# IFDS DRDS Workshop 2022: Abstracts

For the **full schedule**, please see the webpage.

## Samory Kpotufe

**Date & Time**: 9:45 to 10:30 am on Thursday, August 4, 2022

**Title**: Tracking Most Significant Arm Switches in Bandits

**Abstract**: In bandit with distribution shifts, one aims to automatically adapt to unknown changes in reward distribution, and restart exploration when necessary. While this problem has received attention for many years, no adaptive procedure was known till a recent breakthrough of Auer et al (2018, 2019) which guarantees an optimal (dynamic) regret (LT)^{1/2}, for T rounds and L stationary phases.

However, while this rate is tight in the worst case, it leaves open whether faster rates are possible, adaptively, if few changes in distribution are actually severe, e.g., involve no change in best arm. We provide a positive answer, showing that in fact, a much weaker notion of change can be adapted to, which can yield significantly faster rates than previously known, whether as expressed in terms of number of best arm switches--for which no adaptive procedure was known, or in terms of total variation. Finally, our parametrization captures at once, both stochastic and non-stochastic adversarial settings.

This is joint work with Joe Suk.

## Hongseok Namkoong

**Date & Time**: 9 to 9:45 am on Friday, August 5, 2022

**Title**: Assessing the external validity (a.k.a. distributional robustness) of causal findings

**Abstract**: Causal inference—analyzing the ceteris paribus effect of an intervention—is key to reliable decision-making. Due to population shifts over time and underrepresentation of marginalized groups, standard causal estimands that measure the average treatment effect often lose validity outside the study population. To guarantee that causal findings remain valid over population shifts, we propose the worst-case treatment effect (WTE) across all subpopulations of a given size. We develop an optimal estimator for the WTE based on flexible prediction methods, which allows analyzing the external validity of the popular doubly robust estimator. On real examples where external validity is of core concern, our proposed framework

successfully guards against brittle findings that are invalidated under unanticipated population shifts.

# Terry Rockafellar

**Date & Time**: 11 to 11:45 am on Friday, August 5, 2022

**Title:** Robustness from the Perspective of Coherent Measures of Risk

**Abstract:** Measures of risk seek to quantify the overall "risk" in a cost- or loss-oriented random variable by a single value, such as its expectation or worst outcome, or better, something in between.Common sense axioms were developed for this in the late 90s by mathematicians working in finance, and they used the term "coherent" for the risk measures that satisfied those axioms. Their work was soon broadened, and it was established by way of duality in convex analysis that coherent measures of risk correspond exactly to looking for robustness with respect to some collection of alternative probability distributions.

The theory has since become highly developed with powerful approaches to quantification like conditional value-at-risk and others based on that. Now also, it includes interesting connections with statistics and regression captured by the "fundamental quadrangle of risk", as will be explained in this talk, with examples.

# Rediet Abebe

**Date & Time**: 2 to 2:45 pm on Friday, August 5, 2022

**Title:** Algorithms on Trial: Interrogating Evidentiary Statistical Software

**Abstract:** The U.S. criminal legal system increasingly relies on software output to convict and incarcerate people. In a large number of cases each year, the government makes these consequential decisions based on evidence from statistical software---such as probabilistic genotyping, environmental audio detection and toolmark analysis tools---that the defense counsel cannot fully cross-examine or scrutinize. This undermines the commitments of the adversarial criminal legal system, which relies on the defense's ability to probe and test the prosecution's case to safeguard individual rights.

Responding to this need to adversarially scrutinize output from such software, in this talk, we propose a novel framework for examining the validity of evidentiary statistical software called Robust Adversarial Testing. We define and operationalize this notion of robust adversarial testing for defense use by drawing on a large body of recent work in robust machine learning and algorithmic fairness. We demonstrate how this framework both standardizes the process for

scrutinizing such tools and empowers defense lawyers to examine their validity for instances most relevant to the case at hand. We further discuss existing structural and institutional challenges within the U.S. criminal legal system which may create barriers for implementing this framework and close with a discussion on policy changes that could help address these concerns. We close with an outline of research directions in this burgeoning area of adversarial ML and adversarial scrutiny in the law.

This talk is based on joint and ongoing work with Moritz Hardt, Angela Jin, John Miller, Ludwig Schmidt, Rebecca Wexler, as well as conversations with numerous public defenders and forensic scientists including Nathan Adams, Clinton Hughes, Daniel Krane, and Richard Torres.

**Biography:** Rediet Abebe is an Assistant Professor of Computer Science at the University of California, Berkeley. She is a 2022 Andrew Carnegie Fellow and on leave as a Junior Fellow at Harvard University. Her research examines the interaction of algorithms and inequality, with a focus on contributing to the mathematical and computational foundations of this emerging research area. Abebe co-launched and served on the Executive Committee for the ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO). She previously co-founded the related global research initiative, MD4SG. Abebe's work has received recognitions including the MIT Technology Reviews' 35 Innovators Under 35, the 2020 ACM SIGKDD Dissertation Award, an honorable mention by the ACM SIGEcom Dissertation Award, and the Bloomberg 50 list as a one to watch. Abebe co-founded and serves on the Board of Directors for Black in AI, a non-profit organization tackling equity issues in AI. Abebe holds a Ph.D. in computer science from Cornell University and masters degrees in mathematics from Harvard University and the University of Cambridge.

# Brian Ziebart

**Date & Time**: 9:45 to 10:30 am on Saturday, August 6, 2022

**Title:** Prediction Games: From Maximum Likelihood Estimation to Active Learning, Fair Machine Learning, and Structured Prediction

**Abstract:** A standard approach to supervised machine learning is to choose the form of a predictor and to then optimize its parameters based on training data. Approximations of the predictor's performance measure are often required to make this optimization problem tractable. Instead of approximating the performance measure and using the exact training data, this talk explores a distributionally robust approach using game-theoretic approximations of the training data while optimizing the exact performance measures of interest. Though the resulting "prediction games" reduce to maximum likelihood estimation in simple cases, they provide new methods for more complicated prediction tasks involving covariate shift, fairness constraint satisfaction, and structured data.

**Biography:** Brian Ziebart is an Associate Professor in the Department of Computer Science at the University of Illinois at Chicago and a Software Engineer at Aurora Innovation. He earned his PhD in Machine Learning from Carnegie Mellon University where he was also a postdoctoral fellow. His interests lie in the intersections between machine learning, game theory, and decision theory. He has published over 35 articles in leading machine learning and artificial intelligence venues, including a Best Paper at the International Conference on Machine Learning.