Thinking Formal Methods:

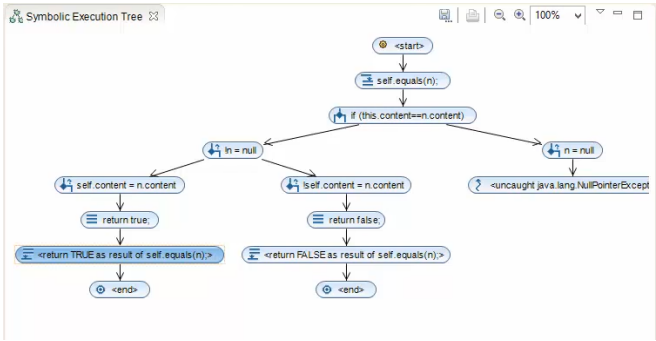
On the Notion of Naturalness in Formal Modeling

Eduard Kamburjan
Sandro Rama Fiorini

University of Oslo
IBM Research Brazil
04.07.2022

Naturalness

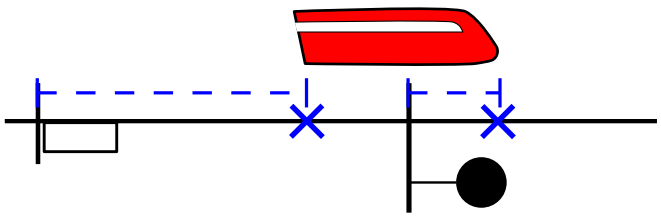
SED: Natural Debugging through Proofs in Terms of Programs



"To improve the efficiency of understanding intermediate proof situation [...] promises considerable gains."

Naturalness

ABS: Natural Formal Modeling through Matching Structures



"We argue that its [ABS's] concurrency and object model are a good match for railway operations, too."

Naturalness

JML: Natural Specification through Tight Integration with Java

```
/*@ ensures \result == n(n(input)); @*/
public Int double_n(Int input) { ... }
public Int /*@ \strictly_pure@*/ n(Int input) { ... }
```

Naturalness

JML: Natural Specification through Tight Integration with Java

```
/*@ ensures \result == n(n(input)); @*/
public Int double_n(Int input) { ... }
public Int /*@ \strictly_pure@*/ n(Int input) { ... }
```

Towards a Notion of Naturalness

In many contexts we argue that a given system or model is *close* to the system or thing it is used for.

Naturalness

Towards a Notion of Naturalness

In many contexts we argue that a given system or model is *close* to the system or thing it is used for.

Naturalness

Towards a Notion of Naturalness

In many contexts we argue that a given system or model is *close* to the system or thing it is used for.

Towards a Notion of Naturalness in Formal Modeling?

- Scenario: A formal model of some system, developed by three persons
  - A technical expert
    (knows formalism, no knowledge about domain)
  - A domain expert
    (knows domain, no knowledge about formalism)
  - A poor formal methods expert (knows both)
- **What does it mean for the model to be natural?**

Models

“ [a model represents] a system in terms of mathematical objects that reflect its observed properties. [...] Modelling usually involves the process of abstraction, i.e., simplifying the description of the system, while preserving only a limited number of the original details. ” *[Doron Peled, 2001]*

Models

```
@XmlRootElement(name = "Car")
public class Car {
  private int nrAxels;  private Pair<Integer, Integer> pos;
  ...
  public Car() { ... }
  public Car(int nrAxels, String name,
    Pair<Integer, Integer> pos,
    Pair<Integer, Integer> v) { ... }
  @XmlAttribute
  public int getNrAxels(){ return nrAxels; }
  public void setNrAxels(int nrAxels){this.nrAxels = nrAxels;}
  ...
}
```

Abstraction alone is not enough to explain why models are developed the way they are in practice.

Models

Three Features of Models [Herbert Stachowiak, 1972]

A model . . .

Mapping Ft. . . . stands for some original.

Reduction Ft. . . . does not cover all attributes of the original.

Pragmatic Ft. . . . stands for its original only for some purpose.

Models

Three Features of Models [Herbert Stachowiak, 1972]

A formal model . . .

Mapping Ft. . . . stands for some original.

Reduction Ft. . . . does not cover all attributes of the original.

Pragmatic Ft. . . . stands for its original only for some purpose.

