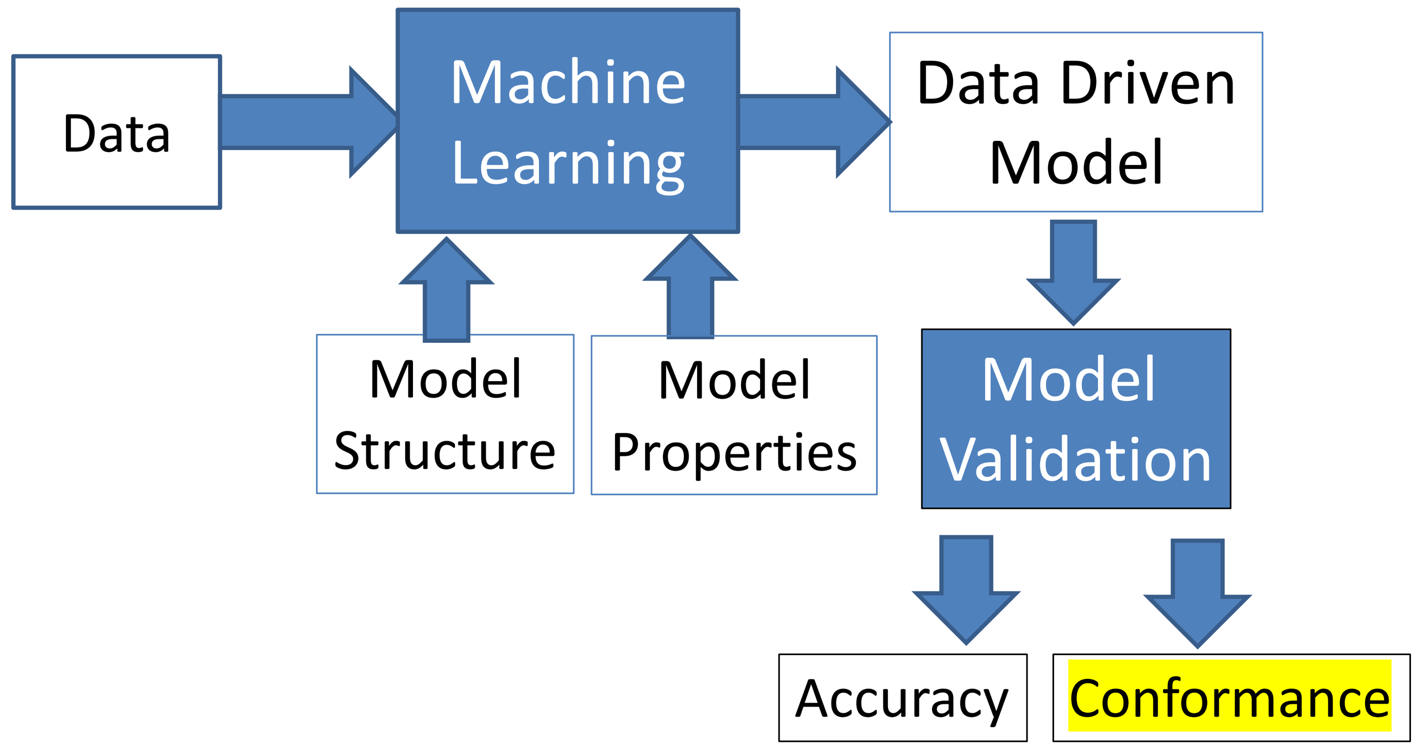
Learning and Verifying Conformant Data-Driven Models for Cyber-Physical Systems.

University of Colorado Boulder
Arizona State University
Sriram Sankaranarayanan (PI), Christoffer Heckman, Georgios Fainekos and Heni Ben-Amor
University of Colorado, Boulder, CO and Arizona State University, Tempe, AZ.

