Mathematical Structures in Computer Science (2021), **31**, pp. 898–917
doi:10.1017/S0960129522000019

CAMBRIDGE UNIVERSITY PRESS

PAPER

E-Unification based on Generalized Embedding

Peter Szabo[1] and Jörg Siekmann[2*]

[1]Kurt-Schumacher-Str. 13, D-75180 Pforzheim, Germany and [2]Saarland University/DFKI, Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany

*Corresponding author. Email: siekmann@dfki.de

(Received 29 January 2019; revised 25 November 2021; accepted 7 January 2022; first published online 24 March 2022)

Abstract

Ordering is a well-established concept in mathematics and also plays an important role in many areas of computer science, where *quasi-orderings*, most notably *well-founded quasi-orderings* and *well-quasi-orderings,* are of particular interest. This paper deals with quasi-orderings on first-order terms and introduces a new notion of unification based on a special quasi-order, known as *homeomorphic tree embedding*. Historically, the development of unification theory began with the central notion of *a most general unifier* based on the *subsumption order*. A unifier σ is most general, if it subsumes any other unifier τ, that is, if there is a substitution λ with $\tau =_E \sigma\lambda$, where E is an equational theory and $=_E$ denotes equality under E. Since there is in general more than one most general unifier for unification problems under equational theories E, called *E-Unification*, we have the notion of a complete and minimal set of unifiers under E for a unification problem Γ, denoted as $\mu\mathcal{U}\Sigma_E(\Gamma)$. This set is still the basic notion in unification theory today. But, unfortunately, the subsumption quasi-order is not a well-founded quasi-order, which is the reason why for certain equational theories there are solvable E-unification problems, but the set $\mu\mathcal{U}\Sigma_E(\Gamma)$ does not exist. They are called type nullaryin the unification hierarchy. In order to overcome this problem and also to substantially reduce the number of most general unifiers, we extended the well-known *encompassment order on terms* to an *encompassment order on substitutions* (modulo E). Unification under the encompassment order is called *essential unification* and if $\mu\mathcal{U}\Sigma_E(\Gamma)$ exists, then the complete set of essential unifiers $e\mathcal{U}\Sigma_E(\Gamma)$ is a subset of $\mu\mathcal{U}\Sigma_E(\Gamma)$. An interesting effect is that many E-unification problems with an infinite set of most general unifiers (under the subsumption order) reduce to a problem with only finitely many *essential* unifiers. Moreover, there are cases of an equational theory E, for which the complete set of most general unifiers does not exist, the *minimal and complete set of essential unifiers* however does exist. Unfortunately again, the encompassment order is not a well-founded quasi-ordering either, that is, there are still theories with a solvable unification problem, for which a minimal and complete set of essential unifiers does not exist. This paper deals with a third approach, namely the extension of the well-known *homeomorphic embedding of terms* to a *homeomorphic embedding of substitutions (modulo E)*. We examine the set of most general, minimal, and complete E-unifiers under the quasi-order of homeomorphic embedment modulo an equational theory E, called $\varphi U\Sigma_E(\Gamma)$, and propose an appropriate definitional framework based on the standard notions of unification theory extended by notions for the *tree embedding theorem* or Kruskal's theorem as it is called. The main results are that for *regular* theories the minimal and complete set $\varphi\mathcal{U}\Sigma_E(\Gamma)$ always exists. If we restrict the E-embedding order to *pure E-embedding, a* well-known technique in logic programming and term rewriting where the difference between variables is ignored, the set $\varphi_\pi\mathcal{U}\Sigma_E(\Gamma)$ always exists and it is even finite for any theory E.

Keywords: Universal algebra; equational theory; ordering; unification theory; *E*-unification; essential unification; (homeomorphic) embedded E-unifiers; pure E-unifiers

1. Introduction

Ordering is a well-established concept in mathematics and it plays an important role in many areas of theoretical computer science too. *Quasi-orderings* (*qo*) and most notably *well-founded quasi-orderings* (*wfqo)* and *well-quasi-orderings (wqo)* in particular are of great general interest, see Kruskal (1972). Probably the most popular application within our own field is the use of quasi-orders and well-quasi-orders on first-order terms to prove the termination of rewriting rules, see Dershowitz (1982, 1987) and logic programs see Leuschel (1998, 2002).

In the theory of E-unification of terms based on an alphabet $\Sigma = F \cup X$, with signature F and variables X and an equational theory E, the set $\mathcal{U}\Sigma_E(\Gamma)$ denotes the set of all E-unifiers of a unification problem Γ. Of great interest is now to find a complete and minimal subset of $\mathcal{U}\Sigma_E(\Gamma)$, denoted as $\mu\mathcal{U}\Sigma_E(\Gamma)$, from which all other E-unifiers can be obtained.

Equality on terms induced by the equational theory E will be denoted as $=_E$ and the *subsumption order on terms* is denoted as $\leq_E$. So, if there are two unifiers τ and σ for terms s and t, such that $s\tau =_E t\tau$ and $s\sigma =_E t\sigma$ and there is a substitution λ, such that $\tau =_E \sigma\lambda$, then τ is an instance of σ, or σ *subsumes* τ, denoted as $\sigma \leq_E \tau$. This led to the notion of *a most general E-unifier* (mgu), that is an E-unifier, which is not an instance of any other E-unifier. The set of most general unifiers is denoted as $\mu\mathcal{U}\Sigma_E(\Gamma)$ and every E-unifier is subsumed by some element of $\mu\mathcal{U}\Sigma_E(\Gamma)$, that is, it can be obtained by instantiation in an automated reasoning process, such as *resolution* (Robinson, 1965). Often we shall drop the E from E-unifiers if it is understood from the context.

To illustrate the role of orderings in E-unification, consider the equational theory A for free semigroups with the axiom of associativity for terms built over a binary function symbol f with $A = \{f(x,f(y,z)) = f(f(x,y),z)\}$. This is also known as the word (or string) algebra and the notation is that of words (strings), where we just drop the function symbol f and have concatenation of symbols.

For example, the string unification problem $\Gamma_1 = \{ax =^? xa\}$ has most general unifiers of the form $\sigma_n = \{x \mapsto a^n : n \geqq 1\}$. Because the σ_n are ground substitutions, they are incomparable with respect to the subsumption order, so $\mu\mathcal{U}\Sigma_A(\Gamma_1) = \{\sigma_n : n \geqq 1\}$ is an infinite set and therefore Γ_1 is of unification type *infinitary*. Furthermore, since the subsumption order is not a well-quasi-order, there are equational theories such that the set of mgus does not exist, see Baader (1988) and Hoche (2016).

In order to address these problems, we proposed a generalization of the *encompassment* of terms to equational encompassment of substitutions, whereby a term s is encompassed by a term t, denoted as $s \sqsubseteq t$, iff an instance of s, say $s\sigma$, is a subterm of t. This allows a decomposition of t in the following sense: if we denote with t' the replacement of the subterm $s\sigma$ of t by a new variable z', then the term t can be written as $t = t'\{z' \to s\}\sigma$. Equational encompassment of terms, denoted as $\sqsubseteq_E$, is then lifted component-wise to substitutions and applied to the set of E-unifiers. We then introduced the notion of an *essential E-unifier* by saying that σ is E-encompassed by τ, $\sigma \sqsubseteq_E \tau$, iff each domain variable x of τ is also a domain variable of σ and $x\tau$ has an instance of $x\sigma$ as a subterm (modulo E). E-unifiers, which are not encompassed by any other unifier, are then called *essential* E-unifiers and the *complete* set of essential E-unifiers is denoted as $e\mathcal{U}\Sigma_E(\Gamma)$ for a unification problem Γ. If $\mu\mathcal{U}\Sigma_E(\Gamma)$ exists, we have $e\mathcal{U}\Sigma_E(\Gamma) \subseteq \mu\mathcal{U}\Sigma_E(\Gamma)$, that is, the encompassment order generalizes the subsumption order and there are cases where an E-unification problem with an infinite set of mgus reduces to a finite set of essential unifiers (Hoche and Szabo, 2006; Szabo et al., 2016). Moreover it can happen that an equational theory E, for which $\mu\mathcal{U}\Sigma_E(\Gamma)$ does not exist, may **have** a minimal and complete set of essential unifiers $e\mathcal{U}\Sigma_E(\Gamma)$.

For example, the unification type of Γ_1 from above changes drastically using the encompassment order: the *essential* unifier $\sigma_1 = \{x \mapsto a\}$ encompasses all the other most general unifiers $\sigma_n = \{x \mapsto a^n\}$, $n > 1$, because $\sigma_1 \sqsubseteq_A \sigma_n$, $n > 1$. More precisely, the decomposition of a term, which encompasses another term, as shown above, is also valid for substitutions. In this case,

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

encompassment allows the decomposition $\sigma_n = \lambda_n\sigma_1$, where $\lambda_n = \{x \mapsto a^n x\},\ n \geqq 0$. So the minimal and complete set of essential unifiers for Γ_1 is $e\mathcal{U}\Sigma_E(\Gamma_1) = \{\sigma_1\}$, that is, it is unitary instead of infinitary as it is under the subsumption ordering.

Nevertheless there are still essentially infinitary string unification problems, as the following example shows. Let $\Gamma_2 = \{xby =^? ayayb\}$ be the string unification problem, which has $eU\Sigma_A(\Gamma_2) = \{\{x \mapsto ab^n a, y \mapsto b^n\} : n > 0\}$ as its minimal and complete set of essential unifiers. The unifiers are incomparable with respect to encompassment, because $ab^n a$ cannot be a substring of $ab^m a$ for $m \neq n$. Furthermore, as the encompassment order on unifying substitutions is not a wqo, unfortunately again, there are theories with a solvable unification problem Γ, for which $e\mathcal{U}\Sigma_E(\Gamma)$ does not exist, see Baader (1988), Hoche (2008), and Szabo et al. (2016).

This paper deals with a further generalization, namely the extension of the well-known *homeomorphic embedding of terms* to *a homeomorphic embedding modulo E of terms and of substitution*s, called E-embedding of terms or substitutions, respectively.[1] Informally, the homeomorphic embedding of terms is understood as follows:

Let $s = f(s_1, ..., s_n)$ and $t = f(t_1, ..., t_n)$ be terms, then s is syntactically embedded into t, denoted as $s \trianglelefteq t$ iff $s = t$ or $s \trianglelefteq t_i$ for some i or $s_i \trianglelefteq t_i$ for all i. For example, $f(x,\ b) \trianglelefteq \mathbf{f}(g(a,\ \mathbf{x}), f(x,\ \mathbf{b}))$ and also $f(x, b) \trianglelefteq \mathbf{f}(f(a, h(\mathbf{x})), f(\mathbf{b}, a))$ and $f(a, x) \trianglelefteq \mathbf{f}(g(\mathbf{a}, b), \mathbf{x})$, but $f(a, b) \not\trianglelefteq f(g(a, b), x)$.

