Open Set Detection

Faculty Member(s): Weng-Keen Wong
(Joint work with Minsuk Kahng, Matt Olson)

University: Oregon State University

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

Machine learning classifiers are everywhere in the IoT. They classify data as one of K possible classes seen during training.

During deployment, what happens if a classifier encounters data from an unseen class?

Not quite sure what the classifier will do....

Sources:
- Mint (https://www.publicdomainpictures.net/pictures/90000/velka/mint-leaves-1397346131HTn.jpg)
- Poison Oak (https://upload.wikimedia.org/wikipedia/commons/4/44/Poisonoakyoung.JPG)
Proposal Objectives

• Solution: **Open set detection** detects novel classes seen during deployment that were not seen during training.

• Long term objectives:
  • Improve **robustness** of real-world ML deployment to “unknown unknowns”
  • Improve **user trust** in ML systems

• Year 1 objectives:
  • Identify weaknesses with state-of-the-art approaches
  • Develop new and improved open set detection algorithms based on density ratio estimation
Approach

1. Understand when cross entropy loss fails for open set detection
2. Develop new algorithm based on deep learning density ratio estimation [Nam and Sugiyama 2015]

\[ R(X) = \frac{P_{\text{Unknown}}(X)}{P_{\text{Known}}(X)} \]

Strategic Connections:
- DARPA Science of AI and Learning for Open-world Novelty (SAIL-ON) project ($1.4 million, Tom Dietterich, Stefan Lee)
- DARPA eXplainable AI (XAI) project ($6.5 million, Alan Fern + many others)
- OSU Computer Vision (Fuxin Li, Stefan Lee) and NLP faculty (Liang Huang)
- CU SafeML projects
Deliverables and Outcomes

• Year 1:
  • **Research papers and algorithms**: deep learning density ratio open set detection algorithm
  • **Software**: research source code
  • **Tutorial**: for industry members

• Year 2:
  • **Research papers and algorithms**: open set detection for time series data
  • **Software**: research source code
  • **Tutorial**: for industry members
Executive Summary

• **Goals**: Improve robustness of deployed ML applications to “unknown unknowns”

• **Methods**: Deep learning density ratio based open set detection

• **Impacts**: More robust classifiers in real world settings, improve user trust in deployed ML systems

• **Deliverables**: Research papers, source code implementation, tutorial for industry

Thank you and I looking forward to the discussion in the small breakout rooms!

We need your written feedback at:
www.iucrc.com (then select the PPI Center)
Password (case sensitive):  PPI Begins!
Visual Analytics for Scalable AI Debugging

Minsuk Kahng

Oregon State University

Proposed Project Duration: 2 years

Together We Go Farther
Problem: Industrial Relevance and Novelty

**AI failed... When and Why?**

Even state-of-the-art ML models fail to make correct predictions for many instances.

- e.g., 97% accuracy for 100K cases -> 3,000 failures!

What if AI fails to recognize certain trucks? Challenging to examine all failed cases

How can we help people effectively analyze _when_ AI fails and reason about _why_ it fails?

Image credit: oreilly.com, vision.stanford.edu
Proposed Solution & Objectives:

**Visual Analytics for Debugging AI**

**SOLUTION:**
Create novel **visual analytics** tools for debugging AI

Visual analytics has been successfully helping practitioners explore and interpret complex ML systems for large data.

**LONG-TERM GOAL:**
- Develop systematic **human-in-the-loop** debugging workflow
  - Identify *when* it fails -> Reason about *why* it fails -> Test *what if* we fix

**SHORT-TERM GOAL:**
- Build visualization tools for analyzing failed data cases backed by failure type inference methods
Approach

- Develop scalable, interactive visual analytics tools integrated with XAI techniques
  - to analyze *when* AI failed at a conceptual-level
- Create novel systematic debugging workflows
  - to reason about *why* AI failed for common dataset-related issues (e.g., insufficient data) and gain insights for debugging
- Iterate with industry through participatory design

