Managing Design-Time Uncertainty

Michalis Famelis, Marsha Chechik

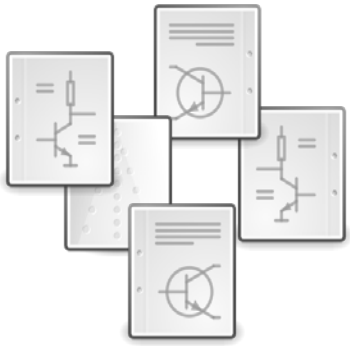
MODELS 2017

Austin TX, USA

Université de Montréal

UNIVERSITY OF TORONTO

Uncertainty in Software Development

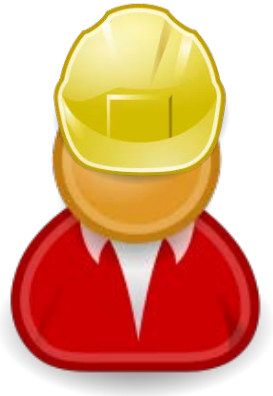


Many design alternatives

Incomplete information

Conflicting stakeholder opinions

Uncertainty during the design of software.



Uncertainty in:

Environment

What conditions will the system operate in?

Main concern:
adapting to change

Mitigated by uncertainty-aware **software**

Design-time

What should the system be like?

Main concern:
making design decisions

Mitigated by uncertainty-aware **software development methodology**

Management of Design-Time Uncertainty

Key development goals:


Quality

Speed (time to market)

What can developers do?

Make a **provisional** decision and "run with it"

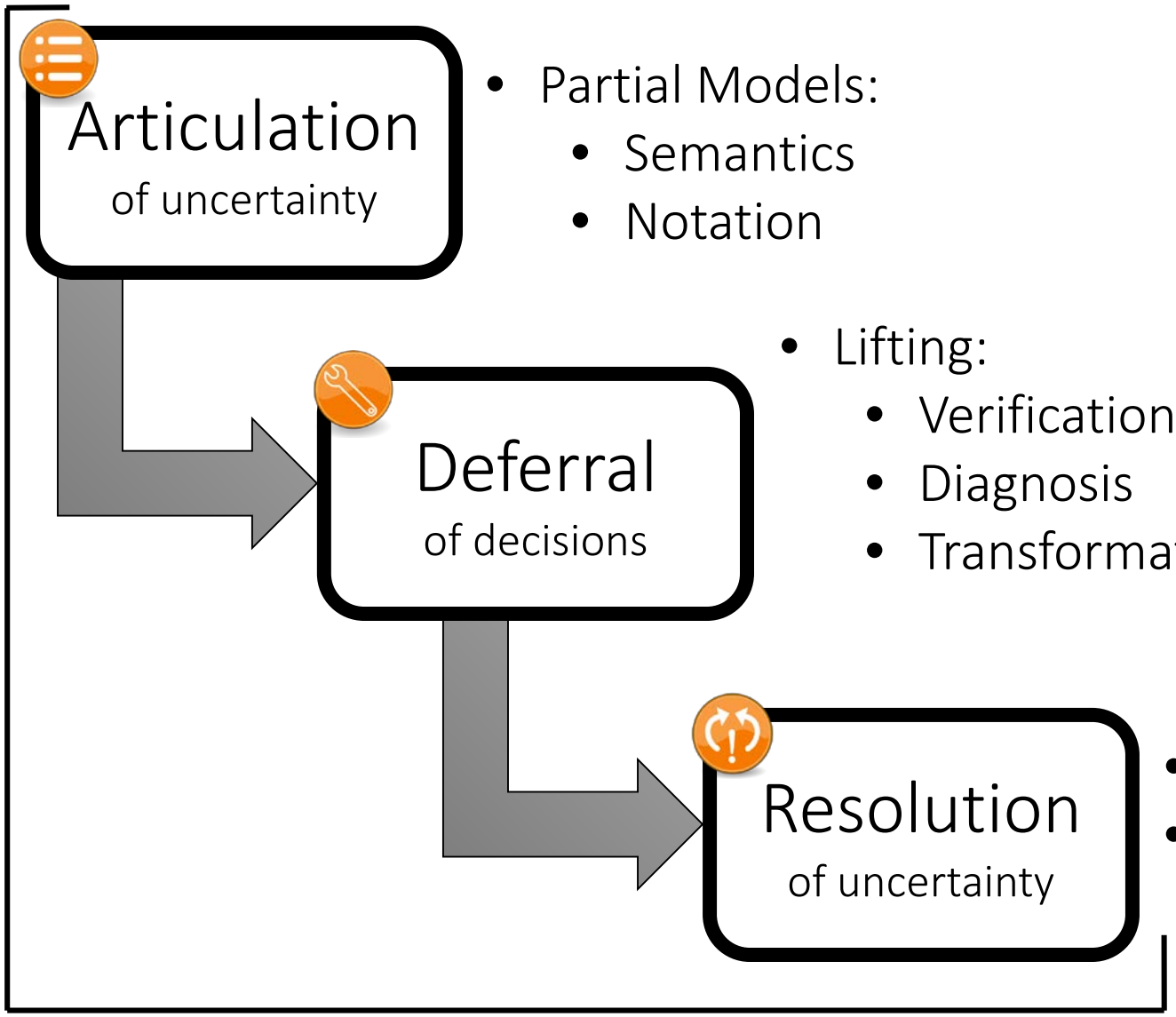

Wait until uncertainty gets resolved


Fork and maintain a set of solutions


We propose:


Defer resolution of uncertainty but incorporate uncertainty handling into the development process to allow progress

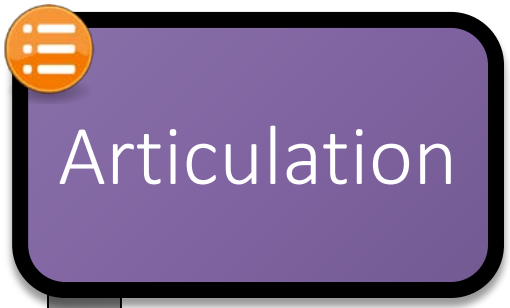
Outline



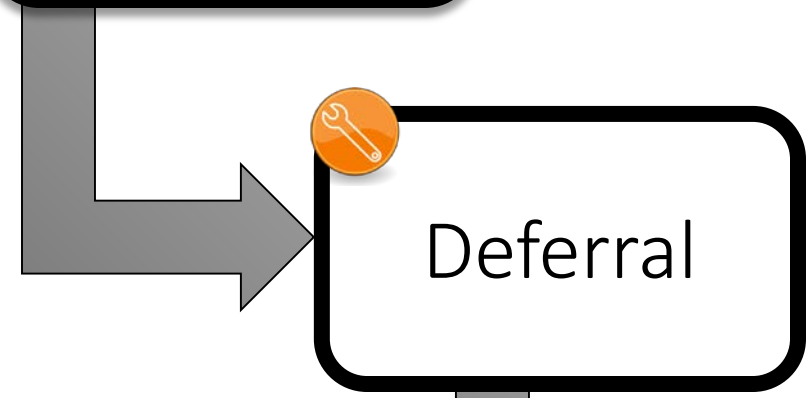
- Partial Models:
  - Semantics
  - Notation
- Lifting:
  - Verification
  - Diagnosis
  - Transformation
- Refinement
- Decision-making

- Methodology and Tool Support
- Worked-out Examples
- Conclusion, Future Work

Outline



- **Partial Models:**
  - **Semantics**
  - **Notation**



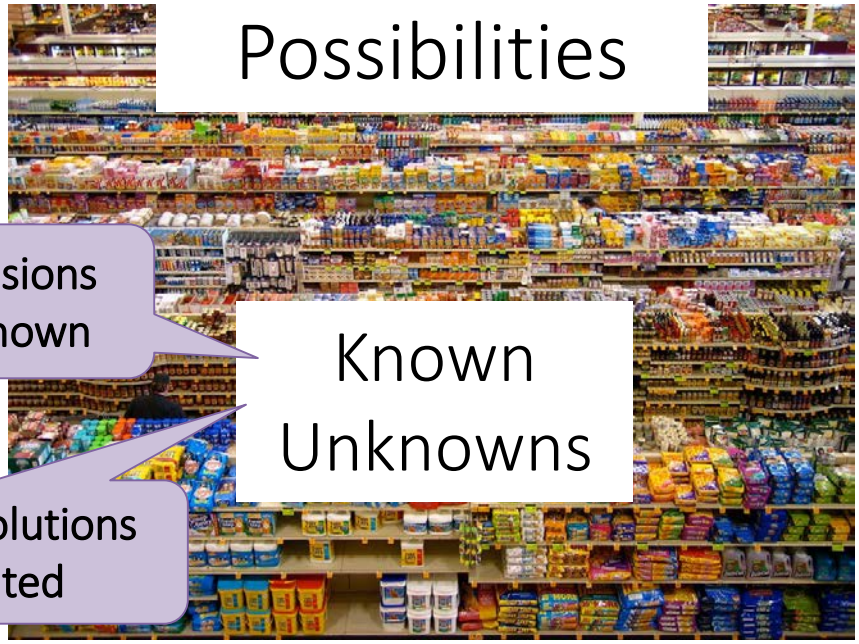
- Lifting:
  - Verification
  - Diagnosis
  - Transformation

