## Workshop on Security in Machine Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Nicolas Papernot · Jacob Steinhardt · Matt Fredrikson · Kamalika Chaudhuri · Florian Tramer*

There is growing recognition that ML exposes new vulnerabilities in software systems. Some of the threat vectors explored so far include training data poisoning, adversarial examples or model extraction. Yet, the technical community's understanding of the nature and extent of the resulting vulnerabilities remains limited. This is due in part to (1) the large attack surface exposed by ML algorithms because they were designed for deployment in benign environments---as exemplified by the IID assumption for training and test data, (2) the limited availability of theoretical tools to analyze generalization, (3) the lack of reliable confidence estimates. In addition, the majority of work so far has focused on a small set of application domains and threat models. This workshop will bring together experts from the computer security and machine learning communities in an attempt to highlight recent work that contribute to address these challenges. Our agenda will complement contributed papers with invited speakers. The latter will emphasize connections between ML security and other research areas such as accountability or formal verification, as well as stress social aspects of ML misuses. We hope this will help identify fundamental directions for future cross-community collaborations, thus charting a path towards secure and trustworthy ML.

---

## Challenges and Opportunities for AI in Financial Services: the Impact of Fairness, Explainability, Accuracy, and Privacy

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Manuela Veloso · Nathan Kallus · Sameena Shah · Senthil Kumar · Isabelle Moulinier · Jiahao Chen · John Paisley*

The adoption of artificial intelligence in the financial service industry, particularly the adoption of machine learning, presents challenges and opportunities. Challenges include algorithmic fairness, explainability, privacy, and requirements of a very high degree of accuracy. For example, there are ethical and regulatory needs to prove that models used for activities such as credit decisioning and lending are fair and unbiased, or that machine reliance doesn’t cause humans to miss critical pieces of data. For some use cases, the operating standards require nothing short of perfect accuracy. Privacy issues around collection and use of consumer and proprietary data require high levels of scrutiny. Many machine learning models are deemed unusable if they are not supported by appropriate levels of explainability. Some challenges like entity resolution are exacerbated because of scale, highly nuanced data points and missing information. On top of these fundamental requirements, the financial industry is ripe with adversaries who purport fraud and other types of risks. The aim of this workshop is to bring together researchers and practitioners to discuss challenges for AI in financial services, and the opportunities such challenges represent to the

community. The workshop will consist of a series of sessions, including invited talks, panel discussions and short paper presentations, which will showcase ongoing research and novel algorithms.

---

## Bayesian Deep Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Yarin Gal · José Miguel Hernández-Lobato · Christos Louizos · Andrew Wilson · Zoubin Ghahramani · Kevin P Murphy · Max Welling*

While deep learning has been revolutionary for machine learning, most modern deep learning models cannot represent their uncertainty nor take advantage of the well studied tools of probability theory. This has started to change following recent developments of tools and techniques combining Bayesian approaches with deep learning. The intersection of the two fields has received great interest from the community over the past few years, with the introduction of new deep learning models that take advantage of Bayesian techniques, as well as Bayesian models that incorporate deep learning elements [1-11]. In fact, the use of Bayesian techniques in deep learning can be traced back to the 1990s', in seminal works by Radford Neal [12], David MacKay [13], and Dayan et al. [14]. These gave us tools to reason about deep models' confidence, and achieved state-of-the-art performance on many tasks. However earlier tools did not adapt when new needs arose (such as scalability to big data), and were consequently forgotten. Such ideas are now being revisited in light of new advances in the field, yielding many exciting new results.Extending on the workshop's success from the past couple of years, this workshop will again study the advantages and disadvantages of the ideas above, and will be a platform to host the recent flourish of ideas using Bayesian approaches in deep learning and using deep learning tools in Bayesian modelling. The program includes a mix of invited talks, contributed talks, and contributed posters. The main theme this year will be applications of Bayesian deep learning in the real world, highlighting the requirements of practitioners from the research community. Future directions for the field will be debated in a panel discussion. The BDL workshop was the second largest workshop at NIPS over the past couple of years, with last year's workshop seeing an almost 100% increase in the number of submissions (75 submissions in total), attracting sponsorship from Google, Microsoft Ventures, Uber, and Qualcomm in the form of student travel awards.Topics:Probabilistic deep models for classification and regression (such as extensions and application of Bayesian neural networks),Generative deep models (such as variational autoencoders),Incorporating explicit prior knowledge in deep learning (such as posterior regularization with logic rules),Approximate inference for Bayesian deep learning (such as variational Bayes / expectation propagation / etc. in Bayesian neural networks),Scalable MCMC inference in Bayesian deep models,Deep recognition models for variational inference (amortized inference),Model uncertainty in deep learning,Bayesian deep reinforcement learning,Deep learning with small data,Deep learning in Bayesian modelling,Probabilistic semi-supervised learning techniques,Active learning and Bayesian optimization for experimental design,Applying non-parametric methods, one-shot learning, and

Bayesian deep learning in general,Implicit inference,Kernel methods in Bayesian deep learning.Call for papers:A submission should take the form of an extended abstract (3 pages long) in PDF format using the NIPS style. Author names do not need to be anonymized and references (as well as appendices) may extend as far as needed beyond the 3 page upper limit. If research has previously appeared in a journal, workshop, or conference (including NIPS 2017 conference), the workshop submission should extend that previous work.Submissions will be accepted as contributed talks or poster presentations. Related previous workshops:Bayesian Deep Learning (NIPS 2017)Principled Approaches to Deep Learning (ICML 2017)Bayesian Deep Learning (NIPS 2016)Data-Efficient Machine Learning (ICML 2016)Deep Learning Workshop (ICML 2015, 2016)Deep Learning Symposium (NIPS 2015 symposium)Advances in Approximate Bayesian Inference (NIPS 2015)Black box learning and inference (NIPS 2015)Deep Reinforcement Learning (NIPS 2015)Deep Learning and Representation Learning (NIPS 2014)Advances in Variational Inference (NIPS 2014)

---

## Modeling the Physical World: Learning, Perception, and Control

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Jiajun Wu · Kelsey Allen · Kevin Smith · Jessica Hamrick · Emmanuel Dupoux · Marc Toussaint · Josh Tenenbaum*

Despite recent progress, AI is still far from achieving common-sense scene understanding and reasoning. A core component of this common sense is a useful representation of the physical world and its dynamics that can be used to predict and plan based on how objects interact. This capability is universal in adults, and is found to a certain extent even in infants. Yet despite increasing interest in the phenomenon in recent years, there are currently no models that exhibit the robustness and flexibility of human physical reasoning.There have been many ways of conceptualizing models of physics, each with their complementary strengths and weaknesses. For instance, traditional physical simulation engines have typically used symbolic or analytic systems with “built-in” knowledge of physics, while recent connectionist methods have demonstrated the capability to learn approximate, differentiable system dynamics. While more precise, symbolic models of physics might be useful for long-term prediction and physical inference; approximate, differentiable models might be more practical for inverse dynamics and system identification. The design of a physical dynamics model fundamentally affects the ways in which that model can, and should, be used.This workshop will bring together researchers in machine learning, computer vision, robotics, computational neuroscience, and cognitive psychology to discuss artificial systems that capture or model the physical world. It will also explore the cognitive foundations of physical representations, their interaction with perception, and their applications in planning and control. There will be invited talks from world leaders in the fields, presentations and poster sessions based on contributed papers, and a panel discussion.Topics of discussion will include- Building and learning physical models (deep networks, structured probabilistic generative models, physics engines)- How to combine model-based and model-free approaches to physical prediction- How to use physics models

in higher-level tasks such as navigation, video prediction, robotics, etc.- How perception and action interact with physical representations- How cognitive science and computational neuroscience may inform the design of artificial systems for physical prediction- Methodology for comparing models of infant learning with artificial systems- Development of new datasets or platforms for physics and visual common sense

---

## Smooth Games Optimization and Machine Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Simon Lacoste-Julien · Ioannis Mitliagkas · Gauthier Gidel · Vasilis Syrgkanis · Eva Tardos · Leon Bottou · Sebastian Nowozin*

