Towards a Notion of Unsatisfiable Cores for LTL

Viktor Schuppan[1]

FBK-irst, Trento, Italy

FSEN'09, Kish Island, Iran, April 15, 2009

[1]Work partly performed while at Verimag/CNRS. Currently supported by the Provincia Autonoma di Trento (project EMTELOS).

Unsatisfiable Cores

Informal definition:

- An unsatisfiable core is an unsatisfiable formula ϕ' that is derived from another unsatisfiable formula ϕ.
- ϕ' focuses on a reason for ϕ being unsatisfiable.

Use in debugging (often in a declarative setting):

Unsatisfiable cores help a user understand why a formula is unsatisfiable.

Unsatisfiable Cores in Debugging

(selection only)

[CRST08b] conjunction of LTL formulas extended with first order theories.
Example: EURAILCHECK project

- Validation of requirements for railway signalling and control.
- Feasibility study: textual requirements of 100+ pages.
- Unsatisfiable core of a conjunction of 80+ formulas was determined.

[CD91] linear programming

[BDTW93] constraint programming (example: Dutch major league soccer)

[BS01,ZM03b] SAT (examples: planning, FPGA routing)

[SSJ+03,TCJ08] first order relational logic (example: Alloy, based on SAT)

[SC03,WHR+05] description logics, ontologies

Motivation and Approach

Previous work for LTL doesn't proceed into temporal formulas.

The resulting cores are conjunctions of toplevel temporal formulas.

E.g., in $(\mathbf{G}(p \wedge \psi)) \wedge (\mathbf{F}(\neg p \wedge \psi'))$, the whole formula would be reported unsatisfiable irrespective of the relevance and complexity of ψ, ψ'.

Goal: Find improved notions of cores for LTL.

Approach: Investigate methods to extract cores for LTL.

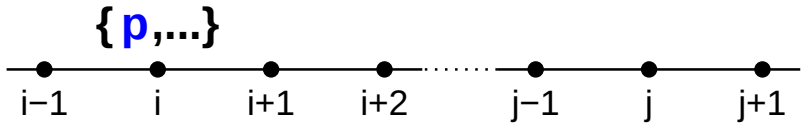
(No implementation in this talk.)

Contents

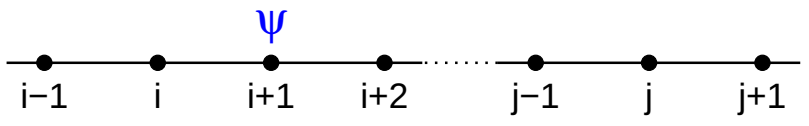
LTL

LTL formulas are evaluated on infinite sequences of sets of atomic propositions, i.e., $\pi \in (2^{AP})^{\omega}$. Constants and Boolean operators as expected.

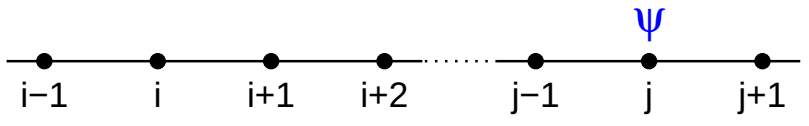
$$\pi, i \models p \Leftrightarrow p \in \pi[i]$$



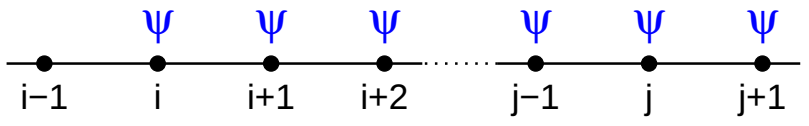
$$\pi, i \models \mathbf{X}\psi \Leftrightarrow \pi, i+1 \models \psi$$



