

Reproducible, Reusable, and Robust Reinforcement Learning

Invited Talk (Posner Lecture) | Wed Dec 5th 08:30 -- 09:20 AM @ Rooms 220 CDE

Joelle Pineau

We have seen significant achievements with deep reinforcement learning in recent years. Yet reproducing results for state-of-the-art deep RL methods is seldom straightforward. High variance of some methods can make learning particularly difficult when environments or rewards are strongly stochastic. Furthermore, results can be brittle to even minor perturbations in the domain or experimental procedure. In this talk, I will review challenges that arise in experimental techniques and reporting procedures in deep RL. I will also describe several recent results and guidelines designed to make future results more reproducible, reusable and robust.

Coffee Break

Break | Wed Dec 5th 09:20 -- 09:45 AM @

A Smoothed Analysis of the Greedy Algorithm for the Linear Contextual Bandit Problem

Spotlight | Wed Dec 5th 09:45 -- 09:50 AM @ Room 220 CD

Sampath Kannan · Jamie Morgenstern · Aaron Roth · Bo Waggoner · Zhiwei Steven Wu

Bandit learning is characterized by the tension between long-term exploration and short-term exploitation. However, as has recently been noted, in settings in which the choices of the learning algorithm correspond to important decisions about individual people (such as criminal recidivism prediction, lending, and sequential drug trials), exploration corresponds to explicitly sacrificing the well-being of one individual for the potential future benefit of others. In such settings, one might like to run a greedy'' algorithm, which always makes the optimal decision for the individuals at hand --- but doing this can result in a catastrophic failure to learn. In this paper, we consider the linear contextual bandit problem and revisit the performance of the greedy algorithm. We give a smoothed analysis, showing that even when contexts may be chosen by an adversary, small perturbations of the adversary's choices suffice for the algorithm to achieve no regret'', perhaps (depending on the specifics of the setting) with a constant amount of initial training data. This suggests that in slightly perturbed environments, exploration and exploitation need not be in conflict in the linear setting.

Deep Network for the Integrated 3D Sensing of Multiple People in Natural Images

Spotlight | Wed Dec 5th 09:45 -- 09:50 AM @ Room 220 E

Andrei Zanfir · Elisabeta Marinoiu · Mihai Zanfir · Alin-Ionut Popa · Cristian Sminchisescu

We present MubyNet -- a feed-forward, multitask, bottom up system for the integrated localization, as well as 3d pose and shape estimation, of multiple people in monocular images. The challenge is the formal modeling of the problem that intrinsically requires discrete and continuous computation, e.g. grouping people vs. predicting 3d pose. The model identifies human body structures (joints and limbs) in images, groups them based on 2d and 3d information fused using learned scoring functions, and optimally aggregates such responses into partial or complete 3d human skeleton hypotheses under kinematic tree constraints, but without knowing in advance the number of people in the scene and their visibility relations. We design a multi-task deep neural network with differentiable stages where the person grouping problem is formulated as an integer program based on learned body part scores parameterized by both 2d and 3d information. This avoids suboptimality resulting from separate 2d and 3d reasoning, with grouping performed based on the combined representation. The final stage of 3d pose and shape prediction is based on a learned attention process where information from different human body parts is optimally integrated. State-of-the-art results are obtained in large scale datasets like Human3.6M and Panoptic, and qualitatively by reconstructing the 3d shape and pose of multiple people, under occlusion, in difficult monocular images.

Revisiting (ϵ, γ, τ) -similarity learning for domain adaptation

Spotlight | Wed Dec 5th 09:45 -- 09:50 AM @ Room 517 CD

Sofiane Dhouib · Ievgen Redko

Similarity learning is an active research area in machine learning that tackles the problem of finding a similarity function tailored to an observable data sample in order to achieve efficient classification. This learning scenario has been generally formalized by the means of a (ϵ, γ, τ) -good similarity learning framework in the context of supervised classification and has been shown to have strong theoretical guarantees. In this paper, we propose to extend the theoretical analysis of similarity learning to the domain adaptation setting, a particular situation occurring when the similarity is learned and then deployed on samples following different probability distributions. We give a new definition of an (ϵ, γ) -good similarity for domain adaptation and prove several results quantifying the performance of a similarity function on a target domain after it has

been trained on a source domain. We particularly show that if the source distribution dominates the target one, then principally new domain adaptation learning bounds can be proved.

Almost Optimal Algorithms for Linear Stochastic Bandits with Heavy-Tailed Payoffs

Spotlight | Wed Dec 5th 09:50 -- 09:55 AM @ Room 220 CD

Han Shao · Xiaotian Yu · Irwin King · Michael Lyu

In linear stochastic bandits, it is commonly assumed that payoffs are with sub-Gaussian noises. In this paper, under a weaker assumption on noises, we study the problem of linear stochastic bandits with heavy-tailed payoffs (LinBET), where the distributions have finite moments of order $1+\epsilon$, for some $\epsilon \in (0,1]$. We rigorously analyze the regret lower bound of LinBET as $\Omega(T^{\frac{1}{1+\epsilon}})$, implying that finite moments of order 2 (i.e., finite variances) yield the bound of $\Omega(\sqrt{T})$, with T being the total number of rounds to play bandits. The provided lower bound also indicates that the state-of-the-art algorithms for LinBET are far from optimal. By adopting median of means with a well-designed allocation of decisions and truncation based on historical information, we develop two novel bandit algorithms, where the regret upper bounds match the lower bound up to polylogarithmic factors. To the best of our knowledge, we are the first to solve LinBET optimally in the sense of the polynomial order on T . Our proposed algorithms are evaluated based on synthetic datasets, and outperform the state-of-the-art results.

Delta-encoder: an effective sample synthesis method for few-shot object recognition

Spotlight | Wed Dec 5th 09:50 -- 09:55 AM @ Room 220 E

Eli Schwartz · Leonid Karlinsky · Joseph Shtok · Sivan Harary · Mattias Marder · Abhishek Kumar · Rogerio Feris · Raja Giryes · Alex Bronstein

Learning to classify new categories based on just one or a few examples is a long-standing challenge in modern computer vision. In this work, we propose a simple yet effective method for few-shot (and one-shot) object recognition. Our approach is based on a modified auto-encoder, denoted delta-encoder, that learns to synthesize new samples for an unseen category just by seeing few examples from it. The synthesized samples are then used to train a classifier. The proposed approach learns to both extract transferable intra-class deformations, or "deltas", between same-class pairs of training examples, and to apply those deltas to the few provided examples of a novel class (unseen during training) in order to efficiently synthesize samples from that new class. The proposed method improves the state-of-the-art of one-shot object-recognition and performs comparably in the few-shot

case.

Leveraged volume sampling for linear regression

Spotlight | Wed Dec 5th 09:50 -- 09:55 AM @ Room 517 CD

Michal Derezhinski · Manfred Warmuth · Daniel Hsu

Suppose an $n \times d$ design matrix in a linear regression problem is given, but the response for each point is hidden unless explicitly requested. The goal is to sample only a small number $k \ll n$ of the responses, and then produce a weight vector whose sum of squares loss over all points is at most $1 + \epsilon$ times the minimum. When k is very small (e.g., $k=d$), jointly sampling diverse subsets of points is crucial. One such method called "volume sampling" has a unique and desirable property that the weight vector it produces is an unbiased estimate of the optimum. It is therefore natural to ask if this method offers the optimal unbiased estimate in terms of the number of responses k needed to achieve a $1 + \epsilon$ loss approximation. Surprisingly we show that volume sampling can have poor behavior when we require a very accurate approximation -- indeed worse than some i.i.d. sampling techniques whose estimates are biased, such as leverage score sampling. We then develop a new rescaled variant of volume sampling that produces an unbiased estimate which avoids this bad behavior and has at least as good a tail bound as leverage score sampling: sample size $k = O(d \log d + d/\epsilon)$ suffices to guarantee total loss at most $1 + \epsilon$ times the minimum with high probability. Thus, we improve on the best previously known sample size for an unbiased estimator, $k = O(d^2/\epsilon)$. Our rescaling procedure leads to a new efficient algorithm for volume sampling which is based on a "determinantal rejection sampling" technique with potentially broader applications to determinantal point processes. Other contributions include introducing the combinatorics needed for rescaled volume sampling and developing tail bounds for sums of dependent random matrices which arise in the process.

End-to-End Differentiable Physics for Learning and Control

Spotlight | Wed Dec 5th 09:55 -- 10:00 AM @ Room 220 CD

Filipe de Avila Belbute-Peres · Kevin Smith · Kelsey Allen · Josh Tenenbaum · J. Zico Kolter

We present a differentiable physics engine that can be integrated as a module in deep neural networks for end-to-end learning. As a result, structured physics knowledge can be embedded into larger systems, allowing them, for example, to match observations by performing precise simulations, while achieves high sample efficiency. Specifically, in this paper we demonstrate how to perform backpropagation analytically through a physical simulator defined via a linear complementarity problem. Unlike traditional finite difference methods, such gradients can be computed analytically, which allows for greater flexibility of the engine. Through experiments in

diverse domains, we highlight the system's ability to learn physical parameters from data, efficiently match and simulate observed visual behavior, and readily enable control via gradient-based planning methods. Code for the engine and experiments is included with the paper.

Text-Adaptive Generative Adversarial Networks: Manipulating Images with Natural Language

Spotlight | Wed Dec 5th 09:55 -- 10:00 AM @ Room 220 E

Seonghyeon Nam · Yunji Kim · Seon Joo Kim

This paper addresses the problem of manipulating images using natural language description. Our task aims to semantically modify visual attributes of an object in an image according to the text describing the new visual appearance. Although existing methods synthesize images having new attributes, they do not fully preserve text-irrelevant contents of the original image. In this paper, we propose the text-adaptive generative adversarial network (TAGAN) to generate semantically manipulated images while preserving text-irrelevant contents. The key to our method is the text-adaptive discriminator that creates word level local discriminators according to input text to classify fine-grained attributes independently. With this discriminator, the generator learns to generate images where only regions that correspond to the given text is modified. Experimental results show that our method outperforms existing methods on CUB and Oxford-102 datasets, and our results were mostly preferred on a user study. Extensive analysis shows that our method is able to effectively disentangle visual attributes and produce pleasing outputs.

Synthesize Policies for Transfer and Adaptation across Tasks and Environments

Spotlight | Wed Dec 5th 09:55 -- 10:00 AM @ Room 517 CD

Hexiang Hu · Liyu Chen · Boqing Gong · Fei Sha

The ability to transfer in reinforcement learning is key towards building an agent of general artificial intelligence. In this paper, we consider the problem of learning to simultaneously transfer across both environments and tasks, probably more importantly, by learning from only sparse (environment, task) pairs out of all the possible combinations. We propose a novel compositional neural network architecture which depicts a meta rule for composing policies from environment and task embeddings. Notably, one of the main challenges is to learn the embeddings jointly with the meta rule. We further propose new training methods to disentangle the embeddings, making them both distinctive signatures of the environments and tasks and effective building blocks for composing the policies. Experiments on GridWorld and THOR, of which the agent takes as input an egocentric view, show that our approach gives rise to high success rates on all the (environment,

task) pairs after learning from only 40% of them.

Near Optimal Exploration-Exploitation in Non-Communicating Markov Decision Processes

Spotlight | Wed Dec 5th 10:00 -- 10:05 AM @ Room 220 CD

Ronan Fruit · Matteo Pirotta · Alessandro Lazaric

While designing the state space of an MDP, it is common to include states that are transient or not reachable by any policy (e.g., in mountain car, the product space of speed and position contains configurations that are not physically reachable). This results in weakly-communicating or multi-chain MDPs. In this paper, we introduce TUCRL, the first algorithm able to perform efficient exploration-exploitation in any finite Markov Decision Process (MDP) without requiring any form of prior knowledge. In particular, for any MDP with S^c communicating states, A actions and $|\Gamma^c| \leq S^c$ possible communicating next states, we derive a $O(D^c \sqrt{|\Gamma^c| S^c A T})$ regret bound, where D^c is the diameter (i.e., the length of the longest shortest path between any two states) of the communicating part of the MDP. This is in contrast with optimistic algorithms (e.g., UCRL, Optimistic PSRL) that suffer linear regret in weakly-communicating MDPs, as well as posterior sampling or regularised algorithms (e.g., REGAL), which require prior knowledge on the bias span of the optimal policy to bias the exploration to achieve sub-linear regret. We also prove that in weakly-communicating MDPs, no algorithm can ever achieve a logarithmic growth of the regret without first suffering a linear regret for a number of steps that is exponential in the parameters of the MDP. Finally, we report numerical simulations supporting our theoretical findings and showing how TUCRL overcomes the limitations of the state-of-the-art.

Neighbourhood Consensus Networks

Spotlight | Wed Dec 5th 10:00 -- 10:05 AM @ Room 220 E

Ignacio Rocco · Mircea Cimpoi · Relja Arandjelović · Akihiko Torii · Tomas Pajdla · Josef Sivic

We address the problem of finding reliable dense correspondences between a pair of images. This is a challenging task due to strong appearance differences between the corresponding scene elements and ambiguities generated by repetitive patterns. The contributions of this work are threefold. First, inspired by the classic idea of disambiguating feature matches using semi-local constraints, we develop an end-to-end trainable convolutional neural network architecture that identifies sets of spatially consistent matches by analyzing neighbourhood consensus patterns in the 4D space of all possible correspondences between a pair of images without the need for a global geometric model. Second, we demonstrate that the model can be trained effectively from weak supervision in the form of matching and non-matching image pairs without the need for costly manual annotation of point to

point correspondences. Third, we show the proposed neighbourhood consensus network can be applied to a range of matching tasks including both category- and instance-level matching, obtaining the state-of-the-art results on the PF Pascal dataset and the InLoc indoor visual localization benchmark.

Sublinear Time Low-Rank Approximation of Distance Matrices

Spotlight | Wed Dec 5th 10:00 -- 10:05 AM @ Room 517 CD

Ainesh Bakshi · David Woodruff

Let $P = \{p_1, p_2, \dots, p_n\}$ and $Q = \{q_1, q_2, \dots, q_m\}$ be two point sets in an arbitrary metric space. Let A represent the $m \times n$ pairwise distance matrix with $A_{i,j} = d(p_i, q_j)$. Such distance matrices are commonly computed in software packages and have applications to learning image manifolds, handwriting recognition, and multi-dimensional unfolding, among other things. In an attempt to reduce their description size, we study low rank approximation of such matrices. Our main result is to show that for any underlying distance metric d , it is possible to achieve an additive error low rank approximation in sublinear time. We note that it is provably impossible to achieve such a guarantee in sublinear time for arbitrary matrices A , and our proof exploits special properties of distance matrices. We develop a recursive algorithm based on additive projection-cost preserving sampling. We then show that in general, relative error approximation in sublinear time is impossible for distance matrices, even if one allows for bicriteria solutions. Additionally, we show that if $P = Q$ and d is the squared Euclidean distance, which is not a metric but rather the square of a metric, then a relative error bicriteria solution can be found in sublinear time. Finally, we empirically compare our algorithm with the SVD and input sparsity time algorithms. Our algorithm is several hundred times faster than the SVD, and about $8\$-20\$$ times faster than input sparsity methods on real-world and synthetic datasets of size 10^8 . Accuracy-wise, our algorithm is only slightly worse than that of the SVD (optimal) and input-sparsity time algorithms.

Exploration in Structured Reinforcement Learning

Oral | Wed Dec 5th 10:05 -- 10:20 AM @ Room 220 CD

Jungseul Ok · Alexandre Proutiere · Damianos Tranos

We address reinforcement learning problems with finite state and action spaces where the underlying MDP has some known structure that could be potentially exploited to minimize the exploration rates of suboptimal (state, action) pairs. For any arbitrary structure, we derive problem-specific regret lower bounds satisfied by any learning algorithm. These lower bounds are made

explicit for unstructured MDPs and for those whose transition probabilities and average reward functions are Lipschitz continuous w.r.t. the state and action. For Lipschitz MDPs, the bounds are shown not to scale with the sizes S and A of the state and action spaces, i.e., they are smaller than $c \log T$ where T is the time horizon and the constant c only depends on the Lipschitz structure, the span of the bias function, and the minimal action sub-optimality gap. This contrasts with unstructured MDPs where the regret lower bound typically scales as $SA \log T$. We devise DEL (Directed Exploration Learning), an algorithm that matches our regret lower bounds. We further simplify the algorithm for Lipschitz MDPs, and show that the simplified version is still able to efficiently exploit the structure.

Visual Memory for Robust Path Following

Oral | Wed Dec 5th 10:05 -- 10:20 AM @ Room 220 E

Ashish Kumar · Saurabh Gupta · David Fouhey · Sergey Levine · Jitendra Malik

Humans routinely retrace a path in a novel environment both forwards and backwards despite uncertainty in their motion. In this paper, we present an approach for doing so. Given a demonstration of a path, a first network generates an abstraction of the path. Equipped with this abstraction, a second network then observes the world and decides how to act in order to retrace the path under noisy actuation and a changing environment. The two networks are optimized end-to-end at training time. We evaluate the method in two realistic simulators, performing path following both forwards and backwards. Our experiments show that our approach outperforms both a classical approach to solving this task as well as a number of other baselines.

Nearly tight sample complexity bounds for learning mixtures of Gaussians via sample compression schemes

Oral | Wed Dec 5th 10:05 -- 10:20 AM @ Room 517 CD

Hassan Ashtiani · Shai Ben-David · Nick Harvey · Christopher Liaw · Abbas Mehrabian · Yaniv Plan

We prove that $\Theta(k d^2 / \epsilon^2)$ samples are necessary and sufficient for learning a mixture of k Gaussians in \mathbb{R}^d , up to error ϵ in total variation distance. This improves both the known upper bounds and lower bounds for this problem. For mixtures of axis-aligned Gaussians, we show that $O(k d / \epsilon^2)$ samples suffice, matching a known lower bound. The upper bound is based on a novel technique for distribution learning based on a notion of sample compression. Any class of distributions that allows such a sample compression scheme can also be learned with few samples. Moreover, if a class of distributions has such a compression scheme, then so do the classes of products and mixtures of those distributions. The core of our main result is showing that the class of Gaussians in \mathbb{R}^d has an efficient sample compression.

Acceleration through Optimistic No-Regret Dynamics

Spotlight | Wed Dec 5th 10:20 -- 10:25 AM @ Room 220 CD

Jun-Kun Wang · Jacob Abernethy

We consider the problem of minimizing a smooth convex function by reducing the optimization to computing the Nash equilibrium of a particular zero-sum convex-concave game. Zero-sum games can be solved using online learning dynamics, where a classical technique involves simulating two no-regret algorithms that play against each other and, after T rounds, the average iterate is guaranteed to solve the original optimization problem with error decaying as $O(\log T/T)$. In this paper we show that the technique can be enhanced to a rate of $O(1/T^2)$ by extending recent work \cite{RS13,SALS15} that leverages \textit{optimistic learning} to speed up equilibrium computation. The resulting optimization algorithm derived from this analysis coincides \textit{exactly} with the well-known \texttt{NA} \cite{N83a} method, and indeed the same story allows us to recover several variants of the Nesterov's algorithm via small tweaks. We are also able to establish the accelerated linear rate for a function which is both strongly-convex and smooth. This methodology unifies a number of different iterative optimization methods: we show that the \texttt{HB} algorithm is precisely the non-optimistic variant of \texttt{NA}, and recent prior work already established a similar perspective on \texttt{FW} \cite{AW17,ALLW18}.

Recurrent Transformer Networks for Semantic Correspondence

Spotlight | Wed Dec 5th 10:20 -- 10:25 AM @ Room 220 E

Seungryong Kim · Stephen Lin · SANG RYUL JEON · Dongbo Min · Kwanghoon Sohn

We present recurrent transformer networks (RTNs) for obtaining dense correspondences between semantically similar images. Our networks accomplish this through an iterative process of estimating spatial transformations between the input images and using these transformations to generate aligned convolutional activations. By directly estimating the transformations between an image pair, rather than employing spatial transformer networks to independently normalize each individual image, we show that greater accuracy can be achieved. This process is conducted in a recursive manner to refine both the transformation estimates and the feature representations. In addition, a technique is presented for weakly-supervised training of RTNs that is based on a proposed classification loss. With RTNs, state-of-the-art performance is attained on several benchmarks for semantic correspondence.

Minimax Statistical Learning with Wasserstein distances

Spotlight | Wed Dec 5th 10:20 -- 10:25 AM @ Room 517 CD

Jaeho Lee · Maxim Raginsky

As opposed to standard empirical risk minimization (ERM), distributionally robust optimization aims to minimize the worst-case risk over a larger ambiguity set containing the original empirical distribution of the training data. In this work, we describe a minimax framework for statistical learning with ambiguity sets given by balls in Wasserstein space. In particular, we prove generalization bounds that involve the covering number properties of the original ERM problem. As an illustrative example, we provide generalization guarantees for transport-based domain adaptation problems where the Wasserstein distance between the source and target domain distributions can be reliably estimated from unlabeled samples.

On Oracle-Efficient PAC RL with Rich Observations

Spotlight | Wed Dec 5th 10:25 -- 10:30 AM @ Room 220 CD

Christoph Dann · Nan Jiang · Akshay Krishnamurthy · Alekh Agarwal · John Langford · Robert Schapire

We study the computational tractability of PAC reinforcement learning with rich observations. We present new provably sample-efficient algorithms for environments with deterministic hidden state dynamics and stochastic rich observations. These methods operate in an oracle model of computation -- accessing policy and value function classes exclusively through standard optimization primitives -- and therefore represent computationally efficient alternatives to prior algorithms that require enumeration. With stochastic hidden state dynamics, we prove that the only known sample-efficient algorithm, OLIVE, cannot be implemented in the oracle model. We also present several examples that illustrate fundamental challenges of tractable PAC reinforcement learning in such general settings.

Sequential Attend, Infer, Repeat: Generative Modelling of Moving Objects

Spotlight | Wed Dec 5th 10:25 -- 10:30 AM @ Room 220 E

Adam Kosiorrek · Hyunjik Kim · Yee Whye Teh · Ingmar Posner

We present Sequential Attend, Infer, Repeat (SQAIR), an interpretable deep generative model for image sequences. It can reliably discover and track objects through the sequence; it can also

conditionally generate future frames, thereby simulating expected motion of objects. This is achieved by explicitly encoding object numbers, locations and appearances in the latent variables of the model. SQAIR retains all strengths of its predecessor, Attend, Infer, Repeat (AIR, Eslami et. al. 2016), including unsupervised learning, made possible by inductive biases present in the model structure. We use a moving multi-\textsc{mnist} dataset to show limitations of AIR in detecting overlapping or partially occluded objects, and show how \textsc{sqair} overcomes them by leveraging temporal consistency of objects. Finally, we also apply SQAIR to real-world pedestrian CCTV data, where it learns to reliably detect, track and generate walking pedestrians with no supervision.

Generalization Bounds for Uniformly Stable Algorithms

Spotlight | Wed Dec 5th 10:25 -- 10:30 AM @ Room 517 CD

Vitaly Feldman · Jan Vondrak

Uniform stability of a learning algorithm is a classical notion of algorithmic stability introduced to derive high-probability bounds on the generalization error (Bousquet and Elisseeff, 2002). Specifically, for a loss function with range bounded in $[0,1]$, the generalization error of γ -uniformly stable learning algorithm on n samples is known to be at most $O((\gamma + 1/n) \sqrt{n \log(1/\delta)})$ with probability at least $1-\delta$. Unfortunately, this bound does not lead to meaningful generalization bounds in many common settings where $\gamma \geq 1/\sqrt{n}$. At the same time the bound is known to be tight only when $\gamma = O(1/n)$. Here we prove substantially stronger generalization bounds for uniformly stable algorithms without any additional assumptions. First, we show that the generalization error in this setting is at most $O(\sqrt{(\gamma + 1/n) \log(1/\delta)})$ with probability at least $1-\delta$. In addition, we prove a tight bound of $O(\gamma^2 + 1/n)$ on the second moment of the generalization error. The best previous bound on the second moment of the generalization error is $O(\gamma + 1/n)$. Our proofs are based on new analysis techniques and our results imply substantially stronger generalization guarantees for several well-studied algorithms.

Constant Regret, Generalized Mixability, and Mirror Descent

Spotlight | Wed Dec 5th 10:30 -- 10:35 AM @ Room 220 CD

Zakaria Mhammedi · Robert Williamson

We consider the setting of prediction with expert advice; a learner makes predictions by aggregating those of a group of experts. Under this setting, and for the right choice of loss function and "mixing" algorithm, it is possible for the learner to achieve a constant regret regardless of the number of prediction rounds. For example, a constant regret can be achieved for *mixable*

losses using the *aggregating algorithm*. The *Generalized Aggregating Algorithm* (GAA) is a name for a family of algorithms parameterized by convex functions on simplices (entropies), which reduce to the aggregating algorithm when using the *Shannon entropy* S . For a given entropy Φ , losses for which a constant regret is possible using the GAA are called Φ -mixable. Which losses are Φ -mixable was previously left as an open question. We fully characterize Φ -mixability and answer other open questions posed by [Reid2015](#). We show that the Shannon entropy S is fundamental in nature when it comes to mixability; any Φ -mixable loss is necessarily S -mixable, and the lowest worst-case regret of the GAA is achieved using the Shannon entropy. Finally, by leveraging the connection between the *mirror descent algorithm* and the update step of the GAA, we suggest a new *adaptive* generalized aggregating algorithm and analyze its performance in terms of the regret bound.

Sanity Checks for Saliency Maps

Spotlight | Wed Dec 5th 10:30 -- 10:35 AM @ Room 220 E

Julius Adebayo · Justin Gilmer · Michael Muelly · Ian Goodfellow · Moritz Hardt · Been Kim

Saliency methods have emerged as a popular tool to highlight features in an input deemed relevant for the prediction of a learned model. Several saliency methods have been proposed, often guided by visual appeal on image data. In this work, we propose an actionable methodology to evaluate what kinds of explanations a given method can and cannot provide. We find that reliance, solely, on visual assessment can be misleading. Through extensive experiments we show that some existing saliency methods are independent both of the model and of the data generating process. Consequently, methods that fail the proposed tests are inadequate for tasks that are sensitive to either data or model, such as, finding outliers in the data, explaining the relationship between inputs and outputs that the model learned, and debugging the model. We interpret our findings through an analogy with edge detection in images, a technique that requires neither training data nor model. Theory in the case of a linear model and a single-layer convolutional neural network supports our experimental findings.

A loss framework for calibrated anomaly detection

Spotlight | Wed Dec 5th 10:30 -- 10:35 AM @ Room 517 CD

Aditya Menon · Robert Williamson

Given samples from a probability distribution, anomaly detection is the problem of determining if a given point lies in a low-density region. This paper concerns calibrated anomaly detection, which is the practically relevant extension where we additionally wish to produce a confidence score for a

point being anomalous. Building on a classification framework for anomaly detection, we show how minimisation of a suitably modified proper loss produces density estimates only for anomalous instances. We then show how to incorporate quantile control by relating our objective to a generalised version of the pinball loss. Finally, we show how to efficiently optimise the objective with kernelised scorer, by leveraging a recent result from the point process literature. The resulting objective captures a close relative of the one-class SVM as a special case.

Efficient Online Portfolio with Logarithmic Regret

Spotlight | Wed Dec 5th 10:35 -- 10:40 AM @ Room 220 CD

Haipeng Luo · Chen-Yu Wei · Kai Zheng

We study the decades-old problem of online portfolio management and propose the first algorithm with logarithmic regret that is not based on Cover's Universal Portfolio algorithm and admits much faster implementation. Specifically Universal Portfolio enjoys optimal regret $\mathcal{O}(N \ln T)$ for N financial instruments over T rounds, but requires log-concave sampling and has a large polynomial running time. Our algorithm, on the other hand, ensures a slightly larger but still logarithmic regret of $\mathcal{O}(N^2 (\ln T)^4)$, and is based on the well-studied Online Mirror Descent framework with a novel regularizer that can be implemented via standard optimization methods in time $\mathcal{O}(TN^{2.5})$ per round. The regret of all other existing works is either polynomial in T or has a potentially unbounded factor such as the inverse of the smallest price relative.

A Probabilistic U-Net for Segmentation of Ambiguous Images

Spotlight | Wed Dec 5th 10:35 -- 10:40 AM @ Room 220 E

Simon Kohl · Bernardino Romera-Paredes · Clemens Meyer · Jeffrey De Fauw · Joseph R. Ledsam · Klaus Maier-Hein · S. M. Ali Eslami · Danilo Jimenez Rezende · Olaf Ronneberger

Many real-world vision problems suffer from inherent ambiguities. In clinical applications for example, it might not be clear from a CT scan alone which particular region is cancer tissue. Therefore a group of graders typically produces a set of diverse but plausible segmentations. We consider the task of learning a distribution over segmentations given an input. To this end we propose a generative segmentation model based on a combination of a U-Net with a conditional variational autoencoder that is capable of efficiently producing an unlimited number of plausible hypotheses. We show on a lung abnormalities segmentation task and on a Cityscapes segmentation task that our model reproduces the possible segmentation variants as well as the frequencies with which they occur, doing so significantly better than published approaches. These models could have

a high impact in real-world applications, such as being used as clinical decision-making algorithms accounting for multiple plausible semantic segmentation hypotheses to provide possible diagnoses and recommend further actions to resolve the present ambiguities.

Sharp Bounds for Generalized Uniformity Testing

Spotlight | Wed Dec 5th 10:35 -- 10:40 AM @ Room 517 CD

Ilias Diakonikolas · Daniel M. Kane · Alistair Stewart

We study the problem of generalized uniformity testing of a discrete probability distribution: Given samples from a probability distribution p over an unknown size discrete domain Ω , we want to distinguish, with probability at least $2/3$, between the case that p is uniform on some subset of Ω versus ϵ -far, in total variation distance, from any such uniform distribution. We establish tight bounds on the sample complexity of generalized uniformity testing. In more detail, we present a computationally efficient tester whose sample complexity is optimal, within constant factors, and a matching worst-case information-theoretic lower bound. Specifically, we show that the sample complexity of generalized uniformity testing is $\Theta(1/(\epsilon^{4/3} \|p\|_3) + 1/(\epsilon^2 \|p\|_2))$.

Solving Large Sequential Games with the Excessive Gap Technique

Spotlight | Wed Dec 5th 10:40 -- 10:45 AM @ Room 220 CD

Christian Kroer · Gabriele Farina · Tuomas Sandholm

There has been tremendous recent progress on equilibrium-finding algorithms for zero-sum imperfect-information extensive-form games, but there has been a puzzling gap between theory and practice. *\emph{First-order methods}* have significantly better theoretical convergence rates than any *\emph{counterfactual-regret minimization (CFR)}* variant. Despite this, CFR variants have been favored in practice. Experiments with first-order methods have only been conducted on small- and medium-sized games because those methods are complicated to implement in this setting, and because CFR variants have been enhanced extensively for over a decade they perform well in practice. In this paper we show that a particular first-order method, a state-of-the-art variant of the *\emph{excessive gap technique}*---instantiated with the *\emph{dilated entropy distance function}*---can efficiently solve large real-world problems competitively with CFR and its variants. We show this on large endgames encountered by the *\emph{Libratus}* poker AI, which recently beat top human poker specialist professionals at no-limit Texas hold'em. We show experimental results on our variant of the excessive gap technique as well as a prior version. We introduce a numerically friendly implementation of the smoothed best response computation associated with first-order methods for extensive-form game solving. We present, to our knowledge, the first GPU implementation of a first-

order method for extensive-form games. We present comparisons of several excessive gap technique and CFR variants.

Virtual Class Enhanced Discriminative Embedding Learning

Spotlight | Wed Dec 5th 10:40 -- 10:45 AM @ Room 220 E

Binghui Chen · Weihong Deng · Haifeng Shen

Recently, learning discriminative features to improve the recognition performances gradually becomes the primary goal of deep learning, and numerous remarkable works have emerged. In this paper, we propose a novel yet extremely simple method Virtual Softmax to enhance the discriminative property of learned features by injecting a dynamic virtual negative class into the original softmax. Injecting virtual class aims to enlarge inter-class margin and compress intra-class distribution by strengthening the decision boundary constraint. Although it seems weird to optimize with this additional virtual class, we show that our method derives from an intuitive and clear motivation, and it indeed encourages the features to be more compact and separable. This paper empirically and experimentally demonstrates the superiority of Virtual Softmax, improving the performances on a variety of object classification and face verification tasks.

Convex Elicitation of Continuous Properties

Spotlight | Wed Dec 5th 10:40 -- 10:45 AM @ Room 517 CD

Jessica Finocchiaro · Rafael Frongillo

A property or statistic of a distribution is said to be elicitable if it can be expressed as the minimizer of some loss function in expectation. Recent work shows that continuous real-valued properties are elicitable if and only if they are identifiable, meaning the set of distributions with the same property value can be described by linear constraints. From a practical standpoint, one may ask for which such properties do there exist convex loss functions. In this paper, in a finite-outcome setting, we show that in fact every elicitable real-valued property can be elicited by a convex loss function. Our proof is constructive, and leads to convex loss functions for new properties.

Perception, sensing, motion planning and robot control using AI for automated feeding of upper-extremity mobility impaired people

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D2

A Cooperative Visually Grounded Dialogue Game with a Humanoid Robot

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D9

Jordan Prince Tremblay · Ismael Balafrej · Felix Labelle · Félix Martel-Denis · Eric Matte · Julien Chouinard-Beaupré · Adam Letourneau · Antoine Mercier-Nicol · Simon Brodeur · François Ferland · Jean ROUAT

This demonstration illustrates how research results in grounded language learning and understanding can be used in a cooperative task between an intelligent agent and a human. The task, undertaken by a robot, is the question answering game GuessWhat?! [1][2] Providing human-robot interactions in the real world requires interfacing GuessWhat?! with: speech recognition and synthesis modules; video processing and recognition algorithms; the robot's control module. One main challenge is adapting GuessWhat?! to work with images outside of MSCOCO's domain. This required implementing a pipeline in ROS which takes images from a Kinect, ensures image quality with blur detection, extracts VGG-16 feature vectors, segments objects using Mask R-CNN, and extracts position information from the segmented objects. Images from the pipeline are used by GuessWhat?! in tandem with utterances from the player. Snips voice assistant recognizes whether the player says "Yes", "No" or "Not Applicable". Snips also provides speech synthesis, converting questions generated by GuessWhat?! into speech for the player. To identify potential players, OpenPose allows IRL-1 to interact with them throughout the game. Our open source code could be useful as intelligent agents are becoming commonplace and the ability to communicate with people in a given context, such as the home or workplace, becomes imperative. The various functionalities implemented on IRL-1 [3], would be beneficial to any agent assisting a person in a cooperative task. [1] <https://www.guesswhat.ai> [2] <https://iglu-chistera.github.io> [3] <http://humanrobotinteraction.org/journal/index.php/HRI/article/view/65>

BigBlueBot: A Demonstration of How to Detect Egregious Conversations with Chatbots

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D1

Casey Dugan · Justin D Weisz · Narendra Nath Joshi · Ingrid Lange · J Johnson · Mohit Jain · Werner Geyer

Play Imperfect Information Games against Neural Networks

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D3

Andy C Kitchen · Michela Benedetti · Hon Weng Chong

In this demonstration, attendees can try their skill (and their luck) against deep neural networks at Poker and other assorted imperfect information games. The deep neural network opponents are trained with cutting edge reinforcement learning algorithms to play near a Nash equilibrium. The neural network's value function e.g. how much the neural network expects to win, is visualised as you play — giving a live running estimate of how the neural network assigns value to changing game situations. We visualise internal activity and the NN's best prediction for the human players hidden information, given their past actions. (e.g. what cards are most likely to be in your hand, given your bets? What's the predicted probability you are bluffing?)

PatentAI: IP Infringement Detection with Enhanced Paraphrase Identification

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D5

Youssef Drissi

The PatentAI technology uses custom natural language processing and machine learning to detect Intellectual Property (IP) infringement. Our experiments and demonstrations shows a significant improvement in the performance of the system by using a custom natural language pre-processing step that converts the patent (legal) language into simple English (which is a desirable function by itself), simplifies the text to capture its essence, and transforms it into a concise graph representation. After this critical pre-processing step, we use a learning model trained on a Paraphrase Identification dataset to detect if two given patent excerpts paraphrase each other, and therefore, the corresponding patents infringe on each other. A key novelty of our approach lies in the techniques used in the pre-processing step to increase the performance of the learning model. In addition, we address the difficult problem of IP infringement detection by converting it to a paraphrase identification problem, and leveraging existing models and datasets. In our demonstration, the user can enter two excerpts from different patents to detect if one patent infringe on the other. The system processes the two texts and interactively shows the user the following: (a) results of converting the patent excerpts from a patent/legal language to simple English, (b) a graph representation of each text to capture the essence of the ideas conveyed in the text (c) key extracted features, and (d) the IP infringement prediction (Match or Mismatch), where the “Match” prediction means that the model predicts that one of the patents infringe on the other.

Autonomous robotic manipulation with a desktop research platform

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D8

Jonathan Long · Brandon Pereira · Max Reynolds · Rahul Rawat

The power of robots in industry is limited both by poor usability of standard programming environments and the absence of modern perception techniques from the research community. At the same time, research progress is limited both by the difficulty of installing reliable and safe robotic systems, and by a dearth of standard benchmarks allowing a fair comparison between algorithms. Symbio Robotics, Inc., a Bay Area startup, is building a suite of tools to address these needs. Symbio will demonstrate a benchmark research platform employing a high level, real time Python programming interface to perform unstructured bin picking. We expect this to be of interest both as a practical demonstration of Symbio's automation capabilities, and as an invitation to researchers to use this platform to convincingly benchmark novel algorithms. Symbio's software provides both robot agnostic, high-level motion programming in Python, a modern language favored among researchers, as well as advanced perception capabilities. In our demo, we will show the ease and simplicity of programming by modifying robot behavior live through a Jupyter notebook. We hope this demonstration will be encouraging to anyone who has struggled to setup and work with the plethora of existing esoteric robot interfaces. To showcase advanced perception, we will display real-time 3D point clouds obtained from a single robot-mounted RGB camera using Symbio's structure-from-motion software. Our software computes grasps from those point clouds and perform unstructured bin picking. We expect this to excite both users who want to employ this technology and researchers who see opportunities for further development.

Automatic Curriculum Generation Applied to Teaching Novices a Short Bach Piano Segment

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D10

Emma Brunskill · Tong Mu · Karan Goel · Jonathan Bragg

Automatic Curriculum Generation Applied to Teaching Novices a Short Bach Piano Segment.pdf

RieszNets: Accurate Real-Time 2D/3D Image Super-Resolution

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D4

Saarthak Sachdeva · Mohnish Chakravarti

Deep Reinforcement Learning for Online Order Dispatching and Driver Repositioning in Ride-sharing

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D6

Zhiwei Qin · Xiaocheng Tang · yan jiao · Chenxi Wang

In this demonstration, we will present a simulation-based human-computer interaction of deep RL in action on order dispatching and driver repositioning in ride-sharing. Specifically, we will demonstrate through several specially designed domains how we use deep RL to train agents (drivers) to have longer optimization horizon and to cooperate to achieve higher business objective values collectively.

Multi-Word Imputation and Sentence Expansion

Demonstration | Wed Dec 5th 10:45 AM -- 07:30 PM @ Room 510 ABCD #D7

Osman Ramadan · Douglas Orr · Dmitry Stratiychuk · Błażej Czapp

INTRODUCTION Word Imputation is about finding and imputing missing words. The task was first proposed by Kaggle in their Billion Word Imputation competition. The model proposed in this demo takes a more challenging task by trying to impute multiple missing words, as opposed to a single word, or add words to a complete sentence, producing a more complex one. The later is called sentence expansion. **OBJECTIVE** * Given an incomplete sentence, find the location of the missing words in the sentence and impute them * Given a complete sentence, find the location where the sentence can be improved and impute the words required to improved. **METHOD** The model is composed of an encoder-decoder network with two learning objectives. One is to find the location of the missing words solved as a binary sequence classification task, and the other is to generate the sequence of the missing words. The embedding of the end-of-sequence in the decoder is computed dynamically as a function of the hidden state of the encoder. The model also employs an RNN-based language model as a scorer in the beam search algorithm to efficiently generate linguistically correct sequences of words. **DEMO** The demo is a mobile-friendly interactive web application, where users get to type a sentence and the model will list the top N predictions for completing or expanding the sentence. To add an engagement element, there will be a fun challenge, before presenting the app, where each one of the audience come up with a sentence from poetry, quotes ..., that has missing words. These sentences will be swapped around to be completed by the audience and the model. Finally, the answers will be presented to compare the creativity of the audience vs the model.

Balanced Policy Evaluation and Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #1

Nathan Kallus

We present a new approach to the problems of evaluating and learning personalized decision policies from observational data of past contexts, decisions, and outcomes. Only the outcome of the enacted decision is available and the historical policy is unknown. These problems arise in personalized medicine using electronic health records and in internet advertising. Existing approaches use inverse propensity weighting (or, doubly robust versions) to make historical outcome (or, residual) data look like it were generated by a new policy being evaluated or learned. But this relies on a plug-in approach that rejects data points with a decision that disagrees with the new policy, leading to high variance estimates and ineffective learning. We propose a new, balance-based approach that too makes the data look like the new policy but does so directly by finding weights that optimize for balance between the weighted data and the target policy in the given, finite sample, which is equivalent to minimizing worst-case or posterior conditional mean square error. Our policy learner proceeds as a two-level optimization problem over policies and weights. We demonstrate that this approach markedly outperforms existing ones both in evaluation and learning, which is unsurprising given the wider support of balance-based weights. We establish extensive theoretical consistency guarantees and regret bounds that support this empirical success.

Exponentiated Strongly Rayleigh Distributions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #2

Zelda Mariet · Suvrit Sra · Stefanie Jegelka

Strongly Rayleigh (SR) measures are discrete probability distributions over the subsets of a ground set. They enjoy strong negative dependence properties, as a result of which they assign higher probability to subsets of diverse elements. We introduce in this paper Exponentiated Strongly Rayleigh (ESR) measures, which sharpen (or smoothen) the negative dependence property of SR measures via a single parameter (the exponent) that can intuitively understood as an inverse temperature. We develop efficient MCMC procedures for approximate sampling from ESRs, and obtain explicit mixing time bounds for two concrete instances: exponentiated versions of Determinantal Point Processes and Dual Volume Sampling. We illustrate some of the potential of ESRs, by applying them to a few machine learning tasks; empirical results confirm that beyond their theoretical appeal, ESR-based models hold significant promise for these tasks.

Parsimonious Bayesian deep networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #3

Mingyuan Zhou

Combining Bayesian nonparametrics and a forward model selection strategy, we construct parsimonious Bayesian deep networks (PBDNs) that infer capacity-regularized network architectures from the data and require neither cross-validation nor fine-tuning when training the model. One of the two essential components of a PBDN is the development of a special infinite-wide single-hidden-layer neural network, whose number of active hidden units can be inferred from the data. The other one is the construction of a greedy layer-wise learning algorithm that uses a forward model selection criterion to determine when to stop adding another hidden layer. We develop both Gibbs sampling and stochastic gradient descent based maximum a posteriori inference for PBDNs, providing state-of-the-art classification accuracy and interpretable data subtypes near the decision boundaries, while maintaining low computational complexity for out-of-sample prediction.

Stein Variational Gradient Descent as Moment Matching

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #4

Qiang Liu · Dilin Wang

Stein variational gradient descent (SVGD) is a non-parametric inference algorithm that evolves a set of particles to fit a given distribution of interest. We analyze the non-asymptotic properties of SVGD, showing that there exists a set of functions, which we call the Stein matching set, whose expectations are exactly estimated by any set of particles that satisfies the fixed point equation of SVGD. This set is the image of Stein operator applied on the feature maps of the positive definite kernel used in SVGD. Our results provide a theoretical framework for analyzing the properties of SVGD with different kernels, shedding insight into optimal kernel choice. In particular, we show that SVGD with linear kernels yields exact estimation of means and variances on Gaussian distributions, while random Fourier features enable probabilistic bounds for distributional approximation. Our results offer a refreshing view of the classical inference problem as fitting Stein's identity or solving the Stein equation, which may motivate more efficient algorithms.

Hamiltonian Variational Auto-Encoder

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #5

Anthony L Caterini · Arnaud Doucet · Dino Sejdinovic

Variational Auto-Encoders (VAE) have become very popular techniques to perform inference and

learning in latent variable models as they allow us to leverage the rich representational power of neural networks to obtain flexible approximations of the posterior of latent variables as well as tight evidence lower bounds (ELBO). Combined with stochastic variational inference, this provides a methodology scaling to large datasets. However, for this methodology to be practically efficient, it is necessary to obtain low-variance unbiased estimators of the ELBO and its gradients with respect to the parameters of interest. While the use of Markov chain Monte Carlo (MCMC) techniques such as Hamiltonian Monte Carlo (HMC) has been previously suggested to achieve this [23, 26], the proposed methods require specifying reverse kernels which have a large impact on performance. Additionally, the resulting unbiased estimator of the ELBO for most MCMC kernels is typically not amenable to the reparameterization trick. We show here how to optimally select reverse kernels in this setting and, by building upon Hamiltonian Importance Sampling (HIS) [17], we obtain a scheme that provides low-variance unbiased estimators of the ELBO and its gradients using the reparameterization trick. This allows us to develop a Hamiltonian Variational Auto-Encoder (HVAE). This method can be re-interpreted as a target-informed normalizing flow [20] which, within our context, only requires a few evaluations of the gradient of the sampled likelihood and trivial Jacobian calculations at each iteration.

Predictive Approximate Bayesian Computation via Saddle Points

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #6

Yingxiang Yang · Bo Dai · Negar Kiyavash · Niao He

Approximate Bayesian computation (ABC) is an important methodology for Bayesian inference when the likelihood function is intractable. Sampling-based ABC algorithms such as rejection- and K2-ABC are inefficient when the parameters have high dimensions, while the regression-based algorithms such as K- and DR-ABC are hard to scale. In this paper, we introduce an optimization-based ABC framework that addresses these deficiencies. Leveraging a generative model for posterior and joint distribution matching, we show that ABC can be framed as saddle point problems, whose objectives can be accessed directly with samples. We present the predictive ABC algorithm (P-ABC), and provide a probabilistically approximately correct (PAC) bound that guarantees its learning consistency. Numerical experiment shows that P-ABC outperforms both K2- and DR-ABC significantly.

Importance Weighting and Variational Inference

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #7

Justin Domke · Daniel Sheldon

Recent work used importance sampling ideas for better variational bounds on likelihoods. We clarify the applicability of these ideas to pure probabilistic inference, by showing the resulting Importance Weighted Variational Inference (IWVI) technique is an instance of augmented variational inference, thus identifying the looseness in previous work. Experiments confirm IWVI's practicality for probabilistic inference. As a second contribution, we investigate inference with elliptical distributions, which improves accuracy in low dimensions, and convergence in high dimensions.

Orthogonally Decoupled Variational Gaussian Processes

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #8

Hugh Salimbeni · Ching-An Cheng · Byron Boots · Marc Deisenroth

Gaussian processes (GPs) provide a powerful non-parametric framework for reasoning over functions. Despite appealing theory, its superlinear computational and memory complexities have presented a long-standing challenge. State-of-the-art sparse variational inference methods trade modeling accuracy against complexity. However, the complexities of these methods still scale superlinearly in the number of basis functions, implying that that sparse GP methods are able to learn from large datasets only when a small model is used. Recently, a decoupled approach was proposed that removes the unnecessary coupling between the complexities of modeling the mean and the covariance functions of a GP. It achieves a linear complexity in the number of mean parameters, so an expressive posterior mean function can be modeled. While promising, this approach suffers from optimization difficulties due to ill-conditioning and non-convexity. In this work, we propose an alternative decoupled parametrization. It adopts an orthogonal basis in the mean function to model the residues that cannot be learned by the standard coupled approach. Therefore, our method extends, rather than replaces, the coupled approach to achieve strictly better performance. This construction admits a straightforward natural gradient update rule, so the structure of the information manifold that is lost during decoupling can be leveraged to speed up learning. Empirically, our algorithm demonstrates significantly faster convergence in multiple experiments.

ATOMO: Communication-efficient Learning via Atomic Sparsification

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #9

Hongyi Wang · Scott Sievert · Shengchao Liu · Zachary Charles · Dimitris Papailiopoulos · Stephen Wright

Distributed model training suffers from communication overheads due to frequent gradient updates transmitted between compute nodes. To mitigate these overheads, several studies propose the use of

sparsified stochastic gradients. We argue that these are facets of a general sparsification method that can operate on any possible atomic decomposition. Notable examples include element-wise, singular value, and Fourier decompositions. We present ATOMO, a general framework for atomic sparsification of stochastic gradients. Given a gradient, an atomic decomposition, and a sparsity budget, ATOMO gives a random unbiased sparsification of the atoms minimizing variance. We show that recent methods such as QSGD and TernGrad are special cases of ATOMO, and that sparsifying the singular value decomposition of neural networks gradients, rather than their coordinates, can lead to significantly faster distributed training.

Sparsified SGD with Memory

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #10

Sebastian Stich · Jean-Baptiste Cordonnier · Martin Jaggi

Huge scale machine learning problems are nowadays tackled by distributed optimization algorithms, i.e. algorithms that leverage the compute power of many devices for training. The communication overhead is a key bottleneck that hinders perfect scalability. Various recent works proposed to use quantization or sparsification techniques to reduce the amount of data that needs to be communicated, for instance by only sending the most significant entries of the stochastic gradient (top-k sparsification). Whilst such schemes showed very promising performance in practice, they have eluded theoretical analysis so far. In this work we analyze Stochastic Gradient Descent (SGD) with k-sparsification or compression (for instance top-k or random-k) and show that this scheme converges at the same rate as vanilla SGD when equipped with error compensation (keeping track of accumulated errors in memory). That is, communication can be reduced by a factor of the dimension of the problem (sometimes even more) whilst still converging at the same rate. We present numerical experiments to illustrate the theoretical findings and the good scalability for distributed applications.

