RESEARCH CENTRE

Inria Lyon Centre

IN PARTNERSHIP WITH:

CNRS, Université Jean Monnet Saint-Etienne

2024

ACTIVITY REPORT

Project-Team

MALICE

MAchine Learning with Integration of surfaCe Engineering knowledge: Theory and Algorithms

IN COLLABORATION WITH: Laboratoire Hubert Curien (LabHC)

DOMAIN

Applied Mathematics, Computation and Simulation

THEME

Optimization, machine learning and statistical methods

Inria

Contents

Project-Team MALICE 1

1 Team members, visitors, external collaborators 2

2 Overall objectives 3

3 Research program 3

4 Application domains 5

5 Social and environmental responsibility 5

6 Highlights of the year 5
6.1 Papers . . . 5
6.2 Awards . . . 6

7 New software, platforms, open data 6
7.1 New software . . . 6
7.1.1 SwiftHohenbergPseudoSpectral . . . 6
7.1.2 GUAP . . . 6
7.1.3 GraSPy . . . 6
7.1.4 Scikit-SpLearn . . . 7
7.1.5 SoundScapeExplorer . . . 7
7.2 Open data . . . 7

8 New results 8
8.1 Theoretical bounds . . . 8
8.1.1 Approximation Error in Physics-informed Neural Networks . . . 8
8.1.2 PAC-Bayes Theory for Generalization Bounds with Complexity Measures . . . 8
8.1.3 A General Framework for the Practical Disintegration of PAC-Bayesian Bounds . . . 8
8.1.4 Length Independent PAC-Bayes Bounds for Simple RNNs . . . 9
8.1.5 A Theoretically Grounded Extension of Universal Attacks from the Attacker's Viewpoint 9
8.1.6 Unsupervised Learning and Effective Complexity . . . 9
8.2 Physics-informed Machine Learning (PIML) . . . 10
8.2.1 Bregman Proximal Viewpoint on Neural Operators . . . 10
8.2.2 PIML for Better Understanding Laser-Matter Interaction . . . 10
8.2.3 Self-Consuming Generative Models . . . 11

9 Bilateral contracts and grants with industry 11
9.1 Bilateral contracts with industry . . . 11
9.1.1 CIFRE Theses with Thalès (2024-2027) . . . 11
9.1.2 I-Démo Région "GREENAI" . . . 11
9.2 Bilateral Grants with Industry . . . 12
9.2.1 "Baby Cry" project - AXA Fundation (2024-2026) . . . 12

10 Partnerships and cooperations 12
10.1 International research visitors . . . 12
10.1.1 Visits of international scientists . . . 12
10.1.2 Visits to international teams . . . 13
10.2 European initiatives . . . 13
10.2.1 ML4Health - Transform4Europe (2024-2026) . . . 13
10.3 National initiatives . . . 14
10.3.1 ANR MELISSA (2024-2029) . . . 14
10.3.2 ANR TAUDoS (2021-2026) . . . 14
10.3.3 AI4OP (2021-2024) . . . 15

10.3.4 ANR SAFE (2022-2026) . . . 15
10.3.5 ANR FAMOUS (2023-2027) . . . 16
10.3.6 EUR SLEIGHT PIMALEA (2023-2024) . . . 16
10.3.7 EUR SLEIGHT TREASURF (2024-2027) . . . 17

11 Dissemination **17**
11.1 Promoting scientific activities . . . 17
11.1.1 Scientific events: organisation . . . 17
11.1.2 Scientific events: selection . . . 18
11.1.3 Journal . . . 18
11.1.4 Invited talks . . . 19
11.1.5 Scientific expertise . . . 19
11.1.6 Research administration . . . 19
11.2 Teaching - Supervision - Juries . . . 19
11.2.1 Teaching . . . 19
11.2.2 Supervision . . . 21
11.2.3 Juries . . . 22
11.3 Popularization . . . 22
11.3.1 Productions (articles, videos, podcasts, serious games, ...) . . . 22
11.3.2 Participation in Live events . . . 22
11.3.3 Others science outreach relevant activities . . . 23

12 Scientific production **23**
12.1 Major publications . . . 23
12.2 Publications of the year . . . 24

Project-Team MALICE

Creation of the Project-Team: 2023 December 01

Keywords

Computer sciences and digital sciences

A3.4.1. – Supervised learning

A3.4.4. – Optimization and learning

A3.4.6. – Neural networks

A3.4.7. – Kernel methods

A3.4.8. – Deep learning

A5.9.1. – Sampling, acquisition

A5.9.4. – Signal processing over graphs

A5.9.5. – Sparsity-aware processing

A5.9.6. – Optimization tools

A6.3.1. – Inverse problems

A6.3.5. – Uncertainty Quantification

A6.5. – Mathematical modeling for physical sciences

A8.2. – Optimization

A8.12. – Optimal transport

A9.2. – Machine learning

Other research topics and application domains

B2.6. – Biological and medical imaging

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.5.3. – Physics

B9.5.6. – Data science

1 Team members, visitors, external collaborators

Research Scientists

- Quentin Bertrand [INRIA, Researcher, from Jul 2024]
- Benjamin Girault [INRIA, ISFP]

Faculty Members

- Marc Sebban [Team leader, UNIV Jean Monnet, Professor]
- Eduardo Brandao [UNIV Jean Monnet, Associate Professor, from Sep 2024]
- Farah Cherfaoui [UNIV Jean Monnet, Associate Professor]
- Rémi Emonet [UNIV Jean Monnet, Associate Professor]
- Rémi Eyraud [UNIV Jean Monnet, Associate Professor]
- Jordan Frecon Patracone [UNIV Jean Monnet, Associate Professor]
- Amaury Habrard [UNIV Jean Monnet, Professor]

Post-Doctoral Fellows

- Eduardo Brandao [UNIV Jean Monnet, Post-Doctoral Fellow, until Aug 2024]
- Antoine Caradot [UNIV Jean Monnet]

PhD Students

- Fayad Ali Banna [UNIV Jean Monnet]
- Hind Atbir [UNIV Jean Monnet, from Sep 2024]
- Sayan Chaki [UNIV Jean Monnet]
- Ben Gao [UNIV Jean Monnet, from Oct 2024]
- Thibault Girardin [UNIV Jean Monnet]
- Erick Gomez [UNIV Jean Monnet, from Sep 2024]
- Dorian Llavata [UNIV Jean Monnet]
- Robin Mermillod-Blondin [UNIV Jean Monnet]
- Abdel-Rahim Mezidi [UNIV Jean Monnet]
- Volodimir Mitarchuk [UNIV Jean Monnet, until Dec 2024]

Interns and Apprentices

- Hind Atbir [UNIV Jean Monnet, Intern, from Feb 2024 until Jul 2024]
- Amrithya Balaji [INRIA, Intern, from Apr 2024 until Jun 2024]
- Younes Essafouri [UNIV Jean Monnet, Intern, from Jun 2024 until Aug 2024]
- Charles Franchi [UNIV Jean Monnet, Intern, from Apr 2024 until Jul 2024]
- Erick Gomez [UNIV Jean Monnet, Intern, from Feb 2024 until Jul 2024]
- Youssef Hannat [UNIV Jean Monnet, Intern, from Jun 2024 until Jul 2024]
- Anna Karolin [UNIV Jean Monnet, Intern, from Apr 2024 until Aug 2024]
- Louis Nicolas [UNIV Jean Monnet, Intern, from Apr 2024 until Jul 2024]
- Hager Othman [INRIA, Intern, from Apr 2024 until Jul 2024]
- Valentin Rieu [UNIV Jean Monnet, Intern, from Apr 2024 until Jul 2024]
- Alexis Roux [UNIV Jean Monnet, Intern, from Jul 2024 until Aug 2024]
- Aubin Sionville [UNIV Jean Monnet, Intern, from May 2024 until Aug 2024]

Administrative Assistant

- Naima Chalais Traore [UNIV Jean Monnet, from Feb 2024]

2 Overall objectives

The objective of MALICE is to combine the interdisciplinary skills present at the Hubert Curien lab in statistical learning and laser-matter interaction to foster the development of new joint methodological contributions in Physics-informed Machine Learning (PiML) at the interface between ML and Surface Engineering. The members of the project-team have complementary backgrounds in computer science, applied mathematics, statistics and optimization. They also benefit from the expertise of physicists of the lab in modeling ultrashort laser-matter interaction which makes possible scientific breakthroughs in both domains. On the one hand, surface engineering raises numerous machine learning challenges, including (i) a limited access to training data due to time-consuming experimental setups and the availability of only incomplete background knowledge (typically in the form of Partial Differential Equations - PDEs), (ii) the need of deriving theoretical (generalization, approximation, optimization) guarantees on models learned from both data and physical knowledge and (iii) a strong necessity to transfer knowledge from one dynamical system to another. On the other hand, the advances carried out in machine learning allow to better understand the physics underlying the mechanisms of laser/radiation-matter interaction, enabling to address numerous societal challenges in the fields of space, nuclear, defense, energy or health.