The E-embedding order for terms, denoted as $\trianglelefteq_E$, will then be extended to an E-embedding order for substitutions similar to the encompassment order in Szabo et al. (2016). We define $\sigma \trianglelefteq_E \tau$ iff each domain variable x of τ is also a domain variable of σ and $x\tau$ homeomorphically E-embeds $x\sigma$, that is if $\tau = \{x_i \mapsto t_i\}$ and $\sigma = \{x_i \mapsto s_i\},\ 1 \leqq i \leqq n$, then $\sigma \trianglelefteq_E \tau$ iff $s_i \trianglelefteq_E t_i$. To illustrate the effect of this E-embedding order, take Γ_2 from above as an example, where E is the equational theory A for strings. In this case, $aba \trianglelefteq_A ab.....ba$ and $b \trianglelefteq_A b.....b$, hence with $\sigma_1 = \{x \mapsto aba, y \mapsto b\}$ we have $\sigma_1 \trianglelefteq_A \sigma_n$ for all $n > 1$. Consequently, σ_1 is the only *minimal* unifier and the set of embedment free unifiers for Γ_2 is $\lambda\mathcal{U}\Sigma_A(\Gamma_2) = \{\sigma_1\}$ and it is finite. In fact, it can be shown that in general the theory is *unitary* instead of infinitary as before.

But in order to generalize the encompassment order for terms to the embedment order for unification problems, we need a more general notion of embedment. This is achieved by defining that a term s is *instance E-embedded* into a term t iff an instance of s, say $s\lambda$, is E-embedded into t, which we call λ_E*-embedding*. This is denoted as $s \lessdot_E t$ and E-unifiers, which have no λ_E-embedded unifier, are called free λ_E*-unifiers*. If the set of free λ_E*-unifiers is complete, then it is denoted as* $\varphi U\Sigma_E(\Gamma)$ for a unification problem Γ.

This paper is organized as follows: The next chapter presents the notions and notation in unification theory, term rewriting, and automated theorem proving giving it an algebraic flair. This is then extended to a chapter on quasi-ordering, the basic algebraic notion of this paper. The third chapter presents the main results on E-unification based on equational homeomorphic embedding.

2. Notions and Notation

Notation and basic definitions in unification theory are well known (see, e.g., Baader and Nipkow (1988)) and have found their way into many and diverse academic fields. Most monographs and textbooks on automated reasoning have sections on unification.

In the following, we unify the various presentations of the necessary concepts for unification toward a concise notation which serves our purpose and we show how the additional concepts for ordering E-unifiers based on homeomorphic embedding can be built upon these definitions. The notion of an algebra given below embraces algebraic structures and the original notions in computational logic, recursive function theory, theory of automata, and automated theorem proving are compatible and natural applications.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

2.1 Signatures, terms, and term algebras

A *signature* is a finite set F of function symbols that come with a nonnegative integer n, called *arity*, which is assigned to each member f of F. f is an n-ary function symbol. The subset of n-ary function symbols in F is denoted by F_n. An *algebra* of type F is an ordered pair $A = \langle A, F \rangle$, where A is a nonempty set and F is a family of finitary operations on A indexed by the signature F such that corresponding to each n-ary function symbol f in F_n there is an n-ary operation f^A on A. The set A is called the carrier of the algebra.

Let X be a set of (distinct) variables. Let F be a signature. The set $T(F, X)$ of (syntactic) *terms* of F over X is the smallest set

(i) comprising X and F_0 and

(ii) if $t_1, \ldots, t_n$ in $T(F, X)$ and f in F_n, then $f(t_1, \ldots, t_n)$ in $T(F, X)$

The set of variable-free terms are called *ground terms*. The set of variables occurring in a term t is denoted by $\mathbf{Var}(t)$. The set of *subterms* of a term $f(t_1, \ldots, t_n)$ contains the term itself and is closed recursively by containing $t_1, \ldots, t_n$. It is denoted by $\mathbf{Sub}(t)$.

The set of terms can be given an algebraic structure called *term algebra* as usual.

2.2 Substitutions

A *substitution* is a (unique) homomorphism in the term algebra generated by a mapping $\sigma : X \longrightarrow T(F, X)$ from a finite set of variables to terms. Substitutions are generally denoted by small Greek letters $\alpha, \beta, \gamma, \sigma$, etc. and they are represented explicitly as a function by a set of variable bindings $\sigma = \{x_1 \mapsto s_1, \ldots, x_m \mapsto s_m\}$. $\mathcal{S}_{F,X}$ denotes the set of all substitutions. The application of the substitution σ to a term t, denoted $t\sigma$, is defined by induction on the structure of terms

$$t\sigma = \begin{cases} s_i & \text{if } t = x_i \\ f(t_1\sigma, \ldots, t_n\sigma) & \text{if } t = f(t_1, \ldots, t_n) \\ t & \textit{otherwise} \end{cases}$$

The substitution $\varepsilon = \{\}$ with $t\varepsilon = t$ for all terms t in $T(F, X)$ is called the *identity*. A substitution $\sigma = \{x_1 \mapsto s_1, \ldots, x_m \mapsto s_m\}$ has the finite *domain:*

$$\mathbf{Dom}(\sigma) := \{x | x\sigma \neq x\} = \{x_1, \ldots, x_m\};$$

The *range* of the substitution σ is the set of terms

$$\mathbf{Ran}(\sigma) := \bigcup_{x \in \mathbf{Dom}(\sigma)} \{x\sigma\} = \{s_1, \ldots, s_{m'}\}, m' \leq m$$

The set of variables occurring in the range is $\mathbf{VRan}(\sigma) := \mathbf{Var}(\mathbf{Ran}(\sigma))$ and $\mathbf{Var}(\sigma) = \mathbf{Dom}(\sigma) \cup \mathbf{VRan}(\sigma)$. The *restriction* of a substitution σ to a set of variables $Y \subseteq X$, denoted by $\sigma_{|Y}$, is the substitution which is equal to the identity everywhere except over $Y \cap \mathbf{Dom}(\sigma)$, where it is equal to σ. The *composition* of two substitutions σ and θ is written $\sigma \circ \theta$ (to emphasize the composition) or just as $\sigma\theta$. The application is defined by $t\sigma\theta = (t\sigma)\theta$. This is fine if $\sigma\theta$ has no contradictory variable bindings, otherwise there are several solutions proposed in the literature which solve this problem and preserve functional composition, see, for example, Baader and Nipkow (1988) and Baader and Snyder (2001).

Relations such as $=, \geq, \ldots$ between substitutions sometimes hold only if they are restricted to a certain set of variables V. A relation R which is restricted to V is denoted as R^V, and defined as $\sigma R^V \tau \Longleftrightarrow x\sigma R x\tau$ for all x in V. Two substitutions σ and θ are *equal*, denoted $\sigma = \theta$ iff $x\sigma = x\theta$ for every variable x; they are *equal restricted to V,* $\mathrm{x}\sigma =^V \mathrm{x}\theta$, iff $x\sigma = x\theta$ for all variables x in V.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

2.3 Congruences and equations

An equivalence relation Θ on the underlying set (the carrier) of an algebra of type F is a *congruence*, if for each n-ary function symbol f in F and elements a_i, b_i of A, for all i in $1 \leq i \leq n$ we have

$$a_i \Theta b_i \Rightarrow f^A(a_1, \ldots, a_n) \Theta f^A(b_1, \ldots, b_n)$$

The quotient algebra is the algebra whose carrier are the equivalence classes A/Θ and whose operations satisfy

$$f^{A/\Theta}(a_1/\Theta, \ldots, a_n/\Theta) = f^A(a_1, \ldots, a_n)/\Theta$$

We are interested in quotient algebras, where the congruence is defined by a set of equations E, which is denoted as $=_E$. For a term t in $T(F, X)$ and the congruence E the equivalence class of t is denoted as $[t]_E$.

2.4 Ordering

Our main interest in this paper is to investigate if the set of most general, minimal, and complete unifiers $\varphi U \Sigma_E(\Gamma)$ exists under certain conditions and the main technique for showing this result is based on orderings, in particular on well-quasi-orderings.

Definition 1. A *quasi-order (also called a pre-order)* is a binary relation that is *reflexive* and *transitive.*

A term t is (syntactically) an *instance* of a term s, if $s\sigma = t$ for some substitution σ. We also say s *subsumes* t and this relation is a quasi-order. It is called the *subsumption order* on terms.
A term t (syntactically) *encompasses* a term s, if an instance of s is a subterm of t. Encompassment conveys the notion that s appears in t with some context "above" (in tree notation) and a substitution instance "below." We say t *encompasses* s or s is *encompassed* by t. In particular, encompassment is called *strict encompassment*, if $s\sigma$ is a proper subterm of t.

A term s is *homeomorphically embedded* into t iff s can be obtained from t by erasing some "parts" in t. We usually abbreviate *homeomorphical embedding* just to *embedding*. Embedment conveys the notion that the structure of s and some corresponding symbols appear within t. A term s is *instance-embedded* into t, we also say it is λ-*embedded* into t, iff an instance of s, that is $s\lambda$, is embedded into t. This is the main notion of this paper, which we will generalize to embedment of substitutions later on.
More formally, we have the following *orders on terms*[2]*:*

Definition 2. (syntactic)

(1) A term s is a *subterm* of t if $s \in \mathbf{Sub}(t)$ and we denote this by $s \leq t$. If s is a proper subterm of t, we write $s < t$.
(2) A term s *subsumes* t, denoted $s \leq t$, iff there exists a substitution σ with $s\sigma = t$
(3) A term s is *encompassed* by t, denoted $s \sqsubseteq t$, iff there exists a substitution σ such that $s\sigma \in \mathbf{Sub}(t)$.
(4) A term s *is embedded into* a term t, denoted $s \trianglelefteq t$, if $s = t$ or s is embedded into an argument of t or the argument terms of s and t embed, respectively:

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

$$s \trianglelefteq t \iff \begin{cases} s = t, \text{ or} \\ t = f(t_1, \ldots, t_n) \text{ and for some } i,\ 1 \le i \le n : s \trianglelefteq t_i, \text{ or} \\ t = f(t_1, \ldots, t_n),\ s = f(s_1, \ldots, s_n) \\ \quad \text{and } \forall i : s_i \trianglelefteq t_i,\ 1 \le i \le n. \end{cases}$$

We denote *strictly embedding* by $s \triangleleft t$ if s and t are not equal.

