Variant-Based Decidable Satisfiability in Initial Algebras with Predicates

Raúl Gutiérrez¹ and José Meseguer²

¹ Universitat Politècnica de València
² University of Illinois at Urbana-Champaign

Abstract. Decision procedures can be either theory-specific, e.g., Presburger arithmetic, or theory-generic, applying to an infinite number of user-definable theories. Variant satisfiability is a theory-generic procedure for quantifier-free satisfiability in the initial algebra of an order-sorted equational theory $\langle \Sigma, E \cup B \rangle$ under two conditions: (i) $E \cup B$ has the finite variant property and $B$ has a finitary unification algorithm; and (ii) $\langle \Sigma, E \cup B \rangle$ protects a constructor subtheory $\langle \Omega, E_\Omega \cup B_\Omega \rangle$ that is OS-compact. These conditions apply to many user-definable theories, but have a main limitation: they apply well to data structures, but often do not hold for user-definable predicates on such data structures. We present a theory-generic satisfiability decision procedure, and a prototype implementation, extending variant-based satisfiability to initial algebras with user-definable predicates under fairly general conditions.

Keywords: finite variant property (FVP), OS-compactness, user-definable predicates, decidable validity and satisfiability in initial algebras.

1 Introduction

Some of the most important recent advances in software verification are due to the systematic use of decision procedures in both model checkers and theorem provers. However, a key limitation in exploiting the power of such decision procedures is their current lack of extensibility. The present situation is as follows. Suppose a system has been formally specified as a theory $T$ about which we want to verify some properties, say $\varphi_1, \ldots, \varphi_n$, using some model checker or theorem prover that relies on an SMT solver for its decision procedures. This limits a priori the decidable subtheory $T_0 \subseteq T$ that can be handled by the SMT solver. Specifically, the SMT solver will typically support a fixed set $Q_1, \ldots, Q_k$ of decidable theories, so that, using a theory combination method such as Nelson and Oppen [24], or Shostak [25], $T_0$ must be a finite combination of the decidable theories $Q_1, \ldots, Q_k$ supported by the SMT solver.

In non-toy applications it is unrealistic to expect that the entire specification $T$ of a software system will be decidable. Obviously, the bigger the decidable subtheory $T_0 \subseteq T$, the higher the levels of automation and the greater the chances

* Partially supported by NSF Grant CNS 14-09416, the EU (FEDER), Spanish MINECO project TIN2015-69175-C4-1-R and GV project PROMETEOII/2015/013.
of scaling up the verification effort. With theory-specific procedures for, say, $Q_1, \ldots, Q_k$, the decidable fragment $T_0$ of $T$ is a priori bounded. One promising way to extend the decidable fragment $T_0$ is to develop theory-generic satisifiability procedures. These are procedures that make decidable not a single theory $Q$, but an infinite class of user-specifiable theories. Therefore, an SMT solver supporting both theory-specific and theory-generic decision procedures becomes user-extensible and can carve out a potentially much bigger Decidable Fragment $T_0$ of the given system specification $T$.

Variant-based satisfiability \cite{2019} is a recent theory-generic decision procedure applying to the following, easily user-specifiable infinite class of equational theories $(\Sigma, E \cup B)$: (i) $\Sigma$ is an order-sorted \cite{13} signature of function symbols, supporting types, subtypes, and subtype polymorphisms; (ii) $E \cup B$ has the finite variant property \cite{8} and $B$ has a finitary unification algorithm; and (iii) $(\Sigma, E \cup B)$ protects a constructor subtheory $(\Omega, E_\Omega \cup B_\Omega)$ that is OS-compact \cite{2019}. The procedure can then decide satisifiability in the initial algebra $T_{\Sigma;E;B}$, that is, in the algebraic data type specified by $(\Sigma, E \cup B)$. These conditions apply to many user-definable theories, but have a main limitation: they apply well to data structures, but often do not hold for user-definable predicates.

The notions of variant and of OS-compactness mentioned above are defined in detail in Section \cite{2} Here we give some key intuitions about each notion. Given $\Sigma$-equations $E \cup B$ such that the equations $E$ oriented as left-to-right rewrite rules are confluent and terminating modulo the equational axioms $B$, a variant of a $\Sigma$-term $t$ is a pair $(u, \theta)$ where $\theta$ is a substitution, and $u$ is the canonical form of the term instance $t\theta$ by the rewrite rules $E$ modulo $B$. Intuitively, the variants of $t$ are the fully simplified patterns to which the instances of $t$ can reduce. Some simplified instances are of course more general (as patterns) than others. $E \cup B$ has the finite variant property (FVP) if any $\Sigma$-term $t$ has a finite set of most general variants. For example, the addition equations $E = \{ x + 0 = x, x + s(y) = s(x + y) \}$ are not FVP, since $(x + y, id), (s(x + y_1), \{ y \mapsto y_1 \}), (s(s(x+y_2)), \{ y \mapsto s(y_2) \}), \ldots, (s^n(x + y_n), \{ y \mapsto s^n(y_n) \})$, are all incomparable variants of $x + y$. Instead, the Boolean equations $G = \{ x \lor \top = \top, x \lor \bot = x, x \land \top = x, x \land \bot = \bot \}$ are FVP. For example, the most general variants of $x \lor y$ are: $(x \lor y, id), (x, \{ y \mapsto \bot \})$, and $(\top, \{ y \mapsto \top \})$. Assuming for simplicity that all sorts in a theory $(\Omega, E_\Omega \cup B_\Omega)$ have an infinite number of ground terms of that sort which are all different modulo the equations $E_\Omega \cup B_\Omega$, then OS-compactness of $(\Omega, E_\Omega \cup B_\Omega)$ means that any conjunction of disequalities $\bigwedge_{1 \leq i \leq n} u_i \neq v_i$ such that $E_\Omega \cup B_\Omega \vdash u_i = v_i$, $1 \leq i \leq n$, is satisfiable in the initial algebra $T_{\Omega;E_\Omega;B_\Omega}$. For example, $\{(0, s), \emptyset\}$ is OS-compact, where $\{0, s\}$ are the usual natural number constructors. Thus, $s(x) \neq s(y) \lor 0 \neq y$ is satisfiable in $T_{\{0,s\}}$.

The key reason why user-definable predicates present a serious obstacle is the following. Variant satisfiability works by reducing satisfiability in the initial algebra $T_{\Sigma;E;B}$ to satisfiability in the much simpler algebra of constructors $T_{\Pi;E_\Pi;B_\Pi}$. In many applications $E_\Pi = \emptyset$, and if the axioms $B_\Pi$ are any combination of associativity, commutativity and identity axioms, except associativity without commutativity, then $(\Omega, B_\Omega)$ is an OS-compact theory
making satisfiability in \( T_{\Omega/B} \) and therefore in \( T_{\Sigma/E \cup B} \) decidable. We can
equationally specify a predicate \( p \) with sorts \( A_1, \ldots, A_n \) in a positive way
as a function \( p : A_1, \ldots, A_n \rightarrow \text{Pred} \), where the sort \( \text{Pred} \) of predicates
contains a “true” constant \( tt \), so that \( p(u_1, \ldots, u_n) \) not holding for concrete ground
arguments \( u_1, \ldots, u_n \) is expressed as the disequality \( p(u_1, \ldots, u_n) \neq tt \). But \( p(u_1, \ldots, u_n) \neq tt \)
means that \( p \) must be a constructor of sort \( \text{Pred} \) in \( \Omega \), and
that the equations defining \( p \) must belong to \( E_{\Omega} \), making \( E_{\Omega} \subset \Xi \) and ruling
out the case when \( T_{\Omega/E_{\Omega \cup B}} = T_{\Omega/B} \) is decidable by OS-compactness.

This work extends variant-based satisfiability to initial algebras with user-
definable predicates under fairly general conditions using two key ideas: (i)
characterizing the cases when \( p(u_1, \ldots, u_n) \neq tt \) by means of constrained patterns;
and (ii) eliminating all occurrences of disequalities of the form \( p(v_1, \ldots, v_n) \neq tt \)
in a quantifier-free (QF) formula by means of such patterns. In this way, the QF
satisfiability problem can be reduced to formulas involving only non-predicate
constructors, for which OS-compactness holds in many applications. More
 generally, if some predicates fall within the OS-compact fragment, they can be kept.

