# The Unification Type of ACUI w.r.t. the Unrestricted Instantiation Preorder is not Finitary


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 unification type of an equational theory is defined using a preorder on substitutions, called the instantiation preorder, whose scope is either restricted to the variables occurring in the unification problem, or unrestricted such that all variables are considered. It is known that the unification type of an equational theory may vary, depending on which instantiation preorder is used. More precisely, it was shown that the theory ACUI of an associative, commutative, and idempotent binary function symbol with a unit is unitary w.r.t. the restricted instantiation preorder, but not unitary w.r.t. the unrestricted one. Here, we improve on this result, by showing that, w.r.t. the unrestricted instantiation preorder, ACUI is not even finitary.


## Introduction

The first preorder introduced to deal with unification [Rob65] was in fact the unrestricted instantiation preorder. It was designed for syntactic unification and it worked pretty well considering that it gave a unitary unification type. Yet, when it comes to equational unification, researchers usually employ the restricted instantiation preorder, though the reason for this change was not explained in early papers.

We use the following notation to distinguish between these two preorders:

$$\sigma \leq_E^X \tau \text{ iff } \exists\lambda\forall x \in X.\ \lambda(\sigma(x)) =_E \tau(x) \quad \text{and} \quad \sigma \leq_E^\infty \tau \text{ iff } \exists\lambda\forall x \in \mathcal{V}.\ \lambda(\sigma(x)) =_E \tau(x)$$

Here, $\mathcal{V}$ is the countably infinite set of all variables, whereas $X$ is a (usually finite) subset of it. From now on, we will use $\leq_E$ to denote the restricted preorder $\leq_E^{Var(\Gamma)}$ when the unification problem $\Gamma$ is clear from the context.

Note that $\leq_E^\infty \subseteq \leq_E$, which has as an easy consequence that the unification type in the restricted case can never be worse than the type in the unrestricted case. In particular, syntactic unification is also unitary w.r.t. $\leq_E$. Hence, for the empty theory it makes no difference which instantiation preorder is used. For this reason, the distinction between these two orders was not always rigorously made clear, though it was known that the unrestricted preorder could lead to unpleasant results in weak unification [Ede85].

It took until 1991 before the first example of an equational theory for which the unrestricted and restricted unification types are different was published. That particular theory is ACUI, the theory of idempotent abelian monoids:

$$\mathsf{ACUI} \ := \ \{x + 0 = x, x + (y + z) = (x + y) + z, x + y = y + x, x + x = x\}$$

From [BB88] it was known that ACUI is unitary in the restricted case; in [Baa91], it was shown that its unrestricted type is not unitary. This paper thus showed that the choice of the instantiation preorder makes a difference for equational unification. However, it did not show how big that difference actually is: the unrestricted type of ACUI might be finitary, which is still a quite pleasant type from the application point of view. Here we show that this is not the case: ACUI is at least infinitary. However, the precise unrestricted unification type of ACUI is still an open problem: it is either infinitary or of type zero.

## Auxiliary Results

In the following, $\mathit{Var}(s)$ denotes the set of variables occurring in the term $s$, $\mathit{Dom}(\sigma) = \{x \in \mathcal{V} \mid \sigma(x) \neq x\}$ the domain of the substitution $\sigma$, and $\mathit{VRan}(\sigma) = \bigcup_{x \in \mathit{Dom}(\sigma)} \mathit{Var}(\sigma(x))$ the variable range of $\sigma$.

The proof of our main result (Theorem 2) is based on the fact that ACUI is a theory in which no variable is going to pop – in or out – of a term, i.e. the set of variables of a term is stable under equality modulo the theory. As a matter of fact, this property is called regularity in unification theory.

**Definition 1.** An identity $s = t$ is *regular* if $\mathit{Var}(s) = \mathit{Var}(t)$. A set of identities $E$ is *regular* if all elements of $E$ are regular.

Regularity of the defining set of identities of an equational theory implies regularity of the whole theory.

**Lemma 1** ([Yel85]). *$E$ is regular iff $=_E$ is regular.*

Obviously, all the identities of ACUI are regular, which by the above lemma yields that $s =_{\mathsf{ACUI}} t$ implies $\mathit{Var}(s) = \mathit{Var}(t)$. Thus, the following lemma applies to ACUI.