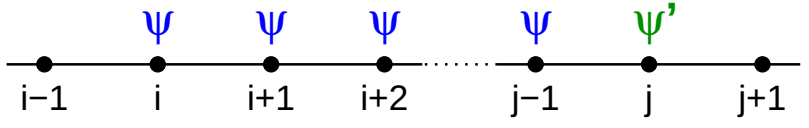
$$\pi, i \models \mathbf{F}\psi \Leftrightarrow \exists j \geq i \,.\, \pi, j \models \psi$$



$$\pi, i \models \mathbf{G}\psi \Leftrightarrow \forall i' \geq i \,.\, \pi, i' \models \psi$$



$$\pi, i \models \psi \mathbf{U} \psi' \Leftrightarrow \exists j \geq i \,.\, \pi, j \models \psi' \quad \wedge \quad \forall i \leq i'' < j \,.\, \pi, i'' \models \psi$$



Notions and Concepts Related to Unsatisfiable Cores

Assume a set of formulas Φ and a function $sat : \Phi \mapsto \{0, 1\}$.

Let $sat(\phi) = 0$. Derive ϕ' with $sat(\phi') = 0$ from ϕ such that

1. ϕ' preserves some reasons for $sat(\phi)$ being 0 without adding new ones,
2. a reason why $sat(\phi') = 0$ is easier to see than why $sat(\phi) = 0$,
3. the derivation of ϕ' from ϕ is such that the user can understand preservation/non-addition of reasons.

Typically 1. and 3. are met by limiting the derivation to some suitable set of operations.

2. might be handled by assuming a suitable cost function.

(No formalization beyond LTL satisfiability in this talk.)

Notions and Concepts Related to Unsatisfiable Cores

Assume a set of formulas Φ, a function $sat : \Phi \mapsto \{0, 1\}$, and a set of operations. Let $\phi, \phi' \in \Phi$ with $sat(\phi) = 0$.

1. ϕ' is a core of ϕ iff ϕ' is derived from ϕ by a sequence of operations.
2. ϕ' is an unsatisfiable core (UC) of ϕ iff 1. and $sat(\phi') = 0$.
3. ϕ' is a proper unsatisfiable core of ϕ iff 2. and ϕ' is syntactically different from ϕ.
4. ϕ' is an irreducible unsatisfiable core (IUC) of ϕ iff 2. and there is no proper unsatisfiable core of ϕ'.

Granularity of a Notion of UC

Of course, the formula ϕ contains all information — implicitly.

Goal: determine relevance of certain aspects of a formula ϕ to $sat(\phi) = 0$ by the mere presence or absence of elements in the UC.

$\Rightarrow$ One notion of core has finer granularity than another iff it provides at least as much information on the relevance of certain aspects as the other notion.

Example: notion of core based on subsets of a set of formulas versus notion that additionally proceeds into the formulas.

(In this talk no formalization.)

Contents

UCs via Syntax Trees

Consider notion of UCs purely based on syntactic structure of formulas given as syntax trees.

Set of operations: as in some forms of vacuity [KV03], replace positive polarity occurrences of subformulas with `1`, negative polarity ones with `0`.

Operations correspond to syntactic weakening of the formula:

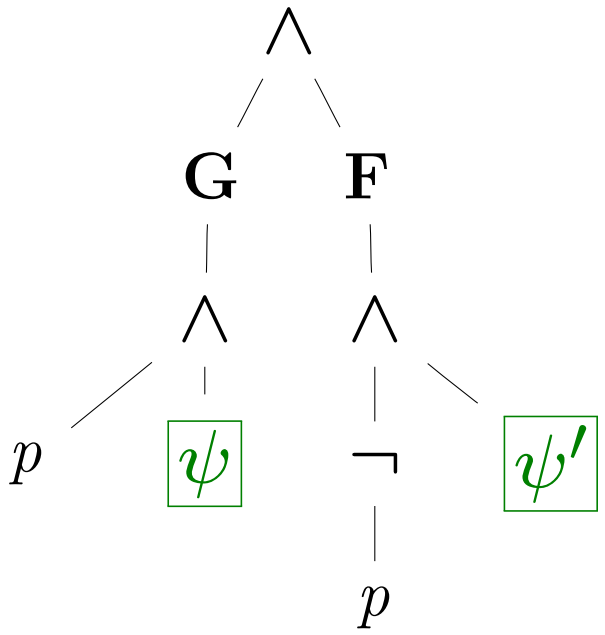
$\Rightarrow$ Preservation of reason(s) for unsatisfiability without addition of new ones (if operations are applied only when preserving unsatisfiability).