SEGA: Variance Reduction via Gradient Sketching

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #11

Filip Hanzely · Konstantin Mishchenko · Peter Richtarik

We propose a novel randomized first order optimization method---SEGA (SkEtched GrAdient method)---which progressively throughout its iterations builds a variance-reduced estimate of the gradient from random linear measurements (sketches) of the gradient provided at each iteration by an oracle. In each iteration, SEGA updates the current estimate of the gradient through a sketch-and-project operation using the information provided by the latest sketch, and this is subsequently used to compute an unbiased estimate of the true gradient through a random relaxation procedure.

This unbiased estimate is then used to perform a gradient step. Unlike standard subspace descent methods, such as coordinate descent, SEGA can be used for optimization problems with a non-separable proximal term. We provide a general convergence analysis and prove linear convergence for strongly convex objectives. In the special case of coordinate sketches, SEGA can be enhanced with various techniques such as importance sampling, minibatching and acceleration, and its rate is up to a small constant factor identical to the best-known rate of coordinate descent.

Non-monotone Submodular Maximization in Exponentially Fewer Iterations

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #12

Eric Balkanski · Adam Breuer · Yaron Singer

In this paper we consider parallelization for applications whose objective can be expressed as maximizing a non-monotone submodular function under a cardinality constraint. Our main result is an algorithm whose approximation is arbitrarily close to $1/2e$ in $O(\log^2 n)$ adaptive rounds, where n is the size of the ground set. This is an exponential speedup in parallel running time over any previously studied algorithm for constrained non-monotone submodular maximization. Beyond its provable guarantees, the algorithm performs well in practice. Specifically, experiments on traffic monitoring and personalized data summarization applications show that the algorithm finds solutions whose values are competitive with state-of-the-art algorithms while running in exponentially fewer parallel iterations.

Stochastic Primal-Dual Method for Empirical Risk Minimization with $O(1)$ Per-Iteration Complexity

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #13

Conghui Tan · Tong Zhang · Shiqian Ma · Ji Liu

Regularized empirical risk minimization problem with linear predictor appears frequently in machine learning. In this paper, we propose a new stochastic primal-dual method to solve this class of problems. Different from existing methods, our proposed methods only require $O(1)$ operations in each iteration. We also develop a variance-reduction variant of the algorithm that converges linearly. Numerical experiments suggest that our methods are faster than existing ones such as proximal SGD, SVRG and SAGA on high-dimensional problems.

Rest-Katyusha: Exploiting the Solution's Structure via Scheduled Restart Schemes

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #14

Junqi Tang · Mohammad Golbabaee · Francis Bach · Mike E davies

We propose a structure-adaptive variant of the state-of-the-art stochastic variance-reduced gradient algorithm Katyusha for regularized empirical risk minimization. The proposed method is able to exploit the intrinsic low-dimensional structure of the solution, such as sparsity or low rank which is enforced by a non-smooth regularization, to achieve even faster convergence rate. This provable algorithmic improvement is done by restarting the Katyusha algorithm according to restricted strong-convexity constants. We demonstrate the effectiveness of our approach via numerical experiments.

Inexact trust-region algorithms on Riemannian manifolds

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #15

HiroYuki Kasai · Bamdev Mishra

We consider an inexact variant of the popular Riemannian trust-region algorithm for structured big-data minimization problems. The proposed algorithm approximates the gradient and the Hessian in addition to the solution of a trust-region sub-problem. Addressing large-scale finite-sum problems, we specifically propose sub-sampled algorithms with a fixed bound on sub-sampled Hessian and gradient sizes, where the gradient and Hessian are computed by a random sampling technique. Numerical evaluations demonstrate that the proposed algorithms outperform state-of-the-art Riemannian deterministic and stochastic gradient algorithms across different applications.

On Markov Chain Gradient Descent

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #16

Tao Sun · Yuejiao Sun · Wotao Yin

Stochastic gradient methods are the workhorse (algorithms) of large-scale optimization problems in machine learning, signal processing, and other computational sciences and engineering. This paper studies Markov chain gradient descent, a variant of stochastic gradient descent where the random samples are taken on the trajectory of a Markov chain. Existing results of this method assume convex objectives and a reversible Markov chain and thus have their limitations. We establish new non-ergodic convergence under wider step sizes, for nonconvex problems, and for non-reversible

finite-state Markov chains. Nonconvexity makes our method applicable to broader problem classes. Non-reversible finite-state Markov chains, on the other hand, can mix substantially faster. To obtain these results, we introduce a new technique that varies the mixing levels of the Markov chains. The reported numerical results validate our contributions.

Gradient Descent Meets Shift-and-Invert Preconditioning for Eigenvector Computation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #17

Zhiqiang Xu

Shift-and-invert preconditioning, as a classic acceleration technique for the leading eigenvector computation, has received much attention again recently, owing to fast least-squares solvers for efficiently approximating matrix inversions in power iterations. In this work, we adopt an inexact Riemannian gradient descent perspective to investigate this technique on the effect of the step-size scheme. The shift-and-inverted power method is included as a special case with adaptive step-sizes. Particularly, two other step-size settings, i.e., constant step-sizes and Barzilai-Borwein (BB) step-sizes, are examined theoretically and/or empirically. We present a novel convergence analysis for the constant step-size setting that achieves a rate at $\tilde{O}(\sqrt{\frac{\lambda_1}{\lambda_1 - \lambda_{p+1}}})$, where λ_i represents the i -th largest eigenvalue of the given real symmetric matrix and p is the multiplicity of λ_1 . Our experimental studies show that the proposed algorithm can be significantly faster than the shift-and-inverted power method in practice.

Global Non-convex Optimization with Discretized Diffusions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #18

Murat A Erdogdu · Lester Mackey · Ohad Shamir

An Euler discretization of the Langevin diffusion is known to converge to the global minimizers of certain convex and non-convex optimization problems. We show that this property holds for any suitably smooth diffusion and that different diffusions are suitable for optimizing different classes of convex and non-convex functions. This allows us to design diffusions suitable for globally optimizing convex and non-convex functions not covered by the existing Langevin theory. Our non-asymptotic analysis delivers computable optimization and integration error bounds based on easily accessed properties of the objective and chosen diffusion. Central to our approach are new explicit Stein factor bounds on the solutions of Poisson equations. We complement these results with improved optimization guarantees for targets other than the standard Gibbs measure.

A theory on the absence of spurious solutions for nonconvex and nonsmooth optimization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #19

Cedric Jozs · Yi Ouyang · Richard Zhang · Javad Lavaei · Somayeh Sojoudi

We study the set of continuous functions that admit no spurious local optima (i.e. local minima that are not global minima) which we term global functions. They satisfy various powerful properties for analyzing nonconvex and nonsmooth optimization problems. For instance, they satisfy a theorem akin to the fundamental uniform limit theorem in the analysis regarding continuous functions. Global functions are also endowed with useful properties regarding the composition of functions and change of variables. Using these new results, we show that a class of non-differentiable nonconvex optimization problems arising in tensor decomposition applications are global functions. This is the first result concerning nonconvex methods for nonsmooth objective functions. Our result provides a theoretical guarantee for the widely-used ℓ_1 norm to avoid outliers in nonconvex optimization.

The Limit Points of (Optimistic) Gradient Descent in Min-Max Optimization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #20

Constantinos Daskalakis · Ioannis Panageas

Motivated by applications in Optimization, Game Theory, and the training of Generative Adversarial Networks, the convergence properties of first order methods in min-max problems have received extensive study. It has been recognized that they may cycle, and there is no good understanding of their limit points when they do not. When they converge, do they converge to local min-max solutions? We characterize the limit points of two basic first order methods, namely Gradient Descent/Ascent (GDA) and Optimistic Gradient Descent Ascent (OGDA). We show that both dynamics avoid unstable critical points for almost all initializations. Moreover, for small step sizes and under mild assumptions, the set of OGDA-stable critical points is a superset of GDA-stable critical points, which is a superset of local min-max solutions (strict in some cases). The connecting thread is that the behavior of these dynamics can be studied from a dynamical systems perspective.

Porcupine Neural Networks: Approximating Neural Network

Landscapes

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #21

Soheil Feizi · Hamid Javadi · Jesse Zhang · David Tse

Neural networks have been used prominently in several machine learning and statistics applications. In general, the underlying optimization of neural networks is non-convex which makes analyzing their performance challenging. In this paper, we take another approach to this problem by constraining the network such that the corresponding optimization landscape has good theoretical properties without significantly compromising performance. In particular, for two-layer neural networks we introduce Porcupine Neural Networks (PNNs) whose weight vectors are constrained to lie over a finite set of lines. We show that most local optima of PNN optimizations are global while we have a characterization of regions where bad local optimizers may exist. Moreover, our theoretical and empirical results suggest that an unconstrained neural network can be approximated using a polynomially-large PNN.

Adding One Neuron Can Eliminate All Bad Local Minima

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #22

SHIYU LIANG · Ruoyu Sun · Jason Lee · R. Srikant

One of the main difficulties in analyzing neural networks is the non-convexity of the loss function which may have many bad local minima. In this paper, we study the landscape of neural networks for binary classification tasks. Under mild assumptions, we prove that after adding one special neuron with a skip connection to the output, or one special neuron per layer, every local minimum is a global minimum.

Improving Explorability in Variational Inference with Annealed Variational Objectives

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #23

Chin-Wei Huang · Shawn Tan · Alexandre Lacoste · Aaron Courville

Despite the advances in the representational capacity of approximate distributions for variational inference, the optimization process can still limit the density that is ultimately learned. We demonstrate the drawbacks of biasing the true posterior to be unimodal, and introduce Annealed Variational Objectives (AVO) into the training of hierarchical variational methods. Inspired by Annealed Importance Sampling, the proposed method facilitates learning by incorporating energy

tempering into the optimization objective. In our experiments, we demonstrate our method's robustness to deterministic warm up, and the benefits of encouraging exploration in the latent space.

Sequential Attend, Infer, Repeat: Generative Modelling of Moving Objects

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #24

Adam Kosiorek · Hyunjik Kim · Yee Whye Teh · Ingmar Posner

We present Sequential Attend, Infer, Repeat (SQAIR), an interpretable deep generative model for image sequences. It can reliably discover and track objects through the sequence; it can also conditionally generate future frames, thereby simulating expected motion of objects. This is achieved by explicitly encoding object numbers, locations and appearances in the latent variables of the model. SQAIR retains all strengths of its predecessor, Attend, Infer, Repeat (AIR, Eslami et. al. 2016), including unsupervised learning, made possible by inductive biases present in the model structure. We use a moving multi-`\textsc{mnist}` dataset to show limitations of AIR in detecting overlapping or partially occluded objects, and show how `\textsc{sqair}` overcomes them by leveraging temporal consistency of objects. Finally, we also apply SQAIR to real-world pedestrian CCTV data, where it learns to reliably detect, track and generate walking pedestrians with no supervision.

Delta-encoder: an effective sample synthesis method for few-shot object recognition

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #25

Eli Schwartz · Leonid Karlinsky · Joseph Shtok · Sivan Harary · Mattias Marder · Abhishek Kumar · Rogerio Feris · Raja Giryes · Alex Bronstein

Learning to classify new categories based on just one or a few examples is a long-standing challenge in modern computer vision. In this work, we propose a simple yet effective method for few-shot (and one-shot) object recognition. Our approach is based on a modified auto-encoder, denoted delta-encoder, that learns to synthesize new samples for an unseen category just by seeing few examples from it. The synthesized samples are then used to train a classifier. The proposed approach learns to both extract transferable intra-class deformations, or "deltas", between same-class pairs of training examples, and to apply those deltas to the few provided examples of a novel class (unseen during training) in order to efficiently synthesize samples from that new class. The proposed method improves the state-of-the-art of one-shot object-recognition and performs comparably in the few-shot case.

Joint Active Feature Acquisition and Classification with Variable-Size Set Encoding

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #26

Hajin Shim · Sung Ju Hwang · Eunho Yang

We consider the problem of active feature acquisition where the goal is to sequentially select the subset of features in order to achieve the maximum prediction performance in the most cost-effective way at test time. In this work, we formulate this active feature acquisition as a jointly learning problem of training both the classifier (environment) and the RL agent that decides either to stop and predict or collect a new feature at test time, in a cost-sensitive manner. We also introduce a novel encoding scheme to represent acquired subsets of features by proposing an order-invariant set encoding at the feature level, which also significantly reduces the search space for our agent. We evaluate our model on a carefully designed synthetic dataset for the active feature acquisition as well as several medical datasets. Our framework shows meaningful feature acquisition process for diagnosis that complies with human knowledge, and outperforms all baselines in terms of prediction performance as well as feature acquisition cost.

PCA of high dimensional random walks with comparison to neural network training

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #27

Joseph Antognini · Jascha Sohl-Dickstein

One technique to visualize the training of neural networks is to perform PCA on the parameters over the course of training and to project to the subspace spanned by the first few PCA components. In this paper we compare this technique to the PCA of a high dimensional random walk. We compute the eigenvalues and eigenvectors of the covariance of the trajectory and prove that in the long trajectory and high dimensional limit most of the variance is in the first few PCA components, and that the projection of the trajectory onto any subspace spanned by PCA components is a Lissajous curve. We generalize these results to a random walk with momentum and to an Ornstein-Uhlenbeck processes (i.e., a random walk in a quadratic potential) and show that in high dimensions the walk is not mean reverting, but will instead be trapped at a fixed distance from the minimum. We finally analyze PCA projected training trajectories for: a linear model trained on CIFAR-10; a fully connected model trained on MNIST; and ResNet-50-v2 trained on Imagenet. In all cases, both the distribution of PCA eigenvalues and the projected trajectories resemble those of a random walk with drift.

Insights on representational similarity in neural networks with canonical correlation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #28

Ari Morcos · Maithra Raghu · Samy Bengio

Comparing different neural network representations and determining how representations evolve over time remain challenging open questions in our understanding of the function of neural networks. Comparing representations in neural networks is fundamentally difficult as the structure of representations varies greatly, even across groups of networks trained on identical tasks, and over the course of training. Here, we develop projection weighted CCA (Canonical Correlation Analysis) as a tool for understanding neural networks, building off of SVCCA, a recently proposed method (Raghu et al, 2017). We first improve the core method, showing how to differentiate between signal and noise, and then apply this technique to compare across a group of CNNs, demonstrating that networks which generalize converge to more similar representations than networks which memorize, that wider networks converge to more similar solutions than narrow networks, and that trained networks with identical topology but different learning rates converge to distinct clusters with diverse representations. We also investigate the representational dynamics of RNNs, across both training and sequential timesteps, finding that RNNs converge in a bottom-up pattern over the course of training and that the hidden state is highly variable over the course of a sequence, even when accounting for linear transforms. Together, these results provide new insights into the function of CNNs and RNNs, and demonstrate the utility of using CCA to understand representations.

Adversarial vulnerability for any classifier

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #29

Alhussein Fawzi · Hamza Fawzi · Omar Fawzi

Despite achieving impressive performance, state-of-the-art classifiers remain highly vulnerable to small, imperceptible, adversarial perturbations. This vulnerability has proven empirically to be very intricate to address. In this paper, we study the phenomenon of adversarial perturbations under the assumption that the data is generated with a smooth generative model. We derive fundamental upper bounds on the robustness to perturbations of any classification function, and prove the existence of adversarial perturbations that transfer well across different classifiers with small risk. Our analysis of the robustness also provides insights onto key properties of generative models, such as their smoothness and dimensionality of latent space. We conclude with numerical experimental results showing that our bounds provide informative baselines to the maximal achievable robustness on several datasets.

Sanity Checks for Saliency Maps

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #30

Julius Adebayo · Justin Gilmer · Michael Muelly · Ian Goodfellow · Moritz Hardt · Been Kim

Saliency methods have emerged as a popular tool to highlight features in an input deemed relevant for the prediction of a learned model. Several saliency methods have been proposed, often guided by visual appeal on image data. In this work, we propose an actionable methodology to evaluate what kinds of explanations a given method can and cannot provide. We find that reliance, solely, on visual assessment can be misleading. Through extensive experiments we show that some existing saliency methods are independent both of the model and of the data generating process. Consequently, methods that fail the proposed tests are inadequate for tasks that are sensitive to either data or model, such as, finding outliers in the data, explaining the relationship between inputs and outputs that the model learned, and debugging the model. We interpret our findings through an analogy with edge detection in images, a technique that requires neither training data nor model. Theory in the case of a linear model and a single-layer convolutional neural network supports our experimental findings.

MetaGAN: An Adversarial Approach to Few-Shot Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #31

Ruixiang ZHANG · Tong Che · Zoubin Ghahramani · Yoshua Bengio · Yangqiu Song

In this paper, we propose a conceptually simple and general framework called MetaGAN for few-shot learning problems. Most state-of-the-art few-shot classification models can be integrated with MetaGAN in a principled and straightforward way. By introducing an adversarial generator conditioned on tasks, we augment vanilla few-shot classification models with the ability to discriminate between real and fake data. We argue that this GAN-based approach can help few-shot classifiers to learn sharper decision boundary, which could generalize better. We show that with our MetaGAN framework, we can extend supervised few-shot learning models to naturally cope with unsupervised data. Different from previous work in semi-supervised few-shot learning, our algorithms can deal with semi-supervision at both sample-level and task-level. We give theoretical justifications of the strength of MetaGAN, and validate the effectiveness of MetaGAN on challenging few-shot image classification benchmarks.

Deep Generative Models with Learnable Knowledge Constraints

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #32

Zhiting Hu · Zichao Yang · Ruslan Salakhutdinov · LIANHUI Qin · Xiaodan Liang · Haoye Dong · Eric Xing

The broad set of deep generative models (DGMs) has achieved remarkable advances. However, it is often difficult to incorporate rich structured domain knowledge with the end-to-end DGMs. Posterior regularization (PR) offers a principled framework to impose structured constraints on probabilistic models, but has limited applicability to the diverse DGMs that can lack a Bayesian formulation or even explicit density evaluation. PR also requires constraints to be fully specified $\{\text{it a priori}\}$, which is impractical or suboptimal for complex knowledge with learnable uncertain parts. In this paper, we establish mathematical correspondence between PR and reinforcement learning (RL), and, based on the connection, expand PR to learn constraints as the extrinsic reward in RL. The resulting algorithm is model-agnostic to apply to any DGMs, and is flexible to adapt arbitrary constraints with the model jointly. Experiments on human image generation and templated sentence generation show models with learned knowledge constraints by our algorithm greatly improve over base generative models.

Learning Attractor Dynamics for Generative Memory

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #33

Yan Wu · Gregory Wayne · Karol Gregor · Timothy Lillicrap

A central challenge faced by memory systems is the robust retrieval of a stored pattern in the presence of interference due to other stored patterns and noise. A theoretically well-founded solution to robust retrieval is given by attractor dynamics, which iteratively cleans up patterns during recall. However, incorporating attractor dynamics into modern deep learning systems poses difficulties: attractor basins are characterised by vanishing gradients, which are known to make training neural networks difficult. In this work, we exploit recent advances in variational inference and avoid the vanishing gradient problem by training a generative distributed memory with a variational lower-bound-based Lyapunov function. The model is minimalistic with surprisingly few parameters. Experiments shows it converges to correct patterns upon iterative retrieval and achieves competitive performance as both a memory model and a generative model.

Fast deep reinforcement learning using online adjustments

from the past

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #34

Steven Hansen · Alexander Pritzel · Pablo Sprechmann · Andre Barreto · Charles Blundell

We propose Ephemeral Value Adjustments (EVA): a means of allowing deep reinforcement learning agents to rapidly adapt to experience in their replay buffer. EVA shifts the value predicted by a neural network with an estimate of the value function found by prioritised sweeping over experience tuples from the replay buffer near the current state. EVA combines a number of recent ideas around combining episodic memory-like structures into reinforcement learning agents: slot-based storage, content-based retrieval, and memory-based planning. We show that EVA is performant on a demonstration task and Atari games.

Blockwise Parallel Decoding for Deep Autoregressive Models

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #35

Mitchell Stern · Noam Shazeer · Jakob Uszkoreit

Deep autoregressive sequence-to-sequence models have demonstrated impressive performance across a wide variety of tasks in recent years. While common architecture classes such as recurrent, convolutional, and self-attention networks make different trade-offs between the amount of computation needed per layer and the length of the critical path at training time, generation still remains an inherently sequential process. To overcome this limitation, we propose a novel blockwise parallel decoding scheme in which we make predictions for multiple time steps in parallel then back off to the longest prefix validated by a scoring model. This allows for substantial theoretical improvements in generation speed when applied to architectures that can process output sequences in parallel. We verify our approach empirically through a series of experiments using state-of-the-art self-attention models for machine translation and image super-resolution, achieving iteration reductions of up to 2x over a baseline greedy decoder with no loss in quality, or up to 7x in exchange for a slight decrease in performance. In terms of wall-clock time, our fastest models exhibit real-time speedups of up to 4x over standard greedy decoding.

Automatic Program Synthesis of Long Programs with a Learned Garbage Collector

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #36

Amit Zohar · Lior Wolf

We consider the problem of generating automatic code given sample input-output pairs. We train a neural network to map from the current state and the outputs to the program's next statement. The neural network optimizes multiple tasks concurrently: the next operation out of a set of high level commands, the operands of the next statement, and which variables can be dropped from memory. Using our method we are able to create programs that are more than twice as long as existing state-of-the-art solutions, while improving the success rate for comparable lengths, and cutting the run-time by two orders of magnitude. Our code, including an implementation of various literature baselines, is publicly available at <https://github.com/amitz25/PCCoder>

The Global Anchor Method for Quantifying Linguistic Shifts and Domain Adaptation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #37

Zi Yin · Vin Sachidananda · Balaji Prabhakar

Language is dynamic, constantly evolving and adapting with respect to time, domain or topic. The adaptability of language is an active research area, where researchers discover social, cultural and domain-specific changes in language using distributional tools such as word embeddings. In this paper, we introduce the global anchor method for detecting corpus-level language shifts. We show both theoretically and empirically that the global anchor method is equivalent to the alignment method, a widely-used method for comparing word embeddings, in terms of detecting corpus-level language shifts. Despite their equivalence in terms of detection abilities, we demonstrate that the global anchor method is superior in terms of applicability as it can compare embeddings of different dimensionalities. Furthermore, the global anchor method has implementation and parallelization advantages. We show that the global anchor method reveals fine structures in the evolution of language and domain adaptation. When combined with the graph Laplacian technique, the global anchor method recovers the evolution trajectory and domain clustering of disparate text corpora.

End-to-End Differentiable Physics for Learning and Control

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #38

Filipe de Avila Belbute-Peres · Kevin Smith · Kelsey Allen · Josh Tenenbaum · J. Zico Kolter

We present a differentiable physics engine that can be integrated as a module in deep neural networks for end-to-end learning. As a result, structured physics knowledge can be embedded into larger systems, allowing them, for example, to match observations by performing precise simulations, while achieves high sample efficiency. Specifically, in this paper we demonstrate how to perform backpropagation analytically through a physical simulator defined via a linear complementarity problem. Unlike traditional finite difference methods, such gradients can be

computed analytically, which allows for greater flexibility of the engine. Through experiments in diverse domains, we highlight the system's ability to learn physical parameters from data, efficiently match and simulate observed visual behavior, and readily enable control via gradient-based planning methods. Code for the engine and experiments is included with the paper.

Neural Arithmetic Logic Units

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #39

Andrew Trask · Felix Hill · Scott Reed · Jack Rae · Chris Dyer · Phil Blunsom

Neural networks can learn to represent and manipulate numerical information, but they seldom generalize well outside of the range of numerical values encountered during training. To encourage more systematic numerical extrapolation, we propose an architecture that represents numerical quantities as linear activations which are manipulated using primitive arithmetic operators, controlled by learned gates. We call this module a neural arithmetic logic unit (NALU), by analogy to the arithmetic logic unit in traditional processors. Experiments show that NALU-enhanced neural networks can learn to track time, perform arithmetic over images of numbers, translate numerical language into real-valued scalars, execute computer code, and count objects in images. In contrast to conventional architectures, we obtain substantially better generalization both inside and outside of the range of numerical values encountered during training, often extrapolating orders of magnitude beyond trained numerical ranges.

Reinforced Continual Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #40

Ju Xu · Zhanxing Zhu

Most artificial intelligence models are limited in their ability to solve new tasks faster, without forgetting previously acquired knowledge. The recently emerging paradigm of continual learning aims to solve this issue, in which the model learns various tasks in a sequential fashion. In this work, a novel approach for continual learning is proposed, which searches for the best neural architecture for each coming task via sophisticatedly designed reinforcement learning strategies. We name it as Reinforced Continual Learning. Our method not only has good performance on preventing catastrophic forgetting but also fits new tasks well. The experiments on sequential classification tasks for variants of MNIST and CIFAR-100 datasets demonstrate that the proposed approach outperforms existing continual learning alternatives for deep networks.

Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #41

Ali Shafahi · W. Ronny Huang · Mahyar Najibi · Octavian Suci · Christoph Studer · Tudor Dumitras · Tom Goldstein

Data poisoning is an attack on machine learning models wherein the attacker adds examples to the training set to manipulate the behavior of the model at test time. This paper explores poisoning attacks on neural nets. The proposed attacks use clean-labels''; they don't require the attacker to have any control over the labeling of training data. They are also targeted; they control the behavior of the classifier on a specific test instance without degrading overall classifier performance. For example, an attacker could add a seemingly innocuous image (that is properly labeled) to a training set for a face recognition engine, and control the identity of a chosen person at test time. Because the attacker does not need to control the labeling function, poisons could be entered into the training set simply by putting them online and waiting for them to be scraped by a data collection bot. We present an optimization-based method for crafting poisons, and show that just one single poison image can control classifier behavior when transfer learning is used. For full end-to-end training, we present "awatermarking" strategy that makes poisoning reliable using multiple (approx. 50) poisoned training instances. We demonstrate our method by generating poisoned frog images from the CIFAR dataset and using them to manipulate image classifiers.

Generalizing to Unseen Domains via Adversarial Data Augmentation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #42

Riccardo Volpi · Hongseok Namkoong · Ozan Sener · John Duchi · Vittorio Murino · Silvio Savarese

We are concerned with learning models that generalize well to different unseen domains. We consider a worst-case formulation over data distributions that are near the source domain in the feature space. Only using training data from a single source distribution, we propose an iterative procedure that augments the dataset with examples from a fictitious target domain that is "hard" under the current model. We show that our iterative scheme is an adaptive data augmentation method where we append adversarial examples at each iteration. For softmax losses, we show that our method is a data-dependent regularization scheme that behaves differently from classical regularizers that regularize towards zero (e.g., ridge or lasso). On digit recognition and semantic segmentation tasks, our method learns models improve performance across a range of a priori unknown target domains.

On the Local Hessian in Back-propagation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #43

Huishuai Zhang · Wei Chen · Tie-Yan Liu

Back-propagation (BP) is the foundation for successfully training deep neural networks. However, BP sometimes has difficulties in propagating a learning signal deep enough effectively, e.g., the vanishing gradient phenomenon. Meanwhile, BP often works well when combining with "designing tricks" like orthogonal initialization, batch normalization and skip connection. There is no clear understanding on what is essential to the efficiency of BP. In this paper, we take one step towards clarifying this problem. We view BP as a solution of back-matching propagation which minimizes a sequence of back-matching losses each corresponding to one block of the network. We study the Hessian of the local back-matching loss (local Hessian) and connect it to the efficiency of BP. It turns out that those designing tricks facilitate BP by improving the spectrum of local Hessian. In addition, we can utilize the local Hessian to balance the training pace of each block and design new training algorithms. Based on a scalar approximation of local Hessian, we propose a scale-amended SGD algorithm. We apply it to train neural networks with batch normalization, and achieve favorable results over vanilla SGD. This corroborates the importance of local Hessian from another side.

Lipschitz-Margin Training: Scalable Certification of Perturbation Invariance for Deep Neural Networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #44

Yusuke Tsuzuku · Issei Sato · Masashi Sugiyama

High sensitivity of neural networks against malicious perturbations on inputs causes security concerns. To take a steady step towards robust classifiers, we aim to create neural network models provably defended from perturbations. Prior certification work requires strong assumptions on network structures and massive computational costs, and thus the range of their applications was limited. From the relationship between the Lipschitz constants and prediction margins, we present a computationally efficient calculation technique to lower-bound the size of adversarial perturbations that can deceive networks, and that is widely applicable to various complicated networks. Moreover, we propose an efficient training procedure that robustifies networks and significantly improves the provably guarded areas around data points. In experimental evaluations, our method showed its ability to provide a non-trivial guarantee and enhance robustness for even large networks.

Tangent: Automatic differentiation using source-code transformation for dynamically typed array programming

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #45

Bart van Merrienboer · Dan Moldovan · Alexander Wiltschko

The need to efficiently calculate first- and higher-order derivatives of increasingly complex models expressed in Python has stressed or exceeded the capabilities of available tools. In this work, we explore techniques from the field of automatic differentiation (AD) that can give researchers expressive power, performance and strong usability. These include source-code transformation (SCT), flexible gradient surgery, efficient in-place array operations, and higher-order derivatives. We implement and demonstrate these ideas in the Tangent software library for Python, the first AD framework for a dynamic language that uses SCT.

Simple, Distributed, and Accelerated Probabilistic Programming

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #46

Dustin Tran · Matthew Hoffman · Dave Moore · Christopher Suter · Srinivas Vasudevan · Alexey Radul · Matthew Johnson · Rif A. Saurous

We describe a simple, low-level approach for embedding probabilistic programming in a deep learning ecosystem. In particular, we distill probabilistic programming down to a single abstraction—the random variable. Our lightweight implementation in TensorFlow enables numerous applications: a model-parallel variational auto-encoder (VAE) with 2nd-generation tensor processing units (TPUv2s); a data-parallel autoregressive model (Image Transformer) with TPUv2s; and multi-GPU No-U-Turn Sampler (NUTS). For both a state-of-the-art VAE on 64x64 ImageNet and Image Transformer on 256x256 CelebA-HQ, our approach achieves an optimal linear speedup from 1 to 256 TPUv2 chips. With NUTS, we see a 100x speedup on GPUs over Stan and 37x over PyMC3.

Power-law efficient neural codes provide general link between perceptual bias and discriminability

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #47

Michael Morais · Jonathan W Pillow

Recent work in theoretical neuroscience has shown that information-theoretic "efficient" neural codes, which allocate neural resources to maximize the mutual information between stimuli and

neural responses, give rise to a lawful relationship between perceptual bias and discriminability that is observed across a wide variety of psychophysical tasks in human observers (Wei & Stocker 2017). Here we generalize these results to show that the same law arises under a much larger family of optimal neural codes, introducing a unifying framework that we call power-law efficient coding. Specifically, we show that the same lawful relationship between bias and discriminability arises whenever Fisher information is allocated proportional to any power of the prior distribution. This family includes neural codes that are optimal for minimizing L_p error for any p , indicating that the lawful relationship observed in human psychophysical data does not require information-theoretically optimal neural codes. Furthermore, we derive the exact constant of proportionality governing the relationship between bias and discriminability for different power laws (which includes information-theoretically optimal codes, where the power is 2, and so-called discrimax codes, where power is $1/2$), and different choices of optimal decoder. As a bonus, our framework provides new insights into "anti-Bayesian" perceptual biases, in which percepts are biased away from the center of mass of the prior. We derive an explicit formula that clarifies precisely which combinations of neural encoder and decoder can give rise to such biases.

DropBlock: A regularization method for convolutional networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #48

Golnaz Ghiasi · Tsung-Yi Lin · Quoc V Le

Deep neural networks often work well when they are over-parameterized and trained with a massive amount of noise and regularization, such as weight decay and dropout. Although dropout is widely used as a regularization technique for fully connected layers, it is often less effective for convolutional layers. This lack of success of dropout for convolutional layers is perhaps due to the fact that activation units in convolutional layers are spatially correlated so information can still flow through convolutional networks despite dropout. Thus a structured form of dropout is needed to regularize convolutional networks. In this paper, we introduce DropBlock, a form of structured dropout, where units in a contiguous region of a feature map are dropped together. We found that applying DropBlock in skip connections in addition to the convolution layers increases the accuracy. Also, gradually increasing number of dropped units during training leads to better accuracy and more robust to hyperparameter choices. Extensive experiments show that DropBlock works better than dropout in regularizing convolutional networks. On ImageNet classification, ResNet-50 architecture with DropBlock achieves 78.13% accuracy, which is more than 1.6% improvement on the baseline. On COCO detection, DropBlock improves Average Precision of RetinaNet from 36.8% to 38.4%.

Learning sparse neural networks via sensitivity-driven regularization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #49

Enzo Tartaglione · Skjalg Lepsøy · Attilio Fiandrotti · Gianluca Francini

The ever-increasing number of parameters in deep neural networks poses challenges for memory-limited applications. Regularize-and-prune methods aim at meeting these challenges by sparsifying the network weights. In this context we quantify the output sensitivity to the parameters (i.e. their relevance to the network output) and introduce a regularization term that gradually lowers the absolute value of parameters with low sensitivity. Thus, a very large fraction of the parameters approach zero and are eventually set to zero by simple thresholding. Our method surpasses most of the recent techniques both in terms of sparsity and error rates. In some cases, the method reaches twice the sparsity obtained by other techniques at equal error rates.

Critical initialisation for deep signal propagation in noisy rectifier neural networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #50

Arnu Pretorius · Elan van Biljon · Steve Kroon · Herman Kamper

Stochastic regularisation is an important weapon in the arsenal of a deep learning practitioner. However, despite recent theoretical advances, our understanding of how noise influences signal propagation in deep neural networks remains limited. By extending recent work based on mean field theory, we develop a new framework for signal propagation in stochastic regularised neural networks. Our \textit{noisy signal propagation} theory can incorporate several common noise distributions, including additive and multiplicative Gaussian noise as well as dropout. We use this framework to investigate initialisation strategies for noisy ReLU networks. We show that no critical initialisation strategy exists using additive noise, with signal propagation exploding regardless of the selected noise distribution. For multiplicative noise (e.g. dropout), we identify alternative critical initialisation strategies that depend on the second moment of the noise distribution. Simulations and experiments on real-world data confirm that our proposed initialisation is able to stably propagate signals in deep networks, while using an initialisation disregarding noise fails to do so. Furthermore, we analyse correlation dynamics between inputs. Stronger noise regularisation is shown to reduce the depth to which discriminatory information about the inputs to a noisy ReLU network is able to propagate, even when initialised at criticality. We support our theoretical predictions for these trainable depths with simulations, as well as with experiments on MNIST and CIFAR-10.

The streaming rollout of deep networks - towards fully model-parallel execution

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #51

Volker Fischer · Jan Koehler · Thomas Pfeil

Deep neural networks, and in particular recurrent networks, are promising candidates to control autonomous agents that interact in real-time with the physical world. However, this requires a seamless integration of temporal features into the network's architecture. For the training of and inference with recurrent neural networks, they are usually rolled out over time, and different rollouts exist. Conventionally during inference, the layers of a network are computed in a sequential manner resulting in sparse temporal integration of information and long response times. In this study, we present a theoretical framework to describe rollouts, the level of model-parallelization they induce, and demonstrate differences in solving specific tasks. We prove that certain rollouts, also for networks with only skip and no recurrent connections, enable earlier and more frequent responses, and show empirically that these early responses have better performance. The streaming rollout maximizes these properties and enables a fully parallel execution of the network reducing runtime on massively parallel devices. Finally, we provide an open-source toolbox to design, train, evaluate, and interact with streaming rollouts.

The Spectrum of the Fisher Information Matrix of a Single-Hidden-Layer Neural Network

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #52

Jeffrey Pennington · Pratik Worah

An important factor contributing to the success of deep learning has been the remarkable ability to optimize large neural networks using simple first-order optimization algorithms like stochastic gradient descent. While the efficiency of such methods depends crucially on the local curvature of the loss surface, very little is actually known about how this geometry depends on network architecture and hyperparameters. In this work, we extend a recently-developed framework for studying spectra of nonlinear random matrices to characterize an important measure of curvature, namely the eigenvalues of the Fisher information matrix. We focus on a single-hidden-layer neural network with Gaussian data and weights and provide an exact expression for the spectrum in the limit of infinite width. We find that linear networks suffer worse conditioning than nonlinear networks and that nonlinear networks are generically non-degenerate. We also predict and demonstrate empirically that by adjusting the nonlinearity, the spectrum can be tuned so as to improve the efficiency of first-order optimization methods.

Learning Optimal Reserve Price against Non-myopic Bidders

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #53

Jinyan Liu · Zhiyi Huang · Xiangning Wang

We consider the problem of learning optimal reserve price in repeated auctions against non-myopic bidders, who may bid strategically in order to gain in future rounds even if the single-round auctions are truthful. Previous algorithms, e.g., empirical pricing, do not provide non-trivial regret bounds in this setting in general. We introduce algorithms that obtain small regret against non-myopic bidders either when the market is large, i.e., no bidder appears in a constant fraction of the rounds, or when the bidders are impatient, i.e., they discount future utility by some factor mildly bounded away from one. Our approach carefully controls what information is revealed to each bidder, and builds on techniques from differentially private online learning as well as the recent line of works on jointly differentially private algorithms.

Beyond Log-concavity: Provable Guarantees for Sampling Multi-modal Distributions using Simulated Tempering Langevin Monte Carlo

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #54

HOLDEN LEE · Andrej Risteski · Rong Ge

A key task in Bayesian machine learning is sampling from distributions that are only specified up to a partition function (i.e., constant of proportionality). One prevalent example of this is sampling posteriors in parametric distributions, such as latent-variable generative models. However sampling (even very approximately) can be $\#P$ -hard. Classical results (going back to Bakry and Emery) on sampling focus on log-concave distributions, and show a natural Markov chain called Langevin diffusion mix in polynomial time. However, all log-concave distributions are uni-modal, while in practice it is very common for the distribution of interest to have multiple modes. In this case, Langevin diffusion suffers from torpid mixing. We address this problem by combining Langevin diffusion with simulated tempering. The result is a Markov chain that mixes more rapidly by transitioning between different temperatures of the distribution. We analyze this Markov chain for a mixture of (strongly) log-concave distributions of the same shape. In particular, our technique applies to the canonical multi-modal distribution: a mixture of gaussians (of equal variance). Our algorithm efficiently samples from these distributions given only access to the gradient of the log-pdf. To the best of our knowledge, this is the first result that proves fast mixing for multimodal distributions.

On Binary Classification in Extreme Regions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #55

Hamid JALALZAI · Stephan Cléménçon · Anne Sabourin

In pattern recognition, a random label Y is to be predicted based upon observing a random vector X valued in \mathbb{R}^d with $d > 1$ by means of a classification rule with minimum probability of error. In a wide variety of applications, ranging from finance/insurance to environmental sciences through teletraffic data analysis for instance, extreme (i.e. very large) observations X are of crucial importance, while contributing in a negligible manner to the (empirical) error however, simply because of their rarity. As a consequence, empirical risk minimizers generally perform very poorly in extreme regions. It is the purpose of this paper to develop a general framework for classification in the extremes. Precisely, under non-parametric heavy-tail assumptions for the class distributions, we prove that a natural and asymptotic notion of risk, accounting for predictive performance in extreme regions of the input space, can be defined and show that minimizers of an empirical version of a non-asymptotic approximant of this dedicated risk, based on a fraction of the largest observations, lead to classification rules with good generalization capacity, by means of maximal deviation inequalities in low probability regions. Beyond theoretical results, numerical experiments are presented in order to illustrate the relevance of the approach developed.

PAC-Bayes bounds for stable algorithms with instance-dependent priors

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #56

Omar Rivasplata · Csaba Szepesvari · John Shawe-Taylor · Emilio Parrado-Hernandez · Shiliang Sun

PAC-Bayes bounds have been proposed to get risk estimates based on a training sample. In this paper the PAC-Bayes approach is combined with stability of the hypothesis learned by a Hilbert space valued algorithm. The PAC-Bayes setting is used with a Gaussian prior centered at the expected output. Thus a novelty of our paper is using priors defined in terms of the data-generating distribution. Our main result estimates the risk of the randomized algorithm in terms of the hypothesis stability coefficients. We also provide a new bound for the SVM classifier, which is compared to other known bounds experimentally. Ours appears to be the first uniform hypothesis stability-based bound that evaluates to non-trivial values.

Improved Algorithms for Collaborative PAC Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #57

Huy Nguyen · Lydia Zakynthinou

We study a recent model of collaborative PAC learning where k players with k different tasks collaborate to learn a single classifier that works for all tasks. Previous work showed that when there is a classifier that has very small error on all tasks, there is a collaborative algorithm that finds a single classifier for all tasks and has $O((\ln(k))^2)$ times the worst-case sample complexity for learning a single task. In this work, we design new algorithms for both the realizable and the non-realizable setting, having sample complexity only $O(\ln(k))$ times the worst-case sample complexity for learning a single task. The sample complexity upper bounds of our algorithms match previous lower bounds and in some range of parameters are even better than previous algorithms that are allowed to output different classifiers for different tasks.

Data Amplification: A Unified and Competitive Approach to Property Estimation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #58

Yi HAO · Alon Orlitsky · Ananda Theertha Suresh · Yihong Wu

Estimating properties of discrete distributions is a fundamental problem in statistical learning. We design the first unified, linear-time, competitive, property estimator that for a wide class of properties and for all underlying distributions uses just $2n$ samples to achieve the performance attained by the empirical estimator with $n\sqrt{\log n}$ samples. This provides off-the-shelf, distribution-independent, "amplification" of the amount of data available relative to common-practice estimators. We illustrate the estimator's practical advantages by comparing it to existing estimators for a wide variety of properties and distributions. In most cases, its performance with n samples is even as good as that of the empirical estimator with $n\log n$ samples, and for essentially all properties, its performance is comparable to that of the best existing estimator designed specifically for that property.

Mean-field theory of graph neural networks in graph partitioning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #59

Tatsuro Kawamoto · Masashi Tsubaki · Tomoyuki Obuchi

A theoretical performance analysis of the graph neural network (GNN) is presented. For classification tasks, the neural network approach has the advantage in terms of flexibility that it can be employed in a data-driven manner, whereas Bayesian inference requires the assumption of a specific model. A fundamental question is then whether GNN has a high accuracy in addition to this flexibility. Moreover, whether the achieved performance is predominately a result of the backpropagation or the architecture itself is a matter of considerable interest. To gain a better insight into these questions, a mean-field theory of a minimal GNN architecture is developed for the graph partitioning problem. This demonstrates a good agreement with numerical experiments.

Statistical mechanics of low-rank tensor decomposition

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #60

Jonathan Kadmon · Surya Ganguli

Often, large, high dimensional datasets collected across multiple modalities can be organized as a higher order tensor. Low-rank tensor decomposition then arises as a powerful and widely used tool to discover simple low dimensional structures underlying such data. However, we currently lack a theoretical understanding of the algorithmic behavior of low-rank tensor decompositions. We derive Bayesian approximate message passing (AMP) algorithms for recovering arbitrarily shaped low-rank tensors buried within noise, and we employ dynamic mean field theory to precisely characterize their performance. Our theory reveals the existence of phase transitions between easy, hard and impossible inference regimes, and displays an excellent match with simulations. Moreover, it reveals several qualitative surprises compared to the behavior of symmetric, cubic tensor decomposition. Finally, we compare our AMP algorithm to the most commonly used algorithm, alternating least squares (ALS), and demonstrate that AMP significantly outperforms ALS in the presence of noise.

Plug-in Estimation in High-Dimensional Linear Inverse Problems: A Rigorous Analysis

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #61

Alyson Fletcher · Parthe Pandit · Sundeeep Rangan · Subrata Sarkar · Philip Schniter

Estimating a vector \mathbf{x} from noisy linear measurements $\mathbf{Ax} + \mathbf{w}$ often requires use of prior knowledge or structural constraints on \mathbf{x} for accurate reconstruction. Several recent works have considered combining linear least-squares estimation with a generic or "plug-in denoiser" function that can be designed in a modular manner based on the prior knowledge about \mathbf{x} . While these methods have shown excellent performance, it has been difficult to obtain rigorous performance guarantees. This work considers plug-in denoising combined with the recently-developed Vector Approximate Message

Passing (VAMP) algorithm, which is itself derived via Expectation Propagation techniques. It shown that the mean squared error of thisplug-in" VAMP can be exactly predicted for a large class of high-dimensional random \mathcal{A} and denoisers. The method is illustrated in image reconstruction and parametric bilinear estimation.

The Description Length of Deep Learning models

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #62

Léonard Blier · Yann Ollivier

Deep learning models often have more parameters than observations, and still perform well. This is sometimes described as a paradox. In this work, we show experimentally that despite their huge number of parameters, deep neural networks can compress the data losslessly even when taking the cost of encoding the parameters into account. Such a compression viewpoint originally motivated the use of variational methods in neural networks. However, we show that these variational methods provide surprisingly poor compression bounds, despite being explicitly built to minimize such bounds. This might explain the relatively poor practical performance of variational methods in deep learning. Better encoding methods, imported from the Minimum Description Length (MDL) toolbox, yield much better compression values on deep networks.

Deepcode: Feedback Codes via Deep Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #63

Hyeji Kim · Yihan Jiang · Sreeram Kannan · Sewoong Oh · Pramod Viswanath

The design of codes for communicating reliably over a statistically well defined channel is an important endeavor involving deep mathematical research and wide- ranging practical applications. In this work, we present the first family of codes obtained via deep learning, which significantly beats state-of-the-art codes designed over several decades of research. The communication channel under consideration is the Gaussian noise channel with feedback, whose study was initiated by Shannon; feedback is known theoretically to improve reliability of communication, but no practical codes that do so have ever been successfully constructed. We break this logjam by integrating information theoretic insights harmoniously with recurrent-neural-network based encoders and decoders to create novel codes that outperform known codes by 3 orders of magnitude in reliability. We also demonstrate several desirable properties in the codes: (a) generalization to larger block lengths; (b) composability with known codes; (c) adaptation to practical constraints. This result also presents broader ramifications to coding theory: even when the channel has a clear mathematical model, deep learning methodologies, when combined with channel specific information-theoretic insights, can potentially beat state-of-the-art codes, constructed over decades of mathematical

research.

Binary Rating Estimation with Graph Side Information

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #64

Kwangjun Ahn · Kangwook Lee · Hyunseung Cha · Changho Suh

Rich experimental evidences show that one can better estimate users' unknown ratings with the aid of graph side information such as social graphs. However, the gain is not theoretically quantified. In this work, we study the binary rating estimation problem to understand the fundamental value of graph side information. Considering a simple correlation model between a rating matrix and a graph, we characterize the sharp threshold on the number of observed entries required to recover the rating matrix (called the optimal sample complexity) as a function of the quality of graph side information (to be detailed). To the best of our knowledge, we are the first to reveal how much the graph side information reduces sample complexity. Further, we propose a computationally efficient algorithm that achieves the limit. Our experimental results demonstrate that the algorithm performs well even with real-world graphs.

Optimization of Smooth Functions with Noisy Observations: Local Minimax Rates

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #65

Yining Wang · Sivaraman Balakrishnan · Aarti Singh

We consider the problem of global optimization of an unknown non-convex smooth function with noisy zeroth-order feedback. We propose a local minimax framework to study the fundamental difficulty of optimizing smooth functions with adaptive function evaluations. We show that for functions with fast growth around their global minima, carefully designed optimization algorithms can identify a near global minimizer with many fewer queries than worst-case global minimax theory predicts. For the special case of strongly convex and smooth functions, our implied convergence rates match the ones developed for zeroth-order convex optimization problems. On the other hand, we show that in the worst case no algorithm can converge faster than the minimax rate of estimating an unknown functions in linf-norm . Finally, we show that non-adaptive algorithms, although optimal in a global minimax sense, do not attain the optimal local minimax rate.

Parameters as interacting particles: long time convergence and asymptotic error scaling of neural networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #66

Grant Rotskoff · Eric Vanden-Eijnden

The performance of neural networks on high-dimensional data distributions suggests that it may be possible to parameterize a representation of a given high-dimensional function with controllably small errors, potentially outperforming standard interpolation methods. We demonstrate, both theoretically and numerically, that this is indeed the case. We map the parameters of a neural network to a system of particles relaxing with an interaction potential determined by the loss function. We show that in the limit that the number of parameters n is large, the landscape of the mean-squared error becomes convex and the representation error in the function scales as $O(n^{-1})$. In this limit, we prove a dynamical variant of the universal approximation theorem showing that the optimal representation can be attained by stochastic gradient descent, the algorithm ubiquitously used for parameter optimization in machine learning. In the asymptotic regime, we study the fluctuations around the optimal representation and show that they arise at a scale $O(n^{-1})$. These fluctuations in the landscape identify the natural scale for the noise in stochastic gradient descent. Our results apply to both single and multi-layer neural networks, as well as standard kernel methods like radial basis functions.