**Lemma 2.** *Let $E$ be a regular theory and $\Gamma = \langle s = t \rangle$ an $E$-unification problem s.t. $\mathit{Var}(s) \cap \mathit{Var}(t) = \emptyset$. Then the set $\mathcal{U}$ of all unifiers $\sigma$ of $\Gamma$ satisfying*

$$\forall y \in \mathit{VRan}(\sigma). \exists x, x' \in \mathcal{V} \text{ s.t. } x \neq x' \text{ and } y \in \mathit{Var}(\sigma(x)) \cap \mathit{Var}(\sigma(x'))$$

*is complete w.r.t. $\leq_E^\infty$.*

*Proof.* Let $\sigma$ be a unifier of $\Gamma$ that does not belong to $\mathcal{U}$, i.e., there is $y_0 \in \mathit{VRan}(\sigma)$ s.t. there exists a unique $x_0$ verifying $y_0 \in \mathit{Var}(\sigma(x_0))$ (note that $x_0 = y_0$ is possible). Let $\tau = \{x_0 \mapsto y_0, y_0 \mapsto x_0\}$ be the substitution that exchanges $x_0$ with $y_0$ (and is the identity if $x_0 = y_0$). Then define the new substitution $\sigma'$ as $\sigma'(x) := \tau(\sigma(x))$ for $x \in \mathcal{V} \setminus \{x_0\}$ and $\sigma'(x_0) := x_0$. Note that $\mathit{VRan}(\sigma') \subsetneq \mathit{VRan}(\sigma)$: in fact, if $x_0 \in \mathit{VRan}(\sigma)$, then $x_0 \notin \mathit{VRan}(\sigma')$; otherwise, $y_0 \notin \mathit{VRan}(\sigma')$. Using the fact that, in any case, $x_0 \notin \mathit{VRan}(\sigma')$, we can show that $\sigma$ is an (unrestricted) instance of $\sigma'$:

$$\begin{aligned}\forall x \in \mathcal{V} \setminus \{x_0\} : \quad (\tau \circ \{x_0 \mapsto \tau \circ \sigma(x_0)\} \circ \sigma')(x) &= (\tau \circ \{x_0 \mapsto \tau \circ \sigma(x_0)\})(\sigma'(x)) \\ &= \tau(\sigma'(x)) = \tau \circ \tau \circ \sigma(x) = \sigma(x)\end{aligned}$$

Additionally, we have for the variable $x_0$:

$$\begin{aligned}(\tau \circ \{x_0 \mapsto \tau \circ \sigma(x_0)\} \circ \sigma')(x_0) &= (\tau \circ \{x_0 \mapsto \tau \circ \sigma(x_0)\})(x_0) \\ &= \tau(\tau \circ \sigma(x_0)) = \sigma(x_0)\end{aligned}$$

This shows $\sigma' \leq_E^\infty \sigma$. However, we need to show that $\sigma'$ is a unifier of $\Gamma$ in order to make the comparison useful. Because $E$ is a regular theory, $\sigma(s) =_E \sigma(t)$ implies $\mathit{Var}(\sigma(s)) = \mathit{Var}(\sigma(t))$. Then, if $x_0$ occurs in one of the terms $s, t$, it also has to occur in the other one since it is the unique producer of $y_0$. This contradicts our assumption on $\Gamma$. Since, on the variables different from $x_0$, $\sigma'$ is an instance of $\sigma$, we thus know that $\sigma'$ is a unifier of $\Gamma$.

Consequently, we can replace $\sigma$ with $\sigma'$ and so shrink $\mathit{VRan}(\sigma)$. Since $\mathit{VRan}(\sigma)$ is finite, repeating this process will end with a unifier $\sigma^*$ that satisfies the required condition and is more general w.r.t. $\leq_E^\infty$ than the original unifier $\sigma$. $\square$

A second auxiliary result that will be employed in the proof of our main theorem follows easily from the order-theoretic point of view on unification types [Baa89, BS01]. Given any preorder $\preceq$ on the set $U$ of $E$-unifiers of $\Gamma$, we denote with $\sim$ its induced equivalence relation, i.e., $\sigma \sim \tau$ iff $\sigma \preceq \tau$ and $\tau \preceq \sigma$. We denote the $\sim$-equivalence class of a unifier $\sigma$ as $[\sigma]$ and the set of all equivalence classes of unifiers as $[U]$. The partial order induced by $\preceq$ on equivalence classes is defined as usual, i.e., $[\sigma] \leq [\tau]$ iff $\sigma \preceq \tau$. We say that $M \subseteq [U]$ is complete w.r.t. $\leq$ if every element of $[U]$ is above (w.r.t. $\leq$) some element of $M$.

