Verification of Blocking Analyses for Multicore Real-Time Systems

Topic:	Verification of real-time scheduling and synchronization theory with the *Coq* proof assistant
Location:	Max Planck Institute for Software Systems (MPI-SWS, https://www.mpi-sws.org) Kaiserslautern, Germany — *Only about 2 hours by TGV to Paris!*
Language:	English
Duration:	6 Months (flexible)
Compensation:	MPI-SWS provides **free accommodation** and a **monthly stipend** of about 950 EUR to cover living expenses.
Team:	Real-Time Systems Group, PROSA team (http://prosa.mpi-sws.org)
Advisor:	Björn Brandenburg (https://people.mpi-sws.org/~bbb)

Project Context

Real-time systems are computing systems that must react to external stimuli within stringent *response-time bounds* and can be found at the heart of many safety-critical systems (e.g., think airbags, anti-lock brakes, collision avoidance systems, etc.).

To ensure the safety of such systems, *schedulability analysis* (i.e., real-time scheduling theory) is used to assess and validate their timing correctness *a priori* (i.e., before deployment, it is checked that all deadlines will always be met). However, such schedulability analyses can be quite complicated and rely on non-obvious reasoning — so how do we even know that the analyses used to validate the safety of real-time systems are themselves correct?

The PROSA project is a systematic and large-scale effort to create **a trustworthy foundation for provably sound schedulability analyses**, using the *Coq* proof assistant. A key characteristic of PROSA is that we *prioritize readability* over all other concerns to ensure that specifications remain accessible to readers without a background in formal proofs.

Project Objective

Virtually all multicore real-time systems require some form of *synchronization primitive* to ensure mutually exclusive access to shared resources (e.g., data structures in shared memory, I/O ports, etc.).

The most simple and most widely used synchronization primitive for multicore systems is a *spin lock*, where tasks that wait to gain access to locked resources busy-wait by executing a delay loop that wastes cycles (i.e., something like `while (!try_to_lock()) { /* do nothing */ }`).

Of course, such spinning causes extra delays that can be dangerous in real-time systems. Therefore, a subfield of real-time scheduling theory called *blocking analysis* has developed methods for statically bounding the worst-case delays due to lock contention. However, such blocking analysis is both tedious and error-prone, and thus a prime candidate for formal proof.

The objective of this project is **the first mechanization and verification of a state-of-the-art blocking analysis** (based on mixed-integer linear programming) for spin locks using the Coq proof assistant and the PROSA framework.

Prerequisites

- A taste for formal reasoning — if you like playing with *Coq* and want to apply it to real problems, this project is for you.
- Some experience with *Coq* or other proof assistants (basic knowledge is sufficient, although more advanced knowledge is very welcome).
- Prior knowledge of real-time systems and real-time scheduling theory is **not** required.
- Proficiency in English. (Proficiency in German **not** required; the institute language is English.)

Follow-Up and Collaboration Opportunities

- The work carried out as part of the internship is expected to directly contribute to a paper submission to a top real-time conference.
- MPI-SWS offers a world-class graduate program. We are actively looking for talented PhD students.
- This internship provides an excellent opportunity to get to know MPI-SWS and its lively and friendly academic community.
- The PROSA effort is supported by the German-French joint project *RT-Proofs* (funded by ANR and DFG, 2018–2021). Close collaboration with groups at INRIA Grenoble – Rhône-Alpes, Verimag (Grenoble), ONERA (Toulouse), and TU Braunschweig (Germany) are expected. There exist several open PhD and post-doc positions in the project in both Germany and France.

References

- F. Cerqueira, F. Stutz, and B. Brandenburg, “PROSA: A Case for Readable Mechanized Schedulability Analysis”, *Proc. 28th Euromicro Conference on Real-Time Systems* (ECRTS 2016), pp. 273–284, July 2016. *Best Paper Award.*
- A. Wieder and B. Brandenburg, “On Spin Locks in AUTOSAR: Blocking Analysis of FIFO, Unordered, and Priority-Ordered Spin Locks”, *Proc. 34th IEEE Real-Time Systems Symposium* (RTSS 2013), pp. 45–56, December 2013.

Any Questions?

Please feel free to contact Björn Brandenburg (bbb@mpi-sws.org)!