- Refinement
- Decision-making

- Methodology and Tool Support
- Worked-out Examples
- Conclusion, Future Work

Design-time Uncertainty

Possibilities



Design decisions assumed known

Alternative solutions assumed elicited

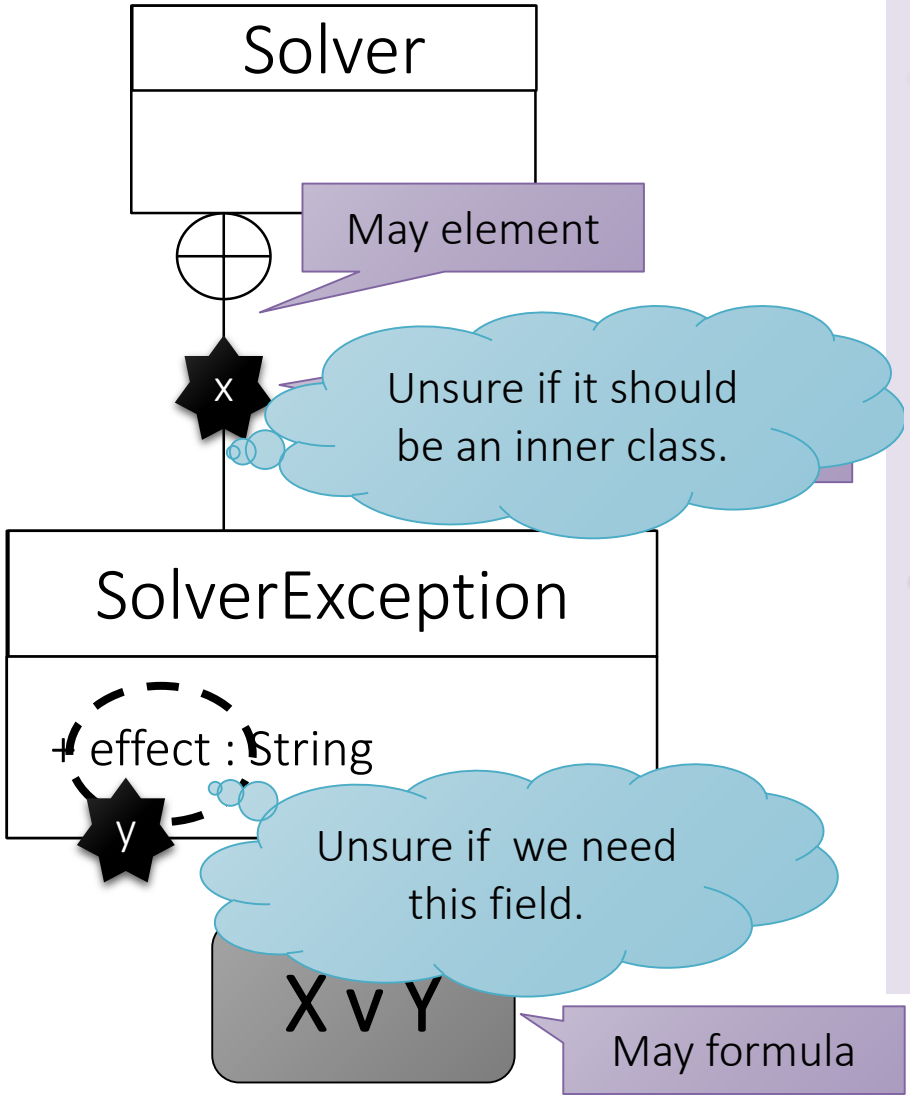
Known Knowns

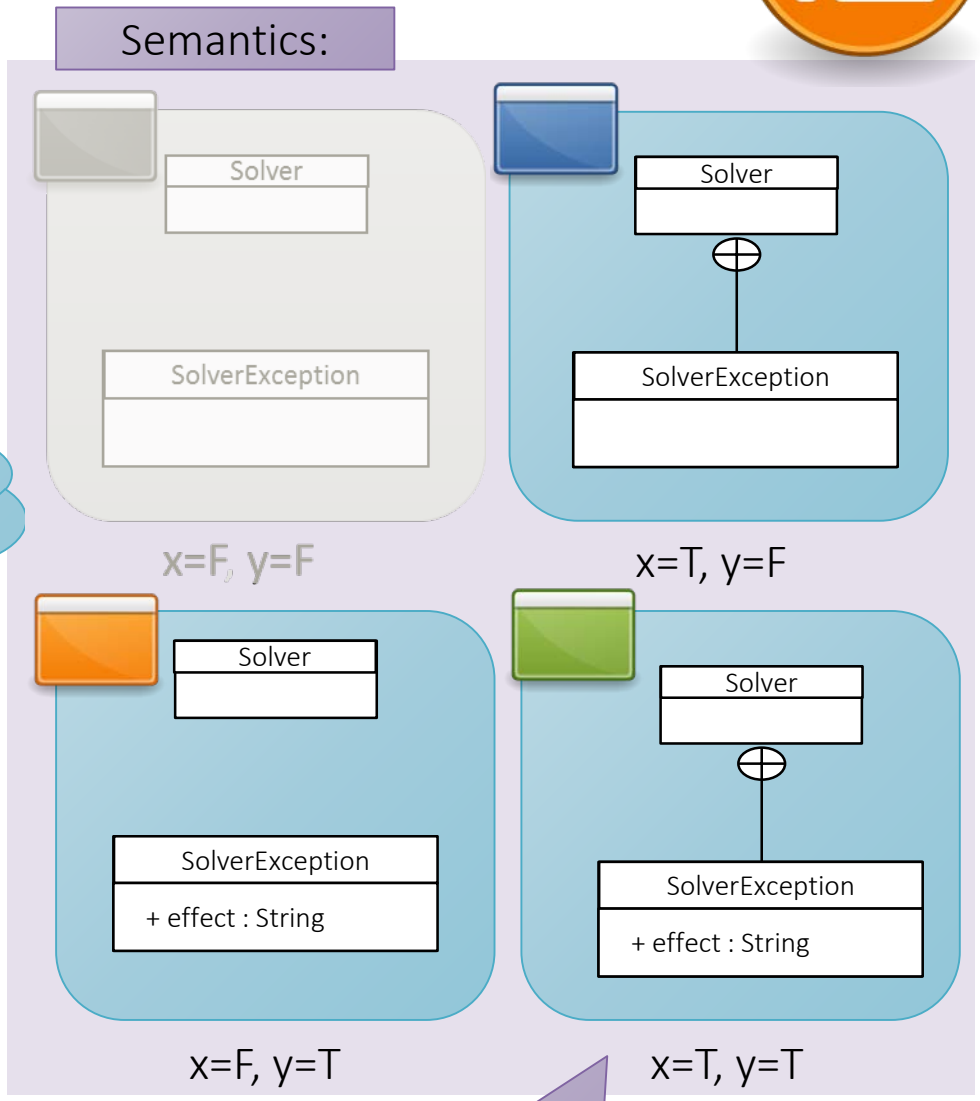
Known Unknowns

US Secretary of Defense, Donald Rumsfeld discusses Iraqi WMDs, February 12, 2002

Unknown Unknowns

Representing Uncertainty with Partial Models

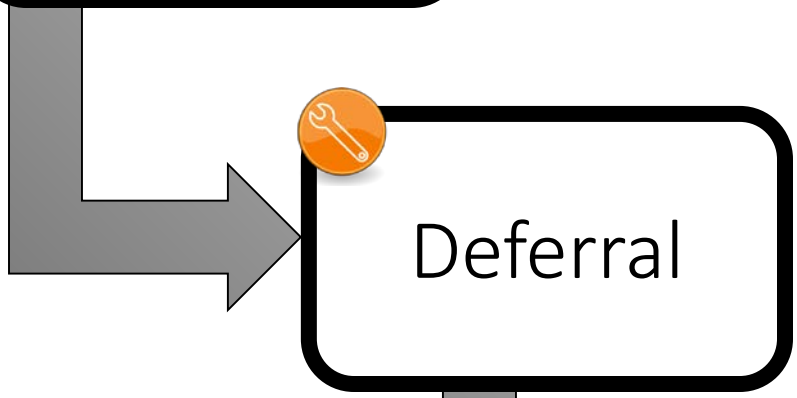




[ICSE'12] *Partial Models: Towards Modeling and Reasoning with Uncertainty,* M. Famelis, R. Salay and M. Chechik

Outline

- Partial Models:
  - Semantics
  - Notation

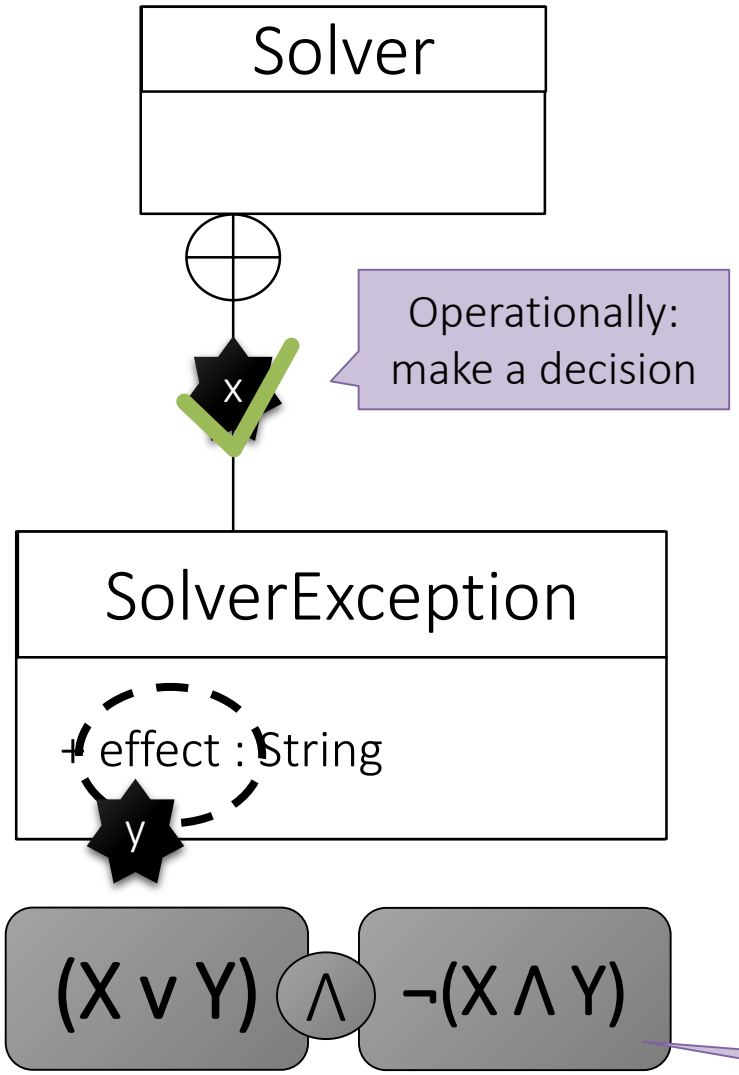


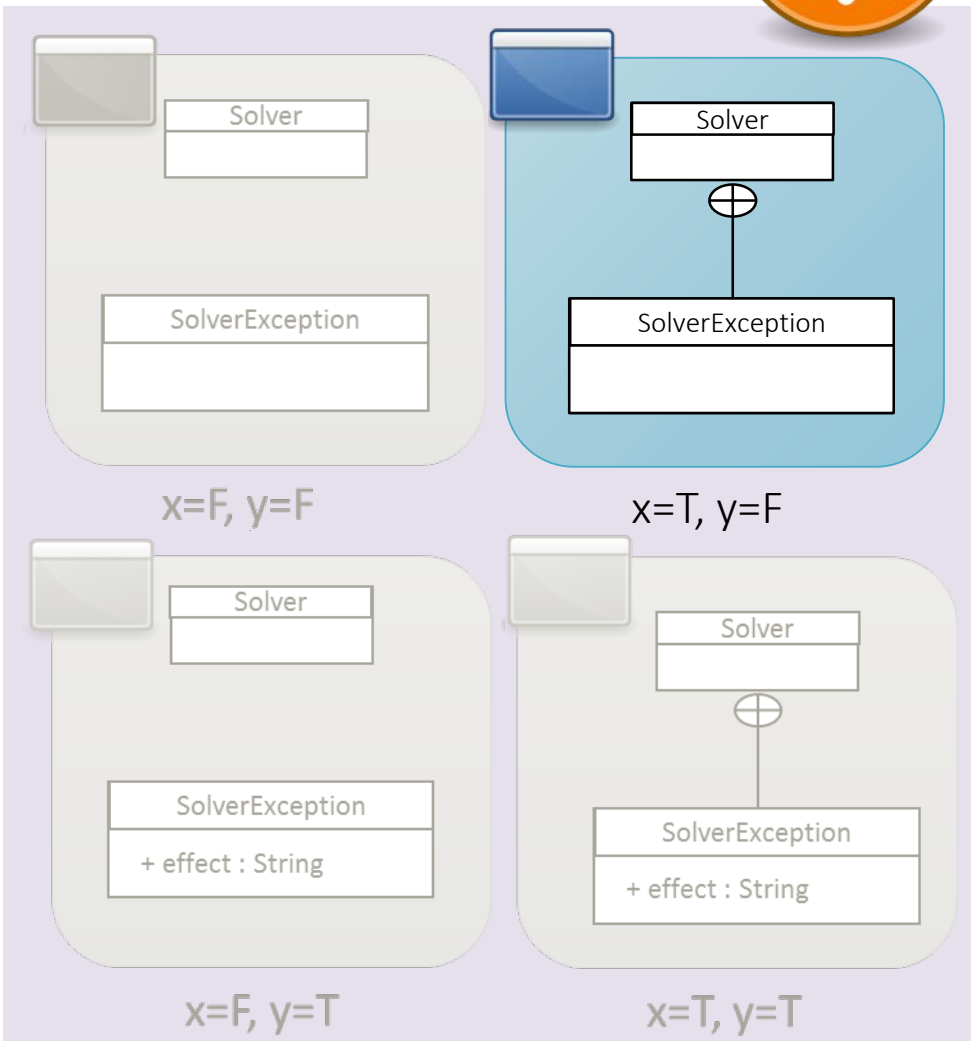
- Lifting:
  - Verification
  - Diagnosis
  - Transformation