**Theorem 1** ([BS01])**.** *Let $M$ be the set of $\leq$-minimal elements of $[U]$. If $C$ is a minimal complete set of $E$-unifiers of $\Gamma$ w.r.t. $\preceq$, then $M = \{[\sigma] \mid \sigma \in C\}$. Conversely, if $M$ is complete in $U$, then any set of representatives of $M$ is a minimal complete set of $E$-unifiers of $\Gamma$.*

The following easy consequence of this result holds w.r.t. any preorder on unifiers, and thus in particular both for the restricted and the unrestricted instantiation preorder.

**Lemma 3.** *Let $C$ be a complete set of $E$-unifiers of an $E$-unification problem $\Gamma$. Then $\Gamma$ has a minimal complete set of $E$-unifiers iff $C$ contains a minimal complete set of $E$-unifiers of $\Gamma$.*

## The Unrestricted Type of ACUI is at Least Infinitary

We will more generally show the result for regular theories satisfying certain properties, and then show that ACUI satisfies these properties. From now on we assume that

- $E$ is a regular theory,
- $\Gamma = \langle s = t \rangle$ is an $E$-unification problem s.t. $Var(s) \cap Var(t) = \emptyset$,
- there is a $\leq_E^\infty$-minimal unifier $\sigma$ of $\Gamma$ that uses fresh variables, i.e., $VRan(\sigma) \setminus X \neq \emptyset$ where $X = Var(s) \cup Var(t)$, and
- this unifier $\sigma$ belongs to the set $\mathcal{U}$ defined in the formulation of Lemma 2.

We will prove that in such a configuration, $\Gamma$, and so $E$, is at least infinitary w.r.t. unrestricted instantiation.

Let $x_0 \in VRan(\sigma) \setminus X$ and consider the following construction of substitutions:

$$\sigma_z := \sigma \circ (x_0 z) \quad \text{where } (x_0 z) := \{x_0 \mapsto z, z \mapsto x_0\} \text{ and } z \in \mathcal{V}.$$

We will show that, under certain conditions on $z$, such substitutions $\sigma_z$ are $\leq_E^\infty$-minimal unifiers that are incomparable to each other w.r.t. $\leq_E^\infty$. By Theorem 1, this implies that $\Gamma$ cannot have a finite minimal complete set of unifiers w.r.t. $\leq_E^\infty$ since there are infinitely many variables $z$ satisfying these conditions.

**Lemma 4.** *For any $z \notin X$, $\sigma_z$ is a minimal unifier of $\Gamma$ w.r.t. $\leq_E^\infty$.*

*Proof.* Note that $\sigma_z$ is a unifier of $\Gamma$ because $x_0, z \notin X$. Moreover, let $\theta$ be a unifier of $\Gamma$ s.t. $\theta \leq_E^\infty \sigma_z$, i.e., there is a substitution $\lambda$ s.t.

$$\forall x \in \mathcal{V}. \quad \sigma_z(x) =_E \lambda \circ \theta(x)$$

Consequently, if we "multiply" from the right with $(x_0 z)$, we obtain

$$\forall x \in \mathcal{V}. \quad \sigma(x) =_E \lambda \circ (\theta \circ (x_0 z))(x).$$

Because $(\theta \circ (x_0 z))$ is a unifier of $\Gamma$ with $(\theta \circ (x_0 z)) \leq_E^\infty \sigma$, minimality of $\sigma$ yields $\sigma \leq_E^\infty (\theta \circ (x_0 z))$, i.e., there exists $\mu$ s.t.

$$\forall x \in \mathcal{V}. \quad (\theta \circ (x_0 z))(x) =_E \mu \circ \sigma(x).$$

