Workshop organizers make last-minute changes to their schedule. Download this document again to get the lastest changes, or use the NeurIPS mobile application.

Schedule Highlights

**Dec. 13, 2019**

East Ballroom A, Safety and Robustness in Decision-making
Ghavamzadeh, Mannor, Yue, Petrik, Chow

East Ballroom B, Learning Meaningful Representations of Life

East Ballroom C, Optimal Transport for Machine Learning
Cuturi, Peyré, Flamary, Suvarikova

East Exhibition Hall A, Information Theory and Machine Learning
Zhao, Song, Han, Choi, Kalluri, Poole, Dimakis, Jiao, Weissman, Ermon

East Meeting Rooms 11 + 12, MLSys: Workshop on Systems for ML
Lakshmiratan, Sen, Gonzalez, Crankshaw, Bird

East Meeting Rooms 1 - 3, Perception as generative reasoning: structure, causality, probability
Rosenbaum, Garnelo, Battaglia, Allen, Yıldırım

East Meeting Rooms 8 + 15, Minding the Gap: Between Fairness and Ethics
Rubinov, Kondor, Poullon, Warmuth, Moss, Hagerty

West 109 + 110, KR2ML - Knowledge Representation and Reasoning Meets Machine Learning
Thost, Muise, Talamadupula, Singh, Ré

West 114 + 115, Retrospectives: A Venue for Self-Reflection in ML Research
Lowe, Bengio, Pineau, Paganini, Forde, Sodhani, Gupta, Lehman, Henderson, Madan, Sinha, Bouthillier

West 116 + 117, Competition Track Day 1 Escalante

West 118 - 120, Workshop on Federated Learning for Data Privacy and Confidentiality
Fan, Kong, Liu, McMahan, Smith, Yu

West 121 + 122, Machine Learning for the Developing World (ML4D): Challenges and Risks
De-Arteaga, Coston, Alfonja

West 202 - 204, Visually Grounded Interaction and Language
Strub, Das, Wijmans, de Vries, Lee, Suhr, Arad Hudson

West 205 - 207, Robust AI in Financial Services: Data, Fairness, Explainability, Trustworthiness, and Privacy
Oprea, Gal, Moulinier, Chen, Veloso, Kumar, Faruquie

West 208 + 209, Learning with Rich Experience: Integration of Learning Paradigms
Hu, Wilson, Finn, Lee, Berg-Kirkpatrick, Salakhutdinov, Xing

West 211 - 214, Beyond first order methods in machine learning systems
Kyrillidis, Berahas, Roosta, Mahoney

West 215 + 216, CiML 2019: Machine Learning Competitions for All
Mendrik, Tu, Guyon, Viegas, LI

West 217 - 219, AI for Humanitarian Assistance and Disaster Response
Gupta, Murphy, Darrell, Heim, Wang, Goodman, Biliński

West 220 - 222, Shared Visual Representations in Human and Machine Intelligence
Deza, Peterson, Murty, Griffiths

West 223 + 224, Workshop on Human-Centric Machine Learning
Angelov, Oliver, Weller, Rodriguez, Valera, Chiappa, Heidari, Kilbertus

West 301 - 305, Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications
Heckel, Hand, Baraniuk, Bruna, Dimakis, Needell

Parihar, Goldfarb, Srivastava, SHENG, Pal

West Ballroom A, Machine Learning for Health (ML4H): What makes machine learning in medicine different?
Beam, Naumann, Beaulieu-Jones, Chen, Finlayson, Alsentzer, Dalca, McDermott

West Ballroom B, Meta-Learning
Calandra, Clavera Gilaberte, Hutter, Vanschoren, Wang

West Ballroom C, Biological and Artificial Reinforcement Learning
Chua, Zannone, Behbahani, Ponte Costa, Clopath, Richards, Precup

West Exhibition Hall A, Graph Representation Learning
Hamilton, van den Berg, Bronstein, Jegelka, Kipf, Leskovec, Liao, Sun, Veclkov

West Exhibition Hall C, Bayesian Deep Learning
Gal, Fernández-Lobato, Louizos, Nalisnick, Ghahramani, Murphy, Welling

**Dec. 14, 2019**

East Ballroom A, Real Neurons & Hidden Units: future directions at the intersection of neuroscience and AI
Lajoie, Shlizerman, Puelma Touzel, Thompson, Kording

East Ballroom B, Fair ML in Healthcare
Joshi, Chen, Saleh

East Ballroom C, Tackling Climate Change with ML
Rolnick, Donini, Kaack, Lacoste, Maharaj, Ng, Platt, Chayes, Bengio

East Meeting Rooms 11 + 12, Joint Workshop on AI for Social Good
Fang, Bullock, Dilhaç, Green, saltiel, Adjodah, Clark, McGregor, Luck, Penn, Sylvain, Boucher, Swaine-Simon, Tadese, Coté, Bethke, Bengio

East Meeting Rooms 1 - 3, Machine Learning for Autonomous Driving
McAllister, Rhinehart, Yu, Li, Dragan

East Meeting Rooms 8 + 15, Privacy in Machine Learning (PriML)
Balle, Chaudhuri, Honkela, Koskela, Meehan, Park, Smart, Welling

West 109 + 110, Machine Learning and the Physical Sciences
Baydin, Carrasquilla, Ho, Kashinath, Paganini, Thais, Anandkumar, Crannier, Melko, Prabhat, Wood

West 114 + 115, Program Transformations for ML
Lambin, Baydin, Wiltschko, van Memmelenboer, Fertig, Pearlmutter, Duvenaud, Hascoët

West 116 + 117, Competition Track Day 2 Escalante

West 118 - 120, Emergent Communication: Towards Natural Language
Gupta, Noukhovitch, Resnick, Jaques, Filos, Ossenkopf, Lazaridou, Foerster, Lowe, Kiela, Cho

West 202 - 204, ML For Systems
Hashemi, Mirhoseini, Goldfarb, Swersky, Xu, Raiman

West 205 - 207, The third Conversational AI workshop – today's practice and tomorrow's potential
Geramifard, Williams, Byrne, Celikyilmaz, Gasic, Hakkani-Tur, Henderson, Lastras, Ostendorf

West 208 + 209, Document Intelligence
Duffy, Akkiraju, Bedrax Weiss, Bennett, Motahari-Nezhad
West 211 - 214, **Learning Transferable Skills** Mattar, Juliani, Lange, Crosby, Beyret

West 215 + 216, **Sets and Partitions** Monath, Zaheer, McCallum, Kobren, Oliva, Poczos, Salakhutdinov

West 217 - 219, **Context and Compositionality in Biological and Artificial Neural Systems** Turek, Jain, Huth, Wehbe, Strubell, Yuille, Linzen, Honey, Cho

West 220 - 222, **Robot Learning: Control and Interaction in the Real World** Calandra, Rakelly, Kamthe, Kragic, Schaal, Wulfmeier

West 223 + 224, **NeurIPS Workshop on Machine Learning for Creativity and Design 3.0** Elliott, Dieleman, Roberts, Engel, White, Fiebrink, Mital, Payne, Tokui

West 301 - 305, **Medical Imaging meets NeurIPS** Lombaert, Glocker, Konukoglu, de Bruijne, Feragen, Oguz, Teuwen

West 306, **Learning with Temporal Point Processes** Rodriguez, Song, Valera, Liu, De, Zha

West Ballroom A, **The Optimization Foundations of Reinforcement Learning** Dai, He, Le Roux, Li, Schuurmans, White

West Ballroom B, **Machine Learning with Guarantees** London, Dziugaite, Roy, Joachims, Madry, Shawe-Taylor

West Ballroom C, **"Do the right thing": machine learning and causal inference for improved decision making** Santacatterina, Joachims, Kallus, Swaminathan, Sontag, Zhou

West Exhibition Hall A, **Bridging Game Theory and Deep Learning** Mitliagkas, Gidel, He, Askari Hemmat, Haghtalab, Lacoste-Julien

West Exhibition Hall C, **Deep Reinforcement Learning** Abbeel, Finn, Pineau, Silver, Singh, Achiam, Florensa, Grimm, Tang, Veeriah

**Dec. 9, 2019**

East Meeting Rooms 11 + 12, **New In Machine Learning**
Safety and Robustness in Decision-making

Mohammad Ghavamzadeh, Shie Mannor, Yisong Yue, Marek Petrik, Yinlam Chow

East Ballroom A, Fri Dec 13, 08:00 AM

Interacting with increasingly sophisticated decision-making systems is becoming more and more a part of our daily life. This creates an immense responsibility for designers of these systems to build them in a way to guarantee safe interaction with their users and good performance, in the presence of noise and changes in the environment, and/or of model misspecification and uncertainty. Any progress in this area will be a huge step forward in using decision-making algorithms in emerging high stakes applications, such as autonomous driving, robotics, power systems, health care, recommendation systems, and finance.

This workshop aims to bring together researchers from academia and industry in order to discuss main challenges, describe recent advances, and highlight future research directions pertaining to develop safe and robust decision-making systems. We aim to highlight new and emerging theoretical and applied research opportunities for the community that arise from the evolving needs for decision-making systems and algorithms that guarantee safe interaction and good performance under a wide range of uncertainties in the environment.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:55 AM</td>
<td>Daniel Kuhn: From Data to Decisions: Distributionally Robust Optimization is Optimal</td>
</tr>
<tr>
<td>09:35 AM</td>
<td>Poster Session</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Finale Doshi-Velez: Combining Statistical methods with Human Input for Evaluation and Optimization in Batch Settings</td>
</tr>
<tr>
<td>11:10 AM</td>
<td>Marco Pavone: On Safe and Efficient Human-robot Interactions via Multi-modal Intent Modeling and Reachability-based Safety Assurance</td>
</tr>
<tr>
<td>11:50 AM</td>
<td>Dimitar Filev: Practical Approaches to Driving Policy Design for Autonomous Vehicles</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch Break</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Nathan Kallus: Efficiently Breaking the Curse of Horizon with Double Reinforcement Learning</td>
</tr>
<tr>
<td>02:40 PM</td>
<td>Scott Niekum: Scaling Probabilistically Safe Learning to Robotics</td>
</tr>
<tr>
<td>03:20 PM</td>
<td>Poster Session and Coffee Break</td>
</tr>
<tr>
<td>Time</td>
<td>Speaker</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>04:30 PM</td>
<td>Andy Sun</td>
</tr>
<tr>
<td>05:10 PM</td>
<td>Thorsten Joachim</td>
</tr>
<tr>
<td>05:50 PM</td>
<td></td>
</tr>
</tbody>
</table>

Abstracts (9):


How can we build autonomous robots that operate in unstructured and dynamic environments such as homes or hospitals? This problem has been investigated under several disciplines, including planning (motion planning, task planning, etc.), and reinforcement learning. While both of these fields have witnessed tremendous progress, each have fundamental drawbacks: planning approaches require substantial manual engineering in mapping perception to a formal planning problem, while RL, which can operate directly on raw percepts, is data hungry, cannot generalize to new tasks, and is 'black box' in nature.

Motivated by humans’ remarkable capability to imagine and plan complex manipulations of objects, and recent advances in imagining images such as GANs, we present Visual Plan Imagination (VPI) — a new computational problem that combines image imagination and planning. In VPI, given off-policy image data from a dynamical system, the task is to 'imagine' image sequences that transition the system from start to goal. Thus, VPI focuses on the essence of planning with high-dim perception, and abstracts away low level control and reward engineering. More importantly, VPI provides a safe and interpretable basis for robotic control — before the robot acts, a human inspects the imagined plan the robot will act upon, and can intervene if necessary.

I will describe our approach to VPI based on Causal InfoGAN, a deep generative model that learns features that are compatible with strong planning algorithms. We show that Causal InfoGAN can generate convincing visual plans, and we demonstrate learning to imagine and execute real robot rope manipulation from image data. I will also discuss our VPI simulation benchmarks, and recent efforts in novelty detection, an important component in VPI, and in safe decision making in general.

Abstract 3: Daniel Kuhn: From Data to Decisions: Distributionally Robust Optimization is Optimal in Safety and Robustness in Decision-making, Kuhn 08:55 AM

We study stochastic optimization problems where the decision-maker cannot observe the distribution of the exogenous uncertainties but has access to a finite set of independent training samples. In this setting, the goal is to find a procedure that transforms the data to an estimate of the expected cost function under the unknown data-generating distribution, i.e., a predictor, and an optimizer of the estimated cost function that serves as a near-optimal candidate decision, i.e., a prescriptor. As functions of the data, predictors and prescriptors constitute statistical estimators. We propose a meta-optimization problem to find the least conservative predictors and prescriptors subject to constraints on their out-of-sample disappointment. The out-of-sample disappointment quantifies the probability that the actual expected cost of the candidate decision under the unknown true distribution exceeds its predicted cost. Leveraging tools from large deviations theory, we prove that this meta-optimization problem admits a unique solution: The best predictor-prescriptor pair is obtained by solving a distributionally robust optimization problem over all distributions within a given relative entropy distance from the empirical distribution of the data.

Abstract 5: Finale Doshi-Velez: Combining Statistical methods with Human Input for Evaluation and Optimization in Batch Settings in Safety and Robustness in Decision-making, Doshi-Velez 10:30 AM

Statistical methods for off-policy evaluation and counterfactual reasoning will have fundamental limitations based on what assumptions can be made and what kind of exploration is present in the data (some of which is being presented here by other speakers!). In this talk, I’ll discuss some recent directions in our lab regarding ways to integrate human experts into the process of policy evaluation and selection in batch settings. The first deals with statistical limitations by seeking a diverse collection of statistically-indistinguishable (with respect to outcome) policies for humans to eventually decide from. The second involves directly integrating human feedback to eliminate or validate specific sources of sensitivity in an off-policy evaluation to get more robust estimates (or at least better understand the source of their non-robustness). More broadly, I will discuss open directions for moving from purely-statistical (e.g. off-policy evaluation) or purely-human (e.g. interpretability-based) approaches for robust/safe decision-making toward combining the advantages of both.

Abstract 6: Marco Pavone: On Safe and Efficient Human-robot Interactions via Multi-modal Intent Modeling and Reachability-based Safety Assurance in Safety and Robustness in Decision-making, Pavone 11:10 AM

In this talk I will present a decision-making and control stack for human-robot interactions by using autonomous driving as a motivating example. Specifically, I will first discuss a data-driven approach for learning multimodal interaction dynamics between robot-driven and human-driven vehicles based on recent advances in deep generative modeling. Then, I will discuss how to incorporate such a learned interaction model into a real-time, interaction-aware decision-making framework. The framework is designed to be minimally interventional; in particular, by leveraging backward reachability analysis, it ensures safety even when other cars defy the robot’s expectations without unduly sacrificing performance. I will present recent results from experiments on a full-scale steer-by-wire platform, validating the framework and providing practical insights. I will conclude the talk by providing an overview of related efforts from my group on infusing safety assurances in robot autonomy stacks equipped with learning-based components, with an emphasis on adding structure within robot learning via control-theoretical and formal methods.

Abstract 7: Dimitar Filev: Practical Approaches to Driving Policy Design for Autonomous Vehicles in Safety and Robustness in Decision-making, 11:50 AM

The presentation deals with some practical facets of application of AI methods to designing driving policy for autonomous vehicles. Relationship between the reinforcement learning (RL) based solutions and the use of rule-based and model-based techniques for improving
their robustness and safety are discussed. One approach to obtaining explainable RL models by learning alternative rule-based representations is proposed. The presentation also elaborates on the opportunities for extending the AI driving policy approaches by applying game theory inspired methodology to addressing diverse and unforeseen scenarios, and representing the negotiation aspects of decision making in autonomous driving.

Abstract 9: Nathan Kallus: Efficiently Breaking the Curse of Horizon with Double Reinforcement Learning in Safety and Robustness in Decision-making, Kallus 02:00 PM

Off-policy evaluation (OPE) is crucial for reinforcement learning in domains like medicine with limited exploration, but OPE is also notoriously difficult because the similarity between trajectories generated by any proposed policy and the observed data diminishes exponentially as horizon grows, known as the curse of horizon. To understand precisely when this curse bites, we consider for the first time the semi-parametric efficiency limits of OPE in Markov decision processes (MDP), establishing the best-possible estimation errors and characterizing the curse as a problem-dependent phenomenon rather than method-dependent. Efficiency in OPE is crucial because, without exploration, we must use the available data to its fullest. In finite horizons, this shows standard doubly-robust (DR) estimators are in fact inefficient for MDPs. In infinite horizons, while the curse renders certain problems fundamentally intractable, OPE may be feasible in ergodic time-invariant MDPs. We develop the first OPE estimator that achieves the efficiency limits in both setting, termed Double Reinforcement Learning (DRL). In both finite and infinite horizons, DRL improves upon existing estimators, which we show are inefficient, and leverages problem structure to its fullest in the face of the curse of horizon. We establish many favorable characteristics for DRL including efficiency even when nuisances are estimated slowly by blackbox models, finite-sample guarantees, and model double robustness.

Abstract 10: Scott Niekum: Scaling Probabilistically Safe Learning to Robotics in Safety and Robustness in Decision-making, Niekum 02:40 PM

In recent years, high-confidence reinforcement learning algorithms have enjoyed success in application areas with high-quality models and plentiful data, but robotics remains a challenging domain for scaling up such approaches. Furthermore, very little work has been done on the even more difficult problem of safe imitation learning, in which the demonstrator’s reward function is not known. This talk focuses on three recent developments in this emerging area of research: (1) a theory of safe imitation learning; (2) scalable reward inference in the absence of models; (3) efficient off-policy policy evaluation. The proposed algorithms offer a blend of safety and practicality, making a significant step towards safe robot learning with modest amounts of real-world data.

Abstract 12: Andy Sun: Recent Advances in Multistage Decision-making under Uncertainty: New Algorithms and Complexity Analysis in Safety and Robustness in Decision-making, Sun 04:30 PM

In this talk, we will review some recent advances in the area of multistage decision making under uncertainty, especially in the domain of stochastic and robust optimization. We will present some new algorithmic development that allows for exactly solving huge-scale stochastic programs with integer recourse decisions, and algorithms in a dual perspective that can deal with infeasibility in problems. This significantly extends the scope of stochastic dual dynamic programming (SDDP) algorithms from convex or binary state variable cases to general nonconvex problems. We will also present a new analysis of the iteration complexity of the proposed algorithms. This settles some open questions in regards of the complexity of SDDP.

Abstract 13: Thorsten Joachim: Fair Ranking with Biased Data in Safety and Robustness in Decision-making, Joachims 05:10 PM

Search engines and recommender systems have become the dominant matchmaker for a wide range of human endeavors -- from online retail to finding romantic partners. Consequently, they carry immense power in shaping markets and allocating opportunity to the participants. In this talk, I will discuss how the machine learning algorithms underlying these system can produce unfair ranking policies for both exogenous and endogenous reasons. Exogenous reasons often manifest themselves as biases in the training data, which then get reflected in the learned ranking policy and lead to rich-get-richer dynamics. But even when trained with unbiased data, reasons endogenous to the algorithms can lead to unfair allocation of opportunity. To overcome these challenges, I will present new machine learning algorithms that directly address both endogenous and exogenous unfairness.

Learning Meaningful Representations of Life

Elizabeth Wood, Yakir Reshef, Jon Bloom, Jasper Snoek, Barbara Engelhardt, Scott Linderman, Suchi Saria, Alexander Willschko, Casey Greene, Chang Liu, Kresten Lindorff-Larsen, Debora Marks

East Ballroom B, Fri Dec 13, 08:00 AM

The last decade has seen both machine learning and biology transformed: the former by the ability to train complex predictors on massive labelled data sets; the latter by the ability to perturb and measure biological systems with staggering throughput, breadth, and resolution. However, fundamentally new ideas in machine learning are needed to translate biomedical data at scale into a mechanistic understanding of biology and disease at a level of abstraction beyond single genes. This challenge has the potential to drive the next decade of creativity in machine learning as the field grapples with how to move beyond prediction to a regime that broadly catalyzes and accelerates scientific discovery.

To seize this opportunity, we will bring together current and future leaders within each field to introduce the next generation of machine learning specialists to the next generation of biological problems. Our full-day workshop will start a deeper dialogue with the goal of Learning Meaningful Representations of Life (LMRL), emphasizing interpretable representation learning of structure and principles. The workshop will address this challenge at five layers of biological abstraction (genome, molecule, cell, system, phenome) through interactive breakout sessions led by a diverse team of experimentalists and computational scientists to facilitate substantive discussion.

We are calling for short abstracts from computer scientists and biological scientists. Submission deadline is Friday, September 20. Significant travel support is also available. Details here:

https://lmrl-bio.github.io/call
https://lmrl-bio.github.io/travel
## Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 AM</td>
<td>Opening Remarks</td>
<td></td>
</tr>
<tr>
<td>08:45 AM</td>
<td>Opening Remarks</td>
<td>Yeshwant</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Keynote - Bio/ML</td>
<td>Regev</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Keynote - ML</td>
<td>Welling</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>In conversations: Daphne Koller and Barbara Englehardt</td>
<td>Koller, Engelhardt</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:45 AM</td>
<td>Molecules and Genomes</td>
<td>Haussler, Clevert, Keiser, Aspuru-Guzik, Duvenaud, Jones, Wei, D'Amour</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Synthetic Systems</td>
<td>Silver, Marks, Liu, Huang</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Poster Session I (Lunch Provided)</td>
<td></td>
</tr>
<tr>
<td>01:15 PM</td>
<td>Phenotype</td>
<td>HaCohen, Reshef, Johnson, Morris, Nagy, Eraslan, Singer, Van Allen, Krishnaswamy, Greene, Linderman, Wiltschko, Kotliar, Zou, Bulik-Sullivan</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Cell</td>
<td>Carpenter, Zhou, Chikina, Tong, Lengerich, Abdelkareem, Eraslan, Ra, Burkhardt, Matsen IV, Moses, Chen, Haghighi, Lu, Schau, Nivala, Shiftman, Habrecht, Masengo Wa Umba, Weinstein</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Closing Remarks</td>
<td>Sander, Fiete, Peer</td>
</tr>
<tr>
<td>05:45 PM</td>
<td>Last Look at Posters (Drinks Provided)</td>
<td></td>
</tr>
</tbody>
</table>

### Abstracts (11):

**Abstract 1:** Opening Remarks in Learning Meaningful Representations of Life, 08:30 AM

Opening Remarks by Francis Collins, Director, NIH (by video)

**Abstract 2:** Opening Remarks in Learning Meaningful Representations of Life, Yeshwant 08:45 AM

Opening remarks by Francis Collins (Director, National Institutes of Health) via video and Krishna Yeshwant, General Partner at Google Ventures.

**Abstract 3:** Keynote - Bio/ML in Learning Meaningful Representations of Life, Regev 09:00 AM

Aviv Regev. Professor of Biology; Core Member, Broad Institute; Investigator, Howard Hughes Medical Institute. Aviv Regev pioneers the use of single-cell genomics and other techniques to dissect the molecular networks that regulate genes, define cells and tissues, and influence health and disease.

Max Welling is a research chair in Machine Learning at the University of Amsterdam and a VP Technologies at Qualcomm.

Daphne Koller is the Rajeev Motwani Professor in the Computer Science Department at Stanford University and founder of insitro.

David Duvenaud & Alan Aspuru-Guzik; Michael Keiser & Jennifer Wei; David Jones & John Jumper; David Haussler & Alex D’Amour speak on jointly identified challenges.

Pamela Silver, Debora Marks, and Chang Liu in conversation.

Information Theory and Machine Learning

Shengjia Zhao, Jiaming Song, Yanjun Han, Kristy Choi, Pratyusha Kalluri, Ben Poole, Alex Dimakis, Jiatao Jiao, Tsachy Weissman, Stefano Ermon

East Exhibition Hall A, Fri Dec 13, 08:00 AM

Information theory is deeply connected to two key tasks in machine learning: prediction and representation learning. Because of these connections, information theory has found wide applications in machine learning tasks, such as proving generalization bounds, certifying fairness and privacy, optimizing information content of unsupervised/supervised representations, and proving limitations to prediction performance. Conversely, progress in machine learning have been successfully applied to classical information theory tasks such as compression and transmission.

These recent progress have lead to new open questions and opportunities: to marry the simplicity and elegance of information theoretic analysis with the complexity of modern high dimensional machine learning setups. However, because of the diversity of information theoretic research, different communities often progress independently despite shared questions and tools. For example, variational bounds to mutual information are concurrently developed in information theory, generative model, and learning theory communities.

This workshop hopes to bring together researchers from different disciplines, identify common grounds, and spur discussion on how information theory can apply to and benefit from modern machine learning setups.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:30 AM</td>
<td>Invited Talk: Ayfer Ozgur Aydin</td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Invited Talk: Stefano Soatto and Alessandro Achille</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Contributed Talk</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Invited Talk: Varun Jog</td>
<td></td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Invited Talk: Po-Ling Loh</td>
<td></td>
</tr>
<tr>
<td>03:20 PM</td>
<td>Invited Talk: Aaron van den Oord</td>
<td></td>
</tr>
<tr>
<td>03:50 PM</td>
<td>Invited Talk: Alexander A Alemi</td>
<td></td>
</tr>
<tr>
<td>04:20 PM</td>
<td>Poster Spotlight</td>
<td></td>
</tr>
</tbody>
</table>
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.

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 AM</td>
<td>Welcome</td>
<td></td>
</tr>
<tr>
<td>08:40 AM</td>
<td>Keynote 1: Machine Learning Reproducibility:</td>
<td>An update from the NeurIPS 2019 Reproducibility Co-Chairs, Joelle Pineau, McGill University and Facebook</td>
</tr>
<tr>
<td>09:10 AM</td>
<td>Contributed Talk: SLIDE: Training Deep Neural Networks with Large Outputs on a CPU faster than a V100-GPU</td>
<td></td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Contributed Talk: NeMo: A Toolkit for Building AI Applications Using Neural Modules</td>
<td></td>
</tr>
<tr>
<td>09:50 AM</td>
<td>Poster Overview</td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Posters and Coffee</td>
<td></td>
</tr>
<tr>
<td>11:10 AM</td>
<td>Keynote 2: Vivienne Sze, MIT</td>
<td></td>
</tr>
<tr>
<td>11:40 AM</td>
<td>Contributed Talk: 5 Parallel Prism: A Topology for Pipelined Implementations of Convolutional Neural Networks Using Computational Memory</td>
<td></td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Systems Bonanza (10 minutes each) PyTorch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TensorFlow Keras TVM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ray ONNX Runtime</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CoreML Flux MLFlow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MLPerf Microsoft RL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems MXNet</td>
<td></td>
</tr>
</tbody>
</table>
Perception as generative reasoning: structure, causality, probability

Dan Rosenbaum, Marta Garnelo, Peter Battaglia, Kelsey Allen, Ilker Yildirim

East Meeting Rooms 1 - 3, Fri Dec 13, 08:00 AM

Many perception tasks can be cast as ‘inverse problems’ where the input signal is the outcome of a causal process and perception is to invert that process. For example in visual object perception, the image is caused by an object and perception is to infer which object gave rise to that image. Following an analysis-by-synthesis approach, modelling the forward and causal direction of the data generation process is a natural way to capture the underlying scene structure, which typically leads to broader generalisation and better sample efficiency. Such a forward model can be applied to solve the inverse problem (inferring the scene structure from an input image) using Bayes rule, for example. This workflow stands in contrast to common approaches in deep learning, where typically one first defines a task, and then optimises a deep model end-to-end to solve it. In this workshop we propose to revisit ideas from the generative approach and advocate for learning-based analysis-by-synthesis methods for perception and inference. In addition, we pose the question of how ideas from these research areas can be combined with and complement modern deep learning practices.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:50 AM</td>
<td>Opening Remarks</td>
<td>Rosenbaum, Garnelo, Battaglia, Allen, Yildirim</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Tatiana Lopez-Guevara</td>
<td>López-Guevara</td>
</tr>
<tr>
<td>09:35 AM</td>
<td>Spotlights 1</td>
<td>Chang, Chorowski, Dirks</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Josh Tenenbaum</td>
<td>Tenenbaum</td>
</tr>
<tr>
<td>11:05 AM</td>
<td>Sanja Fidler</td>
<td>Fidler</td>
</tr>
<tr>
<td>11:40 AM</td>
<td>Spotlights 2</td>
<td>Deng, Crawford</td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Niloy Mitra</td>
<td>Mitra</td>
</tr>
<tr>
<td>02:05 PM</td>
<td>Danilo Rezende</td>
<td>Jimenez Rezende</td>
</tr>
</tbody>
</table>

Minding the Gap: Between Fairness and Ethics

Igor Rubinov, Risi Kondor, Jack Pouls, Manfred K. Warmuth, Emanuel Moss, Alex Hagerty

East Meeting Rooms 8 + 15, Fri Dec 13, 08:00 AM

When researchers and practitioners, as well as policy makers and the public, discuss the impacts of deep learning systems, they draw upon multiple conceptual frames that do not sit easily beside each other. Questions of algorithmic fairness arise from a set of concerns that are similar, but not identical, to those that circulate around AI safety, which in turn overlap with, but are distinct from, the questions that motivate work on AI ethics, and so on. Robust bodies of research on privacy, security, transparency, accountability, interpretability, explainability, and opacity are also incorporated into each of these frames and conversations in variable ways. These frames reveal gaps that persist across both highly technical and socially embedded approaches, and yet collaboration across these gaps has proven challenging.

Fairness, Ethics, and Safety in AI each draw upon different disciplinary prerogatives, variously centering applied mathematics, analytic philosophy, behavioral sciences, legal studies, and the social sciences in ways that make conversation between these frames fraught with misunderstandings. These misunderstandings arise from a high degree of linguistic slippage between different frames, and reveal the epistemic fractures that undermine valuable synergy and productive collaboration. This workshop focuses on ways to translate between these ongoing efforts and bring them into necessary conversation in order to understand the profound impacts of algorithmic systems in society.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
<td>Pouls, Warmuth</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Invited Talk</td>
<td>Bengio</td>
</tr>
<tr>
<td>08:45 AM</td>
<td>Approaches to</td>
<td>Bengio, Dobbe, Elish, Kroll, Mcal, Pouls</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Spectrogram</td>
<td>Moss</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
</tbody>
</table>
Abstract 3: Approaches to Understanding AI in Minding the Gap: Between Fairness and Ethics, Bengio, Dobbe, Elish, Kroll, Metcalf, Poulsom 08:45 AM

The stakes of AI certainly alter how we relate to each other as humans - how we know what we know about reality, how we communicate, how we work and earn money, and about how we think of ourselves as human. But in grappling with these changing relations, three fairly concrete approaches have dominated the conversation: ethics, fairness, and safety. These approaches come from very different academic backgrounds, draw attention to very different aspects of AI, and imagine very different problems and solutions as relevant, leading us to ask:

- What are the commonalities and differences between ethics, fairness, and safety as approaches to addressing the challenges of AI?
- How do these approaches imagine different problems and solutions for the challenges posed by AI?
- How can these approaches work together, or are there some areas where they are mutually incompatible?

Abstract 6: Detecting and Documenting AI Impacts in Minding the Gap: Between Fairness and Ethics, Christian, Hagerty, Rogers, Schuur, Snow, Elish 10:30 AM

Algorithmic systems are being widely used in key social institutions and while they promise radical improvements in fields from public health to energy allocation, they also raise troubling issues of bias, discrimination, and “automated inequality.” They also present irresolvable challenges related to the dual-use nature of these technologies, secondary effects that are difficult to anticipate, and alter power relations between individuals, companies, and governments.

- How should we delimit the scope of AI impacts? What can properly be considered an AI impact, as opposed to an impact arising from some other cause?
- How do we detect and document the social impacts of AI?
- What tools, processes, and institutions ought to be involved in addressing these questions?

Abstract 7: Responsibilities in Minding the Gap: Between Fairness and Ethics, Kim, O’Sullivan, Schuur, Smart, Metcalf 11:30 AM

While there is a great deal of AI research happening in academic settings, much of that work is operationalized within corporate contexts. Some companies serve as vendors, selling AI systems to government entities, some sell to other companies, some sell directly to end-users, and yet others sell to any combination of the above.

- What set of responsibilities does the AI industry have w.r.t. AI impacts?
- What responsibilities does government have to society, with respect to AI impacts arising from industry?
- What role does civil society organizations have to play in this conversation?

Abstract 10: Global Implications in Minding the Gap: Between Fairness and Ethics, Malliaraki, Poulsom, Prabhakaran, Sloane, Hagerty 02:45 PM

The risks and benefits of AI are unevenly distributed within societies and across the globe. Governance regimes are drastically different in various regions of the world, as are the political and ethical implications of AI technologies.

- How do we better understand how AI technologies operate around the world and the range of risks they carry for different societies?
- Are there global claims about the implications of AI that can apply everywhere around the globe? If so, what are they?
- What can we learn from AI’s impacts on labor, environment, public health and agriculture in diverse settings?

Abstract 12: Solutions in Minding the Gap: Between Fairness and Ethics, Christian, Hu, Kondor, Marshall, Rogers, Schuur, Moss 04:30 PM

With the recognition that there are no fully sufficient steps that can be taken to addressing all AI impacts, there are concrete things that ought to be done, ranging across technical, socio-technical, and legal or regulatory possibilities.

- What are the technical, social, and/or regulatory solutions that are necessary to address the riskiest aspects of AI?
- What are key approaches to minimize the risks of AI technologies?
aims at the intersection of these two subfields of AI. It will shine a light on the synergies that (could/should) exist between KRR and ML, and will initiate a discussion about the key challenges in the field.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:05 AM</td>
<td>Invited Talk (William W. Cohen)</td>
</tr>
<tr>
<td>08:35 AM</td>
<td>Contributed Talk: Neural-Guided Symbolic Regression with Asymptotic Constraints</td>
</tr>
<tr>
<td>08:50 AM</td>
<td>Contributed Talk: Towards Finding Longer Proofs</td>
</tr>
<tr>
<td>09:05 AM</td>
<td>Contributed Talk: Neural Markov Logic Networks</td>
</tr>
<tr>
<td>09:20 AM</td>
<td>Poster Spotlights A (23 posters)</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break + Poster Session</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Invited Talk (Xin Luna Dong)</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Contributed Talk: Layerwise Knowledge Extraction from Deep Convolutional Networks</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Contributed Talk: Ontology-based Interpretable Machine Learning with Learnable Anchors</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Contributed Talk: Learning multi-step spatio-temporal reasoning with Selective Attention Memory Network</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Contributed Talk: MARLeME: A Multi-Agent Reinforcement Learning Model Extraction Library</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Invited Talk (Vivek Srikumar)</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch Break</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Contributed Talk: TP-N2F: Tensor Product Representation for Natural To Formal Language Generation</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>Contributed Talk: TabFact: A Large-scale Dataset for Table-based Fact Verification</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Contributed Talk: LeDeepChef: Deep Reinforcement Learning Agent for Families of Text-Based Games</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Poster Spotlights B (13 posters)</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Invited Talk (Yejin Choi)</td>
</tr>
<tr>
<td>04:45 PM</td>
<td>Invited Talk (Guy Van den Broeck)</td>
</tr>
<tr>
<td>05:15 PM</td>
<td>Discussion Panel</td>
</tr>
<tr>
<td>05:55 PM</td>
<td>Closing Remarks</td>
</tr>
</tbody>
</table>

### Retrospectives: A Venue for Self-Reflection in ML Research

Ryan Lowe, Yoshua Bengio, Joelle Pineau, Michela Paganini, Jessica Forde, Shagun Sodhani, Abhishek Gupta, Joel Lehman, Peter Henderson, Kanika Madan, Koustuv Sinha, Xavier Bouthillier

West 114 + 115, Fri Dec 13, 08:00 AM

The NeurIPS Workshop on Retrospectives in Machine Learning will kick-start the exploration of a new kind of scientific publication, called retrospectives. The purpose of a retrospective is to answer the question:

“What should readers of this paper know now, that is not in the original publication?”

Retrospectives provide a venue for authors to reflect on their previous publications, to talk about how their intuitions have changed, to identify shortcomings in their analysis or results, and to discuss resulting extensions that may not be sufficient for a full follow-up paper. A retrospective is written about a single paper, by that paper’s author, and takes the form of an informal paper. The overarching goal of retrospectives is to improve the science, openness, and accessibility of the machine learning field, by widening what is publishable and helping to identifying opportunities for improvement. Retrospectives will also give researchers and practitioners who are unable to attend top conferences access to the author’s updated understanding of their work, which would otherwise only be accessible to their immediate circle.
Schedule

09:00 AM  Opening Remarks
09:10 AM  Invited talk: Leon Bottou
09:30 AM  Invited talk: Melanie Mitchell, "Active Symbols and Analogy-Making: Reflections on Hofstadter & Mitchell's Copycat project"
09:50 AM  Invited talk: Zach Lipton, "Fairness & Interpretability in Machine Learning and the Dangers of Solutionism"
10:10 AM  Coffee break + poster set-up
10:25 AM  Contributed talk: Juergen Schmidhuber, "Unsupervised minimax"
10:35 AM  Contributed talk: Prabhu Pradhan, "Smarter prototyping for neural learning"
10:45 AM  Contributed talk: Andre Pacheco, "Recent advances in deep learning applied for skin cancer detection"
10:55 AM  Invited talk: Veronika Cheplygina, "How I Fail in Writing Papers"
12:15 PM  Lunch break
01:45 PM  Invited talk: Emily Denton
02:05 PM  Invited talk: Percy Liang
02:25 PM  Retrospectives lightning talks
03:00 PM  Posters + Coffee Break
04:00 PM  Invited talk: David Duvenaud, "Reflecting on Neural ODEs"
04:20 PM  Invited talk: Michael Littman, "Reflecting on 'Markov games that people play'"
04:40 PM  Retrospectives brainstorming session: how do we produce impact?

Abstracts (4):


In our 1995 paper “The Copycat Project: A Model of Mental Fluidity and Analogy-Making”, Douglas Hofstadter and I described Copycat, a computer program that makes analogies in an idealized domain of letter strings. The goal of the project was to model the general-purpose ability of humans to fluidly perceive abstract similarities between situations. Copycat's active symbol architecture, inspired by human perception, was a unique combination of symbolic and subsymbolic components. Now, 25 years later, AI is refocusing on abstraction and analogy as core aspects of robust intelligence, and the ideas underlying Copycat have new relevance. In this talk I will reflect on these ideas, on the limitations of Copycat and its idealized domain, and on possible novel contributions of this decades-old work to current open problems in AI.

Abstract 4: Invited talk: Zach Lipton, "Fairness & Interpretability in Machine Learning and the Dangers of Solutionism" in Retrospectives: A Venue for Self-Reflection in ML Research, 09:50 AM

Supervised learning algorithms are increasingly operationalized in real-world decision-making systems. Unfortunately, the nature and desiderata of real-world tasks rarely fit neatly into the supervised learning contract. Real data deviates from the training distribution, training targets are often weak surrogates for real-world desiderata, error is seldom the right utility function, and while the framework ignores interventions, predictions typically drive decisions. While the deep questions concerning the ethics of AI necessarily address the processes that generate our data and the impacts that automated decisions will have, neither ML tools, nor proposed ML-based solutions tackle these problems head on. This talk explores the consequences and limitations of employing ML-based technology in the real world, the limitations of recent solutions (so-called fair and interpretable algorithms) for mitigating societal harms, and contemplates the meta-question: when should (today’s) ML systems be off the table altogether?


