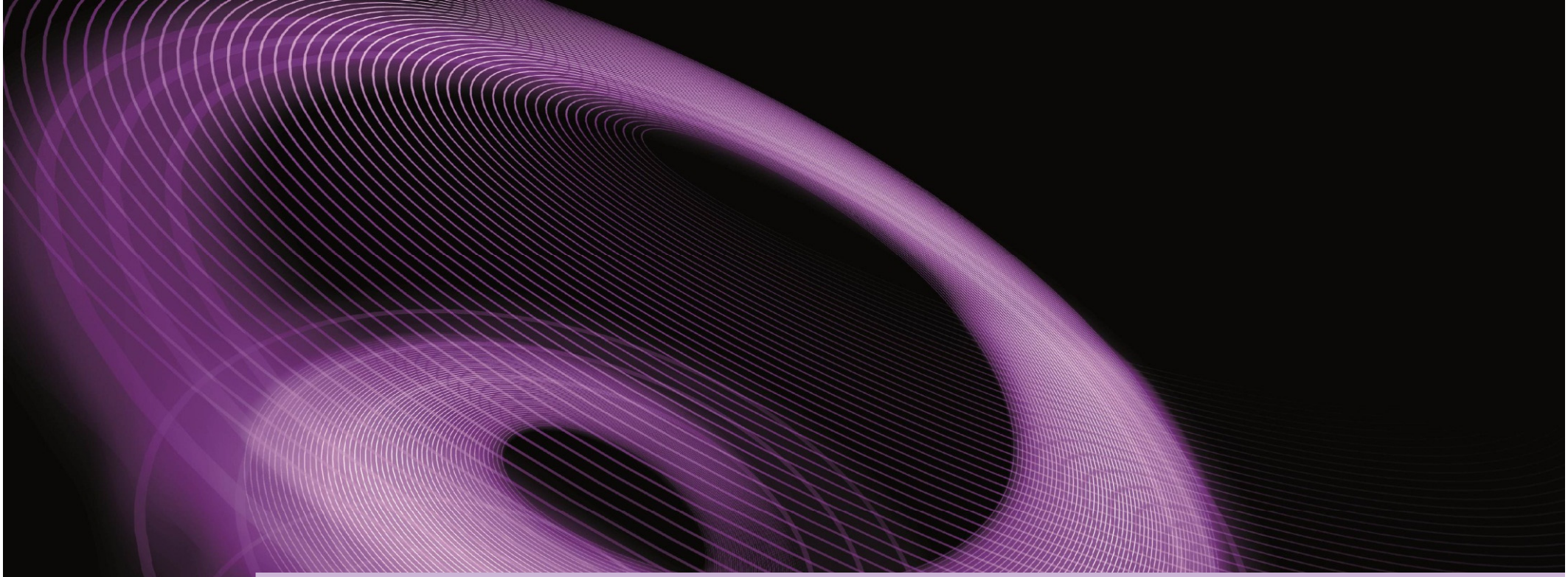
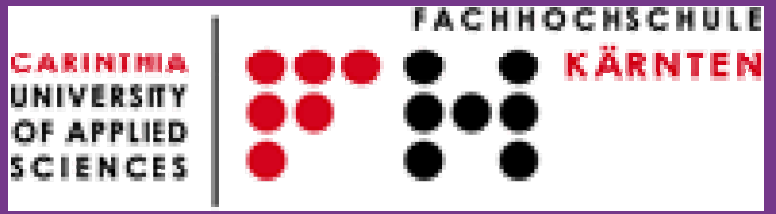


Formal Specification Comprehension

The Art of Reading and Writing Z

Andreas Bollin, Alpen-Adria Universität Klagenfurt
Dominik Rauner-Reithmayer, Carinthia University of Applied Sciences

FAKULTÄT FÜR TECHNISCHE WISSENSCHAFTEN



Content in a Nutshell

- Motivation
  - Size and Complexity
  - Resistance and a chance
- Comprehending Specifications
  - Understandability
  - Preferences
  - Time/Effort
- A first Study
  - Setting
  - Results
- Conclusion and Discussion

Motivation (1/3)

Size and Complexity

- Our Systems and software are getting to **new dimensions**
  - Voyager … 3 KLOC (1977),
    Cassini … 10 KLOC (1997),
    Mars Rover 160 KLOC (2003),
    ISS … 5 MLOC (2009),
    Boing 787 … 6.4 MLOC (2011),
    General Motors GMC … 100 MLOC (2011)

- Nearly **1,100 deaths** attributable to computer errors
  - stemming from poor to no specifications, not from incorrect implementations [McKenzie 01]

Motivation (2/3)

Resistance as no way out

- FS are beneficial artifacts during SW development (**validation**, **verification**) and maintenance phases (**comprehension**, **concept identification**).