3 Research program

MALICE is rooted at the interface of applied mathematics, statistical learning theory, optimization, physics and differentiable simulation. The following three scientific axes aim at addressing the aforementioned challenges from both theoretical (Axis 1) and algorithmic (Axes 2 and 3) perspectives.

Axis 1: Theoretical Frameworks when learning from data and background knowledge Generalization guarantees typically aim at bounding the deviation of the true risk of an hypothesis from its empirical counterpart. These bounds, often referred to as PAC (Probably Approximately Correct) bounds, are usually derived by resorting to concentration inequalities (*e.g.* Chebyshev, Hoeffding, McDiarmid, etc.). Several theoretical frameworks have been introduced in the literature for establishing generalization bounds, including uniform convergence, uniform stability, algorithmic robustness or PAC-Bayesian theory, to cite a few. The state of the art bounds differ in the way (i) they incorporate some complexity measure (*e.g.* VC-dimension, Rademacher complexity, fat-shattering dimension, uniform stability constant, covering number, divergence, etc.) and (ii) take into account how the learning algorithm searches (or not) the parameter space. The ambitious goal of this Axis is to investigate how generalization bounds can be derived when the learning algorithm has access to both (non i.i.d) training data and background knowledge (in the form of PDEs). Addressing this task raises several challenges: How to define complexity measures that capture dynamics' characteristics of the physical models? Can we derive theoretical bounds with arbitrary complexity measures? Can we derive such bounds in a transfer learning setting where two different but related dynamics are involved? As bilevel optimization seems to be very promising for addressing tasks involving data and knowledge, we also investigate how to derive statistical guarantees of nonsmooth bilevel problems. On the other hand, it is worth noticing that most of the physics-informed machine learning methods, like PINNs, minimize, as a term of the loss function, the residuals of the PDE. In this context, the team aims to study the approximation guarantees of such neural networks so as to ensure that minimizing the residuals leads to a small prediction error on the target vector field. Such guarantees are key in laser-matter interaction where the dynamics is governed by complex high-order non linear PDEs, like the Swift-Hohenberg equation.

Note that the methodological contributions of this Axis aim to guide the design of the algorithms developed in Axes 2 and 3.

Tools and methods used in this axis: *complexity measures, PAC-Bayes theory, algorithmic robustness, uniform stability, concentration inequalities, bilevel optimization, functional analysis, Sobolev norms.*

Axis 2: Integration and extraction of knowledge in Surface Engineering In this axis, we aim at dealing, from an algorithmic perspective, with low data and low knowledge regimes that are typically observed in surface engineering, *i.e.* where (i) the amount of training data at our disposal is limited because of heavy experimental setups, (ii) the physical models describe partially the underlying dynamics and finally, (iii) the actual continuous dynamics is not observable. Indeed, unlike other dynamical systems (e.g. in meteorology, temperature lake modeling, fluid mechanics, etc.), because light propagates too fast and the interaction with the matter lasts only a few femtoseconds (preventing any optical devices from taking images), we do not have easily access with the same initial conditions to the states of the system at time t, $t+\delta_t$, ..., $t+n\delta_t$. Among the research avenues that are explored to address this strongly constrained scenario, we aim to design hybrid (data+knowledge) methods for benefiting from the best of the two worlds, while leveraging symmetries present in the physical priors. This latter may allow to drastically reduce the amount of required examples when learning the dynamics from real data or optimizing surrogates PDE solvers from simulated examples. Another line of research consists in studying how bilevel optimization can integrate into two nested levels both the data and the surface engineering knowledge, and investigating (i) how sparse modeling might overcome the lack of data and (ii) how to augment/discover the underlying physical knowledge by seeing the orders of the partial derivatives as (real) hyperparameters. Finally, in this low data regime characterizing surface engineering, a special focus is placed on generative models for data augmentation.

Tools and methods used in this axis: *invariance, symmetries, sparse modeling, PDE learning, automatic differentiation, generative AI, bilevel optimization, neural operators.*

Axis 3: Domain Generalization and Transfer Learning for Surface Engineering Standard machine learning algorithms work well under the common assumption that the training and test data are drawn according to the same distribution. When the latter changes at test time, most statistical models must

be reconstructed from newly collected data, which for some applications can be costly or impossible to obtain. Therefore, it has become necessary to develop approaches that reduce the need and the effort to obtain new labeled samples by exploiting pre-trained models and/or data that are available in related areas, and using these further across similar fields. This has given rise to the transfer learning and domain generalization frameworks which received a tremendous interest in the past years from the machine learning community. A key challenge in the MALICE project is to develop novel transfer learning methods for surface engineering that are able to adapt to a change of physical context (matter properties, governing PDEs, spatio-temporal conditions, initial/boundary conditions, etc.). The objective of this axis is to define new differentiable measures of discrepancy able to capture these shifts of background knowledge. We investigate the use of these measures in bilevel optimization-based transfer learning methods. We also study the links that can be established between diffusion models, flow matching, optimal transport and domain adaptation.

Tools and methods used in this axis: *knowledge divergences, flow matching, diffusion, optimal transport, cross-knowledge modeling, entropy of dynamical systems, foundation models.*

4 Application domains

The scientific advances that are carried out in the team can be directly exploitable in numerous applications related to surface engineering and laser matter interaction, including automotive sector, health, biology, medicine, micro-surgery, environment, energy, security, space, to cite a few. This is made possible by texturing and thus giving a function to the surface of the matter. Mastering this physics allows to enhance the way one can give specific properties to a material, e.g. to obtain different optical effects of a glass according to the field of observation (reflection, transmission), to structure or texture tissues to control some biological behavior or to adapt surface matter to control the friction or adherence. For instance, the control of the nanopeak organization would open the door to advances in the protection of materials (living or not) against the attacks of bacteria or virus. On the other hand, nanocavities might be of great interest in the nanostructuring of car cylinders leading to CO2 emission reduction. The scientific breakthroughs achieved in MALICE aim at strengthening the existing collaborations between the laboratory and major economic and public stakeholders in the fields of space, nuclear, defense, energy, automotive, health, including CNES, CERN, ORANO, CEA, DGA, EXAIL, HEF, RENAULT, BIOMERIEUX, HID GLOBAL, THALES, ST MICROELECTRONICS, to cite some of them.

5 Social and environmental responsibility

One objective of the team is to show that it is possible to learn (theoretically) well from less data by leveraging physical knowledge. The assumption is that the latter can play the role of regularization leading to the prediction of plausible solutions while allowing a reduction of the number of examples required to train neural networks. This might have an impact on the carbon footprint by reducing the amount of costly collected data (involving matter irradiation and microscopy imaging) and therefore the computational resources needed for training the models.

6 Highlights of the year

6.1 Papers

Our work [2] presented at ECML'24, involving several members of the team, is the first paper published by MALICE on theoretical guarantees in Physics-informed Machine Learning.

Our paper [1] presented at NeurIPS'24 was the subject of an article on generative models published in *The New York Times*.

6.2 Awards

- Eduardo Brandao - Best thesis award 2024 - French Complex Systems Society.
- Eduardo Brandao - "Prix d'Excellence Jeune Docteur" awarded by the Foundation of Jean Monnet University, 2024.

7 New software, platforms, open data

7.1 New software

7.1.1 SwiftHohenbergPseudoSpectral

Keywords: Partial differential equation, Numerical solver, Self-organization

Functional Description: This software solves the dimensionless Swift-Hohenberg Equation with a cubic-quadratic nonlinear term. The Swift-Hohenberg Equation is a widely studied model for pattern formation, derived using symmetry arguments. As such, it serves as a maximally symmetric model for systems exhibiting spontaneous pattern formation, making it broadly applicable to various physical contexts.

The solver employs pseudospectral methods based on Fourier representations to ensure efficient and accurate computation. Importantly, the solver is physically constrained, using a Lyapunov functional to validate solutions, ensuring that the computed results remain consistent with the physical behavior expected from the system.