- **Refinement**
- **Decision-making**

- Methodology and Tool Support
- Worked-out Examples
- Conclusion, Future Work

Refinement: Reduce the Set

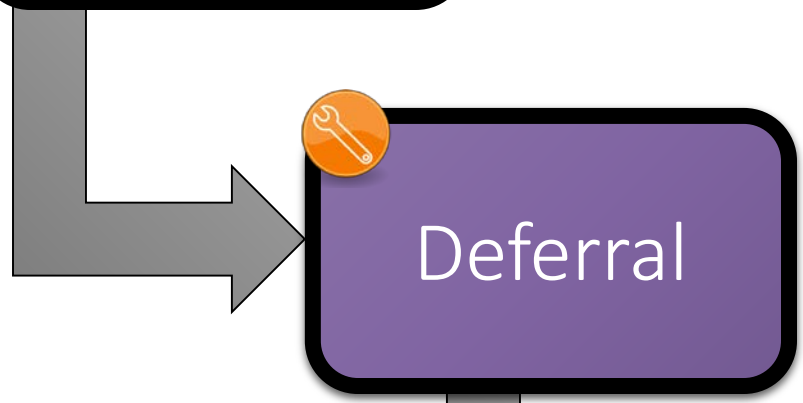




[ICSE'12] *Partial Models: Towards Modeling and Reasoning with Uncertainty,* M. Famelis, R. Salay and M. Chechik

Outline

- Partial Models:
  - Semantics
  - Notation

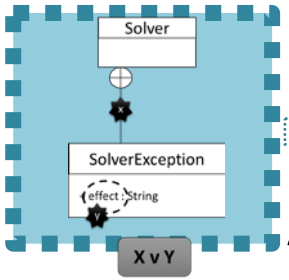


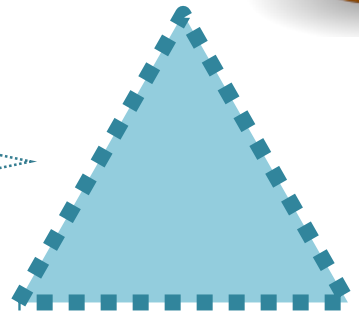
- **Lifting:**
  - **Verification**
  - **Diagnosis**
  - **Transformation**

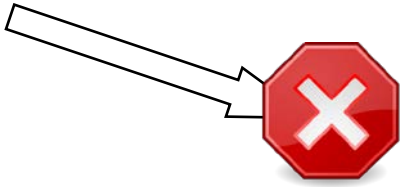
- Refinement
- Decision-making

- Methodology and Tool Support
- Worked-out Examples
- Conclusion, Future Work

Deferring Uncertainty Resolution

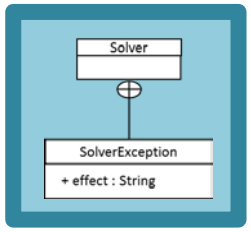


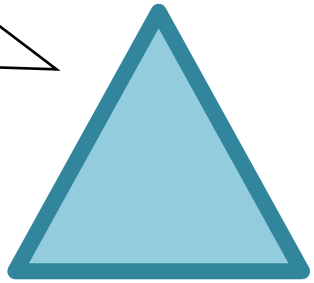




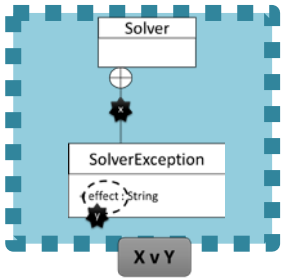
DOES NOT COMPUTE
MAKE DECISIONS FIRST

Automated Procedure

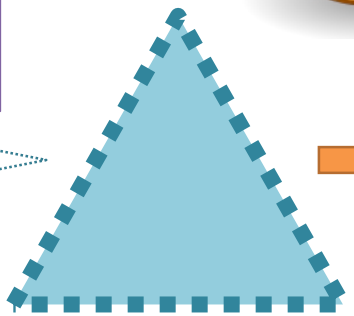


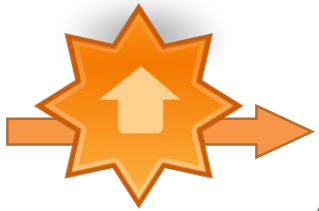


Deferral Through "Lifting"

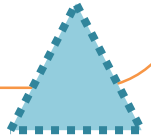


Verification: thorough checking.
Transformations: preservation of set of concretizations.

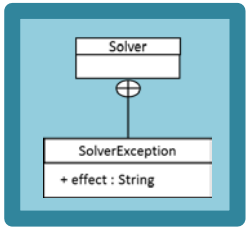




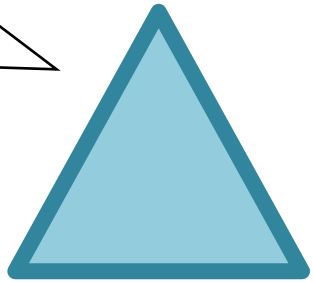
Development can continue with



Automated Procedure



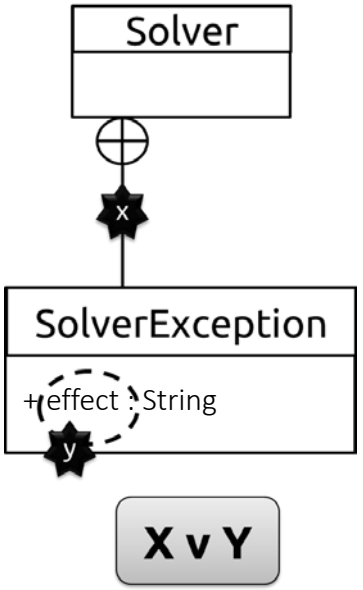
Adapting automation to work with partial models

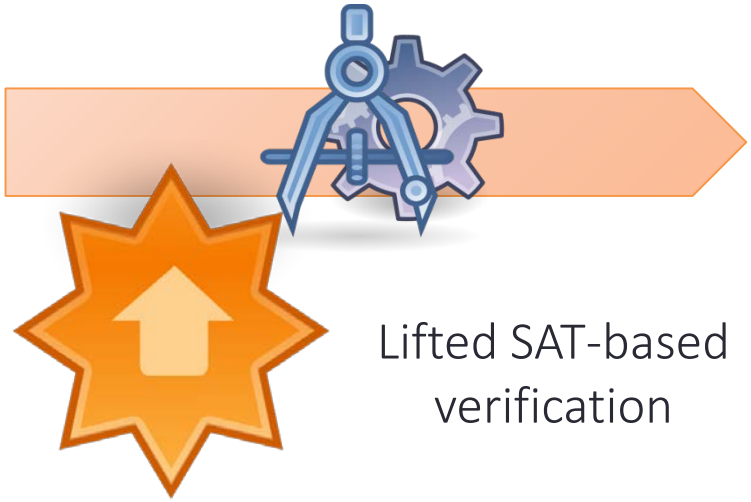


Lifting Verification

Example property:

"Every inner class has at least one attribute"





Lifted SAT-based verification

Property holds for…

…all concretizations

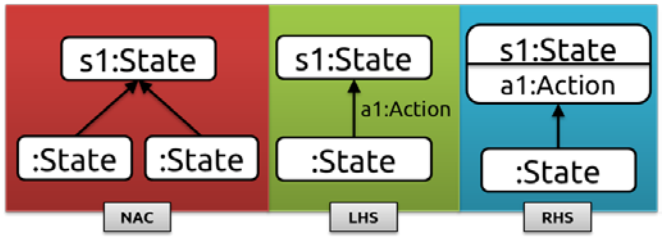
…some but not all

…none

- Applies directly to the partial model
- Does **not** enumerate concretizations
- Computes result using three-valued logic

[ICSE'12] *Partial Models: Towards Modeling and Reasoning with Uncertainty,* M. Famelis, R. Salay and M. Chechik

Lifting Transformations



? Can users initiate seeding? H

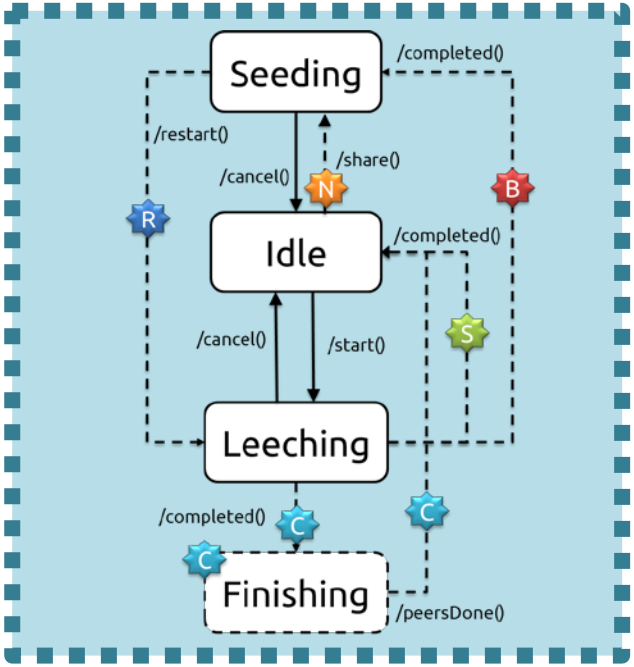
? Can users restart downloads? R

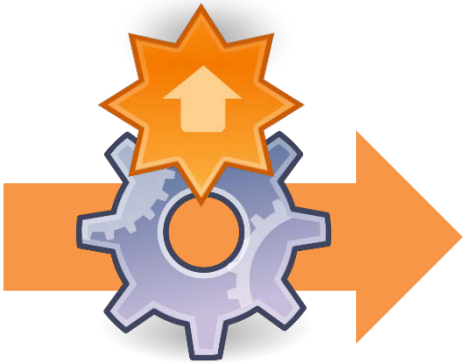
? What happens when a download is completed?

