The Exact Unification Type of Commutative Theories

Franz Baader[1] and Pierre Ludmann[2]

[1] TU Dresden, Germany, franz.baader@tu-dresden.de
[2] École Normale Supérieure de Cachan, France, pierre.ludmann@ens-cachan.fr

Abstract

The exact unification type of an equational theory is based on a new preorder on substitutions, called the exactness preorder, which is tailored towards transferring decidability results for unification to disunification. We show that two important results regarding the unification type of commutative theories hold not only for the usual instantiation preorder, but also for the exactness preorder: w.r.t. elementary unification, commutative theories are of type unary or nullary, and the theory ACUIh of Abelian idempotent monoids with a homomorphism is nullary.

1 Introduction

It is well-known that deciding solvability of a disunification problem modulo an equational theory E [BB94, Com91] can be reduced to E-unification in case the theory E is *effectively finitary*, i.e., for every E-unification problem a finite complete set of E-unifiers always exists and can be effectively computed. Given a disunification problem Γ, one first computes a finite complete set of E-unifiers for the equations in Γ, and then checks whether this set contains a substitution that also satisfies all the disequations of Γ.

In order to extend this approach to non-finitary equational theories, Cabrer and Metcalfe [CM14] introduced a new preorder on substitutions that contains, but is usually larger than, the instantiation preorder:

$$\sigma \sqsubseteq_E^X \tau \text{ iff } \sigma(s) =_E \sigma(t) \Rightarrow \tau(s) =_E \tau(t) \text{ for all terms } s, t \text{ built using only variables from } X.$$

Using this preorder in place of the instantiation preorder (where X is the set of variables occurring in the unification problem), one can now define (minimal) complete sets of unifiers, and thus obtain a new classification of equational theories w.r.t. their type, which we call *exact unification type*. The definition of the exactness preorder is tailored towards ensuring that the above reduction from disunification to unification still works. The advantage of using the exactness preorder rather than the instantiation preorder is that the former is larger, and thus it may be the case that a theory that is non-finitary w.r.t. the instantiation preorder is finitary w.r.t. the exactness preorder. For instance the theories of Idempotent Semigroups and of Distributive Lattices are nullary w.r.t. the instantiation preorder, yet their exact types are respectively finitary and unitary (see [CM14] for these and more examples). In the following, we will denote the instantiation preorder as $\leq_E$ and the exactness preorder as $\sqsubseteq_E$, where the set of variables X on which the substitutions are compared is always assumed to be the set of variables occurring in the unification problem under consideration.

Commutative theories were introduced in [Baa89] in order to generalize approaches and results for unification in the theories axiomatizing Abelian Monoids (ACU), idempotent Abelian Monoids (ACUI), and Abelian groups (AG). One important result in [Baa89] is the fact that, w.r.t. elementary unification, commutative theories are of unification type either unitary or nullary. Recall that a unification problem is elementary if it does not contain free constant or function symbols. The three theories mentioned above are all unitary. To provide an example for a non-unitary (and thus nullary) equational theory, it is shown in [Baa89] that the theory ACUIh of idempotent Abelian monoids with a homomorphism is nullary:

$$\begin{aligned}\mathsf{ACUIh} \quad := \quad & \{x + 0 = x, x + (y + z) = (x + y) + z, x + y = y + x, x + x = x,\\ & h(x + y) = h(x) + h(y), h(0) = 0\}\end{aligned}$$

The mentioned results use the instantiation preorder to compare substitutions. We will show below that these results also hold if the exactness preorder is used in place of the instantiation preorder.

2 The Dichotomy Result for Exact Types

The class of commutative theories is defined in [Baa89] using the category of finitely generated free algebras.[1] To be more precise, let E be an equational theory and V a denumerable set (of variables). Then the category $\mathcal{C}(E)$ is defined as follows:

- The objects of $\mathcal{C}(E)$ are the algebras $F_E(X)$ for finite subsets X of V, where $F_E(X)$ is the free algebra generated by X in the variety defined by E.
- The morphisms of $\mathcal{C}(E)$ are the homomorphisms between these objects, where the composition of morphisms is the usual composition of mappings.

An equational theory E is *commutative* if the associated category $\mathcal{C}(E)$ is semiadditive. The exact definition of semiadditive categories can be found in [HS73, Baa89]. For the purpose of this paper it is sufficient to know that in such a category the coproduct is also a product. In [Baa89] there is also a more algebraic characterization of commutative theories, which shows that the theories ACU, ACUI, AG, and ACUIh are commutative.

The following theorem generalizes Theorem 6.3 in [Baa89] from the instantiation preorder to all preorders extending the instantiation preorder. It thus applies to the exactness preorder, but also to the preorder on substitutions introduced in [HS06].

