito.it/do/home.pl/View?doc=/master/Master_MPM_Aviation_Sciences.html&sb=0_

MPM Aviation Sciences

Courses

Academic year 2021-2022

Part 1 - Foundations

Analytical methods

Vivina Barutello, *Department of Mathematics, Università di Torino*.
Andrea Bacciotti, *Politecnico di Torino - Former faculty member*.
Susanna Terracini, *Department of Mathematics, Università di Torino*.
4 CFU.

MODULUS 1 - Celestial mechanics

Contents

1. Central force fields and Kepler problem
2. Some generalities on the N-body problem
3. RC3BP and stability of lagrangian points

Publications

[1] R. Fitzpatrick, An introduction to Celestial Mechanics, Cambridge University press 2012

MODULUS 2 - Optimal control

Contents

1. Introduction and basic examples
2. Controllability, bang-bang principle
3. Linear time-optimal control
4. The Pontryagin Maximum Principle
5. Dynamic programming
6. Introduction to stochastic control theory

Publications

[1] L. C. Evans, n Introduction to Mathematical Optimal Control Theory, `https://math.berkeley.edu/~evans/control.course.pdf`

MODULUS 3 - Basics of mathematical control theory with applications to orbital opti-

mization

Objectives

This modulus is aimed at introducing the basic concepts mathematica optimal control, with applications to orbital optimization. This task presents us with these mathematical issues: does an optimal control exist? How can we characterize an optimal control mathematically? How can we construct an optimal control?

Contents

1. Introduction to the mathematical control theory: controllability, bang-bang principle, dynamic programming
2. Examples and applications concerning the control of attitude of satellites and orbital transfer

Publications

[1] Lawrence C. Evans, Introduction to Mathematical Optimal Control Theory, Lecture notes, Berkeley Math. 1983

[2] B. Bonnard, L. Faubourg, E. Trélat, Mécanique céleste et controle de systèmes spatiaux, Math. & Appl., Vol. 51, Springer Verlag, 2006

Numerical methods for engineering modeling

Simona Perotto, *Department of Mathematics*, Politecnico di Milano.

3 CFU.

Objectives

Goal of this course is the introduction of the basic analytical and numerical tools to analyze and approximate some of the most recurrent problems in engineering modeling.

Prerequisites

Basics in Functional Analysis and Linear Algebra are advisable.

Contents

Elliptic differential problems: purely diffusive problems (the Laplace and the Poisson problems); Dirichlet, Neumann and Robin boundary conditions; strong versus weak formulation; well-posedness of the weak form (the Lax-Milgram lemma); discretization of the Poisson problem with finite differences (hints) and with the Galerkin method (consistency, stability and convergence analysis); the finite element space (convergence analysis and algebraic formulation); generalization to an advection-diffusion-reaction problem.

Time-dependent differential problems: the heat equation; the semi-discrete and the discrete forms; space discretization with the finite difference scheme (hints) and with the finite element method; the theta-method for the time discretization; stability and convergence analysis.

The lectures of the course will be completed with computer labs, to provide a practical feedback to theoretical knowledge.

Publications

[1] A. Quarteroni, Numerical Models for Differential Problems, Springer

Physics of fluids with elements of aeronautical applications

Miguel Onorato, *Department of Physics*, Università di Torino.

3 CFU.

Objectives

This course provides an introduction to the physics of fluids with application to aeronautics

Contents

Fundamental principles of fluid mechanics
Fundamental principles of aerodynamics
Equations of motion
Inviscid and Incompressible flows
Boundary layer
Incompressible flows over airfoils
Inviscid, compressible flows
Shock waves

Publications

[1] P. Kundo and I. Cohen, Fluid Mechanics

[2] John D. Anderson, Fundamentals of Aerodynamics

Part 2 - Core topics

Basic lean and six-sigma knowledge

Antonio Di Leva, *Department of Informatics*, Università di Torino.
Luca Centinaro, *Avio Aero*.
Patrizia Mazza, *Avio Aero*.
3 CFU.

MODULUS 1

Contents
Seminario BPM e rilevazione problemi

MODULUS 2

Contents
History of lean
5 Step Lean Manufacturing
Mura Muri Muda
VAA NVAA the founder
Lead Time Cycle time Takt Time
VSM
Toyota Production System
Flow Game and VSM Current and Future state
5S - SMED - TOC - TPM
5T Lean Logistic
Problem solving tool
GEMBA
DMAIC

Cybersecurity

Nadir Murru, *Department of Mathematics*, Università di Trento.
4 CFU.

