MODELLING CYCLIC STRUCTURES IN AGDA

COINDUCTIVE FORMALIZATIONS OF LINEAR TEMPORAL LOGIC

AUTHOR

Calin-Marian Diacicov (c.m.diacicov@student.tudelft.nl)

SUPERVISORS

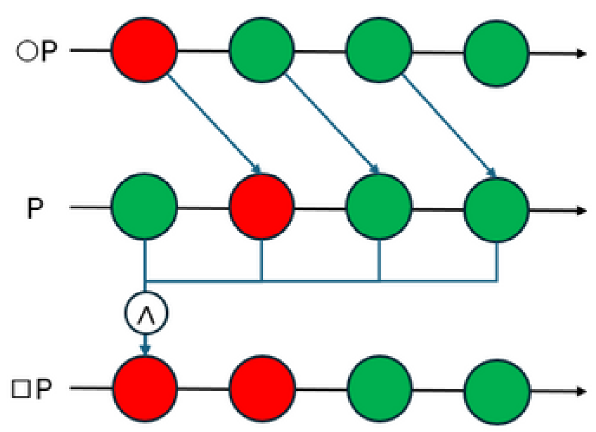
Jesper Cockx, Bohdan Liesnikov

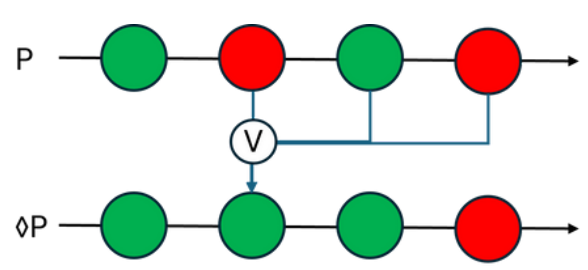
TU Delft

1. BACKGROUND

LINEAR TEMPORAL LOGIC (LTL)

- Truth value of propositions varies in time.
- Pointwise lifting of classical operators and temporal modalities.
- A proposition is satisfied if it is currently true.
- A proposition is valid if it is true at any time point.
- *Kripke structure*: infinite sequence of valuations of propositional constants.





COINDUCTION

- *Corecursion*: Construct objects of a coinductive data type, by constructing the observations.
- Agda supports three types of coinduction:
  a. *Musical* coinduction: compose delays with ♯ and force them with ♭ operators.
  b. *Guarded* coinduction: use coinductive records and copattern matching to define coinductive types.
  c. *Sized types*: tracks depth of recursion structurally by embedding types with a size.

2. RESEARCH QUESTION

How can linear temporal logic be formalized in Agda?

- How can coinduction be used to model LTL formulas?
- What limitations of Agda arise in the process of modeling and reasoning about temporal logic?

3. ENCODINGS

DEEP EMBEDDING OF SEMANTICS

- Encode the syntax explicitly as an inductive type.
- Encode Kripke structures as streams of states.
- Encode the semantics using pattern matching.

```
_⊢_ : (KripkeStructure n) → LTLFormula {n} → Set
K ⊢ (Var x₁) = (head K) x₁ ≡ true
K ⊢ (Neg x₁) = (head K) x₁ ≡ false
K ⊢ (◯ P) = (tail K) ⊢ P
K ⊢ (□ P) = K ⊨ P
K ⊢ (◇ P) = Σ ℕ (eventually K P)

record _⊨_ (K : KripkeStructure n) (P : LTLFormula) : Set where
  coinductive
  field
    TrueNow : K ⊢ P
    TrueInFuture : (tail K) ⊨ P
```

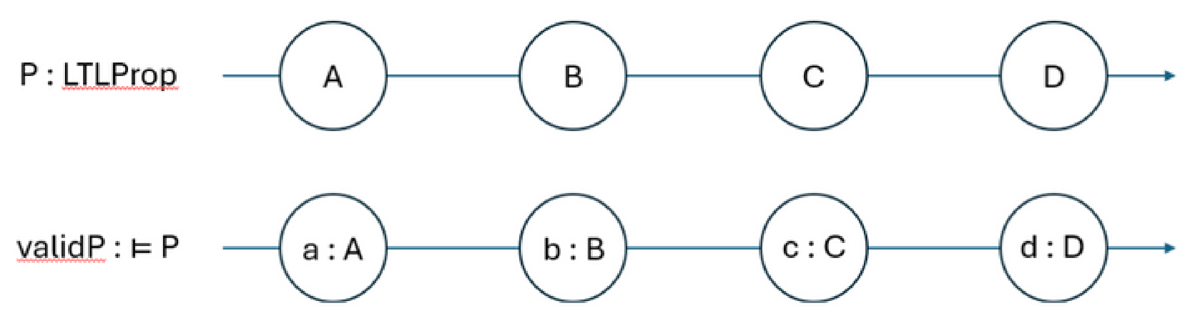
Listing 1: Definition of satisfaction for the temporal operators, propositional constants, and negation.

SHALLOW EMBEDDING OF SEMANTICS

- Encode LTL propositions as streams of sets.
- Use propositions as types to encode logical operations.

```
record ⊨_ (P : LTLProp) : Set where
  coinductive
  field
    ⊨-head : head P
    ⊨-tail : ⊨ (tail P)
```

Listing 2: Encoding of validity of an LTL proposition.



4. EXPERIMENTS

1. ***Soundness***: Derived an axiomatization of LTL to prove correctness of the formalization.
2. **Absorption theorems:** Proved identities exploring the interaction between ◊ and ☐ temporal modalities.
3. **Towers of Hanoi**: Encoded Towers of Hanoi as a state system and prove properties of the system.

$(A_2)\ K \vDash (A \to (B \to C)) \to (A \to B) \to A \to C$

$(A_3)\ K \vDash (\neg B \to \neg A) \to A \to B$

$(\text{Fun})\ K \vDash \neg \bigcirc A \leftrightarrow \bigcirc \neg A$

$(\text{K}\bigcirc)\ K \vDash \bigcirc(A \to B) \to (\bigcirc A \to \bigcirc B)$

$(\text{ltl3})\ K \vDash \Box A \to A \land \bigcirc \Box A$

$(\text{MP})\ K \vDash A \to (A \to B) \to B$

$(\text{N}\Box)\ K \vDash A \to \Box A$

$(\text{Ind})\ K \vDash (A \to \bigcirc A) \Rightarrow K \vDash (A \to \Box A)$

Axiomatization of Linear Temporal Logic

1. $\Box \Box P \Leftrightarrow \Box P$
2. $\Diamond \Diamond P \Leftrightarrow \Diamond P$
3. $\Box \Diamond \Box P \Leftrightarrow \Diamond \Box P$
4. $\Diamond \Box \Diamond P \Leftrightarrow \Box \Diamond P$

Absorption Theorems

Encoding	Soundness	Absorption Theorems	Towers of Hanoi
Shallow embedding	✓	✓	✓
Deep embedding	✓	✓	✗

Table 1: Summary of the results of the experiments.

5. AGDA LIMITATIONS

- **Documentation:** Documentation for certain topics is missing or incomplete.
- **Error messages:** Oftentimes error messages are confusing and do not point to the actual problem.
- **Termination checking:** The termination checker fails to identify structurally decreasing parameters.

6. FUTURE WORK

- Explore **extensions** of the LTL we considered.
- Investigate formalizations of LTL using other types of coinduction.