Overview Advances in generative modeling and adversarial learning gave rise to a recent surge of interest in smooth two-players games, specifically in the context of learning generative adversarial networks (GANs). Solving these games raise intrinsically different challenges than the minimization tasks the machine learning community is used to. The goal of this workshop is to bring together the several communities interested in such smooth games, in order to present what is known on the topic and identify current open questions, such as how to handle the non-convexity appearing in GANs. Background and objectives A number of problems and applications in machine learning are formulated as games. A special class of games, smooth games, have come into the spotlight recently with the advent of GANs. In a two-players smooth game, each player attempts to minimize their differentiable cost function which depends also on the action of the other player. The dynamics of such games are distinct from the better understood dynamics of optimization problems. For example, the Jacobian of gradient descent on a smooth two-player game, can be non-symmetric and have complex eigenvalues. Recent work by ML researchers has identified these dynamics as a key challenge for efficiently solving similar problems. A major hurdle for relevant research in the ML community is the lack of interaction with the mathematical programming and game theory communities where similar problems have been tackled in the past, yielding useful tools. While ML researchers are quite familiar with the convex optimization toolbox from mathematical programming, they are less familiar with the tools for solving games. For example, the extragradient algorithm to solve variational inequalities has been known in the mathematical programming literature for decades, however the ML community has until recently mainly appealed to gradient descent to optimize adversarial objectives. The aim of this workshop is to provide a platform for both theoretical and applied researchers from the ML, mathematical programming and game theory community to discuss the status of our understanding on the interplay between smooth games, their applications in ML, as well existing tools and methods for dealing with them. We also encourage, and will devote time during the workshop, on work that identifies and discusses open, forward-looking problems of interest to the NIPS community. Examples of topics of interest to the workshop are as follow:

Other examples of smooth games in machine learning (e.g. actor-critic models in RL). Standard or

novel algorithms to solve smooth games. Empirical test of algorithms on GAN applications. Existence and unicity results of equilibria in smooth games. Can approximate equilibria have better properties than the exact ones ? [Arora 2017, Lipton and Young 1994]. Variational inequality algorithms [Harker and Pang 1990, Gidel et al. 2018]. Handling stochasticity [Hazan et al. 2017] or non-convexity [Grnarova et al. 2018] in smooth games. Related topics from mathematical programming (e.g. bilevel optimization) [Pfau and Vinyals 2016].

---

## Modeling and decision-making in the spatiotemporal domain

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Ransalu Senanayake · Neal Jean · Fabio Ramos · Girish Chowdhary*

Abstract Understanding the evolution of a process over space and time is fundamental to a variety of disciplines. To name a few, such phenomena that exhibit dynamics in both space and time include propagation of diseases, variations in air pollution, dynamics in fluid flows, and patterns in neural activity. In addition to these fields in which modeling the nonlinear evolution of a process is the focus, there is also an emerging interest in decision-making and controlling of autonomous agents in the spatiotemporal domain. That is, in addition to learning what actions to take, when and where to take actions is crucial for an agent to efficiently and safely operate in dynamic environments. Although various modeling techniques and conventions are used in different application domains, the fundamental principles remain unchanged. Automatically capturing the dependencies between spatial and temporal components, making accurate predictions into the future, quantifying the uncertainty associated with predictions, real-time performance, and working in both big data and data scarce regimes are some of the key aspects that deserve our attention. Establishing connections between Machine Learning and Statistics, this workshop aims at;(1) raising open questions on challenges of spatiotemporal modeling and decision-making,(2) establishing connections among diverse application domains of spatiotemporal modeling, and(3) encouraging conversation between theoreticians and practitioners to develop robust predictive models.Keywords Theory: deep learning/convolutional LSTM, kernel methods, chaos theory, reinforcement learning for dynamic environments, dynamic policy learning, biostatistics, epidemiology, geostatistcs, climatology, neuroscience, etc. Applications: Natural phenomena: disease propagation and outbreaks, environmental monitoring, climate modeling, etc. Social and economics: predictive policing, population mapping, poverty mapping, food resources, agriculture, etc. Engineering/robotics: active data collection, traffic modeling, motion prediction, fluid dynamics, spatiotemporal prediction for safe autonomous driving, etc. Web: https://sites.google.com/site/nips18spatiotemporal/

---

# Continual Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Razvan Pascanu · Yee Teh · Marc Pickett · Mark Ring*

Continual learning (CL) is the ability of a model to learn continually from a stream of data, building on what was learnt previously, hence exhibiting positive transfer, as well as being able to remember previously seen tasks. CL is a fundamental step towards artificial intelligence, as it allows the agent to adapt to a continuously changing environment, a hallmark of natural intelligence. It also has implications for supervised or unsupervised learning. For example, when the dataset is not properly shuffled or there exists a drift in the input distribution, the model overfits the recently seen data, forgetting the rest -- phenomena referred to as catastrophic forgetting, which is part of CL and is something CL systems aim to address.Continual learning is defined in practice through a series of desiderata. A non-complete lists includes: * Online learning -- learning occurs at every moment, with no fixed tasks or data sets and no clear boundaries between tasks; * Presence of transfer (forward/backward) -- the model should be able to transfer from previously seen data or tasks to new ones, as well as possibly new task should help improve performance on older ones; * Resistance to catastrophic forgetting -- new learning does not destroy performance on previously seen data; * Bounded system size -- the model capacity should be fixed, forcing the system use its capacity intelligently as well as gracefully forgetting information such to ensure maximising future reward; * No direct access to previous experience -- while the model can remember a limited amount of experience, a continual learning algorithm should not have direct access to past tasks or be able to rewind the environment;In the previous edition of the workshop the focus has been on defining a complete list of desiderata, of what a continual learning (CL) enabled system should be able to do. We believe that in this edition we should further constrain the discussion with a focus on how to evaluate CL and how it relates to other existing topics (e.g. life-long learning, transfer learning, meta-learning) and how ideas from these topics could be useful for continual learning.Different aspects of continual learning are in opposition of each other (e.g. fixed model capacity and not-forgetting), which also raises the question of how to evaluate continual learning systems. One one hand, what are the right trade-offs between these different opposing forces? How do we compare existing algorithms given these different dimensions along which we should evaluate them (e.g. forgetting, positive transfer)? What are the right metrics we should report? On the other hand, optimal or meaningful trade-offs will be tightly defined by the data or at least type of tasks we use to test the algorithms. One prevalent task used by many recent papers is PermutedMNIST. But as MNIST is not a reliable dataset for classification, so PermutedMNIST might be extremely misleading for continual learning. What would be the right benchmarks, datasets or tasks for fruitfully exploiting this topic?Finally, we will also encourage presentation of both novel approaches to CL and implemented systems, which will help concretize the discussion of what CL is and how to evaluate CL systems.

---

# NIPS 2018 workshop on Compact Deep Neural Networks with industrial applications

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Lixin Fan · Zhouchen Lin · Max Welling · Yurong Chen · Werner Bailer*

This workshop aims to bring together researchers, educators, practitioners who are interested in techniques as well as applications of making compact and efficient neural network representations. One main theme of the workshop discussion is to build up consensus in this rapidly developed field, and in particular, to establish close connection between researchers in Machine Learning community and engineers in industry. We believe the workshop is beneficial to both academic researchers as well as industrial practitioners. ===News and announcements: For authors of following accepted papers, please revise your submission as per reviewers comments to address raised issues. If there are too much contents to be included in 3 page limit, you may use appendix for supporting contents such as proofs or detailed experimental results. The camera ready abstract should be prepared with authors information (name, email address, affiliation) using the NIPS camera ready template. Please submit the camera ready abstract through OpenReview (https://openreview.net/group?id=NIPS.cc/2018/Workshop/CDNNRIA) by Nov. 12th. Use your previous submission page to update the abstract. In case you have to postpone the submission, please inform us immeidately. Otherwise, the abstract will be removed from the workshop schedule. ===We invite you to submit original work in, but not limited to, following areas:Neural network compression techniques:. Binarization, quantization, pruning, thresholding and coding of neural networks. Efficient computation and acceleration of deep convolutional neural networks. Deep neural network computation in low power consumption applications (e.g., mobile or IoT devices) . Differentiable sparsification and quantization of deep neural networks. Benchmarking of deep neural network compression techniquesNeural network representation and exchange:. Exchange formats for (trained) neural networks. Efficient deployment strategies for neural networks. Industrial standardization of deep neural network representations. Performance evaluation methods of compressed networks in application context (e.g., multimedia encoding and processing)Video & media compression methods using DNNs such as those developed in MPEG group:. To improve video coding standard development by using deep neural networks . To increase practical applicability of network compression methodsAn extended abstract (3 pages long using NIPS style, see https://nips.cc/Conferences/2018/PaperInformation/StyleFiles ) in PDF format should be submitted for evaluation of the originality and quality of the work. The evaluation is double-blind and the abstract must be anonymous. References may extend beyond the 3 page limit, and parallel submissions to a journal or conferences (e.g. AAAI or ICLR) are permitted. Submissions will be accepted as contributed talks (oral) or poster presentations. Extended abstract should be submitted through OpenReview (https://openreview.net/group?id=NIPS.cc/2018/Workshop/CDNNRIA) by 20 Oct 2018.  All accepted abstracts will be posted on the workshop website and archived.  Selection policy: all submitted abstracts will be evaluted based on their novelty, soundness and impacts. At the workshop we encourage DISCUSSION about NEW IDEAS, each submitter is thus expected to actively respond on OpenReview webpage and answer any questions about his/her ideas. The

