Integrating Reasoning With SysML

Henson Graves

Outline

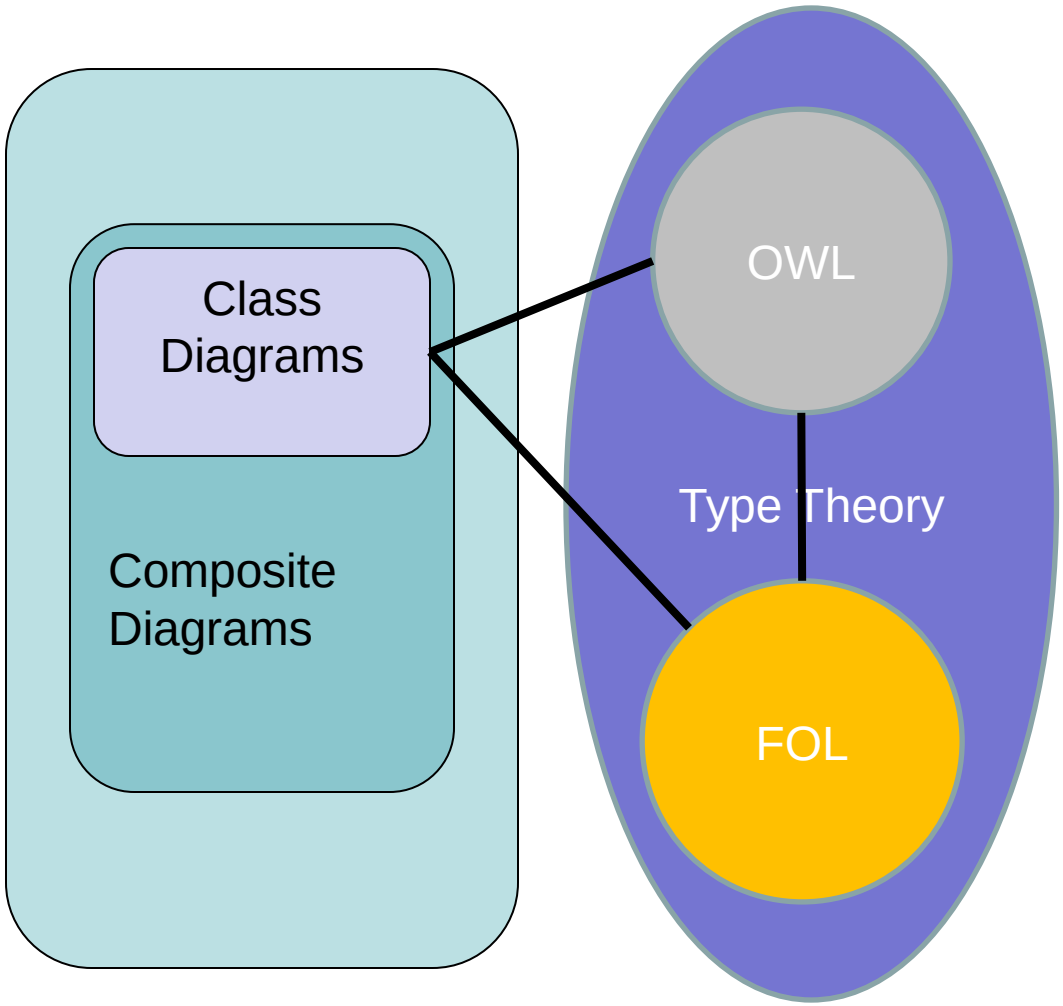
- Engineering tasks where automated reasoning is needed and is feasible
- Representing engineering questions as questions about a SysML model
- Embedding SysML into a logical framework
- Engineering problems as logic problems
- Examples of reasoning
- Recommendations for the SysML specification

tasks where automated reasoning is feasible

- Verification of a system capability (or requirement satisfaction)
  - Can an aircraft under specific operating conditions loiter in an area for specific time duration.
- Verification whether a design change invalidates design constraints
  - Adding a connection to the electrical system may violate electrical system constraints
  - Adding a pump to a system which is not consistent with the pump specification
- Logic can also be used to justify computational results
  - The weight computed from a model is correct in any implementation