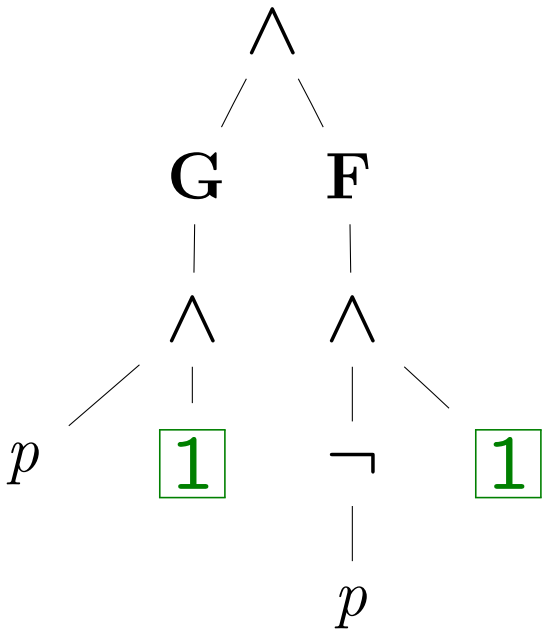
$\Rightarrow$ UC is smaller than the original formula, hence, unsatisfiability is easier to see.

$\Rightarrow$ Operations are easy to understand by a human.

UCs via Syntax Trees

Example





$(\mathbf{G}(p \wedge \boxed{\psi})) \wedge (\mathbf{F}(\neg p \wedge \boxed{\psi'}))$

$(\mathbf{G}(p \wedge \boxed{1})) \wedge (\mathbf{F}(\neg p \wedge \boxed{1}))$

(In this talk no simplification, no sharing of subformulas.)

UCs via Definitional Conjunctive Normal Forms

Translate formula ϕ into equisatisfiable $dCNF(\phi)$:

1. Introduce a fresh atomic proposition $x \in X$ for each node in the syntax tree.

2. Let

ψ	Conjunct $\in dCNF_{aux}(\phi)$
b with $b \in \{0, 1\}$	$x_\psi \leftrightarrow b$
p with $p \in AP$	$x_\psi \leftrightarrow p$
$\circ_1 \psi'$ with $\circ_1 \in \{\neg, \mathbf{X}, \mathbf{F}, \mathbf{G}\}$	$x_\psi \leftrightarrow \circ_1 x_{\psi'}$
$\psi' \circ_2 \psi''$ with $\circ_2 \in \{\vee, \wedge, \mathbf{U}\}$	$x_\psi \leftrightarrow x_{\psi'} \circ_2 x_{\psi''}$

3. Set

$$dCNF(\phi) \equiv x_\phi \wedge \mathbf{G} \bigwedge_{c \in dCNF_{aux}(\phi)} c$$

(For Fisher's SNF see paper.)

UCs via Definitional Conjunctive Normal Forms

Consider notion of UCs based on removal of conjuncts from a dCNF.

Set of operations: as in many notions of UCs in other settings, remove conjuncts from a set of conjuncts (and make sure no superfluous conjuncts are left).

Removal of conjuncts clearly constitutes weakening of the original formula:

$\Rightarrow$ Preservation of reason(s) for unsatisfiability without addition of new ones (if operations are applied only when preserving unsatisfiability).

$\Rightarrow$ UC is smaller than the original formula, hence, unsatisfiability is easier to see.

$\Rightarrow$ Operations are easy to understand by a human.

