Consistent Partial Model Checking

Michael Huth
Department of Computing
Imperial College London

Shekhar Pradhan
Department of Computer Science
Vassar College

Thursday, July 10, 2003 at DIMACS

Acknowledgments: Glenn Bruns, Patrice Godefroid, Rahda Jagadeesan, and David Schmidt.

Objectives of talk

1. Sketch model-checking framework that
   - deals with **inconsistencies**
   - allows for **under-specification**
   - has sound notions of **refinement** and abstraction
   - allows for **multiple viewpoints** and
   - **re-uses** existing model checkers whenever possible.
2. Compare this to work on multiple-valued model checking.

Threats to consistency

- **distributed** contents
- **multiple** viewpoints
- **over-constrained** system
- system **evolution**
- **hidden** assumptions
- **emotionally** driven judgments
- etc.

Treating Inconsistency

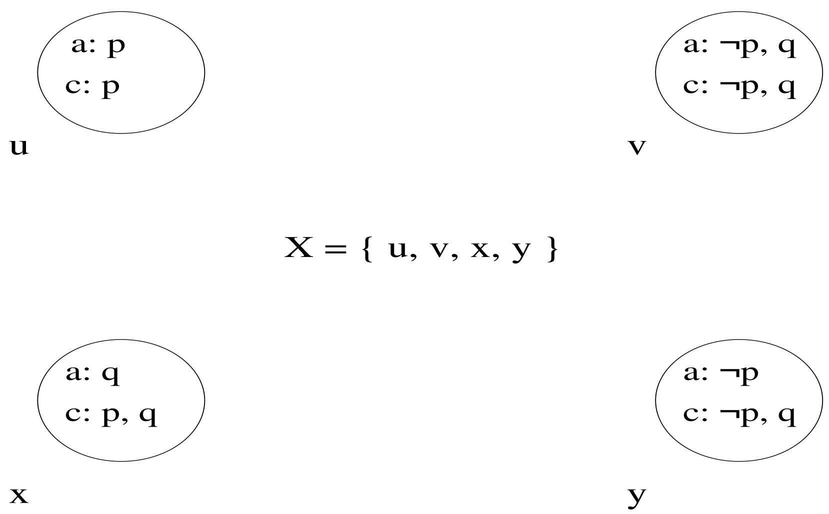
Based on [Nuseibeh, Kramer, and Finkelstein 1994]:

- **detect** inconsistencies
- locate **sources** of inconsistencies
- negotiate **conflict resolution**
- **repair** inconsistencies if possible & feasible
- **mitigate** effect of inconsistencies
- etc.

Bundled models

- Models P comprise finite bundles: $P = (P_x)_{x \in X}$.
- Each P_x model in **some** ontology.
- Each $x \in X$ may stand for
  - an application **aspect**
  - a stake-holder's **viewpoint**
  - a component's **version number**
  - a model's "**information horizon**"
  - a domain-specific **expert** [Fitting 1992]
  - etc.

Example of bundled model



Legend: x rules "p is consistent" and "q is valid assertion" etc.

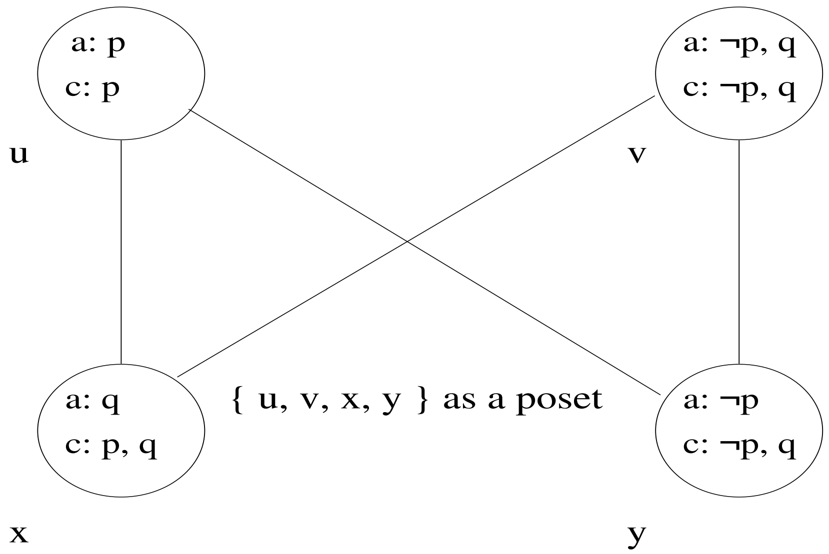
Priorities for bundles

1. Models $P = (P_x)_{x \in X}$ bundled over partial order $(X, \leq)$ of **priorities** [Fitting'92: "dominance"]

2. $x \leq y$ varying interpretations:

   - aspect x' more **crucial** than aspect x
   - expert x' more **authoritative** than expert x
   - version x' more **recent** than version x
   - x' contains the **information horizon** of x
   - etc.

