ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

Optimization and Games for AI

J. Bolte & J.B. Lasserre

September 28-29, 2020

Université Fédérale
Toulouse Midi-Pyrénées

Overview

MEMBERS

Scientific perimeter of the theme

Theme: Optimization and Games in AI

On-going work

Highlight & main results

Scientific animation of the theme

MEMBERS

Chairs: J. Bolte, S. Gratton, J. Lasserre, J.-M. Loubes, J. Renault

People involved: (co chairs): N. Couellan, F. de Gournay, F. Gensbittel, S. Gerchinovitz, M. Korda, V. Magron, F. Malgouyres, E. Pauwels, M. Serrurier, P. Weiss

ANITI Resources (post doc, PhD, Mise à Disposition Industrielle, DEEL)

- PhD Students: E. M. Achour (FM, SG), M. d'Andrea (JR, FG), J. Bona-Pellisier (FM), Tong Chen (JBL, VM, EP), R. Dragomir (JB), A. Gonzalez (JML, EdB), Tam-Ngoc Le (JB, EP), E. de Montbrun (JR, SG)
- Post-doctoral fellows: T. Cesari (JR, SG), L. Glaudin (JB, EP), D. Pizzaro (JR, FG), R. Rios-Zertuche (JB, EP)
- MAD: M. Ducoffe, A. Gauffriau, J. Sen Gupta
- Data scientists IRT St-Exupéry: D. Bertoin, T. Boissin, F. Mamalet

Other Resources (other Phd project) 2 PhD from Ecole Polytechnique, ERC student of Févotte, C. Castera, H. Mai (PhD EDMITT, JBL,VM). Post-doc Jie Wang (ANR of VM)

Scientific perimeter of the theme

Develop theory and algorithms in optimization and games for ML/AI

- Structural results (role of geometry, algebra, strategy, information)
- Algorithm design (FOM, SOM, SOS, GANS)
- Convergence, rates issues in training phases global guarantees
- Robust predictions/solutions
- Strategy and training
- Strategic behaviors in AI environments

Divided into 3 threads

1. Optimization theory for AI
2. Robustness
3. Game theory and AI

Optimization for AI: structural results

ARTIFICIAL & NATURAL INTELLIGENCE TOULOUSE INSTITUTE

- **Scalable positivity certificates**. ML problems are often semi-algebraic optimization problems for which a global optimum is highly desired (e.g. certifications of robustness). Goal: develop based on positivity certificates for larger problems.

  Challenge: scalability, solutions sparsity, correlative-sparsity

- **Landscapes in Deep Learning**: Understand geometric structure of loss functions (linear networks, classification of critical points).

  Goals: simple tests for optimization guarantees, recommendations towards better design of network architectures, regularization

  Challenge: nonlinear NN.

- **Automatic differentiation in ML**: Backpropagation is central in ML. It applies smooth calculus to nonsmooth problems.

  Goal: understanding the phenomenon for a wide variety of DL problems. Algorithm design, convergence theory, robustness

Optimization for AI: algorithms

- **Zero-order global bandit optimization** Find approximate minimum, level-set, or other global characteristics of functions by using only loss evaluation

  Goal: design bandit algorithms with finite-time error bounds.

- **Analysis and convergence of first-order methods** Deep learning involves nonconvex nonsmooth optimization stochastic algorithms; these are poorly understood.

  Goal: build convergence theory from stabilization to rate estimation.

- **Higher-order methods** (e.g. Newton's method) They dramatically decrease complexity but are computationally more expensive.

  Goal: develop *multilevel strategy* with hierarchy of approximating problems of decreasing dimension.

- **Worst-case analysis** Build worst-case scenarios to understand the limit of a given optimization strategy.

Optimization for AI and interactions

ARTIFICIAL & NATURAL INTELLIGENCE TOULOUSE INSTITUTE

- **Surrogate input-output models for complex problems**
  Neural networks can be used as surrogate models for complex functions whose evaluation requires heavy simulations.
  Goal: Construct a data set and a neural network architecture guaranteeing the performances of such a surrogate model.
- **Surrogate input-output models with high precision** Approximate solutions/parameters of some PDE by large learning problems.
  Goal: develop some Gauss-Newton solver to approximate solutions of PDEs. Use multilevel Levenberg- Marquardt method for training.
- **Optimization on measures spaces** These problems may be seen as large scale semi-infinite programs.
  Goals: develop certified methods with a low complexity.
  Applications include two-layer neural networks, super-resolution and sampling theory in imaging.