- But,
  - **not all stakeholders** are able to speak and think in the same technical terms
  - developers do have different preferences in expressing (and documenting) their thoughts
  - even formal specification contain errors

➔ **Every activity raising comprehensibility helps in dealing with resistance**

Motivation (3/3)

Problems and challenges:

- **Logic**, and with it
  - Mistakable Logic Expressions

$$DivByThree : \mathbb{P}\,\mathbb{N}_1 \mid \forall x : \mathbb{N}_1 \mid x \bmod 3 = 0 \bullet x \in DivByThree$$

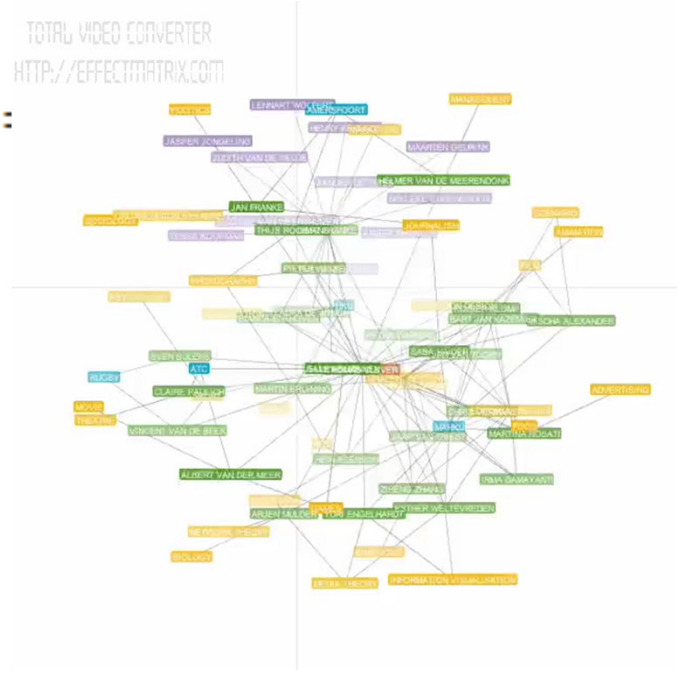
$$DivByThree : \mathbb{P}\,\mathbb{N}_1 \mid \forall x : \mathbb{N}_1 \bullet x \bmod 3 = 0 \Rightarrow x \in DivByThree$$

- **Notation**
  - Misleading and hard to understand notations [Gravel 90]

$$primes_1 == \{n : \mathbb{N} \mid n \geq 2 \wedge \neg (\exists m : 2 \mathinner{..} n \bullet n \bmod m =$$

$$\mathbb{N}_2 == \mathbb{N} \setminus \{0, 1\}$$
$$primes_2 == \mathbb{N}_2 \setminus \{n, m : \mathbb{N}_2 \bullet n * m\}$$

- **Comprehensibility**
  - Too complex (large) specifications and ill-structured specifications



Comprehending Specifications

- **How to deal with this situation?**
  - Taking a closer look at “quality” attributes of formal specifications with the focus on comprehensibility
  - The assumption is that, by raising comprehensibility, one is also very likely raising acceptability

Working Definition: A **good formal specification** is a syntactically and semantically correct specification which enables a lossless mapping between all the concepts in/behind the specification and the mental model of the specified system. The mapping process should **not** be **perceived as exhausting** and it should be **completed** within **reasonable time**.

The Study

- **Guidelines as a way out?**
  - Investigate the sense of style in reading and writing formal specifications
  - Which style (of writing) is less error prone

- **For the study (conducted during the Winter term 2013) we focused on:**
  - KQ1) Do common guidelines support the correct understanding of a formal specification?
  - KQ2) Do common guidelines support an easier and faster understanding of a formal specification?

