Resolution-based decision procedures for the positive theory of some finitely generated varieties of algebras

Viorica Sofronie-Stokkermans
Max-Planck-Institut für Informatik, Stuhlsatzenhausweg 85, Saarbrücken, Germany
e-mail: sofronie@mpi-sb.mpg.de

Abstract

In this paper we give resolution-based decision procedures for the positive theory of certain finitely-generated varieties of algebras. The method is based on the existence of natural dualities for such classes of algebras.

1 Introduction

From an algebraic point of view, testing unifiability can be seen as testing the solvability of systems of equations in the initial or free algebra of an equational theory. Apart from its theoretical interest, unification is used e.g. in resolution-based theorem proving and in term rewriting to deal with certain equational axioms, such as associativity and commutativity. In addition, several papers argue for the importance of unification and matching in knowledge representation (we mention, for instance, the results of Baader and Narendran on unification of concept terms in description logics [1]).

The unification problem has thoroughly been studied for equationally defined theories characterized by axioms such as associativity, commutativity, distributivity, associativity-commutativity, associativity-commutativity-idempotency; and for several theories related to algebra (abelian groups, commutative and Boolean rings, semilattices, Boolean algebras, primal algebras, discriminator varieties). For details cf. [3] and the bibliography cited there. Usually, it is quite complicated to use equational reasoning for deciding unification. Also direct checking by using descriptions of the free algebras is often not feasible, even for relatively simple finitely generated varieties, due to the complexity of the free algebras.

Representation and duality theorems in algebra allow, in many situations, to replace the algebraic reasoning with reasoning about structured spaces which are in some sense simpler or more tractable than the original algebras.

In this paper we present several situations in which representation theorems can be used for obtaining efficient decision procedures for the positive theory of certain classes of algebras; the method for deciding unification for bounded distributive lattices proposed in [8] is a particular case. The main advantage of the method is that it allows us to use efficient implementations of the resolution method for deciding the positive theory of these varieties; the structure-preserving translation to first-order logic we give is very natural and does not involve any sophisticated encodings.

The paper is structured as follows. We start with generalities on unification and on natural dualities. We then use these representation theorems for encoding several classes of unfication problems into satisfiability problems, and prove that, for clauses generated by this translation, superposition specializes to an extension of many-valued resolution (cf. [4, 7]). We end by showing how this method specializes to various classes of algebras.

2 Preliminaries

Let Σ be a signature and $a : \Sigma \to \mathbb{N}$ an arity function. A Σ-algebra is a structure $\mathbf{A} = (A, \{\sigma_A\}_{\sigma \in \Sigma})$, where A is a non-empty set and for every $\sigma \in \Sigma$, $\sigma_A : A^{a(\sigma)} \to A$. We denote by $T_\Sigma(X)$ the term algebra over Σ in the variables X. An *equation* is an expression of the form $t_1 = t_2$ where $t_1, t_2 \in T_\Sigma(X)$. A Σ-algebra $\mathbf{A} = (A, \{\sigma_A\}_{\sigma \in \Sigma})$ *satisfies* an equation $t_1 = t_2$ if t_1 and t_2 become equal for every substitution of elements in A for the variables. An equational class is the class of all algebras that satisfy a set of equations. If E is a set of equations in the signature Σ, then we denote by $F_\Sigma^E(X) := T_\Sigma(X)/\equiv_E$ the free algebra over X in the equational class of all algebras that satisfy E (where $\equiv_E$ is the Σ-congruence on $T_\Sigma(X)$ generated by E).

A *system of equations* is a finite set of equations $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$, where $s_i, t_i \in T_\Sigma(X)$ for every $1 \leq i \leq k$. Let $\{y_1, \dots, y_n\} \subseteq X$ be the set of all variables in $\mathcal{S}$. An algebra $\mathbf{A} = (A, \{\sigma_A\}_{\sigma \in \Sigma})$ satisfies the existential closure, $\exists y_1, \dots y_n (s_1 = t_1 \wedge \dots \wedge s_k = t_k)$, of $\mathcal{S}$ if there exists a map $h : X \to A$ such that $\overline{h}(s_i) = \overline{h}(t_i)$ for every $1 \leq i \leq k$, where $\overline{h} : T_\Sigma(X) \to \mathbf{A}$ is the unique homomorphism of Σ-algebras that extends h.

2.1 E-Unification

We present the definitions and results on E-unification needed in the paper.

Definition 1 *Let E be an equational theory, Σ its signature, and Δ a signature containing Σ. Let $\mathcal{S} : \{s_1 = t_1, \ldots, s_k = t_k\}$ be a system of equations, where $s_i, t_i \in T_\Delta(Y)$. Then $\mathcal{S}$ defines an E-*unification problem *over Δ.*

- *$\mathcal{S}$ is* elementary *iff $\Delta \subseteq \Sigma$;*
- *$\mathcal{S}$ is an E-unification problem with* (free) constants *iff $\Delta \backslash \Sigma$ is a set of constant symbols; and*
- *$\mathcal{S}$ is an E-unification problem with* linear constant restrictions *iff it is an E-unification problem with constants and, in addition, a linear ordering $<$ on the variables and free constants occurring in $\mathcal{S}$ is given.*
- *In a* general E-unification problem *$\Delta \backslash \Sigma$ may contain arbitrary function symbols.*

Definition 2 *A unification problem $\mathcal{S}$* has a solution *w.r.t. E if there is a substitution $\sigma : Y \to T_\Delta(Y)$ such that $\sigma(s_i) \equiv_E \sigma(t_i)$ for all $1 \leq i \leq k$.*

If $\mathcal{S}$ is an E-unification problem with linear constant restrictions, a solution for $\mathcal{S}$ is a substitution $\sigma : Y \to T_\Delta(Y)$ with the additional property that for every variable $y \in Y$ and every constant c, if $y < c$ then c does not occur in $\sigma(y)$.

