Fully-funded PhD position on formal verification of distributed systems

A PhD position is open at the **University of Groningen**, NL, aimed at applicants interested in working at the intersection between formal verification and distributed systems. The position is embedded in the **Fundamental Computing group** of the Bernoulli Institute for Math, CS and AI, and is funded for 4 years under the employment terms of the Collective Labour Agreement for Dutch Universities.

Background

Formal verification aims at providing strong guarantees about the behaviour of programs and systems. It relies on logic to precisely describe the program or system in question and check desired properties, with both academia and industry recognising the need for formal verification, e.g., formal verification is used extensively at Amazon Web Services [1].

Distribution has become an integral part of a large number of computer systems, providing them with essential improvements to aspects such as performance and fault-tolerance. Due to the critical nature of many distributed systems, their correctness is of crucial importance. The verification of distributed systems is, however, notoriously difficult, due to the numerous interleavings of steps inherent to distributed algorithms.

Research directions

The formal verification of distributed systems can be approached at different levels of abstraction, and can be tailored to classes of systems with different specificities. The PhD research is envisioned to broadly follow one of three directions, but can be adapted to suit the interests of an excellent applicant.

The use of **formal languages** to specify and reason about distributed systems has been an object of intensive research over the last decades. While verification support for these languages does exist, it is limited in either the guarantees it can provide or in its level of automation. Lifting this limitation is a clear goal, with a potential target language being TLA+. In light of recent advances on (bounded) symbolic model checking for TLA+ [2], the idea is to pursue unbounded model checking via first-order logic reasoning.

The advent of **smart contracts**, which are programs deployed on blockchain platforms, promises to significantly change how financial assets are held and manipulated. Due to their evergrowing use, they are likely targets of attacks, with unintended behaviours regularly being exploited to affect assets estimated in millions of US Dollars. Ensuring that deployed contracts cannot be exploited is critical. Following on a promising result w.r.t. the verification of contracts written in Solidity [3], the idea is to pursue an approach that is general and thus independent of specific implementation languages.

While our current digital infrastructure relies on classical networks, **quantum networks** are slowly becoming a reality. Their use can both improve existing applications and allow for fundamentally new ones to arise. The coordination algorithms that govern their operation are quite complex and unlike those employed in classical networks, necessitating novel verification approaches. Since quantum networks is a nascent technology, the formalisation of its behaviour is ongoing [4], the idea is thus to design an automated reasoning approach in tandem with formalisation efforts, with a focus on probabilistic behaviours.

Candidate profile

Applicants are expected to have an interest in both **theory and practice** as well as:

- Have (or be close to completing) an MSc in computer science or a related field.
- Preferably have experience in (some of) the topics below (not a strict requirement).
  - Model checking and automata theory.
  - SAT, SMT, and CHC solving.
  - Temporal logic and TLA+.
  - Distributed algorithms, blockchains, and smart contracts.
  - Quantum information theory and Markov decision processes.
- Have strong programming skills and interest in developing state-of-the-art tools.
- Have excellent communication skills in English (both oral and written).

How to apply

The successful applicant will be advised by **Rodrigo Otoni**. Applications should include a CV, reference letter(s), and a short motivation letter, and should be sent via e-mail to r.b.otoni@rug.nl; informal queries about the position can be sent to the same address.

Applications will be reviewed until the position is filled. The selected applicant is expected to start in November 2025 (or soon thereafter); some flexibility is possible, if needed.

References

[1] C. Newcombe et al.. *How Amazon Web Services uses Formal Methods*. Communications of the ACM, 58(4), pp. 66–73 (2015). DOI: https://doi.org/10.1145/2699417
[2] R. Otoni et al.. *Symbolic Model Checking for TLA+ Made Faster*. 29th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, pp. 126–144 (2023). DOI: https://doi.org/10.1007/978-3-031-30823-9_7
[3] R. Otoni et al.. *A Solicitous Approach to Smart Contract Verification*. ACM Transactions on Privacy and Security, 26(2), pp. 1-28 (2023). DOI: https://doi.org/10.1145/3564699
[4] A. Buckley et al.. *An Algebraic Language for Specifying Quantum Networks*. Proceedings of the ACM on Programming Languages, 8(PLDI), pp. 1313-1335 (2024). DOI: https://doi.org/10.1145/3656430