The Study Setting (1/3)

- **Following aspects have been taken into consideration:**

  - Understandability of **mathematical idioms** (symbols in Z). Here, we focus on the relational override and the use of functions
  - Correct perception of the **logical implication** (following the observations of [Vinter, Loomes and Kornbrot 98]. Here, we focus on “natural order" [Gravell 91, p.4], logic equivalence and its use in orders that are not natural
  - Correct interpretation of **incomplete operations**

  - Correctness of (a subset of) the **recommendations** of Gravell [Gravell 91, p.12].

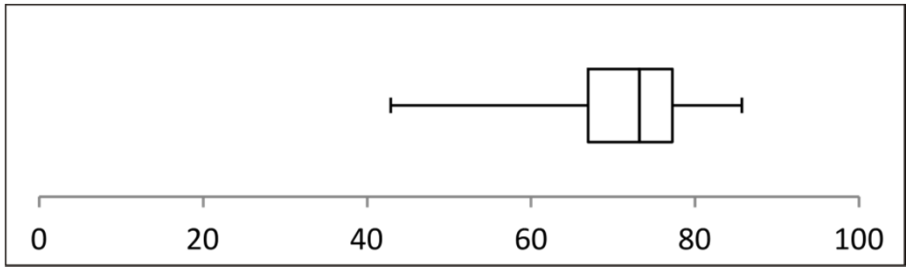
The Study Setting (2/3)

- **Additionally, correctness of (a subset of) the recommendations of Gravell [Gravell 91, p.12]**

  - G1 Prefer clarity to brevity
  - G2 Choose the state so as to minimize the invariant
  - G3 Choose the state to simplify the description of the operations
  - G4 Give an implication its natural order, or avoid implications entirely
  - G5 Give names to important concepts
  - G6 Where the mathematical idiom is commonly understood, use it.

The Study Setting (3/3)

- **Skill of students have been quite high (n=25)**
  - 6 Master, 19 Bachelor
  - 28 European credit points (~ 700 hours) on Math and Theoretical Computer Science
  - overall performance is above 50% of achievable points



- **Two (of 3) on-line questionnaires (Moodle):**
  - Q1: **14 questions** in multiple choice select form
  - Q2: **24 tasks**. In order to minimize the influence of the duration for understanding the **problem domain**:
    1. Description of the example in natural language
    2. Specification of the example in Z
    3. Question to decide if the specification represents the described situation in a correct manner

The Study Results (1/6)

- **Correct Understanding**
  - Mathematical Idioms (89% correctly understood)
  - Logical Implications
    - single implication (83%),
    - equivalent logical form using negation (82.5%)
    - implication contained in another implication (66%)
  - Incomplete Operations (63% correctly understood)
- **Developers Preferences**
  - G1 Prefer **clarity to brevity**
  - Guideline: do not use Variant 2
  - Study result: variant 2 or variant 3

$$SWITCH ::= on \mid off$$

Variant1

$$s, s' : SWITCH$$

$$s' \neq s$$

Variant2

$$s, s' : SWITCH$$

$$(s = off \land s' = on) \lor (s = on \land s' = off)$$

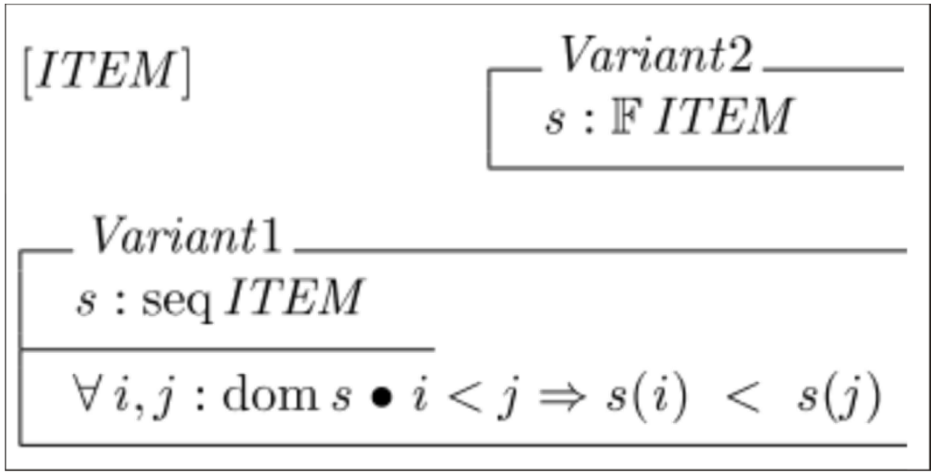
Variant3

$$s, s' : SWITCH$$

$$s = off \Rightarrow s' = on$$
$$s = on \Rightarrow s' = off$$

The Study Results (2/6)