In this paper we focus on testing unifiability. This is sufficient in many applications (e.g. in constraint-based approaches to automated deduction) and is simpler than computing complete sets of unifiers. Testing unifiability w.r.t. an equational theory can be formulated as a satisfiability problem w.r.t. the free algebra freely generated by the constants. Let $\mathcal{V}$ be a (quasi)variety.

Lemma 1 *If $\mathcal{S} = \{s_1 = t_1, \ldots, s_n = t_n\}$ is an $\mathcal{V}$-unification problem with linear constant restrictions* lcr, *then the following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. $\mathcal{V}$.

(2) There exists $h : Y \to F_\mathcal{V}(C)$ with:

(i) $\overline{h}(s_i) = \overline{h}(t_i)$ for all $i \in \{1, \ldots, n\}$ (where $\overline{h} : T_\mathcal{V}(Y \cup C) \to F_\mathcal{V}(C)$ is the unique extension of h to a homomorphism, such that, for all $c \in C$, $\overline{h}(c) = [c]$, the equivalence class of c in $F_\mathcal{V}(C)$), and,

(ii) for every variable $y \in Y$ and every constant c, if $y < c$ is in lcr *then there exists a term $t^y_c \in T_\mathcal{V}(C \backslash \{c\})$ such that $h(y) = [t^y_c]$.*

The importance of E-unification with linear constant restrictions is justified by its link with the positive theory of E. The positive theory of E is the collection of those closed formulae valid in the class of all models of E which are (equivalent to a formula) of the form

$$\phi = Q_1 x_1 \ldots Q_m x_m \bigvee_{i=1}^{q} \bigwedge_{j=1}^{n_i} s_{ij} = t_{ij}, \tag{1}$$

where $Q_1, \ldots, Q_m \in \{\exists, \forall\}$, and $x_1, \ldots, x_m$ are distinct variables. With every problem of the form (1) we can associate a set of E-unification problems with linear constant restrictions, namely the set consisting of q problems, $\mathcal{S}_1, \ldots, \mathcal{S}_q$, where $\mathcal{S}_i = \{s_{i1} = t_{i1}, \ldots, s_{in_i} = t_{in_i}\}$ in which the existentially quantified variables are treated as variables, the universally quantified variables are treated as constants, and the linear order $x_1 < x_2 < \cdots < x_m$ is induced by the quantifier prefix of ϕ.

Proposition 2 ([3, 2]) *Let ϕ be a positive Σ-sentence. Then ϕ is valid in all models of E iff one of the E-unification problems with linear constant restrictions associated with ϕ as explained above has a solution.*

2.2 Natural Dualities

Given a class $\mathcal{V} = ISP(\underline{P})$ of algebras, the main idea of so-called *natural duality theorems* [6], is to seek an "alter ego" for the generating algebra $\underline{P}$, which we require to be a topological structure $\underline{\underline{P}} = (P, \tau, R)$ on the underlying set P of $\underline{P}$, so chosen that there is a dual equivalence between $\mathcal{V}$ and a suitable category Sp of topological relational structures of the same type as $\underline{\underline{P}}$. The goal is to obtain a concrete representation of any $\mathbf{A} \in \mathcal{V}$ as the algebra of continuous R-preserving maps from $D(\mathbf{A}) = \mathsf{Hom}_\mathcal{V}(\mathbf{A}, \underline{P})$[1] into $\underline{\underline{P}}$, this algebra inheriting its operations pointwise from $\underline{P}^{D(\mathbf{A})}$. Then it is said that $\underline{\underline{P}}$ yields a duality for $\mathcal{V}$ and Sp.

It is usually of advantage to take into account separately total functions, partial functions and relations on $\underline{\underline{P}}$. (For the sake of simplicity, we here consider only the relational case (cf. [6] Ch. 2.1).) Numerous varieties for which natural duality theorems exist are presented in [6]. Some examples are discussed in Section 4.1.

3 Unification and natural dualities

If $\mathcal{V} = ISP(\underline{P})$ is a finitely-generated variety then every finitely generated algebra in $\mathcal{V}$ is finite; in particular, $F_\mathcal{V}(C)$ is finite for every finite C. Therefore, $\mathcal{V}$-unification with free constants and with linear constant restrictions are decidable. However, it is usually quite complicated to use the description of the free algebras as such for giving a decision procedure for $\mathcal{V}$-unification. The next lemma shows that, if a natural duality holds for $\mathcal{V}$ (w.r.t. a suitable category of topological relational structures Sp), it provides alternative ways of describing the free algebras in $\mathcal{V}$.