Formal Ft. . . . is represented in some mathematical formalism

Models

Three Features of Models [Herbert Stachowiak, 1972]

A formal model . . .

Mapping Ft. . . . stands for some original.

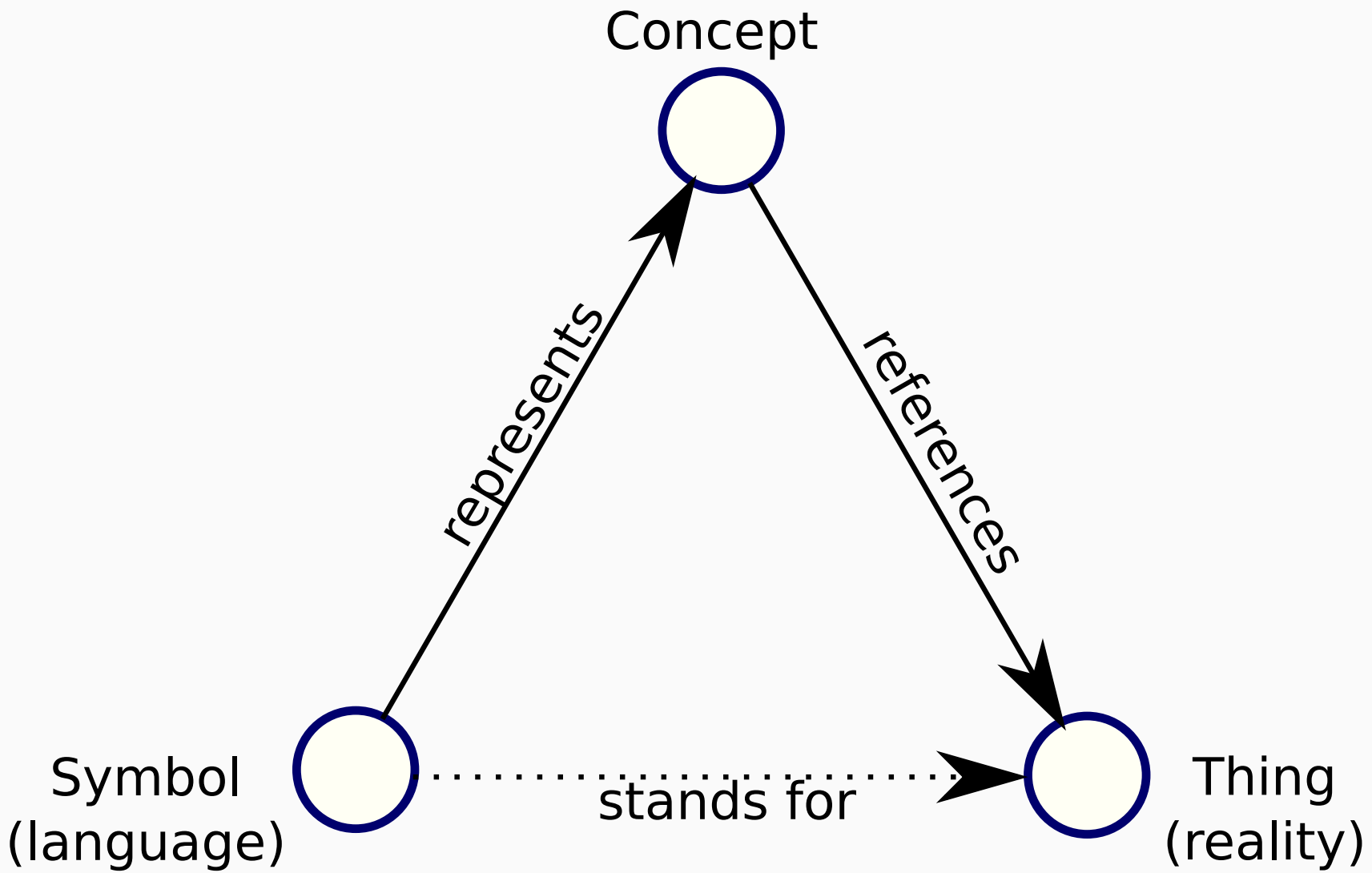
Reduction Ft. . . . does not cover all attributes of the original.

Pragmatic Ft. . . . stands for its original only for some purpose.

