Formal Methods in Software Engineering

2024/25

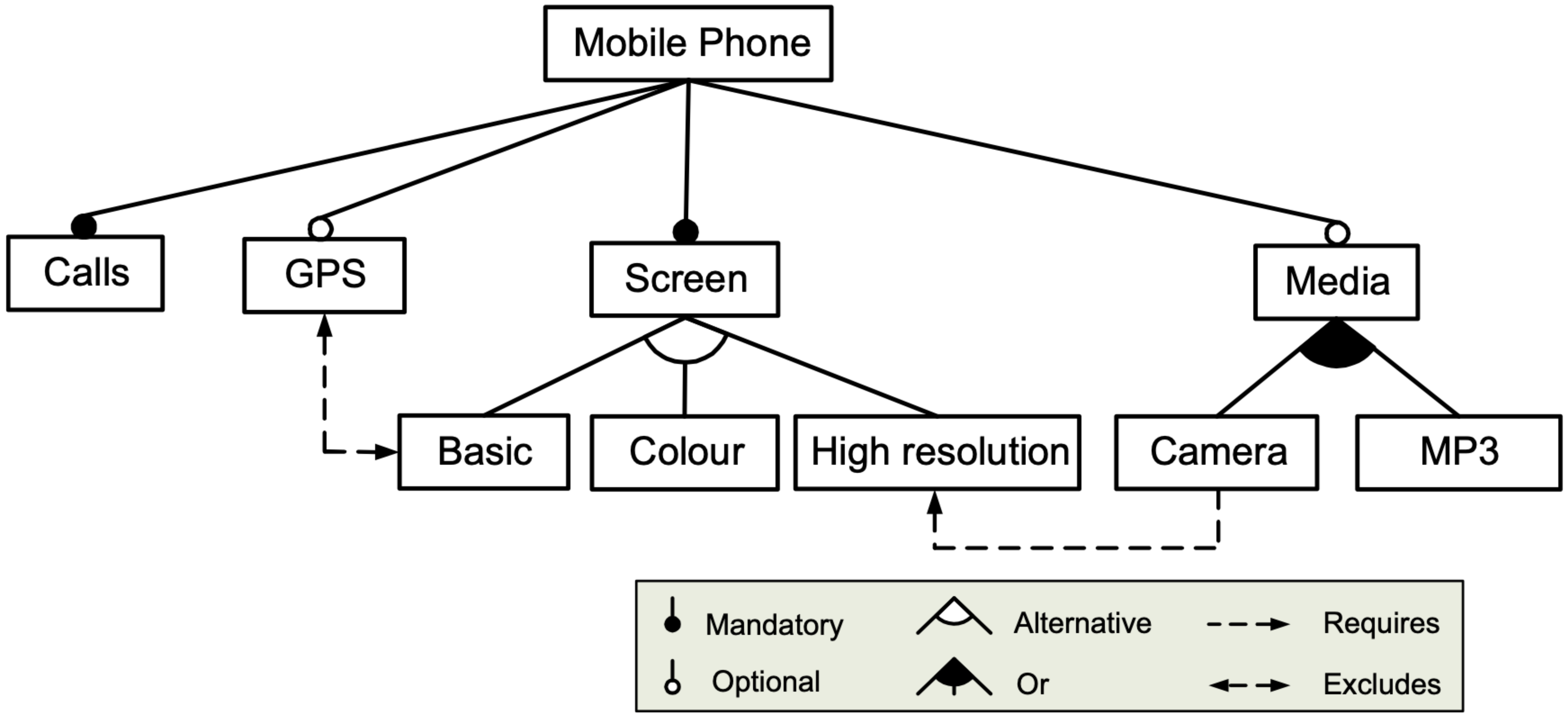
(Lightweight) formal methods

- Rigorous approaches
- Formal languages (logics)
- Automatic proof techniques
- High-level and user-friendly tools