Consequently, "multiplying" again from the right with $(x_0 z)$ yields

$$\forall x \in \mathcal{V}. \quad \theta(x) =_E \mu \circ \sigma_z(x).$$

Thus, we have shown that $\theta \leq_E^\infty \sigma_z$ for a unifier $\theta$ of $\Gamma$ implies $\sigma_z \leq_E^\infty \theta$, which proves that $\sigma_z$ is a minimal unifier of $\Gamma$ w.r.t. $\leq_E^\infty$. □

**Lemma 5.** *For any two different variables $z, z' \notin Dom(\sigma) \cup VRan(\sigma)$, $\sigma_z$ and $\sigma_{z'}$ are incomparable w.r.t. $\leq_E^\infty$.*

*Proof.* Assume there exists $\lambda$ s.t. $\forall x \in \mathcal{V}.\ \sigma_{z'}(x) =_E \lambda \circ \sigma_z(x)$, and let $t_0 := \sigma(x_0)$.

Case 1: $Var(t_0) = \emptyset$
Then $\sigma_{z'}(z) =_E \lambda \circ \sigma_z(z)$ implies $z =_E \lambda(t_0)$. This definitely contradicts the existence of $\lambda$ since it cannot create a variable from a ground term.

Case 2: $Var(t_0) \neq \emptyset$
Then there exists $y_0 \in Var(t_0)$. Note that, independent of whether $y_0 = x_0$ or $y_0 \neq x_0$, we have $y_0 \in VRan(\sigma)$. Since $\sigma \in \mathcal{U}$ by our assumptions on $\sigma$, there is $x_1 \in \mathcal{V}$ different from $x_0$ s.t. $\sigma(x_1) =_E t_1$ and $y_0 \in Var(t_1)$. Again, $\sigma_{z'}(z) =_E \lambda \circ \sigma_z(z)$ implies $z =_E \lambda(t_0)$. Because $E$ is regular, this implies $Var(\lambda(y_0)) \subseteq \{z\}$.

Since $z, z' \notin Dom(\sigma) \cup VRan(\sigma)$, $x_1 \neq z$ and $x_1 \neq z'$; so $\sigma_{z'}(x_1) =_E \lambda \circ \sigma_z(x_1)$ implies $t_1 =_E \lambda(t_1)$ Again, regularity yields $Var(\lambda(y_0)) \subseteq Var(t_1)$.

Then $Var(\lambda(y_0)) = \emptyset$ as $z \notin VRan(\sigma)$ and $Var(t_1) \subseteq VRan(\sigma)$. In fact, if $x_1 \in Dom(\sigma)$, then $Var(t_1)$ is contained in $VRan(\sigma)$ by the definition of *VRan*. Otherwise, we must have $x_1 = \sigma(x_1) =_E t_1$. Since $y_0 \in Var(t_1)$, regularity of $E$ yields $y_0 = x_1$ and $Var(t_1) = \{y_0\}$. Thus, $y_0 \in VRan(\sigma)$ yields $Var(t_1) \subseteq VRan(\sigma)$.

However, since $z =_E \lambda(t_0)$, the variable $z$ is produced by $\lambda$ from at least one variable $y$ that occurs in $t_0$, i.e., there is a variable $y \in Var(t_0) \setminus \{y_0\}$ such that $Var(\lambda(y)) = \{z\}$.[1] Since $y \in VRan(\sigma)$ and $\sigma \in \mathcal{U}$, there exists $x \neq x_0$ s.t. $y \in Var(\sigma(x))$. Yet again, as $z, z' \notin Dom(\sigma) \cup VRan(\sigma)$, we know $x \neq z$ and $x \neq z'$, and thus $\sigma_{z'}(x) =_E \lambda \circ \sigma_z(x)$ implies $\sigma(x) =_E \lambda \circ \sigma(x)$. Since we know that $z \in Var(\lambda \circ \sigma(x))$, regularity yields $z \in Var(\sigma(x))$. However, this is absurd since $x \neq z$ and $z \notin VRan(\sigma)$.