LEVERAGING:
- Deployed technologies by Facebook (e.g., ActiVis, most cited VIS’17 paper)
- Successful collaboration with Google AI and support ($100K)
  (e.g., GAN Lab used by 130,000 people from 180 countries)
- DARPA-funded XAI projects with OSU faculty (Total $6.5M)
Deliverables and Outcomes

• Year 1:
  • Visualization tool for AI failure analysis
  • Qualitative study results on current industry practice and expert patterns in model debugging
  • Technical paper describing tool development, qualitative study, and technical details

• Year 2:
  • Improved tool supporting the entire workflow
  • Human subject evaluation study results conducted with industry partners
  • Open-sourced tools
Executive Summary:

**Visual Analytics for Scalable AI Debugging**

- Create *visual analytics* tools for *AI failure* analysis
- Develop new workflow to analyze *when & why*
- Leverage our successful collaboration experience (e.g., ActiVis for Facebook, GAN Lab with Google)
- Deliver open-sourced tools developed in close collaboration with industry partners

**We need your written feedback at:**

[www.iucrc.com](http://www.iucrc.com) (then select the PPI Center)

Password (case sensitive): PPI Begins!

**Minsuk Kahng**

Oregon State University

[https://minsuk.com](https://minsuk.com)
Safe Programmatic Reinforcement Learning

Faculty Member: Ashutosh Trivedi
University: University of Colorado Boulder
Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

Program Synthesis

Adaptive Software
Problem: Industrial Relevance and Novelty

Pain-points with state-of-the-art solutions:

- **(Usability)** Learning requirements must be specified as scalar reward signals
- **(Scalability)** Infinite state-space due to numerical data-types and potentially unbounded procedural call stacks
- **(Usability)** ML expertise in providing suitable approximation schemes
- **(Trustworthiness)** Manual approximations lead to low productivity and low assurance

*Lack of automation results in significant barrier to entry*
Proposed Solution & Project Objectives

Goal:  
*Develop Formal methods to improve the scalability, usability, and trustworthiness of programmatic Reinforcement Learning (RL).*

1. **Usability.** Enable *formal specifications* in expressing learning requirements.

2. **Scalability.** Integrate specification-guided software abstractions to achieve scalability.

3. **Trustworthiness.** Develop formal verification approaches for RL-enabled software systems to refine abstractions.
Approach: Abstraction-based RL

- Programmatic RL built around the state-of-the-art formal RL Mungojerrie
- Extend Mungojerrie with programmatic inputs for the environment, agents, and reward.
- Specification-guided software abstraction approach to tackle infinite state space
- Novel RL algorithms to handle potentially recursive structure
- Integrate formal policy verification to provide rigorous guarantees about the learning outcomes

Leverage: Mungojerrie (funded by NSF at $500,000)
Deliverables and Outcomes

Year One:
1. Programmatic Reinforcement Learning based synthesis tool for Python programs
2. Easy-to-use DSL to specify learning requirements

Year Two:
1. Extend the programmatic Reinforcement Learning for Recursive Programs
2. Verification engine capable of reasoning with software with Neural-Networks-based components
Executive Summary

- Create a Programmatic RL framework integrating formal specifications to synthesize programs
- Exploit Specification-Guided Software Abstractions to Scale Reinforcement Learning
- Develop Formal Verification support for software with deep neural networks (DNN)-based components to refine abstractions

We need your written feedback at:
www.iucrc.com (then select the PPI Center)
Password (case sensitive): PPI Begins!