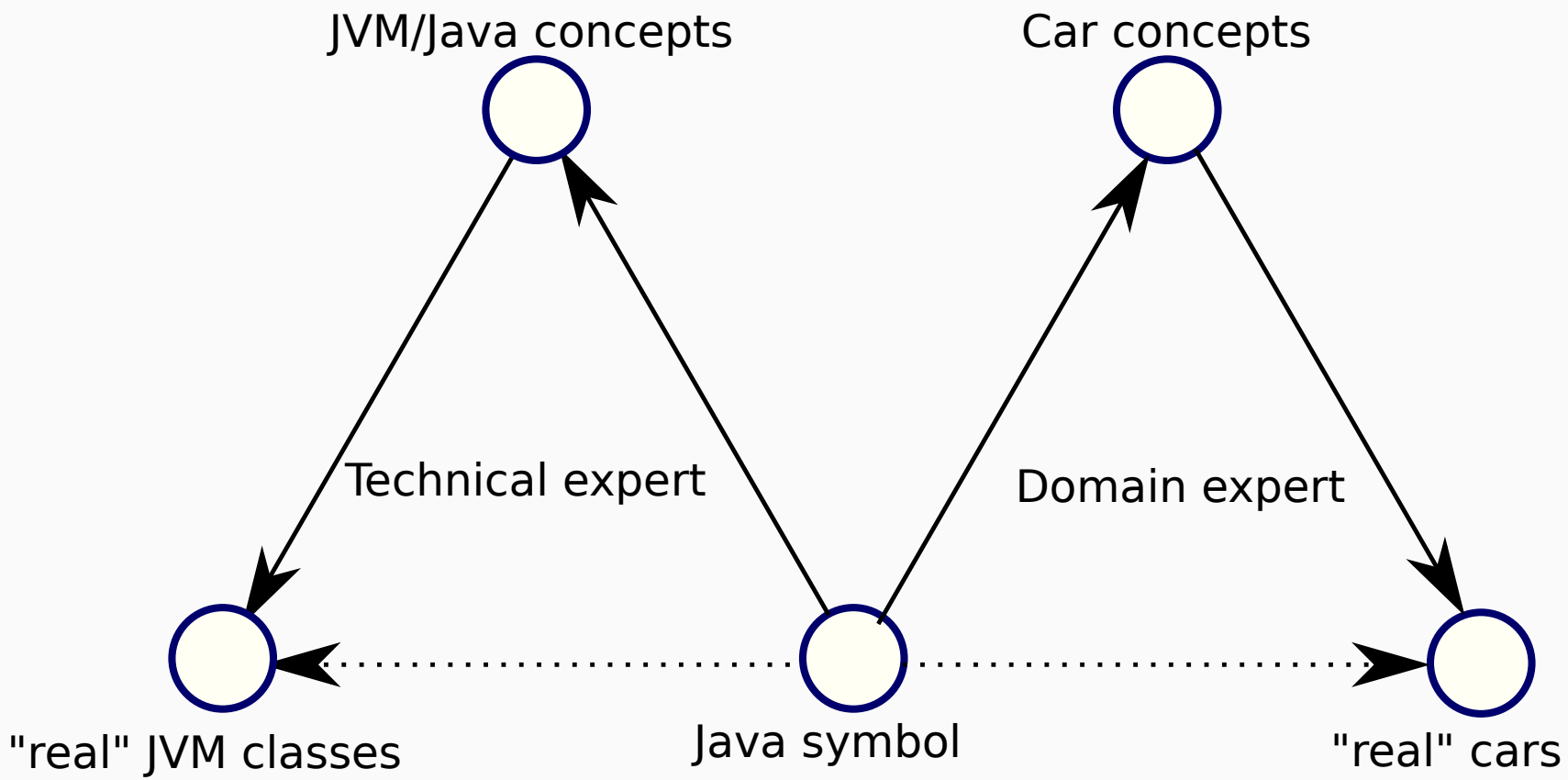
Formal Ft. . . . is represented in some mathematical formalism

What does it mean to stand for something?

