Combining Decision Procedures for Positive Theories Sharing Constructors

Franz Baader[1]
baader@informatik.rwth-aachen.de

Cesare Tinelli
tinelli@cs.uiowa.edu

Department of Computer Science
University of Iowa

Report No. 02-02

February 2002

[1]Address: Lehr- und Forschungsgebiet Theoretische Informatik, RWTH Aachen, Ahornstraße 55, 52074 Aachen, Germany.

Combining Decision Procedures for Positive Theories Sharing Constructors

Franz Baader
Lehr- und Forschungsgebiet Theoretische Informatik
RWTH Aachen
Ahornstraße 55, 52074 Aachen, Germany
baader@informatik.rwth-aachen.de

Cesare Tinelli
Department of Computer Science
University of Iowa
14 McLean Hall, Iowa City, IA 52242 – USA
tinelli@cs.uiowa.edu

February 2002

Abstract

This paper addresses the following combination problem: given two equational theories E_1 and E_2 whose positive theories are decidable, how can one obtain a decision procedure for the positive theory of $E_1 \cup E_2$? For theories over disjoint signatures, this problem was solved by Baader and Schulz in 1995. Our main new contribution is to extend this result to the case of theories sharing so-called constructors (and satisfying certain additional conditions). Since there is a close connection between positive theories and unification problems, this also extends to the non-disjoint case the work on combining decision procedures for unification modulo equational theories.

Keywords: Combination of positive theories, decision procedures, unification procedures.

Contents

1 Introduction

Built-in decision procedures for certain types of theories (like equational theories) can greatly speed up the performance of theorem provers. In many applications, however, the theories actually encountered are combinations of theories for which dedicated decision procedure are available. Thus, one must find ways of combining the decision procedures for the single theories into one for their combination. In the context of *equational theories over disjoint signatures*, this combination problem has thoroughly been investigated in the following three instances:[1] the word problem, the validity problem for universally quantified formulae, and the unification problem. For the word problem, i.e., the problem whether a single (universally quantified) equation $s \equiv t$ follows from the equational theory, the first positive solution to the combination problem was given by Pigozzi [Pig74] in 1974. The problem of combining decision procedures for universally quantified formulae, i.e., arbitrary Boolean combinations of equations that are universally quantified, was solved by Nelson and Oppen [NO79] in 1979. Work on combining unification algorithms also started in the seventies with Stickel's paper [Sti81] on unification of terms containing several associative-commutative and free symbols. The first general result on how to combine *decision procedures* for unification was published by Baader and Schulz [BS92] in 1992. It turned out that decision procedures for unification (with constants) are not sufficient to allow for a combination result. Instead, one needs decision procedures for unification *with linear constant restrictions* in the theories to be combined. In 1995, Baader and Schulz [BS95] described a modified version of their combination procedure that applies to *positive theories*, i.e., positive Boolean combinations of equations with an arbitrary quantifier prefix. They also showed [BS96] that the decidability of the positive theory is equivalent to the decidability of unification with linear constant restrictions.

Since then, the main open problem in the area has been how to extend these results to the combination of *theories having symbols in common*. In general, the existence of shared symbols may lead to undecidability results for the union theory (see, e.g., [DKR94, BT02] for some examples). This means that a controlled form of sharing of symbols is necessary. For the word problem and for universally quantified formulae, a suitable notion of *shared constructors* has turned out to be useful. In [BT02], Pigozzi's combination result for the word problem was extended to theories all of whose shared symbols are constructors. A similar extensions of the Nelson-Oppen combination procedure for universally quantified formulae can be found in [TR02].

[1] Actually, some of the work mentioned below can also handle more general theories. To simplify the presentation, we restrict our attention in this paper to the equational case.

In a similar vein, we show in this paper that the combination results in [BS95] for positive theories (and thus for unification) can be extended to theories sharing constructors. We do that by extending the combination procedure in [BS95] with an extra step that deals with shared symbols and proving that the extended procedure is sound, complete and, under some assumptions on the equational theory of the shared symbols, also terminating.