willingness to respond in OpenReview Q/A disucssions will be an important factor for the selection of accepted oral or poster presentations. Important dates: . Extended abstract submission deadline: 20 Oct 2018, . Acceptance notification: 29 Oct. 2018, . Camera ready submission: 12 November 2018, . Workshop: 7 December 2018Submission: Please submit your extended abstract through OpenReivew system (https://openreview.net/group?id=NIPS.cc/2018/Workshop/CDNNRIA). For prospective authors: please send author information to workshop chairs (lixin.fan@nokia.com), so that you submission can be assigned to reviewers without conflict of interests. . Reviewers comments will be released by Oct. 24th, then authors have to reply by Oct. 27th, which leaving us two days for decision-making. . It is highly recommended for authors submit abstracts early, in case you need more time to address reviewers' comments. NIPS Complimentary workshop registrationWe will help authors of accepted submissions to get access to a reserve pool of NIPS tickets. So please register to the workshop early.===Accepted papers & authors: 1. Minimal Random Code Learning: Getting Bits Back from Compressed Model Parameters, Marton Havasi, Robert Peharz, José Miguel Hernández-Lobato2. Neural Network Compression using Transform Coding and Clustering, Thorsten Laude, Jörn Ostermann3. Pruning neural networks: is it time to nip it in the bud?, Elliot J. Crowley, Jack Turner, Amos Storkey, Michael O'Boyle4. Compressing Recurrent Neural Networks with Tensor Ring for Action Recognition, Yu Pan, Jing Xu, Maolin Wang, Fei Wang, Kun Bai, Zenglin Xu5. Efficient Inference on Deep Neural Networks by Dynamic Representations and Decision Gates, Mohammad Saeed Shafiee, Mohammad Javad Shafiee, Alexander Wong6. Iteratively Training Look-Up Tables for Network Quantization, Fabien Cardinaux, Stefan Uhlich, Kazuki Yoshiyama, Javier Alonso García, Stephen Tiedemann, Thomas Kemp, Akira Nakamura7. Hybrid Pruning: Thinner Sparse Networks for Fast Inference on Edge Devices, Xiaofan Xu, Mi Sun Park, Cormac Brick8. Compression of Acoustic Event Detection Models with Low-rank Matrix Factorization and Quantization Training, Bowen Shi, Ming Sun, Chieh-Chi Kao, Viktor Rozgic, Spyros Matsoukas, Chao Wang9. On Learning Wire-Length Efficient Neural Networks, Christopher Blake, Luyu Wang, Giuseppe Castiglione, Christopher Srinavasa, Marcus Brubaker10. FLOPs as a Direct Optimization Objective for Learning Sparse Neural Networks, Raphael Tang, Ashutosh Adhikari, Jimmy Lin11. Three Dimensional Convolutional Neural Network Pruning with Regularization-Based Method, Yuxin Zhang, Huan Wang, Yang Luo, Roland Hu12. Differentiable Training for Hardware Efficient LightNNs, Ruizhou Ding, Zeye Liu, Ting-Wu Chin, Diana Marculescu, R.D. (Shawn) Blanton13. Structured Pruning for Efficient ConvNets via Incremental Regularization, Huan Wang, Qiming Zhang, Yuehai Wang, Haoji Hu14. Block-wise Intermediate Representation Training for Model Compression, Animesh Koratana, Daniel Kang, Peter Bailis, Matei Zahaira15. Targeted Dropout, Aidan N. Gomez, Ivan Zhang, Kevin Swersky, Yarin Gal, Geoffrey E. Hinton16. Adaptive Mixture of Low-Rank Factorizations for Compact Neural Modeling, Ting Chen, Ji Lin, Tian Lin, Song Han, Chong Wang, Denny Zhou17. Differentiable Fine-grained Quantization for Deep Neural Network Compression, Hsin-Pai Cheng, Yuanjun Huang, Xuyang Guo, Yifei Huang, Feng Yan, Hai Li, Yiran Chen18. Transformer to CNN: Label-scarce distillation for efficient text classification, Yew Ken Chia, Sam Witteveen, Martin Andrews19. EnergyNet: Energy-Efficient Dynamic Inference, Yue Wang, Tan Nguyen, Yang Zhao, Zhangyang Wang, Yingyan Lin, Richard Baraniuk20. Recurrent Convolutions: A Model Compression Point of View, Zhendong Zhang, Cheolkon Jung21, Rethinking the Value of Network Pruning, Zhuang Liu, Mingjie Sun, Tinghui Zhou, Gao Huang, Trevor Darrell22. Linear Backprop in non-linear networks, Mehrdad Yazdani23. Bayesian Sparsification of Gated Recurrent

Neural Networks, Ekaterina Lobacheva, Nadezhda Chirkova, Dmitry Vetrov24. Demystifying Neural Network Filter Pruning, Zhuwei Qin, Fuxun Yu, Chenchen Liu, Xiang Chen25. Learning Compact Networks via Adaptive Network Regularization, Sivaramakrishnan Sankarapandian, Anil Kag, Rachel Manzelli, Brian Kulis26. Pruning at a Glance: A Structured Class-Blind Pruning Technique for Model CompressionAbdullah Salama, Oleksiy Ostapenko, Moin Nabi, Tassilo Klein27. Succinct Source Coding of Deep Neural NetworksSourya Basu, Lav R. Varshney28. Fast On-the-fly Retraining-free Sparsification of Convolutional Neural NetworksAmir H. Ashouri, Tarek Abdelrahman, Alwyn Dos Remedios29. PocketFlow: An Automated Framework for Compressing and Accelerating Deep Neural NetworksJiaxiang Wu, Yao Zhang, Haoli Bai, Huasong Zhong, Jinlong Hou, Wei Liu, Junzhou Huang30. Universal Deep Neural Network CompressionYoojin Choi, Mostafa El-Khamy, Jungwon Lee31. Compact and Computationally Efficient Representations of Deep Neural NetworksSimon Wiedemann, Klaus-Robert Mueller, Wojciech Samek32. Dynamic parameter reallocation improves trainability of deep convolutional networksHesham Mostafa, Xin Wang33. Compact Neural Network Solutions to Laplace's Equation in a Nanofluidic DeviceMartin Magill, Faisal Z. Qureshi, Hendrick W. de Haan34. Distilling Critical Paths in Convolutional Neural NetworksFuxun Yu, Zhuwei Qin, Xiang Chen35. SeCSeq: Semantic Coding for Sequence-to-Sequence based Extreme Multi-label ClassificationWei-Cheng Chang, Hsiang-Fu Yu, Inderjit S. Dhillon, Yiming Yang===A best paper award will be presented to the contribution selected by reviewers, who will also take into account active disucssions on OpenReview. One FREE NIPS ticket will be awarded to the best paper presenter. The best paper award is given to the authors of "Rethinking the Value of Network Pruning", Zhuang Liu, Mingjie Sun, Tinghui Zhou, Gao Huang, Trevor Darrell=====Acknowledgement to reviewersThe workshop organizers gratefully acknowledge the assistance of the following people, who reviewed submissions and actively disucssed with authors: Zhuang Liu, Ting-Wu Chin, Fuxun Yu, Huan Wang, Mehrdad Yazdani, Qigong Sun, Tim Genewein, Abdullah Salama, Anbang Yao, Chen Xu, Hao Li, Jiaxiang Wu, Zhisheng Zhong, Haoji Hu, Hesham Mostafa, Seunghyeon Kim, Xin Wang, Yiwen Guo, Yu Pan, Fereshteh Lagzi, Martin Magill, Wei-Cheng Chang, Yue Wang, Caglar Aytekin, Hannes Fassold, Martin Winter, Yunhe Wang, Faisal Qureshi, Filip Korzeniowski, jianguo Li, Jiashi Feng, Mingjie Sun, Shiqi Wang, Tinghuai Wang, Xiangyu Zhang, Yibo Yang, Ziqian Chen, Francesco Cricri, Jan Schlüter, Jing Xu, Lingyu Duan, Maoin Wang, Naiyan Wang, Stephen Tyree, Tianshui Chen, Vasileios Mezaris, Christopher Blake, Chris Srinivasa, Giuseppe Castiglione, Amir Khoshamam, Kevin Luk, Luyu Wang, Jian Cheng, Pavlo Molchanov, Yihui He, Sam Witteveen, Peng Wang,with special thanks to Ting-Wu Chin who contributed 7 reviewer comments. =====Workshop schedule on December 7th, 2018:

---

## Machine Learning for Geophysical & Geochemical Signals

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Laura Pyrak-Nolte · James R Rustad · Richard Baraniuk*

MotivationThe interpretation of Earth's subsurface evolution from full waveform analysis requires a method to identify the key signal components related to the evolution in physical properties from

changes in stress, fluids, geochemical interactions and other natural and anthropogenic processes. The analysis of seismic waves and other geophysical/geochemical signals remains for the most part a tedious task that geoscientists may perform by visual inspection of the available seismograms. The complexity and noisy nature of a broad array of geoscience signals combined with sparse and irregular sampling make this analysis difficult and imprecise. In addition, many signal components are ignored in tomographic imaging and continuous signal analysis that may prevent discovery of previously unrevealed signals that may point to new physics. Ideally a detailed interpretation of the geometric contents of these data sets would provide valuable prior information for the solution of corresponding inverse problems. This unsatisfactory state of affairs is indicative of a lack of effective and robust algorithms for the computational parsing and interpretation of seismograms (and other geoscience data sets). Indeed, the limited frequency content, strong nonlinearity, temporally scattered nature of these signals make their analysis with standard signal processing techniques difficult and insufficient. Once important seismic phases are identified, the next challenge is determining the link between a remotely-measured geophysical response and a characteristic property (or properties) of the fractures and fracture system. While a strong laboratory-based foundation has established a link between the mechanical properties of simple fracture systems (i.e. single fractures, parallel sets of fractures) and elastic wave scattering, bridging to the field scale faces additional complexity and a range of length scales that cannot be achieved from laboratory insight alone. This fundamental knowledge gap at the critical scale for long-term monitoring and risk assessment can only be narrowed or closed with the development of appropriate mathematical and numerical representations at each scale and across scales using multiphysics models that traverse spatial and temporal scales.TopicMajor breakthroughs in bridging the knowledge gaps in geophysical sensing are anticipated as more researchers turn to machine learning (ML) techniques; however, owing to the inherent complexity of machine learning methods, they are prone to misapplication, may produce uninterpretable models, and are often insufficiently documented. This combination of attributes hinders both reliable assessment of model validity and consistent interpretation of model outputs. By providing documented datasets and challenging teams to apply fully documented workflows for ML approaches, we expect to accelerate progress in the application of data science to longstanding research issues in geophysics. The goals of this workshop are to: (1) bring together experts from different fields of ML and geophysics to explore the use of ML techniques related to the identification of the physics contained in geophysical and chemical signals, as well as from images of geologic materials (minerals, fracture patterns, etc.); and (2) announce a set of geophysics machine learning challenges to the community that address earthquake detection and the physics of rupture and the timing of earthquakes.Target AudienceWe aim to elicit new connections among these diverse fields, identify novel tools and models that can be transferred from one to the other, and explore novel ML applications that will benefit from ML algorithms paradigm. We believe that a successful workshop will lead to new research directions in a variety of areas and will also inspire the development of novel theories and tools.

# Visually grounded interaction and language

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Florian Strub · Harm de Vries · Erik T Wijmans · Samyak Datta · Ethan Perez · Mateusz Malinowski · Stefan Lee · Peter Anderson · Aaron Courville · Jeremie MARY · Dhruv Batra · Devi Parikh · Olivier Pietquin · Chiori HORI · Tim Marks · Anoop Cherian*

The dominant paradigm in modern natural language understanding is learning statistical language models from text-only corpora. This approach is founded on a distributional notion of semantics, i.e. that the "meaning" of a word is based only on its relationship to other words. While effective for many applications, methods in this family suffer from limited semantic understanding, as they miss learning from the multimodal and interactive environment in which communication often takes place - the symbols of language thus are not grounded in anything concrete. The symbol grounding problem first highlighted this limitation, that “meaningless symbols (i.e.) words cannot be grounded in anything but other meaningless symbols” [18].On the other hand, humans acquire language by communicating about and interacting within a rich, perceptual environment. This behavior provides the necessary grounding for symbols, i.e. to concrete objects or concepts (i.e. physical or psychological). Thus, recent work has aimed to bridge vision, interactive learning, and natural language understanding through language learning tasks based on natural images (ReferIt [1], GuessWhat?! [2], Visual Question Answering [3,4,5,6], Visual Dialog [7], Captioning [8]) or through embodied agents performing interactive tasks [13,14,17,22,23,24,26] in physically simulated environments (DeepMind Lab [9], Baidu XWorld [10], OpenAI Universe [11], House3D [20], Matterport3D [21], GIBSON [24], MINOS [25], AI2-THOR [19], StreetLearn [17]), often drawing on the recent successes of deep learning and reinforcement learning. We believe this line of research poses a promising, long-term solution to the grounding problem faced by current, popular language understanding models.While machine learning research exploring visually-grounded language learning may be in its earlier stages, it may be possible to draw insights from the rich research literature on human language acquisition. In neuroscience, recent progress in fMRI technology has enabled to better understand the interleave between language, vision and other modalities [15,16] suggesting that the brains shares neural representation of concepts across vision and language. Differently, developmental cognitive scientists have also argued that children acquiring various words is closely linked to them learning the underlying concept in the real world [12].This workshop thus aims to gather people from various backgrounds - machine learning, computer vision, natural language processing, neuroscience, cognitive science, psychology, and philosophy - to share and debate their perspectives on why grounding may (or may not) be important in building machines that truly understand natural language.We invite you to submit papers related to the following topics:- language acquisition or learning through interactions- visual captioning, dialog, and question-answering- reasoning in language and vision- visual synthesis from language- transfer learning in language and vision tasks- navigation in virtual worlds via natural-language instructions or multi-agent communication- machine translation with visual cues- novel tasks that combine language, vision and actions- modeling of natural language and visual stimuli representations in the human brain- position papers on grounded language learning- audio visual scene-aware dialog- audio-visual fusion Submissions should be up to 4 pages excluding references, acknowledgements,