UCs via Definitional Conjunctive Normal Forms

Example $(\mathbf{G}(p \wedge \psi)) \wedge (\mathbf{F}(\neg p \wedge \psi'))$ continued:

$$
\begin{array}{lcl}
x_{(\mathbf{G}(p \wedge \psi)) \wedge (\mathbf{F}(\neg p \wedge \psi'))} & \leftrightarrow & x_{\mathbf{G}(p \wedge \psi)} \wedge x_{\mathbf{F}(\neg p \wedge \psi')} \\
x_{\mathbf{G}(p \wedge \psi)} & \leftrightarrow & \mathbf{G} x_{p \wedge \psi} \\
x_{p \wedge \psi} & \leftrightarrow & x_p \wedge x_\psi \\
x_p & \leftrightarrow & p \\
x_\psi & \leftrightarrow & \ldots \\
\ldots & \leftrightarrow & \ldots \\
x_{\mathbf{F}(\neg p \wedge \psi')} & \leftrightarrow & \mathbf{F} x_{\neg p \wedge \psi'} \\
x_{\neg p \wedge \psi'} & \leftrightarrow & x_{\neg p} \wedge x_{\psi'} \\
x_{\neg p} & \leftrightarrow & \neg x'_p \\
x'_p & \leftrightarrow & p \\
x_{\psi'} & \leftrightarrow & \ldots \\
\ldots & \leftrightarrow & \ldots
\end{array}
$$

UCs via Definitional Conjunctive Normal Forms

Example $(\mathbf{G}(p \wedge \psi)) \wedge (\mathbf{F}(\neg p \wedge \psi'))$ continued:

$$
\begin{array}{lcl}
x_{(\mathbf{G}(p \wedge \psi)) \wedge (\mathbf{F}(\neg p \wedge \psi'))} & \leftrightarrow & x_{\mathbf{G}(p \wedge \psi)} \wedge x_{\mathbf{F}(\neg p \wedge \psi')} \\
x_{\mathbf{G}(p \wedge \psi)} & \leftrightarrow & \mathbf{G} x_{p \wedge \psi} \\
x_{p \wedge \psi} & \leftrightarrow & x_p \wedge x_\psi \\
x_p & \leftrightarrow & p \\
\boxed{x_\psi} & \boxed{\leftrightarrow} & \boxed{\ldots} \\
\boxed{\ldots} & \boxed{\leftrightarrow} & \boxed{\ldots} \\
x_{\mathbf{F}(\neg p \wedge \psi')} & \leftrightarrow & \mathbf{F} x_{\neg p \wedge \psi'} \\
x_{\neg p \wedge \psi'} & \leftrightarrow & x_{\neg p} \wedge x_{\psi'} \\
x_{\neg p} & \leftrightarrow & \neg x'_p \\
x'_p & \leftrightarrow & p \\
\boxed{x_{\psi'}} & \boxed{\leftrightarrow} & \boxed{\ldots} \\
\boxed{\ldots} & \boxed{\leftrightarrow} & \boxed{\ldots}
\end{array}
$$

UCs via Definitional Conjunctive Normal Forms

Variants by example of a positive polarity $\mathbf{U}$:

