

# An extension of LTL model-checking

S. Ghilardi<sup>1</sup>, E. Nicolini<sup>2</sup>, S. Ranise<sup>2</sup>, and D. Zucchelli<sup>1,2</sup>

<sup>1</sup>Università degli Studi di Milano

<sup>2</sup>LORIA & INRIA-Lorraine

Nancy - March, 29 2007



# Motivations

- [Manna and Pnueli 1995]: First-Order Logic (FOL) + Linear time Temporal Logic (LTL) precisely state verification problems for the class of reactive systems;
- FOL: (possibly infinite) data structures used by a reactive system;
- LTL: dynamic behavior of a reactive system;
- LTL + FOL = interaction between data flow and control flow in infinite state systems.



# Motivations

- [Manna and Pnueli 1995]: First-Order Logic (FOL) + Linear time Temporal Logic (LTL) precisely state verification problems for the class of reactive systems;
- FOL: (possibly infinite) data structures used by a reactive system;
- LTL: dynamic behavior of a reactive system;
- LTL + FOL = interaction between data flow and control flow in infinite state systems.



# Motivations

- [Manna and Pnueli 1995]: First-Order Logic (FOL) + Linear time Temporal Logic (LTL) precisely state verification problems for the class of reactive systems;
- FOL: (possibly infinite) data structures used by a reactive system;
- LTL: dynamic behavior of a reactive system;
- LTL + FOL = interaction between data flow and control flow in infinite state systems.



# Motivations

- [Manna and Pnueli 1995]: First-Order Logic (FOL) + Linear time Temporal Logic (LTL) precisely state verification problems for the class of reactive systems;
- FOL: (possibly infinite) data structures used by a reactive system;
- LTL: dynamic behavior of a reactive system;
- LTL + FOL = interaction between data flow and control flow in infinite state systems.



# The RoadMap

- 1 LTL-theories
- 2 Transition Systems
- 3 Main Result



# The RoadMap

- 1 LTL-theories
- 2 Transition Systems
- 3 Main Result



# The RoadMap

- 1 LTL-theories
- 2 Transition Systems**
- 3 Main Result



# The RoadMap

- 1 LTL-theories
- 2 Transition Systems
- 3 Main Result**



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# Safety Model-Checking Problem

The problem of checking if ‘bad states’ are reachable by a given transition system.

## 1 LTL-theories

- ▶ First-order  $\Sigma$ -theory  $T$ ;
- ▶ Temporal model: a sequence  $\mathcal{M}_1, \mathcal{M}_2, \dots$  of standard (first-order) models of  $T$  over the same carrier;
- ▶ Symbols from  $\Sigma_r \subseteq \Sigma$  are *time independent*, other symbols are *time dependent*.

## 2 Transition Systems

- ▶ The *initial/bad states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

## 3 Main Result

- ▶ Approach inspired by [Ghilardi 2004]: combination over non-disjoint theories.



# The RoadMap

## 1 LTL-theories



# LTL-theory: Syntax

## Definition (LTL-theory)

An *LTL-theory* is a 5-tuple  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  where  $\Sigma$  is a signature,  $T$  is a  $\Sigma$ -theory (called the underlying theory of  $\mathcal{T}$ ),  $\Sigma_r$  is a subsignature of  $\Sigma$ , and  $\underline{a}, \underline{c}$  are sets of free constants.

- $\Sigma_r$  is the *time-independent subsignature* of the LTL-theory;
- the constants  $\underline{c}$  (called *system parameters*) will be interpreted in a time-independent way;
- the constants  $\underline{a}$  (called *system variables*) will be interpreted in a time-dependent way.



# LTL-theory: Syntax

## Definition (LTL-theory)

An *LTL-theory* is a 5-tuple  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  where  $\Sigma$  is a signature,  $T$  is a  $\Sigma$ -theory (called the underlying theory of  $\mathcal{T}$ ),  $\Sigma_r$  is a subsignature of  $\Sigma$ , and  $\underline{a}, \underline{c}$  are sets of free constants.

- $\Sigma_r$  is the *time-independent subsignature* of the LTL-theory;
- the constants  $\underline{c}$  (called *system parameters*) will be interpreted in a time-independent way;
- the constants  $\underline{a}$  (called *system variables*) will be interpreted in a time-dependent way.



# LTL-theory: Syntax

## Definition (LTL-theory)

An *LTL-theory* is a 5-tuple  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  where  $\Sigma$  is a signature,  $T$  is a  $\Sigma$ -theory (called the underlying theory of  $\mathcal{T}$ ),  $\Sigma_r$  is a subsignature of  $\Sigma$ , and  $\underline{a}, \underline{c}$  are sets of free constants.