The paper is organized as follows. Section 2 contains some formal preliminaries. Section 3 defines our notion of constructors and presents some of their properties, which will be used later to prove the correctness of the combination procedure. Section 4 describes our extension of the Baader-Schulz procedure to component theories sharing constructors. It then shows under what conditions it is possible to use the procedure to decide the positive consequences of their union, and gives an example of a theory satisfying these conditions. Finally, it proves that the procedure is sound and complete. Section 5 concludes the paper with a comparison to related work and suggestions for further research.

2 Preliminaries

In this paper we will use standard notions from universal algebra such as formula, sentence, algebra, subalgebra, reduct, entailment, model, homomorphism and so on. Notable differences are reported in the following.

We will consider only first-order theories (with equality) over a functional signature. A *signature* Σ is a set of *function symbols*, each with an associated *arity*, an integer $n \geq 0$. A *constant* symbol is a function symbol of zero arity. We use the letters Σ, Ω, Δ to denote signatures. Throughout the paper, we fix a countably-infinite set V of *variables*, disjoint with any signature Σ. For any $X \subseteq V$, $T(\Sigma, X)$ denotes the set of Σ-*terms*, i.e., first-order terms with variables in X and function symbols in Σ. Formulae in the signature Σ are defined as usual. We use $\equiv$ to denote the equality symbol.

We also use the standard notion of substitution, with the usual postfix notation. We call a substitution a *renaming* iff it is a bijection of V onto itself. We say that a subset T of $T(\Sigma, V)$ is *closed under renaming* iff $t\sigma \in T$ for all terms $t \in T$ and renamings σ.

If A is a set, we denote by A^* the set of all finite tuples made of elements of A. If $\mathbf{a}$ and $\mathbf{b}$ are two tuples, we denote by $\mathbf{a}, \mathbf{b}$ the tuple obtained as the concatenation of $\mathbf{a}$ and $\mathbf{b}$. In general, if h is a map from a set A to a set B and $\mathbf{a} = (a_1, \ldots, a_n) \in A^*$ we denote by $h(\mathbf{a})$ the tuple $(h(a_1), \ldots, h(a_n)) \in B^*$.

If φ is term or a formula, we denote by $\mathcal{V}ar(\varphi)$ the set of φ's free variables. We will often write $\varphi(\mathbf{v})$ to indicate, as usual, that $\mathbf{v}$ is a tuple of variables with no repetitions and all elements of $\mathcal{V}ar(\varphi)$ occur in $\mathbf{v}$.

A formula is *positive* iff it is in prenex normal form and its matrix is obtained from atomic formulae using only conjunctions and disjunctions. A formula is *existential*, or an *$\exists$-formula*, iff it has the form $\exists \mathbf{u}\, \varphi(\mathbf{u}, \mathbf{v})$ where $\varphi(\mathbf{u}, \mathbf{v})$ is a quantifier-free formula.

If $\mathcal{A}$ is an algebra of signature Ω, we denote by A the universe of $\mathcal{A}$ and by $\mathcal{A}^{\Sigma}$ the reduct of $\mathcal{A}$ to a given subsignature Σ of Ω. If $a \in A$ and $X \subseteq A$ we say that a is *(Ω-)generated by X in $\mathcal{A}$* iff a is an element of the subalgebra of $\mathcal{A}$ generated by X; if B and X are sets or tuples of elements of A, we say that B is (Ω-)generated by X in $\mathcal{A}$ iff every element of B is Ω-generated in $\mathcal{A}$ by the elements of X. If $\varphi(\mathbf{v})$ is an Ω-formula and α is a valuation of $\mathbf{v}$ into A, we write $(\mathcal{A}, \alpha) \models \varphi(\mathbf{v})$ iff $\varphi(\mathbf{v})$ is satisfied by the interpretation $(\mathcal{A}, \alpha)$. Equivalently, where $\mathbf{a} = \alpha(\mathbf{v})$, we may also write $\mathcal{A} \models \varphi(\mathbf{a})$. If $t(\mathbf{v})$ is an Ω-term, we denote by $[\![t]\!]^{\mathcal{A}}_{\alpha}$ the interpretation of t in $\mathcal{A}$ under the valuation α of $\mathbf{v}$. Similarly, if T is a set of terms, we denote by $[\![T]\!]^{\mathcal{A}}_{\alpha}$ the set $\{[\![t]\!]^{\mathcal{A}}_{\alpha} \mid t \in T\}$. If $\mathbf{a} = \alpha(\mathbf{v})$, we may also write $t^{\mathcal{A}}(\mathbf{a})$ instead $[\![t]\!]^{\mathcal{A}}_{\alpha}$ when convenient.