Some of the questions that will be discussed: (1) how can we encourage researchers to share their real thoughts and feelings about their work? and (2) how can we improve the dissemination of ‘soft knowledge’ in the field?

Abstract 14: Retrospectives lightning talks in Retrospectives, 02:25 PM

Lightning talks:
An Intriguing Failing of Convolutional Neural Networks and the CoordConv Solution (Rosanne Liu)
Learning the structure of deep sparse graphical models (Zoubin Ghahramani)
Lessons Learned from The Lottery Ticket Hypothesis (Jonathan Frankle)
FiLM: Visual Reasoning with a General Conditioning Layer (Ethan Perez)
Conditional computation in neural networks for faster models (Emmanuel Bengio)

**Competition Track Day 1**

**Hugo Jair Escalante**

West 116 + 117, Fri Dec 13, 08:00 AM

https://nips.cc/Conferences/2019/CallForCompetitions

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:10 AM</td>
<td><strong>Disentanglement Challenge - Disentanglement and Results of the Challenge Stages 1 &amp; 2</strong></td>
<td>Miladinovic, Bauer, Keysers</td>
</tr>
<tr>
<td>08:40 AM</td>
<td><strong>Robot open-Ended Autonomous Learning: a challenge</strong></td>
<td>Cartoni, Baldassarre</td>
</tr>
<tr>
<td>09:00 AM</td>
<td><strong>The Pommerman competition</strong></td>
<td>Resnick, Bouhenguel, Görög, Zhang, Jasek</td>
</tr>
<tr>
<td>09:30 AM</td>
<td><strong>The CellSignal challenge</strong></td>
<td>Mabey, Sypetkowski, Haque, Earnshaw, Shen, Goldbloom</td>
</tr>
<tr>
<td>10:00 AM</td>
<td><strong>Learn to Move: Walk Around</strong></td>
<td>Song, Kidzinski, Peng, Zhou, Kolesnikov, Wang, Akimov, Zubkov, Zeng</td>
</tr>
<tr>
<td>10:30 AM</td>
<td><strong>Coffee break</strong></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td><strong>AI Driving Olympics 3</strong></td>
<td>Dicle, Paull, Tani, Mallya, Genc, Bowser, Sun, Tao, Marcotte, Chiu, Wolff</td>
</tr>
<tr>
<td>01:00 PM</td>
<td><strong>Lunch break</strong></td>
<td></td>
</tr>
<tr>
<td>02:15 PM</td>
<td><strong>MicroNet Challenge</strong></td>
<td>Wang, Leng, Cheng, Yan, Wang, Gale, Eisen</td>
</tr>
<tr>
<td>03:15 PM</td>
<td><strong>Reconnaissance Blind Chess competition</strong></td>
<td>Llorens, Gardner, Perrotta, Highley, Clark, Perrotta, Bernardoni, Jordan, Wang, Peng</td>
</tr>
<tr>
<td>04:15 PM</td>
<td><strong>The 3D Object Detection over HD Maps for Autonomous Cars Challenge</strong></td>
<td>Vincent, Jain, Zhang, Addicam, Iglovikov, Ondruska, MURAMATSU</td>
</tr>
</tbody>
</table>

**Abstracts (4):**

**Abstract 1:** **Disentanglement Challenge - Disentanglement and Results of the Challenge Stages 1 & 2 in Competition Track Day 1.**

*Miladinovic, Bauer, Keysers 08:10 AM*

Stefan Bauer: Learning Disentangled Representations
Djordje Miladinovic: Disentanglement in the Real-World
Daniel Keysers: Disentanglement, lib
Bernhard Schölkopf: Hand-out-of-certificates

**Abstract 4:** **The CellSignal challenge in Competition Track Day 1.**

*Mabey, Sypetkowski, Haque, Earnshaw, Shen, Goldbloom 09:30 AM*

* Opening remarks, description of competition, summary of results.
* Description of first prize solution.
* Description of second prize solution.
* Mention of third prize solution
* Congratulations to winners and description of AutoML solution.
* Prize ceremony.

**Abstract 9:** **MicroNet Challenge in Competition Track Day 1.**

*Wang, Leng, Cheng, Yan, Wang, Gale, Elsen 02:15 PM*

Trevor Gale and Erich Elsen. Introduction to the competition and overview of results.
Peisong Wang, Cong Leng, and Jian Cheng. An Empirical Study of Network Compression for Image Classification.

**Abstract 10:** **Reconnaissance Blind Chess competition in Competition Track Day 1.**

*Llorens, Gardner, Perrotta, Highley, Clark, Perrotta, Bernardoni, Jordan, Wang, Peng 03:15 PM*

* Chair: i-Jeng Wang
* Competition and Game Overview (Ashley Llorens)
* Challenges of the Game (Ryan Gardner)
* Competition Results (Casey Richardson)
* Overview of the StrangeFish Bot (Gino Perrotta and Robert Perrotta)
* Overview of the LaSalle Bot (T.J. Highley)
* Overview of the penumbra Bot (Gregory Clark)
* Overview of the wbernar5 Bot (William Bernardoni)
* Overview of the MBot Bot (Mark Jordan)

**Workshop on Federated Learning for Data Privacy and Confidentiality**

*Lixin Fan, Jakub Konečný, Yang Liu, Brendan McMahan, Virginia Smith, Han Yu*

West 118 - 120, Fri Dec 13, 08:00 AM
Overview

Privacy and security have become critical concerns in recent years, particularly as companies and organizations increasingly collect detailed information about their products and users. This information can enable machine learning methods that produce better products. However, it also has the potential to allow for misuse, especially when private data about individuals is involved. Recent research shows that privacy and utility do not necessarily need to be at odds, but can be addressed by careful design and analysis. The need for such research is reinforced by the recent introduction of new legal constraints, led by the European Union’s General Data Protection Regulation (GDPR), which is already inspiring novel legislative approaches around the world such as Cyber-security Law of the People’s Republic of China and The California Consumer Privacy Act of 2018.

An approach that has the potential to address a number of problems in this space is federated learning (FL). FL is an ML setting where many clients (e.g., mobile devices or whole organizations) collaboratively train a model under the orchestration of a central server (e.g., service provider), while keeping the training data decentralized. Organizations and mobile devices have access to increasing amounts of sensitive data, with scrutiny of ML privacy and data handling practices increasing correspondingly. These trends have produced significant interest in FL, since it provides a viable path to state-of-the-art ML without the need for the centralized collection of training data – and the risks and responsibilities that come with such centralization. Nevertheless, significant challenges remain open in the FL setting, the solution of which will require novel techniques from multiple fields, as well as improved open-source tooling for both FL research and real-world deployment.

This workshop aims to bring together academic researchers and industry practitioners with common interests in this domain. For industry participants, we intend to create a forum to communicate what kind of problems are practically relevant. For academic participants, we hope to make it easier to become productive in this area. Overall, the workshop will provide an opportunity to share the most recent and innovative work in FL, and discuss open problems and relevant approaches. The technical issues encouraged to be submitted include general computation based on decentralized data (i.e., not only machine learning), and how such computations can be combined with other research areas, such as differential privacy, secure multi-party computation, computational efficiency, coding theory, etc. Contributions in theory as well as applications are welcome, including proposals for novel system design. Work on fully-decentralized (peer-to-peer) learning will also be considered, as there is significant overlap in both interest and techniques with federated learning.

Call for Contributions
We welcome high-quality submissions in the broad area of federated learning (FL). A few (non-exhaustive) topics of interest include:

- Optimization algorithms for FL, particularly communication-efficient algorithms tolerant of non-IID data
- Approaches that scale FL to larger models, including model and gradient compression techniques
- Novel applications of FL
- Theory for FL
- Approaches to enhancing the security and privacy of FL, including cryptographic techniques and differential privacy
- Bias and fairness in the FL setting
- Attacks on FL including model poisoning, and corresponding defenses
- Incentive mechanisms for FL
- Software and systems for FL
- Novel applications of techniques from other fields to the FL setting: information theory, multi-task learning, model-agnostic meta-learning, and etc.
- Work on fully-decentralized (peer-to-peer) learning will also be considered, as there is significant overlap in both interest and techniques with FL.

Submissions in the form of extended abstracts must be at most 4 pages long (not including references), be anonymized, and adhere to the NeurIPS 2019 format. Submissions will be accepted as contributed talks or poster presentations. The workshop will not have formal proceedings, but accepted papers will be posted on the workshop website.

We support reproducible research and will sponsor a prize to be given to the best contribution that provides code to reproduce their results.

Submission link: https://easychair.org/conferences/?conf=flneurips2019

Important Dates (2019)
Submission deadline: Sep 9
Author notification: Sep 30
Camera-Ready Papers Due: TBD
Workshop: Dec 13

Organizers:
Lixin Fan, WeBank
Jakub Konečný, Google
Yang Liu, WeBank
Brendan McMahan, Google
Virginia Smith, CMU
Han Yu, NTU

Invited Speakers:
Francoise Beaufays, Principal Researcher, Google
Shahrok Dajavat, Distinguished Research, IBM
Dawn Song, Professor, University of California, Berkeley
Ameet Talwalkar, Assistant Professor, CMU; Chief Scientist, Determined AI
Max Welling, Professor, University of Amsterdam; VP Technologies, Qualcomm
Qiang Yang, Hong Kong University of Science and Technology, Hong Kong; Chief AI Officer, WeBank

FAQ
Can supplementary material be added beyond the 4-page limit and are there any restrictions on it?
Yes, you may include additional supplementary material, but you should ensure that the main paper is self-contained, since looking at supplementary material is at the discretion of the reviewers. The supplementary material should also follow the same NeurIPS format as the paper and be limited to a reasonable amount (max 10 pages in addition to the main submission).
Can a submission to this workshop be submitted to another NeurIPS workshop in parallel?
We discourage this, as it leads to more work for reviewers across multiple workshops. Our suggestion is to pick one workshop to submit to. Can a paper be submitted to the workshop that has already appeared at a previous conference with published proceedings?
We won’t be accepting such submissions unless they have been
adapted to contain significantly new results (where novelty is one of the qualities reviewers will be asked to evaluate).

Can a paper be submitted to the workshop that is currently under review or will be under review at a conference during the review phase? It is fine to submit a condensed version (i.e., 4 pages) of a parallel conference submission, if it also fine for the conference in question. Our workshop does not have archival proceedings, and therefore parallel submissions of extended versions to other conferences are acceptable.

 Accepted papers:
2. Xin Yao, Tianchi Huang, Rui-Xiao Zhang, Ruiyu Li and Lifeng Sun. Federated Learning with Unbiased Gradient Aggregation and Controllable Meta Updating
3. Daniel Peterson, Pallika Kanani and Virendra Marathe. Private Federated Learning with Domain Adaptation
4. Daliang Li and Junpu Wang. FedMD: Heterogeneous Federated Learning via Model Distillation
5. Sebastian Caldas, Jakub Konečný, H. Brendan McMahan and Ameet Talwalkar. Mitigating the Impact of Federated Learning on Client Resources
7. Sebastian Caldas, Sai Meher Karthik Duddu, Peter Wu, Tian Li, Jakub Konečný, H. Brendan McMahan, Virginia Smith and Ameet Talwalkar. Leaf. A Benchmark for Federated Settings
13. Yang Liu, Xiong Zhang, Shuqi Qin and Xiaoping Lei. Differentially Private Linear Regression over Fully Decentralized Datasets
14. Florian Hartmann, Sunah Suh, Arkadiusz Komarzewski, Tim D. Smith and Ilana Segall. Federated Learning for Ranking Browser History Suggestions
15. Aleksei Triastcyn and Boi Faltings. Federated Learning with Bayesian Differential Privacy
18. Mingshu Cong, Zhongming Ou, Yanxin Zhang, Han Yu, Xi Weng, Jiabo Qu, Siu Ming Yu, Yang Liu and Qiang Yang. Neural Network Optimization for a VCG-based Federated Learning Incentive Mechanism
20. Suyi Li, Yong Cheng, Yang Liu and Wei Wang. Abnormal Client Behavior Detection in Federated Learning
22. Shicong Cen, Huihuai Zhang, Yuejie Chi, Wei Chen and Tie-Yan Liu. Convergence and Regularization of Distributed Stochastic Variance Reduced Methods
23. Zhaorui Li, Zhicong Huang, Chaochao Chen and Cheng Hong. Quantification of the Leakage in Federated Learning
25. Boyue Li, Shicong Cen, Yuxin Chen and Yuejie Chi. Communication-Efficient Distributed Optimization in Networks with Gradient Tracking
27. Felix Sattler, Klaus-Robert Müller and Wojciech Samek. Clustered Federated Learning
28. Ziteng Sun, Peter Kairouz, Ananda Theertha Suresh and Brendan McMahan. Backdoor Attacks on Federated Learning and Corresponding Defenses
29. Neta Shoham, Tomer Avidor, Aviv Keren, Nadav Israel, Daniel BentSitik, Liron Mor-Yosef and Itai Zeilack. Overcoming Forgetting in Federated Learning on Non-IID Data
30. Ahmed Khaled and Peter Richtárik. Gradient Descent with Compressed Iterates
31. Jiahuan Luo, Xueyang Wu, Yun Luo, Anbu Huang, Yunfeng Huang, Yang Liu and Qiang Yang. Real-World Image Datasets for Federated Learning
32. Ahmed Khaled, Konstantin Mishchenko and Peter Richtárik. First
Analysis of Local GD on Heterogeneous Data

33. Dashan Gao, Ce Ju, Xiguang Wei, Yang Liu, Tianjian Chen and Qiang Yang. HHHFL: Hierarchical Heterogeneous Horizontal Federated Learning for Electroencephalography

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:55 AM</td>
<td>Opening remarks</td>
<td>Fan</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Federated Learning for Recommendation Systems</td>
<td>Yang</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>TBD</td>
<td>Talwalkar</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Coffee break and posters</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>TBD</td>
<td>Welling</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>TBD</td>
<td>Song</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Think Locally, Act Globally: Federated Learning with Local and Global Representations</td>
<td></td>
</tr>
<tr>
<td>11:40 AM</td>
<td>FedMD: Heterogenous Federated Learning via Model Distillation</td>
<td></td>
</tr>
<tr>
<td>11:50 AM</td>
<td>Private Federated Learning with Domain Adaptation</td>
<td></td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Improving Federated Learning Personalization via Model Agnostic Meta Learning</td>
<td>Sattler, El Mekkoui, Shoham, Hong, Hartmann, Li, Li, Caltas Rivera, Wang, Bhardwaj, Orekony, KANG, Gao, Cong, Yao, Lu, LUO, Cen, Kairouz, Jiang, Hsu, Triastcyn, Liu, Khaled Ragab Bayoumi, Liang, Failings, Moon, Li, Fan, Huang, Miao, Qi, Brown, Glass, Wang, Chen, Marculescu, avidor, Wu, Hong, Ju, Rush, Zhang, ZOU, Beaufays, Zhu, Xia</td>
</tr>
<tr>
<td>12:10 PM</td>
<td>Lunch break and poster</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>TBD</td>
<td>Ramage</td>
</tr>
<tr>
<td>02:20 PM</td>
<td>TBD</td>
<td>Beaufays</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>MATCHA: Speeding Up Decentralized SGD via Matching Decomposition Sampling</td>
<td></td>
</tr>
<tr>
<td>02:40 PM</td>
<td>Mitigating the Impact of Federated Learning on Client Resources</td>
<td></td>
</tr>
</tbody>
</table>

Machine Learning for the Developing World (ML4D): Challenges and Risks

Maria De-Arteaga, Amanda Coston, Tejumade Afonja

West 121 + 122, Fri Dec 13, 08:00 AM

As the use of machine learning becomes ubiquitous, there is growing interest in understanding how machine learning can be used to tackle global development challenges. The possibilities are vast, and it is important that we explore the potential benefits of such technologies, which has driven the agenda of the ML4D workshop in the past. However, there is a risk that technology optimism and a categorization of ML4D research as inherently “social good” may result in initiatives failing to account for unintended harms or deviating scarce funds towards initiatives that appear exciting but have no demonstrated effect. Machine learning technologies deployed in developing regions have often been created for different contexts and are trained with data that is not representative of the new deployment setting. Most concerning of all, companies sometimes make the deliberate choice to deploy new technologies in countries with little regulation in order to experiment.

This year’s program will focus on the challenges and risks that arise when deploying machine learning in developing regions. This one-day workshop will bring together a diverse set of participants from across the globe to discuss essential elements for ensuring ML4D research moves...
forward in a responsible and ethical manner. Attendees will learn about potential unintended harms that may result from ML4D solutions, technical challenges that currently prevent the effective use of machine learning in vast regions of the world, and lessons that may be learned from other fields.

The workshop will include invited talks, a poster session of accepted papers and panel discussions. We welcome paper submissions featuring novel machine learning research that characterizes or tackles challenges of ML4D, empirical papers that reveal unintended harms of machine learning technology in developing regions, and discussion papers that examine the current state of the art of ML4D and propose paths forward.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:45 AM</td>
<td>AI's Blindspots and Where to Find Them</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Algorithmic Colonization</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Lessons from ICTD -- Information &amp; Communication Tech</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Poster session</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Data sharing in and for Africa</td>
</tr>
<tr>
<td>02:15 PM</td>
<td>Risks of Using Non-verified Open Data: A case study on using Machine Learning techniques for predicting Pregnancy Outcomes in India</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>A Noxious Market for Personal Data</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>HumBug Zooniverse: a crowdsourced acoustic mosquito dataset</td>
</tr>
</tbody>
</table>

Abstracts (7):

Abstract 2: AI's Blindspots and Where to Find Them in Machine Learning for the Developing World (ML4D): Challenges and Risks, Raji 08:45 AM

When we deploy machine learning models, what are the known scenarios in which the technology does not work? In this talk, we will go over the many potential blindspots in ML deployments, and how, as a fundamentally narrow and limited technology, we need to be careful to communicate, evaluate for and directly address these risks in a way that protects users and reinforces developer accountability.


As algorithmic systems become an ever more integral aspect of much of the social sphere, their application for “social good” has also increased. Western-made AI is deployed throughout the African continent with great enthusiasm and little regulation or critical engagement, in a manner that resembles past colonial conquests. This talk explores some of the critical and ethical questions that need to be raised with the “digitization” of the African continent and the use of AI for “social good”.


Since the turn of the millennium, the interdisciplinary field of information & communication technologies and development (ICTD) has explored how digital technologies could contribute to international socio-economic development. The associated research community includes both techno-utopians who imagine that just about any problem can be solved with the right application of technology, as well as extreme skeptics wary of any attempts at intervention. Debates continue, but in this talk, I will attempt to summarize some of the expressed consensus in ICTD -- things that not everyone necessarily believes, but will at least pay lip service to. I will also discuss what I call technology’s “Law of Amplification,” which reconciles some of the differing opinions in ICTD and also offers guidance for how machine learning can have real-world impact.
Abstract 8: Data sharing in and for Africa in Machine Learning for the Developing World (ML4D): Challenges and Risks, Remy 02:00 PM

Data accessibility, including the ability to make data shareable, is important for knowledge creation, scientific learning, and progress. In many locations, including Africa, data is a central engine for economic growth and there have been recent calls to increase data access and shareability by organizations including the UN, AU, and many others. Discussions around data inaccessibility, however, revolve around lack of resources, human capital, and advanced technologies, hiding the complex and dynamic data ecosystem and intricate challenges faced in sharing data across the continent. In this piece, we shed light on these overlooked issues around data inaccessibility and sharing within the continent using a storytelling perspective. Using the perspectives of multiple stakeholders, we surface tensions and trade-offs that are that are inadequately captured in current discussions around data accessibility in the continent.


While applications of AI are now becoming more common in fields like retail and marketing, application of AI in solving problems related to developing countries is still an emerging topic. Specially, AI applications in resource-poor settings remains relatively nascent. There is a huge scope of AI being used in such settings. For example, researchers have started exploring AI applications to reduce poverty and deliver a broad range of critical public services. However, despite many promising use cases, there are many dataset related challenges that one has to overcome in such projects. These challenges often take the form of missing data, incorrectly collected data and improperly labeled variables, among other factors. As a result, we can often end up using data that is not representative of the problem we are trying to solve. In this case study, we explore the challenges of using such an open dataset from India, to predict an important health outcome. We highlight how the use of AI without proper understanding of reporting metrics can lead to erroneous conclusions.

Abstract 10: A Noxious Market for Personal Data in Machine Learning for the Developing World (ML4D): Challenges and Risks, Abdurahim 02:30 PM

Many policymakers, academics and governments have advocated for exchangeable property rights over information as it presents a market solution to what could be considered a market failure. Particularly in jurisdictions such as Africa, Asia or South America, where weaker legal protections and fleeting regulatory enforcement leaves data subjects vulnerable or exploited regardless of the outcome. We argue that whether we could achieve this personal data economy in which individuals have ownership rights akin to property rights over their data should be approached with caution as a solution to ensuring individuals have agency over their data across different legal landscapes.

We present an objection to the use of property rights, a market solution, due to the noxious nature of personal data - which is founded on Satz and Sandell's objection to markets. Ultimately, our rights over personal data and privacy are borne out of our basic human rights and are a precondition for the self-development, personal fulfillment and the free enjoyment of other fundamental human rights - and putting it up for sale risks corrupting its essence and value.

Abstract 12: Mathematics of identity at trial: Digital ID at the constitutional court in Kenya in Machine Learning for the Developing World (ML4D): Challenges and Risks, Mutungu 03:00 PM

In September and October 2019, a three judge bench in Kenya heard a case protesting digital ID. The case arose after the state rolled out a mandatory digital ID system, known as Huduma Namba that would be a prerequisite for access to government services. Being a constitutional case, arguments on human rights such as privacy were expected. However, the state framed its case of digital ID as inevitable technological development and those opposed to the advancement as being fearful of technology. To understand whether there were human rights implications with the digital ID, parties had to explain about the technology choices taken, the data practices and parties involved in the project. Hence the court (and public at large) spent a significant amount of time getting to understand multi-modal deduplication. While judgement on the case is yet to be delivered, the case brings to fore the societal implications of technology. It also calls for dialogue between technologists and sociologists in design and execution of projects aimed at low and middle income countries.

Visually Grounded Interaction and Language

Florian Strub, Abhishek Das, Erik Wijmans, Harm de Vries, Stefan Lee, Alane Suhr, Drew Arad Hudson

West 202 - 204, Fri Dec 13, 08:00 AM

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, this approach suffers from limited semantic understanding -- symbols learned this way lack any concrete groundings into the multimodal, interactive environment in which communication takes place. The symbol grounding problem first highlighted this limitation, that “meaningless symbols (i.e. words) cannot be grounded in anything but other meaningless symbols”.

On the other hand, humans acquire language by communicating about and interacting within a rich, perceptual environment -- providing concrete groundings, e.g. to objects or concepts either physical or psychological. Thus, recent works have aimed to bridge computer vision, interactive learning, and natural language understanding through language learning tasks based on natural images or through embodied agents performing interactive tasks in physically simulated environments, often drawing on the recent successes of deep learning and reinforcement learning. We believe these lines of research pose a promising approach for building models that do grasp the world’s underlying complexity.

The goal of this third ViGiL workshop is to bring together scientists from various backgrounds - machine learning, computer vision, natural language processing, neuroscience, cognitive science, psychology, and philosophy - to share their perspectives on grounding, embodiment, and interaction. By providing this opportunity for cross-discipline discussion, we hope to foster new ideas about how to learn and leverage grounding in machines as well as build new bridges between the science of human
cognition and machine learning.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:20 AM</td>
<td>Opening Remarks</td>
<td>Strub, de Vries, Das, Lee, Wijmans, Arad Hudson, Suhr</td>
</tr>
<tr>
<td>08:30 AM</td>
<td>Grasping Language</td>
<td>Baldridge</td>
</tr>
<tr>
<td>09:10 AM</td>
<td>From Human Language to Agent Action</td>
<td>Thomason</td>
</tr>
<tr>
<td>09:50 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Spotlight</td>
<td></td>
</tr>
<tr>
<td>10:50 AM</td>
<td>Why language understanding is not a solved problem</td>
<td>McClelland</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Louis-Philippe Morency</td>
<td>Morency</td>
</tr>
<tr>
<td>12:10 PM</td>
<td>Poster session</td>
<td>Ross, Mrabet, Subramanian, Cideron, Mu, Bhoshan, Okur Kavil, Delbrouck, Kuo, Lair, Ilharco, Jayram, Herrera Palacio, Fujiyama, Tielman, Potapenko, Chao, Sutter, Kovaleva, Lai, Wang, Sharma, Cangea, Krishnaswamy, Tsuboi, Kuhnle, Nguyen, Yu, Saha, Xiang, Venkataraman, Kalra, Xie, Doran, Goodwin, Kadav, Daghaghi, Baldridge, Wu, Lin, Jain</td>
</tr>
<tr>
<td>01:50 PM</td>
<td>Lisa Anne Hendricks</td>
<td>Hendricks</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Linda Smith</td>
<td>Smith</td>
</tr>
<tr>
<td>03:10 PM</td>
<td>Poster Session</td>
<td></td>
</tr>
<tr>
<td>04:00 PM</td>
<td>Timothy Lillicrap</td>
<td>Lillicrap</td>
</tr>
<tr>
<td>04:40 PM</td>
<td>Josh Tenenbaum</td>
<td>Tenenbaum</td>
</tr>
<tr>
<td>05:20 PM</td>
<td>Panel Discussion</td>
<td>Smith, Tenenbaum, Hendricks, McClelland, Lillicrap, Thomason, Baldridge, Morency</td>
</tr>
<tr>
<td>06:00 PM</td>
<td>Closing Remarks</td>
<td></td>
</tr>
</tbody>
</table>

### Abstracts (7):

**Abstract 2: Grasping Language in Visually Grounded Interaction and Language, Baldridge 08:30 AM**

There is a usability gap between manipulation-capable robots and helpful in-home digital agents. Dialog-enabled smart assistants have recently seen widespread adoption, but these cannot move or manipulate objects. By contrast, manipulation-capable and mobile robots are still largely deployed in industrial settings and do not interact with human users. Language-enabled robots can bridge this gap—natural language interfaces help robots and non-experts collaborate to achieve their goals.

Navigation in unexplored environments to high-level targets like “Go to the room with a plant” can be facilitated by enabling agents to ask questions and react to human clarifications on-the-fly. Further, high-level instructions like “Put a plate of toast on the table” require inferring many steps, from finding a knife to operating a toaster. Low-level instructions can serve to clarify these individual steps. Through two new datasets and accompanying models, we study human-human dialog for cooperative navigation, and high- and low-level language instructions for cooking, cleaning, and tidying in interactive home environments. These datasets are a first step towards collaborative, dialog-enabled robots helpful in human spaces.

**Abstract 3: From Human Language to Agent Action in Visually Grounded Interaction and Language, Thomason 09:10 AM**

There is a usability gap between manipulation-capable robots and helpful in-home digital agents. Dialog-enabled smart assistants have recently seen widespread adoption, but these cannot move or manipulate objects. By contrast, manipulation-capable and mobile robots are still largely deployed in industrial settings and do not interact with human users. Language-enabled robots can bridge this gap—natural language interfaces help robots and non-experts collaborate to achieve their goals.

**Abstract 6: Why language understanding is not a solved problem in Visually Grounded Interaction and Language, McClelland 10:50 AM**

Over the years, periods of intense excitement about the prospects of machine intelligence and language understanding have alternated with periods of skepticism, to say the least. It is possible to look back over the ~70 year history of this effort and see great progress, and I for one am pleased to see how far we have come. Yet from where I sit we still have a long way to go, and language understanding may be one of those parts of intelligence that will be the hardest to solve. In spite of recent breakthroughs, humans create and comprehend more structured discourse than our current machines. At the same time, psycholinguistic research suggests that humans suffer from some of the same limitations as these machines. How can humans create and comprehend structured arguments given these limitations? Will it be possible for machines to emulate these aspects of human achievement as well?

**Abstract 7: Louis-Philippe Morency in Visually Grounded Interaction and Language, Morency 11:30 AM**

Note that the schedule is not final, and may change.

**Abstract 9: Lisa Anne Hendricks in Visually Grounded Interaction and Language, Hendricks 01:50 PM**

Note that the schedule is not final, and may change.
Robust AI in Financial Services: Data, Fairness, Explainability, Trustworthiness, and Privacy

Alina Oprea, Avigdor Gal, Isabelle Moulinier, Jiahao Chen, Manuela Veloso, Senthil Kumar, Tanveer Faruquie

West 205 - 207, Fri Dec 13, 08:00 AM

The financial services industry has unique needs for robustness when adopting artificial intelligence and machine learning (AI/ML). Many challenges can be described as intricate relationships between algorithmic fairness, explainability, privacy, data management, and trustworthiness. 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 does not cause humans to miss critical pieces of data. The use and protection of customer data necessitates secure and privacy-aware computation, as well as explainability around the use of sensitive data. 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, resulting in large-scale data breaches and loss of confidential information in the financial industry. The need to counteract malicious actors therefore calls for robust methods that can tolerate noise and adversarial corruption of data. However, recent advances in adversarial attacks of AI/ML systems demonstrate how often generic solutions for robustness and security fail, thus highlighting the need for further advances. The challenge of robust AI/ML is further complicated by constraints on data privacy and fairness, as imposed by ethical and regulatory concerns like GDPR.

This workshop aims to bring together researchers and practitioners to discuss challenges for AI/ML in financial services, and the opportunities such challenges represent to research communities. The workshop will consist of invited talks, panel discussions and short paper presentations, which will showcase ongoing research and novel algorithms resulting from collaboration of AI/ML and cybersecurity communities, as well as the challenges that arise from applying these ideas in domain-specific contexts.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Authors/Contributors</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
<td>Chen, Veloso, Kumar, Moulinier, Gal, Oprea, Faruquie, Kurshan</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>In search of predictability</td>
<td>Perlich</td>
</tr>
<tr>
<td>08:45 AM</td>
<td>Oral highlight presentations for selected contributed papers (10 min x 3)</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Invited Talk by Louiqa Raschid (University of Maryland)</td>
<td>Raschid</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Oral highlight presentations for selected contributed papers (10 min x 6)</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Understanding equilibrium properties of multi-agent systems</td>
<td>Wooldridge</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Oral highlight presentations for selected contributed papers (10 min x 6)</td>
<td></td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Discussion Panel</td>
<td>Veloso</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Putting Ethical AI to the Vote</td>
<td>Procaccia</td>
</tr>
<tr>
<td>05:15 PM</td>
<td>Invited Talk by Yuan (Alan) Qi (Ant Financial)</td>
<td>Qi</td>
</tr>
<tr>
<td>05:45 PM</td>
<td>Closing remarks</td>
<td>Kumar</td>
</tr>
</tbody>
</table>

Learning with Rich Experience: Integration of Learning Paradigms

Zhiting Hu, Andrew Wilson, Chelsea Finn, Lisa Lee, Taylor Berg-Kirkpatrick, Ruslan Salakhutdinov, Eric Xing
Machine learning is about computational methods that enable machines to learn concepts and improve performance from experience. Here, experience can take diverse forms, including data examples, abstract knowledge, interactions and feedback from the environment, other models, and so forth. Depending on different assumptions on the types and amount of experience available there are different learning paradigms, such as supervised learning, active learning, reinforcement learning, knowledge distillation, adversarial learning, and combinations thereof. On the other hand, a hallmark of human intelligence is the ability to learn from all sources of information. In this workshop, we aim to explore various aspects of learning paradigms, particularly theoretical properties and formal connections between them, and new algorithms combining multiple modes of supervisions, etc.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:40 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:50 AM</td>
<td>Lightning Talks - I</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Raia Hadsell</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Tom Mitchell</td>
</tr>
<tr>
<td>11:05 AM</td>
<td>Jeffrey Bilmes</td>
</tr>
<tr>
<td>11:40 AM</td>
<td>Lightning Talks - II</td>
</tr>
<tr>
<td>11:55 AM</td>
<td>Poster Session</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch</td>
</tr>
<tr>
<td>02:10 PM</td>
<td>Contributed Oral</td>
</tr>
<tr>
<td>02:20 PM</td>
<td>Pieter Abbeel</td>
</tr>
<tr>
<td>02:55 PM</td>
<td>Yejin Choi</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>04:20 PM</td>
<td>Tom Griffiths</td>
</tr>
<tr>
<td>04:55 PM</td>
<td>Contributed Oral</td>
</tr>
<tr>
<td>05:05 PM</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>05:50 PM</td>
<td>Closing Remarks</td>
</tr>
</tbody>
</table>

Beyond first order methods in machine learning systems

**Anastasios Kyrillidis, Albert Berahas, Fred Roosta, Michael W Mahoney**

**West 211 - 214, Fri Dec 13, 08:00 AM**

Optimization lies at the heart of many exciting developments in machine learning, statistics and signal processing. As models become more complex and datasets get larger, finding efficient, reliable and provable methods is one of the primary goals in these fields.

In the last few decades, much effort has been devoted to the development of first-order methods. These methods enjoy a low per-iteration cost and have optimal complexity, are easy to implement, and have proven to be effective for most machine learning applications. First-order methods, however, have significant limitations: (1) they require fine hyper-parameter tuning, (2) they do not incorporate curvature information, and thus are sensitive to ill-conditioning, and (3) they are often unable to fully exploit the power of distributed computing architectures.

Higher-order methods, such as Newton, quasi-Newton and adaptive gradient descent methods, are extensively used in many scientific and engineering domains. At least in theory, these methods possess several nice features: they exploit local curvature information to mitigate the effects of ill-conditioning, they avoid or diminish the need for hyper-parameter tuning, and they have enough concurrency to take advantage of distributed computing environments. Researchers have even developed stochastic versions of higher-order methods, that feature speed and scalability by incorporating curvature information in an economical and judicious manner. However, often higher-order methods are “undervalued.”

This workshop will attempt to shed light on this statement. Topics of interest include --but are not limited to-- second-order methods, adaptive gradient descent methods, regularization techniques, as well as techniques based on higher-order derivatives.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:30 AM</td>
<td>Economical use of second-order information in training machine learning models</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Spotlight talks</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Poster Session</td>
</tr>
</tbody>
</table>
How does mini-batching affect curvature information for second order deep learning optimization? Diego Granziol (Oxford); Stephen Roberts (Oxford); Xingchen Wan (Oxford University); Stefano Zanette (University of Oxford); Binxin Ru (University of Oxford); Michael A. Osborne (University of Oxford); Andrew Wilson (NYU); Sebastien Ehrhardt (Oxford); Dmitry P. Vetrov (Higher School of Economics); Timur Garipov (Samsung AI Center in Moscow)

Acceleration through Spectral Modeling. Fabian Pedregosa (Google); Damien Scieur (Princeton University)

Using better models in stochastic optimization. Hilal Asi (Stanford University); John Duchi (Stanford University)


Poster Session

Abstract 5: Adaptive gradient methods: efficient implementation and generalization in Beyond first order methods in machine learning systems, 10:30 AM

Adaptive gradient methods have had a transformative impact in deep learning. We will describe recent theoretical and experimental advances in their understanding, including low-memory adaptive preconditioning, and insights into their generalization ability.

Abstract 6: Spotlight talks in Beyond first order methods in machine learning systems, Scieur, Mishchenko, Anil 11:15 AM

Symmetric Multisecant quasi-Newton methods. Damien Scieur (Samsung AI Research Montreal); Thomas Pumir (Princeton University); Nicolas Boumal (Princeton University)

Stochastic Newton Method and its Cubic Regularization via Majorization-Minimization. Konstantin Mishchenko (King Abdullah University of Science & Technology (KAUST)); Peter Richtarik (KAUST); Dmitry Kraljevic (KAUST)

Full Matrix Preconditioning Made Practical. Rohan Anil (Google); Vineet Gupta (Google); Tomer Koren (Google); Kevin Regan (Google); Yoram Singer (Princeton)

Abstract 8: K-FAC: Extensions, improvements, and applications in Beyond first order methods in machine learning systems, Martens 02:00 PM

Second order optimization methods have the potential to be much faster than first order methods in the deterministic case, or pre-asymptotically in the stochastic case. However, traditional second order methods have proven ineffective or impractical for neural network training, due in part to the extremely high dimension of the parameter space. Kronecker-factored Approximate Curvature (K-FAC) is second-order optimization method based on a tractable approximation to the Gauss-Newton/Fisher matrix that exploits the special structure present in neural network training objectives. This approximation is neither low-rank

Abstracts (12):

Abstract 1: Opening Remarks in Beyond first order methods in machine learning systems, Kyrillidis, Berahas, Roosta, Mahoney 08:00 AM

Opening remarks for the workshop by the organizers

Abstract 2: Economical use of second-order information in training machine learning models in Beyond first order methods in machine learning systems, Goldfarb 08:30 AM

Stochastic gradient descent (SGD) and variants such as Adam and Adam, are extensively used today to train modern machine learning models. In this talk we will discuss ways to economically use second-order information to modify both the step size (learning rate) used in SGD and the direction taken by SGD. Our methods adaptively control the batch sizes used to compute gradient and Hessian approximations and and ensure that the steps that are taken decrease the loss function with high probability assuming that the latter is self-concordant, as is true for many problems in empirical risk minimization. For such cases we prove that our basic algorithm is globally linearly convergent. A slightly modified version of our method is presented for training deep learning models. Numerical results will be presented that show that it exhibits excellent performance without the need for learning rate tuning. If there is time, additional ways to efficiently make use of second-order information will be presented.

Abstract 3: Spotlight talks in Beyond first order methods in machine learning systems, Granziol, Pedregosa, Asi 09:00 AM

Opening remarks for the workshop by the organizers

Abstract 4: Adaptive gradient methods: efficient implementation and generalization in Beyond first order methods in machine learning systems, 10:30 AM

Adaptive gradient methods have had a transformative impact in deep learning. We will describe recent theoretical and experimental advances in their understanding, including low-memory adaptive preconditioning, and insights into their generalizaton ability.