Ashutosh Trivedi
Ashutosh.Trivedi@Colorado.Edu
http://plv.colorado.edu
Explaining and Improving Deep Networks for Vision and Language Tasks

Faculty Member(s): Prasad Tadepalli

University: Oregon State University

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

- Deep neural networks have achieved overwhelming success in many tasks
- But do they give the right answer for right reasons?
- Trust is crucial for safety-critical applications
  - Autonomous driving
  - Personalized news service

- How can we build trust?
  - More faithful visualizations than current approaches
  - Better understanding of how the deep models operate

- Improving the neural network technology
  - Robust adversarial testing of deep networks
  - Better learning algorithms and architectures
Proposed Solution & Project Objectives

• The network decided it is a racecar. But why?
  • The 3 attention maps on the right represent 3 distinct reasons
• Develop visualizations and representations that are more transparent and faithful to the original network
• Explain the workings of neural language models by analyzing what information is retained at each layer
• Develop methods for robust adversarial testing of language models
Approach

- Computer Vision
  - Structured attention graphs (SAGs) show a set of high scoring attention maps and how the scores change when different parts (outlined in red) are occluded in the form of a graph
    - Work supported by DARPA as part of XAI project ($6,545,123, PI: Alan Fern)
  - Implement new algorithms for generating SAGs and other transparent representations with high coverage

- Natural Language Processing
  - Use probing tasks to explain their inner workings of neural models
  - Study human adversarial attacks of question-answering systems
  - Develop algorithms for automatically generating adversarial examples
Deliverables and Outcomes

• First Year Objectives
  • **Local explanations**: Software for translating neural nets into equivalent transparent representations. Due date: Jan 2021
  • **Global explanations**: Software for probing NLP models. Tutorial on explainable machine learning. Due date: June 2021

• Second Year Objectives
  • **Adversarial testing**: Interactive interfaces for collecting human-generated adversarial examples. Due date: Jan 2022
  • **Example generation**: Software for automatically generating adversarial examples. Tutorial on adversarial example generation. Due date: June 2022
Executive Summary

• Goals of our research
  • **Deeper understanding** of how neural networks work on language and vision tasks
  • **Improving the performance** of deep networks through robust training and better architectures

• Methods
  • Constructing equivalent transparent representations
  • Explaining language models through probing
  • Adversarial example generation and training

• Deliverables
  • Algorithms and code for generating structured explanations and adversarial examples
  • Tutorials on explainable machine learning and adversarial example generation

We need your written feedback at:
www.iucrc.com (then select the PPI Center)
Password (case sensitive): PPI Begins!
Improved Accessibility and Mobility Using a Topological Approach

Faculty Member: Eugene Zhang

University: Oregon State University

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

• Accessibility and mobility need is constantly changing
  • Population growth and migration
  • Evacuation during natural disasters (e.g. wildfires)
Problem: Industrial Relevance and Novelty

• Accessibility and mobility need is constantly changing
  • Population growth and migration
  • Evacuation during natural disasters (e.g. wildfires)

• Accessibility and mobility is greatly impacted by
  • Location and capacity of resources (e.g. hospitals, shelters)
  • Connectivity and capacity of the road network

• How to improve the resilience against the uncertainty in accessibility and mobility?
Proposed Solution & Project Objectives

• Long-term: The ability to accommodate our society’s needs for accessibility and mobility based on statistical prediction of short-term and long-term changes

• Year 1 objectives:
  • Work closely with our industrial partners to identify critical issues in route planning, resource placement, and emergency management
  • Develop topology-based analysis and visualization tools that allow data stakeholders to better understand their accessibility and mobility data

• Year 2 objectives:
  • Incorporate prediction models into our analysis and visualization
  • Continue collaboration with our industrial partners to deploy our software
Approach

- Solutions: Apply and adapt modern topological approaches which are concerned with the connectivity of spaces

Path Planning Using Topology
Xu et al., SIGGRAPH ASIA 2017
Approach

• **Solutions**: Develop and apply modern topological approaches which are concerned with the connectivity of spaces
  - Network homology for accessibility and mobility analysis
  - Tensor field singularity identification for path planning and resource placement
  - Bifurcations for modeling changing accessibility and mobility needs

---

**Strategic Connections:**
- Past research in path planning using topology [SIGGRAPH ASIA 2017] and procedural road network design [SIGGRAPH 2008]
- Ongoing NSF project on tensor field topology
- International collaboration with University of Stuttgart (eyetracking and UI), University of Leipzig (tensor field visualization), King Abdulal University of Science and Technology (mesh connectivity editing), and University of Nottingham (flow visualization)
Deliverables and Outcomes

