Empowering Algorithms to Solve Societal-Scale Challenges

The future is cyberphysical, according to Ming Jin, an ECE assistant professor. Cities will be smart; the electric grid will be highly adaptive, secure, and efficient; and we will use data and algorithms to solve our greatest challenges—including how to improve people’s living conditions and combat climate change. Jin wants to empower algorithms to help solve these problems.

“Unlike traditional machine learning tasks, these problems involve complex physical systems with a significant cyber core that are safety-critical and need to have humans in the loop,” said Jin. “Systems like these require a new paradigm of artificial intelligence that can be trusted to do critical work.”

To be considered trustworthy, a system must make decisions that are reliable, safe, and understandable, explained Jin. To move this vision closer to reality, he is developing fundamental theories to improve optimization, control, and machine learning.

COMPLEXITY IN THE POWER SYSTEM

The power grid is considered the biggest, most expensive machine in the world. It’s becoming increasingly complex as we integrate renewable energies and interconnected devices like advanced sensors and power electronics that can gather data and collaboratively manage the grid assets—which makes it a perfect application for Jin’s research.

Systems as large as a power grid churn out gigantic pools of data, and Jin is investigating machine learning methods to digest the data into actionable intelligence so that the data can be useful, cost-effective, and empowering.

ASSURED REINFORCEMENT LEARNING

Reinforcement learning is a branch of machine learning that deals with sequential decision making, and Jin is applying it to vital infrastructures like power grids. “As you push data through the complex learning and control pipeline, things may not turn out the way you expected,” Jin explained. “And that becomes a real issue for power grids, where a bad decision can cost millions of dollars, or even human lives.”

Establishing theoretical and computational foundations for assurance is key to protecting us from the potential harm of artificial intelligence, explained Jin.

To resolve this challenge, Jin and his group are using tools from multiple disciplines, most prominently, dynamical systems theory and statistical learning theory. “The fact that many classical tools no longer suffice and that we are constantly pressed to invent new ones, is very exciting to me,” said Jin. “Assurance is integral to trust. Without trust, AI cannot go far. To get there, we must reimagine the field.”

WEAKLY SUPERVISED LEARNING

Besides reinforcement learning, machine learning problems are often categorized as...
supervised or unsupervised learning depending on whether there is a label attached to each item in a training dataset, explained Jin. But the lack of “hand-labeled” data—data that has been manually categorized for training purposes—has been a huge bottleneck in scaling up data analytics from the power grid and other applications.

One of Jin’s research projects focuses on employing “weakly supervised learning,” which leverages domain knowledge to collect lots of datapoints and assign them lower quality annotations, explained Jin. For example, they might only be 80% certain that the data are labeled correctly, but they compensate for this lower quality data by having access to more of it.

**UNTRUSTWORTHY DATA**

Decision-making algorithms are built on data from the real world, and researchers don’t control the quality of that data. “If part of the data is corrupted, the optimization problems we solve are meaningless because the objective is biased,” said Jin.

Jin and his team are developing theoretical and computational techniques for robust optimization, including an algorithm based on penalized semidefinite programming, a subfield of convex optimization. With this tool, Jin’s team generated the first vulnerability map of the entire U.S. power grid to assess the security of data-driven decision-making algorithms against cyberattacks.