Abstract 5: Spotlight talks in Beyond first order methods in machine learning systems, Scieur, Mishchenko, Anil 11:15 AM

Symmetric Multisecant quasi-Newton methods. Damien Scieur (Samsung AI Research Montreal); Thomas Pumir (Princeton University); Nicolas Boumal (Princeton University)

Stochastic Newton Method and its Cubic Regularization via Majorization-Minimization. Konstantin Mishchenko (King Abdullah University of Science & Technology (KAUST)); Peter Richtarik (KAUST); Dmitry Kraljevic (KAUST)

Full Matrix Preconditioning Made Practical. Rohan Anil (Google); Vineet Gupta (Google); Tomer Koren (Google); Kevin Regan (Google); Yoram Singer (Princeton)

Abstract 8: K-FAC: Extensions, improvements, and applications in Beyond first order methods in machine learning systems, Martens 02:00 PM

Second order optimization methods have the potential to be much faster than first order methods in the deterministic case, or pre-asymptotically in the stochastic case. However, traditional second order methods have proven ineffective or impractical for neural network training, due in part to the extremely high dimension of the parameter space. Kronecker-factored Approximate Curvature (K-FAC) is second-order optimization method based on a tractable approximation to the Gauss-Newton/Fisher matrix that exploits the special structure present in neural network training objectives. This approximation is neither low-rank

Abstracts (12):

Abstract 1: Opening Remarks in Beyond first order methods in machine learning systems, Kyrillidis, Berahas, Roosta, Mahoney 08:00 AM

Opening remarks for the workshop by the organizers

Abstract 2: Economical use of second-order information in training machine learning models in Beyond first order methods in machine learning systems, Goldfarb 08:30 AM

Stochastic gradient descent (SGD) and variants such as Adam and Adam, are extensively used today to train modern machine learning models. In this talk we will discuss ways to economically use second-order information to modify both the step size (learning rate) used in SGD and the direction taken by SGD. Our methods adaptively control the batch sizes used to compute gradient and Hessian approximations and and ensure that the steps that are taken decrease the loss function with high probability assuming that the latter is self-concordant, as is true for many problems in empirical risk minimization. For such cases we prove that our basic algorithm is globally linearly convergent. A slightly modified version of our method is presented for training deep learning models. Numerical results will be presented that show that it exhibits excellent performance without the need for learning rate tuning. If there is time, additional ways to efficiently make use of second-order information will be presented.

Abstract 3: Spotlight talks in Beyond first order methods in machine learning systems, Granziol, Pedregosa, Asi 09:00 AM

Opening remarks for the workshop by the organizers

Abstract 4: Adaptive gradient methods: efficient implementation and generalization in Beyond first order methods in machine learning systems, 10:30 AM

Adaptive gradient methods have had a transformative impact in deep learning. We will describe recent theoretical and experimental advances in their understanding, including low-memory adaptive preconditioning, and insights into their generalizaton ability.

Abstract 5: Spotlight talks in Beyond first order methods in machine learning systems, Scieur, Mishchenko, Anil 11:15 AM

Symmetric Multisecant quasi-Newton methods. Damien Scieur (Samsung AI Research Montreal); Thomas Pumir (Princeton University); Nicolas Boumal (Princeton University)

Stochastic Newton Method and its Cubic Regularization via Majorization-Minimization. Konstantin Mishchenko (King Abdullah University of Science & Technology (KAUST)); Peter Richtarik (KAUST); Dmitry Kraljevic (KAUST)

Full Matrix Preconditioning Made Practical. Rohan Anil (Google); Vineet Gupta (Google); Tomer Koren (Google); Kevin Regan (Google); Yoram Singer (Princeton)

Abstract 8: K-FAC: Extensions, improvements, and applications in Beyond first order methods in machine learning systems, Martens 02:00 PM

Second order optimization methods have the potential to be much faster than first order methods in the deterministic case, or pre-asymptotically in the stochastic case. However, traditional second order methods have proven ineffective or impractical for neural network training, due in part to the extremely high dimension of the parameter space. Kronecker-factored Approximate Curvature (K-FAC) is second-order optimization method based on a tractable approximation to the Gauss-Newton/Fisher matrix that exploits the special structure present in neural network training objectives. This approximation is neither low-rank
nor diagonal, but instead involves Kronecker-products, which allows for efficient estimation, storage and inversion of the curvature matrix. In this talk I will introduce the basic K-FAC method for standard MLPs and then present some more recent work in this direction, including extensions to CNNs and RNNs, both of which require new approximations to the Fisher. For these I will provide mathematical intuitions and empirical results which speak to their efficacy in neural network optimization. Time permitting, I will also discuss some recent results on large-batch optimization with K-FAC, and the use of adaptive adjustment methods that can eliminate the need for costly hyperparameter tuning.

Abstract 9: **Spotlight talks in Beyond first order methods in machine learning systems**, Grigas, Yao, Lucchi, Meng 02:45 PM

Hessian-Aware trace-Weighted Quantization. Zhen Dong (UC Berkeley); Zhewei Yao (University of California, Berkeley); Amir Gholami (UC Berkeley); Yaohui Cai (Peking University); Dayaan Arfeen (UC Berkeley); Michael Mahoney ("University of California, Berkeley"); Kurt Keutzer (UC Berkeley)

New Methods for Regularization Path Optimization via Differential Equations. Paul Grigas (UC Berkeley); Heyuan Liu (University of California, Berkeley)

Ellipsoidal Trust Region Methods for Neural Nets. Leonard Adolphe (ETHZ); Jonas Kohler (ETHZ)

Sub-sampled Newton Methods Under Interpolation. Si Yi Meng (University of British Columbia); Sharan Vaswani (Mila, Université de Montréal); Issam Laradji (University of British Columbia); Mark Schmidt (University of British Columbia); Simon Lacoste-Julien (Mila, Université de Montréal)

Abstract 10: **Poster Session (same as above) in Beyond first order methods in machine learning systems**, 03:30 PM

An Accelerated Method for Derivative-Free Smooth Stochastic Convex Optimization. Eduard Gorbunov (Moscow Institute of Physics and Technology); Pavel Dvurechenskii (WIAS Germany); Alexander Gasnikov (Moscow Institute of Physics and Technology)

Fast Bregman Gradient Methods for Low-Rank Minimization Problems. Radu-Alexandru Dragomir (Univ. Toulouse 1); Jérôme Bolte (Univ. Toulouse 1); Alexandre d’Aspremont (Ecole Normale Superieure)

Gluster: Variance Reduced Mini-Batch SGD with Gradient Clustering. Fartash Faghri (University of Toronto); David Duvenaud (University of Toronto); David Fleet (University of Toronto); Jimmy Ba (University of Toronto)

Neural Policy Gradient Methods: Global Optimality and Rates of Convergence. Lingxiao Wang (Northwestern University); Qi Cai (Northwestern University); Zhaoran Wang (Princeton University); Zhonghao Yang (Princeton University); Zhaoran Wang (Northwestern University)

A Gram-Gauss-Newton Method Learning Overparameterized Deep Neural Networks for Regression Problems. Tianle Cai (Peking University); Ruigi Gao (Peking University); Jikai Hou (Peking University); Siyu Chen (Peking University); Dong Wang (Peking University); Di He (Peking University); Zhihua Zhang (Peking University); Liwei Wang (Peking University)

Stochastic Gradient Methods with Layerwise Adaptive Moments for Training of Deep Networks. Boris Ginsburg (NVIDIA); Oleksii Hrinchuk (NVIDIA); Jason Li (NVIDIA); Vitaly Lavrukhin (NVIDIA); Ryan Leary (NVIDIA); Oleksii Kuchaiev (NVIDIA); Jonathan Cohen (NVIDIA); Huyen Nguyen (NVIDIA); Yang Zhang (NVIDIA)

Accelerating Neural ODEs with Spectral Elements. Alessio Quaglino (NNAISENSE SA); Marco Gallieri (NNAISENSE); Jonathan Masci (NNAISENSE); Jan Koulik (NNAISENSE)

An Inertial Newton Algorithm for Deep Learning. Camille Castera (CNRS, IRIT); Jérôme Bolte (Université Toulouse 1); Cédric Févotte (CNRS, IRIT); Edouard Pauwels (Toulouse 3 University)

Nonlinear Conjugate Gradients for Scaling Synchronous Distributed DNN Training. Saurabh Adya (Apple); Vinay Palakkode (Apple Inc.); Oncel Tuzel (Apple Inc.)

* How does mini-batching affect Curvature information for second order deep learning optimization? Diego Granziol (Oxford); Stephen Roberts (Oxford); Xingchen Wan (Oxford University); Stefan Zohren (University of Oxford); Binxin Ru (University of Oxford); Michael A. Osborne (University of Oxford); Andrew Wilson (NYU); sebastien ehrhardt (Oxford); Dmitry P Vetrov (Higher School of Economics); Timur Garipov (Samsung AI Center in Moscow)

On the Convergence of a Biased Version of Stochastic Gradient Descent. Rudrajit Das (University of Texas at Austin); Jiong Zhang (UT-Austin); Inderjit S. Dhillon (UT Austin & Amazon)

Adaptive Sampling Quasi-Newton Methods for Derivative-Free Stochastic Optimization. Raghu Bollapragada (Argonne National Laboratory); Stefan Wild (Argonne National Laboratory)

* Acceleration through Spectral Modeling. Fabian Pedregosa (Google); Damien Scieur (Princeton University)

Accelerating Distributed Stochastic L-BFGS by sampled 2nd-Order Information. Jie Liu (Lehigh University); Yu Rong (Tencent AI Lab); Martin Takac (Lehigh University); Junzhou Huang (Tencent AI Lab)

Grow Your Samples and Optimize Better via Distributed Newton CG and Accumulating Strategy. Majid Jahani (Lehigh University); Xi He (Lehigh University); Chenzin Ma (Lehigh University); Aryan Mokhtari (UT Austin); Dheevatsa Mudigere (Intel Labs); Alejandro Ribeiro (University of Pennsylvania); Martin Takac (Lehigh University)

Global linear convergence of trust-region Newton’s method without strong-convexity or smoothness. Sai Praneeth Karimireddy (EPFL); Sebastian Stich (EPFL); Martin Jaggi (EPFL)

FD-Net with Auxiliary Time Steps: Fast Prediction of PDEs using Hessian-Free Trust-Region Methods. Nur Sila Gulgec (Lehigh University); Zheng Shi (Lehigh University); Neil Deshmukh (MIT BeaverWorks - Medlytics); Shamin Pakzad (Lehigh University); Martin Takac (Lehigh University)

* Using better models in stochastic optimization. Hilal Asi (Stanford University); John Duchi (Stanford University)
Tangent space separability in feedforward neural networks. Bálint Daróczy (Institute for Computer Science and Control, Hungarian Academy of Sciences); Rita Alekzeiev (Institute for Computer Science and Control, Hungarian Academy of Sciences); Andras Benczur (Hungarian Academy of Sciences)

* Ellipsoidal Trust Region Methods for Neural Nets. Leonard Adolphs (ETHZ); Jonas Kohler (ETHZ)

Closing the K-FAC Generalisation Gap Using Stochastic Weight Averaging. Xingchen Wan (University of Oxford); Diego Granziol (Oxford); Stefan Zohren (University of Oxford); Stephen Roberts (Oxford)

* Sub-sampled Newton Methods Under Interpolation. Si Yi Meng (University of British Columbia); Sharar Vaswani (Mila, Université de Montréal); Issam Laradji (University of British Columbia); Mark Schmidt (University of British Columbia); Simon Lacoste-Julien (Mila, Université de Montréal)

Learned First-Order Preconditioning. Aditya Rawal (Uber AI Labs); Rui Wang (Uber AI); Theodore Moskovitz (Gatsby Computational Neuroscience Unit); Sanyam Kapoor (Uber); Janice Lan (Uber AI); Jason Yosinski (Uber AI Labs); Thomas Miconi (Uber AI Labs)

Iterative Hessian Sketch in Input Sparsity Time. Charlie Dickens (University of Warwick); Graham Cormode (University of Warwick)

Nonlinear matrix recovery. Florentin Goyens (University of Oxford); Coralia Cartis (Oxford University); Armin Eftekhari (EPFL)

Making Variance Reduction more Effective for Deep Networks. Nicolas Brandt (EPFL); Farnood Salehi (EPFL); Patrick Thiran (EPFL)

Novel and Efficient Approximations for Zero-One Loss of Linear Classifiers. Hiva Ghanbari (Lehigh University); Minhan Li (Lehigh University); Katya Scheinberg (Lehigh)

A Model-Based Derivative-Free Approach to Black-Box Adversarial Examples: BOBYQA. Giuseppe Ughi (University of Oxford)

Distributed Accelerated Inexact Proximal Gradient Method via System of Coupled Ordinary Differential Equations. Chhavi Sharma (IIT Bombay); Vishnu Narayanan (IIT Bombay); Balamurugan Palaniappan (IIT Bombay)

Finite-Time Convergence of Continuous-Time Optimization Algorithms via Differential Inclusions. Orlando Romero (Rensselaer Polytechnic Institute); Mouhacine Benosman (MERL)

Loss Landscape Sightseeing by Multi-Point Optimization. Ivan Skorokhodov (MIPT); Mikhail Burtsev (NI)

* Symmetric Multisecant quasi-Newton methods. Damien Scieur (Samsung AI Research Montreal); Thomas Pumir (Princeton University); Nicolas Boumal (Princeton University)

Does Adam optimizer keep close to the optimal point? Kwwook Bae (KAIST)*; Heechang Ryu (KAIST); Hayong Shin (KAIST)

* Stochastic Newton Method and its Cubic Regularization via

Majorization-Minimization. Konstantin Mishchenko (King Abdullah University of Science & Technology (KAUST)); Peter Richtarik (KAUST); Dmitry Koraev (KAUST)

* Full Matrix Preconditioning Made Practical. Rohan Anil (Google); Vineet Gupta (Google); Tomer Koren (Google); Kevin Regan (Google); Yoram Singer (Princeton)

Memory-Sample Tradeoffs for Linear Regression with Small Error. Vatsal Sharan (Stanford University); Aaron Sidford (Stanford); Gregory Valiant (Stanford University)

On the Higher-order Moments in Adam. Zhanhong Jiang (Johnson Controls International); Aditya Balu (Iowa State University); Sin Yong Tan (Iowa State University); Young M Lee (Johnson Controls International); Chimmay Hegde (Iowa State University); Soumik Sarkar (Iowa State University)

h-matrix approximation for Gauss-Newton Hessian. Chao Chen (UT Austin)

* Hessian-Aware trace-Weighted Quantization. Zhen Dong (UC Berkeley); Zhewei Yao (University of California, Berkeley); Amir Gholami (UC Berkeley); Yaohui Cai (Peking University); Daiyaan Arfeen (UC Berkeley); Michael Mahoney ("University of California, Berkeley"); Kurt Keutzer (UC Berkeley)

Random Projections for Learning Non-convex Models. Tolga Ergen (Stanford University); Emmanuel Candès (Stanford University); Mert Pilanci (Stanford)

* New Methods for Regularization Path Optimization via Differential Equations. Paul Grigas (UC Berkeley); Heyuan Liu (University of California, Berkeley)

Hessian-Aware Zeroth-Order Optimization. Haishan Ye (HKUST); Zhichao Huang (HKUST); Cong Fang (Peking University); Chris Junchi Li (Tencent); Tong Zhang (HKUST)

Higher-Order Accelerated Methods for Faster Non-Smooth Optimization. Brian Bullins (TTIC)

Abstract 11: Analysis of linear search methods for various gradient approximation schemes for noisy derivative free optimization. in Beyond first order methods in machine learning systems, Scheinberg 04:15 PM

We develop convergence analysis of a modified line search method for objective functions whose value is computed with noise and whose gradient estimates are not directly available. The noise is assumed to be bounded in absolute value without any additional assumptions. In this case, gradient approximation can be constructed via interpolation or sample average approximation of smoothing gradients and thus they are always inexact and possibly random. We extend the framework based on stochastic methods which was developed to provide analysis of a standard line-search method with exact function values and random gradients to the case of noisy function. We introduce a condition on the gradient which when satisfied with some sufficiently large probability at each iteration, guarantees convergence properties of the line search method. We derive expected complexity bounds for convex, strongly convex and nonconvex functions. We motivate these results with several
bring together potential partners to organize such challenges and stimulate "machine learning for good" i.e. the organization of challenges for the benefit of society. We have invited prominent speakers that have experience in this domain.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Welcome and Opening Remarks</td>
<td>Mendrik, Tu, Guyon, Viegas, Li</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>&quot;AI for Good via Machine Learning Challenges&quot;</td>
<td>Banifatemi</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Emily Bender (University of Washington) &quot;Making Stakeholder Impacts Visible in the Evaluation Cycle: Towards Fairness-Integrated Shared Tasks and Evaluation Metrics&quot;</td>
<td>Bender</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Dina Machuve (Nelson Mandela African Institution of Science and Technology) &quot;Machine Learning Competitions: The Outlook from Africa&quot;</td>
<td>Machuve</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Dog Image Generation Competition on Kaggle</td>
<td>Kan, Culliton</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Learning To Run a Power Network Competition</td>
<td>Donnot</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>The AI Driving Olympics: An Accessible Robot Learning Benchmark</td>
<td>Walter</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Conclusion on TrackML, a Particle Physics Tracking Machine Learning Challenge Combining Accuracy and Inference Speed</td>
<td>Rousseau, vlimant</td>
</tr>
<tr>
<td>12:15 PM</td>
<td>Catered Lunch and Poster Viewing (in Workshop Room)</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Frank Hutter (University of Freiburg) &quot;A Proposal for a New Competition Design Emphasizing Scientific Insights&quot;</td>
<td>Hutter</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>Design and Analysis of Experiments: A Challenge Approach in Teaching</td>
<td>Pavao</td>
</tr>
</tbody>
</table>
The model-to-data paradigm: overcoming data access barriers in biomedical competitions

The Deep Learning Epilepsy Detection Challenge: Design, Implementation, and Test of a New Crowd-Sourced AI Challenge Ecosystem

Abstracts (11):

Abstract 2: Amir Banifatemi (XPrize) "AI for Good via Machine Learning Challenges" in CiML 2019: Machine Learning Competitions for All, Banifatemi 08:15 AM

"AI for Good" efforts (e.g., applications work in sustainability, education, health, financial inclusion, etc.) have demonstrated the capacity to simultaneously advance intelligent system research and the greater good. Unfortunately, the majority of research that could find motivation in real-world "good" problems still center on problems with industrial or toy problem performance baselines.

Competitions can serve as an important shaping reward for steering academia towards research that is simultaneously impactful on our state of knowledge and the state of the world. This talk covers three aspects of AI for Good competitions. First, we survey current efforts within the AI for Good application space as a means of identifying current and future opportunities. Next we discuss how more qualitative notions of "Good" can be used as benchmarks in addition to more quantitative competition objective functions. Finally, we will provide notes on building coalitions of domain experts to develop and guide socially-impactful competitions in machine learning.

Abstract 3: Emily Bender (University of Washington) "Making Stakeholder Impacts Visible in the Evaluation Cycle: Towards Fairness-Integrated Shared Tasks and Evaluation Metrics" in CiML 2019: Machine Learning Competitions for All, Bender 09:00 AM

In a typical machine learning competition or shared task, success is measured in terms of systems' ability to reproduce gold-standard labels. The potential impact of the systems being developed on stakeholder populations, if considered at all, is studied separately from system ‘performance’. Given the tight train-eval cycle of both shared tasks and system development in general, we argue that making disparate impact on vulnerable populations visible in dataset and metric design will be key to making the potential for such impact present and salient to developers. We see this as an effective way to promote the development of machine learning technology that is helpful for people, especially those who have been subject to marginalization. This talk will explore how to develop such shared tasks, considering task choice, stakeholder community input, and annotation and metric design desiderata.

Joint work with Hal Daumé III, University of Maryland, Bemease Herman, University of Washington, and Brandeis Marshall, Spelman College.

Abstract 5: Dina Machuve (Nelson Mandela African Institution of Science and Technology) "Machine Learning Competitions: The Outlook from Africa" in CiML 2019: Machine Learning Competitions for All, Machuve 10:30 AM

The current AI landscape in Africa mainly focuses on capacity building. The ongoing efforts to strengthen the AI capacity in Africa are organized in summer schools, workshops, meetups, competitions and one long-term program at the Masters level. The main AI initiatives driving the AI capacity building agenda in Africa include a) Deep Learning Indaba, b) Data Science Africa, c) Data Science Nigeria, d) Nairobi Women in Machine Learning and Data Science, e) Zindi and f) The African Master’s in Machine Intelligence (AMMI) at AIMS. The talk will summarize our experience on low participation of African AI developers at machine learning competitions and our recommendations to address the current challenges.

Abstract 6: Dog Image Generation Competition on Kaggle in CiML 2019: Machine Learning Competitions for All, Kan, Culliton 11:15 AM

We present a novel format of machine learning competitions where a user submits code that generates images trained on training samples, the code then runs on Kaggle, produces dog images, and user receives scores for the performance of their generative content based on 1. quality of images, 2. diversity of images, and 3. memorization penalty. This style of competition targets the usage of Generative Adversarial Networks (GAN)[4], but is open for all generative models. Our implementation addresses overfitting by incorporating two different pre-trained neural networks, as well as two separate "ground truth" image datasets, for the public and private leaderboard. We also have an enclosed compute environment to prevent submissions of non-generated images. In this paper, we describe both the algorithmic and system design of our competition, as well as sharing our lessons learned from running this competition [6] in July 2019 with 900+ teams participating and over 37,000 submissions and their code received.

Abstract 7: Learning To Run a Power Network Competition in CiML 2019: Machine Learning Competitions for All, Donnot 11:30 AM

We present the results of the first edition as well as some perspective for a next potential edition of the "Learning To Run a Power Network" (L2RPN) competition to test the potential of Reinforcement Learning to solve a real-world problem of great practical importance: controlling power transportation in power grids while keeping people and equipment safe.


Despite recent breakthroughs, the ability of deep learning and reinforcement learning to outperform traditional approaches to control physically embodied robotic agents remains largely unproven. To help bridge this gap, we have developed the "AI Driving Olympics" (AI-DO), a competition with the objective of evaluating the state-of-the-art in machine learning and artificial intelligence for mobile robotics. Based on the simple and well specified autonomous driving and navigation environment called "Duckietown," AI-DO includes a series of tasks of
Increasing complexity—from simple lane-following to fleet management. For each task, we provide tools for competitors to use in the form of simulators, data logs, code templates, baseline implementations, and low-cost access to robotic hardware. We evaluate submissions in simulation online, on standardized hardware environments, and finally at the competition events. We have held successful AI-DO competitions at NeurIPS 2018 and ICRA 2019, and will be holding AI-DO 3 at NeurIPS 2020. Together, these competitions highlight the need for better benchmarks, which are lacking in robotics, as well as improved mechanisms to bridge the gap between simulation and reality.

Abstract 10: Catered Lunch and Poster Viewing (in Workshop Room) in CiML 2019: Machine Learning Competitions for All, Stolovitzky, Pradhan, Duboue, Tang, Natekin, Bondi, Bouthiller, Milani, Müller, Holzinger, Harrer, Day, Ustyuzhanin, Guss, Mirmomeni 12:15 PM

Accepted Posters

Kandinsky Patterns: An open toolbox for creating explainable machine learning challenges
Heimo Muller · Andreas Holzinger

MOCA: An Unsupervised Algorithm for Optimal Aggregation of Challenge Submissions
Robert Vogel · Mehmet Eren Ahsen · Gustavo A. Stolovitzky

FDL: Mission Support Challenge
Luis F. Simões · Ben Day · Vinutha M. Shreenath · Callum Wilson

From data challenges to collaborative gig science. Competitive research process and platform
Andrey Ustyuzhanin · Mikhail Belous · Leyla Khatbullina · Giles Strong

Smart(er) Machine Learning for Practitioners
Prabhu Pradhan

Improving Reproducibility of Benchmarks
Xavier Bouthiller

Guaranteeing Reproducibility in Deep Learning Competitions
Brandon Houghton

Organizing crowd-sourced AI challenges in enterprise environments: opportunities and challenges
Mahtab Mirmomeni · Isabell Kiral · Subhrajit Roy · Todd Mumert · Alan Braz · Jason Tsay · Jianbin Tang · Umar Asif · Thomas Schaffter · Eren Mehmet · Bruno De Assis Marques · Stefan Maetschke · Rania Khalaf · Michal Rosen-Zvi · John Cohn · Gustavo Stolovitzky · Stefan Harrer

WikiCities: a Feature Engineering Educational Resource
Pablo Duboue

Reinforcement Learning Meets Information Seeking: Dynamic Search Challenge
Zhiwen Tang · Grace Hui Yang

AI Journey 2019: School Tests Solving Competition
Alexey Natekin · Peter Romov · Valentin Malych

A BIRDSSAI View for Conservation
Elizabeth Bondi · Milind Tambe · Raghav Jain · Palash Aggrawal · Saket

Anand · Robert Hannaford · Ashish Kapoor · Jim Piavis · Shital Shah · Lucas Joppa · Bistra Dilkina

Abstract 11: Frank Hutter (University of Freiburg) "A Proposal for a New Competition Design Emphasizing Scientific Insights" in CiML 2019: Machine Learning Competitions for All, Hutter 02:00 PM

The typical setup in machine learning competitions is to provide one or more datasets and a performance metric, leaving it entirely up to participants which approach to use, how to engineer better features, whether and how to pretrain models on related data, how to tune hyperparameters, how to combine multiple models in an ensemble, etc. The fact that work on each of these components often leads to substantial improvements has several consequences: (1) amongst several skilled teams, the one with the most manpower and engineering drive often wins; (2) it is often unclear "why" one entry performs better than another one; and (3) scientific insights remain limited.

Based on my experience in both participating in several challenges and also organizing some, I will propose a new competition design that instead emphasizes scientific insight by dividing the various ways in which teams could improve performance into (largely orthogonal) modular components, each of which defines its own competition. E.g., one could run a competition focussing only on effective hyperparameter tuning of a given pipeline (across private datasets). With the same code base and datasets, one could likewise run a competition focussing only on finding better neural architectures, or only better preprocessing methods, or only a better training pipeline, or only better pre-training methods, etc. One could also run multiple of these competitions in parallel, hot-swapping better components found in one competition into the other competitions. I will argue that the result would likely be substantially more valuable in terms of scientific insights than traditional competitions and may even lead to better final performance.

Abstract 12: Design and Analysis of Experiments: A Challenge Approach in Teaching in CiML 2019: Machine Learning Competitions for All, Pavao 02:45 PM

Over the past few years, we have explored the benefits of involving students both in organizing and in participating in challenges as a pedagogical tool, as part of an international collaboration. Engaging in the design and resolution of a competition can be seen as a hands-on means of learning proper design and analysis of experiments and gaining a deeper understanding other aspects of Machine Learning. Graduate students of University Paris-Sud (Paris, France) are involved in class projects in creating a challenge end-to-end, from defining the research problem, collecting or formatting data, creating a starting kit, to implementing and testing the website. The application domains and types of data are extremely diverse: medicine, ecology, marketing, computer vision, recommendation, text processing, etc. The challenges thus created are then used as class projects of undergraduate students who have to solve them, both at University Paris-Sud, and at Rensselaer Polytechnic Institute (RPI, New York, USA), to provide rich learning experiences at scale. New this year, students are involved in creating challenges motivated by "AI for good" and will create re-usable templates to inspire others to create challenges for the benefit of humanity.

Abstract 13: The model-to-data paradigm: overcoming data access barriers in biomedical competitions in CiML 2019: Machine Learning Competitions for All, Guinney 03:00 PM
Data competitions often rely on the physical distribution of data to challenge participants, a significant limitation given that much data is proprietary, sensitive, and often non-shareable. To address this, the DREAM Challenges has advanced a challenge framework called model-to-data (MTD), requiring participants to submit re-runnable algorithms instead of model predictions. The DREAM organization has successfully completed multiple MTD-based challenges, and is expanding this approach to unlock highly sensitive and non-distributable human data for use in biomedical data challenges.

Abstract 16: Open Space Topic “The Organization of Challenges for the Benefit of More Diverse Communities” in CiML 2019: Machine Learning Competitions for All, Mendrik, Guyon, Tu, Viegas, L/04:15 PM

“Open Space” is a technique for running meetings where the participants create and manage the agenda themselves. Participants can propose ideas that address the open space topic, these will be divided into various sessions that all other participants can join and brainstorm about. After the open space we will collect all the ideas and post them on the CiML website.

AI for Humanitarian Assistance and Disaster Response

Ritwik Gupta, Robin Murphy, Trevor Darrell, Eric Heim, Zhangyang Wang, Bryce Goodman, Piotr Bilski

West 217 - 219, Fri Dec 13, 08:00 AM

Natural disasters are one of the oldest threats to not just individuals but to the societies they co-exist in. As a result, humanity has ceaselessly sought way to provide assistance to people in need after disasters have struck. Further, natural disasters are but a single, extreme example of the many possible humanitarian crises. Disease outbreak, famine, and oppression against disadvantaged groups can pose even greater dangers to people that have less obvious solutions.

In this proposed workshop, we seek to bring together the Artificial Intelligence (AI) and Humanitarian Assistance and Disaster Response (HADR) communities in order to bring AI to bear on real-world humanitarian crises.

Through this workshop, we intend to establish meaningful dialogue between the communities.

By the end of the workshop, the NeurIPS research community can come to understand the practical challenges of in aiding those in crisis, while the HADR can understand the landscape that is the state of art and practice in AI.

Through this, we seek to begin establishing a pipeline of transitioning the research created by the NeurIPS community to real-world humanitarian issues.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Introduction and Welcome</td>
<td>Gupta, Sajeev</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Invited Talks (x4)</td>
<td>Matias, Adole, Brown, Jaimes</td>
</tr>
<tr>
<td>10:15 AM</td>
<td>Break</td>
<td></td>
</tr>
</tbody>
</table>

Abstracts (6):

Abstract 2: Invited Talks (x4) in AI for Humanitarian Assistance and Disaster Response, Matias, Adole, Brown, Jaimes 08:15 AM

* Tracy Adole (WorldPop)
* Yossi Matias (Google)
* Col Jason Brown (US Air Force)
* Alex Jaimes (Dataminr)

Abstract 4: Spotlight Talks 1 in AI for Humanitarian Assistance and Disaster Response, Wang, Dalmasso, Doshi, See, Kapadia, Kruspe 10:30 AM

Paper IDs
* 8 - “Two Case Studies of Building Modeling using Machine Learning”
* 9 - “Feature Engineering for Entity Resolution with Arabic Names: Improving Estimates of Observed Casualties in the Syrian Civil War”
* 12 - “Revisiting Classical Bagging with Modern Transfer Learning for On-the-fly Disaster Damage Detector”
* 13 - “FireNet: Real-time Segmentation of Fire Perimeter from Aerial Video”
* 14 - “Deep Crowd-Flow Prediction in Built Environments”
* 15 - “Few-shot Tweet Detection in Emerging Disaster Events”

Abstract 6: Invited Talks (x2) in AI for Humanitarian Assistance and Disaster Response, Rasmussen, Stromberg 01:30 PM

* Maj Megan Stromberg (US Air Force)
* Eric Rasmussen (Infinitum Humanitarian Systems)

Abstract 7: Spotlight Talks 2 in AI for Humanitarian Assistance and Disaster Response, Veitch-Michaelis, Sidrane, Nevo, Oh 02:30 PM

Paper IDs
* 18 - “Flood Detection On Low Cost Orbital Hardware”
* 19 - “Machine Learning for Generalizable Prediction of Flood Susceptibility”
* 20 - “Inundation Modeling in Data Scarce Regions”
* 24 - “Explainable Semantic Mapping for First Responders”

Abstract 9: Spotlight Talks 3 in AI for Humanitarian Assistance and Disaster Response, Schrempf, Dubey, Lu 03:45 PM
## Shared Visual Representations in Human and Machine Intelligence

**Arturo Deza, Joshua Peterson, Apurva Ratan Murty, Tom Griffiths**

**West 220 - 222, Fri Dec 13, 08:00 AM**

The goal of the Shared Visual Representations in Human and Machine Intelligence (SVRHM) workshop is to disseminate relevant, parallel findings in the fields of computational neuroscience, psychology, and cognitive science that may inform modern machine learning methods.

In the past few years, machine learning methods—especially deep neural networks—have widely permeated the vision science, cognitive science, and neuroscience communities. As a result, scientific modeling in these fields has greatly benefited, producing a swath of potentially critical new insights into human learning and intelligence, which remains the gold standard for many tasks. However, the machine learning community has been largely unaware of these cross-disciplinary insights and analytical tools, which may help to solve many of the current problems that ML theorists and engineers face today (e.g., adversarial attacks, compression, continual learning, and unsupervised learning).

Thus we propose to invite leading cognitive scientists with strong computational backgrounds to disseminate their findings to the machine learning community with the hope of closing the loop by nourishing new ideas and creating cross-disciplinary collaborations.

See more information at the official conference website: [https://www.svrhm2019.com/](https://www.svrhm2019.com/)

Follow us on twitter for announcements: [https://twitter.com/svrhm2019](https://twitter.com/svrhm2019)

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:50 AM</td>
<td>Opening Remarks</td>
<td>Deza, Peterson, Murty, Griffiths</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Predictable representations in humans and machines</td>
<td>Henaff</td>
</tr>
<tr>
<td>09:25 AM</td>
<td>What is disentangling and does intelligence need it?</td>
<td>Higgins</td>
</tr>
<tr>
<td>09:50 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:10 AM</td>
<td>A “distribution mismatch” dataset for comparing representational similarity in ANNs and the brain</td>
<td>Xiao</td>
</tr>
<tr>
<td>10:35 AM</td>
<td>Feathers, wings and the future of computer vision research</td>
<td>Freeman</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Taxonomic structure in learning from few positive examples</td>
<td>Grant</td>
</tr>
<tr>
<td>11:25 AM</td>
<td>CIFAR-10H: using human-derived soft-label distributions to support more robust and generalizable classification</td>
<td>Battleday</td>
</tr>
<tr>
<td>11:50 AM</td>
<td>Making the next generation of machine learning datasets: ObjectNet a new object recognition benchmark</td>
<td>Barbu</td>
</tr>
<tr>
<td>12:15 PM</td>
<td>The building blocks of vision</td>
<td>Tarr</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Poster Session</td>
<td></td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Q&amp;A from the Audience. Ask the Grad Students</td>
<td>Grant, Battleday, Sanborn, Chang, Parthasarathy</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Object representation in the human visual system</td>
<td>Konkie</td>
</tr>
<tr>
<td>03:55 PM</td>
<td>Cognitive computational neuroscience of vision</td>
<td>Kriegeskorte</td>
</tr>
<tr>
<td>04:20 PM</td>
<td>Perturbation-based remodeling of visual neural Bethe network representations</td>
<td>Bethge</td>
</tr>
<tr>
<td>04:45 PM</td>
<td>Local gain control and perceptual invariances</td>
<td>Simoncelli</td>
</tr>
</tbody>
</table>
Despite recent progress in artificial intelligence, humans and animals vastly surpass machine agents in their ability to quickly learn about their environment. While humans generalize to new concepts from small numbers of examples, state-of-the-art artificial neural networks still require huge amounts of supervision. We hypothesize that humans benefit from such data-efficiency because their internal representations support a much wider set tasks (such as planning and decision-making) which often require making predictions about future events. Using the curvature of natural videos as a measure of predictability, we find that human perceptual representations are indeed more predictable than their inputs, whereas current deep neural networks are not. Conversely, by optimizing neural networks for an information-theoretic measure of predictability, we arrive at artificial classifiers whose data-efficiency greatly surpasses that of purely supervised ones. Learning predictable representations may therefore enable artificial systems to perceive the world in a manner that is closer to biological ones.

Abstract 3: What is disentangling and does intelligence need it? in Shared Visual Representations in Human and Machine Intelligence, Higgins 09:25 AM

Despite the advances in modern deep learning approaches, we are still quite far from the generality, robustness and data efficiency of biological intelligence. In this talk I will suggest that this gap may be narrowed by re-focusing from implicit representation learning prevalent in end-to-end deep learning approaches to explicit unsupervised representation learning. In particular, I will discuss the value of disentangled visual representations acquired in an unsupervised manner loosely inspired by biological intelligence. In particular, this talk will connect disentangling with the ideas of symmetry transformations from physics to make a claim that disentangled representations reflect important world structure. I will then go over a few first demonstrations of how such representations can be useful in practice for continual learning, acquiring reinforcement learning (RL) policies that are more robust to transfer scenarios that standard RL approaches, and building abstract compositional visual concepts which make possible imagination of meaningful and diverse samples beyond the training data distribution.

Abstract 5: A “distribution mismatch” dataset for comparing representational similarity in ANNs and the brain in Shared Visual Representations in Human and Machine Intelligence, Xiao 10:10 AM

A “distribution mismatch” dataset for comparing representational similarity in ANNs and the brain

Abstract 8: CIFAR-10H: using human-derived soft-label distributions to support more robust and generalizable classification in Shared Visual Representations in Human and Machine Intelligence, Battleday 11:25 AM

The classification performance of deep neural networks has begun to asymptote at near-perfect levels on natural image benchmarks. However, their ability to generalize outside the training set and their robustness to adversarial attacks have not. Humans, by contrast, exhibit robust and graceful generalization far outside their set of training samples. In this talk, I will discuss one strategy for translating these properties to machine-learning classifiers: training them to be uncertain in the same way as humans, rather than always right. When we integrate human uncertainty into training paradigms by using human guess distributions as labels, we find the generalize better and are more robust to adversarial attacks. Rather than expect all image datasets to come with such labels, we instead intend our CIFAR10H dataset to be used as a gold standard, with which algorithmic means of capturing the same information can be evaluated. To illustrate this, I present one automated method that does so—deep prototype models inspired by the cognitive science literature.

Abstract 12: Q&A from the Audience. Ask the Grad Students in Shared Visual Representations in Human and Machine Intelligence, Grant, Battleday, Sanborn, Chang, Parthasarathy 03:00 PM

"Cross-disciplinary research experiences and tips for Graduate School Admissions Panelists"
The growing field of Human-centric ML seeks to minimize the potential harms, risks, and burdens of big data technologies on the public, and at the same time, maximize their societal benefits. In this workshop, we address a wide range of challenges from diverse, multi-disciplinary viewpoints. We bring together experts from a diverse set of backgrounds. Our speakers are leading experts in ML, human-computer interaction, ethics, and law. Each of our speakers will focus on one core human-centred challenge (namely, fairness, accountability, interpretability, transparency, security, and privacy) in specific application domains (such as medicine, welfare programs, governance, and regulation). One of the main goals of this workshop is to help the community understand where it stands after a few years of rapid technical development and identify promising research directions to pursue in the years to come. Our speakers identify in their presentations 3-5 research directions that they consider to be of crucial importance. These directions are further debated in one of our panel discussions.

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 AM</td>
<td>Welcome and introduction</td>
<td></td>
</tr>
<tr>
<td>08:45 AM</td>
<td>Invited talk #1</td>
<td>Gummadi</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Contributed talks (3)</td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Panel #1: On the role of industry, academia, and government in developing HCML</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Coffe break</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Invited talk #2</td>
<td>Mulligan</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Contributed talks (2)</td>
<td></td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch and poster session</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Invited talk #3</td>
<td>Roth</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Contributed talks (4)</td>
<td></td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Invited talk #4</td>
<td>Doshi-Velez</td>
</tr>
<tr>
<td>04:00 PM</td>
<td>Invited talk #5</td>
<td>Kim</td>
</tr>
<tr>
<td>04:30 PM</td>
<td>Panel #2: Future research directions and interdisciplinary collaborations in HCML</td>
<td></td>
</tr>
</tbody>
</table>

**Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications**

Reinhard Heckel, Paul Hand, Richard Baraniuk, Joan Bruna, Alex Dimakis, Deanna Needell

West 301 - 305, Fri Dec 13, 08:00 AM

There is a long history of algorithmic development for solving inverse problems arising in sensing and imaging systems and beyond. Examples include medical and computational imaging, compressive sensing, as well as community detection in networks. Until recently, most algorithms for solving inverse problems in the imaging and network sciences were based on static signal models derived from physics or intuition, such as wavelets or sparse representations.

