On model checking multiple hybrid views

Altaf Hussain & Michael Huth
Department of Computing
Imperial College London

outline

1 Motivation:

- View as abstraction of parameterized systems
- Modelling & analysis with multiple views

2 Views and their refinement

3 Decision problems for refinement

4 Common refinement checks

5 Summary views

6 Future work, leverage, and conclusions

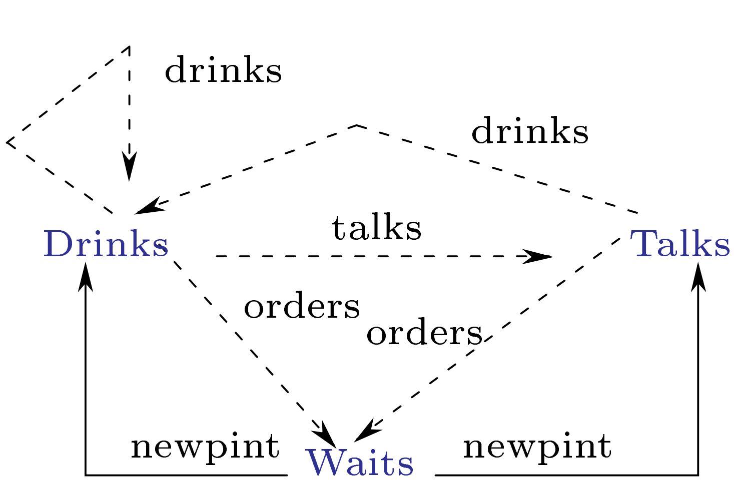
Motivation: View as abstraction of parameterized systems

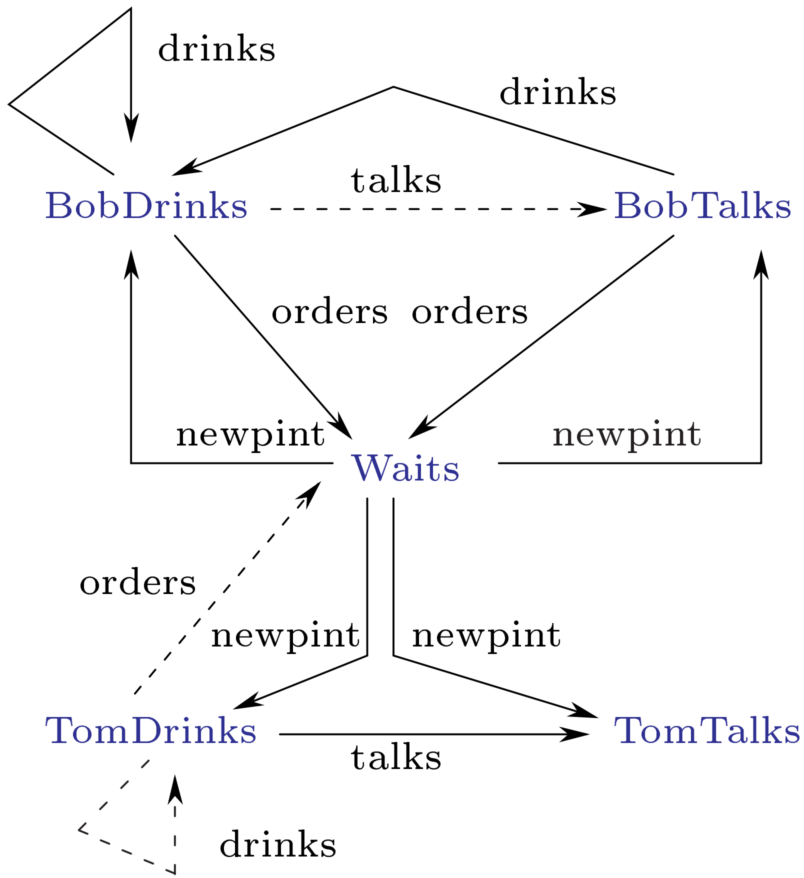
Uses of parameters in model checking:

- number of protocols, e.g., in cache coherence protocols,
- length of queue, e.g., in bakery protocol, or
- topology of network

Under-specified systems: describe sets of completely specified systems.
Abstraction used to achieve above usages of parameters.

An example of abstraction of parameters





BobDrinks refines Drinks,

TomTalks refines Talks ...

$$Q = \{(\text{Drinks}, \text{BobDrinks}), (\text{Drinks}, \text{TomDrinks}), (\text{Waits}, \text{Waits}),$$
$$(\text{Talks}, \text{BobTalks}), (\text{Talks}, \text{TomTalks})\}$$

Motivation: Modelling & analysis with multiple views

Views as mathematical models occur in many settings:

1. Local and relative perception of asynchronous communication, modelled by message sequence chart.
2. 'View' of a local database.
3. High-risk requirements of stakeholders in a development project, etc.