Preliminaries are in Section \ref{section:preliminaries}. Constructor variants and OS-compactness in
Section \ref{section:constructors}. The satisfiability decision procedure is defined and proved correct in
Section \ref{section:procedure} and its prototype implementation is described in Section \ref{section:implementation}. Related
work and conclusions are discussed in Section \ref{section:conclusion}. All proofs can be found in \cite{14}.

\section{Many-Sorted Logic, Rewriting, and Variants}

We present some preliminaries on many-sorted (MS) logic, rewriting and finite
variant and variant unification notions needed in the paper. For a more general
treatment using order-sorted (OS) logic see \cite{14}.

We assume familiarity with the following basic concepts and notation that
are explained in full detail in, e.g., \cite{22}: (i) many-sorted (MS) signature as a
pair \( \Sigma = (S, \Sigma) \) with \( S \) a set of sorts and \( \Sigma \) an \( S^* \times S \)-indexed family \( \Sigma = \{\Sigma_{w,s}\}_{(w,s)\in S^* \times S} \) of function symbols, where \( f \in \Sigma_{s_1 \ldots s_n, s} \) is displayed as \( f : s_1 \ldots s_n \rightarrow s \); (ii) \( \Sigma \)-algebra \( A \) as a pair \( A = (A, -) \) with \( A = \{A_s\}_{s \in S} \) an \( S \)-
indexed family of sets, and \( - \) a mapping interpreting each \( f : s_1 \ldots s_n \rightarrow s \n \) as a
function in the set \( \{A_{s_1} \times \ldots \times A_{s_n} \rightarrow A_s\} \). (iii) \( \Sigma \)-homomorphism \( h : A \rightarrow B \)
as an \( S \)-indexed family of functions \( h = \{h_s : A_s \rightarrow B_s\}_{s \in S} \) preserving the
operations in \( \Sigma \); (iv) the term \( \Sigma \)-algebra \( T_{\Sigma} \) and its initiality in the category
\( \text{MSAlg}_\Sigma \) of \( \Sigma \)-algebras when \( \Sigma \) is unambiguous.

An \( S \)-sorted set \( X = \{X_s\}_{s \in S} \) of variables, satisfies \( s \neq s' \Rightarrow X_s \cap X_{s'} = \emptyset \),
and the variables in \( X \) are always assumed disjoint from all constants in \( \Sigma \). The
\( \Sigma \)-term algebra on variables \( X \), \( T_{\Sigma}(X) \), is the initial algebra for the signature
\( \Sigma(X) \) obtained by adding to \( \Sigma \) the variables \( X \) as extra constants. Since a
\( \Sigma(X) \)-algebra is just a pair \( (A, \alpha) \), with \( A \) a \( \Sigma \)-algebra, and \( \alpha \) an interpretation of the constants
in \( X \), i.e., an \( S \)-sorted function \( \alpha \in [X \rightarrow A] \), the \( \Sigma(X) \)-initiality
of \( T_{\Sigma}(X) \) means that for each \( A \in \text{MSAlg}_{\Sigma} \) and \( \alpha \in [X \rightarrow A] \), there exists a
unique \( \Sigma \)-homomorphism \( \alpha : T_{\Sigma}(X) \rightarrow A \) extending \( \alpha \), i.e., such that for each
\( s \in S \) and \( x \in X_s \) we have \( x\alpha_s = \alpha_s(x) \). In particular, when \( A = T_{\Sigma}(Y) \), an
interpretation of the constants in \(X\), i.e., an \(S\)-sorted function \(\sigma \in [X \rightarrow \text{T}_\Sigma(Y)]\) is called a substitution, and its unique homomorphic extension \(\sigma : \text{T}_\Sigma(X) \rightarrow \text{T}_\Sigma(Y)\) is also called a substitution. Define \(\text{dom}(\sigma) = \{ x \in X \mid x + x\sigma \} \), and \(\text{ran}(\sigma) = \bigcup_{x \in \text{dom}(\sigma)} \text{vars}(x\sigma)\). Given variables \(Z\), the substitution \(\sigma |_Z\) agrees with \(\sigma\) on \(Z\) and is the identity elsewhere.

We also assume familiarity with many-sorted first-order logic including: (i) the first-order language of \(\Sigma\)-formulas for \(\Sigma\) a signature (in our case \(\Sigma\) has only function symbols and the = predicate); (ii) given a \(\Sigma\)-algebra \(A\), a formula \(\varphi \in \text{Form}(\Sigma)\), and an assignment \(\alpha \in [Y \rightarrow A]\), with \(Y = \text{fvars}(\varphi)\) the free variables of \(\varphi\), the satisfaction relation \(A, \alpha \models \varphi\); (iii) the notions of a formula \(\varphi \in \text{Form}(\Sigma)\) being valid, denoted \(A \models \varphi\), resp. satisfiable, in a \(\Sigma\)-algebra \(A\). For a subsignature \(\Omega \subseteq \Sigma\) and \(A \in \text{MSAlg}_\Sigma\), the reduct \(A |_\Omega \in \text{MSAlg}_\Omega\) agrees with \(A\) in the interpretation of all sorts and operations in \(\Omega\) and discards everything in \(\Sigma \setminus \Omega\). If \(\varphi \in \text{Form}(\Omega)\) we have the equivalence \(A \models \varphi \iff A |_\Omega \models \varphi\).

An MS equational theory is a pair \(T = (\Sigma, E)\), with \(E\) a set of \(\Sigma\)-equations. \(\text{MSAlg}_{(\Sigma, E)}\) denotes the full subcategory of \(\text{MSAlg}_\Sigma\) with objects those \(A \in \text{MSAlg}_\Sigma\) such that \(A \models E\), called the \((\Sigma, E)\)-algebras. \(\text{MSAlg}_{(\Sigma, E)}\) has an initial algebra \(\text{T}_{\Sigma / E}\) \([22]\). The inference system in \([22]\) is sound and complete for MS equational deduction, i.e., for any MS equational theory \((\Sigma, E)\), and \(\Sigma\)-equation \(u = v\) we have an equivalence \(E \vdash u = v \iff E \models u = v\). For the sake of simpler inference we assume non-empty sorts, i.e., \(\forall s \in S, T_\Sigma; s \neq \emptyset\). Deducibility \(E \vdash u = v\) is abbreviated as \(u =_E v\).

In the above notions there is only an apparent lack of predicate symbols: full many-sorted first-order logic can be reduced to many-sorted algebra and the above language of equational formulas. The reduction is achieved as follows.

A many-sorted first-order (MS-FO) signature, is a pair \((\Sigma, \Pi)\) with \(\Sigma\) a MS signature with set of sorts \(S\), and \(\Pi\) an \(S^*\)-indexed set \(\Pi = \{ \Pi_w \}_{w \in S^*}\) of predicate symbols. We associate to a MS-FO signature \((\Sigma, \Pi)\) a MS signature \((\Sigma \cup \Pi)\) by adding to \(\Sigma\) a new sort \(\text{Pred}\) with a constant \(tt\) and viewing each \(p \in \Pi_w\) as a function symbol \(p : s_1 \ldots s_n \rightarrow \text{Pred}\). The reduction at the model level is now very simple: each \((\Sigma \cup \Pi)\)-algebra \(A\) defines a \((\Sigma, \Pi)\)-model \(A^\circ\) with \(\Sigma\)-algebra structure \(A |_\Sigma\) and having for each \(p \in \Pi_w\) the predicate interpretation \(A^\circ_p = A_{\Pi_w}^{-1} \text{Pred}(tt)\). The reduction at the formula level is also quite simple: we map a \((\Sigma, \Pi)\)-formula \(\varphi\) to an equational formula \(\varphi\), called its equational version, by just replacing each atom \(p(t_1, \ldots, t_n)\) by the equational atom \(p(t_1, \ldots, t_n) = tt\). The correctness of this reduction is just the easy to check equivalence:

\[ A^\circ \models \varphi \iff A \models \varphi. \]

A MS-FO theory is just a pair \(((\Sigma, \Pi), \Gamma)\), with \((\Sigma, \Pi)\) a MS-FO signature and \(\Gamma\) a set of \((\Sigma, \Pi)\)-formulas. Call \(((\Sigma, \Pi), \Gamma)\) equational iff \((\Sigma \cup \Pi, \tilde{\Gamma})\) is a many-sorted equational theory. By the above equivalence and the completeness of many-sorted equational logic such theories allow a sound and complete use of equational deduction also with predicate atoms. Note that if \(((\Sigma, \Pi), \Gamma)\) is equational, it is a very simple type of theory in many-sorted Horn Logic with
Equality and therefore has an initial model $T_{(\Sigma,\Pi),R}$. A useful, easy to check fact is that we have an identity: $T^0_{(\Sigma,\Pi),R} = T_{(\Sigma,\Pi),R}$.