Theorem 1. *For elementary unification, commutative theories are either unitary or nullary w.r.t. any preorder $\preceq$ containing the instantiation preorder.*

Proof. A theory is either at most finitary or at least infinitary. In the first case, use the first lemma below to show that it is actually unitary. In the second case, the condition of the second lemma is satisfied, which shows that the theory is actually nullary. ☐

For the remainder of this section, we assume that $\preceq$ is a preorder that contains the instantiation preorder. To align our proofs of the two lemmata with the corresponding ones given in [Baa89] for the instantiation preorder, we use the categorical formulation of unification introduced there. To obtain this formulation, a unification problem $\langle s_i = t_i \mid 1 \leq i \leq n\rangle$ is translated into a pair of morphisms $\langle \sigma = \tau\rangle$, where

$$Dom(\sigma) = Dom(\tau) = I = \{x_1, \ldots, x_n\} \text{ and } \sigma(x_i) = s_i \wedge \tau(x_i) = t_i \text{ for all } i, 1 \leq i \leq n.$$

In this setting, a unifier is a morphism γ such that $\sigma\gamma = \tau\gamma$.

Lemma 1. *Let E be a commutative theory and $\Gamma = \langle \sigma = \tau\rangle$ be an elementary E-unification problem, and let $\{\gamma_1, \ldots, \gamma_n\}$ be a finite complete set of E-unifiers of Γ w.r.t. $\preceq$. Then there exists a E-unifier γ of Γ s.t. the singleton set $\{\gamma\}$ is a complete set of E-unifiers of Γ w.r.t. $\preceq$.*

[1] See [Nut90] for an algebraic definition of the closely related class of monoidal theories.

Proof. Let $\sigma, \tau : F_E(I) \to F_E(X)$ and $\gamma_i : F_E(X) \to F_E(Y_i)$.

Let $Y = Y_1 \uplus \cdots \uplus Y_n$ is the disjoint union of the generating sets Y_i. Then $F_E(Y)$ is the coproduct and the product of the objects $F_E(Y_i)$. Let $p_1, \ldots, p_n$ be the projections for the product. Then there exists a unique morphism $\gamma : F_E(X) \to F_E(Y)$ such that $\gamma p_i = \gamma_i$ for all $i, 1 \leq i \leq n$. Consequently, $\gamma \leq_E \gamma_i$ and thus also $\gamma \preceq \gamma_i$. The morphism γ is an E-unifier of Γ since $\sigma\gamma p_i = \sigma\gamma_i = \tau\gamma_i = \tau\gamma p_i$ for $i = 1, \ldots, n$ implies $\sigma\gamma = \tau\gamma$ (by the definition of product).

It remains to show that $\{\gamma\}$ is complete w.r.t. $\preceq$. Thus, let δ be an E-unifier of Γ. Since $\{\gamma_1, \ldots, \gamma_n\}$ is complete w.r.t. $\preceq$, there is an index i such that $\gamma_i \preceq \delta$. But now transitivity of the preorder $\preceq$ yields $\gamma \preceq \delta$, which shows that $\{\gamma\}$ is indeed complete. $\square$

Lemma 2. *Let E be a commutative theory and $\Gamma = \langle \sigma = \tau \rangle$ be an elementary E-unification problem, and let $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$ be an infinite set of E-unifiers of Γ such that there is no E-unifier α of Γ with $\alpha \preceq \gamma_i$ for all $i \geq 1$. Then there does not exist a minimal complete set of E-unifiers of Γ.*

Proof. Let $\sigma, \tau : F_E(I) \to F_E(X)$ and $\gamma_n : F_E(X) \to F_E(Y_n)$, and let $U_E(\Gamma)$ denote the set of E-unifiers of Γ.

The morphisms δ_n are inductively defined as follows: δ_1 is just γ_1. Assuming that $\delta_n : F_E(X) \to F_E(Z_n)$ is already defined, we consider the product $F_E(Z_{n+1})$ with the projections p_1, p_2 of $F_E(Y_{n+1})$ and $F_E(Z_n)$. Then $\delta_{n+1} : F_E(X) \to F_E(Z_{n+1})$ is defined to be the unique morphism such that $\delta_{n+1} p_1 = \gamma_{n+1}$ and $\delta_{n+1} p_2 = \delta_n$.

As in the proof of the previous lemma, it is easy to see that the morphisms δ_n are E-unifiers of Γ, and that $\delta_{n+1} \leq_E \delta_n$ and thus $\delta_{n+1} \preceq \delta_n$. The condition imposed on $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$ implies that the decreasing chain $\delta_1 \succeq \delta_2 \succeq \delta_3 \succeq \ldots$ has no lower bound in $U_E(\Gamma)$. As a matter of fact, if such a bound α existed, then we would have for all $n \geq 1$ that $\alpha \preceq \delta_n \preceq \gamma_n$, which contradicts our assumption regarding the set $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$.

