Snooper: A Flexible Tracing Solution for Fast Simulation and Analysis in RISC-V

Santiago Monserrat Campanello, Julian Pavon, and Adrián Cristal
santiago.monserrat@bsc.es

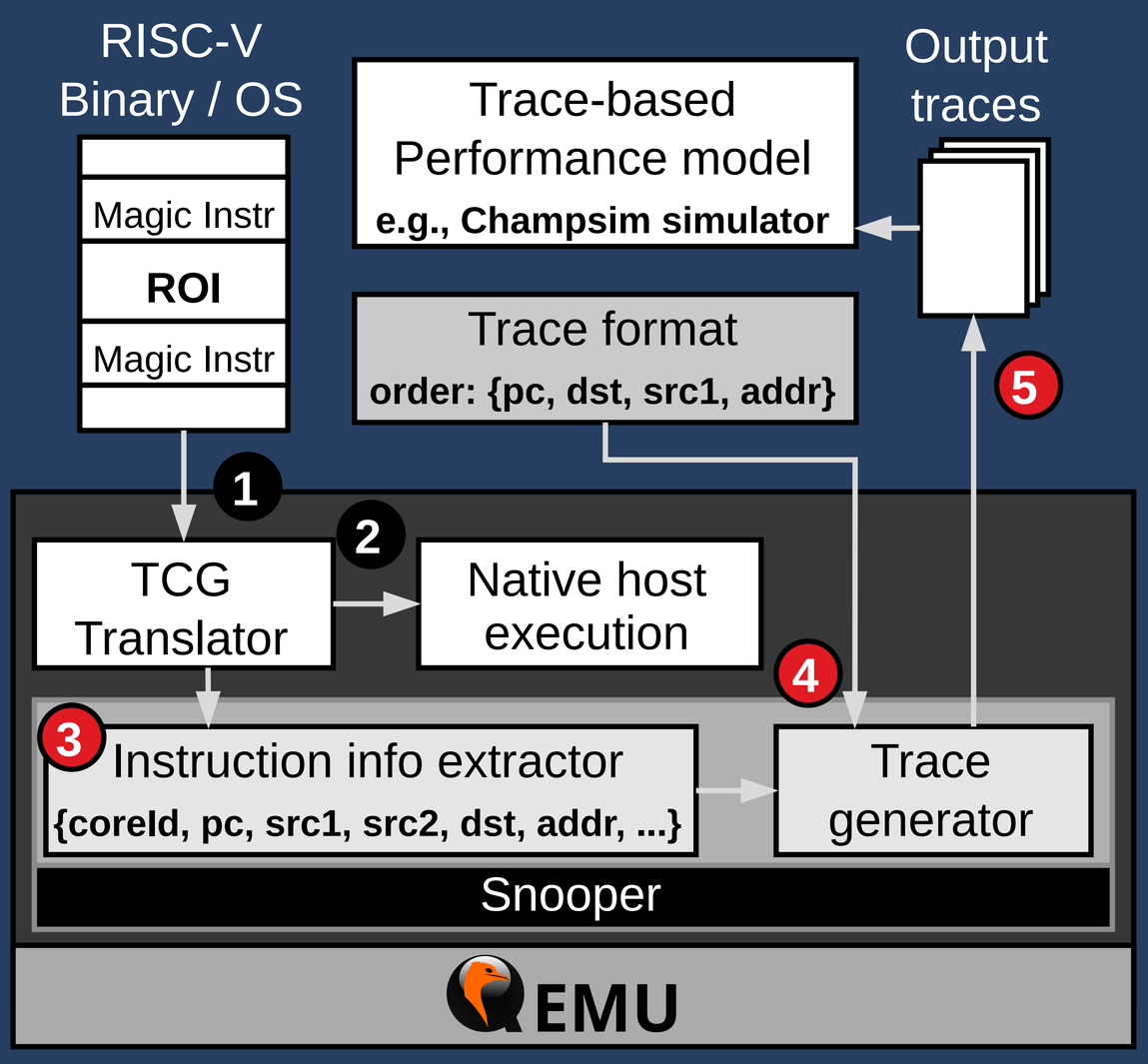
Driving RISC-V® Innovation for HPC

1. Background and motivation

Hardware simulation is essential for computer architecture research.
Trace-based simulators enable fast CPU and memory system modeling.
Existing trace-based simulators lack RISC-V ISA support.
Snooper fills this gap, providing a fast and flexible RISC-V tracing solution.

