Variant-Based Decidable Satisfiability in Initial Algebras with Predicates

Raúl Gutiérrez[1] José Meseguer[2]

[1]DSIC, Universitat Politècnica de València, Spain

[2]University of Illinois at Urbana-Champaign,Illinois, USA

NAMUR (BELGIUM), OCTOBER 11, 2017

Motivation

1. Some of the most recent advances in software verification are due to the systematic use of decision procedures in model checkers and theorem provers.
2. For a system specified by theory T, SMT solving can partially automate verification by using procedures for decidable subtheories T_i.
3. Limitation of SMT tools: lack of extensibility of decidable fragment.
4. Users can extend a specification's decidable fragment if theory-generic decision procedures are added.
5. Variant-based satisfiability (VS): a decision procedure for initial algebras $T_{\Sigma/E \cup B}$ generic on theories $(\Sigma, E \cup B)$ under quite general conditions.
6. Limitation: current VS algorithm applies well to user-definable data structures, but cannot handle user-definable predicates.

Goal

Goal

Extend variant-based satisfiability to initial algebras with user-definable predicates under fairly general conditions using two key ideas:

1. characterizing the cases when $p(u_1, \ldots, u_n) \neq tt$ by means of constrained patterns; and
2. eliminating all occurrences of disequalities of the form $p(u_1, \ldots, u_n) \neq tt$ in a quantifier-free (QF) formula by means of such patterns.

Outline

Example: Sets of Natural Numbers $(\Sigma, E \cup B)$

```
fmod ACU-NAT is
  sort Natural .

  op 0   : -> Natural [ctor] .
  op 1   : -> Natural [ctor] .
  op _+_ : Natural Natural -> Natural
           [ctor assoc comm id: 0] .
endfm
```

```
fmod ACU-NAT-FUN is
  pr ACU-NAT .

  op max : Natural Natural -> Natural
           [comm] .
  op min : Natural Natural -> Natural
           [comm] .
  op _-_ : Natural Natural -> Natural .
           *** monus

  vars N M : Natural .

  eq max(N,N + M) = N + M [variant] .
  eq min(N,N + M) = N [variant] .

  eq N - (N + M) = 0 [variant].
  eq (N + M) - N = M [variant] .
endfm
```

Example: Sets of Natural Numbers $(\Sigma, E \cup B)$

```
fmod ACU-NAT-SET is
  pr ACU-NAT .

  sort NaturalSet .
  sort Pred .

  subsort Natural < NaturalSet .

  op mt : -> NaturalSet [ctor] .
  op _,_ : NaturalSet NaturalSet ->
           NaturalSet [ctor assoc comm] .
  op tt : -> Pred [ctor] .
  *** set containment
  op _=C_ : NaturalSet NaturalSet ->
            Pred [ctor] .

  vars NS NS' : NaturalSet .

  *** identity of set union
  eq NS , mt = NS [variant] .
  *** idempotency of set union
  eq NS , NS = NS [variant] .
  *** idempotency of set union
  eq NS , NS , NS' = NS , NS'
                         [variant] .

  eq mt =C NS = tt [variant] .
  eq NS =C NS = tt [variant] .
  eq NS =C NS , NS' = tt [variant] .
endfm
```

Variants

Given a decomposition $\mathcal{R} = (\Sigma, B, \vec{E})$ of a MS equational theory (Σ, E) and a Σ-term t, a variant of t is a pair (u, θ) such that:

- $u =_B (t\theta)!_{\vec{E},B}$,
- $dom(\theta) \subseteq vars(t)$, and
- $\theta = \theta!_{\vec{E},B}$, that is, $\theta(x) = \theta(x)!_{\vec{E},B}$ for all variables x. (u, θ) is called a ground variant iff, furthermore, $u \in T_\Sigma$.

Given variants (u, θ) and (v, γ) of t, (u, θ) is called more general than (v, γ), denoted $(u, \theta) \sqsupseteq_B (v, \gamma)$, iff there is a substitution ρ such that:

- $(\theta\rho)|_{vars(t)} =_B \gamma$, and
- $u\rho =_B v$.

Let $[\![t]\!]_{\vec{E},B} = \{(u_i, \theta_i) \mid i \in I\}$ denote a complete set of variants of t, that is, a set of variants such that for any variant (v, γ) of t there is an $i \in I$, such that $(u_i, \theta_i) \sqsupseteq_B (v, \gamma)$.

