

CEGAR

<http://d3s.mff.cuni.cz>

Department of
Distributed and
Dependable
Systems



Pavel Parízek



FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Tools

- Connect to some Linux machine
 - using SSH (Putty)
- Download
 - <http://d3s.mff.cuni.cz/files/teaching/nswi132/files/cegar.tgz>
- Package contains Linux binaries of
 - BOPPO
 - Model checker for boolean programs
 - SATABS v1.9
 - CEGAR + SAT
 - BLAST v2.5
 - Lazy abstraction
 - Examples
 - Some taken from tutorials created by authors of respective tools

- Verification tool for C and C++ programs
 - Based on CEGAR
 - Uses a SAT solver
- Key features
 - Variables represented as bit vectors (binary level)
 - Computer arithmetic (overflow, bit operators, ...)
- Developed at ETH Zurich & Carnegie Mellon Uni
- <http://www.cprover.org/satabs/>
- Source code and binaries freely available
 - Platforms: Windows, Linux, Mac OS

BLAST

- Key feature: lazy predicate abstraction
- Developed at UC Berkeley & EPFL (Lausanne)
- <https://www.sosy-lab.org/~dbeyer/Blast/index-epfl.php>
- Obsoleted by CPAchecker
 - Many advanced features and optimizations

- Modern successor of BLAST
 - Still under development
- Input: programs in C
- Advantages
 - Highly configurable
 - abstraction, merging data from control-flow paths
 - More user- friendly
- Web: <https://cpachecker.sosy-lab.org/>