- **Developers Preferences (contd.)**
  - G2 Choose the state so as to **minimize the invariant**
  - Example used: collection of an Item store
  - Guideline: prefer Variant 2
  - Study result: Variant 1



  - G3 Choose the state to **simplify the description** of the operations. Guideline: confirmed

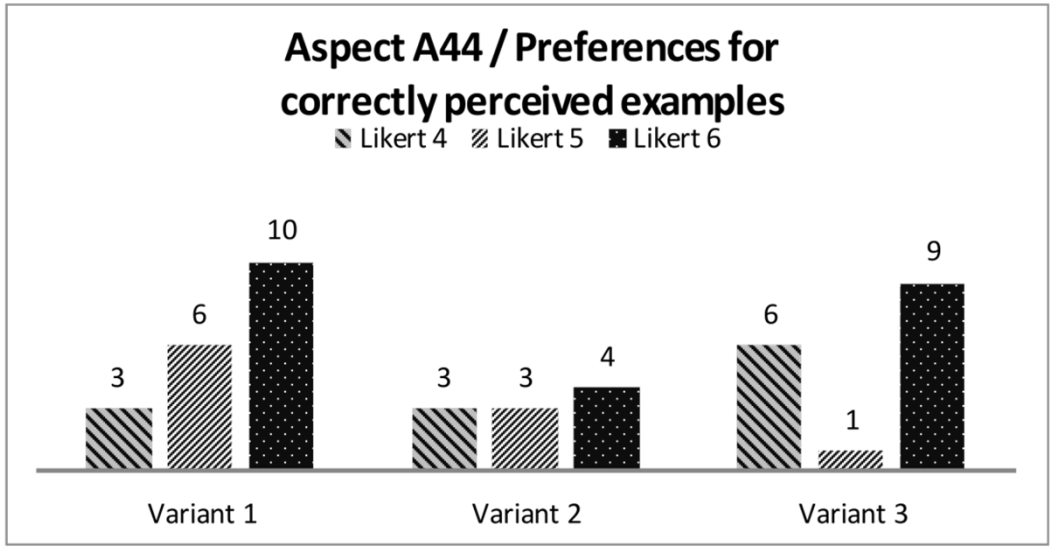
The Study Results (3/6)

- **Developers Preferences (contd.)**
  - G4 Give an implication its **natural order**, or **avoid implications** entirely
  - Guideline: prefer variant 1
  - Study result: Variant 1, but Variant 3 also OK

$$\forall i, j : \mathrm{dom}\, s \bullet i < j \Rightarrow s(i) < s(j)$$

$$\forall i, j : \mathrm{dom}\, s \bullet s(i) \geq s(j) \Rightarrow i \geq j$$

$$\forall i, j : \mathrm{dom}\, s \mid i < j \bullet s(i) < s(j)$$



The Study Results (4/6)

- **Developers Preferences (contd.)**
  - G5 Give **names** to important concepts
  - Guideline: prefer variant 2
  - Study result: no clear tendency
  - G6 Where the **mathematical idiom** is commonly understood, use it. Guideline: confirmed

$$[CUSTID, BOOKID, DATE, NAME]$$
$$[ADDRESS, TITLE, AUTHOR]$$

Variant1

$$BookDB : BOOKID \pfun (AUTHOR \times TITLE)$$
$$CustDB : CUSTID \pfun (NAME \times ADDRESS)$$
$$LoanDB : BOOKID \pfun (CUSTID \times DATE)$$

$$\dom LoanDB \subseteq \dom BookDB$$
$$\forall c : CUSTID \mid (\exists b : BOOKID;\ d : DATE \bullet b \mapsto (c, d) \in LoanDB) \bullet c \in \dom CustDB$$

