Offer #2024-07880

PhD Position F/M Responsible Reinforcement Learning: Robustness and Privacy in and by Sequential Decision Making

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

About the research centre or Inria department

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT)

Context

In his/her journey to the doctoral thesis, the candidate will be supported by PEPR project FOUNDRY, and supervised by Debabrota Basu and Emilie Kaufmann. Debabrota and Emilie are affiliated with theScool project-team (previously SequeL) of Inria Centre at University of Lille. As a team, Scool is internationally recognised for developing theories and algorithms for sequential learning and decision making, i.e. in the fields of bandits and reinforcement learning.

As RL algorithms are getting deployed in real-life the questions of responsible deployment, such as robustness to noise and perturbation to the feedback from environment, and privacy if users are involved in the environment yielding data.

Our works have shown that for structure-less and linear settings of multi-armed bandits and active testing (aka pure exploration) imposing privacy yields two regimes of performance. For the regime used in practice, privacy can be preserved without loss of utility. But our existing approach is not directly applicable to more practically appealing settings of RL, like MDPs or bandits with side-information (aka contexts). In these settings, there is a gap between achievable performances and the algorithms. Thus, we want to study whether the cost of privacy in contextual bandits and MDPs, and also to design optimal, computationally efficient algorithms.

Similarly, we have studied impact of unbounded corruption in feedback and safety constraints in stochastic multi-armed bandits and active testing (aka pure exploration). We want to understand how do they impact more structured RL problems and how can we design optimal algorithms in these setting.

The project is expected to simulate the existing and new collaborations with researchers and groups working on privacy-preserving machine learning, robustness, adaptive testing, and reinforcement learning. In future, the candidate will be encouraged to not only work with us but collaborate internationally. The candidate will also be part of the HumAIn alliance that aims toward studying humane impact of deploying AI.

From the application point of view, Scool is involved in multiple projects that incorporates medical data, and agricultural data. Depending on the future development, we will be interested to deploy such responsible RL systems and algorithm in such socially-meaningful applications.

Assignment

This position is entirely dedicated to do one's Ph.D. thesis. French rules put a strong emphasis on the fact that the Ph.D. is completed within 3 full years of studies.

It is also possible to teach up to a reasonnable amount of time per year (say 30 hours / year to give a

rough idea of what we mean by "reasonable"). More details about the topic of the Ph.D. is available at this link.

Main activities

All research activities, that is bibliographical search, proposing original ideas related to the topic of the Ph.D. and developing them, presenting the work in the Scool seminar, workshops and conferences. The candidate should aim to publish the research results in premier conferences and journals of our field of research (e.g. ICML, NeurIPS, COLT, IJCAI, AAAI, JMLR). Since the work involves and impacts the responsible AI in general, the successful candidate should collaborate in writing scientific articles aiming towards the larger audience.

Skills

The candidate should preferably have the following skills:

- A strong background in mathematics/statistics
- A good knowledge of machine learning, statistics, and algorithms
- Broad interest for differential privacy and robustenss
- Knowledge of programming languages such as Python. C/C++
- Some experience with implementation and experimentation (a plus)
- A good command of English

Please follow the instructions given in https://team.inria.fr/magnet/how-to-apply/ to set up your application file.

In brief, the application of the candidate should include his/her CV, an application letter, (two or more) recommendation letters, and the school transcripts. It is reccommended that the candidate contacts Debabrota and Emilie while preparing the application.

The deadline for application is 15th July, 2024.

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration

1st and 2nd year : 2100 € (gross monthly salarye)

3rd year : 2190 € (gross monthly salary)

General Information

- **Theme/Domain :** Optimization, machine learning and statistical methods
  Statistics (Big data) (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2024-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-08-01

Contacts

- **Inria Team :** SCOOL
- **PhD Supervisor :**
  Basu Debabrota / debabrota.basu@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and

entrepreneurial projects that have a worldwide impact.

The keys to success

A successful candidate should:

- collaborate inside the team, and with the external researchers and engineers, if needed
- organise the work systematically
- be keen to learn new theory and algorithms developed in the fast-changing field of RL, robust ML, and privacy
- engage in meetings and discussions regularly

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.