A *theory* of signature Ω, or an Ω-theory, is any set of Ω-sentences, that is, of closed Ω-formulae. An algebra $\mathcal{A}$ is *a model of a theory $\mathcal{T}$*, or *models $\mathcal{T}$*, iff each sentence in $\mathcal{T}$ is satisfied by the interpretation $(\mathcal{A}, \alpha)$ where α is the empty valuation. Let $\mathcal{T}$ be an Ω-theory. We denote by $Mod(\mathcal{T})$ the set of all Ω-algebras that model $\mathcal{T}$. We say that $\mathcal{T}$ is *satisfiable* if it has a model, and *trivial* if it has only *trivial models*, that is, models of cardinality 1. For all sentences φ (of any signature), we say as usual that $\mathcal{T}$ *entails* φ, or that φ *is valid in* $\mathcal{T}$, and write $\mathcal{T} \models \varphi$, iff the theory $\mathcal{T} \cup \{\neg\varphi\}$ is unsatisfiable. We call *(existential) positive theory of $\mathcal{T}$* the set of all (existential) positive sentences that *have the signature of* $\mathcal{T}$ and are entailed by $\mathcal{T}$.

An *equational theory* is a set of (universally quantified) equations. We will mostly consider equational theories in this paper. If E is an equational theory of signature Ω and Σ is an arbitrary signature, we denote by E^{Σ} the set of all (universally quantified) Σ-equations entailed by E. Note that E and E^{Σ} are logically equivalent whenever $\Sigma = \Omega$. When $\Sigma \subseteq \Omega$ we call E^{Σ} the *Σ-restriction of E*. For all Ω-terms $s(\mathbf{v}), t(\mathbf{v})$, we write $s =_E t$ and say that s and t are *equivalent in E* iff $E \models \forall \mathbf{v}\; s \equiv t$.

Lemma 2.1 *Let $\mathcal{T}$ be any theory and γ any sentence in prenex normal form. Let $\hat{\gamma}$ be the $\exists$-sentence obtained from γ by Skolemizing its universal quantifiers. Then, $\mathcal{T} \models \gamma$ iff $\mathcal{T} \models \hat{\gamma}$.*

Proof. To prove the claim we show that $\mathcal{T} \cup \{\neg\gamma\}$ is satisfiable iff $\mathcal{T} \cup \{\neg\hat{\gamma}\}$ is satisfiable.

By the usual, well-known results about the satisfiability of Skolemized sets of formulae, we know that $\mathcal{T} \cup \{\neg\gamma\}$ $(\mathcal{T} \cup \{\neg\hat{\gamma}\})$ is satisfiable iff the set obtained by Skolemizing the existential quantifiers in every formula of $\mathcal{T} \cup \{\neg\gamma\}$ $(\mathcal{T} \cup \{\neg\hat{\gamma}\})$ is satisfiable. To prove our claim then it is enough to show that $\neg\gamma$ and $\neg\hat{\gamma}$ can be Skolemized into the same formula. But this is an easy consequence of the fact that $\neg\hat{\gamma}$'s prenex normal form is a universal formula and that all the existential variables in $\neg\gamma$'s prenex normal form are universal in γ's prenex normal form. □

We will later appeal to the two basic model theory results below about subalgebras (see [Hod93] among others).