Designed with versatility and automation in mind, the solver is capable of generating a large number of solutions with minimal supervision. This feature makes it particularly well-suited for creating synthetic datasets to be used in Physics Guided Machine Learning. Specifically, it addresses problems related to the femtosecond laser-induced self-organization of matter, where data augmentation is crucial for improving the performance and generalization of machine learning models.

Publications: ujm-04157829, ujm-03823722, tel-04515418v1

Contact: Eduardo Brandao

7.1.2 GUAP

Name: Generalized Universal Adversarial Perturbations

Keyword: Machine learning

Functional Description: The software extends universal attacks by jointly learning a set of perturbations to choose from, aiming to maximize the success rate of attacks against deep neural network models.

URL: https://github.com/JordanFrecon/guap

Contact: Jordan Frecon Patracone

Partner: LITIS

7.1.3 GraSPy

Name: Graph Signal Processing for Python

Keywords: Graph, Signal processing, Machine learning

Functional Description: Implements classic components of such a toolbox, including (weighted) graph generalization and transformation and of their signals (a.k.a. vertex attributes), specific data visualization using Plotly, signal transformation with spectral methods (using IAGFTs), and graph learning.

URL: https://gitlab.inria.fr/begiraul/joint-graph-learning

Publication: hal-04025968

Contact: Benjamin Girault

7.1.4 Scikit-SpLearn

Name: Toolbox for the spectral learning of weighted automata

Keywords: Machine learning, Weighted automata

Scientific Description: The core idea of the spectral learning of weighted automata is to use a rank factorization of a complete sub-block of the Hankel matrix of a target series to induce a weighted automaton.

Functional Description: The toolkit contains an efficient implementation of weighted automata, a library to transformed any dataset containing strings of different length into the scitkit-learn format for data, 4 variants of the spectral learning algorithm.

URL: https://remieyraud.github.io/scikit-splearn/

Publication: hal-01777169

Contact: Rémi Eyraud

Partner: Laboratoire d'Informatique et des Systèmes (LIS) Université Aix-Marseille

7.1.5 SoundScapeExplorer

Keywords: Acoustics, Data analysis, Data visualization, Soundscape

Functional Description: SSE stands for SoundScapeExplorer and works with passive acoustic monitoring campaigns made of several microphones recording during hours, days or week.

It analyzes these data by extracting various features and indicators for each signal window (typically 1 second) then aggregating them by chunks (e.g. from 5 seconds to 1 or more minutes). Using a selection of dimensionality reduction techniques, it allows to visualize the whole campaign as a point cloud where each point corresponds to a temporal chunk on one microphone. The visualization is interactive, allowing coloring by criteria, filtering, listening to audio data, cluster analysis and beyond.

URL: https://sound-scape-explorer.github.io/

Contact: Rémi Emonet

Partner: Laboratoire ENES

7.2 Open data

TAYSIR Benchmark

Contributors: Rémi Eyraud

Description: The Transformers+RNN: Algorithms to Yield Simple and Interpretable Representations (TAYSIR, the Arabic word for 'simple') Benchmark was created for an on-line challenge on extracting simpler models from already trained neural networks held in Spring 2023. These neural nets were trained on sequential categorial/symbolic data. Some of these data were artificial, some came from real world problems (such as Natural Language Processing, Bioinformatics, and Software Engineering). The trained models covered a wide spectrum of architectures, from Simple Recurrent neural Network (SRN) to Transformers, including Gated Recurrent Unit (GRU) and Long Short-Term memory (LSTM). The benchmark contains Neural Nets trained on two types of tasks: neural networks trained on Binary Classification tasks, and on Language Modeling tasks.

Project link: https://remieyraud.github.io/TAYSIR/

Publication: https://proceedings.mlr.press/v217/eyraud23a.html

Contact: remi.eyraud@univ-st-etienne.fr

8 New results

8.1 Theoretical bounds

Several works of the team aimed at deriving theoretical guarantees in the context of (i) physics-informed Machine Learning with an approximation bound [2], (ii) PAC-Bayes theory with generalization bounds [3, 6, 7] or (iii) adversarial attacks with generalization/convergence bounds [5]. Moreover, in [17], we studied how to measure the complexity of arbitrary data. These latter advances might be of great help for deriving new bounds when learning physical dynamics. All these results fall into the scope covered by the objectives of Axis 1.1 "*Complexity measures and generalization bounds*".

8.1.1 Approximation Error in Physics-informed Neural Networks

Participants: Benjamin Girault, Rémi Emonet, Amaury Habrard, Jordan Patracone, Marc Sebban.

Considering the key role played by derivatives in Partial Differential Equations (PDEs), using the tanh activation function in Physics-Informed Neural Networks(PINNs) yields useful smoothness properties to derive theoretical guarantees in Sobolev norm. In [2], we conduct an extensive functional analysis, unveiling tighter approximation bounds compared to prior works, especially for higher order PDEs. These better guarantees translate into smaller PINN architectures and improved generalization error with arbitrarily small Sobolev norms of the PDE residuals.

8.1.2 PAC-Bayes Theory for Generalization Bounds with Complexity Measures

Participants: Rémi Emonet, Amaury Habrard.

Collaboration with Paul Viallard (Inria Rennes), Emilie Morvant (LabHC) and Valentina Zantedeschi (ServiceNow Research)

In statistical learning theory, a generalization bound usually involves a complexity measure imposed by the considered theoretical framework. This limits the scope of such bounds, as other forms of capacity measures or regularizations are used in algorithms. In [6], we leverage the framework of disintegrated PAC-Bayes bounds to derive a general generalization bound instantiable with arbitrary complexity measures. One trick to prove such a result involves considering a commonly used family of distributions: the Gibbs distributions. Our bound stands in probability jointly over the hypothesis and the learning sample, which allows the complexity to be adapted to the generalization gap as it can be customized to fit both the hypothesis class and the task.

8.1.3 A General Framework for the Practical Disintegration of PAC-Bayesian Bounds

Participants: Amaury Habrard.

Collaboration with Paul Viallard (Inria Rennes), Emilie Morvant (LabHC) and Pascal Germain (Dep. CS and Soft. Eng. [Québec])

PAC-Bayesian bounds are known to be tight and informative when studying the generalization ability of randomized classifiers. However, they require a loose and costly derandomization step when applied to some families of deterministic models such as neural networks. As an alternative to this step, we introduce in [7] new PAC-Bayesian generalization bounds that have the originality to provide disintegrated bounds, i.e., they give guarantees over one single hypothesis instead of the usual averaged analysis. Our bounds are easily optimizable and can be used to design learning algorithms. We illustrate this behavior on neural networks, and we show a significant practical improvement over the state-of-the-art framework.

8.1.4 Length Independent PAC-Bayes Bounds for Simple RNNs

Participants: Volodimir Mitarchuk, Rémi Eyraud, Rémi Emonet, Amaury Habrard.

Collaboration with Clara Lacroce from McGill (Canada) and Guillaume Rabusseau from MILA (Canada)

While the practical interest of Recurrent Neural Networks (RNNs) is attested, much remains to be done to develop a thorough theoretical understanding of their abilities, particularly in what concerns their learning capacities. A powerful framework to tackle this question is the one of PAC-Bayes theory, which allows one to derive bounds providing guarantees on the expected performance of learning models on unseen data. In [3], we provide an extensive study on the conditions leading to PAC-Bayes bounds for non-linear RNNs that are independent of the length of the data. The derivation of our results relies on a perturbation analysis on the weights of the network. We prove bounds that hold for β-saturated and DS β-saturated SRNs, classes of RNNs we introduce to formalize saturation regimes of RNNs. The first regime corresponds to the case where the values of the hidden state of the SRN are always close to the boundaries of the activation functions. The second one, closely related to practical observations, only requires that it happens at least once in each component of the hidden state on a sliding window of a given size.

8.1.5 A Theoretically Grounded Extension of Universal Attacks from the Attacker's Viewpoint

Participants: Jordan Patracone, Amaury Habrard.