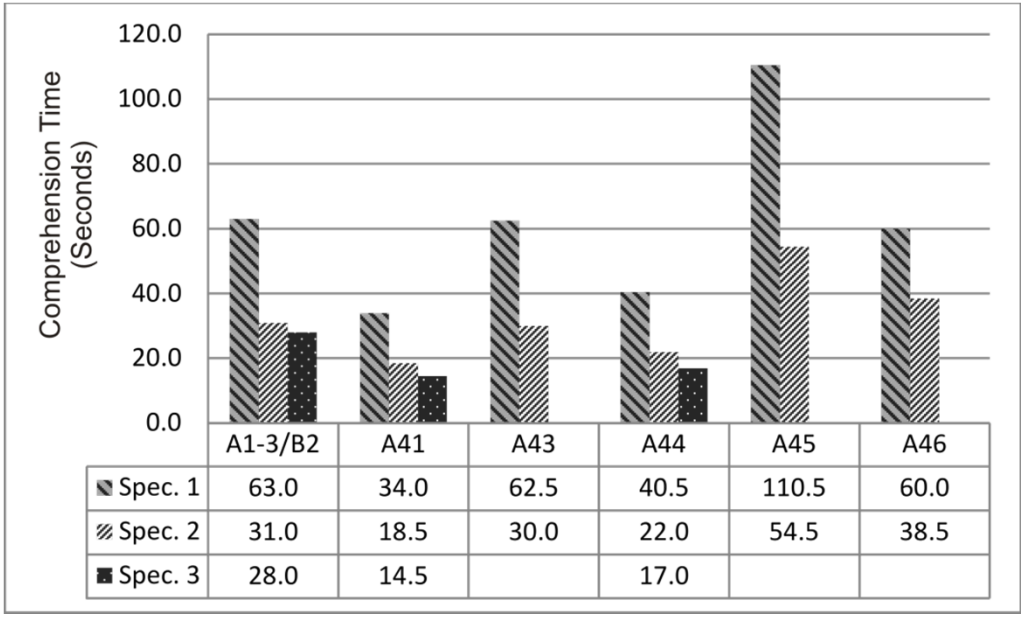
Variant2

$$author : BOOKID \pfun AUTHOR$$
$$title : BOOKID \pfun TITLE$$
$$name : CUSTID \pfun NAME$$
$$address : CUSTID \pfun ADDRESS$$
$$borrower : BOOKID \pfun CUSTID$$
$$due : BOOKID \pfun DATE$$

$$\dom borrower = \dom due \subseteq \dom author = \dom title$$
$$\ran borrower \subseteq \dom name = \dom address$$

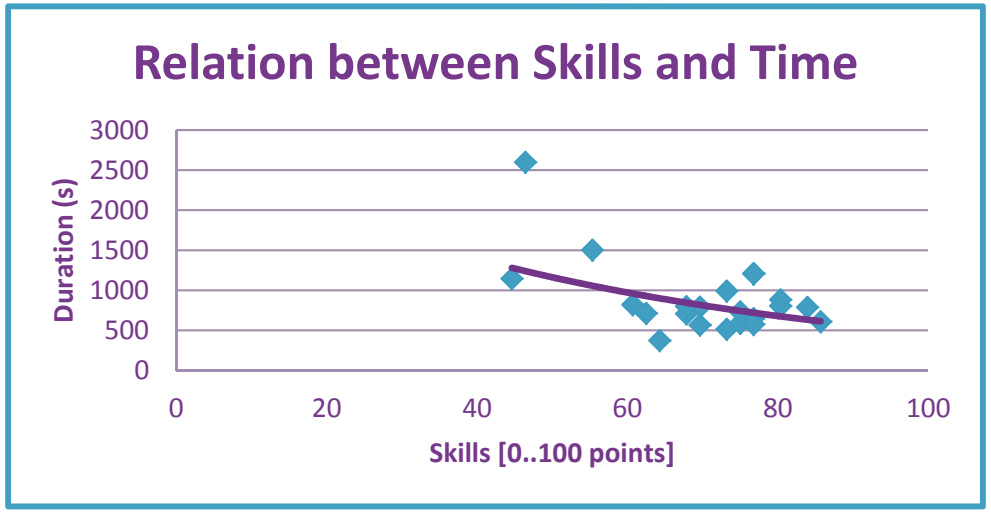
The Study Results (5/6)

- **Duration – a first look**
  - We tested for the **time needed** to complete the task of comprehending a specification. Two different settings:
    (1) we kept the specification the same and varied the question
    (2) we kept the problem description the same, but varied the style of the specification
  - **Results**:
  - Small specifications:
    no correlation between time and correctness
    (weak positive, p=0.13)
  - Larger specifications
    positive correlation



