Research Statement

Overview

My work takes inspiration from formal epistemology to solve problems within various domains of theoretical computer science, e.g. distributed consensus, game theory, and cryptography. Formal epistemology attempts to resolve epistemological issues having to do with knowledge, belief, and uncertainty by use of formal methods. In doing so, the field is able to shed light not only on long standing philosophical problems but also the very formal methods it uses to examine these problems in the first place. Below, I discuss my ongoing projects and show how formal epistemology has helped me make concrete progress in each of them. Higher level summaries as well as posters and presentations can be found at my `website`.

Ongoing Projects

Topological Semantics for Common Inductive Knowledge: Suppose we have a group of agents who are deciding to report whether a proposition P is true or defer judgement. Further imagine that agents possibly receive distinct streams of information and have different tolerances for how many times they are willing to change their mind between saying 'Yes' and deferring judgement on P. What joint learning strategies are available to agents if they want to guarantee they will all eventually converge to the same answer and further that their answers will be correct in the limit? One might hope to find some notion of 'common knowledge' to characterize the solutions to this inductive version of the coordinated attack problem in the same vein as `Halpern and Moses`. Separately, `Kevin Kelly` has been developing an epistemic logic based on reliabilist theories of knowledge which admits an elegant topological semantics. By extending Kelly's approach to the multiagent setting, we formulate a novel notion of common inductive knowledge which turns out to perfectly characterize the joint strategies which solve our consensus problem. Future work will involve creating a sound and complete proof system to accompany our semantics.

Eliciting Causal Bayesian Networks with Scoring Rules: How might we elicit an agent's beliefs about the causal Bayesian network governing a set of variables? Broadly speaking, if the designer creates a set of possible interventions rich enough to identify the agent's entire causal Bayesian network and randomizes uniformly over which intervention will be performed, they can ex-ante present the agent a set of conditional scoring rules (each of which pays out in case a given intervention is performed) to elicit their entire causal Bayesian network. However, if agents have costs to processing the information gained from each intervention, the designer's infimum worst case loss to attain incentive compatibility will be an increasing function of how many interventions they are randomizing over. `Peter Spirtes et al.` have used causal faithfulness assumptions (which can be justified by Humean 'no miracles' arguments) to design algorithms which drastically reduce the number of interventions necessary to identify a causal Bayesian network. Using similar causal faithfulness assumptions, we propose two alternative mechanisms with improved worst case losses. The latter assumes agents are myopic and needs further non-myopic analysis.

Resource Bounded Randomness for Instantiating Cryptographic Security: `Tadaki and Doi` show Martin-Löf random sequences, often taken to represent exactly those sequences which are 'epistemically random' in Cantor space, can serve to safely instantiate any signature scheme proven secure in the random oracle model. While this result is interesting, it is of little practical concern. In addition to being deterministic, all hash functions in practice must also be computable. Martin-Löf random sequences, while deterministic, are not computable. So far, it is an open conjecture whether all signature schemes proven secure in the random oracle model can be safely instantiated by a computable hash function. I have recently shown that another algorithmic randomness notion, called primitive recursive Schnorr randomness, also suffices to safely instantiate any signature scheme proven secure in the random oracle model. Since there are computable sequences which are primitive recursive Schnorr random, this settles the conjecture. I now conjecture that polynomial space randomness will also suffice and plan to establish time complexity bounds on the simplest hashes which can safely instantiate cryptographic security.

Siddharth Namachivayam
✉ *snamachi@andrew.cmu* • 🌐 *snamachi.github.io*