We also say that t *embeds* s, $t \trianglerighteq s$, and use it either way depending on the context. Embedding is of practical interest, notably in term rewriting systems and logic programming languages, where it is used in termination proofs. Sometimes an equivalent definition is used in these fields based on a reduction system:

Definition 3. For a set of terms $T(F, X)$, the **Embedding Reduction System**, $\mathcal{R}_{\mathrm{F}}$, associated with the signature F is defined as
$\mathcal{R}_{\mathrm{F}} := \{f(x_1, \ldots x_n) \longrightarrow x_i : n \ge 1, f \in F_n \subseteq \Sigma, \textit{for } i,\ 1 \le i \le n\}$.

The following Proposition states a well-known fact, see, for example, Dershowitz and Jouannaud (1991) and Baader and Nipkow (1988).

Proposition 4. *For terms* s, t: *t embeds* s, $t \trianglerighteq s$, *iff* $t \xrightarrow[\mathcal{R}_F]{*} s$.

The next definition for embedding involves instances of terms.

Definition 5. A term s is *instance-embedded* into a term t, denoted $s \lessdot t$, if there is an instantiating substitution λ for s, such that $s\lambda$ is embedded into t: $s\lambda \trianglelefteq t$. We also say that s is λ-*embedded* into t.

Some remarks: embedding implies λ-embedding, but λ-embedding does not necessarily imply embedding.

Remark 6. For terms s and t and a substitution λ:
if $s \trianglelefteq t$, then s is λ-embedded into t, $s\varepsilon \trianglelefteq t$, with the empty substitution ε.
Otherwise: $s \lessdot t$ does not imply $s \trianglelefteq t$, for example, $s = f(a, x)$ and
$t = f(g(a, b), f(b, h(a)))$ and $\lambda = \{x \mapsto a\}$. We have $s \lessdot t$, because $s\lambda \trianglelefteq t$,
but $s \not\trianglelefteq t$ since $s = f(a, x) \not\trianglelefteq f(g(a, b), f(b, h(a))) = t$.

These standard order relations are now extended to equality modulo E for the congruences induced by the equations in E.

Definition 7. Let E be an equational theory:

(1) A term s is a *subterm of* t *modulo* E, *denoted* $s \trianglelefteq_E t$, iff there exists an $s' =_E s$ and a term $t' =_E t$ such that $s' \trianglelefteq t'$. We say s is an E-subterm of t.
(2) A term s subsumes t *modulo* E, $s \lessdot_E t$, iff there exists a substitution σ with $s\sigma =_E t$. We say s E-subsumes t.
(3) A term s is *encompassed by* t *modulo* E, $s \sqsubseteq_E t$ iff there is a substitution σ such that $s\sigma \trianglelefteq_E t$. We say s is E-encompassed by t.

The subterm and the encompassment order are quasi-orders (reflexive and transitive). Fortunately, the extension to *E-subterm* and *E-encompassment* order preserves transitivity, so they are quasi-orders too:

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

Proposition 8. *The E-subterm order, $\preceq_E$, is a quasi-order, that is, it is reflexive and transitive*

Proof. Reflexivity: for a term t it is obvious, that $t \preceq_E t$.
Transitivity: for terms r, s, t if $r \preceq_E s,\ s \preceq_E t \Longrightarrow r \preceq_E t$.
$r \preceq_E s \Longrightarrow \exists r' \in [r]_E, s' \in [s]_E : r' \preceq s'$ and
$s \preceq_E t \Longrightarrow \exists s'' \in [s]_E, t'' \in [t]_E : s'' \preceq t''$. Now because
$s'' =_E s'$ we get a new term t' from t'' by replacing s'' by s'.
And then we have $s' \preceq t'$.
That is: $r' \preceq s' \preceq t'$ and transitivity of $\preceq$ yields $r' \preceq t'$.
Hence, $r =_E r' \preceq t' =_E t \Longrightarrow r \preceq_E t$. □

The important observation for the following is that the term r' in the above proof is not necessarily a subterm of t'. It is a subterm of t' only when t'' is transformed under $=_E$ into t'. This property is not valid for E-embedding and hence transitivity does not hold for this and other reasons. Thus, we cannot prove its quasi-order property. The reason is that if a term t embeds a term p, then there is not necessarily a $t' \in [t]_E$, such that for a given E-variant of p, $p' \in [p]_E$, $t' \trianglerighteq_E p'$. To see this and in order to motivate our Definition 10 below, consider the usual method to extend a quasi-order (relation) R to "R modulo E," which is to take the transitive closure $=_E \circ R \circ =_E$. Originally, we used this idea, where E-embedding is defined as: $t \trianglerighteq_E s$ iff $t =_E s$, *or* $\exists t' \in [t]_E, s' \in [s]_E : t' \trianglerighteq s'$. The problem is, however, that transitivity, namely: $t \trianglerighteq_E s \trianglerighteq_E r \Rightarrow t \trianglerighteq_E r$ does not hold in this case. Consider the following example:
Let $F = \{f, g, h, a, b, c\}$ be a signature and $E = \{f(b, b) = g(c, h(a))\}$
be an equational theory.
Now consider $t = f(g(b, a), f(b, a))$ and $s = f(b, b)$ and $r = h(a)$, where
transitivity of $\trianglerighteq_E$: $t \trianglerighteq_E s \trianglerighteq_E r \Rightarrow t \trianglerighteq_E r$ does not hold:
$t \trianglerighteq_E s$ because $t \trianglerighteq s$ and $s \trianglerighteq_E r$ because $s =_E s' = g(c, h(a)) \trianglerighteq h(a) = r$.
But there is no $t' \in [t]_E$ and no $r' \in [r]_E$, such that $t' \trianglerighteq r'$.
Therefore, we propose an enhanced definition for equational embedding by requiring that if an embedded term p of a term t E-embeds a term s, then t also E-embeds s. For our contribution, it is important that this E-embedding, respectively λ_E–embedding, enhances the comparison of objects (i.e. unifying substitutions) and allows us to use the famous *tree-embedding* theorem Kruskal (1960). This theorem is valid for first-order terms and can be lifted to substitutions and we show later on that it holds for E-embeddings as well. E-embedment, respectively λ_E–embedment, is then our fundamental tool in the rest of this paper. In the following definition and for the rest of this paper note: if two terms are equal under E, then they are *embedment equivalent* $\equiv_E$ too, because $s =_E t$ implies $\exists s' \in [s]_E$ and $\exists t' \in [t]$ with $s' = t'$ which implies $s' \trianglelefteq t'$ and $s' \trianglerighteq t'$, hence $s \equiv_E t$. So we just use $=_E$ in the following.

Definition 9. For a term t and an equational theory E:
Let $\mathbf{Emb_E}(t) := \{p : p =_E p' \text{ and } p' \trianglelefteq t\}$ be the set of the closure under E of all embedded terms in t.

The following is the crucial definition in this paper:

Definition 10. (E-embedding) A term t *E-embeds* a term s, denoted $t \trianglerighteq_E s$, if $s =_E t$, or there are terms $t' =_E t$ and $s' =_E s$ and there is an **embedded** term $p \in \mathbf{Emb_E}(t')$ such that $p \triangleright s'$:

$$t \trianglerighteq_E s \iff \begin{cases} s =_E t \text{ or} \\ \exists t' \in [t]_E, s' \in [s]_E \text{ and } \exists p \in \mathbf{Emb_E}(t') : p \triangleright s' \end{cases}$$

Note that if $p = t'$ and $t \trianglerighteq_E s$ then $\exists t' \in [t]_E, s' \in [s]_E : t' \triangleright s'$ is just a special case of the above definition for $t \trianglerighteq_E s$.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

In order to show that $t \trianglerighteq_E s$, we can use an *E-embedding-chain* of the following form:
$t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright t_3 =_E t'_3 \triangleright \ldots\ldots \triangleright t_n =_E s$
where $\triangleright$ denotes strict embedding as in Definition 2. We abbreviate this chain as $t \blacktriangleright^n_E s$, $n \geq 1$. Note that this embedding chain has the typical regular structure where $=_E$ and $\triangleright$ alternate. The t_i may be an embedded term as denoted by p in the second line of Definition 10.

Lemma 11. *Let s, t be terms, t E-embeds s, $t \trianglerighteq_E s$, iff*
$t =_E s$, or there exists a strictly descending chain of the form:
$t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright t_3 =_E t'_3 \triangleright \ldots\ldots \triangleright t'_n =_E s$, abbreviated as $t \blacktriangleright^n_E s$.

Proof. The first case in Definition 10 is obvious and we show the existence of the E-embedding chain by induction:
$t \blacktriangleright^1_E s$: by Definition 10 $\exists t'_1 \in [t]_E, \exists s' \in [s]_E$ *and* $\exists p \in \mathbf{Emb_E}(t') : p \triangleright s'$.
Hence, $t =_E t'_1 \triangleright s' =_E s$.
$t \blacktriangleright^{n+1}_E s$: that is $t \blacktriangleright^n_E t_n$ and $t_n \blacktriangleright^1_E s$. By induction hypothesis, we have the chain
$t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright \ldots\ldots \triangleright t_n$ and $t_n \blacktriangleright^1_E s$ with $t_n =_E t'_n \triangleright t_{n+1}$, where $t_{n+1} = s'$.
So the whole E-embedding-chain is the following:
$t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright t_3 =_E \ldots\ldots\ldots \triangleright t_n =_E t'_n \triangleright t_{n+1} =_E s$. □

The next definition extends instance-embedding to instance embedding modulo an equational theory E.

Definition 12. (instance E-embedding) A term s is *instance-embedded modulo E* into t, denoted $s \lessdot_E t$, if an instance of s is E-embedded into t, that is $s\lambda \trianglelefteq_E t$ for a substitution λ. We say s is λ_E-embedded into t.

The relation E-embedding is recursively defined in Definition 10 and it can be computed using Proposition 4 as follows:

Proposition 13. *For a set of terms $T(F, X)$ and an equational theory E the*
***E-embedding Rewrite System**, $\mathcal{E}_F$, is defined as $\mathcal{E}_F := (\overset{*}{\longrightarrow}_{\mathcal{R}_F} . \overset{*}{\longrightarrow}_E)$.*
Then for terms s, t: $t \trianglerighteq_E s$ iff $\exists t' \in [t]_E, \exists s' \in [s]_E : t' \overset{*}{\longrightarrow}_{\mathcal{E}_F} s'$.
That is: there is a finite chain of the form:
$t \overset{*}{\longrightarrow}_E t' \overset{*}{\longrightarrow}_{\mathcal{R}_F} t_1 \overset{*}{\longrightarrow}_E t'_1 \overset{*}{\longrightarrow}_{\mathcal{R}_F} t_2 \ldots\ldots \overset{*}{\longrightarrow}_{\mathcal{R}_F} t_n \overset{*}{\longrightarrow}_E s$.

