Formal Verification of Evolution

Software Evolution — L7T2

Dr. Vadim Zaytsev aka @grammarware, March 2021

UNIVERSITY OF TWENTE.
Formal Methods & Tools

What's *Formal Verification*?

- **Formal** verification method
  - technique to prove consistency
  - system satisfies requirements
- Requires
  - formal description of the system
  - formal spec of the requirements
  - rigorous reasoning rules
- (Assumed to be automated)

Regression Verification

- Writing specs is hard
  - ⟹ can we reuse existing revisions?
  - “*trust by experience*”
- Hand in hand with regression testing
  - RV proves tested values generalise
- Need an equivalence definition

Generalised Test Tables

- Writing specs is hard
  - ⟹ can we simplify writing them down?
- Make a table relating inputs to outputs
- Replace concrete values
  - with constraints
- Check for weak/strict conformance

Interdisciplinary Models

- Writing specs is hard
  - ⇒ can we infer them?
- Take the multidomain model
- Use it to infer a number of smaller models
  - tailored to their tool/notation

Conclusion

- Formal verification in practice is extremely hard
  - system specs, req specs, proof rules
- Can be linked to testing
- Tackes the consistency challenge
- Q&A Sessions @ Canvas
  - ⇒ v.zaytsev@utwente.nl
  - ⇒ https://discord.gg/n7VQAPNBPD