CPS 1932189
CPS 1932068

Abstract

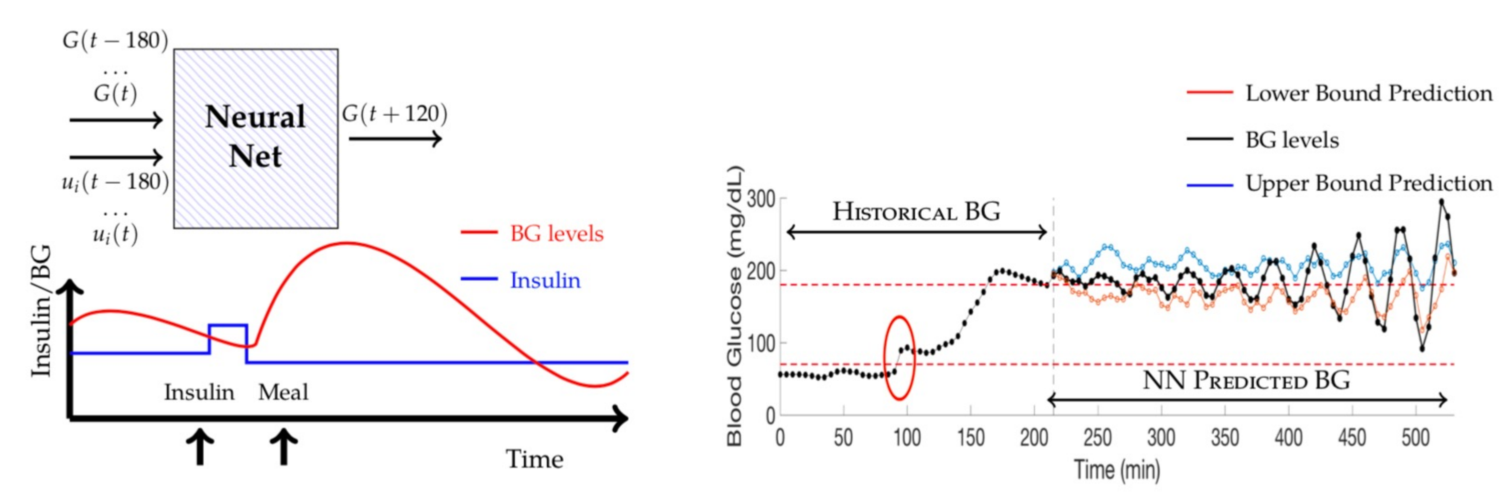
This project investigates fundamental techniques for building mathematical models that can be safely used to make trustworthy predictions and control decisions. Mathematical models form the foundation for modern Cyber-Physical Systems (CPS). Examples include vehicle models that predict how a car will move when brakes are applied, or physiological models that predict how the blood glucose levels change in a patient with type-1 diabetes when insulin is administered. The success of machine learning tools has yielded data-driven models such as neural networks. However, depending on how data is collected, and the models are learned, it is possible to obtain models that violate fundamental physical, chemical, or physiological facts that can potentially threaten life and property. The approach of the project is to expose these model flaws through advanced analysis. The project seeks to broaden participation in computing through mentoring activities that will encourage undergraduate women and members of underrepresented minority groups to consider a career in research.



Conformance: Does the model satisfy scientific facts?

- Conservation of energy, mass, momentum, charge,..
- Interrelationships between input and outputs.
- Safety/Liveness properties satisfied by the model.