- $\Sigma_r$  is the *time-independent subsignature* of the LTL-theory;
- the constants  $\underline{c}$  (called *system parameters*) will be interpreted in a time-independent way;
- the constants  $\underline{a}$  (called *system variables*) will be interpreted in a time-dependent way.



# LTL-theory: Syntax

## Definition (LTL-theory)

An *LTL-theory* is a 5-tuple  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  where  $\Sigma$  is a signature,  $T$  is a  $\Sigma$ -theory (called the underlying theory of  $\mathcal{T}$ ),  $\Sigma_r$  is a subsignature of  $\Sigma$ , and  $\underline{a}, \underline{c}$  are sets of free constants.

- $\Sigma_r$  is the *time-independent subsignature* of the LTL-theory;
- the constants  $\underline{c}$  (called *system parameters*) will be interpreted in a time-independent way;
- the constants  $\underline{a}$  (called *system variables*) will be interpreted in a time-dependent way.



# LTL-theory: Semantic

## Definition

An LTL( $\Sigma^{\underline{a}, \underline{c}}$ )-structure  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  is *appropriate* for an LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  iff we have

$$\mathcal{M}_n \models T, \quad \mathcal{I}_n(f) = \mathcal{I}_m(f), \quad \mathcal{I}_n(P) = \mathcal{I}_m(P), \quad \mathcal{I}_n(c) = \mathcal{I}_m(c).$$

for all  $m, n \in \mathbb{N}$ , for each function symbol  $f \in \Sigma_r$ , for each relational symbol  $P \in \Sigma_r$ , and for all constant  $c \in \underline{c}$ .



# Locally finite compatible LTL-theories

## Definition (Locally finite compatible LTL-theories)

An LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  is *locally finite compatible* iff there is a universal and effectively locally finite  $\Sigma_r$ -theory  $T_r$  such that  $T$  is  $T_r$ -compatible and the constraint satisfiability problem for  $T$  is decidable.

- $T_r$ -compatibility and local finiteness requirements are the key ingredients to guarantee completeness and termination of our procedure;
- the (safety) model-checking problem we are going to introduce is related to a combination of **infinite** (partially renamed) copies of the theory  $T$  sharing the common subtheory  $T_r$ .



# Locally finite compatible LTL-theories

## Definition (Locally finite compatible LTL-theories)

An LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  is *locally finite compatible* iff there is a universal and effectively locally finite  $\Sigma_r$ -theory  $T_r$  such that  $T$  is  $T_r$ -compatible and the constraint satisfiability problem for  $T$  is decidable.

- $T_r$ -compatibility and local finiteness requirements are the key ingredients to guarantee completeness and termination of our procedure;
- the (safety) model-checking problem we are going to introduce is related to a combination of **infinite** (partially renamed) copies of the theory  $T$  sharing the common subtheory  $T_r$ .



# Locally finite compatible LTL-theories

## Definition (Locally finite compatible LTL-theories)

An LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  is *locally finite compatible* iff there is a universal and effectively locally finite  $\Sigma_r$ -theory  $T_r$  such that  $T$  is  $T_r$ -compatible and the constraint satisfiability problem for  $T$  is decidable.

- $T_r$ -compatibility and local finiteness requirements are the key ingredients to guarantee completeness and termination of our procedure;
- the (safety) model-checking problem we are going to introduce is related to a combination of **infinite** (partially renamed) copies of the theory  $T$  sharing the common subtheory  $T_r$ .



# Digression: Non-Disjoint Combination

- 1 The  $T_r$ -compatibility of a  $\Sigma$ -theory  $T$  is a (quite technical) model-theoretic notion;
  - ▶ In practice (sufficient condition):  $T$  includes a (universal)  $\Sigma_r$ -theory  $T_r$  which admits quantifier elimination ( $\Sigma_r \subseteq \Sigma$ );
  - ▶ Notice that we do not need to have a characterization of  $T_r$ : the mere information of its existence is enough for our decision procedures to be sound and complete and to implement them;
- 2 A  $\Sigma_r$ -theory  $T_r$  is (*effectively*) *locally finite* iff  $\Sigma_r$  is finite and there exists a finite (and computable) set of terms that are “representative” modulo  $T_r$ -equivalence of the whole set of  $\Sigma_r$ -terms.
  - ▶ Examples: purely relational signature, orders, arithmetic modulo.