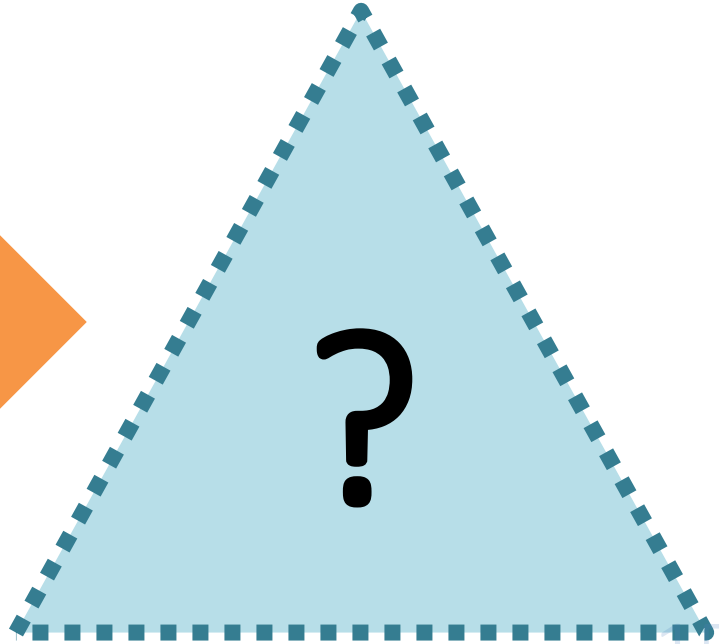
"Benevolent" B

"Selfish" S

"Compromise" C

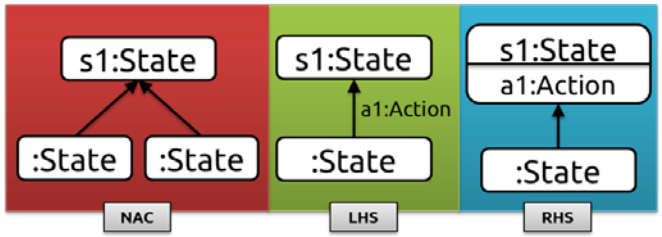






[MODELS 2013] *Transformation of Models Containing Uncertainty,* M. Famelis, R. Salay, A. Di Sandro and M. Chechik

Lifting Transformations



? Can users initiate seeding? H

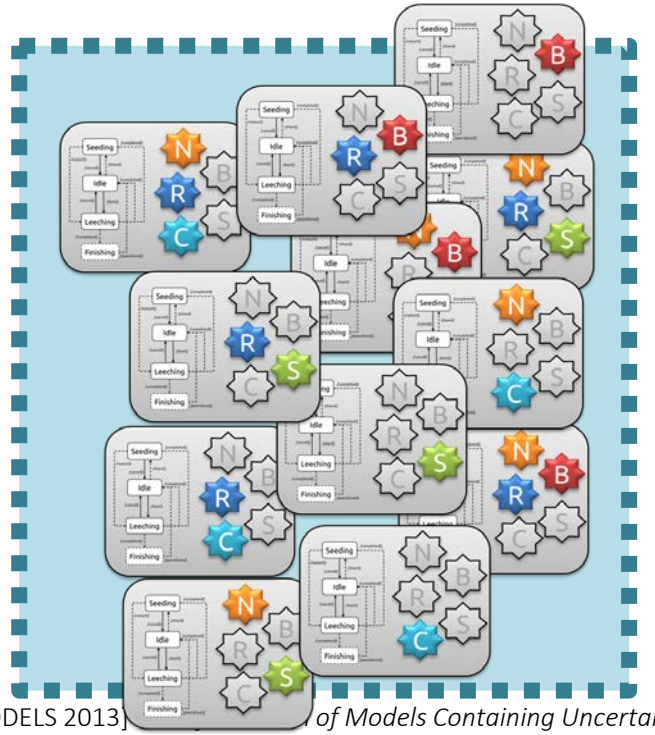
? Can users restart downloads? R

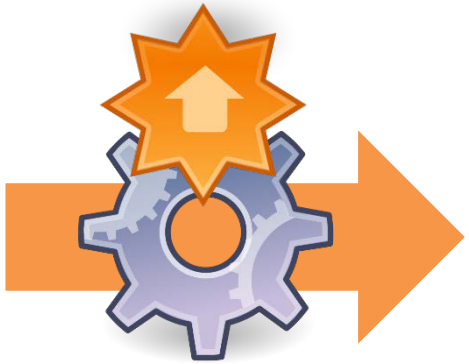
? What happens when a download is completed?

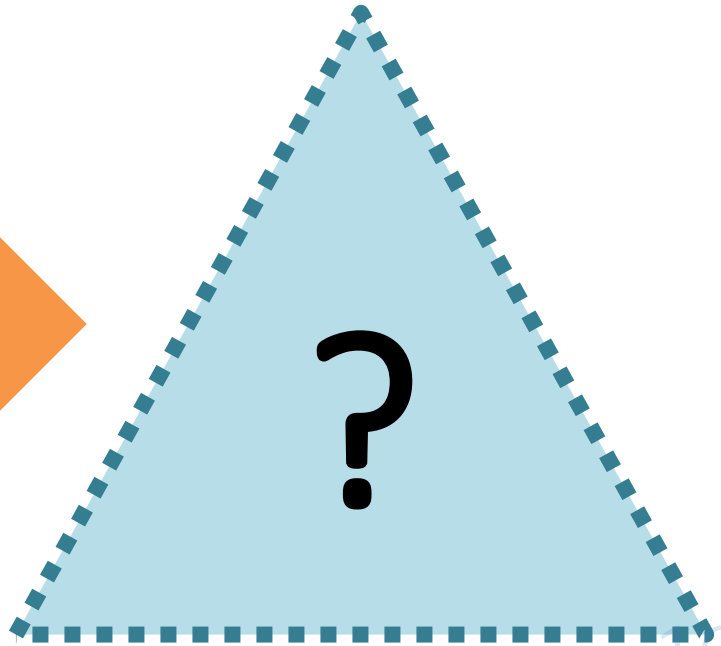
"Benevolent" B

"Selfish" S

"Compromise" C

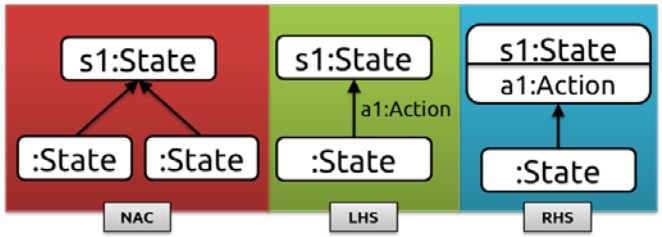






[MODELS 2013] *of Models Containing Uncertainty,* M. Famelis, R. Salay, A. Di Sandro and M. Chechik

Lifting Transformations



? Can users initiate seeding? H

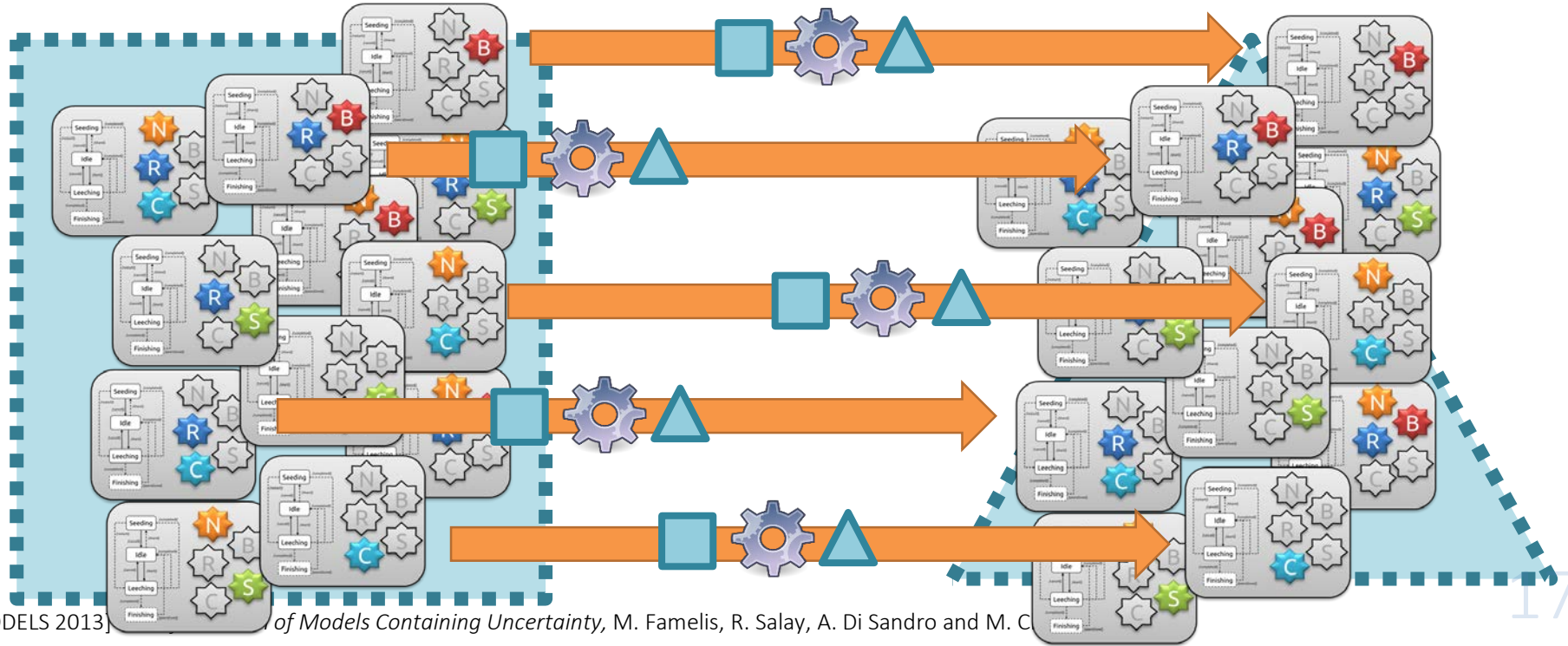
? Can users restart downloads? R

? What happens when a download is completed?