Prioritized example



Legend: both u and v have higher priority than x and y.

Partiality of bundles

- Assume range of queries $\phi \in \mathcal{L}$.
- Each P_x answerable to each query $\phi \in \mathcal{L}$.
- Two kinds of answers:
  - $P_x {\models^{\mathrm{a}}} \phi$: x rules "ϕ **valid** assertion in P_x" and
  - $P_x {\models^{\mathrm{c}}} \phi$: x rules "ϕ **consistent** in P_x."
- Q_x **refines** P_x iff P_x **abstracts** Q_x iff

$$\text{(Ass)} \qquad \forall \phi \in \mathcal{L} \colon P_x {\models^{\mathrm{a}}} \phi \;\Rightarrow\; Q_x {\models^{\mathrm{a}}} \phi \,.$$

- If "$P_x {\models^{\mathrm{a}}} \phi$ and $P_x \not\models^{\mathrm{c}} \phi$" for **no** ϕ and x, the latter means

$$\text{(Con)} \qquad \forall \phi \in \mathcal{L} \colon Q_x {\models^{\mathrm{c}}} \phi \;\Rightarrow\; P_x {\models^{\mathrm{c}}} \phi \,.$$

Obligation cones

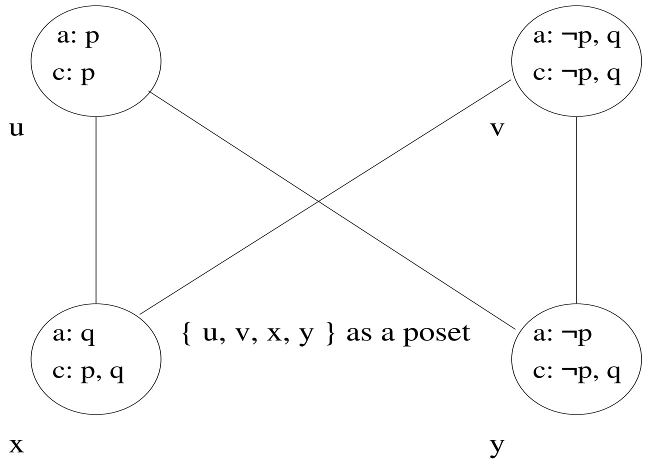
Platonic bundles:

- defined by $\forall x, y \in X \colon x \leq y \;\Rightarrow\; P_x$ refines P_y
- have no inconsistencies **across** model boundary $\leq$
- ideal **reference frame** against which to detect and locate inconsistencies

$\Rightarrow$ results in "flow laws" of **obligations**:

$$\begin{array}{ll} \text{(Ass)} & \{\!| X : \phi |\!\}^{\mathrm{a}} \stackrel{\text{def}}{=} \{ x \in X \mid \exists y \in X \colon x \leq y,\; P_y {\models^{\mathrm{a}}} \phi \} \\ \text{(Con)} & \{\!| X : \phi |\!\}^{\mathrm{c}} \stackrel{\text{def}}{=} \{ x \in X \mid \exists y \in X \colon y \leq x,\; P_y {\models^{\mathrm{c}}} \phi \} \,. \end{array}$$

Example cones of influence



$$
\begin{aligned}
\{\!|X : p|\!\}^{\mathrm{a}} = \{v \in X \mid \exists w \in X : v \leq w,\ P_w \models^{\mathrm{a}} p\} &\quad = \quad \{u, x, y\} \\
\{\!|X : \neg p|\!\}^{\mathrm{c}} = \{v \in X \mid \exists w \in X : w \leq v,\ P_w \models^{\mathrm{c}} \neg p\} &\quad = \quad \{u, v, y\}\,.
\end{aligned}
$$

Computing obligation cones

```
if (m == a) { leq = <=; } else { leq = >=; }
U = X; L = emptyset;
while (U != emptyset) {
  for all x in max(U,leq) {
    if (check(P_x,phi,m)) { % P_x |=^m phi ?
      let A = { y | y leq x } in {
        L = L union A;
        U = U \ A;
      }
    } else {
      U = U \ { x };
    }
  }
} return L;
```

Comments on algorithm

- **not** compositional in ϕ
- **parametric** in mode `m` and local checks `check(P_x,phi,m)`
- complexity $\leq$ complexity for local checks **times** $|X|$
- parametricity in local checks allows for
  - `check` being an abstract **interface**
  - different local **ontologies**
  - **re-use** of model checkers, e.g. [Bruns & Godefroid 2000]
  - **semi-formal** or informal expert rulings.