[1] The topology on $D(\mathbf{A})$ is that induced by the product topology on $\underline{\underline{P}}^A$. If the topology on $\underline{\underline{P}}$ is discrete then, for every finite $\mathbf{A} \in \mathcal{V}$, the topology on $D(\mathbf{A})$ is discrete.

Lemma 3 *Assume that $\mathcal{V} = ISP(\underline{P})$ and $\underline{P}$ is a relational structure with the discrete topology which yields a duality for $\mathcal{V}$ and* Sp. *Then, for every finite X the following hold:*

(i) *$D(F_\mathcal{V}(X)) = \mathsf{Hom}_\mathcal{V}(F_\mathcal{V}(X), \underline{P})$ is isomorphic to the space $\{f | f{:}X \to P\}$, with relations inherited (pointwise) from $\underline{P}$, and the product (i.e. discrete) topology.*

(ii) *The map $\eta{:}F_\mathcal{V}(X) \to \mathsf{Hom}_{\mathsf{Sp}}(D(F_\mathcal{V}(X)), \underline{P})$ is an isomorphism, where $\eta(t){:}D(F_\mathcal{V}(X)) \to \underline{P}$ is defined by $\eta(t)(h) = h(t)$ for every $t \in F_\mathcal{V}(X)$, $\overline{h}{:}F_\mathcal{V}(X) \to \underline{P}$.*

The characterization of free algebras in Lemma 3 can be used to reduce the problem of checking whether a unification problem $\mathcal{S}$ has a solution to the problem of checking the satisfiability of a system of finite domain constraints.

Theorem 4 *Assume that $\mathcal{V} = ISP(\underline{P})$ and $\underline{P}$ is a relational structure with the discrete topology which yields a duality for $\mathcal{V}$ and* Sp. *Let $\mathcal{S} : \{s_1 = t_1, \ldots, s_k = t_k\}$ be a unification problem with linear constant restrictions* lcr, *constants C and variables Y. The following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. $\mathcal{V}$;

(2) There exists $h : Y \to F_\mathcal{V}(C)$ such that $\overline{h}(s_i) = \overline{h}(t_i)$ for all $i \in \{1, \ldots, k\}$, where $\overline{h}$ is the unique homomorphism extending h with the property that (i) $\overline{h}(c) = [c]$, and (ii) for every $y \in Y$, if $y < c$ in lcr *then $h(y) = [t]$, where t is a term not containing c;*

(3) There exists $h : Y \to \mathsf{Hom}_{\mathsf{Sp}}(\underline{P}^C, \underline{P})$ such that $\overline{h}(s_i) = \overline{h}(t_i)$ for all $i \in \{1, \ldots, k\}$, where $\overline{h}$ is the unique homomorphism extending h such that:

(i) $\overline{h}(c)(f) := f(c)$ for every $f \in \underline{P}^X$, and

(ii) for every $y \in Y$, if $y < c$ in lcr *then $\overline{h}(y)(f) = \overline{h}(y)(g)$ for all $f, g : C \to P$ which agree everywhere except possibly on c;*

(4) There exists a family $\{I^f_e\}^{f:C\to P}_{e \in ST(\phi)}$ such that:

1. *$I^f_y \in P$ for every $y \in Y$ and $f : C \to P$;*
2. *$R_{\underline{P}}(I^{f_1}_y, \ldots, I^{f_l}_y)$ whenever, for every $c \in C$, $R_{\underline{P}}(f_1(c), \ldots, f_l(c))$; for all relations $R_{\underline{P}}$ on $\underline{P}$;*
3. *$I^f_y = I^g_y$ if $y < c$ in* lcr *and $f_{|C\setminus\{c\}} = g_{|C\setminus\{c\}}$;*
4. *$I^f_c = f(c)$ for every $c \in C$;*
5. *$I^f_{\sigma(e_1,\ldots,e_n)} = \sigma_{\underline{P}}(I^f_{e_1}, \ldots, I^f_{e_n})$;*
6. *$I^f_{s_i} = I^f_{t_i}$ for every $i \in \{1, \ldots, k\}$;*

(5) The conjunction of the following formulae (in language $\mathcal{L}$, consisting of a constant for every element of P (which, for simplicity, we denote the same as the elements in P), a set $\mathcal{H}(\mathcal{S}) = \{H^f_e | e \in ST(\mathcal{S}), f{:}C \to P\}$ and a predicate symbol R for every relation $R_{\underline{P}}$ on $\underline{P}$) is satisfiable:

(Eq)	*congruence axioms for* $\approx$	
(Fin)	$\bigvee_{p \in P} x \approx p$	
(Φ_P)	$p_1 \not\approx p_2$;	$p_1, p_2 \in P, p_1 \neq p_2$;
	$(\neg)R(p_1, \ldots, p_n)$	*whenever it holds in* $\underline{P}$
(Her)	$R(H^{f_1}_y, \ldots, H^{f_l}_y)$	*whenever,* $\forall c \in C$, $R_{\underline{P}}(f_1(c), \ldots, f_l(c))$;
(Lcr)	$\bigwedge_{p \in P}(H^f_y \approx p \leftrightarrow H^g_y \approx p)$	*if $y < c$ in* lcr, *whenever* $f_{\|C\setminus\{c\}} = g_{\|C\setminus\{c\}}$;
(Ren)	$H^f_c \approx f(c)$	$c \in C, f : C \to P$;
	$H^f_{\sigma(e_1 \ldots e_n)} \approx \sigma_{\underline{P}}(H^f_{e_1} \ldots H^f_{e_n})$	$f : C \to P$;
($\mathcal{S}$)	$\bigwedge_{p \in P}(H^f_{s_i} \approx p \leftrightarrow H^f_{t_i} \approx p)$	*for all* $i \in \{1, \ldots, k\}$.

where $ST(\mathcal{S})$ denotes the set of all subterms of terms occurring in $\mathcal{S}$ (including the terms s_i, t_i themselves, all the constants in C and all the variables in Y).