Applications

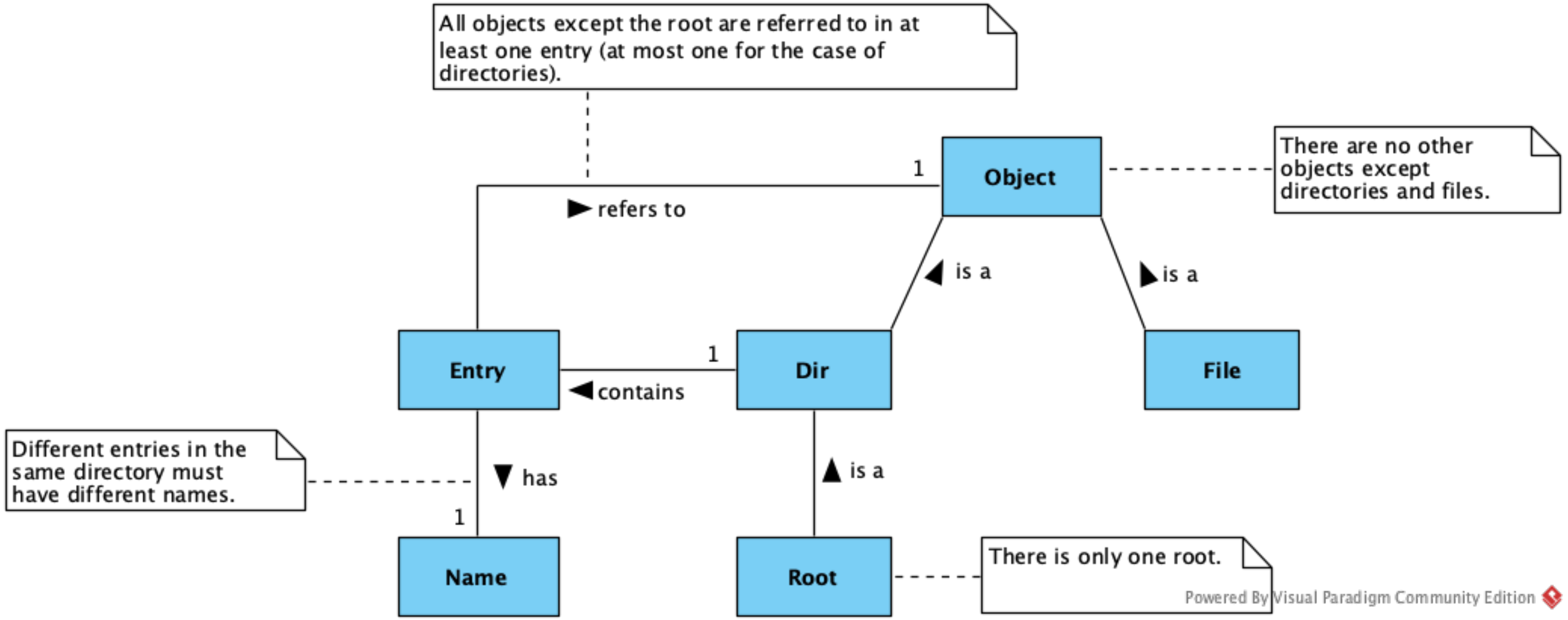
- Variability modelling
- Domain modelling
- Data-structure design
- App design
- Program testing
- Progam verification