Lemma 2.2 *Let $\mathcal{B}$ be a Σ-algebra and $\mathcal{A}$ a subalgebra of $\mathcal{B}$. For all quantifier-free formulae $\varphi(v_1, \ldots, v_n)$ and individuals $a_1, \ldots, a_n \in A$, $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ iff $\mathcal{B} \models \varphi(a_1, \ldots, a_n)$.*

Lemma 2.3 *For all equational theories E, the set $Mod(E)$ is closed under subalgebras.*

Similarly to [BS95], our procedure's correctness proof will be based on free algebras.

Definition 2.4 (Free Algebra) *Given a class $\mathbf{K}$ of Σ-algebras and a set X, a Σ-algebra $\mathcal{A}$ is* free for $\mathbf{K}$ over X *iff*

1. *$\mathcal{A}$ is generated by X;*
2. *every map from X into the universe of an algebra $\mathcal{B} \in \mathbf{K}$ extends to a (necessarily unique) homomorphism of $\mathcal{A}$ into $\mathcal{B}$.*

We say that $\mathcal{A}$ is free in $\mathbf{K}$ *over X (or free over X in $\mathbf{K}$) if $\mathcal{A}$ is free for $\mathbf{K}$ over X and $\mathcal{A} \in \mathbf{K}$. In either case, we call X a* basis *of $\mathcal{A}$.*

For convenience, given an equational Σ-theory E, we will say that $\mathcal{A}$ *is free in E over X*, if $\mathcal{A}$ is free in $Mod(E)$ over X. In that case, we will also say that $\mathcal{A}$ *is a free model of E (with basis X)*.[2] A Σ-algebra is *absolutely free* (over a set X) iff it is free (over X) in the empty Σ-theory, that is, in the theory consisting in an empty set of Σ-equations. We will implicitly appeal to following result, providing a sufficient condition for the existence of free models with countably infinite basis.

[2] Note that for $\mathcal{A}$ to be a free model of E it is not enough that $\mathcal{A}$ is a model of E free for some class. It must be free for the class $Mod(E)$.

Proposition 2.5 *Every non-trivial equational theory E admits a free model with a countably infinite basis.*[3]

Free models have the following well-known characterization (see, e.g., [Hod93]):

Proposition 2.6 *Let E be a Σ-theory and $\mathcal{A}$ a Σ-algebra. Then, $\mathcal{A}$ is free in E over some set X iff the following holds:*

1. *$\mathcal{A}$ is a model of E;*
2. *$\mathcal{A}$ is generated by X;*
3. *for all $s, t \in T(\Sigma, V)$ and injections α of $\mathcal{V}ar(s \equiv t)$ into X, if $(\mathcal{A}, \alpha) \models s \equiv t$ then $s =_E t$.*

We will rely on the following result from [BS95] about free algebras and positive formulae.

Lemma 2.7 *Let $\mathcal{B}$ be a free Ω-algebra over a countably infinite set X. For all positive Ω-formulae $\varphi(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2m-1}, \mathbf{v}_{2m})$ the following are equivalent:*

1. *$\mathcal{B} \models \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}.\ \varphi(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2m-1}, \mathbf{v}_{2m})$;*
2. *there exist tuples $\mathbf{x}_1, \ldots, \mathbf{x}_m \in X^*$ and $\mathbf{b}_1, \ldots, \mathbf{b}_m \in B^*$ and finite subsets $Z_1, \ldots, Z_m$ of X such that*
   - *(a) $\mathcal{B} \models \varphi(\mathbf{x}_1, \mathbf{b}_1, \ldots, \mathbf{x}_m, \mathbf{b}_m)$,*
   - *(b) all components of $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are distinct,*
   - *(c) for all $n \in \{1, \ldots, m\}$, all components of $\mathbf{b}_n$ are generated by Z_n in $\mathcal{B}$,*
   - *(d) for all $n \in \{1, \ldots, m-1\}$, no components of $\mathbf{x}_{n+1}$ are in $Z_1 \cup \cdots \cup Z_n$.*

We will also use the following result from [BS95].