Recall the notation for term positions, subterms, and term replacement from [9]: (i) positions in a term viewed as a tree are marked by strings $p \in \mathbb{N}^*$ specifying a path from the root, (ii) $t|_p$ denotes the subterm of term $t$ at position $p$, and (iii) $t[u|_p]$ denotes the result of replacing subterm $t|_p$ at position $p$ by $u$.

**Definition 1.** A rewrite theory is a triple $\mathcal{R} = (\Sigma, B, R)$ with $(\Sigma, B)$ a MS equational theory and $R$ a set of $\Sigma$-rewrite rules, i.e., sequents $l \rightarrow r$, with $l, r \in T_\Sigma(X)_s$ for some $s \in S$. In what follows it is always assumed that: (1) For each $l \rightarrow r \in R$, $l \notin X$ and $\text{vars}(r) \subseteq \text{vars}(l)$. (2) Each equation $u = v \in B$ is regular, i.e., $\text{vars}(u) = \text{vars}(v)$, and linear, i.e., there are no repeated variables in either $u$ or $v$. The one-step $R,B$-rewrite relation $t \rightarrow_{R,B} t'$, holds between $t, t' \in T_\Sigma(X)_s$, $s \in S$, if there is a rewrite rule $l \rightarrow r \in R$, a substitution $\sigma \in [X \rightarrow T_\Sigma(X)]$, and a term position $p$ in $t$ such that $t|_p = B \sigma$ and $t' = t[\sigma|_p]$. $\mathcal{R}$ is called: (i) terminating iff the relation $\rightarrow_{R,B}$ is well-founded; (ii) strictly $B$-coherent [21] iff whenever $u \rightarrow_{R,B} v$ and $u =_B u'$ there is a $v'$ such that $u' \rightarrow_{R,B} v'$ and $v =_B v'$; (iii) confluent iff $u \rightarrow_{R,B}^* v_1$ and $u \rightarrow_{R,B}^* v_2$ imply that there are $w_1, w_2$ such that $v_1 \rightarrow_{R,B}^* w_1$, $v_2 \rightarrow_{R,B}^* w_2$, and $w_1 =_B w_2$ (where $\rightarrow_{R,B}^*$ denotes the reflexive-transitive closure of $\rightarrow_{R,B}$); and (iv) convergent if (i)-(iii) hold. If $\mathcal{R}$ is convergent, for each $\Sigma$-term $t$ there is a term $u$ such that $t \rightarrow_{R,B}^* u$ and (\$) $u \rightarrow_{R,B} v$. We then write $u = t|_{R,B}$ and $t \rightarrow_{R,B}^* v|_{R,B}$, and call $t|_{R,B}$ the $R,B$-normal form of $t$, which, by confluence, is unique up to $B$-equality.

Given a set $E$ of $\Sigma$-equations, let $R(E) = \{u \rightarrow v \mid u = v \in E\}$. A decomposition of a MS equational theory $(\Sigma, E)$ is a convergent rewrite theory $\mathcal{R} = (\Sigma, B, R)$ such that $E = E_0 \cup B$ and $R = R(E_0)$. The key property of a decomposition is the following:

**Theorem 1.** (Church-Rosser Theorem) [13,21] Let $\mathcal{R} = (\Sigma, B, R)$ be a decomposition of $(\Sigma, E)$. Then we have an equivalence:

$$E \vdash u = v \iff u|_{R,B} =_B v|_{R,B}.$$ 

If $\mathcal{R} = (\Sigma, B, R)$ is a decomposition of $(\Sigma, E)$, and $X$ an $S$-sorted set of variables, the canonical term algebra $C_\mathcal{R}(X)$ has $C_\mathcal{R}(X)_s = \{[t|_{R,B}]_B \mid t \in T_\Sigma(X)_s\}$, and interprets each $f : s_1 ... s_n \rightarrow s$ as the function $C_\mathcal{R}(X)_{(f)} : \langle [u_1|_{R,B}], ... [u_n|_{R,B}] \rangle \mapsto [f[u_1, ... , u_n]|_{R,B}]_B$. By the Church-Rosser Theorem we then have an isomorphism $h : T^\Sigma_{E}(X) \cong C_\mathcal{R}(X)$, where $h : [t]_E \mapsto [t|_{R,B}]_B$. In particular, when $X$ is the empty family of variables, the canonical term algebra $C_\mathcal{R}$ is an initial algebra, and is the most intuitive possible model for $T^\Sigma_{E}$ as an algebra of values computed by $R, B$-simplification.

Quite often, the signature $\Sigma$ on which $T^\Sigma_{E}$ is defined has a natural decomposition as a disjoint union $\Sigma = \Omega \cup \Delta$, where the elements of $C_\mathcal{R}$, that is, the values computed by $R, B$-simplification, are $\Omega$-terms, whereas the function symbols $f \in \Delta$ are viewed as defined functions which are evaluated away by
**R. Gutierrez and J. Meseguer**

R, B-simplification, \( \Omega \) (with same poset of sorts as \( \Sigma \)) is then called a constructor subsignature of \( \Sigma \). Call a decomposition \( \mathcal{R} = (\Sigma, B, R) \) of \( (\Sigma, E) \) sufficiently complete with respect to the constructor subsignature \( \Omega \) iff for each \( t \in T_{\Sigma} \) we have: (i) \( t!_{R,B} \in T_{\Omega} \), and (ii) if \( u \in T_{\Omega} \) and \( u =_B v \), then \( v \in T_{\Omega} \). This ensures that for each \( [u]_B \in C_{\mathcal{R}} \) we have \( [u]_B \subseteq T_{\Omega} \). We will give several examples of decompositions \( \Sigma = \Omega \oplus \Delta \) into constructors and defined functions.

As we can see in the following definition, sufficient completeness is closely related to the notion of a protecting theory inclusion.

**Definition 2.** An equational theory \( (\Sigma, E) \) protects another theory \( (\Omega, E_\Omega) \) iff \( (\Omega, E_\Omega) \subseteq (\Sigma, E) \) and the unique \( \Omega \)-homomorphism \( h : T_{\Omega/\Omega_0} \rightarrow T_{\Sigma/E_\Omega} \) is an isomorphism \( h : T_{\Omega/\Omega_0} \cong T_{\Sigma/E_\Omega} \). A decomposition \( \mathcal{R} = (\Sigma, B, R) \) protects another decomposition \( \mathcal{R}_0 = (\Sigma_0, B_0, R_0) \) iff \( \mathcal{R}_0 \subseteq \mathcal{R} \), i.e., \( \Sigma_0 \subseteq \Sigma \), \( B_0 \subseteq B \), and \( R_0 \subseteq R \), and for all \( t, t' \in T_{\Sigma_0}(X) \) we have: (i) \( t =_{B_0} t' \iff t = B t' \), (ii) \( t = t!_{R_0,B_0} \iff t = t!_{R,B} \), and (iii) \( C_{\mathcal{R}_0} = C_{\mathcal{R}}|_{\Sigma_0} \).

\( \mathcal{R}_H = (\Omega, B_H, R_H) \) is a constructor decomposition of \( \mathcal{R} = (\Sigma, B, R) \) iff \( \mathcal{R} \) protects \( \mathcal{R}_H \) and \( \Sigma \) and \( \Omega \) have the same poset of sorts, so that by (iii) above \( \mathcal{R} \) is sufficiently complete with respect to \( \Omega \). Furthermore, \( \Omega \) is called a subsignature of free constructors modulo \( B_H \) if \( \mathcal{R}_H = \emptyset \), so that \( C_{\mathcal{R}_H} = T_{\Omega/\Omega_0} \).

The case where all constructor terms are \( R, B \)-normal form is captured by \( \Omega \) being a subsignature of free constructors modulo \( B_H \). Note also that conditions (i) and (ii) are, so called, “no confusion” conditions, and for protecting extensions (iii) is a “no junk” condition, that is, \( \mathcal{R} \) does not add new data to \( C_{\mathcal{R}_H} \).