Today, the best performing approaches for the aforementioned image reconstruction and sensing problems are based on deep learning, which learn various elements of the method including i) signal representations, ii) stepsizes and parameters of iterative algorithms, iii) regularizers, and iv) entire inverse functions. For example, it has recently been shown that solving a variety of inverse problems by transforming an iterative, physics-based algorithm into a deep network whose parameters can be learned from training data, offers faster convergence and/or a better quality solution. Moreover, even with very little or no learning, deep neural networks enable superior performance for classical linear inverse problems such as denoising and compressive sensing. Motivated by those success stories, researchers are redesigning traditional imaging and sensing systems.

However, the field is mostly wide open with a range of theoretical and practical questions unanswered. In particular, deep-neural network based approaches often lack the guarantees of the traditional physics based methods, and while typically superior can make drastic reconstruction errors, such as fantasizing a tumor in an MRI reconstruction.

This workshop aims at bringing together theoreticians and practitioners in order to chart out recent advances and discuss new directions in deep neural network based approaches for solving inverse problems in the imaging and network sciences.
### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 AM</td>
<td>Opening Remarks</td>
<td>Heckel, Hand, Dimakis, Bruna, Needell, Baraniuk</td>
</tr>
<tr>
<td>08:40 AM</td>
<td>The spiked matrix model with generative priors</td>
<td>Zdeborová</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Robust One-Bit Recovery via ReLU Generative Networks: Improved Statistical Rate and Global Landscape Analysis</td>
<td>Qiu, Wei, Yang</td>
</tr>
<tr>
<td>09:40 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Computational microscopy in scattering media</td>
<td>Waller</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Denoising via Early Stopping</td>
<td>Soltanolkotabi</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Neural Reparameterization Improves Structural Optimization</td>
<td>Hoyer, Sohl-Dickstein, Greydanus</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch Break</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Learning-Based Low-Rank Approximations</td>
<td>Indyk</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Blind Denoising, Self-Supervision, and Implicit Inverse Problems</td>
<td>Batson</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Learning Regularizers from Data</td>
<td>Chandrasekaran</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Poster Session</td>
<td></td>
</tr>
</tbody>
</table>

### Abstracts (6):

**Abstract 2: The spiked matrix model with generative priors in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications. Zdeborová 08:40 AM**

Using a low-dimensional parametrization of signals is a generic and powerful way to enhance performance in signal processing and statistical inference. A very popular and widely explored type of dimensionality reduction is sparsity; another type is generative modelling of signal distributions. Generative models based on neural networks, such as GANs or variational auto-encoders, are particularly performant and are gaining on applicability. In this paper we study spiked matrix models, where a low-rank matrix is observed through a noisy channel. This problem with sparse structure of the spikes has attracted broad attention in the past literature. Here, we replace the sparsity assumption by generative modelling, and investigate the consequences on statistical and algorithmic properties. We analyze the Bayes-optimal performance under specific generative models for the spike. In contrast with the sparsity assumption, we do not observe regions of parameters where statistical performance is superior to the best known algorithmic performance. We show that in the analyzed cases the approximate message passing algorithm is able to reach optimal performance. We also design enhanced spectral algorithms and analyze their performance and thresholds using random matrix theory, showing their superiority to the classical principal component analysis. We complement our theoretical results by illustrating the performance of the spectral algorithms when the spikes come from real datasets.

**Abstract 3: Robust One-Bit Recovery via ReLU Generative Networks: Improved Statistical Rate and Global Landscape Analysis in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications. Qiu, Wei, Yang 09:10 AM**

We study the robust one-bit compressed sensing problem whose goal is to design an algorithm that faithfully recovers any sparse target vector \( \theta_0 \in \mathbb{R}^d \) \( \text{uniformly} \) from \( m \) quantized noisy measurements. Under the assumption that the measurements are sub-Gaussian, to recover any \( k \)-sparse \( \theta_0 \) via \( m \) quantized noisy measurements, the best known computationally tractable algorithm requires a logarithm factor of \( \varepsilon^{-1} \). We study the robust one-bit compressed sensing problem where the sparsity is implicitly enforced via mapping a low dimensional representation \( x_0 \) through a known \( n \)-layer ReLU generative network \( G : \mathbb{R}^k \rightarrow \mathbb{R}^d \). Such a framework poses low-dimensional priors on \( \theta_0 \) without a known basis. We propose to recover the target \( G(x_0) \) via an unconstrained empirical risk minimization (ERM) problem under a much weaker sub-exponential measurement assumption. For such a problem, we establish a joint statistical and computational analysis. In particular, we prove that the ERM estimator in this new framework achieves an improved statistical rate of \( m \geq \tilde{\mathcal{O}}(k \log d / \varepsilon^2) \) recovering any \( G(x_0) \) uniformly up to an error \( \varepsilon \).

Moreover, from the lens of computation, despite non-convexity, we prove that the joint statistical performance of the ERM problem has no spurious stationary point,
that is, any stationary point is equally good for recovering the true target up to scaling with a certain accuracy. Our analysis sheds some light on the possibility of inverting a deep generative model under partial and quantized measurements, complementing the recent success of using deep generative models for inverse problems.

Abstract 5: Computational microscopy in scattering media in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications, Waller 10:30 AM

Computational imaging involves the joint design of imaging system hardware and software, optimizing across the entire pipeline from acquisition to reconstruction. Computers can replace bulky and expensive optics by solving computational inverse problems. This talk will describe new microscopes that use computational imaging to enable 3D fluorescence and phase measurement using image reconstruction algorithms that are based on large-scale nonlinear non-convex optimization combined with unrolled neural networks. We further discuss engineering of data capture for computational microscopes by end-to-end learned design.

Abstract 7: Neural Reparameterization Improves Structural Optimization in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications, Hoyer, Sohl-Dickstein, Greydanus 11:30 AM

Structural optimization is a popular method for designing objects such as bridge trusses, airplane wings, and optical devices. Unfortunately, the quality of solutions depends heavily on how the problem is parameterized. In this paper, we propose using the implicit bias over functions induced by neural networks to improve the parameterization of structural optimization. Rather than directly optimizing densities on a grid, we instead optimize the parameters of a neural network which outputs those densities. This reparameterization leads to different and often better solutions. On a selection of 116 structural optimization tasks, our approach produces an optimal design 50% more often than the best baseline method.

Abstract 10: Blind Denoising, Self-Supervision, and Implicit Inverse Problems in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications, Batson 02:30 PM

We will discuss a self-supervised approach to the foundational inverse problem of denoising (Noise2Self). By taking advantage of statistical independence in the noise, we can estimate the mean-square error for a large class of deep architectures without access to ground truth. This allows us to train a neural network to denoise from noisy data alone, and also to compare between architectures, selecting one which will produce images with the lowest MSE. However, architectures with the same MSE performance can produce qualitatively different results, i.e., the hypersurface of images with fixed MSE is very heterogeneous. We will discuss ongoing work in understanding the types of artifacts which different denoising architectures give rise to.

Abstract 11: Learning Regularizers from Data in Solving inverse problems with deep networks: New architectures, theoretical foundations, and applications, Chandrasekaran 03:00 PM

Regularization techniques are widely employed in the solution of inverse problems in data analysis and scientific computing due to their effectiveness in addressing difficulties due to ill-posedness. In their most common manifestation, these methods take the form of penalty functions added to the objective in variational approaches for solving inverse problems. The purpose of the penalty function is to induce a desired structure in the solution, and these functions are specified based on prior domain-specific expertise. We consider the problem of learning suitable regularization functions from data in settings in which precise domain knowledge is not directly available; the objective is to identify a regularizer to promote the type of structure contained in the data. The regularizers obtained using our framework are specified as convex functions that can be computed efficiently via semidefinite programming. Our approach for learning such semidefinite regularizers combines recent techniques for rank minimization problems along with the Operator Sinkhorn procedure. (Joint work with Yong Sheng Soh)


Raj Parihar, Michael Goldfarb, Satyam Srivastava, TAO SHENG, Debajyoti Pal

West 306, Fri Dec 13, 08:00 AM

A new wave of intelligent computing, driven by recent advances in machine learning and cognitive algorithms coupled with process technology and new design methodologies, has the potential to usher unprecedented disruption in the way modern computing systems are designed and deployed. These new and innovative approaches often provide an attractive and efficient alternative not only in terms of performance but also power, energy, and area. This disruption is easily visible across the whole spectrum of computing systems -- ranging from low end mobile devices to large scale data centers and servers including intelligent infrastructures.

A key class of these intelligent solutions is providing real-time, on-device cognition at the edge to enable many novel applications including computer vision and image processing, language understanding, speech and gesture recognition, malware detection and autonomous driving. Naturally, these applications have diverse requirements for performance, energy, reliability, accuracy, and security that demand a holistic approach to designing the hardware, software, and intelligence algorithms to achieve the best power, performance, and area (PPA).

Topics:
- Architectures for the edge: IoT, automotive, and mobile
- Approximation, quantization reduced precision computing
- Hardware/software techniques for sparsity
- Neural network architectures for resource constrained devices
- Neural network pruning, tuning and and automatic architecture search
- Novel memory architectures for machine learning
- Communication/computation scheduling for better performance and energy
- Load balancing and efficient task distribution techniques
- Exploring the interplay between precision, performance, power and energy
- Exploration of new and efficient applications for machine learning
- Characterization of machine learning benchmarks and workloads
- Performance profiling and synthesis of workloads
- Simulation and emulation techniques, frameworks and platforms for machine learning
- Power, performance and area (PPA) based comparison of neural networks
- Verification, validation and determinism in neural networks
- Efficient on-device learning techniques
- Security, safety and privacy challenges and building secure AI systems

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>TBD</td>
<td>LeCun</td>
</tr>
<tr>
<td>08:45 AM</td>
<td>Efficient Computing for AI and Robotics</td>
<td>Sze</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Putting the “Machine” Back in Machine Learning: The Case for Hardware-ML Model Co-design</td>
<td>Marculescu</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Poster Session 1</td>
<td>Spasov, Nayak, Diego Andilla, Zhang, Trivedi</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Abandoning the Dark Arts: New Directions in Efficient DNN Design</td>
<td>Keutzer</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Hardware-aware Neural Architecture Design for Small and Fast Models: from 2D to 3D</td>
<td>Han</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Oral Session 1</td>
<td>Yu, Hartmann, Li, Shafiee, Yang, Zafrir</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Cheap, Fast, and Low Power Deep Learning: I need it now!</td>
<td>Delp</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>Advances and Prospects for In-memory Computing</td>
<td>Verma</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Algorithm-Accelerator Co-Design for Neural Network Specialization</td>
<td>Zhang</td>
</tr>
<tr>
<td>03:45 PM</td>
<td>Poster Session 2</td>
<td>Prato, Thakker, Galindez Olascoaga, Zhang, Partovi Nia, Adamczewski</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Adaptive Multi-Task Neural Networks for Efficient Inference</td>
<td>Feris</td>
</tr>
<tr>
<td>04:45 PM</td>
<td>Kernel and Graph Optimization for DL Model Execution</td>
<td>Lee</td>
</tr>
<tr>
<td>05:15 PM</td>
<td>Configurable Cloud-Scale DNN Processor for Real-Time AI</td>
<td>Darvish Rouhani</td>
</tr>
<tr>
<td>05:45 PM</td>
<td>Oral Session 2</td>
<td>Liao, McKinstry, Izsak, Li, Huang, Mordido</td>
</tr>
</tbody>
</table>

Abstracts (7):

Abstract 1: TBD in EMC2: Energy Efficient Machine Learning and Cognitive Computing (5th edition), LeCun 08:00 AM

TBD


Computing near the sensor is preferred over the cloud due to privacy and/or latency concerns for a wide range of applications including robotics/drones, self-driving cars, smart Internet of Things, and portable/wearable electronics. However, at the sensor there are often stringent constraints on energy consumption and cost in addition to the throughput and accuracy requirements of the application. In this talk, we will describe how joint algorithm and hardware design can be used to reduce energy consumption while delivering real-time and robust performance for applications including deep learning, computer vision, autonomous navigation/exploration and video/image processing. We will show how energy-efficient techniques that exploit correlation and sparsity to reduce compute, data movement and storage costs can be applied to various tasks including image classification, depth estimation, super-resolution, localization and mapping.


Machine learning (ML) applications have entered and impacted our lives unlike any other technology advance from the recent past. Indeed, almost every aspect of how we live or interact with others relies on or uses ML for applications ranging from image classification and object detection, to processing multimodal and heterogeneous datasets. While the holy grail for judging the quality of a ML model has largely been serving accuracy, and only recently its resource usage, neither of these metrics translate directly to energy efficiency, runtime, or mobile device battery lifetime. This talk will uncover the need for building accurate, platform-specific power and latency models for convolutional neural networks (CNNs) and efficient hardware-aware CNN design methodologies, thus allowing machine learners and hardware designers to identify not just the best accuracy NN configuration, but also those that satisfy given hardware constraints. Our proposed modeling framework is applicable to both high end and mobile platforms and achieves 88.24% accuracy for latency, 88.34% for power, and 97.21% for energy prediction. Using similar predictive models, we demonstrate a novel differentiable neural architecture search (NAS) framework, dubbed Single-Path NAS, that uses one single-path over-parameterized CNN to encode all architectural decisions based on shared convolutional kernel parameters. Single-Path NAS achieves state-of-the-art top-1 ImageNet accuracy (75.62%), outperforming existing mobile NAS methods for similar latency constraints (~80ms) and finds the final configuration up to 5,000× faster compared to prior work. Combined with our quantized CNNs (Flexible Lightweight CNNs or FLightNNs) that customize precision level in a layer-wise fashion and achieve almost iso-accuracy at 5-10x energy reduction, such a modeling, analysis, and optimization framework is poised to lead to true co-design of hardware and ML model, orders of magnitude faster than state of the art, while satisfying both accuracy and latency or energy constraints.

Deep Neural Net models have provided the most accurate solutions to a very wide variety of problems in vision, language, and speech; however, the design, training, and optimization of efficient DNNs typically requires resorting to the “dark arts” of ad hoc methods and extensive hyperparameter tuning. In this talk we present our progress on abandoning these dark arts by using Differential Neural Architecture Search to guide the design of efficient DNNs and by using Hessian-based methods to guide the processes of training and quantizing those DNNs.


In this talk I will describe the need for low power machine learning systems. I will motivate this by describing several current projects at Purdue University that have a need for energy efficient deep learning and in some cases the real deployment of these methods will not be possible without lower power solutions. The applications include precision farming, health care monitoring, and edge-based surveillance.


Edge AI applications retain the need for high-performing inference models, while driving platforms beyond their limits of energy efficiency and throughput. Digital hardware acceleration, enabling 10-100x gains over general-purpose architectures, is already widely deployed, but is ultimately restricted by data-movement and memory accessing that dominates deep-learning computations. In-memory computing, based on both SRAM and emerging memory, offers fundamentally new tradeoffs for overcoming these barriers, with the potential for 10x higher energy efficiency and area-normalized throughput demonstrated in recent designs. But, those tradeoffs instate new challenges, especially affecting scaling to the level of computations required, integration in practical heterogeneous architectures, and mapping of diverse software. This talk examines those tradeoffs to characterize the challenges. It then explores recent research that provides promising paths forward, making in-memory computing more of a practical reality than ever before.


In recent years, machine learning (ML) with deep neural networks (DNNs) has been widely deployed in diverse application domains. However, the growing complexity of DNN models, the slowdown of technology scaling, and the proliferation of edge devices are driving a demand for higher DNN performance and energy efficiency. ML applications have shifted from general-purpose processors to dedicated hardware accelerators in both academic and commercial settings. In line with this trend, there has been an active body of research on both algorithms and hardware architectures for neural network specialization.

This talk presents our recent investigation into DNN optimization and low-precision quantization, using a co-design approach featuring contributions to both algorithms and hardware accelerators. First, we review static network pruning techniques and show a fundamental link between group convolutions and circulant matrices — two previously disparate lines of research in DNN compression. Then we discuss channel gating, a dynamic, fine-grained, and trainable technique for DNN acceleration. Unlike static approaches, channel gating exploits input-dependent dynamic sparsity at run time. This results in a significant reduction in compute cost with a minimal impact on accuracy. Finally, we present outlier channel splitting, a technique to improve DNN weight quantization by removing outliers from the weight distribution without retraining.

Machine Learning for Health (ML4H): What makes machine learning in medicine different?

Andrew Beam, Tristan Naumann, Brett Beaulieu-Jones, Irene Y Chen, Sam Finlayson, Emily Alsentzer, Adrian Dalca, Matthew McDermott

West Ballroom A, Fri Dec 13, 08:00 AM

The goal of the NeurIPS 2019 Machine Learning for Health Workshop (ML4H) is to foster collaborations that meaningfully impact medicine by bringing together clinicians, health data experts, and machine learning researchers. Attendees at this workshop can also expect to broaden their network of collaborators to include clinicians and machine learning researchers who are focused on solving some of the most important problems in medicine and healthcare. The organizers of this proposal have successfully run NeurIPS workshops in the past and are well-equipped to run this year’s workshop should this proposal be accepted.

This year’s theme of “What makes machine learning in medicine different?” aims to elucidate the obstacles that make the development of machine learning models for healthcare uniquely challenging. To speak to this theme, we have received commitments to speak from some of the leading researchers and physicians in this area. Below is a list of confirmed speakers who have agreed to participate.

Luke Oakden-Raynor, MBBS (Adelaide)
Russ Altman, MD/PhD (Stanford)
Lilly Peng, MD/PhD (Google)
Daphne Koller, PhD (in sitro)
Jeff Dean, PhD (Google)

Attendees at the workshop will gain an appreciation for problems that are unique to the application of machine learning for healthcare and a better understanding of how machine learning techniques may be leveraged to solve important clinical problems. This year’s workshop builds on the last two NeurIPS ML4H workshops, which were both attended by more than 500 people each year, and helped form the foundations of an emerging research community.

Please see the attached document for the full program.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:45 AM</td>
<td>Daphne Koller Talk</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Spotlight Paper Talks</td>
</tr>
</tbody>
</table>

Page 35 of 87
09:45 AM Coffee Break
10:30 AM Alan Karthikesalingam & Nenad Tomasev Talk
11:00 AM Paper spotlight talks
11:20 AM Message from sponsor

11:30 AM Poster Session I

01:30 PM Emily Fox
02:00 PM Luke Oakden-Rayner Talk
02:30 PM Spotlight Paper Talks
03:00 PM Anna Goldenberg Talk
03:30 PM Coffee Break
04:15 PM Lily Peng & Dale Webster talk
04:45 PM Panel Discussion (Luke Oakden-Rayner, Emily Fox, Alan Karthikesalingam, Daphne Koller, Anna Goldenberg)

Abstract 2: Spotlight Paper Talks in Machine Learning for Health (ML4H): What makes machine learning in medicine different?.
Kapur, Raghu, Li 09:15 AM

"Non-Invasive Silent Speech Recognition in Multiple Sclerosis with Dysphonia", Arnav Kapur et al.

"Transfusion: Understanding Transfer Learning for Medical Imaging", Maithra Raghu et al.


Abstract 5: Paper spotlight talks in Machine Learning for Health (ML4H): What makes machine learning in medicine different?, Asif, Jaeger 11:00 AM

"Privacy Preserving Human Fall Detection using Video Data", Umar Asif et al.

"Retina U-Net: Embarrassingly Simple Exploitation of Segmentation Supervision for Medical Object Detection" Paul Jäger et al.

Abstract 8: Emily Fox in Machine Learning for Health (ML4H): What makes machine learning in medicine different?, Fox 01:30 PM

Models of Cognition: From Predicting Cognitive Impairment to the Brain Networks underlying Complex Cognitive Processes Talk

The ubiquity of smartphone usage in many people’s lives makes it a rich source of information about a person’s mental and cognitive state. In this talk, we first consider how such data sources can be used to provide insights into an individual’s potential cognitive impairment. Based on a study enriched with subjects diagnosed with mild cognitive impairment or Alzheimer’s disease, we develop structured models of users’ smartphone interactions to reveal differences in phone usage patterns between people with and without cognitive impairment. In particular, we focus on inferring specific types of phone usage sessions that are predictive of cognitive impairment. Our model achieves state-of-the-art results when discriminating between healthy and symptomatic subjects, and its interpretability enables novel insights into which aspects of phone usage strongly relate with cognitive health in our dataset.

We then turn to a scientific analysis of brain functioning underlying cognitive behaviors. Recent neuroimaging modalities, such as magnetoencephalography (MEG), provide rich descriptions of brain activity over time enabling new studies of the neural underpinnings of complex cognitive processes. We focus on inferring the functional connectivity of auditory attention using MEG recordings. We explore notions of undirected, contemporaneous interactions using sparse and interpretable deep generative models, as well as time-varying directed interactions using Bayesian dynamical models.

Abstract 10: Spotlight Paper Talks in Machine Learning for Health (ML4H): What makes machine learning in medicine different?, Rozenberg, Wei, Xu 02:30 PM

“Localization with Limited Annotation for Chest X-rays”, Eyal Rozenberg et al.

“Generative Image Translation for Data Augmentation in Colorectal Histopathology Images”, Jerry Wei et al.
Meta-Learning

Roberto Calandra, Ignasi Clavera Gilaberte, Frank Hutter, Joaquin Vanschoren, Jane Wang

West Ballroom B, Fri Dec 13, 08:00 AM

Recent years have seen rapid progress in metalearning methods, which learn (and optimize) the performance of learning methods based on data, generate new learning methods from scratch, and learn to transfer knowledge across tasks and domains. Metalearning can be seen as the logical conclusion of the arc that machine learning has undergone in the last decade, from learning classifiers, to learning representations, and finally to learning algorithms that themselves acquire representations and classifiers. The ability to improve one’s own learning capabilities through experience can also be viewed as a hallmark of intelligent beings, and there are strong connections with work on human learning in neuroscience. The goal of this workshop is to bring together researchers from all the different communities and topics that fall under the umbrella of metalearning. We expect that the presence of these different communities will result in a fruitful exchange of ideas and stimulate an open discussion about the current challenges in metalearning, as well as possible solutions.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>09:10 AM</td>
<td>Meta-learning as hierarchical modeling</td>
</tr>
<tr>
<td>09:40 AM</td>
<td>How Meta-Learning Could Help Us Accomplish Our Grandest AI Ambitions, and Early, Exotic Steps in that Direction</td>
</tr>
<tr>
<td>10:10 AM</td>
<td>Poster Spotlights 1</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Poster Spotlights 2</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Interaction of Model-based RL and Meta-RL</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Discussion 1</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Abstraction &amp; Meta-Reinforcement Learning</td>
</tr>
</tbody>
</table>

Abstracts (3):

Abstract 3: How Meta-Learning Could Help Us Accomplish Our Grandest AI Ambitions, and Early, Exotic Steps in that Direction in Meta-Learning, Clune 09:40 AM

A dominant trend in machine learning is that hand-designed pipelines are replaced by higher-performing learned pipelines once sufficient compute and data are available. I argue that trend will apply to machine learning itself, and thus that the fastest path to truly powerful AI is to create AI-generating algorithms (AI-GAs) that on their own learn to solve the hardest AI problems. This paradigm is an all-in bet on meta-learning. To produce AI-GAs, we need work on Three Pillars: meta-learning architectures, meta-learning algorithms, and automatically generating environments. In this talk I will present recent work from our team in each of the three pillars: Pillar 1: Generative Teaching Networks (GTNs); Pillar 2: Differential plasticity, differentiable neuromodulated plasticity (“backpropamine”), and a Neuromodulated Meta-Learning algorithm (ANML); Pillar 3: the Paired Open-Ended Trailblazer (POET). My goal is to motivate future research into each of the three pillars and their combination.

Abstract 8: Abstraction & Meta-Reinforcement Learning in Meta-Learning, Abel 02:00 PM

Reinforcement learning is hard in a fundamental sense: even in finite and deterministic environments, it can take a large number of samples to find a near-optimal policy. In this talk, I discuss the role that abstraction can play in achieving reliable yet efficient learning and planning. I first introduce classes of state abstraction that induce a trade-off between optimality and the size of an agent’s resulting abstract model, yielding a practical algorithm for learning useful and compact representations from a demonstrator. Moreover, I show how these learned, simple representations can underlie efficient learning in complex environments.
Second, I analyze the problem of searching for options that make planning more efficient. I present new computational complexity results that illustrate it is NP-hard to find the optimal options that minimize planning time, but show this set can be approximated in polynomial time. Collectively, these results provide a partial path toward abstractions that minimize the difficulty of high quality learning and decision making.

Abstract 14: Compositional generalization in minds and machines in Meta-Learning. Lake 05:00 PM

People learn in fast and flexible ways that elude the best artificial neural networks. Once a person learns how to “dax,” they can effortlessly understand how to “dax twice” or “dax vigorously” thanks to their compositional skills. In this talk, we examine how people and machines generalize compositionally in language-like instruction learning tasks. Artificial neural networks have long been criticized for lacking systematic compositionality (Fodor & Pylyshyn, 1988; Marcus, 1998), but new architectures have been tackling increasingly ambitious language tasks. In light of these developments, we reevaluate these classic criticisms and find that artificial neural nets still fall spectacularly when systematic compositionality is required. We then show how people succeed in similar few-shot learning tasks and find they utilize three inductive biases that can be incorporated into models. Finally, we show how more structured neural nets can acquire compositional skills and human-like inductive biases through meta-learning.

Biological and Artificial Reinforcement Learning

Raymond Chua, Sara Zannone, Feryal Behbahani, Rui Ponte Costa, Claudia Clopath, Blake Richards, Doina Precup

West Ballroom C, Fri Dec 13, 08:00 AM

Reinforcement learning (RL) algorithms learn through rewards and a process of trial-and-error. This approach was strongly inspired by the study of animal behaviour and has led to outstanding achievements in machine learning (e.g. in games, robotics, science). However, artificial agents still struggle with a number of difficulties, such as sample efficiency, learning in dynamic environments and over multiple timescales, generalizing and transferring knowledge. On the other end, biological agents excel at these tasks. The brain has evolved to adapt and learn in dynamic environments, while integrating information and learning on different timescales and for different duration. Animals and humans are able to extract information from the environment in efficient ways by directing their attention and actively choosing what to focus on. They can achieve complicated tasks by solving sub-problems and combining knowledge as well as representing the environment in efficient ways and plan their decisions off-line. Neuroscience and cognitive science research has largely focused on elucidating the workings of these mechanisms. Learning more about the neural and cognitive underpinnings of these functions could be key to developing more intelligent and autonomous agents. Similarly, having a computational and theoretical framework, together with a normative perspective to refer to, could and does contribute to elucidate the mechanisms used by animals and humans to perform these tasks. Building on the connection between biological and artificial reinforcement learning, our workshop will bring together leading and emergent researchers from Neuroscience, Psychology and Machine Learning to share: (i) how neural and cognitive mechanisms can provide insights to tackle challenges in RL research and (ii) how machine learning advances can help further our understanding of the brain and behaviour.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Invited Talk #1: From brains to agents and back</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break &amp; Poster Session</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Contributed Talk #1: Humans flexibly transfer options at multiple levels of abstractions</td>
</tr>
<tr>
<td>10:45 AM</td>
<td>Contributed Talk #2: Slow processes of neurons enable a biologically plausible approximation to policy gradient</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Invited Talk 2: Understanding information demand at different levels of complexity</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Invited Talk #3: Predictive Cognitive Maps with Multi-scale Successor Representations and Replay</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch Break &amp; Poster Session</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Invited Talk #4: Multi-Agent Interaction and Online Optimization in RL</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Invited Talk #5 : Materials Matter: How biologically inspired alternatives to conventional neural networks improve meta-learning and continual learning</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Invited Talk #6: Features or Bugs: Synergistic Idiosyncrasies in Human Learning and Decision-Making</td>
</tr>
</tbody>
</table>
Contributed Talk #3: MEMENTO: Further Progress Through Forgetting

Invited Talk #7: Richard Sutton

Panel Discussion led by Grace Lindsay

Abstracts (8):

Abstract 4: Contributed Talk #1: Humans flexibly transfer options at multiple levels of abstractions in Biological and Artificial Reinforcement Learning. Xia 10:30 AM

Humans are great at using prior knowledge to solve novel tasks, but how they do so is not well understood. Recent work showed that in contextual multi-armed bandits environments, humans create simple one-step policies that they can transfer to new contexts by inferring context clusters. However, the daily tasks humans face are often temporally extended, and demand more complex, hierarchically structured skills. The options framework provides a potential solution for representing such transferable skills. Options are abstract multi-step policies, assembled from simple actions or other options, that can represent meaningful reusable skills. We developed a novel two-stage decision making protocol to test if humans learn and transfer multi-step options. We found transfer effects at multiple levels of policy complexity that could not be explained by flat reinforcement learning models. We also devised an option model that can qualitatively replicate the transfer effects in human participants. Our results provide evidence that humans create options, and use them to explore in novel contexts, consequently transferring past knowledge and speeding up learning.

Abstract 5: Contributed Talk #2: Slow processes of neurons enable a biologically plausible approximation to policy gradient in Biological and Artificial Reinforcement Learning. Maass 10:45 AM

Recurrent neural networks underlie the astounding information processing capabilities of the brain, and play a key role in many state-of-the-art algorithms in deep reinforcement learning. But it has remained an open question how such networks could learn from rewards in a biologically plausible manner, with synaptic plasticity that is both local and online. We describe such an algorithm that approximates actor-critic policy gradient in recurrent neural networks. Building on an approximation of backpropagation through time (BPTT): e-prop, and using the equivalence between forward and backward view in reinforcement learning (RL), we formulate a novel learning rule for RL that is both online and local, called reward-based e-prop. This learning rule uses neuroscience inspired slow processes and top-down signals, while still being rigorously derived as an approximation to actor-critic policy gradient. To empirically evaluate this algorithm, we consider a delayed reaching task, where an arm is controlled using a recurrent network of spiking neurons. In this task, we show that reward-based e-prop performs as well as an agent trained with actor-critic policy gradient with biologically implausible BPTT.
intrinsic motivation in environments that have sparse rewards and complex structures. These findings can lead to novel directions of human and animal experimentation. I will summarize behavioral and neural findings in human and rodent studies by us and other groups and discuss the road ahead.

Abstract 9: Invited Talk #4: Multi-Agent Interaction and Online Optimization in RL in Biological and Artificial Reinforcement Learning, Mordatch 02:00 PM

AI and robotics have made inspiring progress over the recent years on training systems to solve specific, well-defined tasks. But the need to specify tasks bounds the level of complexity that can ultimately be reached in training with such an approach. The sharp distinction between training and deployment stages likewise limits the degree to which these systems can improve and adapt after training. In my talk, I will advocate for multi-agent interaction and online optimization processes as key ingredients to towards overcoming these limitations.

In the first part, I will show that through multi-agent competition, a simple objective such as hide-and-seek game, and standard reinforcement learning algorithms at scale, agents can create a self-supervised autocurriculum with multiple distinct rounds of emergent strategy, many of which require sophisticated tool use and coordination. Multi-agent interaction leads to behaviors that center around more human-relevant skills than other self-supervised reinforcement learning methods such as intrinsic motivation and holds promise of open-ended growth of complexity.

In the second part, I will argue for usefulness and generality of online optimization processes and show examples of incorporating them in model-based control and generative modeling contexts via energy-based models. I will show intriguing advantages, such as compositionality, robustness to distribution shift, non-stationarity, and adversarial attacks in generative modeling problems and planned exploration and fast adaptation to changing environments in control problems.

This is joint work with many wonderful colleagues and students at OpenAI, MIT, University of Washington, and UC Berkeley.

Abstract 10: Invited Talk #5 : Materials Matter: How biologically inspired alternatives to conventional neural networks improve meta-learning and continual learning in Biological and Artificial Reinforcement Learning, Clune 02:30 PM

I will describe how alternatives to conventional neural networks that are very loosely biologically inspired can improve meta-learning, including continual learning. First I will summarize differentiable Hebbian learning and differentiable neuromodulated Hebbian learning (aka “backpropamine”). Both are techniques for training deep neural networks with synaptic plasticity, meaning the weights can change during meta-testing/inference. Whereas meta-learned RNNs can only store within-episode information in their activations, such plastic Hebbian networks can store information in their weights in addition to its activations, improving performance on some classes of problems. Second, I will describe a new, unpublished method that improves the state of the art in continual learning, ANML (A Neuromodulated Meta-Learning algorithm) meta-learns a neuromodulatory network that gates the activity of the main prediction network, enabling the learning of up to 600 simple tasks sequentially.

Abstract 11: Invited Talk #6: Features or Bugs: Synergistic Idiosyncrasies in Human Learning and Decision-Making in Biological and Artificial Reinforcement Learning, Yu 03:00 PM

Combining a multi-armed bandit task and Bayesian computational modeling, we find that humans systematically underestimate reward availability in the environment. This apparent pessimism turns out to be an optimism bias in disguise, and one that compensates for other idiosyncrasies in human learning and decision-making under uncertainty, such as a default tendency to assume non-stationarity in environmental statistics as well as the adoption of a simplistic decision policy. In particular, reward rate underestimation discourages the decision-maker from switching away from a “good” option, thus achieving near-optimal behavior (which never switches away after a win). Furthermore, we demonstrate that the Bayesian model that best predicts human behavior is equivalent to a particular form of Q-learning often used in the brain sciences, thus providing statistical, normative grounding to phenomenological models of human and animal behavior.

Abstract 13: Contributed Talk #3 MEMENTO: Further Progress Through Forgetting in Biological and Artificial Reinforcement Learning, Fedus 04:15 PM

Modern Reinforcement Learning (RL) algorithms, even those with intrinsic reward bonuses, suffer performance plateaus in hard-exploration domains suggesting these algorithms have reached their ceiling. However, in what we describe as the MEMENTO observation, we find that new agents launched from the position where the previous agent saturated, can reliably make further progress. We show that this is not an artifact of limited model capacity or training duration, but rather indicative of interference in learning dynamics between various stages of the domain [Schaul et al., 2019], signatures of multi-task and continual learning. To mitigate interference we design an end-to-end learning agent which partitions the environment into various segments, and models the value function separately in each score context per Jain et al. [2019]. We demonstrate increased learning performance by this ensemble of agents on Montezuma’s Revenge and further show how this ensemble can be distilled into a single agent with the same model capacity as the original learner. Since the solution is empirically expressible by the original network, this provides evidence of interference and our approach validates an avenue to circumvent it.

Graph Representation Learning

Will Hamilton, Rianne van den Berg, Michael Bronstein, Stefanie Jegelka, Thomas Kipf, Jure Leskovec, Renjie Liao, Yizhou Sun, Petar Veli

West Exhibition Hall A, Fri Dec 13, 08:00 AM

Graph-structured data is ubiquitous throughout the natural and social sciences, from telecommunication networks to quantum chemistry. Building relational inductive biases into deep learning architectures is crucial if we want systems that can learn, reason, and generalize from this kind of data. Furthermore, graphs can be seen as a natural generalization of simpler kinds of structured data (such as images), and therefore, they represent a natural avenue for the next breakthroughs in machine learning.

Recent years have seen a surge in research on graph representation
learning, including techniques for deep graph embeddings, generalizations of convolutional neural networks to graph-structured data, and neural message-passing approaches inspired by belief propagation. These advances in graph neural networks and related techniques have led to new state-of-the-art results in numerous domains, including chemical synthesis, 3D-vision, recommender systems, question answering, and social network analysis.

The workshop will consist of contributed talks, contributed posters, and invited talks on a wide variety of methods and problems related to graph representation learning. We will welcome 4-page original research papers on work that has not previously been published in a machine learning conference or workshop. In addition to traditional research paper submissions, we will also welcome 1-page submissions describing open problems and challenges in the domain of graph representation learning. These open problems will be presented as short talks (5-10 minutes) immediately preceding a coffee break to facilitate and spark discussions.

The primary goal for this workshop is to facilitate community building; with hundreds of new researchers beginning projects in this area, we hope to bring them together to consolidate this fast-growing area of graph representation learning into a healthy and vibrant subfield.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:40 AM</td>
<td>Opening remarks</td>
<td>Hamilton</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Marco Gori: Graph Representations, Backpropagation, and Biological Plausibility</td>
<td>Gori</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Peter Battaglia: Graph Networks for Learning Physics</td>
<td>Battaglia</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Open Challenges - Spotlight Presentations</td>
<td>Sumba Toral, Maron, Kolbeinsson</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Andrew McCallum: Learning DAGs and Trees with Box Embeddings and Hyperbolic Embeddings</td>
<td>McCallum</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Poster Session #1</td>
<td></td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Outstanding Contribution Talk: Pre-training Graph Neural Networks</td>
<td>Liu</td>
</tr>
</tbody>
</table>

Abstracts (3):

Abstract 2: Marco Gori: Graph Representations, Backpropagation, and Biological Plausibility in Graph Representation Learning, Gori

09:00 AM

Neural architectures and many learning environments can conveniently be expressed by graphs. Interestingly, it has been recently shown that the notion of receptive field and the correspondent convolutional computation can nicely be extended to graph-based data domains with successful results. On the other hand, graph neural networks (GNN) were introduced by extending the notion of time-unfolding, which ended up into a state-based representation along with a learning process that requires state relaxation to a fixed-point. It turns out that algorithms based on this approach applied to learning tasks on
collections of graphs are more computationally expensive than recent graph convolutional nets.

In this talk we advocate the importance of refreshing state-based graph representations in the spirit of the early introduction of GNN for the case of “network domains” that are characterized by a single graph (e.g. traffic nets, social nets). In those cases, data over the graph turn out to be a continuous stream, where time plays a crucial role and blurs the classic statistical distinction between training and test set. When expressing the graphical domain and the neural network within the same Lagrangian framework for dealing with constraints, we show novel learning algorithms that seem to be very appropriate for network domains. Finally, we show that in the proposed learning framework, the Lagrangian multipliers are associated with the delta term of Backpropagation, and provide intriguing arguments on its biological plausibility.

**Abstract 3:** Peter Battaglia: Graph Networks for Learning Physics in Graph Representation Learning, Battaglia 09:30 AM

I’ll describe a series of studies that use graph networks to reason about and interact with complex physical systems. These models can be used to predict the motion of bodies in particle systems, infer hidden physical properties, control simulated robotic systems, build physical structures, and interpret the symbolic form of the underlying laws that govern physical systems. More generally, this work underlines graph neural networks’ role as a first-class member of the deep learning toolkit.

