Research Plan 2017-2021*

Sasha Rubin

Research Background. My background is in theoretical foundations of Formal Methods (FM), a branch of theoretical computer science that supplies mathematical foundations for the analysis of systems with a digital component. The complexity of such systems arises from the interaction of concurrency, non-determinism, embedded components, distributed components, real-time demands, etc. Typical modern systems display some or all of these: multi-core processes, cloud computing, autonomous agents, etc. While classic FM models systems as finite-state systems, my work has focused on infinite-state systems. This obviously vastly increases the class of systems one model, and unavoidably limits the properties that one can reason about.

The three cornerstones of FM are modeling, verification and synthesis, and I have contributed to all of these.

Specifically, I have worked on the following mathematical models of computation: Markov chains [30], timed systems [11], Petri nets [12], automatic structures [23-36]; the following models of communication in Multi-agent Systems (MAS): token-passing [6,13,16], broadcast and asynchronous rendezvous [11,12,13]; and on mobile MAS [3,10,14,15].

To reason about systems, properties about need to be expressed formally, and this is typically done using logics. I have broad expertise in classical logics (first-order, second-order), modal logics (temporal, strategic, epistemic, dynamic), as well as quantitative extensions of these, i.e., by counting and aggregation [1,2,5,9,18,24,25], that can be used to express non-functional properties, e.g., about resource consumption.

In my work I have used and developed techniques in mathematical logic, automata theory, game theory and graph theory.

Projected Research Activities. My research trajectory has been shifting from the investigation of logical and computational properties of abstract mathematical objects [18-36] towards more concrete systems [1-17], including recent contributions in AI and MAS venues [2,3,4,8,10,14,15]. I expect this trend to continue. That said, my current interest is in rigorous mathematical foundations rather than simulation and heuristic techniques.

I project two main research activities for the next 5 years, one normal and one speculative[1]

WHAT IS THE NEED THAT MY PROGRAM IS ADDRESSING?

- "what is synthesis"
- "strategic reasoning that works"

*All numbered citations, e.g., [3], are listed in the CV.

[1]I use "normal" in a similar sense to Kuhn's "normal science", i.e., research that is acknowledged, for a time, as supplying the foundation for its further practice.

1. I intend to investigate normal and speculative questions in FM, with a focus on key classes of infinite-state systems. Namely:
   (a) foundational issues (modeling, verification, synthesis) in formal methods for parameterised systems and networks.
   (b) more speculative questions such as "What is synthesis and how should it be formalised?" (an active topic of debate, and work in progress with Giuseppe De Giacomo).

2. A second goal, building on the first, and arguably more important, is that I intend contribute to building bridges (technical and social) between Formal Methods (FM) and both Multi-agent Systems (MAS) and Artificial Intelligence (AI).

   There is a non-trivial overlap between these fields, both on the level of problems and gross techniques. For instance, "synthesis" in FM is called "planning" or "supervisory control" in AI; many influential languages for modeling and reasoning in all three fields are explicitly based on mathematical logic (e.g., situation calculus, alternating-time temporal logic).

   I have recently contributed a number of works that import and adapt methodologies and techniques from FM to MAS/AI [2,3,4,8,10,14,15]. I stress that besides novel technical content, my key contributions were to identify which models and techniques from FM, amongst many possibilities, are suitable for MAS/AI.

   As my recent research visits indicate (see CV), I am currently working to bridge communities, not just technical fields. In particular, I have a number of ongoing collaborations that bring logical foundations to bear on a broad variety of issues and problems in MAS and AI, including strategic reasoning for data-aware systems, automatic decomposition of business processes into human-understandable representations, and foundations of synthesis (including synthesis under assumptions, rational synthesis, strategic-epistemic logics).