• Year 1:
  • Tutorial on topological data analysis
  • Analysis and visualization techniques for partners’ accessibility and mobility data
  • Software tools implementing the above analysis and visualization techniques
  • Research publications

• Year 2:
  • Incorporate prediction models of accessibility and mobility into our analysis and visualization framework
  • Software implementation
  • Publications
Executive Summary

• Goals:
  • Improve the resilience of our ability to address constantly changing accessibility and mobility needs

• Methods:
  • Apply modern topology
  • Incorporate prediction modeling into our topology-driven approach

• Impacts:
  • Better understanding of data
  • Increased resilience against short-term and long-term changes in accessibility and mobility needs

• Deliverables:
  • Tutorial, software with source code and research papers,

We need your written feedback at:
www.iucrc.com (then select the PPI Center)
Password (case sensitive): PPI Begins!
Device-Based Exploratory Analytics

Faculty Member: Danielle Albers Szafir
University: University of Colorado Boulder
Proposed Project Duration: 2 years
Problem: Industrial Relevance & Novelty
Problem: Industrial Relevance & Novelty
Problem: Industrial Relevance & Novelty

**Temporal Gap**
*Timely decision-making*
- Operating on stale data
- Unable to react to changing environments
- Analysis at end of day or whole operation

**Spatial Gap**
*Remote collaboration*
- Decontextualized data
- No shared context for collaboration
- Limited connectivity

Whitlock, Wu, & Szafir, 2020
Proposed Solution & Proposed Objectives

**Goal:** Develop a suite of responsive visual analytics tools tailored to support exploratory insight and decision making at the point of action

Design intelligent & responsive visualization interfaces tailored to devices people actually use

Optimize decision making at point of action

Leverage traditional & natural language interaction for efficient, accessible exploration
Approach

1. Determine device-optimal representations

2. Construct responsive toolkit

3. Integrate & expand natural language query engine

4. Develop active learning assistive agent
Deliverables & Outcomes

**Year One:**
- Responsive visualization toolkit with:
  1. Display-based visualizations
  2. Preliminary natural language interaction

**Year Two:**
- Expanded natural language query toolkit
- Adaptive intelligent agent
- Interface integration with agent
Executive Summary

Create a visual analytics suite for analysis and data-driven decision making at point of action.

Design visualizations tailored to user needs to optimize analytical efficiency.

Integrate natural language interaction to facilitate data use at scale in context.

We need your written feedback at: www.iucrc.com (then select the PPI Center) Password (case sensitive): PPI Begins!
System Support to Enable AI at the Edge

Faculty Member(s): Shiv Mishra
University of Colorado

Proposed Project Duration: 2 years
We ran this algorithm on a video dataset "Peds1". Anomaly Detection in Video Streams: Anomalous events could be abnormal motion patterns or high variation in local spatio-temporal neighborhoods, we would expect video streams have several security applications. For example, one remote sensing data to process in the cloud when an immediate of natural images of a pedestrian walkway. Given that we model method to a video dataset. (a) represents the frame on which we time. Figure 4 shows the result of applying our anomaly detection amount of variation in pixel values that lasts for a short amount of probabilistic anomaly detection framework (KDD-17 under review). identify unattended bags or other objects. We recently developed a could monitor video streams at airports and other public places to by the farmer before its too late. time detection of weeds and crop diseases will allow timely action using the spatiotemporal edge computing framework. Such real-processing outright. The following are some example cases:

1. Computations: Context aware, compute-intensive, real or near real time, privacy preserving, ...
2. Examples - face recognition & tracking, anomaly detection, pattern matching, optimization, ...
3. Data: Large volume, hybrid, multiple sources, location-specific, privacy-sensitive, limited lifetime
Problem: Industrial Relevance and Novelty

*Computing on the cloud has serious drawbacks – high latency, high bandwidth consumption, privacy leakage, lost context, ...*