and supplementary material, and should be NIPS format and anonymous. The review process is double-blind.We also welcome published papers that are within the scope of the workshop (without re-formatting). This specific papers do not have to be anonymous. They are not eligible for oral session and will only have a very light review process.Please submit your paper to the following address: https://cmt3.research.microsoft.com/VIGIL2018 Accepted workshop papers are eligible to the pool of reserved conference tickets (one ticket per accepted papers).If you have any question, send an email to: vigilworkshop2018@gmail.com[1] Sahar Kazemzadeh et al. "ReferItGame: Referring to Objects in Photographs of Natural Scenes." EMNLP, 2014.[2] Harm de Vries et al. "GuessWhat?! Visual object discovery through multi-modal dialogue." CVPR, 2017.[3] Stanislaw Antol et al. "Vqa: Visual question answering." ICCV, 2015.[4] Mateusz Malinowski et al. “Ask Your Neurons: A Neural-based Approach to Answering Questions about Images.” ICCV, 2015.[5] Mateusz Malinowski et al. “A Multi-World Approach to Question Answering about Real-World Scenes based on Uncertain Input.” NIPS, 2014.[6] Geman Donald, et al. “Visual Turing test for computer vision systems.” PNAS, 2015.[7] Abhishek Das et al. "Visual dialog." CVPR, 2017.[8] Anna Rohrbach et al. “Generating Descriptions with Grounded and Co-Referenced People.” CVPR, 2017.[9] Charles Beattie et al. Deepmind lab. arXiv, 2016.[10] Haonan Yu et al. “Guided Feature Transformation (GFT): A Neural Language Grounding Module for Embodied Agents.” arXiv, 2018.[11] Openai universe. https://universe.openai.com, 2016.[12] Alison Gopnik et al. “Semantic and cognitive development in 15- to 21-month-old children.” Journal of Child Language, 1984.[13] Abhishek Das et al. "Learning Cooperative Visual Dialog Agents with Deep Reinforcement Learning." ICCV, 2017.[14] Karl Moritz Hermann et al. "Grounded Language Learning in a Simulated 3D World." arXiv, 2017.[15] Alexander G. Huth et al. "Natural speech reveals the semantic maps that tile human cerebral cortex." Nature, 2016.[16] Alexander G. Huth, et al. "Decoding the semantic content of natural movies from human brain activity." Frontiers in systems neuroscience, 2016.[17] Piotr Mirowski et al. “Learning to Navigate in Cities Without a Map.” arXiv, 2018.[18] Stevan Harnad. “The symbol grounding problem.” CNLS, 1989.[19] E Kolve, R Mottaghi, D Gordon, Y Zhu, A Gupta, A Farhadi. “AI2-THOR: An Interactive 3D Environment for Visual AI.” arXiv, 2017.[20] Yi Wu et al. “House3D: A Rich and Realistic 3D Environment.” arXiv, 2017.[21] Angel Chang et al. “Matterport3D: Learning from RGB-D Data in Indoor Environments.” arXiv, 2017.[22] Abhishek Das et al. “Embodied Question Answering.” CVPR, 2018.[23] Peter Anderson et al. “Vision-and-Language Navigation: Interpreting visually-grounded navigation instructions in real environments.” CVPR, 2018.[24] Fei Xia et al. “Gibson Env: Real-World Perception for Embodied Agents.” CVPR, 2018.[25] Manolis Savva et al. “MINOS: Multimodal indoor simulator for navigation in complex environments.” arXiv, 2017.[26] Daniel Gordon, Aniruddha Kembhavi, Mohammad Rastegari, Joseph Redmon, Dieter Fox, Ali Farhadi. “IQA: Visual Question Answering in Interactive Environments.” CVPR, 2018.

---

## Critiquing and Correcting Trends in Machine Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @**

*Tom Rainforth · Matt Kusner · Benjamin Bloem-Reddy · Brooks Paige · Rich Caruana · Yee Whye Teh*

Workshop Webpage: https://ml-critique-correct.github.io/ Recently there have been calls to make machine learning more reproducible, less hand-tailored, fair, and generally more thoughtful about how research is conducted and put into practice. These are hallmarks of a mature scientific field and will be crucial for machine learning to have the wide-ranging, positive impact it is expected to have. Without careful consideration, we as a field risk inflating expectations beyond what is possible. To address this, this workshop aims to better understand and to improve all stages of the research process in machine learning. A number of recent papers have carefully considered trends in machine learning as well as the needs of the field when used in real-world scenarios [1-18]. Each of these works introspectively analyzes what we often take for granted as a field. Further, many propose solutions for moving forward. The goal of this workshop is to bring together researchers from all subfields of machine learning to highlight open problems and widespread dubious practices in the field, and crucially, to propose solutions. We hope to highlight issues and propose solutions in areas such as:
- Common practices [1, 8] - Implicit technical and empirical assumptions that go unquestioned [2, 3, 5, 7, 11, 12, 13, 17, 18] - Shortfalls in publication and reviewing setups [15, 16] - Disconnects between research focus and application requirements [9, 10, 14] - Surprising observations that make us rethink our research priorities [4, 6] The workshop program is a collection of invited talks, alongside contributed posters and talks. For some of these talks, we plan a unique open format of 10 minutes of talk + 10 minutes of follow up discussion. Additionally, a separate panel discussion will collect researchers with a diverse set of viewpoints on the current challenges and potential solutions. During the panel, we will also open the conversation to the audience. The discussion will further be open to an online Q&A which will be solicited prior to the workshop. A key expected outcome of the workshop is a collection of important open problems at all levels of machine learning research, along with a record of various bad practices that we should no longer consider to be acceptable. Further, we hope that the workshop will make inroads in how to address these problems, highlighting promising new frontiers for making machine learning practical, robust, reproducible, and fair when applied to real-world problems.

Call for Papers: Deadline: October 30rd, 2018, 11.59pm UTC The one day NIPS 2018 Workshop: Critiquing and Correcting Trends in Machine Learning calls for papers that critically examine current common practices and/or trends in methodology, datasets, empirical standards, publication models, or any other aspect of machine learning research. Though we are happy to receive papers that bring attention to problems for which there is no clear immediate remedy, we particularly encourage papers which propose a solution or indicate a way forward. Papers should motivate their arguments by describing gaps in the field. Crucially, this is not a venue for settling scores or character attacks, but for moving machine learning forward as a scientific discipline. To help guide submissions, we have split up the call for papers into the follows tracks. Please indicate the intended track when making your submission. Papers are welcome from all subfields of machine learning. If you have a paper which you feel falls within the remit of the workshop but does not clearly fit one of these tracks, please contact the organizers at: ml.critique.correct@gmail.com. Bad Practices (1-4 pages) Papers that highlight common bad practices or unjustified assumptions at any stage of the research process. These can either be technical shortfalls in a particular machine learning subfield, or more procedural bad practices of the ilk of those discussed in [17]. When possible, papers should

also try to highlight work which does not fall foul of these bad practices, as examples of how they can be avoided. Flawed Intuitions or Unjustified Assumptions (3-4 pages) Papers that call into question commonly held intuitions or provide clear evidence either for or against assumptions that are regularly taken for granted without proper justification. For example, we would like to see papers which provide empirical assessments to test out metrics, verify intuitions, or compare popular current approaches with historic baselines that may have unfairly fallen out of favour (see e.g. [2]). Such submissions are encouraged regardless of whether these assessments ultimately result in positive or negative results. We would also like to see work which provides results which makes us rethink our intuitions or the assumptions we typically make. Negative Results (3-4 pages) Papers which show failure modes of existing algorithms or suggest new approaches which one might expect to perform well but which do not. The aim of the latter of these is to provide a venue for work which might otherwise go unpublished but which is still of interest to the community, for example by dissuading other researchers from similar ultimately unsuccessful approaches. Though it is inevitably preferable that papers are able to explain why the approach performs poorly, this is not essential if the paper is able to demonstrate why the negative result is of interest to the community in its own right. Research Process (1-4 pages) Papers which provide carefully thought through critiques, provide discussion on, or suggest new approaches to areas such as the conference model, the reviewing process, the role of industry in research, open sourcing of code and data, institutional biases and discrimination in the field, research ethics, reproducibility standards, and allocation of conference tickets. Debates (1-2 pages) Short proposition papers which discuss issues either affecting all of machine learning or significantly sized subfields (e.g. reinforcement learning, Bayesian methods, etc). Selected papers will be used as the basis for instigating online forum debates before the workshop, leading up to live discussions on the day itself. Open Problems (1-4 papers/short talks) Papers that describe either (a) unresolved questions in existing fields that need to be addressed, (b) desirable operating characteristics for ML in particular application areas that have yet to be achieved, or (c) new frontiers of machine learning research that require rethinking current practices (e.g., error diagnosis for when many ML components are interoperating within a system, automating dataset collection/creation). Submission Instructions Papers should be submitted as pdfs using the NIPS LaTeX style file. Author names should be anonymized. Page limits do not include references. Appendices may be included after the references, but reviewers are not obliged to read them. All accepted papers will be made available through the workshop website and presented as a poster. Selected papers will also be given contributed talks. We are able to add a moderate number of accepted paper authors to the pool of reserved tickets. In the event that the number of accepted papers exceeds our reserved ticket allocation, assignments to the reserved ticket pool will be allocated based on review scores. We further have a small number of complimentary workshop registrations that will be handed out to selected papers. If any authors are unable to attend the workshop due visa, ticketing, or funding issues, they will be allowed to provide a video presentation for their work that will be made available through the workshop website in lieu of a poster presentation. Please submit papers here: https://easychair.org/conferences/?conf=cract2018 Deadline: October 30rd, 2018, 11:59 UTCReferences[1] Mania, H., Guy, A., & Recht, B. (2018). Simple random search provides a competitive approach to reinforcement learning. arXiv preprint arXiv:1803.07055.[2] Rainforth, T., Kosiorek, A. R., Le, T. A., Maddison, C. J., Igl, M., Wood, F., & Teh, Y. W. (2018). Tighter variational

