A Library of Formal-Methods Tools

Dirk Beyer
LMU Munich, Germany

April 23, 2023, at COOP 2023

Vision

At the Summer School on Formal Techniques SSFT '18,
I started a lecture five years ago like this:

I have a dream ...

- ... that one day, all tools for formal methods work together to solve hard verification problems and make our world safer and more secure.
- ... that one day, model checkers and theorem provers can be integrated into the software-development process as seamless as unit testing today.
- ... that one day, model checkers, theorem provers, SMT solvers, and testers use common interfaces for interaction and composition.

Remaining Problems

- Which tools for software verification exist?
- ... for test-case generation?
- ... for SMT solving?
- ... for hardware verification?
- Where to find documentation?
- Am I allowed to use it?
- How to use them?

Requirements

- Approach must be compatible with competitions
- Blend well with CoVeriTeam
- Support documentation and reuse
- Long-term availability/executability

Solution

One central repository:
https://gitlab.com/sosy-lab/benchmarking/fm-tools
which gives information about:

- Location of the tool (via DOI, just like other literature)
- License
- Contact
- Project web site
- Options
- Requirements (certain Docker container / VM)
- Limits

Example

```
name: CPAchecker
lang: C
url: https://cpachecker.sosy-lab.org
required-ubuntu-packages:
  - openjdk-11-jre-headless
contact:
  name: Dirk Beyer
   institution : LMU Munich
  country: Germany
   url: https://www.sosy-lab.org/people/dbeyer/
```

Example (cont.)

```
actor_name: cpachecker
toolinfo_module: https://.../benchexec/tools/cpachecker.py
 spdx_license_identifier : Apache-2.0
 resourcelimits :
   memlimit: 15 GB
    timelimit : 15 min
   cpuCores: 8
format_version: '1.3'
```

Example (cont.)

```
archives :
  – version : 2.2
    doi : 10.5281/zenodo.7700944
    options : ['-svcomp23', '-heap', '10000M', '-benchmark', '-timelimit', '900 s']
  – version : svcomp22
    location : https://gitlab.com/sosy-lab/sv-comp/archives-2022/-/raw/main/2022/
    options : ['-svcomp22', '-heap', '10000M', '-benchmark', '-timelimit', '900 s']
  – version : 2.1
    doi : 10.5281/zenodo.5720557
    options : ['-svcomp22', '-heap', '10000M', '-benchmark', '-timelimit', '900 s']
```

Conclusion

- fm-tools collection can be used by competitions
- ... can be used by CoVeriTeam
- ... can be used to generate a web encyclopedia about formal-methods tools
- ... can be used to make tools long-term executable