Collaboration with Paul Viallard (Inria Rennes), Emilie Morvant (LabHC), Gilles Gasso (LITIS) and Stéphane Canu (LITIS)

In this work [5], we extend universal attacks by jointly learning a set of perturbations to choose from to maximize the chance of attacking deep neural network models. Specifically, we embrace the attacker's perspective and introduce a theoretical bound quantifying how much the universal perturbations are able to fool a given model on unseen examples. An extension to assert the transferability of universal attacks is also provided. To learn such perturbations, we devise an algorithmic solution with convergence guarantees under Lipschitz continuity assumptions. Moreover, we demonstrate how it can improve the performance of state-of-the-art gradient-based universal perturbation. As evidenced by our experiments, these novel universal perturbations result in more interpretable, diverse, and transferable attacks.

8.1.6 Unsupervised Learning and Effective Complexity

Participants: Erick Gomez, Rémi Emonet, Marc Sebban.

Measuring the complexity of arbitrary data has been of interest to many scientific domains, including machine learning and particularly unsupervised learning. In [17], we cover relevant concepts including Kolmogorov complexity, entropy and minimum description length. We argue that these measures alone are failing to distinguish noise from meaningful complexity. We push for the concept sophistication which measures the complexity of the structured part of the data, ignoring unstructured noise. This concept is reified in two manners: using image compression algorithms and using autoencoders. We aim at leveraging this work for taking into account the complexity of physical dynamics into PIML algorithms.

8.2 Physics-informed Machine Learning (PIML)

Complementary to the theoretical results presented above, the following works pave the way for algorithmics advances in Physics-informed Machine Learning for surface engineering (Axis 2), especially by (i) learning fast surrogate solvers for predicting energy absorption [12], (ii) generalizing neural operators and studying the impact on Fourier Neural Operators (FNO) [19] and (iii) studying the risks of iterative retraining [1], a key challenge especially in the low-data regimes that are observed in self-organization of matter.

8.2.1 Bregman Proximal Viewpoint on Neural Operators

Participants: Abdel-Rahim Mezidi, Jordan Patracone, Amaury Habrard, Rémi Emonet, Marc Sebban.

Collaboration with Saverio Salzo (DIAG) and Massimiliano Pontil (IIT, UCL)

In this work [19], we present several advances on neural operators by viewing the action of operator layers as the minimizers of Bregman regularized optimization problems over Banach function spaces. The proposed framework allows interpreting the activation operators as Bregman proximity operators from dual to primal space. This novel viewpoint is general enough to recover classical neural operators as well as a new variant, coined Bregman neural operators, which includes a skip-like connection and features the same expressivity of standard neural operators. Numerical experiments support the added benefits of the Bregman variant of Fourier neural operators for training deeper and more accurate models.

8.2.2 PIML for Better Understanding Laser-Matter Interaction

Participants: Fayad Ali Banna, Rémi Emonet, Marc Sebban.

Collaboration with Jean-Philippe Colombier (LabHC)

Physics-informed machine learning typically assumes that the underlying physical laws are known and abundant training data is available. These assumptions do not hold in the context of self-organization of matter, a phenomenon that leads to the emergence of patterns when a surface is irradiated with an ultrafast laser beam. Indeed, due to the constraints of the electronic data acquisition devices, the creation of large datasets is made impossible. Moreover, modeling this dynamic process is challenging as it involves coupling between electromagnetism, thermodynamics and fluid mechanics under far-from-equilibrium conditions that are not yet fully understood. This work [12] aims at taking a step forward towards a better understanding of this complex phenomenon. We specifically focus on the laser energy absorption of the surface, which is governed by the distinctive characteristics of Maxwell's equations in an inhomogeneous lossy medium. This involves modelling physics at the nano scale and incurs high simulation costs that make any exploration impractical. To address this major issue, we investigate different physics-informed learning models. In this low data regime, our study reveals that learning a simple U-Net-based surrogate model surpasses (i) more sophisticated neural architectures and (ii) the FDTD-based solver in speed by several orders of magnitude. Interestingly, our study highlights a link between the formation of patterns and the magnitude of absorbed energy.

8.2.3 Self-Consuming Generative Models

Participants: Quentin Bertrand.

The rapid progress in generative models has resulted in impressive leaps in generation quality, blurring the lines between synthetic and real data. Web-scale datasets are now prone to the inevitable contamination by synthetic data, directly impacting the training of future generated models. Already, some theoretical results on self-consuming generative models (a.k.a., iterative retraining) have emerged in the literature, showcasing that either model collapse or stability could be possible depending on the fraction of generated data used at each retraining step. However, in practice, synthetic data is often subject to human feedback and curated by users before being used and uploaded online. For instance, many interfaces of popular text-to-image generative models, such as Stable Diffusion or Midjourney, produce several variations of an image for a given query which can eventually be curated by the users. In [1], we theoretically study the impact of data curation on iterated retraining of generative models and show that it can be seen as an implicit preference optimization mechanism. However, unlike standard preference optimization, the generative model does not have access to the reward function or negative samples needed for pairwise comparisons. Moreover, our study doesn't require access to the density function, only to samples. We prove that, if the data is curated according to a reward model, then the expected reward of the iterative retraining procedure is maximized. We further provide theoretical results on the stability of the retraining loop when using a positive fraction of real data at each step. Finally, we conduct illustrative experiments on both synthetic datasets and on CIFAR10 showing that such a procedure amplifies biases of the reward model. We aim at leveraging this work for better filtering synthetic examples; This might be of great help in data augmentation, especially in the low-data regimes observed in surface engineering-informed machine learning.

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

9.1.1 CIFRE Theses with Thalès (2024-2027)

Participants: Rémi Eyraud.

Partners: SESAM (LabHC-UJM), Thalès

During Falls 2024, a collaboration with the DIS (Digital Identity & Security) lab of the Thalès firm started via a CIFRE PhD (Wissal Ghamour). Rémi Eyraud took the academic direction of the PhD together with members of the SESAME team of the Hubert Curien Laboratory. The subject aims at leveraging the tools of Machine Learning for Side Channel Attacks of embedded microchips. Information from physics can be added to the process, since the leak mainly relies on an electro-magnetic sensor. This followed the Ph.D of Dorian Llavata that started in 2022 on the same subject in collaboration with the CESTI Leti of the CEA.

9.1.2 I-Démo Région "GREENAI"

Participants: Jordan Patracone.

Partners: Dracula Technologies, ASYGN.

The project I-Démo Région "GREENAI" involves three key actors working collaboratively towards sustainable Internet of Things (IoT) solutions. Dracula Technologies specializes in developing organic photovoltaic cells that harness ambient light to power IoT devices, aligning with environmental sustainability goals. ASYGN contributes by designing ultra-low-power hardware accelerators to enable advanced AI processing directly on IoT devices. The Laboratoire Hubert Curien (Jordan Patracone) focuses on energy-efficient artificial intelligence for computer vision, optimizing neural network architectures for low-resource hardware through two scientific theses (among which, that of Ben Gao). This work is sponsored by a public grant overseen by the Auvergne-Rhône-Alpes region, Grenoble Alpes Métropole, and BPIFrance.

9.2 Bilateral Grants with Industry

9.2.1 "Baby Cry" project - AXA Fundation (2024-2026)

Participants: Rémi Emonet.

Partners: ENES (UJM), SAINBIOSE-MoVE, CHU Saint-Étienne.

Lead by the ENES, the AXA Baby Cry 1000 project aims at recording 1000 babies, each for one day after they are born to help early diagnosis of cognitive development issues and compare with the development of premature babies. The project is a joint effort by three labs (ENES, Laboratoire Hubert Curien (Rémi Emonet), and SAINBIOSE-MoVE, CHU Saint-Étienne) and is funded by the AXA Fundation for a total of 1M€ and a duration of 3 years.

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits of international scientists

Three professors visited our team in 2024.

Participants: Jeffrey Heinz (invited professor), Rémi Eyraud (host) .

Status Researcher

Institution of origin: New York State University at Stony Brook

Country: USA

Dates: April 2024 (one month)

Mobility program: Research stay funded by "Invited Professors" UJM grant

Participants: Saverio Salzo (invited professor), Jordan Patracone (host) .

Status Associate Professor

Institution of origin: Sapienza Università di Roma

Country: Italy

Dates: September 2024 (two weeks)

Mobility program: Research stay funded by "Invited Professors" UJM grant

Participants: Jorge Azorin (invited professor), Marc Sebban (host) .

Status Researcher

Institution of origin: University of Alicante

Country: Spain

Dates: July 2024 (one month)

Mobility program: Research stay funded by "Invited Professors" UJM grant

10.1.2 Visits to international teams

Participants: Quentin Bertrand (visiting researcher) Gauthier Gidel (host) .