Proof. Follows from Lemma 11 by replacing $=_E$ by its equivalent rewrite system $\overset{*}{\longrightarrow}_E$ and $\trianglerighteq_E$ by its reduction system $\overset{*}{\longrightarrow}_{\mathcal{R}_F}$. □

With Definition 10 and Lemma 11, we obtain our first main result:

Theorem 14. *The E-embedment order $\trianglerighteq_E$ is a quasi-order on terms.*

Proof. Let r, s, t be terms and let E be an equational theory.
reflexivity: Because terms embed themselves.
transitivity: $t \trianglerighteq_E s \trianglerighteq_E r \Longrightarrow t \trianglerighteq_E r$.
By Definition 10 and Lemma 11, we have $t \blacktriangleright^m_E s$ and $s \blacktriangleright^n_E r$
that is $t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright t_3 =_E t'_3 \ldots\ldots\ldots \triangleright t_m =_E s$ and
$s =_E s'_1 \triangleright s_2 =_E s'_2 \triangleright s_3 =_E s'_3 \ldots\ldots\ldots \triangleright s_n =_E r$.
But since $t_m =_E s'_1$ we have the correct chain
$t =_E t'_1 \triangleright t_2 =_E t'_2 \triangleright t_3 =_E t_3 \ldots\ldots\ldots \triangleright t_m =_E s'_1 \triangleright s_2 =_E s'_2 \triangleright s_3 =_E s'_3 \ldots\ldots\ldots \triangleright s_n =_E r$
Hence, $t \blacktriangleright^{n+m}_E r$, which means $t \trianglerighteq_E r$. □

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

The negation of E-subsumption and E-encompassment is obvious: $s \not\trianglelefteq_E t$ iff there exists **no** substitution σ with $s\sigma =_E t$ and $s \not\sqsubseteq_E t$ iff there is **no** substitution σ such that $s\sigma \preceq_E t$. But the notions "not embedded" and "incomparable" with respect to $\trianglelefteq_E$ should be made more explicit.

Definition 15. (not embedded modulo E)

(1) A term s is ***not*** *embedded* modulo E into a term t , $s \not\trianglelefteq_E t$, iff for every element s' of the class $[s]_E$ there exists **no** element t' of the class $[t]_E$ such that $s' \trianglelefteq_E t'$.
(2) Terms s and t are *incomparable* with respect to $\trianglelefteq_E$ iff $s \not\trianglelefteq_E t$ and $t \not\trianglelefteq_E s$.
(3) Terms s and t are *incomparable* with respect to $\preccurlyeq_E$ iff there exist **no** substitutions λ_1 and λ_2 with $s\lambda_1 \trianglelefteq_E t$ and $t\lambda_2 \trianglelefteq_E s$.

We shall lift these orderings modulo E on terms now component-wise to orderings on substitutions in the sense that for all variables in the domain of the substitution we require that the corresponding images fulfill the order relation modulo E.

Definition 16. (ordering modulo E for substitutions restricted to a set of variables)
In the following, let σ, τ be substitutions with $\mathbf{Dom}(\sigma) = \mathbf{Dom}(\tau) \supseteq$ V, where V is some set of variables.

(1) A substitution σ is a *sub-substitution modulo E* of τ *restricted to V*, denoted as $\sigma \preceq_E^V \tau$, if for all x in V, $x\sigma$ is a subterm of $x\tau$ modulo E, that is $x\sigma \preceq_E x\tau$.
(2) A substitution σ *E-subsumes* a substitution τ *restricted to V*, denoted as $\sigma \preceq_E^V \tau$, if there exists a substitution λ such that $\sigma\lambda =_E^V \tau$. The relation $\preceq_E^V$ is called the *E-subsumption order for substitution*s restricted to V.
We denote *E-subsumption equivalence* as $\sigma \sim_E^V \tau$, if $\sigma \preceq_E^V \tau$ *and* $\tau \preceq_E^V \sigma$.
(3) A substitution σ is *E-encompassed* by τ *restricted to V*, denoted $\sigma \sqsubseteq_E^V \tau$, if there exists λ, such that $(\sigma\lambda)$ restricted to V is a sub-substitution of τ modulo E, $\sigma\lambda \preceq_E^V \tau$.
We denote *E-encompassment equivalence* as $\sigma \approx_E^V \tau$ if $\sigma \sqsubseteq_E^V \tau$ *and* $\tau \sqsubseteq_E^V \sigma$.
(4) A substitution σ is *E-embedded* into a substitution τ *restricted to V*, denoted as $\sigma \trianglelefteq_E^V \tau$, iff for all x in V we have $x\sigma \trianglelefteq_E^V x\tau$.
(5) A substitution σ is λ_E*-embedded* into a substitution τ *restricted to V*, denoted as $\sigma \preccurlyeq_E^V \tau$, iff there is a substitution λ, such that $\forall x \in V : x(\sigma\lambda)$ is E-embedded into $x\tau$.

The encompassment and embedment order on terms are well known as quasi-orderings, but the *modulo E* extension to substitutions requires verification.

Theorem 17. *The E-encompassment order is a quasi-order on substitutions.*

Proof. This is an improved version of the proof published before in Szabo et al. (2016) and even earlier in Hoche and Szabo (2006).

reflexivity: $\sigma \sqsubseteq_E \sigma$ by Definition 16 .3 means $\sigma\lambda \preceq_E^V \sigma$, setting λ to the substitution identity ε we have $\sigma =_E \varepsilon\sigma = \sigma$.

transitivity: $\sigma \sqsubseteq_E^V \tau$ and $\tau \sqsubseteq_E^V \psi$ implies $\sigma \sqsubseteq_E^V \psi$, where by definition we have $\mathbf{Dom}(\sigma) = \mathbf{Dom}(\tau) = \mathbf{Dom}(\psi)$, so by Definition 16. 3.:

$$\sigma\lambda_1 \preceq_E^V \tau$$
$$\tau\lambda_2 \preceq_E^V \psi$$

and by composition with λ_2 from the right

$$\sigma\lambda_1\lambda_2 \preceq_E^V \tau\lambda_2 \preceq_E^V \psi \Rightarrow \sigma \sqsubseteq_E^V \psi$$

□

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

Theorem 18. *The E-embedment order is a quasi-order on substitutions.*

Proof. Let σ, τ, ψ be substitutions and $V := \mathbf{Dom}(\sigma) = \mathbf{Dom}(\tau) = \mathbf{Dom}(\psi)$.
reflexivity: $\sigma \trianglelefteq_E^V \sigma$ since $x\sigma$ embeds itself for all x in V.
transitivity: we show: $\sigma \trianglelefteq_E^V \tau \trianglelefteq_E^V \psi$ implies $\sigma \trianglelefteq_E^V \psi$
By Definition 16.(4) : For $\sigma \trianglelefteq_E^V \tau$ we have $\forall x \in V : x\sigma \trianglelefteq_E x\tau$
and for $\tau \trianglelefteq_E^V \psi$ we have $\forall x \in V : x\tau \trianglelefteq_E x\psi$.
Now $\forall x \in V : x\sigma \trianglelefteq_E x\tau$ *and* $x\tau \trianglelefteq_E x\psi$ are assertions on terms,
so using Theorem 14 we have $\forall x \in V : x\sigma \trianglelefteq_E x\psi$
and then by Definition 16.(4) we have $\sigma \trianglelefteq_E^V \psi$. □

The following lemma asserts that if a term s (a substitution σ) is embedded into a term t (a substitution τ) then their instances are embedded too, that is, the relation $\trianglelefteq$ is right composable with substitutions.

Lemma 19. *Let s, t be terms and let σ,τ, and λ be a substitution. Then*
(1) For all λ, if $s \trianglelefteq t$, then $s\lambda \trianglelefteq t\lambda$
(2) For all λ, if $s \trianglelefteq_E t$, then $s\lambda \trianglelefteq_E t\lambda$
(3) For all λ, if $\sigma \trianglelefteq_E \tau$, then $\sigma\lambda \trianglelefteq_E \tau\lambda$

Proof. (1) $s \trianglelefteq t$ implies $s\lambda \trianglelefteq t\lambda$:
By Definition 2.(4), we have three cases:
(i) $s = t$ is trivial.
(ii) Let $t = f(t_1, \ldots, t_n)$ and $s \trianglelefteq t_j$ for some $j \leq n$.
Now $t\lambda = f(t_1, \ldots, t_n)\lambda = f(t_1\lambda, \ldots, t_n\lambda)$. Since t_j is smaller than t we
obtain by an inductive argument that $s\lambda \trianglelefteq t_j\lambda$. Hence, $s\lambda \trianglelefteq t\lambda$.
(iii) Let $s = f(s_1, \ldots, s_n)$ and $t = f(t_1, \ldots, t_n)$ with $s_1 \trianglelefteq t_1$, ..., $s_n \trianglelefteq t_n$.
We have $s\lambda = f(s_1\lambda, \ldots, s_n\lambda)$ and $f(t_1\lambda, \ldots t_n\lambda) = t\lambda$ and again by an inductive
argument, we obtain $s_i\lambda \trianglelefteq t_i\lambda$ for $1 \leq i \leq n$.
Hence, $s\lambda \trianglelefteq t\lambda$.
(2) This is shown using the $\trianglerighteq_E$-chain of Lemma 11 $t \overset{n}{\blacktriangleright}_E s$,
that is, there is a $\triangleright_E$-chain $t =_E t_1 \triangleright t_1' =_E t_2 \triangleright \ldots\ldots \triangleright t_n' =_E s$.
Applying assertion (1) of this lemma to every element of the chain yields:
$t =_E t_1 \Longrightarrow t\lambda =_E t_1\lambda$, $t_1 \triangleright t_1' \Longrightarrow t_1\lambda \triangleright t_1'\lambda$, ..., $t_n' =_E s \Longrightarrow t_n'\lambda =_E s\lambda$.
Combining these into one chain yields: $t\lambda =_E t_1\lambda \triangleright t_1\lambda =_E t_2\lambda \triangleright \ldots\ldots t_n\lambda =_E s\lambda$.
Hence, $t\lambda \trianglerighteq_E s\lambda$, resp. $s\lambda \trianglelefteq_E t\lambda$.
(3) By Definition 16.(4) $\sigma \trianglelefteq_E \tau$: $\forall x \in \mathbf{Dom}(\sigma) = \mathbf{Dom}(\tau) : x\sigma \trianglelefteq_E x\tau$ and since
these are terms, we have with 19(2) that $\forall x \in \mathbf{Dom}(\sigma) = \mathbf{Dom}(\tau) : x\sigma\lambda \trianglelefteq_E x\tau\lambda$
and thus $\sigma\lambda \trianglelefteq_E \tau\lambda$. □

The next theorem shows that instance E-embedding is also a quasi-order on first-order terms.