**Edge Server:** (Storage, CPU, GPU, FPGA, ASICs)

**Edge computing:** Low latency, low bandwidth consumption, security & privacy, separate administrative domains

**Challenges in edge computing**
- Lack of any integrated system level support
- Heterogeneity of computing devices and computing & networking elements
- Minimal support to manage resource sharing
Proposed Solution & Project Objectives

Long-term

Develop system support to enable AI computations at the Edge
- A microservice-based architecture: Containers, VMs, serverless…
  - Complementary to contemporary middlewares – EdgeX, Kura, …
- Utilize diverse computing resources at the edge
  - Sensors, drones, smartphones, edge server(s) equipped with CPUs, GPUs, FPGAs and other ASICs
- Humans in the loop

Short-term

Y1: Investigate distributed execution of AI algorithms over ASICs
Y1: Develop individual components for the microservice architecture

Y2: Extend AI implementations to *fluidly* distribute AI computations
Y2: Develop a fully-fledged flexible microservice-based architecture
Approach

• Integrate *Shimmy* and *Dynamic Graphs* with Kubernetes
  
  • *Shimmy*: an efficient inter-container communication tool
  
  • *Dynamic Graphs*: a dynamic container orchestration tool

• Investigate serverless solutions for the edge: Firecracker, Openwhisk

• Experiment with AI algorithms (face/object recognition, anomaly detection, optimization, gesture recognition)
  
  • Fluidly distributed over different accelerator architectures
  
  • Use state-of-the-art programming models such as oneAPI

---

**Leverage**

• More than $3.0 M current NSF funding on topics related to system support and applications for edge computing

• Active collaboration with The City of Denver, several non-profits (Growhaus, Groundwork Denver, Clinica Tepeyac), and several low socio-economic communities (Globeville, Elyria-Swansea, Cole)

• Interdisciplinary research involving environmental engineering, social science and education researchers
Deliverables and Outcomes

• Y1: A Kubernetes-compatible dynamic container orchestration

• Y1: Prototype implementations of common AI algorithms over CPU, GPU and FPGA

• Y1: Integration of Firecracker into Openwhisk

• Y2: An extended version of AI algorithm implementations incorporating fluidity

• Y2: A flexible microservice architecture incorporating diverse computing elements, devices and software components to enable AI at the edge
Executive Summary

Edge computing is the key driving technology for IoT systems and smart city enabling PPI applications

• **Problem:** Building sophisticated AI applications at the edge is a complex task at present

• **Our solution:** A flexible, microservice-based architecture comprised of diverse computing elements, devices and software components to enable AI at the edge

• **Several deliverables throughout the course of the project**
  - A dynamic container orchestration tool; prototypes of popular AI algorithms distributed fluidly over CPUs, GPUs, FPGAs; serverless solution at the edge; microservice-based edge architecture

We need your written feedback at: http://www.iucrc.com/ (then select the PPI Center) Password (case sensitive): PPI Begins!
Network as a Reusable Programming Platform

Faculty Member(s): Sangtae Ha
(Joint work with Dirk Grunwald)
University: CU Boulder
Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

The trend towards more programmability and flexibility in the networks makes it possible to program everything.

- Network interface cards at edge and IoT devices
- Network devices such as edge routers and switches
- Even physical layers are programmable

However, an individual application might implement non-reusable proprietary code to offload part of its application into the network, resulting in time-consuming duplicate efforts.
Proposal Objectives

- Long-term:
  Develop reusable network primitives that can help offload common system components of a broad range of edge and IoT applications into the programmable network hardware for enhancing performance, reliability, and scalability.

- Short-term:
  Y1: Identify the list of common reusable network primitives
  Y2: Develop those primitives using a data plane programming language (P4) and evaluate them with real applications.
Approach

• **Divide the process execution** into two phases:
  
  **Fast path:** failure-free operation involving H/W; the most efficient way to enhance access latency, throughput, and scalability.
  
