

FMfI2023 Program

Name	Ichiro Hasuo
Affiliation	National Institute of Informatics
Title	Proving Safety of Automated Driving Vehicles
Abstract	<p>I will introduce our recent work on using mathematical logic to rigorously prove the safety of automated driving vehicles. The main challenge in such formal verification attempts for real-world systems is the absence of target system models. We follow the methodology called RSS (responsibility-sensitive safety, Shalev-Shwartz et al., 2017) that tells what to model (and what not to model) in a both technically and socially sensible way. Our logical formalization and extension of RSS allows us to handle complex driving scenarios in a compositional manner. Overall, the work suggests the potential of mathematical logic as a social infrastructure for establishing trust in novel ICT.</p>