   High rewards typically come with high risks, and this second goal is no exception. There are principled differences between these communities that should be carefully understood in order to build bridges between them. For instance, Knowledge Representation (a central field in AI) is under-represented in the theoretical side of the FM community. In time, as I further integrate in the MAS/AI community, I will develop the insight and experience to isolate and expand the *appropriate* connections between these communities.

Integration in WASP. My scientific work cuts across a number of WASP's thematic dimensions, notably:

1. Software for Engineering Design, Synthesis, and Autonomous Systems.
2. Model-Based Systems Engineering.

I forsee my second goal, i.e., bridging FM with MAS/AI, as my main contribution to WASP.

I will collaborate with PhD students interested in my research area. Exciting PhD topics include parameterised synthesis (known as "generalised planning"

in AI), rational synthesis (a topic at the intersection of game-theory and FM), foundations and applications of quantitative specification languages, and connections between automata theory and classical subfields of AI such as argumentation theory.

I have built a large network of collaborators, and have connections with a number of groups, including those in Naples, Rome, Imperial, Oxford, Paris, Graz, Vienna, and Singapore.

——— strategically motivated basic research,

THEMATIC = scientific challenges - Software for Engineering Design, Synthesis, and Autonomous Systems (FM) - Model-Based Systems Engineering (FM) - Collaboration and Interaction (KRR) - Networked and Distributed Systems (FTDA, Cyberphysical systems, TPS)

——— Surveying the current WASP projects, I find the following connections:

1. Software Engineering for Smart Systems project. One of the visions is to have "Families of similar systems will learn from each other automatically". However,

Surveying the current WASP researchers, I find the following close connections.

1. Bengt Lennartsson's work on supervisory control has connections my work on synthesis, automata-theory, and formalisms related to petri-nets. Also, his work on human-comprehensible synthesis is in line with one of the topics of my recent research visit to Marco Montali and Diego Calvanese (see CV).

Bosch: CONEX: KRR for large multi-agent systems The importance of stressing the components and their connectors of a software system is generally recognized and has led to better control over the design, development, and evolution of large and increasingly dynamic software systems

———-

Lennartson: EFAs, SCT, PN CONEX: synthesis, planning, BPM

A problem that is typically encountered in industrial applications is that the resulting supervisor is not easily comprehensible for the users.

First, modeling such huge systems with explicit state-transition models typically results in an intractable mode

The second problem concerns the ease to understand and implement the supervisor.

We propose general Petri net building blocks for the construction of recipes.

Hierarchical supervisory control for batch processes

———-

Sands: Information Flow in Security (interference, leaking), DYNAMIC systems, Fault-tolerance, unreliable systems CONEX: KALT*, DEL, FTDA

The static verification of secure information flow has been a popular theme in recent programming language research, but information flow policies considered are based on multilevel security which presents a static view of security levels

This work is about specifying and ensuring security in unreliable systems

The particular security characterization we study is ¡i¿non-interference¡/i¿, an information-flow security property which says that public outputs of a program (the ¡i¿low¡/i¿ security channel) do not reveal anything about its secrets (the ¡i¿high¡/i¿ security inputs).

it makes its assumptions precise and provides formal guarantees.

Pellicionne: KRR for specifying properties

CNEX: TL, graded TL for quantitative properties.

Today, property specification patterns provide general rules that help practitioners to qualify order and occurrence, to quantify time bounds, and to express probabilities of events. Nevertheless, a comprehensive framework combining qualitative, real-time, and probabilistic property specification patterns has remained elusive

---

Heintz: stream-based knowledge processing, autonomous, DYKNOW?? CONEX: time, knowledge

Engineering autonomous agents that display rational and goal-directed behavior in dynamic physical environments requires a steady flow of information from sensors to high-level reasoning components. The gap between sensing and reasoning... DyKnow is also used to generate event streams representing for example changes in qualitative spatial relations, which are used to detect traffic violations expressed as declarative chronicles.

———- Kragic: CONEX: verifications of sensor models; epistemic logics;

Perception is the basis of any interactive autonomous systems.