Example: Variants

```
get variants in ACU-NAT-FUN :
min(1, N:Natural + K:Natural) .

Variant #1
Natural: min(1, N:Natural + K:Natural)

Variant #2
Natural: 1
K:Natural --> 1 + K1:Natural

Variant #3
Natural: 1
N:Natural --> 1 + N1:Natural

Variant #4
Natural: 0
N:Natural --> 0
K:Natural --> 0
```

```
get variants in ACU-NAT-FUN:
N:Natural - K:Natural .

Variant #1
Natural: N:Natural - K:Natural

Variant #2
Natural: 0
K:Natural --> K1:Natural + N:Natural

Variant #3
Natural: N1:Natural
N:Natural --> N1:Natural + K:Natural
```

Finite Variant Property

- A decomposition $\mathcal{R} = (\Sigma, B, R)$ has the finite variant property (FVP) iff for each Σ-term t there is a finite complete set of variants $[\![t]\!]_{R,B} = \{(u_1, \theta_1) \ldots (u_n, \theta_n)\}$.
- If B has a finitary B-unification algorithm, and $\mathcal{R} = (\Sigma, B, R)$ has FVP, $[\![t]\!]_{R,B}$ can be chosen to be the set of most general variants.

Note

FVP easy to check when it holds. Example: `ACU-NAT-SET` is FVP.

Representing Predicates

- A predicate is viewed as a function symbol $p : s_1 \ldots s_n \to \texttt{Pred}$, with $\texttt{Pred}$ a new sort having constant $\texttt{tt}$.
- An atomic formula $p(t_1, \ldots, t_n)$ is then expressed as the equation $\mathrm{p}(t_1, \ldots, t_n) = \texttt{tt}$.

Example: Predicates on Sets of Natural Numbers

```
fmod ACU-NAT-SET-PREDS is
  pr ACU-NAT-SET .

  *** strict order
  op _>_ : Natural Natural -> Pred [ctor] .
  *** sort predicates
  op natural : NaturalSet -> Pred [ctor] .
  op even : NaturalSet -> Pred [ctor] .
  op odd : NaturalSet -> Pred [ctor] .

  vars N M : Natural .

  eq N + M + 1 > N = tt [variant] .

  eq natural(N) = tt [variant] .

  eq even(N + N) = tt [variant] .

  eq odd(N + N + 1) = tt [variant] .
endfm
```

Constructor Variants

Question

What variants of t cover as instances modulo B all canonical forms of all ground instances of t?

Let $\mathcal{R} = (\Sigma, B, R)$ be an FVP decomposition of (Σ, E) protecting a constructor decomposition $\mathcal{R}_\Omega = (\Omega, B_\Omega, R_\Omega)$. Assume that:

- $\Sigma = \Omega \cup \Delta$ with $\Omega \cap \Delta = \varnothing$;
- B has a finitary B-unification algorithm and $B = B_\Omega \uplus B_\Delta$, with B_Ω Ω-equations and if $u = v \in B_\Delta$, u, v are non-variable Δ-terms.

Call $[\![t]\!]^\Omega_{R,B} = \{(v, \theta) \in [\![t]\!]_{R,B} \mid v \in T_\Omega(X)\}$ the set of constructor variants of t.

Answer

If $[u] \in \mathcal{C}_{\mathcal{R}_\Omega}$ is of the form $u =_B (t\gamma)!_{R,B}$, then there is $(v, \theta) \in [\![t]\!]^\Omega_{R,B}$ and a normalized ground substitution τ such that $u =_B v\tau$.

OS-Compactness

An equational OS-FO theory (Σ, E) is called OS-compact iff:

- for each sort s in Σ we can effectively determine whether s is finite or infinite in $T_{\Sigma/E,s}$, and, if finite, can effectively compute a representative ground term $rep([u]) \in [u]$ for each $[u] \in T_{\Sigma/E,s}$;
- $=_E$ is decidable and E has a finitary unification algorithm; and
- any finite conjunction $\bigwedge D$ of negated Σ-atoms whose variables all have infinite sorts and such that $\bigwedge D$ is E-consistent is satisfiable in $T_{\Sigma,E}$.

Call an OS theory (Σ, E) OS-compact iff OS-FO theory (Σ, E) is OS-compact.