# Digression: Non-Disjoint Combination

- 1 The  $T_r$ -compatibility of a  $\Sigma$ -theory  $T$  is a (quite technical) model-theoretic notion;
  - ▶ In practice (sufficient condition):  $T$  includes a (universal)  $\Sigma_r$ -theory  $T_r$  which admits quantifier elimination ( $\Sigma_r \subseteq \Sigma$ );
  - ▶ Notice that we do not need to have a characterization of  $T_r$ : the mere information of its existence is enough for our decision procedures to be sound and complete and to implement them;
- 2 A  $\Sigma_r$ -theory  $T_r$  is (*effectively*) *locally finite* iff  $\Sigma_r$  is finite and there exists a finite (and computable) set of terms that are “representative” modulo  $T_r$ -equivalence of the whole set of  $\Sigma_r$ -terms.
  - ▶ Examples: purely relational signature, orders, arithmetic modulo.



# Digression: Non-Disjoint Combination

- 1 The  $T_r$ -compatibility of a  $\Sigma$ -theory  $T$  is a (quite technical) model-theoretic notion;
  - ▶ In practice (sufficient condition):  $T$  includes a (universal)  $\Sigma_r$ -theory  $T_r$  which admits quantifier elimination ( $\Sigma_r \subseteq \Sigma$ );
  - ▶ Notice that we do not need to have a characterization of  $T_r$ : the mere information of its existence is enough for our decision procedures to be sound and complete and to implement them;
- 2 A  $\Sigma_r$ -theory  $T_r$  is (*effectively*) *locally finite* iff  $\Sigma_r$  is finite and there exists a finite (and computable) set of terms that are “representative” modulo  $T_r$ -equivalence of the whole set of  $\Sigma_r$ -terms.
  - ▶ Examples: purely relational signature, orders, arithmetic modulo.



# Digression: Non-Disjoint Combination

- 1 The  $T_r$ -compatibility of a  $\Sigma$ -theory  $T$  is a (quite technical) model-theoretic notion;
  - ▶ In practice (sufficient condition):  $T$  includes a (universal)  $\Sigma_r$ -theory  $T_r$  which admits quantifier elimination ( $\Sigma_r \subseteq \Sigma$ );
  - ▶ Notice that we do not need to have a characterization of  $T_r$ : the mere information of its existence is enough for our decision procedures to be sound and complete and to implement them;
- 2 A  $\Sigma_r$ -theory  $T_r$  is (*effectively*) *locally finite* iff  $\Sigma_r$  is finite and there exists a finite (and computable) set of terms that are “representative” modulo  $T_r$ -equivalence of the whole set of  $\Sigma_r$ -terms.
  - ▶ Examples: purely relational signature, orders, arithmetic modulo.



# Digression: Non-Disjoint Combination

- 1 The  $T_r$ -compatibility of a  $\Sigma$ -theory  $T$  is a (quite technical) model-theoretic notion;
  - ▶ In practice (sufficient condition):  $T$  includes a (universal)  $\Sigma_r$ -theory  $T_r$  which admits quantifier elimination ( $\Sigma_r \subseteq \Sigma$ );
  - ▶ Notice that we do not need to have a characterization of  $T_r$ : the mere information of its existence is enough for our decision procedures to be sound and complete and to implement them;
- 2 A  $\Sigma_r$ -theory  $T_r$  is (*effectively*) *locally finite* iff  $\Sigma_r$  is finite and there exists a finite (and computable) set of terms that are “representative” modulo  $T_r$ -equivalence of the whole set of  $\Sigma_r$ -terms.
  - ▶ Examples: purely relational signature, orders, arithmetic modulo.



# The RoadMap

- 1 LTL-theories
- 2 **Transition Systems**



# LTL-System Specifications: Syntax

## Definition (LTL-System Specification)

An *LTL-system specification* is an LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  (with finitely many system variables and parameters) endowed with a transition relation  $\delta(\underline{a}^0, \underline{a}^1)$  and with an initial state description  $\iota(\underline{a})$ .

What is the transition relation  $\delta(\underline{a}^0, \underline{a}^1)$ ?



# LTL-System Specifications: Syntax

## Definition (LTL-System Specification)

An *LTL-system specification* is an LTL-theory  $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$  (with finitely many system variables and parameters) endowed with a **transition relation**  $\delta(\underline{a}^0, \underline{a}^1)$  and with an initial state description  $\iota(\underline{a})$ .

What is the transition relation  $\delta(\underline{a}^0, \underline{a}^1)$ ?