Conformant Models for Type-1 Diabetes

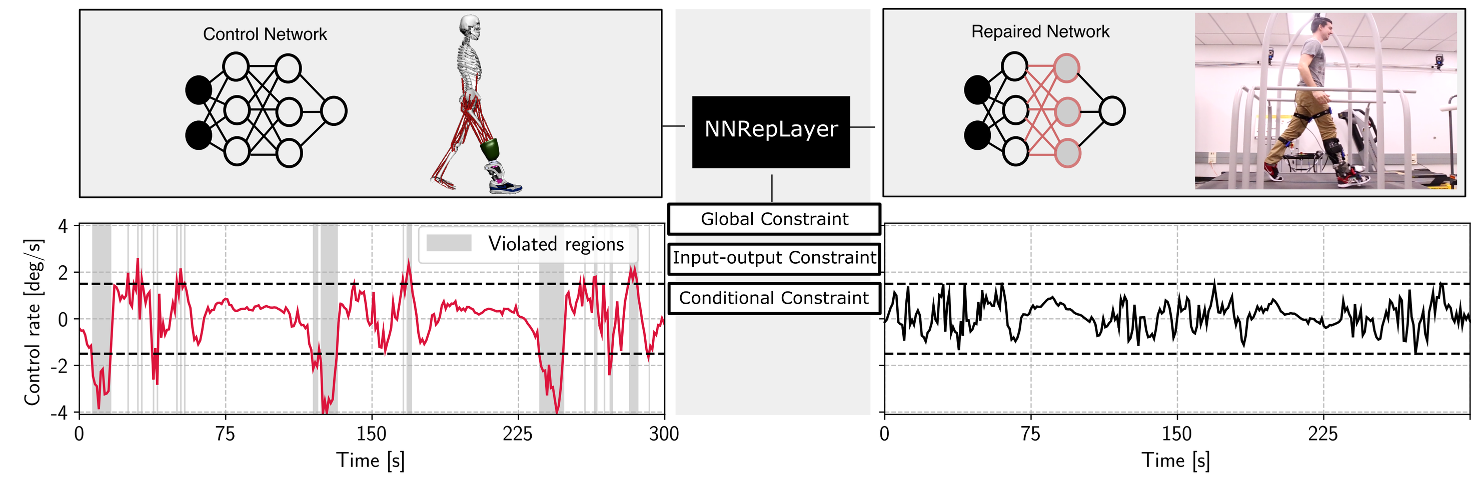


Failure of conformance in Insulin Glucose Regulation Neural Network Model

Goal: Accurate models to predict blood glucose levels from data. We discovered that models learned from clinical trials are dangerously flawed.
Use in artificial pancreas can have deadly result for patients.

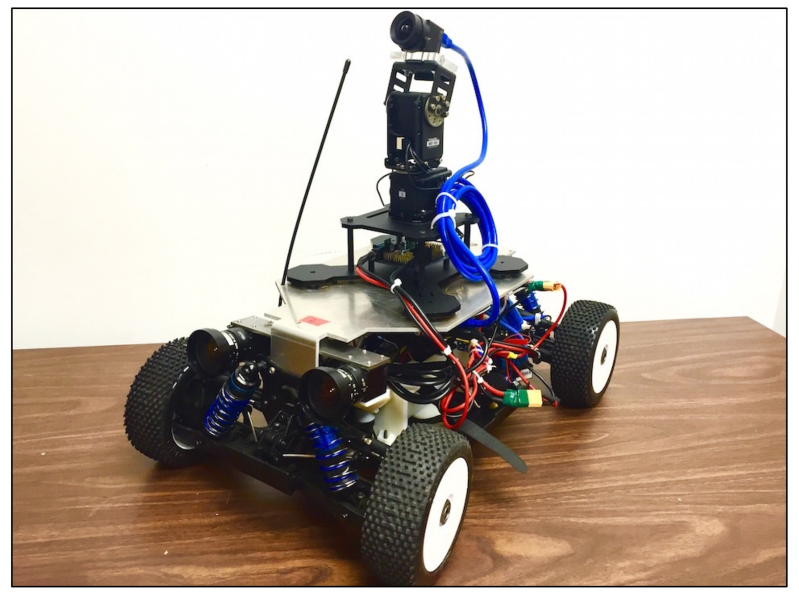
Neural Network Repair (NNRepLayer)

Given neural network with safety violations, modify weights to satisfy the property.



Control inputs before and after repair.

Path Following: Parkour Car



Goal: Construct guaranteed path following algorithm using neural control Lyapunov functions learned from a simple dynamical model of the car.

- Learn a neural network + associated control Lyapunov fn.
- CLF defines a set of possible control inputs.
- Bounds on curvature of trajectories that can be followed.
- Test on actual vehicle platform.

Algorithmic Foundations for Hybrid SysID

Goal: Learning linear hybrid dynamics from full state observations with noise given number of discrete modes. **(**NP-hard problem).
Contribution: Algorithm that is linear time in the number of data points but exponential in the number of dimensions.
Ideas from non-smooth optimization for complexity improvements.

Contact

Sriram Sankaranarayanan
University of Colorado Boulder
Email: srirams@Colorado.edu
Website: http://www.cs.colorado.edu/~srirams

References

1. Narasimhamurthy, Kushner, Dutta and Sankaranarayanan, Verifying Conformance of Neural Network Models, ICCAD 2019.
2. Kushner, Sankaranarayanan and Breton, Conformance verification for neural network models of glucose-insulin dynamics HSCC 2020.
3. Yaghoubi and Fainekos, Worst-case satisfaction of STL specifications using feedforward neural network controllers: a Lagrange multipliers approach, ACM Trans. on Embedded Comp. Sys. (TECS) 18 (5s), 107
4. Berger et al, An algorithm for learning switched linear systems from data, NeurIPS 2022 (to appear) .
5. Majid et al, Safe robot learning for assistive devices through neural network repair, Conference on Robot Learning (CoRL) 2022 (to appear).
6. Reed et al, Verified path following using neural control Lyapunov functions, CoRL 2022 (to appear)