Visited institution: Mila and Université de Montréal

Country: Canada

Dates: December 2024 (one week)

Mobility program/type of mobility: Research stay funded by Inria

Participants: Marc Sebban (invited professor) Jorge Azorin (host) .

Visited institution: University of Alicante

Country: Spain

Dates: May 2024 (one week)

Mobility program/type of mobility: Research stay funded by Univ. Alicante

10.2 European initiatives

10.2.1 ML4Health - Transform4Europe (2024-2026)

Participants: Amaury Habrard, Marc Sebban (coordinator) .

Partners: University of Alicante, Dpto.Tecnologia Informatica y Computacion (DTIC)
Type: Seed Funding T4EU (co-funded by the European Union)
Duration: 2 years (2024-2026)

The objective of ML4Health is two-fold: (i) from an training perspective, develop a double master degree in AI between the two T4EU partners, built from two existing complementary programmes

(Machine Learning & Data Mining master track at UJM and Máster Universitario en Inteligencia Artificial at UA); (ii) from a scientific standpoint, benefit from the expertise in statistical learning and physics-informed Machine Learning (UJM) and in 3D perception and intelligent systems (DTIC) to focus on the morphological evolution of bodies of obese patients and the early detection of neurodegenerative diseases. In particular, the two partners study (data+theory) hybrid machine learning models combining both 3D+t images and biological/morphometric knowledge.

10.3 National initiatives

We describe below the main national projects we are involved in.

10.3.1 ANR MELISSA (2024-2029)

MELISSA: MEthodological contributions in statistical Learning InSpired by SurfAce engineering

Participants: Eduardo Brandao, Rémi Emonet, Benjamin Girault, Amaury Habrard, Jordan Patracone, Marc Sebban (coordinator) .

Partners: MAGNET (Inria Lille), MLIA (ISIR, PSL) and F. Garrelie and JP Colombier (LabHC-UJM)
Type: ANR PRC

The underlying dynamics of many physical problems are governed by parameterized partial differential equations (PDEs). Despite important scientific advances in numerical simulation, solving efficiently PDEs remains complex and often prohibitively expensive. Physics-informed Machine Learning (PiML) has recently emerged as a promising way to learn efficient surrogate solvers, and augment the physical laws by leveraging knowledge extracted from data. Despite indisputable advances, several open problems remain to be addressed in PIML: (i) Deriving generalization guarantees; (ii) Learning with a limited amount of data; (iii) Augmenting partially known physical laws; (v) Modeling uncertainty; (vi) Building foundation models for physics. MELISSA will deal with these problems from both theoretical and algorithmic perspectives. The objective is to design the next generation of provably accurate PIML algorithms in the challenging context of laser-matter interaction where data is scarce and the available physical laws only partially explain the observed dynamics.

10.3.2 ANR TAUDoS (2021-2026)

TAUDoS: Theory and Algorithms for the Understanding of Deep learning On Sequential data

Participants: Rémi Emonet, Rémi Eyraud (Principal coordinator) , Amaury Habrard, Marc Sebban.

Partners: LIS (Aix-Marseille University), EURA NOVA (Firm), MILA (Canadian State)
Type: ANR PRCE
Website: TAUDoS

The ambition of this project is to provide a better understanding of the mechanisms that allow the amazing recent achievements of Machine Learning, and in particular of Deep Learning. This is achieved by providing elements that allow a better scientific comprehension of the models, strengthening our experimental results by theoretical guarantees, incorporating components dedicated to interpretability within the models, and allowing trustful quantitative comparison between learned models.

The originality and the specificities of TAUDoS are due to three major characteristics:

- The focus on models for sequential data, such as Recurrent Neural Networks (RNN), while most works concentrate on feed-forward networks

- The will to analyze these models in the light of formal language theory
- The goal to target both rigorous theoretical analyses and empirical evidence related to interpretability.

10.3.3 AI4OP (2021-2024)

AI4OP: Artificial Intelligence for Onco-Plasma

Participants: Rémi Eyraud (Principal coordinator) .

Partners: LIS (Aix-Marseille University), AP-HM, INT (Aix-Marseille University)
Type: ITMO-Cancer Math-Info for Cancers
Website: AI4OP

The objective of this project was to create a universal and non-invasive method to help diagnose cancers. The proposed method is based on the existence of unique plasma denaturation profiles (signatures) for different cancers. The plasma denaturation profile represents the total denaturation curve (under the influence of temperature) of its constituent proteins. Due to homeostasis, the plasma denaturation profiles of healthy individuals do not vary significantly. However, due to disease, the composition of the blood or the thermal stability of circulating proteins may change, thus altering the plasma denaturation profile.

In the context of this project, we demonstrated that nanoDSF can unambiguously distinguish several cancers using developed machine learning methods from a simple plasma sample. To achieve these objectives, we worked closely with oncologists to select cohorts of blood plasma from patients different types of cancers, including melanoma, lung, colorectal cancer, gliobastoma, breast., as well as from healthy donors. We determined the denaturation profiles for all plasma samples using the Prometheus NT.Plex. The profiles generated by each tool were stored in a developed in this project database with web interface and automatically classified using machine learning methods design in the frame of the proposed project.

10.3.4 ANR SAFE (2022-2026)

SAFE: Controlling networks with safety bounded and interpretable machine learning

Participants: Amaury Habrard.

Partners: XLIM / Univ. Poitiers, IRISA / Univ. Rennes 1, Huawei, QOS DESIGN and B. Jeudy & K. Singh (LabHC-UJM)
Type: ANR PRCE

When applied to communication networks, traditional approaches for control and decision-making require a comprehensive knowledge of system and user behaviours, which is unrealistic in practice when there is an increase in scale and complexity. Data-driven AI approaches do not have this drawback, but offer no safety bounds and are difficult to interpret. The SAFE project aims to design an innovative approach by combining the best of both worlds. In this new approach, intelligence is distributed in the network between a global AI (at the central level) and local AIs (at the edge level) collaborating with each other by integrating traditional models with graph neural networks and reinforcement learning. The approach, developed for partially or completely observable/controllable environments, will natively integrate safety bounds, interpretability and provide self-adaptive systems for routing, traffic engineering and scheduling. SAFE has following scientific objectives with an open source strategy: 1) Hierarchical architecture: Assuming modern network architectures, we will design a ML architecture based on global

AI (running at central controller level) and local AI (running at edge device level) for decision-making in partially as well as fully observable and controllable environments. Global AI will be able to control, configure and install policies on local AI. 2) Algorithms for partially observable environments: We will design new safety bounded and interpretable algorithms for self-adaptive traffic engineering, automatic scheduling algorithms for partially observable and controllable environments. These methods find use cases in SD-WAN (Software-Defined Wide Area Networks), where edge devices present at customer premises need to collaboratively operate in overlay on top of partially observable core networks. 3) Algorithms for fully observable environments: We will investigate the application of the global and local AI architecture for fully observable and controllable environments. Specifically, we will design new safety bounded and interpretable algorithms for software-defined routing and traffic engineering, which find use cases in data centers as well as private WANs connecting multiple sites.

10.3.5 ANR FAMOUS (2023-2027)

Famous: Fair Multi-modal Learning

Participants: Rémi Eyraud, Amaury Habrard.

Partners: LIS Aix-Marseille, LITIS Rouen, INT Marseille, Euranova and A. Gouru, C. Largeron & E. Morvant (LabHC-UJM)

The aim of this project is to explore the first avenues of research into the contribution of multimodality in datasets to meet the requirements of fair learning. Fairness refers here to the biases (in the data and/or induced), while being interested in the interpretability of the models to help their certification. Each modality has its own statistical and topological characteristics, which requires upstream research on the adjustment of distributions when biased, adapted metrics, etc. Moreover, each one being itself a bias of observation of the data, this will be taken into account to establish a joint distribution (trans-modal) unbiased on all these modalities. With theoretical research in cross-modal statistical learning, we will study methods for reducing some types of identified biases (non iid, imbalances, sensitive variables) in the case of multimodal data. Two levels of treatment are privileged: (1) cross-modal pre-processing of biases in the data, by learning metrics, neural representations, and optimization constraints on kernel pre-images; (2) cross-modal algorithms for eliminating biases in model learning: cross-modal optimization algorithms, as well as optimal transfer and transport approaches between modalities to debias the concerned ones, based on the theoretical results previously obtained. Parsimony will be considered for scaling and explainability. Transversally, our work will be based on problems arising from real data sets in biology and health, multi-modal and presenting various types of bias, and on toy data sets to be generated. They have modalities where the data are structured in graphs: all our fundamental works will be declined to take into account this specificity impacting the treatment of the considered biases.