Proof: (*Sketch*) (1) $\Leftrightarrow$ (2) follows from Lemma 1.

(2) $\Leftrightarrow$ (3) follows from the fact that, by Lemma 3, η is an isomorphism between $F_\mathcal{V}(C)$ and $\mathsf{Hom}_{\mathsf{Sp}}(\underline{P}^C, \underline{P})$ and if a term t does not contain c then $\overline{f}(t) = \overline{g}(t)$ for every $f, g : C \to P$ with $f_{|C\setminus\{c\}} = g_{|C\setminus\{c\}}$.

(4) is a reformulation of (3).

(4) $\Rightarrow$ (5) Assume (4) holds. Let $\mathcal{I}$ be the interpretation with domain P such that $\mathcal{I}(\overline{p}) = p$ for every constant $\overline{p}$ associated to the element p in P, and $\mathcal{I}(H^f_e) = I^f_e \in P$ as in (4), and interprete all relation symbols according to (4). Then $\mathcal{I}$ satisfies the conjunction in (5). Since the domain P is finite, we can replace every atom of the form $L_1 \approx L_2$, where none of L_1, L_2 is an element of P, with the conjunction: $\bigwedge_{p \in P}(L_1 \approx p \leftrightarrow L_2 \approx p)$. This transformation can be applied, for instance, to (Lcr) and to ($\mathcal{S}$), and increases, in each case, the number of clauses with a factor of $|P|$.

(5) $\Rightarrow$ (4) Conversely, any model $\mathcal{I}$ of the conjunction in (5) defines an assignment with $\mathcal{I}(H^f_e) = I^f_e \in P$ such that all conditions in (4) are satisfied. $\square$

The equivalence of (1) and (5) in Theorem 4 can be used to give a structure-preserving translation to clause form.

Note. We can simplify the second formula in Theorem 4(5) Ren by using the truth table of $\underline{P}$. As in the structure-preserving translation to clause form for many-valued logics in ([4], Section 4), we can replace this formula with:

$$\bigwedge_{\substack{p_1 \ldots p_n, p \\ \sigma(p_1, \ldots, p_n) = p}} H^f_{e_1} \not\approx p_1 \vee \cdots \vee H^f_{e_n} \not\approx p_n \vee H^f_{\sigma(e_1 .. e_n)} \approx p$$

Fin allows to replace every negative atom $L \not\approx p$ by the disjunction $\bigvee_{q \neq p} L \approx q$. We thus obtain a transformation to a clause form, $\Phi(\mathcal{S}, P)$, containing unit clauses of the form $p_1 \not\approx p_2$, and $\neg R(p_1, \ldots, p_n)$, and, in addition, only positive clauses in which all literals are of the form $L \approx p$, and $R(L_1, \ldots, L_n)$. $\Phi(\mathcal{S}, P)$ contains a number of clauses of order $(|Y| \cdot |P|^{|C|})^{\max \mathsf{arity}(\Sigma)} \cdot |\Sigma| + |Y| \cdot |P|^{|C|+1} +$

$|C| \cdot |P|^{|C|} + |ST(\mathcal{S})| \cdot |P|^{\max \mathsf{arity}(\Sigma)-1+|C|}$; if $C = \emptyset$, the number of clauses is of order $|Y|^{\max \mathsf{arity}(\Sigma)} \cdot |\Sigma| + |ST(\mathcal{S})| \cdot |P|^{\max \mathsf{arity}(\Sigma)-1}$.

4 A resolution calculus

Let $\Phi(\mathcal{S}, P)$ be the set of clauses associated with $Eq \cup \mathsf{Fin} \cup \Phi_\mathsf{P} \cup \mathsf{Her} \cup \mathsf{Ren} \cup \mathcal{S}$ as explained above. The form of the clauses in $\Phi(\mathcal{S}, P)$ is very similar to the form of MV-clauses studied in the context of many-valued logics in [4, 7]. We extend the definition in [4, 7] as follows.

Definition 3 *An MV-*literal *is an equation of the form $L \approx p$, where $L \in \mathcal{H}(\mathcal{S})$, and $p \in P$. An R-*literal *is a literal of the form $(\neg)R(L_1, \dots, L_n)$, where, for every i, $L_i \in \mathcal{H}(\mathcal{S}) \cup P$, and R is a relation on $\underline{\underline{P}}$. An MVR-*clause *is a clause consisting only of MV-literals and positive R-literals.*

The satisfiability of $\Phi(\mathcal{S}, P)$ can be checked by using superposition [5]. For the remainder of this section we will use the same terminology on the superposition calculus as used in [5] and [7]. We will assume that $\succ$ is an admissible clause ordering such that $H^f_e \succ p$ for every H^f_e and every constant $p \in P$; and that $R(\dots, H^f_e, \dots) \succ H^g_{e'} \approx p$; and $H^g_{e'} \approx p \succ R(p_1, \dots, p_n)$. When applied to MVR-clauses, the superposition calculus specializes to the following calculus, $SMVR$:

Positive MV-superposition. From $H \approx p \vee C$ and $H \approx q \vee D$ derive $C \vee D$ provided that $p \neq q$ and (i) $H \approx p \succ C$; (ii) $H \approx q \succ D$; (iii) $H \approx q \succ H \approx p$.

