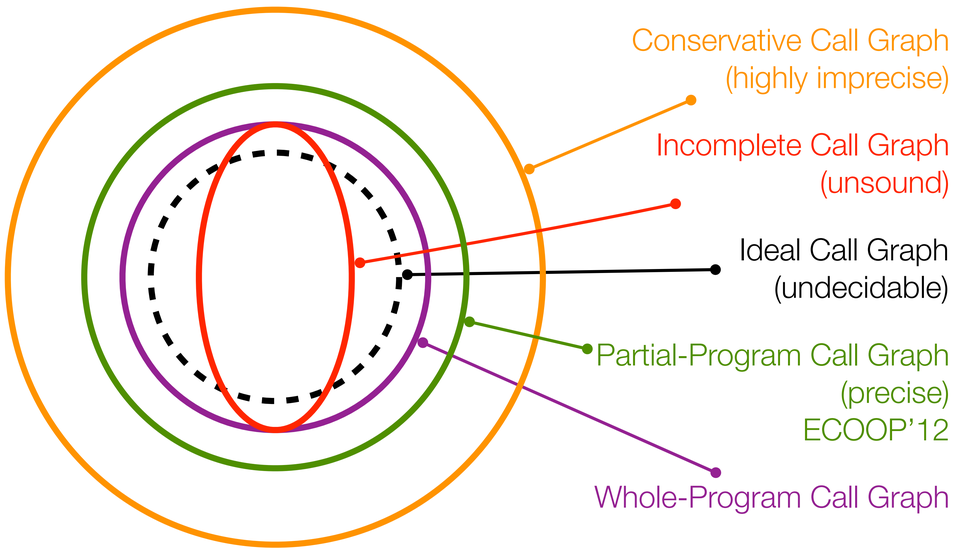
Averroes: Whole-Program Analysis Without the Whole Program

Karim Ali and Ondřej Lhoták

CHERITON SCHOOL OF COMPUTER SCIENCE

http://plg.uwaterloo.ca/~karim/averroes

Call Graph Construction

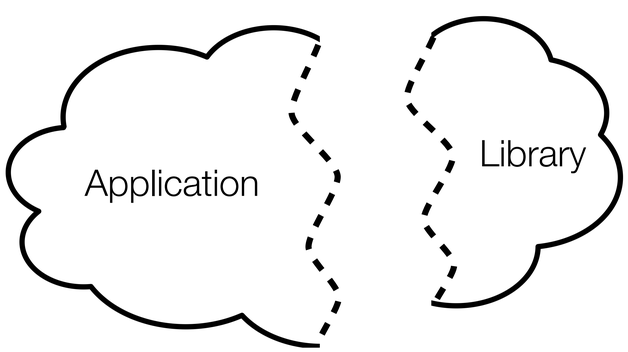


Averroes Workflow

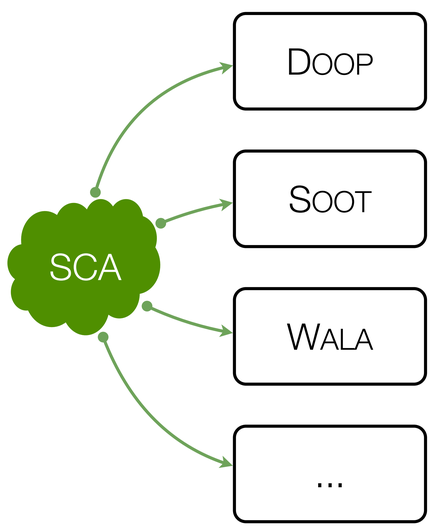
Averroes analyzes the constant pool and the class hierarchy of the input classes. It then generates a placeholder library that encodes the constraints of the separate compilation assumption as explicit bytecode instructions.

Separate Compilation Assumption

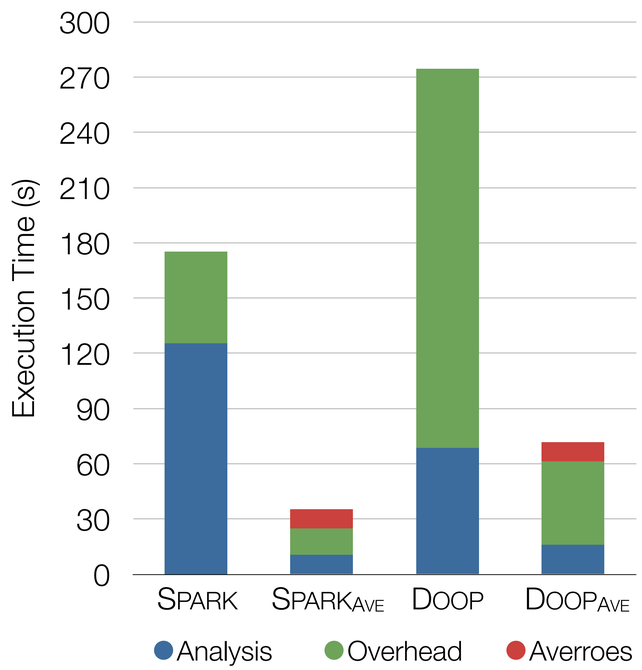
The separate compilation assumption states that the library code can be separately compiled from any application code that uses it. Following this assumption, we define a set of constraints that model the behaviour of the unanalyzed library code. These constraints enable fairly precise application-only call graph construction.



Goal



Results



Missing edges compared to dynamic call graph

	SPARK	SPARKAVE	DOOP	DOOPAVE
hsqldb	4%	0%	20%	0%
luindex	1%	0%	42%	0%
lusearch	34%	0%	45%	0%
pmd	0.1%	0%	11%	0%
xalan	3%	0%	12%	0%

- ☑ 32x smaller library size
- ☑ Up to 12x faster call graph construction
- ☑ Up to 13x less memory
- ☑ Out-of-the box support for reflection