Basic Form	Replacing Biimplications with Implications	Temporal Unfolding	Splitting Conjunctions in Temporal Unfolding
$x_{\psi'\mathbf{U}\psi''} \leftrightarrow x_{\psi'}\mathbf{U}x_{\psi''}$	$x_{\psi'\mathbf{U}\psi''} \rightarrow x_{\psi'}\mathbf{U}x_{\psi''}$	$x_{\psi'\mathbf{U}\psi''} \rightarrow$ $x_{\psi''} \vee (x_{\psi'} \wedge \mathbf{X}x_{\psi'\mathbf{U}\psi''})$	$x_{\psi'\mathbf{U}\psi''} \rightarrow$ $x_{\psi''} \vee x_{\psi'}$ $x_{\psi'\mathbf{U}\psi''} \rightarrow$ $x_{\psi''} \vee \mathbf{X}x_{\psi'\mathbf{U}\psi''}$
		$x_{\psi'\mathbf{U}\psi''} \rightarrow \mathbf{F}x_{\psi''}$	$x_{\psi'\mathbf{U}\psi''} \rightarrow \mathbf{F}x_{\psi''}$
$\{x_{\psi'} \leftrightarrow \ldots\}$	$\{x_{\psi'} \rightarrow \ldots\}$	$\{x_{\psi'} \rightarrow \ldots\}$	$\{x_{\psi'} \rightarrow \ldots\}$
$\{x_{\psi''} \leftrightarrow \ldots\}$	$\{x_{\psi''} \rightarrow \ldots\}$	$\{x_{\psi''} \rightarrow \ldots\}$	$\{x_{\psi''} \rightarrow \ldots\}$

(Potentially) Finer Granularity

UCs via Definitional Conjunctive Normal Forms

Example:

	Replacing Biimplications with Implications	Temporal Unfolding
$(\psi' \mathbf{U} \psi'') \quad \wedge$ $(\neg\psi' \wedge \neg\psi'')$	$\ldots$ $x_{\psi' \mathbf{U} \psi''} \rightarrow x_{\psi'} \mathbf{U} x_{\psi''}$ $\{x_{\psi'} \rightarrow \ldots\}$ $\{x_{\psi''} \rightarrow \ldots\}$ $\ldots$	$\ldots$ $x_{\psi' \mathbf{U} \psi''} \rightarrow$ $\quad x_{\psi''} \vee (x_{\psi'} \wedge \mathbf{X} x_{\psi' \mathbf{U} \psi''})$ $\{x_{\psi'} \rightarrow \ldots\}$ $\{x_{\psi''} \rightarrow \ldots\}$ $\ldots$
$(\psi' \mathbf{U} \psi'') \wedge$ $((\neg\psi' \wedge \neg\psi'') \vee$ $(\mathbf{G} \neg\psi''))$		$\ldots$ $x_{\psi' \mathbf{U} \psi''} \rightarrow$ $\quad x_{\psi''} \vee (x_{\psi'} \wedge \mathbf{X} x_{\psi' \mathbf{U} \psi''})$ $x_{\psi' \mathbf{U} \psi''} \rightarrow \mathbf{F} x_{\psi''}$ $\{x_{\psi'} \rightarrow \ldots\}$ $\{x_{\psi''} \rightarrow \ldots\}$ $\ldots$

UCs via Bounded Model Checking

In the most fine-granular version of the dCNF all conjuncts are of one of the two forms:

$$(\bigvee_i [\mathbf{X}]\ [\neg]\ x_{\psi_i}) \qquad \text{or} \qquad ([\neg]\ x_{\psi}\ \vee\ \mathbf{F}\ [\neg]\ x_{\psi'})$$

Dropping conjuncts of the latter form results in a transition relation.