Towards Understanding Acceleration Tradeoff between Momentum and Asynchrony in Nonconvex Stochastic Optimization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #67

Tianyi Liu · Shiyang Li · Jianping Shi · Enlu Zhou · Tuo Zhao

Asynchronous momentum stochastic gradient descent algorithms (Async-MSGD) have been widely used in distributed machine learning, e.g., training large collaborative filtering systems and deep neural networks. Due to current technical limit, however, establishing convergence properties of Async-MSGD for these highly complicated nonconvex problems is generally infeasible. Therefore, we propose to analyze the algorithm through a simpler but nontrivial nonconvex problems --- streaming PCA. This allows us to make progress toward understanding Async-MSGD and gaining new insights for more general problems. Specifically, by exploiting the diffusion approximation of stochastic optimization, we establish the asymptotic rate of convergence of Async-MSGD for streaming PCA. Our results indicate a fundamental tradeoff between asynchrony and momentum: To ensure convergence and acceleration through asynchrony, we have to reduce the momentum (compared with Sync-MSGD). To the best of our knowledge, this is the first theoretical attempt on understanding Async-MSGD for distributed nonconvex stochastic optimization. Numerical

experiments on both streaming PCA and training deep neural networks are provided to support our findings for Async-MSGD.

Asymptotic optimality of adaptive importance sampling

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #68

François Portier · Bernard Delyon

\textit{Adaptive importance sampling} (AIS) uses past samples to update the \textit{sampling policy} q_t at each stage t . Each stage t is formed with two steps : (i) to explore the space with n_t points according to q_t and (ii) to exploit the current amount of information to update the sampling policy. The very fundamental question raised in this paper concerns the behavior of empirical sums based on AIS. Without making any assumption on the \textit{allocation policy} n_t , the theory developed involves no restriction on the split of computational resources between the explore (i) and the exploit (ii) step. It is shown that AIS is asymptotically optimal : the asymptotic behavior of AIS is the same as some "oracle" strategy that knows the targeted sampling policy from the beginning. From a practical perspective, weighted AIS is introduced, a new method that allows to forget poor samples from early stages.

Inference Aided Reinforcement Learning for Incentive Mechanism Design in Crowdsourcing

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #69

Zehong Hu · Yitao Liang · Jie Zhang · Zhao Li · Yang Liu

Incentive mechanisms for crowdsourcing are designed to incentivize financially self-interested workers to generate and report high-quality labels. Existing mechanisms are often developed as one-shot static solutions, assuming a certain level of knowledge about worker models (expertise levels, costs for exerting efforts, etc.). In this paper, we propose a novel inference aided reinforcement mechanism that acquires data sequentially and requires no such prior assumptions. Specifically, we first design a Gibbs sampling augmented Bayesian inference algorithm to estimate workers' labeling strategies from the collected labels at each step. Then we propose a reinforcement incentive learning (RIL) method, building on top of the above estimates, to uncover how workers respond to different payments. RIL dynamically determines the payment without accessing any ground-truth labels. We theoretically prove that RIL is able to incentivize rational workers to provide high-quality labels both at each step and in the long run. Empirical results show that our mechanism performs consistently well under both rational and non-fully rational (adaptive learning) worker models. Besides, the payments offered by RIL are more robust and have lower variances compared to existing one-shot mechanisms.

A Game-Theoretic Approach to Recommendation Systems with Strategic Content Providers

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #70

Omer Ben-Porat · Moshe Tennenholtz

We introduce a game-theoretic approach to the study of recommendation systems with strategic content providers. Such systems should be fair and stable. Showing that traditional approaches fail to satisfy these requirements, we propose the Shapley mediator. We show that the Shapley mediator satisfies the fairness and stability requirements, runs in linear time, and is the only economically efficient mechanism satisfying these properties.

A Mathematical Model For Optimal Decisions In A Representative Democracy

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #71

Malik Magdon-Ismail · Lirong Xia

Direct democracy, where each voter casts one vote, fails when the average voter competence falls below 50%. This happens in noisy settings when voters have limited information. Representative democracy, where voters choose representatives to vote, can be an elixir in both these situations. We introduce a mathematical model for studying representative democracy, in particular understanding the parameters of a representative democracy that gives maximum decision making capability. Our main result states that under general and natural conditions,

for fixed voting cost, the optimal number of representatives is linear; for polynomial cost, the optimal number of representatives is logarithmic.

Universal Growth in Production Economies

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #72

Simina Branzei · Ruta Mehta · Noam Nisan

We study a simple variant of the von Neumann model of an expanding economy, in which multiple producers make goods according to their production function. The players trade their goods at the market and then use the bundles received as inputs for the production in the next round. The decision that players have to make is how to invest their money (i.e. bids) in each round. We show

that a simple decentralized dynamic, where players update their bids on the goods in the market proportionally to how useful the investments were, leads to growth of the economy in the long term (whenever growth is possible) but also creates unbounded inequality, i.e. very rich and very poor players emerge. We analyze several other phenomena, such as how the relation of a player with others influences its development and the Gini index of the system.

Convex Elicitation of Continuous Properties

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #73

Jessica Finocchiaro · Rafael Frongillo

A property or statistic of a distribution is said to be elicitable if it can be expressed as the minimizer of some loss function in expectation. Recent work shows that continuous real-valued properties are elicitable if and only if they are identifiable, meaning the set of distributions with the same property value can be described by linear constraints. From a practical standpoint, one may ask for which such properties do there exist convex loss functions. In this paper, in a finite-outcome setting, we show that in fact every elicitable real-valued property can be elicited by a convex loss function. Our proof is constructive, and leads to convex loss functions for new properties.

Contextual Pricing for Lipschitz Buyers

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #74

Jieming Mao · Renato Leme · Jon Schneider

We investigate the problem of learning a Lipschitz function from binary feedback. In this problem, a learner is trying to learn a Lipschitz function $f: [0,1]^d \rightarrow [0,1]$ over the course of T rounds. On round t , an adversary provides the learner with an input x_t , the learner submits a guess y_t for $f(x_t)$, and learns whether $y_t > f(x_t)$ or $y_t \leq f(x_t)$. The learner's goal is to minimize their total loss $\sum_t \ell(f(x_t), y_t)$ (for some loss function ℓ). The problem is motivated by *contextual dynamic pricing*, where a firm must sell a stream of differentiated products to a collection of buyers with non-linear valuations for the items and observes only whether the item was sold or not at the posted price.

For the symmetric loss $\ell(f(x_t), y_t) = |f(x_t) - y_t|$, we provide an algorithm for this problem achieving total loss $O(\log T)$ when $d=1$ and $O(T^{\frac{d-1}{d}})$ when $d>1$, and show that both bounds are tight (up to a factor of $\sqrt{\log T}$). For the pricing loss function $\ell(f(x_t), y_t) = f(x_t) - y_t \cdot \mathbf{1}\{y_t \leq f(x_t)\}$ we show a regret bound of $O(T^{\frac{d}{d+1}})$ and show that this bound is tight. We present improved bounds in the special case of a population of linear buyers.

Learning in Games with Lossy Feedback

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #75

Zhengyuan Zhou · Panayotis Mertikopoulos · Susan Athey · Nicholas Bambos · Peter W Glynn · Yinyu Ye

We consider a game-theoretical multi-agent learning problem where the feedback information can be lost during the learning process and rewards are given by a broad class of games known as variationally stable games. We propose a simple variant of the classical online gradient descent algorithm, called reweighted online gradient descent (ROGD) and show that in variationally stable games, if each agent adopts ROGD, then almost sure convergence to the set of Nash equilibria is guaranteed, even when the feedback loss is asynchronous and arbitrarily correlated among agents. We then extend the framework to deal with unknown feedback loss probabilities by using an estimator (constructed from past data) in its replacement. Finally, we further extend the framework to accommodate both asynchronous loss and stochastic rewards and establish that multi-agent ROGD learning still converges to the set of Nash equilibria in such settings. Together, these results contribute to the broad landscape of multi-agent online learning by significantly relaxing the feedback information that is required to achieve desirable outcomes.

Multiplicative Weights Updates with Constant Step-Size in Graphical Constant-Sum Games

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #76

Yun Kuen Cheung

Since Multiplicative Weights (MW) updates are the discrete analogue of the continuous Replicator Dynamics (RD), some researchers had expected their qualitative behaviours would be similar. We show that this is false in the context of graphical constant-sum games, which include two-person zero-sum games as special cases. In such games which have a fully-mixed Nash Equilibrium (NE), it was known that RD satisfy the permanence and Poincare recurrence properties, but we show that MW updates with any constant step-size $\epsilon > 0$ converge to the boundary of the state space, and thus do not satisfy the two properties. Using this result, we show that MW updates have a regret lower bound of $\Omega(1 / (\epsilon T))$, while it was known that the regret of RD is upper bounded by $O(1 / T)$. Interestingly, the regret perspective can be useful for better understanding of the behaviours of MW updates. In a two-person zero-sum game, if it has a unique NE which is fully mixed, then we show, via regret, that for any sufficiently small ϵ , there exist at least two probability densities and a constant $Z > 0$, such that for any arbitrarily small $z > 0$, each of the two densities fluctuates above Z and below z infinitely often.

Solving Large Sequential Games with the Excessive Gap Technique

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #77

Christian Kroer · Gabriele Farina · Tuomas Sandholm

There has been tremendous recent progress on equilibrium-finding algorithms for zero-sum imperfect-information extensive-form games, but there has been a puzzling gap between theory and practice. *First-order methods* have significantly better theoretical convergence rates than any *counterfactual-regret minimization (CFR)* variant. Despite this, CFR variants have been favored in practice. Experiments with first-order methods have only been conducted on small- and medium-sized games because those methods are complicated to implement in this setting, and because CFR variants have been enhanced extensively for over a decade they perform well in practice. In this paper we show that a particular first-order method, a state-of-the-art variant of the *excessive gap technique*---instantiated with the *dilated entropy distance function*---can efficiently solve large real-world problems competitively with CFR and its variants. We show this on large endgames encountered by the *Libratus* poker AI, which recently beat top human poker specialist professionals at no-limit Texas hold'em. We show experimental results on our variant of the excessive gap technique as well as a prior version. We introduce a numerically friendly implementation of the smoothed best response computation associated with first-order methods for extensive-form game solving. We present, to our knowledge, the first GPU implementation of a first-order method for extensive-form games. We present comparisons of several excessive gap technique and CFR variants.

Practical exact algorithm for trembling-hand equilibrium refinements in games

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #78

Gabriele Farina · Nicola Gatti · Tuomas Sandholm

Nash equilibrium strategies have the known weakness that they do not prescribe rational play in situations that are reached with zero probability according to the strategies themselves, for example, if players have made mistakes. Trembling-hand refinements---such as extensive-form perfect equilibria and quasi-perfect equilibria---remedy this problem in sound ways. Despite their appeal, they have not received attention in practice since no known algorithm for computing them scales beyond toy instances. In this paper, we design an exact polynomial-time algorithm for finding trembling-hand equilibria in zero-sum extensive-form games. It is several orders of magnitude faster than the best prior ones, numerically stable, and quickly solves game instances with tens of

thousands of nodes in the game tree. It enables, for the first time, the use of trembling-hand refinements in practice.

Improving Online Algorithms via ML Predictions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #79

Manish Purohit · Zoya Svitkina · Ravi Kumar

In this work we study the problem of using machine-learned predictions to improve performance of online algorithms. We consider two classical problems, ski rental and non-clairvoyant job scheduling, and obtain new online algorithms that use predictions to make their decisions. These algorithms are oblivious to the performance of the predictor, improve with better predictions, but do not degrade much if the predictions are poor.

Variance-Reduced Stochastic Gradient Descent on Streaming Data

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #80

Ellango Jothimurugesan · Ashraf Tahmasbi · Phillip Gibbons · Srikanta Tirthapura

We present an algorithm STRSAGA for efficiently maintaining a machine learning model over data points that arrive over time, quickly updating the model as new training data is observed. We present a competitive analysis comparing the sub-optimality of the model maintained by STRSAGA with that of an offline algorithm that is given the entire data beforehand, and analyze the risk-competitiveness of STRSAGA under different arrival patterns. Our theoretical and experimental results show that the risk of STRSAGA is comparable to that of offline algorithms on a variety of input arrival patterns, and its experimental performance is significantly better than prior algorithms suited for streaming data, such as SGD and SSVRG.

Regret Bounds for Robust Adaptive Control of the Linear Quadratic Regulator

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #81

Sarah Dean · Horia Mania · Nikolai Matni · Benjamin Recht · Stephen Tu

We consider adaptive control of the Linear Quadratic Regulator (LQR), where an unknown linear system is controlled subject to quadratic costs. Leveraging recent developments in the estimation of

linear systems and in robust controller synthesis, we present the first provably polynomial time algorithm that achieves sub-linear regret on this problem. We further study the interplay between regret minimization and parameter estimation by proving a lower bound on the expected regret in terms of the exploration schedule used by any algorithm. Finally, we conduct a numerical study comparing our robust adaptive algorithm to other methods from the adaptive LQR literature, and demonstrate the flexibility of our proposed method by extending it to a demand forecasting problem subject to state constraints.

PAC-learning in the presence of adversaries

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #82

Daniel Cullina · Arjun Nitin Bhagoji · Prateek Mittal

The existence of evasion attacks during the test phase of machine learning algorithms represents a significant challenge to both their deployment and understanding. These attacks can be carried out by adding imperceptible perturbations to inputs to generate adversarial examples and finding effective defenses and detectors has proven to be difficult. In this paper, we step away from the attack-defense arms race and seek to understand the limits of what can be learned in the presence of an evasion adversary. In particular, we extend the Probably Approximately Correct (PAC)-learning framework to account for the presence of an adversary. We first define corrupted hypothesis classes which arise from standard binary hypothesis classes in the presence of an evasion adversary and derive the Vapnik-Chervonenkis (VC)-dimension for these, denoted as the adversarial VC-dimension. We then show that sample complexity upper bounds from the Fundamental Theorem of Statistical learning can be extended to the case of evasion adversaries, where the sample complexity is controlled by the adversarial VC-dimension. We then explicitly derive the adversarial VC-dimension for halfspace classifiers in the presence of a sample-wise norm-constrained adversary of the type commonly studied for evasion attacks and show that it is the same as the standard VC-dimension, closing an open question. Finally, we prove that the adversarial VC-dimension can be either larger or smaller than the standard VC-dimension depending on the hypothesis class and adversary, making it an interesting object of study in its own right.

Tight Bounds for Collaborative PAC Learning via Multiplicative Weights

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #83

Jiecao Chen · Qin Zhang · Yuan Zhou

We study the collaborative PAC learning problem recently proposed in Blum et al.~\cite{BHPQ17}, in which we have k players and they want to learn a target function collaboratively, such that the

learned function approximates the target function well on all players' distributions simultaneously. The quality of the collaborative learning algorithm is measured by the ratio between the sample complexity of the algorithm and that of the learning algorithm for a single distribution (called the overhead). We obtain a collaborative learning algorithm with overhead $O(\ln k)$, improving the one with overhead $O(\ln^2 k)$ in \cite{BHPQ17}. We also show that an $\Omega(\ln k)$ overhead is inevitable when k is polynomial bounded by the VC dimension of the hypothesis class. Finally, our experimental study has demonstrated the superiority of our algorithm compared with the one in Blum et al. \cite{BHPQ17} on real-world datasets.

Understanding Weight Normalized Deep Neural Networks with Rectified Linear Units

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #84

Yixi Xu · Xiao Wang

This paper presents a general framework for norm-based capacity control for $L_{p,q}$ weight normalized deep neural networks. We establish the upper bound on the Rademacher complexities of this family. With an $L_{p,q}$ normalization where $q \leq p$ and $1/p + 1/q = 1$, we discuss properties of a width-independent capacity control, which only depends on the depth by a square root term. We further analyze the approximation properties of $L_{p,q}$ weight normalized deep neural networks. In particular, for an $L_{1,\infty}$ weight normalized network, the approximation error can be controlled by the L_1 norm of the output layer, and the corresponding generalization error only depends on the architecture by the square root of the depth.

Generalization Bounds for Uniformly Stable Algorithms

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #85

Vitaly Feldman · Jan Vondrak

Uniform stability of a learning algorithm is a classical notion of algorithmic stability introduced to derive high-probability bounds on the generalization error (Bousquet and Elisseeff, 2002). Specifically, for a loss function with range bounded in $[0,1]$, the generalization error of a γ -uniformly stable learning algorithm on n samples is known to be at most $O((\gamma + 1/n) \sqrt{n \log(1/\delta)})$ with probability at least $1 - \delta$. Unfortunately, this bound does not lead to meaningful generalization bounds in many common settings where $\gamma \geq 1/\sqrt{n}$. At the same time the bound is known to be tight only when $\gamma = O(1/n)$. Here we prove substantially stronger generalization bounds for uniformly stable algorithms without any additional assumptions. First, we show that the generalization error in this setting is at most $O(\sqrt{(\gamma + 1/n) \log(1/\delta)})$ with probability at least $1 - \delta$. In addition, we prove a tight bound of

$O(\gamma^2 + 1/n)$ on the second moment of the generalization error. The best previous bound on the second moment of the generalization error is $O(\gamma + 1/n)$. Our proofs are based on new analysis techniques and our results imply substantially stronger generalization guarantees for several well-studied algorithms.

Minimax Statistical Learning with Wasserstein distances

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #86

Jaeho Lee · Maxim Raginsky

As opposed to standard empirical risk minimization (ERM), distributionally robust optimization aims to minimize the worst-case risk over a larger ambiguity set containing the original empirical distribution of the training data. In this work, we describe a minimax framework for statistical learning with ambiguity sets given by balls in Wasserstein space. In particular, we prove generalization bounds that involve the covering number properties of the original ERM problem. As an illustrative example, we provide generalization guarantees for transport-based domain adaptation problems where the Wasserstein distance between the source and target domain distributions can be reliably estimated from unlabeled samples.

Differentially Private Uniformly Most Powerful Tests for Binomial Data

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #87

Jordan Awan · Aleksandra Slavković

We derive uniformly most powerful (UMP) tests for simple and one-sided hypotheses for a population proportion within the framework of Differential Privacy (DP), optimizing finite sample performance. We show that in general, DP hypothesis tests can be written in terms of linear constraints, and for exchangeable data can always be expressed as a function of the empirical distribution. Using this structure, we prove a ‘Neyman-Pearson lemma’ for binomial data under DP, where the DP-UMP only depends on the sample sum. Our tests can also be stated as a post-processing of a random variable, whose distribution we coin “Truncated-Uniform-Laplace” (Tulap), a generalization of the Staircase and discrete Laplace distributions. Furthermore, we obtain exact p-values, which are easily computed in terms of the Tulap random variable. We show that our results also apply to distribution-free hypothesis tests for continuous data. Our simulation results demonstrate that our tests have exact type I error, and are more powerful than current techniques.

Sketching Method for Large Scale Combinatorial Inference

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #88

Wei Sun · Junwei Lu · Han Liu

We present computationally efficient algorithms to test various combinatorial structures of large-scale graphical models. In order to test the hypotheses on their topological structures, we propose two adjacency matrix sketching frameworks: neighborhood sketching and subgraph sketching. The neighborhood sketching algorithm is proposed to test the connectivity of graphical models. This algorithm randomly subsamples vertices and conducts neighborhood regression and screening. The global sketching algorithm is proposed to test the topological properties requiring exponential computation complexity, especially testing the chromatic number and the maximum clique. This algorithm infers the corresponding property based on the sampled subgraph. Our algorithms are shown to substantially accelerate the computation of existing methods. We validate our theory and method through both synthetic simulations and a real application in neuroscience.

An Improved Analysis of Alternating Minimization for Structured Multi-Response Regression

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #89

Sheng Chen · Arindam Banerjee

Multi-response linear models aggregate a set of vanilla linear models by assuming correlated noise across them, which has an unknown covariance structure. To find the coefficient vector, estimators with a joint approximation of the noise covariance are often preferred than the simple linear regression in view of their superior empirical performance, which can be generally solved by alternating-minimization type procedures. Due to the non-convex nature of such joint estimators, the theoretical justification of their efficiency is typically challenging. The existing analyses fail to fully explain the empirical observations due to the assumption of resampling on the alternating procedures, which requires access to fresh samples in each iteration. In this work, we present a resampling-free analysis for the alternating minimization algorithm applied to the multi-response regression. In particular, we focus on the high-dimensional setting of multi-response linear models with structured coefficient parameter, and the statistical error of the parameter can be expressed by the complexity measure, Gaussian width, which is related to the assumed structure. More importantly, to the best of our knowledge, our result reveals for the first time that the alternating minimization with random initialization can achieve the same performance as the well-initialized one when solving this multi-response regression problem. Experimental results support our theoretical developments.

MixLasso: Generalized Mixed Regression via Convex Atomic-Norm Regularization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #90

Ian En-Hsu Yen · Wei-Cheng Lee · Kai Zhong · Sung-En Chang · Pradeep Ravikumar · Shou-De Lin

We consider a generalization of mixed regression where the response is an additive combination of several mixture components. Standard mixed regression is a special case where each response is generated from exactly one component. Typical approaches to the mixture regression problem employ local search methods such as Expectation Maximization (EM) that are prone to spurious local optima. On the other hand, a number of recent theoretically-motivated *Tensor-based methods* either have high sample complexity, or require the knowledge of the input distribution, which is not available in most of practical situations. In this work, we study a novel convex estimator *MixLasso* for the estimation of generalized mixed regression, based on an atomic norm specifically constructed to regularize the number of mixture components. Our algorithm gives a risk bound that trades off between prediction accuracy and model sparsity without imposing stringent assumptions on the input/output distribution, and can be easily adapted to the case of non-linear functions. In our numerical experiments on mixtures of linear as well as nonlinear regressions, the proposed method yields high-quality solutions in a wider range of settings than existing approaches.

A Theory-Based Evaluation of Nearest Neighbor Models Put Into Practice

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #91

Hendrik Fichtenberger · Dennis Rohde

In the k -nearest neighborhood model (k -NN), we are given a set of points P , and we shall answer queries q by returning the k nearest neighbors of q in P according to some metric. This concept is crucial in many areas of data analysis and data processing, e.g., computer vision, document retrieval and machine learning. Many k -NN algorithms have been published and implemented, but often the relation between parameters and accuracy of the computed k -NN is not explicit. We study property testing of k -NN graphs in theory and evaluate it empirically: given a point set $P \subset \mathbb{R}^\Delta$ and a directed graph $G=(P,E)$, is G a k -NN graph, i.e., every point $p \in P$ has outgoing edges to its k nearest neighbors, or is it ϵ -far from being a k -NN graph? Here, ϵ -far means that one has to change more than an ϵ -fraction of the edges in order to make G a k -NN graph. We develop a randomized algorithm with one-sided error that decides this question, i.e., a property tester for the k -NN property, with complexity $O(\sqrt{n} \cdot k^2 / \epsilon^2)$ measured in terms of the number of vertices and edges it inspects, and we prove a lower bound of $\Omega(\sqrt{n / \epsilon k})$. We evaluate our tester empirically on the k -NN models computed by various algorithms and show that it can be used to

detect k -NN models with bad accuracy in significantly less time than the building time of the k -NN model.

Sharp Bounds for Generalized Uniformity Testing

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #92

Ilias Diakonikolas · Daniel M. Kane · Alistair Stewart

We study the problem of generalized uniformity testing of a discrete probability distribution: Given samples from a probability distribution p over an unknown size discrete domain Ω , we want to distinguish, with probability at least $2/3$, between the case that p is uniform on some subset of Ω versus ϵ -far, in total variation distance, from any such uniform distribution. We establish tight bounds on the sample complexity of generalized uniformity testing. In more detail, we present a computationally efficient tester whose sample complexity is optimal, within constant factors, and a matching worst-case information-theoretic lower bound. Specifically, we show that the sample complexity of generalized uniformity testing is $\Theta(1/(\epsilon^{4/3} \|p\|_3) + 1/(\epsilon^2 \|p\|_2))$.

Testing for Families of Distributions via the Fourier Transform

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #93

Alistair Stewart · Ilias Diakonikolas · Clement Canonne

We study the general problem of testing whether an unknown discrete distribution belongs to a specified family of distributions. More specifically, given a distribution family P and sample access to an unknown discrete distribution D , we want to distinguish (with high probability) between the case that $D \in P$ and the case that D is ϵ -far, in total variation distance, from every distribution in P . This is the prototypical hypothesis testing problem that has received significant attention in statistics and, more recently, in computer science. The main contribution of this work is a simple and general testing technique that is applicable to all distribution families whose Fourier spectrum satisfies a certain approximate sparsity property. We apply our Fourier-based framework to obtain near sample-optimal and computationally efficient testers for the following fundamental distribution families: Sums of Independent Integer Random Variables (SIIRVs), Poisson Multinomial Distributions (PMDs), and Discrete Log-Concave Distributions. For the first two, ours are the first non-trivial testers in the literature, vastly generalizing previous work on testing Poisson Binomial Distributions. For the third, our tester improves on prior work in both sample and time complexity.

High Dimensional Linear Regression using Lattice Basis Reduction

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #94

Ilias Zadik · David Gamarnik

We consider a high dimensional linear regression problem where the goal is to efficiently recover an unknown vector β^* from n noisy linear observations $Y = X\beta^* + W$ in \mathbb{R}^n , for known X in $\mathbb{R}^{n \times p}$ and unknown W in \mathbb{R}^n . Unlike most of the literature on this model we make no sparsity assumption on β^* . Instead we adopt a regularization based on assuming that the underlying vectors β^* have rational entries with the same denominator Q . We call this Q -rationality assumption. We propose a new polynomial-time algorithm for this task which is based on the seminal Lenstra-Lenstra-Lovasz (LLL) lattice basis reduction algorithm. We establish that under the Q -rationality assumption, our algorithm recovers exactly the vector β^* for a large class of distributions for the iid entries of X and non-zero noise W . We prove that it is successful under small noise, even when the learner has access to only one observation ($n=1$). Furthermore, we prove that in the case of the Gaussian white noise for W , $n=o(p/\log p)$ and Q sufficiently large, our algorithm tolerates a nearly optimal information-theoretic level of the noise.

ℓ_1 -regression with Heavy-tailed Distributions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #95

Lijun Zhang · Zhi-Hua Zhou

In this paper, we consider the problem of linear regression with heavy-tailed distributions. Different from previous studies that use the squared loss to measure the performance, we choose the absolute loss, which is capable of estimating the conditional median. To address the challenge that both the input and output could be heavy-tailed, we propose a truncated minimization problem, and demonstrate that it enjoys an $O(\sqrt{d/n})$ excess risk, where d is the dimensionality and n is the number of samples. Compared with traditional work on ℓ_1 -regression, the main advantage of our result is that we achieve a high-probability risk bound without exponential moment conditions on the input and output. Furthermore, if the input is bounded, we show that the classical empirical risk minimization is competent for ℓ_1 -regression even when the output is heavy-tailed.

Constant Regret, Generalized Mixability, and Mirror Descent

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #96

We consider the setting of prediction with expert advice; a learner makes predictions by aggregating those of a group of experts. Under this setting, and for the right choice of loss function and "mixing" algorithm, it is possible for the learner to achieve a constant regret regardless of the number of prediction rounds. For example, a constant regret can be achieved for ϕ -mixable losses using the aggregating algorithm. The Generalized Aggregating Algorithm (GAA) is a name for a family of algorithms parameterized by convex functions on simplices (entropies), which reduce to the aggregating algorithm when using the Shannon entropy H_S . For a given entropy H , losses for which a constant regret is possible using the GAA are called H -mixable. Which losses are H -mixable was previously left as an open question. We fully characterize H -mixability and answer other open questions posed by [Reid2015]. We show that the Shannon entropy H_S is fundamental in nature when it comes to mixability; any H -mixable loss is necessarily H_S -mixable, and the lowest worst-case regret of the GAA is achieved using the Shannon entropy. Finally, by leveraging the connection between the mirror descent algorithm and the update step of the GAA, we suggest a new adaptive generalized aggregating algorithm and analyze its performance in terms of the regret bound.

Stochastic Composite Mirror Descent: Optimal Bounds with High Probabilities

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #97

Yunwen Lei · Ke Tang

We study stochastic composite mirror descent, a class of scalable algorithms able to exploit the geometry and composite structure of a problem. We consider both convex and strongly convex objectives with non-smooth loss functions, for each of which we establish high-probability convergence rates optimal up to a logarithmic factor. We apply the derived computational error bounds to study the generalization performance of multi-pass stochastic gradient descent (SGD) in a non-parametric setting. Our high-probability generalization bounds enjoy a logarithmic dependency on the number of passes provided that the step size sequence is square-summable, which improves the existing bounds in expectation with a polynomial dependency and therefore gives a strong justification on the ability of multi-pass SGD to overcome overfitting. Our analysis removes boundedness assumptions on subgradients often imposed in the literature. Numerical results are reported to support our theoretical findings.

Uniform Convergence of Gradients for Non-Convex Learning and Optimization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #98

Dylan Foster · Ayush Sekhari · Karthik Sridharan

We investigate 1) the rate at which refined properties of the empirical risk---in particular, gradients---converge to their population counterparts in standard non-convex learning tasks, and 2) the consequences of this convergence for optimization. Our analysis follows the tradition of norm-based capacity control. We propose vector-valued Rademacher complexities as a simple, composable, and user-friendly tool to derive dimension-free uniform convergence bounds for gradients in non-convex learning problems. As an application of our techniques, we give a new analysis of batch gradient descent methods for non-convex generalized linear models and non-convex robust regression, showing how to use any algorithm that finds approximate stationary points to obtain optimal sample complexity, even when dimension is high or possibly infinite and multiple passes over the dataset are allowed. Moving to non-smooth models we show---in contrast to the smooth case---that even for a single ReLU it is not possible to obtain dimension-independent convergence rates for gradients in the worst case. On the positive side, it is still possible to obtain dimension-independent rates under a new type of distributional assumption.

Fast Rates of ERM and Stochastic Approximation: Adaptive to Error Bound Conditions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #99

Mingrui Liu · Xiaoxuan Zhang · Lijun Zhang · Jing Rong · Tianbao Yang

Error bound conditions (EBC) are properties that characterize the growth of an objective function when a point is moved away from the optimal set. They have recently received increasing attention in the field of optimization for developing optimization algorithms with fast convergence. However, the studies of EBC in statistical learning are hitherto still limited. The main contributions of this paper are two-fold. First, we develop fast and intermediate rates of empirical risk minimization (ERM) under EBC for risk minimization with Lipschitz continuous, and smooth convex random functions. Second, we establish fast and intermediate rates of an efficient stochastic approximation (SA) algorithm for risk minimization with Lipschitz continuous random functions, which requires only one pass of n samples and adapts to EBC. For both approaches, the convergence rates span a full spectrum between $\widetilde{O}(1/\sqrt{n})$ and $\widetilde{O}(1/n)$ depending on the power constant in EBC, and could be even faster than $O(1/n)$ in special cases for ERM. Moreover, these convergence rates are automatically adaptive without using any knowledge of EBC. Overall, this work not only strengthens the understanding of ERM for statistical learning but also brings new fast stochastic algorithms for solving a broad range of statistical learning problems.

Nearly tight sample complexity bounds for learning mixtures of Gaussians via sample compression schemes

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #100

Hassan Ashtiani · Shai Ben-David · Nick Harvey · Christopher Liaw · Abbas Mehrabian · Yaniv Plan

We prove that $\Theta(k d^2 / \epsilon^2)$ samples are necessary and sufficient for learning a mixture of k Gaussians in \mathbb{R}^d , up to error ϵ in total variation distance. This improves both the known upper bounds and lower bounds for this problem. For mixtures of axis-aligned Gaussians, we show that $O(k d / \epsilon^2)$ samples suffice, matching a known lower bound. The upper bound is based on a novel technique for distribution learning based on a notion of sample compression. Any class of distributions that allows such a sample compression scheme can also be learned with few samples. Moreover, if a class of distributions has such a compression scheme, then so do the classes of products and mixtures of those distributions. The core of our main result is showing that the class of Gaussians in \mathbb{R}^d has an efficient sample compression.

Early Stopping for Nonparametric Testing

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #101

Meimei Liu · Guang Cheng

Early stopping of iterative algorithms is an algorithmic regularization method to avoid over-fitting in estimation and classification. In this paper, we show that early stopping can also be applied to obtain the minimax optimal testing in a general non-parametric setup. Specifically, a Wald-type test statistic is obtained based on an iterated estimate produced by functional gradient descent algorithms in a reproducing kernel Hilbert space. A notable contribution is to establish a "sharp" stopping rule: when the number of iterations achieves an optimal order, testing optimality is achievable; otherwise, testing optimality becomes impossible. As a by-product, a similar sharpness result is also derived for minimax optimal estimation under early stopping. All obtained results hold for various kernel classes, including Sobolev smoothness classes and Gaussian kernel classes.

Chaining Mutual Information and Tightening Generalization Bounds

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #102

Amir Asadi · Emmanuel Abbe · Sergio Verdu

Bounding the generalization error of learning algorithms has a long history, which yet falls short in explaining various generalization successes including those of deep learning. Two important difficulties are (i) exploiting the dependencies between the hypotheses, (ii) exploiting the dependence between the algorithm's input and output. Progress on the first point was made with the chaining method, originating from the work of Kolmogorov, and used in the VC-dimension bound. More recently, progress on the second point was made with the mutual information method by Russo and Zou '15. Yet, these two methods are currently disjoint. In this paper, we introduce a technique to combine chaining and mutual information methods, to obtain a generalization bound that is both algorithm-dependent and that exploits the dependencies between the hypotheses. We provide an example in which our bound significantly outperforms both the chaining and the mutual information bounds. As a corollary, we tighten Dudley's inequality when the learning algorithm chooses its output from a small subset of hypotheses with high probability.

Dimensionality Reduction has Quantifiable Imperfections: Two Geometric Bounds

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #103

Kry Lui · Gavin Weiguang Ding · Ruitong Huang · Robert McCann

In this paper, we investigate Dimensionality reduction (DR) maps in an information retrieval setting from a quantitative topology point of view. In particular, we show that no DR maps can achieve perfect precision and perfect recall simultaneously. Thus a continuous DR map must have imperfect precision. We further prove an upper bound on the precision of Lipschitz continuous DR maps. While precision is a natural measure in an information retrieval setting, it does not measure 'how' wrong the retrieved data is. We therefore propose a new measure based on Wasserstein distance that comes with similar theoretical guarantee. A key technical step in our proofs is a particular optimization problem of the L_2 -Wasserstein distance over a constrained set of distributions. We provide a complete solution to this optimization problem, which can be of independent interest on the technical side.

Minimax Estimation of Neural Net Distance

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #104

Kaiyi Ji · Yingbin Liang

An important class of distance metrics proposed for training generative adversarial networks (GANs) is the integral probability metric (IPM), in which the neural net distance captures the practical GAN training via two neural networks. This paper investigates the minimax estimation problem of the neural net distance based on samples drawn from the distributions. We develop the first known

minimax lower bound on the estimation error of the neural net distance, and an upper bound tighter than an existing bound on the estimator error for the empirical neural net distance. Our lower and upper bounds match not only in the order of the sample size but also in terms of the norm of the parameter matrices of neural networks, which justifies the empirical neural net distance as a good approximation of the true neural net distance for training GANs in practice.

Quantifying Learning Guarantees for Convex but Inconsistent Surrogates

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #105

Kirill Struminsky · Simon Lacoste-Julien · Anton Osokin

We study consistency properties of machine learning methods based on minimizing convex surrogates. We extend the recent framework of Osokin et al. (2017) for the quantitative analysis of consistency properties to the case of inconsistent surrogates. Our key technical contribution consists in a new lower bound on the calibration function for the quadratic surrogate, which is non-trivial (not always zero) for inconsistent cases. The new bound allows to quantify the level of inconsistency of the setting and shows how learning with inconsistent surrogates can have guarantees on sample complexity and optimization difficulty. We apply our theory to two concrete cases: multi-class classification with the tree-structured loss and ranking with the mean average precision loss. The results show the approximation-computation trade-offs caused by inconsistent surrogates and their potential benefits.

Learning Signed Determinantal Point Processes through the Principal Minor Assignment Problem

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #106

Victor-Emmanuel Brunel

Symmetric determinantal point processes (DPP) are a class of probabilistic models that encode the random selection of items that have a repulsive behavior. They have attracted a lot of attention in machine learning, where returning diverse sets of items is sought for. Sampling and learning these symmetric DPP's is pretty well understood. In this work, we consider a new class of DPP's, which we call signed DPP's, where we break the symmetry and allow attractive behaviors. We set the ground for learning signed DPP's through a method of moments, by solving the so called principal assignment problem for a class of matrices K that satisfy $K_{i,j} = \pm K_{j,i}$, $i \neq j$, in polynomial time.

Data-dependent PAC-Bayes priors via differential privacy

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #107

Gintare Karolina Dziugaite · Daniel Roy

The Probably Approximately Correct (PAC) Bayes framework (McAllester, 1999) can incorporate knowledge about the learning algorithm and (data) distribution through the use of distribution-dependent priors, yielding tighter generalization bounds on data-dependent posteriors. Using this flexibility, however, is difficult, especially when the data distribution is presumed to be unknown. We show how a differentially private data-dependent prior yields a valid PAC-Bayes bound, and then show how non-private mechanisms for choosing priors can also yield generalization bounds. As an application of this result, we show that a Gaussian prior mean chosen via stochastic gradient Langevin dynamics (SGLD; Welling and Teh, 2011) leads to a valid PAC-Bayes bound due to control of the 2-Wasserstein distance to a differentially private stationary distribution. We study our data-dependent bounds empirically, and show that they can be nonvacuous even when other distribution-dependent bounds are vacuous.

Computationally and statistically efficient learning of causal Bayes nets using path queries

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #108

Kevin Bello · Jean Honorio

Causal discovery from empirical data is a fundamental problem in many scientific domains. Observational data allows for identifiability only up to Markov equivalence class. In this paper we first propose a polynomial time algorithm for learning the exact correctly-oriented structure of the transitive reduction of any causal Bayesian network with high probability, by using interventional path queries. Each path query takes as input an origin node and a target node, and answers whether there is a directed path from the origin to the target. This is done by intervening on the origin node and observing samples from the target node. We theoretically show the logarithmic sample complexity for the size of interventional data per path query, for continuous and discrete networks. We then show how to learn the transitive edges using also logarithmic sample complexity (albeit in time exponential in the maximum number of parents for discrete networks), which allows us to learn the full network. We further extend our work by reducing the number of interventional path queries for learning rooted trees. We also provide an analysis of imperfect interventions.

PAC-Bayes Tree: weighted subtrees with guarantees

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #109

Tin D Nguyen · Samory Kpotufe

We present a weighted-majority classification approach over subtrees of a fixed tree, which provably achieves excess-risk of the same order as the best tree-pruning. Furthermore, the computational efficiency of pruning is maintained at both training and testing time despite having to aggregate over an exponential number of subtrees. We believe this is the first subtree aggregation approach with such guarantees.

A loss framework for calibrated anomaly detection

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #110

Aditya Menon · Robert Williamson

Given samples from a probability distribution, anomaly detection is the problem of determining if a given point lies in a low-density region. This paper concerns calibrated anomaly detection, which is the practically relevant extension where we additionally wish to produce a confidence score for a point being anomalous. Building on a classification framework for anomaly detection, we show how minimisation of a suitably modified proper loss produces density estimates only for anomalous instances. We then show how to incorporate quantile control by relating our objective to a generalised version of the pinball loss. Finally, we show how to efficiently optimise the objective with kernelised scorer, by leveraging a recent result from the point process literature. The resulting objective captures a close relative of the one-class SVM as a special case.

On Oracle-Efficient PAC RL with Rich Observations

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #111

Christoph Dann · Nan Jiang · Akshay Krishnamurthy · Alekh Agarwal · John Langford · Robert Schapire

We study the computational tractability of PAC reinforcement learning with rich observations. We present new provably sample-efficient algorithms for environments with deterministic hidden state dynamics and stochastic rich observations. These methods operate in an oracle model of computation -- accessing policy and value function classes exclusively through standard optimization primitives -- and therefore represent computationally efficient alternatives to prior algorithms that require enumeration. With stochastic hidden state dynamics, we prove that the only known sample-efficient algorithm, OLIVE, cannot be implemented in the oracle model. We also present several

examples that illustrate fundamental challenges of tractable PAC reinforcement learning in such general settings.

Adversarial Risk and Robustness: General Definitions and Implications for the Uniform Distribution

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #112

Dimitrios Diochnos · Saeed Mahloujifar · Mohammad Mahmoody

We study adversarial perturbations when the instances are uniformly distributed over $\{0,1\}^n$. We study both "inherent" bounds that apply to any problem and any classifier for such a problem as well as bounds that apply to specific problems and specific hypothesis classes. As the current literature contains multiple definitions of adversarial risk and robustness, we start by giving a taxonomy for these definitions based on their direct goals; we identify one of them as the one guaranteeing misclassification by pushing the instances to the error region. We then study some classic algorithms for learning monotone conjunctions and compare their adversarial risk and robustness under different definitions by attacking the hypotheses using instances drawn from the uniform distribution. We observe that sometimes these definitions lead to significantly different bounds. Thus, this study advocates for the use of the error-region definition, even though other definitions, in other contexts with context-dependent assumptions, may coincide with the error-region definition. Using the error-region definition of adversarial perturbations, we then study inherent bounds on risk and robustness of any classifier for any classification problem whose instances are uniformly distributed over $\{0,1\}^n$. Using the isoperimetric inequality for the Boolean hypercube, we show that for initial error 0.01, there always exists an adversarial perturbation that changes $O(\sqrt{n})$ bits of the instances to increase the risk to 0.5, making classifier's decisions meaningless. Furthermore, by also using the central limit theorem we show that when $n \rightarrow \infty$, at most $c\sqrt{n}$ bits of perturbations, for a universal constant $c < 1.17$, suffice for increasing the risk to 0.5, and the same $c\sqrt{n}$ bits of perturbations on average suffice to increase the risk to 1, hence bounding the robustness by $c\sqrt{n}$.

Learning from discriminative feature feedback

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #113

Sanjoy Dasgupta · Sivan Sabato · Nicholas Roberts · Akansha Dey

We consider the problem of learning a multi-class classifier from labels as well as simple explanations that we call "discriminative features". We show that such explanations can be provided whenever the target concept is a decision tree, or more generally belongs to a particular subclass of DNF formulas. We present an efficient online algorithm for learning from such feedback and we give tight bounds on the number of mistakes made during the learning process. These bounds depend

only on the size of the target concept and not on the overall number of available features, which could be infinite. We also demonstrate the learning procedure experimentally.

How to Start Training: The Effect of Initialization and Architecture

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #114

Boris Hanin · David Rolnick

We identify and study two common failure modes for early training in deep ReLU nets. For each, we give a rigorous proof of when it occurs and how to avoid it, for fully connected, convolutional, and residual architectures. We show that the first failure mode, exploding or vanishing mean activation length, can be avoided by initializing weights from a symmetric distribution with variance $2/\text{fan-in}$ and, for ResNets, by correctly scaling the residual modules. We prove that the second failure mode, exponentially large variance of activation length, never occurs in residual nets once the first failure mode is avoided. In contrast, for fully connected nets, we prove that this failure mode can happen and is avoided by keeping constant the sum of the reciprocals of layer widths. We demonstrate empirically the effectiveness of our theoretical results in predicting when networks are able to start training. In particular, we note that many popular initializations fail our criteria, whereas correct initialization and architecture allows much deeper networks to be trained.

Bilevel Distance Metric Learning for Robust Image Recognition

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #115

Jie Xu · Lei Luo · Cheng Deng · Heng Huang

Metric learning, aiming to learn a discriminative Mahalanobis distance matrix M that can effectively reflect the similarity between data samples, has been widely studied in various image recognition problems. Most of the existing metric learning methods input the features extracted directly from the original data in the preprocess phase. What's worse, these features usually take no consideration of the local geometrical structure of the data and the noise existed in the data, thus they may not be optimal for the subsequent metric learning task. In this paper, we integrate both feature extraction and metric learning into one joint optimization framework and propose a new bilevel distance metric learning model. Specifically, the lower level characterizes the intrinsic data structure using graph regularized sparse coefficients, while the upper level forces the data samples from the same class to be close to each other and pushes those from different classes far away. In addition, leveraging the KKT conditions and the alternating direction method (ADM), we derive an efficient algorithm to solve the proposed new model. Extensive experiments on various occluded datasets demonstrate the

effectiveness and robustness of our method.

Deep Non-Blind Deconvolution via Generalized Low-Rank Approximation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #116

Wenqi Ren · Jiawei Zhang · Lin Ma · Jinshan Pan · Xiaochun Cao · Wangmeng Zuo · Wei Liu · Ming-Hsuan Yang

In this paper, we present a deep convolutional neural network to capture the inherent properties of image degradation, which can handle different kernels and saturated pixels in a unified framework. The proposed neural network is motivated by the low-rank property of pseudo-inverse kernels. We first compute a generalized low-rank approximation for a large number of blur kernels, and then use separable filters to initialize the convolutional parameters in the network. Our analysis shows that the estimated decomposed matrices contain the most essential information of the input kernel, which ensures the proposed network to handle various blurs in a unified framework and generate high-quality deblurring results. Experimental results on benchmark datasets with noise and saturated pixels demonstrate that the proposed algorithm performs favorably against state-of-the-art methods.

Unsupervised Depth Estimation, 3D Face Rotation and Replacement

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #117

Joel Ruben Antony Moniz · Christopher Beckham · Simon Rajotte · Sina Honari · Chris Pal

We present an unsupervised approach for learning to estimate three dimensional (3D) facial structure from a single image while also predicting 3D viewpoint transformations that match a desired pose and facial geometry. We achieve this by inferring the depth of facial keypoints of an input image in an unsupervised manner, without using any form of ground-truth depth information. We show how it is possible to use these depths as intermediate computations within a new backpropable loss to predict the parameters of a 3D affine transformation matrix that maps inferred 3D keypoints of an input face to the corresponding 2D keypoints on a desired target facial geometry or pose. Our resulting approach, called DepthNets, can therefore be used to infer plausible 3D transformations from one face pose to another, allowing faces to be frontalized, transformed into 3D models or even warped to another pose and facial geometry. Lastly, we identify certain shortcomings with our formulation, and explore adversarial image translation techniques as a post-processing step to re-synthesize complete head shots for faces re-targeted to different poses or identities.

Neighbourhood Consensus Networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #118

Ignacio Rocco · Mircea Cimpoi · Relja Arandjelović · Akihiko Torii · Tomas Pajdla · Josef Sivic

We address the problem of finding reliable dense correspondences between a pair of images. This is a challenging task due to strong appearance differences between the corresponding scene elements and ambiguities generated by repetitive patterns. The contributions of this work are threefold. First, inspired by the classic idea of disambiguating feature matches using semi-local constraints, we develop an end-to-end trainable convolutional neural network architecture that identifies sets of spatially consistent matches by analyzing neighbourhood consensus patterns in the 4D space of all possible correspondences between a pair of images without the need for a global geometric model. Second, we demonstrate that the model can be trained effectively from weak supervision in the form of matching and non-matching image pairs without the need for costly manual annotation of point to point correspondences. Third, we show the proposed neighbourhood consensus network can be applied to a range of matching tasks including both category- and instance-level matching, obtaining the state-of-the-art results on the PF Pascal dataset and the InLoc indoor visual localization benchmark.

Recurrent Transformer Networks for Semantic Correspondence

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #119

Seungryong Kim · Stephen Lin · SANG RYUL JEON · Dongbo Min · Kwanghoon Sohn

We present recurrent transformer networks (RTNs) for obtaining dense correspondences between semantically similar images. Our networks accomplish this through an iterative process of estimating spatial transformations between the input images and using these transformations to generate aligned convolutional activations. By directly estimating the transformations between an image pair, rather than employing spatial transformer networks to independently normalize each individual image, we show that greater accuracy can be achieved. This process is conducted in a recursive manner to refine both the transformation estimates and the feature representations. In addition, a technique is presented for weakly-supervised training of RTNs that is based on a proposed classification loss. With RTNs, state-of-the-art performance is attained on several benchmarks for semantic correspondence.

Deep Network for the Integrated 3D Sensing of Multiple People in Natural Images

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #120

Andrei Zanfir · Elisabeta Marinoiu · Mihai Zanfir · Alin-Ionut Popa · Cristian Sminchisescu

We present MubyNet -- a feed-forward, multitask, bottom up system for the integrated localization, as well as 3d pose and shape estimation, of multiple people in monocular images. The challenge is the formal modeling of the problem that intrinsically requires discrete and continuous computation, e.g. grouping people vs. predicting 3d pose. The model identifies human body structures (joints and limbs) in images, groups them based on 2d and 3d information fused using learned scoring functions, and optimally aggregates such responses into partial or complete 3d human skeleton hypotheses under kinematic tree constraints, but without knowing in advance the number of people in the scene and their visibility relations. We design a multi-task deep neural network with differentiable stages where the person grouping problem is formulated as an integer program based on learned body part scores parameterized by both 2d and 3d information. This avoids suboptimality resulting from separate 2d and 3d reasoning, with grouping performed based on the combined representation. The final stage of 3d pose and shape prediction is based on a learned attention process where information from different human body parts is optimally integrated. State-of-the-art results are obtained in large scale datasets like Human3.6M and Panoptic, and qualitatively by reconstructing the 3d shape and pose of multiple people, under occlusion, in difficult monocular images.

A Neural Compositional Paradigm for Image Captioning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #121

Bo Dai · Sanja Fidler · Dahua Lin

Mainstream captioning models often follow a sequential structure to generate captions, leading to issues such as introduction of irrelevant semantics, lack of diversity in the generated captions, and inadequate generalization performance. In this paper, we present an alternative paradigm for image captioning, which factorizes the captioning procedure into two stages: (1) extracting an explicit semantic representation from the given image; and (2) constructing the caption based on a recursive compositional procedure in a bottom-up manner. Compared to conventional ones, our paradigm better preserves the semantic content through an explicit factorization of semantics and syntax. By using the compositional generation procedure, caption construction follows a recursive structure, which naturally fits the properties of human language. Moreover, the proposed compositional procedure requires less data to train, generalizes better, and yields more diverse captions.