Positive MVR-superposition. From $H \approx p \vee C$ and $L[H] \vee D$ derive $L[p] \vee C \vee D$ provided that (i) $H \approx p \succ C$; (ii) $L[H] = R(\dots, H, \dots) \succ D$.

Ordered factoring. From $A \vee A \vee C$ derive $A \vee C$ provided that A is an atom and $A \succ C$.

Φ_P-resolution. From $R(p_1, \dots, p_n) \vee D$ derive D provided that $p_1, \dots, p_n \in P$, $\neg R_{\underline{P}}(p_1, \dots, p_n)$, and $R(p_1, \dots, p_n) \succ D$.

Let T be a set of clauses intended to be built into an inference system. A T-interpretation is a (Herbrand) interpretation which is a model of T. In the following definition the term *main premise* refers to the rightmost premise of an inference, while the other premises are called *side-premises*.

Definition 4 *A clause D is called* T-redundant *w.r.t. a set N of clauses if there exist clauses $D_1, \dots, D_k$ in N such that $D \succ D_i$, $1 \leq i \leq k$, and for every T-interpretation I, if $D_1, \dots, D_k$ are true in I then D is true in I.*

An inference with main premise C, side premises $C_1, \dots, C_n$, and conclusion D is called T-redundant *w.r.t. a set N of clauses if either some premise is redundant, or else there exist clauses $D_1, \dots, D_k \in N$ such that $C \succ D_i$, $1 \leq i \leq k$, and for every T-interpretation I such that $D_1, \dots, D_k, C_1, \dots, C_n$ are true in I, D is also true in I.*

A set N of clauses is called *saturated up to* T*-redundancy* w.r.t. an inference system if all inferences from non-redundant premises are redundant in N.

Lemma 5 *Let N be a set of MVR-clauses. If $N \cup \mathsf{Fin}$ is saturated up to $Eq \cup \Phi_P$-redundancy w.r.t. $SMVR$ then $N \cup \mathsf{Fin} \cup \Phi_P$ is saturated up to Eq-redundancy w.r.t. superposition.*

Proof: (*Sketch*) We first note that if a non-empty MVR-clause C is Eq-irredundant in $N \cup \mathsf{Fin} \cup \Phi_P$ then C is $Eq \cup \Phi_P$-irredundant in $N \cup \mathsf{Fin}$. For this, note that all clauses in Φ_P are smaller in $\succ$ than any clause C containing at least one symbol in $\mathcal{H}(\mathcal{S})$.

Assume that $N \cup \mathsf{Fin}$ is saturated up to $Eq \cup \Phi_P$-redundancy with respect to $SMVR$. The following facts were already proven in [7], Lemma 2: In any superposition inference in which the main premise is an equality clause in Φ_P the side premise must be a tautology in Fin, which is redundant; Due to restrictions in the superposition calculus (cf. [5] and [7] for the terminology and, resp., proofs) superposition inferences into an MV-literal in the main premise and a Fin clause as the side premise are not possible. Superposition inferences with a Fin clause as the main premise are redundant. Inferences by negative superposition and reflexivity resolution are not possible for MVR-clauses; equality factoring is redundant since the conclusion has a negative literal of the form $u \not\approx v$, with $u \neq v$, implied by Φ_P. Any positive superposition inference between two non-redundant (in N) MVR-clauses, where the literals resolved upon are MV-literals, is redundant.

The only remaining inferences to be considered are those in which at least one of the literals resolved upon is an R-literal. Note that all clauses in N contain only positive occurrences of R-literals. We first consider ordered resolution inferences in which the literal resolved upon is an R-literal. These inferences can only be of the form

$$\frac{R(p_1, \dots, p_n) \vee D \quad \neg R(p_1, \dots, p_n)}{D}$$

where $\neg R(p_1, \dots, p_n) \in \Phi_P$. As $N \cup \mathsf{Fin}$ is saturated up to $Eq \cup \Phi_P$-redundancy with respect to $SMVR$ (in particular since every Φ_P-resolution inference from non-redundant axioms is redundant in $N \cup \mathsf{Fin}$), it follows that these inferences are redundant. Redundancy of positive superposition inferences into R-literals follows similarly from the fact that every positive MVR-superposition inference from non-redundant axioms is redundant in $N \cup \mathsf{Fin}$. $\square$

The refutational completeness of $SMVR$ follows directly:

Theorem 6 *Let N be a class of MVR-clauses such that $N \cup \mathsf{Fin}$ is saturated up to $Eq \cup \Phi_P$-redundancy w.r.t. $SMVR$. Then either N contains the empty clause or else $N \cup \mathsf{Fin} \cup \Phi_P$ is saturated up to Eq-redundancy w.r.t. superposition.*

All superposition inferences with Fin where the literal resolved upon is an MV-literal are redundant. Positive superposition inferences from Fin as side premise, into an R-literal may be necessary.