Lemma 2.8 *For every equational theory E having a countable signature and a free model $\mathcal{A}$ with a countably infinite basis, the positive theory of E coincides with the set of positive sentences true in $\mathcal{A}$.*

One consequence of Lemma 2.8 is that the set of logically valid positive formulae over an infinite (functional) signature is decidable.

---

[3] This free model can be obtained as the quotient term algebra $T(\Sigma, V)/{=_E}$.

Proposition 2.9 *Let E be the empty Ω-theory for some infinite signature Ω. Then, the positive theory of E is decidable.*

Proof. In [Mah88], Maher shows that the class of locally absolutely free Ω-algebras[4] is axiomatizable and that the corresponding theory $\mathcal{T}$ is complete. To prove this result he uses a quantifier-elimination procedure that can also be used to decide the validity in $\mathcal{T}$ of first-order Ω-sentences (and so, in particular, of positive Ω-sentences).

Now, let $\mathcal{A}$ be an absolutely free Ω-algebra with a countably infinite basis. It is easy to show that $\mathcal{A}$ is locally absolutely free and so it is a model of $\mathcal{T}$. From the completeness of $\mathcal{T}$ it follows that an Ω-sentence is true in $\mathcal{A}$ iff it is valid in $\mathcal{T}$. The claim then follows by Lemma 2.8, given that $\mathcal{A}$ is free in E by definition. □

In this paper, we will deal with *combined* equational theories, that is, theories of the form $E_1 \cup E_2$, where E_1 and E_2 are two *component* equational theories of (possibly non-disjoint) signatures Σ_1 and Σ_2, respectively.

Where $\Sigma := \Sigma_1 \cap \Sigma_2$, we call *shared symbols* the elements of Σ and *shared terms* the elements of $T(\Sigma, V)$. Notice that when Σ_1 and Σ_2 are disjoint, the only shared terms are the variables. We call (strict) 1*-symbols* the elements of Σ_1 ($\Sigma_1 \setminus \Sigma$) and (strict) 2*-symbols* the elements of Σ_2 ($\Sigma_2 \setminus \Sigma$). Shared symbols are both 1- and 2-symbols, and they are strict for neither signature.

A term $t \in T(\Sigma_1 \cup \Sigma_2, V)$ is an i*-term* iff its top symbol is in $V \cup \Sigma_i$, i.e., if it is a variable or has the form $t = f(t_1, ..., t_n)$ for some i-symbol f ($i = 1, 2$). Variables and terms t with top symbol in $\Sigma_1 \cap \Sigma_2$ are both 1- and 2-terms. For $i = 1, 2$, an i-term is *pure* iff it contains only i-symbols and variables.

Most combination procedures, including the one described in this paper, work with $(\Sigma_1 \cup \Sigma_2)$-formulae by first "purifying" them into a set of Σ_1-formulae and a set of Σ_2-formulae. The purification process is achieved by replacing "alien" subterms by new variables and adding appropriate new equations. Intuitively, an alien subterm of an i-term t is a maximal subterm of t that is not itself an i-term. When the signatures Σ_1 and Σ_2 are disjoint the formal definition of alien subterm is straightforward. For the general case of possibly non-disjoint signatures, however, the definition gets more involved because one has to decide how to treat shared function symbols (see [BT02] for a detailed discussion). We adopt the following definition, among a number of possible ones.

Definition 2.10 (Alien subterms) *Let $t \in T(\Sigma_1 \cup \Sigma_2, V)$. If the top symbol of t is a strict i-symbol, then a subterm s of t is an* alien subterm *of t iff it is not an*

[4] An Ω-algebra is *locally absolutely free* iff all of its finitely-generated subalgebras are absolutely free.

i-term and it is maximal with this property, i.e., every proper superterm of s in t is an i-term.

If the top symbol of t is a shared symbol, then for $i = 1, 2$, let S_i be the set of all (proper) maximal subterms of t whose top symbol is a strict i-symbol.

