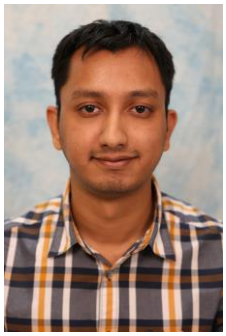
Carnegie Mellon University
Computer Science Department

THESIS ORAL



Ankush Das

Resource-Aware Session Types for Digital Contracts

Thursday, April 22, 2021 – 10:30 a.m. – REMOTE

Programming distributed systems is already challenging due to the presence of data races and deadlocks; bugs are difficult to detect and reproduce when they only arise in certain thread interleavings. With the pervasive usage of distributed systems in software design, there is an urgent need for formal tools for qualitative and quantitative analysis of distributed software.

In response, this thesis designs novel resource-aware session types that serve as a sound and practical foundation for distributed systems with strong type-theoretic guarantees. Session types statically enforce bidirectional communication protocols for message-passing processes. However, in their current form, they cannot express quantitative properties such as energy consumption, latency, and throughput of a system. This thesis addresses this limitation by proposing two extensions to express the work and span of parallel computation. To compute work, the key innovation is that messages and processes carry an abstract notion of potential which is consumed to perform work. To compute span, the key innovation is to introduce operators from temporal logic to capture the timing of message exchanges. Underlying both these systems are novel refinement session types that capture data structure sizes and values which are central to expressing cost bounds.

The thesis concludes with an application of resource-aware session types to the blockchain domain. Blockchains allow execution of complex protocols between mutually distrusting parties through smart contracts. Programming smart contracts comes with unique challenges such as enforcing transaction protocols, computing the execution cost of transactions, and ensuring that assets are not accidentally duplicated or discarded accidentally. This thesis presents Nomos: a smart contract language with resource-aware session types at its core. Session types statically express contract protocols. Resource-aware types automatically infer the execution cost of transactions leveraging ideas from automatic amortized resource analysis. The linear fragment of session types tracks assets, preventing their accidental duplication or deletion. To simplify programming, Nomos is enhanced with blockchain-specific constructs, surface syntax to easily access standard data structures, and constructive type checking error messages. Finally, the thesis evaluates Nomos on a variety of standard smart contracts highlighting the verified properties and efficiency of type checking and cost inference.

Thesis Committee:
Jan Hoffmann, Chair
Frank Pfenning
Bryan Parno
Andrew Miller, UIUC
Shaz Qadeer, Facebook