We now assume that there exists a minimal complete set M of E-unifiers of Γ w.r.t. $\prec$. Since M is complete, there is $\theta \in M$ such that $\theta \preceq \delta_1$. The fact that $\delta_1 \succeq \delta_2 \succeq \delta_3 \succeq \ldots$ has no lower bound in $U_E(\Gamma)$ yields an $n \geq 1$ satisfying $\theta \preceq \delta_n$, but $\theta \not\preceq \delta_{n+1}$. Let $\theta : F_E(X) \to F_E(Y)$, and let $F_E(Z)$ with the projections q_1, q_2 be the product of $F_E(Z_{n+1})$ and $F_E(Y)$. The morphism $\hat{\theta} : F_E(X) \to F_E(Z)$ is defined to be the unique morphism such that $\hat{\theta} q_1 = \delta_{n+1}$ and $\hat{\theta} q_2 = \theta$. Again, it is easy to see that $\hat{\theta}$ is an E-unifier of Γ, $\hat{\theta} \preceq \delta_{n+1}$, and $\hat{\theta} \preceq \theta$. Since M is complete there is $\theta' \in M$ such that $\theta' \preceq \hat{\theta}$. Now $\theta' \preceq \theta$ for $\theta, \theta' \in M$ yields $\theta = \theta'$ by minimality of M. But then $\theta = \theta' \preceq \hat{\theta} \preceq \delta_{n+1}$ is a contradiction to our choice of n. $\square$

3 A Commutative Theory whose Exact Type is Nullary

The following unification problem was used in [Baa89] to show that the theory ACUIh is nullary (w.r.t. the instantiation preorder):

$$\Gamma = \langle\ h(x_1) + h(x_2) = x_2 + h^2(x_3)\ \rangle$$

In [BN96] the same problem was used to extend this result to a large subclass of the class of commutative theories. The proofs use the fact that for all $n \geq 0$ the substitution

$$\theta_n := \{x_1 \mapsto y,\ x_2 \mapsto h(y) + h^2(y) + \cdots + h^{n+1}(y),\ x_3 \mapsto h^n(y)\}$$

is a unifier of Γ. Below, we use the same problem and the same sequence of unifiers to show that an appropriate variant of Lemma 8.1 in [Baa89] also holds if the instantiation preorder is replaced by the exactness preorder. However, the proof is a bit more involved.

Lemma 3. *Let γ be an* ACUIh*-unifier of Γ such that $\gamma \sqsubseteq_{\mathsf{ACUIh}} \theta_n$. Then there is a variable z and a number $k \geq n$ such that $x_3\gamma$ contains $h^k(z)$ as a summand.*

Proof. For simplicity, we denote ACUIh as E in this proof.

First, note that $x_1\gamma \neq_E 0\gamma = 0$ since $\gamma \sqsubseteq_E \theta_n$ and $x_1\theta_n = y \neq_E 0 = 0\theta_n$. Consequently, $x_1\gamma$ is of the form $x_1\gamma = \sum_{i=1}^p h^{n_i}(y_i)$ where $p \geq 1$ and $n_i \geq 0$ and y_i is a variable (possibly, but not necessarily, distinct from the variables x_1, x_2, x_3) for all $1 \leq i \leq p$.

Now, assume that $h^m(\alpha)$ is a summand of $(h(x_1) + h(x_2))\gamma$, where α is a variable. Since $(h(x_1) + h(x_2))\gamma$ is finite, there is a nonnegative integer k s.t.

- $h^{m+k}(\alpha)$ is a summand of $(h(x_1) + h(x_2))\gamma$, but
- $h^{m+k+1}(\alpha)$ is not a summand of $(h(x_1) + h(x_2))\gamma$.

Consequently, $h^{m+k}(\alpha)$ must be a summand of $h^2(x_3)\gamma$, which implies that $m + k \geq 2$ and $h^{m+k-2}(\alpha)$ is a summand of $x_3\gamma$.

Because the terms $h^{n_i+1}(y_i)$ are all summands of $(h(x_1) + h(x_2))\gamma$, we obtain nonnegative integers $k_1, \ldots, k_p$ s.t. $h^{n_i+k_i-1}(y_i)$ is a summand of $x_3\gamma$ for all $i, 1 \leq i \leq n$. Without loss of generality we can assume that $k_1 \geq k_2 \geq \cdots \geq k_p$. Now, consider $t = h^{k_1-1}(x_1) + x_3 + \sum_{i=2}^p h^{k_1-k_i}(x_3)$ and $u = x_3 + \sum_{i=2}^p h^{k_1-k_i}(x_3)$. A simple calculation shows that

$$\begin{aligned}(h^{k_1-1}(x_1))\gamma &= h^{n_1+k_1-1}(y_1) + \sum_{i=2}^{p} h^{n_i+k_1-1}(y_i)\\ &= h^{n_1+k_1-1}(y_1) + \sum_{i=2}^{p} h^{k_1-k_i}(h^{n_i+k_i-1}(y_i)).\end{aligned}$$