Detecting and locating inconsistencies

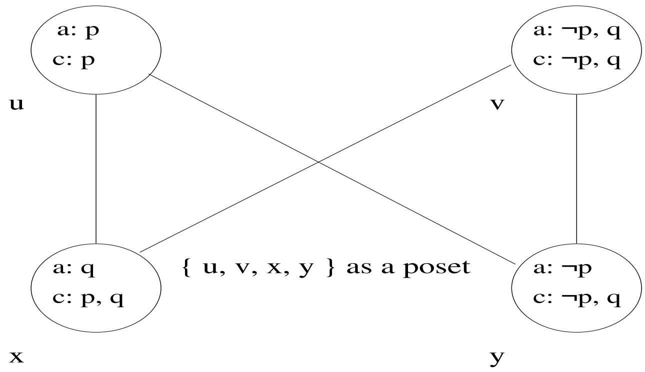
For finite $\Phi \subseteq \mathcal{L}$ and $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$:

$$\begin{aligned} \bigcap_{\phi\in\Phi} \{\!|X : \phi|\!\}^{\mathrm{m}} &\not\subseteq \{\!|X : \bigwedge \Phi|\!\}^{\mathrm{m}} \\ \{\!|X : \bigvee \Phi|\!\}^{\mathrm{a}} &\not\subseteq \bigcup_{\phi\in\Phi} \{\!|X : \phi|\!\}^{\mathrm{a}} \\ \{\!|X : \bigvee \Phi|\!\}^{\mathrm{c}} &= \bigcup_{\phi\in\Phi} \{\!|X : \phi|\!\}^{\mathrm{c}} . \end{aligned}$$

Use $\bigcup$, $\bigcap$, and $\setminus$ to **instrument** detection and location queries. E.g.

$$\bigcap_{\phi\in\Phi} \{\!|X : \phi|\!\}^{\mathrm{c}} = \{x \in X \mid x \text{ obliged to hold } \bigwedge \Phi \text{ consistent}\} .$$

Example instrumentation



1. **Detection** of inconsistency:
   $\{\!|X : p|\!\}^{\mathrm{c}} \cap \{\!|X : \neg p|\!\}^{\mathrm{c}} = \{u, v, x\} \cap \{u, v, y\} = \{u, v\}$.
2. **Location** of inconsistency for u: product of all **minimal witnesses** for membership; here $\{(x, y)\}$ only.
3. **Conflict resolution**: experts of **all** tuples re-assess.

Primer on obligation cones

- all P_x consistent $\Rightarrow$ cones are **internally consistent**:

$$\{\!|X : \phi|\!\}^{\mathrm{a}} = \downarrow\!(\{\!|X : \phi|\!\}^{\mathrm{a}} \cap \{\!|X : \phi|\!\}^{\mathrm{c}})$$

- all P_x consistent and P Platonic $\Rightarrow$ $\{\!|X : \phi|\!\}^{\mathrm{a}} \subseteq \{\!|X : \phi|\!\}^{\mathrm{c}}$
- $\forall x \in X : Q_x$ refines P_x $\Rightarrow$ obligation cones **sound** under refinement:

$$\{\!|X_P : \phi|\!\}^{\mathrm{a}} \subseteq \{\!|X_Q : \phi|\!\}^{\mathrm{a}} \qquad \& \qquad \{\!|X_Q : \phi|\!\}^{\mathrm{c}} \subseteq \{\!|X_P : \phi|\!\}^{\mathrm{c}}$$

- **mixed power-domain** [Gunter 1992] & [Heckmann 1993] of $(X, \leq)$ right concept for "internal consistency" and "soundness of refinement."