Variability modelling

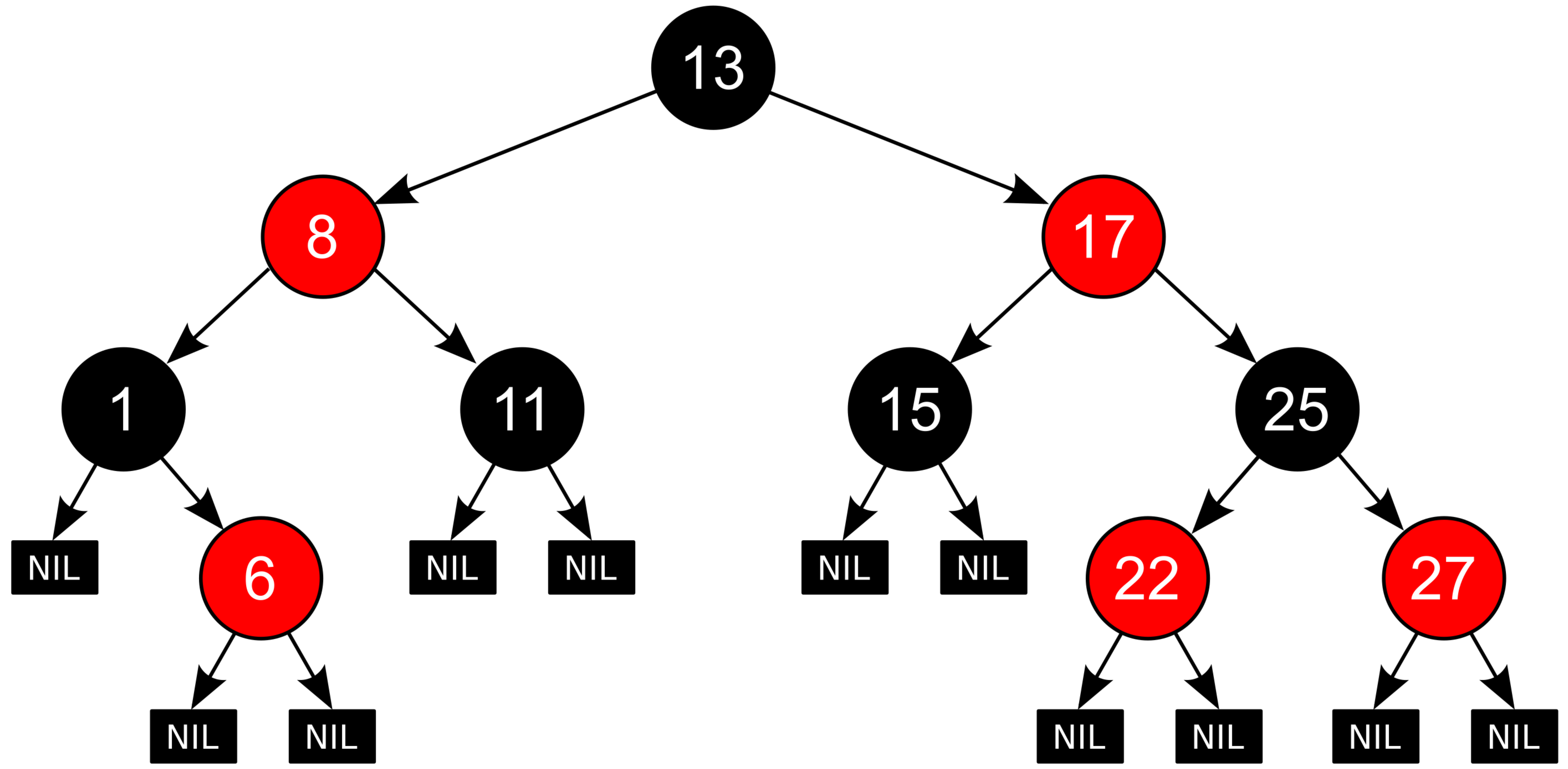


https://doi.org/10.1016/j.is.2010.01.001

Domain modelling

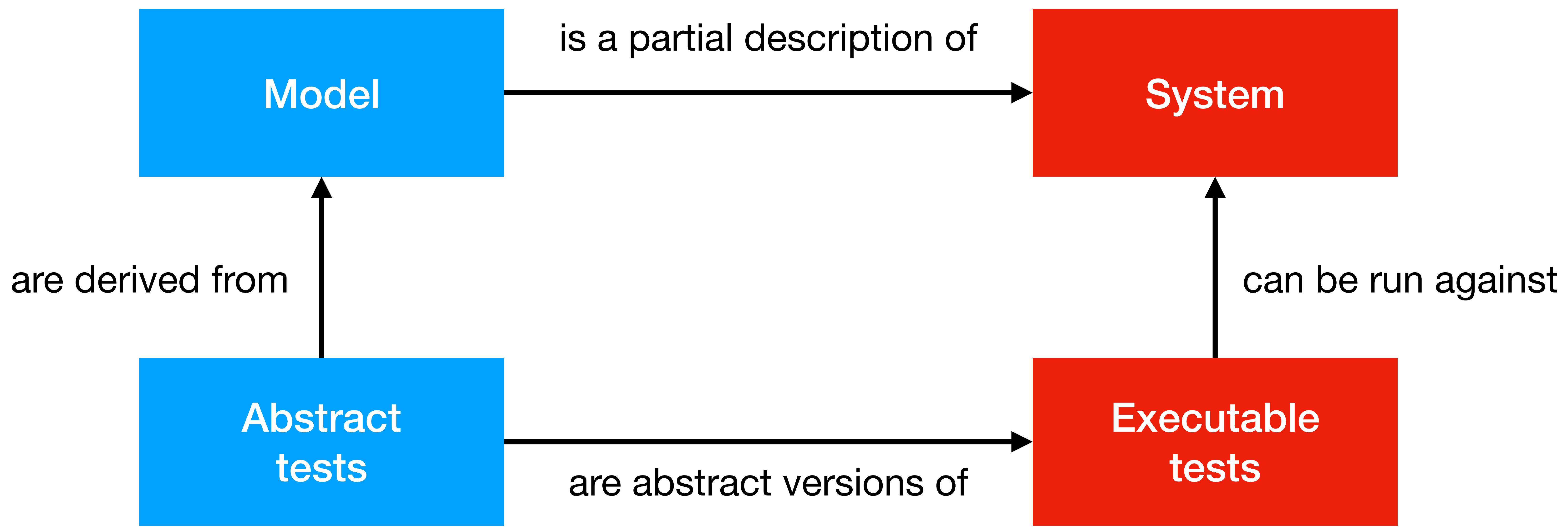

All objects except the root are referred to in at least one entry (at most one for the case of directories).
1
Object
▶ refers to
There are no other objects except directories and files.
◀ is a
▶ is a
Entry
1
Dir
File
◀ contains
Different entries in the same directory must have different names.
▼ has
▲ is a
1
Name
Root
There is only one root.
Powered By Visual Paradigm Community Edition