- *If $S_1 \neq \emptyset$, then t is considered to be a 1-term, i.e., a subterm s of t is an* alien subterm *of t iff it is not a 1-term and it is maximal with this property.*

- *If $S_1 = \emptyset$ and $S_2 \neq \emptyset$, then t is considered to be a 2-term, i.e., a subterm s of t is an* alien subterm *of t iff it is not a 2-term and it is maximal with this property.*[5]

We extend the definition of alien subterm from terms to atomic formulae by treating the equality symbol as if it was a shared function symbol.

There is a standard *purification procedure* that when Σ_1 and Σ_2 are disjoint can convert any set S of equations of signature $\Sigma_1 \cup \Sigma_2$ into a set of pure equations (see [BS95] among others). With the definition of alien subterm above, this procedure applies unchanged even when Σ_1 and Σ_2 are not disjoint.

The gist of the procedure is to abstract by a fresh variable v_s each alien subterm s of an equation in S and add the equation $v_s \equiv s$ to S. This abstraction process is applied repeatedly to S until no more subterms can be abstracted. It is not hard to prove that the purification procedure always terminates, and produces a set of equations that is satisfiable in a $(\Sigma_1 \cup \Sigma_2)$-algebra $\mathcal{A}$ iff the original set is satisfiable in $\mathcal{A}$.

3 Theories with Constructors

In the next section we show how the combination procedure described in [BS95] generalizes to some cases of component theories with non-disjoint signatures. The main requirement for this generalization will be that the symbols shared by the two theories are *constructors* as defined in [BT02, TR02]. We start this section then by providing a formal definition of constructors and related notions, plus a few results on them that will be useful in proving the correctness of the generalized combination procedure.

For the rest of the section, let E be a non-trivial equational theory of signature Ω. Also, let Σ be a subsignature of Ω.

[5] If $S_1 = \emptyset$ and $S_2 = \emptyset$, then t is pure and so it has no aliens subterms.

Definition 3.1 (Constructors [BT02]) *The signature* Σ *is a* set of constructors for E *iff for every free model* $\mathcal{A}$ *of* E *with a countably infinite basis* X, $\mathcal{A}^\Sigma$ *is a free model of* E^Σ *with a basis* Y *including* X.

It is easy to show that the both empty signature and the whole signature Ω are always a set of constructors for E. Consequently, our combination results are a generalization of the known results for the disjoint case. For non-empty and proper subsignatures of Ω, however, it is usually non-trivial to show that they are a set of constructors for E by using just the definition above. Instead, using a syntactic characterization of constructors given in terms of certain subsets of $T(\Omega, V)$ is usually more helpful. We provide this characterization below because we will use it in some of our proofs. Before that though we need a little more notation.

Given a subset G of $T(\Omega, V)$, we denote by $T(\Sigma, G)$ the set of terms over the "variables" G. More precisely, every member of $T(\Sigma, G)$ is obtained from a term $s \in T(\Sigma, V)$ by replacing the variables of s with terms from G. To express this construction we will denote any such term by $s(\mathbf{r})$ where $\mathbf{r}$ is a tuple collecting the terms of G that replace the variables of s. Note that this notation is consistent with the assumption $G \subseteq T(\Sigma, G)$. In fact, every $r \in G$ can be represented as $s(r)$ where s is a variable of V. Also note that $T(\Sigma, V) \subseteq T(\Sigma, G)$ whenever $V \subseteq G$. In that case, every $s \in T(\Sigma, V)$ can be trivially represented as $s(\mathbf{v})$ where $\mathbf{v}$ are the variables of s.

Definition 3.2 (Σ-base) *A subset* G *of* $T(\Omega, V)$ *is a* Σ-base of E *iff the following holds:*

1. $V \subseteq G$.