To sum up, we have shown that $\sigma_z \leq_E^\infty \sigma_{z'}$ does not hold. A symmetric argument yields that $\sigma_{z'} \leq_E^\infty \sigma_z$ also does not hold. □

Since the complement of the finite set $X \cup Dom(\sigma) \cup VRan(\sigma)$ in the countably infinite set $\mathcal{V}$ of all variables is infinite, the set of unifiers of $\Gamma$ must have infinitely many minimal elements. By Theorem 1, this shows that $\Gamma$ cannot have a finite minimal complete set of unifiers.

**Lemma 6.** *The unification problem $\Gamma$ does not have a finite minimal complete set of $E$-unifiers w.r.t unrestricted instantiation, and thus $E$ is at least infinitary w.r.t. $\leq_E^\infty$.*

We are now ready to apply this result to ACUI.

**Theorem 2.** ACUI *is at least infinitary w.r.t. $\leq_{\mathsf{ACUI}}^\infty$.*

*Proof.* Since ACUI is regular, it is sufficient to show that there is an ACUI-unification problem $\Gamma$ and a minimal unifier $\sigma$ of $\Gamma$ satisfying the conditions stated at the beginning of this section.

[1] Note that, if there is no such additional variable in $t_0$, then this already contradicts the existence of $\lambda$, making the point.

According to Corollary 3.6 in [BB88], any most general unifier (w.r.t. restricted instantiation) of the ACUI-unification problem $\Gamma = \langle x + y + z = u + v\rangle$ must use a fresh variable. Let $\theta$ be such an mgu.

If $\Gamma$ does not have a minimal complete set of ACUI-unifiers w.r.t. unrestricted instantiation, then we are done. Thus, assume that $\Gamma$ has a minimal complete set $M$ w.r.t. unrestricted instantiation. By Lemma 2 and Lemma 3, we can assume without loss of generality that $M \subseteq \mathcal{U}$, and by Theorem 1 we know that the elements of $M$ are $\leq^{\infty}_{\mathsf{ACUI}}$-minimal. Since $\theta$ is an ACUI-unifier of $\Gamma$, there is a $\sigma \in M$ such that $\sigma \leq^{\infty}_{\mathsf{ACUI}} \theta$. Since $\leq^{\infty}_{\mathsf{ACUI}} \subseteq \leq^{X}_{\mathsf{ACUI}}$, this implies that $\sigma$ is also an mgu of $\Gamma$ w.r.t. restricted instantiation, and thus it introduces a fresh variable.

Consequently, we have shown that all prerequisites for applying Lemma 6 are satisfied, which proves the theorem. $\square$

## Conclusion

In this paper we have shown that the gap between the unification types of equational theories w.r.t restricted and unrestricted instantiation is wider than previously known. In fact, for ACUI, which is unitary w.r.t. restricted instantiation, it was only known that the unrestricted type is at least finitary [Baa91]. Now we know that it is at least infinitary, which makes using unrestricted instantiation in this setting even less desirable.

Regarding future work, it would of course be good if we could determine the exact unification type of ACUI w.r.t. unrestricted instantiation (infinitary or type zero), but we have not been able to achieve this yet.

# References

[Baa89] Franz Baader. Characterizations of unification type zero. In N. Dershowitz, editor, *Proceedings of the 3rd International Conference on Rewriting Techniques and Applications*, volume 355 of *Lecture Notes in Computer Science*, pages 2–14, Chapel Hill, North Carolina, 1989. Springer-Verlag.

[Baa91] Franz Baader. Unification, weak unification, upper bound, lower bound, and generalization problems. In R. V. Book, editor, *Proceedings of the 4th International Conference on Rewriting Techniques and Applications*, volume 488 of *Lecture Notes in Computer Science*, pages 86–97, Como, Italy, 1991. Springer-Verlag.

[BB88] Franz Baader and Wolfram Büttner. Unification in commutative idempotent monoids. *Theoretical Computer Science*, 56(3):345–353, 1988.

[BS01] Franz Baader and Wayne Snyder. Unification theory. In J.A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, pages 447–533. Elsevier Science Publishers, 2001.

[Ede85] Elmar Eder. Properties of substitutions and unifications. *Journal of Symbolic Computation*, 1(1):31–46, 1985.

[Rob65] John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM (JACM)*, 12(1):23–41, 1965.

[Yel85] Katherine A Yelick. A generalized approach to equational unification. Technical Report TR-344, MIT Lab. for Computer Science, 1985.