  **Slow path:** used to recover from errors; processing is relatively slow compared to the fast path.

• **Design, implement, and evaluate reusable network primitives** that execute in the fast path of the network.

• **Leverage** multiple awards from NSF and NIST totaling 2.1M
Deliverables and Outcomes

• Year 1:
  • **Research papers**: survey paper that describes the list of common reusable network primitives for various network applications
  • **Software**: sample code for a set of reusable network primitives for achieving network reliability
  • **Tutorial**: for industry members

• Year 2:
  • **Research papers**: research paper that describes the design and implementation of practical network applications built on top of these primitives
  • **Software**: software code for a representative application and its reusable network primitives
  • **Tutorial**: for industry members
Executive Summary

• **Goals**: Develop reusable network primitives that can be offloaded into programmable hardware to enhance edge and IoT applications’ performance

• **Methods**: Divide the process execution into two phases, fast path and slow path, and identify the list of reusable network primitives that can benefit from running on the programmable hardware (fast path) and implement them

• **Impacts**: Emerging edge and IoT applications can leverage network hardware to enhance their latency, throughput, and scalability

• **Deliverables**: Research papers, source code of reusable network primitives, tutorial for industry

Committed to working with industry partners to shape our research direction

We need your written feedback at:
www.iucrc.com (then select the PPI Center)
Password (case sensitive): PPI Begins!
Privacy-Preserving Data Reconciliation

Mike Rosulek
Oregon State University

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

• Data all in one place? Simple computation!
• What if data can’t be in one place?

Ad impressions

<table>
<thead>
<tr>
<th>userid</th>
<th>date</th>
</tr>
</thead>
<tbody>
<tr>
<td>mike@or..</td>
<td>2020-09...</td>
</tr>
<tr>
<td>danny@...</td>
<td>2018-04...</td>
</tr>
<tr>
<td>evan@co..</td>
<td>2019-11...</td>
</tr>
<tr>
<td>shiv@col..</td>
<td>2020-02...</td>
</tr>
</tbody>
</table>

Purchases

<table>
<thead>
<tr>
<th>userid</th>
<th>amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>minsuk@..</td>
<td>8235</td>
</tr>
<tr>
<td>evan@co..</td>
<td>1143</td>
</tr>
<tr>
<td>mike@or..</td>
<td>27</td>
</tr>
<tr>
<td>ben@col..</td>
<td>4999</td>
</tr>
</tbody>
</table>

• How much spent by people who saw the ad?

```sql
select sum(purchase.amount)
where impression.userid = purchase.userid
```
Proposed Solution & Project Objectives

• Long-term vision: “SQL on distributed, private data”
  • centralization → cryptography
• Release only result of query that all parties agree to

<table>
<thead>
<tr>
<th>id</th>
<th>date</th>
<th>rid</th>
</tr>
</thead>
<tbody>
<tr>
<td>mike@or.</td>
<td>2020-09...</td>
<td>87cf..</td>
</tr>
<tr>
<td>danny@..</td>
<td>2018-04...</td>
<td>a920..</td>
</tr>
<tr>
<td>evan@co.</td>
<td>2019-11...</td>
<td>23db..</td>
</tr>
<tr>
<td>shiv@col.</td>
<td>2020-02...</td>
<td>64d8..</td>
</tr>
</tbody>
</table>

• Feasible in short term:
  • select id where A.id = B.id → “evan, mike”
  • select count(*) where A.id = B.id → “2”
  • select sum(B.val) where A.id = B.id → “1170”
  • Compute encrypted representation of common items
  • “Align” datasets via common random identifiers
Approach

• Leverage our ongoing cryptographic research
  • leading group in designing Private Set Intersection protocols
  • Prototype implementations (fastest, least communication to date)

• Adapt our successful PSI techniques to related problems where less information is revealed