Reasoning about a collection of such 'views' is of considerable practical value, e.g. in determining consistency or locating conflicts.

Contributions of this paper

Given finitely many views (M_i) for $i \in I$:

1. Generalized model checking problem:

   "For a property ϕ, is there a 2-valued refinement of *all* M_i satisfying ϕ?"

   is EXPTIME-complete.

2. The decision problem:

   "Is there a 2-valued refinement of all M_i?"

   is in PTIME.

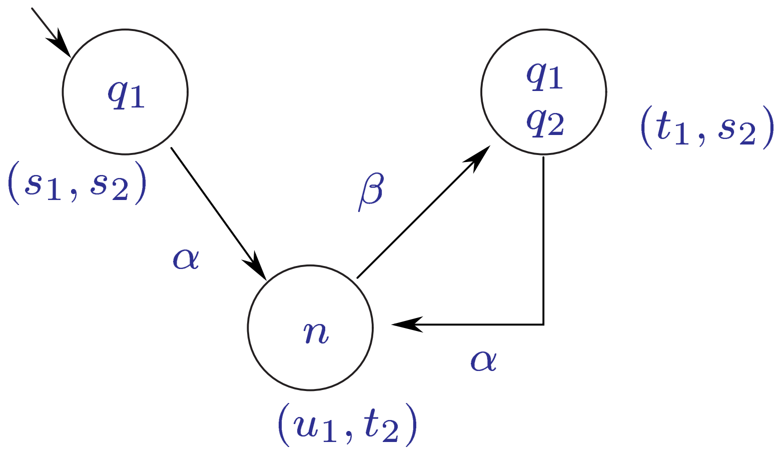
3. Construct 3-valued "summary" views as consistent & informative common abstractions & refinements of all M_i.

Views as 3-valued hybrid models

A 3-valued hybrid model $M = (\Sigma, R^a, R^c, L^a, L^c)$

- $\Sigma = \{\text{Drinks}, \text{Talks}, \text{Waits}\}$ state space
- $R^a, R^c \subseteq \Sigma \times Act \times \Sigma$, and $R^a \subseteq R^c$ (consistency condition)
- R^a solid lines and $\Sigma \times Act \times \Sigma \setminus R^c$ (*contractual guarantees*)
- $R^c \setminus R^a$ dashed lines (*contractual possibilities*)
- $L^a, L^c \colon AP \cup Nom \to \mathbb{P}(S)$ with $L^a(q) \subseteq L^c(q)$ for all $q \in AP \cup Nom$ subject to:
  1. for all $n \in Nom$, $\mid L^a(n) \mid \geq 1$ and $L^c(n) \neq \{\}$,
  2. for all $n \in Nom$, if $L^a(n)$ is non-empty, $L^a(n) = L^c(n)$.

Example of a 2-valued view



A 2-valued view with $AP = \{q_1, q_2\}$, $Nom = \{n\}$, $Act = \{\alpha, \beta, u\}$, and three states (s_1, s_2), (u_1, t_2), and (t_1, s_2). It is a common completion of two 3-valued views shown later.

Multiple views and their decision problems

Let $\mathcal{C}(\mathcal{V}) = \{(N, t) \mid \forall (M, s) \in \mathcal{V} \colon (N, t) \in \mathcal{C}(M, s)\}$ = the set of *common completions* of $\mathcal{V}$. For property ϕ of *hybrid mu-calculus*, we define:

1. *Consistency:* $\mathbb{C}(\mathcal{V})$ holds iff all views of $\mathcal{V}$ have common completion, i.e. iff $\mathcal{C}(\mathcal{V}) \neq \{\}$.

2. *Satisfiability:* $\mathbb{S}(\mathcal{V}, \phi)$ is true iff there is common completion of $\mathcal{V}$ that satisfies ϕ, i.e. iff $\{(N, t) \in \mathcal{C}(\mathcal{V}) \mid t \models \phi\} \neq \{\}$.

3. *Validity:* $\mathbb{V}(\mathcal{V}, \phi)$ holds iff all common completions of $\mathcal{V}$ satisfy ϕ.

Complexity of the decision problems

1. Each pointed 3-valued view (M_i, s_i) has a formula $[M_i, s_i]$ of the hybrid mu-calculus such that $\mathbb{S}(\mathcal{V}, \phi)$ reduces to $SAT(\phi \wedge \bigwedge_i [M_i, s_i])$.