	A1-3/B2	A41	A43	A44	A45	A46
Spec. 1	63.0	34.0	62.5	40.5	110.5	60.0
Spec. 2	31.0	18.5	30.0	22.0	54.5	38.5
Spec. 3	28.0	14.5		17.0		

The Study Results (6/6)

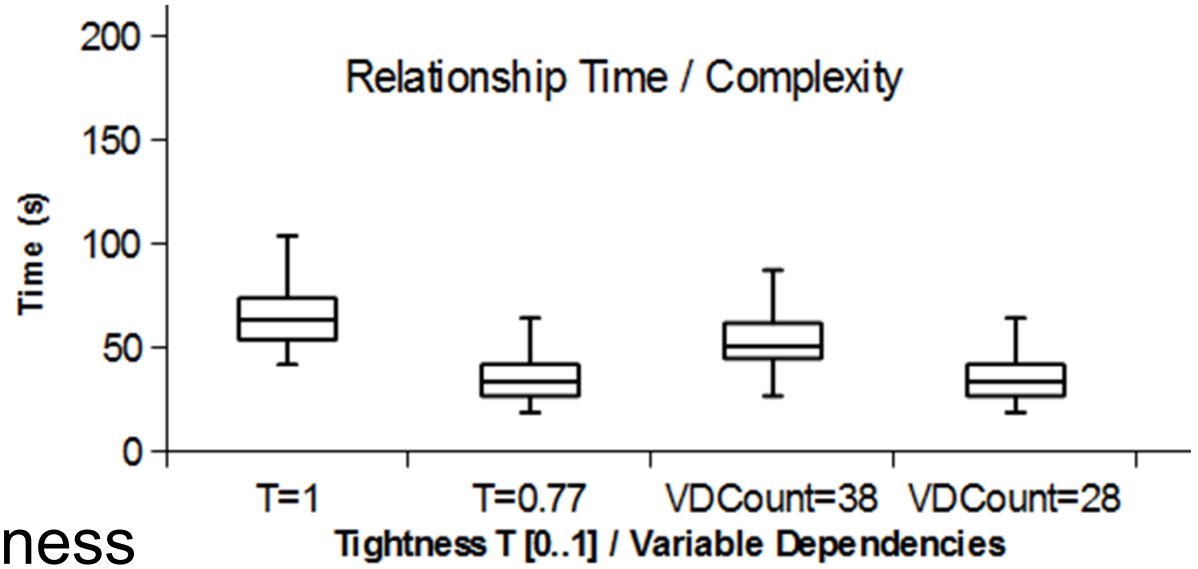


- **Duration – a second look**
  We checked for the relation between **time needed** and **skills** of the developers
  - **Result**:
  - Negative correlation ($\rho_{Pearson}$= -0.57, p<0.007)

We checked for the relation between **complexity** and **time needed**

Results:

- Influence on time
- Influence on correctness



Conclusion

- **The study confirmed by large that common guidelines do support comprehensibility, but**
  - **not** all of them are **valid** (at least in our setting)
  - 3 guidelines could **not be confirmed** totally (“prefer clarity to brevity”, “choose the state so as to minimize the invariant”, “give names to important concepts”)
- **We found another guideline:**

  “When giving a specification of an operation, always make it total!”

- **This study is just a first step in a series of necessary investigations**
  - We think that comprehension time and complexity are related.
  - Complementary guidelines will have to follow

Thank you!

Contact:

Andreas.Bollin@uni-klu.ac.at
D.Rauner-Reithmayer@fh-kaernten.at

References

- [Gravell 91] A. M. Gravell. What is a Good Formal Specification? In Proceedings of the Fifth Annual Z User Meeting on Z User Workshop, pages 137-150, London, UK, 1991. Springer-Verlag.
- [McKenzie 01] D. MacKenzie, Mechanizing Proof: Computing, Risk, and Trust, MIT Press, 2001.
- [Vinter, Loomes, Kornbrot 98] R. Vinter, M. Loomes, and D. Kornbrot. Applying Software Metrics to Formal Specifications: A Cognitive Approach. In 5th International Symposium on Software Metrics, pages 216-223, Bethesda, Maryland, 1998. IEEE Computer Society.