

# On unification in certain finitely generated varieties of algebras

Viorica Sofronie-Stokkermans

Max-Planck-Institut für Informatik, Stuhlsatzenhausweg 85, Saarbrücken, Germany

**Abstract.** We present 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

Unification is important in computer science; it is used e.g. in resolution-based theorem proving and in term rewriting to deal with certain equational axioms, such as associativity and commutativity; or in knowledge representation (cf. 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. It can be 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.

We show that representation theorems and a specially tuned resolution calculus can be used for obtaining efficient decision procedures for the positive theory of certain classes of algebras. The results presented here appear in [9].

## 2 Preliminaries

**Unification.** Let  $E$  be an equational theory,  $\Sigma$  its signature, and  $\Delta$  a signature containing  $\Sigma$ . Let  $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$  be a system of equations, where  $s_i, t_i \in T_\Delta(Y)$ . Then  $\mathcal{S}$  defines an *E-unification problem* over  $\Delta$ . In a *general E-unification problem*  $\Delta \setminus \Sigma$  may contain arbitrary function symbols.  $\mathcal{S}$  is an *E-unification problem with (free) constants* iff  $\Delta \setminus \Sigma$  is a set of constant symbols; and  $\mathcal{S}$  is an *E-unification problem with linear constant restrictions* (l.c.r.) 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.

A unification problem  $\mathcal{S}$  has a *solution* w.r.t.  $E$  if there is a substitution  $\sigma : Y \rightarrow T_\Delta(Y)$  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  $\sigma : Y \rightarrow T_{\Delta}(Y)$  with the additional property that for every variable  $y \in Y$  and every constant  $c$ , if  $y < c$  then  $c$  does not occur in  $\sigma(y)$ .

Testing unifiability w.r.t. an equational theory  $\mathcal{V}$  can be formulated as a satisfiability problem w.r.t. the free algebra freely generated by the constants.

**Lemma 1.** *If  $\mathcal{S} = \{s_1 = t_1, \dots, s_n = t_n\}$  is an  $\mathcal{V}$ -unification problem with linear constant restrictions lcr, then  $\mathcal{S}$  has a solution w.r.t.  $\mathcal{V}$  if and only if there exists  $h : Y \rightarrow F_{\mathcal{V}}(C)$  with:*

- (i)  $\bar{h}(s_i) = \bar{h}(t_i)$  for all  $i \in \{1, \dots, n\}$  (where  $\bar{h} : T_{\mathcal{V}}(Y \cup C) \rightarrow F_{\mathcal{V}}(C)$  is the unique extension of  $h$  to a homomorphism, such that, for all  $c \in C$ ,  $\bar{h}(c) = [c]$ , 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  $t_c^y \in T_{\mathcal{V}}(C \setminus \{c\})$  such that  $h(y) = [t_c^y]$ .

The importance of  $E$ -unification with linear constant restrictions is justified by its link with the positive theory of  $E$ : Any decision procedure for  $E$ -unification with l.c.r. yields a decision procedure for the positive theory of  $E$  [3,2].

**Natural Dualities.** Assume  $\mathcal{V} = ISP(\underline{P})$ . The idea of *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  $\mathbf{Sp}$  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  $D(\mathbf{A}) = \text{Hom}_{\mathcal{V}}(\mathbf{A}, \underline{P})^1$  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  $\mathbf{Sp}$ . Numerous varieties for which natural duality theorems exist are presented in [6].

### 3 Unification, natural dualities, resolution

If  $\mathcal{V} = ISP(\underline{P})$  is a finitely-generated variety then  $F_{\mathcal{V}}(C)$  is finite for every finite  $C$ , so  $\mathcal{V}$ -unification with free constants and with linear constant restrictions are decidable. However, it can be complicated to use the description of the free algebras for giving a decision procedure for  $\mathcal{V}$ -unification. Lemma 2 shows that, if a natural duality holds for  $\mathcal{V}$  (w.r.t. a suitable category of topological relational structures  $\mathbf{Sp}$ ), it provides alternative ways of describing the free algebras in  $\mathcal{V}$ .

**Lemma 2.** *Let  $\mathcal{V} = ISP(\underline{P})$  such that  $\underline{\underline{P}}$  is a relational structure with the discrete topology yielding a duality for  $\mathcal{V}$ . For every finite  $X$  the following hold:*

- (1)  $D(F_{\mathcal{V}}(X)) = \text{Hom}_{\mathcal{V}}(F_{\mathcal{V}}(X), \underline{P})$  is isomorphic to the space  $\{f | f : X \rightarrow P\}$ , with relations inherited (pointwise) from  $\underline{\underline{P}}$ , and the product topology.
- (2)  $\eta : F_{\mathcal{V}}(X) \rightarrow \text{Hom}_{\mathbf{Sp}}(D(F_{\mathcal{V}}(X)), \underline{\underline{P}})$  is an isomorphism, where  $\eta(t) : D(F_{\mathcal{V}}(X)) \rightarrow \underline{\underline{P}}$  is defined by  $\eta(t)(h) = h(t)$  for every  $t \in F_{\mathcal{V}}(X), h : F_{\mathcal{V}}(X) \rightarrow \underline{P}$ .