Embedding SysML into a logical framework

SysML
- Classes & properties
- Composite structure
- Behavior

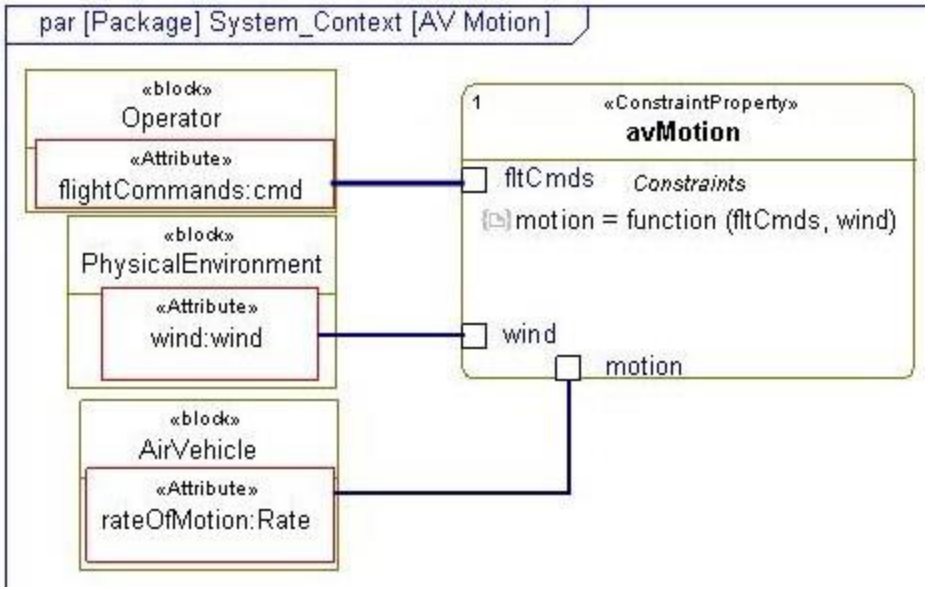


OWL
- Classes & properties correspond to a fragment of FOL
- Decidability
- Rich class constructors
- Individuals

First Order Logic
- Quantifiers
- Nary-predicates
- Functions

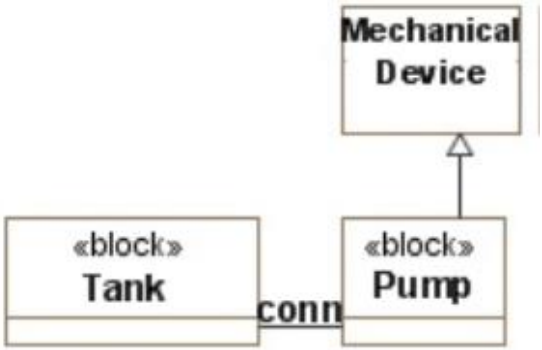
Type theory
- Contains a higher order logic
- Set theory like abstraction

Example: Checking Whether Aircraft Operating Condition Implies Loitering Condition



Embedding a Class Model in DL and FOF

SysML



Description Logic (OWL)

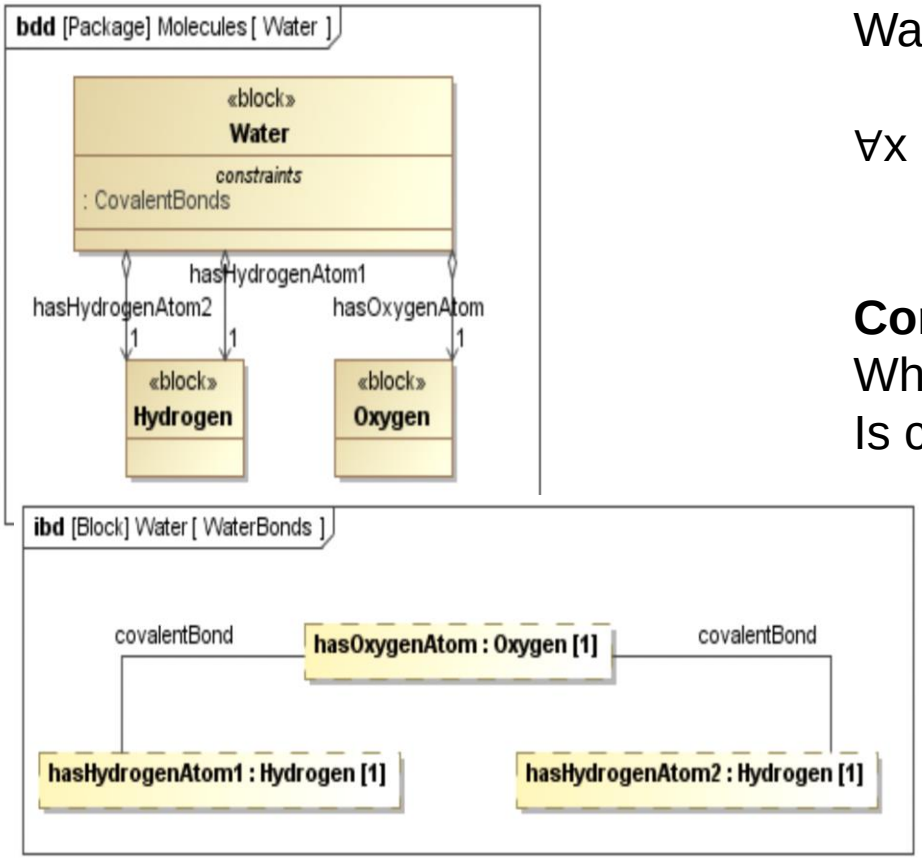
Pump ⊑ MechanicalDevice
Dom(conn) = Tank
Range(conn) = Pump