**Abstract 15:** Bistra Dilkina: Graph Representation Learning for Optimization on Graphs in Graph Representation Learning, Dilkina 04:15 PM

Numerous real world applications involve discrete optimization problems on graphs, many of which are NP-hard and hence developing effective combinatorial algorithms is a research challenge. In this talk, I will show how leveraging the power of machine learning, and in particular graph representation learning, can provide a new paradigm for designing data-driven algorithms to solve combinatorial graph optimization problems. Our approaches automatically learn solution strategies from distribution of instances by explicitly considering the combinatorial task during training. We show that we match and often outperform hand-designed algorithms both with learning greedy algorithms for Minimum Vertex Cover, Maxcut and TSP, as well as when using our new framework ClusterNet to learn a graph representation for an efficient differential kmeans proxy for graph problems such as partitioning for Community Detection and node selection for Facility Location.

Bayesian Deep Learning

Yarin Gal, Jose Miguel Hernández-Lobato, Christos Louizos, Eric Nalisnick, Zoubin Ghahramani, Kevin Murphy, Max Welling

West Exhibition Hall C, Fri Dec 13, 08:00 AM

Extending on the workshop’s success from the past 3 years, this workshop will study the developments in the field of Bayesian deep learning (BDL) over the past year. The workshop 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. Future directions for the field will be debated in a panel discussion.

Speakers:
- Andrew Wilson
- Deborah Marks
- Jasper Snoek
- Roger Grosse
- Chelsea Finn
- Yingzhen Li
- Alexander Matthews

Workshop summary:
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, with the introduction of new deep learning models that take advantage of Bayesian techniques, and Bayesian models that incorporate deep learning elements. Many ideas from the 1990s are now being revisited in light of recent advances in the fields of approximate inference and deep learning, yielding many exciting new results.

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening remarks</td>
</tr>
<tr>
<td>08:05 AM</td>
<td>Invited talk</td>
</tr>
<tr>
<td>08:25 AM</td>
<td>Contributed talk</td>
</tr>
<tr>
<td>08:40 AM</td>
<td>Invited talk 2</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Contributed talk 2</td>
</tr>
<tr>
<td>09:20 AM</td>
<td>Poster spotlights</td>
</tr>
</tbody>
</table>
09:35 AM  **Poster session**

10:35 AM  **Invited talk 3**

10:55 AM  **Contributed talk 3**

11:10 AM  **Invited talk 4**

11:30 AM  **Contributed talk 4**

01:20 PM  **Invited talk 5**

01:40 PM  **Contributed talk 5**

01:55 PM  **Invited talk 6**

02:10 PM  **Contributed talk 6**

02:30 PM  **Poster session 2**

03:30 PM  **Contributed talk 7**

03:50 PM  **Invited talk 7**

04:05 PM  **Contributed talk 8**

04:30 PM  **Panel session**

05:30 PM  **Poster session 3**
Real Neurons & Hidden Units: future directions at the intersection of neuroscience and AI

Guillaume Lajoie, Eli Shlizerman, Maximilian Puelma Touzel, Jessica Thompson, Konrad Kording

East Ballroom A, Sat Dec 14, 08:00 AM

Recent years have witnessed an explosion of progress in AI. With it, a proliferation of experts and practitioners are pushing the boundaries of the field without regard to the brain. This is in stark contrast with the field's transdisciplinary origins, when interest in designing intelligent algorithms was shared by neuroscientists, psychologists and computer scientists alike. Similar progress has been made in neuroscience where novel experimental techniques now afford unprecedented access to brain activity and function. However, it is unclear how to maximize them to truly advance an end-to-end understanding of biological intelligence. The traditional neuroscience research program, however, lacks frameworks to truly advance an end-to-end understanding of biological intelligence. For the first time, mechanistic discoveries emerging from deep learning, reinforcement learning and other AI fields may be able to steer fundamental neuroscience research in ways beyond standard uses of machine learning for modelling and data analysis. For example, successful training algorithms in artificial networks, developed without biological constraints, can motivate research questions and hypotheses about the brain. Conversely, a deeper understanding of brain computations at the level of large neural populations may help shape future directions in AI. This workshop aims to address this novel situation by building on existing AI-Neuro relationships but, crucially, outline new directions for artificial systems and next-generation neuroscience experiments. We invite contributions concerned with the modern intersection between neuroscience and AI and in particular, addressing questions that can only now be tackled due to recent progress in AI on the role of recurrent dynamics, inductive biases to guide learning, global versus local learning rules, and interpretability of network activity. This workshop will promote discussion and showcase diverse perspectives on these open questions.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 08:15 AM | Opening Remarks  
Lajoie, Thompson, Puelma Touzel, Shlizerman, Kording |
| 08:30 AM | Invited Talk: Hierarchical Reinforcement Learning: Computational Advances and Neuroscience Connections  
Precup |
| 09:00 AM | Invited Talk: Deep learning without weight transport  
Lillicrap |
| 09:30 AM | Contributed talk: Eligibility traces provide a data-inspired alternative to backpropagation through time.  
Guillaume Bellec, Franz Scherr, Elias Hajek, Darjan Salaj, Anand Subramoney, Robert Legenstein, Wolfgang Maass |
| 09:45 AM | Coffee Break + Posters |
| 10:30 AM | Invited Talk: Computing and learning in the presence of neural noise  
Savin |
| 11:00 AM | Invited Talk: Universality and individuality in neural dynamics across large populations of recurrent networks  
Sussillo |
| 11:30 AM | Contributed talk: How well do deep neural networks trained on object recognition characterize the mouse visual system?  
Santiago A. Cadena, Fabian H. Sinz, Taliah Muhammad, Emmanouil Froudarakis, Erick Cobos, Edgar Y. Walker, Jake Reimer, Matthias Bethge, |
| 11:45 AM | Contributed talk: Functional Annotation of Human Cognitive States using Graph Convolution Networks  
Yu Zhang, Pierre Bellec |
| 12:00 PM | Lunch Break |
| 02:00 PM | Invited Talk: Simultaneous rigidity and flexibility through modularity in cognitive maps for navigation  
Fiete |
| 02:30 PM | Invited Talk: Theories for the emergence of internal representations in neural networks: from perception to navigation  
Ganguli |
| 03:00 PM | Contributed talk: Adversarial Training of Neural Encoding Models on Population Spike Trains  
Poornima Ramesh, Mohamad Atayi, Jakob H Macke |
Recent advances in machine learning have been made possible by employing the backpropagation-of-error algorithm. Backprop enables the delivery of detailed error feedback across multiple layers of representation to adjust synaptic weights, allowing us to effectively train even very large networks. Whether or not the brain employs similar deep learning algorithms remains contentious; how it might do so remains a mystery. In particular, backprop uses the weights in the forward pass of the network to precisely compute error feedback in the backward pass. This way of computing errors across multiple layers is fundamentally at odds with what we know about the local computations of brains. We will describe new proposals for biologically motivated learning algorithms that are as effective as backpropagation without requiring weight transport.

Abstract 6: Invited Talk: Computing and learning in the presence of neural noise in Real Neurons & Hidden Units: future directions at the intersection of neuroscience and AI, Richards 04:45 AM

One key distinction between artificial and biological neural networks is the presence of noise, both intrinsic, e.g. due to synaptic failures, and extrinsic, arising through complex recurrent dynamics. Traditionally, this noise has been viewed as a 'bug', and the main computational challenge that the brain needs to face. More recently, it has been argued that circuit stochasticity may be a 'feature', in that can be recruited for useful computations, such as representing uncertainty about the state of the world. Here we lay out a new argument for the role of stochasticity during learning. In particular, we use a mathematically tractable stochastic neural network model that allows us to derive local plasticity rules for understanding hierarchical inference in the neocortex, and potentially guide circuit function.

Abstract 17: Invited Talk: Sensory prediction error signals in the neocortex in Real Neurons & Hidden Units: future directions at the intersection of neuroscience and AI, Richards 04:45 PM

Many models have postulated that the neocortex implements hierarchical inference system, whereby each region sends predictions of the inputs it expects to lower-order regions, allowing the latter to learn from any prediction errors. The combining of top-down predictions with bottom-up sensory information to generate errors that can then be communicated across the hierarchy is critical to credit assignment in deep predictive learning algorithms. Indirect experimental evidence supporting a hierarchical prediction system in the neocortex comes from both human and animal work. However, direct evidence for top-down guided prediction errors in the neocortex that can be used for deep credit assignment during unsupervised learning remains limited. Here, we address this issue with 2-photon calcium imaging of layer 2/3 and layer 5 pyramidal neurons in the primary visual cortex of awake mice during passive exposure to visual stimuli where unexpected events occur. To assess the evidence for top-down guided prediction errors we recorded from both the somatic compartments, and the apical dendrites in layer 1, where a large number of top-down inputs are received. We find evidence for a diversity of prediction error signals depending on both the stimulus type and cell type. These signals can be learnt in some cases, and in turn, they appear to drive some learning. This data will help us to both understand hierarchical inference in the neocortex, and potentially guide new unsupervised techniques for machine learning.
Fair ML in Healthcare

Shalmali Joshi, Irene Y Chen, Shems Saleh

East Ballroom B, Sat Dec 14, 08:00 AM

Clinical healthcare has been a natural application domain for ML with a few modest success stories of practical deployment. Inequity and healthcare disparity has long been a concern in clinical and public health for decades. However, the challenges of fair and equitable care using ML in health has largely remained unexplored. While a few works have attempted to highlight potential concerns and pitfalls in recent years, there are massive gaps in academic ML literature in this context. The goal of this workshop is to investigate issues around fairness that are specific to ML based healthcare. We hope to investigate a myriad of questions via the workshop.

Schedule

09:00 AM  Check-in and set up contributed posters
09:15 AM  Opening Remarks
09:30 AM  Keynote - Milind Tambe
10:00 AM  Invited Talk - Zlad Obermeyer  Obermeyer
10:30 AM  Coffee Break and Poster Session
11:00 AM  Breakout Sessions
12:45 PM  Lunch Break
02:00 PM  Invited Talk - Sharad Goel
02:30 PM  Invited Talk - Noa Dagan/Noam Barda  Barda, Dagan
03:00 PM  Invited Talk - Chelsea Barabas
03:30 PM  Coffee Break and Poster Session
04:00 PM  Discussion Panel - All invited speakers will be panelists
05:00 PM  Spotlight Talks and Poster Session

Tackling Climate Change with ML

David Rolnick, Priya Donti, Lynn Kaack, Alexandre Lacoste, Tegan Maharaj, Andrew Ng, John Platt, Jennifer Chayes, Joshua Bengio

East Ballroom C, Sat Dec 14, 08:00 AM

Climate change is one of the greatest problems society has ever faced, with increasingly severe consequences for humanity as natural disasters multiply, sea levels rise, and ecosystems falter. Since climate change is a complex issue, action takes many forms, from designing smart electric grids to tracking greenhouse gas emissions through satellite imagery. While no silver bullet, machine learning can be an invaluable tool in fighting climate change via a wide array of applications and techniques. These applications require algorithmic innovations in machine learning and close collaboration with diverse fields and practitioners. This workshop is intended as a forum for those in the machine learning community who wish to help tackle climate change.

Schedule

08:15 AM  Welcome and Opening Remarks
08:30 AM  Jeff Dean (Google AI)  Dean
09:05 AM  Spotlight talks
09:45 AM  Coffee Break + Poster Session
10:30 AM  Felix Creutzig (TU Berlin, MCC)  Creutzig
11:05 AM  Spotlight talks
11:15 AM  Climate Change: A Grand Challenge for ML  Bengio, Gomes, Ng, Dean, Mackey
12:00 PM  Lunch + Poster Session
02:00 PM  Carla Gomes (Cornell)  Gomes
Joint Workshop on AI for Social Good

Fei Fang, Joseph Bullock, Marc-Antoine Dilhac, Brian Green, natalie saltiel, Dhaval Adnodah, Jack Clark, Sean McGregor, Margaux Luck, Jonnie Penn, Tristan Sylvaarin, Geneviève Boucher, Sydney Swaine-Simon, Gimaw Abebe Tadesse, Myriam Côté, Anna Bethke, Yoshua Bengio

East Meeting Rooms 11 + 12, Sat Dec 14, 08:00 AM

The accelerating pace of intelligent systems research and real world deployment presents three clear challenges for producing “good” intelligent systems: (1) the research community lacks incentives and venues for results centered on social impact, (2) deployed systems often produce unintended negative consequences, and (3) there is little consensus for public policy that maximizes “good” social impacts, while minimizing the likelihood of harm. As a result, researchers often find themselves without a clear path to positive real world impact.

The Workshop on AI for Social Good addresses these challenges by bringing together machine learning researchers, social impact leaders, ethicists, and public policy leaders to present their ideas and applications for maximizing the social good. This workshop is a collaboration of three formerly separate lines of research (i.e., this is a "joint" workshop), including researchers in applications-driven AI research, applied ethics, and AI policy. Each of these research areas are unified into a 3-track framework promoting the exchange of ideas between the practitioners of each track.

We hope that this gathering of research talent will inspire the creation of new approaches and tools, provide for the development of intelligent systems benefiting all stakeholders, and converge on public policy mechanisms for encouraging these goals.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening remarks</td>
</tr>
<tr>
<td>08:05 AM</td>
<td>Computational Sustainability: Computing for a Better World and a Sustainable Future</td>
</tr>
<tr>
<td>08:25 AM</td>
<td>Translating AI Research into operational impact to achieve the Sustainable Development Goals</td>
</tr>
</tbody>
</table>
Speaker bio:
Yoshua Bengio is Full Professor of the Department of Computer Science and Operations Research, scientific director of Mila, CIFAR Program co-director of the CIFAR Learning in Machines and Brains program (formerly Neural Computation and Adaptive Perception), scientific director of IVADO and Canada Research Chair in Statistical Learning Algorithms. His main research ambition is to understand principles of learning that yield intelligence. He supervises a large group of graduate students and post-docs. His research is widely cited (over 130000 citations found by Google Scholar in August 2018, with an H-index over 120, and rising fast).

Abstract 2: **Computational Sustainability: Computing for a Better World and a Sustainable Future in Joint Workshop on AI for Social Good**, Gomes 08:05 AM

Computational sustainability is a new interdisciplinary research field with the overarching goal of developing computational models, methods, and tools to help manage the balance of environmental, economic, and societal needs for a sustainable future. I will provide a short overview of computational sustainability, with examples ranging from wildlife conservation and biodiversity to evaluating the impacts of hydropower dam proliferation in the Amazon basin. Our research leverages the recent artificial intelligence (AI) advances in deep learning, reasoning, and decision making. I will highlight cross-cutting computational themes, how AI enriches sustainability sciences and conversely, how sustainability questions enrich AI and computer science.
Abstract 5: Balancing Competing Objectives for Welfare-Aware Machine Learning with Imperfect Data in Joint Workshop on AI for Social Good, Rolf 09:15 AM

From financial loans and humanitarian aid, to medical diagnosis and criminal justice, consequential decisions in society increasingly rely on machine learning. In most cases, the machine learning algorithms used in these contexts are trained to optimize a single metric of performance; however, most real-world decisions exist in a multi-objective setting that requires the balance of multiple incentives and outcomes. To this end, we develop a methodology for optimizing multi-objective decisions. Building on the traditional notion of Pareto optimality, we focus on understanding how to balance multiple objectives when those objectives are measured noisily or not directly observed. We believe this regime of imperfect information is far more common in real-world decisions, where one cannot easily measure the social consequences of an algorithmic decision. To show how the multi-objective framework can be used in practice, we present results using data from roughly 40,000 videos promoted by YouTube’s recommendation algorithm. This illustrates the empirical trade-off between maximizing user engagement and promoting high-quality videos. We show that multi-objective optimization could produce substantial increases in average video quality at the expense of almost negligible reductions in user engagement.

Speaker bio:
Esther Rolf is a 4th year Ph.D. student in the Computer Science department at the University of California, Berkeley, advised by Benjamin Recht and Michael I. Jordan. She is an NSF Graduate Research Fellow and is a fellow in the Global Policy Lab in the Goldman School of Public Policy at UC Berkeley. Esther’s research targets machine learning algorithms that interact with society. Her current focus lies in two main domains: the field of algorithmic fairness, which aims to design and audit black-box decision algorithms to ensure equity and benefit for all individuals, and in machine learning for environmental monitoring, where abundant sources of temporally recurrent data provide an exciting opportunity to make inferences and predictions about our planet.

Abstract 6: Dilated LSTM with ranked units for Classification of suicide note in Joint Workshop on AI for Social Good, Schoene 09:20 AM

Recent statistics in suicide prevention show that people are increasingly posting their last words online and with the unprecedented availability of textual data from social media platforms researchers have the opportunity to analyse such data. This work focuses on identifying suicide notes from other types of text in a document-level classification task, using a hierarchical recurrent neural network to uncover linguistic patterns in the data.

Speaker bio:
Annika Marie Schoene is a third-year PhD candidate in Natural Language Processing at the University of Hull and is affiliated to IBM Research UK. The main focus of her work lies in investigating recurrent neural networks for fine-grained emotion detection in social media data. She also has an interest in mental health issues on social media, where she looks at how to identify suicidal ideation in textual data.

Abstract 7: Speech in Pixels: Automatic Detection of Offensive Memes for Moderation in Joint Workshop on AI for Social Good, Giro-i-Nieto 09:25 AM

This work addresses the challenge of hate speech detection in Internet memes, and attempts using visual information to automatically detect hate speech, unlike previous works that have focused in language.

Speaker bio:
Xavier Giro-i-Nieto is an associate professor at the Universitat Politècnica de Catalunya (UPC) in Barcelona and visiting researcher at Barcelona Supercomputing Center (BSC). His obtained his doctoral degree from UPC in 2012 under the supervision of Prof. Ferran Marques (UPC) and Prof. Shih-Fu Chang (Columbia University). His research interests focus on deep learning applied to multimedia and reinforcement learning.

Abstract 8: Towards better healthcare: What could and should be automated? in Joint Workshop on AI for Social Good, Fruehwirt 09:30 AM

While artificial intelligence (AI) and other automation technologies might lead to enormous progress in healthcare, they may also have undesired consequences for people working in the field. In this interdisciplinary study, we capture empirical evidence of not only what healthcare work could be automated, but also what should be automated. We quantitatively investigate these research questions by utilizing probabilistic machine learning models trained on thousands of ratings, provided by both healthcare practitioners and automation experts. Based on our findings, we present an analytical tool (Automatability-Desirability Matrix) to support policymakers and organizational leaders in developing practical strategies on how to harness the positive power of automation technologies, while accompanying change and empowering stakeholders in a participatory fashion.

Speaker bio:
Wolfgang Frühwirt is an Associate Member of the Oxford-Man Institute (University of Oxford, Engineering Department), where he works with the Machine Learning Research Group.
Abstract 11: Towards a Social Good? Theories of Change in AI in Joint Workshop on AI for Social Good, saltiel, Richardson, Hamid
10:30 AM

Considerable hope and energy is put into AI -- and its critique -- under the assumption that the field will make the world a “better” place by maximizing social good. Will it? For who? At what time scale? Most importantly, who defines “social good”?

This panel invites dissent. Leading voices will pick apart these questions by sharing their own competing theories of social change in relation to AI. In addition to answering audience questions, they will share how they decide on trade-offs between pragmatism and principles and how they resist elements of AI research that are known to be dangerous and/or socially degenerative, particularly in relation to surveillance, criminal justice and privacy.

We undertake a probing and genuine conversation around these questions. Audience members are invited to submit questions at: https://app.slido.com/l/3v3/bm3/live/questions.

Facilitators bio:
Dhaval Adjodah is a research scientist at the MIT Media Lab. His research investigates the current limitations of generalization in machine learning as well as how to move beyond them by leveraging the social cognitive adaptations humans evolved to collaborate effectively at scale. Beyond pushing the limits of modern machine learning, he is also interested in improving institutions by using online human experiments to better understand the cognitive limits and biases that affect everyday individual economic, political, and social decisions. During his PhD, Dhaval was an intern in Prof. Yoshua Bengio’s group at MILA, a member of the Harvard Berkman Assembly on Ethics and Governance in Artificial Intelligence, and a fellow at the Dalai Lama Center For Ethics And Transformative Values. He has a B.S. in Physics from MIT, and an M.S. in Technology Policy from the MIT Institute for Data, Systems, and Society.

Natalie Saltiel (MIT)

Speakers bio:
Dr. Prem Natarajan is a Vice President in Amazon’s Alexa unit where he leads the Natural Understanding (NU) organization within Alexa AI. NU is a multidisciplinary science and engineering organization that develops, deploys, and maintains state-of-the-art conversational AI technologies including natural language understanding, intelligent dialog systems, entity linking and resolution, and associated worldwide runtime operations. Dr. Natarajan joined Amazon from the University of Southern California (USC) where he was Senior Vice Dean of Engineering in the Viterbi School of Engineering, Executive Director of the Information Sciences Institute (a 300-person R&D organization), and Research Professor of computer science with distinction. Prior to that, as Executive VP at Raytheon BBN Technologies, he led the speech, language, and multimedia business unit, which included research and development operations, and commercial products for real-time multimedia monitoring, document analysis, and information extraction. During his tenure at USC and at BBN, Dr. Natarajan directed R&D efforts in speech recognition, natural language processing, computer vision, and other applications of machine learning. While at USC, he directly led nationally influential DARPA and IARPA sponsored research efforts in biometrics/face recognition, OCR, NLP, media forensics, and forecasting. Most recently, he helped to launch the Fairness in AI (FAI) program – a collaborative effort between NSF and Amazon for funding fairness focused research efforts in US Universities.

Rashida Richardson: As Director of Policy Research, Rashida designs, implements, and coordinates AI Now’s research strategy and initiatives on the topics of law, policy, and civil rights. Rashida joins AI Now after working as Legislative Counsel at the American Civil Liberties Union of New York (NYCLU), where she led the organization’s work on privacy, technology, surveillance, and education issues. Prior to the NYCLU, she was a staff attorney at the Center for HIV Law and Policy, where she worked on a wide-range of HIV-related legal and policy issues nationally, and she previously worked at Facebook Inc. and HIP Investor in San Francisco. Rashida currently serves on the Board of Trustees of Wesleyan University, the Advisory Board of the Civil Rights and Restorative Justice Project, the Board of Directors of the College & Community Fellowship, and she is an affiliate and Advisory Board member of the Center for Critical Race + Digital Studies. She received her BA with honors in the College of Social Studies at Wesleyan University and her JD from Northeastern University School of Law.

Sarah T. Hamid is an abolitionist and organizer in Southern California, working to build community defense against carceral technologies. She's built and worked on campaigns against predictive policing, risk assessment technologies, public/private surveillance partnerships, electronic monitoring, and automated border screening. In March 2019, she co-founded the Prison Tech Research Group (PTR-Grp), a coalition of abolitionists working on the intersection of technology/innovation and the prison-industrial complex. PTR-Grp focuses on private-public research partnerships deployed under the guise of prison reform, which stage the prison as a site for technological innovation and low-cost testing. The project centers the needs and safety of incarcerated and directly impacted people who face the violently exploitative data science industry with few safety nets. Sarah also facilitates the monthly convening of the Community Defense Syllabus, during which activists of color from all over the country work to theorize the intersection of race and carceral computing. In 2020, she will lead the launch and roll-out of the Carceral Tech Resistance Network, a community archive and knowledge-sharing project that seeks to amplify the capacity of community organizations to resist the encroachment and experimentation of harmful technologies.

Abstract 12: Hard Choices in AI Safety in Joint Workshop on AI for Social Good, Dobbe, Gilbert, Mintz 11:30 AM

As AI systems become prevalent in high stakes domains such as surveillance and healthcare, researchers now examine how to design and implement them in a safe manner. However, the potential harms caused by systems to stakeholders in complex social contexts and how to address these remains unclear. In this paper, we explain the inherent normative uncertainty in debates about the safety of AI systems. We then address this as a problem of vagueness by examining its place in the design, training, and deployment stages of AI system development. We adopt Ruth Chang’s theory of intuitive comparability to illustrate the dilemmas that manifest at each stage. We then discuss how stakeholders can navigate these dilemmas by incorporating distinct forms of dissent into the development pipeline, drawing on Elizabeth Anderson’s work on the epistemic powers of democratic institutions. We outline a framework of sociotechnical commitments to formal, substantive and discursive challenges that address normative uncertainty across stakeholders, and propose the cultivation of related virtues by those responsible for development.
Abstract 13: The Effects of Competition and Regulation on Error Inequality in Data-driven Markets in Joint Workshop on AI for Social Good, Elzayn 11:35 AM

Much work has documented instances of unfairness in deployed machine learning models, and significant effort has been dedicated to creating algorithms that take into account issues of fairness. Our work highlight an important but understudied source of unfairness: market forces that drive differing amounts of firm investment in data across populations. We develop a high-level framework, based on insights from learning theory and industrial organization, to study this phenomenon. In a simple model of this type of data-driven market, we first show that a monopoly will invest unequally in the groups. There are two natural avenues for preventing this disparate impact: promoting competition and regulating firm behavior. We show first that competition, under many natural models, does not eliminate incentives to invest unequally, and can even exacerbatate it. We then consider two avenues for regulating the monopoly - requiring the monopoly to ensure that each group’s error rates are low, or forcing each group’s error rates to be similar to each other - and quantify the price of fairness (and who pays it). These models imply that mitigating fairness concerns may require policy-driven solutions, and not only technological ones.

Speaker bio:
Hadi Elzayn is a 4th year PhD Candidate in Applied Math and Computational Science at the University of Pennsylvania, advised by Michael Kearns. He is interested in the intersection of computer science and economics, and in the particular topics of how algorithmic learning interacts with social concerns like fairness, privacy, and markets (and how to design algorithms respecting those concerns). He received his BA from Columbia University in Mathematics and Economics. He has interned at Microsoft Research, and previously worked at the consulting firm TGG.

Abstract 14: Learning Fair Classifiers in Online Stochastic Setting in Joint Workshop on AI for Social Good, Sun 11:40 AM

One thing that differentiates policy-driven machine learning is that new public policies are often implemented in a trial-and-error fashion, as data might not be available upfront. In this work, we try to accomplish approximate group fairness in an online decision-making process where examples are sampled i.i.d from an underlying distribution. Our work follows from the classical learning-from-experts scheme, extending the multiplicative weights algorithm by keeping separate weights for label classes as well as groups. Although accuracy and fairness are often conflicting goals, we try to mitigate the trade-offs using an optimization step and demonstrate the performance on real data set.

Speaker bio:
Yi (Alicia) Sun is a PhD Candidate in Institute for Data, Systems and Society at MIT. Her research interests are designing algorithms that are robust and reliable, and as well as align with societal values.

Abstract 15: Fraud detection in telephone conversations for financial services using linguistic features in Joint Workshop on AI for Social Good, 11:45 AM

In collaboration with linguistics and expert interrogators, we present an approach for fraud detection in transcribed telephone conversations. The proposed approach exploits the syntactic and semantic information of the transcription to extract both the linguistic markers and the sentiment of the customer’s response. The results of the proposed approach are demonstrated with real-world financial services data using efficient, robust and explainable classifiers such as Naive Bayes, Decision Tree, Nearest Neighbours, and Support Vector Machines.

Speaker bio:
Nikesh Bajaj is a Postdoctoral Research Fellow at the University of East London, working on the Innovate UK funded project - Automation and Transparency across Financial and Legal Services, in collaboration with Intelligent Voice Ltd. and Strenuus Ltd. The project includes working with machine learning researchers, data scientists, linguistics experts and expert interrogators to model human behaviour for deception detection. He completed his PhD from Queen Mary University of London in a joint program with University of Genova. His PhD work is focused on predictive analysis of auditory attention using physiological signals (e.g. EEG, PPG, GSR). In addition to research, Nikesh has 5+ years of teaching experience. His research interests focus on signal processing,
Abstract 16: A Typology of AI Ethics Tools, Methods and Research to Translate Principles into Practices in Joint Workshop on AI for Social Good, Kinsey 11:50 AM

What tools are available to guide the ethically aligned research, development and deployment of intelligence systems? We construct a typology to help practically-minded developers ‘apply ethics’ at each stage of the AI development pipeline, and to signal to researchers where further work is needed.

Speaker bio: Libby Kinsey: Libby is lead technologist for AI at Digital Catapult, the UK’s advanced digital technology innovation centre, where she works with a multi-disciplinary team to support organisations in building their AI capabilities responsibly. She spent her early career in technology venture capital before returning to university to study machine learning in 2014.

Abstract 17: AI Ethics for Systemic Issues: A Structural Approach in Joint Workshop on AI for Social Good, Schim van der Loeff 11:55 AM

Much of the discourse on AI ethics has focused on technical improvements and holding individuals accountable to prevent accidents and malicious use of AI. While this is useful and necessary, such an “agency-focused” approach does not cover all the harmful outcomes caused by AI. In particular it ignores the more indirect and complex risks resulting from AI’s interaction with the socio-economic and political context. A “structural” approach is needed to account for such broader negative impacts where no individual can be held accountable. This is particularly relevant for AI applied to systemic issues such as climate change. This talk explains why a structural approach is needed in addition to the existing agency approach to AI ethics, and offers some preliminary suggestions for putting this into practice.

Speaker bio: Agnes Schim van der Loeff: Hi, my name is Agnes and I do ethics and policy research at Cervest, which is developing Earth Science AI to quantify climate uncertainty and inform decisions on more sustainable land use. As part of Cervest’s research residency programme earlier this year I started exploring the ethical implications of such use of AI, which resulted in this NeurIPS paper! Now I am developing a framework to ensure all steps in the development, distribution and use of Cervest’s AI-driven platform are ethical and prevent any harmful outcomes. I hold a first class Honours degree in Arabic and Development Studies from SOAS University of London. Having studied the intersection of social, economic and political aspects of development, I am interested in how dilemmas around AI reflect wider debates on power relations in society and I want to explore how AI could be a vehicle for transformative social change. I am particularly passionate about climate justice, which I have engaged with academically and through campaigning.

Abstract 19: ML system documentation for transparency and responsible AI development - a process and an artifact in Joint Workshop on AI for Social Good, Yang 02:00 PM

One large-scale multistakeholder effort to implement the values of the Montreal Declaration as well as other AI ethical principles is ABOUT ML, a recently-launched project led by the Partnership on AI to synthesize and advance the existing research by bringing PAI’s Partner community and beyond into a public conversation and catalyze building a set of resources that allow more organizations to experiment with pilots. Eventually ABOUT ML aims to surface research-driven best practices and aid with translating those into new industry norms. This talk will be an overview of the work to date and ways to get involved moving forward.

Speaker bio: Jingying Yang is a Program Lead on the Research team at the Partnership on AI, where she leads a portfolio of collaborative multistakeholder projects on the topics of safety, fairness, transparency, and accountability, including the ABOUT ML project to set new industry norms on ML documentation. Previously, she worked in Product Operations at Lyft, for the state of Massachusetts on health care policy, and in management consulting at Bain & Company.

Abstract 20: Beyond Principles and Policy Proposals: A framework for the agile governance of AI in Joint Workshop on AI for Social Good, Wallach 02:05 PM

The mismatch between the speed at which innovative technologies are deployed and the slow traditional implementation of ethical/lethal oversight, requires creative, agile, multi-stakeholder, and cooperative approaches to governance. Agile governance must go beyond hard law and regulations to accommodate soft law, corporate self-governance, and technological solutions to challenges. This presentation will summarize the concepts, insights, and creative approaches to AI oversight that have led to the 1st International Congress for the Governance of AI, which will convene in Prague on April 16-18, 2020.

Speaker bio: Wendell Wallach is an internationally recognized expert on the ethical and governance concerns posed by emerging technologies, particularly artificial intelligence and neuroscience. He is a consultant, an ethicist, and a scholar at Yale University’s Interdisciplinary Center for Bioethics, where he chairs the working research group on technology and ethics. He is co-author (with Colin Allen) of Moral Machines: Teaching Robots Right from Wrong, which maps the new field variously called machine ethics, machine morality, computational morality, and friendly AI. His latest book is A Dangerous Master: How to Keep Technology from Slipping Beyond Our Control. Wallach is the principal investigator of a Hastings Center project on the control and responsible innovation in the development of autonomous machines.

Abstract 21: Untangling AI Ethics: Working Toward a Root Issue in Joint Workshop on AI for Social Good, Lin 02:30 PM

Given myriad issues in AI ethics as well as many competing frameworks/declarations, it may be useful to step back to see if we can find a root or common issue, which may help to suggest a broad solution to the complex problem. This involves returning to first principles: what is the nature of AI? I will suggest that AI is the power of increasing omniscience, which is not only generally disruptive to society but also a threat to our autonomy. A broad solution, then, is to aim at restoring that autonomy.

Speaker bio: Patrick Lin is the director of the Ethics + Emerging Sciences Group, based at California Polytechnic State University, San Luis Obispo, where he is also a philosophy professor. He has published several books and papers in the field of technology ethics, especially with respect to robotics—including Robot Ethics (MIT Press, 2012) and Robot Ethics 2.0
Abstract 22: Artificial intelligence (AI) applications in healthcare hold great promise, aiming to empower clinicians to diagnose and treat medical conditions earlier and more effectively. To ensure that AI solutions deliver on this promise, it is important to approach the design of prototype solutions with clinical applicability in mind, envisioning how they might fit within existing clinical workflows. Here we provide a brief overview of how we are incorporating this thinking in our research projects, while highlighting challenges that lie ahead.

Speaker bio:
Nenad Tomasev: My research interests lie at the intersection of theory and impactful real-world AI applications, with a particular focus on AI in healthcare, which I have been pursuing at DeepMind since early 2016. In our most recent work, published in Nature in July 2019, we demonstrate how deep learning can be used for accurate early predictions of patient deterioration from electronic health records and alerting that opens possibilities for timely interventions and preventative care. Prior to moving to London, I had been involved with other applied projects at Google, such as Email Intelligence and the Chrome Data team. I obtained my PhD in 2013 from the Artificial Intelligence Laboratory at JSI in Slovenia, where I was working on better understanding the consequences of the curse of dimensionality in instance-based learning in many dimensions.

Abstract 23: Implementing Responsible AI in Joint Workshop on AI for Social Good. Green, Wallach, Lin, Tomasev, Yang, Kinsey 03:00 PM

This panel will discuss what might be some practical solutions for encouraging and implementing responsible AI. There will be time for audience Q&A.

Audience members are invited to submit questions at https://app.sli.do/event/kdhmkb4d/live/questions

Facilitator:
Brian Patrick Green is Director of Technology Ethics at the Markkula Center for Applied Ethics at Santa Clara University. His interests include AI and ethics, the ethics of space exploration and use, the ethics of technological manipulation of humans, the ethics of catastrophic risk, and the intersection of human society and technology, including religion and technology. Green teaches AI ethics in the Graduate School of Engineering and is co-author of the Ethics in Technology Practice corporate technology ethics resources.

Speakers bio:
Wendell Wallach is an internationally recognized expert on the ethical and governance concerns posed by emerging technologies, particularly artificial intelligence and neuroscience. He is a consultant, an ethicist, and a scholar at Yale University’s Interdisciplinary Center for Bioethics, where he chairs the working research group on technology and ethics. He is co-author (with Colin Allen) of Moral Machines: Teaching Robots Right from Wrong, which maps the new field variously called machine ethics, machine morality, computational morality, and friendly AI. His latest book is A Dangerous Master: How to Keep Technology from Slipping Beyond Our Control. Wallach is the principal investigator of a Hastings Center project on the control and responsible innovation in the development of autonomous machines.

Patrick Lin is the director of the Ethics + Emerging Sciences Group, based at California Polytechnic State University, San Luis Obispo, where he is also a philosophy professor. He has published several books and papers in the field of technology ethics, especially with respect to robotics—including Robot Ethics (MIT Press, 2012) and Robot Ethics 2.0 (Oxford University Press, 2017)—human enhancement, cyberwarfare, space exploration, nanotechnology, and other areas.

Nenad Tomasev: My research interests lie at the intersection of theory and impactful real-world AI applications, with a particular focus on AI in healthcare, which I have been pursuing at DeepMind since early 2016. In our most recent work, published in Nature in July 2019, we demonstrate how deep learning can be used for accurate early predictions of patient deterioration from electronic health records and alerting that opens possibilities for timely interventions and preventative care. Prior to moving to London, I had been involved with other applied projects at Google, such as Email Intelligence and the Chrome Data team. I obtained my PhD in 2013 from the Artificial Intelligence Laboratory at JSI in Slovenia, where I was working on better understanding the consequences of the curse of dimensionality in instance-based learning in many dimensions.

Jingying Yang is a Program Lead on the Research team at the Partnership on AI, where she leads a portfolio of collaborative multistakeholder projects on the topics of safety, fairness, transparency, and accountability, including the ABOUT ML project to set new industry norms on ML documentation. Previously, she worked in Product Operations at Lyft, for the state of Massachusetts on health care policy, and in management consulting at Bain & Company.

Libby Kinsey: Libby is lead technologist for AI at Digital Catapult, the UK’s advanced digital technology innovation centre, where she works with a multi-disciplinary team to support organisations in building their AI capabilities responsibly. She spent her early career in technology venture capital before returning to university to study machine learning in 2014.

Abstract 25: “Good” isn’t good enough in Joint Workshop on AI for Social Good. Green 04:15 PM

Despite widespread enthusiasm among computer scientists to contribute to "social good," the field's efforts to promote good lack a rigorous foundation in politics or social change. There is limited discourse regarding what “good” actually entails, and instead a reliance on vague notions of what aspects of society are good or bad. Moreover, the field rarely considers the types of social change that result from algorithmic interventions, instead following a “greedy algorithm” approach of pursuing technology-centric incremental reform at all points. In order to reason well about doing good, computer scientists must adopt language and practices to reason reflexively about political commitments, a praxis that considers the long-term impacts of technological interventions, and an interdisciplinary focus that no longer prioritizes technical considerations as superior to other forms of knowledge.

Speaker bio:
Ben Green is a PhD Candidate in Applied Math at Harvard, an Affiliate at the Berkman Klein Center for Internet & Society at Harvard, and a
Research Fellow at the AI Now Institute at NYU. He studies the social and policy impacts of data science, with a focus on algorithmic fairness, municipal governments, and the criminal justice system. His book, The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future, was published in 2019 by MIT Press.

Abstract 26: Automated Quality Control for a Weather Sensor Network in Joint Workshop on AI for Social Good, Dietterich 04:20 PM

TAHMO (the Trans-African Hydro-Meteorological Observatory) is a growing network of more than 500 automated weather stations. The eventual goal is to operate 20,000 stations covering all of sub-Saharan Africa and providing ground truth for weather and climate models. Because sensors fail and go out of calibration, some form of quality control is needed to detect bad values and determine when a technician needs to visit a station. We are deploying a three-layer architecture that consists of (a) fitted anomaly detection models, (b) probabilistic diagnosis of broken sensors, and (c) spatial statistics to detect extreme weather events (that may exonerate flagged sensors).