Visual Memory for Robust Path Following

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #122

Ashish Kumar · Saurabh Gupta · David Fouhey · Sergey Levine · Jitendra Malik

Humans routinely retrace a path in a novel environment both forwards and backwards despite uncertainty in their motion. In this paper, we present an approach for doing so. Given a demonstration of a path, a first network generates an abstraction of the path. Equipped with this abstraction, a second network then observes the world and decides how to act in order to retrace the path under noisy actuation and a changing environment. The two networks are optimized end-to-end at training time. We evaluate the method in two realistic simulators, performing path following both forwards and backwards. Our experiments show that our approach outperforms both a classical approach to solving this task as well as a number of other baselines.

Learning to Exploit Stability for 3D Scene Parsing

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #123

Yilun Du · Zhijian Liu · Hector Basevi · Ales Leonardis · Bill Freeman · Josh Tenenbaum · Jiajun Wu

Human scene understanding uses a variety of visual and non-visual cues to perform inference on object types, poses, and relations. Physics is a rich and universal cue which we exploit to enhance scene understanding. We integrate the physical cue of stability into the learning process using a REINFORCE approach coupled to a physics engine, and apply this to the problem of producing the 3D bounding boxes and poses of objects in a scene. We first show that applying physics supervision to an existing scene understanding model increases performance, produces more stable predictions, and allows training to an equivalent performance level with fewer annotated training examples. We then present a novel architecture for 3D scene parsing named Prim R-CNN, learning to predict bounding boxes as well as their 3D size, translation, and rotation. With physics supervision, Prim R-CNN outperforms existing scene understanding approaches on this problem. Finally, we show that applying physics supervision on unlabeled real images improves real domain transfer of models training on synthetic data.

Learning to Decompose and Disentangle Representations for Video Prediction

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #124

Jun-Ting Hsieh · Bingbin Liu · De-An Huang · Li Fei-Fei · Juan Carlos Niebles

Our goal is to predict future video frames given a sequence of input frames. Despite large amounts of video data, this remains a challenging task because of the high-dimensionality of video frames. We address this challenge by proposing the Decompositional Disentangled Predictive Auto-Encoder (DDPAE), a framework that combines structured probabilistic models and deep networks to automatically (i) decompose the high-dimensional video that we aim to predict into components, and (ii) disentangle each component to have low-dimensional temporal dynamics that are easier to predict. Crucially, with an appropriately specified generative model of video frames, our DDPAE is able to learn both the latent decomposition and disentanglement without explicit supervision. For the Moving MNIST dataset, we show that DDPAE is able to recover the underlying components (individual digits) and disentanglement (appearance and location) as we would intuitively do. We further demonstrate that DDPAE can be applied to the Bouncing Balls dataset involving complex interactions between multiple objects to predict the video frame directly from the pixels and recover physical states without explicit supervision.

Weakly Supervised Dense Event Captioning in Videos

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #125

Xuguang Duan · Wenbing Huang · Chuang Gan · Jingdong Wang · Wenwu Zhu · Junzhou Huang

Dense event captioning aims to detect and describe all events of interest contained in a video. Despite the advanced development in this area, existing methods tackle this task by making use of dense temporal annotations, which is dramatically source-consuming. This paper formulates a new problem: weakly supervised dense event captioning, which does not require temporal segment annotations for model training. Our solution is based on the one-to-one correspondence assumption, each caption describes one temporal segment, and each temporal segment has one caption, which holds in current benchmark datasets and most real world cases. We decompose the problem into a pair of dual problems: event captioning and sentence localization and present a cycle system to train our model. Extensive experimental results are provided to demonstrate the ability of our model on both dense event captioning and sentence localization in videos.

Text-Adaptive Generative Adversarial Networks: Manipulating Images with Natural Language

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #126

Seonghyeon Nam · Yunji Kim · Seon Joo Kim

This paper addresses the problem of manipulating images using natural language description. Our task aims to semantically modify visual attributes of an object in an image according to the text describing the new visual appearance. Although existing methods synthesize images having new

attributes, they do not fully preserve text-irrelevant contents of the original image. In this paper, we propose the text-adaptive generative adversarial network (TAGAN) to generate semantically manipulated images while preserving text-irrelevant contents. The key to our method is the text-adaptive discriminator that creates word level local discriminators according to input text to classify fine-grained attributes independently. With this discriminator, the generator learns to generate images where only regions that correspond to the given text is modified. Experimental results show that our method outperforms existing methods on CUB and Oxford-102 datasets, and our results were mostly preferred on a user study. Extensive analysis shows that our method is able to effectively disentangle visual attributes and produce pleasing outputs.

A Probabilistic U-Net for Segmentation of Ambiguous Images

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #127

Simon Kohl · Bernardino Romera-Paredes · Clemens Meyer · Jeffrey De Fauw · Joseph R. Ledsam · Klaus Maier-Hein · S. M. Ali Eslami · Danilo Jimenez Rezende · Olaf Ronneberger

Many real-world vision problems suffer from inherent ambiguities. In clinical applications for example, it might not be clear from a CT scan alone which particular region is cancer tissue. Therefore a group of graders typically produces a set of diverse but plausible segmentations. We consider the task of learning a distribution over segmentations given an input. To this end we propose a generative segmentation model based on a combination of a U-Net with a conditional variational autoencoder that is capable of efficiently producing an unlimited number of plausible hypotheses. We show on a lung abnormalities segmentation task and on a Cityscapes segmentation task that our model reproduces the possible segmentation variants as well as the frequencies with which they occur, doing so significantly better than published approaches. These models could have a high impact in real-world applications, such as being used as clinical decision-making algorithms accounting for multiple plausible semantic segmentation hypotheses to provide possible diagnoses and recommend further actions to resolve the present ambiguities.

Forward Modeling for Partial Observation Strategy Games - A StarCraft Defogger

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #128

Gabriel Synnaeve · Zeming Lin · Jonas Gehring · Dan Gant · Vegard Mella · Vasil Khalidov · Nicolas Carion · Nicolas Usunier

We formulate the problem of defogging as state estimation and future state prediction from previous, partial observations in the context of real-time strategy games. We propose to employ

encoder-decoder neural networks for this task, and introduce proxy tasks and baselines for evaluation to assess their ability of capturing basic game rules and high-level dynamics. By combining convolutional neural networks and recurrent networks, we exploit spatial and sequential correlations and train well-performing models on a large dataset of human games of StarCraft: Brood War. Finally, we demonstrate the relevance of our models to downstream tasks by applying them for enemy unit prediction in a state-of-the-art, rule-based StarCraft bot. We observe improvements in win rates against several strong community bots.

Adversarial Text Generation via Feature-Mover's Distance

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #129

Liqun Chen · Shuyang Dai · Chenyang Tao · Haichao Zhang · Zhe Gan · Dinghan Shen · Yizhe Zhang · Guoyin Wang · Ruiyi Zhang · Lawrence Carin

Generative adversarial networks (GANs) have achieved significant success in generating real-valued data. However, the discrete nature of text hinders the application of GAN to text-generation tasks. Instead of using the standard GAN objective, we propose to improve text-generation GAN via a novel approach inspired by optimal transport. Specifically, we consider matching the latent feature distributions of real and synthetic sentences using a novel metric, termed the feature-mover's distance (FMD). This formulation leads to a highly discriminative critic and easy-to-optimize objective, overcoming the mode-collapsing and brittle-training problems in existing methods. Extensive experiments are conducted on a variety of tasks to evaluate the proposed model empirically, including unconditional text generation, style transfer from non-parallel text, and unsupervised cipher cracking. The proposed model yields superior performance, demonstrating wide applicability and effectiveness.

Virtual Class Enhanced Discriminative Embedding Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #130

Binghui Chen · Weihong Deng · Haifeng Shen

Recently, learning discriminative features to improve the recognition performances gradually becomes the primary goal of deep learning, and numerous remarkable works have emerged. In this paper, we propose a novel yet extremely simple method Virtual Softmax to enhance the discriminative property of learned features by injecting a dynamic virtual negative class into the original softmax. Injecting virtual class aims to enlarge inter-class margin and compress intra-class distribution by strengthening the decision boundary constraint. Although it seems weird to optimize with this additional virtual class, we show that our method derives from an intuitive and clear motivation, and it indeed encourages the features to be more compact and separable. This paper

empirically and experimentally demonstrates the superiority of Virtual Softmax, improving the performances on a variety of object classification and face verification tasks.

Learning Pipelines with Limited Data and Domain Knowledge: A Study in Parsing Physics Problems

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #131

Mrinmaya Sachan · Kumar Avinava Dubey · Tom Mitchell · Dan Roth · Eric Xing

As machine learning becomes more widely used in practice, we need new methods to build complex intelligent systems that integrate learning with existing software, and with domain knowledge encoded as rules. As a case study, we present such a system that learns to parse Newtonian physics problems in textbooks. This system, Nuts&Bolts, learns a pipeline process that incorporates existing code, pre-learned machine learning models, and human engineered rules. It jointly trains the entire pipeline to prevent propagation of errors, using a combination of labelled and unlabelled data. Our approach achieves a good performance on the parsing task, outperforming the simple pipeline and its variants. Finally, we also show how Nuts&Bolts can be used to achieve improvements on a relation extraction task and on the end task of answering Newtonian physics problems.

Pipe-SGD: A Decentralized Pipelined SGD Framework for Distributed Deep Net Training

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #132

Youjie Li · Mingchao Yu · Songze Li · Salman Avestimehr · Nam Sung Kim · Alexander Schwing

Distributed training of deep nets is an important technique to address some of the present day computing challenges like memory consumption and computational demands. Classical distributed approaches, synchronous or asynchronous, are based on the parameter server architecture, i.e., worker nodes compute gradients which are communicated to the parameter server while updated parameters are returned. Recently, distributed training with AllReduce operations gained popularity as well. While many of those operations seem appealing, little is reported about wall-clock training time improvements. In this paper, we carefully analyze the AllReduce based setup, propose timing models which include network latency, bandwidth, cluster size and compute time, and demonstrate that a pipelined training with a width of two combines the best of both synchronous and asynchronous training. Specifically, for a setup consisting of a four-node GPU cluster we show wall-clock time training improvements of up to 5.4x compared to conventional approaches.

MULAN: A Blind and Off-Grid Method for Multichannel Echo Retrieval

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #133

Helena Peic Tukuljac · Antoine Deleforge · Remi Gribonval

This paper addresses the general problem of blind echo retrieval, i.e., given M sensors measuring in the discrete-time domain M mixtures of K delayed and attenuated copies of an unknown source signal, can the echo location and weights be recovered? This problem has broad applications in fields such as sonars, seismology, ultrasounds or room acoustics. It belongs to the broader class of blind channel identification problems, which have been intensively studied in signal processing. All existing methods proceed in two steps: (i) blind estimation of sparse discrete-time filters and (ii) echo information retrieval by peak picking. The precision of these methods is fundamentally limited by the rate at which the signals are sampled: estimated echo locations are necessary on-grid, and since true locations never match the sampling grid, the weight estimation precision is also strongly limited. This is the so-called basis-mismatch problem in compressed sensing. We propose a radically different approach to the problem, building on top of the framework of finite-rate-of-innovation sampling. The approach operates directly in the parameter-space of echo locations and weights, and enables near-exact blind and off-grid echo retrieval from discrete-time measurements. It is shown to outperform conventional methods by several orders of magnitudes in precision.

Diminishing Returns Shape Constraints for Interpretability and Regularization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #134

Maya Gupta · Dara Bahri · Andrew Cotter · Kevin Canini

We investigate machine learning models that can provide diminishing returns and accelerating returns guarantees to capture prior knowledge or policies about how outputs should depend on inputs. We show that one can build flexible, nonlinear, multi-dimensional models using lattice functions with any combination of concavity/convexity and monotonicity constraints on any subsets of features, and compare to new shape-constrained neural networks. We demonstrate on real-world examples that these shape constrained models can provide tuning-free regularization and improve model understandability.

Fairness Through Computationally-Bounded Awareness

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #135

Michael Kim · Omer Reingold · Guy Rothblum

We study the problem of fair classification within the versatile framework of Dwork et al. [ITCS '12], which assumes the existence of a metric that measures similarity between pairs of individuals. Unlike earlier work, we do not assume that the entire metric is known to the learning algorithm; instead, the learner can query this arbitrary metric a bounded number of times. We propose a new notion of fairness called metric multifairness and show how to achieve this notion in our setting. Metric multifairness is parameterized by a similarity metric d on pairs of individuals to classify and a rich collection C of (possibly overlapping) "comparison sets" over pairs of individuals. At a high level, metric multifairness guarantees that similar subpopulations are treated similarly, as long as these subpopulations are identified within the class C .

On preserving non-discrimination when combining expert advice

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #136

Avrim Blum · Suriya Gunasekar · Thodoris Lykouris · Nati Srebro

We study the interplay between sequential decision making and avoiding discrimination against protected groups, when examples arrive online and do not follow distributional assumptions. We consider the most basic extension of classical online learning: Given a class of predictors that are individually non-discriminatory with respect to a particular metric, how can we combine them to perform as well as the best predictor, while preserving non-discrimination? Surprisingly we show that this task is unachievable for the prevalent notion of "equalized odds" that requires equal false negative rates and equal false positive rates across groups. On the positive side, for another notion of non-discrimination, "equalized error rates", we show that running separate instances of the classical multiplicative weights algorithm for each group achieves this guarantee. Interestingly, even for this notion, we show that algorithms with stronger performance guarantees than multiplicative weights cannot preserve non-discrimination.

Fairness Behind a Veil of Ignorance: A Welfare Analysis for Automated Decision Making

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #137

Hoda Heidari · Claudio Ferrari · Krishna Gummadi · Andreas Krause

We draw attention to an important, yet largely overlooked aspect of evaluating fairness for automated decision making systems---namely risk and welfare considerations. Our proposed family of measures corresponds to the long-established formulations of cardinal social welfare in

economics, and is justified by the Rawlsian conception of fairness behind a veil of ignorance. The convex formulation of our welfare-based measures of fairness allows us to integrate them as a constraint into any convex loss minimization pipeline. Our empirical analysis reveals interesting trade-offs between our proposal and (a) prediction accuracy, (b) group discrimination, and (c) Dwork et al's notion of individual fairness. Furthermore and perhaps most importantly, our work provides both heuristic justification and empirical evidence suggesting that a lower-bound on our measures often leads to bounded inequality in algorithmic outcomes; hence presenting the first computationally feasible mechanism for bounding individual-level inequality.

Inequity aversion improves cooperation in intertemporal social dilemmas

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #138

Edward Hughes · Joel Leibo · Matthew Phillips · Karl Tuyls · Edgar Dueñez-Guzman · Antonio García Castañeda · Iain Dunning · Tina Zhu · Kevin McKee · Raphael Koster · Heather Roff · Thore Graepel

Groups of humans are often able to find ways to cooperate with one another in complex, temporally extended social dilemmas. Models based on behavioral economics are only able to explain this phenomenon for unrealistic stateless matrix games. Recently, multi-agent reinforcement learning has been applied to generalize social dilemma problems to temporally and spatially extended Markov games. However, this has not yet generated an agent that learns to cooperate in social dilemmas as humans do. A key insight is that many, but not all, human individuals have inequity averse social preferences. This promotes a particular resolution of the matrix game social dilemma wherein inequity-averse individuals are personally pro-social and punish defectors. Here we extend this idea to Markov games and show that it promotes cooperation in several types of sequential social dilemma, via a profitable interaction with policy learnability. In particular, we find that inequity aversion improves temporal credit assignment for the important class of intertemporal social dilemmas. These results help explain how large-scale cooperation may emerge and persist.

On Misinformation Containment in Online Social Networks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #139

Amo Tong · Ding-Zhu Du · Weili Wu

The widespread online misinformation could cause public panic and serious economic damages. The misinformation containment problem aims at limiting the spread of misinformation in online social networks by launching competing campaigns. Motivated by realistic scenarios, we present the first analysis of the misinformation containment problem for the case when an arbitrary number of cascades are allowed. This paper makes four contributions. First, we provide a formal model for

multi-cascade diffusion and introduce an important concept called as cascade priority. Second, we show that the misinformation containment problem cannot be approximated within a factor of $\Omega(2^{\log^{1-\epsilon} n^4})$ in polynomial time unless $NP \subseteq TIME(n^{\text{polylog}\{n\}})$. Third, we introduce several types of cascade priority that are frequently seen in real social networks. Finally, we design novel algorithms for solving the misinformation containment problem. The effectiveness of the proposed algorithm is supported by encouraging experimental results.

Found Graph Data and Planted Vertex Covers

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #140

Austin Benson · Jon Kleinberg

A typical way in which network data is recorded is to measure all interactions involving a specified set of core nodes, which produces a graph containing this core together with a potentially larger set of fringe nodes that link to the core. Interactions between nodes in the fringe, however, are not present in the resulting graph data. For example, a phone service provider may only record calls in which at least one of the participants is a customer; this can include calls between a customer and a non-customer, but not between pairs of non-customers. Knowledge of which nodes belong to the core is crucial for interpreting the dataset, but this metadata is unavailable in many cases, either because it has been lost due to difficulties in data provenance, or because the network consists of "found data" obtained in settings such as counter-surveillance. This leads to an algorithmic problem of recovering the core set. Since the core is a vertex cover, we essentially have a planted vertex cover problem, but with an arbitrary underlying graph. We develop a framework for analyzing this planted vertex cover problem, based on the theory of fixed-parameter tractability, together with algorithms for recovering the core. Our algorithms are fast, simple to implement, and out-perform several baselines based on core-periphery structure on various real-world datasets.

Inferring Networks From Random Walk-Based Node Similarities

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #141

Jeremy Hoskins · Cameron Musco · Christopher Musco · Babis Tsourakakis

Digital presence in the world of online social media entails significant privacy risks. In this work we consider a privacy threat to a social network in which an attacker has access to a subset of random walk-based node similarities, such as effective resistances (i.e., commute times) or personalized PageRank scores. Using these similarities, the attacker seeks to infer as much information as possible about the network, including unknown pairwise node similarities and edges. For the

effective resistance metric, we show that with just a small subset of measurements, one can learn a large fraction of edges in a social network. We also show that it is possible to learn a graph which accurately matches the underlying network on all other effective resistances. This second observation is interesting from a data mining perspective, since it can be expensive to compute all effective resistances or other random walk-based similarities. As an alternative, our graphs learned from just a subset of effective resistances can be used as surrogates in a range of applications that use effective resistances to probe graph structure, including for graph clustering, node centrality evaluation, and anomaly detection. We obtain our results by formalizing the graph learning objective mathematically, using two optimization problems. One formulation is convex and can be solved provably in polynomial time. The other is not, but we solve it efficiently with projected gradient and coordinate descent. We demonstrate the effectiveness of these methods on a number of social networks obtained from Facebook. We also discuss how our methods can be generalized to other random walk-based similarities, such as personalized PageRank scores. Our code is available at <https://github.com/cnmusco/graph-similarity-learning>.

Fast Greedy MAP Inference for Determinantal Point Process to Improve Recommendation Diversity

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #142

Laming Chen · Guoxin Zhang · Eric Zhou

The determinantal point process (DPP) is an elegant probabilistic model of repulsion with applications in various machine learning tasks including summarization and search. However, the maximum a posteriori (MAP) inference for DPP which plays an important role in many applications is NP-hard, and even the popular greedy algorithm can still be too computationally expensive to be used in large-scale real-time scenarios. To overcome the computational challenge, in this paper, we propose a novel algorithm to greatly accelerate the greedy MAP inference for DPP. In addition, our algorithm also adapts to scenarios where the repulsion is only required among nearby few items in the result sequence. We apply the proposed algorithm to generate relevant and diverse recommendations. Experimental results show that our proposed algorithm is significantly faster than state-of-the-art competitors, and provides a better relevance-diversity trade-off on several public datasets, which is also confirmed in an online A/B test.

Unorganized Malicious Attacks Detection

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #143

Ming Pang · Wei Gao · Min Tao · Zhi-Hua Zhou

Recommender systems have attracted much attention during the past decade. Many attack detection

algorithms have been developed for better recommendations, mostly focusing on shilling attacks, where an attack organizer produces a large number of user profiles by the same strategy to promote or demote an item. This work considers another different attack style: unorganized malicious attacks, where attackers individually utilize a small number of user profiles to attack different items without organizer. This attack style occurs in many real applications, yet relevant study remains open. We formulate the unorganized malicious attacks detection as a matrix completion problem, and propose the Unorganized Malicious Attacks detection (UMA) algorithm, based on the alternating splitting augmented Lagrangian method. We verify, both theoretically and empirically, the effectiveness of the proposed approach.

Scalable Robust Matrix Factorization with Nonconvex Loss

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #144

Quanming Yao · James Kwok

Robust matrix factorization (RMF), which uses the ℓ_1 -loss, often outperforms standard matrix factorization using the ℓ_2 -loss, particularly when outliers are present. The state-of-the-art RMF solver is the RMF-MM algorithm, which, however, cannot utilize data sparsity. Moreover, sometimes even the (convex) ℓ_1 -loss is not robust enough. In this paper, we propose the use of nonconvex loss to enhance robustness. To address the resultant difficult optimization problem, we use majorization-minimization (MM) optimization and propose a new MM surrogate. To improve scalability, we exploit data sparsity and optimize the surrogate via its dual with the accelerated proximal gradient algorithm. The resultant algorithm has low time and space complexities and is guaranteed to converge to a critical point. Extensive experiments demonstrate its superiority over the state-of-the-art in terms of both accuracy and scalability.

Differentially Private Robust Low-Rank Approximation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #145

Raman Arora · Vladimir Braverman · Jalaj Upadhyay

In this paper, we study the following robust low-rank matrix approximation problem: given a matrix $A \in \mathbb{R}^{n \times d}$, find a rank- k matrix B , while satisfying differential privacy, such that $\|A - B\|_p \leq \alpha \mathsf{OPT}_k(A) + \tau$, where $\|M\|_p$ is the entry-wise ℓ_p -norm and $\mathsf{OPT}_k(A) := \min\{\mathsf{rank}(X) \leq k \mid \|A - X\|_p\}$. It is well known that low-rank approximation w.r.t. entrywise ℓ_p -norm, for $p \in [1, 2]$, yields robustness to gross outliers in the data. We propose an algorithm that guarantees $\alpha = \tilde{O}(k^2)$, $\tau = \tilde{O}(k^2(n+kd)/\epsilon)$, runs in $\tilde{O}((n+d)\text{poly}(k))$ time and uses $O(k(n+d)\log k)$ space. We study extensions to the streaming

setting where entries of the matrix arrive in an arbitrary order and output is produced at the very end or continually. We also study the related problem of differentially private robust principal component analysis (PCA), wherein we return a rank- k projection matrix Π such that $\|A - A\Pi\|_F \leq \alpha \mathsf{OPT}_k(A) + \tau$.

Differential Privacy for Growing Databases

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #146

Rachel Cummings · Sara Krehbiel · Kevin A Lai · Uthaipon Tantipongpipat

The large majority of differentially private algorithms focus on the static setting, where queries are made on an unchanging database. This is unsuitable for the myriad applications involving databases that grow over time. To address this gap in the literature, we consider the dynamic setting, in which new data arrive over time. Previous results in this setting have been limited to answering a single non-adaptive query repeatedly as the database grows. In contrast, we provide tools for richer and more adaptive analysis of growing databases. Our first contribution is a novel modification of the private multiplicative weights algorithm, which provides accurate analysis of exponentially many adaptive linear queries (an expressive query class including all counting queries) for a static database. Our modification maintains the accuracy guarantee of the static setting even as the database grows without bound. Our second contribution is a set of general results which show that many other private and accurate algorithms can be immediately extended to the dynamic setting by rerunning them at appropriate points of data growth with minimal loss of accuracy, even when data growth is unbounded.

Efficient Neural Network Robustness Certification with General Activation Functions

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #147

Huan Zhang · Tsui-Wei Weng · Pin-Yu Chen · Cho-Jui Hsieh · Luca Daniel

Finding minimum distortion of adversarial examples and thus certifying robustness in neural networks classifiers is known to be a challenging problem. Nevertheless, recently it has been shown to be possible to give a non-trivial certified lower bound of minimum distortion, and some recent progress has been made towards this direction by exploiting the piece-wise linear nature of ReLU activations. However, a generic robustness certification for general activation functions still remains largely unexplored. To address this issue, in this paper we introduce CROWN, a general framework to certify robustness of neural networks with general activation functions. The novelty in our algorithm consists of bounding a given activation function with linear and quadratic functions, hence allowing it to tackle general activation functions including but not limited to the four popular

choices: ReLU, tanh, sigmoid and arctan. In addition, we facilitate the search for a tighter certified lower bound by \textit{adaptively} selecting appropriate surrogates for each neuron activation. Experimental results show that CROWN on ReLU networks can notably improve the certified lower bounds compared to the current state-of-the-art algorithm Fast-Lin, while having comparable computational efficiency. Furthermore, CROWN also demonstrates its effectiveness and flexibility on networks with general activation functions, including tanh, sigmoid and arctan.

Spectral Signatures in Backdoor Attacks

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #148

Brandon Tran · Jerry Li · Aleksander Madry

A recent line of work has uncovered a new form of data poisoning: so-called backdoor attacks. These attacks are particularly dangerous because they do not affect a network's behavior on typical, benign data. Rather, the network only deviates from its expected output when triggered by an adversary's planted perturbation. In this paper, we identify a new property of all known backdoor attacks, which we call spectral signatures. This property allows us to utilize tools from robust statistics to thwart the attacks. We demonstrate the efficacy of these signatures in detecting and removing poisoned examples on real image sets and state of the art neural network architectures. We believe that understanding spectral signatures is a crucial first step towards a principled understanding of backdoor attacks.

Constructing Unrestricted Adversarial Examples with Generative Models

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #149

Yang Song · Rui Shu · Nate Kushman · Stefano Ermon

Adversarial examples are typically constructed by perturbing an existing data point within a small matrix norm, and current defense methods are focused on guarding against this type of attack. In this paper, we propose a new class of adversarial examples that are synthesized entirely from scratch using a conditional generative model, without being restricted to norm-bounded perturbations. We first train an Auxiliary Classifier Generative Adversarial Network (AC-GAN) to model the class-conditional distribution over data samples. Then, conditioned on a desired class, we search over the AC-GAN latent space to find images that are likely under the generative model and are misclassified by a target classifier. We demonstrate through human evaluation that these new kind of adversarial images, which we call Generative Adversarial Examples, are legitimate and belong to the desired class. Our empirical results on the MNIST, SVHN, and CelebA datasets show that generative adversarial examples can bypass strong adversarial training and certified defense

methods designed for traditional adversarial attacks.

Sublinear Time Low-Rank Approximation of Distance Matrices

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #150

Ainesh Bakshi · David Woodruff

Let $PP = \{p_1, p_2, \dots, p_n\}$ and $QQ = \{q_1, q_2, \dots, q_m\}$ be two point sets in an arbitrary metric space. Let AA represent the $m \times n$ pairwise distance matrix with $AA_{\{i,j\}} = d(p_i, q_j)$. Such distance matrices are commonly computed in software packages and have applications to learning image manifolds, handwriting recognition, and multi-dimensional unfolding, among other things. In an attempt to reduce their description size, we study low rank approximation of such matrices. Our main result is to show that for any underlying distance metric d , it is possible to achieve an additive error low rank approximation in sublinear time. We note that it is provably impossible to achieve such a guarantee in sublinear time for arbitrary matrices AA , and our proof exploits special properties of distance matrices. We develop a recursive algorithm based on additive projection-cost preserving sampling. We then show that in general, relative error approximation in sublinear time is impossible for distance matrices, even if one allows for bicriteria solutions. Additionally, we show that if $PP = QQ$ and d is the squared Euclidean distance, which is not a metric but rather the square of a metric, then a relative error bicriteria solution can be found in sublinear time. Finally, we empirically compare our algorithm with the SVD and input sparsity time algorithms. Our algorithm is several hundred times faster than the SVD, and about $8\text{--}20$ times faster than input sparsity methods on real-world and synthetic datasets of size 10^8 . Accuracy-wise, our algorithm is only slightly worse than that of the SVD (optimal) and input-sparsity time algorithms.

Leveraged volume sampling for linear regression

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #151

Michal Dereziński · Manfred Warmuth · Daniel Hsu

Suppose an $n \times d$ design matrix in a linear regression problem is given, but the response for each point is hidden unless explicitly requested. The goal is to sample only a small number $k \ll n$ of the responses, and then produce a weight vector whose sum of squares loss over all points is at most $1 + \epsilon$ times the minimum. When k is very small (e.g., $k = d$), jointly sampling diverse subsets of points is crucial. One such method called "volume sampling" has a unique and desirable property that the weight vector it produces is an unbiased estimate of the optimum. It is therefore natural to ask if this method offers the optimal unbiased estimate in terms of the number of responses k

needed to achieve a $1+\epsilon$ loss approximation. Surprisingly we show that volume sampling can have poor behavior when we require a very accurate approximation -- indeed worse than some i.i.d. sampling techniques whose estimates are biased, such as leverage score sampling. We then develop a new rescaled variant of volume sampling that produces an unbiased estimate which avoids this bad behavior and has at least as good a tail bound as leverage score sampling: sample size $k=O(d \log d + d/\epsilon)$ suffices to guarantee total loss at most $1+\epsilon$ times the minimum with high probability. Thus, we improve on the best previously known sample size for an unbiased estimator, $k=O(d^2/\epsilon)$. Our rescaling procedure leads to a new efficient algorithm for volume sampling which is based on a "determinantal rejection sampling" technique with potentially broader applications to determinantal point processes. Other contributions include introducing the combinatorics needed for rescaled volume sampling and developing tail bounds for sums of dependent random matrices which arise in the process.

Revisiting (ϵ, γ, τ) -similarity learning for domain adaptation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #152

Sofiane Dhouib · Ievgen Redko

Similarity learning is an active research area in machine learning that tackles the problem of finding a similarity function tailored to an observable data sample in order to achieve efficient classification. This learning scenario has been generally formalized by the means of a (ϵ, γ, τ) -good similarity learning framework in the context of supervised classification and has been shown to have strong theoretical guarantees. In this paper, we propose to extend the theoretical analysis of similarity learning to the domain adaptation setting, a particular situation occurring when the similarity is learned and then deployed on samples following different probability distributions. We give a new definition of an (ϵ, γ) -good similarity for domain adaptation and prove several results quantifying the performance of a similarity function on a target domain after it has been trained on a source domain. We particularly show that if the source distribution dominates the target one, then principally new domain adaptation learning bounds can be proved.

Differential Properties of Sinkhorn Approximation for Learning with Wasserstein Distance

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #153

Giulia Luise · Alessandro Rudi · Massimiliano Pontil · Carlo Ciliberto

Applications of optimal transport have recently gained remarkable attention as a result of the computational advantages of entropic regularization. However, in most situations the Sinkhorn

approximation to the Wasserstein distance is replaced by a regularized version that is less accurate but easy to differentiate. In this work we characterize the differential properties of the original Sinkhorn approximation, proving that it enjoys the same smoothness as its regularized version and we explicitly provide an efficient algorithm to compute its gradient. We show that this result benefits both theory and applications: on one hand, high order smoothness confers statistical guarantees to learning with Wasserstein approximations. On the other hand, the gradient formula allows to efficiently solve learning and optimization problems in practice. Promising preliminary experiments complement our analysis.

Algorithms and Theory for Multiple-Source Adaptation

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #154

Judy Hoffman · Mehryar Mohri · Ningshan Zhang

We present a number of novel contributions to the multiple-source adaptation problem. We derive new normalized solutions with strong theoretical guarantees for the cross-entropy loss and other similar losses. We also provide new guarantees that hold in the case where the conditional probabilities for the source domains are distinct. Moreover, we give new algorithms for determining the distribution-weighted combination solution for the cross-entropy loss and other losses. We report the results of a series of experiments with real-world datasets. We find that our algorithm outperforms competing approaches by producing a single robust model that performs well on any target mixture distribution. Altogether, our theory, algorithms, and empirical results provide a full solution for the multiple-source adaptation problem with very practical benefits.

Synthesize Policies for Transfer and Adaptation across Tasks and Environments

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #155

Hexiang Hu · Liyu Chen · Boqing Gong · Fei Sha

The ability to transfer in reinforcement learning is key towards building an agent of general artificial intelligence. In this paper, we consider the problem of learning to simultaneously transfer across both environments and tasks, probably more importantly, by learning from only sparse (environment, task) pairs out of all the possible combinations. We propose a novel compositional neural network architecture which depicts a meta rule for composing policies from environment and task embeddings. Notably, one of the main challenges is to learn the embeddings jointly with the meta rule. We further propose new training methods to disentangle the embeddings, making them both distinctive signatures of the environments and tasks and effective building blocks for composing the policies. Experiments on GridWorld and THOR, of which the agent takes as input an

egocentric view, show that our approach gives rise to high success rates on all the (environment, task) pairs after learning from only 40% of them.

Acceleration through Optimistic No-Regret Dynamics

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #156

Jun-Kun Wang · Jacob Abernethy

We consider the problem of minimizing a smooth convex function by reducing the optimization to computing the Nash equilibrium of a particular zero-sum convex-concave game. Zero-sum games can be solved using online learning dynamics, where a classical technique involves simulating two no-regret algorithms that play against each other and, after T rounds, the average iterate is guaranteed to solve the original optimization problem with error decaying as $O(\log T/T)$. In this paper we show that the technique can be enhanced to a rate of $O(1/T^2)$ by extending recent work \cite{RS13,SALS15} that leverages \textit{optimistic learning} to speed up equilibrium computation. The resulting optimization algorithm derived from this analysis coincides \textit{exactly} with the well-known \NA \cite{N83a} method, and indeed the same story allows us to recover several variants of the Nesterov's algorithm via small tweaks. We are also able to establish the accelerated linear rate for a function which is both strongly-convex and smooth. This methodology unifies a number of different iterative optimization methods: we show that the \HB algorithm is precisely the non-optimistic variant of \NA, and recent prior work already established a similar perspective on \FW \cite{AW17,ALLW18}.

Efficient Online Portfolio with Logarithmic Regret

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #157

Haipeng Luo · Chen-Yu Wei · Kai Zheng

We study the decades-old problem of online portfolio management and propose the first algorithm with logarithmic regret that is not based on Cover's Universal Portfolio algorithm and admits much faster implementation. Specifically Universal Portfolio enjoys optimal regret $\mathcal{O}(N \ln T)$ for N financial instruments over T rounds, but requires log-concave sampling and has a large polynomial running time. Our algorithm, on the other hand, ensures a slightly larger but still logarithmic regret of $\mathcal{O}(N^2 (\ln T)^4)$, and is based on the well-studied Online Mirror Descent framework with a novel regularizer that can be implemented via standard optimization methods in time $\mathcal{O}(TN^{2.5})$ per round. The regret of all other existing works is either polynomial in T or has a potentially unbounded factor such as the inverse of the smallest price relative.

Almost Optimal Algorithms for Linear Stochastic Bandits with Heavy-Tailed Payoffs

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #158

Han Shao · Xiaotian Yu · Irwin King · Michael Lyu

In linear stochastic bandits, it is commonly assumed that payoffs are with sub-Gaussian noises. In this paper, under a weaker assumption on noises, we study the problem of $\text{linear stochastic bandits with heavy-tailed payoffs}$ (LinBET), where the distributions have finite moments of order $1+\epsilon$, for some $\epsilon \in (0,1]$. We rigorously analyze the regret lower bound of LinBET as $\Omega(T^{\frac{1}{1+\epsilon}})$, implying that finite moments of order 2 (i.e., finite variances) yield the bound of $\Omega(\sqrt{T})$, with T being the total number of rounds to play bandits. The provided lower bound also indicates that the state-of-the-art algorithms for LinBET are far from optimal. By adopting median of means with a well-designed allocation of decisions and truncation based on historical information, we develop two novel bandit algorithms, where the regret upper bounds match the lower bound up to polylogarithmic factors. To the best of our knowledge, we are the first to solve LinBET optimally in the sense of the polynomial order on T . Our proposed algorithms are evaluated based on synthetic datasets, and outperform the state-of-the-art results.

A Smoothed Analysis of the Greedy Algorithm for the Linear Contextual Bandit Problem

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #159

Sampath Kannan · Jamie Morgenstern · Aaron Roth · Bo Waggoner · Zhiwei Steven Wu

Bandit learning is characterized by the tension between long-term exploration and short-term exploitation. However, as has recently been noted, in settings in which the choices of the learning algorithm correspond to important decisions about individual people (such as criminal recidivism prediction, lending, and sequential drug trials), exploration corresponds to explicitly sacrificing the well-being of one individual for the potential future benefit of others. In such settings, one might like to run a greedy algorithm, which always makes the optimal decision for the individuals at hand --- but doing this can result in a catastrophic failure to learn. In this paper, we consider the linear contextual bandit problem and revisit the performance of the greedy algorithm. We give a smoothed analysis, showing that even when contexts may be chosen by an adversary, small perturbations of the adversary's choices suffice for the algorithm to achieve no regret, perhaps (depending on the specifics of the setting) with a constant amount of initial training data. This suggests that in slightly perturbed environments,

exploration and exploitation need not be in conflict in the linear setting.

Exploration in Structured Reinforcement Learning

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #160

Jungseul Ok · Alexandre Proutiere · Damianos Tranos

We address reinforcement learning problems with finite state and action spaces where the underlying MDP has some known structure that could be potentially exploited to minimize the exploration rates of suboptimal (state, action) pairs. For any arbitrary structure, we derive problem-specific regret lower bounds satisfied by any learning algorithm. These lower bounds are made explicit for unstructured MDPs and for those whose transition probabilities and average reward functions are Lipschitz continuous w.r.t. the state and action. For Lipschitz MDPs, the bounds are shown not to scale with the sizes S and A of the state and action spaces, i.e., they are smaller than $c \log T$ where T is the time horizon and the constant c only depends on the Lipschitz structure, the span of the bias function, and the minimal action sub-optimality gap. This contrasts with unstructured MDPs where the regret lower bound typically scales as $SA \log T$. We devise DEL (Directed Exploration Learning), an algorithm that matches our regret lower bounds. We further simplify the algorithm for Lipschitz MDPs, and show that the simplified version is still able to efficiently exploit the structure.

Near Optimal Exploration-Exploitation in Non-Communicating Markov Decision Processes

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #161

Ronan Fruit · Matteo Pirota · Alessandro Lazaric

While designing the state space of an MDP, it is common to include states that are transient or not reachable by any policy (e.g., in mountain car, the product space of speed and position contains configurations that are not physically reachable). This results in weakly-communicating or multi-chain MDPs. In this paper, we introduce TUCRL, the first algorithm able to perform efficient exploration-exploitation in any finite Markov Decision Process (MDP) without requiring any form of prior knowledge. In particular, for any MDP with S^c communicating states, A actions and $|\Gamma^c| \leq S^c$ possible communicating next states, we derive a $O(D^c \sqrt{|\Gamma^c| S^c A T})$ regret bound, where D^c is the diameter (i.e., the length of the longest shortest path between any two states) of the communicating part of the MDP. This is in contrast with optimistic algorithms (e.g., UCRL, Optimistic PSRL) that suffer linear regret in weakly-communicating MDPs, as well as posterior sampling or regularised algorithms (e.g., REGAL), which require prior knowledge on the bias span of the optimal policy to bias the exploration to achieve sub-linear regret.

We also prove that in weakly-communicating MDPs, no algorithm can ever achieve a logarithmic growth of the regret without first suffering a linear regret for a number of steps that is exponential in the parameters of the MDP. Finally, we report numerical simulations supporting our theoretical findings and showing how TUCRL overcomes the limitations of the state-of-the-art.

A Block Coordinate Ascent Algorithm for Mean-Variance Optimization

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #162

Tengyang Xie · Bo Liu · Yangyang Xu · Mohammad Ghavamzadeh · Yinlam Chow · Daoming Lyu · Daesub Yoon

Risk management in dynamic decision problems is a primary concern in many fields, including financial investment, autonomous driving, and healthcare. The mean-variance function is one of the most widely used objective functions in risk management due to its simplicity and interpretability. Existing algorithms for mean-variance optimization are based on multi-time-scale stochastic approximation, whose learning rate schedules are often hard to tune, and have only asymptotic convergence proof. In this paper, we develop a model-free policy search framework for mean-variance optimization with finite-sample error bound analysis (to local optima). Our starting point is a reformulation of the original mean-variance function with its Fenchel dual, from which we propose a stochastic block coordinate ascent policy search algorithm. Both the asymptotic convergence guarantee of the last iteration's solution and the convergence rate of the randomly picked solution are provided, and their applicability is demonstrated on several benchmark domains.

Learning Safe Policies with Expert Guidance

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #163

Jessie Huang · Fa Wu · Doina Precup · Yang Cai

We propose a framework for ensuring safe behavior of a reinforcement learning agent when the reward function may be difficult to specify. In order to do this, we rely on the existence of demonstrations from expert policies, and we provide a theoretical framework for the agent to optimize in the space of rewards consistent with its existing knowledge. We propose two methods to solve the resulting optimization: an exact ellipsoid-based method and a method in the spirit of the "follow-the-perturbed-leader" algorithm. Our experiments demonstrate the behavior of our algorithm in both discrete and continuous problems. The trained agent safely avoids states with potential negative effects while imitating the behavior of the expert in the other states.

M-Walk: Learning to Walk over Graphs using Monte Carlo Tree Search

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #164

Yelong Shen · Jianshu Chen · Po-Sen Huang · Yuqing Guo · Jianfeng Gao

Learning to walk over a graph towards a target node for a given query and a source node is an important problem in applications such as knowledge base completion (KBC). It can be formulated as a reinforcement learning (RL) problem with a known state transition model. To overcome the challenge of sparse rewards, we develop a graph-walking agent called M-Walk, which consists of a deep recurrent neural network (RNN) and Monte Carlo Tree Search (MCTS). The RNN encodes the state (i.e., history of the walked path) and maps it separately to a policy and Q-values. In order to effectively train the agent from sparse rewards, we combine MCTS with the neural policy to generate trajectories yielding more positive rewards. From these trajectories, the network is improved in an off-policy manner using Q-learning, which modifies the RNN policy via parameter sharing. Our proposed RL algorithm repeatedly applies this policy-improvement step to learn the model. At test time, MCTS is combined with the neural policy to predict the target node. Experimental results on several graph-walking benchmarks show that M-Walk is able to learn better policies than other RL-based methods, which are mainly based on policy gradients. M-Walk also outperforms traditional KBC baselines.

Is Q-Learning Provably Efficient?

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #165

Chi Jin · Zeyuan Allen-Zhu · Sebastien Bubeck · Michael Jordan

Model-free reinforcement learning (RL) algorithms directly parameterize and update value functions or policies, bypassing the modeling of the environment. They are typically simpler, more flexible to use, and thus more prevalent in modern deep RL than model-based approaches. However, empirical work has suggested that they require large numbers of samples to learn. The theoretical question of whether not model-free algorithms are in fact *sample efficient* is one of the most fundamental questions in RL. The problem is unsolved even in the basic scenario with finitely many states and actions. We prove that, in an episodic MDP setting, Q-learning with UCB exploration achieves regret $\tilde{O}(\sqrt{H^3 SAT})$ where S and A are the numbers of states and actions, H is the number of steps per episode, and T is the total number of steps. Our regret matches the optimal regret up to a single \sqrt{H} factor. Thus we establish the sample efficiency of a classical model-free approach. Moreover, to the best of our knowledge, this is the first model-free analysis to establish \sqrt{T} regret *without* requiring access to a "simulator."

Variational Inverse Control with Events: A General Framework for Data-Driven Reward Definition

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #166

Justin Fu · Avi Singh · Dibya Ghosh · Larry Yang · Sergey Levine

The design of a reward function often poses a major practical challenge to real-world applications of reinforcement learning. Approaches such as inverse reinforcement learning attempt to overcome this challenge, but require expert demonstrations, which can be difficult or expensive to obtain in practice. We propose inverse event-based control, which generalizes inverse reinforcement learning methods to cases where full demonstrations are not needed, such as when only samples of desired goal states are available. Our method is grounded in an alternative perspective on control and reinforcement learning, where an agent's goal is to maximize the probability that one or more events will happen at some point in the future, rather than maximizing cumulative rewards. We demonstrate the effectiveness of our methods on continuous control tasks, with a focus on high-dimensional observations like images where rewards are hard or even impossible to specify.

An Off-policy Policy Gradient Theorem Using Emphatic Weightings

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #167

Ehsan Imani · Eric Graves · Martha White

Policy gradient methods are widely used for control in reinforcement learning, particularly for the continuous action setting. There have been a host of theoretically sound algorithms proposed for the on-policy setting, due to the existence of the policy gradient theorem which provides a simplified form for the gradient. In off-policy learning, however, where the behaviour policy is not necessarily attempting to learn and follow the optimal policy for the given task, the existence of such a theorem has been elusive. In this work, we solve this open problem by providing the first off-policy policy gradient theorem. The key to the derivation is the use of emphatic weightings. We develop a new actor-critic algorithm—called Actor Critic with Emphatic weightings (ACE)—that approximates the simplified gradients provided by the theorem. We demonstrate in a simple counterexample that previous off-policy policy gradient methods—particularly OffPAC and DPG—converge to the wrong solution whereas ACE finds the optimal solution.

Near-Optimal Time and Sample Complexities for Solving Markov Decision Processes with a Generative Model

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #168

Aaron Sidford · Mengdi Wang · Xian Wu · Lin Yang · Yinyu Ye

In this paper we consider the problem of computing an ϵ -optimal policy of a discounted Markov Decision Process (MDP) provided we can only access its transition function through a generative sampling model that given any state-action pair samples from the transition function in $O(1)$ time. Given such a MDP with states S , actions A , discount factor $\gamma \in (0, 1)$, and rewards in range $[0, 1]$ we provide an algorithm which computes an ϵ -optimal policy with probability $1 - \delta$ where both the run time spent and number of sample taken is upper bounded by $O\left(\frac{|S||A|}{(1-\gamma)^3 \epsilon^2} \log\left(\frac{|S||A|}{(1-\gamma)\delta \epsilon}\right) \log\left(\frac{1}{(1-\gamma)\epsilon}\right)\right) \sim$.] For fixed values of ϵ , this improves upon the previous best known bounds by a factor of $(1 - \gamma)^{-1}$ and matches the sample complexity lower bounds proved in \cite{azar2013minimax} up to logarithmic factors. We also extend our method to computing ϵ -optimal policies for finite-horizon MDP with a generative model and provide a nearly matching sample complexity lower bound.

Monte-Carlo Tree Search for Constrained POMDPs

Poster | Wed Dec 5th 10:45 AM -- 12:45 PM @ Room 210 & 230 AB #169

Jongmin Lee · Geon-hyeong Kim · Pascal Poupart · Kee-Eung Kim

Monte-Carlo Tree Search (MCTS) has been successfully applied to very large POMDPs, a standard model for stochastic sequential decision-making problems. However, many real-world problems inherently have multiple goals, where multi-objective formulations are more natural. The constrained POMDP (CPOMDP) is such a model that maximizes the reward while constraining the cost, extending the standard POMDP model. To date, solution methods for CPOMDPs assume an explicit model of the environment, and thus are hardly applicable to large-scale real-world problems. In this paper, we present CC-POMCP (Cost-Constrained POMCP), an online MCTS algorithm for large CPOMDPs that leverages the optimization of LP-induced parameters and only requires a black-box simulator of the environment. In the experiments, we demonstrate that CC-POMCP converges to the optimal stochastic action selection in CPOMDP and pushes the state-of-the-art by being able to scale to very large problems.

Investigations into the Human-AI Trust Phenomenon

Invited Talk | Wed Dec 5th 02:15 -- 03:05 PM @ Rooms 220 CDE

Ayanna Howard

As intelligent systems become more fully interactive with humans during the performance of our day-to-day activities, the role of trust must be examined more carefully. Trust conveys the concept that when interacting with intelligent systems, humans tend to exhibit similar behaviors as when interacting with other humans and thus may misunderstand the risks associated with deferring their decisions to a machine. Bias further impacts this potential risk for trust, or overtrust, in that these systems are learning by mimicking our own thinking processes, inheriting our own implicit biases. In this talk, we will discuss this phenomenon through the lens of intelligent systems that interact with people in scenarios that are realizable in the near-term.

Coffee Break

Break | Wed Dec 5th 03:05 -- 03:30 PM @

Breaking the Curse of Horizon: Infinite-Horizon Off-Policy Estimation

Spotlight | Wed Dec 5th 03:30 -- 03:35 PM @ Room 220 CD

Qiang Liu · Lihong Li · Ziyang Tang · Dengyong Zhou

We consider the off-policy estimation problem of estimating the expected reward of a target policy using samples collected by a different behavior policy. Importance sampling (IS) has been a key technique to derive (nearly) unbiased estimators, but is known to suffer from an excessively high variance in long-horizon problems. In the extreme case of infinite-horizon problems, the variance of an IS-based estimator may even be unbounded. In this paper, we propose a new off-policy estimation method that applies IS directly on the stationary state-visitation distributions to avoid the exploding variance issue faced by existing estimators. Our key contribution is a novel approach to estimating the density ratio of two stationary distributions, with trajectories sampled from only the behavior distribution. We develop a mini-max loss function for the estimation problem, and derive a closed-form solution for the case of RKHS. We support our method with both theoretical and empirical analyses.