Thread Robustness

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

Diverse robustness issues involving sensitivity to the input or to the training set, resistance to outliers, or distributional shift are key for practical applications

- Understand generalization
- Robustness of neural networks
- Towards certification

*Core research topic for the Certifiable AI IP.

Robustness: the optimization viewpoint

- **Robustness and sensitivity via certificates of positivity**. Robustness of DNNs by certifying sharp bound on the Lipschitz constant the input-output map.

  Goal: sensitivity and robustness analysis

- **Robustness via worst case analyses**. Robustness via worst-case analyses or counterfactual models.

  e.g.: an adversary tries to modify the outcomes by changing some parameters of the input.

  Goal: study of potential counterfactual models provides both a study of the robustness of algorithms and explainability of the model

- **Trust region with variable accuracy on function and gradient**

  Trust-region algorithms are extremely robust.

  Goal: develop Trust-region with dynamic accuracy for very high-performance computing where multi-precision computation

Robustness: statistical perspectives

- **High confidence prediction regions**. Point predictions are insufficient in practice, while confidence regions are more desirable.

  Goal: design and prove coverage guarantees for methods that work with any black-box prediction model (e.g., conformal predictions).

- **Testing conditions of stability**

  Optimal neural networks are very sensitive to the optimization procedure (choice of the algorithm, initialization, batches).

  Goal: Necessary/sufficient conditions granting that features, outputs of NN are well defined from the data, independently algorithms

- **The Wasserstein paradigm for robustness**

  Wasserstein distances have fine sensitivity for measuring differences between distribution/images.

  Goal: Devise robust classification algorithms by taking advantage of this sensitivity.

Robustness: low resources NN

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

- **Neural network with quantized weights**

  Common neural network architectures require heavy computations that prevent their use in embedded systems.

  Goal: Optimization and analysis of NN with low energy consumption

- **Robustness and automatic differentiation**. Automatic differentiation is considerably impacted by low precision computation (16 or 32 bits). Considerable changes may occur due to rounding errors.

  Goal: optimize autodiff solver in order to make robust training/generalization phases.

Thread: Game Theory

The game theory thread investigates possible applications of game theory concepts and methods to AI, and study strategic behavior in complex (AI-related) environments.

Learning and bandit problems

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

- No-regret learning,
- Strategic experimentation with observed actions and private rewards,
- Bilateral trade with bandits.

Neural networks and GANs

- GANs: Proving convergence bounds for the computation of optimal strategies. Modifying the zero-sum game to improve GANs, inventing new games for GANs and studying new game-oriented algorithms,
- Non-parametric adversarial sequential regression: predict almost as well as the unknown best neural network predictor.

Decision making in complex strategic environments

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

- Theoretical premises: dynamic games (repeated games), games with incomplete information and strategic use of information.
- Games with restricted sets of strategies (e.g., automata or neural networks), games between autonomous devices,
- Algorithms for games with (piecewise) differentiable payoffs
- Hybrid games with both autonomous devices and rational agents (human machine interactions + malicious attacks)
- Matching markets: algorithms for matching several sides of a market

New collaborations?

ARTIFICIAL & NATURAL INTELLIGENCE TOULOUSE INSTITUTE

- N. Asher, Verification of Machine Learning systems: e.g., Banach-Mazur-like games are used to model conversation, and properties of bias relevant to learning
- H. Fargier, Games and knowledge compilation; possibilistic games with incomplete information.