Given a MS equational theory \( (\Sigma, E) \) and a conjunction of \( \Sigma \)-equations \( \phi = \phi_1 \land \ldots \land \phi_n \), an \( E \)-unifier of \( \phi \) is a substitution \( \sigma \) such that \( \phi_1 \sigma =_E \phi_2 \sigma \), \( 1 \leq i \leq n \). An \( E \)-unification algorithm for \( (\Sigma, E) \) is an algorithm generating for each system of \( \Sigma \)-equations \( \phi \) and finite set of variables \( W \supseteq \text{vars}(\phi) \) a complete set of \( E \)-unifiers \( \text{Unif}_E^W(\phi) \) where each \( \tau \in \text{Unif}_E^W(\phi) \) is assumed idempotent and with \( \text{dom}(\tau) = \text{vars}(\phi) \), and is “away from \( W \)” in the sense that \( \text{ran}(\tau) \cap W = \emptyset \). The set \( \text{Unif}_E^W(\phi) \) is called “complete” in the precise sense that for any \( E \)-unifier \( \sigma \) of \( \phi \) there is a \( \tau \in \text{Unif}_E^W(\phi) \) and a substitution \( \rho \) such that \( \sigma|_W =_E (\tau \rho)|_W \), where, by definition, \( \alpha =_E \beta \) means \( (\forall x \in X) \alpha(x) =_E \beta(x) \) for substitutions \( \alpha, \beta \). Such an algorithm is called finitary if it always terminates with a finite set \( \text{Unif}_E^W(\phi) \) for any \( \phi \).

The notion of variant answers, in a sense, two questions: (i) how can we best describe symbolically the elements of \( C_{\mathcal{R}}(X) \) that are reduced substitution instances of a pattern term \( t \) and (ii) given an original pattern \( t \), how many other patterns do we need to describe the reduced instances of \( t \) in \( C_{\mathcal{R}}(X) \)?

**Definition 3.** Given a decomposition \( \mathcal{R} = (\Sigma, B, R) \) of a MS equational theory \( (\Sigma, E) \) and a \( \Sigma \)-term \( t \), a variant of \( t \) is a pair \( (u, \theta) \) such that: (i) \( u =_B (\theta t)!_{R,B} \), (ii) \( \text{dom}(\theta) \subseteq \text{vars}(t) \), and (iii) \( \theta = \theta!_{R,B} \), that is, \( \theta(x) = (\theta(x))!_{R,B} \) for

---

3 For a discussion of similar but not exactly equivalent versions of the variant notion see [3]. Here we follow the shaper formulation in [11], rather than the one in [8], because it is technically essential for some results to hold [3].
all variables \( x \). \((u, \theta, \gamma)\) is called a ground variant iff, furthermore, \( u \in T_{\Sigma} \). Given variants \((u, \theta, \gamma)\) and \((v, \gamma)\) of \( t \), \((u, \theta, \gamma)\) is called more general than \((v, \gamma)\), denoted \((u, \theta, \gamma) \supseteq_B (v, \gamma)\), iff there is a substitution \( \rho \) such that: (i) \( (\theta \rho) \mid_{\text{vars}(t)} = \gamma \), and (ii) \( u \rho = B v \). Let \( [t]_{B} = \{(u, \theta) \mid i \in I\} \) denote a complete set of variants of \( t \), that is, a set of variants such that for any variant \((v, \gamma)\) of \( t \) there is an \( i \in I \), such that \((u, \theta) \supseteq_B (v, \gamma)\).

A decomposition \( R = (\Sigma, B, R) \) of \( (\Sigma, E) \) has the finite variant property \([8]\) (FVP) iff for each \( \Sigma \)-term \( t \) there is a finite complete set of variants \( [t]_{B} \) can be chosen to be not only complete, but also a set of most general variants, in the sense that for \( 1 \leq i < j \leq n \), \( (u_{i}, \theta_{i}) \supseteq_B (u_{j}, \theta_{j}) \). Also, given any finite set of variables \( W \supseteq \text{vars}(t) \) we can always choose \( [t]_{B} \) to be of the form \( [t]_{B}^{W} \), where each \((u_{i}, \theta_{i}) \in [t]_{B}^{W} \) has \( \theta_{i} \) idempotent with \( \text{dom}(\theta_{i}) = \text{vars}(t) \), and “away from \( W \),” in the sense that \( \text{ran}(\theta_{i}) \cap W = \emptyset \).

If \( B \) has a finitary unification algorithm, the folding variant narrowing strategy described in \([11]\) provides an effective method to generate \( [t]_{B} \). Furthermore, folding variant narrowing terminates for each input \( t \in T_{\Sigma}(X) \) with a finite set \( [t]_{B} \) iff \( R \) has FVP \([11]\).

Two example theories, one FVP and another not FVP, were given in the Introduction. Many other examples are given in \([20]\). The following will be used as a running example of an FVP theory:

**Example 1.** (Sets of Natural Numbers). Let \( \text{NatSet} = (\Sigma, B, R) \) be the following equational theory. \( \Sigma \) has sorts \( \text{Nat}, \text{NatSet} \) and \( \text{Pred} \), subsort inclusion, \( \text{Nat} \subset \text{NatSet} \), and decomposes as \( \Sigma = \Omega_{\Sigma} \uplus \Delta \), where the constructors \( \Omega_{\Sigma} \) include the following operators: 0 and 1 of sort \( \text{Nat} \), \( +, \cdot : \text{NatNat} \rightarrow \text{Nat} \) (addition), \( \subseteq \) of sort \( \text{NatSet} \), \( \subseteq_{\text{NatSetNatSet}} \rightarrow \text{NatSet} \) (set union), \( tt \) of sort \( \text{Nat} \), and a subset containment predicate expressed as a function \( \subseteq_{\text{NatSetNatSet}} \rightarrow \text{Pred} \). \( B \) decomposes as \( B = B_{\Omega} \uplus B_{\Delta} \). The axioms \( B_{\Omega} \) include: (i) the associativity and commutativity of \( +, \cdot \) with identity 0, the associativity and commutativity of \( \subseteq_{\text{NatSet}} \) \( R \) decomposes as \( R = R_{\Omega} \uplus R_{\Delta} \). The rules \( R_{\Omega} \) include: (i) an identity rule for union \( NS \), \( \subseteq_{\text{NatSetNatSet}} \rightarrow NS \); (ii) idempotency rules for union \( NS, NS \rightarrow NS \), and \( NS, NS \rightarrow NS, NS' \); and (iii) rules defining the \( \subseteq_{\text{NatSetNatSet}} \subseteq_{\text{NatSetNatSet}} \subseteq_{\text{NatSetNatSet}} tt, NS \subseteq NS \rightarrow tt, and NS \subseteq NS \rightarrow NS' \rightarrow tt \), where \( NS \) and \( NS' \) have sort \( \text{NatSet} \). The signature \( \Delta \) of defined functions has operators \( \text{max} : \text{NatNat} \rightarrow \text{Nat}, \text{min} : \text{NatNatNat} \rightarrow \text{Nat} \), \( \leftarrow : \text{NatNatNat} \rightarrow \text{Nat} \), for the maximum, minimum and “minus” (subtraction) functions. The axioms \( B_{\Delta} \) are the commutativity of the \( \text{max} \) and \( \text{min} \) functions. The rules \( R_{\Delta} \) for the defined functions are: \( \text{max}(N, N + M) \rightarrow N + M, \text{min}(N, N + M) \rightarrow N, N \rightarrow (N + M) \rightarrow 0 \), and \( (N + M) \rightarrow N \rightarrow M \), where \( N \) and \( M \) have sort \( \text{Nat} \).

---

4 As pointed out at the beginning of Section \([2]\) \([11]\) treats the more general order-sorted case, where sorts form a poset \((S, \leq)\) with \( s \leq s' \) interpreted as set containment \( A_{s} \subseteq A_{s'} \) in a \( \Sigma \)-algebra \( A \). All results in this paper hold in the order-sorted case.
The predicates ∈ and ⊆ need not be explicitly defined, since they can be expressed by the definitional equivalences $N ∈ NS = tt ↔ N, NS = NS$, and $NS ⊆ NS' = tt ↔ NS ⊆ NS' = tt ∧ NS + NS'$. FVP is a semi-decidable property [5], which can be easily verified (when it holds) by checking, using folding variant narrowing (supported by Maude 2.7), that for each function symbol $f : s_1 . . . s_n → s$ the term $f(x_1, . . . , x_n)$, with $x_i$ of sort $s_i$, $1 ≤ i ≤ n$, has a finite number of most general variants. Given an FVP decomposition $R$ its variant complexity is the total number $n$ of variants for all such $f(x_1, . . . , x_n)$, provided $f$ has some associated rules of the form $f(t_1, . . . , t_n) → t'$. This gives a rough measure of how costly it is to perform variant computations relative to the cost of performing $B$-unification. For example, the variant complexity of NatSet above is 20.

