

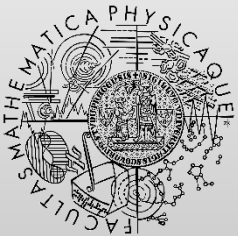
Static Analysis Tools

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

Department of
Distributed and
Dependable
Systems



Pavel Parízek



FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Categories

- Buggy and suspicious code patterns
- Shape analysis (heap object graphs)
- Advanced type systems (annotations)

Detecting buggy code patterns

- SpotBugs/FindBugs (Java)
 - <https://spotbugs.github.io/>, <http://findbugs.sourceforge.net/>
- PMD (Java)
 - <http://pmd.github.io/>
- Clang static analyzer (C,C++)
 - <http://clang-analyzer.llvm.org/>
- PREfast (C,C++)
 - [https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms933794\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms933794(v=msdn.10))
- FxCop (C#/.NET)
 - [https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/bb429476\(v=vs.80\)](https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/bb429476(v=vs.80))
- ReSharper (C#/.NET, free trial)
 - <https://www.jetbrains.com/resharper/>

LLVM compiler infrastructure

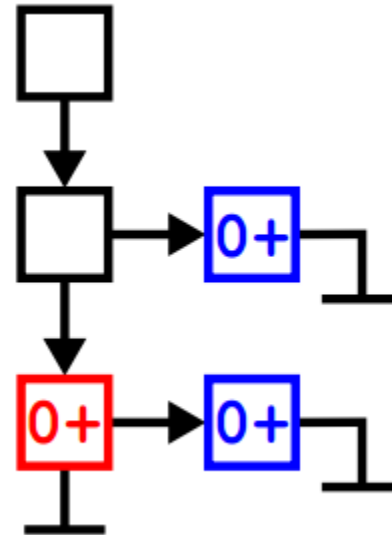
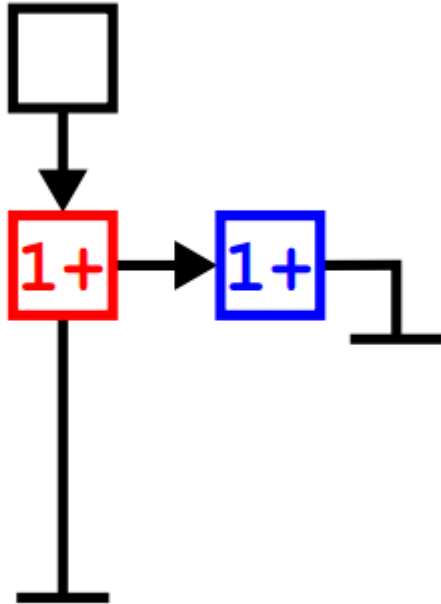
- Web site: <http://llvm.org/>
- Internal code representation
 - compiler IR (SSA-based, memory)
 - Serialized bitcode (on hard disk)
 - Human-readable assembly language
- Supported languages: C, C++, Objective-C
- Supported target hardware architectures
 - x86, x86-64, ARM, SPARC, PowerPC
- Clang compiler
 - fast, useful error messages, nice API

Predator

- Authors: FIT VUTBR
 - Kamil Dudka, Petr Peringer, Tomáš Vojnar
- Target domain
 - sequential programs in C that use heap, pointers, and dynamic linked lists
- Supports low-level memory operations
 - pointer arithmetic, reinterpretation, memory block operations
- Plugin for GCC
- Home page
 - <http://www.fit.vutbr.cz/research/groups/verifit/tools/predator/>

Predator: details

- Symbolic Memory Graphs (SMG)



Predator: how to run it

- Download & build from sources

- <http://www.fit.vutbr.cz/research/groups/verifit/tools/predator/>

- Setup environment

- `./sl_build/register-paths.sh`

- Running

- `gcc -fplugin=libsl.so <program>`

The Checker Framework

- Detects various runtime errors in Java programs
 - Pluggable custom type systems
 - Java source code annotations
- Checkers: null references, array accesses, locks, purity, format strings, ...
- <https://checkerframework.org/>
- Limited expressive power
 - Motivation: practical usefulness