Any satisfiable formula ϕ has at least one witness π such that

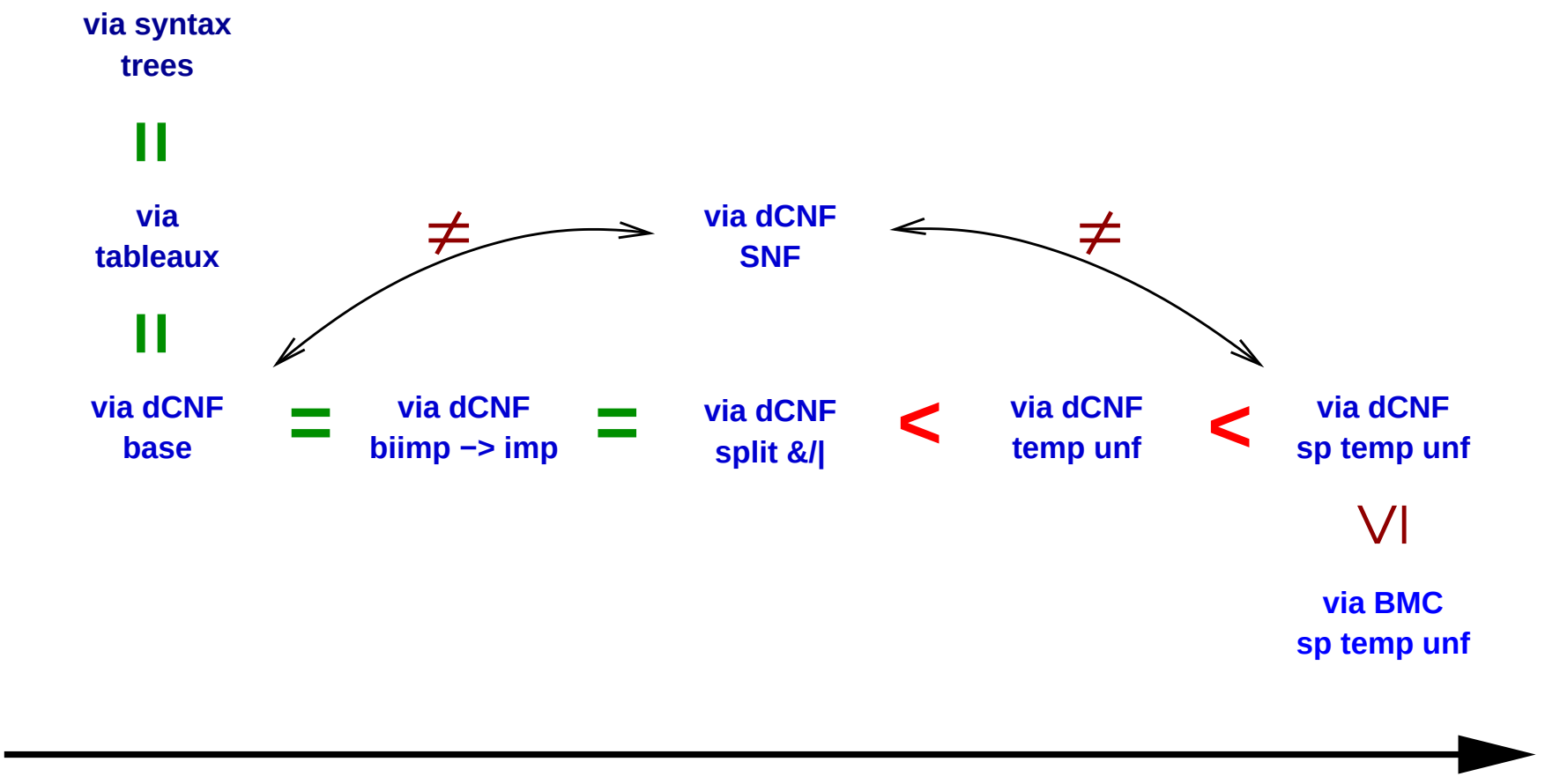
- π has infinite length, and
- π observes the above transition relation.

If there is some k s.t. no prefix of length k exists that observes (1) the initial condition and (2) the transition relation from 0 up to $k-1$, then ϕ is unsatisfiable. (Incomplete!)

For a given k, the path from 0 to k is finite. Hence, it can be encoded as a SAT problem. $\Rightarrow$ Map back core from SAT solver to LTL.

Close relation to SAT-based Bounded Model Checking [HLJ05].

Granularity



Finer Granularity

Contents

Vacuity detection

- Technique in model checking for quality assurance (mostly) of passing specifications.
- Finds parts of specifications that are not used during verification.
- Original notion [BBDER01,KV03] replaces occurrences of subformulas with 0/1 depending on polarity.