Theorem 20. *The λ_E-embedment order $\geqslant_E$ is a quasi-order on terms.*

Proof. Let r, s, t be terms:
reflexivity: is obvious because every term λ-embeds itself.
transitivity: we show $t \geqslant_E s \geqslant_E r$ implies $t \geqslant_E r$.
By Definition 12, we have:
$s \geqslant_E r$ implies $\exists\sigma : s \trianglerighteq_E r\sigma$ and $t \geqslant_E s$ implies $\exists\tau : t \trianglerighteq_E s\tau$.
Furthermore with Lemma 20 and Theorem 14:
$s \trianglerighteq_E r\sigma \Longrightarrow \exists m : s \overset{m}{\blacktriangleright}_E r\sigma$ and $t \trianglerighteq_E s\tau \Longrightarrow \exists n : t \overset{n}{\blacktriangleright}_E s\tau$.
By Lemma 19 $\blacktriangleright$ is substitution-composable from the right, hence we have
$s\tau \overset{m}{\blacktriangleright}_E r\sigma\tau$, which implies $t \overset{n}{\blacktriangleright}_E s\tau \overset{m}{\blacktriangleright}_E r\sigma\tau$.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

Using the transitivity of $\trianglerighteq_E$ we get: $t \overset{n+m}{\blacktriangleright_E} r\sigma\tau$ and hence $t \trianglerighteq_E r(\sigma\tau)$,
that is $t \gtrdot_E r$. □

Using Theorem 20, we can now show that instance E-embedding of terms lifted to substitutions is also a quasi-order:

Theorem 21. *The λ_E-embedment order $\gtrdot_E$ is a quasi-order on substitutions.*

Proof. reflexivity: is a trivial consequence with the identity substitution ε: $\sigma\varepsilon \gtrdot_E \sigma$
transitivity: $\tau \gtrdot_E \sigma \gtrdot_E \varrho$ implies $\tau \gtrdot_E \varrho$
By Definition 16.(5), we have: $\sigma \gtrdot_E \varrho$ implies $\exists\lambda : \sigma \trianglerighteq_E \varrho\lambda$ and $\tau \gtrdot_E \sigma$ implies
$\exists\delta : \tau \trianglelefteq_E \sigma\delta$. Hence, by Lemma 19.(3) on the components of σ and ϱ
we have $\sigma\delta \trianglerighteq_E \varrho(\lambda\delta)$, which implies by definition $\tau \gtrdot_E \varrho$. □

The following definition lists some well-known notions (see Kruskal (1960) and Nash-Williams (1963)) on quasi-orderings, which we shall use later on.

Definition 22. Let $\leq$ be a quasi-ordering on a set S, then:

(1) An infinite sequence of elements of S, $a_1, a_2, a_3, \ldots$ is called a $\leq$*−chain* if $a_i \leq a_{i+1}$ for all $i \geq 1$. The sequence $a_1, a_2, a_3, \ldots$ is said to *contain a chain* if it has a subsequence that is a chain.
(2) The infinite sequence $a_1, a_2, a_3, \ldots$ is called an *anti-chain* if neither $a_i \leq a_j$ nor $a_j \leq a_i$, for all $1 \leq i < j$.
(3) The quasi-ordering $\leq$ is *well-founded* (wfo) if it contains no infinite strictly descending $<$-chain; that is, there is no infinite sequence $a_1, a_2, a_3, \ldots$ of elements of S such that $a_i > a_{i+1}$ for every i *in* $\mathbb{N}$.
(4) A *well-quasi-ordering on S* (wqo), $\leq$, is a quasi-ordering which is well-founded and it has no infinite anti-chains in S with respect to $\leq$.

Lemma 23. *Let E be an equational theory and let $t_1 \gtrdot_E t_2 \gtrdot_E t_3 \gtrdot_E \ldots$ be an infinitely descending $\gtrdot_E$-chain of terms $t_i, 1 \leq i$. Then there exists an infinitely descending $\trianglerighteq_E$-chain of instances of t_i with corresponding instantiating substitutions σ_i: $t_1 \trianglerighteq_E t_2\sigma_2 \trianglerighteq_E t_3\sigma_3 \trianglerighteq_E t_4\sigma_4 \trianglerighteq_E \ldots$, where the σ_i are composed from the σ_k for $1 \leq k \leq i$.*

Proof. By Definition 12, we have $t_1 \gtrdot_E t_2 \Longrightarrow \exists\lambda_2 : t_1 \trianglerighteq_E t_2\lambda_2$
and $t_2 \gtrdot_E t_3 \Longrightarrow \exists\lambda_3 : t_2 \trianglerighteq_E t_3\lambda_3$.
With Lemma 19.(2), we get $t_2\lambda_2 \trianglerighteq_E t_3\lambda_3\lambda_2$. Hence, $t_1 \trianglerighteq_E t_2\lambda_2 \trianglerighteq_E t_3\lambda_3\lambda_2$.
Now we have the following induction hypotheses: with $\sigma_2 := \lambda_2$ and for $n > 2$
$t_1 \gtrdot_E t_2 \gtrdot_E t_3 \gtrdot_E \ldots \gtrdot_E t_n \Longrightarrow \exists\lambda_i : t_1 \trianglerighteq_E t_2\lambda_2 \trianglerighteq_E t_3\lambda_3\lambda_2 \trianglerighteq_E \ldots \trianglerighteq_E t_n\lambda_n\lambda_{n-1}\lambda_{n-2}\ldots\lambda_2$
For more readability, let us use the following notation:
(*1) $\sigma_1 := \varepsilon, \sigma_2 := \lambda_2, \sigma_3 := \lambda_3\lambda_2$, that is: $\sigma_i := \lambda_i\sigma_{i-1}, i \geq 2$.
Now by induction.
$n = 2 : t_1 \gtrdot_E t_2 \Longrightarrow \exists\lambda_2 : t_1 \trianglerighteq_E t_2\lambda_2$ and using (*1) we have: $t_1 \trianglerighteq_E t_2\sigma_2$
$n \to n+1$: by induction hypotheses there exist substitutions $\lambda_2, \lambda_3, \ldots, \lambda_n$
such that $t_1 \trianglerighteq_E t_2\sigma_2 \trianglerighteq_E t_3\sigma_3 \trianglerighteq_E \ldots \trianglerighteq_E t_n\sigma_n$, where $\sigma_i := \lambda_i\sigma_{i-1}, i \geq 2$,
as notated in (*1).
Now at the tail of the chain, we have $t_n \gtrdot_E t_{n+1}$ and by Definition 12 there is a
substitution λ_{n+1}, such that $t_n \trianglerighteq_E t_{n+1}\lambda_{n+1}$. Moreover with Lemma 19.(2) :
$t_n\sigma_n \trianglerighteq_E t_{n+1}\lambda_{n+1}\sigma_n$, and using notation (*1): $t_n\sigma_n \trianglerighteq_E t_{n+1}\sigma_{n+1}$.
Hence in the limit we obtain $t_1 \trianglerighteq_E t_2\sigma_2 \trianglerighteq_E t_3\sigma_3 \trianglerighteq_E \ldots$. □

The following ***Tree Theorem*** was first proposed as a hypothesis by A. Vázsonyi and proved by Kruskal (1960, 1972), and later with a more elegant proof by Nash-Williams (1963). It states

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

that the set of finite trees over a well-quasi-ordered set of labels is itself well-quasi-ordered under homeomorphic embedding. Kruskal uses a notation, where T(Y) denotes the collection of all (structured) trees over an alphabet Y.

Theorem 24. ***The Tree Theorem.***
If Y is well-quasi-ordered, then T(Y) is well-quasi-ordered too.

The following theorem is a consequence of the tree theorem for the set of first-order terms $T(F, X)$, built over a finite signature F and a finite set of variable symbols X. Hereby, we refer to the work of Gallier (1991), whose terminology we like to use. He proves that "Given a finite alphabet $\Sigma = F \cup X$ which is well quasi ordered then $\trianglerighteq$ is also a well quasi order on $T(F, X)$" and the next theorem is a generalization to "modulo E." In the following, we assume that Σ is well-quasi-ordered.

Theorem 25. *Let E be an equational theory. The E-embedding quasi-order $\trianglerighteq_E$ is a well-quasi-order on the set of terms built over a* ***finite*** *alphabet $\Sigma = F \cup X$.*

Proof. (i) $\trianglerighteq_E$ is *well founded.*
If not, then there exists an infinite strictly descending $\triangleright_E$ −chain over a finite alphabet: $t_1 \triangleright_E t_2 \triangleright_E t_3 \triangleright_E \ldots$.
From this chain, we obtain the (sub-) sequence $s_1, s_2, s_3, \ldots$ where each s_i corresponds to some t_j with $s_i =_E t_j$.
Then by the tree embedding theorem, there are indices $i < j$ such that $t_i \trianglelefteq t_j$.
(see Gallier (1991) for this formulation).
But $t_i \trianglelefteq t_j$ implies in particular $t_i \trianglelefteq_E t_j$ and hence contradicts that there is a strictly descending $\triangleright_E$ −chain.
(ii) There are *no infinite anti-chains* with respect to $\trianglerighteq_E$.
The argument is in the same spirit by contradiction, reducing $\trianglerighteq_E$ to $\trianglerighteq$. □

Theorem 26. *Let E be an equational theory. The λ_E−embedding quasi-order $\leqslant_E$ is a well-quasi-order on the set of terms built over a* ***finite*** *alphabet $\Sigma = F \cup X$.*

Proof. Similar to Theorem 25.[3] □

E-unification of first-order terms is based on an *infinite* set of variable symbols and it is well known that the embedding order of terms with an infinite set of variable symbols is not a well-quasi-order, since we have the anti-chain $x_1, x_2, x_3, \ldots$. Of course the same is the case then for embedment modulo E.
But *well foundedness* of the syntactic embedding ordering is valid, since the number of symbols decreases in a strictly descending syntactic $\triangleright$ −chain. This well-known fact is stated in the next proposition.

Proposition 27. *In a strictly descending $\triangleright$ −chain the number of occurrences of symbols decreases.*

Our interest in this paper is the extension to equational theories. But with an infinite set of variables Proposition 27 is not applicable, since in an infinite strictly decreasing $\trianglerighteq_E$-chain the number of occurrences of symbols could increase. So one would conjecture that the E-embedding order is not a well-founded order (WFO). Unfortunately, we have yet no proof either way.