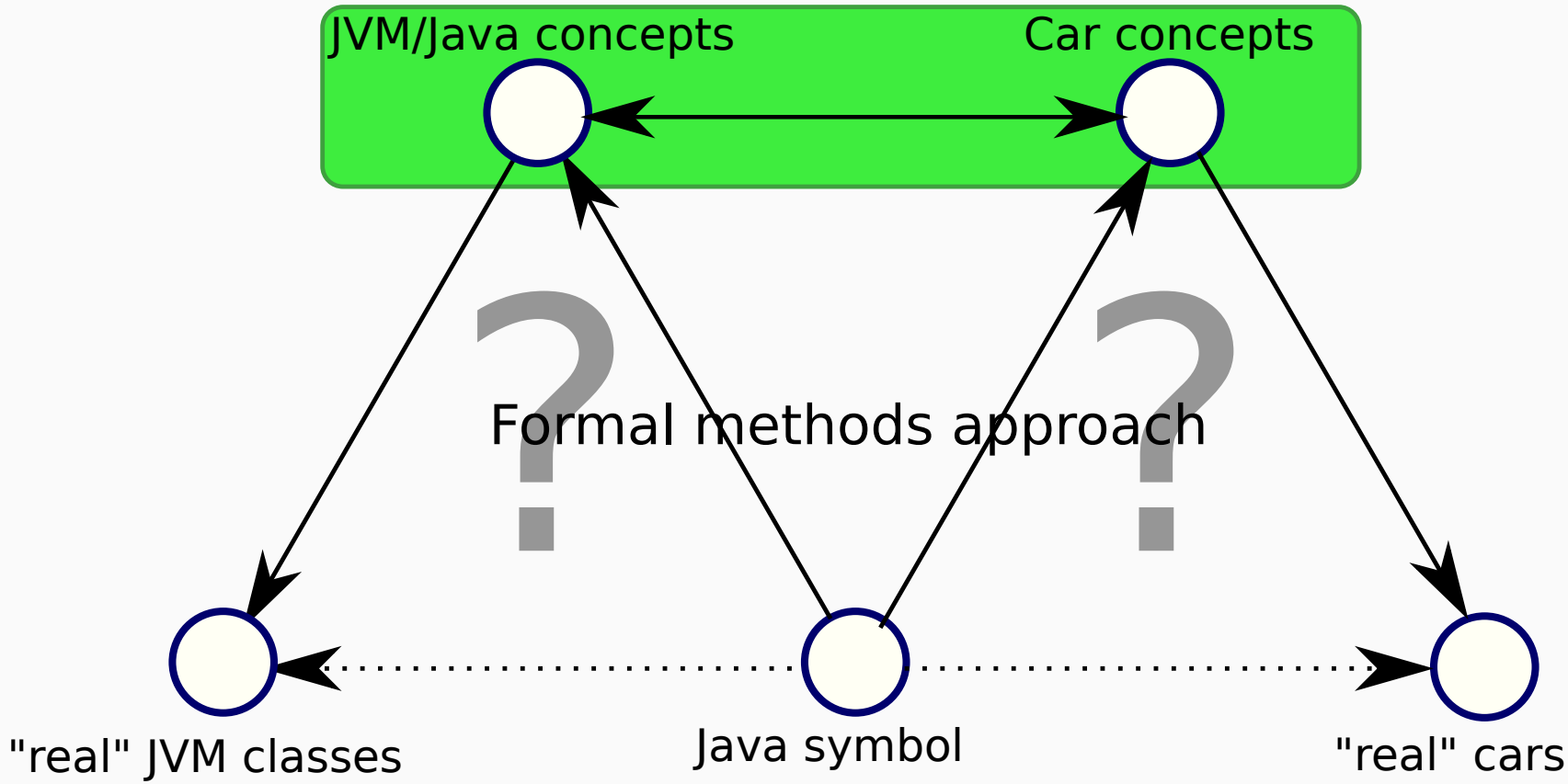
Signs [Charles Sanders Peirce, 1839-1914]



Signs [Charles Sanders Peirce, 1839-1914]



Signs [Charles Sanders Peirce, 1839-1914]



How to reconcile and compare the concepts of two signification processes within one agent?

Metaphors

> *"Metaphors [are] mappings across conceptual domains that preserve the cognitive topology [...] of the source domain, in a way consistent with [...] the target domain.* "
>
> *[George Lakoff, 1993]*

Formal models should be metaphors.

Metaphors

> *"Metaphors [are] mappings across conceptual domains that preserve the cognitive topology [...] of the source domain, in a way consistent with [...] the target domain.* *[George Lakoff, 1993]* "

Formal models should be metaphors.

Theories of Metaphors [Indurkhya, 1992]

Comparative Metaphors emphasize preexisting similarities.