4.1 Examples

We present several examples: unification for bounded distributive lattices and Boolean algebras; for varieties generated by primal algebras; and for Kleene algebras.

4.1.1 Bounded distributive lattices

The Priestley representation theorem for bounded distributive lattices is a natural duality for the class $\mathsf{D}_{01} = ISP(L_2)$, obtained by choosing as an alter ego for the two element bounded distributive lattice L_2 the two element partially-ordered set $(\{0,1\}, \leq)$ with $0 \leq 1$ and the discrete topology. Theorem 4 specializes as follows:

Theorem 7 *Let $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$ be a D_{01}-unification problem with linear constant restrictions* lcr*, constants C and variables Y. The following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. D_{01};

(2) The following conjunction is satisfiable:

$$
\begin{array}{llcll}
(\mathsf{Her}) & H^f_y & \leq & H^g_y & \textit{if } f(c) \leq g(c) \forall c \in C \\
(\mathsf{Ren}) & H^f_{e_1 \wedge e_2} & = & H^f_{e_1} \wedge P^f_{e_2} & \\
 & H^f_{e_1 \vee e_2} & = & H^f_{e_1} \vee P^f_{e_2} & \\
 & H^f_1 = 1 & & H^f_0 = 0 & \\
 & H^f_c & = & f(c) & \\
(\mathsf{Lcr}) & H^f_y & = & H^g_y & \textit{if } y < c \textit{ in } \mathsf{lcr}, \textit{ whenever} \\
 & & & & f_{|C\backslash\{c\}} = g_{|C\backslash\{c\}} \\
(\mathcal{S}) & H^f_{s_i} & = & H^f_{t_i}, & \forall 1 \leq i \leq k.
\end{array}
$$

where $f, g : C \to \{0,1\}$ and the lower indices are terms in $ST(\mathcal{S})$.

We can encode $1, 0 \in L_2$ by true, resp. false; the lattice operations $\vee$ and $\wedge$, and the order $\leq$ can be encoded by logical disjunction, resp. conjunction, and logical implication. The maps $f : C \to \{0,1\}$ can alternatively be represented by the sets $X_f := f^{-1}(1)$ (note that $f \leq g$ iff $X_f := f^{-1}(1) \subseteq g^{-1}(1) = X_g$), and, therefore, every H^f_e can encoded as a (two-valued) propositional variable $P_e(X_f)$. With this encoding, the following result established in [8] follows immediately:

Corollary 8 ([8]) *Let $\mathcal{S} : \{s_1{=}t_1, \dots, s_k{=}t_k\}$ be a D_{01}-unification problem with linear constant restrictions* lcr*, constants C and variables Y. The following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. D_{01};

(2) The following conjunction is satisfiable:

$$
\begin{array}{llcll}
(\mathsf{Her}) & P_y(X_1) & \rightarrow & P_y(X_2) & \textit{if } X_1 \subseteq X_2 \\
(\mathsf{Ren}) & P_{e_1 \wedge e_2}(X) & \leftrightarrow & P_{e_1}(X) \wedge P_{e_2}(X) & \\
 & P_{e_1 \vee e_2}(X) & \leftrightarrow & P_{e_1}(X) \vee P_{e_2}(X) & \\
 & P_1(X) & & \neg P_0(X) & \\
 & P_c(X) & & & \textit{if } c \in X \\
 & \neg P_c(X) & & & \textit{if } c \notin X \\
(\mathsf{Lcr}) & P_y(X) & \rightarrow & P_y(X \backslash \{c\}) & \textit{if } y < c \textit{ in } \mathsf{lcr} \\
(\mathcal{S}) & P_{s_i}(X) & \leftrightarrow & P_{t_i}(X), & \forall 1 \leq i \leq k.
\end{array}
$$

where $X, X_1, X_2 \subseteq C$ and the lower indices are terms in $ST(\mathcal{S})$.

The satisfiability of the set of clauses above can be checked either by resolution or by using a SAT checker.

4.1.2 Boolean algebras

Stone's representation theorem for Boolean algebras is obtained for the class $\mathsf{B} = ISP(B_2)$ of Boolean algebras, by choosing as an alter ego for the two element Boolean algebra B_2 the two element set with the discrete topology. Theorem 4, followed by an encoding into classical logic as that preceding Corollary 8, leads to:

Theorem 9 *Let $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$ be a* B*-unification problem with linear constant restrictions* lcr*, constants C and variables Y. The following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. B*.*

(2) The following conjunction is satisfiable:

$$
\begin{array}{llcll}
(\mathsf{Ren}) & P_{e_1 \wedge e_2}(X) & \leftrightarrow & P_{e_1}(X) \wedge P_{e_2}(X) & \\
 & P_{e_1 \vee e_2}(X) & \leftrightarrow & P_{e_1}(X) \vee P_{e_2}(X) & \\
 & P_1(X) & & \neg P_0(X) & \\
 & P_c(X) & & & \textit{if } c \in X \\
 & \neg P_c(X) & & & \textit{if } c \notin X \\
(\mathsf{Lcr}) & P_y(X) & \leftrightarrow & P_y(X \backslash \{c\}) & \textit{if } y < c \textit{ in } \mathsf{lcr} \\
(\mathcal{S}) & P_{s_i}(X) & \leftrightarrow & P_{t_i}(X), & \forall 1 \leq i \leq k.
\end{array}
$$

where $X \subseteq C$ and the terms occurring as indices are in $ST(\mathcal{S})$.