• Prior support/awards ($700k)
Deliverables and Outcomes

- **Y1**: New designs / security analysis for protocols that hide more partial information (compute only aggregate information about common items)
- Usable open-source library implementations & benchmarks
  - **Y1**: revealing all common items
  - **Y1**: computing aggregate information about common items
  - **Y2**: aligning datasets via common random identifiers
  - **Y2**: compute common items in encrypted form
- **Y1-Y2**: Whitepapers explaining provable security guarantees and limitations to non-cryptographers
- **Y2**: Tools for integrating with data sources of interest
Executive Summary

• **Goal**: towards “SQL on distributed, private data”

• **Method**: state-of-art cryptographic protocols

• **Impacts**: get insights from data even when it can’t be collected centrally

• **Deliverables**: open-source libraries that you can use (even without a crypto R&D dept)

We need your written feedback: [www.iucrc.com](http://www.iucrc.com) -> PPI Center -> password “PPI Begins!”
Conformance Verification for Machine Learning Models

Faculty Member(s): Sriram Sankaranarayanan

University: University of Colorado, Boulder

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

Machine Learning

Data → Model Structure → Prediction Model

Decision Support Control Actions
Warnings/Advisories

Blood Gluc. → Insulin

Future Blood Glucose.

Vehicle State

Throttle/Brakes

Future Vehicle Position/Velocity

AutoRally Car
[Goldfain et al. 2019]

More brakes/less throttle → slower future velocity?

More insulin → lower blood glucose predictions?

Narasimhamurthy et al’ 2019; Kushner et al’2020

Insulin Glucose Regulation for Type-1 Diabetes
[Cobelli et al 2011]
Proposed Solution & Project Objectives

• **Specification:** conformance for ML models.
  - *What properties* do we expect when we train a machine learning model?
  - How do we express the properties formally?

• **Verification and Falsification.**
  - Can we **prove conformance**?
  - Can we **find “realistic” counterexamples**?

• **Data Debugging**
  - Detect/Predict potential conformance violations even before a model is trained.
Approach

• Year 1
  • **Survey Industry Members:** Find ML applications/domains of interest to industry partners.
  • **Try out existing solutions:** Retrofit Sherlock tool built by PI and collaborators.

• Year 2
  • **Work with Industry Members** on solution.
  • Integrated specification/verification mechanism for machine learning models.
  • **Data Debugging:** from data collection and learning pipeline to predicting potential conformance failures.

Existing Funding:
• NSF CPS award Conformant Learning - $1.2M for 3 years.
• NSF SHF award Verification of Data-Driven Models: $500K for 3 years.
• Juvenile Diabetes Research Foundation (JDRF) grant on data-driven treatments for diabetes.

SHERLOCK Tool: https://github.com/souradeep-111/sherlock
Deliverables and Outcomes

• Year 1 Deliverables.
  • Case study reports for conformance properties in applications of interest to industry members.
  • Specification formalisms and prototype of an integrated analysis tool.

• Year 2.
  • Richer specification languages with verification tools.
  • Better integration into ML frameworks used by our industry members.
  • Solutions for understanding root causes and fixing issues with conformance.
Executive Summary

• Machine learning techniques are focused on getting accurate classification with low errors.
• Often models must satisfy important properties.

Ongoing basic research supported by existing grants:

• NSF CPS award Conformant Learning - $1.1M for 3 years.
• NSF SHF award Verification of Data-Driven Models: $500K for 3 years.
• Juvenile Diabetes Research Foundation (JDRF) grant on data-driven treatments for diabetes.

Existing Infrastructure/tools that will be developed further:

• SHERLOCK https://github.com/souradeep-111/sherlock

References (papers from our research group):

Intelligent Assistants for Creating PPI Applications

Bor-Yuh Evan Chang

Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

I don’t know what caused the crash.
Problem: Industrial Relevance and Novelty

I don’t know what caused the crash.
Proposed Solution:

Imagining tomorrow’s social programming ...

I am not alone

“Transfer” a bug fix with algorithmic and data-driven program analysis and synthesis.

I don’t know what caused the crash.
Proposed Solution & Project Objectives

Long Term

Intelligent, data-driven tools that leverage communities to search, test, repair, and verify PPI apps

Shorter Term

Study PPI Application Development: How is intelligent IoT software developed today? Shortcomings of software frameworks?