Interactive Metaphors create new similarities.

Metaphors

> *"Metaphors [are] mappings across conceptual domains that preserve the cognitive topology [...] of the source domain, in a way consistent with [...] the target domain.* [George Lakoff, 1993] "

Formal models should be metaphors.

Theories of Metaphors [Indurkhya, 1992]

Comparative Metaphors emphasize preexisting similarities.

Interactive Metaphors create new similarities.

Metaphors in Computer Science

From Domain Use domain to explain formal artifact ("*Stack*")

To Domain Use formal artifact to detect structures in domain

Signification in Formal Models

Sequential Signification

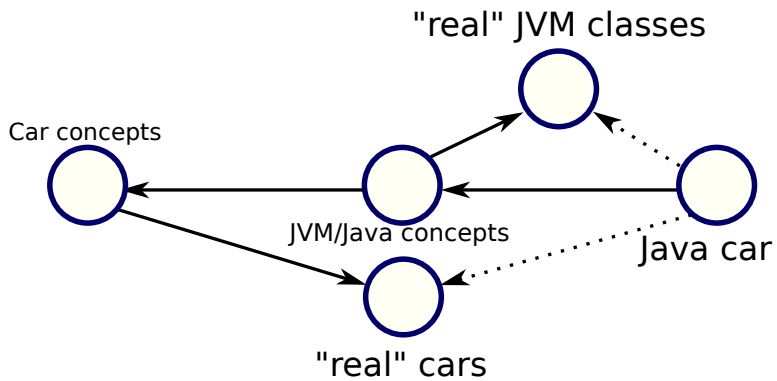
For the formal method expert, both signification processes happen weakly sequentially: first the code is understood, then it is interpreted in the domain.

Signification in Formal Models

Sequential Signification

For the formal method expert, both signification processes happen weakly sequentially: first the code is understood, then it is interpreted in the domain.

Relation of the two concepts for FM is a transformation sequence

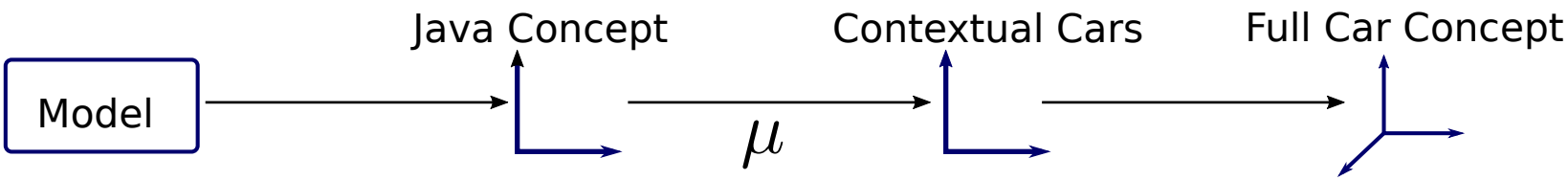


Signification in Formal Models

Sequential Signification

For the formal method expert, both signification processes happen weakly sequentially: first the code is understood, then it is interpreted in the domain.

Relation of the two concepts for FM is a transformation sequence

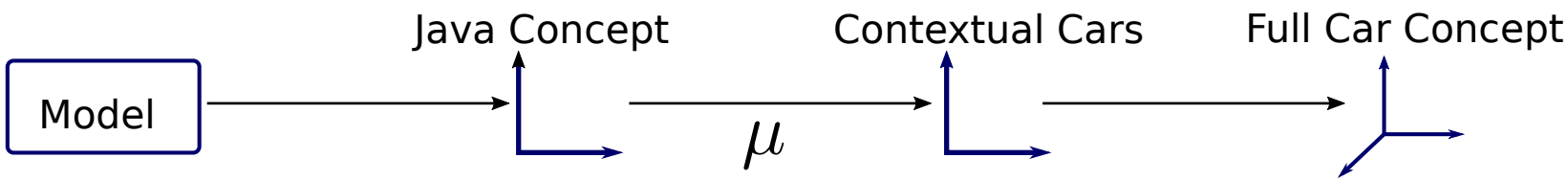


Signification in Formal Models

Sequential Signification

For the formal method expert, both signification processes happen weakly sequentially: first the code is understood, then it is interpreted in the domain.

Relation of the two concepts for FM is a transformation sequence



A metaphor is a mapping μ between concepts.