"Benevolent" B

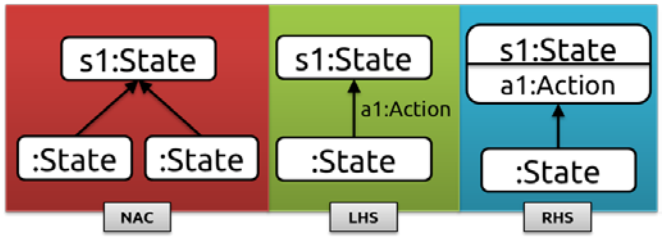
"Selfish" S

"Compromise" C



[MODELS 2013] *of Models Containing Uncertainty,* M. Famelis, R. Salay, A. Di Sandro and M. C

Lifting Transformations



Design decisions not affected

Neither is the transformation!

? Can users initiate seeding? H

? Can users restart downloads? R

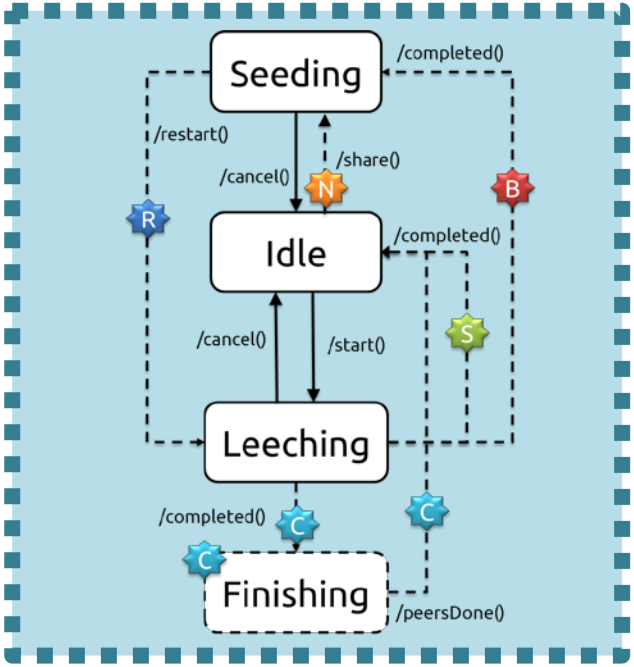
? What happens when a download is completed?

"Benevolent" B

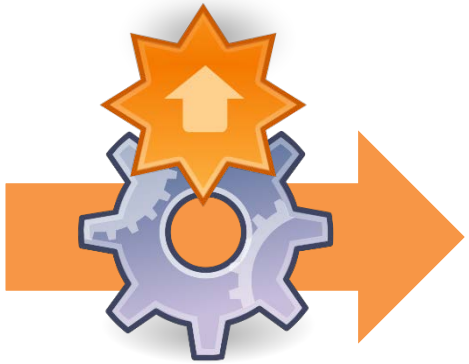
"Selfish" S

"Compromise" C

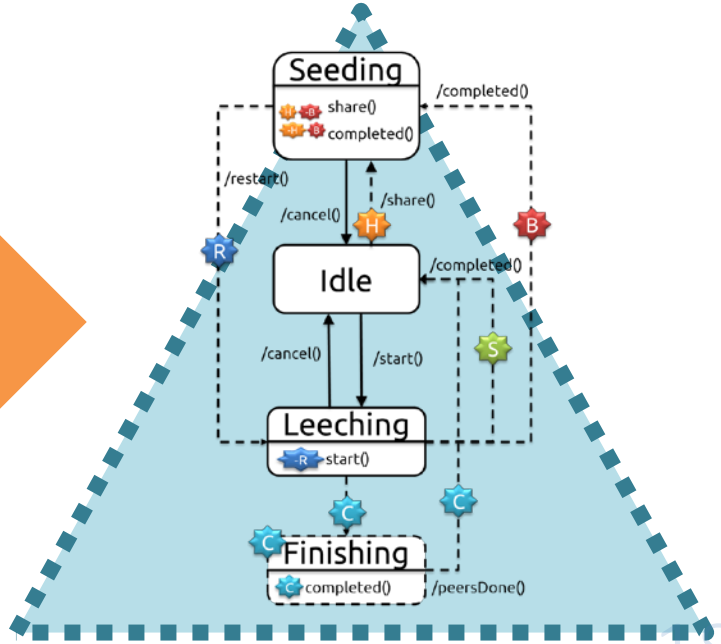
Step 1:
Determine applicability



Step 2:
Transform graph

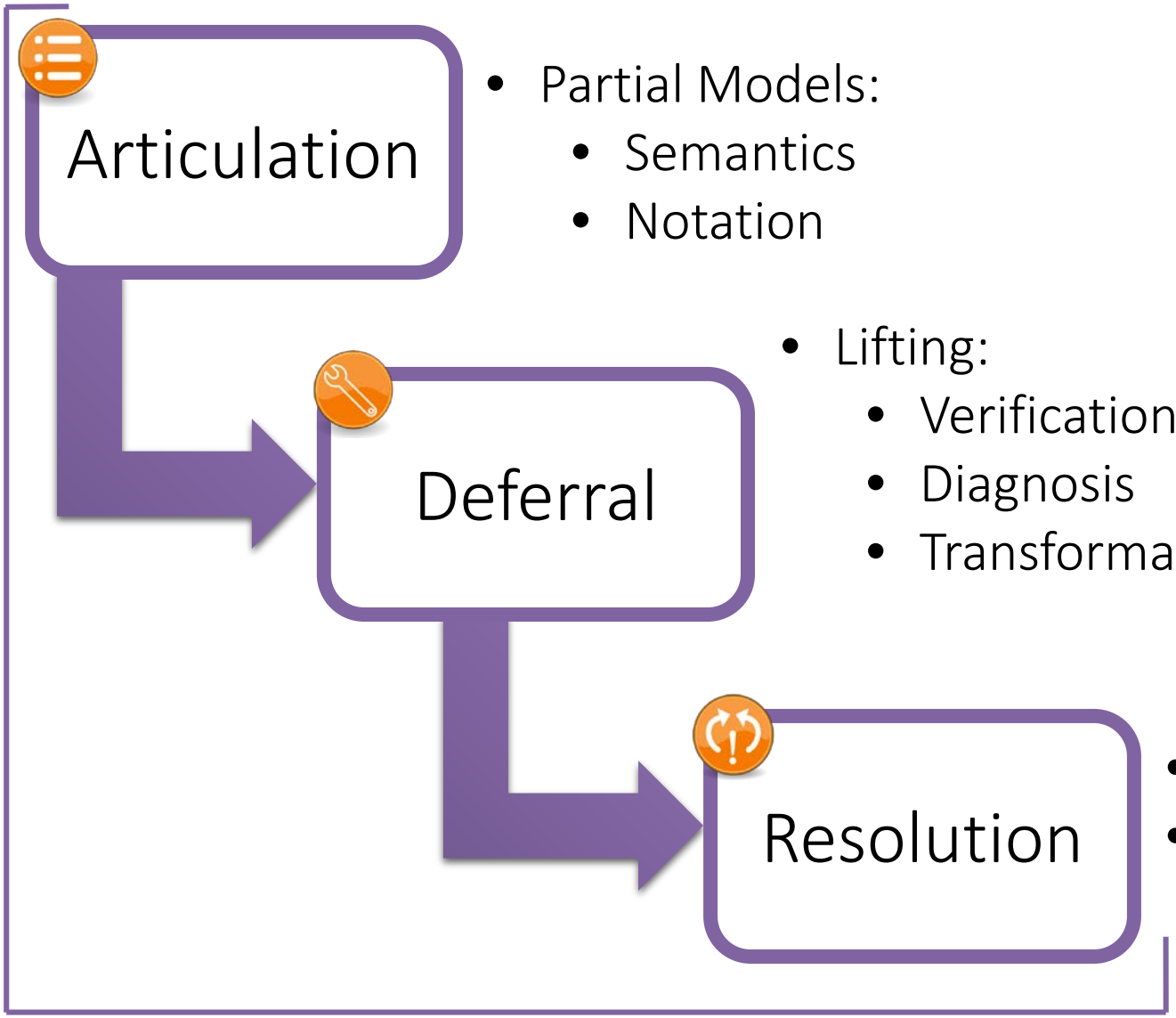


Step 3:
Transform constraints



[MODELS 2013] *Transformation of Models Containing Uncertainty,* M. Famelis, R. Salay, A. Di Sandro and M. Chechik