Objectives
The course has firstly the objective to provide the basic notion about cryptography (symmetric and asymmetric) and the main modern ciphers in order to be able to apply this knowledge in practical contexts for the cyber protection of telecommunications and critical infrastructures. The course aims at introducing the students to real-world applications, implementations and practical problems of modern cryptography. During the course, basic implementation mistakes, exploitation techniques and mitigations will be shown. Additionally, some recent real-world vulnerabilities on cryptographic implementations will be presented. Some of the examples will be practically demonstrated using the Python programming language. The last part of the course focuses on blockchains, one of the

most disrupting technologies of the last years. In particular, we will examine how the main features of a blockchain, like its security and its decentralization, are achieved thanks to a smart use of cryptographic protocols. At the end of the course, students will be able to:

1. Understand the basic implementation techniques of modern cryptographic schemes
2. Recognize bad implementations of modern cryptography and the techniques to exploit and mitigate them
3. Be critic about self-implemented cryptographic protocols
4. Properly use cryptographic language to communicate the results of their findings
5. Understand the basic notion of blockchain and some possible applications

MODULUS 1

Contents

- Introduction to the basic ideas of cryptography (channel, plaintext space, ciphertext space, key space, encryption/decryption, Kerckhoffs's principle)
- private (or symmetric) cryptography: AES (Advanced Encryption Standard), the ECB mode of operation for block ciphers and the ECB oracle attack, The CBC mode of operation for block ciphers, bitflipping and padding oracle attacks, other attacks against TLS: data compression attacks, stream ciphers and the CTR mode of operation: bitflipping attacks and reused nonce attacks, sketch of the GCM mode of operation and the Forbidden Attack against AES-GCM, sketch of the "Invisible Salamanders" vulnerability on AES-GCM
- public (or asymmetric) cryptography: Diffie-Hellman key exchange, RSA system (with classic vulnerability and bad generation of prime numbers), elliptic curve cryptography and invalid curve attacks, security of picking random primes, the Curveball vunerability on Microsoft products, attacks on biased nonces in ECDSA: from the PlayStation 3 hack to lattice attacks
- introduction to hash functions, the Merkle-Damgard construction, the length-extension attack and the vulnerability on Flickr
- Side-Channel attacks: sketch of correlation power analysis and template attacks on generic ciphers, sketch of the LadderLeak vulnerability against ECDSA in OpenSSL (2020), sketch of the PLATYPUS attack on Intel CPUs to reveal cryptographic keys, sketch on timing attacks and fault injections attacks against RSA-CRT.

MODULUS 2

Contents

- introduction to blockchain: the example of Bitcoin (framework, cryptocurrency, transactions, consensus algorithm).
- introduction to blockchain 2.0: Ethereum and smart contracts.
- Examples of blockchain applications: decentralized finance, Internet of Things.

Publications

[1] A. Antonopoulos, The internet of Money, Volume 1-3, 2017-2019.

[2] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly, 2017.

[3] A. M. Antonopoulos and Dr. Gavin Wood, Mastering Ethereum, O'Reilly, 2018.

[4] D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem, `https://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf`

[5] D. Boneh, V. Shoup, A graduate course in applied cryptography, http://toc.cryptobook.us/,2020.

[6] T. Duong, J. Rizzo, The CRIME Attack, https://docs.google.com/presentation/d/11eBmGiHbYcHR9gL5nDyZChu_-lCa2GizeuOfaLU2HOU/edit.

[7] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, 1985.

Introduction to (semi)automated certification

Luca Roversi, *Department of Informatics*, Università di Torino.

4 CFU.

Software ubiquitously supervises and controls safety-critical systems, typically characterized by highly complex behavior and interaction with their surrounding environment. The overall correct behavior of sophisticated software systems is incremental: the disciplined composition of simple correct programs preserves correctness. Formal verification is the use of mathematical techniques that assures correctness. Formal verification techniques differ from testing or simulation-based approaches, for they are exhaustive, providing much stronger guarantees on dependability.

Objectives

The course is designed for people who need to build their own concrete idea of how mission-critical software should be developed, not for professional developers of that kind of software. The main purpose of the course is to answer the question "Is my program correct?", providing practical exposure to the proof assistant Coq, one of the most used industrial-class computer-aided formal verification tools, to structured deductive logical systems, and to programming language semantics.

Contents

Motivating examples based on widely used but ill-implemented algorithms; Overview of the main formal verification techniques; Hands-on sessions with the proof assistant in parallel with pen & paper reformulations, when relevant, of the proof assistant proof-search process and outcomes. The course will cover a fairly amount of the introductory, not necessarily obvious, aspects on the subject in order to fulfill course objectives.

Bibliography

Teaching material will be a careful selection of the huge amount of resources accessible from deepspec.org, rearranged to ease the fulfillment of the course objectives. A hands-on approach will require specific software which runs on standard machines. The possibly required configuration will be part of one of the introductory classes.

Part 3 - Data analysis

Data analysis

Donata Bonino, *Department of Mathematical Sciences*, Politecnico di Torino.
Michele Caselle, *Department of Physics*, Università di Torino.
6 CFU.

MODULUS 1 - Statistical analysis

Objectives

The modulus aims to give an introduction to some statistical techniques useful in astronomical fields. Some prerequisites are required (basics of probability and statistics). The theoretical lectures will be completed by pratical lessons using the R software.