To be able to express systems of equations, say, $u_1 = v_1 ∧ . . . ∧ u_n = v_n$, as terms, we can extend an MS signature $Σ$ with sorts $S$ to an OS signature $Σ^\prec$ by: (1) adding to $S$ fresh new sorts $\text{Lit}$ and $\text{Conj}$ with a sortset inclusion $\text{Lit} < \text{Conj}$; (2) adding a binary conjunction operator $\_ \& \_ : \text{Lit Conj} → \text{Conj}$; and (3) adding for each $s ∈ S$ binary operators $\_ = \_ : s s → \text{Lit}$ and $\_ + \_ : s s → \text{Lit}$.

Variant-based unification goes back to [11]. The paper [20] gives a more precise characterization using $Σ^\prec$-terms as follows. If $R = (Σ, B, R)$ is an FVP decomposition of $(Σ, E)$ and $B$ has a finitary $B$-unification algorithm, given a system of $Σ$-equations $φ$ with variables $W$, folding variant narrowing computes a finite set $\text{VarUnif}_E^W (φ)$ of $E$-unifiers away from $W$ that is complete in the strong sense that if $α$ is an $R, B$-normalized $E$-unifier of $φ$ there exists $θ ∈ \text{VarUnif}_E^W (φ)$ and an $R, B$-normalized $ρ$ such that $α|_W = B (θρ)|_W$.

3 Constructor Variants and OS-Compactness

We gather some technical notions and results needed for the inductive satisfiability procedure given in Section 4.

The notion of constructor variant answers the question: what variants of $t$ cover as instances modulo $B_D$ all canonical forms of all ground instances of $t$? The following lemma (stated and proved at the more general order-sorted level in [14], but stated here for the MS case for simplicity) gives a precise answer under reasonable assumptions. For more on constructor variants see [20][26][14].

**Lemma 1.** Let $R = (Σ, B, R)$ be an FVP decomposition of $(Σ, E)$ protecting a constructor decomposition $R_D = (Ω, B_O, R_D)$. Assume that: (i) $Σ = Ω ∪ Δ$ with $Ω ∩ Δ = \emptyset$; (ii) $B$ has a finitary $B$-unification algorithm and $B = B_Ω ∪ B_Δ$, with $B_Ω$ $Ω$-equations and if $u = v ∈ B_Δ$, $u, v$ are non-variable $Δ$-terms. Call $\{ \{v, θ\} ∈ \text{VarUnif}_E^W (φ) \mid v ∈ T_D(X)\}$ the set of constructor variants of $t$. If $[u] ∈ C_{x_t}$ is of the form $u = B (τγ)|_{R, B}$, then there is $(v, θ) ∈ \{ \}^D_{R, B}$ and a normalized ground substitution $τ$ such that $u = B v τ$.

We finally need the notion of an order-sorted OS-compact equational OS-FO theory $(Σ, Π, Θ)$, generalizing the compactness notion in [7]. The notion is the same (but called MS-compactness) for the special case of MS theories treated in
the preliminaries to simplify the exposition. It is stated here in the more general OS case because the satisfiability algorithm in Section 4 works for the more general OS case, and the paper’s examples are in fact OS theories.

Given a OS equational theory \((\Sigma, E)\), call a \(\Sigma\)-equality \(u = v\) \(E\)-trivial iff \(u = v\) \(E\), and a \(\Sigma\)-disequality \(u \neq v\) \(E\)-consistent iff \(u \neq v\) \(E\). Likewise, call a conjunction \(\bigwedge D\) of \(\Sigma\)-disequalities \(E\)-consistent if each \(u \neq v\) in \(D\) is so. Call a sort \(s \in S\) finite in both \((\Sigma, E)\) and \(T_{\Sigma/E, s}\) is a finite set, and infinite otherwise.

**Definition 4.** An equational OS-FO theory \((\Sigma, \Pi, \Gamma)\) is called OS-compact iff: (i) for each sort \(s \in \Sigma\) we can effectively determine whether \(s\) is finite or infinite in \(T_{\Sigma, \Pi, \Gamma}\); and, if finite, can effectively compute a representative ground term \(\text{rep}(\bar{u}) \in [u]\) for each \([u] \in T_{\Sigma, \Pi, \Gamma, s}\); (ii) \(\bar{F}\) is decidable and \(\bar{F}\) has a finitary unification algorithm; and (iii) any finite conjunction \(\bigwedge D\) of negated \((\Sigma, \Pi)\)-atoms whose variables all have infinite sorts and such that \(\bigwedge D\) is \(\bar{F}\)-consistent is satisfiable in \(T_{\Sigma, \Pi, \Gamma}\).

Call an OS theory \((\Sigma, E)\) OS-compact iff OS-FO theory \((\Sigma, \emptyset, E)\) is OS-compact.

The key theorem, generalizing a similar one in [7] is the following:

**Theorem 2.** [20, 19] If \((\Sigma, \Pi, \Gamma)\) is an OS-compact theory, then satisfiability of QF \((\Sigma, \Pi)\)-formulas in \(T_{\Sigma, \Pi, \Gamma}\) is decidable.

The following OS-compactness results are proved in detail in [20]: (i) a free constructor decomposition modulo axioms \(\mathcal{R}_B = (\Omega, B_\Omega, \mathcal{R}_\Omega)\) for \(B_\Omega\) any combination of associativity, commutativity and identity axioms, except associativity without commutativity, is OS-compact; and (ii) the constructor decompositions for parameterized modules for lists, compact lists, multisets, sets, and hereditarily finite (HF) sets are all OS-compact-preserving, in the sense that if the actual parameter has an OS-compact constructor decomposition, then the corresponding instantiation of the parameterized constructor decomposition is OS-compact.

**Example 2.** The constructor decomposition \(\mathcal{R}_\Omega = (\Omega, B_\Omega, \mathcal{R}_\Omega)\) for the NatSet theory in Example 1 is OS-compact. This follows from the fact that NatSet with set containment predicate \(\subseteq\) is just the instantiation of the constructor decomposition for the parameterized module of (finite) sets in [20] to the natural numbers with 0, 1, and \(\_\_\), which is itself a theory of free constructors modulo associativity, commutativity and identity 0 for \(\_\_\) and therefore OS-compact by (i), so that, by (ii), \(\mathcal{R}_\Omega = (\Omega, B_\Omega, \mathcal{R}_\Omega)\) is also OS-compact.

4 QF Satisfiability in Initial Algebras with Predicates

The known variant-based quantifier-free (QF) satisfiability and validity results [20, 19] apply to the initial algebra \(T_{\Sigma/E}\) of an equational theory \((\Sigma, E)\) having an FVP variant-decomposition \(\mathcal{R} = (\Sigma, B, \mathcal{R})\) protecting a constructor decomposition \(\mathcal{R}_B = (\Omega, B_\Omega, \mathcal{R}_\Omega)\) and such that: (i) \(\mathcal{R}\) has a finitary unification algorithm; and (ii) the equational theory of \(\mathcal{R}_\Omega = (\Omega, B_\Omega, \mathcal{R}_\Omega)\) is OS-compact.
Example 3. QF validity and satisfiability in the initial algebra $T_{\Sigma,E}$ for $(\Sigma,E)$ the theory with the NatSet FVP variant-decomposition $R = (\Sigma,B,R)$ in Example 1 are decidable because its axioms $B$ have a finitary unification algorithm and, as explained in Example 2, its constructor decomposition $R_B = (\Omega,B_B,R_B)$ is OS-compact.

The decidable inductive validity and satisfiability results in [20] apply indeed to many data structures of interest, which may obey structural axioms $B$ such as commutativity, associativity-commutativity, or identity. Many useful examples are given in [23], and a prototype Maude implementation is presented in [20]. There is, however, a main limitation about the range of examples to which these results apply, which this work directly addresses. The limitation comes from the introduction of user-definable predicates. Recall that we represent a predicate $p$ with sorts $s_1,\ldots,s_n$ as a function $p: s_1,\ldots,s_n \rightarrow \text{Pred}$ defined in the positive case by confluent and terminating equations $p(u_1^i,\ldots,u_n^i) = tt$, $1 \leq i \leq k$. The key problem with such predicates $p$ is that, except in trivial cases, there are typically ground terms $p(v_1,\ldots,v_n)$ for which the predicate does not hold. This means that $p$ must be a constructor operator of sort $\text{Pred}$ which is not a free constructor modulo the axioms $B_B$. This makes proving OS-compactness for a constructor decomposition $R_B = (\Omega,B_B,R_B)$ including user-definable predicates a non-trivial case-by-case task. For example, the proofs of OS-compactness for the set containment predicate $\subseteq$ in the parameterized module of finite sets and for other such predicates in other FVP parameterized modules in [20] all required non-trivial analyses. Furthermore, OS-compactness may fail for some $R_B$ precisely because of predicates (see Example 4 below).