# Transition Relations: $(\Sigma \oplus_{\Sigma_r} \Sigma)$ -sentences

- We define the *one-step signature* as

$$\Sigma \oplus_{\Sigma_r} \Sigma := ((\Sigma \setminus \Sigma_r) \uplus (\Sigma \setminus \Sigma_r)) \cup \Sigma_r;$$

- $\delta(\underline{a}^0, \underline{a}^1)$  is a  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -sentence, i.e. a sentence on the signature having two renamed occurrences of the time-dependent symbol ( $r^0$  and  $r^1$  for  $r \in \Sigma^{\underline{a}, \underline{c}} \setminus \Sigma_r^{\underline{c}}$ );
- A  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -structure for  $\delta(\underline{a}^0, \underline{a}^1)$  can be seen as  $\mathcal{M}_0 \oplus_{\Sigma_r^{\underline{c}}} \mathcal{M}_1$  where  $\mathcal{M}_i$  are  $\Sigma^{\underline{a}, \underline{c}}$ -structures with the same  $\Sigma_r^{\underline{c}}$ -reduct. (*Combination!*)



# Transition Relations: $(\Sigma \oplus_{\Sigma_r} \Sigma)$ -sentences

- We define the *one-step signature* as

$$\Sigma \oplus_{\Sigma_r} \Sigma := ((\Sigma \setminus \Sigma_r) \uplus (\Sigma \setminus \Sigma_r)) \cup \Sigma_r;$$

- $\delta(\underline{a}^0, \underline{a}^1)$  is a  $(\Sigma^{\underline{a},c} \oplus_{\Sigma_r^c} \Sigma^{\underline{a},c})$ -sentence, i.e. a sentence on the signature having two renamed occurrences of the time-dependent symbol ( $r^0$  and  $r^1$  for  $r \in \Sigma^{\underline{a},c} \setminus \Sigma_r^c$ );
- A  $(\Sigma^{\underline{a},c} \oplus_{\Sigma_r^c} \Sigma^{\underline{a},c})$ -structure for  $\delta(\underline{a}^0, \underline{a}^1)$  can be seen as  $\mathcal{M}_0 \oplus_{\Sigma_r^c} \mathcal{M}_1$  where  $\mathcal{M}_i$  are  $\Sigma^{\underline{a},c}$ -structures with the same  $\Sigma_r^c$ -reduct. (*Combination!*)



# Transition Relations: $(\Sigma \oplus_{\Sigma_r} \Sigma)$ -sentences

- We define the *one-step signature* as

$$\Sigma \oplus_{\Sigma_r} \Sigma := ((\Sigma \setminus \Sigma_r) \uplus (\Sigma \setminus \Sigma_r)) \cup \Sigma_r;$$

- $\delta(\underline{a}^0, \underline{a}^1)$  is a  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -sentence, i.e. a sentence on the signature having two renamed occurrences of the time-dependent symbol ( $r^0$  and  $r^1$  for  $r \in \Sigma^{\underline{a}, \underline{c}} \setminus \Sigma_r^{\underline{c}}$ );
- A  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -structure for  $\delta(\underline{a}^0, \underline{a}^1)$  can be seen as  $\mathcal{M}_0 \oplus_{\Sigma_r^{\underline{c}}} \mathcal{M}_1$  where  $\mathcal{M}_i$  are  $\Sigma^{\underline{a}, \underline{c}}$ -structures with the same  $\Sigma_r^{\underline{c}}$ -reduct. (*Combination!*)



# Transition Relations: $(\Sigma \oplus_{\Sigma_r} \Sigma)$ -sentences

- We define the *one-step signature* as

$$\Sigma \oplus_{\Sigma_r} \Sigma := ((\Sigma \setminus \Sigma_r) \uplus (\Sigma \setminus \Sigma_r)) \cup \Sigma_r;$$

- $\delta(\underline{a}^0, \underline{a}^1)$  is a  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -sentence, i.e. a sentence on the signature having two renamed occurrences of the time-dependent symbol ( $r^0$  and  $r^1$  for  $r \in \Sigma^{\underline{a}, \underline{c}} \setminus \Sigma_r^{\underline{c}}$ );
- A  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -structure for  $\delta(\underline{a}^0, \underline{a}^1)$  can be seen as  $\mathcal{M}_0 \oplus_{\Sigma_r^{\underline{c}}} \mathcal{M}_1$  where  $\mathcal{M}_i$  are  $\Sigma^{\underline{a}, \underline{c}}$ -structures with the same  $\Sigma_r^{\underline{c}}$ -reduct. (*Combination!*)



# LTL-System Specifications: Semantic

## Definition

An LTL( $\Sigma^{\underline{a}, \underline{c}}$ )-structure  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  is a *run* for an LTL-system specification  $(\mathcal{T}, \delta, \iota)$  iff it is appropriate for  $\mathcal{T}$  and

- 1  $\mathcal{M}_0 \models \iota(\underline{a})$
- 2  $\mathcal{M}_n \oplus_{\Sigma^{\underline{c}}} \mathcal{M}_{n+1} \models \delta(\underline{a}^0, \underline{a}^1)$ , for every  $n \geq 0$ .