First Order Logic

$\forall x.\ Pump^{\wedge}(x)$ implies $MechanicalDevice^{\wedge}(x)$

$\forall x\ \forall y.\ Tank^{\wedge}(x)$ and $conn^{\wedge}(x,y)$ implies $Pump^{\wedge}(y)$

Embedding a Structure Diagram in Logic



Parts

Water ⊑ hasOxygentAtom(1).Oxygen

∀x ∃y. Water(x)
implies hasOxygentAtom(x,y)

Connections

What one wants is that the oxygen part
Is connected to the hydrogen part

∀ x. Water(x) implies
x.hasOxygen^^.connectbond =
x.hasHydrogen1^^

Water ⊑
Water{hasOxygen^^.connectbond,
hasHydrogen1^^}

Translating Engineering into Logic Problems

A Model translates to an axiom set

Questions about model translate to questions about axioms

- Is the model (axiom set) consistent
- Can a statement be added to the model (axiom set) without making it inconsistent
- What do all of the interpretations look like, do they look like what was intended

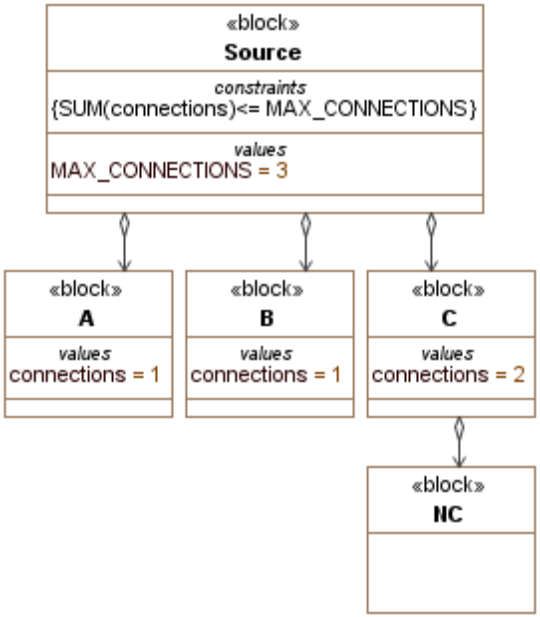
Taking Advantage Of Results From Logic

- In examples we show changes to model imply inconsistency

- Inconsistency
  - Thing = NoThing
  - Conjunction of axioms = false
  - {x : f(x) = true} = NoThing

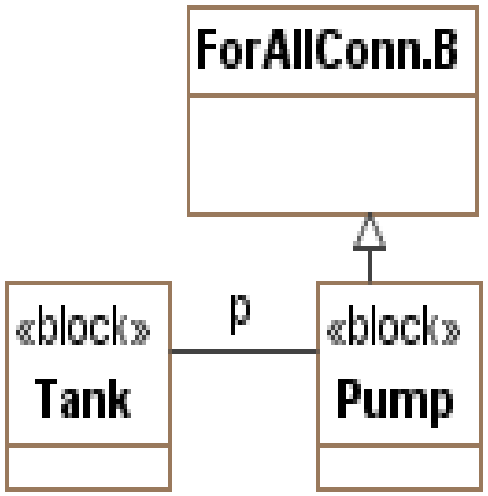
- Realize details of axiom system make a lot of difference regarding decidability

Example: Checking Whether Connecting a Device to the Electrical System is OK



- Source block constraint
  - sum of all connections must be less than 3.
- A connection is a path connection
  - not just the direct connections to A, B, and C
- A connection of NC to C violates Source constraint

Example: Adding An Incompatible Pump To a System



- pump can only be connected to components of type B.
- Pump to a component A where A and B are disjoint, the connection violates the original model.
- To use the pump model, the assumption must be modified as this assumption is incompatible with Pump assumptions

SysML Recommendations

- Additions to SysML
  - Add DL class constructions
  - Add individuals
  - Add “function call” to block diagrams
- Formal semantics should be part of the SysML specification
- Find axioms for behavior
- Redo the SysML Metamodel to have meta-classes for Model, BDD, IBD,…