On-going work

On-going collaboration between chairs [6 projects]
Bolte-Lasserre (Pauwels), Bolte-Loubes (Pauwels, Serrurier), Bolte-Renault (Gerchinovitz, Malgouyres), Loubès-Renault (Gerchinovitz), Bolte-Dobigeon (Bolte, Févotte, Pauwels), Delahaye-Loubès (Couellan)

On-going collaboration with ANITI Industrial partners

- IRT Saint-Exupéry: S. Gerchinovitz, T. Cesari and Etienne de Montbrun.
- Package python UT3/IRT (Loubès)
  `https://pypi.org/project/deel-lip/1.0.0/`
- Mission Certification working group at IRT, with experts from French transport companies, data-scientitsts and academic researchers (Think Tank about ML in certified systems, S. Gerchinovitz, F. Mamalet)
- Future project : Gradient descent on overparameterized neural networks (T. Cesari+ I. Kuzborskij, Deep Mind London)

On-going work

On-going collaboration with external projects (national, EU, industry)
ANR MasDol (Gadat): AI and stochastic methods, ANR (Magron), ANR Bold (Bachoc), ERC Factory (Févotte), ERC Androma (S. Leonardi, markets with bandits), US Air Force grant (Bolte-Pauwels): Deep Learning

On-going ANITI Phd & Post doc
J. Bona-Pellisier (FM), A. Gonzalez (Loubes, del Barrio), Tong Chen (JBL, VM, EP), Tam Le Ngoc (JB, EP), E. de Montbrun (JR, SG), M. d'Andrea (JR, FG)

Associate PhD: R. Dragomir (JB), E. M. Achour (FM, SG).

Post-doctoral fellows: R. Rios-Zertuche (JB, EP), T. Cesari (JR, SG), D. Pizzaro (JR, FG)

Highlight: talks

- Deep Mind Seminar (S. Gerchinovitz, Paris March 2020)
- Exploring the interplay between Dynamical Systems and Function Spaces2020 American Control Conference, (J. Lasserre, July 2020)
- Learning Week of the POEMA workshop (August 2020) http://poema-network.eu/meeting/online-learning-weeks, (June 2020, E. Pauwels)
- Seminaire Français d'optimisation, virtual, (E. Pauwels, June 2020)
- Seminar at The International Centre for Theoretical Sciences, Bangalore India, (S. Gratton, June 2020).
- One-World Game Theory seminar (J. Renault, June 2020).
- One-World Optimization Seminar, (J. Bolte, July 2020).

Highlights: Awards and Grants

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

- E. Pauwels is awarded the CNRS Bronze Medal,
- P. Weiss wins an European Space Agency challenge, Deep learning for detecting objects in the geostationary ring, `https://kelvins.esa.int/spot-the-geo-satellites/leaderboard/` with Agenium SPACE.
- Submissions to ANR, EU-related projects
  - **ANR** de Magron
  - **ANR** de Gadat, participants ANITI: Bolte, Pauwels, Serrurier, Renault
  - **Air Force Grant** Bolte & Pauwels
  - **Zeiss Grant:** Weiss

Scientific animation of the theme

- S Sabach & M. Teboulle at UT1: Lectures on *Large scale optimization*, Toulouse, 05-09-2019.
- Matinée optimisation et statistiques: Toulouse 12-09-2019: J. Fadili (IUF), S. Gadat (IUF), S. Sabach (The Technion), M. Teboulle (Tel Aviv University),
- Reinforcement Learning school: Spring 2021, distancial (S. Gerchinovitz head of the organization, T. Cesari)
- Worskhop: Machine Learning in Certified Systems, Theoretical and Practical Challenges (Toulouse and Montreal, January 2021, head of organization: S. Gerchinovitz)
- Introduction to Game Theory: J.Renault, 4h 2021, ISAE, Neuroergonomics and AI domain
- Seminar ANITI of Ph. Toint, (July 2020)

Scientific animation of the theme

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

- Synergy with **SPOT** (*Multidisciplinary Optimization Seminar in Toulouse*)
- AI Lectures at MVA, Paris Saclay, by E. Pauwels, S. Gerchinovitz and F. Malgouyres
- Participation to the creation of "Séminaire français d'optimisation", online monthly event
- New emerging collaboration between chairs & industrial partner: Collaboration with RTE company on efficient algorithms for solving large-scale *Optimum Power Flow*

The theme in numbers

The theme in numbers

- Number of articles and preprints: 47
- "Rank A" papers: NIPS, MPA, MOR, SIAM J., FOCM, GEB: 18 papers
- Number of students (PhD, Post-Doc): 12
- Number of prizes/awards/grant: 6