# LTL-System Specifications: Semantic

## Definition

An LTL( $\Sigma^{\underline{a}, \underline{c}}$ )-structure  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  is a *run* for an LTL-system specification  $(\mathcal{T}, \delta, \iota)$  iff it is appropriate for  $\mathcal{T}$  and

- 1  $\mathcal{M}_0 \models \iota(\underline{a})$
- 2  $\mathcal{M}_n \oplus_{\Sigma^{\underline{c}}} \mathcal{M}_{n+1} \models \delta(\underline{a}^0, \underline{a}^1)$ , for every  $n \geq 0$ .



# LTL-System Specifications: Semantic

## Definition

An LTL( $\Sigma^{\underline{a}, \underline{c}}$ )-structure  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  is a *run* for an LTL-system specification  $(\mathcal{T}, \delta, \iota)$  iff it is appropriate for  $\mathcal{T}$  and

- 1  $\mathcal{M}_0 \models \iota(\underline{a})$
- 2  $\mathcal{M}_n \oplus_{\Sigma^{\underline{c}}} \mathcal{M}_{n+1} \models \delta(\underline{a}^0, \underline{a}^1)$ , for every  $n \geq 0$ .



# The RoadMap

- 1 LTL-theories
- 2 Transition Systems
- 3 **Main Result**



# Statement of the Problem

## Definition (Safety Model-Checking Problem)

The *safety model-checking problem* for the system specification  $(\mathcal{T}, \delta, \iota)$  is the following: decide whether there is a run  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  for  $(\mathcal{T}, \delta, \iota)$  such that  $\mathcal{M}_n \models v$  for some  $n \in \mathbb{N}$ . The system specification  $(\mathcal{T}, \delta, \iota)$  is *safe for  $v$*  iff the safety model-checking problem for  $v$  has a negative solution.

- Here  $v$  is a  $\Sigma^{a,c}$ -sentence describes the set of **unsafe** states;
- When  $\delta, \iota$  and  $v$  are ground sentences, we talk of *ground safety model-checking problem*.

Main result: the **ground** safety model-checking problem for **locally finite compatible LTL-theories** is decidable!



# Statement of the Problem

## Definition (Safety Model-Checking Problem)

The *safety model-checking problem* for the system specification  $(\mathcal{T}, \delta, \iota)$  is the following: decide whether there is a run  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  for  $(\mathcal{T}, \delta, \iota)$  such that  $\mathcal{M}_n \models v$  for some  $n \in \mathbb{N}$ . The system specification  $(\mathcal{T}, \delta, \iota)$  is *safe for  $v$*  iff the safety model-checking problem for  $v$  has a negative solution.

- Here  $v$  is a  $\Sigma^{a,c}$ -sentence describes the set of **unsafe** states;
- When  $\delta, \iota$  and  $v$  are ground sentences, we talk of *ground safety model-checking problem*.

Main result: the **ground** safety model-checking problem for **locally finite compatible LTL-theories** is decidable!



# Statement of the Problem

## Definition (Safety Model-Checking Problem)

The *safety model-checking problem* for the system specification  $(\mathcal{T}, \delta, \iota)$  is the following: decide whether there is a run  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  for  $(\mathcal{T}, \delta, \iota)$  such that  $\mathcal{M}_n \models v$  for some  $n \in \mathbb{N}$ . The system specification  $(\mathcal{T}, \delta, \iota)$  is *safe for  $v$*  iff the safety model-checking problem for  $v$  has a negative solution.

- Here  $v$  is a  $\Sigma^{a,c}$ -sentence describes the set of **unsafe** states;
- When  $\delta, \iota$  and  $v$  are ground sentences, we talk of *ground safety model-checking problem*.

Main result: the **ground** safety model-checking problem for **locally finite compatible LTL-theories** is decidable!



