Abstract Response-Time Analysis: A Formal Foundation for the Busy-Window Principle (Artifact)

Sergey Bozhko
Max Planck Institute for Software Systems (MPI-SWS)
sbozhko@mpi-sws.org

Björn B. Brandenburg
Max Planck Institute for Software Systems (MPI-SWS)
bbb@mpi-sws.org

Abstract

This artifact provides the means to validate and reproduce the results of the associated paper "Abstract Response-Time Analysis: A Formal Foundation for the Busy-Window Principle". In this artifact we demonstrate how to compile the source code and automatically check the proofs of each theorem. We also provide references to all key results claimed to be proven in the paper (including Abstract RTA and all eight instantiations), so that readers may confirm that no proofs have been omitted.

2012 ACM Subject Classification Computer systems organization → Real-time systems; Software and its engineering → Scheduling; Theory of computation → Scheduling algorithms

Keywords and phrases hard real-time systems, response-time analysis, uniprocessor, busy window, fixed priority, EDF, verification, Coq, Prosa, preemptive, non-preemptive, limited-preemptive

Digital Object Identifier 10.4230/DARTS.6.1.3

Related Article Sergey Bozhko and Björn B. Brandenburg, "Abstract Response-Time Analysis: A Formal Foundation for the Busy-Window Principle", in 32nd Euromicro Conference on Real-Time Systems (ECRTS 2020), LIPIcs, Vol. 165, pp. 22:1–22:24, 2020.
`https://doi.org/10.4230/LIPIcs.ECRTS.2020.22`

Related Conference 32nd Euromicro Conference on Real-Time Systems (ECRTS 2020), July 7–10, 2020, Virtual Conference

1 Scope

All definitions and proofs in the associated paper have been mechanized and verified with the Coq proof assistant. The artifact provides the source code of the Coq development and references to the important results claimed to be proven in the paper. Namely, the artifact contains the code showing the correctness of the central result of the associated paper:

- Abstract RTA theorem (Theorem 18);[1]
- The refinement model with sequential tasks – sequential abstract RTA theorem (Theorem 27);
- Instantiations of the analysis to general FP and EDF models (Theorems 31 and 32); and
- Instantiations of the analysis to eight response-time analyses for non-self-suspending sporadic tasks with arbitrary deadlines and arbitrary arrival curves under EDF, NP-EDF, LP-EDF, EDF-NPS, FP, NP-FP, LP-FP, and FP-NPS uniprocessor scheduling.

The artifact thereby supports our claim that the proposed analysis is correct.

[1] All references to sections, definitions, lemmas, and theorems refer to the related paper.

2 Content

The artifact package includes:

- `Abstract.html`: an overview providing installation instructions and links to all the result presented in the paper;
- `/html`: automatically generated hypertext specification of the Coq development; and
- `/specification`: the Coq files that realize the mechanization of the result presented in the paper.

Furthermore, each Coq file contains a generous number of explanatory comments that aid understanding of the presented content.

3 Getting the artifact

The artifact endorsed by the Artifact Evaluation Committee is available free of charge on the Dagstuhl Research Online Publication Server (DROPS). In addition, the artifact is also available at `https://people.mpi-sws.org/~sbozhko/ECRTS20/AbstractRTA.html`. Furthermore, Abstract RTA is included in the current version of Prosa: `http://prosa.mpi-sws.org/releases/v0.4`.

4 Tested platforms

The artifact was tested on a desktop computer using 64-bit macOS 10.15, 64-bit Ubuntu 19.10, and 64-bit Windows 10 Home Edition; it does not assume or require any particular hardware configuration. The artifact should work on any system that supports:

- Coq 8.10.2,
- Mathematical Components 1.9, and
- Python 3.7.

5 License

The artifact is freely available under the BSD 2-Clause License.

6 MD5 sum of the artifact

5f10805963fcb235c83f7a7f0be07a52

7 Size of the artifact

6.7 MB