10.3.6 EUR SLEIGHT PIMALEA (2023-2024)

PIMALEA: Physics-Informed MAchine LEARning: From extraction to transfer of knowledge in surface engineering

Participants: Eduardo Brandao, Rémi Emonet (co-coordinator) , Marc Sebban.

Partners: JP Colombier (co-coordinator)
Type: EUR Manutech SLEIGHT

During the past few years, machine learning has been massively used to better understand multiscale physics, e.g. (i) by overcoming the limitations of costly numerical solvers of Partial Differential Equations

(PDE), (ii) by learning from data the residuals of known physical models or more recently (iii) by discovering the latter explaining the underlying dynamics of observed data. In this context, a new generation of machine learning models emerged by integrating physical information to guide the learning process. This collection of techniques is generally grouped in under the "Physics-guided" or "Physics-informed" machine learning topic. In order to train the corresponding deep neural networks, these methods typically assume that they have access to a large enough amount of empirical data and/or they know the underlying physics allowing the generation of simulated examples. The ambitious goal of this project PIMALEA is to achieve scientific breakthroughs in the domain of self-organization of matter whose specificities constitute important pitfalls for a direct use of machine learning.

10.3.7 EUR SLEIGHT TREASURF (2024-2027)

TREASURF: TRansfer lEarning for Frugal and Accurate modeling of SURface Functionalization prediction –application to multicomponent alloys

Participants: Amaury Habrard (coordinator) , Rémi Emonet, Marc Sebban.

Partners: F. Garrelie and JP Colombier (LabHC-UJM)
Type: EUR Manutech SLEIGHT

TREASURF is an interdisciplinary project focusing on the development of novel machine learning approaches for the prediction of surface functionalization of different families of metals and metal alloys by (femto)laser irradiation. The ability to predict the micro- or nanopatterns induced by laser functionalization is a crucial challenge for an optimal use of surface properties. In this context, machine learning methods have been subject of a growing interest recently but they have to cope with of limited amounts of experimental data due to the very high acquisition costs. In the TREASURF project, we propose to address this problem by developing methods able to transfer the knowledge of a prediction model learned from a given metal or alloy to another, different but sharing certain properties. Re-training a new model is not a plausible hypothesis, mainly because of the difficulties involved in acquiring large quantities of data (laser irradiation + nanoscale imaging). This project is therefore situated in a difficult context of "frugal" learning. Our aim is to focus primarily on topographic predictions for two or more different alloy families. The project also envisages taking into account variability due to chemical changes to guide the transfer process. The advances made in this project will enable us to better characterize the impact of laser-matter interaction with the perspective of designing new surface functionalizations on various novel metal alloys, opening the door to new application prospects in numerous societal challenges related to health, energy, space, nuclear or defense.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Benjamin Girault, Theme Day of GdR IASIS (Apprentissage de Graphe), 2024, Paris.

Member of the organizing committees

- Jordan Patracone, Regional Workshop POPILS, 2024, Lyon.

Workshop organization

- T4EU core of AI Workshop, November 2024, Saint-Etienne: Quentin Bertrand "Generative Models some Challenges", Amaury Habrard "Foundations of ML", Jordan Patracone "Optimization and Robustness"

- Marc Sebban, "Extract full information and meaning from surface imaging" workshop, SLEIGHT Science Event, January 2024, Saint-Etienne.

11.1.2 Scientific events: selection

Member of the conference program committees

- Amaury Habrard, ICML, 2024, Vienna, area chair.

- Amaury Habrard, ECAI, 2024, Santiago de Compostella, area chair.

- Amaury Habrard, NeurIPS, 2024, Vancouver, area chair.

- Amaury Habrard, ICLR, 2025, Singapore, area chair.

- Marc Sebban, SLEIGHT Science Event, Saint-Etienne, 2024, programme committee.

Reviewer

- Amaury Habrard, IJCAI, 2024, JeJu.

- Jordan Patracone, NeurIPS, 2024, Vancouver.

- Quentin Bertrand, ICLR, 2024, Vienna.

- Quentin Bertrand, ICML, 2024, Vienna.

- Quentin Bertrand, NeurIPS, 2024, Vancouver.

- Rémi Emonet, CAp, 2024, Lille.

- Marc Sebban, CAp, 2024, Lille.

- Amaury Habrard, CAp, 2024, Lille.

11.1.3 Journal

Member of the editorial boards

- Amaury Habrard, Journal of Machine Learning Research, editorial board of reviewers.

- Jordan Patracone, Journal of Machine Learning Research, Reviewer.

Reviewer - reviewing activities

- Quentin Bertrand, Journal of Machine Learning Research.

- Farah Cherfaoui, journal IEEE Transactions on Information Theory.

- Amaury Habrard, journal IEEE Transactions on Pattern Analysis and Machine Intelligence.

11.1.4 Invited talks

- Quentin Bertrand: "*Some Challenges Around Retraining Generative Models on their Own Data*", ECCV 2024 Workshop The Dark Side of Generative AIs and Beyond, October 2024.
- Rémi Emonet "*Détection d'Anomalies dans les Images par Apprentissage Auto-supervisé*", Journée FIL, Lyon, 13 June 2024.
- Benjamin Girault: "*Learning a Graph and Importances of its Vertices*", Machine Learning and Signal Processing Seminar, ENS Lyon, Jan 2024.
- Benjamin Girault: "*Learning a Graph and Importances of its Vertices*", Laboratoire Jean Kuntzman, Grenoble, May 2024.
- Amaury Habrard: "*Domain Adaptation and Transfer Learning*", invited speaker, Inter-PEPR Day (DIADEM, IA, NumPex), 18 November 2024.
- Amaury Habrard: "*Choosing the right complexity measure: a data-driven artificial intelligence perspective*", Congrès de l'IUF, 29 May 2024.
- Marc Sebban: "*Physics-informed Machine Learning: From algorithms to theoretical questions*", Journée scientifique "Simulation et IA" 3DS & Inria, Paris, 29 November 2024.
- Marc Sebban: "*Is it possible to learn well from both data and physical knowledge?*", invited speaker, Univ. Alicante, Spain, 29 May 2024.

11.1.5 Scientific expertise

- Rémi Emonet, scientific expert for the ANR AAPG2024 call.
- Amaury Habrard, scientific expert for the ANR AAPG2024 call, scientific expert for the ANRT (CIFRE), scientific expert for ERC project call (STG)
- Marc Sebban, scientific expert for the "Dispositif Doctorants" Normandy Region, 2024

11.1.6 Research administration

- Rémi Emonet is head of the Machine Learning project at laboratoire Hubert Curien.
- Amaury Habrard is head of the Data Intelligence team, member of the scientific board of the MIAI AI Cluster, co-head of the AI and ML axis of the *Fédération des Laboratoires d'Informatique de Lyon* (FIL), co-responsible of the working group on Physics-aware Machine Learning of the GdR IASIS
- Marc Sebban is deputy director of the Hubert Curien Lab (UMR CNRS 5516), Member of the Board of Directors of the *Fédération des Laboratoires d'informatique de Lyon* (FIL), Member of the executive committee of the EUR Manutech Sleight, Member of the COMEX Labex MILYON, Member of the COS Inria Lyon Centre.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Quentin Bertrand:
  - Computer Science Master, Numerical Optimal Transport for Machine and Deep Learning, 10h, M2, ENS Lyon.
- Eduardo Brandao:
  - Diplôme Universitaire Cycle initial en Technologie de l'Information de Saint-Étienne: Mathèmatiques pour l'ingénieur 1, 52.5h, L1, Télécom Saint-Étienne, UJM

  - Formation Ingénieur Télécom Saint-Étienne: Programmation Orientée Objet, 30h, 1AL3, Télécom Saint- Étienne, UJM
  - Formation Ingénieur Télécom Saint-Étienne: Mini-projet, 12h, 1AL3, Télécom Saint- Étienne, UJM

- Farah Cherfaoui:
  - Licence Mathématiques-Physique-Chimie: Outils informatiques, 91h, L1, Faculté des Sciences, UJM.
  - Licence informatique: programmation impérative, 56h, L1, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Advanced Machine Learning, 4h, M2, Faculté des Sciences, UJM.