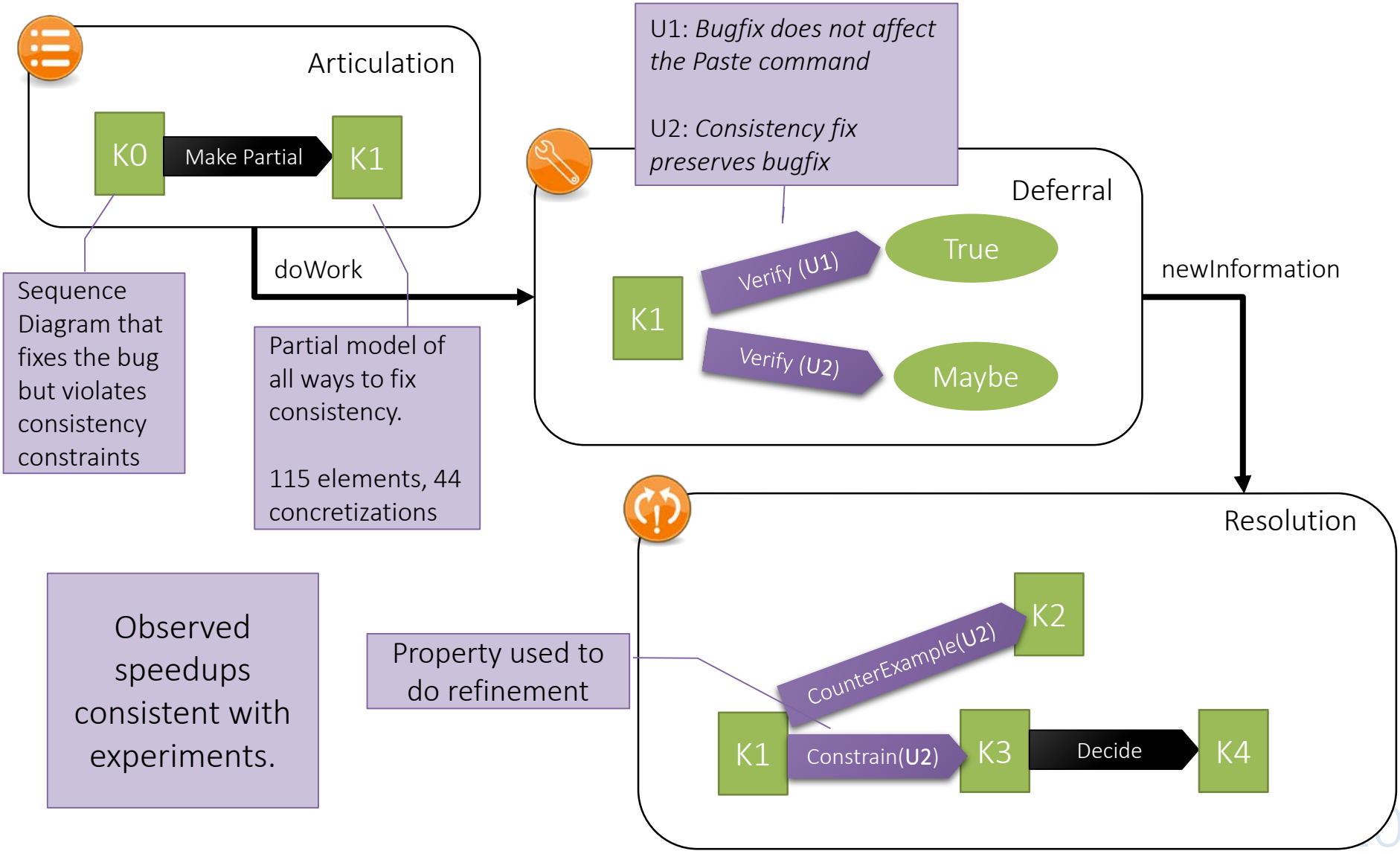
Outline



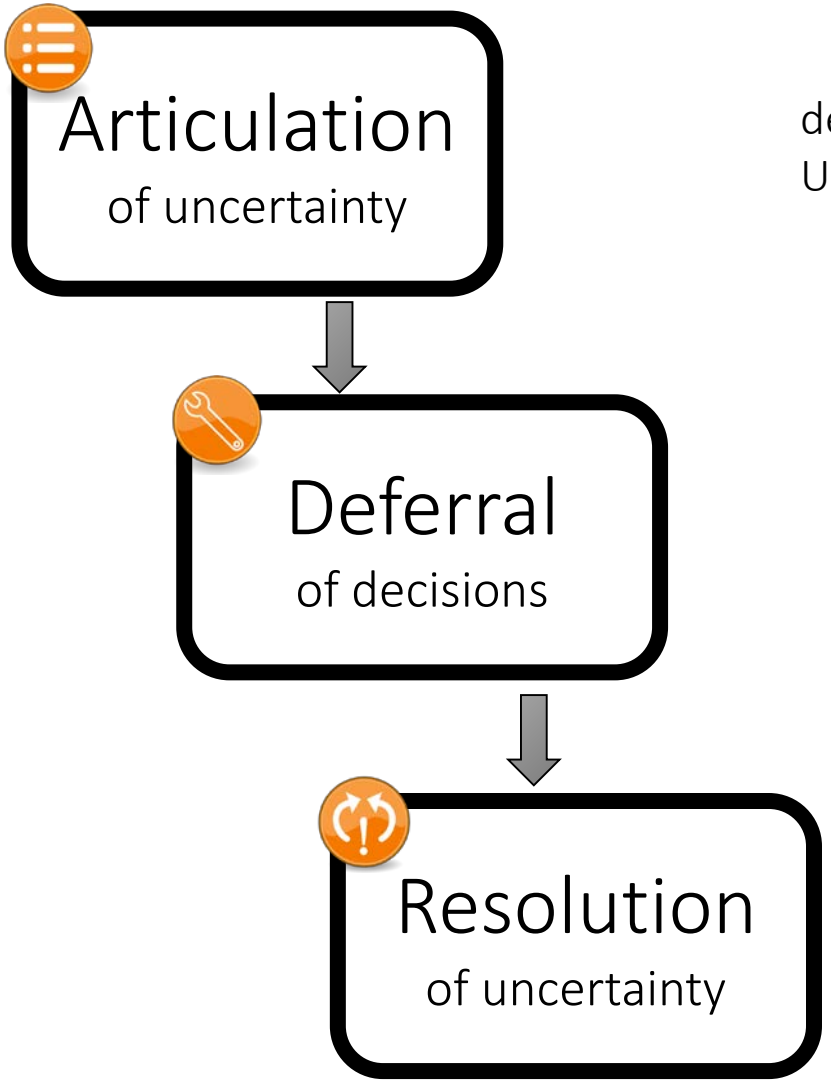
- Partial Models:
  - Semantics
  - Notation
- Lifting:
  - Verification
  - Diagnosis
  - Transformation
- Refinement
- Decision-making

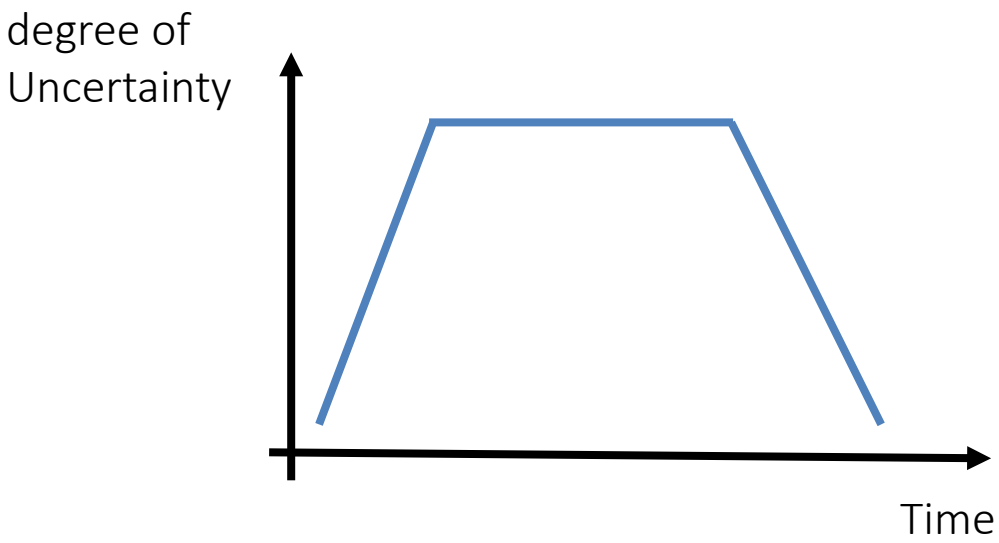
- **Methodology and Tool Support**
- Worked-out Examples
- Conclusion, Future Work

UMLet Bug #10


Articulation
K0
Make Partial
K1
Sequence Diagram that fixes the bug but violates consistency constraints
doWork
Partial model of all ways to fix consistency.
115 elements, 44 concretizations
U1: Bugfix does not affect the Paste command
U2: Consistency fix preserves bugfix
Deferral
K1
Verify (U1)
True
Verify (U2)
Maybe
newInformation
Resolution
K2
CounterExample(U2)
K1
Constrain(U2)
K3
Decide
K4
Property used to do refinement
Observed speedups consistent with experiments.