Contents

1. Introduction to statistics for astronomical data
2. Regression: linear models and linear models with mixed effects models
3. Time series analysis: ARMA and ARIMA models, time domain and frequency domain

MODULUS 2 - Software packages for observed data

Objectives

These lectures are intended to provide basic notions on the use of Information theory and Network theory for Data Analysis.

Contents

1. Introduction to information theory and its use in data science: Shannon Entropy, Kullblack-Leibler divergence, Mutual information.
2. Introduction to Network Theory and its use in data analysis: Community detection, Multiplex analysis, Dimensional reduction

Publications

[1] Lecture notes provided by the teacher

Machine learning

Roberta Sirovich, *Department of Matehmatics*, Università di Torino.
Piergiorgio Lanza, *Thales Alenia Space*.
4 CFU.

Objectives

This course provides a general introduction to Machine Learning and to the Deep Learning specification.

Machine Learning and Statistical Learning refer to a set of tools for modeling and understanding complex datasets. They are recently developed areas blended with computer science and statistics

and involve many methods. The course has not the ambition to cover all the topics, but rather to give an overview of the elements of Machine Learning and then to specialize in the framework of Deep Learning.
Deep Learning is based on artificial neural networks and it's widely and successfully used in image processing, which is the application that leads the choice to this second part of the course. Deep Learning is nowadays the most promising and revolutionary approach. It is at the basis of a radical approach in our society. It is the "new electricity" as stated by Andrew Ng. This approach is presented in this course limited to image processing.

Contents

1. Introduction to machine learning
2. Linear methods and beyond
3. Neural networks
4. The deep learning approach
5. Categories/Object identification
6. Applications of deep learning

Publications

[1] Hastie, Trevor, Tibshirani, Robert, Friedman, Jerome, *The Elements of Statistical Learning, Data Mining, Inference and Prediction* (2009)

[2] Murphy, *Machine Learning, A Probabilistic Perspective* (2012)

[3] Shalev-Shwartz, Ben-David, *Understanding Machine Learning, From Theory to Algorithms* (2014)

[4] Pointer, *Programming PyTorch for Deep Learning: Creating and Deploying Deep Learning Applications* (2019)

[5] Howard, Gugger, *Deep Learning for Coders with fastai and PyTorch First Edition* (2020)

[6] Mishra, *PyTorch Recipes: A Problem-Solution Approach* (2018)

Advanced machine learning

Giovanni Siragusa, *Department of Informatics*, Università di Torino.

3 CFU.

Contents

- Basics of Linear Algebra (matrices, determinant, rank, diagonalisation)
- Singular Value Decomposition, Principal Component Analysis and dimensionality reduction
- Reminders of Linear Methods
- Validating a model, train-test, k-fold cross validation.
- Bias-Variance trade-off
- L1 and L2 Regularisation
- Beyond linearity, polynomial regression

- Support-vector machine
- SVM: dual problem
- Kernels
- Decision Tree
- Ensemble methods, bagging and boosting
- From decision tree to Random Forest

Verranno effettuati esempi del linguaggio di programmazione Python e dei package numpy e scikit-learn, in quanto permettono la definizione ed esecuzione di modelli di machine learning

Publications

[1] Elements of statistical learning

[2] An introduction to statistical learning (with R)

Advanced deep learning

Enzo Tartaglione, *Department of Informatics*, Università di Torino.
4 CFU.

Contents

1. Recap on Deep Learning for Image Classification
   Datasets: CIFAR, ImageNet
   Architectures: LeNet, VGG, MobileNet, ResNet, Inception-v3
   Loss functions: Cross Entropy Loss, Hinge Loss, MSE
   Optimizers: SGD, Nesterov, Adam, RMS-Prop
   Regularizers: Dropout, weight-decay
   Dataset augmentation strategies
   Real case scenario: CIFAR10 classification
2. Expectation Maximization
   Latent variable models
   Gaussian Mixture Model
   Jensen's inequality & Kullback Leibler divergence
   The Expectation-Maximization algorithm
3. Autoencoders
   Vanilla Autoencoders
   Variational Autoencoders (*)
   Autoencoders for segmentation: U-Net, Nabla-Net, Mask-RCNN
   Real case scenario: semantic segmentation
4. GANs
   Motivation & Structure
   Problem with BCE Loss
   Wasserstein Loss
   Conditional generation
   Inception score and application: Celeb-A

5. Improving the efficiency
   - Pruning
     - The lottery ticket hypothesis
     - Second order optimization strategies (Optimal Brain Damage)
     - Variational Dropout (*)
     - Sensitivity-based approach to unstructured sparsity
     - Unstructured sparsity vs Structured sparsity
     - L0 regularization proxies and Structured Sensitivity
   - Quantization
     - Quantizing parameters
     - Quantizing activations
     - Use of int libraries on embedded devices
   - Application: Quantize and prune VGG for mobile devices deployment