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

Lemma 2 can be used to reduce any  $\mathcal{V}$ -unification problem  $\mathcal{S}$  to the problem of checking the satisfiability of a system of finite domain constraints.

**Theorem 1.** *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  $\mathbf{Sp}$ . Let  $\mathcal{S} : \{s_1 = t_1, \dots, s_k = t_k\}$  be a unification problem with linear constant restrictions  $\text{lcr}$ , constants  $C$  and variables  $Y$ . The following are equivalent:*

- (1)  $\mathcal{S}$  has a solution w.r.t.  $\mathcal{V}$ , i.e. there exists  $h : Y \rightarrow F_{\mathcal{V}}(C)$  such that  $\bar{h}(s_i) = \bar{h}(t_i)$  for all  $i \in \{1, \dots, k\}$ , where  $\bar{h}$  is the unique homomorphism extending  $h$  with the property that (i)  $\bar{h}(c) = [c]$ , and (ii) for every  $y \in Y$ , if  $y < c$  in  $\text{lcr}$  then  $h(y) = [t]$ , where  $t$  is a term not containing  $c$ ;
- (2) There exists  $h : Y \rightarrow \text{Hom}_{\mathbf{Sp}}(\underline{P}^C, \underline{P})$  such that  $\bar{h}(s_i) = \bar{h}(t_i)$  for all  $i \in \{1, \dots, k\}$ , where  $\bar{h}$  is the unique homomorphism extending  $h$  such that:
  - (i)  $\bar{h}(c)(f) := f(c)$  for every  $f \in \underline{P}^X$ , and
  - (ii) for every  $y \in Y$ , if  $y < c$  in  $\text{lcr}$  then  $\bar{h}(y)(f) = \bar{h}(y)(g)$  for all  $f, g : C \rightarrow P$  which agree everywhere except possibly on  $c$ ;
- (3) There exists a family  $\{I_e^f\}_{e \in ST(\phi)}^{f: C \rightarrow P}$  such that:
  1.  $I_y^f \in P$  for every  $y \in Y$  and  $f : C \rightarrow P$ ;
  2.  $R_{\underline{P}}(I_y^{f_1}, \dots, I_y^{f_l})$  whenever, for every  $c \in C$ ,  $R_{\underline{P}}(f_1(c), \dots, f_l(c))$ , for all relations  $R_{\underline{P}}$  on  $\underline{P}$ ;
  3.  $I_y^f = I_y^g$  if  $y < c$  in  $\text{lcr}$  and  $f|_{C \setminus \{c\}} = g|_{C \setminus \{c\}}$ ;
  4.  $I_c^f = f(c)$  for every  $c \in C$ ;
  5.  $I_{\sigma(e_1, \dots, e_n)}^f = \sigma_{\underline{P}}(I_{e_1}^f, \dots, I_{e_n}^f)$ ;
  6.  $I_{s_i}^f = I_{t_i}^f$  for every  $i \in \{1, \dots, k\}$ ;
- (4) The conjunction of the congruence axioms (Eq) for  $\approx$ , the axiom (Fin):  $\bigvee_{p \in P} x \approx p$ , and 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  $\mathcal{H}(\mathcal{S}) = \{H_e^f | e \in ST(\mathcal{S}), f : C \rightarrow P\}$  and a predicate symbol  $R$  for every relation  $R_{\underline{P}}$  on  $\underline{P}$ ) is satisfiable:
 

(Φ <sub>P</sub> )	$p_1 \not\approx p_2$	$p_1, p_2 \in P, p_1 \neq p_2$ ;
	$(\neg)R(p_1, \dots, p_n)$	whenever this holds in $\underline{P}$ ;
(Her)	$R(H_y^{f_1}, \dots, H_y^{f_l})$	whenever, $\forall c \in C, R_{\underline{P}}(f_1(c), \dots, f_l(c))$ ;
(Lcr)	$\bigwedge_{p \in P} (H_y^f \approx p \leftrightarrow H_y^g \approx p)$	if $y < c$ in $\text{lcr}$ , whenever $f _{C \setminus \{c\}} = g _{C \setminus \{c\}}$ ;
(Ren)	$H_c^f \approx f(c)$	$c \in C, f : C \rightarrow P$ ;
	$H_{\sigma(e_1 \dots e_n)}^f \approx \sigma_{\underline{P}}(H_{e_1}^f \dots H_{e_n}^f)$	$f : C \rightarrow P$ ;
(S)	$\bigwedge_{p \in P} (H_{s_i}^f \approx p \leftrightarrow H_{t_i}^f \approx p)$	for all $i \in \{1, \dots, k\}$ ;

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  $Y$ ).

