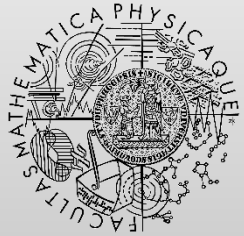
Formal Approaches in Mainstream:
Software Development and Programming Languages

http://d3s.mff.cuni.cz

Department of Distributed and Dependable Systems

Pavel Parízek



FACULTY OF MATHEMATICS AND PHYSICS
Charles University

Software development process

Phase	Formal
Requirements	Specification
Design	Model & properties
Architecture	Validation
Implementation	Model-based testing Program verification
Documentation	Math expressions

Programming languages

- Tool support (IDEs)
  - Reporting source code bugs on-the-fly
  - Validating consistency (contracts)
- Formal semantics
  - Concurrency (memory models)
  - Advanced complex type systems

Architecture: modeling and validating

- What is needed
  - Interfaces of components (big modules)
  - Safe interaction between components

- “Composition problem”
  - Individual components: with safe local behavior
  - The whole system: unexpected errors may arise
  - https://cacm.acm.org/magazines/2018/11/232196-the-big-picture