Overview of the advantages and disadvantages of **static analysis tools**

Liisa Sakerman
Rain Hallikas

Introduction

The aim - to give an overview of the advantages and limitations of static tool analysers and how the limitations can be overcome.

I. Definition of research questions
II. Data search
III. Study selection and quality assessment
IV. Data extraction
V. Results

Research Questions

RQ1: What are the **main advantages** to the usage of static tool analysers.

RQ2: What are the **main disadvantages** to the usage of static tool analysers.

RQ3: Which **static analysis tools** are more used in studies in the last 10 years.

RQ4: How can the problems related to the static analysis be **minimized**.

Database

- EBSCO Discovery Service

Search Strategy

(static tool analysis) OR (static code analysis) OR (static analysis tools) OR (source code analysis) OR (static tool analysers) OR (static code analysers) OR (source code analysers)

- **4041 results**

Study Selection

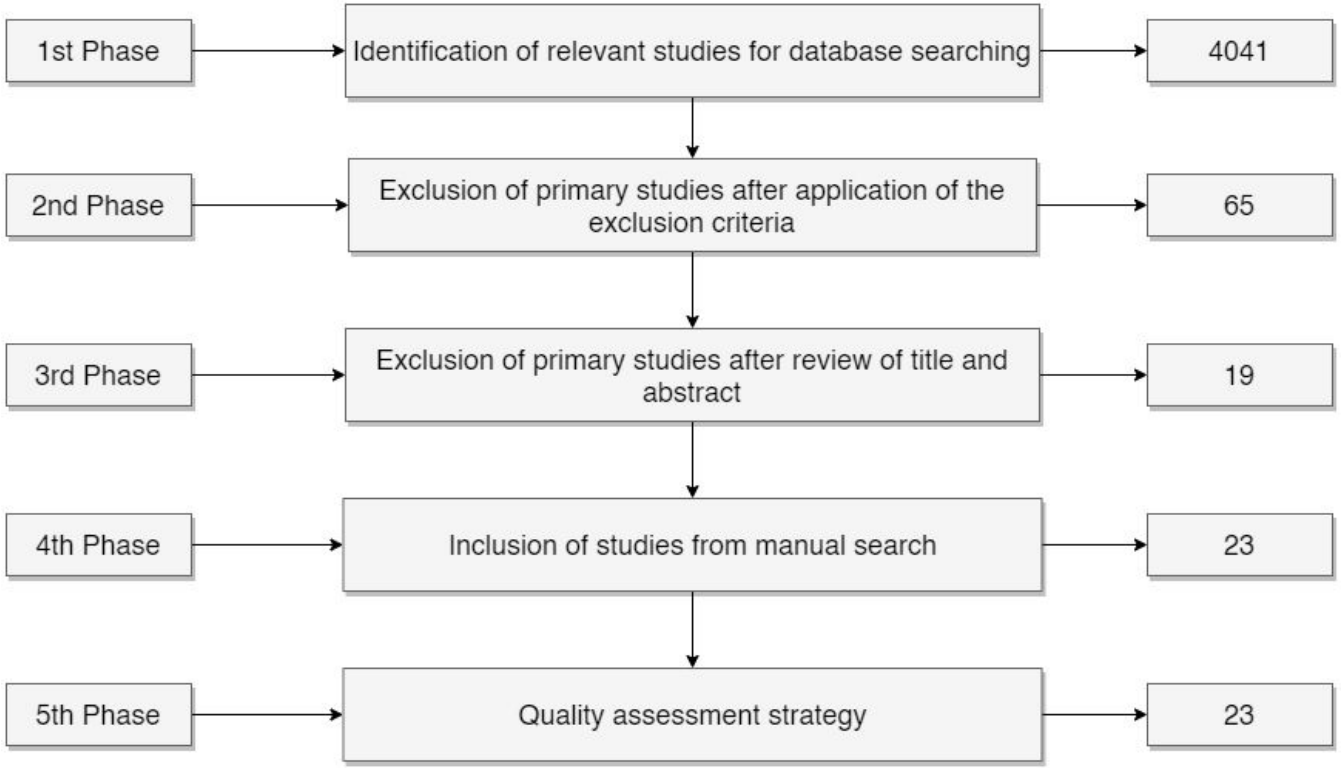
- EC1: Papers published later than 2010 (2414 remaining)
- EC2: Papers not in English (1888 remaining)
- EC3: Papers that are not conference materials or academic journals (1543 remaining)
- EC4: Papers that do not have full text available (1180 remaining)
- EC5: Papers that do not contain subject “tools” (65 remaining)

QA and Addition

- IC1: Papers mentioning static code analysis tools in use
- IC2: Papers discussing the advantages of tools
- IC3: Papers discussing problems related to tools
- IC4: Papers suggesting solutions to problems with static code analysis tools
- QC1: Are the aim, methodology and results of the study clearly stated?

- 19 papers remained
- 4 papers added
- Final papers: **23**

Stages


1st Phase
Identification of relevant studies for database searching
4041
2nd Phase
Exclusion of primary studies after application of the exclusion criteria
65
3rd Phase
Exclusion of primary studies after review of title and abstract
19
4th Phase
Inclusion of studies from manual search
23
5th Phase
Quality assessment strategy
23

Data Extraction Table Structure

Data Item	**Value**	**RQ**
Article Title	Name of the article	
Author(s)	Set of names of the authors	
Advantages	Advantages mentioned	RQ1
Disadvantages	Disadvantages mentioned	RQ2
Tools	Tools mentioned	RQ3
Solutions	Solutions to the disadvantages mentioned	RQ4

RQ1 - Advantages

What are the **main advantages** to the usage of static analysis tools?

General advantage	Occurrence
Early detection of defects without execution	11
Understand the behaviour of the code	7
Using tools is less time-consuming	6
Can detect more advanced but common problems	6
Keep code at high quality with best practice patterns	4
Reduce code review effort	3
High customization	1
Easy to achieve full coverage	1
Wide range of tools	1
Increasingly easier to use	1

RQ2 - Disadvantages

What are the **main disadvantages** to the usage of static analysis tools?

General disadvantage	Occurrence
False positives	12
False negatives	7
A single tool cannot detect all defects	5
Unclear warning messages	4
Complex defects lack efficient tools	3
Difficult to integrate	2
Defects must be visible in static code	2
Small fraction of issues are fixed	1
High memory consumption	1
Complex code reduces success rate	1
Low customizability	1

RQ3 - Tools

Which **static analysis tools** are more used in studies in the last 10 years?

Tool	Occurrence
FindBugs	12
PMD	7
Cppcheck	5
SonarQube	5
CheckStyle	4
Splint	3
Flawfinder	3
Coverty	3
FindSecBugs	3
Parasoft	2
Sparse	2
Clang	2

RQ4 - Solutions

How can the problems related to the static analysis tools be **minimized**?

General solution	Occurrence
Combining tools can help detect more defects	6
Specific tools need to be selected	5
Tools are to be continuously improved	4
Machine learning can reduce false results	3
Tools' usefulness can be improved by suggesting solutions	3
Tools are configurable and customizable	2
Writing code in a specific, correct way	2
Ranking the bugs by weight or priority	2
Tools should be used to compliment review and testing	2
Tools can be integrated into frameworks for evaluation	1

Reflection

- Could have defined a more accurate search string to include **“tools”**
- Could have specified **a programming language**
- Would have been interesting to include and read more papers (**3 ECTS...**)
- Conducting the mapping study was **very insightful** and definitely helpful in writing a master’s thesis in the future