A consequence of Theorem 9 is the well-known fact that $\mathsf{B} \models \forall \overline{c} \exists \overline{y} (\bigwedge_{i=1}^k s_i{=}t_i)$ iff $\mathsf{B}_2 \models \forall \overline{c} \exists \overline{y} (\bigwedge_{i=1}^k s_i{=}t_i)$ (Lcr is empty, so we have 2^C independent satisfiability problems, one for each $X \subseteq C$). A generalization is presented below.

4.1.3 Varieties generated by primal algebras

Also in the case of primal algebras the "alter ego" topological spaces have the discrete topology and do not contain any relations. Theorem 4 specializes in this case as follows:

Theorem 10 *Let $\mathcal{V} = ISP(\mathsf{P})$, where* P *is a primal algebra. Let $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$ be a $\mathcal{V}$-unification problem with linear constant restrictions* lcr*, constants C and variables Y. The following are equivalent:*

(1) $\mathcal{S}$ has a solution w.r.t. $\mathcal{V}$;

(2) The following conjunction is satisfiable:

$$
\begin{array}{lll}
(\mathsf{Eq}) & \textit{congruence axioms for } \approx & \\
(\mathsf{Fin}) & \bigvee_{p \in P} H^f_y \approx p & y \in Y, f : C \to P; \\
(\Phi_{\mathsf{P}}) & p_1 \not\approx p_2 & p_1, p_2 \in P, p_1 \neq p_2; \\
(\mathsf{Lcr}) & \bigwedge_{p \in P} (H^f_y \approx p \leftrightarrow H^g_y \approx p) & \textit{if } y < c \textit{ in } \mathsf{lcr}, \textit{ whenever} \\
 & & f_{|C\backslash\{c\}} = g_{|C\backslash\{c\}}; \\
(\mathsf{Ren}) & H^f_c \approx f(c) & c \in C, f : C \to P; \\
 & H^f_{\sigma(e_1 \dots e_n)} \approx \sigma_{\underline{P}}(H^f_{e_1} \dots H^f_{e_n}) & f : C \to P; \\
(\mathcal{S}) & \bigwedge_{p \in P} (H^f_{s_i} \approx p \leftrightarrow H^f_{t_i} \approx p) & \forall i = 1, \dots, k.
\end{array}
$$

where $f, g : C \to \{0,1\}$ and the lower indices are terms in $ST(\mathcal{S})$.

Corollary 11 *The following are equivalent:*

(1) $\mathcal{V} \models \forall \overline{c} \exists \overline{y} (\bigwedge_{i=1}^k s_i = t_i)$;

(2) $\mathsf{P} \models \forall \overline{c} \exists \overline{y} (\bigwedge_{i=1}^k s_i = t_i)$.

Proof: (*Sketch*) (1) $\Rightarrow$ (2) is obvious. (2) $\Rightarrow$ (1): Let C (resp. Y) be the set of all variables in $\overline{c}$ (resp. $\overline{y}$). In the absence of Lcr, (1) is equivalent to the statement: "for all $f : C \to \mathsf{P}$ exists $g : Y \to \mathsf{P}$ such that if $h : C \cup Y \to P$ extends both f and g, then $\overline{h}(s_j) = \overline{h}(t_j)$ for every $j \in \{1, \dots, k\}$", which is equivalent to (2). $\square$

4.1.4 The variety of Kleene algebras

A Kleene algebra $(K, \vee, \wedge, 0, 1, \neg)$ is a bounded distributive lattice with a unary operator $\neg$ satisfying the axioms: $\neg\neg x = x$, $\neg 0 = 1$, $\neg(x \wedge y) = \neg x \vee \neg y$, $x \wedge \neg x \leq y \vee \neg y$.

The class of Kleene algebras is a variety $\mathsf{K} = ISP(K_3)$, generated by the algebra $K_3 = (\{0, 1, a\}, \vee, \wedge, 0, 1, \neg)$, where $0 \leq a \leq 1$, $\neg 0 = 1$, $\neg 1 = 0$, and $\neg a = a$.

It is known (cf. e.g. [6], Sect. 4.3) that a strong duality on K is yielded by the space $\underline{K_3} = (\{0, a, 1\}, \preceq, \sim, K_0)$ with the discrete topology where K_0 is the unary relation containing 0 and 1, $\sim$ is the binary reflexive, symmetric relation on $\{0, a, 1\}$ relating all pairs except for 0 and 1, and $\preceq = \{(0,0), (0,a), (1,1), (1,a), (a,a)\}$. Theorem 4 specializes in this case as follows:

Theorem 12 *Let* $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$ *be a* K*-unification problem with linear constant restrictions* lcr*, constants* C *and variables* Y*. The following are equivalent:*

(1) $\mathcal{S}$ *has a solution w.r.t.* K.