Example 4. Consider the following extension by predicates $\text{NatSetPreds}$ of the NatSet theory in Example 1 where the constructor signature $\Omega = \Omega_c \cup \Omega_B$ adds the subsignature $\Omega_B$ containing the strict order predicate $\prec : \text{Nat} \rightarrow \text{Nat}$, the “sort predicate” $\succ : \text{Nat} \rightarrow \text{NatSet} \rightarrow \text{Pred}$, characterizing when a set of natural numbers is a natural, and the even and odd predicates $\text{even} : \text{NatSet} \rightarrow \text{Pred}$, $\text{odd} : \text{NatSet} \rightarrow \text{Pred}$, defined by the rules $R_B$: $N + M + 1 > N \rightarrow tt$, $N : \text{Nat} \rightarrow tt$, $\text{even}(N + N) \rightarrow tt$, $\text{odd}(N + N + 1) \rightarrow tt$, where $N$ and $M$ have sort $\text{Nat}$. $\text{NatSetPreds}$ is FVP, but its constructor decomposition $R_B = (\Omega_c \cup \Omega_B, B_B, R_B)$ is not OS-compact, since the negation of the trichotomy law $N > M \lor M > N \lor N = M$ is the $B_B$-consistent but unsatisfiable conjunction of disequalities $N > M \lor tt \land M > N \lor tt \land N + M$.

The goal of this work is to provide a decision procedure for validity and satisfiability of QF formulas in the initial algebra of an FVP theory $R$ that may contain user-definable predicates and protects a constructor decomposition $R_B$ that need not be OS-compact, under the following reasonable assumptions: (1) $R = (\Delta \cup \Omega_c \cup \Omega_B, B_B, R_B)$ protects $R_B = (\Omega_c \cup \Omega_B, B_B, R_B)$, where $\Omega_B$ consists only of predicates, and $R_B$ consists of rules of the form $p(u_1^i,\ldots,u_n^i) \rightarrow tt$, $1 \leq i \leq k_p$, defining each $p \in \Omega_B$; furthermore, $R_B$ satisfies conditions (i)–(ii) in Lemma 1. (2) $R_B = (\Omega_c, B_B, R_B)$ is OS-compact, its finite sorts (if any) are different from
Pred, and is the constructor decomposition of \((\Delta \cup \Omega_c \cup B_{\Delta} \cup R_{\Delta} \cup R_{\Omega})\); and (3) each \(p \in \Omega_{\Pi}\) has an associated set of negative constrained patterns of the form:

\[
\bigwedge_{1 \leq i \leq \ell} w^i_1 \uplus w^i_r \Rightarrow p(v^i_1, \ldots, v^i_n) \uplus tt, \ 1 \leq j \leq m_p
\]

with the \(v^i_1, w^i_1\) and \(w^i_r\) \(\Omega_c\)-terms with variables in \(Y_j = \text{vars}(p(v^i_1, \ldots, v^i_n))\). These negative constrained patterns are interpreted as meaning that the following semantic equivalences are valid in \(C_{\mathcal{R}}\) for each \(p \in \Omega_{\Pi}\), where \(\rho_j \in \{\rho \in [Y_j \rightarrow T_{\Omega_c}] \mid \rho = p_{1 R, B}\}, B = B_{\Delta} \cup B_{\Omega_c}\), and \(R = R_{\Delta} \cup R_{\Omega_c} \cup R_{\Pi}\):

\[
[p(v^i_1, \ldots, v^i_n)\rho_j] \in C_{\mathcal{R}} \iff \bigwedge_{1 \leq i \leq \ell} (w^i_1 \uplus w^i_r)\rho_j
\]

\[
[p(t_1, \ldots, t_n)] \in C_{\mathcal{R}} \iff \exists j \exists \rho_j [p(t_1, \ldots, t_n)] = [p(v^i_1, \ldots, v^i_n)\rho_j] \land \bigwedge_{1 \leq i \leq \ell} (w^i_1 \uplus w^i_r)\rho_j
\]

The first equivalence means that any instance of a negative pattern by a normalized ground substitution \(\rho_j\) satisfying its constrain is normalized, so that \(C_{\mathcal{R}} \models p(v^i_1, \ldots, v^i_n)\rho_j \uplus tt\). The second means that \(p(t_1, \ldots, t_n)] \in C_{\mathcal{R}}\) iff \(p(t_1, \ldots, t_n)]\) instantiates a negative pattern satisfying its constraint.

**Example 5.** The module \(\text{NatSetPreds}\) from Example 4 satisfies above conditions (1)–(3). Indeed, (1), including conditions (i)–(ii) in Lemma 1 follows easily from its definition and that of \(\text{NatSet}\), and (2) also follows easily from the definition of \(\text{NatSet}\) and the remarks in Example 2. This leaves us with condition (3), where the negative constrained patterns for \(\Omega_{\Pi} = \{\_ > \_ \text{ even, odd, } \_ : \text{Nat}\}\) are the following:

- \(N > N + M \uplus tt\)
- \(\text{even}(N + N + 1) \uplus tt, \ \text{even}(\emptyset) \uplus tt, \ (N \leq NS \uplus tt \land NS + \emptyset) \Rightarrow \text{even}(N, NS) \uplus tt\)
- \(\text{odd}(N + N) \uplus tt, odd(\emptyset) \uplus tt, (N \leq NS \uplus tt \land NS + \emptyset) \Rightarrow odd(N, NS) \uplus tt\)
- \(\emptyset : \text{Nat} \uplus tt, \ (N \leq NS \uplus tt \land NS + \emptyset) \Rightarrow (N, NS): \text{Nat} \uplus tt\)

where \(N\) and \(M\) have sort \(\text{Nat}\) and \(NS\) sort \(\text{Natset}\). As explained in Appendix A of [13], the first equivalence can be automatically checked using folding variant narrowing. For a proof that the two equivalences hold in \(C_{\mathcal{R}}\) for these predicates and their patterns (a few patterns are missing in the proof by mistake) see [13].

**The Inductive Satisfiability Decision Procedure.** Assume \(\mathcal{R}\) satisfies conditions (1)–(3) above and let \(\Sigma = \Delta \cup \Omega_c \cup \Omega_{\Pi}\), and \(E\) be the axioms \(B\) plus the equations associated with the rules \(R\) in \(\mathcal{R}\). Given a QF \(\Sigma\)-formula \(\varphi\) the procedure decides if \(\varphi\) is satisfiable in \(C_{\mathcal{R}}\). We can reduce the inductive validity decision problem of whether \(C_{\mathcal{R}} \models \varphi\) to deciding whether \(\neg \varphi\) is unsatisfiable in \(C_{\mathcal{R}}\). Since any QF \(\Sigma\)-formula \(\varphi\) can be put in disjunctive normal form, a disjunction is satisfiable in \(C_{\mathcal{R}}\) iff one of the disjuncts is, and all predicates have been turned into functions of sort \(\text{Pred}\), it is enough to decide the satisfiability of a conjunction of \(\Sigma\)-literals of the form \(\bigwedge G \land \bigvee D\), where the \(G\) are equations and the \(D\) are disequations. The procedure performs the following steps:
1. **Unification.** Satisfiability of the conjunction $\bigwedge G \land \bigwedge D$ is replaced by satisfiability for some conjunction in the set $\{(\bigwedge D_\alpha)_{R,B} \mid \alpha \in \text{VarUnif}_E(\bigwedge G)\}$, discarding any obviously unsatisfiable $\bigwedge D_\alpha$ in such a set.