- Rémi Emonet:
  - Master Machine Learning and Data Mining: Probablistic Graphical Models, 20h, M2, Faculté des Sciences, UJM.
  - Master Données et Systèmes Connectés: Programmation Web Avancée, 30h, M1, Faculté des Sciences, UJM.

- Rémi Eyraud:
  - Master Machine Learning and Data Mining: Research Methodology, 20h, 1A, Faculté des Sciences, UJM.
  - Master Données et Systèmes Connectés: Research Methodology, 20h, 2A, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Machine Learning Fundamentals and Algorithms, 30h, 1A, Faculté des Sciences, UJM.
  - Master Données et Systèmes Connectés: Machine Learning Fundamentals and Algorithms, 30h, 1A, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Advanced Machine Learning, 3h, M2, Faculté des Sciences, UJM.
  - GACO: Base de Données, 18h, 2A, IUT de Saint-Etienne, UJM.
  - GACO: Conception de Sites Web Dynamiques, 112h, 2A, IUT de Saint-Etienne, UJM.
  - GACO: Etablir le Diagnostique Marketing d'une Organisation (SAE), 8h, 2A, IUT de Saint-Etienne, UJM.
  - GACO: Traitement des Données, 20h, 3A, IUT de Saint-Etienne, UJM.
  - GACO: Environnement Informatique, 16h, 1A, IUT de Saint-Etienne, UJM.

- Benjamin Girault:
  - Master Machine Learning and Data Mining: Deep Learning I, 20h, M1, Faculté des Sciences, UJM.

- Amaury Habrard:
  - Master Machine Learning and Data Mining: Advanced Algorithms and Programming, 20h, M2, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Advanced Machine Learning, 20h, M2, Faculté des Sciences, UJM.
  - joint course Master Machine Learning and Data Mining and Master Données and Systèmes Connectés: Deep Learning II, 15h, M2, Faculté des Sciences, UJM.

- Jordan Patracone:

  - Formation Ingénieur Télécom Saint-Étienne: Langage C Algorithmie et structures de données, 32h, 1A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur Télécom Saint-Étienne: Algorithmique et structures de données, 13h, 1A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur Télécom Saint-Étienne: Projet recherche et innovation, 5h, 3A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur Télécom Saint-Étienne: Big Data Project, 10h, 3A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur Télécom Saint-Étienne: Projet d'ingéniérie, 14h, 2A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur en Apprentissage Data Engineering: Statistiques inférentielles, 33h, 2A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur en Apprentissage Data Engineering: Algorithms for data analysis, 28h, 2A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur en Apprentissage Data Engineering: Qualité de fonctionnement, 11h, 3A, Telecom Saint-Etienne, UJM.
  - Formation Ingénieur en Apprentissage Data Engineering: Innovation en data, 2h, 3A, Telecom Saint-Etienne, UJM.
  - Master Machine Learning and Data Mining: Advanced Machine Learning, 6h, M2, Faculté des Sciences, UJM.

- Marc Sebban:

  - Licence Informatique: Probabilités-Statistiques, 24h, L3, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Introduction to Machine Learning, 20h, M1, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Data Analysis, 24h, M1, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Advanced Machine Learning, 12h, M2, Faculté des Sciences, UJM.
  - Master Machine Learning and Data Mining: Machine Learning Project, 20h, M2, Faculté des Sciences, UJM.

11.2.2 Supervision

- PhD in progress: Fayad Ali Banna. Physics-guided Machine Learning, since Octo. 2022. Marc Sebban and Rémi Emonet.
- PhD in progress: Hind Atbir. Learning fair and robust kernel-based models with generalization guarantees, since Oct. 2024. Remi Eyraud and Farah Cherfaoui.
- Postdoc in progress: Antoine Caradot. On the estimation of integrals of functions: applications in PIML, since Oct. 2024. Rémi Emonet, Amaury Habrard and Marc Sebban.
- PhD in progress: Wissal Ghamour. Nouvelles approches de l'Intelligence Artificielle pour les attaques par canaux auxiliaires, since Dec. 2024. Rémi Eyraud
- PhD in progress: Dorian Llavata. Apprentissage Profond Diversement Supervisé Pour Les Attaques Par Canaux Auxiliaires, Rémi Eyraud, since 2022
- PhD in progress: Volodimir Mitarchuk, Theory and Algorithms for the Understanding of Deep Neural Network on Sequential Data, since 2021. Rémi Eyraud, Amaury Habrard, Rémi Emonet.

- PhD in progress: Robin Mermillod-blondin, Optimisation multicritère de couleurs plasmoniques pour les documents d'identité. Rémi Emonet.
- PhD in progress: Sayan Chaki, Unsupervised Analysis of Ornaments extracted from Ancient Books, Rémi Emonet.
- PhD in progress: Abdel-Rahim Mezidi, Unveiling and Incorporating Knowledge in Physics-Guided Machine Learning Models, Amaury Habrard, Jordan Patracone.
- PhD in progress: Ben Gao, Toward frugal machine learning with physics-aware models, Jordan Patracone.
- PhD in progress: Thibault Girardin, Prediction of multidimensional colors printed by laser on plasmonic metamaterials using deep learning and adaptive strategies, Amaury Habrard.
- PhD in progress: Erick Gomez, TRansfer lEarning for Frugal and Accurate modeling of SURface Functionalization prediction – application to multicomponent alloys, Amaury Habrard.
- PhD defended in 01/2024: Rehan Jhuboo. Morphometry-guided Super Resolution for Bone Microstructure CT lmaging, Marc Sebban

11.2.3 Juries

- Marc Sebban: Antonio Rios Vila (Univ. Alicante, President), Etienne Le Naour (PSL, Member), Eduardo Brandao (Univ. Saint-Etienne, Member), Rehan Jhuboo (Univ. Saint-Etienne, Director), Rémi Emonet (HDR, Univ. Saint-Etienne, Tutor).
- Rémi Emonet: Ashna Jose (PhD, Université Grenoble Alpes, Reviewer), Eduardo Brandao (Univ. Saint-Etienne, Supervisor).
- Rémi Eyraud: Reda Marzouk (Univ. Nantes, Member)
- Amaury Habrard: Steeven Janny (INSA Lyon, President), Emmanuel Menier (U.Paris-Saclay, Reviewer), Antoine de Mathelin (ENS-Paris-Saclay, Reviewer), Marin Scalbert (U.Paris-Saclay, Reviewer), Hoel Le Capitaine (HDR, Univ. Nantes, member), Eduardo Brandao (Univ. Saint-Etienne, invited)

11.3 Popularization

11.3.1 Productions (articles, videos, podcasts, serious games, ...)

- Marc Sebban: interviews leading to several articles related to the creation of the MALICE team (IF Saint-Etienne, l'ESSOR, L'Usine Nouvelle, Dépêche AEF Info, Carnot TSN).
- Amaury Habrard: co-author of the white paper "Generative AI and Hypertrucages" from Minalogic for the Auvergne Rhone-Alpes Region
- Rémi Emonet, Quentin Bertrand, collaboration with Ockham, we wrote a friendly blog post on recent flow matching techniques.

11.3.2 Participation in Live events

- Rémi Eyraud: 2h of conference titled "de l'Algorithme à l'IA". Conférences pour Tous.tes – MJC Annonay (14/03/2024) ; Association Culturelle des Monts du Matin – St-Genis l'Argentière (10/12/02024)
- Rémi Eyraud: 2h conference titled "Démystifier l'IA". Saison culturelle, villes de Sorbiers et St-Jean-Bonnefond, 26/11/2024.

11.3.3 Others science outreach relevant activities

- Jordan Patracone: presentation to the executive committee of CARSAT Rhône-Alpes (Artificial intelligence at the service of public organizations)
- Rémi Eyraud: round table on "IA: au-delà des craintes", Comité Loire Connect, Département de la Loire.
- Amaury Habrard: round table on Artificial Intelligence, Club Eco - agence d'urbanisme EPURES (04/12/2024).
- Amaury Habrard: round table on the future of the Labex MILyon (14/10/2024)

12 Scientific production

12.1 Major publications

[1] D. Ferbach, Q. Bertrand, A. J. Bose and G. Gidel. 'Self-Consuming Generative Models with Curated Data Provably Optimize Human Preferences'. In: NeurIPS. Vancouver (BC), Canada, 10th Dec. 2024, pp. 1–27. URL: https://hal.science/hal-04711701 (cit. on pp. 5, 10, 11).