# Statement of the Problem

## Definition (Safety Model-Checking Problem)

The *safety model-checking problem* for the system specification  $(\mathcal{T}, \delta, \iota)$  is the following: decide whether there is a run  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  for  $(\mathcal{T}, \delta, \iota)$  such that  $\mathcal{M}_n \models v$  for some  $n \in \mathbb{N}$ . The system specification  $(\mathcal{T}, \delta, \iota)$  is *safe for  $v$*  iff the safety model-checking problem for  $v$  has a negative solution.

- Here  $v$  is a  $\Sigma^{a,c}$ -sentence describes the set of **unsafe** states;
- When  $\delta, \iota$  and  $v$  are ground sentences, we talk of *ground safety model-checking problem*.

Main result: the **ground** safety model-checking problem for **locally finite compatible LTL-theories** is decidable!



# Statement of the Problem

## Definition (Safety Model-Checking Problem)

The *safety model-checking problem* for the system specification  $(\mathcal{T}, \delta, \iota)$  is the following: decide whether there is a run  $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$  for  $(\mathcal{T}, \delta, \iota)$  such that  $\mathcal{M}_n \models v$  for some  $n \in \mathbb{N}$ . The system specification  $(\mathcal{T}, \delta, \iota)$  is *safe for  $v$*  iff the safety model-checking problem for  $v$  has a negative solution.

- Here  $v$  is a  $\Sigma^{a,c}$ -sentence describes the set of **unsafe** states;
- When  $\delta, \iota$  and  $v$  are ground sentences, we talk of *ground safety model-checking problem*.

Main result: the **ground** safety model-checking problem for **locally finite compatible LTL-theories** is decidable!



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $\mathcal{T}$ -satisfiable.



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $\mathcal{T}$ -satisfiable.



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $\mathcal{T}$ -satisfiable.



# The Key Technical Concept

Our main definition of safety graph relies on the following

## Definition (Purely Left/Right Sentence)

A ground  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -sentence  $\delta$  is said to be *purely left* (*purely right*) iff for each symbol  $r \in \Sigma \setminus \Sigma_r$ , we have that  $r^1$  ( $r^0$ , resp.) does not occur in  $\delta$ .

- Each assignment to the atoms of the purification  $\tilde{\delta}$  of the transition relation  $\delta$  can be seen as a conjunction of **purely left** and **purely right** literals.



# The Key Technical Concept

Our main definition of safety graph relies on the following

## Definition (Purely Left/Right Sentence)

A ground  $(\Sigma^{\underline{a}, \underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a}, \underline{c}})$ -sentence  $\delta$  is said to be *purely left* (*purely right*) iff for each symbol  $r \in \Sigma \setminus \Sigma_r$ , we have that  $r^1$  ( $r^0$ , resp.) does not occur in  $\delta$ .

- Each assignment to the atoms of the purification  $\tilde{\delta}$  of the transition relation  $\delta$  can be seen as a conjunction of **purely left** and **purely right** literals.



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $T$ -satisfiable.

**initial nodes** nodes  $(V, G)$  such that  $\iota(\underline{a}^0) \wedge V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $T$ -satisfiable;

**terminal nodes** nodes  $(V, G)$  such that  $V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge v(\underline{a}^1) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $T$ -satisfiable.



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $\mathcal{T}$ -satisfiable.

**initial nodes** nodes  $(V, G)$  such that  $\iota(\underline{a}^0) \wedge V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $\mathcal{T}$ -satisfiable;

**terminal nodes** nodes  $(V, G)$  such that  $V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge v(\underline{a}^1) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $\mathcal{T}$ -satisfiable.



# Main Definition

## Definition (Safety Graph)

The *safety graph* associated to the LTL-system specification  $(\mathcal{T}, \delta, \iota)$  based on the locally finite compatible LTL-theory  $\mathcal{T}$  is the directed graph defined as follows:

- the nodes are the pairs  $(V, G)$  where  $V$  is a  $\tilde{\delta}$ -assignment and  $G$  is a transition  $\Sigma_r$ -guessing;
- there is an edge  $(V, G) \rightarrow (W, H)$  iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1)$$

is  $T$ -satisfiable.

**initial nodes** nodes  $(V, G)$  such that  $\iota(\underline{a}^0) \wedge V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $T$ -satisfiable;

**terminal nodes** nodes  $(V, G)$  such that  $V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge v(\underline{a}^1) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$  is  $T$ -satisfiable.



# Main Result

## Proposition

The system is unsafe iff either  $\iota(\underline{a}) \wedge v(\underline{a})$  is  $T$ -satisfiable or there is a path in the safety graph from an initial to a terminal node.