Speaker bio:
Dr. Dietterich is Distinguished Emeritus Professor of computer science at Oregon State University and currently pursues interdisciplinary research at the boundary of computer science, ecology, and sustainability policy.

Abstract 27: AI and Sustainable Development in Joint Workshop on AI for Social Good, Fang, Gomes, Luengo-Oroz, Dietterich, Cornebise 04:50 PM

The focus on this panel is the use of AI for Sustainable Development and will explore the many opportunities this technology presents to improve lives around the world, as well as address the challenges and barriers to its applications. While there is much outstanding work being done to apply AI to such situations, too often this research is not deployed and there is a disconnect between the research and industry communities and the public sector actors. With leading researchers and practitioners from across the academic, public, UN and private sectors this panel brings a diversity of experience to address these important issues.

Audience members are invited to submit questions at: https://app.sli.do/event/skehgej/live/questions

Facilitator: I am an Assistant Professor in the Institute for Software Research in the School of Computer Science at Carnegie Mellon University.

Speaker bio:
Carla Gomes is a Professor of Computer Science and the Director of the Institute for Computational Sustainability at Cornell University. Her research area is artificial intelligence with a focus on large-scale constraint-based reasoning, optimization and machine learning. She is noted for her pioneering work in developing computational methods to address challenges in sustainability.

Dr. Miguel Luengo-Oroz is the Chief Data Scientist at UN Global Pulse, an innovation initiative of the United Nations Secretary-General. He is the head of the data science teams across the network of Pulse labs in New York, Jakarta & Kampala. Over the last decade, Miguel has built and directed teams bringing data and AI to operations and policy through innovation projects with international organizations, govs, private sector & academia. He has worked in multiple domains including poverty, food security, refugees & migrants, conflict prevention, human rights, economic indicators, gender, hate speech and climate change.

Thomas G. Dietterich: Dr. Dietterich is Distinguished Emeritus Professor of computer science at Oregon State University and currently pursues interdisciplinary research at the boundary of computer science, ecology, and sustainability policy.

Julien Cornebise is an Honorary Associate Professor at University College London. He focuses on putting Machine Learning firmly into the hands of nonprofits, certain part of certain, governments, NGOs, UN agencies: those who actually work on tackling our societies’ biggest problems: He built and until recently was a Director of Research of Element AI’s AI for Good team, and head of its London Office. Prior to this, Julien was at DeepMind (later acquired by Google) as an early employee, where he led several fundamental research projects used in early demos and fundraising then co-created its Health Research team. Since leaving DeepMind in 2016, he has been working with Amnesty International, Human Rights Watch, and other actors. Julien holds an MSc in Computer Engineering, an MSc in Mathematical Statistics, and a PhD in Mathematics, specialized in Computational Statistics, from University Paris VI Pierre and Marie Curie and Telecom ParisTech. He received the 2010 Savage Award in Theory and Methods from the International Society for Bayesian Analysis for his PhD work.

Machine Learning for Autonomous Driving

Rowan McAllister, Nick Rhinehart, Fisher Yu, Li Erren Li, Anca Dragan

East Meeting Rooms 1 - 3, Sat Dec 14, 08:00 AM

Autonomous vehicles (AVs) provide a rich source of high-impact research problems for the machine learning (ML) community at NeurIPS in diverse fields including computer vision, probabilistic modeling, gesture recognition, pedestrian and vehicle forecasting, human-machine interaction, and multi-agent planning. The common goal of autonomous driving can catalyze discussion between these subfields, generating a cross-pollination of research ideas. Beyond the benefits to the research community, AV research can improve society by reducing road accidents; giving independence to those unable to drive; and inspiring younger generations towards ML with tangible examples of ML-based technology clearly visible on local streets.

As many NeurIPS attendees are key drivers behind AV-applied ML, the proposed NeurIPS 2019 Workshop on Autonomous Driving intends to bring researchers together from both academia and industries to discuss machine learning applications in autonomous driving. Our proposal includes regular paper presentations, invited speakers, and technical benchmark challenges to present the current state of the art, as well as the limitations and future directions for autonomous driving.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:50 AM</td>
<td>Welcome</td>
<td>McAllister, Rhinehart, Li</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Invited Talk</td>
<td>Koltun</td>
</tr>
<tr>
<td>Time</td>
<td>Event</td>
<td>Speakers</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Towards Robust Interactive Autonomy</td>
<td>Gilitschenski</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Human-inspired AI for autonomous driving</td>
<td>Baker</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>ArgoAI Challenge</td>
<td>Chang, Singh, Hartnett, Cebron, Luo, Huang</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Invited Talk</td>
<td>Urtasun</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>DiDi Challenge</td>
<td></td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Invited Talk</td>
<td>Wolff</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Patch Refinement - Localized 3D Object Detection</td>
<td>Lehner</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Conditional Flow Variational Autoencoders for Structured Sequence Prediction</td>
<td>Bhattacharyya</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Coffee + Posters</td>
<td></td>
</tr>
<tr>
<td>04:30 PM</td>
<td>Meta Learning Deep Visual Words for Fast Video Object Segmentation</td>
<td>Behl</td>
</tr>
<tr>
<td>04:45 PM</td>
<td>Urban Driving With Conditional Imitation Learning</td>
<td>Reda</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Safety and Interaction: the Game Theory of Autonomous Vehicles</td>
<td>Fernández Fisac</td>
</tr>
<tr>
<td>05:30 PM</td>
<td>Mixed Autonomy Traffic: A</td>
<td>Wu</td>
</tr>
</tbody>
</table>

Privacy in Machine Learning (PriML)

**Borja Balle, Kamalika Chaudhuri, Antti Honkela, Antti Koskela, Casey Meehan, Mi Jung Park, Mary Anne Smart, Adrian Weller**

East Meeting Rooms 8 + 15, Sat Dec 14, 08:00 AM

The goal of our workshop is to bring together privacy experts working in academia and industry to discuss the present and the future of privacy-aware technologies powered by machine learning. The workshop will focus on the technical aspects of privacy research and deployment with invited and contributed talks by distinguished researchers in the area. The programme of the workshop will emphasize the diversity of points of view on the problem of privacy. We will also ensure there is ample time for discussions that encourage networking between researchers, which should result in mutually beneficial new long-term collaborations.

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:10 AM</td>
<td>Opening</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Privacy for Federated Learning, and Federated Learning for Privacy</td>
</tr>
<tr>
<td>09:05 AM</td>
<td>Gaussian Differential Privacy</td>
</tr>
<tr>
<td>09:25 AM</td>
<td>QUOTIENT: Two-Party Secure Neural Network Training &amp; Prediction</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Fair Decision Making using Privacy-Protected Data</td>
</tr>
<tr>
<td>11:20 AM</td>
<td>Spotlight talks</td>
</tr>
</tbody>
</table>
Differential privacy has seen remarkable success as a rigorous and attractive property that allows for privacy-preserving data analysis. The concept of differential privacy (DP) has been pivotal in enabling the utility of data while ensuring privacy. Recent developments have introduced variants such as Gaussian differential privacy (GDP), which offers improved privacy guarantees for certain classes of data distributions.

1. **GDP** is a concept that is focal among the f-DP class, representing a single-parameter family of privacy notions within the f-DP class that is referred to as “Gaussian differential privacy” (GDP), defined based on testing two shifted Gaussians. GDP is a core concept in the f-DP class because of a central limit theorem we prove. More precisely, the privacy guarantees of any hypothesis testing based definition of privacy (including original DP) converges to GDP in the limit under composition. The CLT also yields a computationally inexpensive tool for analyzing the exact composition of private algorithms. Taken together, this collection of attractive properties render f-DP a mathematically coherent, analytically tractable, and versatile framework for private data analysis. Finally, we demonstrate the use of the tools we develop by giving an improved privacy analysis of noisy stochastic gradient descent.

Abstract 4: **QUOTIENT: Two-Party Secure Neural Network Training & Prediction in Privacy in Machine Learning (PriML)**, Agrawal, Kusner, Gascon 09:25 AM

Recently, there has been a wealth of effort devoted to the design of secure protocols for machine learning tasks. Much of this is aimed at enabling secure prediction from highly-accurate Deep Neural Networks (DNNs). However, as DNNs are trained on data, a key question is how such models can be also trained securely. The few prior works on secure DNN training have focused either on designing custom protocols for existing training algorithms or on developing tailored training algorithms and then applying generic secure protocols. In this work, we investigate the advantages of designing training algorithms alongside a novel secure protocol, incorporating optimizations on both fronts. We present QUOTIENT, a new method for discretized training of DNNs, along with a customized secure two-party protocol for it. QUOTIENT incorporates key components of state-of-the-art DNN training such as layer normalization and adaptive gradient methods, and improves upon the state-of-the-art in DNN training in two-party computation. Compared to prior work, we obtain an improvement of 50X in WAN time and 6% in absolute accuracy.

Abstract 6: **Fair Decision Making using Privacy-Protected Data in Privacy in Machine Learning (PriML)**, Machanavajjhala 10:30 AM

Data collected about individuals is regularly used to make decisions that impact those same individuals. We consider settings where sensitive personal data is used to decide who will receive resources or benefits. While it is well known that there is a tradeoff between protecting privacy and the accuracy of decisions, in this talk, I will describe our recent work on a first-of-its-kind empirical study into the impact of formally private mechanisms (based on differential privacy) on fair and equitable decision-making.

Abstract 7: **Spotlight talks in Privacy in Machine Learning (PriML)**, Dong, Roth 09:05 AM

Differential privacy has seen remarkable success as a rigorous and practical formalization of data privacy in the past decade. This privacy definition and its divergence based relaxations, however, have several acknowledged weaknesses, either in handling composition of private algorithms or in analyzing important primitives like privacy amplification by subsampling. Inspired by the hypothesis testing formulation of privacy, this paper proposes a new relaxation, which we term “f-differential privacy” (f-DP). This notion of privacy has a number of appealing properties and, in particular, avoids difficulties associated with divergence based relaxations. First, f-DP preserves the hypothesis testing interpretation. In addition, f-DP allows for lossless reasoning about composition in an algebraic fashion. Moreover, we provide a powerful technique to import existing results proven for original DP to f-DP and, as an application, obtain a simple subsampling theorem for f-DP. In addition to the above findings, we introduce a canonical single-parameter family of privacy notions within the f-DP class that is referred to as “Gaussian differential privacy” (GDP), defined based on testing two shifted Gaussians. GDP is focal among the f-DP class because of a central limit theorem we prove. More precisely, the privacy guarantees of any hypothesis testing based definition of privacy (including original DP) converges to GDP in the limit under composition. The CLT also yields a computationally inexpensive tool for analyzing the exact composition of private algorithms. Taken together, this collection of attractive properties render f-DP a mathematically coherent, analytically tractable, and versatile framework for private data analysis. Finally, we demonstrate the use of the tools we develop by giving an improved privacy analysis of noisy stochastic gradient descent.

Abstracts (8):

Abstract 3: **Gaussian Differential Privacy in Privacy in Machine Learning (PriML)**, Dong, Roth 09:05 AM

Differential privacy has seen remarkable success as a rigorous and practical formalization of data privacy in the past decade. This privacy definition and its divergence based relaxations, however, have several acknowledged weaknesses, either in handling composition of private algorithms or in analyzing important primitives like privacy amplification by subsampling. Inspired by the hypothesis testing formulation of privacy, this paper proposes a new relaxation, which we term “f-differential privacy” (f-DP). This notion of privacy has a number of appealing properties and, in particular, avoids difficulties associated with divergence based relaxations. First, f-DP preserves the hypothesis testing interpretation. In addition, f-DP allows for lossless reasoning about composition in an algebraic fashion. Moreover, we provide a powerful technique to import existing results proven for original DP to f-DP and, as an application, obtain a simple subsampling theorem for f-DP. In addition to the above findings, we introduce a canonical single-parameter family of privacy notions within the f-DP class that is referred to as “Gaussian differential privacy” (GDP), defined based on testing two shifted Gaussians. GDP is focal among the f-DP class because of a central limit theorem we prove. More precisely, the privacy guarantees of any hypothesis testing based definition of privacy (including original DP) converges to GDP in the limit under composition. The CLT also yields a computationally inexpensive tool for analyzing the exact composition of private algorithms. Taken together, this collection of attractive properties render f-DP a mathematically coherent, analytically tractable, and versatile framework for private data analysis. Finally, we demonstrate the use of the tools we develop by giving an improved privacy analysis of noisy stochastic gradient descent.
4. [Amrita Roy Chowdhury, Chenghong Wang, Xi He, Ashwin Machanavajjhala and Somesh Jha] Crypto$\varepsilon$pilon$: Crypto-Assisted Differential Privacy on Untrusted Servers (#31)

5. [Jiaming Xu and Dana Yang] Optimal Query Complexity of Private Sequential Learning (#32)

6. [Hsiang Hsu, Shahab Asdoodeh and Flavio Calmon] Discovering Information-Leaking Samples and Features (#43)

7. [Martine De Cock, Rafael Dowsley, Anderson Nascimento, Davis Railback, Jianwei Shen and Ariel Todoji] Fast Secure Logistic Regression for High Dimensional Gene Data (#44)

8. [Giuseppe Vietri, Grace Tian, Mark Bun, Thomas Steinke and Steven Wu] New Oracle-Efficient Algorithms for Private Synthetic Data Release (#45)

Abstract 10: Fair Universal Representations via Generative Models and Model Auditing Guarantees in Privacy in Machine Learning (PriML), Sankar 02:00 PM

There is a growing demand for ML methods that limit inappropriate use of protected information to avoid both disparate treatment and disparate impact. In this talk, we present Generative Adversarial rePresentations (GAP) as a data-driven framework that leverages recent advancements in adversarial learning to allow a data holder to learn universal representations that decouple a set of sensitive attributes from the rest of the dataset while allowing learning multiple downstream tasks. We will briefly highlight the theoretical and practical results of GAP.

In the second half of the talk we will focus on model auditing. Privacy concerns have led to the development of privacy-preserving approaches for learning models from sensitive data. Yet, in practice, models (even those learned with privacy guarantees) can inadvertently memorize unique training examples or leak sensitive features. To identify such privacy violations, existing model auditing techniques use finite adversaries defined as machine learning models with (a) access to some finite side information (e.g., a small auditing dataset), and (b) finite capacity (e.g., a fixed neural network architecture). In the second half of the talk, we present requirements under which an unsuccessful attempt to identify privacy violations by a finite adversary implies that no stronger adversary can succeed at such a task. We will do so via parameters that quantify the capabilities of the finite adversary, including the size of the neural network employed by such an adversary and the amount of side information it has access to as well as the regularity of the (perhaps privacy-guaranteeing) audited model.

Abstract 11: Pan-Private Uniformity Testing in Privacy in Machine Learning (PriML), Amin, Joseph 02:50 PM

A centrally differentially private algorithm maps raw data to differentially private outputs. In contrast, a locally differentially private algorithm may only access data through public interaction with data holders, and this interaction must be a differentially private function of the data. We study the intermediate model of pan-privacy. Unlike a locally private algorithm, a pan-private algorithm receives data in the clear. Unlike a centrally private algorithm, the algorithm receives data one element at a time and must maintain a differentially private internal state while processing this stream. First, we show that pan-privacy against multiple intrusions on the internal state is equivalent to sequentially interactive local privacy. Next, we contextualize pan-privacy against a single intrusion by analyzing the sample complexity of uniformity testing over domain $[k]$. Focusing on the dependence on $k$, centrally private uniformity testing has sample complexity $\Theta(\sqrt{k})$, while noninteractive locally private uniformity testing has sample complexity $\Theta(k)$. We show that the sample complexity of pan-private uniformity testing is $\Theta(k^{2/3})$. By a new $\Omega(k)$ lower bound for the sequentially interactive setting, we also separate pan-private from sequentially interactive locally private and multi-intrusion pan-private uniformity testing.

Abstract 12: Private Stochastic Convex Optimization: Optimal Rates in Linear Time in Privacy in Machine Learning (PriML), Feldman, Koren, Talwar 03:10 PM

We study differentially private (DP) algorithms for stochastic convex optimization: the problem of minimizing the population loss given i.i.d. samples from a distribution over convex loss functions. A recent work of Bassily et al. (2019) has established the optimal bound on the excess population loss achievable given $n$ samples. Unfortunately, their algorithm achieving this bound is relatively inefficient: it requires $O(\min(n^3/2,n^5/2d))$ gradient computations, where $d$ is the dimension of the optimization problem. We describe two new techniques for deriving DP convex optimization algorithms both achieving the optimal bound on excess loss and using $O(\min(n,n^2d))$ gradient computations. In particular, the algorithms match the running time of the optimal non-private algorithms. The first approach relies on the use of variable batch sizes and is analyzed using the privacy amplification by iteration technique of Feldman et al. (2018). The second approach is based on a general reduction to the problem of localizing an approximately optimal solution with differential privacy. Such localization, in turn, can be achieved using existing (non-private) uniformly stable optimization algorithms. As in the earlier work, our algorithms require a mild smoothness assumption. We also give a linear-time algorithm achieving the optimal bound on the excess loss for the strongly convex case, as well as a faster algorithm for the non-smooth case.

Abstract 14: Formal Privacy At Scale: The 2020 Decennial Census TopDown Disclosure Limitation Algorithm in Privacy in Machine Learning (PriML), Leclerc 04:15 PM

To control vulnerabilities to reconstruction-abetted re-identification attacks that leverage massive external data stores and cheap computation, the U.S. Census Bureau has elected to adopt a formally private approach to disclosure limitation in the 2020 Decennial Census of Population and Housing. To this end, a team of disclosure limitation specialists have worked over the past 3 years to design and implement the U.S. Census Bureau TopDown Disclosure Limitation Algorithm (TDA). This formally private algorithm generates Persons and Households micro-data, which will then be tabulated to produce the final set of demographic statistics published as a result of the 2020 Census enumeration. In this talk, I outline the main features of TDA, describe the current iteration of the process used to help policy makers decide how to set and allocate privacy-loss budget, and outline known issues with - and intended fixes for - the current implementation of TDA.

Machine Learning and the Physical Sciences

Atilim Gunes Baydin, Juan Carraquilla, Shirley Ho, Karthik Kashinath, Michela Paganini, Savannah Thais, Anima Anandkumar, Kyle Cranmer, Roger Melko, Mr. Prabhat, Frank Wood

West 109 + 110, Sat Dec 14, 08:00 AM

Machine learning methods have had great success in learning complex representations that enable them to make predictions about unobserved
data. Physical sciences span problems and challenges at all scales in the universe: from finding exoplanets in trillions of sky pixels, to finding machine learning inspired solutions to the quantum many-body problem, to detecting anomalies in event streams from the Large Hadron Collider. Tackling a number of associated data-intensive tasks including, but not limited to, segmentation, 3D computer vision, sequence modeling, causal reasoning, and efficient probabilistic inference are critical for furthering scientific discovery. In addition to using machine learning models for scientific discovery, the ability to interpret what a model has learned is receiving an increasing amount of attention.

In this targeted workshop, we would like to bring together computer scientists, mathematicians and physical scientists who are interested in applying machine learning to various outstanding physical problems, in particular in inverse problems and approximating physical processes; understanding what the learned model really represents; and connecting tools and insights from physical sciences to the study of machine learning models. In particular, the workshop invites researchers to contribute papers that demonstrate cutting-edge progress in the application of machine learning techniques to real-world problems in physical sciences, and using physical insights to understand what the learned model means.

By bringing together machine learning researchers and physical scientists who apply machine learning, we expect to strengthen the interdisciplinary dialogue, introduce exciting new open problems to the broader community, and stimulate production of new approaches to solving open problems in sciences. Invited talks from leading individuals in both communities will cover the state-of-the-art techniques and set the stage for this workshop.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:10 AM</td>
<td>Opening Remarks</td>
<td>Baydin, Carrasquilla, Ho, Kashinath, Paganini, Thais, Anandkumar, Cranmer, Melko, Prabhat, Wood</td>
</tr>
<tr>
<td>08:20 AM</td>
<td>Bernhard Schölkopf</td>
<td>Schölkopf</td>
</tr>
<tr>
<td>08:40 AM</td>
<td>Towards physics-informed deep learning for turbulent flow prediction</td>
<td>Yu</td>
</tr>
<tr>
<td>09:20 AM</td>
<td>JAX, M.D.: End-to-End Differentiable, Hardware Accelerated, Molecular Dynamics in Pure Python</td>
<td>Schoenholz</td>
</tr>
<tr>
<td>09:40 AM</td>
<td>Morning Coffee Break &amp; Poster Session</td>
<td></td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Katie Bouman</td>
<td>Bouman</td>
</tr>
<tr>
<td>11:20 AM</td>
<td>Alán Aspuru-Guzik</td>
<td>Aspuru-Guzik</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Hamiltonian Graph Networks with ODE Integrators</td>
<td>Sanchez Gonzalez</td>
</tr>
<tr>
<td>12:20 PM</td>
<td>Lunch Break</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Maria Schuld</td>
<td>Schuld</td>
</tr>
<tr>
<td>02:40 PM</td>
<td>Lenka Zdeborova</td>
<td>Zdeborová</td>
</tr>
<tr>
<td>03:20 PM</td>
<td>Afternoon Coffee Break &amp; Poster Session</td>
<td></td>
</tr>
<tr>
<td>04:20 PM</td>
<td>Towards an understanding of wide, deep neural networks</td>
<td>Bahri</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Learning Symbolic Physics with Graph Networks</td>
<td>Cranmer</td>
</tr>
</tbody>
</table>
Program Transformations for ML

Pascal Lamblin, Atilim Gunes Baydin, Alexander Wiltschko, Bart van Merrienboer, Emily Fertig, Barak Pearlmutter, David Duvenaud, Laurent Hascoet

West 114 + 115, Sat Dec 14, 08:00 AM

Machine learning researchers often express complex models as a program, relying on program transformations to add functionality. New languages and transformations (e.g., TorchScript and TensorFlow AutoGraph) are becoming core capabilities of ML libraries. However, existing transformations, such as automatic differentiation (AD), inference in probabilistic programming languages (PPL), and optimizing compilers are often built in isolation, and limited in scope. This workshop aims at viewing program transformations in ML in a unified light, making these capabilities more accessible, and building entirely new ones.

Program transformations are an area of active study. AD transforms a program performing numerical computation into one computing the gradient of those computations. In PPL, a program describing a sampling procedure can be modified to perform inference on model parameters given observations. Other examples are vectorizing a program expressed on one data point, and learned transformations where ML models use programs as inputs or outputs.

This workshop will bring together researchers in the fields of AD, programming languages, compilers, and ML, with the goal of understanding the commonalities between disparate approaches and views, and sharing ways to make these techniques broadly available. It would enable ML practitioners to iterate faster on novel models and architectures (e.g., those naturally expressed through high-level constructs like recursion).

Topics:
— Abstractions and syntax (beyond meta-programming and operator overloading) to naturally express a program (expression, or procedure) as an object to be manipulated.
— Techniques from AD and PPL the ML community could adopt to enable research on new models
— How to overcome challenges due to the ML’s specific hardware (GPUs, specialized chips) and software (Python) stacks, and the particular demands of practitioners for their tools
— Greater collaboration between ML and programming languages communities

Schedule

08:30 AM  Opening statements

Jan-Willem van de Meent - Compositional Methods for Learning and Inference in Deep Probabilistic Programs

08:40 AM  Applications of a disintegration transformation

Narayanan

09:30 AM  Applications of a disintegration transformation

Narayanan

09:50 AM  Coffee break

10:30 AM  Christine Tasson - Semantics of Functional Probabilistic Programs

Tasson

11:20 AM  The Differentiable Curry

Vytiniotis

11:40 AM  Functional Tensors for Probabilistic Programming

Obermeyer

12:00 PM  Lunch break & Poster session

Considine, Innes, Phan, Maclaurin, Manhaeve, Radul, Gowda, Sharma, Sennesh, Kochurov, Plotkin, Wiecki, Kukreja, Shan, Johnson, Belov, Pradhan, Meert, Kimmig, De Raedt, Patton, Hoffman, A. Saurous, Roy, Bingham, Jankowiak, Carroll, Lao, Paul, Abadi, Rojas Jimenez, Chen

02:00 PM  Optimized execution of PyTorch programs with TorchScript

DeVito

02:50 PM  Skye Wanderman-Milne - JAX: accelerated machine-learning research via composable function transformations in Python

Wanderman-Milne

03:40 PM  Coffee break

04:20 PM  Generalized Abs-Linear Learning

Griewank

04:40 PM  Towards Polyhedral Automatic Differentiation

Hueckelheim

05:00 PM  Taylor-Mode Automatic Differentiation for Higher-Order Derivatives in JAX

Bettencourt

05:20 PM  Panel and general discussion

Abstracts (3):

Abstract 2: Jan-Willem van de Meent - Compositional Methods for Learning and Inference in Deep Probabilistic Programs in Program Transformations for ML, van de Meent 08:40 AM

Deep learning and probabilistic programming are domains that have a lot in common in certain respects; both rely on software abstractions to enable iterative model development.

In this talk we discuss how we can integrate techniques from both domains in problems where we would like to use priors to induce...
structured representations. To do so, we employ reweighted wake-sleep methods, which combine importance sampling methods (which have been operationalized in probabilistic programming) with variational methods for learning proposals.

To enable a more iterative design of these methods, we introduce compositional constructs, which we refer to as combinators, which serve to define both model structure and evaluation strategies that correspond to different importance sampling schemes. Together these constructs define a path towards a more compositional design of variational methods that are correct by construction.

Abstract 5: Christine Tasson - Semantics of Functional Probabilistic Programs in Program Transformations for ML, Tasson 10:30 AM

Probabilities are extensively used in Computer Science. Algorithms use probabilistic choices for improving efficiency or even for tackling problems that are unsolvable with deterministic computing. Recently, (Functional) Probabilistic Programming has been introduced for applications in Machine Learning and Artificial Intelligence. Probabilistic programs are used to describe statistical models and for developing probabilistic data analysis.

In Probabilistic Programming Languages, inference algorithms are often delegated to compilers including optimizations. This program transformations are error prone, yet they should not change the probabilistic models. Hence the need for formal methods to avoid bugs. Developing formal semantics for probabilistic computing is challenging but crucial in order to systematize the analysis and certification of probabilistic programs.

In this talk, I will first introduce functional probabilistic programing and the related problems. Then, I will present recent works in semantics of probabilistic computing, based on approximation of programs according to their use of resources.


JAX is a system for high-performance machine learning research. It offers the familiarity of Python+NumPy together with hardware acceleration, and it enables the definition and composition of user-wielded function transformations useful for machine learning programs. These transformations include automatic differentiation, automatic batching, end-to-end compilation (via XLA), parallelizing over multiple accelerators, and more. Composing these transformations is the key to JAX’s power and simplicity.

## Competition Track Day 2

**Hugo Jair Escalante**

West 116 + 117, Sat Dec 14, 08:00 AM

https://nips.cc/Conferences/2019/CallForCompetitions

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Causality for Climate (CAC) Käding, Gerhardus, Runge</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>The MineRL competition</td>
</tr>
<tr>
<td></td>
<td>Ogura, Booth, Sun, Topin, Houghton, Guss, Milani, Vinyals, Hofmann,</td>
</tr>
<tr>
<td></td>
<td>KIM, Ramaanuskas, Laurent, Nishio, Kanervisto, Slynkin, Amiranashvili,</td>
</tr>
<tr>
<td></td>
<td>Scheller, WANG, Schraner</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Coffee break</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>The Animal-AI Olympics</td>
</tr>
<tr>
<td></td>
<td>Makoviichuk, Crosby, Beyret, Feyereisl, Yamakawa</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>The AutoDL Challenge</td>
</tr>
<tr>
<td></td>
<td>Treguer, Kim, Guo, Luo, Zhao, Li, Guo, Zhang, Ota</td>
</tr>
<tr>
<td>01:00 PM</td>
<td>Lunch break</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Overview of the Live Reinforcement Learning Malaria Challenge</td>
</tr>
<tr>
<td></td>
<td>Remy</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Traffic4cast -- Traffic Map Movie Forecasting</td>
</tr>
<tr>
<td></td>
<td>Hochreiter, Sigal, Neun, Jonietz, Choi, Martin, Yu, Liu, Nguyen,</td>
</tr>
<tr>
<td></td>
<td>Hennu Sanchez, Shi, Gruca, Sutherland, Kreil, Kopp</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>The Game of Drones Competition</td>
</tr>
<tr>
<td></td>
<td>Toumieh, Vemprala, Shin, Kumar, Ivanov, Shim, Martinez-Carranza, Gyde,</td>
</tr>
<tr>
<td></td>
<td>Kapoor, Nagami, Taubner, Madaan, Gillette, Stubbs</td>
</tr>
</tbody>
</table>

Abstracts (2):


Ogura, Booth, Sun, Topin, Houghton, Guss, Milani, Vinyals, Hofmann, KIM, Ramaanuskas, Laurent, Nishio, Kanervisto, Slynkin, Amiranashvili, Scheller, WANG, Schraner 09:00 AM

MineRL Competition on Sample Efficient Reinforcement Learning.

Competition chairs: Brandon Houghton, William Guss, Stephanie Milani, Nicholas Topin

* Overview and highlights of the competition. Brandon Houghton, William Guss

* Competition Awards. Stephanie Milani

* Special Awards. Oriol Vinyals & advisory board.

* Discussion of future competitions. Katja Hofmann

* Competitors Presentations


Toumieh, Vemprala, Shin, Kumar, Ivanov, Shim, Martinez-Carranza, Gyde, Kapoor, Nagami, Taubner, Madaan, Gillette, Stubbs 04:15 PM
Emergent Communication: Towards Natural Language

Abhinav Gupta, Michael Noukhovitch, Cinjon Resnick, Natasha Jaques, Angelos Filos, Marie Ossenkopf, Angeliki Lazaridou, Jakob Foerster, Ryan Lowe, Douwe Kiela, Kyunghyun Cho

West 118 - 120, Sat Dec 14, 08:00 AM

Communication is one of the most impressive human abilities but historically it has been studied in machine learning on confined datasets of natural language, and by various other fields in simple low-dimensional spaces. Recently, with the rise of deep RL methods, the questions around the emergence of communication can now be studied in new, complex multi-agent scenarios. Two previous successful workshops (2017, 2018) have gathered the community to discuss how, when, and to what end communication emerges, producing research that was later published at top ML venues such as ICLR, ICML, AAAI. Now, we wish to extend these ideas and explore a new direction: how emergent communication can become more like natural language, and what natural language understanding can learn from emergent communication.

The push towards emergent natural language is a necessary and important step in all facets of the field. For studying the evolution of human language, emerging a natural language can uncover the requirements that spurred crucial aspects of language (e.g. compositionality). When emerging communication for multi-agent scenarios, protocols may be sufficient for machine-machine interactions, but emerging a natural language is necessary for human-machine interactions. Finally, it may be possible to have truly general natural language understanding if agents learn the language through interaction as humans do. To make this progress, it is necessary to close the gap between artificial and natural language learning.

To tackle this problem, we want to take an interdisciplinary approach by inviting researchers from various fields (machine learning, game theory, evolutionary biology, linguistics, cognitive science, and programming languages) to participate and engaging them to unify the differing perspectives. We believe that the third iteration of this workshop with a novel, unexplored goal and strong commitment to diversity will allow this burgeoning field to flourish.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:55 AM</td>
<td>Introductory Remarks</td>
<td></td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Invited Talk - 1</td>
<td>Gibson</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Contributed Talk - 1</td>
<td>Lee</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Coffee Break / Poster Session</td>
<td>Zaslavsky</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Invited Talk - 2</td>
<td>Cowen-Rivers</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Contributed Talk - 2</td>
<td>LaCroix, Ossenkopf, Lee, Fitzgerald, Mihai, Hare, Zaidi, Cowen-Rivers, Marzoev, Khartonov, Yuan, Korbak, Liang, Ren, Dessi, Potash, Guo, Hashimoto, Liang, Zubek, Fu, Zhu, Lerer</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Extended Poster Session</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Invited Talk - 3</td>
<td>Eisner</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>Contributed Talk - 3</td>
<td>Lerer</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Invited Talk - 4</td>
<td>Andreas</td>
</tr>
<tr>
<td>03:45 PM</td>
<td>Coffee Break / Poster Session</td>
<td></td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Invited Talk - 5</td>
<td>Lee</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Panel Discussion</td>
<td>Andreas, Gibson, Lee, Zaslavsky, Eisner, Schmidhuber</td>
</tr>
<tr>
<td>05:55 PM</td>
<td>Closing Remarks</td>
<td></td>
</tr>
</tbody>
</table>
language. However, it is not yet clear what computational principles could give rise to human-like semantics and pragmatics in machines. In this talk, I will propose a possible answer to this open question by hypothesizing that pressure for efficient coding may underlie both abilities. First, I will argue that languages efficiently encode meanings into words by optimizing the Information Bottleneck (IB) tradeoff between the complexity and accuracy of the lexicon. This proposal is supported by cross-linguistic data from three semantic domains: names for colors, artifacts, and animals. Furthermore, it suggests that semantic systems may evolve by navigating along the IB theoretical limit via an annealing-like process. This process generates quantitative predictions, which are directly supported by an analysis of recent data documenting changes over time in the color naming system of a single language. Second, I will derive a theoretical link between optimized semantic systems and local, context-dependent interactions that involve pragmatic skills. Specifically, I will show that pressure for efficient coding may also give rise to human pragmatic reasoning, as captured by the Rational Speech Act framework. This line of work identifies information-theoretic optimization principles that characterize human semantic and pragmatic communication, and that could be used to inform artificial agents with human-like communication systems.

Science meets Engineering of Deep Learning

Levent Sagun, CAGLAR Gulcehre, Adriana Romero, Negar Rostamzadeh, Nando de Freitas

West 121 + 122, Sat Dec 14, 08:00 AM

Deep learning can still be a complex mix of art and engineering despite its tremendous success in recent years, and there is still progress to be made before it has fully evolved into a mature scientific discipline. The interdependence of architecture, data, and optimization gives rise to an enormous landscape of design and performance intricacies that are not well-understood. The evolution from engineering towards science in deep learning can be achieved by pushing the disciplinary boundaries. Unlike in the natural and physical sciences -- where experimental capabilities can hamper progress, i.e. limitations in what quantities can be probed and measured in physical systems, how much and how often -- "in deep learning the vast majority of relevant quantities that we wish to measure can be tracked in some way". As such, a greater limiting factor towards scientific understanding and principled design in deep learning is how to "insightfully harness the tremendous collective experimental capability of the field". As a community, some primary aims would be to (i) identify obstacles to better models and algorithms, (ii) identify the general trends that are potentially important which we wish to understand scientifically and potentially theoretically and; (iii) careful design of scientific experiments whose purpose is to clearly resolve and pinpoint the origin of mysteries (so-called 'smoking-gun' experiments).

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Welcoming remarks and introduction</td>
<td>Sagun, Gulcehre, Romero,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rostamzadeh, de Freitas</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Surya Ganguli - An analytic theory of generalization dynamics and transfer learning in deep linear networks</td>
<td>Ganguli</td>
</tr>
<tr>
<td>08:35 AM</td>
<td>Yasaman Bahri - Tractable limits for deep networks: an overview of the large width regime</td>
<td>Bahri</td>
</tr>
<tr>
<td>08:55 AM</td>
<td>Florent Krzakala - Learning with &quot;realistic&quot; synthetic data</td>
<td>Krzakala</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Surya Ganguli, Yasaman Bahri, Florent Krzakala moderated by Lenka Zdeborova</td>
<td>Krzakala, Bahri, Ganguli,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zdeborová, Dieng, Bruna</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee and posters</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Carl Doersch - On Self-Supervised Learning for Vision</td>
<td>Doersch</td>
</tr>
<tr>
<td>10:50 AM</td>
<td>Raquel Urtasun - Science and Engineering for Self-driving</td>
<td>Urtasun</td>
</tr>
<tr>
<td>11:10 AM</td>
<td>Sanja Fidler - TBA</td>
<td>Fidler</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Carl Doersch, Raquel Urtasun, Sanja Fidler moderated by Natalia Neverova</td>
<td>Urtasun, Fidler, Neverova,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Radosavovic, Doersch</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch Break and Posters</td>
<td></td>
</tr>
</tbody>
</table>

Douwe Kiela - Benchmarking Progress in AI: A New Benchmark for Natural Language Understanding

02:00 PM

Kiela
ML For Systems

Milad Hashemi, Azalia Mirhoseini, Anna Goldie, Kevin Swersky, Xinlei Xu, Jonathan Raiman

West 202 - 204, Sat Dec 14, 08:00 AM

Compute requirements are growing at an exponential rate, and optimizing these computer systems often involves complex high-dimensional combinatorial problems. Yet, current methods rely heavily on heuristics. Very recent work has outlined a broad scope where machine learning vastly outperforms these traditional heuristics: including scheduling, data structure design, microarchitecture, compilers, circuit design, and the control of warehouse scale computing systems. In order to continue to scale these computer systems, new learning approaches are needed. The goal of this workshop is to develop novel machine learning methods to optimize and accelerate software and hardware systems.

Machine Learning for Systems is an interdisciplinary workshop that brings together researchers in computer architecture and systems and machine learning. This workshop is meant to serve as a platform to promote discussions between researchers in the workshops target areas.

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.

Schedule

09:00 AM Opening

09:10 AM Invited Speaker: Eytan Bakshy

09:45 AM Break

10:30 AM Poster Session 1

Mao, Nathan, Baldini, Sivakumar, Wang, Magalle, Hewa, Shi, Kaufman, Fang, Zhou, Ding, He, Lubin
The third Conversational AI workshop – today’s practice and tomorrow’s potential

Alborz Geramifard, Jason Williams, Bill Byrne, Asli Celikyilmaz, Milica Gasic, Dilek Hakkani-Tur, Matt Henderson, Luis Lastras, Mari Ostendorf

West 205 - 207, Sat Dec 14, 08:00 AM

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. Such movement has not been unnoticed by major publications. This year in collaboration with AAAI community, the AI magazine will have a special issue on conversational AI (https://tinyurl.com/y6shq2id). Moreover, 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 two NeurIPS workshops:

2017: 9 invited talks, 26 submissions, 3 oral papers, 13 accepted papers, 37 reviewers
2018: 4 invited talks, 42 submission, 6 oral papers, 23 accepted papers, 58 reviewers, 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, understand well-founded methods, share findings from large-scale real-world deployments, and generate new ideas for future lines of research.