2. The decision problems $\mathbb{C}(\mathcal{V})$, $\mathbb{S}(\mathcal{V}, \phi)$, and $\mathbb{V}(\mathcal{V}, \phi)$ are reducible to satisfiability checks of hybrid mu-calculus over 2-valued views and in EXPTIME.

Refinement between views

Let $\mathcal{V} = \{(M_i, s_i) \mid 1 \leq i \leq k\}$, each M_i having state space S_i.

1. We denote product space $\prod_{i=1}^{k} S_i$ by $S_{\mathcal{V}}$, write $\mathbf{t}$ for tuples $(t_1, t_2, \ldots, t_k) \in S_{\mathcal{V}}$, and use $\mathcal{V}_{\mathbf{s}}$ to stress that s_i is the initial state in each (M_i, s_i) of $\mathcal{V}$.

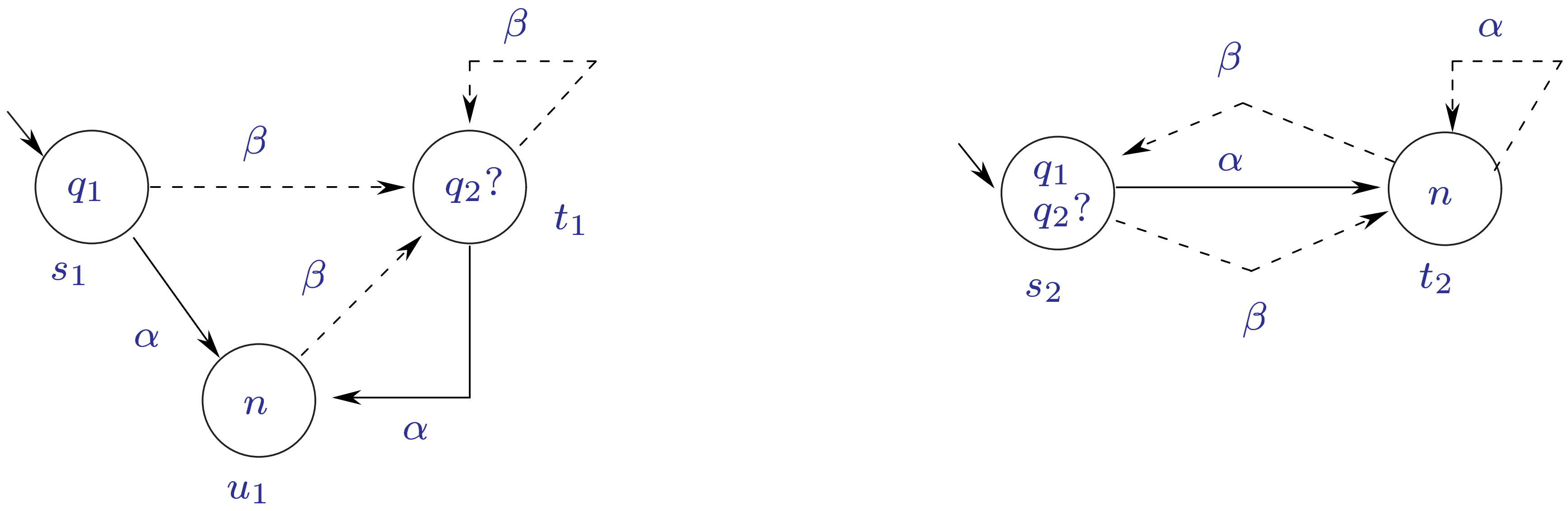
2. A *common refinement witness* is a relation $W \subseteq S_{\mathcal{V}}$ such that $\mathbf{t} \in W$ implies
   (a) for all i and $q \in AP \cup Nom$, if $t_i \in L^a(q)$ then $t_j \in L^c(q)$ for all $j \neq i$, % "Shadow a-moves by c-moves"
   (b) for all i and $\alpha \in Act \cup \overline{Act}$, if $(t_i, \alpha, t'_i) \in R^a$, there is $\mathbf{t}' \in W$ such that $(t_j, \alpha, t'_j) \in R^c$ for all $j \neq i$, and % "Shadow a-moves by c-moves"
   (c) for all $n \in Nom$, there is $\mathbf{t} \in W$ such that for all i, $t_i \in L^c(n)$ % "consistency for nominals"