[2] B. Girault, R. Emonet, A. Habrard, J. Patracone and M. Sebban. 'Approximation Error of Sobolev Regular Functions with tanh Neural Networks: Theoretical Impact on PINNs'. In: 2024 Joint European Conference on Machine Learning and Knowledge Discovery in Databases (ECML PKDD 2024). Machine Learning and Knowledge Discovery in Databases: Research Track. Vilnius, Lithuania, 9th Sept. 2024. URL: https://inria.hal.science/hal-04518335 (cit. on pp. 5, 8).

[3] V. Mitarchuk, C. Lacroce, R. Eyraud, R. Emonet, A. Habrard and G. Rabusseau. 'Length Independent PAC-Bayes Bounds for Simple RNNs'. In: *Proceedings of the 27th International Conference on Artificial Intelligence and Statistics (AISTATS) 2024, Valencia,Spain. PMLR: Volume 238*. AISTATS 2024 - 27th International Conference on Artificial Intelligence and Statistics. Vol. 238. Valence, Spain, 2nd May 2024. URL: https://hal.science/hal-04488664 (cit. on pp. 8, 9).

[4] J. Patracone, L. Anquetil, Y. Liu, G. Gasso and S. Canu. 'Linear Modeling of the Adversarial Noise Space'. In: ECML PKDD 2024 - European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases. Vilnius, Lithuania, 2024. URL: https://inria.hal.science/hal-04589704.

[5] J. Patracone, P. Viallard, E. Morvant, G. Gasso, A. Habrard and S. Canu. 'A Theoretically Grounded Extension of Universal Attacks from the Attacker's Viewpoint'. In: ECML PKDD 2024 - European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases. Vilnius, Lithuania, 2024, pp. 1–27. DOI: 10.1007/978-3-031-70359-1_17. URL: https://hal.science/hal-03615461 (cit. on pp. 8, 9).

[6] P. Viallard, R. Emonet, A. Habrard, E. Morvant and V. Zantedeschi. 'Leveraging PAC-Bayes Theory and Gibbs Distributions for Generalization Bounds with Complexity Measures'. In: AISTATS 2024 - 27th International Conference on Artificial Intelligence and Statistics. Valencia, Spain, 2024. URL: https://hal.science/hal-04473777 (cit. on p. 8).

[7] P. Viallard, P. Germain, A. Habrard and E. Morvant. 'A General Framework for the Practical Disintegration of PAC-Bayesian Bounds'. In: *Machine Learning* 113.2 (2024), pp. 519–604. DOI: 10.1007/s10994-023-06391-0. URL: https://hal.science/hal-03143025 (cit. on pp. 8, 9).

12.2 Publications of the year

International journals

[8] K. Bilko, R. G. Alía, M. S. Barbero, S. Girard, Y. Aguiar, M. Cecchetto, C. Belanger-Champagne, S. Danzeca, W. Hajdas, A. Hands, P. M. Holgado, Y. M. Garcia, A. R. Maestre, D. Prelipcean, F. Ravotti and M. Sebban. 'Mixed-field Radiation Monitoring and Beam Characterisation Through Silicon Diode Detectors'. In: *IEEE Transactions on Nuclear Science* 71.4 (5th Jan. 2024), pp. 777–784. DOI: 10.1109/TNS.2024.3350342. URL: https://hal.science/hal-04378518.

[9] K. Bilko, R. G. Alía, A. Constantino, A. Coronetti, S. Danzeca, M. Delrieux, N. Emriskova, M. A. Fraser, S. Girard, E. P. Johnson, M. Sebban, F. Ravotti and A. Waets. 'CHARM High-energy Ions for Micro Electronics Reliability Assurance (CHIMERA)'. In: *IEEE Transactions on Nuclear Science* (25th Jan. 2024), pp. 1–1. DOI: 10.1109/TNS.2024.3358376. URL: https://hal.science/hal-04421732.

[10] V. Mitarchuk, R. Emonet, R. Eyraud and A. Habrard. 'On the theoretical limit of gradient descent for Simple Recurrent Neural Networks with finite precision'. In: *Transactions on Machine Learning Research Journal* 3124 (2024). URL: https://hal.science/hal-04874202.

[11] D. Robissout, L. Bossuet and A. Habrard. 'Scoring the predictions: a way to improve profiling side-channel attacks'. In: *Journal of Cryptographic Engineering* (8th Apr. 2024). DOI: 10.1007/s13389-024-00346-4. URL: https://hal.science/hal-04538242.

International peer-reviewed conferences

[12] F. Ali Banna, J.-P. Colombier, R. Emonet, M. Sebban and R. Emonet. 'Physics-informed Machine Learning for Better Understanding Laser-Matter Interaction'. In: *IEEE*. The 36th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2024). Vol. 1. 1-7. Herndon, VA, United States: IEEE Trans, 2024, p. 7. URL: https://hal.science/hal-04717837 (cit. on p. 10).

[13] J. Azorin-Lopez, M. Sebban, N. Garcia-d'Urso, A. Habrard and A. Fuster-Guillo. 'Generative shape deformation with optimal transport using learned transformations'. In: *IEEE 2024, ISBN 979-8-3503-5931-2*. International Joint Conference on Neural Networks (IJCNN). YOKOHAMA, Japan, 30th June 2024. URL: https://hal.science/hal-04628534.

[14] S. K. Chaki, Z. S. Baltaci, E. Vincent, R. Emonet, F. Vial-Bonacci, C. Bahier-Porte, M. Aubry and T. Fournel. 'Historical Printed Ornaments: Dataset and Tasks'. In: ICDAR 2024 - International Conference on Document Analysis and Recognition. Vol. 14806. Lecture Notes in Computer Science. Athens, Greece: Springer Nature Switzerland, 9th Sept. 2024, pp. 251–270. DOI: 10.1007/978-3-031-70543-4_15. URL: https://hal.science/hal-04720711.

[15] S. Marouani, K. Singh, B. Jeudy, A. Bradai and A. Habrard. 'Advanced Traffic Engineering in WAN Using Graph Attention Networks'. In: *Proceedings of the 20th International Conference on Wireless and Mobile Computing, Networking and Communications, Wimob 2024*. The 20th International Conference on Wireless and Mobile Computing, Networking and Communications, Wimob 2024. Paris, France, 21st Oct. 2024. URL: https://hal.science/hal-04698713.

[16] V. Mitarchuk and R. Eyraud. 'A Theoretical Analysis of the Incremental Counting Ability of LSTM in Finite Precision'. In: LearnAut workshop 2024. Tallinn, Estonia, 2024. URL: https://hal.science/hal-04619401.

[17] E. G. Soto, R. Emonet and M. Sebban. 'Unsupervised Learning and Effective Complexity: introducing JPG and Neural Sophistication'. In: International Conference on Tools with Artificial Intelligence (ICTAI). Herndon, United States, 30th Oct. 2024. URL: https://hal.science/hal-04830374 (cit. on pp. 8, 10).

Conferences without proceedings

[18] J.-P. Colombier, E. Brandao, A. Nakhoul, F. Ali Banna, R. Emonet, A. Habrard, F. Jacquenet, F. Garrelie and M. Sebban. 'Deciphering the complexity behind laser-induced selforganized nanopatterns'. In: 17th International Conference on Laser Ablation (COLA 2024). Hersonissos, Greece, 29th Sept. 2024. URL: https://ujm.hal.science/ujm-04881596.

Reports & preprints

[19] A.-R. Mezidi, J. Patracone, S. Salzo, A. Habrard, M. Pontil, R. Emonet and M. Sebban. *Bregman Proximal Viewpoint on Neural Operators*. 6th June 2024. URL: https://inria.hal.science/hal-04584456 (cit. on p. 10).

[20] M. de Santis, J. Patracone, F. Rinaldi, S. Salzo, M. Schmidt and S. Venturini. *Relax and penalize: a new bilevel approach to mixed-binary hyperparameter optimization*. 16th Jan. 2025. URL: https://hal.science/hal-04183917.

Other scientific publications

[21] F. Ali Banna, R. Emonet, A. Rudenko, M. Sebban and J.-P. Colombier. 'Predicting laser energy absorption on nanostructured surfaces with deep learning'. In: Machine Learning in Photonics. Strasbourg, France: SPIE, 7th Apr. 2024, p. 74. DOI: 10.1117/12.3022317. URL: https://hal.science/hal-04888157.