Multiple-valued model checking

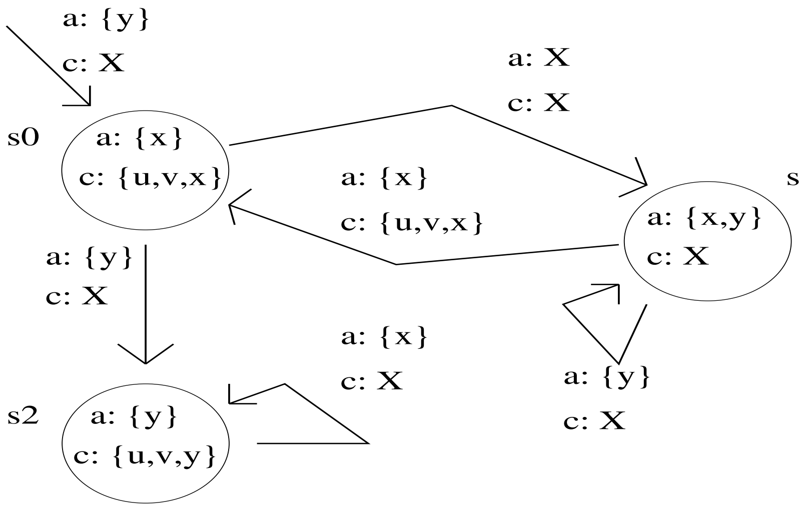
- **compositional** semantics $[\![\ \phi\ ]\!]$ element of finite distributive lattice D e.g. [Chechik et al. 2001], i.e.

$$[\![\ \phi\ ]\!]\ \textbf{lower}\ \text{set in}\ (X, \leq) \stackrel{\text{def}}{=} \textbf{primes}\ \text{of}\ D\ .$$

- observables of model (transitions etc) lower sets of $(X, \leq)$;
- **amend** model: observables **pairs** (L, U) of lower and upper sets of $(X, \leq)$ (resp.); compositional semantics in **two modes** $[\![\ \phi\ ]\!]^{\mathrm{m}}$, $\mathrm{m} \in \{\mathrm{c}, \mathrm{a}\}$;
- amended model $\rightsquigarrow$ **projected** bundled model $P = (P_x)_{x \in X}$;
- P Platonic $\Rightarrow$

$$\{\![X : \phi]\!\}^{\mathrm{m}} = [\![\ \phi\ ]\!]^{\mathrm{m}}\ \text{for all}\ \phi\ \text{and}\ \mathrm{m}\ .$$

Example: multiple-valued modal state machines



Legend: X as before; "s_0 initial state" consistent for all, but valid for y only, etc; single predicate p valid for x only at s_0, consistent for all but y at s_0 etc.

Compositional query semantics

$\llbracket \perp \rrbracket^{\mathrm{P}}_{\rho} = (\{\}, \{\})$ $\qquad$ $\llbracket \mathtt{p}(\mathtt{u}) \rrbracket^{\mathrm{P}}_{\rho} = \mathrm{Lb}(p, \rho(\mathtt{u}))$

$\llbracket \mathtt{R}(\mathtt{u}, \mathtt{v}) \rrbracket^{\mathrm{P}}_{\rho} = R(\rho(\mathtt{u}), \rho(\mathtt{v}))$ $\qquad$ $\llbracket +\mathtt{R}(\mathtt{u}, \mathtt{v}) \rrbracket^{\mathrm{P}}_{\rho} = R^{+}(\rho(\mathtt{u}), \rho(\mathtt{v}))$

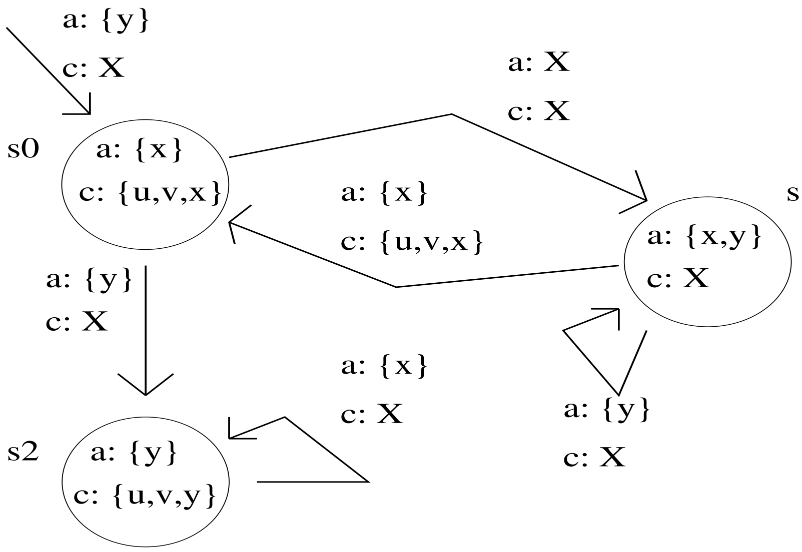
$\llbracket \neg\phi \rrbracket^{\mathrm{P}}_{\rho} = (X \setminus \llbracket \phi \rrbracket^{\mathrm{P_c}}_{\rho}, X \setminus \llbracket \phi \rrbracket^{\mathrm{P_a}}_{\rho})$ $\qquad$ $\llbracket \phi \vee \psi \rrbracket^{\mathrm{P}}_{\rho} = \llbracket \phi \rrbracket^{\mathrm{P}}_{\rho} \sqcup \llbracket \psi \rrbracket^{\mathrm{P}}_{\rho}$

$\llbracket \exists \mathtt{u}\, \phi \rrbracket^{\mathrm{P}}_{\rho} = \bigsqcup_{s \in S} \llbracket \phi \rrbracket^{\mathrm{P}}_{\rho[\mathtt{u} \mapsto s]}$.