PTIME common refinement check

```
No = {};
let (bad (t, No)) = // fails clause (a) of definition:
  ((some i, j, q | t_i in L^a(q) && not t_j in L^c(q))
  ||                 // fails clause (b) of definition:
   (some (t_i,a,x) in R^a | all t' in S_V minus No |
      x = t'_i ==> some j | not (t_j,a,t_j') in R^c
  )) in
  { while (some t in S_V minus No | (bad (t, No))) {
      No = No union {t};
  } // else-branch: fails clause (c) of definition
if (all n in Nom | some t' in S_V minus No | all i | t_i in L^c(n))
  { Yes = S_V minus No; } else { Yes = {}; }
```

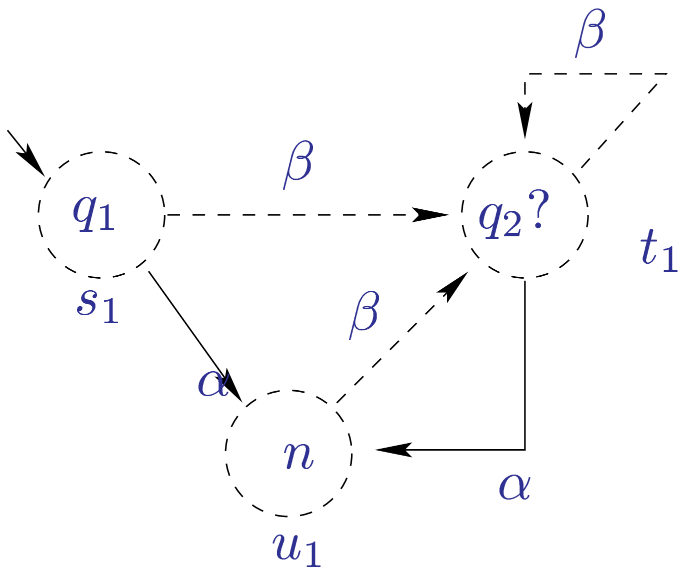
Yes returns all tuples that have common refinement

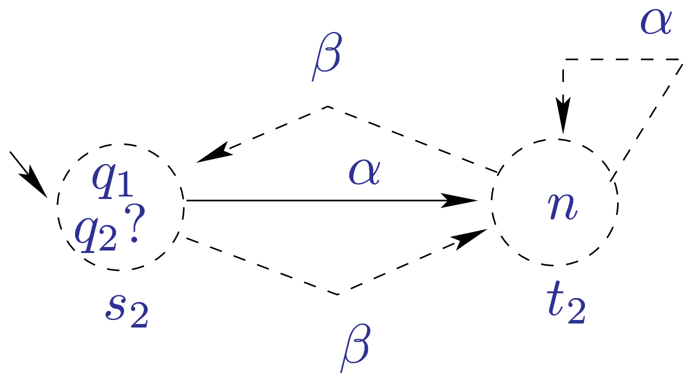
Static summary views

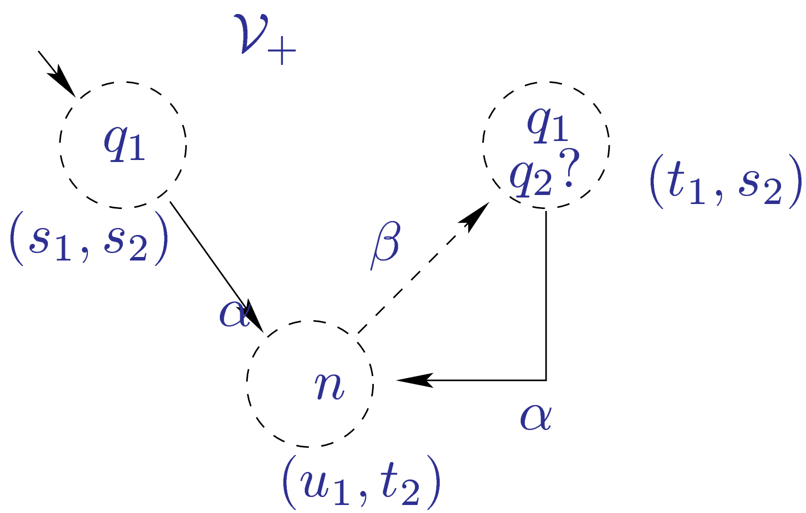


A $\mathcal{V} = \{(M_1, s_1), (M_2, s_2)\}$ for which there are common refinements.