For an infinite set of variable symbols, we have to look for appropriate constraints on the equational theory E and a possible candidate is that for a term t the total number of variable symbols in $[t]_E$ is finite. This is achieved by requiring that every axiom $l = r$ in E has the property, that $\mathbf{Var}(l) = \mathbf{Var}(r)$, a class of theories called *regular* theories.

Lemma 28. *Let E= $\{l_1 = r_1, l_2 = r_2, \ldots, l_k = r_k\}$ be a* ***regular*** *equational theory, that is for each $i \in \{1, \ldots, n\}$: $\mathbf{Var}(l_i) = \mathbf{Var}(r_i)$. For any term $t \in T(F, X)$, the total number of variable symbols in the equational class $[t]_E$ is finite.*

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

Proof. Consider $t' \in [t]_E$ and a number $n \geqq 1$ of rewrite steps $t \overset{n}{\longrightarrow}_E t'$.
Then for every rewrite step: $t_i \longrightarrow_{l_i \to r_i} t_{i+1}$ or $t_i \longrightarrow_{r_i \to l_i} t_{i+1}$
there is a substitution λ_i such that $l_i\lambda_i$ (or $r_i\lambda_i$) is a subterm of t_i,
$l_i\lambda \preceq t$ (or $l_i\lambda \preceq t$) and t_{i+1} is the result of replacing $l_i\lambda$ by $r_i\lambda$ (or $r_i\lambda$ by $l_i\lambda$).
But since $\mathbf{Var}(l_i) = \mathbf{Var}(r_i)$ this cannot introduce new variables in t_{i+1} and
hence $\mathbf{Var}(t') \subseteq \mathbf{Var}(t)$. □

Well foundedness of E-embedding is now an easy consequence.

Theorem 29. *Let E be a **regular** equational theory. E-embedding $\trianglerighteq_E$ is a well-founded quasi-order on the set of terms.*

Proof. If not, then there exists an infinite strictly descending $\triangleright_E$-chain
$t_1 \triangleright_E t_2 \triangleright_E t_3 \ldots \triangleright_E t_i \triangleright_E \ldots\ldots$
With Definition 10 and Lemma 11, this chain has the form:
$t_1 =_E t_1' \overset{n_1}{\blacktriangleright}_E t_2 =_E t_2' \overset{n_2}{\blacktriangleright}_E t_3 =_E t_3' \overset{n_3}{\blacktriangleright}_E t_4 \ldots\ldots$ which consists of E-variants of embedded terms. Now with Lemma 28 and $W := \mathbf{Var}(t_1) \cup V_E$ we have,
that for all terms $\hat{t}$, which appear in the chain: $Var(\hat{t}) \subseteq W$.
But then all elements of the chain and its E-equivalents are built over a *finite* alphabet. Hence by Theorem 25, the $\trianglerighteq_E$ ordering is well founded. □

The next theorem is similar and shows that λ_E-embedding preserves well foundedness.

Theorem 30. *Let E be a **regular** equational theory. λ_E–embedding $\trianglerighteq_E$ is a well-founded quasi-order on the set of terms.*

Proof. If not, then there is an infinite strictly descending $\rhd_E$-chain
$t_1 \rhd_E t_2 \rhd_E t_3 \ldots \rhd_E t_i \rhd_E \ldots\ldots$
By Lemma 23, there exists a corresponding infinite strictly descending
$\triangleright_E$-chain $t_1 \triangleright_E t_2\sigma_2 \triangleright_E t_3\sigma_3 \triangleright_E t_4\sigma_4 \triangleright_E \ldots$. contradicting Theorem 29.

□

3. Ordering E-unifiers under homeomorphic embedding

We shall now look at unification under λ_E-embedding, which is our main interest in this paper, and we start with a recapitulation of the standard notions of E-unification.

3.1 E-*Unification*

Let E be an equational theory and let F be the signature of the term algebra. An *E-unification problem* is a finite set of equations

$$\Gamma = \{s_1 \stackrel{?}{=}_E t_1, \ldots, s_n \stackrel{?}{=}_E t_n\}$$

Let V denote the set of variables in Γ, $V = \mathbf{Var}(\Gamma)$. An *E-unifier* for Γ is a substitution σ such that

$$s_1\sigma =_E t_1\sigma, \ldots, s_n\sigma =_E t_n\sigma$$

The set of all E-unifiers of Γ is denoted $\mathcal{U}\Sigma_E(\Gamma)$. A *complete* set of E-unifiers $\mathcal{CU}\Sigma_E(\Gamma)$ for Γ is a set of E-unifiers, such that for every E-unifier τ there exists $\sigma \in \mathcal{CU}\Sigma_E(\Gamma)$ with $\sigma \leq_E^V \tau$. The set $\mu\mathcal{U}\Sigma_E(\Gamma)$ is called a *minimal complete set* of E-unifiers for Γ, if it is complete and for all distinct elements σ and σ' in $\mu\mathcal{U}\Sigma_E(\Gamma)$ if $\sigma \leq_E^V \sigma'$ then $\sigma =_E^V \sigma'$.

When a minimal complete set of E-unifiers of a unification problem Γ exists, it is unique up to E-subsumption equivalence $\sim_E^V$. Minimal complete sets of E-unifiers need not always exist, and if they do, they might be singular, finite, or infinite. Since minimal complete sets of E-unifiers

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

are isomorphic whenever they exist, they can be used to classify theories with respect to their corresponding unification problem. This leads naturally to the concept of a *unification hierarchy*, see Siekmann (1989), Knight (1989), Gallier (1991), Baader and Siekmann (1994), and Baader and Snyder (2001) for the standard surveys on this aspect.

A unification problem Γ is

- *nullary*, if Γ is unifiable, but the minimal complete set of E-unifiers does not exist.
- *unitary*, if it is not nullary and the minimal complete set of E-unifiers for Γ is of cardinality less than or equal to 1.
- *finitary*, if it is not nullary and the minimal complete set of E-unifiers is always finite.
- *infinitary*, if it is not nullary and the minimal complete set of E-unifiers is infinite.

An equational theory E is

- *unitary*, if all unification problems for E are unitary
- *finitary*, if all unification problems are finitary.
- *infinitary*, if there is at least one infinitary unification problem and all unification problems have minimal complete sets of E-unifiers.
- If there exists a solvable unification problem Γ not having a minimal complete set of E-unifiers, then the equational theory E is *nullary* or of *type zero*.

3.2 E-Unifiers ordered by homeomorphic embedding

The essential problem in unification theory is to determine the relationship between the solutions of term equations. In other words: what is the structure of the solution space?

In the case of syntactic unification, the *structural relationship* between the unifiers is based on the fact that terms form a lattice under the subsumption order, that is, there is a least upper bound and a max lower bound. Hence, if a unification problem is solvable, then there is a single *most general unifier*. But for unification under an equational theory the answer is not as easy, because:

– the complete set of most general unifiers is mostly infinite

– the complete set of most general unifiers may not even exist for a solvable E-unification problem.

So the search for an order relation better than subsumption comes naturally. Our first idea was based on the observation that certain solutions contain the instances of other solutions as a *sub-structure*. We captured this idea technically with the *encompassment order* on terms and substitutions, which led to the notion of *an E-essential unifier*[4]. Sub-structure means, in this case, that a unifying substitution encompasses other unifiers and hence they need not necessarily be part of the new set that represents all solutions. Unfortunately, the encompassment order is not a wqo either and hence there are equational theories for which there are solvable E-unification problems, but the minimal and complete set of essential E-unifiers does not exist, so they are E-*nullary w.r.t. encompassment* (Baader, 1988; Hoche, 2016; Szabo et al., 2016).

This paper is based on the observation that certain solutions *embed* the instances of other solutions in the sense of the *homeomorphic tree embedding theorem* or Kruskal's theorem. That is, the components of a unifying substitution embed the components of another unifying substitution. This then leads to the notion of *free (instance embedment-) E-unifiers,* free λ_E-unifiers, where these free λ_E-unifiers are the candidates of our new minimal and complete set of unifiers, which we name $\varphi U \Sigma_E(\Gamma)$.

Definition 31. Let E be an equational theory, Γ be a solvable E-unification problem, and $\mathcal{U}\Sigma_E(\Gamma)$ be the set of all E-unifiers for Γ. If an E-unifier σ in $\mathcal{U}\Sigma_E(\Gamma)$ does *not* have any λ_E-embedded

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

unifier, then σ is called a *free* λ_E*-unifier*. If the set of free λ_E-unifiers is *complete*, it will be denoted as $\varphi\mathcal{U}\,\Sigma_E(\Gamma)$.

Since homeomorphic embedding is not a well-quasi-order on the set of terms with infinitely many variable symbols, we cannot use Theorem 25. But for all practical purposes it may be possible for an automated deduction system to set a limit to the number of new variables and the theorem may still be useful in that case.

Nevertheless, the infinite sequence of variables $x_1, x_2, x_3, \ldots$. is normally used as a case in point that we have an anti-chain and hence Kruskal's theorem cannot be applied. But for the instance embedding order $\geqslant_E$ this is not the case: For example, x_1 instance embeds x_2 with the instantiating substitution $\lambda = \{x_2 \to x_1\}$. So there is the open problem whether or not the λ_E-embedding is a well-quasi-order. Unfortunately, currently we have neither a counter example nor a proof – so we state it here as an:

Open problem: Is the $\geqslant_E$-order a WQO even for an infinite number of variables?

For the rest of the paper, we shall also employ a standard technique used in the quest for termination proofs in logic programming Leuschel (1998, 2002) as well as termination of term rewriting systems Dershowitz and Jouannaud (1990), namely to disregard the name of a variable and simply treat all variables as the same. In other words, the unification procedure processes them as if they were embedment equivalent. This observation leads to the notion of *pure embedding,* which we abbreviate to π*-embedding* in the following and denote it as $t \trianglerighteq^{\pi} s$. As before, we generalize embedding to *pure instance embedding* or λ^{π}-embedding by saying a term s is λ^{π}*-embedded* into a term t, if it is λ-embedded and in addition all variables are embedding equivalent. It is defined (almost identical to Definition 2.(4), Definition 5 and 10) as follows:

Definition 32. (*Pure embedding*, π–embedding)

(1) A term t π*-embeds* a term s if:

$$t \trianglerighteq^{\pi} s \iff \begin{cases} s = t \text{ or } s, t \in X \text{ or} \\ t = f(t_1, \ldots, t_n) \text{ and for some } i,\ 1 \leq i \leq n,\ t_i \trianglerighteq^{\pi} s, \text{ or} \\ t = f(t_1, \ldots t_n),\ \ s = f(s_1, \ldots s_n) \text{ and } \forall i:\ t_i \trianglerighteq^{\pi} s_i,\ 1 \leq i \leq n. \end{cases}$$

(2) A term s is *instance* π*-embedded* (λ^{π}-embedded) into a term t, denoted $s \lessdot^{\pi} t$, if there is an instantiating substitution λ such that $s\lambda$ is π-embedded into t: $s\lambda \trianglelefteq^{\pi} t$. We also say that s is λ^{π}*-embedded* into t.