bounds are not necessarily better. ICML.[3] Torralba, A., & Efros, A. A. (2011). Unbiased look at dataset bias. In Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on (pp. 1521-1528). IEEE.[4] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199.[5] Mescheder, L., Geiger, A., Nowozin S. (2018) Which Training Methods for GANs do actually Converge? ICML[6] Daumé III, H. (2009). Frustratingly easy domain adaptation. arXiv preprint arXiv:0907.1815[7] Urban, G., Geras, K. J., Kahou, S. E., Wang, O. A. S., Caruana, R., Mohamed, A., ... & Richardson, M. (2016). Do deep convolutional nets really need to be deep (or even convolutional)?.[8] Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., & Meger, D. (2017). Deep reinforcement learning that matters. arXiv preprint arXiv:1709.06560.[9] Narayanan, M., Chen, E., He, J., Kim, B., Gershman, S., & Doshi-Velez, F. (2018). How do Humans Understand Explanations from Machine Learning Systems? An Evaluation of the Human-Interpretability of Explanation. arXiv preprint arXiv:1802.00682.[10] Schulam, S., Saria S. (2017). Reliable Decision Support using Counterfactual Models. NIPS.[11] Rahimi, A. (2017). Let's take machine learning from alchemy to electricity. Test-of-time award presentation, NIPS. [12] Lucic, M., Kurach, K., Michalski, M., Gelly, S., Bousquet, O. (2018). Are GANs Created Equal? A Large-Scale Study. arXiv preprint arXiv:1711.10337.[13] Le, T.A., Kosiorek, A.R., Siddharth, N., Teh, Y.W. and Wood, F., (2018). Revisiting Reweighted Wake-Sleep. arXiv preprint arXiv:1805.10469.[14] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J. and Mané, D., (2016). Concrete problems in AI safety. arXiv preprint arXiv:1606.06565.[15] Sutton, C. (2018) Making unblinding manageable: Towards reconciling prepublication and double-blind review. http://www.theexclusive.org/2017/09/arxiv-double-blind.html[16] Langford, J. (2018) ICML Board and Reviewer profiles. http://hunch.net/?p=8962378

---

## Deep Reinforcement Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Pieter Abbeel · David Silver · Satinder Singh · Joelle Pineau · Joshua Achiam · Rein Houthooft · Aravind Srinivas*

In recent years, the use of deep neural networks as function approximators has enabled researchers to extend reinforcement learning techniques to solve increasingly complex control tasks. The emerging field of deep reinforcement learning has led to remarkable empirical results in rich and varied domains like robotics, strategy games, and multiagent interaction. This workshop will bring together researchers working at the intersection of deep learning and reinforcement learning, and it will help interested researchers outside of the field gain a high-level view about the current state of the art and potential directions for future contributions.

---

# All of Bayesian Nonparametrics (Especially the Useful Bits)

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Diana Cai · Trevor Campbell · Michael Hughes · Tamara Broderick · Nick Foti · Sinead A Williamson*

Bayesian nonparametric (BNP) methods are well suited to the large data sets that arise in a wide variety of applied fields. By making use of infinite-dimensional mathematical structures, BNP methods allow the complexity of a learned model to grow as the size of a data set grows, exhibiting desirable Bayesian regularization properties for small data sets and allowing the practitioner to learn ever more from larger data sets. These properties have resulted in the adoption of BNP methods across a diverse set of application areas---including, but not limited to, biology, neuroscience, the humanities, social sciences, economics, and finance.This workshop aims to highlight recent advances in modeling and computation through the lens of applied, domain-driven problems that require the infinite flexibility and interpretability of BNP. In this workshop, we will explore new BNP methods for diverse applied problems, including cutting-edge models being developed by application domain experts. We will also discuss the limitations of existing methods and discuss key problems that need to be solved. A major focus of the workshop will be to expose participants to practical software tools for performing Bayesian nonparametric analyses. In particular, we plan to host hands-on tutorials to introduce workshop participants to some of the software packages that can be used to easily perform posterior inference for BNP models. On the software panel, we will have researchers who have experience with BNP and development experience with popular software systems, such as TensorFlow, Edward, Stan, and Autograd. We expect workshop participants to come from a variety of fields, including but not limited to machine learning, statistics, engineering, the social sciences, and biological sciences. The workshop will be relevant both to BNP experts as well as those interested in learning how to apply BNP models. There will be a special emphasis on novel application areas and computational developments that make BNP more accessible to the broader machine learning audience. Participants will leave the workshop with (i) exposure to recent advances in the field, (ii) hands-on experience with software implementing BNP methods, and (iii) an idea of the current major challenges in the field. These goals will be accomplished through a series of invited and contributed talks, a poster session, and at least one hands-on tutorial session where participants can get their hands dirty with BNP methods.This workshop builds off of:1. NIPS 2015: “Bayesian Nonparametrics: The Next Generation”: https://sites.google.com/site/nipsbnp2015/, and2. NIPS 2016: “Practical Bayesian Nonparametrics”: https://sites.google.com/site/nipsbnp2016/, which have spanned various areas of BNP, such as theory, applications and computation. This year’s workshop will have a fresh take on recent developments in BNP in connection to the broader range of research in statistics, machine learning, and application domains. The 2018 workshop has received an endorsement from the International Society of Bayesian Analysis (ISBA) and sponsorship from Google.Organizing Committee:Diana Cai (Princeton) Trevor Campbell (MIT/UBC)Mike Hughes (Harvard/Tufts)Tamara Broderick (MIT)Nick Foti (U Washington)Sinead Williamson (UT Austin)Advisory Committee:Emily Fox (U Washington)Antonio Lijoi (Bocconi U) Sonia Petrone (Bocconi U) Igor Prünster (Bocconi U)Erik Sudderth (UC Irvine)

## MLSys: Workshop on Systems for ML and Open Source Software

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Aparna Lakshmiratan · Sarah Bird · Siddhartha Sen · Joseph Gonzalez · Daniel Crankshaw*

This workshop is part two of a two-part series with one day focusing on ML for Systems and the other on Systems for ML. Although the two workshops are being led by different organizers, we are coordinating our call for papers to ensure that the workshops complement each other and that submitted papers are routed to the appropriate venue. The ML for Systems workshop focuses on developing ML to optimize systems while we focus on designing systems to enable large scale ML with Systems for ML. Both fields are mature enough to warrant a dedicated workshop. Organizers on both sides are open to merging in the future, but this year we plan to run them separately on two different days.A new area is emerging at the intersection of artificial intelligence, machine learning, and systems design. This has been accelerated by the explosive growth of diverse applications of ML in production, the continued growth in data volume, and the complexity of large-scale learning systems. The goal of this workshop is to bring together experts working at the crossroads of machine learning, system design and software engineering to explore the challenges faced when building large-scale ML systems. In particular, we aim to elicit new connections among these diverse fields, identifying theory, tools and design principles tailored to practical machine learning workflows. We also want to think about best practices for research in this area and how to evaluate it. The workshop will cover state of the art ML and AI platforms and algorithm toolkits (e.g. TensorFlow, PyTorch1.0, MXNet etc.), as well as dive into machine learning-focused developments in distributed learning platforms, programming languages, data structures, GPU processing, and other topics.This workshop will follow the successful model we have previously run at ICML, NIPS and SOSP 2017.Our plan is to run this workshop annually co-located with one ML venue and one Systems venue, to help build a strong community which we think will complement newer conferences like SysML targeting research at the intersection of systems and machine learning. We believe this dual approach will help to create a low barrier to participation for both communities.