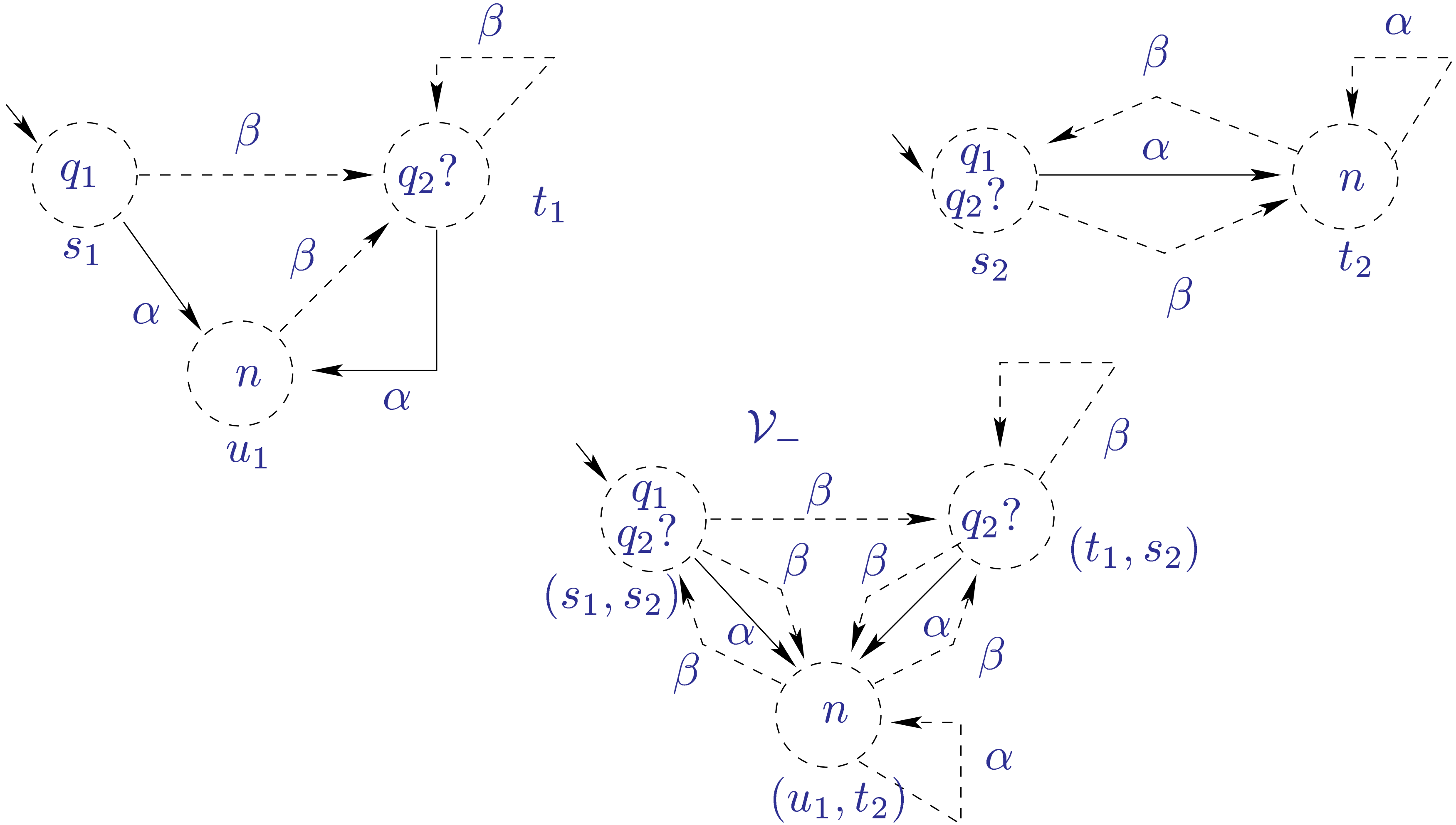
Summary view: informative common refinement







Summary view: informative common abstraction



Future work and leverage

- Model checking $\mathcal{V}_- \models \phi$ too crude for $\mathbb{S}(\mathcal{V}, \phi)$.

- Dually, Model checking $\mathcal{V}_+ \models \phi$ too crude for $\mathbb{V}(\mathcal{V}, \phi)$.

- Proof-of-concept implementations for specifying and reasoning about multiple views collectively.

- Tools guided by empirical issues, e.g., identifying domains were guided simulations in common refinements are more valuable than model checking.

Conclusions

Studied finite sets of hybrid views $\mathcal{V}$ and their common refinement.

- Decision problems "Is there is common refinement of $\mathcal{V}$ satisfying ϕ?" (satisfiability) and "Does ϕ hold for all common refinements of $\mathcal{V}$?" (validity) are EXPTIME-complete for the hybrid mu-calculus.

- Gave a PTIME decision procedure for checking whether such a set $\mathcal{V}$ has common refinement (satisfiability for ϕ being $\mathtt{true}$).

- Used this procedure to compute state space of "summary" views that are informative and consistent common refinements (respectively, abstractions).