Given what we know about the summands of $x_3\gamma$, this implies $t\gamma =_E u\gamma$, which in turn yields $t\theta_n =_E u\theta_n$, i.e.,

$$h^{k_1-1}(y) + h^n(y) + \sum_{i=2}^{p} h^{n+k_1-k_i}(y) =_E h^n(y) + \sum_{i=2}^{p} h^{n+k_1-k_i}(y).$$

Thus, $k_1 - 1 = n$ or there is an $i, 1 \leq i \leq n$, with $k_1 - 1 = n + k_1 - k_i$. In the first case, $h^{n_1+n}(y_1)$ is a summand of $x_3\gamma$, and in the second, $h^{n_1+n}(y_i)$ is a summand of $x_3\gamma$. ☐

Obviously, this lemma implies that the E-unification problem Γ satisfies the prerequisite of Lemma 2 for $\preceq\ =\ \sqsubseteq_E$. Thus, Γ does not have a minimal complete set of E-unifiers for $E =$ ACUIh.

Theorem 2. *For elementary unification,* ACUIh *is nullary w.r.t. the exactness preorder.*

4 Conclusion

The theory ACUIh actually axiomatizes equivalence in the Description Logic $\mathcal{FL}_0$ [BN01], and thus ACUIh-unification corresponds to unification in $\mathcal{FL}_0$. As shown in [BN01], deciding solvability of such unification problems is ExpTime-complete (for unification with constants). Since ACUIh is of exact type nullary, disunification in $\mathcal{FL}_0$ (modulo ACUIh) cannot be reduced to unification using the method outlined in the introduction. Nevertheless, solvability of disunification problems (with constants) was shown to be decidable (more precisely, ExpTime-complete) in [BO12] using an extension of the automata-based decision procedure for $\mathcal{FL}_0$-unification.

Another Description Logic for which unification has been investigated in detail is the Description Logic $\mathcal{EL}$. Equivalence in this logic can be axiomatized by the equational theory SLMO of semilattices with monotone operator, which is not a commutative theory. As shown in [BM10], deciding solvability of $\mathcal{EL}$-unification problems is NP-complete and the unification type (w.r.t. the instantiation preorder) is again nullary. Whether $\mathcal{EL}$ (and thus SLMO) also has exact unification type nullary is still an open problem.

References

[Baa89] Franz Baader. Unification in commutative theories. *Journal of Symbolic Computation*, 8(5):479–497, 1989.

[BB94] Wray L. Buntine and Hans-Jürgen Bürckert. On solving equations and disequations. *J. of the ACM*, 41(4):591–629, 1994.

[BM10] Franz Baader and Barbara Morawska. Unification in the description logic $\mathcal{EL}$. *Logical Methods in Computer Science*, 6(3), 2010.

[BN96] Franz Baader and Werner Nutt. Combination problems for commutative/monoidal theories or how algebra can help in equational unification. *Applicable Algebra in Engineering, Communication and Computing*, 7(4):309–337, 1996.

[BN01] Franz Baader and Paliath Narendran. Unification of concept terms in description logics. *Journal of Symbolic Computation*, 31(3):277–305, 2001.

[BO12] Franz Baader and Alexander Okhotin. Solving language equations and disequations with applications to disunification in description logics and monadic set constraints. In Nikolaj Bjørner and Andrei Voronkov, editors, *Proceedings of the 18th International Conference on Logic for Programming, Artifical Intelligence, and Reasoning (LPAR-12)*, volume 7180 of *Lecture Notes in Computer Science*, pages 107–121, Mérida, Venezuela, 2012. Springer-Verlag.

[CM14] Leonardo Cabrer and George Metcalfe. From admissibility to a new hierarchy of unification types. In *Proceedings of the 28th International Workshop on Unification*, Vienna, Austria, 2014.

[Com91] Hubert Comon. Disunification: A survey. In J.-L. Lassez and G. Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson*, pages 322–359. MIT Press, 1991.

[HS73] H. Herrlich and G. E. Strecker. *Category Theory.* Allyn and Bacon, Boston, 1973.

[HS06] Michael Hoche and Peter Szabó. Essential unifiers. *Journal of Applied Logic*, 4(1):1–25, 2006.

[Nut90] Werner Nutt. Unification in monoidal theories. In M. E. Stickel, editor, *Proceedings of the 10th International Conference on Automated Deduction*, volume 449 of *Lecture Notes in Artificial Intelligence*, pages 618–632, Kaiserslautern, Germany, 1990. Springer-Verlag.