Mumak

Efficient and blackbox detection of bugs in Persistent Memory programs

João Gonçalves (joao.tiago.goncalves@tecnico.ulisboa.pt)
Instituto Superior Tecnico, Universidade Lisboa & INESC-ID

Supervisors: Miguel Matos and Rodrigo Rodrigues

Motivation

- Persistent Memory (PM) combines durability with performance close to that of DRAM
- Stores are persisted asynchronously and non-deterministically (stores can be reordered)
- Flush and fence instructions enforce ordering constraints. However, crashes can still lead to inconsistencies in the post-failure state

State-of-the-art

- PM bug detection tools fall into two categories:
- Automatic space exploration is exhaustive but slow and cannot scale to complex applications
- Annotation-based debugging is fast but error-prone, since it delegates the effort to the developer
- Additionally, all existing works leverage the semantics of the application or PM library (PMDK)

Mumak

Goal: design a tool that detects PM bugs automatically and efficiently, while being agnostic of application code, application semantics, and underlying libraries

Insight

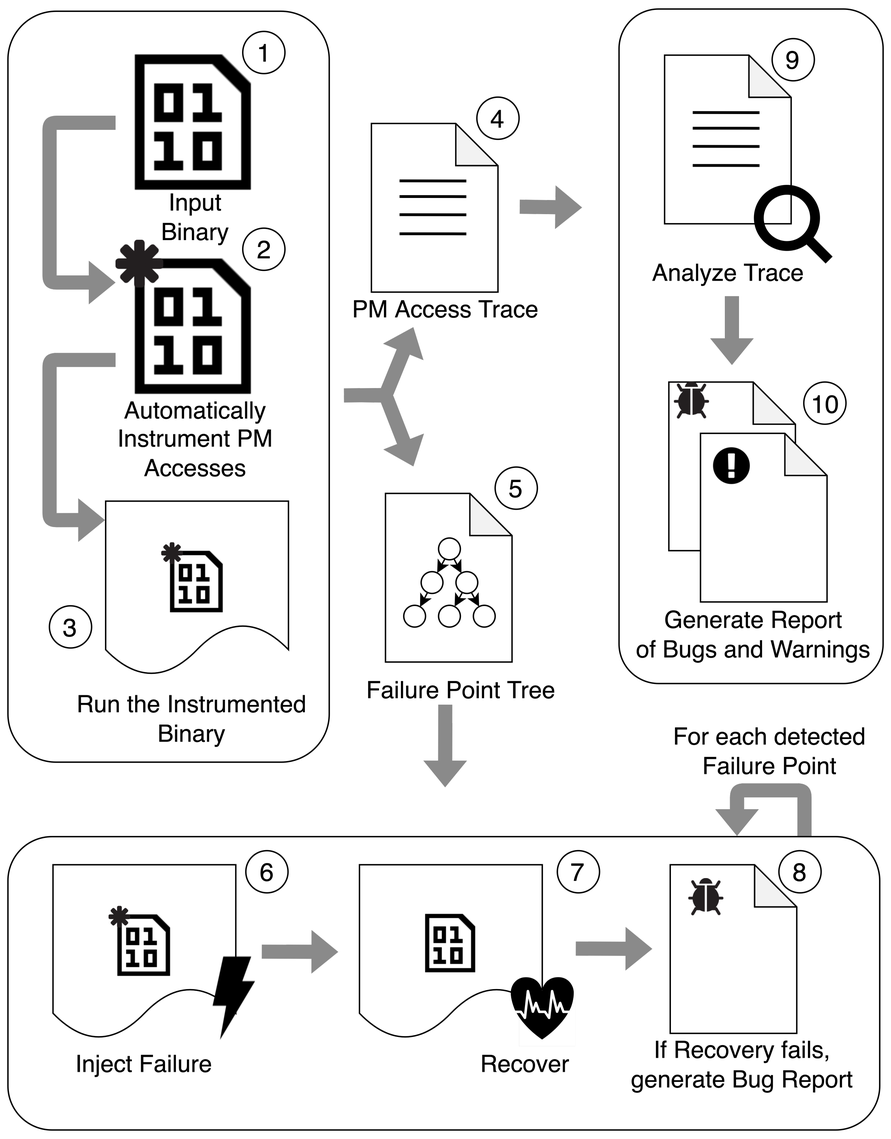
- Combination of fault injection and trace analysis based on automatic and blackbox instrumentation of target binaries

Fault Injection

- Construction of a failure point tree, comprised of unique execution paths that lead to relevant execution points (PM interactions)
- Systematic fault injection, producing deterministic and reproducible post-failure states without shadow memory
- Use of the application's recovery as a consistency oracle
- Reduction of the search space by only exploring states that respect some prefix of program-order

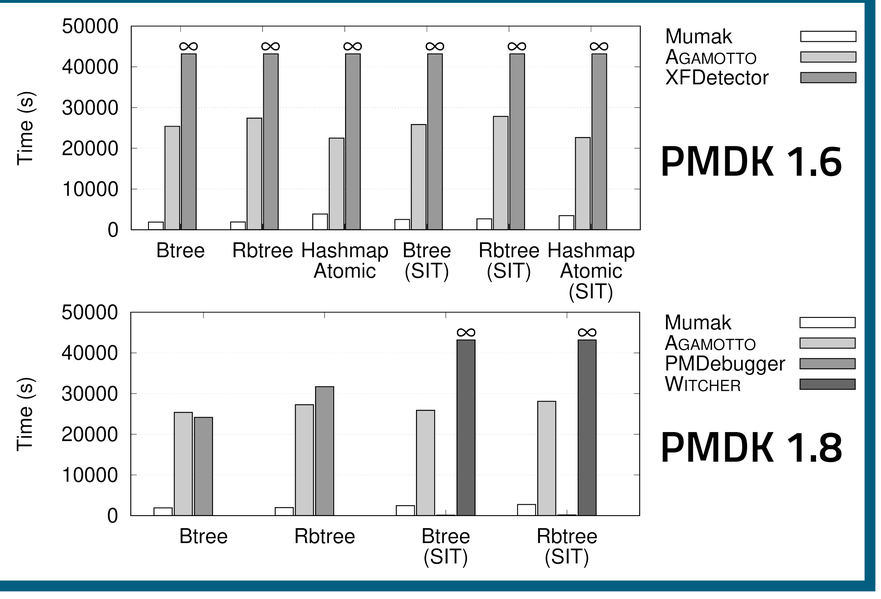
Trace Analysis

- Dynamic collection of PM access trace using complete workload
- Bug detection based on 5 well-defined generic patterns of misuse



Results

- Microbenchmarks show that Mumak is up to 10x faster than Witcher, Agamotto, XFDetector, and PMDebugger
- Coverage evaluation using Witcher as baseline: 90% coverage (70%* of correctness bugs and 100% of performance bugs)
- 3 **NEW** bugs found: 1 in PMDK 1.12.0 (latest stable version) and 2 in Montage (an example of a system that does not use PMDK)



This work was supported by national funds through FCT, Fundação para a Ciência e a Tecnologia, under projects UIDB/50021/2020 and Ainur (PTDC/CCI-COM/4485/2021), and grant 2021.07401.BD