Dynamic Network Model from Partial Observations

Spotlight | Wed Dec 5th 03:30 -- 03:35 PM @ Room 220 E

Elahe Ghalebi · Baharan Mirzasoleiman · Radu Grosu · Jure Leskovec

Can evolving networks be inferred and modeled without directly observing their nodes and edges? In many applications, the edges of a dynamic network might not be observed, but one can observe the dynamics of stochastic cascading processes (e.g., information diffusion, virus propagation) occurring over the unobserved network. While there have been efforts to infer networks based on such data, providing a generative probabilistic model that is able to identify the underlying time-varying network remains an open question. Here we consider the problem of inferring generative dynamic network models based on network cascade diffusion data. We propose a novel framework for providing a non-parametric dynamic network model---based on a mixture of coupled hierarchical Dirichlet processes---based on data capturing cascade node infection times. Our approach allows us to infer the evolving community structure in networks and to obtain an explicit predictive distribution over the edges of the underlying network---including those that were not involved in transmission of any cascade, or are likely to appear in the future. We show the effectiveness of our approach using extensive experiments on synthetic as well as real-world networks.

The Nearest Neighbor Information Estimator is Adaptively Near Minimax Rate-Optimal

Spotlight | Wed Dec 5th 03:30 -- 03:35 PM @ Room 517 CD

Jiantao Jiao · Weihao Gao · Yanjun Han

We analyze the Kozachenko-Leonenko (KL) fixed k-nearest neighbor estimator for the differential entropy. We obtain the first uniform upper bound on its performance for any fixed k over $H^{\{o\}}$ -balls on a torus without assuming any conditions on how close the density could be from zero. Accompanying a recent minimax lower bound over the $H^{\{o\}}$ -ball, we show that the KL estimator for any fixed k is achieving the minimax rates up to logarithmic factors without cognizance of the smoothness parameter s of the $H^{\{o\}}$ -ball for $s \in (0, 2]$ and arbitrary dimension d , rendering it the first estimator that provably satisfies this property.

Graph Convolutional Policy Network for Goal-Directed Molecular Graph Generation

Spotlight | Wed Dec 5th 03:35 -- 03:40 PM @ Room 220 CD

Jiaxuan You · Bowen Liu · Zhitao Ying · Vijay Pande · Jure Leskovec

Generating novel graph structures that optimize given objectives while obeying some given underlying rules is fundamental for chemistry, biology and social science research. This is especially important in the task of molecular graph generation, whose goal is to discover novel molecules with desired properties such as drug-likeness and synthetic accessibility, while obeying physical laws such as chemical valency. However, designing models that finds molecules that optimize desired properties while incorporating highly complex and non-differentiable rules remains to be a challenging task. Here we propose Graph Convolutional Policy Network (GCPN), a general graph convolutional network based model for goal-directed graph generation through reinforcement learning. The model is trained to optimize domain-specific rewards and adversarial loss through policy gradient, and acts in an environment that incorporates domain-specific rules. Experimental results show that GCPN can achieve 61% improvement on chemical property optimization over state-of-the-art baselines while resembling known molecules, and achieve 184% improvement on the constrained property optimization task.

Stochastic Nonparametric Event-Tensor Decomposition

Spotlight | Wed Dec 5th 03:35 -- 03:40 PM @ Room 220 E

Shandian Zhe · Yishuai Du

Tensor decompositions are fundamental tools for multiway data analysis. Existing approaches, however, ignore the valuable temporal information along with data, or simply discretize them into time steps so that important temporal patterns are easily missed. Moreover, most methods are limited to multilinear decomposition forms, and hence are unable to capture intricate, nonlinear relationships in data. To address these issues, we formulate event-tensors, to preserve the complete temporal information for multiway data, and propose a novel Bayesian nonparametric decomposition model. Our model can (1) fully exploit the time stamps to capture the critical, causal/triggering effects between the interaction events, (2) flexibly estimate the complex relationships between the entities in tensor modes, and (3) uncover hidden structures from their temporal interactions. For scalable inference, we develop a doubly stochastic variational Expectation-Maximization algorithm to conduct an online decomposition. Evaluations on both synthetic and real-world datasets show that our model not only improves upon the predictive performance of existing methods, but also discovers interesting clusters underlying the data.

Contextual Stochastic Block Models

Spotlight | Wed Dec 5th 03:35 -- 03:40 PM @ Room 517 CD

Yash Deshpande · Subhabrata Sen · Andrea Montanari · Elchanan Mossel

We provide the first information theoretical tight analysis for inference of latent community

structure given a sparse graph along with high dimensional node covariates, correlated with the same latent communities. Our work bridges recent theoretical breakthroughs in detection of latent community structure without nodes covariates and a large body of empirical work using diverse heuristics for combining node covariates with graphs for inference. The tightness of our analysis implies in particular, the information theoretic necessity of combining the different sources of information. Our analysis holds for networks of large degrees as well as for a Gaussian version of the model.

Memory Augmented Policy Optimization for Program Synthesis and Semantic Parsing

Spotlight | Wed Dec 5th 03:40 -- 03:45 PM @ Room 220 CD

Chen Liang · Mohammad Norouzi · Jonathan Berant · Quoc V Le · Ni Lao

We present Memory Augmented Policy Optimization (MAPO), a simple and novel way to leverage a memory buffer of promising trajectories to reduce the variance of policy gradient estimate. MAPO is applicable to deterministic environments with discrete actions, such as structured prediction and combinatorial optimization tasks. We express the expected return objective as a weighted sum of two terms: an expectation over the high-reward trajectories inside the memory buffer, and a separate expectation over trajectories outside the buffer. To make an efficient algorithm of MAPO, we propose: (1) memory weight clipping to accelerate and stabilize training; (2) systematic exploration to discover high-reward trajectories; (3) distributed sampling from inside and outside of the memory buffer to scale up training. MAPO improves the sample efficiency and robustness of policy gradient, especially on tasks with sparse rewards. We evaluate MAPO on weakly supervised program synthesis from natural language (semantic parsing). On the WikiTableQuestions benchmark, we improve the state-of-the-art by 2.6%, achieving an accuracy of 46.3%. On the WikiSQL benchmark, MAPO achieves an accuracy of 74.9% with only weak supervision, outperforming several strong baselines with full supervision. Our source code is available at <https://goo.gl/TXBp4e>

On GANs and GMMs

Spotlight | Wed Dec 5th 03:40 -- 03:45 PM @ Room 220 E

Eitan Richardson · Yair Weiss

A longstanding problem in machine learning is to find unsupervised methods that can learn the statistical structure of high dimensional signals. In recent years, GANs have gained much attention as a possible solution to the problem, and in particular have shown the ability to generate remarkably realistic high resolution sampled images. At the same time, many authors have pointed

out that GANs may fail to model the full distribution ("mode collapse") and that using the learned models for anything other than generating samples may be very difficult. In this paper, we examine the utility of GANs in learning statistical models of images by comparing them to perhaps the simplest statistical model, the Gaussian Mixture Model. First, we present a simple method to evaluate generative models based on relative proportions of samples that fall into predetermined bins. Unlike previous automatic methods for evaluating models, our method does not rely on an additional neural network nor does it require approximating intractable computations. Second, we compare the performance of GANs to GMMs trained on the same datasets. While GMMs have previously been shown to be successful in modeling small patches of images, we show how to train them on full sized images despite the high dimensionality. Our results show that GMMs can generate realistic samples (although less sharp than those of GANs) but also capture the full distribution, which GANs fail to do. Furthermore, GMMs allow efficient inference and explicit representation of the underlying statistical structure. Finally, we discuss how GMMs can be used to generate sharp images.

Entropy Rate Estimation for Markov Chains with Large State Space

Spotlight | Wed Dec 5th 03:40 -- 03:45 PM @ Room 517 CD

Yanjun Han · Jiantao Jiao · Chuan-Zheng Lee · Tsachy Weissman · Yihong Wu · Tiancheng Yu

Entropy estimation is one of the prototypical problems in distribution property testing. To consistently estimate the Shannon entropy of a distribution on S elements with independent samples, the optimal sample complexity scales sublinearly with S as $\Theta(\frac{S}{\log S})$ as shown by Valiant and Valiant [Valiant-Valiant2011]. Extending the theory and algorithms for entropy estimation to dependent data, this paper considers the problem of estimating the entropy rate of a stationary reversible Markov chain with S states from a sample path of n observations. We show that

- Provided the Markov chain mixes not too slowly, i.e., the relaxation time is at most $O(\frac{S}{\ln^3 S})$, consistent estimation is achievable when $n \gg \frac{S^2}{\log S}$.
- Provided the Markov chain has some slight dependency, i.e., the relaxation time is at least $1 + \Omega(\frac{\ln^2 S}{\sqrt{S}})$, consistent estimation is impossible when $n \lesssim \frac{S^2}{\log S}$.

Under both assumptions, the optimal estimation accuracy is shown to be $\Theta(\frac{S^2}{n \log S})$. In comparison, the empirical entropy rate requires at least $\Omega(S^2)$ samples to be consistent, even when the Markov chain is memoryless. In addition to synthetic experiments, we also apply the estimators that achieve the optimal sample complexity to estimate the entropy rate of the English language in the Penn Treebank and the Google One Billion Words corpora, which provides a natural benchmark for language modeling and relates it directly to the widely used perplexity measure.

Meta-Reinforcement Learning of Structured Exploration Strategies

Spotlight | Wed Dec 5th 03:45 -- 03:50 PM @ Room 220 CD

Abhishek Gupta · Russell Mendonca · YuXuan Liu · Pieter Abbeel · Sergey Levine

Exploration is a fundamental challenge in reinforcement learning (RL). Many current exploration methods for deep RL use task-agnostic objectives, such as information gain or bonuses based on state visitation. However, many practical applications of RL involve learning more than a single task, and prior tasks can be used to inform how exploration should be performed in new tasks. In this work, we study how prior tasks can inform an agent about how to explore effectively in new situations. We introduce a novel gradient-based fast adaptation algorithm – model agnostic exploration with structured noise (MAESN) – to learn exploration strategies from prior experience. The prior experience is used both to initialize a policy and to acquire a latent exploration space that can inject structured stochasticity into a policy, producing exploration strategies that are informed by prior knowledge and are more effective than random action-space noise. We show that MAESN is more effective at learning exploration strategies when compared to prior meta-RL methods, RL without learned exploration strategies, and task-agnostic exploration methods. We evaluate our method on a variety of simulated tasks: locomotion with a wheeled robot, locomotion with a quadrupedal walker, and object manipulation.

GILBO: One Metric to Measure Them All

Spotlight | Wed Dec 5th 03:45 -- 03:50 PM @ Room 220 E

Alexander Alemi · Ian Fischer

We propose a simple, tractable lower bound on the mutual information contained in the joint generative density of any latent variable generative model: the GILBO (Generative Information Lower Bound). It offers a data-independent measure of the complexity of the learned latent variable description, giving the log of the effective description length. It is well-defined for both VAEs and GANs. We compute the GILBO for 800 GANs and VAEs each trained on four datasets (MNIST, FashionMNIST, CIFAR-10 and CelebA) and discuss the results.

Blind Deconvolutional Phase Retrieval via Convex Programming

Spotlight | Wed Dec 5th 03:45 -- 03:50 PM @ Room 517 CD

Ali Ahmed · Alireza Aghasi · Paul Hand

We consider the task of recovering two real or complex m -vectors from phaseless Fourier measurements of their circular convolution. Our method is a novel convex relaxation that is based on a lifted matrix recovery formulation that allows a nontrivial convex relaxation of the bilinear measurements from convolution. We prove that if the two signals belong to known random subspaces of dimensions k and n , then they can be recovered up to the inherent scaling ambiguity with $m \gg (k+n) \log^2 m$ phaseless measurements. Our method provides the first theoretical recovery guarantee for this problem by a computationally efficient algorithm and does not require a solution estimate to be computed for initialization. Our proof is based Rademacher complexity estimates. Additionally, we provide an ADMM implementation of the method and provide numerical experiments that verify the theory.

Policy Optimization via Importance Sampling

Oral | Wed Dec 5th 03:50 -- 04:05 PM @ Room 220 CD

Alberto Maria Metelli · Matteo Papini · Francesco Faccio · Marcello Restelli

Policy optimization is an effective reinforcement learning approach to solve continuous control tasks. Recent achievements have shown that alternating online and offline optimization is a successful choice for efficient trajectory reuse. However, deciding when to stop optimizing and collect new trajectories is non-trivial, as it requires to account for the variance of the objective function estimate. In this paper, we propose a novel, model-free, policy search algorithm, POIS, applicable in both action-based and parameter-based settings. We first derive a high-confidence bound for importance sampling estimation; then we define a surrogate objective function, which is optimized offline whenever a new batch of trajectories is collected. Finally, the algorithm is tested on a selection of continuous control tasks, with both linear and deep policies, and compared with state-of-the-art policy optimization methods.

Isolating Sources of Disentanglement in Variational Autoencoders

Oral | Wed Dec 5th 03:50 -- 04:05 PM @ Room 220 E

Tian Qi Chen · Xuechen Li · Roger Grosse · David Duvenaud

We decompose the evidence lower bound to show the existence of a term measuring the total correlation between latent variables. We use this to motivate the beta-TCVAE (Total Correlation Variational Autoencoder) algorithm, a refinement and plug-in replacement of the beta-VAE for learning disentangled representations, requiring no additional hyperparameters during training. We further propose a principled classifier-free measure of disentanglement called the mutual information gap (MIG). We perform extensive quantitative and qualitative experiments, in both

restricted and non-restricted settings, and show a strong relation between total correlation and disentanglement, when the model is trained using our framework.

Stochastic Cubic Regularization for Fast Nonconvex Optimization

Oral | Wed Dec 5th 03:50 -- 04:05 PM @ Room 517 CD

Nilesh Tripuraneni · Mitchell Stern · Chi Jin · Jeffrey Regier · Michael Jordan

This paper proposes a stochastic variant of a classic algorithm---the cubic-regularized Newton method [Nesterov and Polyak]. The proposed algorithm efficiently escapes saddle points and finds approximate local minima for general smooth, nonconvex functions in only $\tilde{O}(\epsilon^{-3.5})$ stochastic gradient and stochastic Hessian-vector product evaluations. The latter can be computed as efficiently as stochastic gradients. This improves upon the $\tilde{O}(\epsilon^{-4})$ rate of stochastic gradient descent. Our rate matches the best-known result for finding local minima without requiring any delicate acceleration or variance-reduction techniques.

A Bayesian Approach to Generative Adversarial Imitation Learning

Spotlight | Wed Dec 5th 04:05 -- 04:10 PM @ Room 220 CD

Wonseok Jeon · Seokin Seo · Kee-Eung Kim

Generative adversarial training for imitation learning has shown promising results on high-dimensional and continuous control tasks. This paradigm is based on reducing the imitation learning problem to the density matching problem, where the agent iteratively refines the policy to match the empirical state-action visitation frequency of the expert demonstration. Although this approach has shown to robustly learn to imitate even with scarce demonstration, one must still address the inherent challenge that collecting trajectory samples in each iteration is a costly operation. To address this issue, we first propose a Bayesian formulation of generative adversarial imitation learning (GAIL), where the imitation policy and the cost function are represented as stochastic neural networks. Then, we show that we can significantly enhance the sample efficiency of GAIL leveraging the predictive density of the cost, on an extensive set of imitation learning tasks with high-dimensional states and actions.

Sparse Covariance Modeling in High Dimensions with Gaussian Processes

Spotlight | Wed Dec 5th 04:05 -- 04:10 PM @ Room 220 E

Rui Li · Kishan KC · Feng Cui · Justin Domke · Anne Haake

This paper studies statistical relationships among components of high-dimensional observations varying across non-random covariates. We propose to model the observation elements' changing covariances as sparse multivariate stochastic processes. In particular, our novel covariance modeling method reduces dimensionality by relating the observation vectors to a lower dimensional subspace. To characterize the changing correlations, we jointly model the latent factors and the factor loadings as collections of basis functions that vary with the covariates as Gaussian processes. Automatic relevance determination (ARD) encodes basis sparsity through their coefficients to account for the inherent redundancy. Experiments conducted across domains show superior performances to the state-of-the-art methods.

Stochastic Nested Variance Reduced Gradient Descent for Nonconvex Optimization

Spotlight | Wed Dec 5th 04:05 -- 04:10 PM @ Room 517 CD

Dongruo Zhou · Pan Xu · Quanquan Gu

We study finite-sum nonconvex optimization problems, where the objective function is an average of n nonconvex functions. We propose a new stochastic gradient descent algorithm based on nested variance reduction. Compared with conventional stochastic variance reduced gradient (SVRG) algorithm that uses two reference points to construct a semi-stochastic gradient with diminishing variance in each epoch, our algorithm uses $K+1$ nested reference points to build an semi-stochastic gradient to further reduce its variance in each epoch. For smooth functions, the proposed algorithm converges to an approximate first order stationary point (i.e., $\|\nabla F(\mathbf{x})\|_2 \leq \epsilon$) within $\mathcal{O}(n \log \frac{1}{\epsilon} + \frac{n^2}{\epsilon})$ number of stochastic gradient evaluations, where n is the number of component functions, and ϵ is the optimization error. This improves the best known gradient complexity of SVRG $\mathcal{O}(n + \frac{n^2}{\epsilon})$ and the best gradient complexity of SCSG $\mathcal{O}(\frac{n^2}{\epsilon^{1/3}} + \frac{n}{\epsilon})$. For gradient dominated functions, our algorithm achieves $\mathcal{O}(n \log \frac{1}{\epsilon} + \frac{n^2}{\epsilon})$ gradient complexity, which again beats the existing best gradient complexity $\mathcal{O}(n \log \frac{1}{\epsilon} + \frac{n^2}{\epsilon})$ achieved by SCSG. Thorough experimental results on different nonconvex optimization problems back up our theory.

Visual Reinforcement Learning with Imagined Goals

Spotlight | Wed Dec 5th 04:10 -- 04:15 PM @ Room 220 CD

Ashvin Nair · Vitchyr Pong · Murtaza Dalal · Shikhar Bahl · Steven Lin · Sergey Levine

For an autonomous agent to fulfill a wide range of user-specified goals at test time, it must be able to learn broadly applicable and general-purpose skill repertoires. Furthermore, to provide the requisite level of generality, these skills must handle raw sensory input such as images. In this paper, we propose an algorithm that acquires such general-purpose skills by combining unsupervised representation learning and reinforcement learning of goal-conditioned policies. Since the particular goals that might be required at test-time are not known in advance, the agent performs a self-supervised "practice" phase where it imagines goals and attempts to achieve them. We learn a visual representation with three distinct purposes: sampling goals for self-supervised practice, providing a structured transformation of raw sensory inputs, and computing a reward signal for goal reaching. We also propose a retroactive goal relabeling scheme to further improve the sample-efficiency of our method. Our off-policy algorithm is efficient enough to learn policies that operate on raw image observations and goals in a real-world physical system, and substantially outperforms prior techniques.

Efficient High Dimensional Bayesian Optimization with Additivity and Quadrature Fourier Features

Spotlight | Wed Dec 5th 04:10 -- 04:15 PM @ Room 220 E

Mojmir Mutny · Andreas Krause

We develop an efficient and provably no-regret Bayesian optimization (BO) algorithm for optimization of black-box functions in high dimensions. We assume a generalized additive model with possibly overlapping variable groups. When the groups do not overlap, we are able to provide the first provably no-regret $\text{\emph{polynomial time}}$ (in the number of evaluations of the acquisition function) algorithm for solving high dimensional BO. To make the optimization efficient and feasible, we introduce a novel deterministic Fourier Features approximation based on numerical integration with detailed analysis for the squared exponential kernel. The error of this approximation decreases $\text{\emph{exponentially}}$ with the number of features, and allows for a precise approximation of both posterior mean and variance. In addition, the kernel matrix inversion improves in its complexity from cubic to essentially linear in the number of data points measured in basic arithmetic operations.

On the Local Minima of the Empirical Risk

Spotlight | Wed Dec 5th 04:10 -- 04:15 PM @ Room 517 CD

Chi Jin · Lydia T. Liu · Rong Ge · Michael Jordan

Population risk is always of primary interest in machine learning; however, learning algorithms only have access to the empirical risk. Even for applications with nonconvex non-smooth losses (such as modern deep networks), the population risk is generally significantly more well behaved from an optimization point of view than the empirical risk. In particular, sampling can create many spurious local minima. We consider a general framework which aims to optimize a smooth nonconvex function F (population risk) given only access to an approximation f (empirical risk) that is pointwise close to F (i.e., $\|F - f\|_{\infty} \leq \nu$). Our objective is to find the ϵ -approximate local minima of the underlying function F while avoiding the shallow local minima arising because of the tolerance ν which exist only in f . We propose a simple algorithm based on stochastic gradient descent (SGD) on a smoothed version of f that is guaranteed to achieve our goal as long as $\nu \leq O(\epsilon^{1.5}/d)$. We also provide an almost matching lower bound showing that our algorithm achieves optimal error tolerance ν among all algorithms making a polynomial number of queries of f . As a concrete example, we show that our results can be directly used to give sample complexities for learning a ReLU unit.

Randomized Prior Functions for Deep Reinforcement Learning

Spotlight | Wed Dec 5th 04:15 -- 04:20 PM @ Room 220 CD

Ian Osband · John Aslanides · Albin Cassirer

Dealing with uncertainty is essential for efficient reinforcement learning. There is a growing literature on uncertainty estimation for deep learning from fixed datasets, but many of the most popular approaches are poorly-suited to sequential decision problems. Other methods, such as bootstrap sampling, have no mechanism for uncertainty that does not come from the observed data. We highlight why this can be a crucial shortcoming and propose a simple remedy through addition of a randomized untrainable 'prior' network to each ensemble member. We prove that this approach is efficient with linear representations, provide simple illustrations of its efficacy with nonlinear representations and show that this approach scales to large-scale problems far better than previous attempts.

Regret bounds for meta Bayesian optimization with an

unknown Gaussian process prior

Spotlight | Wed Dec 5th 04:15 -- 04:20 PM @ Room 220 E

Zi Wang · Beomjoon Kim · Leslie Kaelbling

Bayesian optimization usually assumes that a Bayesian prior is given. However, the strong theoretical guarantees in Bayesian optimization are often regrettably compromised in practice because of unknown parameters in the prior. In this paper, we adopt a variant of empirical Bayes and show that, by estimating the Gaussian process prior from offline data sampled from the same prior and constructing unbiased estimators of the posterior, variants of both GP-UCB and \emph{probability of improvement} achieve a near-zero regret bound, which decreases to a constant proportional to the observational noise as the number of offline data and the number of online evaluations increase. Empirically, we have verified our approach on challenging simulated robotic problems featuring task and motion planning.

How Much Restricted Isometry is Needed In Nonconvex Matrix Recovery?

Spotlight | Wed Dec 5th 04:15 -- 04:20 PM @ Room 517 CD

Richard Zhang · Cedric Jozs · Somayeh Sojoudi · Javad Lavaei

When the linear measurements of an instance of low-rank matrix recovery satisfy a restricted isometry property (RIP) --- i.e. they are approximately norm-preserving --- the problem is known to contain no spurious local minima, so exact recovery is guaranteed. In this paper, we show that moderate RIP is not enough to eliminate spurious local minima, so existing results can only hold for near-perfect RIP. In fact, counterexamples are ubiquitous: every x is the spurious local minimum of a rank-1 instance of matrix recovery that satisfies RIP. One specific counterexample has RIP constant $\delta=1/2$, but causes randomly initialized stochastic gradient descent (SGD) to fail 12% of the time. SGD is frequently able to avoid and escape spurious local minima, but this empirical result shows that it can occasionally be defeated by their existence. Hence, while exact recovery guarantees will likely require a proof of no spurious local minima, arguments based solely on norm preservation will only be applicable to a narrow set of nearly-isotropic instances.

Playing hard exploration games by watching YouTube

Spotlight | Wed Dec 5th 04:20 -- 04:25 PM @ Room 220 CD

Yusuf Aytar · Tobias Pfaff · David Budden · Thomas Paine · Ziyu Wang · Nando de Freitas

Deep reinforcement learning methods traditionally struggle with tasks where environment rewards are particularly sparse. One successful method of guiding exploration in these domains is to imitate trajectories provided by a human demonstrator. However, these demonstrations are typically collected under artificial conditions, i.e. with access to the agent’s exact environment setup and the demonstrator’s action and reward trajectories. Here we propose a method that overcomes these limitations in two stages. First, we learn to map unaligned videos from multiple sources to a common representation using self-supervised objectives constructed over both time and modality (i.e. vision and sound). Second, we embed a single YouTube video in this representation to learn a reward function that encourages an agent to imitate human gameplay. This method of one-shot imitation allows our agent to convincingly exceed human-level performance on the infamously hard exploration games Montezuma’s Revenge, Pitfall! and Private Eye for the first time, even if the agent is not presented with any environment rewards.

Adversarially Robust Optimization with Gaussian Processes

Spotlight | Wed Dec 5th 04:20 -- 04:25 PM @ Room 220 E

Ilija Bogunovic · Jonathan Scarlett · Stefanie Jegelka · Volkan Cevher

In this paper, we consider the problem of Gaussian process (GP) optimization with an added robustness requirement: The returned point may be perturbed by an adversary, and we require the function value to remain as high as possible even after this perturbation. This problem is motivated by settings in which the underlying functions during optimization and implementation stages are different, or when one is interested in finding an entire region of good inputs rather than only a single point. We show that standard GP optimization algorithms do not exhibit the desired robustness properties, and provide a novel confidence-bound based algorithm StableOpt for this purpose. We rigorously establish the required number of samples for StableOpt to find a near-optimal point, and we complement this guarantee with an algorithm-independent lower bound. We experimentally demonstrate several potential applications of interest using real-world data sets, and we show that StableOpt consistently succeeds in finding a stable maximizer where several baseline methods fail.

SPIDER: Near-Optimal Non-Convex Optimization via Stochastic Path-Integrated Differential Estimator

Spotlight | Wed Dec 5th 04:20 -- 04:25 PM @ Room 517 CD

Cong Fang · Chris Junchi Li · Zhouchen Lin · Tong Zhang

In this paper, we propose a new technique named \textit{Stochastic Path-Integrated Differential Estimator} (SPIDER), which can be used to track many deterministic quantities of interests with

significantly reduced computational cost. Combining SPIDER with the method of normalized gradient descent, we propose SPIDER-SFO that solve non-convex stochastic optimization problems using stochastic gradients only. We provide a few error-bound results on its convergence rates. Specially, we prove that the SPIDER-SFO algorithm achieves a gradient computation cost of $\mathcal{O}(\min(n^{1/2} \epsilon^{-2}, \epsilon^{-3}))$ to find an ϵ -approximate first-order stationary point. In addition, we prove that SPIDER-SFO nearly matches the algorithmic lower bound for finding stationary point under the gradient Lipschitz assumption in the finite-sum setting. Our SPIDER technique can be further applied to find an $(\epsilon, \mathcal{O}(\epsilon^{0.5}))$ -approximate second-order stationary point at a gradient computation cost of $\tilde{\mathcal{O}}(\min(n^{1/2} \epsilon^{-2} + \epsilon^{-2.5}, \epsilon^{-3}))$.

Recurrent World Models Facilitate Policy Evolution

Oral | Wed Dec 5th 04:25 -- 04:40 PM @ Room 220 CD

David Ha · Jürgen Schmidhuber

A generative recurrent neural network is quickly trained in an unsupervised manner to model popular reinforcement learning environments through compressed spatio-temporal representations. The world model's extracted features are fed into compact and simple policies trained by evolution, achieving state of the art results in various environments. We also train our agent entirely inside of an environment generated by its own internal world model, and transfer this policy back into the actual environment. Interactive version of this paper is available at <https://worldmodels.github.io>

Approximate Knowledge Compilation by Online Collapsed Importance Sampling

Oral | Wed Dec 5th 04:25 -- 04:40 PM @ Room 220 E

Tal Friedman · Guy Van den Broeck

We introduce collapsed compilation, a novel approximate inference algorithm for discrete probabilistic graphical models. It is a collapsed sampling algorithm that incrementally selects which variable to sample next based on the partial compilation obtained so far. This online collapsing, together with knowledge compilation inference on the remaining variables, naturally exploits local structure and context-specific independence in the distribution. These properties are used implicitly in exact inference, but are difficult to harness for approximate inference. Moreover, by having a partially compiled circuit available during sampling, collapsed compilation has access to a highly effective proposal distribution for importance sampling. Our experimental evaluation shows that collapsed compilation performs well on standard benchmarks. In particular, when the amount of

exact inference is equally limited, collapsed compilation is competitive with the state of the art, and outperforms it on several benchmarks.

Analysis of Krylov Subspace Solutions of Regularized Non-Convex Quadratic Problems

Oral | Wed Dec 5th 04:25 -- 04:40 PM @ Room 517 CD

Yair Carmon · John Duchi

We provide convergence rates for Krylov subspace solutions to the trust-region and cubic-regularized (nonconvex) quadratic problems. Such solutions may be efficiently computed by the Lanczos method and have long been used in practice. We prove error bounds of the form $1/t^2$ and $e^{-4t/\sqrt{\kappa}}$, where κ is a condition number for the problem, and t is the Krylov subspace order (number of Lanczos iterations). We also provide lower bounds showing that our analysis is sharp.

Reducing Network Agnostophobia

Spotlight | Wed Dec 5th 04:40 -- 04:45 PM @ Room 220 CD

Akshay Raj Dhamija · Manuel Günther · Terrance Boulton

Agnostophobia, the fear of the unknown, can be experienced by deep learning engineers while applying their networks to real-world applications. Unfortunately, network behavior is not well defined for inputs far from a network's training set. In an uncontrolled environment, networks face many instances that are not of interest to them and have to be rejected in order to avoid a false positive. This problem has previously been tackled by researchers by either a) thresholding softmax, which by construction cannot return "none of the known classes", or b) using an additional background or garbage class. In this paper, we show that both of these approaches help, but are generally insufficient when previously unseen classes are encountered. We also introduce a new evaluation metric that focuses on comparing the performance of multiple approaches in scenarios where such unseen classes or unknowns are encountered. Our major contributions are simple yet effective Entropic Open-Set and Objectosphere losses that train networks using negative samples from some classes. These novel losses are designed to maximize entropy for unknown inputs while increasing separation in deep feature space by modifying magnitudes of known and unknown samples. Experiments on networks trained to classify classes from MNIST and CIFAR-10 show that our novel loss functions are significantly better at dealing with unknown inputs from datasets such as Devanagari, NotMNIST, CIFAR-100 and SVHN.

DAGs with NO TEARS: Continuous Optimization for Structure Learning

Spotlight | Wed Dec 5th 04:40 -- 04:45 PM @ Room 220 E

Xun Zheng · Bryon Aragam · Pradeep Ravikumar · Eric Xing

Estimating the structure of directed acyclic graphs (DAGs, also known as Bayesian networks) is a challenging problem since the search space of DAGs is combinatorial and scales superexponentially with the number of nodes. Existing approaches rely on various local heuristics for enforcing the acyclicity constraint. In this paper, we introduce a fundamentally different strategy: we formulate the structure learning problem as a purely continuous optimization problem over real matrices that avoids this combinatorial constraint entirely. This is achieved by a novel characterization of acyclicity that is not only smooth but also exact. The resulting problem can be efficiently solved by standard numerical algorithms, which also makes implementation effortless. The proposed method outperforms existing ones, without imposing any structural assumptions on the graph such as bounded treewidth or in-degree.

Natasha 2: Faster Non-Convex Optimization Than SGD

Spotlight | Wed Dec 5th 04:40 -- 04:45 PM @ Room 517 CD

Zeyuan Allen-Zhu

We design a stochastic algorithm to find ϵ -approximate local minima of any smooth nonconvex function in rate $O(\epsilon^{-3.25})$, with only oracle access to stochastic gradients. The best result before this work was $O(\epsilon^{-4})$ by stochastic gradient descent (SGD).

Life-Long Disentangled Representation Learning with Cross-Domain Latent Homologies

Spotlight | Wed Dec 5th 04:45 -- 04:50 PM @ Room 220 CD

Alessandro Achille · Tom Eccles · Loic Matthey · Chris Burgess · Nicholas Watters · Alexander Lerchner · Irina Higgins

Intelligent behaviour in the real-world requires the ability to acquire new knowledge from an ongoing sequence of experiences while preserving and reusing past knowledge. We propose a novel

algorithm for unsupervised representation learning from piece-wise stationary visual data: Variational Autoencoder with Shared Embeddings (VASE). Based on the Minimum Description Length principle, VASE automatically detects shifts in the data distribution and allocates spare representational capacity to new knowledge, while simultaneously protecting previously learnt representations from catastrophic forgetting. Our approach encourages the learnt representations to be disentangled, which imparts a number of desirable properties: VASE can deal sensibly with ambiguous inputs, it can enhance its own representations through imagination-based exploration, and most importantly, it exhibits semantically meaningful sharing of latents between different datasets. Compared to baselines with entangled representations, our approach is able to reason beyond surface-level statistics and perform semantically meaningful cross-domain inference.

Proximal Graphical Event Models

Spotlight | Wed Dec 5th 04:45 -- 04:50 PM @ Room 220 E

Debarun Bhattacharjya · Dharmashankar Subramanian · Tian Gao

Event datasets include events that occur irregularly over the timeline and are prevalent in numerous domains. We introduce proximal graphical event models (PGEM) as a representation of such datasets. PGEMs belong to a broader family of models that characterize relationships between various types of events, where the rate of occurrence of an event type depends only on whether or not its parents have occurred in the most recent history. The main advantage over the state of the art models is that they are entirely data driven and do not require additional inputs from the user, which can require knowledge of the domain such as choice of basis functions or hyperparameters in graphical event models. We theoretically justify our learning of optimal windows for parental history and the choices of parental sets, and the algorithm are sound and complete in terms of parent structure learning. We present additional efficient heuristics for learning PGEMs from data, demonstrating their effectiveness on synthetic and real datasets.

Escaping Saddle Points in Constrained Optimization

Spotlight | Wed Dec 5th 04:45 -- 04:50 PM @ Room 517 CD

Aryan Mokhtari · Asuman Ozdaglar · Ali Jadbabaie

In this paper, we study the problem of escaping from saddle points in smooth nonconvex optimization problems subject to a convex set \mathcal{C} . We propose a generic framework that yields convergence to a second-order stationary point of the problem, if the convex set \mathcal{C} is simple for a quadratic objective function. Specifically, our results hold if one can find a ρ -approximate solution of a quadratic program subject to \mathcal{C} in polynomial time, where $\rho < 1$ is a positive constant that depends on the structure of the set \mathcal{C} .

Under this condition, we show that the sequence of iterates generated by the proposed framework reaches an (ϵ, γ) -second order stationary point (SOSP) in at most $\mathcal{O}(\max\{\epsilon^{-2}, \rho^{-3}\} \gamma^{-3})$ iterations. We further characterize the overall complexity of reaching an SOSP when the convex set \mathcal{C} can be written as a set of quadratic constraints and the objective function Hessian has a specific structure over the convex \mathcal{C} . Finally, we extend our results to the stochastic setting and characterize the number of stochastic gradient and Hessian evaluations to reach an (ϵ, γ) -SOSP.

Geometrically Coupled Monte Carlo Sampling

Spotlight | Wed Dec 5th 04:50 -- 04:55 PM @ Room 220 CD

Mark Rowland · Krzysztof Choromanski · François Chalus · Aldo Pacchiano · Tamas Sarlos · Richard E Turner · Adrian Weller

Monte Carlo sampling in high-dimensional, low-sample settings is important in many machine learning tasks. We improve current methods for sampling in Euclidean spaces by avoiding independence, and instead consider ways to couple samples. We show fundamental connections to optimal transport theory, leading to novel sampling algorithms, and providing new theoretical grounding for existing strategies. We compare our new strategies against prior methods for improving sample efficiency, including QMC, by studying discrepancy. We explore our findings empirically, and observe benefits of our sampling schemes for reinforcement learning and generative modelling.

Heterogeneous Multi-output Gaussian Process Prediction

Spotlight | Wed Dec 5th 04:50 -- 04:55 PM @ Room 220 E

Pablo Moreno-Muñoz · Antonio Artés · Mauricio Álvarez

We present a novel extension of multi-output Gaussian processes for handling heterogeneous outputs. We assume that each output has its own likelihood function and use a vector-valued Gaussian process prior to jointly model the parameters in all likelihoods as latent functions. Our multi-output Gaussian process uses a covariance function with a linear model of coregionalisation form. Assuming conditional independence across the underlying latent functions together with an inducing variable framework, we are able to obtain tractable variational bounds amenable to stochastic variational inference. We illustrate the performance of the model on synthetic data and two real datasets: a human behavioral study and a demographic high-dimensional dataset.

On Coresets for Logistic Regression

Spotlight | Wed Dec 5th 04:50 -- 04:55 PM @ Room 517 CD

Alexander Munteanu · Chris Schwiegelshohn · Christian Sohler · David Woodruff

Coresets are one of the central methods to facilitate the analysis of large data. We continue a recent line of research applying the theory of coresets to logistic regression. First, we show the negative result that no strongly sublinear sized coresets exist for logistic regression. To deal with intractable worst-case instances we introduce a complexity measure $\mu(X)$, which quantifies the hardness of compressing a data set for logistic regression. $\mu(X)$ has an intuitive statistical interpretation that may be of independent interest. For data sets with bounded $\mu(X)$ -complexity, we show that a novel sensitivity sampling scheme produces the first provably sublinear $(1 \pm \epsilon)$ -coreset. We illustrate the performance of our method by comparing to uniform sampling as well as to state of the art methods in the area. The experiments are conducted on real world benchmark data for logistic regression.

Scalable Laplacian K-modes

Spotlight | Wed Dec 5th 04:55 -- 05:00 PM @ Room 220 CD

Imtiaz Ziko · Eric Granger · Ismail Ben Ayed

We advocate Laplacian K-modes for joint clustering and density mode finding, and propose a concave-convex relaxation of the problem, which yields a parallel algorithm that scales up to large datasets and high dimensions. We optimize a tight bound (auxiliary function) of our relaxation, which, at each iteration, amounts to computing an independent update for each cluster-assignment variable, with guaranteed convergence. Therefore, our bound optimizer can be trivially distributed for large-scale data sets. Furthermore, we show that the density modes can be obtained as byproducts of the assignment variables via simple maximum-value operations whose additional computational cost is linear in the number of data points. Our formulation does not need storing a full affinity matrix and computing its eigenvalue decomposition, neither does it perform expensive projection steps and Lagrangian-dual inner iterates for the simplex constraints of each point. Furthermore, unlike mean-shift, our density-mode estimation does not require inner-loop gradient-ascent iterates. It has a complexity independent of feature-space dimension, yields modes that are valid data points in the input set and is applicable to discrete domains as well as arbitrary kernels. We report comprehensive experiments over various data sets, which show that our algorithm yields very competitive performances in term of optimization quality (i.e., the value of the discrete-variable objective at convergence) and clustering accuracy.

GPyTorch: Blackbox Matrix-Matrix Gaussian Process Inference with GPU Acceleration

Spotlight | Wed Dec 5th 04:55 -- 05:00 PM @ Room 220 E

Jacob Gardner · Geoff Pleiss · Kilian Weinberger · David Bindel · Andrew Wilson

Despite advances in scalable models, the inference tools used for Gaussian processes (GPs) have yet to fully capitalize on developments in computing hardware. We present an efficient and general approach to GP inference based on Blackbox Matrix-Matrix multiplication (BBMM). BBMM inference uses a modified batched version of the conjugate gradients algorithm to derive all terms for training and inference in a single call. BBMM reduces the asymptotic complexity of exact GP inference from $O(n^3)$ to $O(n^2)$. Adapting this algorithm to scalable approximations and complex GP models simply requires a routine for efficient matrix-matrix multiplication with the kernel and its derivative. In addition, BBMM uses a specialized preconditioner to substantially speed up convergence. In experiments we show that BBMM effectively uses GPU hardware to dramatically accelerate both exact GP inference and scalable approximations. Additionally, we provide GPyTorch, a software platform for scalable GP inference via BBMM, built on PyTorch.

Legendre Decomposition for Tensors

Spotlight | Wed Dec 5th 04:55 -- 05:00 PM @ Room 517 CD

Mahito Sugiyama · Hiroyuki Nakahara · Koji Tsuda

We present a novel nonnegative tensor decomposition method, called Legendre decomposition, which factorizes an input tensor into a multiplicative combination of parameters. Thanks to the well-developed theory of information geometry, the reconstructed tensor is unique and always minimizes the KL divergence from an input tensor. We empirically show that Legendre decomposition can more accurately reconstruct tensors than other nonnegative tensor decomposition methods.

Equality of Opportunity in Classification: A Causal Approach

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #1

Junzhe Zhang · Elias Bareinboim

The Equalized Odds (for short, EO) is one of the most popular measures of discrimination used in the supervised learning setting. It ascertains fairness through the balance of the misclassification rates (false positive and negative) across the protected groups -- e.g., in the context of law enforcement, an African-American defendant who would not commit a future crime will have an equal opportunity

of being released, compared to a non-recidivating Caucasian defendant. Despite this noble goal, it has been acknowledged in the literature that statistical tests based on the EO are oblivious to the underlying causal mechanisms that generated the disparity in the first place (Hardt et al. 2016). This leads to a critical disconnect between statistical measures readable from the data and the meaning of discrimination in the legal system, where compelling evidence that the observed disparity is tied to a specific causal process deemed unfair by society is required to characterize discrimination. The goal of this paper is to develop a principled approach to connect the statistical disparities characterized by the EO and the underlying, elusive, and frequently unobserved, causal mechanisms that generated such inequality. We start by introducing a new family of counterfactual measures that allows one to explain the misclassification disparities in terms of the underlying mechanisms in an arbitrary, non-parametric structural causal model. This will, in turn, allow legal and data analysts to interpret currently deployed classifiers through causal lens, linking the statistical disparities found in the data to the corresponding causal processes. Leveraging the new family of counterfactual measures, we develop a learning procedure to construct a classifier that is statistically efficient, interpretable, and compatible with the basic human intuition of fairness. We demonstrate our results through experiments in both real (COMPAS) and synthetic datasets.

Confounding-Robust Policy Improvement

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #2

Nathan Kallus · Angela Zhou

We study the problem of learning personalized decision policies from observational data while accounting for possible unobserved confounding in the data-generating process. Unlike previous approaches that assume unconfoundedness, i.e., no unobserved confounders affected both treatment assignment and outcomes, we calibrate policy learning for realistic violations of this unverifiable assumption with uncertainty sets motivated by sensitivity analysis in causal inference. Our framework for confounding-robust policy improvement optimizes the minimax regret of a candidate policy against a baseline or reference "status quo" policy, over an uncertainty set around nominal propensity weights. We prove that if the uncertainty set is well-specified, robust policy learning can do no worse than the baseline, and only improve if the data supports it. We characterize the adversarial subproblem and use efficient algorithmic solutions to optimize over parametrized spaces of decision policies such as logistic treatment assignment. We assess our methods on synthetic data and a large clinical trial, demonstrating that confounded selection can hinder policy learning and lead to unwarranted harm, while our robust approach guarantees safety and focuses on well-evidenced improvement.

Causal Discovery from Discrete Data using Hidden Compact Representation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #3

Ruichu Cai · Jie Qiao · Kun Zhang · Zhenjie Zhang · Zhifeng Hao

Causal discovery from a set of observations is one of the fundamental problems across several disciplines. For continuous variables, recently a number of causal discovery methods have demonstrated their effectiveness in distinguishing the cause from effect by exploring certain properties of the conditional distribution, but causal discovery on categorical data still remains to be a challenging problem, because it is generally not easy to find a compact description of the causal mechanism for the true causal direction. In this paper we make an attempt to find a way to solve this problem by assuming a two-stage causal process: the first stage maps the cause to a hidden variable of a lower cardinality, and the second stage generates the effect from the hidden representation. In this way, the causal mechanism admits a simple yet compact representation. We show that under this model, the causal direction is identifiable under some weak conditions on the true causal mechanism. We also provide an effective solution to recover the above hidden compact representation within the likelihood framework. Empirical studies verify the effectiveness of the proposed approach on both synthetic and real-world data.

Dirichlet belief networks for topic structure learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #4

He Zhao · Lan Du · Wray Buntine · Mingyuan Zhou

Recently, considerable research effort has been devoted to developing deep architectures for topic models to learn topic structures. Although several deep models have been proposed to learn better topic proportions of documents, how to leverage the benefits of deep structures for learning word distributions of topics has not yet been rigorously studied. Here we propose a new multi-layer generative process on word distributions of topics, where each layer consists of a set of topics and each topic is drawn from a mixture of the topics of the layer above. As the topics in all layers can be directly interpreted by words, the proposed model is able to discover interpretable topic hierarchies. As a self-contained module, our model can be flexibly adapted to different kinds of topic models to improve their modelling accuracy and interpretability. Extensive experiments on text corpora demonstrate the advantages of the proposed model.

Approximate Knowledge Compilation by Online Collapsed

Importance Sampling

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #5

Tal Friedman · Guy Van den Broeck

We introduce collapsed compilation, a novel approximate inference algorithm for discrete probabilistic graphical models. It is a collapsed sampling algorithm that incrementally selects which variable to sample next based on the partial compilation obtained so far. This online collapsing, together with knowledge compilation inference on the remaining variables, naturally exploits local structure and context-specific independence in the distribution. These properties are used implicitly in exact inference, but are difficult to harness for approximate inference. Moreover, by having a partially compiled circuit available during sampling, collapsed compilation has access to a highly effective proposal distribution for importance sampling. Our experimental evaluation shows that collapsed compilation performs well on standard benchmarks. In particular, when the amount of exact inference is equally limited, collapsed compilation is competitive with the state of the art, and outperforms it on several benchmarks.

Proximal Graphical Event Models

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #6

Debarun Bhattacharjya · Dharmashankar Subramanian · Tian Gao

Event datasets include events that occur irregularly over the timeline and are prevalent in numerous domains. We introduce proximal graphical event models (PGEM) as a representation of such datasets. PGEMs belong to a broader family of models that characterize relationships between various types of events, where the rate of occurrence of an event type depends only on whether or not its parents have occurred in the most recent history. The main advantage over the state of the art models is that they are entirely data driven and do not require additional inputs from the user, which can require knowledge of the domain such as choice of basis functions or hyperparameters in graphical event models. We theoretically justify our learning of optimal windows for parental history and the choices of parental sets, and the algorithm are sound and complete in terms of parent structure learning. We present additional efficient heuristics for learning PGEMs from data, demonstrating their effectiveness on synthetic and real datasets.

Dynamic Network Model from Partial Observations

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #7

Elahe Ghalebi · Baharan Mirzasoleiman · Radu Grosu · Jure Leskovec

Can evolving networks be inferred and modeled without directly observing their nodes and edges? In many applications, the edges of a dynamic network might not be observed, but one can observe the dynamics of stochastic cascading processes (e.g., information diffusion, virus propagation) occurring over the unobserved network. While there have been efforts to infer networks based on such data, providing a generative probabilistic model that is able to identify the underlying time-varying network remains an open question. Here we consider the problem of inferring generative dynamic network models based on network cascade diffusion data. We propose a novel framework for providing a non-parametric dynamic network model---based on a mixture of coupled hierarchical Dirichlet processes---based on data capturing cascade node infection times. Our approach allows us to infer the evolving community structure in networks and to obtain an explicit predictive distribution over the edges of the underlying network---including those that were not involved in transmission of any cascade, or are likely to appear in the future. We show the effectiveness of our approach using extensive experiments on synthetic as well as real-world networks.

HOGWILD!-Gibbs can be PanAccurate

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #8

Constantinos Daskalakis · Nishanth Dikkala · Siddhartha Jayanti

Asynchronous Gibbs sampling has been recently shown to be fast-mixing and an accurate method for estimating probabilities of events on a small number of variables of a graphical model satisfying Dobrushin's condition~\cite{DeSaOR16}. We investigate whether it can be used to accurately estimate expectations of functions of {\em all the variables} of the model. Under the same condition, we show that the synchronous (sequential) and asynchronous Gibbs samplers can be coupled so that the expected Hamming distance between their (multivariate) samples remains bounded by $O(\tau \log n)$, where n is the number of variables in the graphical model, and τ is a measure of the asynchronicity. A similar bound holds for any constant power of the Hamming distance. Hence, the expectation of any function that is Lipschitz with respect to a power of the Hamming distance, can be estimated with a bias that grows logarithmically in n . Going beyond Lipschitz functions, we consider the bias arising from asynchronicity in estimating the expectation of polynomial functions of all variables in the model. Using recent concentration of measure results~\cite{DaskalakisDK17,GheissariLP17,GotzeSS18}, we show that the bias introduced by the asynchronicity is of smaller order than the standard deviation of the function value already present in the true model. We perform experiments on a multi-processor machine to empirically illustrate our theoretical findings.

DAGs with NO TEARS: Continuous Optimization for

Structure Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #9

Xun Zheng · Bryon Aragam · Pradeep Ravikumar · Eric Xing

Estimating the structure of directed acyclic graphs (DAGs, also known as Bayesian networks) is a challenging problem since the search space of DAGs is combinatorial and scales superexponentially with the number of nodes. Existing approaches rely on various local heuristics for enforcing the acyclicity constraint. In this paper, we introduce a fundamentally different strategy: we formulate the structure learning problem as a purely continuous optimization problem over real matrices that avoids this combinatorial constraint entirely. This is achieved by a novel characterization of acyclicity that is not only smooth but also exact. The resulting problem can be efficiently solved by standard numerical algorithms, which also makes implementation effortless. The proposed method outperforms existing ones, without imposing any structural assumptions on the graph such as bounded treewidth or in-degree.