Data-structure design

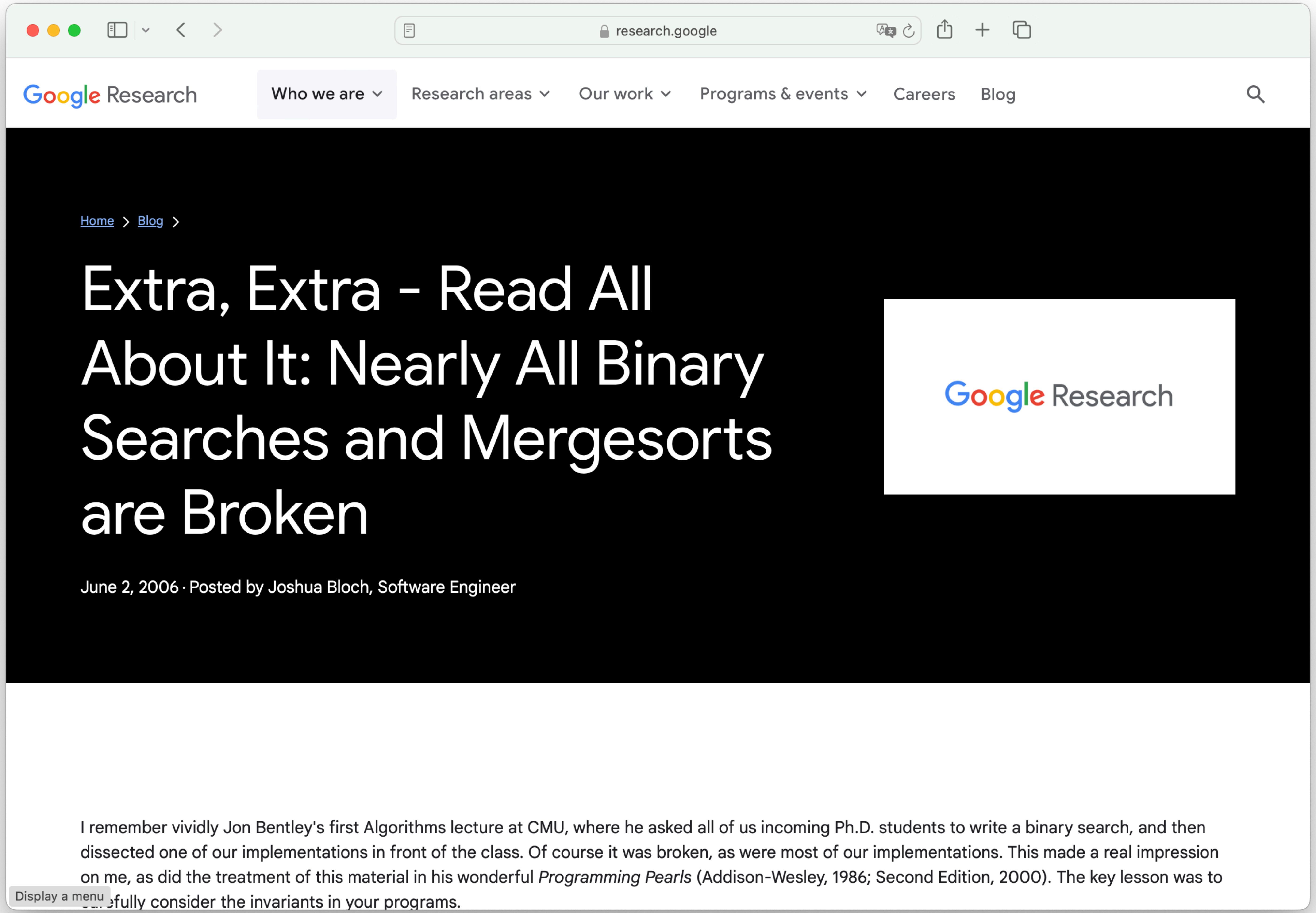


App design

Program testing



Program verification



Extra, Extra - Read All About It: Nearly All Binary Searches and Mergesorts are Broken

June 2, 2006 · Posted by Joshua Bloch, Software Engineer

I remember vividly Jon Bentley's first Algorithms lecture at CMU, where he asked all of us incoming Ph.D. students to write a binary search, and then dissected one of our implementations in front of the class. Of course it was broken, as were most of our implementations. This made a real impression on me, as did the treatment of this material in his wonderful *Programming Pearls* (Addison-Wesley, 1986; Second Edition, 2000). The key lesson was to carefully consider the invariants in your programs.

Lecturers

- Alcino Cunha (MAC)
  - alcino@di.uminho.pt
  - Ed7 2.15
- Jorge Sousa Pinto (JSP)
  - jsp@di.uminho.pt
  - Ed7 2.28

Program

- Computational logic (MAC + JSP)
- Formal software design with Alloy (MAC)
- Deductive program verification with Why3 (JSP)

Schedule

11h	TP2 (JSP) CP2 2.06	TP4 (MAC) CP1 0.17
12h		
13h	T (MAC + JSP) CP1 0.08	
14h		
15h	TP1 (JSP) CP2 2.02	TP3 (MAC) Ed7 1.10
16h		
17h	TP5 (MAC) CP1 2.23	

Assessment

- Continuous assessment
  - Written test (80%) - 14 Dez
  - Practical exercises (20%) - 27 Set, 18 Out, 1 Nov, 29 Nov (e-learning)
- Assessment by examination
  - Written exam (100%) - 20 Jan
- Final grades above 18 require a “defence” with a small project/challenge

https://haslab.github.io/MFES/

Questions?