(2) The following conjunction is satisfiable:

(Eq) *congruence axioms for* $\approx$

(Fin) $H^f_y \approx 0 \vee H^f_y \approx a \vee H^f_y \approx 1 \quad y \in Y, f : C \to K_3$;

(Φ_{P}) $0 \not\approx a \wedge 1 \not\approx a \wedge 0 \not\approx 1$; *tables for* $\preceq, \sim, K_0$ *on* $\underline{K_3}$

(Her) $K_0(H^f_y)$ *if* $\forall c \in C, K_0(f(c))$
$H^f_y \preceq H^g_y$ *if* $\forall c \in C, f(c) \preceq g(c)$;
$H^f_y \sim H^g_y$ *if* $\forall c \in C, f(c) \sim g(c)$;

(Lcr) $H^f_y \approx p \leftrightarrow H^g_y \approx p$, $p \in \{0, a, 1\}$ *if* $y < c$ *in* lcr, *whenever* $f_{|C\backslash\{c\}} = g_{|C\backslash\{c\}}$;

(Ren) $H^f_c \approx f(c)$; $c \in C$,
$H^f_{e_1 \vee e_2} \approx H^f_{e_1} \vee H^f_{e_2}$ $\quad H^f_{\neg e} \approx \neg H^f_e$
$H^f_{e_1 \wedge e_2} \approx H^f_{e_1} \wedge H^f_{e_2}$ $\quad H^f_0 \approx 0$; $H^f_1 \approx 1$

($\mathcal{S}$) $H^f_{s_i} \approx p \leftrightarrow H^f_{t_i} \approx p$, $p \in \{0, a, 1\}$ $\quad \forall i = 1, \dots, k$.

where $f, g : C \to \{0, 1\}$ *and the lower indices are terms in* $ST(\mathcal{S})$.

We illustrate the translation to clause normal form for $(\mathsf{Ren})(\vee)$: Note that $H^f_{e_1 \vee e_2} \not\approx H^f_{e_1} \vee H^f_{e_2}$ iff there exist p_1, p_2 with $H^f_{e_1} \approx p_1 \wedge H^f_{e_2} \approx p_2 \wedge H^f_{e_1 \vee e_2} \not\approx p_1 \vee p_2$. Hence, $H^f_{e_1 \vee e_2} \approx H^f_{e_1} \vee H^f_{e_2}$ iff $\bigwedge_{p_1, p_2} (H^f_{e_1} \not\approx p_1 \vee H^f_{e_2} \not\approx p_2 \vee H^f_{e_1 \vee e_2} \approx p_1 \vee p_2$. Therefore $(\mathsf{Ren})(\vee)$ can be equivalently expressed by:

$$\bigwedge_{p_1, p_2} \bigvee_{q_1 \neq p_2} H^f_{e_1} \approx q_1 \vee \bigvee_{q_2 \neq p_2} H^f_{e_2} \approx q_2 \vee H^f_{e_1 \vee e_2} \approx p_1 \vee p_2.$$

The clause form of the conjunction in (2) can be obtained by similarly handling the renaming rules for $\vee$ and $\neg$ and replacing all literals $H^f_e \not\approx p$ with $\bigvee_{q \neq p} H^f_e \approx q$; satisfiability can be checked using the (many-valued) resolution calculus in Section 4.

5 Conclusions

We presented a resolution-based decision procedure which can be used for deciding unification with linear constant restriction for a large class of finitely-generated varieties of algebras. Since the decidability of $\mathcal{V}$-unification with linear constant restrictions implies the decidability of the positive theory of $\mathcal{V}$, the method presented above yields a decision algorithm for the positive theory of $\mathcal{V}$. The method is based on the existence of natural duality theorems for such classes of algebras, and is a natural generalization of our previous results in which uniform word problems in distributive lattices with operators [9] or unification for distributive lattices [8] were considered. In [8] it was often of advantage to represent sets of similar clauses using *constrained clauses*. This concept can be easily generalized to the present context, but lack of space prevented us from presenting the details here.

References

[1] F. Baader and P. Narendran. Unification of concept terms in description logics. In H. Prade, editor, *Proceedings of ECAI'98*, pages 331–335. Wiley, 1998.

[2] F. Baader and K.U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. *J. Symbolic Computation*, 21:211–243, 1996.

[3] F. Baader and W. Snyder. Unification theory. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 8, pages 445–532. Elsevier, 2001.

[4] M. Baaz and C.G. Fermüller. Resolution-based theorem proving for many-valued logics. *J. Symbolic Computation*, 19:353–391, 1995.

[5] L. Bachmair and H. Ganzinger. Rewrite-based equational theorem proving with selection and simplification. *J. of Logic and Computation*, 4(3):217–247, 1994.

[6] D.M. Clark and B.A. Davey. *Natural dualities for the working algebraist*. Cambridge studies in adv. math. Vol.57. Cambridge Univ. Press, 1998.

[7] H. Ganzinger and V. Sofronie-Stokkermans. Chaining techniques for automated theorem proving in many-valued logics. In *Proc. 30th ISMVL*, pages 337–344. IEEE Comp. Soc. Press, 2000.

[8] V. Sofronie-Stokkermans. On unification for bounded distributive lattices. In D. McAllester, editor, *Proc. CADE-17, LNAI 1831*, pages 465–481. Springer, 2000.

[9] V. Sofronie-Stokkermans. Resolution-based decision procedures for the universal theory of some classes of distributive lattices with operators. *J. Symbolic Computation*, 36(6):891–924, 2003.