2. **II-Elimination.** After Step (1), each conjunction is a conjunction of disequalities $\bigwedge D'$. If $\bigwedge D'$ is a $\Delta \omega \Omega_c$-formula, we go directly to Step (3); otherwise $\bigwedge D'$ has the form $\bigwedge D' = \bigwedge D_1 \land p(t_1, \ldots, t_n) \neq tt \land \bigwedge D_2$, where $p \in \Omega_R$ and $D_1$ and/or $D_2$ may be empty conjunctions. We then replace $\bigwedge D'$ by all not obviously unsatisfiable conjunctions of the form:

$$\bigwedge_{1 \leq i \leq n_j} w^i_1 + w^i_2 \land \bigwedge D_2 \sigma$$

where $1 \leq j \leq m_p$, $W = \text{vars}(\bigwedge D')$, $(p(t'_1, \ldots, t'_n), \theta) \in [p(t_1, \ldots, t_n)]_{R,B}^W$, and $\alpha$ is a disjoint $B_{\Omega_c}$-unifier of the equation $p(t'_1, \ldots, t'_n) = p(v^1_1, \ldots, v^1_n)$ (i.e., sides are renamed to share no variables and $\text{ran}(\alpha) \land (W \cup \text{ran}(\theta)) = \emptyset$).

We use the negative constrained patterns of $p$ and the constructor variants of $p(t_1, \ldots, t_n)$ to eliminate the disequality $p(t_1, \ldots, t_n) \neq tt$. If for some $p' \in \Omega_R$ some disequality remains in $\bigwedge D_1 \land \bigwedge D_2 \sigma$, we iterate Step 2.

3. **Computation of $\Omega_c^\omega$-Variants and Elimination of Finite Sorts.** For $\bigwedge D'$ a $\Delta \omega \Omega_c$-conjunction of disequalities, viewed as a $(\Delta \omega \Omega_c)^\omega$-term its constructor $\Omega_c^\omega$-variants are of the form $\bigwedge D'^\omega$, with $\Delta \omega \Omega_c$-conjunction of disequalities. The variables of $\bigwedge D'^\omega$ are then $Y_{\text{fin}} \sqcup Y_{\text{inf}}$, with $Y_{\text{fin}}$ the variables whose sorts are finite, and $Y_{\text{inf}}$ the variables with infinite sorts. Compute all normalized ground substitution $\tau$ of the variables $Y_{\text{fin}}$ obtained by: (i) independently choosing for each variable $y \in Y_{\text{fin}}$ a canonical representative for the sort of $y$ in all possible ways, and (ii) checking that for the $\tau$ so chosen $\bigwedge D'^\omega \tau$ is normalized, keeping $\tau$ if this holds and discarding it otherwise. Then $\bigwedge D'$ is satisfiable in $\mathcal{C}_R$ iff some $\bigwedge D'^\omega \tau$ so obtained is $B_{\Omega_c}^\omega$-consistent for some $\Omega_c^\omega$-variant $\bigwedge D'^\omega \gamma$ of $\bigwedge D'$.

**Example 6.** We can illustrate the use of the above decision procedure by proving the validity of the QF formula $\text{odd}(N) = tt \Leftrightarrow \text{even}(N) \neq tt$ in the initial algebra $\mathcal{C}_R$ of NatSetPreds. That is, we need to show that its negation $(\text{odd}(N) = tt \land \text{even}(N) = tt) \lor (\text{odd}(N) \neq tt \land \text{even}(N) \neq tt)$ is unsatisfiable in $\mathcal{C}_R$.

Applying the **Unification** step to the first disjunct $\text{odd}(N) = tt \land \text{even}(N) = tt$ no variant unifiers are found, making this disjunct unsatisfiable. Applying the **II-Elimination** step to the first disequality in the second disjunct $\text{odd}(N) \neq tt \land \text{even}(N) \neq tt$, since the only constructor variant of $\text{odd}(N)$ different from $tt$ is the identity variant, and the only disjoint $B_{\Omega_c}$-unifier of $\text{odd}(N)$ with the negative patterns for odd is $\{N \mapsto M + M\}$ for the (renamed) unconstrained negative pattern $\text{odd}(M + M) \neq tt$, we get the disequality $\text{even}(M + M) \neq tt$, whose normal form $tt \neq tt$ is unsatisfiable.

**Theorem 3.** For $\mathcal{FVP} = (\Delta \omega \Omega_c \cup \Omega_R, B_\Delta \cup B_{\Omega_c}, R_\Delta \cup R_{\Omega_c}, w \cup w_R)$ protecting $\mathcal{R}_\Omega = (\Omega_c \cup R_R, B_{\Omega_R}, R_\Omega \cup R_R)$ and satisfying above conditions (1)–(3), the above procedure correctly decides the satisfiability of a QF $\Sigma$-formula $\varphi$ in the canonical term algebra $\mathcal{C}_R$. 

Sort Predicates for Recursive Data Structures. We can axiomatize many (non-circular) recursive data structures as the elements of an initial algebra $T_\Omega$ on a many-sorted signature of free constructors $\Omega$. For example, lists can be so axiomatized with $\Omega$ consisting of just two sorts, Elt, viewed as a parametric sort of list elements, and List, a constant nil of sort List, and a “cons” constructor

$\lambda x: \text{Elt} \rightarrow \text{List}. \text{cons} x \rightarrow \text{List}$

In general, however, adding to such data structures defined functions corresponding to “selectors” that can extract the constituent parts of each data structure cannot be done in a satisfactory way if we remain within a many-sorted setting. For example, for lists we would like to have selectors head and tail (the usual car and cdr in Lisp notation). For head the natural equation is $\text{head}(x;l) = x$. Likewise, the natural equation for tail is $\text{tail}(x;l) = l$. But this leaves open the problem of how to define $\text{head}(\text{nil})$, for which no satisfactory solution exists. J. Meseguer and J.A. Goguen proposed a simple solution to this “constructor-selector” problem using initial order-sorted algebras in [23]. The key idea is the following. For each non-constant constructor symbol, say $c: A_1 \ldots A_n \rightarrow B$, $n \geq 1$, we introduce a subsort $B_c < B$ and give the tighter typing $c: A_1 \ldots A_n \rightarrow B_c$. The selector problem is now easily solved by associating to each non-constant constructor $c$ selector functions $\text{sel}_i^c : B_c \rightarrow A_i$, $1 \leq i \leq n$, defined by the equations $\text{sel}_i^c(c(x_1, \ldots, x_n)) = x_i$, $1 \leq i \leq n$. Outside the subsort $B_c$ the selectors $\text{sel}_i^c$ are actually undefined. For the above example of lists this just means adding a subsort $\text{List}_{\text{NeList}} < \text{List}$, where $\text{List}_{\text{NeList}}$ is usually written as $\text{NeList}$ (non-empty lists), and tightening the typing of “cons” to

$\lambda x: \text{Elt} \rightarrow \text{NeList}. \text{NeList} \rightarrow \text{NeList}$

In this way the head and tail selectors have typings $\text{head} : \text{NeList} \rightarrow \text{Elt}$ and $\text{tail} : \text{NeList} \rightarrow \text{List}$, again with equations $\text{head}(x;l) = x$ and $\text{tail}(x;l) = l$, with $x$ of sort $\text{Elt}$ and $l$ of sort $\text{List}$.

We have just described a general theory transformation $\Omega \rightarrow (\widehat{\Omega} \uplus \Delta, E_\Delta)$ from any MS signature $\Omega$ to an OS theory with selectors $\Delta$. Due to space limitations, the following key facts are discussed in detail in Section 4.2 of [14]:

1. $(\widehat{\Omega} \uplus \Delta, \emptyset, R(E_\Delta))$ is FVP with $(\hat{\Omega}, \emptyset, \emptyset)$ as its constructor decomposition.
2. To increase expressiveness, we can define for each subsort $B_c$ associated with a constructor $c$ a corresponding equationally-defined sort predicate $\_ : B_c$, thus obtaining a decomposition $(\widehat{\Omega} \uplus \mathcal{I} \uplus \Delta, \emptyset, R(E_\Delta) \cup R(E_{\mathcal{I}}))$ that is also FVP.
3. Each sort predicate $\_ : B_c$ has an associated set of negative patterns, so that our variant satisfiability algorithm makes satisfiability of QF formulas in the initial algebra $T_{\widehat{\Omega} \uplus \mathcal{I} \uplus \Delta / E_\Delta = E_{\mathcal{I}}}$ decidable.