(3) A term t π_E*-embeds* a term s modulo E, denoted $t \trianglerighteq^{\pi}_E s$, if s and t are variables, or $s =_E t$, or there is a term $s' =_E s$ and a term $t' =_E t$ and there is an **embedded** term p in $\mathbf{Emb_E}(t')$ such that $p \triangleright^{\pi} s'$. More precisely:

$$t \trianglerighteq^{\pi}_E s \iff \begin{cases} s =_E t,\ \text{or } s, t \in X \text{ or} \\ \exists t' \in [t]_E, s' \in [s]_E \text{ and } \exists p \in \mathbf{Emb_E}(t') : p \triangleright^{\pi} s' \end{cases}$$

(4) Similar to Definition 10 and Definition 12, we define that a term s is instance π*-embedded modulo* E (λ^{π}_E-embedded) into a term t, $s \lessdot^{\pi}_E t$.

(5) A substitution σ is π*-embedded into a substitution* τ *for a set of variables* V, denoted as $\sigma \lessdot^{V}_{\pi} \tau$, iff $V \subseteq \mathbf{Dom}(\sigma)$ and $\forall x \in V : x\sigma$ is π–embedded into $x\tau$.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

(6) A substitution σ is *instance π–embedded modulo E (λ_E^π-embedded) into a substitution τ for a set of variables V*, denoted as $\sigma \preccurlyeq_{\pi,E}^{V} \tau$, iff $V \subseteq \mathbf{Dom}(\sigma)$ and there is a substitution λ, such that $\forall x \in V : x(\sigma\lambda)$ is π-embedded into $x\tau$.

π_E-embedding and λ_E^π-embedding are special cases of E-embedding and λ_E-embedding, so we can use Theorem 25 using the fact that we now have only one variable (see also Leuschel (1998)):

Corollary 33. *π_E-embedding and λ_E^π-embedding are well-quasi-orders on the set of terms.*

In order to show the results below, we recall some well-known notions originally found in Higman (1952) and Nash-Williams (1963) and others, but now restricted to first-order terms (Gallier, 1991). Moreover, we define that a list of terms $l_1 = (s_1, s_2, s_3, ..., s_n)$ is λ_E-embedded (is λ_E^π-embedded) into a list of terms $l_2 = (t_1, t_2, t_3, ..., t_n)$, $n \geq 1$, if there is an instantiating substitution σ, such that $l_1\sigma$ is E-embedded into l_2. That is every component $s_i\sigma$ of the list l_1 is E-embedded into the component t_i of the list l_2 *for* $1 \leqslant i \leqslant n$.
In the following proofs, we use two standard notions:

Definition 34. (good and bad sequences)

(1) A sequence of terms $t_1, t_2, t_3, ...$ is called ***good***, if there are indices i, j, and $i < j : t_i \trianglelefteq t_j$ otherwise it is called ***bad***. A well-quasi-ordering (wqo) is a quasi-ordering over which every infinite sequence is good.
(2) Let $l_1 := (s_1, s_2, s_3, ...s_n), l_2 := (t_1, t_2, t_3, ...t_n)$ be lists of terms (of equal length). Then l_1 is embedded into l_2, $l_1 \trianglelefteq l_2$, iff $s_i \trianglelefteq t_i$, $1 \leqq i \leqq n$.

Since a substitution is in fact a list of terms labeled with a variable, we have:

Lemma 35. *Let $T(F, X)$ be a well-quasi-ordered set of terms with respect to term-embedding $\trianglelefteq$. Then every infinite sequence of terms $t_1, t_2, t_3, ...$ has an infinite ascending sub-sequence, ($\trianglelefteq$-chain), $t'_1 \trianglelefteq t'_2 \trianglelefteq t'_3, ...$*

Proof. See the proof in, for example, Nash-Williams (1963) and Gallier (1991) □

This lemma can now be extended to equational embedding:

Corollary 36. *Let $T(F, X)$ be a well-quasi-ordered set of terms and E an equational theory. Then every infinite sequence of terms $t_1, t_2, t_3, ...$ has an infinite ascending sub-sequence, ($\trianglelefteq_E$-chain), $t'_1 \trianglelefteq_E t'_2 \trianglelefteq_E t'_3 \trianglelefteq_E .....$*

Proof. See Gallier (1991) where this is proved in a more general setting. □

Lemma 37. *Let $T(F, X)$ be a well founded, resp. a well-quasi-ordered set of terms with respect to embedding. Then the set of finite lists of terms $T(F, X)^\omega$ is also well founded, resp. well-quasi-ordered.*

Proof. See the proof in Nash-Williams (1963), Gallier (1991), and Singh et al. (2013). □

The following lemma lifts the previous results from terms to substitutions and note we have only a finite set of variables, since the terms are wqo:

Lemma 38. Let $T(F, X)$, where X is finite, be a well-quasi-ordered set of terms with respect to E-embedding, then the set of substitutions $\mathcal{S}_{F,X}$ is also well-quasi-ordered.

Proof. A substitution can be seen as a list of terms, so by induction on the size of the associated lists.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

n = 1: If $T(F, X)$ is wqo, then for every infinite sequence of substitutions
with a single component $\sigma_1 = \{x \to s_1\}, \sigma_2 = \{x \to s_2\}, \sigma_3 = \{x \to s_3\}, ...$
the associated sequence of lists is $l_1, l_2, ..., l_i, ...$ where $l_i = (s_i)$, $i \geq 1$
and the corresponding infinite sequence is $s_1, s_2, s_3, ...$
Now because $s_1, s_2, s_3, ...$ is good, that is there exists an $i, j, i < j$: $s_i \trianglelefteq_E s_j$
the sequence $l_1, l_2, l_3, ...$ is also good. Consequently, $\sigma_1, \sigma_2, \sigma_3, ...$ is good.
n → n + 1 : By induction hypothesis $\sigma_1, \sigma_2, \sigma_3, ...$
with $\sigma_i = \{x_1 \to s_{i1}, x_2 \to s_{i2}, ..., x_n \to s_{in}\}$ has the associated sequences of lists
$l_1, l_2, ..., l_i, ...$ with $l_i = (s_{i1}, s_{i2}, ..., s_{in})$ which is good and therefore
$\sigma_1, \sigma_2, \sigma_3, ...$ is also good.
Now Lemma 35 can be used, which says that there exists an infinite ascending
E-embedding sub-chain $l'_1 \trianglelefteq_E l'_2 \trianglelefteq_E l'_3 \trianglelefteq_E ... \trianglelefteq_E l'_i \trianglelefteq_E ...$ where $l'_i = (s'_{i1}, s'_{i2}, ..., s'_{in})$.
Looking now for lists with size $n + 1$ we have a similar list but with
$l'_i = (s'_{i1}, s'_{i2}, ..., s'_{in}, s'_{in+1})$, $i \geq 1$ and its ascending $\trianglelefteq_E$-subchain
$l'_1 \trianglelefteq_E l'_2 \trianglelefteq_E l'_3 \trianglelefteq_E ....$
Now because $T(F, X)$ is a wqo set w.r.t. E-embedding, the corresponding infinite sequence consisting of the $n + 1$'th members, $s'_{1n+1}, s'_{2n+1}, ..., s'_{in+1}, ...$ must be good; therefore, there are indices i', j' such that $s'_{i'n+1} \leq s'_{j'n+1}$ which implies $l'_{i'} = (s'_{i'1}, s'_{i'2}, ..., s'_{i'n+1}) \trianglelefteq_E l'_{j'} = (s'_{j'1}, s'_{j'2}, ..., s'_{j'n+1})$, hence $l'_1, l'_2, l'_3, ...$is good. So if we assume that $l_1, l_2, l_3, ...$ is bad then $\sigma_1, \sigma_2, \sigma_3, ...$ is also bad, **but** the infinite subsequence $l'_1, l'_2, l'_3, ...$ is good; therefore, $l_1, l_2, l_3, ...$ must also be good from which follows that $\sigma_1, \sigma_2, \sigma_3, ...$ is also good. Hence, $\mathcal{S}_{F,X}$ is a well-quasi-ordered set. □

The proofs for our various E-embeddings on substitutions are almost identical to those in Lemma 38; hence, we collect them in one lemma:

Lemma 39. *Let* $T(F, X)$, where X is finite, be a well-quasi-ordered set of terms with respect to λ_E-embedding, π_E*-embedding and* λ^{π}_E*-embedding* then the set of substitutions $\mathcal{S}_{F,X}$ is also a well-quasi-ordered set with respect to these embeddings.

The results so far, namely the (homeomorphic) embedding of first-order terms and substitutions extended to various *equational embeddings*, namely E-embedding ($\trianglelefteq_E$), instance E-embedding ($\lessdot_E$), pure E-embedding ($\trianglelefteq^{\pi}_E$), and pure instance E-embedding ($\lessdot^{\pi}_E$) can now be used to show the following properties for the set of E-unifiers, more importantly for the set of minimal E-unifiers, which is of course our main interest.

Theorem 40. *Let T(F,X) be the set of first-order terms and E a* ***regular*** *equational theory. Then for a solvable E-unification problem* Γ*, the set of free* λ_E*-unifiers,* $\varphi U \Sigma_E(\Gamma)$ *always exists and it is minimal and complete (but not necessarily finite).*

Proof. T(F,X) is a well-founded quasi-order with respect to instance E-embedding as a consequence of Theorem 30 and Lemma 37. □

Definition 41. An E-unification problem Γ_E *is bounded* if there is a number N such that $U\Sigma_E(\Gamma)$ uses at most N variables. A *theory E is bounded* if every E-unification problem Γ_E is bounded.