Main differences

- Normally defined w.r.t. a specific model. But see vacuity without design [CS07] and inherent vacuity [FKSFV08].
- Geared to answer whether there exists a strengthening s.t. the model still satisfies the specification. But see mutual vacuity [GC04b, CS07] and work on strongest passing formulas [CGS08].
- Focuses on strengthening a formula. But vacuity is defined, e.g., in [BBDER01,KV03,FKSFV08] for both passing and failing formulas.

Related Work — Vacuity

Inherent vacuity [FKSFV08] defines a framework for vacuity without design [CS07] with 4 parameters:

- vacuity type: non-shared vs. shared subformulas,
- equivalence type: closed vs. open systems,
- tightening type: equivalence vs. preservance of satisfiability/realizability, and
- polarity type: strengthening vs. weakening.

Close relation between (I)UCs and the (non-shared, closed systems, equivalence, weakening) instance of the framework:

Given a proper UC ϕ' via syntax tree of some unsatisfiable formula ϕ,
1. ϕ is inherently vacuous, and
2. ϕ' is an IUC iff it is not inherently vacuous.

Summary

- We propose notions of UC for LTL.
- Some notions have higher granularity than others — and there's hope for more.
- We discuss a connection to vacuity.

Ongoing and Future Work

- Implementation and evaluation.
- Improve notions.
- Complexity.
- Formalize general concepts.

References (1)

BBDER01 I. Beer, S. Ben-David, C. Eisner, Y. Rodeh: Efficient Detection of Vacuity in Temporal Model Checking. Formal Methods in System Design 18(2)2001:141–163.

BDTW93 R. Bakker, F. Dikker, F. Tempelman, P. Wognum: Diagnosing and Solving Over-Determined Constraint Satisfaction Problems. IJCAI'93.

BS01 R. Bruni, A. Sassano: Restoring Satisfiability or Maintaining Unsatisfiability by finding small Unsatisfiable Subformulae. SAT'01.

CD91 J. Chinneck, E. Dravnieks: Locating Minimal Infeasible Constraint Sets in Linear Programs. ORSA Journal on Computing 3(2):157–168, 1991.

CGS08 H. Chockler, A. Gurfinkel, O. Strichman: Beyond Vacuity: Towards the Strongest Passing Formula. FMCAD'08.

CRST08b A. Cimatti, M. Roveri, A. Susi, S. Tonetta: From Informal Requirements to Property-Driven Formal Validation. FMICS'08.

CS07 H. Chockler, O. Strichman: Easier and More Informative Vacuity Checks. MEMOCODE'07.

FKSFV08 D. Fisman, O. Kupferman, S. Sheinvald-Faragy, M. Vardi: A Framework for Inherent Vacuity. HVC'08.

References (2)

GC04b A. Gurfinkel, M. Chechik: How Vacuous Is Vacuous? TACAS'04.

HLJ05 K. Heljanko, T. Junttila, T. Latvala: Incremental and Complete Bounded Model Checking for Full PLTL. CAV'05.

KV03 O. Kupferman, M. Vardi: Vacuity detection in temporal model checking. STTT 4(2)2003:224–233.

SC03 S. Schlobach, R. Cornet: Non-Standard Reasoning Services for the Debugging of Description Logic Terminologies. IJCAI'03.

SSJ+03 I. Shlyakhter, R. Seater, D. Jackson, M. Sridharan, M. Taghdiri: Debugging Over-constrained Declarative Models Using Unsatisfiable Cores. ASE'03.

TCJ08 E. Torlak, F. Chang, D. Jackson: Finding Minimal Unsatisfiable Cores of Declarative Specifications. FM'08.

WHR+05 H. Wang, M. Horridge, A. Rector, N. Drummond, J. Seidenberg: Debugging OWL-DL Ontologies: A Heuristic Approach. ISWC'05.

ZM03b L. Zhang, S. Malik: Extracting Small Unsatisfiable Cores from Unsatisfiable Boolean Formula. SAT'03.