# Avaljot Singh

Department of Computer Science
University of Illinois, Urbana-Champaign

singhasavaljot@gmail.com
avaljot2@illinois.edu

## Research Interest

My current research is focused on making Neural Networks trustworthy by making it easy to verify properties like robustness using formal methods. We are currently building ConstraintFlow, a DSL for defining Neural Network analysis algorithms.

## Education

**University of Illinois, Urbana-Champaign** [*PhD*] *2022 - Present*
Advisors: Prof. Gagandeep Singh, Prof. Charith Mendis

**Indian Institute of Technology, Delhi** [*B.Tech + M.Tech*] *2016 - 2021*
Advisor: Prof. Sanjiva Prasad

## Publications

**Interpreting Robustness Proofs of Deep Neural Networks** *ICLR, 2023*
Debangshu Banerjee, Avaljot Singh, Gagandeep Singh ***In submission***

**ConstraintFlow: A Declarative DSL for Certified Artificial Intelligence** *SRC @ PLDI, 2023*
Avaljot Singh ***Bronze medal***

**Interpreting Robustness Proofs of Deep Neural Networks** *WFVML @ ICML, 2023*
Debangshu Banerjee, Avaljot Singh, Gagandeep Singh ***Outstanding paper***

## Research Experience

- **M4L: Mixed-mode MPC for Machine Learning** *March, 2021 - June, 2021*
  *Rahul Sharma* *MSR Bangalore*
  - Designed DSL and a type system for **Mixed-mode MPC**
  - Proved the **formal guarantees** of correctness and cryptographic security for well-typed programs.
- **Algebraic techniques for network routing** [M.Tech Thesis] *January 2020 - December 2020*
  *Prof. Sanjiva Prasad* *IIT Delhi*
  - Conservatively extended NetKAT to **Cost-InterNetKAT** involving three distinct innovations
  - Introduced inter-layer routing and cost algebra, thus allowing composition of cost-dependent NetKAT policies
  - Designed Cost-InterNetKAT **homomorphisms, refinements, absrtractions and translations**
- **Synthesis and Unified Management of Hybrid Networks** *May, 2019 - July, 2019*
  *Prof. Nate Foster* *Cornell University*
  - Defined the syntax and semantics of **Edge-NetKAT**
  - Pushing the functionality of NetKAT programs to configurable edge devices.
- **Object Detection for Local Spotting using 2DOF Actuator** *June, 2018 - July, 2018*
  *Prof. Idaku Ishii* *Robotics Lab, Hiroshima University*
  - Implemented a facial recognition system mounted on **mechanical tracking system** for security cameras
  - Used **High speed Camera Interfacing** for real-time image synthesis and real-time tracking system

## Projects

**ContsraintFlow: A Declarative DSL for Certified Artificial Intelligence**

- Designing a DSL for DNN Verification and developing its type system and operational semantics
- Automatic verification for over-approximation-based soundness of the DNN certifier specified in ConstraintFlow

**Data Driven Approach for Loop termination**

- Designing ranking functions using trace data to prove the termination of loops
- Mutually Reinforcing Development of ranking functions and invariants using program synthesis

**Polynomial abstract domain for Neural Network Verification**

- Designing a novel abstract domain and abstract transformers using polynomials
- Enriching the domain of robustness properties for DNN verification tasks

## Teaching Assistant

**Analysis and Design of Algorithms** *Spring 2021*
Prof. Naveen Garg *IIT Delhi*

**Introduction to Functional Programming** *Fall 2020*
Prof. Sanjiva Prasad *IIT Delhi*

**Programming Languages** *Spring 2020*
Prof. Sanjiva Prasad *IIT Delhi*

**Introduction to Computer Science** *Fall 2019*
Prof. Prem Kalra *IIT Delhi*