Example 7. (Lists of Naturals with Sort Predicates). We can instantiate the above order-sorted theory of lists with selectors head and tail by instantiating the parameter sort Elt to a sort Nat with constant 0, subsort NzNat < Nat, and unary constructor $s : \text{Nat} \rightarrow \text{NzNat}$ with selector $p : \text{NzNat} \rightarrow \text{Nat}$ satisfying the equation $p(s(n)) = n$. We then extend this specification with sort predicates

$\_ : \text{NzNat} \rightarrow \text{Pred}$ and $\_ : \text{NeList} \rightarrow \text{List} \rightarrow \text{Pred}$, defined by equations $n' : \text{NzNat} = tt$ and $\_ : \text{NeList} = tt$, with $n'$ of sort $\text{NzNat}$ and $\_ : \text{NeList}$ of sort $\text{NeList}$. Their corresponding negative patterns are: $0 : \text{NzNat} \perp tt$ and $nil : \text{NeList} \perp tt$. 
One advantage of adding these sort predicates is that some properties not expressible as QF formulas become QF-expressible. For example, to state that every number is either 0 or a non-zero number (resp. every list is either nil or a non-empty list) we need the formula $n \not= 0 \lor (\exists n') n = n'$ (resp. $l = \text{nil} \lor (\exists l') l = l'$), where $n$ has sort Nat and $n'$ sort NzNat (resp. $l$ has sort List and $l'$ sort NeList). But with sort predicates this can be expressed by means of the QF formula $n = 0 \lor n : \text{Nat} = t$ (resp. $l = \text{nil} \lor l : \text{List} = t$).

5 Implementation

We have implemented the variant satisfiability decision procedure of Section 4 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. Let us illustrate them for NatSetPreds.

Example 8. We can prove the inductive validity of the formula $N - M = 0 \iff (M > N = t \lor N = M)$, where $N - M$ denotes $N$ “minus” $M$, by showing that each conjunction in its negation, $(N - M = 0 \land M > N = t \land N = M)$ is unsatisfiable. For the first conjunct, the algorithm’s three steps are as follows. After the unification step, we obtain $(V2 + V3) > V2 = V2 + V3$, where $V2$ and $V3$ are variables of sort Natural. Applying the II-elimination step, we obtain: $V4 \neq V4 + 0$, where $V4$ is a variable of sort Natural. After normalization, the formula becomes $B_{\Omega c}$-inconsistent and therefore unsatisfiable. The other two conjuncts are likewise unsatisfiable.

For a more detailed discussion of the implementation see Section 5 of [14].

6 Related Work and Conclusions

The original paper proposing the concepts of variant and FVP is [8]. FVP ideas have been further advanced in [11,6,3,5]. Variant satisfiability has been studied on [20,19,26]. In relation to that work, the main contribution of this paper is the extension of variant satisfiability to handle user-definable predicates.

As mentioned in the Introduction, satisfiability decision procedures can be either theory-specific or theory-generic. Two recent advanced textbooks on theory-specific decision procedures are [4] and [16]. These two classes of procedures complement each other: theory specific ones are more efficient; but theory-generic ones are user-definable and can substantially increase the range of SMT solvers.

Other theory-generic satisfiability approaches include: (i) the superposition-based one, e.g., [11,18,127], where it is proved that a superposition theorem proving inference system terminates for a given first-order theory together with any given set of ground clauses representing a satisfiability problem; and (ii) that
of decidable theories defined by means of formulas with triggers [10], that allows a user to define a new theory with decidable QF satisfiability by axiomatizing it according to some requirements, and then making an SMT solver extensible by such a user-defined theory. While not directly comparable to the present one, these approaches (discussed in more detail in [20]) can be seen as complementary ones, further enlarging the repertoire of theory-generic satisfiability methods.

In conclusion, the present 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 defined in [20,19] and implemented in [26] with the present one. To simplify both the exposition and the prototype implementation, a few simplifying assumptions, such as the assumption that the signature \( \Omega \) of constructors and that \( \Delta \) of defined functions share no subsort-overloaded symbols, have been made. For both greater efficiency and wider applicability, the combined generic algorithm will drop such assumptions and will use constructor unification [20,26].

References

1. Armando, A., Bonacina, M.P., Ranise, S., Schulz, S.: New results on rewrite-based satisfiability procedures. ACM Trans. Comput. Log. 10(1) (2009)
2. Armando, A., Ranise, S., Rusinowitch, M.: A rewriting approach to satisfiability procedures. Inf. Comput. 183(2), 140–164 (2003)
3. Bouchard, C., Gero, K.A., Lynch, C., Narendran, P.: On forward closure and the finite variant property. In: Proc. FroCoS 2013. LNCS, vol. 8152, pp. 327–342. Springer (2013)
4. Bradley, A.R., Manna, Z.: The calculus of computation - decision procedures with applications to verification. Springer (2007)
5. Cholewa, A., Meseguer, J., Escobar, S.: Variants of variants and the finite variant property. Tech. rep., http://hdl.handle.net/2142/47117
6. Ciobaca., S.: Verification of Composition of Security Protocols with Applications to Electronic Voting. Ph.D. thesis, ENS Cachan (2011)
7. Comon, H.: Complete axiomatizations of some quotient term algebras. Theor. Comput. Sci. 118(2), 167–191 (1993)
8. Comon-Lundhth, H., Delaune, S.: The finite variant property: how to get rid of some algebraic properties, in Proc RTA '05, Springer LNCS 3467, 294–307, 2005
9. Dershowitz, N., Jouanna, J.P.: Rewrite systems. In: van Leeuwen, J. (ed.) Handbook of Theoretical Computer Science, Vol. B, pp. 243–320. North-Holland (1990)
10. Dross, C., Conchon, S., Kanig, J., Paskevich, A.: Adding decision procedures to SMT solvers using axioms with triggers. J. Autom. Reasoning 56(4), 387–457 (2016)
11. Escobar, S., Sasse, R., Meseguer, J.: Folding variant narrowing and optimal variant termination. J. Algebraic and Logic Programming 81, 898–928 (2012)
12. Goguen, J., Meseguer, J.: Models and equality for logical programming. In: Proc. TAPSOFT’87, Springer LNCS, vol. 250, pp. 1–22. Springer (1987)
13. Goguen, J., Meseguer, J.: Order-sorted algebra I: Equational deduction for multiple inheritance, overloading, exceptions and partial operations. Theoretical Computer Science 105, 217–273 (1992)

14. Gutiérrez, R., Meseguer, J.: Variant-based decidable satisfiability in initial algebras with predicates. Tech. Rep. http://hdl.handle.net/2142/96264, University of Illinois at Urbana-Champaign (June 2017)

15. Jouannaud, J.P., Kirchner, H.: Completion of a set of rules modulo a set of equations. SIAM Journal of Computing 15, 1155–1194 (November 1986)

16. Kroening, D., Strichman, O.: Decision Procedures - An Algorithmic Point of View. Texts in Theoretical Computer Science. An EATCS Series, Springer (2008)

17. Lynch, C., Morawska, B.: Automatic decidability. In: Proc. LICS 2002. p. 7. IEEE Computer Society (2002)

18. Lynch, C., Tran, D.: Automatic decidability and combinability revisited. In: Proc. CADE 2007. vol. 4603, pp. 328–344. Springer LNCS (2007)

19. Meseguer, J.: Variant-based satisfiability in initial algebras. In: Artho, C., Ölveczky, P. (eds.) Proc. FTSCS 2015. pp. 1–32. Springer CCIS 596 (2016)

20. Meseguer, J.: Variant-based satisfiability in initial algebras. Sci. Comp. Prog. (2017), to appear; 2015 Tech. Rep. http://hdl.handle.net/2142/88408

21. Meseguer, J.: Strict coherence of conditional rewriting modulo axioms. Theor. Comput. Sci. 672, 1–35 (2017)

22. Meseguer, J., Goguen, J.: Initiality, induction and computability. In: Nivat, M., Reynolds, J. (eds.) Algebraic Methods in Semantics, pp. 459–541. Cambridge University Press (1985)

23. Meseguer, J., Goguen, J.: Order-sorted algebra solves the constructor-selector, multiple representation and coercion problems. Info.&Comp. 103(1), 114–158 (1993)

24. Nelson, G., Oppen, D.C.: Simplification by cooperating decision procedures. ACM Trans. Program. Lang. Syst. 1(2), 245–257 (1979)

25. Shostak, R.E.: Deciding combinations of theories. Journal of the ACM 31(1), 1–12 (Jan 1984)

26. Skeirik, S., Meseguer, J.: Metalevel algorithms for variant-based satisfiability. In: Lucanu, D. (ed.) Proc. WRLA 2016. vol. 9942, pp. 167–184. Springer LNCS (2016)

27. Tushkanova, E., Giorgetti, A., Ringeissen, C., Koucharenko, O.: A rule-based system for automatic decidability and combinability. Sci. Comput. Program. 99, 3–23 (2015)