This one day workshop will include invited talks and a panel from academia and industry, contributed work, and open discussion.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:45 AM</td>
<td>Opening Remarks</td>
<td>Williams</td>
</tr>
<tr>
<td>08:55 AM</td>
<td>Invited talk - Alan Ritter</td>
<td></td>
</tr>
<tr>
<td>09:25 AM</td>
<td>Contributed talk 1</td>
<td></td>
</tr>
<tr>
<td>09:55 AM</td>
<td>Poster lighting round</td>
<td>Zheng, Seggaard, Saleh, Jang, Gong, Florez, Li, Madotto, Nguyen, Kulikov, einolghozati, Wang, Eric, Hansen, Lubis, Wu</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Invited Speaker: Ion Stoica</td>
<td>Stoica</td>
</tr>
<tr>
<td>10:55 AM</td>
<td>Contributed talk 2: Persona-aware Dialogue Generation with Enriched Profile</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Contributed talk 3: HSCJN: A Holistic Semantic Constraint Joint Network for Diverse Response Generation</td>
<td></td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Invited Speaker: Akanksha Jain</td>
<td>Jain</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:45 PM</td>
<td>Invited talk - David Traum</td>
<td>Traum</td>
</tr>
</tbody>
</table>

### The third Conversational AI workshop – today’s practice and tomorrow’s potential

Alborz Geramifard, Jason Williams, Bill Byrne, Asli Celikyilmaz, Milica Gasic, Dilek Hakkani-Tur, Matt Henderson, Luis Lastras, Mari Ostendorf

West 205 - 207, Sat Dec 14, 08:00 AM

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. Such movement has not been unnoticed by major publications. This year in collaboration with AAAI community, the AI magazine will have a special issue on conversational AI (https://tinyurl.com/y6shq2id). Moreover, 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 two NeurIPS workshops:

2017: 9 invited talks, 26 submissions, 3 oral papers, 13 accepted papers, 37 reviewers
2018: 4 invited talks, 42 submission, 6 oral papers, 23 accepted papers, 58 reviewers, 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, understand well-founded methods, share findings from large-scale real-world deployments, and generate new ideas for future lines of research.

This one day workshop will include invited talks and a panel from academia and industry, contributed work, and open discussion.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:45 AM</td>
<td>Opening Remarks</td>
<td>Williams</td>
</tr>
<tr>
<td>08:55 AM</td>
<td>Invited talk - Alan Ritter</td>
<td></td>
</tr>
<tr>
<td>09:25 AM</td>
<td>Contributed talk 1</td>
<td></td>
</tr>
<tr>
<td>09:55 AM</td>
<td>Poster lighting round</td>
<td>Zheng, Seggaard, Saleh, Jang, Gong, Florez, Li, Madotto, Nguyen, Kulikov, einolghozati, Wang, Eric, Hansen, Lubis, Wu</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Invited Speaker: Ion Stoica</td>
<td>Stoica</td>
</tr>
<tr>
<td>10:55 AM</td>
<td>Contributed talk 2: Persona-aware Dialogue Generation with Enriched Profile</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Contributed talk 3: HSCJN: A Holistic Semantic Constraint Joint Network for Diverse Response Generation</td>
<td></td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Invited Speaker: Akanksha Jain</td>
<td>Jain</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:45 PM</td>
<td>Invited talk - David Traum</td>
<td>Traum</td>
</tr>
</tbody>
</table>
Document Intelligence

Nigel Duffy, Rama Akkiraju, Tania Bedrax Weiss, Paul Bennett, Hamid Reza Motahari-Nezhad

West 208 + 209, Sat Dec 14, 08:00 AM

Business documents are central to the operation of business. Such documents include sales agreements, vendor contracts, mortgage terms, loan applications, purchase orders, invoices, financial statements, employment agreements and a wide many more. The information in such business documents is presented in natural language, and can be organized in a variety of ways from straight text, multi-column formats, and a wide variety of tables. Understanding these documents is made challenging due to inconsistent formats, poor quality scans and OCR, internal cross references, and complex document structure. Furthermore, these documents often reflect complex legal agreements and reference, explicitly or implicitly, regulations, legislation, case law and standard business practices.

The ability to read, understand and interpret business documents, collectively referred to here as “Document Intelligence”, is a critical and challenging application of artificial intelligence (AI) in business. While a variety of research has advanced the fundamentals of document understanding, the majority have focused on documents found on the web which fail to capture the complexity of analysis and types of understanding needed across business documents. Realizing the vision of document intelligence remains a research challenge that requires a multi-disciplinary perspective spanning not only natural language processing and understanding, but also computer vision, knowledge representation and reasoning, information retrieval, and more -- all of which have been profoundly impacted and advanced by neural network-based approaches and deep learning in the last few years.

We propose to organize a workshop for AI researchers, academics and industry practitioners to discuss the opportunities and challenges for document intelligence.

Schedule

08:00 AM Opening Remarks

08:10 AM David Lewis: Artificial Intelligence in Legal Discovery

Ndapa Nakashole: Generalizing Representations of Language for Documents Analysis across Different Domains

10:00 AM Coffee Break

10:30 AM Poster Teaser Presentations

12:05 PM Posters

Rajasekar Krishnamurthy: Document Intelligence for Enterprise AI Applications: Krishnamurthy

01:30 PM Requirements & Research Challenges

Asli Celikyilmaz: Learning Structure in Text Generation

02:30 PM Celikyilmaz

03:30 PM Coffee Break

Discussion: Document Intelligence Research Challenges & Directions

04:00 PM Best Paper Talk: BERTGrid Contextualized Embedding for 2D Document Representation and Understanding

05:00 PM
Abstracts (6):

Abstract 2: David Lewis: Artificial Intelligence in Legal Discovery in Document Intelligence. Lewis 08:10 AM

Abstract: In December 2006, a change to the US Federal Rules of Civil Procedure made “electronically stored information” – effectively every bit of storage in an enterprise – fair game for discovery requests in civil litigation. The result was a multi-billion dollar electronic discovery industry, a remarkable embrace by lawyers and judges of the artifacts of experimental machine learning (learning curves, effectiveness estimates, active learning,...), and a torrent of technical challenges for machine learning, natural language processing, information retrieval, and statistics. I will discuss the state of e-discovery science and technology, and its spread to new applications such as internal investigation and breach response.

Biography: David D. Lewis, Ph.D. is Chief Data Scientist atBrainspace, a Cyxtera business, where he leads their research efforts as well as the machine learning software development team. Prior to joining Brainspace, he was variously a freelance consultant, corporate researcher (Bell Labs, AT&T Labs), research professor, and software company co-founder. Dave has published more than 40 peer-reviewed scientific publications and 9 patents. He was elected a Fellow of the American Association for Advancement of Science in 2006 for foundational work in text categorization, and won a Test of Time Award from ACM SIGIR in 2017 for his paper w/ Gale introducing uncertainty sampling

Abstract 3: Ndapa Nakashole: Generalizing Representations of Language for Documents Analysis across Different Domains in Document Intelligence. Nakashole 09:05 AM

Abstract. Labeled data for tasks such as information extraction, question answering, text classification, and other types of document analysis are often drawn from a limited set of document types and genres because of availability, and cost. At test time, we would like to apply the trained models to different document types and genres. However, a model trained on one dataset often fails to generalize to data drawn from distributions other than that of the training data. In this talk, I will talk about our work on generalizing representations of language, and discuss some of the document types we are studying.

Biography: Ndapa Nakashole is an Assistant Professor at the University of California, San Diego, where she teaches and carries out research on Statistical Natural Language Processing. Before that she was postdoctoral scholar at Carnegie Mellon University. She obtained her PhD from Saarland University and the Max Planck Institute for Informatics. She completed undergraduate studies in Computer Science at the University of Cape Town, South Africa.

Abstract 5: Poster Teaser Presentations in Document Intelligence, 10:30 AM

Papers presented as re follows:


“Semantic Structure Extraction for Spreadsheet Tables with a Multi-task Learning Architecture”, by Haoyu Dong, Shijie Liu, Zhoyy Fu, Shi Han, Dongmei Zhang.


“Representation Learning in Geology and GilBERT”, by Zikri Bayraktar, Hedi Driss, Marie Lefranc.

“Neural Contract Element Extraction Revisited”, by Ilias Chalkidis, Manos Feragadiotis, Prodomos Malakasiotis, Ion Androustopoulos.


“Information Extraction from Text Regions with Complex Structure”, by Kaixuan Zhang, Zeijiang Shen, Jie Zhou, Melissa Dell.


Abstract 7: Rajasekar Krishnamurthy: Document Intelligence for Enterprise AI Applications: Requirements & Research Challenges in Document Intelligence, Krishnamurthy 01:30 PM

Abstract: Enterprise applications and Business processes rely heavily on experts and knowledge workers reading, searching and analyzing business documents to perform their daily tasks. For instance, legal professionals read contracts to identify non-standard clauses, risks and exposures. Loan officers analyze borrower business documents to understand income, expense and contractual commitments before making lending decisions.

Document Intelligence is the ability for a system to read, understand and interpret business documents through the application of AI-based technologies. It has the potential to significantly improve an employee’s productivity and an organization’s effectiveness by augmenting the expert in their daily task. Several challenges arise in this context such as variability in document authoring, necessity to contextually understand textual and tabular content and organization/role-specific variations in semantic interpretations. Furthermore, as experts rely on document intelligence, they expect the system to exhibit key properties such as explainability, consistent model evolution and ability to enhance the system’s knowledge with a few examples.

In this talk, using real-world enterprise application examples, I first describe how document intelligence can play a key role in augmenting enterprise AI applications. I then outline key challenges that arise in business document understanding and desiderata that enterprise AI applications and users expect. I conclude with a set of open research challenges that need to be tackled spanning across language understanding, knowledge representation and reasoning, deep learning and systems research.

Biography: Rajasekar Krishnamurthy is a Principal Research Staff Member and Senior Manager leading the Watson Discovery team in the Watson AI organization. Prior to this role, he was a Principal Research Staff Member at IBM Research - Almaden leading the NLP, Entity Resolution and Discovery department. Rajasekar’s technical interests focus around helping enterprises derive business insights from a variety of unstructured content sources ranging from public and third-party data sources to governing business documents within an enterprise. Rajasekar has expertise in building scalable and usable analytics tools for individual stages in analyzing unstructured documents, such as text analytics, document structure analysis and entity resolution. He is a member of the IBM Academy of Technology. He received a B.Tech in Computer Science and Engineering from the Indian Institute of Technology-Madras, and a Ph.D.in Computer Science from the University of Wisconsin-Madison.

Abstract 8: Asli Celikyilmaz: Learning Structure in Text Generation in Document Intelligence, Celikyilmaz 02:30 PM

Abstract: Automatic text generation enables computers to summarize text, describe pictures to visually impaired, write stories or articles about an event, have conversations in customer-service, chat with individuals, and other settings, and customize content based on the characteristics and goal of the human interlocutor. Neural text generation (NLG) – using neural network models to generate coherent text – have seen a paradigm shift in the last years, caused by the advances in deep contextual language modeling (e.g., LSTMs, GPT, GPT2) and transfer learning (e.g., ELMo, BERT). While these tools have dramatically improved the state of NLG, particularly for low resources tasks, state-of-the-art NLG models still face many challenges: a lack of diversity in generated text, commonsense violations in depicted situations, difficulties in making use of factual information, and difficulties in designing reliable evaluation metrics. In this talk I will discuss existing work on text only transformers that specifies how to generate long-text with better discourse structure and narrative flow, generate multi-document summaries, build automatic knowledge graphs with commonsense transformers as text generators. I will conclude the talk with a discussion of current challenges and shortcomings of neural text generation, pointing to avenues for future research.

Biography: Asli Celikyilmaz is a Principal Researcher at Microsoft Research in Redmond, Washington. She is also an Affiliate Professor at the University of Washington. Her research interests are mainly in deep learning and natural language, specifically on language generation with long-term coherence, language understanding, language grounding with vision, and building intelligent agents for human-computer interaction. She has received several “best of” awards including NAFIPS 2007, Semantic Computing 2009, and CVPR 2019.

Learning Transferable Skills

Marwan Mattar, Arthur Juliani, Danny Lange, Matthew Crosby, Benjamin Beyret

West 211 - 214, Sat Dec 14, 08:00 AM

After spending several decades on the margin of AI, reinforcement learning has recently emerged as a powerful framework for developing
intelligent systems that can solve complex tasks in real-world environments. This has had a tremendous impact on a wide range of tasks ranging from playing games such as Go and StarCraft to learning dexterity. However, one attribute of intelligence that still eludes modern learning systems is generalizability. Until very recently, the majority of reinforcement learning research involved training and testing algorithms on the same, sometimes deterministic, environment. This has resulted in algorithms that learn policies that typically perform poorly when deployed in environments that differ, even slightly, from those they were trained on. Even more importantly, the paradigm of task-specific training results in learning systems that scale poorly to a large number of (even interrelated) tasks.

Recently there has been an enduring interest in developing learning systems that can learn transferable skills. This could mean robustness to changing environment dynamics, the ability to quickly adapt to environment and task variations or the ability to learn to perform multiple tasks at once (or any combination thereof). This interest has also resulted in a number of new data sets and challenges (e.g. Obstacle Tower Environment, Animal-AI, CoinRun) and an urgency to standardize the metrics and evaluation protocols to better assess the generalization abilities of novel algorithms. We expect this area to continue to increase in popularity and importance, but this can only happen if we manage to build consensus on which approaches are promising, and, equally important, how to test them.

The workshop will include a mix of invited speakers, accepted papers (oral and poster sessions) and a panel discussion. The workshop welcomes both theoretical and applied research, in addition to novel data sets and evaluation protocols.

**Schedule**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 AM</td>
<td>Opening Remarks</td>
<td>Mattar, Juliani, Crosby, Beyret, Lange</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Challenges of Deep RL in Complex Environments</td>
<td>Hadsell</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Environments and Data Sets</td>
<td>Cobbe, De Fabritiis, Makovitchuk</td>
</tr>
<tr>
<td>11:20 AM</td>
<td>Vladlen Koltun (Intel)</td>
<td>Koltun</td>
</tr>
<tr>
<td>12:05 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>01:30 PM</td>
<td>Innate Bodies, Innate Brains, and Innate World Models</td>
<td>Ha</td>
</tr>
<tr>
<td>02:15 PM</td>
<td>Oral Presentations</td>
<td>Petangoda, Pascual-Diaz, Grau-Moya, Marinier, Pietquin, Efros, Isola, Darrell, Lu, Pathak, Ferret</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Poster Presentations</td>
<td></td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Multi-Task Reinforcement</td>
<td>Holtmann</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Solving Rubik's Cube with a Robot Hand</td>
<td>Zaremba</td>
</tr>
<tr>
<td>05:45 PM</td>
<td>Closing Remarks</td>
<td>Mattar, Juliani, Crosby, Beyret, Lange</td>
</tr>
</tbody>
</table>

**Sets and Partitions**

_Nicholas Monath, Manzil Zaheer, Andrew McCallum, Ari Kobren, Junier Oliva, Barnabas Poczos, Ruslan Salakhutdinov_

**West 215 + 216, Sat Dec 14, 08:00 AM**

Classic problems for which the input and/or output is set-valued are ubiquitous in machine learning. For example, multi-instance learning, estimating population statistics, and point cloud classification are all problem domains in which the input is set-valued. In multi-label classification the output is a set of labels, and in clustering, the output is a partition. New tasks that take sets as input are also rapidly emerging in a variety of application areas including: high energy physics, cosmology, crystallography, and art. As a natural means of succinctly capturing large collections of items, techniques for learning representations of sets and partitions have significant potential to enhance scalability, capture complex dependencies, and improve interpretability. The importance and potential of improved set processing has led to recent work on permutation invariant and equivariant representations (Ravanbakhsh et al, 2016; Zaheer et al, 2017; Ilse et al, 2018; Hartford et al, 2018; Lee et al, 2019, Cotter et al, 2019, Bloom-Reddy & Teh, 2019, and more) and continuous representations of set-based outputs and partitions (Tai and Lin, 2012; Belanger & McCallum, 2015; Wiseman et al, 2016; Caron et al, 2018; Zhang et al, 2019; Vikram et al 2019).

The goal of this workshop is to explore:
- Permutation invariant and equivariant representations; empirical performance, limitations, implications, inductive biases of proposed representations of sets and partitions, as well as rich models of interaction among set elements;
- Inference methods for predicting sets or clusterings; approaches based on gradient-descent, continuous representations, amenable to end-to-end optimization with other models;
The First Workshop on Sets and Partitions, to be held as a part of the NeurIPS 2019 conference, focuses on models for tasks with set-based inputs/outputs as well as models of partitions and novel clustering methodology. The workshop welcomes both methodological and theoretical contributions, and also new applications. Connections to related problems in optimization, algorithms, theory as well as investigations of learning approaches to set/partition problems are also highly relevant to the workshop. We invite both paper submissions and submissions of open problems. We hope that the workshops will inspire further progress in this important field.

Organizing Committee:
Andrew McCallum, UMass Amherst
Ruslan Salakhutdinov, CMU
Barnabas Poczos, CMU
Junier Oliva, UNC Chapel Hill
Manzil Zaheer, Google Research
Ari Kobren, UMass Amherst
Nicholas Monath, UMass Amherst
with senior advisory support from Alex Smola.

Invited Speakers:
Siamak Ravanbakhsh
Abhishek Khetan
Eunsu Kang
Amr Ahmed
Stefanie Jegelka

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30 AM</td>
<td>Invited Talk - Siamak Ravanbakhsh - Equivariant Ravanbakhsh Multilayer Perceptrons</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Contributed Talk - Towards deep amortized clustering Lee, Lee, Teh</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Contributed Talk - Fair Hierarchical Clustering Ahmadian, Epasto, Knittel, Kumar, Mahdian, Pham</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Invited Talk - Abhishek Khetan - Molecular geometries as point clouds: Learning physico-chemical properties using DeepSets Khetan</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch Break (on your own)</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Contributed Talk - Limitations of Deep Learning on Point Clouds Bueno</td>
</tr>
<tr>
<td>02:15 PM</td>
<td>Contributed Talk - Chirality Nets: Exploiting Structure in Human Pose Regression Yeh, Hu, Schwing</td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Invited Talk - Eunsu Kang - Sets for Arts Kang</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Coffee Break &amp; Poster Session 2</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Invited Talk - Alexander J. Smola - Sets and symmetries Smola</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>05:40 PM</td>
<td>Closing Remarks</td>
</tr>
</tbody>
</table>

Abstracts (3):


Poster Session 1 Paper Titles & Authors:

Deep Set Prediction Networks. Yan Zhang, Jonathon Hare, Adam
Prügel-Bennett


FSPool: Learning Set Representations with Featurewise Sort Pooling. Yan Zhang, Jonathon Hare, Adam Prügel-Bennett

Deep Learning Features Through Dictionary Learning with Improved Clustering for Image Classification. Shengda Luo, Alex Po Leung, Haichi Zhang

Globally Optimal Model-based Clustering via Mixed Integer Nonlinear Programming. Patrick Flaherty, Pitchaya Wiratchotisatian, Andrew C. Trapp

Sliding Window Algorithms for k-Clustering Problems. Michele Borassi, Alessandro Epasto, Silvio Lattanzi, Sergei Vassilvitski, Morteza Zadimoghaddam

Optimized Recommendations When Customers Select Multiple Products. Prasoon Patidar, Deeksha Sinha, Theja Tulabandhula

Manipulating Person Videos with Natural Language. Levent Karacan, Mehmet Gunel, Aykut Erdem, Erkut Erdem

Permutation Invariance and Relational Reasoning in Multi-Object Tracking. Fabian B. Fuchs, Adam R. Kosiorek, Li Sun, Oiwi Parker Jones, Ingmar Posner.

Clustering by Learning to Optimize Normalized Cuts. Azade Nazi, Will Hang, Anna Goldie, Sujith Ravi, Azalia Mirhoseini

Deformable Filter Convolution for Point Cloud Reasoning. Yuwen Xiong, Mengye Ren, Renjie Liao, Kelvin Wong, Raquel Urtasun

Learning Embeddings from Cancer Mutation Sets for Classification Tasks. Geoffroy Dubourg-Felonneau, Yasmeen Kussad, Dominic Kirkham, John Cassidy, Harry W Clifford

Exchangeable Generative Models with Flow Scans. Christopher M. Bender, Kevin O'Connor, Yang Li, Juan Jose Garcia, Manzil Zaheer, Junier Oliva

Conditional Invertible Flow for Point Cloud Generation. Stypulkowski Michal, Zamorski Maciej, Zieba Maciej, Chorowski Jan

Getting Topology and Point Cloud Generation to Mesh. Austin Dill, Chun-Liang Li, Songwei Ge, Eunsu Kang

Distributed Balanced Partitioning and Applications in Large-scale Load Balancing. Aaron Archer, Kevin Aydin, Mohammad-Hossein Bateni, Vahab Mirrokni, Aaron Schild, Ray Yang, Richard Zhuang

Abstract 9: Contributed Talk - Limitations of Deep Learning on Point Clouds in Sets and Partitions. Bueno 02:00 PM


Poster Session 2 Paper Titles & Authors:

Towards deep amortized clustering. Juho Lee, Yoonho Lee, Yee Whye Teh

Chirality Nets: Exploiting Structure in Human Pose Regression. Raymond Yeh, Yuan-Ting Hu, Alexander Schwing

Fair Hierarchical Clustering. Sara Ahmadian, Alessandro Epasto, Marina Knittel, Ravi Kumar, Mohammad Mahdian, Philip Pham


How Powerful Are Randomly Initialized Pointcloud Set Functions? Aditya Sanghi, Pradeep Kumar Jayaraman

On the Possibility of Rewarding Structure Learning Agents: Mutual Information on Linguistic Random Sets. Ignacio Arroyo-Fernández, Mauricio Carrasco-Ruiz, José Aníbal Arias-Aguilar

Modelling Convolution as a Finite Set of Operations Through Transformation Semigroup Theory. Andrew Hryniowski, Alexander Wong

HCA-DBSCAN: HyperCube Accelerated Density Based Spatial Clustering for Applications with Noise. Vinayak Mathur, Jinesh Mehta, Sanjay Singh

Finding densest subgraph in probabilistically evolving graphs. Sara Ahmadian, Shahrzad Haddadan

Representation Learning with Multisets. Vasco Portilheiro

PairNets: Novel Fast Shallow Artificial Neural Networks on Partitioned Subspaces. Luna Zhang

Fair Correlation Clustering. Sara Ahmadian, Alessandro Epasto, Ravi Kumar, Mohammad Mahdian

Learning Maximally Predictive Prototypes in Multiple Instance Learning. Mert Yuksekgonul, Ozgur Emre Sivrikaya, Mustafa Gokce Baydogan

Deep Clustering using MMD Variational Autoencoder and Traditional Clustering Algorithms. Jhosimar Arias

Hypergraph Partitioning Using Tensor Eigenvector Decomposition. Deepak Maurya, Balaraman Ravindran, Shankar Narasimhan

Information Geometric Set Embeddings: From Sets to Distributions. Ke Sun, Frank Nielsen

Document Representations using Fine-Grained Topics. Justin Payan, Andrew McCallum
Context and Compositionality in Biological and Artificial Neural Systems

Javier Turek, Shailee Jain, Alexander Huth, Leila Wehbe, Emma Strubell, Alan Yuille, Tal Linzen, Christopher Honey, Kyunghyun Cho

West 217 - 219, Sat Dec 14, 08:00 AM

The ability to integrate semantic information across narratives is fundamental to language understanding in both biological and artificial cognitive systems. In recent years, enormous strides have been made in NLP and Machine Learning to develop architectures and techniques that effectively capture these effects. The field has moved away from traditional bag-of-words approaches that ignore temporal ordering, and instead embraced RNNs, Temporal CNNs and Transformers, which incorporate contextual information at varying timescales. While these architectures have lead to state-of-the-art performance on many difficult language understanding tasks, it is unclear what representations these networks learn and how exactly they incorporate context. Interpreting these networks, systematically analyzing the advantages and disadvantages of different elements, such as gating or attention, and reflecting on the capacity of the networks across various timescales are open and important questions.

On the biological side, recent work in neuroscience suggests that areas in the brain are organized into a temporal hierarchy in which different areas are not only sensitive to specific semantic information but also to the composition of information at different timescales. Computational neuroscience has moved in the direction of leveraging deep learning to gain insights about the brain. By answering questions on the underlying mechanisms and representational interpretability of these artificial networks, we can also expand our understanding of temporal hierarchies, memory, and capacity effects in the brain.

In this workshop we aim to bring together researchers from machine learning, NLP, and neuroscience to explore and discuss how computational models should effectively capture the multi-timescale, context-dependent effects that seem essential for processes such as language understanding.

We invite you to submit papers related to the following (non-exhaustive) topics:
* Contextual sequence processing in the human brain
* Compositional representations in the human brain
* Systematic generalization in deep learning
* Compositionality in human intelligence
* Compositionality in natural language
* Understanding composition and temporal processing in neural network models
* New approaches to compositionality and temporal processing in language
* Hierarchical representations of temporal information
* Datasets for contextual sequence processing
* Applications of compositional neural networks to real-world problems

Submissions should be up to 4 pages excluding references, 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 will only have a very light review process.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Gary Marcus - Deep Understanding: The Next Challenge for AI</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Gina Kuperberg - How probabilistic is language comprehension in the brain? Insights from multimodal neuroimaging studies</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Poster Session + Break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Uncovering the compositional structure of vector representations with Role Learning Networks</td>
</tr>
<tr>
<td>10:40 AM</td>
<td>Spiking Recurrent Networks as a Model to Probe Neuronal Timescales Specific to Working Memory</td>
</tr>
<tr>
<td>10:50 AM</td>
<td>Learning Compositional Rules via Neural Program Synthesis</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Tom Mitchell - Understanding Neural Processes: Getting Beyond Where and When, to How</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Poster Session + Lunch</td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Yoshua Bengio - Towards compositional understanding of the world by agent-based deep learning</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Ev Fedorenko - Composition as the core driver of the human language system</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Break</td>
</tr>
<tr>
<td>04:00 PM</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>05:30 PM</td>
<td>Closing remarks</td>
</tr>
</tbody>
</table>

Nye, Kim, St Clere Smithe, Itoh, Florez, G. Djokic, Aenugu, Toneva, Schlag, Schwartz, Sobroza Marques, Sainath, Li, Bommansari, Kim, Soulos, Frankland, Chirikova, Han, Kortylewski, Pang, Rabovsky, Mamou, Kumar, Marra

Nye, Kim, St Clere Smithe, Itoh, Florez, G. Djokic, Aenugu, Toneva, Schlag, Schwartz, Sobroza Marques, Sainath, Li, Bommansari, Kim, Soulos, Frankland, Chirikova, Han, Kortylewski, Pang, Rabovsky, Mamou, Kumar, Marra

Yoshua Bengio - Towards compositional understanding of the world by agent-based deep learning

Ev Fedorenko - Composition as the core driver of the human language system

Willke, Fedorenko, Lee, Smolensky

Wehbe
We will use our work studying language processing as a case study to activity when humans and the program process the same input stimuli. To see which computer program aligns best with the observed neural processing, equation solving). Alternative hypotheses can then be tested to perform the same computation (e.g., visual object recognition, sentence computation is done in the brain, in the form of computer programs that

The good news is that a new paradigm has begun to emerge over the past few years, to directly address the how question. The key idea in this paradigm shift is to create explicit hypotheses concerning how computation is done in the brain, in the form of computer programs that perform the same computation (e.g., visual object recognition, sentence processing, equation solving). Alternative hypotheses can then be tested to see which computer program aligns best with the observed neural activity when humans and the program process the same input stimuli. We will use our work studying language processing as a case study to illustrate this new paradigm, in our case using ELMo and BERT deep neural networks as the computer programs that process the same input sentences as the human. Using this case study, we will examine the potential and the limits of this new paradigm as a route toward understanding how the brain computes.

Note: schedule not final and may change

Abstract 10: Yoshua Bengio - Towards compositional understanding of the world by agent-based deep learning in Context and Compositionality in Biological and Artificial Neural Systems, Bengio 02:00 PM

Note: schedule not final and may change

Abstract 13: Panel Discussion in Context and Compositionality in Biological and Artificial Neural Systems, Wilke, Fedorenko, Lee, Smolensky 04:00 PM

Note: schedule not final and may change

Robot Learning: Control and Interaction in the Real World

Roberto Calandra, Kate Rakelly, Sanket Kamthe, Danica Kragic, Stefan Schaal, Markus Wulfmeier

West 220 - 222, Sat Dec 14, 08:00 AM

The growing capabilities of learning-based methods in control and robotics has precipitated a shift in the design of software for autonomous systems. Recent successes fuel the hope that robots will increasingly perform varying tasks working alongside humans in complex, dynamic environments. However, the application of learning approaches to real-world robotic systems has been limited because real-world scenarios introduce challenges that do not arise in simulation.

In this workshop, we aim to identify and tackle the main challenges to learning on real robotic systems. First, most machine learning methods rely on large quantities of labeled data. While raw sensor data is available at high rates, the required variety is hard to obtain and the human effort to annotate or design reward functions is an even larger burden. Second, algorithms must guarantee some measure of safety and robustness to be deployed in real systems that interact with property and people. Instantaneous reset mechanisms, as common in simulation to recover from even critical failures, present a great challenge to real robots. Third, the real world is significantly more complex and varied than curated datasets and simulations. Successful approaches must scale to this complexity and be able to adapt to novel situations.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 AM</td>
<td>Introduction and opening remarks</td>
</tr>
<tr>
<td>09:15 AM</td>
<td>Invited Talk - Marc Deisenroth</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Posters 1</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Contributed Talk - Laura Smith</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Invited Talk - Takayuki Osa</td>
</tr>
</tbody>
</table>
### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:15 AM</td>
<td>Welcome and Introduction</td>
</tr>
<tr>
<td>08:30 AM</td>
<td>Transfer Learning for Text Generation</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Deepfakes: commodification, consequences and countermeasures</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>AI Art Gallery Overview</td>
</tr>
<tr>
<td>09:45 AM</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Artist Lightning Talks</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Neural Painters: A learned differentiable constraint for generating brushstroke paintings</td>
</tr>
<tr>
<td>11:10 AM</td>
<td>Transform the Set: Memory ATTentive Generation of Guided and Unguided Image Collages</td>
</tr>
<tr>
<td>11:20 AM</td>
<td>Paper Dreams: An Interactive Interface for Generative Visual Expression</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Deep reinforcement learning for 2D soft body locomotion</td>
</tr>
<tr>
<td>11:40 AM</td>
<td>Towards Sustainable Architecture: 3D Convolutional Neural Networks for Computational Fluid Dynamics Simulation and Reverse Design Workflow</td>
</tr>
<tr>
<td>11:50 AM</td>
<td>Human and GAN collaboration to create haute couture dress</td>
</tr>
</tbody>
</table>

### NeurIPS Workshop on Machine Learning for Creativity and Design 3.0

**Luba Elliott, Sander Dieleman, Adam Roberts, Jesse Engel, Tom White, Rebecca Fiebrink, Parag Mital, Christine Payne, Nao Tokui**

*West 223 + 224, Sat Dec 14, 08:00 AM*

Generative machine learning and machine creativity have continued to grow and attract a wider audience to machine learning. Generative models enable new types of media creation across images, music, and text - including recent advances such as StyleGAN, MuseNet and GPT-2. This one-day workshop broadly explores issues in the applications of machine learning to creativity and design. We will look at algorithms for generation and creation of new media, engaging researchers building the next generation of generative models (GANs, RL, etc). We investigate the social and cultural impact of these new models, engaging researchers from HCI/UX communities and those using machine learning to develop new creative tools. In addition to covering the technical advances, we also address the ethical concerns ranging from the use of biased datasets to the use of synthetic media such as “DeepFakes”. Finally, we’ll hear from some of the artists and musicians who are adopting machine learning including deep learning and reinforcement learning as part of their own artistic process. We aim to balance the technical issues and challenges of applying the latest generative models to creativity and design with philosophical and cultural issues that surround this area of research.

### Abstracts (4):

**Abstract 4: Posters 1 in Robot Learning: Control and Interaction in the Real World, 10:30 AM**

All poster presenters are welcome to present at both poster sessions. Please see the list of accepted papers at our website: http://www.robot-learning.ml/2019/

**Abstract 5: Contributed Talk - Laura Smith in Robot Learning: Control and Interaction in the Real World, Smith 11:15 AM**

AVID: Translating Human Demonstrations for Automated Learning

**Abstract 10: Posters 2 in Robot Learning: Control and Interaction in the Real World, 02:30 PM**

All poster presenters are welcome to present at both poster sessions. Please see the list of accepted papers at our website: http://www.robot-learning.ml/2019/

**Abstract 12: Contributed Talk (Best Paper) - Michelle Lee & Carlos Florensa in Robot Learning: Control and Interaction in the Real World, Florensa, Lee 04:00 PM**

Combining Model-Free and Model-Based Strategies for Sample-Efficient Reinforcement Learning
### Medical Imaging meets NeurIPS

*Hervé Lombaert, Ben Glocker, Ender Konukoglu, Marleen de Bruijne, Aasa Feragen, Ipek Oguz, Jonas Teuwen*

**West 301 - 305, Sat Dec 14, 08:00 AM**

Medical imaging and radiology are facing a major crisis with an ever-increasing complexity and volume of data along an immense economic pressure. The current advances and widespread use of imaging technologies now overload the human capacity of interpreting medical images, dangerously posing a risk of missing critical patterns of diseases. Machine learning has emerged as a key technology for developing novel tools in computer aided diagnosis, therapy and intervention. Still, progress is slow compared to other fields of visual recognition, which is mainly due to the domain complexity and constraints in clinical applications, i.e., robustness, high accuracy and reliability.

“Medical Imaging meets NeurIPS” aims to bring researchers together from the medical imaging and machine learning communities to discuss the major challenges in the field and opportunities for research and novel applications. The proposed event will be the continuation of a successful workshop organized in NeurIPS 2017 and 2018 (https://sites.google.com/view/med-nips-2018). It will feature a series of invited speakers from academia, medical sciences and industry to give an overview of recent technological advances and remaining major challenges.

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00 AM</td>
<td>Opening Remarks</td>
<td>Lombaert, Glocker, Konukoglu, de Bruijne, Feragen, Oguz, Teuwen</td>
</tr>
<tr>
<td>08:15 AM</td>
<td>Keynote I – Rene Vidal (Johns Hopkins University)</td>
<td>Vidal</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Oral Session I – Methods</td>
<td>Weng, Kohl, Patra</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Coffee Break + Poster Session I</td>
<td>Fadnavis, Roth, Liu, Zhang, Preuhs, Eitel, Trivedi, Weiss, Stern, Vazquez Romaguera, Hofmanninger, Kaku, Olatunji, Razdabiedina, Zhang</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Keynote II – Julia Schnabel (King's College London)</td>
<td>Schnabel</td>
</tr>
<tr>
<td>11:15 AM</td>
<td>Oral Session II – Image Analysis and Segmentation</td>
<td>Taleb, Namdar, Perkonigg, Gong</td>
</tr>
<tr>
<td>12:35 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Keynote III – Leo Grady (Paige AI)</td>
<td>Grady</td>
</tr>
<tr>
<td>02:45 PM</td>
<td>Oral Session III – Imaging</td>
<td>Parmar, Hallgrimsson, Kames</td>
</tr>
<tr>
<td>03:45 PM</td>
<td>Coffee Break + Poster Session II</td>
<td>Macaya, Tamir, OOTA, Heckel, Douglas, Sidorov, Wang, Garcia, Soni, Shukla</td>
</tr>
<tr>
<td>04:15 PM</td>
<td>Keynote IV – Daniel Sodickson (NYU Langone Health)</td>
<td>Sodickson</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>fastMRI Challenge Talks</td>
<td>Yakubova, Pezzotti, Wang, Zitnick, Karkalousos, Sun, Caan, Murrell, Putzky</td>
</tr>
<tr>
<td>06:00 PM</td>
<td>Closing Remarks</td>
<td></td>
</tr>
</tbody>
</table>

### Abstracts (10):

**Abstract 2: Keynote I – Rene Vidal (Johns Hopkins University) in Medical Imaging meets NeurIPS, Vidal 08:15 AM**
Machine Learning in Hematology: Reinventing the Blood Test

Abstract 3: Oral Session I – Methods in Medical Imaging meets NeurIPS, Weng, Kohl, Patra 09:00 AM

09:00 – Multimodal Multitask Representation Learning for Metadata Prediction in Pathology – Weng, Cai, Lin, Tan, Chen
09:40 – Task incremental learning of Chest X-ray data on compact architectures – Patra

Multimodal Multitask Representation Learning for Metadata Prediction in Pathology – Weng, Cai, Lin, Tan, Chen [ORAL+Poster]
Task incremental learning of Chest X-ray data on compact architectures – Patra [ORAL+Poster]

Multimodal Self-Supervised Learning for Medical Image Analysis – Taleb, Lip pert, Nabi, Klein [ORAL+Poster]
Evolution-based Fine-tuning of CNNs for Prostate Cancer Detection – Namdar, Gui rathi, Haider, Khvalati [ORAL+Poster]
Unsupervised deep clustering for predictive texture pattern discovery in medical images – Perkonigg, Sobotka, Ba-Ssalama, Langs [ORAL+Poster]

Abstract 4: Coffee Break + Poster Session I in Medical Imaging meets NeurIPS, Weng, Kohl, Taleb, Patra, Namdar, Perkonigg, Gong, Imran, Abdi, Manakov, Paetzold, Glocker, Sahoo, Fadnavis, Roth, Liu, Zhang, Preuhs, Eitel, Trivedi, Weiss, Stern, Vazquez Romaguera, Hofmanninger, Kaku, Olatunji, Razdai biedina, Zhang 10:00 AM

Multimodal Multitask Representation Learning for Metadata Prediction in Pathology – Weng, Cai, Lin, Tan, Chen [ORAL+Poster]
Task incremental learning of Chest X-ray data on compact architectures – Patra [ORAL+Poster]

Multimodal Self-Supervised Learning for Medical Image Analysis – Taleb, Lip pert, Nabi, Klein [ORAL+Poster]
Evolution-based Fine-tuning of CNNs for Prostate Cancer Detection – Namdar, Gui rathi, Haider, Khvalati [ORAL+Poster]
Unsupervised deep clustering for predictive texture pattern discovery in medical images – Perkonigg, Sobotka, Ba-Ssalama, Langs [ORAL+Poster]

Large-scale classification of breast MRI exams using deep convolutional networks – Gong, Muckley, Wu, Makino, Kim, Heacock, My, Knoll, Geras [ORAL+Poster]
Bipartite Distance For Shape-Aware Landmark Detection in Spinal X-Rays – Zubaer, Huang, Fan, Cheung, To, Qian, Terzopoulos
GAN-enhanced Conditional Echocardiogram – Abdi, Tsang, Abolmaesumi
Invasiveness Prediction of Pulmonary Adenocarcinomas Using Deep Feature Fusion Networks – Li, Ma, Li
Push it to the Limit: Discover Edge-Cases in Image Data with Autoencoders – Manakov, Tresp, Maximilian
Noise-aware PET image Enhancement with Adaptive Deep Learning – Autoencoders – Manakov, Tresp, Maximilian
Modeling of Multiple Independent Operators with Deep Feature Fusion Networks – Li, Gu, Li

Abstract 5: Keynote II – Julia Schnabel (King’s College London) in Medical Imaging meets NeurIPS, Schnabel 10:30 AM

Deep learning for medical image quality control

Abstract 6: Oral Session II – Image Analysis and Segmentation in Medical Imaging meets NeurIPS, Taleb, Namdar, Perkonigg, Gong 11:15 AM

11:15 – Multimodal Self-Supervised Learning for Medical Image Analysis – Taleb, Lip pert, Nabi, Klein
11:35 – Evolution-based Fine-tuning of CNNs for Prostate Cancer Detection – Namdar, Gui rathi, Haider, Khvalati
11:55 – Unsupervised deep clustering for predictive texture pattern discovery in medical images – Perkonigg, Sobotka, Ba-Ssalama, Langs
12:15 – Large-scale classification of breast MRI exams using deep convolutional networks – Gong, Muckley, Wu, Makino, Kim, Heacock, My, Knoll, Geras

Abstract 7: Keynote III – Leo Grady (Paige AI) in Medical Imaging meets NeurIPS, Grady 02:00 PM

Changing the Paradigm of Pathology: AI and Computational Diagnostics

Abstract 8: Oral Session II – Image Analysis and Segmentation in Medical Imaging meets NeurIPS, Taleb, Namdar, Perkonigg, Gong 12:35 PM

12:35 – Multimodal Self-Supervised Learning for Medical Image Analysis – Taleb, Lip pert, Nabi, Klein
12:55 – Evolution-based Fine-tuning of CNNs for Prostate Cancer Detection – Namdar, Gui rathi, Haider, Khvalati
13:15 – Unsupervised deep clustering for predictive texture pattern discovery in medical images – Perkonigg, Sobotka, Ba-Ssalama, Langs
13:35 – Large-scale classification of breast MRI exams using deep convolutional networks – Gong, Muckley, Wu, Makino, Kim, Heacock, My, Knoll, Geras

Abstract 9: Oral Session III – Imaging in Medical Imaging meets NeurIPS, Parmar, Hallgrimsson, Kames 02:45 PM

14:45 – High Resolution Medical Image Analysis with Spatial Partitioning – Hou, Cheng, Shazeer, Parmar, Li, Korfias, Drucker, Blezek, Song
15:05 – Estimating localized complexity of white-matter wiring with GANs – Hallgrimsson, Sharan, Grafton, Singh
15:25 – Training a Variational Network for use on 3D High Resolution MRI Data in 1 Day – Kames, Doucette, Rauscher

Abstract 10: Coffee Break + Poster Session II in Medical Imaging meets NeurIPS, Parmar, Hallgrimsson, Kames, Patra, Imran, Yang, Zimmerer, Chakravarty, Schobs, Gossmann, CHEN, Dutt, Yao, Martinez Manzanera, Pinckaer, Dalmis, Gupta, Haq, Ruhe, Gamper, De
Learning with Temporal Point Processes

Manuel Rodriguez, Le Song, Isabel Valera, Yan Liu, Abir De, Hongyuan Zha

West 306, Sat Dec 14, 08:00 AM

In recent years, there has been an increasing number of machine learning models and algorithms based on the theory of temporal point processes, which is a mathematical framework to model asynchronous event data. These models and algorithms have found a wide range of human-centered applications, from social and information networks and recommender systems to crime prediction and health. Moreover, this emerging line of research has already established connections to deep learning, deep generative models, Bayesian nonparametrics, causal inference, stochastic optimal control and reinforcement learning. However, despite these recent advances, learning with temporal point processes is still a relatively niche topic within the machine learning community—there are only a few research groups across the world with the necessary expertise to make progress. In this workshop, we aim to popularize temporal point processes within the machine learning community at large. In our view, this is the right time to organize such a workshop because, as algorithmic decisions become more consequential to individuals and society, temporal point processes will play a major role in the development of human-centered machine learning models and algorithms accounting for the feedback loop between algorithmic and human decisions, which are inherently asynchronous events. Moreover, it will be a natural follow up of a very successful and well-attended ICML 2018 tutorial on learning with temporal point processes, which two of us recently taught.
The Optimization Foundations of Reinforcement Learning

Bo Dai, Niao He, Nicolas Le Roux, Lihong Li, Dale Schuurmans, Martha White

West Ballroom A, Sat Dec 14, 08:00 AM

Interest in reinforcement learning (RL) has boomed with recent improvements in benchmark tasks that suggest the potential for a revolutionary advance in practical applications. Unfortunately, research in RL remains hampered by limited theoretical understanding, making the field overly reliant on empirical exploration with insufficient principles to guide future development. It is imperative to develop a stronger fundamental understanding of the success of recent RL methods, both to expand the usability of the methods and accelerate future deployment. Recently, fundamental concepts from optimization and control theory have provided a fresh perspective that has led to the development of sound RL algorithms with provable efficiency. The goal of this workshop is to catalyze the growing synergy between RL and optimization research, promoting a rational reconsideration of the foundational principles for reinforcement learning, and bridging the gap between theory and practice.