Let  $\Phi(\mathcal{S}, P)$  be the set of clauses associated with  $Eq \cup \text{Fin} \cup \Phi_P \cup \text{Her} \cup \text{Ren} \cup \text{S}$  as explained above. A similar class of clauses ( $MV$ -clauses) were studied in the context of many-valued logics in [4,7]. We extend the definition in [4,7] as follows.

**Definition 1.** 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  $\underline{P}$ . 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 assume that  $\succ$  is an admissible clause ordering such that  $H_e^f \succ p$  for every  $H_e^f$  and every constant  $p \in P$ ; and that  $R(\dots, H_e^f, \dots) \succ H_e^g \approx p$ ; and  $H_e^g \approx p \succ R(p_1, \dots, p_n)$ . 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  $A \succ C$ .

**$\Phi_P$ -resolution.** From  $R(p_1, \dots, p_n) \vee D$  derive  $D$  provided that  $p_1, \dots, p_n \in P$ ,  $\neg R_P(p_1, \dots, p_n)$ , and  $R(p_1, \dots, p_n) \succ D$ .

Let  $\mathsf{T}$  be a set of clauses intended to be built into an inference system. A  $\mathsf{T}$ -interpretation is a (Herbrand) interpretation which is a model of  $\mathsf{T}$ . 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 2.** A clause  $D$  is  $\mathsf{T}$ -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  $\mathsf{T}$ -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  $\mathsf{T}$ -redundant w.r.t. a set  $N$  of clauses if either some premise is redundant, or there exist clauses  $D_1, \dots, D_k \in N$  such that  $C \succ D_i$ ,  $1 \leq i \leq k$ , and for every  $\mathsf{T}$ -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 saturated up to  $\mathsf{T}$ -redundancy w.r.t. an inference system if all inferences from non-redundant premises are redundant in  $N$ .

**Lemma 3.** Let  $N$  be a set of MVR-clauses. If  $N \cup \text{Fin}$  is saturated up to  $\text{Eq} \cup \Phi_P$ -redundancy w.r.t. SMVR then  $N \cup \text{Fin} \cup \Phi_P$  is saturated up to  $\text{Eq}$ -redundancy w.r.t. superposition.

### 3.1 Examples

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

**Bounded distributive lattices.** The Priestley representation theorem for bounded distributive lattices is a natural duality for the class  $\mathsf{D}_{01} = \text{ISP}(L_2)$ , 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 1 specializes to the main theorem in [8,10].

**Boolean algebras.** Stone’s representation theorem for Boolean algebras is obtained for the class  $\mathbf{B} = ISP(B_2)$  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. A consequence of Theorem 1 is the well-known fact that  $\mathbf{B} \models \forall \bar{c} \exists \bar{y} (\bigwedge_{i=1}^k s_i = t_i)$  iff  $\mathbf{B}_2 \models \forall \bar{c} \exists \bar{y} (\bigwedge_{i=1}^k s_i = t_i)$  (Lcr is empty, so we have  $2^C$  independent satisfiability problems, one for each  $X \subseteq C$ ).

**Varieties generated by primal algebras.** Also in this case the “alter ego” topological spaces have the discrete topology and do not contain any relations. As a consequence of Theorem 1, if  $\mathcal{V}$  is the variety generated by the primal algebra  $P$  then  $\mathcal{V} \models \forall \bar{c} \exists \bar{y} (\bigwedge_{i=1}^k s_i = t_i)$  iff  $P \models \forall \bar{c} \exists \bar{y} (\bigwedge_{i=1}^k s_i = t_i)$ .

**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  $\mathbf{K} = ISP(K_3)$ , generated by the three-element Kleene algebra  $K_3 = (\{0, 1, a\}, \vee, \wedge, 0, 1, \neg)$ , where  $0 \leq a \leq 1$ ,  $\neg 0 = 1$ ,  $\neg 1 = 0$ , and  $\neg a = a$ . A strong duality on  $\mathbf{K}$  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  $\preceq = \{(0, 0), (0, a), (1, 1), (1, a), (a, a)\}$  (cf. e.g. [6], Sect. 4.3). Theorem 1 yields a reduction to reasoning with 3-valued predicates.

## References

1. F. Baader and P. Narendran. Unification of concept terms in description logics. *J. Symbolic Computation*, 31(3):277–305, 2001.
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*, Vol. I, Ch. 8, 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 positive theory of some finitely-generated varieties of algebras. In *Proceedings of the 34th ISMVL*, pages 32–37. IEEE Computer Society, 2004.
10. V. Sofronie-Stokkermans. On unification for bounded distributive lattices. *ACM Transactions on Computational Logic*, 8(2), 2007.