2. *For all* $t \in T(\Omega, V)$, *there is an* $s(\mathbf{r}) \in T(\Sigma, G)$ *such that*

$$t =_E s(\mathbf{r}).$$

3. *For all* $s_1(\mathbf{r}_1), s_2(\mathbf{r}_2) \in T(\Sigma, G)$,

$$s_1(\mathbf{r}_1) =_E s_2(\mathbf{r}_2) \quad \textit{iff} \quad s_1(\mathbf{v}_1) =_E s_2(\mathbf{v}_2),$$

where $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *are tuples of fresh variables abstracting the terms of* $\mathbf{r}_1, \mathbf{r}_2$ *so that two terms in* $\mathbf{r}_1, \mathbf{r}_2$ *are abstracted by the same variable iff they are equivalent in* E.

We say that E admits a Σ-base *if some subset* G *of* $T(\Omega, V)$ *is a* Σ*-base of* E.

Theorem 3.3 (Characterization of constructors) *The signature Σ is a set of constructors for E iff E admits a Σ-base.*

From the definition of Σ-base and the proof of the theorem above it is possible to show the following.

Corollary 3.4 *Where $\mathcal{A}$ is a free model of E with a countably-infinite basis X, let α be an arbitrary bijection of V onto X. If G is a Σ-base of E then $\mathcal{A}^\Sigma$ is free in E^Σ over the superset $[\![G]\!]^{\mathcal{A}}_{\alpha}$ of X.*

A proof of both the theorem and the corollary can be found in [BT02].

In the following, we will assume that the theories we consider admit Σ-bases *closed under renaming.* This assumption is necessary for technical reasons, as it is used in the proof of soundness of the combination procedure we describe later. Although it is not clear if it can be made with no loss of generality, it seems to be satisfied by all "sensible" examples of theories admitting constructors.[6] Also note that the same technical assumption was needed in our work on combining decision procedures for the word problem [BT02].

A general class of theories admitting Σ-bases closed under renaming, which we will use later, is described in the following lemma.

Lemma 3.5 *Let F be a non-trivial equational theory of signature Σ and let F' be the empty Δ-theory for some signature Δ disjoint with Σ. The $(\Sigma \cup \Delta)$-theory $F \cup F'$ admits a Σ-base closed under renaming.*

Proof. Let $E := F \cup F'$. We prove that the set G below, which is clearly closed under renaming, is a Σ-base of E:

$$G \;:=\; V \cup \{t \in T(\Sigma \cup \Delta, V) \mid t \text{ starts with a } \Delta\text{-symbol}\}.$$

It is immediate that G satisfies Point 1 and Point 2 in the definition of Σ-base (Definition 3.2). To prove that G satisfies Point 3 it is enough to show the following: if s_1, s_2 are Σ-terms and σ is a substitution that maps distinct variables to non-E-equivalent terms of G, then $s_1 \neq_E s_2$ implies $s_1\sigma \neq_E s_2\sigma$. For that we will appeal to some results in [BS96] on the union of non-trivial and signature-disjoint equational theories.

Applying unfailing completion to E yields a (possibly infinite) ordered term rewriting system R. By arguing as in [BS96] (page 222) one can show that R is

[6] Theories admitting Σ-bases not closed under renaming are easy to construct. The open question is whether there are theories *none* of whose Σ-bases are closed under renaming.

confluent and terminating[7] and coincides with the union of the term rewriting systems R_F and $R_{F'}$ obtained respectively by applying unfailing completion to F and F'. In our special case, where F' is the empty theory, the system $R_{F'}$ is empty, which means that no Δ-symbols occur in R. It follows that the R-normal form of a $(\Sigma \cup \Delta)$-term starting with a Δ-symbol also starts with a Δ-symbol (the same one).

We say that a substitution σ into $(\Sigma \cup \Delta)$-terms is *R-normalized* iff $v\sigma$ is irreducible by R for all $v \in V$. Let s_1, s_2 be two Σ-terms. Lemma 4.1 in [BS96] states that for all R-normalized substitutions σ,

$$s_1\sigma =_E s_2\sigma \quad \text{iff} \quad (s_1\sigma)^\pi =_E (s_2\sigma)^\pi \tag{1}$$

where π is an "abstraction" function that replaces variables and subterms starting with a Δ-symbol by new variables so that two terms are replaced by the same variable iff they have the same R-normal form.