Schedule

08:00 AM Opening Remarks Dai, He, Le Roux, Li, Schuurmans, White

08:10 AM Unsupervised State Embedding and Aggregation towards Scalable Reinforcement Learning Wang

08:50 AM Adaptive Trust Region Policy Optimization: Convergence and Faster Rates of regularized MDPs Shani, Efroni, Mannor

09:10 AM Poster Spotlight 1 Brandfonbrener, Bruna, Zahavy, Kaplan, Mansour, Karampatziakis, Langford, Mineiro, Lee, He

09:30 AM Insider Threat Detection via Hierarchical Neural Temporal Point Processes Wu

09:45 AM Coffee Break

10:30 AM Invited Talk By Niloy Ganguly ganguly

11:00 AM Multivariate coupling estimation between continuous signals and point processes Besserve

11:10 AM Intermittent Demand Forecasting with Deep Renewal Processes Turkmen

11:25 AM Temporal Logic Point Processes

11:40 AM The Graph Hawkes Network for Reasoning on Temporal Knowledge Graphs

11:55 AM Multivariate coupling estimation between continuous signals and point processes Besserve

12:10 PM Lunch Break

01:50 PM Invited Talk by Walter Dempsey Dempsey

02:30 PM Better Approximate Inference for Partial Likelihood Models with a Latent Structure Setlur

02:45 PM Deep Point Process Destructors

03:00 PM A sleep-wake detection algorithm for memory-constrained wearable devices: Change Point Decoder Cakmak

03:15 PM Topics are not Marks: Modeling Text-based Cascades using Multi-network Hawkes Process Choudhari

03:30 PM Poster Setup + Coffee Break

04:15 PM Temporal point process models vs. discrete time models

Cakmak, Zhang, Prabhatkarannair Kusumam, Ahmed, Wu, Choudhari, Inouye, Taylor, Besserve, Turkmen, Islam, Artés, Setlur, Fu, Han, De, Du, Sanchez Martin

05:00 PM Poster Session
09:30 AM  Poster and Coffee Break 1

10:30 AM  The Provable Effectiveness of Policy Gradient Methods in Reinforcement Learning

11:10 AM  Panel Discussion

11:40 AM  Poster Spotlight 2

02:00 PM  Reinforcement Learning Beyond Optimization

02:40 PM  Learning in structured MDPs with convex cost function: improved regret bounds for inventory management

03:20 PM  Poster and Coffee Break 2

04:20 PM  On the Convergence of GTD($\lambda$) with General $\lambda$

05:00 PM  Continuous Online Learning and New Insights to Online Imitation Learning

05:20 PM  Logarithmic Regret for Online Control

05:40 PM  Closing Remarks

Abstracts (10):

Abstract 2: Unsupervised State Embedding and Aggregation towards Scalable Reinforcement Learning in The Optimization Foundations of Reinforcement Learning, Wang 08:10 AM

TBA

Abstract 3: Adaptive Trust Region Policy Optimization: Convergence and Faster Rates of Regularized MDPs in The Optimization Foundations of Reinforcement Learning, Shani, Efroni, Mannor 08:50 AM

Trust region policy optimization (TRPO) is a popular and empirically successful policy search algorithm in Reinforcement Learning (RL) in...
which a surrogate problem, that restricts consecutive policies to be ‘close’ to one another, is iteratively solved. Nevertheless, TRPO has been considered a heuristic algorithm inspired by Conservative Policy Iteration (CPI). We show that the adaptive scaling mechanism used in TRPO is in fact the natural ‘RL version’ of traditional trust-region methods from convex analysis. We first analyze TRPO in the planning setting, in which we have access to the model and the entire state space. Then, we consider sample-based TRPO and establish $O(1/\sqrt{N})$ convergence rate to the global optimum. Importantly, the adaptive scaling mechanism allows us to analyze TRPO in regularized MDPs for which we prove fast rates of $O(1/N)$, much like results in convex optimization. This is the first result in RL of better rates when regularizing the instantaneous cost or reward.

Abstract 6: The Provable Effectiveness of Policy Gradient Methods in Reinforcement Learning in The Optimization Foundations of Reinforcement Learning, Kakade 10:30 AM

Reinforcement learning is now the dominant paradigm for how an agent learns to interact with the world in order to achieve some long term objectives. Here, policy gradient methods are among the most effective methods in challenging reinforcement learning problems, due to that they: are applicable to any differentiable policy parameterization; admit easy extensions to function approximation; easily incorporate structured state and action spaces; are easy to implement in a simulation based, model-free manner.

However, little is known about even their most basic theoretical convergence properties, including:
- do they converge to a globally optimal solution, say with a sufficiently rich policy class?
- how well do they cope with approximation error, say due to using a class of neural policies?
- what is their finite sample complexity?

This talk will survey a number of results on these basic questions. We will highlight the interplay of theory, algorithm design, and practice.

Joint work with: Alekh Agarwal, Jason Lee, Gaurav Mahajan

Abstract 7: Panel Discussion in The Optimization Foundations of Reinforcement Learning, Sutton,Precup 11:10 AM

TBA

Abstract 9: Reinforcement Learning Beyond Optimization in The Optimization Foundations of Reinforcement Learning, Van Roy 02:00 PM

The reinforcement learning problem is often framed as one of quickly optimizing an uncertain Markov decision process. This formulation has led to substantial insight and progress in algorithms and theory. However, this perspective is limiting and can also give rise to poor algorithm designs. I will discuss this issue and how it is addressed by popular reinforcement learning algorithms.

Abstract 10: Learning in structured MDPs with convex cost function: improved regret bounds for inventory management in The Optimization Foundations of Reinforcement Learning, Agrawal 02:40 PM

We present a learning algorithm for the stochastic inventory control problem under lost sales penalty and positive lead times, when the demand distribution is a priori unknown. Our main result is a regret bound of $O(\sqrt{T})$ for the algorithm, where $T$ is the time horizon, $L$ is the fixed and known lead time, and $D$ is an unknown parameter of the demand distribution described roughly as the number of time steps needed to generate enough demand for depleting one unit of inventory. Our results significantly improve the existing regret bounds for this problem. Notably, even though the state space of the underlying Markov Decision Process (MDP) in this problem is continuous and L-dimensional, our regret bounds depend linearly on L. Our techniques utilize convexity of the long run average cost and a newly derived bound on the ‘bias’ of base-stock policies, to establish an almost blackbox connection between the problem of learning and optimization in such MDPs and stochastic convex bandit optimization. The techniques presented here may be of independent interest for other settings that involve learning large structured MDPs but with convex cost functions.

Abstract 12: On the Convergence of GTD($\lambda$) with General $\lambda$ in The Optimization Foundations of Reinforcement Learning, Yu 04:20 PM

Gradient temporal-difference (GTD) algorithms are an important family of extensions of the standard TD algorithm, overcoming the stability issues in off-policy learning with function approximation by minimizing the projected Bellman error using stochastic gradient descent (SGD). In this talk, we consider GTD($\lambda$) for policy evaluation in the case of linear function approximation and finite-space Markov decision processes (MDPs) with discounted rewards. GTD($\lambda$) differs from the typical SGD algorithm for minimizing an objective function, in the following way. In an MDP, each stationary policy is associated with a family of Bellman equations. By selecting the values of the eligibility trace parameters, $\lambda$, we determine the Bellman operator that defines the objective function. This choice influences both the approximation error and learning behavior of the resulting algorithm. We first describe a dynamic scheme to judiciously set $\lambda$ in a history-dependent way. This scheme is based on the idea of randomized stopping times and generalized Bellman equations, and it is useful for balancing the bias-variance tradeoff in off-policy learning. We then present asymptotic convergence results for several variations of GTD($\lambda$), including saddle-point and mirror-descent TD variants, for different choices of $\lambda$: constant, state-dependent, and history-dependent. These convergence results are obtained by combining special properties of the joint state and eligibility trace process in TD learning with ergodic theory for weak Feller Markov chains, mean-ODE-based proof methods, and convex optimization theory. Our results not only resolve long-standing open questions regarding the convergence of GTD($\lambda$) but also provide the basis for using a broader class of generalized Bellman operators for approximate policy evaluation with linear TD methods.

Abstract 13: Continuous Online Learning and New Insights to Online Imitation Learning in The Optimization Foundations of Reinforcement Learning, Lee, Cheng, Goldberg, Boots 05:00 PM

Online learning is a powerful tool for analyzing iterative algorithms. However, the classic adversarial setup sometimes fails to capture certain regularity in online problems in practice. Motivated by this, we establish a new setup, called Continuous Online Learning (COL), where the gradient of online loss function changes continuously across rounds with respect to the learner’s decisions. We show that COL covers and more appropriately describes many interesting applications, from general equilibrium problems (EPs) to optimization in episodic MDPs. Using this new setup, we revisit the difficulty of achieving sublinear dynamic regret.
We prove that there is a fundamental equivalence between achieving sublinear dynamic regret in COL and solving certain EPs, and we present a reduction from dynamic regret to both static regret and convergence rate of the associated EP. At the end, we specialize these new insights into online imitation learning and show improved understanding of its learning stability.

Abstract 14: Logarithmic Regret for Online Control in The Optimization Foundations of Reinforcement Learning, Agarwal, Hazan, Singh 05:20 PM

We study optimal regret bounds for control in linear dynamical systems under adversarially changing strongly convex cost functions, given the knowledge of transition dynamics. This includes several well studied and fundamental frameworks such as the Kalman filter and the linear quadratic regulator. State of the art methods achieve regret which scales as $T^{0.5}$, where $T$ is the time horizon.

We show that the optimal regret in this setting can be significantly smaller, scaling as polylog $T$. This regret bound is achieved by two different efficient iterative methods, online gradient descent and online natural gradient.

Abstract 15: Closing Remarks in The Optimization Foundations of Reinforcement Learning, Dai, He, Le Roux, Li, Schuurmans, White 05:40 PM

Awards Announcement

Machine Learning with Guarantees

Ben London, Gintare Karolina Dziugaite, Dan Roy, Thorsten Joachims, Aleksander Madry, John Shawe-Taylor

West Ballroom B, Sat Dec 14, 08:00 AM

As adoption of machine learning grows in high-stakes application areas (e.g., industry, government and health care), so does the need for guarantees: how accurate a learned model will be; whether its predictions will be fair; whether it will divulge information about individuals; or whether it is vulnerable to adversarial attacks. Many of these questions involve unknown or intractable quantities (e.g., risk, regret or posterior likelihood) and complex constraints (e.g., differential privacy, fairness, and adversarial robustness). Thus, learning algorithms are often designed to yield (and optimize) bounds on the quantities of interest. Beyond providing guarantees, these bounds also shed light on black-box machine learning systems.

Classical examples include structural risk minimization (Vapnik, 1991) and support vector machines (Cristianini & Shawe-Taylor, 2000), while more recent examples include non-vacuous risk bounds for neural networks (Dziugaite & Roy, 2017, 2018), algorithms that optimize both the weights and structure of a neural network (Cortes, 2017), counterfactual risk minimization for learning from logged bandit feedback (Swaminathan & Joachims, 2015; London & Sandler, 2019), robustness to adversarial attacks (Schmidt et al., 2018; Wong & Kolter, 2018), differentially private learning (Dwork et al., 2006, Chaudhuri et al., 2011), and algorithms that ensure fairness (Dwork et al., 2012).

This one-day workshop will bring together researchers in both theoretical and applied machine learning, across areas such as statistical learning theory, adversarial learning, fairness and privacy, to discuss the problem of obtaining performance guarantees and algorithms to optimize them. The program will include invited and contributed talks, poster sessions and a panel discussion. We particularly welcome contributions describing fundamentally new problems, novel learning principles, creative bound optimization techniques, and empirical studies of theoretical findings.
Abstract 2: Tengyu Ma, “Designing Explicit Regularizers for Deep Models” in Machine Learning with Guarantees, Ma 09:00 AM

I will discuss some recent results on designing explicit regularizers to improve the generalization performances of deep neural networks. We derive data-dependent generalization bounds for deep neural networks. We empirically regularize the bounds and obtain improved generalization performance (in terms of the standard accuracy or the robust accuracy). I will also touch on recent results on applying these techniques to imbalanced datasets.

Based on joint work with Colin Wei, Kaidi Cao, Adrien Gaidon, and Nikos Arechiga


Abstract 3: Vatsal Sharan, “Sample Amplification: Increasing Dataset Size even when Learning is Impossible” in Machine Learning with Guarantees, Sharan 09:45 AM

Given data drawn from an unknown distribution, $\mathcal{D}$, to what extent is it possible to “amplify” this dataset and faithfully output a larger set of samples that appear to have been drawn from $\mathcal{D}$? We formalize this question as follows: an $(n,m)$ amplification procedure takes as input $n$ independent draws from an unknown distribution $\mathcal{D}$, and outputs a set of $m > n$ “samples” which must be indistinguishable from $m$ samples drawn i.i.d. from $\mathcal{D}$. We consider this sample amplification problem in two fundamental settings: the case where $\mathcal{D}$ is an arbitrary discrete distribution supported on $k$ elements, and the case where $\mathcal{D}$ is a $d$-dimensional Gaussian with unknown mean, and fixed covariance matrix. Perhaps surprisingly, we show a valid amplification procedure exists for both of these settings, even in the regime where the size of the input dataset, $n$, is significantly less than what would be necessary to learn distribution $\mathcal{D}$ to non-trivial accuracy. We also show that our procedures are optimal up to constant factors. Beyond these results, we also formalize a number of curious directions for future research along this vein.

This is a joint work with Alex Levine and Sahil Singla.

Abstract 4: Soheil Feizi, “Certifiable Defenses against Adversarial Attacks” in Machine Learning with Guarantees, Feizi 01:45 PM

While neural networks have achieved high performance in different learning tasks, their accuracy drops significantly in the presence of small adversarial perturbations to inputs. In the last couple of years, several practical defenses based on regularization and adversarial training have been proposed which are often followed by stronger attacks to defeat them. To escape this cycle, a new line of work focuses on developing certifiably robust classifiers. In these models, for a given input sample, one can calculate a robustness certificate such that for ‘any’ perturbation of the input within the robustness radius, the classification output will ‘provably’ remain unchanged. In this talk, I will present two certifiable defenses: (1) Wasserstein smoothing to defend against non-additive Wasserstein adversarial attacks, and (2) Curvature-based robust training to certifiably defend against L2 attacks by globally bounding curvature values of the network.

This is a joint work with Alex Levine and Sahil Singla.

Abstract 5: Maksym Andriushchenko, ”Provably Robust Boosted Decision Stumps and Trees against Adversarial Attacks” in Machine Learning with Guarantees, Andriushchenko 02:30 PM

The problem of adversarial robustness has been studied extensively for neural networks. However, for boosted decision trees and decision stumps there are almost no results, even though they are widely used in practice (e.g. XGBoost) due to their accuracy, interpretability, and...
establish the evidence base for important decision-making processes.

differently?”, and “What if had ranked a list differently?” thus helping to counterfactual questions, such as “What if I had treated a patient
embracing causal reasoning autonomous systems will be able to answer citations.

decision, one must understand the process of identifying causality. By a short version of the corresponding NeurIPS 2019 paper have important consequences, and so, in seeking to make the best
increased expectations for autonomous systems to make the right
drastic success has led to improved decision making.

---

NeurIPS 2019 Workshop book

We show in this paper that for boosted decision stumps the exact min-max robust loss and test error for an $l_\infty$-attack can be computed in $O(T \log T)$ time per input, where $T$ is the number of decision stumps and the optimal update step of the ensemble can be done in $O(n^2T \log T)$, where $n$ is the number of data points. For boosted trees we show how to efficiently calculate and optimize an upper bound on the robust loss, which leads to state-of-the-art robust test error for boosted trees on MNIST (12.5% for $\epsilon=0.9$), FMNIST (23.2% for $\epsilon=0.1$), and CIFAR-10 (74.7% for $\epsilon=8/255$). Moreover, the robust test error rates we achieve are competitive to the ones of provably robust CNNs. Code of our method is available at https://git.io/Je18r. This is a short version of the corresponding NeurIPS 2019 paper cite{andriushchenko2019provably}.

Abstract 10: Coffee Break / Poster Session 2 in Machine Learning with Guarantees, 03:00 PM

Visit https://sites.google.com/view/mlwithguarantees/accepted-papers for the list of papers.

Posters will be up all day.

Abstract 12: Hussein Mozannar, “Fair Learning with Private Data” in Machine Learning with Guarantees, Mozannar 04:15 PM

We study learning non-discriminatory predictors when the protected attributes are privatized or noisy. We observe that, in the population limit, non-discrimination against noisy attributes is equivalent to that against original attributes. We show this to hold for various fairness criteria. We then characterize the amount of difficulty, in sample complexity, that privacy adds to testing non-discrimination. Using this relationship, we propose how to carefully adapt existing non-discriminatory learners to work with privatized protected attributes. Care is crucial, as naively using these learners may create the illusion of non-discrimination, while continuing to be highly discriminatory.

“Do the right thing”: machine learning and causal inference for improved decision making

Michele Santacatterina, Thorsten Joachims, Nathan Kallus, Adith Swaminathan, David Sontag, Angela Zhou

West Ballroom C, Sat Dec 14, 08:00 AM

In recent years, machine learning has seen important advances in its theoretical and practical domains, with some of the most significant applications in online marketing and commerce, personalized medicine, and data-driven policy-making. This dramatic success has led to increased expectations for autonomous systems to make the right decision at the right target at the right time. This gives rise to one of the major challenges of machine learning today that is the understanding of the cause-effect connection. Indeed, actions, intervention, and decisions have important consequences, and so, in seeking to make the best decision, one must understand the process of identifying causality. By embracing causal reasoning autonomous systems will be able to answer counterfactual questions, such as “What if I had treated a patient differently?”, and “What if I had ranked a list differently?” thus helping to establish the evidence base for important decision-making processes.

The purpose of this workshop is to bring together experts from different fields to discuss the relationships between machine learning and causal inference and to discuss and highlight the formalization and algorithmization of causality toward achieving human-level machine intelligence.

This purpose will guide the makeup of the invited talks and the topics for the panel discussions. The panel discussions will tackle controversial topics, with the intent of drawing out an engaging intellectual debate and conversation across fields.

This workshop will lead to advance and extend knowledge on how machine learning could be used to conduct causal inference, and how causal inference could support the development of machine learning methods for improved decision-making.

Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:45 AM</td>
<td>Opening Remarks</td>
<td>Joachims, Kallus, Santacatterina, Swaminathan, Sontag, Zhou</td>
</tr>
<tr>
<td>09:00 AM</td>
<td>Susan Athey</td>
<td>Athey</td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Andrea Rotnitzky</td>
<td>Rotnitzky</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Poster Spotlights</td>
<td>Namkoong, Charpignon, Rudolph, Coston, Saito, Dhillon, Markham</td>
</tr>
<tr>
<td>10:15 AM</td>
<td>Coffee break, posters, and 1-on-1 discussions</td>
<td>Lu, Chen, Namkoong, Charpignon, Rudolph, Coston, von Kügelgen, Prasad, Dhillon, Xu, Wang, Markham, Rohde, Singh, Zhang, Hassanpour, Sharma, Lee, Pouget-Abadie, Krijthe, Mahajan, Ke, Winsberger, Semenova, Mykhaylov, Shen, Takatsu, Sun, Yang, Franks, Wong, Zaman, Mitchell, kang, Yang</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Susan Murphy</td>
<td>Murphy</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Ying-Qi Zhao</td>
<td>Zhao</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Tentative topic: Reasoning about untestable assumptions in the face of unknowable counterfactuals</td>
<td></td>
</tr>
<tr>
<td>12:45 PM</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>02:30 PM</td>
<td>Susan Shortreed</td>
<td>Shortreed</td>
</tr>
<tr>
<td>03:00 PM</td>
<td>Contributed talk 1</td>
<td>Chen, Boehnke, Wang, Bonaldi</td>
</tr>
<tr>
<td>03:15 PM</td>
<td>Contributed talk 2</td>
<td>Mahajan, Khosravi, D'Amour</td>
</tr>
</tbody>
</table>
**NeurIPS 2019 Workshop book**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>03:00 PM</td>
<td>Poster Spotlights</td>
<td>Griveau-Billion, Singh, Zhang, Lee, Krijthe, Charles, Semenova, Ladhania, Oprescu</td>
</tr>
<tr>
<td>03:40 PM</td>
<td>Oral Spotlights 1</td>
<td>von Kügelgen, Rohde, Schumann, Charles, Veitch, Semenova, Demirer, Syrkganis, Nair, Puli, Uehara, Gopalan, Ding, Ng, Khosravi, Sherman, Zeng, Wieczorek, Liu, Gan, Hartford, Oprescu, D'Amour, Boehnke, Saito, Griveau-Billion, Modi, Karimov, Berrevoets, Graham, Josse, Sridhar, Dahabreh, Mishler, Wadsworth, Qureshi, Ladhania, Morishita, Welle</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Poster Spotlights</td>
<td>Griveau-Billion, Gauthier Gidel, Niao He, Reyhane Askari, Hemmat, Nika Haghtalab, Simon Lacoste-Julien</td>
</tr>
<tr>
<td>03:45 PM</td>
<td>Coffee break, posters, and 1-on-1 discussions</td>
<td>von Kügelgen, Rohde, Schumann, Charles, Veitch, Semenova, Demirer, Syrkganis, Nair, Puli, Uehara, Gopalan, Ding, Ng, Khosravi, Sherman, Zeng, Wieczorek, Liu, Gan, Hartford, Oprescu, D'Amour, Boehnke, Saito, Griveau-Billion, Modi, Karimov, Berrevoets, Graham, Josse, Sridhar, Dahabreh, Mishler, Wadsworth, Qureshi, Ladhania, Morishita, Welle</td>
</tr>
<tr>
<td>05:00 PM</td>
<td>Closing Remarks</td>
<td></td>
</tr>
</tbody>
</table>

### Abstracts (5):

**Abstract 4:** Poster Spotlights in “Do the right thing”: machine learning and causal inference for improved decision making. Namkoong, Charpignon, Rudolph, Coston, Saito, Dhillon, Markham 10:00 AM

Poster spotlights ID: 10, 11, 16, 17, 20, 24, 31

**Abstract 8:** Tentative topic: Reasoning about untestable assumptions in the face of unknowable counterfactuals in “Do the right thing”: machine learning and causal inference for improved decision making, 12:00 PM

Tentative topic: How machine learning, and causal inference work together: cross-pollination and new challenges.

**Abstract 11:** Contributed talk 1 in “Do the right thing”: machine learning and causal inference for improved decision making. Chen, Boehnke, Wang, Bonaldi 03:00 PM

**Abstract 12:** Contributed talk 2 in “Do the right thing”: machine learning and causal inference for improved decision making. Mahajan, Khosravi, D'Amour 03:15 PM

**Abstract 13:** Poster Spotlights in “Do the right thing”: machine learning and causal inference for improved decision making. Griveau-Billion, Singh, Zhang, Lee, Krijthe, Charles, Semenova, Ladhania, Oprescu 03:30 PM

### Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:15 AM</td>
<td>Opening remarks</td>
<td></td>
</tr>
<tr>
<td>08:30 AM</td>
<td>Invited talk: Eva Tardos</td>
<td>Tardos (Cornell)</td>
</tr>
<tr>
<td>09:10 AM</td>
<td>Morning poster Spotlight</td>
<td></td>
</tr>
<tr>
<td>09:30 AM</td>
<td>Morning poster session -- coffee break</td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Invited talk: David Balduzzi</td>
<td>Balduzzi (DeepMind)</td>
</tr>
<tr>
<td>11:40 AM</td>
<td>Contributed talk: What is Local Optimality in Nonconvex-Nonconcave Minimax Optimization?</td>
<td>Netrapalli</td>
</tr>
<tr>
<td>12:05 PM</td>
<td>Contributed talk: Characterizing Equilibria in Fiez Stackelberg Games</td>
<td></td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch break</td>
<td></td>
</tr>
<tr>
<td>02:00 PM</td>
<td>Invited talk: Fei Fang</td>
<td>Fang (CMU)</td>
</tr>
<tr>
<td>02:40 PM</td>
<td>Contributed talk: On Solving Local Minimax Optimization: A Follow-the-Ridge Approach</td>
<td>Wang</td>
</tr>
<tr>
<td>03:05 PM</td>
<td>Contributed talk: Exploiting Uncertain Real-Time Information from Deep Learning in Signaling Games for Security and Sustainability</td>
<td>Bondi</td>
</tr>
<tr>
<td>03:30 PM</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>04:00 PM</td>
<td>Invited talk: Aryan Mokhtari</td>
<td>Mokhtari (UT Austin)</td>
</tr>
</tbody>
</table>
Minimax optimization has found extensive applications in modern machine learning, in settings such as generative adversarial networks (GANs), adversarial training and multi-agent reinforcement learning. As most of these applications involve continuous nonconvex-nonconcave formulations, a very basic question arises—"what is a proper definition of local optima?" Most previous work answers this question using classical notions of equilibria from simultaneous games, where the min-player and the max-player act simultaneously. In contrast, most applications in machine learning, including GANs and adversarial training, correspond to sequential games, where the order of which player acts first is crucial (since minimax is in general not equal to maximin due to the nonconvex-nonconcave nature of the problems). The main contribution of this paper is to propose a proper mathematical definition of local optimality for this sequential setting—local minimax, as well as to present the fixed points of gradient dynamics might not be local minimax. In particular, two-player zero-sum games. Moreover, we show that the only stable attractors of the sequential games, where the min-player and the max-player act simultaneously. In contrast, most applications in machine learning, including GANs and adversarial training, correspond to sequential games, where the order of which player acts first is crucial (since minimax is in general not equal to maximin due to the nonconvex-nonconcave nature of the problems). The main contribution of this paper is to propose a proper mathematical definition of local optimality for this sequential setting—local minimax, as well as to present its properties and existence results. Finally, we establish a strong connection to a basic local search algorithm—gradient descent ascent (GDA): under mild conditions, all stable limit points of GDA are exactly local minimax points up to some degenerate points.

This paper investigates the convergence of learning dynamics in Stackelberg games on continuous action spaces, a class of games distinguished by the hierarchical order of play between agents. We establish connections between the Nash and Stackelberg equilibrium concepts and characterize conditions under which attractors of simultaneous gradient descent are Stackelberg equilibria in zero-sum games. Moreover, we show that the only stable attractors of the Stackelberg gradient dynamics are Stackelberg equilibria in zero-sum games. Using this insight, we develop two-timescale learning dynamics that converge to Stackelberg equilibria in zero-sum games and the set of stable attractors in general-sum games.

Many tasks in modern machine learning can be formulated as finding equilibria in (sequential) games. In particular, two-player zero-sum sequential games, also known as minimax optimization, have received growing interest. It is tempting to apply gradient descent to solve minimax optimization given its popularity in supervised learning. However, we note that naive application of gradient descent fails to find local minimax--the analogy of local minima in minimax optimization, since the fixed points of gradient dynamics might not be local minimax. In this paper, we propose (Follow-the-Ridge) (FR), an algorithm that locally converges to and only converges to local minimax. We show theoretically that the algorithm addresses the limit cycling problem around fixed points, and is compatible with preconditioning and positive momentum. Empirically, FR solves quadratic minimax problems and improves GAN training on simple tasks.

Motivated by real-world deployment of drones for conservation, this paper advances the state-of-the-art in security games with signaling. The well-known defender-attacker security games framework can help in planning for such strategic deployments of sensors and human patrollers, and warning signals to ward off adversaries. However, we show that defenders can suffer significant losses when ignoring real-world uncertainties, such as detection uncertainty resulting from imperfect deep learning models, despite carefully planned security game strategies with signaling. In fact, defenders may perform worse than forgoing drones completely in this case. We address this shortcoming by proposing a novel game model that integrates signaling and sensor uncertainty; perhaps surprisingly, we show that defenders can still perform well via a signaling strategy that exploits the uncertain real-time information primarily from deep learning models. For example, even in the presence of uncertainty, the defender still has an informational advantage in knowing that she has or has not actually detected the attacker; and she can design a signaling scheme to "mislead" the attacker who is uncertain as to whether he has been detected. We provide a novel algorithm, scale-up techniques, and experimental results from simulation based on our ongoing deployment of a conservation drone system in South Africa.

This paper investigates the convergence of learning dynamics in Stackelberg games on continuous action spaces, a class of games distinguished by the hierarchical order of play between agents. We establish connections between the Nash and Stackelberg equilibrium concepts and characterize conditions under which attractors of simultaneous gradient descent are Stackelberg equilibria in zero-sum games. Moreover, we show that the only stable attractors of the Stackelberg gradient dynamics are Stackelberg equilibria in zero-sum games. Using this insight, we develop two-timescale learning dynamics that converge to Stackelberg equilibria in zero-sum games and the set of stable attractors in general-sum games.

This paper investigates the convergence of learning dynamics in Stackelberg games on continuous action spaces, a class of games distinguished by the hierarchical order of play between agents. We establish connections between the Nash and Stackelberg equilibrium concepts and characterize conditions under which attractors of simultaneous gradient descent are Stackelberg equilibria in zero-sum games. Moreover, we show that the only stable attractors of the Stackelberg gradient dynamics are Stackelberg equilibria in zero-sum games. Using this insight, we develop two-timescale learning dynamics that converge to Stackelberg equilibria in zero-sum games and the set of stable attractors in general-sum games.

Deep Reinforcement Learning

Pieter Abbeel, Chelsea Finn, Joelle Pineau, David Silver, Satinder Singh, Joshua Achiam, Carlos Fiorenza, Christopher Grimm, Haoran Tang, Vivek Veeriah

West Exhibition Hall C, Sat Dec 14, 08:00 AM

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.

Schedule

08:45 AM Welcome Comments
09:00 AM  Grandmaster Level in StarCraft II using Multi-Agent Reinforcement Learning - Invited Talk  Vinyals

09:30 AM  Contributed Talks  Tang, Guo, Hafner

10:00 AM  Bayes-Adaptive Deep Reinforcement Learning via Meta-Learning - Invited Talk  Whiteson

10:30 AM  Coffee Break

11:00 AM  Optico: A Framework for Model-Based Optimization with MuJoCo Physics - Invited Talk  Todorov

11:30 AM  Contributed Talks  Lu, Hausknecht, Nachum

12:00 PM  Late-Breaking Papers (Talks)  Silver, Du, Plappert

01:30 PM  Invited Talk  Brunskill

02:00 PM  Contributed Talks  Agarwal, Gleave, Lee

02:30 PM  Poster Session

04:00 PM  NeurIPS RL Competitions Results Presentations

05:00 PM  Assessing the Robustness of Deep RL Algorithms - Littman Invited Talk

05:30 PM  Panel Discussion

Abstracts (7):

Abstract 3: Contributed Talks in Deep Reinforcement Learning, Tang, Guo, Hafner 09:30 AM

* "Playing Dota 2 with Large Scale Deep Reinforcement Learning" - OpenAI, Christopher Berner, Greg Brockman, Brooke Chan, Vicki Cheung, Przemyslaw Biak, Christy Dennison, David Farhi, Quirin Fischer, Shariq Hashme, Chris Hesse, Rafal Józefowicz, Scott Gray, Catherine Olsson, Jakub Pachocki, Michael Petrov, Henrique Pondé de Oliveira Pinto, Jonathan Raiman, Tim Salimans, Jeremy Schelter, Jonas Schneider, Szymon Sidor, Ilya Sutskever, Jie Tang, Filip Wolski, Susan Zhang
* "Efficient Exploration with Self-Imitation Learning via Trajectory-Conditioned Policy" - Yijie Guo, Jongwook Choi, Marcin Moczulski, Samy Bengio, Mohammad Norouzi, Honglak Lee
* "Efficient Visual Control by Latent Imagination" - Danijar Hafner, Timothy Lillicrap, Jimmy Ba, Mohammad Norouzi

Abstract 7: Contributed Talks in Deep Reinforcement Learning, Lu, Hausknecht, Nachum 11:30 AM

* "Adaptive Online Planning for Lifelong Reinforcement Learning" - Kevin Lu, Igor Mordatch, Pieter Abbeel
* "Interactive Fiction Games: A Colossal Adventure" - Matthew Hausknecht, Prithviraj V Ammanabrolu, Marc-Alexandre Côté, Xingdi Yuan

Abstract 8: Late-Breaking Papers (Talks) in Deep Reinforcement Learning, Silver, Du, Plappert 12:00 PM

* Is a Good Representation Sufficient for Sample Efficient Reinforcement Learning? - Simon S. Du, Sham M. Kakade, Ruosong Wang, Lin F. Yang
* Solving Rubik's Cube with a Robot Hand - OpenAI, Ilge Akkaya, Marcin Andrychowicz, Maciek Chociej, Mateusz Litwin, Bob McGrew, Arthur Petron, Alex Paino, Matthias Plappert, Glenn Powell, Raphael Ribas, Jonas Schneider, Nikolas Tezak, Jerry Tworek, Peter Welinder, Lilian Weng, Giming Yuan, Wojciech Zaremba, Lei Zhang

Abstract 9: Invited Talk in Deep Reinforcement Learning, Brunskill 01:30 PM

(Talk title and abstract TBD.)

Abstract 10: Contributed Talks in Deep Reinforcement Learning, Agarwal, Gleave, Lee 02:00 PM
* "Striving for Simplicity in Off-Policy Deep Reinforcement Learning" - Rishabh Agarwal, Dale Schuurmans, Mohammad Norouzi
* "Adversarial Policies: Attacking Deep Reinforcement Learning" - Adam R Gleave, Michael Dennis, Neel Kant, Cody Wild, Sergey Levine, Stuart Russell
* "A Simple Randomization Technique for Generalization in Deep Reinforcement Learning" - Kimin Lee, Kibok Lee, Jinwoo Shin, Honglak Lee

Abstract 12: NeurIPS RL Competitions Results Presentations in Deep Reinforcement Learning, 04:00 PM

16:00 - 16:15 Learn to Move: Walk Around
16:15 - 16:30 Animal Olympics
16:30 - 16:45 Robot open-Ended Autonomous Learning (REAL)
16:45 - 17:00 MineRL

Abstract 14: Panel Discussion in Deep Reinforcement Learning, 05:30 PM

(Topic and panelists TBA.)