Design PPI Software Analysis Tools: How to leverage state-of-the-art data-driven and algorithmic program analysis engines?

Apply PPI Software Analysis Tools: How to assist software developers, improving the state-of-practice in intelligent IoT application development?
Approach

infeasible testing space of all possible event inter-leavings

goal-directed slices to prove, for example, 92% of dereferences safe in open-source Android apps

Leverages

DARPA $1.9M. Chang (PI) with Anderson, Cerny, Sankanarayanan, and Yeh. Mining and Understanding Bug Fixes to Address Application-Framework Protocol Defects.

+ $7.2M of other past and present DARPA and NSF investments
Deliverables and Outcomes

**Year 1.** Identify and curate a repository of common defects and important assertions in the most relevant software frameworks for creating PPI apps

**Year 2.** Develop automated reasoning techniques and release tools that address the most pressing issues for PPI-app engineers
Executive Summary

**Goal.** Create intelligent, data-driven tools that leverage communities of developers to help your engineer diagnose, repair, and verify PPI apps

**Methods.** Mining code repositories and automated reasoning (for uniquely PPI frameworks)

**Impacts.** Gain additional confidence in your product's quality (and QA savings), earning trust in products that your customers love

**Deliverables.** Access to state-of-the-art tools for PPI (even without an automated reasoning R&D department)

We need and appreciate your written feedback at [www.iucrc.com](http://www.iucrc.com) (then select the PPI Center)

Password (case sensitive): PPI Begins!
Code Migration for ML-based Software

Faculty Member(s): Danny Dig
University: CU Boulder
Proposed Project Duration: 2 years
Problem: Industrial Relevance and Novelty

90% of software costs are due to evolution

ML code also needs to evolve:

- paradigm transformations (e.g., Eager to Static in TensorFlow)
- optimize performance (e.g., loops to Numpy algorithms)

ML-related change support in infancy stage
- makes ML sw development expensive
Proposed Solution & Project Objectives

Interactive program transformations
human in control, let the tool do the heavy lifting

Mechanize change tasks for ML-components that are expensive, time-consuming, and error-prone

Y1: Mine from code repositories, understand, and catalog common SW changes for ML components

Y2: Automate changes: design, implement, evaluate and deploy Interactive program refactoring tools

Focus on transformations to optimize performance
**Leverage:**
- multiple past and current awards totaling $2.7M
- multiple past and current industry awards totaling $650K
- relationships with IDE providers

**Approach**

**Develop pattern mining tool** for repetitive changes
- fine-grained program dependence graphs [ICSE’19] + Type inference
- deploy on 3000+ open-source repository of top Python ML software
- learn common changes in proprietary ML codebase from industry members

**Design, develop, and evaluate refactoring tools**
- learn & automate transformations from previously mined patterns
- deploy with IDEs used at industry members

![PyCharm](image)
Deliverables and Outcomes

Y1: **Curated repo of best-practices** transformations for ML code: educational, test others tools from PPI Center

Y1: **Design Patterns & Tutorials** tailored for industry (e.g., our repo for Async got 150,000+ industry visitors)

Y1: **Reusable framework for code pattern mining** for Python (train & deploy at industry members, others PPI)

Y2: **Release plugins for IDEs** used by industry members (e.g., our refactoring tools in official IDEs, 20M+/year downloads)
Executive Summary

Change is the only guaranteed constant: **ML code evolves too**
- currently done manually: error-prone, tedious, expensive

Our solution: **interactive program analysis & transformation**
- Grounded on formative studies of real-world changes

**Delivering**: curated repos of best-practices, industry tutorials, reusable frameworks, refactoring tools

**Committed to industry partners to shape our research**
- iterative process, present progress, get feedback, improve, reenter

We need & appreciate your written feedback at: [http://www.iucrc.com/](http://www.iucrc.com/) (then select the PPI Center)
Password (case sensitive):  PPI Begins!