Mean Field for the Stochastic Blockmodel: Optimization Landscape and Convergence Issues

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #10

Soumendu Sundar Mukherjee · Purnamrita Sarkar · Y. X. Rachel Wang · Bowei Yan

Variational approximation has been widely used in large-scale Bayesian inference recently, the simplest kind of which involves imposing a mean field assumption to approximate complicated latent structures. Despite the computational scalability of mean field, theoretical studies of its loss function surface and the convergence behavior of iterative updates for optimizing the loss are far from complete. In this paper, we focus on the problem of community detection for a simple two-class Stochastic Blockmodel (SBM). Using batch co-ordinate ascent (BCAVI) for updates, we give a complete characterization of all the critical points and show different convergence behaviors with respect to initializations. When the parameters are known, we show a significant proportion of random initializations will converge to ground truth. On the other hand, when the parameters themselves need to be estimated, a random initialization will converge to an uninformative local optimum.

Coupled Variational Bayes via Optimization Embedding

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #11

Bo Dai · Hanjun Dai · Niao He · Weiyang Liu · Zhen Liu · Jianshu Chen · Lin Xiao · Le Song

Variational inference plays a vital role in learning graphical models, especially on large-scale datasets. Much of its success depends on a proper choice of auxiliary distribution class for posterior approximation. However, how to pursue an auxiliary distribution class that achieves both good approximation ability and computation efficiency remains a core challenge. In this paper, we proposed coupled variational Bayes which exploits the primal-dual view of the ELBO with the variational distribution class generated by an optimization procedure, which is termed optimization embedding. This flexible function class couples the variational distribution with the original parameters in the graphical models, allowing end-to-end learning of the graphical models by back-propagation through the variational distribution. Theoretically, we establish an interesting connection to gradient flow and demonstrate the extreme flexibility of this implicit distribution family in the limit sense. Empirically, we demonstrate the effectiveness of the proposed method on multiple graphical models with either continuous or discrete latent variables comparing to state-of-the-art methods.

Stochastic Nonparametric Event-Tensor Decomposition

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #12

Shandian Zhe · Yishuai Du

Tensor decompositions are fundamental tools for multiway data analysis. Existing approaches, however, ignore the valuable temporal information along with data, or simply discretize them into time steps so that important temporal patterns are easily missed. Moreover, most methods are limited to multilinear decomposition forms, and hence are unable to capture intricate, nonlinear relationships in data. To address these issues, we formulate event-tensors, to preserve the complete temporal information for multiway data, and propose a novel Bayesian nonparametric decomposition model. Our model can (1) fully exploit the time stamps to capture the critical, causal/triggering effects between the interaction events, (2) flexibly estimate the complex relationships between the entities in tensor modes, and (3) uncover hidden structures from their temporal interactions. For scalable inference, we develop a doubly stochastic variational Expectation-Maximization algorithm to conduct an online decomposition. Evaluations on both synthetic and real-world datasets show that our model not only improves upon the predictive performance of existing methods, but also discovers interesting clusters underlying the data.

GPyTorch: Blackbox Matrix-Matrix Gaussian Process Inference with GPU Acceleration

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #13

Jacob Gardner · Geoff Pleiss · Kilian Weinberger · David Bindel · Andrew Wilson

Despite advances in scalable models, the inference tools used for Gaussian processes (GPs) have yet to fully capitalize on developments in computing hardware. We present an efficient and general approach to GP inference based on Blackbox Matrix-Matrix multiplication (BBMM). BBMM inference uses a modified batched version of the conjugate gradients algorithm to derive all terms for training and inference in a single call. BBMM reduces the asymptotic complexity of exact GP inference from $O(n^3)$ to $O(n^2)$. Adapting this algorithm to scalable approximations and complex GP models simply requires a routine for efficient matrix-matrix multiplication with the kernel and its derivative. In addition, BBMM uses a specialized preconditioner to substantially speed up convergence. In experiments we show that BBMM effectively uses GPU hardware to dramatically accelerate both exact GP inference and scalable approximations. Additionally, we provide GPyTorch, a software platform for scalable GP inference via BBMM, built on PyTorch.

Heterogeneous Multi-output Gaussian Process Prediction

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #14

Pablo Moreno-Muñoz · Antonio Artés · Mauricio Álvarez

We present a novel extension of multi-output Gaussian processes for handling heterogeneous outputs. We assume that each output has its own likelihood function and use a vector-valued Gaussian process prior to jointly model the parameters in all likelihoods as latent functions. Our multi-output Gaussian process uses a covariance function with a linear model of coregionalisation form. Assuming conditional independence across the underlying latent functions together with an inducing variable framework, we are able to obtain tractable variational bounds amenable to stochastic variational inference. We illustrate the performance of the model on synthetic data and two real datasets: a human behavioral study and a demographic high-dimensional dataset.

Probabilistic Matrix Factorization for Automated Machine Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #15

Nicolo Fusi · Rishit Sheth · Melih Elibol

In order to achieve state-of-the-art performance, modern machine learning techniques require careful data pre-processing and hyperparameter tuning. Moreover, given the ever increasing number of machine learning models being developed, model selection is becoming increasingly important. Automating the selection and tuning of machine learning pipelines, which can include different data pre-processing methods and machine learning models, has long been one of the goals of the machine learning community. In this paper, we propose to solve this meta-learning task by combining ideas from collaborative filtering and Bayesian optimization. Specifically, we use a

probabilistic matrix factorization model to transfer knowledge across experiments performed in hundreds of different datasets and use an acquisition function to guide the exploration of the space of possible ML pipelines. In our experiments, we show that our approach quickly identifies high-performing pipelines across a wide range of datasets, significantly outperforming the current state-of-the-art.

Stochastic Expectation Maximization with Variance Reduction

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #16

Jianfei Chen · Jun Zhu · Yee Whye Teh · Tong Zhang

Expectation-Maximization (EM) is a popular tool for learning latent variable models, but the vanilla batch EM does not scale to large data sets because the whole data set is needed at every E-step. Stochastic Expectation Maximization (sEM) reduces the cost of E-step by stochastic approximation. However, sEM has a slower asymptotic convergence rate than batch EM, and requires a decreasing sequence of step sizes, which is difficult to tune. In this paper, we propose a variance reduced stochastic EM (sEM-vr) algorithm inspired by variance reduced stochastic gradient descent algorithms. We show that sEM-vr has the same exponential asymptotic convergence rate as batch EM. Moreover, sEM-vr only requires a constant step size to achieve this rate, which alleviates the burden of parameter tuning. We compare sEM-vr with batch EM, sEM and other algorithms on Gaussian mixture models and probabilistic latent semantic analysis, and sEM-vr converges significantly faster than these baselines.

Generative Neural Machine Translation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #17

Harshil Shah · David Barber

We introduce Generative Neural Machine Translation (GNMT), a latent variable architecture which is designed to model the semantics of the source and target sentences. We modify an encoder-decoder translation model by adding a latent variable as a language agnostic representation which is encouraged to learn the meaning of the sentence. GNMT achieves competitive BLEU scores on pure translation tasks, and is superior when there are missing words in the source sentence. We augment the model to facilitate multilingual translation and semi-supervised learning without adding parameters. This framework significantly reduces overfitting when there is limited paired data available, and is effective for translating between pairs of languages not seen during training.

Sparse Covariance Modeling in High Dimensions with Gaussian Processes

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #18

Rui Li · Kishan KC · Feng Cui · Justin Domke · Anne Haake

This paper studies statistical relationships among components of high-dimensional observations varying across non-random covariates. We propose to model the observation elements' changing covariances as sparse multivariate stochastic processes. In particular, our novel covariance modeling method reduces dimensionality by relating the observation vectors to a lower dimensional subspace. To characterize the changing correlations, we jointly model the latent factors and the factor loadings as collections of basis functions that vary with the covariates as Gaussian processes. Automatic relevance determination (ARD) encodes basis sparsity through their coefficients to account for the inherent redundancy. Experiments conducted across domains show superior performances to the state-of-the-art methods.

Variational Learning on Aggregate Outputs with Gaussian Processes

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #19

Ho Chung Law · Dino Sejdinovic · Ewan Cameron · Tim Lucas · Seth Flaxman · Katherine Battle · Kenji Fukumizu

While a typical supervised learning framework assumes that the inputs and the outputs are measured at the same levels of granularity, many applications, including global mapping of disease, only have access to outputs at a much coarser level than that of the inputs. Aggregation of outputs makes generalization to new inputs much more difficult. We consider an approach to this problem based on variational learning with a model of output aggregation and Gaussian processes, where aggregation leads to intractability of the standard evidence lower bounds. We propose new bounds and tractable approximations, leading to improved prediction accuracy and scalability to large datasets, while explicitly taking uncertainty into account. We develop a framework which extends to several types of likelihoods, including the Poisson model for aggregated count data. We apply our framework to a challenging and important problem, the fine-scale spatial modelling of malaria incidence, with over 1 million observations.

Learning Invariances using the Marginal Likelihood

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #20

Mark van der Wilk · Matthias Bauer · ST John · James Hensman

In many supervised learning tasks, learning what changes do not affect the prediction target is as crucial to generalisation as learning what does. Data augmentation is a common way to enforce a model to exhibit an invariance: training data is modified according to an invariance designed by a human and added to the training data. We argue that invariances should be incorporated into the model structure, and learned using the marginal likelihood, which can correctly reward the reduced complexity of invariant models. We incorporate invariances in a Gaussian process, due to good marginal likelihood approximations being available for these models. Our main contribution is a derivation for a variational inference scheme for invariant Gaussian processes where the invariance is described by a probability distribution that can be sampled from, much like how data augmentation is implemented in practice

Dirichlet-based Gaussian Processes for Large-scale Calibrated Classification

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #21

Dimitrios Milios · Raffaello Camoriano · Pietro Michiardi · Lorenzo Rosasco · Maurizio Filippone

This paper studies the problem of deriving fast and accurate classification algorithms with uncertainty quantification. Gaussian process classification provides a principled approach, but the corresponding computational burden is hardly sustainable in large-scale problems and devising efficient alternatives is a challenge. In this work, we investigate if and how Gaussian process regression directly applied to classification labels can be used to tackle this question. While in this case training is remarkably faster, predictions need to be calibrated for classification and uncertainty estimation. To this aim, we propose a novel regression approach where the labels are obtained through the interpretation of classification labels as the coefficients of a degenerate Dirichlet distribution. Extensive experimental results show that the proposed approach provides essentially the same accuracy and uncertainty quantification as Gaussian process classification while requiring only a fraction of computational resources.

Regret bounds for meta Bayesian optimization with an unknown Gaussian process prior

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #22

Bayesian optimization usually assumes that a Bayesian prior is given. However, the strong theoretical guarantees in Bayesian optimization are often regrettably compromised in practice because of unknown parameters in the prior. In this paper, we adopt a variant of empirical Bayes and show that, by estimating the Gaussian process prior from offline data sampled from the same prior and constructing unbiased estimators of the posterior, variants of both GP-UCB and $\text{probability of improvement}$ achieve a near-zero regret bound, which decreases to a constant proportional to the observational noise as the number of offline data and the number of online evaluations increase. Empirically, we have verified our approach on challenging simulated robotic problems featuring task and motion planning.

Efficient High Dimensional Bayesian Optimization with Additivity and Quadrature Fourier Features

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #23

Mojmir Mutny · Andreas Krause

We develop an efficient and provably no-regret Bayesian optimization (BO) algorithm for optimization of black-box functions in high dimensions. We assume a generalized additive model with possibly overlapping variable groups. When the groups do not overlap, we are able to provide the first provably no-regret polynomial time (in the number of evaluations of the acquisition function) algorithm for solving high dimensional BO. To make the optimization efficient and feasible, we introduce a novel deterministic Fourier Features approximation based on numerical integration with detailed analysis for the squared exponential kernel. The error of this approximation decreases exponentially with the number of features, and allows for a precise approximation of both posterior mean and variance. In addition, the kernel matrix inversion improves in its complexity from cubic to essentially linear in the number of data points measured in basic arithmetic operations.

Adversarially Robust Optimization with Gaussian Processes

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #24

Ilija Bogunovic · Jonathan Scarlett · Stefanie Jegelka · Volkan Cevher

In this paper, we consider the problem of Gaussian process (GP) optimization with an added robustness requirement: The returned point may be perturbed by an adversary, and we require the function value to remain as high as possible even after this perturbation. This problem is motivated by settings in which the underlying functions during optimization and implementation stages are different, or when one is interested in finding an entire region of good inputs rather than only a

single point. We show that standard GP optimization algorithms do not exhibit the desired robustness properties, and provide a novel confidence-bound based algorithm StableOpt for this purpose. We rigorously establish the required number of samples for StableOpt to find a near-optimal point, and we complement this guarantee with an algorithm-independent lower bound. We experimentally demonstrate several potential applications of interest using real-world data sets, and we show that StableOpt consistently succeeds in finding a stable maximizer where several baseline methods fail.

Multi-objective Maximization of Monotone Submodular Functions with Cardinality Constraint

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #25

Rajan Udwani

We consider the problem of multi-objective maximization of monotone submodular functions subject to cardinality constraint, often formulated as $\max_{|A|=k} \min_{i \in \{1, \dots, m\}} f_i(A)$. While it is widely known that greedy methods work well for a single objective, the problem becomes much harder with multiple objectives. In fact, Krause et al. (2008) showed that when the number of objectives m grows as the cardinality k i.e., $m = \Omega(k)$, the problem is inapproximable (unless $P=NP$). On the other hand, when m is constant Chekuri et al. (2010) showed a randomized $(1-1/e)$ -approximation with runtime (number of queries to function oracle) n^{m/ϵ^3} . In fact, the result of Chekuri et al. (2010) is for the far more general case of matroid constant.

We focus on finding a fast and practical algorithm that has (asymptotic) approximation guarantees even when m is super constant. We first modify the algorithm of Chekuri et al. (2010) to achieve a $(1-1/e)$ approximation for $m = o(\frac{k}{\log^3 k})$. This demonstrates a steep transition from constant factor approximability to inapproximability around $m = \Omega(k)$. Then using Multiplicative-Weight-Updates (MWU), we find a much faster $\tilde{O}(n/\delta^3)$ time asymptotic $(1-1/e)^{2-\delta}$ approximation. While the above results are all randomized, we also give a simple deterministic $(1-1/e)$ -approximation with runtime kn^{m/ϵ^4} . Finally, we run synthetic experiments using Kronecker graphs and find that our MWU inspired heuristic outperforms existing heuristics.

Variational PDEs for Acceleration on Manifolds and Application to Diffeomorphisms

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #26

We consider the optimization of cost functionals on manifolds and derive a variational approach to accelerated methods on manifolds. We demonstrate the methodology on the infinite-dimensional manifold of diffeomorphisms, motivated by registration problems in computer vision. We build on the variational approach to accelerated optimization by Wibisono, Wilson and Jordan, which applies in finite dimensions, and generalize that approach to infinite dimensional manifolds. We derive the continuum evolution equations, which are partial differential equations (PDE), and relate them to simple mechanical principles. Our approach can also be viewed as a generalization of the L^2 optimal mass transport problem. Our approach evolves an infinite number of particles endowed with mass, represented as a mass density. The density evolves with the optimization variable, and endows the particles with dynamics. This is different than current accelerated methods where only a single particle moves and hence the dynamics does not depend on the mass. We derive the theory, compute the PDEs for acceleration, and illustrate the behavior of this new accelerated optimization scheme.

Zeroth-order (Non)-Convex Stochastic Optimization via Conditional Gradient and Gradient Updates

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #27

Krishnakumar Balasubramanian · Saeed Ghadimi

In this paper, we propose and analyze zeroth-order stochastic approximation algorithms for nonconvex and convex optimization. Specifically, we propose generalizations of the conditional gradient algorithm achieving rates similar to the standard stochastic gradient algorithm using only zeroth-order information. Furthermore, under a structural sparsity assumption, we first illustrate an implicit regularization phenomenon where the standard stochastic gradient algorithm with zeroth-order information adapts to the sparsity of the problem at hand by just varying the step-size. Next, we propose a truncated stochastic gradient algorithm with zeroth-order information, whose rate of convergence depends only poly-logarithmically on the dimensionality.

Computing Higher Order Derivatives of Matrix and Tensor Expressions

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #28

Soeren Laue · Matthias Mitterreiter · Joachim Giesen

Optimization is an integral part of most machine learning systems and most numerical optimization schemes rely on the computation of derivatives. Therefore, frameworks for computing derivatives are an active area of machine learning research. Surprisingly, as of yet, no existing framework is

capable of computing higher order matrix and tensor derivatives directly. Here, we close this fundamental gap and present an algorithmic framework for computing matrix and tensor derivatives that extends seamlessly to higher order derivatives. The framework can be used for symbolic as well as for forward and reverse mode automatic differentiation. Experiments show a speedup between one and four orders of magnitude over state-of-the-art frameworks when evaluating higher order derivatives.

How SGD Selects the Global Minima in Over-parameterized Learning: A Dynamical Stability Perspective

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #29

Lei Wu · Chao Ma · Weinan E

The question of which global minima are accessible by a stochastic gradient decent (SGD) algorithm with specific learning rate and batch size is studied from the perspective of dynamical stability. The concept of non-uniformity is introduced, which, together with sharpness, characterizes the stability property of a global minimum and hence the accessibility of a particular SGD algorithm to that global minimum. In particular, this analysis shows that learning rate and batch size play different roles in minima selection. Extensive empirical results seem to correlate well with the theoretical findings and provide further support to these claims.

The Effect of Network Width on the Performance of Large-batch Training

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #30

Lingjiao Chen · Hongyi Wang · Jinman Zhao · Dimitris Papailiopoulos · Paraschos Koutris

Distributed implementations of mini-batch stochastic gradient descent (SGD) suffer from communication overheads, attributed to the high frequency of gradient updates inherent in small-batch training. Training with large batches can reduce these overheads; however it besets the convergence of the algorithm and the generalization performance. In this work, we take a first step towards analyzing how the structure (width and depth) of a neural network affects the performance of large-batch training. We present new theoretical results which suggest that--for a fixed number of parameters--wider networks are more amenable to fast large-batch training compared to deeper ones. We provide extensive experiments on residual and fully-connected neural networks which suggest that wider networks can be trained using larger batches without incurring a convergence slow-down, unlike their deeper variants.

COLA: Decentralized Linear Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #31

Lie He · An Bian · Martin Jaggi

Decentralized machine learning is a promising emerging paradigm in view of global challenges of data ownership and privacy. We consider learning of linear classification and regression models, in the setting where the training data is decentralized over many user devices, and the learning algorithm must run on-device, on an arbitrary communication network, without a central coordinator. We propose COLA, a new decentralized training algorithm with strong theoretical guarantees and superior practical performance. Our framework overcomes many limitations of existing methods, and achieves communication efficiency, scalability, elasticity as well as resilience to changes in data and allows for unreliable and heterogeneous participating devices.

Distributed Stochastic Optimization via Adaptive SGD

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #32

Ashok Cutkosky · Róbert Busa-Fekete

Stochastic convex optimization algorithms are the most popular way to train machine learning models on large-scale data. Scaling up the training process of these models is crucial, but the most popular algorithm, Stochastic Gradient Descent (SGD), is a serial method that is surprisingly hard to parallelize. In this paper, we propose an efficient distributed stochastic optimization method by combining adaptivity with variance reduction techniques. Our analysis yields a linear speedup in the number of machines, constant memory footprint, and only a logarithmic number of communication rounds. Critically, our approach is a black-box reduction that parallelizes any serial online learning algorithm, streamlining prior analysis and allowing us to leverage the significant progress that has been made in designing adaptive algorithms. In particular, we achieve optimal convergence rates without any prior knowledge of smoothness parameters, yielding a more robust algorithm that reduces the need for hyperparameter tuning. We implement our algorithm in the Spark distributed framework and exhibit dramatic performance gains on large-scale logistic regression problems.

Non-Ergodic Alternating Proximal Augmented Lagrangian Algorithms with Optimal Rates

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #33

We develop two new non-ergodic alternating proximal augmented Lagrangian algorithms (NEAPAL) to solve a class of nonsmooth constrained convex optimization problems. Our approach relies on a novel combination of the augmented Lagrangian framework, alternating/linearization scheme, Nesterov's acceleration techniques, and adaptive strategy for parameters. Our algorithms have several new features compared to existing methods. Firstly, they have a Nesterov's acceleration step on the primal variables compared to the dual one in several methods in the literature. Secondly, they achieve non-ergodic optimal convergence rates under standard assumptions, i.e. an $\mathcal{O}(\frac{1}{k})$ rate without any smoothness or strong convexity-type assumption, or an $\mathcal{O}(\frac{1}{k^2})$ rate under only semi-strong convexity, where k is the iteration counter. Thirdly, they preserve or have better per-iteration complexity compared to existing algorithms. Fourthly, they can be implemented in a parallel fashion. Finally, all the parameters are adaptively updated without heuristic tuning. We verify our algorithms on different numerical examples and compare them with some state-of-the-art methods.

Breaking the Span Assumption Yields Fast Finite-Sum Minimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #34

Robert Hannah · Yanli Liu · Daniel O'Connor · Wotao Yin

In this paper, we show that SVRG and SARA can be modified to be fundamentally faster than all of the other standard algorithms that minimize the sum of n smooth functions, such as SAGA, SAG, SDCA, and SDCA without duality. Most finite sum algorithms follow what we call the "span assumption": Their updates are in the span of a sequence of component gradients chosen in a random IID fashion. In the big data regime, where the condition number $\kappa = O(n)$, the span assumption prevents algorithms from converging to an approximate solution of accuracy ϵ in less than $n \ln(1/\epsilon)$ iterations. SVRG and SARA do not follow the span assumption since they are updated with a hybrid of full-gradient and component-gradient information. We show that because of this, they can be up to $\Omega(1 + (\ln(n/\kappa))_+)$ times faster. In particular, to obtain an accuracy $\epsilon = 1/n^\alpha$ for $\kappa = n^\beta$ and $\alpha, \beta \in (0, 1)$, modified SVRG requires $O(n)$ iterations, whereas algorithms that follow the span assumption require $O(n \ln(n))$ iterations. Moreover, we present lower bound results that show this speedup is optimal, and provide analysis to help explain why this speedup exists. With the understanding that the span assumption is a point of weakness of finite sum algorithms, future work may purposefully exploit this to yield faster algorithms in the big data regime.

Optimization for Approximate Submodularity

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #35

Yaron Singer · Avinatan Hassidim

We consider the problem of maximizing a submodular function when given access to its approximate version. Submodular functions are heavily studied in a wide variety of disciplines, since they are used to model many real world phenomena, and are amenable to optimization. However, there are many cases in which the phenomena we observe is only approximately submodular and the approximation guarantees cease to hold. We describe a technique which we call the sampled mean approximation that yields strong guarantees for maximization of submodular functions from approximate surrogates under cardinality and intersection of matroid constraints. In particular, we show tight guarantees for maximization under a cardinality constraint and $1/(1+P)$ approximation under intersection of P matroids.

Submodular Maximization via Gradient Ascent: The Case of Deep Submodular Functions

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #36

Wenruo Bai · William Stafford Noble · Jeff Bilmes

We study the problem of maximizing deep submodular functions (DSFs) subject to a matroid constraint. DSFs are an expressive class of submodular functions that include, as strict subfamilies, the facility location, weighted coverage, and sums of concave composed with modular functions. We use a strategy similar to the continuous greedy approach, but we show that the multilinear extension of any DSF has a natural and computationally attainable concave relaxation that we can optimize using gradient ascent. Our results show a guarantee of $\max_{\{0$

Maximizing Induced Cardinality Under a Determinantal Point Process

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #37

Jennifer Gillenwater · Alex Kulesza · Sergei Vassilvitskii · Zelda Mariet

Determinantal point processes (DPPs) are well-suited to recommender systems where the goal is to generate collections of diverse, high-quality items. In the existing literature this is usually formulated as finding the mode of the DPP (the so-called MAP set). However, the MAP objective inherently assumes that the DPP models "optimal" recommendation sets, and yet obtaining such a

DPP is nontrivial when there is no ready source of example optimal sets. In this paper we advocate an alternative framework for applying DPPs to recommender systems. Our approach assumes that the DPP simply models user engagements with recommended items, which is more consistent with how DPPs for recommender systems are typically trained. With this assumption, we are able to formulate a metric that measures the expected number of items that a user will engage with. We formalize this optimization of this metric as the Maximum Induced Cardinality (MIC) problem. Although the MIC objective is not submodular, we show that it can be approximated by a submodular function, and that empirically it is well-optimized by a greedy algorithm.

Efficient Algorithms for Non-convex Isotonic Regression through Submodular Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #38

Francis Bach

We consider the minimization of submodular functions subject to ordering constraints. We show that this potentially non-convex optimization problem can be cast as a convex optimization problem on a space of uni-dimensional measures, with ordering constraints corresponding to first-order stochastic dominance. We propose new discretization schemes that lead to simple and efficient algorithms based on zero-th, first, or higher order oracles; these algorithms also lead to improvements without isotonic constraints. Finally, our experiments show that non-convex loss functions can be much more robust to outliers for isotonic regression, while still being solvable in polynomial time.

Revisiting Decomposable Submodular Function Minimization with Incidence Relations

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #39

Pan Li · Olgica Milenkovic

We introduce a new approach to decomposable submodular function minimization (DSFM) that exploits incidence relations. Incidence relations describe which variables effectively influence the component functions, and when properly utilized, they allow for improving the convergence rates of DSFM solvers. Our main results include the precise parametrization of the DSFM problem based on incidence relations, the development of new scalable alternative projections and parallel coordinate descent methods and an accompanying rigorous analysis of their convergence rates.

Coordinate Descent with Bandit Sampling

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #40

Farnood Salehi · Patrick Thiran · Elisa Celis

Coordinate descent methods minimize a cost function by updating a single decision variable (corresponding to one coordinate) at a time. Ideally, we would update the decision variable that yields the largest marginal decrease in the cost function. However, finding this coordinate would require checking all of them, which is not computationally practical. Therefore, we propose a new adaptive method for coordinate descent. First, we define a lower bound on the decrease of the cost function when a coordinate is updated and, instead of calculating this lower bound for all coordinates, we use a multi-armed bandit algorithm to learn which coordinates result in the largest marginal decrease and simultaneously perform coordinate descent. We show that our approach improves the convergence of the coordinate methods both theoretically and experimentally.

Accelerated Stochastic Matrix Inversion: General Theory and Speeding up BFGS Rules for Faster Second-Order Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #41

Robert Gower · Filip Hanzely · Peter Richtarik · Sebastian Stich

We present the first accelerated randomized algorithm for solving linear systems in Euclidean spaces. One essential problem of this type is the matrix inversion problem. In particular, our algorithm can be specialized to invert positive definite matrices in such a way that all iterates (approximate solutions) generated by the algorithm are positive definite matrices themselves. This opens the way for many applications in the field of optimization and machine learning. As an application of our general theory, we develop the first accelerated (deterministic and stochastic) quasi-Newton updates. Our updates lead to provably more aggressive approximations of the inverse Hessian, and lead to speed-ups over classical non-accelerated rules in numerical experiments. Experiments with empirical risk minimization show that our rules can accelerate training of machine learning models.

Stochastic Cubic Regularization for Fast Nonconvex Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #42

Nilesh Tripuraneni · Mitchell Stern · Chi Jin · Jeffrey Regier · Michael Jordan

This paper proposes a stochastic variant of a classic algorithm---the cubic-regularized Newton method [Nesterov and Polyak]. The proposed algorithm efficiently escapes saddle points and finds approximate local minima for general smooth, nonconvex functions in only $\tilde{O}(\epsilon^{-3.5})$ stochastic gradient and stochastic Hessian-vector product evaluations. The latter can be computed as efficiently as stochastic gradients. This improves upon the $\tilde{O}(\epsilon^{-4})$ rate of stochastic gradient descent. Our rate matches the best-known result for finding local minima without requiring any delicate acceleration or variance-reduction techniques.

On the Local Minima of the Empirical Risk

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #43

Chi Jin · Lydia T. Liu · Rong Ge · Michael Jordan

Population risk is always of primary interest in machine learning; however, learning algorithms only have access to the empirical risk. Even for applications with nonconvex non-smooth losses (such as modern deep networks), the population risk is generally significantly more well behaved from an optimization point of view than the empirical risk. In particular, sampling can create many spurious local minima. We consider a general framework which aims to optimize a smooth nonconvex function F (population risk) given only access to an approximation f (empirical risk) that is pointwise close to F (i.e., $\|F - f\|_{\infty} \leq \nu$). Our objective is to find the ϵ -approximate local minima of the underlying function F while avoiding the shallow local minima---arising because of the tolerance ν ---which exist only in f . We propose a simple algorithm based on stochastic gradient descent (SGD) on a smoothed version of f that is guaranteed to achieve our goal as long as $\nu \leq O(\epsilon^{1.5}/d)$. We also provide an almost matching lower bound showing that our algorithm achieves optimal error tolerance ν among all algorithms making a polynomial number of queries of f . As a concrete example, we show that our results can be directly used to give sample complexities for learning a ReLU unit.

Stochastic Nested Variance Reduced Gradient Descent for Nonconvex Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #44

Dongruo Zhou · Pan Xu · Quanquan Gu

We study finite-sum nonconvex optimization problems, where the objective function is an average of n nonconvex functions. We propose a new stochastic gradient descent algorithm based on nested variance reduction. Compared with conventional stochastic variance reduced gradient (SVRG) algorithm that uses two reference points to construct a semi-stochastic gradient with diminishing

variance in each epoch, our algorithm uses $K+1$ nested reference points to build an semi-stochastic gradient to further reduce its variance in each epoch. For smooth functions, the proposed algorithm converges to an approximate first order stationary point (i.e., $\|\nabla F(\mathbf{x})\|_2 \leq \epsilon$) within $\mathcal{O}(n \land \epsilon^{-2} + \epsilon^{-3} \land n^{\frac{1}{2}} \epsilon^{-2})$ ^{$\mathcal{O}(\cdot)$ hides the logarithmic factors} number of stochastic gradient evaluations, where n is the number of component functions, and ϵ is the optimization error. This improves the best known gradient complexity of SVRG $\mathcal{O}(n + n^{\frac{2}{3}} \epsilon^{-2})$ and the best gradient complexity of SCSG $\mathcal{O}(\epsilon^{-\frac{5}{3}} \land n^{\frac{2}{3}} \epsilon^{-2})$. For gradient dominated functions, our algorithm achieves $\mathcal{O}(n \land \tau \epsilon^{-1} + \tau \cdot (n^{\frac{1}{2}} \land (\tau \epsilon^{-1})^{\frac{1}{2}}))$ gradient complexity, which again beats the existing best gradient complexity $\mathcal{O}(n \land \tau \epsilon^{-1} + \tau \cdot (n^{\frac{1}{2}} \land (\tau \epsilon^{-1})^{\frac{1}{2}})^{\frac{2}{3}})$ achieved by SCSG. Thorough experimental results on different nonconvex optimization problems back up our theory.

NEON2: Finding Local Minima via First-Order Oracles

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #45

Zeyuan Allen-Zhu · Yuanzhi Li

We propose a reduction for non-convex optimization that can (1) turn an stationary-point finding algorithm into an local-minimum finding one, and (2) replace the Hessian-vector product computations with only gradient computations. It works both in the stochastic and the deterministic settings, without hurting the algorithm's performance. As applications, our reduction turns Natasha2 into a first-order method without hurting its theoretical performance. It also converts SGD, GD, SCSG, and SVRG into algorithms finding approximate local minima, outperforming some best known results.

How Much Restricted Isometry is Needed In Nonconvex Matrix Recovery?

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #46

Richard Zhang · Cedric Jozs · Somayeh Sojoudi · Javad Lavaei

When the linear measurements of an instance of low-rank matrix recovery satisfy a restricted isometry property (RIP) --- i.e. they are approximately norm-preserving --- the problem is known to contain no spurious local minima, so exact recovery is guaranteed. In this paper, we show that moderate RIP is not enough to eliminate spurious local minima, so existing results can only hold for near-perfect RIP. In fact, counterexamples are ubiquitous: every \mathbf{x} is the spurious local minimum of a rank-1 instance of matrix recovery that satisfies RIP. One specific counterexample has RIP

constant $\delta=1/2$, but causes randomly initialized stochastic gradient descent (SGD) to fail 12% of the time. SGD is frequently able to avoid and escape spurious local minima, but this empirical result shows that it can occasionally be defeated by their existence. Hence, while exact recovery guarantees will likely require a proof of no spurious local minima, arguments based solely on norm preservation will only be applicable to a narrow set of nearly-isotropic instances.

Escaping Saddle Points in Constrained Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #47

Aryan Mokhtari · Asuman Ozdaglar · Ali Jadbabaie

In this paper, we study the problem of escaping from saddle points in smooth nonconvex optimization problems subject to a convex set \mathcal{C} . We propose a generic framework that yields convergence to a second-order stationary point of the problem, if the convex set \mathcal{C} is simple for a quadratic objective function. Specifically, our results hold if one can find a ρ -approximate solution of a quadratic program subject to \mathcal{C} in polynomial time, where $\rho < 1$ is a positive constant that depends on the structure of the set \mathcal{C} . Under this condition, we show that the sequence of iterates generated by the proposed framework reaches an (ϵ, γ) -second order stationary point (SOSP) in at most $\mathcal{O}(\max\{\epsilon^{-2}, \rho^{-3}\} \gamma^{-3})$ iterations. We further characterize the overall complexity of reaching an SOSP when the convex set \mathcal{C} can be written as a set of quadratic constraints and the objective function Hessian has a specific structure over the convex \mathcal{C} . Finally, we extend our results to the stochastic setting and characterize the number of stochastic gradient and Hessian evaluations to reach an (ϵ, γ) -SOSP.

Analysis of Krylov Subspace Solutions of Regularized Non-Convex Quadratic Problems

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #48

Yair Carmon · John Duchi

We provide convergence rates for Krylov subspace solutions to the trust-region and cubic-regularized (nonconvex) quadratic problems. Such solutions may be efficiently computed by the Lanczos method and have long been used in practice. We prove error bounds of the form $1/t^2$ and $e^{-4t/\sqrt{\kappa}}$, where κ is a condition number for the problem, and t is the Krylov subspace order (number of Lanczos iterations). We also provide lower bounds showing that our analysis is sharp.

SPIDER: Near-Optimal Non-Convex Optimization via Stochastic Path-Integrated Differential Estimator

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #49

Cong Fang · Chris Junchi Li · Zhouchen Lin · Tong Zhang

In this paper, we propose a new technique named `\textit{Stochastic Path-Integrated Differential Estimator}` (SPIDER), which can be used to track many deterministic quantities of interests with significantly reduced computational cost. Combining SPIDER with the method of normalized gradient descent, we propose SPIDER-SFO that solve non-convex stochastic optimization problems using stochastic gradients only. We provide a few error-bound results on its convergence rates. Specially, we prove that the SPIDER-SFO algorithm achieves a gradient computation cost of $\mathcal{O}(\min(n^{1/2} \epsilon^{-2}, \epsilon^{-3}))$ to find an ϵ -approximate first-order stationary point. In addition, we prove that SPIDER-SFO nearly matches the algorithmic lower bound for finding stationary point under the gradient Lipschitz assumption in the finite-sum setting. Our SPIDER technique can be further applied to find an $(\epsilon, \mathcal{O}(\epsilon^{0.5}))$ -approximate second-order stationary point at a gradient computation cost of $\tilde{\mathcal{O}}(\min(n^{1/2} \epsilon^{-2} + \epsilon^{-2.5}, \epsilon^{-3}))$.

Natasha 2: Faster Non-Convex Optimization Than SGD

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #50

Zeyuan Allen-Zhu

We design a stochastic algorithm to find ϵ -approximate local minima of any smooth nonconvex function in rate $\mathcal{O}(\epsilon^{-3.25})$, with only oracle access to stochastic gradients. The best result before this work was $\mathcal{O}(\epsilon^{-4})$ by stochastic gradient descent (SGD).

Zeroth-Order Stochastic Variance Reduction for Nonconvex Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #51

Sijia Liu · Bhavya Kailkhura · Pin-Yu Chen · Paishun Ting · Shiyu Chang · Lisa Amini

As application demands for zeroth-order (gradient-free) optimization accelerate, the need for variance reduced and faster converging approaches is also intensifying. This paper addresses these challenges by presenting: a) a comprehensive theoretical analysis of variance reduced zeroth-order (ZO) optimization, b) a novel variance reduced ZO algorithm, called ZO-SVRG, and c) an experimental evaluation of our approach in the context of two compelling applications, black-box chemical material classification and generation of adversarial examples from black-box deep neural network models. Our theoretical analysis uncovers an essential difficulty in the analysis of ZO-SVRG: the unbiased assumption on gradient estimates no longer holds. We prove that compared to its first-order counterpart, ZO-SVRG with a two-point random gradient estimator could suffer an additional error of order $O(1/b)$, where b is the mini-batch size. To mitigate this error, we propose two accelerated versions of ZO-SVRG utilizing variance reduced gradient estimators, which achieve the best rate known for ZO stochastic optimization (in terms of iterations). Our extensive experimental results show that our approaches outperform other state-of-the-art ZO algorithms, and strike a balance between the convergence rate and the function query complexity.

Structured Local Minima in Sparse Blind Deconvolution

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #52

Yuqian Zhang · Han-wen Kuo · John Wright

Blind deconvolution is a ubiquitous problem of recovering two unknown signals from their convolution. Unfortunately, this is an ill-posed problem in general. This paper focuses on the {short and sparse} blind deconvolution problem, where the one unknown signal is short and the other one is sparsely and randomly supported. This variant captures the structure of the unknown signals in several important applications. We assume the short signal to have unit ℓ^2 norm and cast the blind deconvolution problem as a nonconvex optimization problem over the sphere. We demonstrate that (i) in a certain region of the sphere, every local optimum is close to some shift truncation of the ground truth, and (ii) for a generic short signal of length k , when the sparsity of activation signal $\|\theta\| \lesssim k^{-2/3}$ and number of measurements $m \gtrsim \text{poly}(k)$, a simple initialization method together with a descent algorithm which escapes strict saddle points recovers a near shift truncation of the ground truth kernel.

Algorithmic Regularization in Learning Deep Homogeneous Models: Layers are Automatically Balanced

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #53

Simon Du · Wei Hu · Jason Lee

We study the implicit regularization imposed by gradient descent for learning multi-layer

homogeneous functions including feed-forward fully connected and convolutional deep neural networks with linear, ReLU or Leaky ReLU activation. We rigorously prove that gradient flow (i.e. gradient descent with infinitesimal step size) effectively enforces the differences between squared norms across different layers to remain invariant without any explicit regularization. This result implies that if the weights are initially small, gradient flow automatically balances the magnitudes of all layers. Using a discretization argument, we analyze gradient descent with positive step size for the non-convex low-rank asymmetric matrix factorization problem without any regularization. Inspired by our findings for gradient flow, we prove that gradient descent with step sizes $\eta_t = O(t^{-(1/2 + \delta)})$ (0

Are ResNets Provably Better than Linear Predictors?

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #54

Ohad Shamir

A residual network (or ResNet) is a standard deep neural net architecture, with state-of-the-art performance across numerous applications. The main premise of ResNets is that they allow the training of each layer to focus on fitting just the residual of the previous layer's output and the target output. Thus, we should expect that the trained network is no worse than what we can obtain if we remove the residual layers and train a shallower network instead. However, due to the non-convexity of the optimization problem, it is not at all clear that ResNets indeed achieve this behavior, rather than getting stuck at some arbitrarily poor local minimum. In this paper, we rigorously prove that arbitrarily deep, nonlinear residual units indeed exhibit this behavior, in the sense that the optimization landscape contains no local minima with value above what can be obtained with a linear predictor (namely a 1-layer network). Notably, we show this under minimal or no assumptions on the precise network architecture, data distribution, or loss function used. We also provide a quantitative analysis of approximate stationary points for this problem. Finally, we show that with a certain tweak to the architecture, training the network with standard stochastic gradient descent achieves an objective value close or better than any linear predictor.

Adaptive Methods for Nonconvex Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #55

Manzil Zaheer · Sashank Reddi · Devendra Sachan · Satyen Kale · Sanjiv Kumar

Adaptive gradient methods that rely on scaling gradients down by the square root of exponential moving averages of past squared gradients, such RMSProp, Adam, Adadelta have found wide application in optimizing the nonconvex problems that arise in deep learning. However, it has been recently demonstrated that such methods can fail to converge even in simple convex optimization

settings. In this work, we provide a new analysis of such methods applied to nonconvex stochastic optimization problems, characterizing the effect of increasing minibatch size. Our analysis shows that under this scenario such methods do converge to stationarity up to the statistical limit of variance in the stochastic gradients (scaled by a constant factor). In particular, our result implies that increasing minibatch sizes enables convergence, thus providing a way to circumvent the non-convergence issues. Furthermore, we provide a new adaptive optimization algorithm, Yogi, which controls the increase in effective learning rate, leading to even better performance with similar theoretical guarantees on convergence. Extensive experiments show that Yogi with very little hyperparameter tuning outperforms methods such as Adam in several challenging machine learning tasks.

Alternating optimization of decision trees, with application to learning sparse oblique trees

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #56

Miguel A. Carreira-Perpinan · Pooya Tavallali

Learning a decision tree from data is a difficult optimization problem. The most widespread algorithm in practice, dating to the 1980s, is based on a greedy growth of the tree structure by recursively splitting nodes, and possibly pruning back the final tree. The parameters (decision function) of an internal node are approximately estimated by minimizing an impurity measure. We give an algorithm that, given an input tree (its structure and the parameter values at its nodes), produces a new tree with the same or smaller structure but new parameter values that provably lower or leave unchanged the misclassification error. This can be applied to both axis-aligned and oblique trees and our experiments show it consistently outperforms various other algorithms while being highly scalable to large datasets and trees. Further, the same algorithm can handle a sparsity penalty, so it can learn sparse oblique trees, having a structure that is a subset of the original tree and few nonzero parameters. This combines the best of axis-aligned and oblique trees: flexibility to model correlated data, low generalization error, fast inference and interpretable nodes that involve only a few features in their decision.

GILBO: One Metric to Measure Them All

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #57

Alexander Alemi · Ian Fischer

We propose a simple, tractable lower bound on the mutual information contained in the joint generative density of any latent variable generative model: the GILBO (Generative Information Lower BOund). It offers a data-independent measure of the complexity of the learned latent variable

description, giving the log of the effective description length. It is well-defined for both VAEs and GANs. We compute the GILBO for 800 GANs and VAEs each trained on four datasets (MNIST, FashionMNIST, CIFAR-10 and CelebA) and discuss the results.

Isolating Sources of Disentanglement in Variational Autoencoders

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #58

Tian Qi Chen · Xuechen Li · Roger Grosse · David Duvenaud

We decompose the evidence lower bound to show the existence of a term measuring the total correlation between latent variables. We use this to motivate the beta-TCVAE (Total Correlation Variational Autoencoder) algorithm, a refinement and plug-in replacement of the beta-VAE for learning disentangled representations, requiring no additional hyperparameters during training. We further propose a principled classifier-free measure of disentanglement called the mutual information gap (MIG). We perform extensive quantitative and qualitative experiments, in both restricted and non-restricted settings, and show a strong relation between total correlation and disentanglement, when the model is trained using our framework.

On GANs and GMMs

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #59

Eitan Richardson · Yair Weiss

A longstanding problem in machine learning is to find unsupervised methods that can learn the statistical structure of high dimensional signals. In recent years, GANs have gained much attention as a possible solution to the problem, and in particular have shown the ability to generate remarkably realistic high resolution sampled images. At the same time, many authors have pointed out that GANs may fail to model the full distribution ("mode collapse") and that using the learned models for anything other than generating samples may be very difficult. In this paper, we examine the utility of GANs in learning statistical models of images by comparing them to perhaps the simplest statistical model, the Gaussian Mixture Model. First, we present a simple method to evaluate generative models based on relative proportions of samples that fall into predetermined bins. Unlike previous automatic methods for evaluating models, our method does not rely on an additional neural network nor does it require approximating intractable computations. Second, we compare the performance of GANs to GMMs trained on the same datasets. While GMMs have previously been shown to be successful in modeling small patches of images, we show how to train them on full sized images despite the high dimensionality. Our results show that GMMs can generate realistic samples (although less sharp than those of GANs) but also capture the full distribution,

which GANs fail to do. Furthermore, GMMs allow efficient inference and explicit representation of the underlying statistical structure. Finally, we discuss how GMMs can be used to generate sharp images.

Assessing Generative Models via Precision and Recall

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #60

Mehdi S. M. Sajjadi · Olivier Bachem · Mario Lucic · Olivier Bousquet · Sylvain Gelly

Recent advances in generative modeling have led to an increased interest in the study of statistical divergences as means of model comparison. Commonly used evaluation methods, such as the Frechet Inception Distance (FID), correlate well with the perceived quality of samples and are sensitive to mode dropping. However, these metrics are unable to distinguish between different failure cases since they only yield one-dimensional scores. We propose a novel definition of precision and recall for distributions which disentangles the divergence into two separate dimensions. The proposed notion is intuitive, retains desirable properties, and naturally leads to an efficient algorithm that can be used to evaluate generative models. We relate this notion to total variation as well as to recent evaluation metrics such as Inception Score and FID. To demonstrate the practical utility of the proposed approach we perform an empirical study on several variants of Generative Adversarial Networks and Variational Autoencoders. In an extensive set of experiments we show that the proposed metric is able to disentangle the quality of generated samples from the coverage of the target distribution.

Gather-Excite: Exploiting Feature Context in Convolutional Neural Networks

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #61

Jie Hu · Li Shen · Samuel Albanie · Gang Sun · Andrea Vedaldi

While the use of bottom-up local operators in convolutional neural networks (CNNs) matches well some of the statistics of natural images, it may also prevent such models from capturing contextual long-range feature interactions. In this work, we propose a simple, lightweight approach for better context exploitation in CNNs. We do so by introducing a pair of operators: gather, which efficiently aggregates feature responses from a large spatial extent, and excite, which redistributes the pooled information to local features. The operators are cheap, both in terms of number of added parameters and computational complexity, and can be integrated directly in existing architectures to improve their performance. Experiments on several datasets show that gather-excite can bring benefits comparable to increasing the depth of a CNN at a fraction of the cost. For example, we find ResNet-50 with gather-excite operators is able to outperform its 101-layer counterpart on ImageNet

with no additional learnable parameters. We also propose a parametric gather-excite operator pair which yields further performance gains, relate it to the recently-introduced Squeeze-and-Excitation Networks, and analyse the effects of these changes to the CNN feature activation statistics.

Uncertainty-Aware Attention for Reliable Interpretation and Prediction

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #62

Jay Heo · Hae Beom Lee · Saehoon Kim · Juho Lee · Kwang Joon Kim · Eunho Yang · Sung Ju Hwang

Attention mechanism is effective in both focusing the deep learning models on relevant features and interpreting them. However, attentions may be unreliable since the networks that generate them are often trained in a weakly-supervised manner. To overcome this limitation, we introduce the notion of input-dependent uncertainty to the attention mechanism, such that it generates attention for each feature with varying degrees of noise based on the given input, to learn larger variance on instances it is uncertain about. We learn this Uncertainty-aware Attention (UA) mechanism using variational inference, and validate it on various risk prediction tasks from electronic health records on which our model significantly outperforms existing attention models. The analysis of the learned attentions shows that our model generates attentions that comply with clinicians' interpretation, and provide richer interpretation via learned variance. Further evaluation of both the accuracy of the uncertainty calibration and the prediction performance with "I don't know" decision show that UA yields networks with high reliability as well.

Forecasting Treatment Responses Over Time Using Recurrent Marginal Structural Networks

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #63

Bryan Lim · Ahmed M. Alaa · Mihaela van der Schaar

Electronic health records provide a rich source of data for machine learning methods to learn dynamic treatment responses over time. However, any direct estimation is hampered by the presence of time-dependent confounding, where actions taken are dependent on time-varying variables related to the outcome of interest. Drawing inspiration from marginal structural models, a class of methods in epidemiology which use propensity weighting to adjust for time-dependent confounders, we introduce the Recurrent Marginal Structural Network - a sequence-to-sequence architecture for forecasting a patient's expected response to a series of planned treatments. Using simulations of a state-of-the-art pharmacokinetic-pharmacodynamic (PK-PD) model of tumor growth, we demonstrate the ability of our network to accurately learn unbiased treatment responses from observational data - even under changes in the policy of treatment assignments - and performance

gains over benchmarks.

Backpropagation with Callbacks: Foundations for Efficient and Expressive Differentiable Programming

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #64

Fei Wang · James Decker · Xilun Wu · Gregory Essertel · Tiark Rompf

Training of deep learning models depends on gradient descent and end-to-end differentiation. Under the slogan of differentiable programming, there is an increasing demand for efficient automatic gradient computation for emerging network architectures that incorporate dynamic control flow, especially in NLP. In this paper we propose an implementation of backpropagation using functions with callbacks, where the forward pass is executed as a sequence of function calls, and the backward pass as a corresponding sequence of function returns. A key realization is that this technique of chaining callbacks is well known in the programming languages community as continuation-passing style (CPS). Any program can be converted to this form using standard techniques, and hence, any program can be mechanically converted to compute gradients. Our approach achieves the same flexibility as other reverse-mode automatic differentiation (AD) techniques, but it can be implemented without any auxiliary data structures besides the function call stack, and it can easily be combined with graph construction and native code generation techniques through forms of multi-stage programming, leading to a highly efficient implementation that combines the performance benefits of define-then-run software frameworks such as TensorFlow with the expressiveness of define-by-run frameworks such as PyTorch.