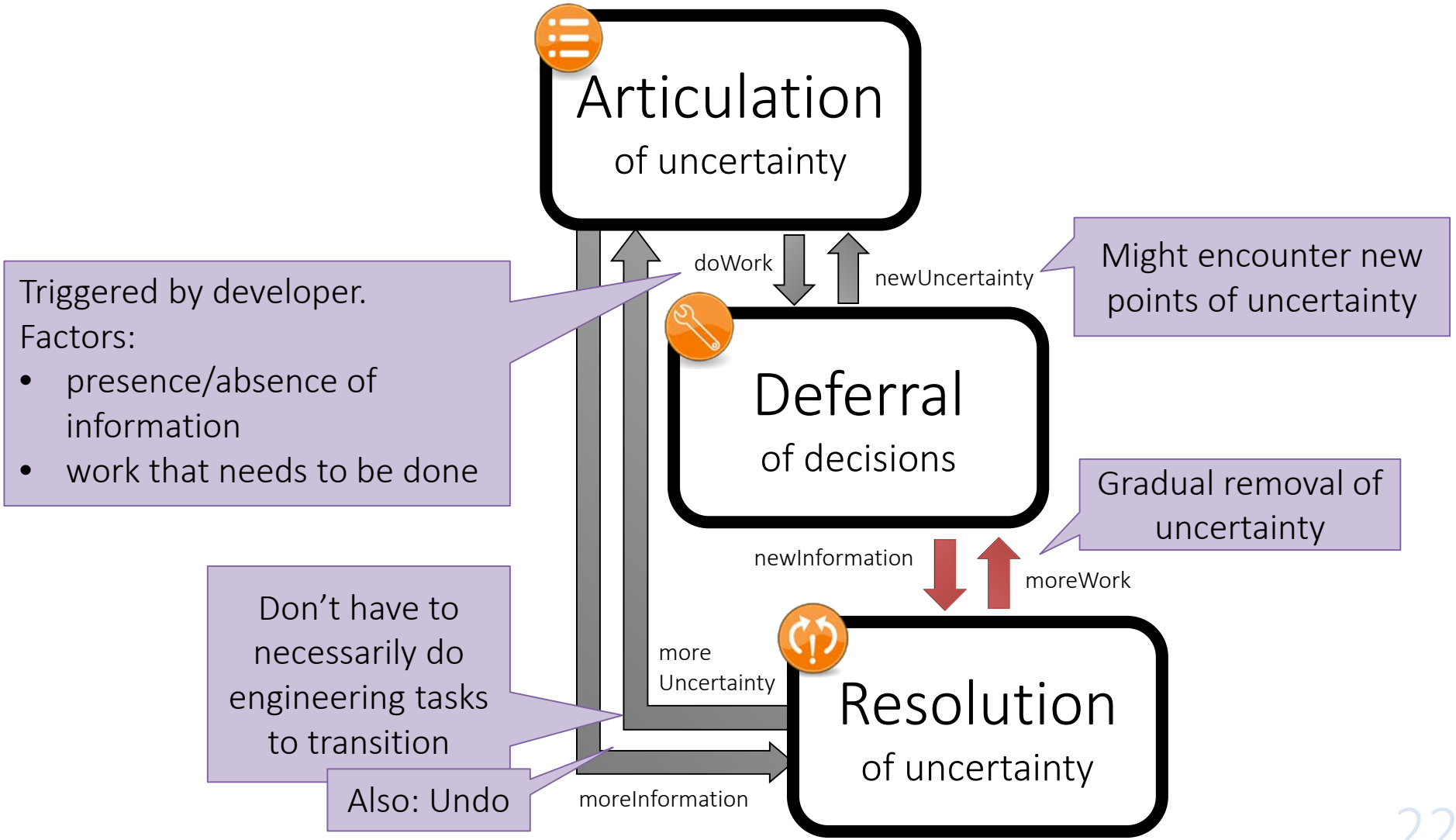
Uncertainty Lifecycle Management



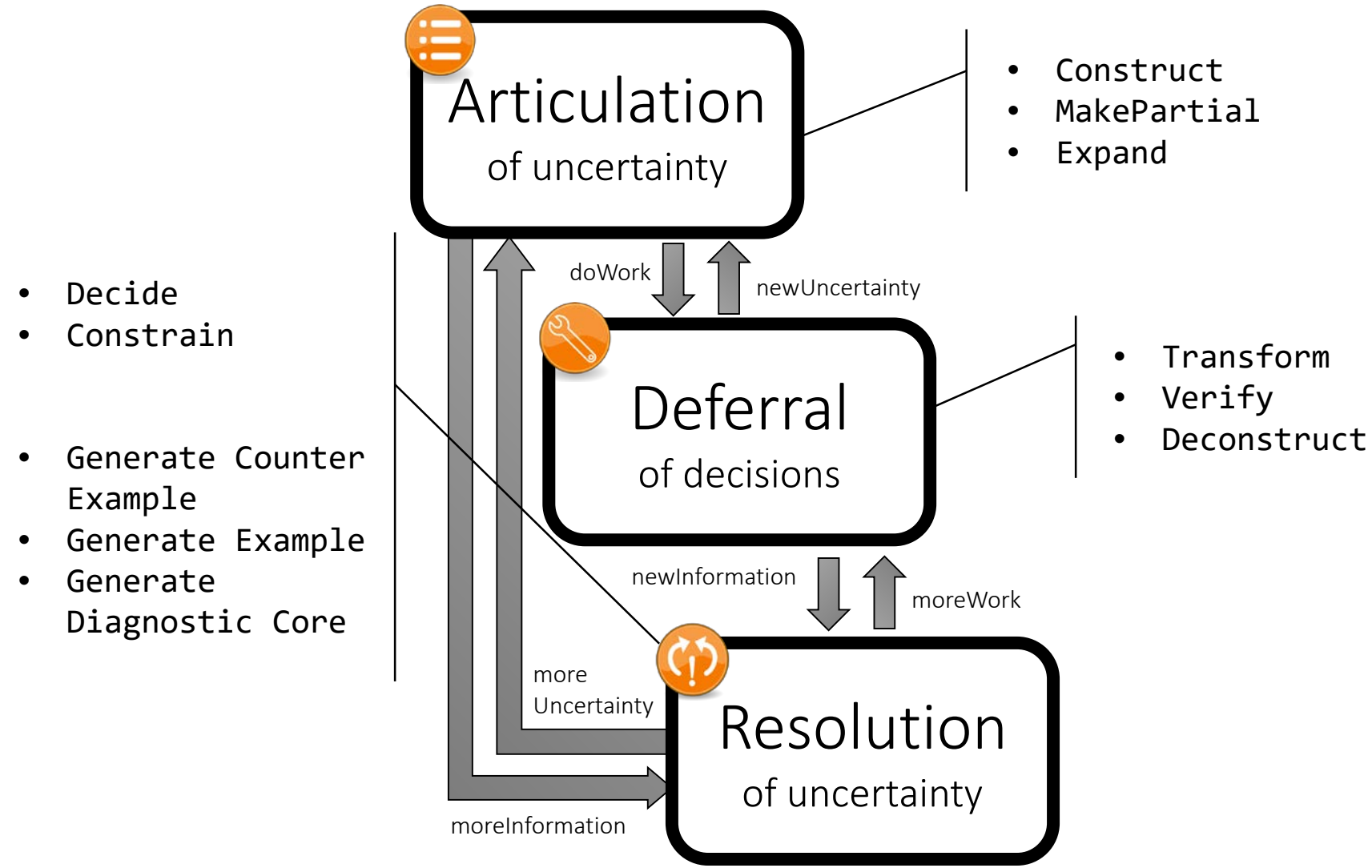


- Degree of uncertainty:
  size of the set of concretizations
- Ultimately, a single concrete model: all uncertainty resolved

Design-Time Uncertainty Management (DeTUM) model



Uncertainty Management Operators



Example Operator Specification

Name	Construct
Description	
Inputs	
Outputs	
Usage context	
Preconditions	
Postconditions	
Limitations	
Implementation	

[ICSE'12] *Partial Models: Towards Modeling and Reasoning with Uncertainty,* M. Famelis, R. Salay and M. Chechik

MU-MMINT

(pronounced “moomin”)

Partial Model Editor

Decision Tree Editor

Dashboard & Traceability

Verification & Refinement Support

Lifted Transformations

MMINT: “Model Management INTeractive”

Eclipse

Z3 SMT Solver

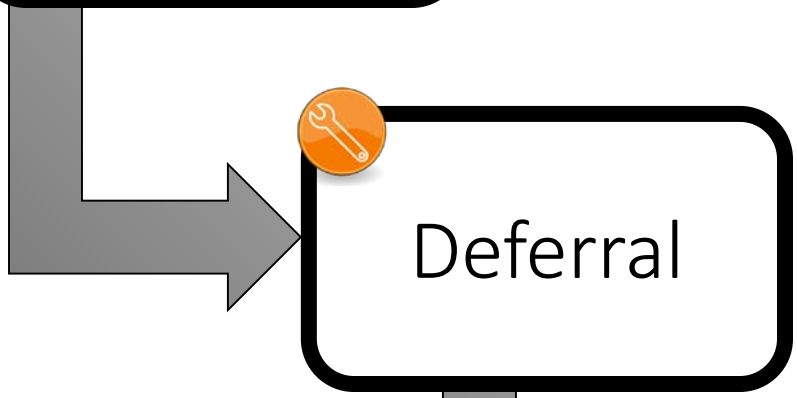
Henshin Graph Transformation Engine

MU-MMINT demo: https://youtu.be/kAWUm-iFatM
MMINT demo: https://youtu.be/7B7YuV-Jvrc
Available at https://github.com/adisandro/MMINT

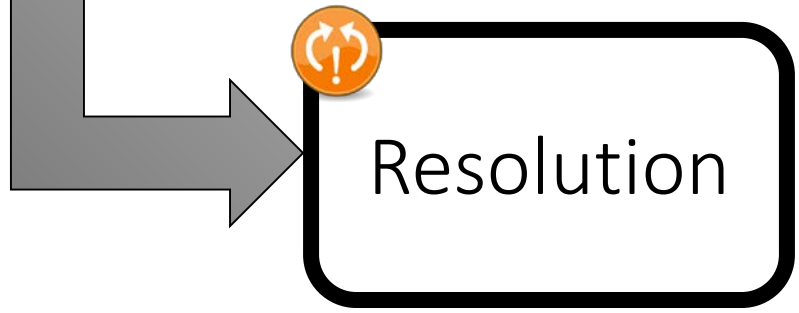
[ICSE 2015] *MU-MMINT: an IDE for Model Uncertainty,* M. Famelis, N. Ben-David, A. Di Sandro, R. Salay, and M. Chechik
[MODELS’15] *MMINT: A Graphical Tool for Interactive Model Management,* A. Di Sandro, R. Salay, M. Famelis, S. Kokaly, and M. Chechik,

Outline

- Partial Models:
  - Semantics
  - Notation



- Lifting:
  - Verification
  - Diagnosis
  - Transformation

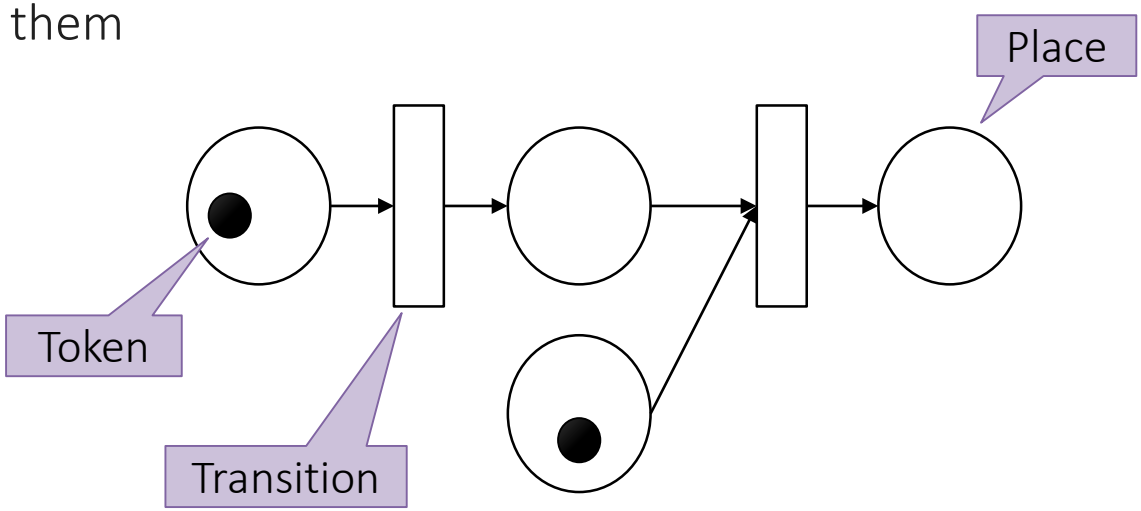


- Refinement
- Decision-making

- Methodology and Tool Support
- **Worked-out Examples**
- Conclusion, Future Work

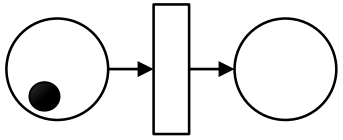
Metamodel to Relational Schema

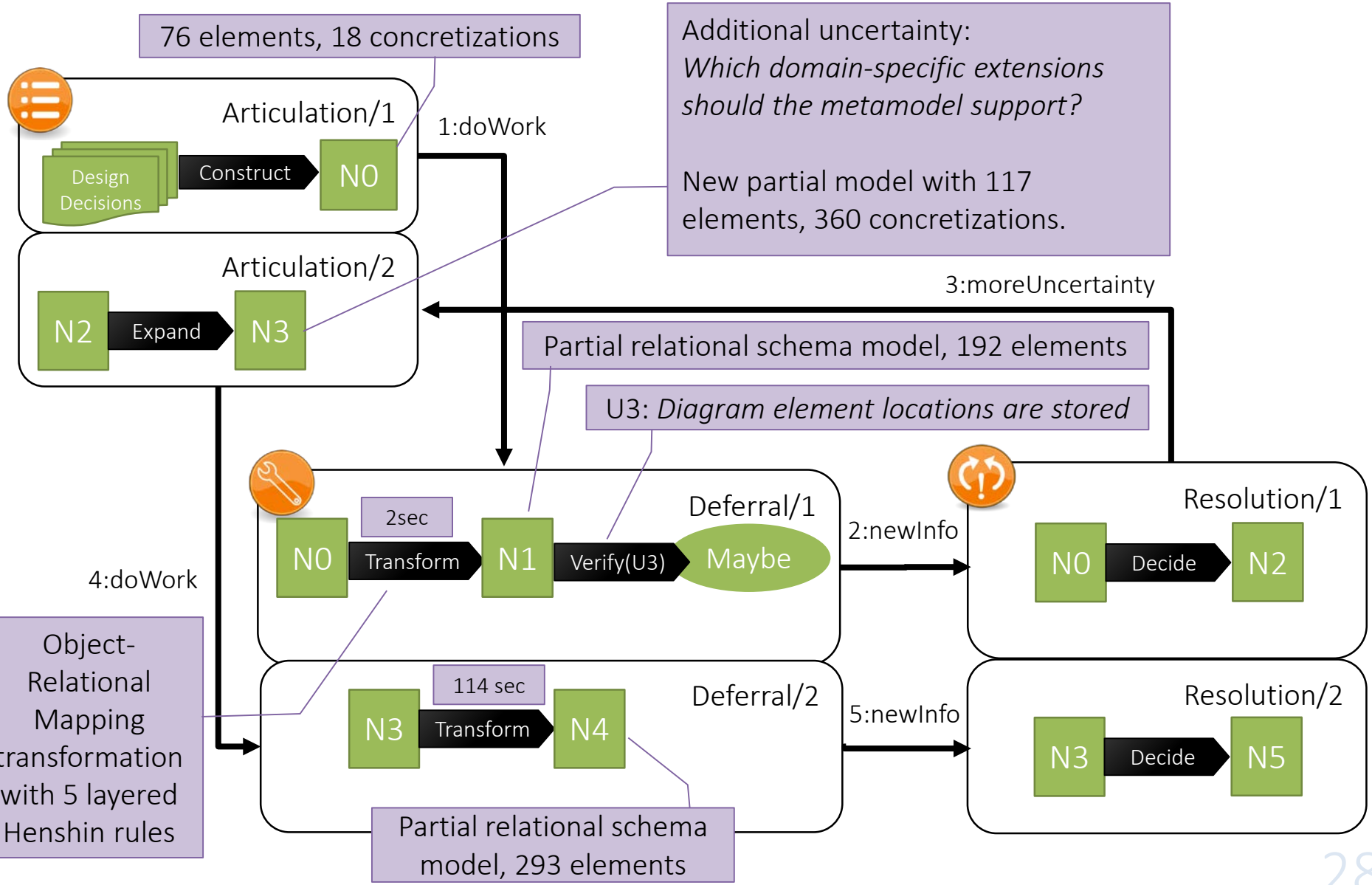
Scenario: create a metamodel for Petri nets, then create a schema for storing them