If the alphabet is finite and Γ_E *is bounded*, we have the following stronger result[5]:

Theorem 42. *Let T(F, X) be the set of first-order terms built over a* ***finite*** *alphabet* $\Sigma = F \cup X$ *and let E be an equational theory. Then for a solvable* ***bounded*** *E-unification problem* Γ*, the set of free* λ_E*-unifiers,* $\varphi U \Sigma_E(\Gamma)$*, always exists, it is minimal, complete, and finite.*

Proof. A consequence of *the tree embedding theorem* extended to equational instance embedding. □

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

For our final result, let us say a *purified E-unification problem* is a problem where we define all variables as embedment equivalent. Let $\varphi_\pi U\Sigma_E(\Gamma)$ be the corresponding complete set of pure and free λ_E-unifiers, then:

Theorem 43. *Let T(F, X) be the set of first-order terms and let E be an equational theory, then for a solvable E-unification problem Γ the set of pure and free λ_E-unifiers, $\varphi_\pi U\Sigma_E(\Gamma)$ exists, it is minimal, complete, and finite.*

4. Conclusion and Future Work

This paper sets forth an abstract setting for equational unification problems, where we redefine the notion of the set of most general unifiers. We now have:

"Unification based on E-subsumption"
"Unification based on E-encompassment"
"Unification based on E-embedding"

where each approach is a generalization of the previous one. For terms s, t, and an instantiating substitution λ, this can be illustrated for the syntactic case as:

- $t \gg s$, that is *t instance embeds s,* is defined using homeomorphic embedding $\trianglerighteq$*:*

$$t \gg s \iff \exists\lambda : \begin{cases} s\lambda = t, \text{ or} \\ t = f(t_1, \ldots, t_n),\ i \in \{1, ..., n\} : t_i \trianglerighteq s\lambda \\ t = f(t_1, \ldots, t_n),\ s\lambda = f(s_1, \ldots, s_n) \\ \quad \text{and } \forall i : t_i \trianglerighteq s_i,\ 1 \le i \le n \end{cases}$$

- $t \sqsupseteq s$, that is *t encompasses s*, is defined by deleting the third line of the previous definition:

$$t \sqsupseteq s \iff \exists\lambda : \begin{cases} s\lambda = t, \text{ or} \\ t = f(t_1, \ldots, t_n),\ i \in \{1, ..., n\} : t_i \sqsupseteq s\lambda \end{cases}$$

- $t \geq s$, that is *t subsumes s*, is defined by deleting the second line of the previous definition:

$$t \geq s \iff \exists\lambda : s = t\lambda$$

Extending this to E-unification, we have the three notions: $\mu U\Sigma_E(\Gamma)$, the standard notion today, essential unification $eU\Sigma_E(\Gamma)$, and finally $\varphi U\Sigma_E(\Gamma)$ under homeomorphic embedding as presented in this paper. In a sequel to this paper, we will show how to compute the set $\varphi U\Sigma_E(\Gamma)$ and its closure and whether it can be used in an inference system like resolution.

Using this general framework, the next tasks are then to look again at the standard unification problems like associativity, commutativity, or idempotency and their combination as well as on the wealth of results about other algebras, in order to see what the potential practical (and theoretical) gains are. A first investigation into these practical problems has been made within the logic programming paradigm (Alpuente et al., 2018)[6]. As in the 1970s, when we started unification theory with a table listing the now standard unification problems in one column and in the adjacent column the type within the unification hierarchy, we could now have a similar table, but with an additional column for the type of $eU\Sigma_E(\Gamma)$ and $\varphi U\Sigma_E(\Gamma)$.

https://doi.org/10.1017/S0960129522000019 Published online by Cambridge University Press

Secondly, there is far more theoretical work needed to better understand the actual structure of and relationship between these unification settings and also how this work relates to similar results obtained within different theoretical settings, like those of Cabrer and Metcalfe (2014, 2015). Moreover how to relate all this to the wealth of theoretical results obtained by Ghilardi (1997) and his students (see, e.g., Ghilardi (2018)) and by Franz Baader (see, e.g., Baader and Ghilardi (2011)).

Acknowledgements. This paper has taken a very long time to take its present form. Starting from the basic observation that a subset of infinitely many most general unifiers more often than not share a basic structure until we came to the more theoretical characterization as presented here. We very much like to thank Michael Hoche who worked with us on earlier drafts of these ideas and we hope that he will soon recover and come back to us, in order to continue our joint work on the problems this paper left open. We also like to thank the referees of UNIF18 for their work and critical ideas. In particular, we like to thank the reviewers of this journal, who contributed substantially to the final formulation and shape of this paper. Not least, they found an embarrassing flaw in the previous version and pointed us to related work in the literature.

Notes

1 This notion is also used with a slightly different definition in *Alpuente et al. (2016)*.
2 Signs and notation are still not uniform in all related fields; our notation is used more often in the field of automated theorem proving and unification theory, whereas term rewriting systems usually prefer notational conventions as proposed in Dershowitz and Jouannaud (1990) and Dershowitz and Jouannaud (1991).
3 As one reviewer remarked, we could argue more abstractly that any quasi-order that extends a well-quasi-order is a well-quasi-order too Gallier (1991). Now, E-embedding and λ_E−embedding are quasi-orderings by Theorem 14 and Theorem 20 and $=_E$ is a quasi-order, hence follows the result of Theorem 25 and Theorem 26, but we feel an explicit proof shows the idea much better.
4 A general introduction to essential unification is presented in Szabo et al. (2016)
5 The notion of *boundedness* actually implies a finite alphabet, but unfortunately some unification problems require the use of infinitely many fresh variables.
6 These works have been brought to our attention, once our paper was finished and submitted, a possible cross fertilization and comparison warrants certainly more research.

References

Alpuente, M., Cuenca-Ortega, A., Escobar, S. and Meseguer, J. (2016). Partial evaluation of order-sorted equational programs modulo axioms. In: Hermenegildo M. and Lopez-Garcia P. (eds.) *Logic-Based Program Synthesis and Transformation, LOPSTR 2016*. Lecture Notes in Computer Science, vol. 10184. Springer.

Alpuente, M., Cuenca-Ortega, A., Escobar, S. and Meseguer, J. (2018). Homeomorphic embedding modulo combinations of associativity and commutativity axioms. In: *International Symposium on Logic-Based Program Synthesis and Transformation*. Springer, pp. 38–55.

Baader, F. (1988). A note on unification type zero. *Information Processing Letters* **27** 91–93.

Baader, F. and Ghilardi, S. (2011). Unification in modal and description logics. *Logic Journal of GPL* **19** (6).

Baader, F. and Nipkow, T. (1998). *Term Rewriting and all That*. Cambridge University Press.

Baader, F. and Siekmann, J. (1994). General unification theory. In: Gabbay, D., Hogger, C. and Robinson, J. (eds.) *Handbook of Logic in Artificial Intelligence and Logic Programming*. Oxford University Press, pp. 41–126.

Baader, F. and Snyder, W. (2001). Unification theory. In: Robinson, A. and Voronkov, A. (eds.) *Handbook of Automated Reasoning*, vol. 1. Elsevier Science Publishers.

Cabrer, L. M. and Metcalfe, G. (2014). From admissibility to a new hierarchy of unification types. *RISC 41,Linz*.

Cabrer, L. M. and Metcalfe, G. (2015). Exact unification and admissibility. *Logical Methods in Computer Science* **11** (3).

Dershowitz, N. (1982). Orderings for term-rewriting systems. *Theoretical Computer Science* **17**, 279–301.

Dershowitz, N. (1987). Termination of rewriting. *Journal of Symbolic Computation* **3** (1) 69–115.

Dershowitz, N. and Jouannaud, J.-P. (1990). Rewrite systems. In: van Leeuwen, J. (ed.), *Handbook of Theoretical Computer Science*. Elsevier Science Publishers (North-Holland), , pp. 244–320.

Dershowitz, N. and Jouannaud, J.-P. (1991). Notations for rewriting. *Bulletin of the EATCS* **43**, 162–174.

Gallier, J. H. (1991). Unification procedures in automated deduction methods based on matings: A survey. Technical Report CIS-436, University of Pennsylvania, Department of Computer and Information Science.

Gallier, J. H. (1991). What's so special about Kruskal's theorem and the ordinal gamma0 ?: A survey of some results in proof theory. *Annals of Pure and Applied Logic* **53** (3) 199–260.

Ghilardi, S. (2018). Handling substitutions via duality. In: *Proceedings of the International Workshop on Unification Theory (UNIF32), FLoC2018, Oxford*.
Ghilardi, S. (1997). Unification through projectivity. *Journal of Logic and Computation* **7** (3).
Higman, G. (1952). Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society*, **3** (1) 326–336.
Hoche, M., Siekmann, J. and Szabo, P. (2008). String unification is essentially infinitary. In: Marin, M. (ed.) *The 22nd International Workshop on Unification (UNIF 2008)*, Hagenberg, Austria, pp. 82–102.
Hoche, M., Siekmann, J. and Szabo, P. (2016). String unification is essentially infinitary. *IFCoLog Journal of Logics and their Applications*.
Hoche, M. and Szabo, P. (2006). Essential unifiers. *Journal of Applied Logic* **4** (1) 1–25.
Knight, K. (1989). Unification: A multidisciplinary survey. *ACM Computing Surveys (CSUR)* **21** (1) 93–124.
Kruskal, J. B. (1960). Well-quasi-ordering, the tree theorem and Vázsonyi's conjecture. *Transactions of the American Mathematical Society* **95** 210–225.
Kruskal, J. B. (1972). The theory of well-quasi-ordering: A frequently discovered concept. *Journal of Combinatorial Theory* **13** 297–305.
Leuschel, M. (1998). Improving homeomorphic embedding for online termination. In: *International Workshop on Logic Programming Synthesis and Transformation*. Berlin, Heidelberg: Springer.
Leuschel, M. (2002). Homeomorphic embedding for online termination of symbolic methods. In: *The Essence of Computation*. Lecture Notes in Computer Science, vol. 2566. Berlin, Heidelberg: Springer.
Nash-Williams, C. St. J. A. (1963). On well-quasi-ordering finite trees. In: Green, B. J. (ed.) *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 59. *04*. Cambridge Philosophical Society, pp. 833–835.
Robinson, J. A. (1965). A machine-oriented logic based on the resolution principle. *Journal of the ACM* **12** (1) 23–41.
Siekmann, J. (1989). Unification theory. *Journal of Symbolic Computation* **7** (3 & 4) 207–274.
Singh, D., Shuaibu, A. M. and Ndayawo, M. S. (2013). Simplified proof of Kruskals tree theorem. *Mathematical Theory and Modeling* **3** (13) 93–100.
Szabo, P., Siekmann, J. and Hoche, M. (2016). What is essential unification? In: *Martin Davis on Computability, Computation, and Computational Logic*. Springer's Series "Outstanding Contributions to Logic".

Cite this article: Szabo P and Siekmann J (2021). E-Unification based on Generalized Embedding. *Mathematical Structures in Computer Science* **31**, 898–917. https://doi.org/10.1017/S0960129522000019