Theorem

If (Σ, E) is an OS-compact theory, then satisfiability of QF Σ-formulas in $T_{\Sigma,E}$ is decidable.

Current Variant Satisfiability

Theorem 1

If (Ω, B_Ω) has B_Ω only with $ACCU$-axioms, then (Ω, B_Ω) is OS-compact.

Theorem 2 (Variant Satisfiability)

If $(\Sigma, E \cup B)$ if FVP and protects (Ω, B_Ω) with $B_\Omega \subseteq ACCU$, then QF satisfiability in $(\Sigma, E \cup B)$ is decidable.

Limitation

Question

What happens with the user-definable predicates?

- p is a constructor operator of sort `Pred` which is not a free constructor modulo the axioms B_Ω.
- The OS-compactness of a constructor decomposition $\mathcal{R}_\Omega = (\Omega, B_\Omega, R_\Omega)$ can be broken (or be a hard to prove task) when adding user-definable predicates.

Solution

We provide a decision procedure for validity and satisfiability of QF formulas in the initial algebra of an FVP theory $\mathcal{R}$ that may contain user-definable predicates and protects a constructor decomposition $\mathcal{R}$ that need not be OS-compact under reasonable assumptions.

Example: Negative Patterns

- Greater than: `N > N + M`
- Even:
  - `even(mt)`
  - `even(N + N + 1)`
  - `((N =C NS /= tt) , (NS /= mt))` $\Longrightarrow$ `even((N , NS))`
- Odd:
  - `odd(mt)`
  - `odd(N + N)`
  - `((N =C NS /= tt) , (NS /= mt))` $\Longrightarrow$ `odd((N , NS))`
- Natural:
  - `natural(mt)`
  - `((N =C NS /= tt) , (NS /= mt))` $\Longrightarrow$ `natural((N , NS))`

Negative Patterns

- Negative constrained patterns are of the form:

$$\bigwedge_{1\leq l\leq n_j} {w^j}_l \neq {w'^j}_l \Rightarrow p({v^j}_1,\ldots,{v^j}_n) \neq tt, \;\; 1 \leq j \leq m_p$$

  with the v_i^j, ${w^j}_l$ and ${w'^j}_l$ Ω_c-terms with variables in $Y_j = vars(p({v^j}_1,\ldots,{v^j}_n))$.
- These negative constrained patterns are interpreted as meaning that the following semantic equivalences are valid in $\mathcal{C}_\mathcal{R}$ for each $p \in \Omega_\Pi$, where $\rho_j \in \{\rho \in [Y_j \rightarrow T_{\Omega_c}] \mid \rho = \rho!_{R,B}\}$, $B = B_\Delta \uplus B_{\Omega_c}$, and $R = R_\Delta \uplus R_{\Omega_c} \uplus R_\Pi$:

$$[p({v^j}_1,\ldots,{v^j}_n)\rho_j] \in \mathcal{C}_\mathcal{R} \Leftrightarrow \bigwedge_{1\leq l\leq n_j} ({w^j}_l \neq {w'^j}_l)\rho_j$$

$$[p(t_1,\ldots,t_n)] \in \mathcal{C}_\mathcal{R} \Leftrightarrow \exists j \exists \rho_j \; [p(t_1,\ldots,t_n)] = [p({v^j}_1,\ldots,{v^j}_n)\rho_j] \wedge \bigwedge_{1\leq l\leq n_j} ({w^j}_l \neq {w'^j}_l)\rho_j$$

The Inductive Satisfiability Decision Procedure (1/2)

- The inductive validity decision problem of whether $\mathcal{C}_{\mathcal{R}} \models \varphi$ is reduced to deciding whether $\neg\varphi$ is unsatisfiable in $\mathcal{C}_{\mathcal{R}}$.
- In this way, it is enough to decide the satisfiability of a conjunction of Σ-literals of the form $\bigwedge G \wedge \bigwedge D$ (the QF Σ-formula in disjunctive normal form), where the G are equations and the D are disequations.

Steps:

1. **Unification**. Satisfiability of the conjunction $\bigwedge G \wedge \bigwedge D$ is replaced by satisfiability for some conjunction in the set $\{(\bigwedge D\alpha)!_{R,B} \mid \alpha \in \mathit{VarUnif}_E(\bigwedge G)\}$.