Recurrent World Models Facilitate Policy Evolution

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #65

David Ha · Jürgen Schmidhuber

A generative recurrent neural network is quickly trained in an unsupervised manner to model popular reinforcement learning environments through compressed spatio-temporal representations. The world model's extracted features are fed into compact and simple policies trained by evolution, achieving state of the art results in various environments. We also train our agent entirely inside of an environment generated by its own internal world model, and transfer this policy back into the actual environment. Interactive version of this paper is available at <https://worldmodels.github.io>

Long short-term memory and Learning-to-learn in networks of spiking neurons

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #66

Guillaume Bellec · Darjan Salaj · Anand Subramoney · Robert Legenstein · Wolfgang Maass

Recurrent networks of spiking neurons (RSNNs) underlie the astounding computing and learning capabilities of the brain. But computing and learning capabilities of RSNN models have remained poor, at least in comparison with ANNs. We address two possible reasons for that. One is that RSNNs in the brain are not randomly connected or designed according to simple rules, and they do not start learning as a tabula rasa network. Rather, RSNNs in the brain were optimized for their tasks through evolution, development, and prior experience. Details of these optimization processes are largely unknown. But their functional contribution can be approximated through powerful optimization methods, such as backpropagation through time (BPTT). A second major mismatch between RSNNs in the brain and models is that the latter only show a small fraction of the dynamics of neurons and synapses in the brain. We include neurons in our RSNN model that reproduce one prominent dynamical process of biological neurons that takes place at the behaviourally relevant time scale of seconds: neuronal adaptation. We denote these networks as LSNNs because of their Long short-term memory. The inclusion of adapting neurons drastically increases the computing and learning capability of RSNNs if they are trained and configured by deep learning (BPTT combined with a rewiring algorithm that optimizes the network architecture). In fact, the computational performance of these RSNNs approaches for the first time that of LSTM networks. In addition RSNNs with adapting neurons can acquire abstract knowledge from prior learning in a Learning-to-Learn (L2L) scheme, and transfer that knowledge in order to learn new but related tasks from very few examples. We demonstrate this for supervised learning and reinforcement learning.

Distributed Weight Consolidation: A Brain Segmentation Case Study

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #67

Patrick McClure · Charles Zheng · Jakub Kaczmarzyk · John Rogers-Lee · Satra Ghosh · Dylan Nielson · Peter A Bandettini · Francisco Pereira

Collecting the large datasets needed to train deep neural networks can be very difficult, particularly for the many applications for which sharing and pooling data is complicated by practical, ethical, or legal concerns. However, it may be the case that derivative datasets or predictive models developed within individual sites can be shared and combined with fewer restrictions. Training on distributed data and combining the resulting networks is often viewed as continual learning, but these methods require networks to be trained sequentially. In this paper, we introduce distributed weight consolidation (DWC), a continual learning method to consolidate the weights of separate neural

networks, each trained on an independent dataset. We evaluated DWC with a brain segmentation case study, where we consolidated dilated convolutional neural networks trained on independent structural magnetic resonance imaging (sMRI) datasets from different sites. We found that DWC led to increased performance on test sets from the different sites, while maintaining generalization performance for a very large and completely independent multi-site dataset, compared to an ensemble baseline.

Learning to Play With Intrinsically-Motivated, Self-Aware Agents

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #68

Nick Haber · Damian Mrowca · Stephanie Wang · Li Fei-Fei · Daniel Yamins

Infants are experts at playing, with an amazing ability to generate novel structured behaviors in unstructured environments that lack clear extrinsic reward signals. We seek to mathematically formalize these abilities using a neural network that implements curiosity-driven intrinsic motivation. Using a simple but ecologically naturalistic simulated environment in which an agent can move and interact with objects it sees, we propose a "world-model" network that learns to predict the dynamic consequences of the agent's actions. Simultaneously, we train a separate explicit "self-model" that allows the agent to track the error map of its world-model. It then uses the self-model to adversarially challenge the developing world-model. We demonstrate that this policy causes the agent to explore novel and informative interactions with its environment, leading to the generation of a spectrum of complex behaviors, including ego-motion prediction, object attention, and object gathering. Moreover, the world-model that the agent learns supports improved performance on object dynamics prediction, detection, localization and recognition tasks. Taken together, our results are initial steps toward creating flexible autonomous agents that self-supervise in realistic physical environments.

Gradient Descent for Spiking Neural Networks

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #69

Dongsung Huh · Terrence J Sejnowski

Most large-scale network models use neurons with static nonlinearities that produce analog output, despite the fact that information processing in the brain is predominantly carried out by dynamic neurons that produce discrete pulses called spikes. Research in spike-based computation has been impeded by the lack of efficient supervised learning algorithm for spiking neural networks. Here, we present a gradient descent method for optimizing spiking network models by introducing a differentiable formulation of spiking dynamics and deriving the exact gradient calculation. For

demonstration, we trained recurrent spiking networks on two dynamic tasks: one that requires optimizing fast (\sim millisecond) spike-based interactions for efficient encoding of information, and a delayed-memory task over extended duration (\sim second). The results show that the gradient descent approach indeed optimizes networks dynamics on the time scale of individual spikes as well as on behavioral time scales. In conclusion, our method yields a general purpose supervised learning algorithm for spiking neural networks, which can facilitate further investigations on spike-based computations.

Demystifying excessively volatile human learning: A Bayesian persistent prior and a neural approximation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #70

Chaitanya Ryali · Gautam Reddy · Angela J Yu

Understanding how humans and animals learn about statistical regularities in stable and volatile environments, and utilize these regularities to make predictions and decisions, is an important problem in neuroscience and psychology. Using a Bayesian modeling framework, specifically the Dynamic Belief Model (DBM), it has previously been shown that humans tend to make the $\{it\}$ default assumption that environmental statistics undergo abrupt, unsignaled changes, even when environmental statistics are actually stable. Because exact Bayesian inference in this setting, an example of switching state space models, is computationally intense, a number of approximately Bayesian and heuristic algorithms have been proposed to account for learning/prediction in the brain. Here, we examine a neurally plausible algorithm, a special case of leaky integration dynamics we denote as EXP (for exponential filtering), that is significantly simpler than all previously suggested algorithms except for the delta-learning rule, and which far outperforms the delta rule in approximating Bayesian prediction performance. We derive the theoretical relationship between DBM and EXP, and show that EXP gains computational efficiency by foregoing the representation of inferential uncertainty (as does the delta rule), but that it nevertheless achieves near-Bayesian performance due to its ability to incorporate a "persistent prior" influence unique to DBM and absent from the other algorithms. Furthermore, we show that EXP is comparable to DBM but better than all other models in reproducing human behavior in a visual search task, suggesting that human learning and prediction also incorporates an element of persistent prior. More broadly, our work demonstrates that when observations are information-poor, detecting changes or modulating the learning rate is both $\{it\}$ difficult and (thus) $\{it\}$ unnecessary for making Bayes-optimal predictions.

Temporal alignment and latent Gaussian process factor

inference in population spike trains

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #71

Lea Duncker · Maneesh Sahani

We introduce a novel scalable approach to identifying common latent structure in neural population spike-trains, which allows for variability both in the trajectory and in the rate of progression of the underlying computation. Our approach is based on shared latent Gaussian processes (GPs) which are combined linearly, as in the Gaussian Process Factor Analysis (GPFA) algorithm. We extend GPFA to handle unbinned spike-train data by incorporating a continuous time point-process likelihood model, achieving scalability with a sparse variational approximation. Shared variability is separated into terms that express condition dependence, as well as trial-to-trial variation in trajectories. Finally, we introduce a nested GP formulation to capture variability in the rate of evolution along the trajectory. We show that the new method learns to recover latent trajectories in synthetic data, and can accurately identify the trial-to-trial timing of movement-related parameters from motor cortical data without any supervision.

Information-based Adaptive Stimulus Selection to Optimize Communication Efficiency in Brain-Computer Interfaces

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #72

Boyla Mainsah · Dmitry Kalika · Leslie Collins · Siyuan Liu · Chandra Throckmorton

Stimulus-driven brain-computer interfaces (BCIs), such as the P300 speller, rely on using a sequence of sensory stimuli to elicit specific neural responses as control signals, while a user attends to relevant target stimuli that occur within the sequence. In current BCIs, the stimulus presentation schedule is typically generated in a pseudo-random fashion. Given the non-stationarity of brain electrical signals, a better strategy could be to adapt the stimulus presentation schedule in real-time by selecting the optimal stimuli that will maximize the signal-to-noise ratios of the elicited neural responses and provide the most information about the user's intent based on the uncertainties of the data being measured. However, the high-dimensional stimulus space limits the development of algorithms with tractable solutions for optimized stimulus selection to allow for real-time decision-making within the stringent time requirements of BCI processing. We derive a simple analytical solution of an information-based objective function for BCI stimulus selection by transforming the high-dimensional stimulus space into a one-dimensional space that parameterizes the objective function - the prior probability mass of the stimulus under consideration, irrespective of its contents. We demonstrate the utility of our adaptive stimulus selection algorithm in improving BCI performance with results from simulation and real-time human experiments.

Model-based targeted dimensionality reduction for neuronal population data

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #73

Mikio Aoi · Jonathan W Pillow

Summarizing high-dimensional data using a small number of parameters is a ubiquitous first step in the analysis of neuronal population activity. Recently developed methods use "targeted" approaches that work by identifying multiple, distinct low-dimensional subspaces of activity that capture the population response to individual experimental task variables, such as the value of a presented stimulus or the behavior of the animal. These methods have gained attention because they decompose total neural activity into what are ostensibly different parts of a neuronal computation. However, existing targeted methods have been developed outside of the confines of probabilistic modeling, making some aspects of the procedures ad hoc, or limited in flexibility or interpretability. Here we propose a new model-based method for targeted dimensionality reduction based on a probabilistic generative model of the population response data. The low-dimensional structure of our model is expressed as a low-rank factorization of a linear regression model. We perform efficient inference using a combination of expectation maximization and direct maximization of the marginal likelihood. We also develop an efficient method for estimating the dimensionality of each subspace. We show that our approach outperforms alternative methods in both mean squared error of the parameter estimates, and in identifying the correct dimensionality of encoding using simulated data. We also show that our method provides more accurate inference of low-dimensional subspaces of activity than a competing algorithm, demixed PCA.

Objective and efficient inference for couplings in neuronal networks

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #74

Yu Terada · Tomoyuki Obuchi · Takuya Isomura · Yoshiyuki Kabashima

Inferring directional couplings from the spike data of networks is desired in various scientific fields such as neuroscience. Here, we apply a recently proposed objective procedure to the spike data obtained from the Hodgkin-Huxley type models and in vitro neuronal networks cultured in a circular structure. As a result, we succeed in reconstructing synaptic connections accurately from the evoked activity as well as the spontaneous one. To obtain the results, we invent an analytic formula approximately implementing a method of screening relevant couplings. This significantly reduces the computational cost of the screening method employed in the proposed objective procedure, making it possible to treat large-size systems as in this study.

The emergence of multiple retinal cell types through efficient coding of natural movies

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #75

Samuel Ocko · Jack Lindsey · Surya Ganguli · Stephane Deny

One of the most striking aspects of early visual processing in the retina is the immediate parcellation of visual information into multiple parallel pathways, formed by different retinal ganglion cell types each tiling the entire visual field. Existing theories of efficient coding have been unable to account for the functional advantages of such cell-type diversity in encoding natural scenes. Here we go beyond previous theories to analyze how a simple linear retinal encoding model with different convolutional cell types efficiently encodes naturalistic spatiotemporal movies given a fixed firing rate budget. We find that optimizing the receptive fields and cell densities of two cell types makes them match the properties of the two main cell types in the primate retina, midget and parasol cells, in terms of spatial and temporal sensitivity, cell spacing, and their relative ratio. Moreover, our theory gives a precise account of how the ratio of midget to parasol cells decreases with retinal eccentricity. Also, we train a nonlinear encoding model with a rectifying nonlinearity to efficiently encode naturalistic movies, and again find emergent receptive fields resembling those of midget and parasol cells that are now further subdivided into ON and OFF types. Thus our work provides a theoretical justification, based on the efficient coding of natural movies, for the existence of the four most dominant cell types in the primate retina that together comprise 70% of all ganglion cells.

Benefits of over-parameterization with EM

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #76

Ji Xu · Daniel Hsu · Arian Maleki

Expectation Maximization (EM) is among the most popular algorithms for maximum likelihood estimation, but it is generally only guaranteed to find its stationary points of the log-likelihood objective. The goal of this article is to present theoretical and empirical evidence that over-parameterization can help EM avoid spurious local optima in the log-likelihood. We consider the problem of estimating the mean vectors of a Gaussian mixture model in a scenario where the mixing weights are known. Our study shows that the global behavior of EM, when one uses an over-parameterized model in which the mixing weights are treated as unknown, is better than that when one uses the (correct) model with the mixing weights fixed to the known values. For symmetric Gaussians mixtures with two components, we prove that introducing the (statistically redundant) weight parameters enables EM to find the global maximizer of the log-likelihood starting from almost any initial mean parameters, whereas EM without this over-parameterization may very often fail. For other Gaussian mixtures, we provide empirical evidence that shows similar behavior. Our

results corroborate the value of over-parameterization in solving non-convex optimization problems, previously observed in other domains.

On Coresets for Logistic Regression

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #77

Alexander Munteanu · Chris Schwiegelshohn · Christian Sohler · David Woodruff

Coresets are one of the central methods to facilitate the analysis of large data. We continue a recent line of research applying the theory of coresets to logistic regression. First, we show the negative result that no strongly sublinear sized coresets exist for logistic regression. To deal with intractable worst-case instances we introduce a complexity measure $\mu(X)$, which quantifies the hardness of compressing a data set for logistic regression. $\mu(X)$ has an intuitive statistical interpretation that may be of independent interest. For data sets with bounded $\mu(X)$ -complexity, we show that a novel sensitivity sampling scheme produces the first provably sublinear $(1 \pm \epsilon)$ -coreset. We illustrate the performance of our method by comparing to uniform sampling as well as to state of the art methods in the area. The experiments are conducted on real world benchmark data for logistic regression.

On Learning Markov Chains

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #78

Yi HAO · Alon Orlitsky · Venkatadheeraj Pichapati

The problem of estimating an unknown discrete distribution from its samples is a fundamental tenet of statistical learning. Over the past decade, it attracted significant research effort and has been solved for a variety of divergence measures. Surprisingly, an equally important problem, estimating an unknown Markov chain from its samples, is still far from understood. We consider two problems related to the min-max risk (expected loss) of estimating an unknown k -state Markov chain from its n sequential samples: predicting the conditional distribution of the next sample with respect to the KL-divergence, and estimating the transition matrix with respect to a natural loss induced by KL or a more general f -divergence measure. For the first measure, we determine the min-max prediction risk to within a linear factor in the alphabet size, showing it is $\Omega(k \log \log n/n)$ and $O(k^2 \log \log n/n)$. For the second, if the transition probabilities can be arbitrarily small, then only trivial uniform risk upper bounds can be derived. We therefore consider transition probabilities that are bounded away from zero, and resolve the problem for essentially all sufficiently smooth f -divergences, including KL-, L_2 -, Chi-squared, Hellinger, and Alpha-divergences.

Contextual Stochastic Block Models

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #79

Yash Deshpande · Subhabrata Sen · Andrea Montanari · Elchanan Mossel

We provide the first information theoretical tight analysis for inference of latent community structure given a sparse graph along with high dimensional node covariates, correlated with the same latent communities. Our work bridges recent theoretical breakthroughs in detection of latent community structure without nodes covariates and a large body of empirical work using diverse heuristics for combining node covariates with graphs for inference. The tightness of our analysis implies in particular, the information theoretic necessity of combining the different sources of information. Our analysis holds for networks of large degrees as well as for a Gaussian version of the model.

Estimators for Multivariate Information Measures in General Probability Spaces

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #80

Arman Rahimzamani · Himanshu Asnani · Pramod Viswanath · Sreeram Kannan

Information theoretic quantities play an important role in various settings in machine learning, including causality testing, structure inference in graphical models, time-series problems, feature selection as well as in providing privacy guarantees. A key quantity of interest is the mutual information and generalizations thereof, including conditional mutual information, multivariate mutual information, total correlation and directed information. While the aforementioned information quantities are well defined in arbitrary probability spaces, existing estimators employ a ΣH method, which can only work in purely discrete space or purely continuous case since entropy (or differential entropy) is well defined only in that regime. In this paper, we define a general graph divergence measure (\mathbb{GDM}), generalizing the aforementioned information measures and we construct a novel estimator via a coupling trick that directly estimates these multivariate information measures using the Radon-Nikodym derivative. These estimators are proven to be consistent in a general setting which includes several cases where the existing estimators fail, thus providing the only known estimators for the following settings: (1) the data has some discrete and some continuous valued components (2) some (or all) of the components themselves are discrete-continuous mixtures (3) the data is real-valued but does not have a joint density on the entire space, rather is supported on a low-dimensional manifold. We show that our proposed estimators significantly outperform known estimators on synthetic and real datasets.

Blind Deconvolutional Phase Retrieval via Convex Programming

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #81

Ali Ahmed · Alireza Aghasi · Paul Hand

We consider the task of recovering two real or complex m -vectors from phaseless Fourier measurements of their circular convolution. Our method is a novel convex relaxation that is based on a lifted matrix recovery formulation that allows a nontrivial convex relaxation of the bilinear measurements from convolution. We prove that if the two signals belong to known random subspaces of dimensions k and n , then they can be recovered up to the inherent scaling ambiguity with $m \gg (k+n) \log^2 m$ phaseless measurements. Our method provides the first theoretical recovery guarantee for this problem by a computationally efficient algorithm and does not require a solution estimate to be computed for initialization. Our proof is based Rademacher complexity estimates. Additionally, we provide an ADMM implementation of the method and provide numerical experiments that verify the theory.

Entropy Rate Estimation for Markov Chains with Large State Space

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #82

Yanjun Han · Jiantao Jiao · Chuan-Zheng Lee · Tsachy Weissman · Yihong Wu · Tiancheng Yu

Entropy estimation is one of the prototypical problems in distribution property testing. To consistently estimate the Shannon entropy of a distribution on S elements with independent samples, the optimal sample complexity scales sublinearly with S as $\Theta(\frac{S}{\log S})$ as shown by Valiant and Valiant [Valiant-Valiant2011]. Extending the theory and algorithms for entropy estimation to dependent data, this paper considers the problem of estimating the entropy rate of a stationary reversible Markov chain with S states from a sample path of n observations. We show that

- Provided the Markov chain mixes not too slowly, i.e., the relaxation time is at most $O(\frac{S}{\ln^3 S})$, consistent estimation is achievable when $n \gg \frac{S^2}{\log S}$.
- Provided the Markov chain has some slight dependency, i.e., the relaxation time is at least $1 + \Omega(\frac{\ln^2 S}{\sqrt{S}})$, consistent estimation is impossible when $n \lesssim \frac{S^2}{\log S}$.

Under both assumptions, the optimal estimation accuracy is shown to be $\Theta(\frac{S^2}{n \log S})$. In comparison, the empirical entropy rate requires at least $\Omega(S^2)$ samples to be consistent, even when the Markov chain is memoryless. In addition to synthetic experiments, we also apply the estimators that achieve the optimal sample complexity to estimate the entropy rate of the English language in the

Penn Treebank and the Google One Billion Words corpora, which provides a natural benchmark for language modeling and relates it directly to the widely used perplexity measure.

Bandit Learning in Concave N-Person Games

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #83

Mario Bravo · David Leslie · Panayotis Mertikopoulos

This paper examines the long-run behavior of learning with bandit feedback in non-cooperative concave games. The bandit framework accounts for extremely low-information environments where the agents may not even know they are playing a game; as such, the agents' most sensible choice in this setting would be to employ a no-regret learning algorithm. In general, this does not mean that the players' behavior stabilizes in the long run: no-regret learning may lead to cycles, even with perfect gradient information. However, if a standard monotonicity condition is satisfied, our analysis shows that no-regret learning based on mirror descent with bandit feedback converges to Nash equilibrium with probability 1. We also derive an upper bound for the convergence rate of the process that nearly matches the best attainable rate for single-agent bandit stochastic optimization.

Depth-Limited Solving for Imperfect-Information Games

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #84

Noam Brown · Tuomas Sandholm · Brandon Amos

A fundamental challenge in imperfect-information games is that states do not have well-defined values. As a result, depth-limited search algorithms used in single-agent settings and perfect-information games do not apply. This paper introduces a principled way to conduct depth-limited solving in imperfect-information games by allowing the opponent to choose among a number of strategies for the remainder of the game at the depth limit. Each one of these strategies results in a different set of values for leaf nodes. This forces an agent to be robust to the different strategies an opponent may employ. We demonstrate the effectiveness of this approach by building a master-level heads-up no-limit Texas hold'em poker AI that defeats two prior top agents using only a 4-core CPU and 16 GB of memory. Developing such a powerful agent would have previously required a supercomputer.

The Physical Systems Behind Optimization Algorithms

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #85

Lin Yang · Raman Arora · Vladimir Braverman · Tuo Zhao

We use differential equations based approaches to provide some $\textit{physics}$ insights into analyzing the dynamics of popular optimization algorithms in machine learning. In particular, we study gradient descent, proximal gradient descent, coordinate gradient descent, proximal coordinate gradient, and Newton's methods as well as their Nesterov's accelerated variants in a unified framework motivated by a natural connection of optimization algorithms to physical systems. Our analysis is applicable to more general algorithms and optimization problems \textit{beyond} convexity and strong convexity, e.g. Polyak-Ljapunov and error bound conditions (possibly nonconvex).

The Nearest Neighbor Information Estimator is Adaptively Near Minimax Rate-Optimal

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #86

Jiantao Jiao · Weihao Gao · Yanjun Han

We analyze the Kozachenko-Leonenko (KL) fixed k -nearest neighbor estimator for the differential entropy. We obtain the first uniform upper bound on its performance for any fixed k over H^{∞} -balls on a torus without assuming any conditions on how close the density could be from zero. Accompanying a recent minimax lower bound over the H^{∞} -ball, we show that the KL estimator for any fixed k is achieving the minimax rates up to logarithmic factors without cognizance of the smoothness parameter s of the H^{∞} -ball for $s \in (0, 2]$ and arbitrary dimension d , rendering it the first estimator that provably satisfies this property.

Robust Learning of Fixed-Structure Bayesian Networks

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #87

Yu Cheng · Ilias Diakonikolas · Daniel Kane · Alistair Stewart

We investigate the problem of learning Bayesian networks in a robust model where an ϵ -fraction of the samples are adversarially corrupted. In this work, we study the fully observable discrete case where the structure of the network is given. Even in this basic setting, previous learning algorithms either run in exponential time or lose dimension-dependent factors in their error guarantees. We provide the first computationally efficient robust learning algorithm for this problem with dimension-independent error guarantees. Our algorithm has near-optimal sample complexity, runs in polynomial time, and achieves error that scales nearly-linearly with the fraction of adversarially corrupted samples. Finally, we show on both synthetic and semi-synthetic data that our algorithm performs well in practice.

Information-theoretic Limits for Community Detection in Network Models

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #88

Chuyang Ke · Jean Honorio

We analyze the information-theoretic limits for the recovery of node labels in several network models. This includes the Stochastic Block Model, the Exponential Random Graph Model, the Latent Space Model, the Directed Preferential Attachment Model, and the Directed Small-world Model. For the Stochastic Block Model, the non-recoverability condition depends on the probabilities of having edges inside a community, and between different communities. For the Latent Space Model, the non-recoverability condition depends on the dimension of the latent space, and how far and spread are the communities in the latent space. For the Directed Preferential Attachment Model and the Directed Small-world Model, the non-recoverability condition depends on the ratio between homophily and neighborhood size. We also consider dynamic versions of the Stochastic Block Model and the Latent Space Model.

Generalizing Graph Matching beyond Quadratic Assignment Model

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #89

Tianshu Yu · Junchi Yan · Yilin Wang · Wei Liu · baoxin Li

Graph matching has received persistent attention over decades, which can be formulated as a quadratic assignment problem (QAP). We show that a large family of functions, which we define as Separable Functions, can approximate discrete graph matching in the continuous domain asymptotically by varying the approximation controlling parameters. We also study the properties of global optimality and devise convex/concave-preserving extensions to the widely used Lawler's QAP form. Our theoretical findings show the potential for deriving new algorithms and techniques for graph matching. We deliver solvers based on two specific instances of Separable Functions, and the state-of-the-art performance of our method is verified on popular benchmarks.

Improving Simple Models with Confidence Profiles

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #90

Amit Dhurandhar · Karthikeyan Shanmugam · Ronny Luss · Peder A Olsen

In this paper, we propose a new method called ProfWeight for transferring information from a pre-trained deep neural network that has a high test accuracy to a simpler interpretable model or a very shallow network of low complexity and a priori low test accuracy. We are motivated by applications in interpretability and model deployment in severely memory constrained environments (like sensors). Our method uses linear probes to generate confidence scores through flattened intermediate representations. Our transfer method involves a theoretically justified weighting of samples during the training of the simple model using confidence scores of these intermediate layers. The value of our method is first demonstrated on CIFAR-10, where our weighting method significantly improves (3-4%) networks with only a fraction of the number of Resnet blocks of a complex Resnet model. We further demonstrate operationally significant results on a real manufacturing problem, where we dramatically increase the test accuracy of a CART model (the domain standard) by roughly 13%.

Online Learning with an Unknown Fairness Metric

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #91

Stephen Gillen · Christopher Jung · Michael Kearns · Aaron Roth

We consider the problem of online learning in the linear contextual bandits setting, but in which there are also strong individual fairness constraints governed by an unknown similarity metric. These constraints demand that we select similar actions or individuals with approximately equal probability, which may be at odds with optimizing reward, thus modeling settings where profit and social policy are in tension. We assume we learn about an unknown Mahalanobis similarity metric from only weak feedback that identifies fairness violations, but does not quantify their extent. This is intended to represent the interventions of a regulator who "knows unfairness when he sees it" but nevertheless cannot enunciate a quantitative fairness metric over individuals. Our main result is an algorithm in the adversarial context setting that has a number of fairness violations that depends only logarithmically on T , while obtaining an optimal $O(\sqrt{T})$ regret bound to the best fair policy.

Legendre Decomposition for Tensors

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #92

Mahito Sugiyama · Hiroyuki Nakahara · Koji Tsuda

We present a novel nonnegative tensor decomposition method, called Legendre decomposition, which factorizes an input tensor into a multiplicative combination of parameters. Thanks to the well-developed theory of information geometry, the reconstructed tensor is unique and always minimizes the KL divergence from an input tensor. We empirically show that Legendre decomposition can more

accurately reconstruct tensors than other nonnegative tensor decomposition methods.

The Price of Privacy for Low-rank Factorization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #93

Jalaj Upadhyay

In this paper, we study what price one has to pay to release $\text{\emph{differentially private low-rank factorization}}$ of a matrix. We consider various settings that are close to the real world applications of low-rank factorization: (i) the manner in which matrices are updated (row by row or in an arbitrary manner), (ii) whether matrices are distributed or not, and (iii) how the output is produced (once at the end of all updates, also known as $\text{\emph{one-shot algorithms}}$ or continually). Even though these settings are well studied without privacy, surprisingly, there are no private algorithm for these settings (except when a matrix is updated row by row). We present the first set of differentially private algorithms for all these settings.

Our algorithms when private matrix is updated in an arbitrary manner promise differential privacy with respect to two stronger privacy guarantees than previously studied, use space and time $\text{\emph{comparable}}$ to the non-private algorithm, and achieve $\text{\emph{optimal accuracy}}$. To complement our positive results, we also prove that the space required by our algorithms is optimal up to logarithmic factors. When data matrices are distributed over multiple servers, we give a non-interactive differentially private algorithm with communication cost independent of dimension. In concise, we give algorithms that incur $\text{\emph{optimal cost across all parameters of interest}}$. We also perform experiments to verify that all our algorithms perform well in practice and outperform the best known algorithm until now for large range of parameters.

Empirical Risk Minimization in Non-interactive Local Differential Privacy Revisited

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #94

Di Wang · Marco Gaboardi · Jinhui Xu

In this paper, we revisit the Empirical Risk Minimization problem in the non-interactive local model of differential privacy. In the case of constant or low dimensions ($p \ll n$), we first show that if the loss function is (∞, T) -smooth, we can avoid a dependence of the sample complexity, to achieve error α , on the exponential of the dimensionality p with base $1/\alpha$ ($\text{\emph{i.e.,}} \alpha^{-p}$), which answers a question in $\text{\emph{smith2017interaction}}$. Our approach is based on polynomial approximation. Then, we propose player-efficient algorithms with 1 -bit communication complexity and $O(1)$ computation cost for each player. The error bound is asymptotically the same as the original one. With some additional assumptions, we also give an efficient algorithm for the

server. In the case of high dimensions (ℓ_p), we show that if the loss function is a convex generalized linear function, the error can be bounded by using the Gaussian width of the constrained set, instead of ℓ_p , which improves the one in \cite{smith2017interaction}.

Differentially Private Change-Point Detection

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #95

Sara Krehbiel · Rachel Cummings · Wanrong Zhang · Yajun Mei · Rui Tuo

The change-point detection problem seeks to identify distributional changes at an unknown change-point k^* in a stream of data. This problem appears in many important practical settings involving personal data, including biosurveillance, fault detection, finance, signal detection, and security systems. The field of differential privacy offers data analysis tools that provide powerful worst-case privacy guarantees. We study the statistical problem of change-point problem through the lens of differential privacy. We give private algorithms for both online and offline change-point detection, analyze these algorithms theoretically, and then provide empirical validation of these results.

Scalable Laplacian K-modes

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #96

Imtiaz Ziko · Eric Granger · Ismail Ben Ayed

We advocate Laplacian K-modes for joint clustering and density mode finding, and propose a concave-convex relaxation of the problem, which yields a parallel algorithm that scales up to large datasets and high dimensions. We optimize a tight bound (auxiliary function) of our relaxation, which, at each iteration, amounts to computing an independent update for each cluster-assignment variable, with guaranteed convergence. Therefore, our bound optimizer can be trivially distributed for large-scale data sets. Furthermore, we show that the density modes can be obtained as byproducts of the assignment variables via simple maximum-value operations whose additional computational cost is linear in the number of data points. Our formulation does not need storing a full affinity matrix and computing its eigenvalue decomposition, neither does it perform expensive projection steps and Lagrangian-dual inner iterates for the simplex constraints of each point. Furthermore, unlike mean-shift, our density-mode estimation does not require inner-loop gradient-ascent iterates. It has a complexity independent of feature-space dimension, yields modes that are valid data points in the input set and is applicable to discrete domains as well as arbitrary kernels. We report comprehensive experiments over various data sets, which show that our algorithm yields very competitive performances in term of optimization quality (i.e., the value of the discrete-variable objective at convergence) and clustering accuracy.

Geometrically Coupled Monte Carlo Sampling

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #97

Mark Rowland · Krzysztof Choromanski · François Chalus · Aldo Pacchiano · Tamas Sarlos · Richard E Turner · Adrian Weller

Monte Carlo sampling in high-dimensional, low-sample settings is important in many machine learning tasks. We improve current methods for sampling in Euclidean spaces by avoiding independence, and instead consider ways to couple samples. We show fundamental connections to optimal transport theory, leading to novel sampling algorithms, and providing new theoretical grounding for existing strategies. We compare our new strategies against prior methods for improving sample efficiency, including QMC, by studying discrepancy. We explore our findings empirically, and observe benefits of our sampling schemes for reinforcement learning and generative modelling.

Continuous-time Value Function Approximation in Reproducing Kernel Hilbert Spaces

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #98

Motoya Ohnishi · Masahiro Yukawa · Mikael Johansson · Masashi Sugiyama

Motivated by the success of reinforcement learning (RL) for discrete-time tasks such as AlphaGo and Atari games, there has been a recent surge of interest in using RL for continuous-time control of physical systems (cf. many challenging tasks in OpenAI Gym and DeepMind Control Suite). Since discretization of time is susceptible to error, it is methodologically more desirable to handle the system dynamics directly in continuous time. However, very few techniques exist for continuous-time RL and they lack flexibility in value function approximation. In this paper, we propose a novel framework for model-based continuous-time value function approximation in reproducing kernel Hilbert spaces. The resulting framework is so flexible that it can accommodate any kind of kernel-based approach, such as Gaussian processes and kernel adaptive filters, and it allows us to handle uncertainties and nonstationarity without prior knowledge about the environment or what basis functions to employ. We demonstrate the validity of the presented framework through experiments.

Faster Online Learning of Optimal Threshold for Consistent

F-measure Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #99

Xiaoxuan Zhang · Mingrui Liu · Xun Zhou · Tianbao Yang

In this paper, we consider online F-measure optimization (OFO). Unlike traditional performance metrics (e.g., classification error rate), F-measure is non-decomposable over training examples and is a non-convex function of model parameters, making it much more difficult to be optimized in an online fashion. Most existing results of OFO usually suffer from high memory/computational costs and/or lack statistical consistency guarantee for optimizing F-measure at the population level. To advance OFO, we propose an efficient online algorithm based on simultaneously learning a posterior probability of class and learning an optimal threshold by minimizing a stochastic strongly convex function with unknown strong convexity parameter. A key component of the proposed method is a novel stochastic algorithm with low memory and computational costs, which can enjoy a convergence rate of $\widetilde{O}(1/\sqrt{n})$ for learning the optimal threshold under a mild condition on the convergence of the posterior probability, where n is the number of processed examples. It is provably faster than its predecessor based on a heuristic for updating the threshold. The experiments verify the efficiency of the proposed algorithm in comparison with state-of-the-art OFO algorithms.

Reducing Network Agnostophobia

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #100

Akshay Raj Dhamija · Manuel Günther · Terrance Boult

Agnostophobia, the fear of the unknown, can be experienced by deep learning engineers while applying their networks to real-world applications. Unfortunately, network behavior is not well defined for inputs far from a networks training set. In an uncontrolled environment, networks face many instances that are not of interest to them and have to be rejected in order to avoid a false positive. This problem has previously been tackled by researchers by either a) thresholding softmax, which by construction cannot return "none of the known classes", or b) using an additional background or garbage class. In this paper, we show that both of these approaches help, but are generally insufficient when previously unseen classes are encountered. We also introduce a new evaluation metric that focuses on comparing the performance of multiple approaches in scenarios where such unseen classes or unknowns are encountered. Our major contributions are simple yet effective Entropic Open-Set and Objectosphere losses that train networks using negative samples from some classes. These novel losses are designed to maximize entropy for unknown inputs while increasing separation in deep feature space by modifying magnitudes of known and unknown samples. Experiments on networks trained to classify classes from MNIST and CIFAR-10 show that our novel loss functions are significantly better at dealing with unknown inputs from datasets such as Devanagari, NotMNIST, CIFAR-100 and SVHN.

Life-Long Disentangled Representation Learning with Cross-Domain Latent Homologies

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #101

Alessandro Achille · Tom Eccles · Loic Matthey · Chris Burgess · Nicholas Watters · Alexander Lerchner · Irina Higgins

Intelligent behaviour in the real-world requires the ability to acquire new knowledge from an ongoing sequence of experiences while preserving and reusing past knowledge. We propose a novel algorithm for unsupervised representation learning from piece-wise stationary visual data: Variational Autoencoder with Shared Embeddings (VASE). Based on the Minimum Description Length principle, VASE automatically detects shifts in the data distribution and allocates spare representational capacity to new knowledge, while simultaneously protecting previously learnt representations from catastrophic forgetting. Our approach encourages the learnt representations to be disentangled, which imparts a number of desirable properties: VASE can deal sensibly with ambiguous inputs, it can enhance its own representations through imagination-based exploration, and most importantly, it exhibits semantically meaningful sharing of latents between different datasets. Compared to baselines with entangled representations, our approach is able to reason beyond surface-level statistics and perform semantically meaningful cross-domain inference.

Near-Optimal Policies for Dynamic Multinomial Logit Assortment Selection Models

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #102

Yining Wang · Xi Chen · Yuan Zhou

In this paper we consider the dynamic assortment selection problem under an uncapacitated multinomial-logit (MNL) model. By carefully analyzing a revenue potential function, we show that a trisection based algorithm achieves an item-independent regret bound of $O(\sqrt{T \log \log T})$, which matches information theoretical lower bounds up to iterated logarithmic terms. Our proof technique draws tools from the unimodal/convex bandit literature as well as adaptive confidence parameters in minimax multi-armed bandit problems.

The Everlasting Database: Statistical Validity at a Fair Price

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #103

The problem of handling adaptivity in data analysis, intentional or not, permeates a variety of fields, including test-set overfitting in ML challenges and the accumulation of invalid scientific discoveries. We propose a mechanism for answering an arbitrarily long sequence of potentially adaptive statistical queries, by charging a price for each query and using the proceeds to collect additional samples. Crucially, we guarantee statistical validity without any assumptions on how the queries are generated. We also ensure with high probability that the cost for M non-adaptive queries is $O(\log M)$, while the cost to a potentially adaptive user who makes M queries that do not depend on any others is $O(\sqrt{M})$.

Scalar Posterior Sampling with Applications

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #104

Georgios Theodorou · Zheng Wen · Yasin Abbasi · Nikos Vlassis

We propose a practical non-episodic PSRL algorithm that unlike recent state-of-the-art PSRL algorithms uses a deterministic, model-independent episode switching schedule. Our algorithm termed deterministic schedule PSRL (DS-PSRL) is efficient in terms of time, sample, and space complexity. We prove a Bayesian regret bound under mild assumptions. Our result is more generally applicable to multiple parameters and continuous state action problems. We compare our algorithm with state-of-the-art PSRL algorithms on standard discrete and continuous problems from the literature. Finally, we show how the assumptions of our algorithm satisfy a sensible parameterization for a large class of problems in sequential recommendations.

Iterative Value-Aware Model Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #105

Amir-massoud Farahmand

This paper introduces a model-based reinforcement learning (MBRL) framework that incorporates the underlying decision problem in learning the transition model of the environment. This is in contrast with conventional approaches to MBRL that learn the model of the environment, for example by finding the maximum likelihood estimate, without taking into account the decision problem. Value-Aware Model Learning (VAML) framework argues that this might not be a good idea, especially if the true model of the environment does not belong to the model class from which we are estimating the model. The original VAML framework, however, may result in an optimization problem that is difficult to solve. This paper introduces a new MBRL class of algorithms, called Iterative VAML, that benefits from the structure of how the planning is performed (i.e., through

approximate value iteration) to devise a simpler optimization problem. The paper theoretically analyzes Iterative VAML and provides finite sample error upper bound guarantee for it.

A Lyapunov-based Approach to Safe Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #106

Yinlam Chow · Ofir Nachum · Edgar Duenez-Guzman · Mohammad Ghavamzadeh

In many real-world reinforcement learning (RL) problems, besides optimizing the main objective function, an agent must concurrently avoid violating a number of constraints. In particular, besides optimizing performance, it is crucial to guarantee the safety of an agent during training as well as deployment (e.g., a robot should avoid taking actions - exploratory or not - which irrevocably harm its hardware). To incorporate safety in RL, we derive algorithms under the framework of constrained Markov decision processes (CMDPs), an extension of the standard Markov decision processes (MDPs) augmented with constraints on expected cumulative costs. Our approach hinges on a novel Lyapunov method. We define and present a method for constructing Lyapunov functions, which provide an effective way to guarantee the global safety of a behavior policy during training via a set of local linear constraints. Leveraging these theoretical underpinnings, we show how to use the Lyapunov approach to systematically transform dynamic programming (DP) and RL algorithms into their safe counterparts. To illustrate their effectiveness, we evaluate these algorithms in several CMDP planning and decision-making tasks on a safety benchmark domain. Our results show that our proposed method significantly outperforms existing baselines in balancing constraint satisfaction and performance.

Temporal Regularization for Markov Decision Process

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #107

Pierre Thodoroff · Audrey Durand · Joelle Pineau · Doina Precup

Several applications of Reinforcement Learning suffer from instability due to high variance. This is especially prevalent in high dimensional domains. Regularization is a commonly used technique in machine learning to reduce variance, at the cost of introducing some bias. Most existing regularization techniques focus on spatial (perceptual) regularization. Yet in reinforcement learning, due to the nature of the Bellman equation, there is an opportunity to also exploit temporal regularization based on smoothness in value estimates over trajectories. This paper explores a class of methods for temporal regularization. We formally characterize the bias induced by this technique using Markov chain concepts. We illustrate the various characteristics of temporal regularization via a sequence of simple discrete and continuous MDPs, and show that the technique provides improvement even in high-dimensional Atari games.

Maximum Causal Tsallis Entropy Imitation Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #108

Kyungjae Lee · Sungjoon Choi · Songhwai Oh

In this paper, we propose a novel maximum causal Tsallis entropy (MCTE) framework for imitation learning which can efficiently learn a sparse multi-modal policy distribution from demonstrations. We provide the full mathematical analysis of the proposed framework. First, the optimal solution of an MCTE problem is shown to be a sparsemax distribution, whose supporting set can be adjusted. The proposed method has advantages over a softmax distribution in that it can exclude unnecessary actions by assigning zero probability. Second, we prove that an MCTE problem is equivalent to robust Bayes estimation in the sense of the Brier score. Third, we propose a maximum causal Tsallis entropy imitation learning (MCTEIL) algorithm with a sparse mixture density network (sparse MDN) by modeling mixture weights using a sparsemax distribution. In particular, we show that the causal Tsallis entropy of an MDN encourages exploration and efficient mixture utilization while Boltzmann Gibbs entropy is less effective. We validate the proposed method in two simulation studies and MCTEIL outperforms existing imitation learning methods in terms of average returns and learning multi-modal policies.

Policy Optimization via Importance Sampling

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #109

Alberto Maria Metelli · Matteo Papini · Francesco Faccio · Marcello Restelli

Policy optimization is an effective reinforcement learning approach to solve continuous control tasks. Recent achievements have shown that alternating online and offline optimization is a successful choice for efficient trajectory reuse. However, deciding when to stop optimizing and collect new trajectories is non-trivial, as it requires to account for the variance of the objective function estimate. In this paper, we propose a novel, model-free, policy search algorithm, POIS, applicable in both action-based and parameter-based settings. We first derive a high-confidence bound for importance sampling estimation; then we define a surrogate objective function, which is optimized offline whenever a new batch of trajectories is collected. Finally, the algorithm is tested on a selection of continuous control tasks, with both linear and deep policies, and compared with state-of-the-art policy optimization methods.

Reinforcement Learning of Theorem Proving

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #110

Cezary Kaliszyk · Josef Urban · Henryk Michalewski · Miroslav Olšák

We introduce a theorem proving algorithm that uses practically no domain heuristics for guiding its connection-style proof search. Instead, it runs many Monte-Carlo simulations guided by reinforcement learning from previous proof attempts. We produce several versions of the prover, parameterized by different learning and guiding algorithms. The strongest version of the system is trained on a large corpus of mathematical problems and evaluated on previously unseen problems. The trained system solves within the same number of inferences over 40% more problems than a baseline prover, which is an unusually high improvement in this hard AI domain. To our knowledge this is the first time reinforcement learning has been convincingly applied to solving general mathematical problems on a large scale.

Simple random search of static linear policies is competitive for reinforcement learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #111

Horia Mania · Aurelia Guy · Benjamin Recht

Model-free reinforcement learning aims to offer off-the-shelf solutions for controlling dynamical systems without requiring models of the system dynamics. We introduce a model-free random search algorithm for training static, linear policies for continuous control problems. Common evaluation methodology shows that our method matches state-of-the-art sample efficiency on the benchmark MuJoCo locomotion tasks. Nonetheless, more rigorous evaluation reveals that the assessment of performance on these benchmarks is optimistic. We evaluate the performance of our method over hundreds of random seeds and many different hyperparameter configurations for each benchmark task. This extensive evaluation is possible because of the small computational footprint of our method. Our simulations highlight a high variability in performance in these benchmark tasks, indicating that commonly used estimations of sample efficiency do not adequately evaluate the performance of RL algorithms. Our results stress the need for new baselines, benchmarks and evaluation methodology for RL algorithms.

Meta-Gradient Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #112

Zhongwen Xu · Hado van Hasselt · David Silver

The goal of reinforcement learning algorithms is to estimate and/or optimise the value function. However, unlike supervised learning, no teacher or oracle is available to provide the true value function. Instead, the majority of reinforcement learning algorithms estimate and/or optimise a proxy for the value function. This proxy is typically based on a sampled and bootstrapped approximation to the true value function, known as a return. The particular choice of return is one of the chief components determining the nature of the algorithm: the rate at which future rewards are discounted; when and how values should be bootstrapped; or even the nature of the rewards themselves. It is well-known that these decisions are crucial to the overall success of RL algorithms. We discuss a gradient-based meta-learning algorithm that is able to adapt the nature of the return, online, whilst interacting and learning from the environment. When applied to 57 games on the Atari 2600 environment over 200 million frames, our algorithm achieved a new state-of-the-art performance.

Reinforcement Learning for Solving the Vehicle Routing Problem

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #113

MohammadReza Nazari · Afshin Oroojlooy · Lawrence Snyder · Martin Takac

We present an end-to-end framework for solving the Vehicle Routing Problem (VRP) using reinforcement learning. In this approach, we train a single policy model that finds near-optimal solutions for a broad range of problem instances of similar size, only by observing the reward signals and following feasibility rules. We consider a parameterized stochastic policy, and by applying a policy gradient algorithm to optimize its parameters, the trained model produces the solution as a sequence of consecutive actions in real time, without the need to re-train for every new problem instance. On capacitated VRP, our approach outperforms classical heuristics and Google's OR-Tools on medium-sized instances in solution quality with comparable computation time (after training). We demonstrate how our approach can handle problems with split delivery and explore the effect of such deliveries on the solution quality. Our proposed framework can be applied to other variants of the VRP such as the stochastic VRP, and has the potential to be applied more generally to combinatorial optimization problems

Learn What Not to Learn: Action Elimination with Deep Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #114

Tom Zahavy · Matan Haroush · Nadav Merlis · Daniel J Mankowitz · Shie Mannor

Learning how to act when there are many available actions in each state is a challenging task for

Reinforcement Learning (RL) agents, especially when many of the actions are redundant or irrelevant. In such cases, it is easier to learn which actions not to take. In this work, we propose the Action-Elimination Deep Q-Network (AE-DQN) architecture that combines a Deep RL algorithm with an Action Elimination Network (AEN) that eliminates sub-optimal actions. The AEN is trained to predict invalid actions, supervised by an external elimination signal provided by the environment. Simulations demonstrate a considerable speedup and added robustness over vanilla DQN in text-based games with over a thousand discrete actions.

REFUEL: Exploring Sparse Features in Deep Reinforcement Learning for Fast Disease Diagnosis

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #115

Yu-Shao Peng · Kai-Fu Tang · Hsuan-Tien Lin · Edward Chang

This paper proposes REFUEL, a reinforcement learning method with two techniques: {\em reward shaping} and {\em feature rebuilding}, to improve the performance of online symptom checking for disease diagnosis. Reward shaping can guide the search of policy towards better directions. Feature rebuilding can guide the agent to learn correlations between features. Together, they can find symptom queries that can yield positive responses from a patient with high probability. Experimental results justify that the two techniques in REFUEL allows the symptom checker to identify the disease more rapidly and accurately.

Learning Plannable Representations with Causal InfoGAN

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #116

Thanard Kurutach · Aviv Tamar · Ge Yang · Stuart Russell · Pieter Abbeel

In recent years, deep generative models have been shown to 'imagine' convincing high-dimensional observations such as images, audio, and even video, learning directly from raw data. In this work, we ask how to imagine goal-directed visual plans -- a plausible sequence of observations that transition a dynamical system from its current configuration to a desired goal state, which can later be used as a reference trajectory for control. We focus on systems with high-dimensional observations, such as images, and propose an approach that naturally combines representation learning and planning. Our framework learns a generative model of sequential observations, where the generative process is induced by a transition in a low-dimensional planning model, and an additional noise. By maximizing the mutual information between the generated observations and the transition in the planning model, we obtain a low-dimensional representation that best explains the causal nature of the data. We structure the planning model to be compatible with efficient planning algorithms, and we propose several such models based on either discrete or continuous states.

Finally, to generate a visual plan, we project the current and goal observations onto their respective states in the planning model, plan a trajectory, and then use the generative model to transform the trajectory to a sequence of observations. We demonstrate our method on imagining plausible visual plans of rope manipulation.

Improving Exploration in Evolution Strategies for Deep Reinforcement Learning via a Population of Novelty-Seeking Agents

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #117

Edoardo Conti · Vashisht Madhavan · Felipe Petroski Such · Joel Lehman · Kenneth Stanley · Jeff Clune

Evolution strategies (ES) are a family of black-box optimization algorithms able to train deep neural networks roughly as well as Q-learning and policy gradient methods on challenging deep reinforcement learning (RL) problems, but are much faster (e.g. hours vs. days) because they parallelize better. However, many RL problems require directed exploration because they have reward functions that are sparse or deceptive (i.e. contain local optima), and it is unknown how to encourage such exploration with ES. Here we show that algorithms that have been invented to promote directed exploration in small-scale evolved neural networks via populations of exploring agents, specifically novelty search (NS) and quality diversity (QD) algorithms, can be hybridized with ES to improve its performance on sparse or deceptive deep RL tasks, while retaining scalability. Our experiments confirm that the resultant new algorithms, NS-ES and two QD algorithms, NSR-ES and NSRA-ES, avoid local optima encountered by ES to achieve higher performance on Atari and simulated robots learning to walk around a deceptive trap. This paper thus introduces a family of fast, scalable algorithms for reinforcement learning that are capable of directed exploration. It also adds this new family of exploration algorithms to the RL toolbox and raises the interesting possibility that analogous algorithms with multiple simultaneous paths of exploration might also combine well with existing RL algorithms outside ES.