2. Design and Features

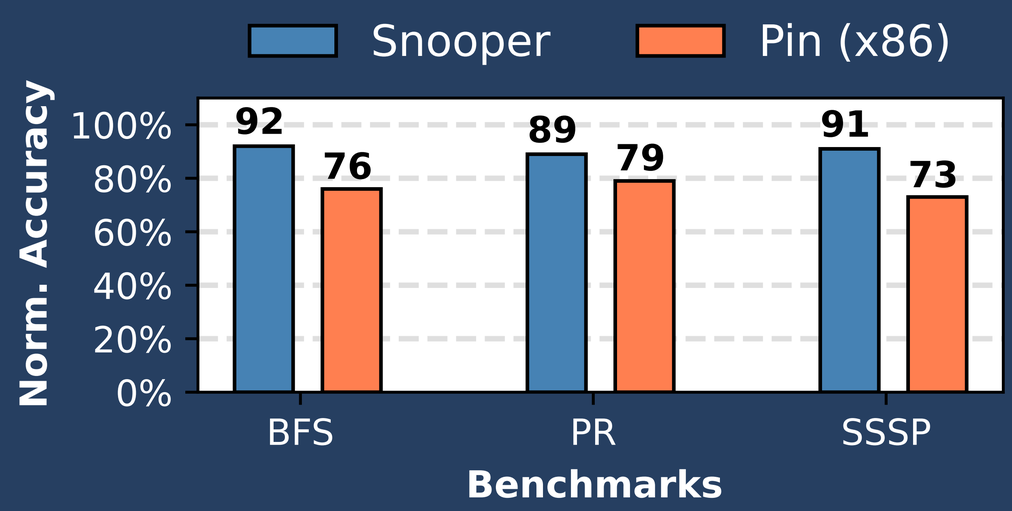
Implemented as a QEMU TCG plugin.
Leverages QEMU's dynamic binary translation.
Extracts metadata characteristics per instruction.
Generates customizable trace files.
Supports user-mode and full-system tracing.
Enables RISC-V OS evaluation.
Two trace generation modes: Plain binary and CSV.



1. QEMU loads executable either a user-mode program or an OS and supports magic instructions to define the Region of Interest (ROI)
2. QEMU translates to IR and executes the code
3. Snooper at the same time as 2 gets the information depending on 4
5. Snooper outputs trace, that then can be analyzed or used in trace-based simulators

3. Evaluation

To validate the accuracy of Snooper's traces, all experimental results are normalized to our in-house RTL SoC execution time (running on an FPGA).
We aim to highlight how existing traces, generated for other ISAs, are unsuitable for evaluating RISC-V performance due to differences in ISA design, compilation tools, and software stack maturity.
We compile the evaluated benchmarks for both RISC-V and x86, generate traces using Snooper and Pin respectively, and evaluate them under the same ChampSim configuration.



Snooper achieves 89% average accuracy.
On average, Pin-based traces perform 2.6 times higher error rates, underscoring the importance of RISC-V trace generation tools for accurate performance evaluation.
Snooper enables fast and accurate RISC-V architecture evaluation.

4. Discussion

Although Snooper generates RISC-V traces, the QEMU TCG plugin shares common data structures across all supported ISAs (e.g., x86 and ARM).
Snooper can be used with simpler analytical models to accelerate simulation time.

References

[1] Nathan Gober et al. The Championship Simulator: Architectural Simulation for Education and Competition. 2022. arXiv: 2210. 14324 [cs.AR]. url: https://arxiv.org/abs/2210.14324.
[2] Ayaz Akram and Lina Sawalha. "A Survey of Computer Architecture Simulation Techniques and Tools". In: IEEE Access 7 (2019), pp. 78120–78145. doi: 10.1109/ACCESS.2019.2917698.
[3] QEMU Project Developers. QEMU, TCG Emulation. https://www.qemu.org/docs/master/devel/index-tcg.html. [Online; accessed 23 Jan-2025]. 2025.
[4] Intel. Pin. http://pintool.intel.com/. [Online; accessed 25-Jan-2025]. 2025.
[5] Trevor E Carlson, Wim Heirman, and Lieven Eeckhout. "Sniper: Exploring the level of abstraction for scalable and accurate parallel multicore simulation". In: Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis. 2011.
[6] Scott Beamer, Krste Asanović, and David Patterson. "The GAP benchmark suite". In: arXiv preprint arXiv: 1508.03619 (2015).

Get more information at bzl.es

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia

Este proyecto está impulsado por el Ministerio para la Transformación Digital y de la Función Pública, en el marco del Fondo de Resiliencia y Recuperación -y la Unión Europea- NextGenerationEU.