---

## NIPS 2018 Competition Track Day 1

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @**

*Sergio Escalera · Ralf Herbrich*

NIPS 2018 Competitions, day 1: Regular data-driven NIPS competitions

## The second Conversational AI workshop – today's practice and tomorrow's potential

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Alborz Geramifard · Jason D. Williams · Larry Heck · James Glass · Milica Gasic · Dilek Hakkani-Tur · Steve Young · Lazaros C. Polymenakos · Y-Lan Boureau · Maxine Eskenazi*

In the span of only a few years, conversational systems have become commonplace. Every day, millions of people use natural-language interfaces such as Siri, Google Now, Cortana, Alexa and others via in-home devices, phones, or messaging channels such as Messenger, Slack, Skype, among others. At the same time, interest among the research community in conversational systems has blossomed: for supervised and reinforcement learning, conversational systems often serve as both a benchmark task and an inspiration for new ML methods at conferences which don't focus on speech and language per se, such as NIPS, ICML, IJCAI, and others. Research community challenge tasks are proliferating, including the seventh Dialog Systems Technology Challenge (DSTC7), the Amazon Alexa prize, and the Conversational Intelligence Challenge live competitions at NIPS (2017, 2018).Following the overwhelming participation in our last year NIPS workshop (9 invited talks, 26 submissions, 3 orals papers, 13 accepted papers, 37 PC members, and couple of hundreds of participants), we are excited to continue promoting cross-pollination of ideas between academic research centers and industry. The goal of this workshop is to bring together researchers and practitioners in this area, to clarify impactful research problems, share findings from large-scale real-world deployments, and generate new ideas for future lines of research. This workshop will include invited talks from academia and industry, contributed work, and open discussion. In these talks, senior technical leaders from many of the most popular conversational services will give insights into real usage and challenges at scale. An open call for papers will be issued, and we will prioritize forward-looking papers that propose interesting and impactful contributions. We will end the day with an open discussion, including a panel consisting of academic and industrial researchers.

---

## 2nd Workshop on Machine Learning on the Phone and other Consumer Devices (MLPCD 2)

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Sujith Ravi · Wei Chai · Yangqing Jia · Hrishikesh Aradhye · Prateek Jain*

The 2nd Workshop on Machine Learning on the Phone and other Consumer Devices (MLPCD 2) aims to continue the success of the 1st MLPCD workshop held at NIPS 2017 in Long Beach, CA.Previously, the first MLPCD workshop edition, held at NIPS 2017 was successful, attracted over 200+ attendees and led to active research & panel discussions as well as follow-up contributions to the open-source community (e.g., release of new inference libraries, tools, models and standardized

representations of deep learning models). We believe that interest in this space is only going to increase, and we hope that the workshop plays the role of an influential catalyst to foster research and collaboration in this nascent community.After the first workshop where we investigated initial directions and trends, the NIPS 2018 MLPCD workshop focuses on theory and practical applications of on-device machine learning, an area that is highly relevant and specializes in the intersection of multiple topics of interest to NIPS and broader machine learning community -- efficient training & inference for deep learning and other machine learning models; interdisciplinary mobile applications involving vision, language & speech understanding; and emerging topics like Internet of Things.We plan to incorporate several new additions this year -- inspirational opening Keynote talk on "future of intelligent assistive & wearable experiences"; two panels including a lively closing panel debate discussing pros/cons of two key ML computing paradigms (Cloud vs. On-device); solicited research papers on new & recent hot topics (e.g., theoretical & algorithmic work on low-precision models, compression, sparsity, etc. for training and inference), related challenges, applications and recent trends; demo session showcasing ML in action for real-world apps.Description & Topics:Deep learning and machine learning, in general, has changed the computing paradigm. Products of today are built with machine intelligence as a central attribute, and consumers are beginning to expect near-human interaction with the appliances they use. However, much of the Deep Learning revolution has been limited to the cloud, enabled by popular toolkits such as Caffe, TensorFlow, and MxNet, and by specialized hardware such as TPUs. In comparison, mobile devices until recently were just not fast enough, there were limited developer tools, and there were limited use cases that required on-device machine learning. That has recently started to change, with the advances in real-time computer vision and spoken language understanding driving real innovation in intelligent mobile applications. Several mobile-optimized neural network libraries were recently announced (CoreML, Caffe2 for mobile, TensorFlow Lite), which aim to dramatically reduce the barrier to entry for mobile machine learning. Innovation and competition at the silicon layer has enabled new possibilities for hardware acceleration. To make things even better, mobile-optimized versions of several state-of-the-art benchmark models were recently open sourced. Widespread increase in availability of connected “smart” appliances for consumers and IoT platforms for industrial use cases means that there is an ever-expanding surface area for mobile intelligence and ambient devices in homes. All of these advances in combination imply that we are likely at the cusp of a rapid increase in research interest in on-device machine learning, and in particular, on-device neural computing.Significant research challenges remain, however. Mobile devices are even more personal than “personal computers” were. Enabling machine learning while simultaneously preserving user trust requires ongoing advances in the research of differential privacy and federated learning techniques. On-device ML has to keep model size and power usage low while simultaneously optimizing for accuracy. There are a few exciting novel approaches recently developed in mobile optimization of neural networks. Lastly, the newly prevalent use of camera and voice as interaction models has fueled exciting research towards neural techniques for image and speech/language understanding. This is an area that is highly relevant to multiple topics of interest to NIPS -- e.g., core topics like machine learning & efficient inference and interdisciplinary applications involving vision, language & speech understanding as well as emerging area (namely, Internet of Things).With this emerging interest as well as the wealth of challenging research problems in mind, we are proposing the second NIPS 2018 workshop dedicated to on-device machine learning for mobile and

ambient home consumer devices. Areas/topics of interest include, but not limited to:* Model compression for efficient inference with deep networks and other ML models* Privacy preserving machine learning* Low-precision training/inference & Hardware acceleration of neural computing on mobile devices* Real-time mobile computer vision* Language understanding and conversational assistants on mobile devices* Speech recognition on mobile and smart home devices* Machine intelligence for mobile gaming* ML for mobile health other real-time prediction scenarios* ML for on-device applications in the automotive industry (e.g., computer vision for self-driving cars)* Software libraries (including open-source) optimized for on-device MLTarget Audience: The next wave of ML applications will have significant processing on mobile and ambient devices. Some immediate examples of these are single-image classification, depth estimation, object recognition and segmentation running on-device for creative effects, or on-device recommender and ranking systems for privacy-preserving, low-latency experiences. This workshop will bring ML practitioners up to speed on the latest trends for on-device applications of ML, offer an overview of the latest HW and SW framework developments, and champion active research towards hard technical challenges emerging in this nascent area. The target audience for the workshop is both industrial and academic researchers and practitioners of on-device, native machine learning. The workshop will cover both “informational” and “aspirational” aspects of this emerging research area for delivering ground-breaking experiences on real-world products. Given the relevance of the topic, target audience (mix of industry + academia & related parties) as well as the timing (confluence of research ideas + practical implementations both in industry as well as through publicly available toolkits ), we feel that NIPS 2018 would continue to be a great venue for this workshop.

---

## Causal Learning

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Martin Arjovsky · Christina Heinze-Deml · Anna Klimovskaia · Maxime Oquab · Leon Bottou · David Lopez-Paz*

Site for the workshop: https://sites.google.com/view/nips2018causallearning/homeThe route from machine learning to artificial intelligence remains uncharted. Recent efforts describe some of the conceptual problems that lie along this route [4, 9, 12]. The goal of this workshop is to investigate how much progress is possible by framing these problems beyond learning correlations, that is, by uncovering and leveraging causal relations:1. Machine learning algorithms solve statistical problems (e.g. maximum likelihood) as a proxy to solve tasks of interest (e.g. recognizing objects). Unfortunately, spurious correlations and biases are often easier to learn than the task itself [14], leading to unreliable or unfair predictions. This phenomenon can be framed as causal confounding.2. Machines trained on large pools of i.i.d. data often crash confidently when deployed in different circumstances (e.g., adversarial examples, dataset biases [18]). In contrast, humans seek prediction rules robust across multiple conditions. Allowing machines to learn robust rules from multiple environments can be framed as searching for causal invariances [2, 11, 16, 17].3. Humans benefit from discrete structures to reason. Such structures seem less useful to learning machines. For

