Risotto: A Dynamic Binary Translator for Weak Memory Architectures

Redha Gouicem [1], Dennis Sprokholt [2], Jasper Ruehl [1], Rodrigo C. O. Rocha [3], Tom Spink [4], Soham Chakraborty [2], Pramod Bhatotia [1]

[1] TU Munich, [2] TU Delft, [3] University of Edinburgh, [4] University of St Andrews

Motivation

New emerging architectures challenge the x86 dominance

Adoption is starting in the industry:

- Apple Silicon
- Amazon Graviton
- Microsoft SQ Series, Volterra

Porting legacy x86 software is not always possible:

- Source code unavailable
- x86-specific assembly code

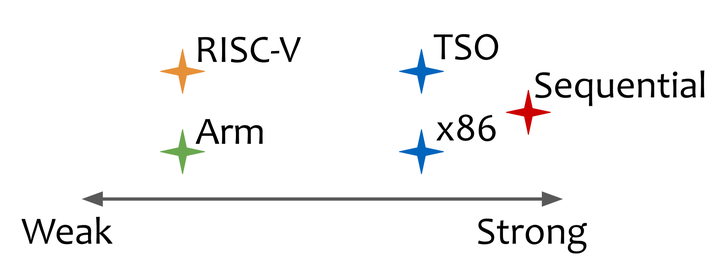
We can execute these legacy applications on new hardware using binary translation!

Problem

Architectures have different **memory models**:

CPUs may reorder memory operations in a different way

The weaker the model, the more reorderings happen



When translating from **strong to weak** models, new behaviors can appear:

```
                X = Y = 0
(thread 1)   X = 1  |  if (Y == 1)
             Y = 1  |      assert(X == 1)   (thread 2)
```

On x86, assert always succeeds

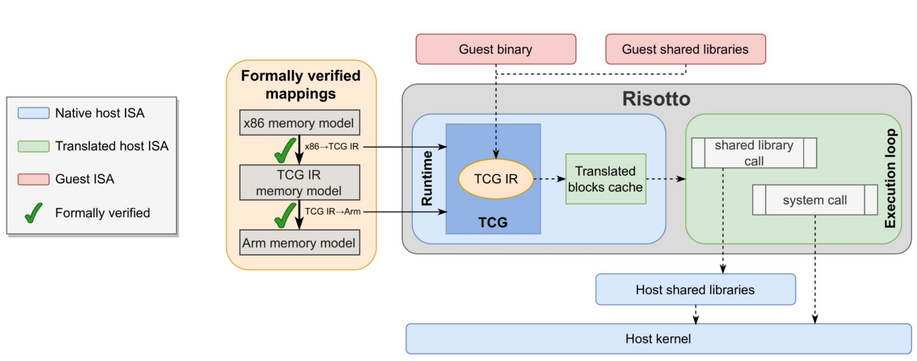
On Arm, assert can fail if *thread 1*'s instructions are re-ordered

The source memory model must be enforced on the target architecture for correct execution

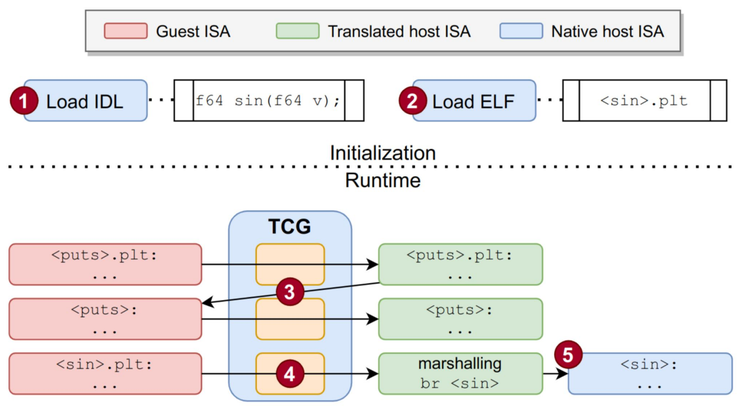
Approach

We design a **dynamic binary translator** based on QEMU, with a focus on *correctness* and *performance*:

Risotto



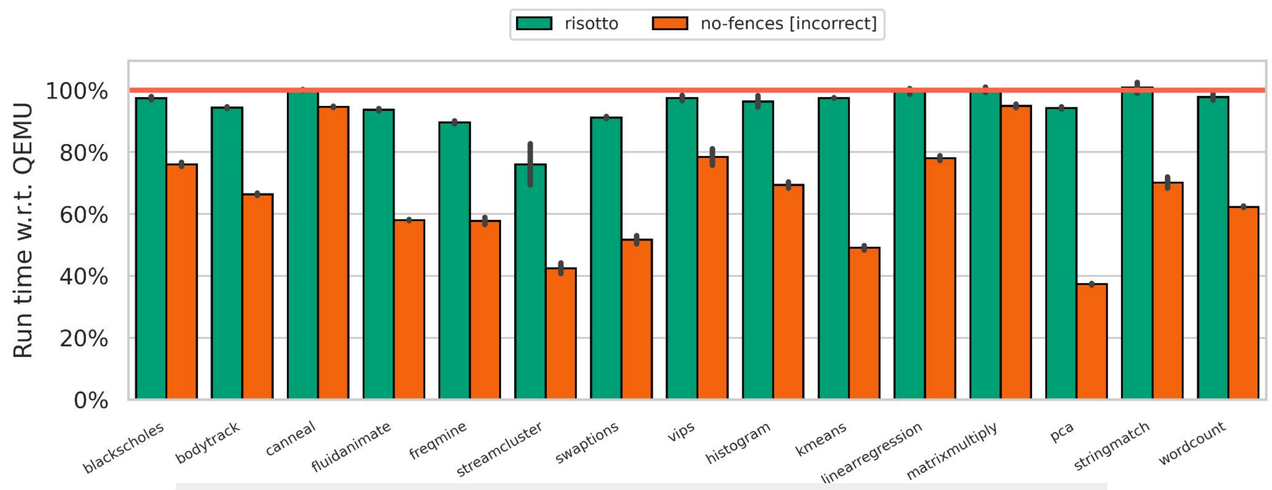
- **Correctness**
  - Formal model of QEMU's intermediate representation, *TCG*
  - *Precise* memory mappings from x86 to Arm via TCG
  - Formal proof of memory model equivalence
- **Performance**
  - Optimized code generation (fence merging, weak fences)
  - Correct native Compare-and-Swap translation
  - Dynamic host shared library linker



Evaluation

- *New memory mappings:*

  Compared to QEMU: up to **19.7%** improvement, **6.7%** on average



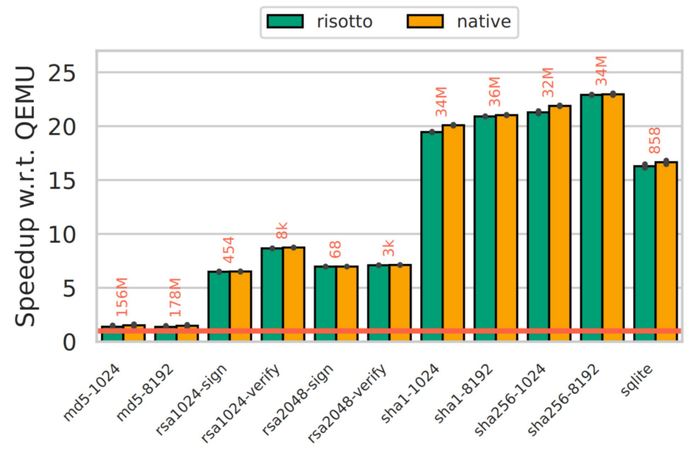
PARSEC and Phoenix benchmarks against QEMU. Lower is better.

- *Compare-and-Swap:*

  Same as QEMU with contention, **14.5%** faster without

- *Dynamic host shared library linker:*

  Native library performance



Speed-up of openssl and sqlite benchmarks against QEMU. Higher is better.

Impact

QEMU patches

Official Arm memory model fix

Technical University of Munich

TU Delft

The University of Edinburgh

University of St Andrews