- $s \in S$ set of states and $\llbracket \phi \rrbracket^{\mathrm{P}}_{\rho} = (\llbracket \phi \rrbracket^{\mathrm{P_a}}_{\rho}, \llbracket \phi \rrbracket^{\mathrm{P_c}}_{\rho})$;
- $p \in \mathtt{AP}$ state predicates; $\mathtt{u}, \mathtt{v}, \dots \in \mathsf{Var}$ variables;
- $R(s, s')$ (one transition), $R^{+}(s, s')$ (one or more transitions), and $\mathrm{Lb}(p, s)$ (labeling) **all** of the form (L, U) with L lower set, U upper set, and $L \subseteq U$;
- $\rho\colon \mathsf{Var} \to S$ environment; and
- $\bigsqcup_{i \in I}(L_i, U_i) \stackrel{\text{def}}{=} (\bigcup_{i \in I} L_i, \bigcup_{i \in I} U_i)$.

A model check

Consider $\phi \stackrel{\text{def}}{=} \exists \mathtt{v}\, (+\mathtt{R}(\mathtt{v}, \mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))$: "There is a state that is on a cycle and does not satisfy p."



Determining bundled model

- The formula

$$\phi \stackrel{\text{def}}{=} \exists \mathtt{v}\,(+\mathtt{R}(\mathtt{v},\mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))$$

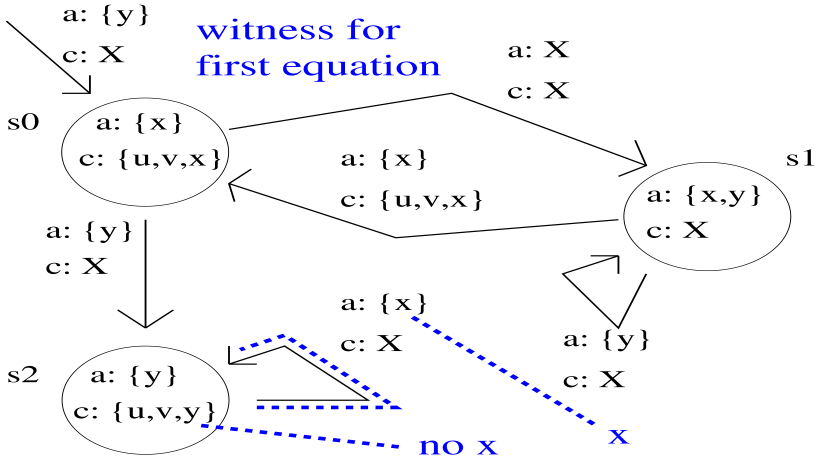
  is closed (p not a variable) $\Rightarrow$ checks independent of ρ.

- In P_x every observable (L, U) turns into observable

1;	if $x \in L$ (**valid** in P_x)
0;	if $x \notin U$ (**inconsistent** in P_x) and
$1/2$;	otherwise (**consistent but invalid** in P_x) .

$\Rightarrow$ each P_x three-valued model.

Computation results



$$[\![\, \exists \mathtt{v}\,(+\mathtt{R}(\mathtt{v},\mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))\,]\!]^{\mathrm{a}} = \{\!|X : \exists \mathtt{v}\,(+\mathtt{R}(\mathtt{v},\mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))|\!\}^{\mathrm{a}} \quad = \quad \{x\}$$

$$[\![\, \exists \mathtt{v}\,(+\mathtt{R}(\mathtt{v},\mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))\,]\!]^{\mathrm{c}} = \{\!|X : \exists \mathtt{v}\,(+\mathtt{R}(\mathtt{v},\mathtt{v}) \wedge \neg \mathtt{p}(\mathtt{v}))|\!\}^{\mathrm{c}} \quad = \quad \{u, v, x\}.$$

Technical reference

M. Huth and S. Pradhan, *Consistent partial model checking*,
Electronic Notes in Theoretical Computer Science 73 (2003),
URL: `http://www.elsevier.nl/locate/entcs/volume73.html`,
39 pages.

Conclusions

(This page is intentionally left blank.)