- Atlas Metamodel zoo: 8 different designs / 5 design decisions
- Partial model N0 created using MU-MMINT
  - Demo partial model editor
  - Demo Verification and Diagnosis
  - Demo Transformation

Petri Net Metamodel





Lessons Learned from Worked Examples

Must better support *Articulation* with automation

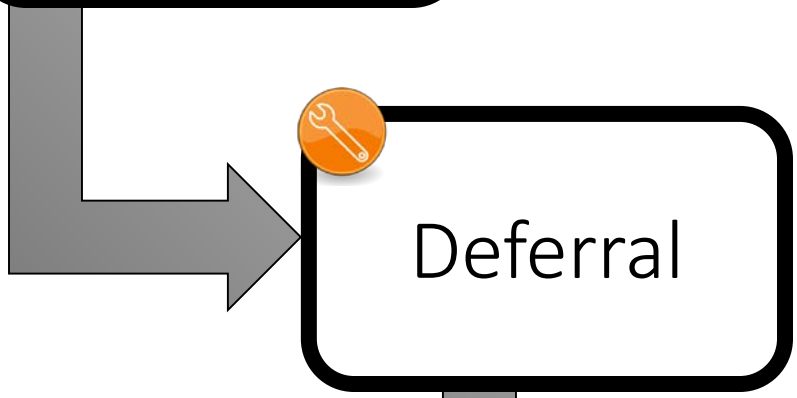
Stages of DETUM not rigid (Verification/Diagnosis)

May formula makes engineering of lifting hard

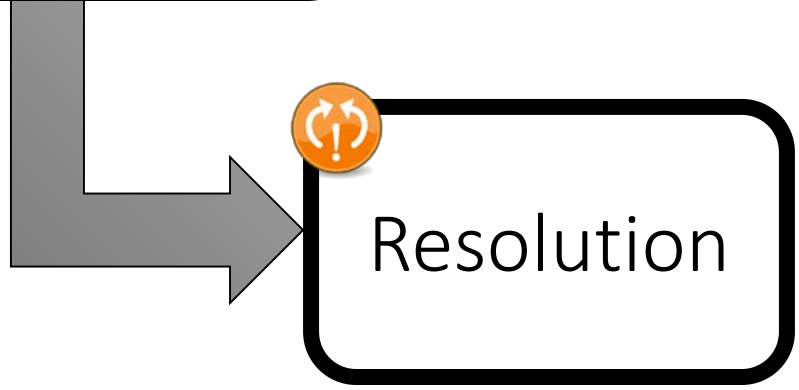
Changing modality of properties may be more appropriate response to bad verification result

Outline

- Partial Models:
  - Semantics
  - Notation



- Lifting:
  - Verification
  - Diagnosis
  - Transformation

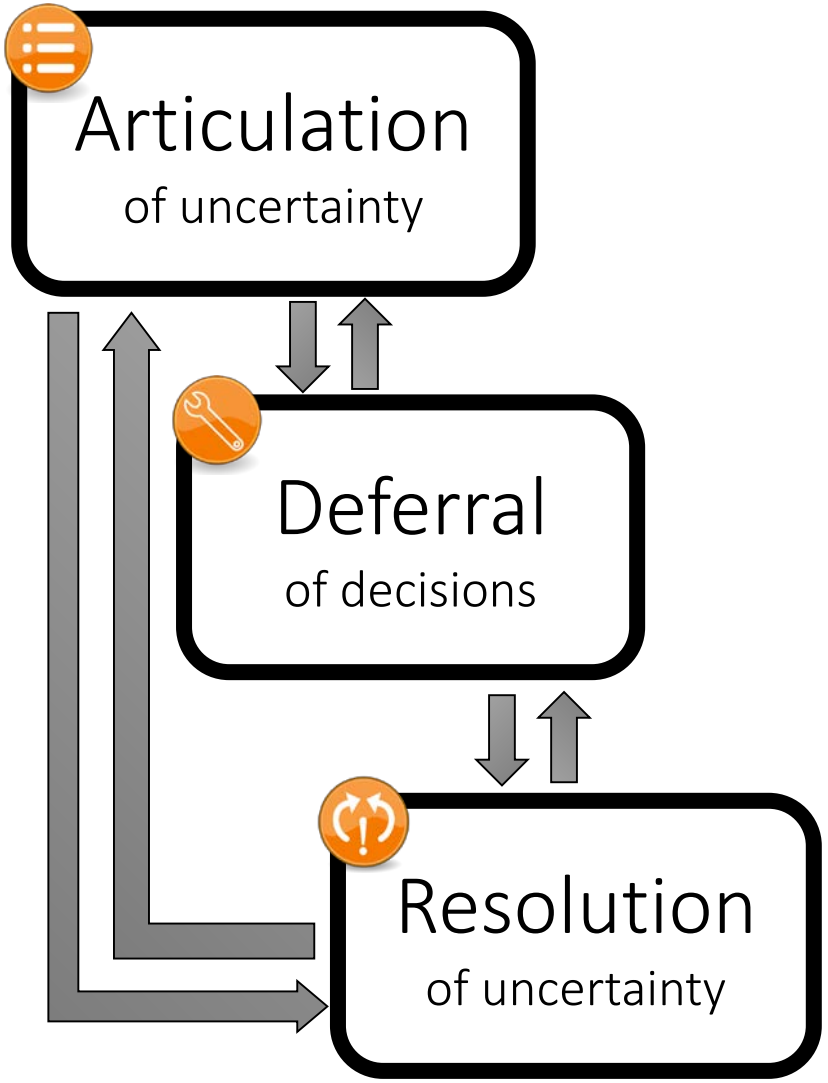


- Refinement
- Decision-making

- Methodology and Tool Support
- Worked-out Examples
- **Conclusion, Future Work**

Managing of Design-Time Uncertainty

Defer resolution of uncertainty but incorporate uncertainty handling into the development process to allow progress



- Partial Models:
  - Semantics
  - Notation
- Lifting:
  - Verification
  - Diagnosis
  - Transformation
- Refinement
- Decision-making

- DETUM model
- Uncertainty Management Ops
- MU-MMINT

Future Work

Relax underlying assumptions
- Design decisions known; alternatives elicited

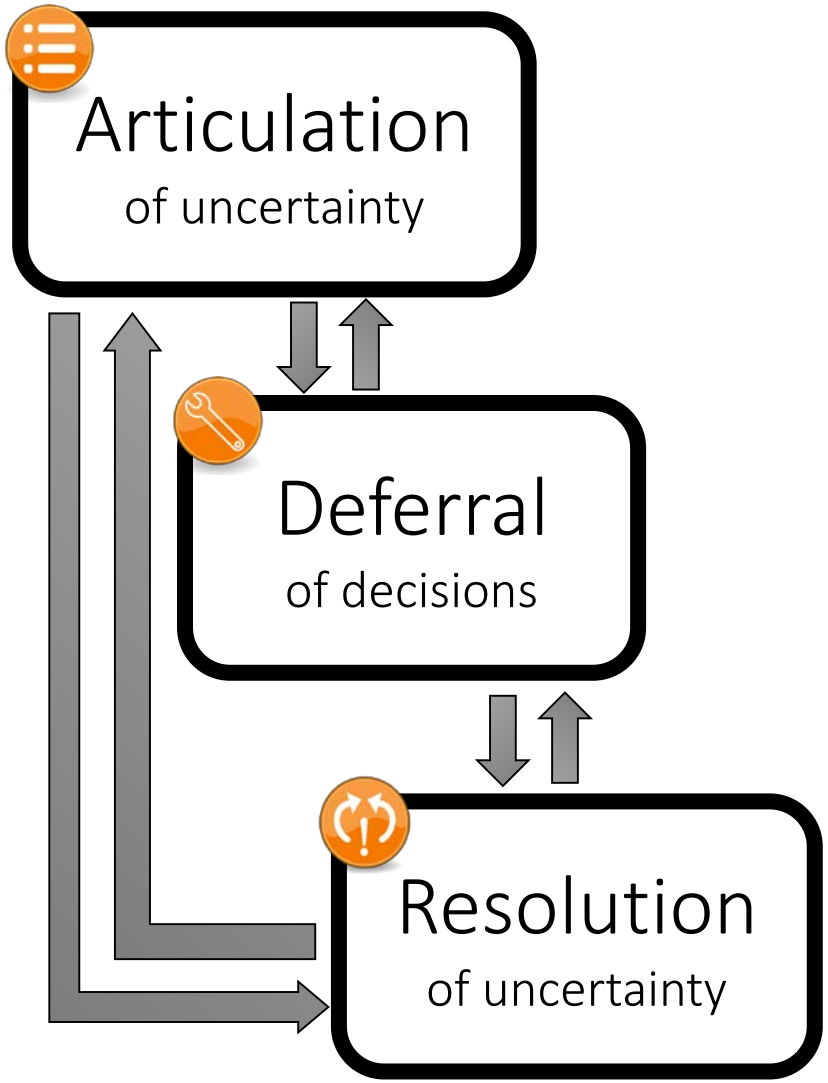
Better support uncertainty articulation
- Leverage development context

Systematically elicit design options

Combine with existing methodologies (e.g. Scrum, Kanban)

Managing of Design-Time Uncertainty

Michalis Famelis, Marsha Chechik



- Partial Models:
  - Semantics
  - Notation
- Lifting:
  - Verification
  - Diagnosis
  - Transformation
- Refinement
- Decision-making
- Methodology and Tool Support
- Worked-out Examples
- Discussion, Future Work

Questions?

Université de Montréal

UNIVERSITY OF TORONTO