## Proof (Sketch)

A bad run of length  $n + 1$  exists iff, for some  $\tilde{\delta}$ -assignments  $V_1, \dots, V_{n+1}$ , the ground  $(\bigoplus_{\Sigma_r^c}^{n+2} \Sigma^{a,c})$ -sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^n (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge v(\underline{a}^{n+1}) \quad (1)$$

is  $\bigoplus_{\Sigma_r^c}^{n+2} T$ -satisfiable. By contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute  $\Sigma_r$ -ground interpolants of (1) between  $T$  and  $\bigoplus_{\Sigma_r}^j T$ , for  $j = n + 1, \dots, 1$  (an argument based on  $T_r$ -compatibility guarantees they exist). This yields the  $T$ -unsatisfiability of the final node (formula) in the graph; contradiction. □



# Main Result

## Proposition

The system is unsafe iff either  $\iota(\underline{a}) \wedge v(\underline{a})$  is  $T$ -satisfiable or there is a path in the safety graph from an initial to a terminal node.

## Proof (Sketch)

A bad run of length  $n + 1$  exists iff, for some  $\tilde{\delta}$ -assignments  $V_1, \dots, V_{n+1}$ , the ground  $(\bigoplus_{\Sigma_r^c}^{n+2} \Sigma^{\underline{a}, \underline{c}})$ -sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^n (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge v(\underline{a}^{n+1}) \quad (1)$$

is  $\bigoplus_{\Sigma_r^c}^{n+2} T$ -satisfiable. By contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute  $\Sigma_r$ -ground interpolants of (1) between  $T$  and  $\bigoplus_{\Sigma_r}^j T$ , for  $j = n + 1, \dots, 1$  (an argument based on  $T_r$ -compatibility guarantees they exist). This yields the  $T$ -unsatisfiability of the final node (formula) in the graph; contradiction. □



# Main Result

## Proposition

The system is unsafe iff either  $\iota(\underline{a}) \wedge v(\underline{a})$  is  $T$ -satisfiable or there is a path in the safety graph from an initial to a terminal node.

## Proof (Sketch)

A bad run of length  $n + 1$  exists iff, for some  $\tilde{\delta}$ -assignments  $V_1, \dots, V_{n+1}$ , the ground  $(\bigoplus_{\Sigma_r^c}^{n+2} \Sigma^{\underline{a}, \underline{c}})$ -sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^n (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge v(\underline{a}^{n+1}) \quad (1)$$

is  $\bigoplus_{\Sigma_r^c}^{n+2} T$ -satisfiable. By contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute  $\Sigma_r$ -ground interpolants of (1) between  $T$  and  $\bigoplus_{\Sigma_r}^j T$ , for  $j = n + 1, \dots, 1$  (an argument based on  $T_r$ -compatibility guarantees they exist). This yields the  $T$ -unsatisfiability of the final node (formula) in the graph; contradiction. □



# Main Result

## Proposition

The system is unsafe iff either  $\iota(\underline{a}) \wedge v(\underline{a})$  is  $T$ -satisfiable or there is a path in the safety graph from an initial to a terminal node.

## Proof (Sketch)

A bad run of length  $n + 1$  exists iff, for some  $\tilde{\delta}$ -assignments  $V_1, \dots, V_{n+1}$ , the ground  $(\bigoplus_{\Sigma_r^c}^{n+2} \Sigma^{\underline{a}, \underline{c}})$ -sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^n (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge v(\underline{a}^{n+1}) \quad (1)$$

is  $\bigoplus_{\Sigma_r^c}^{n+2} T$ -satisfiable. By contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute  $\Sigma_r$ -ground interpolants of (1) between  $T$  and  $\bigoplus_{\Sigma_r}^j T$ , for  $j = n + 1, \dots, 1$  (an argument based on  $T_r$ -compatibility guarantees they exist). This yields the  $T$ -unsatisfiability of the final node (formula) in the graph; contradiction. □



# Main Result

## Proposition

The system is unsafe iff either  $\iota(\underline{a}) \wedge v(\underline{a})$  is  $T$ -satisfiable or there is a path in the safety graph from an initial to a terminal node.