Transfer of Deep Reactive Policies for MDP Planning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #118

Aniket (Nick) Bajpai · Sankalp Garg · Mausam

Domain-independent probabilistic planners input an MDP description in a factored representation language such as PPDDL or RDDL, and exploit the specifics of the representation for faster planning. Traditional algorithms operate on each problem instance independently, and good methods for transferring experience from policies of other instances of a domain to a new instance do not exist.

Recently, researchers have begun exploring the use of deep reactive policies, trained via deep reinforcement learning (RL), for MDP planning domains. One advantage of deep reactive policies is that they are more amenable to transfer learning.

In this paper, we present the first domain-independent transfer algorithm for MDP planning domains expressed in an RDDDL representation. Our architecture exploits the symbolic state configuration and transition function of the domain (available via RDDDL) to learn a shared embedding space for states and state-action pairs for all problem instances of a domain. We then learn an RL agent in the embedding space, making a near zero-shot transfer possible, i.e., without much training on the new instance, and without using the domain simulator at all. Experiments on three different benchmark domains underscore the value of our transfer algorithm. Compared against planning from scratch, and a state-of-the-art RL transfer algorithm, our transfer solution has significantly superior learning curves.

Q-learning with Nearest Neighbors

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #119

Devavrat Shah · Qiaomin Xie

We consider model-free reinforcement learning for infinite-horizon discounted Markov Decision Processes (MDPs) with a continuous state space and unknown transition kernel, when only a single sample path under an arbitrary policy of the system is available. We consider the Nearest Neighbor Q-Learning (NNQL) algorithm to learn the optimal Q function using nearest neighbor regression method. As the main contribution, we provide tight finite sample analysis of the convergence rate. In particular, for MDPs with a d -dimensional state space and the discounted factor $\gamma \in (0,1)$, given an arbitrary sample path with "covering time" L , we establish that the algorithm is guaranteed to output an ϵ -accurate estimate of the optimal Q-function using $O(L/(\epsilon^3(1-\gamma)^7))$ samples. For instance, for a well-behaved MDP, the covering time of the sample path under the purely random policy scales as $O(1/\epsilon^d)$, so the sample complexity scales as $O(1/\epsilon^{d+3})$. Indeed, we establish a lower bound that argues that the dependence of $\Omega(1/\epsilon^{d+2})$ is necessary.

Distributed Multitask Reinforcement Learning with Quadratic Convergence

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #120

Rasul Tutunov · Dongho Kim · Haitham Bou Ammar

Multitask reinforcement learning (MTRL) suffers from scalability issues when the number of tasks or trajectories grows large. The main reason behind this drawback is the reliance on centralised

solutions. Recent methods exploited the connection between MTRL and general consensus to propose scalable solutions. These methods, however, suffer from two drawbacks. First, they rely on predefined objectives, and, second, exhibit linear convergence guarantees. In this paper, we improve over state-of-the-art by deriving multitask reinforcement learning from a variational inference perspective. We then propose a novel distributed solver for MTRL with quadratic convergence guarantees.

Breaking the Curse of Horizon: Infinite-Horizon Off-Policy Estimation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #121

Qiang Liu · Lihong Li · Ziyang Tang · Dengyong Zhou

We consider the off-policy estimation problem of estimating the expected reward of a target policy using samples collected by a different behavior policy. Importance sampling (IS) has been a key technique to derive (nearly) unbiased estimators, but is known to suffer from an excessively high variance in long-horizon problems. In the extreme case of infinite-horizon problems, the variance of an IS-based estimator may even be unbounded. In this paper, we propose a new off-policy estimation method that applies IS directly on the stationary state-visitation distributions to avoid the exploding variance issue faced by existing estimators. Our key contribution is a novel approach to estimating the density ratio of two stationary distributions, with trajectories sampled from only the behavior distribution. We develop a mini-max loss function for the estimation problem, and derive a closed-form solution for the case of RKHS. We support our method with both theoretical and empirical analyses.

Constrained Cross-Entropy Method for Safe Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #122

Min Wen · Ufuk Topcu

We study a safe reinforcement learning problem in which the constraints are defined as the expected cost over finite-length trajectories. We propose a constrained cross-entropy-based method to solve this problem. The method explicitly tracks its performance with respect to constraint satisfaction and thus is well-suited for safety-critical applications. We show that the asymptotic behavior of the proposed algorithm can be almost-surely described by that of an ordinary differential equation. Then we give sufficient conditions on the properties of this differential equation to guarantee the convergence of the proposed algorithm. At last, we show with simulation experiments that the proposed algorithm can effectively learn feasible policies without assumptions on the

feasibility of initial policies, even with non-Markovian objective functions and constraint functions.

Representation Balancing MDPs for Off-policy Policy Evaluation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #123

Yao Liu · Omer Gottesman · Aniruddh Raghu · Matthieu Komorowski · Aldo A Faisal · Finale Doshi-Velez · Emma Brunskill

We study the problem of off-policy policy evaluation (OPPE) in RL. In contrast to prior work, we consider how to estimate both the individual policy value and average policy value accurately. We draw inspiration from recent work in causal reasoning, and propose a new finite sample generalization error bound for value estimates from MDP models. Using this upper bound as an objective, we develop a learning algorithm of an MDP model with a balanced representation, and show that our approach can yield substantially lower MSE in common synthetic benchmarks and a HIV treatment simulation domain.

Dual Policy Iteration

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #124

Wen Sun · Geoffrey Gordon · Byron Boots · J. Bagnell

Recently, a novel class of Approximate Policy Iteration (API) algorithms have demonstrated impressive practical performance (e.g., ExIt from [1], AlphaGo-Zero from [2]). This new family of algorithms maintains, and alternately optimizes, two policies: a fast, reactive policy (e.g., a deep neural network) deployed at test time, and a slow, non-reactive policy (e.g., Tree Search), that can plan multiple steps ahead. The reactive policy is updated under supervision from the non-reactive policy, while the non-reactive policy is improved with guidance from the reactive policy. In this work we study this Dual Policy Iteration (DPI) strategy in an alternating optimization framework and provide a convergence analysis that extends existing API theory. We also develop a special instance of this framework which reduces the update of non-reactive policies to model-based optimal control using learned local models, and provides a theoretically sound way of unifying model-free and model-based RL approaches with unknown dynamics. We demonstrate the efficacy of our approach on various continuous control Markov Decision Processes.

Occam's razor is insufficient to infer the preferences of irrational agents

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #125

Stuart Armstrong · Sören Mindermann

Inverse reinforcement learning (IRL) attempts to infer human rewards or preferences from observed behavior. Since human planning systematically deviates from rationality, several approaches have been tried to account for specific human shortcomings. However, the general problem of inferring the reward function of an agent of unknown rationality has received little attention. Unlike the well-known ambiguity problems in IRL, this one is practically relevant but cannot be resolved by observing the agent's policy in enough environments. This paper shows (1) that a No Free Lunch result implies it is impossible to uniquely decompose a policy into a planning algorithm and reward function, and (2) that even with a reasonable simplicity prior/Occam's razor on the set of decompositions, we cannot distinguish between the true decomposition and others that lead to high regret. To address this, we need simple 'normative' assumptions, which cannot be deduced exclusively from observations.

Transfer of Value Functions via Variational Methods

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #126

Andrea Tirinzoni · Rafael Rodriguez Sanchez · Marcello Restelli

We consider the problem of transferring value functions in reinforcement learning. We propose an approach that uses the given source tasks to learn a prior distribution over optimal value functions and provide an efficient variational approximation of the corresponding posterior in a new target task. We show our approach to be general, in the sense that it can be combined with complex parametric function approximators and distribution models, while providing two practical algorithms based on Gaussians and Gaussian mixtures. We theoretically analyze them by deriving a finite-sample analysis and provide a comprehensive empirical evaluation in four different domains.

Reinforcement Learning with Multiple Experts: A Bayesian Model Combination Approach

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #127

Michael Gimelfarb · Scott Sanner · Chi-Guhn Lee

Potential based reward shaping is a powerful technique for accelerating convergence of

reinforcement learning algorithms. Typically, such information includes an estimate of the optimal value function and is often provided by a human expert or other sources of domain knowledge. However, this information is often biased or inaccurate and can mislead many reinforcement learning algorithms. In this paper, we apply Bayesian Model Combination with multiple experts in a way that learns to trust a good combination of experts as training progresses. This approach is both computationally efficient and general, and is shown numerically to improve convergence across discrete and continuous domains and different reinforcement learning algorithms.

Online Robust Policy Learning in the Presence of Unknown Adversaries

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #128

Aaron Havens · Zhanhong Jiang · Soumik Sarkar

The growing prospect of deep reinforcement learning (DRL) being used in cyber-physical systems has raised concerns around safety and robustness of autonomous agents. Recent work on generating adversarial attacks have shown that it is computationally feasible for a bad actor to fool a DRL policy into behaving sub optimally. Although certain adversarial attacks with specific attack models have been addressed, most studies are only interested in off-line optimization in the data space (e.g., example fitting, distillation). This paper introduces a Meta-Learned Advantage Hierarchy (MLAH) framework that is attack model-agnostic and more suited to reinforcement learning, via handling the attacks in the decision space (as opposed to data space) and directly mitigating learned bias introduced by the adversary. In MLAH, we learn separate sub-policies (nominal and adversarial) in an online manner, as guided by a supervisory master agent that detects the presence of the adversary by leveraging the advantage function for the sub-policies. We demonstrate that the proposed algorithm enables policy learning with significantly lower bias as compared to the state-of-the-art policy learning approaches even in the presence of heavy state information attacks. We present algorithm analysis and simulation results using popular OpenAI Gym environments.

A Bayesian Approach to Generative Adversarial Imitation Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #129

Wonseok Jeon · Seokin Seo · Kee-Eung Kim

Generative adversarial training for imitation learning has shown promising results on high-dimensional and continuous control tasks. This paradigm is based on reducing the imitation learning problem to the density matching problem, where the agent iteratively refines the policy to match the empirical state-action visitation frequency of the expert demonstration. Although this approach has

shown to robustly learn to imitate even with scarce demonstration, one must still address the inherent challenge that collecting trajectory samples in each iteration is a costly operation. To address this issue, we first propose a Bayesian formulation of generative adversarial imitation learning (GAIL), where the imitation policy and the cost function are represented as stochastic neural networks. Then, we show that we can significantly enhance the sample efficiency of GAIL leveraging the predictive density of the cost, on an extensive set of imitation learning tasks with high-dimensional states and actions.

Verifiable Reinforcement Learning via Policy Extraction

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #130

Osbert Bastani · Yewen Pu · Armando Solar-Lezama

While deep reinforcement learning has successfully solved many challenging control tasks, its real-world applicability has been limited by the inability to ensure the safety of learned policies. We propose an approach to verifiable reinforcement learning by training decision tree policies, which can represent complex policies (since they are nonparametric), yet can be efficiently verified using existing techniques (since they are highly structured). The challenge is that decision tree policies are difficult to train. We propose VIPER, an algorithm that combines ideas from model compression and imitation learning to learn decision tree policies guided by a DNN policy (called the oracle) and its Q-function, and show that it substantially outperforms two baselines. We use VIPER to (i) learn a provably robust decision tree policy for a variant of Atari Pong with a symbolic state space, (ii) learn a decision tree policy for a toy game based on Pong that provably never loses, and (iii) learn a provably stable decision tree policy for cart-pole. In each case, the decision tree policy achieves performance equal to that of the original DNN policy.

Deep Reinforcement Learning of Marked Temporal Point Processes

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #131

Utkarsh Upadhyay · Abir De · Manuel Gomez Rodriguez

In a wide variety of applications, humans interact with a complex environment by means of asynchronous stochastic discrete events in continuous time. Can we design online interventions that will help humans achieve certain goals in such asynchronous setting? In this paper, we address the above problem from the perspective of deep reinforcement learning of marked temporal point processes, where both the actions taken by an agent and the feedback it receives from the environment are asynchronous stochastic discrete events characterized using marked temporal point processes. In doing so, we define the agent's policy using the intensity and mark distribution of

the corresponding process and then derive a flexible policy gradient method, which embeds the agent's actions and the feedback it receives into real-valued vectors using deep recurrent neural networks. Our method does not make any assumptions on the functional form of the intensity and mark distribution of the feedback and it allows for arbitrarily complex reward functions. We apply our methodology to two different applications in viral marketing and personalized teaching and, using data gathered from Twitter and Duolingo, we show that it may be able to find interventions to help marketers and learners achieve their goals more effectively than alternatives.

On Learning Intrinsic Rewards for Policy Gradient Methods

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #132

Zeyu Zheng · Junhyuk Oh · Satinder Singh

In many sequential decision making tasks, it is challenging to design reward functions that help an RL agent efficiently learn behavior that is considered good by the agent designer. A number of different formulations of the reward-design problem, or close variants thereof, have been proposed in the literature. In this paper we build on the Optimal Rewards Framework of Singh et al. that defines the optimal intrinsic reward function as one that when used by an RL agent achieves behavior that optimizes the task-specifying or extrinsic reward function. Previous work in this framework has shown how good intrinsic reward functions can be learned for lookahead search based planning agents. Whether it is possible to learn intrinsic reward functions for learning agents remains an open problem. In this paper we derive a novel algorithm for learning intrinsic rewards for policy-gradient based learning agents. We compare the performance of an augmented agent that uses our algorithm to provide additive intrinsic rewards to an A2C-based policy learner (for Atari games) and a PPO-based policy learner (for Mujoco domains) with a baseline agent that uses the same policy learners but with only extrinsic rewards. Our results show improved performance on most but not all of the domains.

Evolution-Guided Policy Gradient in Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #133

Shauharda Khadka · Kagan Tumer

Deep Reinforcement Learning (DRL) algorithms have been successfully applied to a range of challenging control tasks. However, these methods typically suffer from three core difficulties: temporal credit assignment with sparse rewards, lack of effective exploration, and brittle convergence properties that are extremely sensitive to hyperparameters. Collectively, these challenges severely limit the applicability of these approaches to real world problems. Evolutionary Algorithms (EAs), a class of black box optimization techniques inspired by natural evolution, are well

suited to address each of these three challenges. However, EAs typically suffer from high sample complexity and struggle to solve problems that require optimization of a large number of parameters. In this paper, we introduce Evolutionary Reinforcement Learning (ERL), a hybrid algorithm that leverages the population of an EA to provide diversified data to train an RL agent, and reinserts the RL agent into the EA population periodically to inject gradient information into the EA. ERL inherits EA's ability of temporal credit assignment with a fitness metric, effective exploration with a diverse set of policies, and stability of a population-based approach and complements it with off-policy DRL's ability to leverage gradients for higher sample efficiency and faster learning. Experiments in a range of challenging continuous control benchmarks demonstrate that ERL significantly outperforms prior DRL and EA methods.

Meta-Reinforcement Learning of Structured Exploration Strategies

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #134

Abhishek Gupta · Russell Mendonca · YuXuan Liu · Pieter Abbeel · Sergey Levine

Exploration is a fundamental challenge in reinforcement learning (RL). Many current exploration methods for deep RL use task-agnostic objectives, such as information gain or bonuses based on state visitation. However, many practical applications of RL involve learning more than a single task, and prior tasks can be used to inform how exploration should be performed in new tasks. In this work, we study how prior tasks can inform an agent about how to explore effectively in new situations. We introduce a novel gradient-based fast adaptation algorithm – model agnostic exploration with structured noise (MAESN) – to learn exploration strategies from prior experience. The prior experience is used both to initialize a policy and to acquire a latent exploration space that can inject structured stochasticity into a policy, producing exploration strategies that are informed by prior knowledge and are more effective than random action-space noise. We show that MAESN is more effective at learning exploration strategies when compared to prior meta-RL methods, RL without learned exploration strategies, and task-agnostic exploration methods. We evaluate our method on a variety of simulated tasks: locomotion with a wheeled robot, locomotion with a quadrupedal walker, and object manipulation.

Diversity-Driven Exploration Strategy for Deep Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #135

Zhang-Wei Hong · Tzu-Yun Shann · Shih-Yang Su · Yi-Hsiang Chang · Tsu-Jui Fu · Chun-Yi Lee

Efficient exploration remains a challenging research problem in reinforcement learning, especially

when an environment contains large state spaces, deceptive local optima, or sparse rewards. To tackle this problem, we present a diversity-driven approach for exploration, which can be easily combined with both off- and on-policy reinforcement learning algorithms. We show that by simply adding a distance measure to the loss function, the proposed methodology significantly enhances an agent's exploratory behaviors, and thus preventing the policy from being trapped in local optima. We further propose an adaptive scaling method for stabilizing the learning process. We demonstrate the effectiveness of our method in huge 2D gridworlds and a variety of benchmark environments, including Atari 2600 and MuJoCo. Experimental results show that our method outperforms baseline approaches in most tasks in terms of mean scores and exploration efficiency.

Genetic-Gated Networks for Deep Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #136

Simyung Chang · John Yang · Jaeseok Choi · Nojun Kwak

We introduce the Genetic-Gated Networks (G2Ns), simple neural networks that combine a gate vector composed of binary genetic genes in the hidden layer(s) of networks. Our method can take both advantages of gradient-free optimization and gradient-based optimization methods, of which the former is effective for problems with multiple local minima, while the latter can quickly find local minima. In addition, multiple chromosomes can define different models, making it easy to construct multiple models and can be effectively applied to problems that require multiple models. We show that this G2N can be applied to typical reinforcement learning algorithms to achieve a large improvement in sample efficiency and performance.

Memory Augmented Policy Optimization for Program Synthesis and Semantic Parsing

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #137

Chen Liang · Mohammad Norouzi · Jonathan Berant · Quoc V Le · Ni Lao

We present Memory Augmented Policy Optimization (MAPO), a simple and novel way to leverage a memory buffer of promising trajectories to reduce the variance of policy gradient estimate. MAPO is applicable to deterministic environments with discrete actions, such as structured prediction and combinatorial optimization tasks. We express the expected return objective as a weighted sum of two terms: an expectation over the high-reward trajectories inside the memory buffer, and a separate expectation over trajectories outside the buffer. To make an efficient algorithm of MAPO, we propose: (1) memory weight clipping to accelerate and stabilize training; (2) systematic exploration to discover high-reward trajectories; (3) distributed sampling from inside and outside of the memory buffer to scale up training. MAPO improves the sample efficiency and robustness of

policy gradient, especially on tasks with sparse rewards. We evaluate MAPO on weakly supervised program synthesis from natural language (semantic parsing). On the WikiTableQuestions benchmark, we improve the state-of-the-art by 2.6%, achieving an accuracy of 46.3%. On the WikiSQL benchmark, MAPO achieves an accuracy of 74.9% with only weak supervision, outperforming several strong baselines with full supervision. Our source code is available at <https://goo.gl/TXBp4e>

Hardware Conditioned Policies for Multi-Robot Transfer Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #138

Tao Chen · Adithyavairavan Murali · Abhinav Gupta

Deep reinforcement learning could be used to learn dexterous robotic policies but it is challenging to transfer them to new robots with vastly different hardware properties. It is also prohibitively expensive to learn a new policy from scratch for each robot hardware due to the high sample complexity of modern state-of-the-art algorithms. We propose a novel approach called Hardware Conditioned Policies where we train a universal policy conditioned on a vector representation of robot hardware. We considered robots in simulation with varied dynamics, kinematic structure, kinematic lengths and degrees-of-freedom. First, we use the kinematic structure directly as the hardware encoding and show great zero-shot transfer to completely novel robots not seen during training. For robots with lower zero-shot success rate, we also demonstrate that fine-tuning the policy network is significantly more sample-efficient than training a model from scratch. In tasks where knowing the agent dynamics is important for success, we learn an embedding for robot hardware and show that policies conditioned on the encoding of hardware tend to generalize and transfer well. Videos of experiments are available at: <https://sites.google.com/view/robot-transfer-hcp>.

Reward learning from human preferences and demonstrations in Atari

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #139

Jan Leike · Borja Ibarz · Dario Amodei · Geoffrey Irving · Shane Legg

To solve complex real-world problems with reinforcement learning, we cannot rely on manually specified reward functions. Instead, we need humans to communicate an objective to the agent directly. In this work, we combine two approaches to this problem: learning from expert demonstrations and learning from trajectory preferences. We use both to train a deep neural network to model the reward function and use its predicted reward to train an DQN-based deep

reinforcement learning agent on 9 Atari games. Our approach beats the imitation learning baseline in 7 games and achieves strictly superhuman performance on 2 games. Additionally, we investigate the fit of the reward model, present some reward hacking problems, and study the effects of noise in the human labels.

Graph Convolutional Policy Network for Goal-Directed Molecular Graph Generation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #140

Jiaxuan You · Bowen Liu · Zhitao Ying · Vijay Pande · Jure Leskovec

Generating novel graph structures that optimize given objectives while obeying some given underlying rules is fundamental for chemistry, biology and social science research. This is especially important in the task of molecular graph generation, whose goal is to discover novel molecules with desired properties such as drug-likeness and synthetic accessibility, while obeying physical laws such as chemical valency. However, designing models that finds molecules that optimize desired properties while incorporating highly complex and non-differentiable rules remains to be a challenging task. Here we propose Graph Convolutional Policy Network (GCPN), a general graph convolutional network based model for goal-directed graph generation through reinforcement learning. The model is trained to optimize domain-specific rewards and adversarial loss through policy gradient, and acts in an environment that incorporates domain-specific rules. Experimental results show that GCPN can achieve 61% improvement on chemical property optimization over state-of-the-art baselines while resembling known molecules, and achieve 184% improvement on the constrained property optimization task.

Visual Reinforcement Learning with Imagined Goals

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #141

Ashvin Nair · Vitchyr Pong · Murtaza Dalal · Shikhar Bahl · Steven Lin · Sergey Levine

For an autonomous agent to fulfill a wide range of user-specified goals at test time, it must be able to learn broadly applicable and general-purpose skill repertoires. Furthermore, to provide the requisite level of generality, these skills must handle raw sensory input such as images. In this paper, we propose an algorithm that acquires such general-purpose skills by combining unsupervised representation learning and reinforcement learning of goal-conditioned policies. Since the particular goals that might be required at test-time are not known in advance, the agent performs a self-supervised "practice" phase where it imagines goals and attempts to achieve them. We learn a visual representation with three distinct purposes: sampling goals for self-supervised practice, providing a structured transformation of raw sensory inputs, and computing a reward

signal for goal reaching. We also propose a retroactive goal relabeling scheme to further improve the sample-efficiency of our method. Our off-policy algorithm is efficient enough to learn policies that operate on raw image observations and goals in a real-world physical system, and substantially outperforms prior techniques.

Playing hard exploration games by watching YouTube

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #142

Yusuf Aytar · Tobias Pfaff · David Budden · Thomas Paine · Ziyu Wang · Nando de Freitas

Deep reinforcement learning methods traditionally struggle with tasks where environment rewards are particularly sparse. One successful method of guiding exploration in these domains is to imitate trajectories provided by a human demonstrator. However, these demonstrations are typically collected under artificial conditions, i.e. with access to the agent's exact environment setup and the demonstrator's action and reward trajectories. Here we propose a method that overcomes these limitations in two stages. First, we learn to map unaligned videos from multiple sources to a common representation using self-supervised objectives constructed over both time and modality (i.e. vision and sound). Second, we embed a single YouTube video in this representation to learn a reward function that encourages an agent to imitate human gameplay. This method of one-shot imitation allows our agent to convincingly exceed human-level performance on the infamously hard exploration games Montezuma's Revenge, Pitfall! and Private Eye for the first time, even if the agent is not presented with any environment rewards.

Unsupervised Video Object Segmentation for Deep Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #143

Vikash Goel · Jameson Weng · Pascal Poupart

We present a new technique for deep reinforcement learning that automatically detects moving objects and uses the relevant information for action selection. The detection of moving objects is done in an unsupervised way by exploiting structure from motion. Instead of directly learning a policy from raw images, the agent first learns to detect and segment moving objects by exploiting flow information in video sequences. The learned representation is then used to focus the policy of the agent on the moving objects. Over time, the agent identifies which objects are critical for decision making and gradually builds a policy based on relevant moving objects. This approach, which we call Motion-Oriented REinforcement Learning (MOREL), is demonstrated on a suite of Atari games where the ability to detect moving objects reduces the amount of interaction needed with the environment to obtain a good policy. Furthermore, the resulting policy is more

interpretable than policies that directly map images to actions or values with a black box neural network. We can gain insight into the policy by inspecting the segmentation and motion of each object detected by the agent. This allows practitioners to confirm whether a policy is making decisions based on sensible information. Our code is available at <https://github.com/vik-goel/MOREL>.

Learning to Navigate in Cities Without a Map

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #144

Piotr Mirowski · Matt Grimes · Mateusz Malinowski · Karl Moritz Hermann · Keith Anderson · Denis Teplyashin · Karen Simonyan · koray kavukcuoglu · Andrew Zisserman · Raia Hadsell

Navigating through unstructured environments is a basic capability of intelligent creatures, and thus is of fundamental interest in the study and development of artificial intelligence. Long-range navigation is a complex cognitive task that relies on developing an internal representation of space, grounded by recognisable landmarks and robust visual processing, that can simultaneously support continuous self-localisation ("I am here") and a representation of the goal ("I am going there"). Building upon recent research that applies deep reinforcement learning to maze navigation problems, we present an end-to-end deep reinforcement learning approach that can be applied on a city scale. Recognising that successful navigation relies on integration of general policies with locale-specific knowledge, we propose a dual pathway architecture that allows locale-specific features to be encapsulated, while still enabling transfer to multiple cities. A key contribution of this paper is an interactive navigation environment that uses Google Street View for its photographic content and worldwide coverage. Our baselines demonstrate that deep reinforcement learning agents can learn to navigate in multiple cities and to traverse to target destinations that may be kilometres away. A video summarizing our research and showing the trained agent in diverse city environments as well as on the transfer task is available at: <https://sites.google.com/view/learn-navigate-cities-nips18>

Learning Abstract Options

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #145

Matthew Riemer · Miao Liu · Gerald Tesauro

Building systems that autonomously create temporal abstractions from data is a key challenge in scaling learning and planning in reinforcement learning. One popular approach for addressing this challenge is the options framework (Sutton et al., 1999). However, only recently in (Bacon et al., 2017) was a policy gradient theorem derived for online learning of general purpose options in an end to end fashion. In this work, we extend previous work on this topic that only focuses on learning a two-level hierarchy including options and primitive actions to enable learning simultaneously at

multiple resolutions in time. We achieve this by considering an arbitrarily deep hierarchy of options where high level temporally extended options are composed of lower level options with finer resolutions in time. We extend results from (Bacon et al., 2017) and derive policy gradient theorems for a deep hierarchy of options. Our proposed hierarchical option-critic architecture is capable of learning internal policies, termination conditions, and hierarchical compositions over options without the need for any intrinsic rewards or subgoals. Our empirical results in both discrete and continuous environments demonstrate the efficiency of our framework.

Object-Oriented Dynamics Predictor

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #146

Guangxiang Zhu · Zhiao Huang · Chongjie Zhang

Generalization has been one of the major challenges for learning dynamics models in model-based reinforcement learning. However, previous work on action-conditioned dynamics prediction focuses on learning the pixel-level motion and thus does not generalize well to novel environments with different object layouts. In this paper, we present a novel object-oriented framework, called object-oriented dynamics predictor (OODP), which decomposes the environment into objects and predicts the dynamics of objects conditioned on both actions and object-to-object relations. It is an end-to-end neural network and can be trained in an unsupervised manner. To enable the generalization ability of dynamics learning, we design a novel CNN-based relation mechanism that is class-specific (rather than object-specific) and exploits the locality principle. Empirical results show that OODP significantly outperforms previous methods in terms of generalization over novel environments with various object layouts. OODP is able to learn from very few environments and accurately predict dynamics in a large number of unseen environments. In addition, OODP learns semantically and visually interpretable dynamics models.

A Deep Bayesian Policy Reuse Approach Against Non-Stationary Agents

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #147

YAN ZHENG · Zhaopeng Meng · Jianye Hao · Zongzhang Zhang · Tianpei Yang · Changjie Fan

In multiagent domains, coping with non-stationary agents that change behaviors from time to time is a challenging problem, where an agent is usually required to be able to quickly detect the other agent's policy during online interaction, and then adapt its own policy accordingly. This paper studies efficient policy detecting and reusing techniques when playing against non-stationary agents in Markov games. We propose a new deep BPR+ algorithm by extending the recent BPR+ algorithm with a neural network as the value-function approximator. To detect policy accurately, we propose

the \textit{rectified belief model} taking advantage of the \textit{opponent model} to infer the other agent's policy from reward signals and its behaviors. Instead of directly storing individual policies as BPR+, we introduce \textit{distilled policy network} that serves as the policy library in BPR+, using policy distillation to achieve efficient online policy learning and reuse. Deep BPR+ inherits all the advantages of BPR+ and empirically shows better performance in terms of detection accuracy, cumulative rewards and speed of convergence compared to existing algorithms in complex Markov games with raw visual inputs.

Learning Attentional Communication for Multi-Agent Cooperation

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #148

Jiechuan Jiang · Zongqing Lu

Communication could potentially be an effective way for multi-agent cooperation. However, information sharing among all agents or in predefined communication architectures that existing methods adopt can be problematic. When there is a large number of agents, agents cannot differentiate valuable information that helps cooperative decision making from globally shared information. Therefore, communication barely helps, and could even impair the learning of multi-agent cooperation. Predefined communication architectures, on the other hand, restrict communication among agents and thus restrain potential cooperation. To tackle these difficulties, in this paper, we propose an attentional communication model that learns when communication is needed and how to integrate shared information for cooperative decision making. Our model leads to efficient and effective communication for large-scale multi-agent cooperation. Empirically, we show the strength of our model in a variety of cooperative scenarios, where agents are able to develop more coordinated and sophisticated strategies than existing methods.

Deep Dynamical Modeling and Control of Unsteady Fluid Flows

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #149

Jeremy Morton · Antony Jameson · Mykel J Kochenderfer · Freddie Witherden

The design of flow control systems remains a challenge due to the nonlinear nature of the equations that govern fluid flow. However, recent advances in computational fluid dynamics (CFD) have enabled the simulation of complex fluid flows with high accuracy, opening the possibility of using learning-based approaches to facilitate controller design. We present a method for learning the forced and unforced dynamics of airflow over a cylinder directly from CFD data. The proposed approach, grounded in Koopman theory, is shown to produce stable dynamical models that can

predict the time evolution of the cylinder system over extended time horizons. Finally, by performing model predictive control with the learned dynamical models, we are able to find a straightforward, interpretable control law for suppressing vortex shedding in the wake of the cylinder.

Adaptive Skip Intervals: Temporal Abstraction for Recurrent Dynamical Models

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #150

Alexander Neitz · Giambattista Parascandolo · Stefan Bauer · Bernhard Schölkopf

We introduce a method which enables a recurrent dynamics model to be temporally abstract. Our approach, which we call Adaptive Skip Intervals (ASI), is based on the observation that in many sequential prediction tasks, the exact time at which events occur is irrelevant to the underlying objective. Moreover, in many situations, there exist prediction intervals which result in particularly easy-to-predict transitions. We show that there are prediction tasks for which we gain both computational efficiency and prediction accuracy by allowing the model to make predictions at a sampling rate which it can choose itself.

Zero-Shot Transfer with Deictic Object-Oriented Representation in Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #151

Ofir Marom · Benjamin Rosman

Object-oriented representations in reinforcement learning have shown promise in transfer learning, with previous research introducing a propositional object-oriented framework that has provably efficient learning bounds with respect to sample complexity. However, this framework has limitations in terms of the classes of tasks it can efficiently learn. In this paper we introduce a novel deictic object-oriented framework that has provably efficient learning bounds and can solve a broader range of tasks. Additionally, we show that this framework is capable of zero-shot transfer of transition dynamics across tasks and demonstrate this empirically for the Taxi and Sokoban domains.

Total stochastic gradient algorithms and applications in

reinforcement learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #152

Paavo Parmas

Backpropagation and the chain rule of derivatives have been prominent; however, the total derivative rule has not enjoyed the same amount of attention. In this work we show how the total derivative rule leads to an intuitive visual framework for creating gradient estimators on graphical models. In particular, previous "policy gradient theorems" are easily derived. We derive new gradient estimators based on density estimation, as well as a likelihood ratio gradient, which "jumps" to an intermediate node, not directly to the objective function. We evaluate our methods on model-based policy gradient algorithms, achieve good performance, and present evidence towards demystifying the success of the popular PILCO algorithm.

Fighting Boredom in Recommender Systems with Linear Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #153

Romain WARLOP · Alessandro Lazaric · Jérémie Mary

A common assumption in recommender systems (RS) is the existence of a best fixed recommendation strategy. Such strategy may be simple and work at the item level (e.g., in multi-armed bandit it is assumed one best fixed arm/item exists) or implement more sophisticated RS (e.g., the objective of A/B testing is to find the best fixed RS and execute it thereafter). We argue that this assumption is rarely verified in practice, as the recommendation process itself may impact the user's preferences. For instance, a user may get bored by a strategy, while she may gain interest again, if enough time passed since the last time that strategy was used. In this case, a better approach consists in alternating different solutions at the right frequency to fully exploit their potential. In this paper, we first cast the problem as a Markov decision process, where the rewards are a linear function of the recent history of actions, and we show that a policy considering the long-term influence of the recommendations may outperform both fixed-action and contextual greedy policies. We then introduce an extension of the UCRL algorithm (**L IN UCRL**) to effectively balance exploration and exploitation in an unknown environment, and we derive a regret bound that is independent of the number of states. Finally, we empirically validate the model assumptions and the algorithm in a number of realistic scenarios.

Randomized Prior Functions for Deep Reinforcement

Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #154

Ian Osband · John Aslanides · Albin Cassirer

Dealing with uncertainty is essential for efficient reinforcement learning. There is a growing literature on uncertainty estimation for deep learning from fixed datasets, but many of the most popular approaches are poorly-suited to sequential decision problems. Other methods, such as bootstrap sampling, have no mechanism for uncertainty that does not come from the observed data. We highlight why this can be a crucial shortcoming and propose a simple remedy through addition of a randomized untrainable 'prior' network to each ensemble member. We prove that this approach is efficient with linear representations, provide simple illustrations of its efficacy with nonlinear representations and show that this approach scales to large-scale problems far better than previous attempts.

Scalable Coordinated Exploration in Concurrent Reinforcement Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #155

Maria Dimakopoulou · Ian Osband · Benjamin Van Roy

We consider a team of reinforcement learning agents that concurrently operate in a common environment, and we develop an approach to efficient coordinated exploration that is suitable for problems of practical scale. Our approach builds on the seed sampling concept introduced in Dimakopoulou and Van Roy (2018) and on a randomized value function learning algorithm from Osband et al. (2016). We demonstrate that, for simple tabular contexts, the approach is competitive with those previously proposed in Dimakopoulou and Van Roy (2018) and with a higher-dimensional problem and a neural network value function representation, the approach learns quickly with far fewer agents than alternative exploration schemes.

Context-dependent upper-confidence bounds for directed exploration

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #156

Raksha Kumaraswamy · Matthew Schlegel · Adam White · Martha White

Directed exploration strategies for reinforcement learning are critical for learning an optimal policy in a minimal number of interactions with the environment. Many algorithms use optimism to direct

exploration, either through visitation estimates or upper confidence bounds, as opposed to data-inefficient strategies like e-greedy that use random, undirected exploration. Most data-efficient exploration methods require significant computation, typically relying on a learned model to guide exploration. Least-squares methods have the potential to provide some of the data-efficiency benefits of model-based approaches—because they summarize past interactions—with the computation closer to that of model-free approaches. In this work, we provide a novel, computationally efficient, incremental exploration strategy, leveraging this property of least-squares temporal difference learning (LSTD). We derive upper confidence bounds on the action-values learned by LSTD, with context-dependent (or state-dependent) noise variance. Such context-dependent noise focuses exploration on a subset of variable states, and allows for reduced exploration in other states. We empirically demonstrate that our algorithm can converge more quickly than other incremental exploration strategies using confidence estimates on action-values.

Multi-Agent Generative Adversarial Imitation Learning

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #157

Jiaming Song · Hongyu Ren · Dorsa Sadigh · Stefano Ermon

Imitation learning algorithms can be used to learn a policy from expert demonstrations without access to a reward signal. However, most existing approaches are not applicable in multi-agent settings due to the existence of multiple (Nash) equilibria and non-stationary environments. We propose a new framework for multi-agent imitation learning for general Markov games, where we build upon a generalized notion of inverse reinforcement learning. We further introduce a practical multi-agent actor-critic algorithm with good empirical performance. Our method can be used to imitate complex behaviors in high-dimensional environments with multiple cooperative or competing agents.

Actor-Critic Policy Optimization in Partially Observable Multiagent Environments

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #158

Sriram Srinivasan · Marc Lanctot · Vinicius Zambaldi · Julien Perolat · Karl Tuyls · Remi Munos · Michael Bowling

Optimization of parameterized policies for reinforcement learning (RL) is an important and challenging problem in artificial intelligence. Among the most common approaches are algorithms based on gradient ascent of a score function representing discounted return. In this paper, we examine the role of these policy gradient and actor-critic algorithms in partially-observable multiagent environments. We show several candidate policy update rules and relate them to a

foundation of regret minimization and multiagent learning techniques for the one-shot and tabular cases, leading to previously unknown convergence guarantees. We apply our method to model-free multiagent reinforcement learning in adversarial sequential decision problems (zero-sum imperfect information games), using RL-style function approximation. We evaluate on commonly used benchmark Poker domains, showing performance against fixed policies and empirical convergence to approximate Nash equilibria in self-play with rates similar to or better than a baseline model-free algorithm for zero-sum games, without any domain-specific state space reductions.

Learning to Share and Hide Intentions using Information Regularization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #159

Daniel Strouse · Max Kleiman-Weiner · Josh Tenenbaum · Matt Botvinick · David Schwab

Learning to cooperate with friends and compete with foes is a key component of multi-agent reinforcement learning. Typically to do so, one requires access to either a model of or interaction with the other agent(s). Here we show how to learn effective strategies for cooperation and competition in an asymmetric information game with no such model or interaction. Our approach is to encourage an agent to reveal or hide their intentions using an information-theoretic regularizer. We consider both the mutual information between goal and action given state, as well as the mutual information between goal and state. We show how to stochastically optimize these regularizers in a way that is easy to integrate with policy gradient reinforcement learning. Finally, we demonstrate that cooperative (competitive) policies learned with our approach lead to more (less) reward for a second agent in two simple asymmetric information games.

Credit Assignment For Collective Multiagent RL With Global Rewards

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #160

Duc Thien Nguyen · Akshat Kumar · Hoong Chuin Lau

Scaling decision theoretic planning to large multiagent systems is challenging due to uncertainty and partial observability in the environment. We focus on a multiagent planning model subclass, relevant to urban settings, where agent interactions are dependent on their ``collective influence'' on each other, rather than their identities. Unlike previous work, we address a general setting where system reward is not decomposable among agents. We develop collective actor-critic RL approaches for this setting, and address the problem of multiagent credit assignment, and computing low variance policy gradient estimates that result in faster convergence to high quality solutions. We also develop difference rewards based credit assignment methods for the collective setting.

Empirically our new approaches provide significantly better solutions than previous methods in the presence of global rewards on two real world problems modeling taxi fleet optimization and multiagent patrolling, and a synthetic grid navigation domain.

Multi-Agent Reinforcement Learning via Double Averaging Primal-Dual Optimization

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #161

Hoi-To Wai · Zhuoran Yang · Princeton Zhaoran Wang · Mingyi Hong

Despite the success of single-agent reinforcement learning, multi-agent reinforcement learning (MARL) remains challenging due to complex interactions between agents. Motivated by decentralized applications such as sensor networks, swarm robotics, and power grids, we study policy evaluation in MARL, where agents with jointly observed state-action pairs and private local rewards collaborate to learn the value of a given policy. In this paper, we propose a double averaging scheme, where each agent iteratively performs averaging over both space and time to incorporate neighboring gradient information and local reward information, respectively. We prove that the proposed algorithm converges to the optimal solution at a global geometric rate. In particular, such an algorithm is built upon a primal-dual reformulation of the mean squared Bellman error minimization problem, which gives rise to a decentralized convex-concave saddle-point problem. To the best of our knowledge, the proposed double averaging primal-dual optimization algorithm is the first to achieve fast finite-time convergence on decentralized convex-concave saddle-point problems.

Learning Others' Intentional Models in Multi-Agent Settings Using Interactive POMDPs

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #162

Yanlin Han · Piotr Gmytrasiewicz

Interactive partially observable Markov decision processes (I-POMDPs) provide a principled framework for planning and acting in a partially observable, stochastic and multi-agent environment. It extends POMDPs to multi-agent settings by including models of other agents in the state space and forming a hierarchical belief structure. In order to predict other agents' actions using I-POMDPs, we propose an approach that effectively uses Bayesian inference and sequential Monte Carlo sampling to learn others' intentional models which ascribe to them beliefs, preferences and rationality in action selection. Empirical results show that our algorithm accurately learns models of the other agent and has superior performance than methods that use subintentional models. Our approach serves as a generalized Bayesian learning algorithm that learns other agents' beliefs,

strategy levels, and transition, observation and reward functions. It also effectively mitigates the belief space complexity due to the nested belief hierarchy.

Bayesian Control of Large MDPs with Unknown Dynamics in Data-Poor Environments

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #163

Mahdi Imani · Seyedeh Fatemeh Ghoreishi · Ulisses M. Braga-Neto

We propose a Bayesian decision making framework for control of Markov Decision Processes (MDPs) with unknown dynamics and large, possibly continuous, state, action, and parameter spaces in data-poor environments. Most of the existing adaptive controllers for MDPs with unknown dynamics are based on the reinforcement learning framework and rely on large data sets acquired by sustained direct interaction with the system or via a simulator. This is not feasible in many applications, due to ethical, economic, and physical constraints. The proposed framework addresses the data poverty issue by decomposing the problem into an offline planning stage that does not rely on sustained direct interaction with the system or simulator and an online execution stage. In the offline process, parallel Gaussian process temporal difference (GPTD) learning techniques are employed for near-optimal Bayesian approximation of the expected discounted reward over a sample drawn from the prior distribution of unknown parameters. In the online stage, the action with the maximum expected return with respect to the posterior distribution of the parameters is selected. This is achieved by an approximation of the posterior distribution using a Markov Chain Monte Carlo (MCMC) algorithm, followed by constructing multiple Gaussian processes over the parameter space for efficient prediction of the means of the expected return at the MCMC sample. The effectiveness of the proposed framework is demonstrated using a simple dynamical system model with continuous state and action spaces, as well as a more complex model for a metastatic melanoma gene regulatory network observed through noisy synthetic gene expression data.

Negotiable Reinforcement Learning for Pareto Optimal Sequential Decision-Making

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #164

Nishant Desai · Andrew Critch · Stuart J Russell

It is commonly believed that an agent making decisions on behalf of two or more principals who have different utility functions should adopt a Pareto optimal policy, i.e. a policy that cannot be improved upon for one principal without making sacrifices for another. Harsanyi's theorem shows that when the principals have a common prior on the outcome distributions of all policies, a Pareto optimal policy for the agent is one that maximizes a fixed, weighted linear combination of the

principals' utilities. In this paper, we derive a more precise generalization for the sequential decision setting in the case of principals with different priors on the dynamics of the environment. We refer to this generalization as the Negotiable Reinforcement Learning (NRL) framework. In this more general case, the relative weight given to each principal's utility should evolve over time according to how well the agent's observations conform with that principal's prior. To gain insight into the dynamics of this new framework, we implement a simple NRL agent and empirically examine its behavior in a simple environment.

rho-POMDPs have Lipschitz-Continuous epsilon-Optimal Value Functions

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #165

Mathieu Fehr · Olivier Buffet · Vincent Thomas · Jilles Dibangoye

Many state-of-the-art algorithms for solving Partially Observable Markov Decision Processes (POMDPs) rely on turning the problem into a “fully observable” problem—a belief MDP—and exploiting the piece-wise linearity and convexity (PWLC) of the optimal value function in this new state space (the belief simplex Δ). This approach has been extended to solving ρ -POMDPs—i.e., for information-oriented criteria—when the reward ρ is convex in Δ . General ρ -POMDPs can also be turned into “fully observable” problems, but with no means to exploit the PWLC property. In this paper, we focus on POMDPs and ρ -POMDPs with $\lambda \rho$ -Lipschitz reward function, and demonstrate that, for finite horizons, the optimal value function is Lipschitz-continuous. Then, value function approximators are proposed for both upper- and lower-bounding the optimal value function, which are shown to provide uniformly improvable bounds. This allows proposing two algorithms derived from HSVI which are empirically evaluated on various benchmark problems.

Learning Task Specifications from Demonstrations

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #166

Marcell Vazquez-Chanlatte · Susmit Jha · Ashish Tiwari · Mark Ho · Sanjit Seshia

Real-world applications often naturally decompose into several sub-tasks. In many settings (e.g., robotics) demonstrations provide a natural way to specify the sub-tasks. However, most methods for learning from demonstrations either do not provide guarantees that the artifacts learned for the sub-tasks can be safely recombined or limit the types of composition available. Motivated by this deficit, we consider the problem of inferring Boolean non-Markovian rewards (also known as logical trace properties or specifications) from demonstrations provided by an agent operating in an uncertain, stochastic environment. Crucially, specifications admit well-defined composition rules that are typically easy to interpret. In this paper, we formulate the specification inference task as a maximum

a posteriori (MAP) probability inference problem, apply the principle of maximum entropy to derive an analytic demonstration likelihood model and give an efficient approach to search for the most likely specification in a large candidate pool of specifications. In our experiments, we demonstrate how learning specifications can help avoid common problems that often arise due to ad-hoc reward composition.

Teaching Inverse Reinforcement Learners via Features and Demonstrations

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #167

Luis Haug · Sebastian Tschiatschek · Adish Singla

Learning near-optimal behaviour from an expert's demonstrations typically relies on the assumption that the learner knows the features that the true reward function depends on. In this paper, we study the problem of learning from demonstrations in the setting where this is not the case, i.e., where there is a mismatch between the worldviews of the learner and the expert. We introduce a natural quantity, the teaching risk, which measures the potential suboptimality of policies that look optimal to the learner in this setting. We show that bounds on the teaching risk guarantee that the learner is able to find a near-optimal policy using standard algorithms based on inverse reinforcement learning. Based on these findings, we suggest a teaching scheme in which the expert can decrease the teaching risk by updating the learner's worldview, and thus ultimately enable her to find a near-optimal policy.

Single-Agent Policy Tree Search With Guarantees

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #168

Laurent Orseau · Levi Lelis · Tor Lattimore · Theophane Weber

We introduce two novel tree search algorithms that use a policy to guide search. The first algorithm is a best-first enumeration that uses a cost function that allows us to provide an upper bound on the number of nodes to be expanded before reaching a goal state. We show that this best-first algorithm is particularly well suited for "needle-in-a-haystack" problems. The second algorithm, which is based on sampling, provides an upper bound on the expected number of nodes to be expanded before reaching a set of goal states. We show that this algorithm is better suited for problems where many paths lead to a goal. We validate these tree search algorithms on 1,000 computer-generated levels of Sokoban, where the policy used to guide search comes from a neural network trained using A3C. Our results show that the policy tree search algorithms we introduce are competitive with a state-of-the-art domain-independent planner that uses heuristic search.

From Stochastic Planning to Marginal MAP

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #169

Hao Cui · Radu Marinescu · Roni Khardon

It is well known that the problems of stochastic planning and probabilistic inference are closely related. This paper makes two contributions in this context. The first is to provide an analysis of the recently developed SOGBOFA heuristic planning algorithm that was shown to be effective for problems with large factored state and action spaces. It is shown that SOGBOFA can be seen as a specialized inference algorithm that computes its solutions through a combination of a symbolic variant of belief propagation and gradient ascent. The second contribution is a new solver for Marginal MAP (MMAP) inference. We introduce a new reduction from MMAP to maximum expected utility problems which are suitable for the symbolic computation in SOGBOFA. This yields a novel algebraic gradient-based solver (AGS) for MMAP. An experimental evaluation illustrates the potential of AGS in solving difficult MMAP problems.

Dual Principal Component Pursuit: Improved Analysis and Efficient Algorithms

Poster | Wed Dec 5th 05:00 -- 07:00 PM @ Room 210 & 230 AB #170

Zhihui Zhu · Yifan Wang · Daniel Robinson · Daniel Naiman · Rene Vidal · Manolis Tsakiris

Recent methods for learning a linear subspace from data corrupted by outliers are based on convex L1 and nuclear norm optimization and require the dimension of the subspace and the number of outliers to be sufficiently small [27]. In sharp contrast, the recently proposed Dual Principal Component Pursuit (DPCP) method [22] can provably handle subspaces of high dimension by solving a non-convex L1 optimization problem on the sphere. However, its geometric analysis is based on quantities that are difficult to interpret and are not amenable to statistical analysis. In this paper we provide a refined geometric analysis and a new statistical analysis that show that DPCP can tolerate as many outliers as the square of the number of inliers, thus improving upon other provably correct robust PCA methods. We also propose a scalable Projected Sub-Gradient Descent method (DPCP-PSGD) for solving the DPCP problem and show it admits linear convergence even though the underlying optimization problem is non-convex and non-smooth. Experiments on road plane detection from 3D point cloud data demonstrate that DPCP-PSGD can be more efficient than the traditional RANSAC algorithm, which is one of the most popular methods for such computer vision applications.