A model is natural if its internal mapping μ is a metaphor with low *cognitive complexity*.

Consequences for User Studies

The SED User Study

"To improve the efficiency of understanding intermediate proof situation [...] promises considerable gains in the overall user time spend [...]"

- Quantitative study for efficiency
- Qualitative questionnaire for understanding

Consequences for User Studies

The SED User Study

"To improve the efficiency of understanding intermediate proof situation [...] promises considerable gains in the overall user time spend [...]"

- Quantitative study for efficiency
- Qualitative questionnaire for understanding

Beyond Efficiency

- User studies in FM tend to focus on quantitative aspects
- Cognitive hypotheses are rarely explicitly formulated

Conclusion

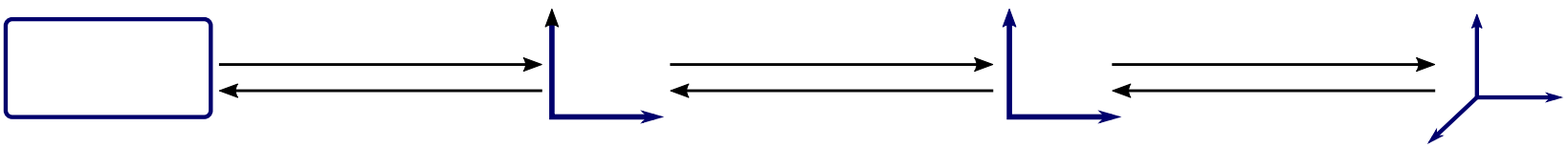
We can have a cognitive theory of formal language design

Conclusion

We can have a cognitive theory of formal language design

Presented

Natural formal models as metaphors with low cognitive complexity

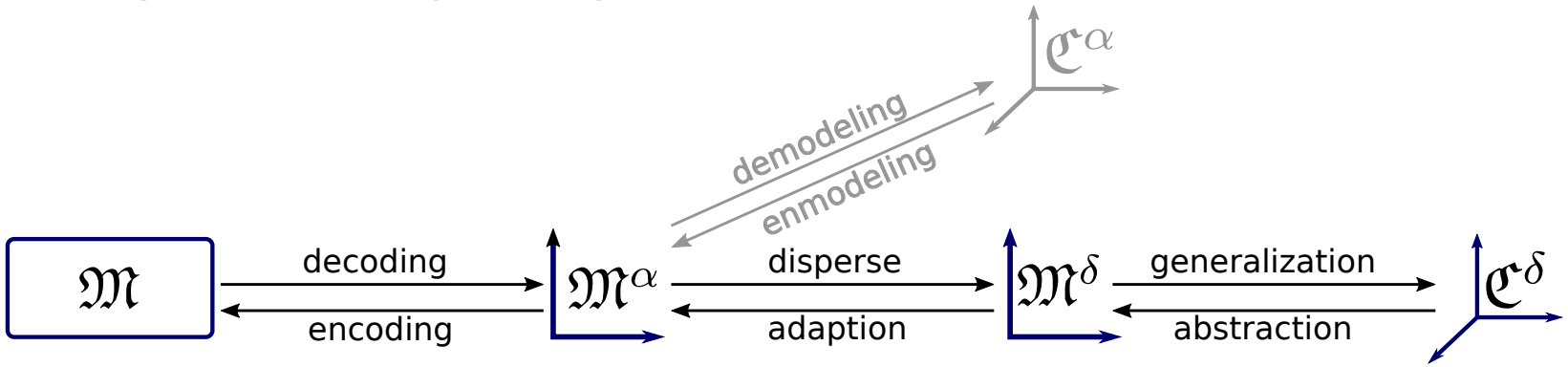


Conclusion

We can have a cognitive theory of formal language design

Not Presented

Perception, conceptual spaces, . . .



Conclusion

We can have a cognitive theory of formal language design

Presented

Natural formal models as metaphors with low cognitive complexity.

- Cognitive linguistics for better arguments in modelling?
- Cognitive linguistics for better design of studies?
- Cognitive linguistics for better design of languages?

Conclusion

We can have a cognitive theory of formal language design

Presented

Natural formal models as metaphors with low cognitive complexity.

- Cognitive linguistics for better arguments in modelling?
- Cognitive linguistics for better design of studies?
- Cognitive linguistics for better design of languages?

Thank you for your attention