## Proof (Sketch)

A bad run of length  $n + 1$  exists iff, for some  $\tilde{\delta}$ -assignments  $V_1, \dots, V_{n+1}$ , the ground  $(\bigoplus_{\Sigma_r^c}^{n+2} \Sigma^{\underline{a}, \underline{c}})$ -sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^n (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge v(\underline{a}^{n+1}) \quad (1)$$

is  $\bigoplus_{\Sigma_r^c}^{n+2} T$ -satisfiable. By contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute  $\Sigma_r$ -ground interpolants of (1) between  $T$  and  $\bigoplus_{\Sigma_r}^j T$ , for  $j = n + 1, \dots, 1$  (an argument based on  $T_r$ -compatibility guarantees they exist). This yields the  $T$ -unsatisfiability of the final node (formula) in the graph; contradiction.  $\square$



# Behind the Proof

## Main ideas:

- ‘splitting’ the transition  $\delta(\underline{a}^0, \underline{a}^1)$  into its left and right assignments allows to obtain (by Craig Interpolation Lemma) interpolants over the time-independent subsignature  $\Sigma_r$ ;
- $T_r$ -compatibility allows to conclude that the interpolants are ground;
- effective local finiteness allows to trade guessings for interpolants.



# Behind the Proof

## Main ideas:

- ‘splitting’ the transition  $\delta(\underline{a}^0, \underline{a}^1)$  into its left and right assignments allows to obtain (by Craig Interpolation Lemma) interpolants over the time-independent subsignature  $\Sigma_r$ ;
- $T_r$ -compatibility allows to conclude that the interpolants are ground;
- effective local finiteness allows to trade guessings for interpolants.



# Behind the Proof

Main ideas:

- ‘splitting’ the transition  $\delta(\underline{a}^0, \underline{a}^1)$  into its left and right assignments allows to obtain (by Craig Interpolation Lemma) interpolants over the time-independent subsignature  $\Sigma_r$ ;
- $T_r$ -compatibility allows to conclude that the interpolants are ground;
- effective local finiteness allows to trade guessings for interpolants.



# Conclusions and Future Work

- We have given the decidability of the restriction to safety properties of the model-checking problem modulo locally finite and compatible theories;
- Three main lines of future work:
  - ① how to exploit SMT solvers to solve model-checking problems (i.e., find suitable heuristics to efficiently explore the safety graph);
  - ② find decidability results for model checking of arbitrary temporal properties and modulo richer background theories [Demri et al. 2006];
  - ③ handle universally quantified transition relations and initial state descriptions.



# Conclusions and Future Work

- We have given the decidability of the restriction to safety properties of the model-checking problem modulo locally finite and compatible theories;
- Three main lines of future work:
  - ① how to exploit SMT solvers to solve model-checking problems (i.e., find suitable heuristics to efficiently explore the safety graph);
  - ② find decidability results for model checking of arbitrary temporal properties and modulo richer background theories [Demri et al. 2006];
  - ③ handle universally quantified transition relations and initial state descriptions.



# Conclusions and Future Work

- We have given the decidability of the restriction to safety properties of the model-checking problem modulo locally finite and compatible theories;
- Three main lines of future work:
  - 1 how to exploit SMT solvers to solve model-checking problems (i.e., find suitable heuristics to efficiently explore the safety graph);
  - 2 find decidability results for model checking of arbitrary temporal properties and modulo richer background theories [Demri et al. 2006];
  - 3 handle universally quantified transition relations and initial state descriptions.



# Conclusions and Future Work




- We have given the decidability of the restriction to safety properties of the model-checking problem modulo locally finite and compatible theories;
- Three main lines of future work:
  - 1 how to exploit SMT solvers to solve model-checking problems (i.e., find suitable heuristics to efficiently explore the safety graph);
  - 2 find decidability results for model checking of arbitrary temporal properties and modulo richer background theories [Demri et al. 2006];
  - 3 handle universally quantified transition relations and initial state descriptions.



# Conclusions and Future Work

- We have given the decidability of the restriction to safety properties of the model-checking problem modulo locally finite and compatible theories;
- Three main lines of future work:
  - 1 how to exploit SMT solvers to solve model-checking problems (i.e., find suitable heuristics to efficiently explore the safety graph);
  - 2 find decidability results for model checking of arbitrary temporal properties and modulo richer background theories [Demri et al. 2006];
  - 3 handle universally quantified transition relations and initial state descriptions.



-  S. Demri, A. Finkel, V. Goranko, and G. van Drimmelen.  
Towards a model-checker for counter systems.  
In *Proc. of ATVA 2006*, volume 4218 of *LNCS*, pages 493–507.  
Springer, 2006.
-  S. Ghilardi.  
Model theoretic methods in combined constraint satisfiability.  
*Journal of Automated Reasoning*, 33(3-4):221–249, 2004.
-  Z. Manna and A. Pnueli.  
*Temporal Verification of Reactive Systems: Safety*.  
Springer-Verlag, New York, 1995.