The Inductive Satisfiability Decision Procedure (2/2)

2. **Π-Elimination**. For each $\bigwedge D' = \bigwedge D_1 \wedge p(t_1, \ldots, t_n) \neq tt \wedge \bigwedge D_2$, we replace $\bigwedge D'$ by all not obviously unsatisfiable conjunctions of the form:

$$(\bigwedge D_1 \wedge \bigwedge_{1 \leq l \leq n_j} w^j{}_l \neq w'^{,j}{}_l \wedge \bigwedge D_2)\theta\alpha$$

   where $1 \leq j \leq m_p$, $W = vars(\bigwedge D')$, $(p(t'_1, \ldots, t'_n), \theta) \in [\![p(t_1, \ldots, t_n)]\!]^{W,\Omega}_{R,B}$, and α is a *disjoint* B_{Ω_c}-unifier of the equation $p(t'_1, \ldots, t'_n) = p(v^j{}_1, \ldots, v^j{}_n)$.

3. **Reduce Conjunctions of Σ Disequalities to Conjunctions of Ω_c Disequalities**. For $\bigwedge D'$ a $\Delta \uplus \Omega_c$-conjunction of disequalities, viewed as a $(\Delta \uplus \Omega_c)^\wedge$-term its constructor $\Omega_c^\wedge$-variants are of the form $(\bigwedge D'', \gamma)$, with $\bigwedge D''$ an Ω_c-conjunction of disequalities. Then $\bigwedge D'$ is satisfiable in $\mathcal{C}_\mathcal{R}$ iff some $\bigwedge D''\tau$ so obtained is B_{Ω_c}-consistent for some $\Omega_c^\wedge$-variant $(\bigwedge D'', \gamma)$ of $\bigwedge D'$.

Implementation

- We have implemented the variant satisfiability decision procedure in a new prototype tool.
- The implementation consists of 11 new Maude modules (from 17 in total), 2345 new lines of code, and uses the Maude's META-LEVEL to carry out the steps of the procedure in a reflective way.
- We have also developed a Maude interface to ease the definition of properties and patterns as equations. The three steps of the variant satisfiability procedure are implemented using Maude's META-LEVEL functions.

Example: Odd and Even

```
mod ACU-NAT-SET-PREDS-CONJECTURES is
  pr ACU-NAT-SET-PREDS-PATTERNS .

*** odd(N) = tt <=> even(N) /= tt .
  op prop1 : Natural -> AtomMagma .
  op prop2 : Natural -> AtomMagma .

  eq prop1(N)
   = (odd(N) = tt) , (even(N) = tt) .
  eq prop2(N)
   = (even(N) /= tt) , (odd(N) /= tt) .
endm
```

```
Unification of prop1:
  No variant unifiers can be found.

Unification of prop2:
  (even(N) /= tt) , (odd(N) /= tt)

Predicate elimination of prop2:
  even(M + M) /= tt , odd(M + M) /= tt =>
  tt /= tt , odd(M + M) /= tt

Unsatisfiable!
```

Example: Greater Than

```
mod ACU-NAT-SET-PREDS-CONJECTURES is
  pr ACU-NAT-SET-PREDS-PATTERNS .

*** N > M = tt \/ N = M \/ M > N = tt
  op prop : Natural Natural -> AtomMagma .

  eq prop(N,M)
   = (N > M /= tt) ,
     (N /= M) ,
     (M > N /= tt) .
endm
```

```
Unification of prop:
  (N > M /= tt) ,
  (N /= M) ,
  (M > N /= tt)

Predicate elimination of prop:
  (N > N + 0 /= tt) ,
  (N /= N + 0) ,
  (N + 0 > N /= tt) =>
  (N /= N)

Unsatisfiable!
```

Conclusions and future work

- Satisfiability decision procedures can be either theory-specific or theory-generic. These two classes of procedures complement each other: theory specific ones are more eficient; but theory-generic ones are user-definable and can substantially increase the range of SMT solvers.
- Our work has extended variant satisfiability to support initial algebras specified by FVP theories with user-definable predicates under fairly general conditions. Since such predicates are often needed in specifications, this substantially enlarges the scope of variant-based initial satisfiability algorithms.
- The most obvious next step is to combine the original variant satisfiability algorithm with the present one.
- Furthermore, our goal is to include this powerful decision procedure in our automatic inductive theorem prover ν-ITP.