instance, neural machine translation systems outperform those that model language structure. However, the purpose of this structure might not be modeling common sentences, but to help us formulate new ones. Modeling new potential sentences rather than observed ones is a form of counterfactual reasoning [8, 9].4. Intelligent agents do not only observe, but also shape the world with actions. Maintaining plausible causal models of the world allows to build intuitions, as well as to design intelligent experiments and interventions to test them [16, 17]. Is causal understanding necessary for efficient reinforcement learning?5. Humans learn compositionally; after learning simple skills, we are able to recombine them quickly to solve new tasks. Such abilities have so far eluded our machine learning systems. Causal models are compositional, so they might offer a solution to this puzzle [4].6. Finally, humans are able to digest large amounts of unsupervised signals into a causal model of the world. Humans can learn causal affordances, that is, imagining how to manipulate new objects to achieve goals, and the outcome of doing so. Humans rely on a simple blueprint for a complex world: models that contain the correct causal structures, but ignore irrelevant details [16, 17].We cannot address these problems by simply performing inference on known causal graphs. We need to learn from data to discover plausible causal models, and to construct predictors that are robust to distributional shifts. Furthermore, much prior work has focused on estimating explicit causal structures from data, but these methods are often unscalable, rely on untestable assumptions like faithfulness or acyclicity, and are difficult to incorporate into high-dimensional, complex and nonlinear machine learning pipelines. Instead of considering the task of estimating causal graphs as their final goal, learning machines may use notions from causation indirectly to ignore biases, generalize across distributions, leverage structure to reason, design efficient interventions, benefit from compositionality, and build causal models of the world in an unsupervised way.Call for papersSubmit your anonymous, NIPS-formatted manuscript here[https://easychair.org/cfp/NIPSCL2018]. All accepted submissions will require a poster presentation. A selection of submissions will be awarded a 5-minute spotlight presentation. We welcome conceptual, thought-provoking material, as well as research agendas, open problems, new tasks, and datasets.Submission deadline: 28 October 2018Acceptance notifications: 9 November 2018 Schedule:See https://sites.google.com/view/nips2018causallearning/home for the up-to-date schedule.Speakers:Judea PearlDavid BleiNicolai MeinshausenBernhard SchölkopfIsabelle GuyonCsaba SzepesvariPietro Perona References1. Krzysztof Chalupka, Pietro Perona, Frederick Eberhardt (2015): Visual Causal Feature Learning [https://arxiv.org/abs/1412.2309]2. Christina Heinze-Deml, Nicolai Meinshausen (2018): Conditional Variance Penalties and Domain Shift Robustness [https://arxiv.org/abs/1710.11469]3. Fredrik D. Johansson, Uri Shalit, David Sontag (2016): Learning Representations for Counterfactual Inference [https://arxiv.org/abs/1605.03661]4. Brenden Lake (2014): Towards more human-like concept learning in machines: compositionality, causality, and learning-to-learn [https://dspace.mit.edu/handle/1721.1/95856]5. Brenden M. Lake, Tomer D. Ullman, Joshua B. Tenenbaum, Samuel J. Gershman (2016): Building Machines That Learn and Think Like People [https://arxiv.org/abs/1604.00289]6. David Lopez-Paz, Krikamol Muandet, Bernhard Schölkopf, Ilya Tolstikhin (2015): Towards a Learning Theory of Cause-Effect Inference [https://arxiv.org/abs/1309.6779]7. David Lopez-Paz, Robert Nishihara, Soumith Chintala, Bernhard Schölkopf, Léon Bottou (2017): Discovering Causal Signals in Images [https://arxiv.org/abs/1605.08179]8. Judea Pearl (2009): Causality: Models, Reasoning, and Inference [http://bayes.cs.ucla.edu/BOOK-2K/]9. Judea Pearl (2018): The Seven Pillars of Causal Reasoning

with Reflections on Machine Learning [http://ftp.cs.ucla.edu/pub/statser/r481.pdf]10. Jonas Peters, Joris Mooij, Dominik Janzing, Bernhard Schölkopf (2014): Causal Discovery with Continuous Additive Noise Models [https://arxiv.org/abs/1309.6779]11. Jonas Peters, Peter Bühlmann, Nicolai Meinshausen (2016): Causal inference using invariant prediction: identification and confidence intervals [https://arxiv.org/abs/1501.01332]12. Jonas Peters, Dominik Janzing, Bernhard Schölkopf (2017): Elements of Causal Inference: Foundations and Learning Algorithms [https://mitpress.mit.edu/books/elements-causal-inference]13. Peter Spirtes, Clark Glymour, Richard Scheines (2001): Causation, Prediction, and Search [http://cognet.mit.edu/book/causation-prediction-and-search]14. Bob L. Sturm (2016): The HORSE conferences [http://c4dm.eecs.qmul.ac.uk/horse2016/, http://c4dm.eecs.qmul.ac.uk/horse2017/]15. Dustin Tran, David M. Blei (2017): Implicit Causal Models for Genome-wide Association Studies [https://arxiv.org/abs/1710.10742]16. Michael Waldmann (2017): The Oxford Handbook of Causal Reasoning [https://global.oup.com/academic/product/the-oxford-handbook-of-causal-reasoning-9780199399550?cc=us&lang=en]17. James Woodward (2005): Making Things Happen: A Theory of Causal Explanation [https://global.oup.com/academic/product/making-things-happen-9780195189537?cc=us&lang=en&]18. Antonio Torralba, Alyosha Efros (2011): Unbiased look at dataset bias. [http://people.csail.mit.edu/torralba/publications/datasetscvpr11.pdf]

---

# Imitation Learning and its Challenges in Robotics

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Mustafa Mukadam · Sanjiban Choudhury · Siddhartha Srinivasa*

Many animals including humans have the ability to acquire skills, knowledge, and social cues from a very young age. This ability to imitate by learning from demonstrations has inspired research across many disciplines like anthropology, neuroscience, psychology, and artificial intelligence. In AI, imitation learning (IL) serves as an essential tool for learning skills that are difficult to program by hand. The applicability of IL to robotics in particular, is useful when learning by trial and error (reinforcement learning) can be hazardous in the real world. Despite the many recent breakthroughs in IL, in the context of robotics there are several challenges to be addressed if robots are to operate freely and interact with humans in the real world.Some important challenges include: 1) achieving good generalization and sample efficiency when the user can only provide a limited number of demonstrations with little to no feedback; 2) learning safe behaviors in human environments that require the least user intervention in terms of safety overrides without being overly conservative; and 3) leveraging data from multiple sources, including non-human sources, since limitations in hardware interfaces can often lead to poor quality demonstrations.In this workshop, we aim to bring together researchers and experts in robotics, imitation and reinforcement learning, deep learning, and human robot interaction to- Formalize the representations and primary challenges in IL as they pertain to robotics- Delineate the key strengths and limitations of existing approaches with respect

to these challenges- Establish common baselines, metrics, and benchmarks, and identify open questions

---

## Workshop on Ethical, Social and Governance Issues in AI

**Workshop | Fri Dec 7th 08:00 AM -- 06:30 PM @ None**

*Chloe Bakalar · Sarah Bird · Tiberio Caetano · Edward W Felten · Dario Garcia · Isabel Kloumann · Finnian Lattimore · Sendhil Mullainathan · D. Sculley*

AbstractEthics is the philosophy of human conduct: It addresses the question “how should we act?” Throughout most of history the repertoire of actions available to us was limited and their consequences constrained in scope and impact through dispersed power structures and slow trade. Today, in our globalised and networked world, a decision can affect billions of people instantaneously and have tremendously complex repercussions. Machine learning algorithms are replacing humans in making many of the decisions that affect our everyday lives. How can we decide how machine learning algorithms and their designers should act? What is the ethics of today and what will it be in the future?In this one day workshop we will explore the interaction of AI, society, and ethics through three general themes.Advancing and Connecting Theory: How do different fairness metrics relate to one another? What are the trade-offs between them? How do fairness, accountability, transparency, interpretability and causality relate to ethical decision making? What principles can we use to guide us in selecting fairness metrics within a given context? Can we connect these principles back to ethics in philosophy? Are these principles still relevant today?Tools and Applications: Real-world examples of how ethical considerations are affecting the design of ML systems and pipelines. Applications of algorithmic fairness, transparency or interpretability to produce better outcomes. Tools that aid identifying and or alleviating issues such as bias, discrimination, filter bubbles, feedback loops etc. and enable actionable exploration of the resulting trade-offs. Regulation: With the GDPR coming into force in May 2018 it is the perfect time to examine how regulation can help (or hinder) our efforts to deploy AI for the benefit of society. How are companies and organisations responding to the GDPR? What aspects are working and what are the challenges? How can regulatory or legal frameworks be designed to continue to encourage innovation, so society as a whole can benefit from AI, whilst still providing protection against its harms. This workshop is designed to be focused on some of the larger ethical issues related to AI and can be seen as a complement to the FATML proposal, which is focused more on fairness, transparency and accountability. We would be happy to link or cluster the workshops together, but we (us and the FATML organizers) think that there is more than 2 day worth of material that the community needs to discuss in the area of AI and ethics, so it would be great to have both workshops if possible.

---

## Coffee Break

**Break | Fri Dec 7th 10:30 -- 11:00 AM @**

—

---

## Coffee Break

**Break | Fri Dec 7th 03:00 -- 03:30 PM @**

—