Now assume that $s_1 \neq_E s_2$ and consider a substitution σ into terms of G that maps distinct variables to non-E-equivalent terms of G. Clearly, for all distinct $u, v \in V$, $u\sigma$ and $v\sigma$ start with a Δ-symbol and have distinct R-normal forms. We can assume that σ is R-normalized. In fact, for all variables v for which $v\sigma \in V \subseteq G$, $v\sigma$ is already R-irreducible; for all variables v for which $v\sigma \in G \setminus V$, the R-normal form of $v\sigma$ (which is E-equivalent to $v\sigma$) starts with a Δ-symbol, as observed earlier, and so it too is in G. Therefore, we can consider in place of σ the substitution that maps every $v \in V$ to the R-normal form of $v\sigma$ without loss of generality. It is easy to show then that for $i = 1, 2$, $(s_i\sigma)^\pi = s_i\rho$ for some renaming substitution ρ. This entails that $(s_1\sigma)^\pi =_E (s_2\sigma)^\pi$ iff $s_1 =_E s_2$. Since $s_1 \neq_E s_2$ by assumptions, it follows from (1) that $s_1\sigma \neq_E s_2\sigma$. □

It is shown in [BT02] that, under the right conditions, constructors and the property of having Σ-bases closed under renaming are modular with respect to the union of theories.

Proposition 3.6 *For $i = 1, 2$ let E_i be a non-trivial equational Σ_i-theory. If $\Sigma := \Sigma_1 \cap \Sigma_2$ is a set of constructors for E_1 and for E_2 and the Σ-restrictions of E_1 and of E_2 coincide (i.e. ${E_1}^\Sigma = {E_2}^\Sigma$), then Σ is a set of constructors for $E_1 \cup E_2$. Furthermore, if both E_1 and E_2 admit a Σ-base closed under renaming, then $E_1 \cup E_2$ also admits a Σ-base closed under renaming.*

A useful consequence of Proposition 3.6 for us will be the following.

[7] Strictly speaking, R is terminating only on ground terms. However, we can consider instead of F' the empty $(\Delta \cup V)$-theory F'' where V is treated as a set of constant symbols. It is immediate that all terms $t_1, t_2 \in T(\Sigma \cup \Delta, V)$ are also in $T(\Sigma \cup \Delta \cup V, \emptyset)$ and that $t_1 =_{F \cup F'} t_2$ iff $t_1 =_{F \cup F''} t_2$.

Proposition 3.7 *Let E be an Ω-theory and let E' be the empty Δ-theory for some signature Δ disjoint with Ω. If $\Sigma \subseteq \Omega$ is a set of constructors for E, then it is a set of constructors for $E \cup E'$. Furthermore, if E admits a Σ-base closed under renaming, then so does $E \cup E'$.*

Proof. Let F be the Σ-theory E^{Σ}, which is certainly non-trivial (otherwise E would be trivial too). By Lemma 3.5, $F \cup E'$ admits a Σ-base closed under renaming. By Proposition 3.3, this entails in particular that Σ is a set of constructors for $F \cup E'$. It is easy to see that $F \cup E'$ is non-trivial. By construction of F, the theories E and $F \cup E'$ have the same Σ-restriction. It follows from Proposition 3.6 that Σ is a set of constructors for $E \cup (F \cup E')$, and that $E \cup (F \cup E')$ admits a Σ-base closed under renaming whenever E does. The claim then follows from the fact that $E \cup E'$ is logically equivalent to $E \cup F \cup E' = E \cup E^{\Sigma} \cup E'$. □

4 Combining Decision Procedures

In this section we present a variant of the Baader-Schulz procedure for combining decision procedures for the validity of positive formulae in equational theories. Extending Baader and Schulz's results in [BS95], our variant applies to two non-trivial equational theories that may share function symbols as long as these symbols are constructors for both theories and are defined in the same way in each of them.

More precisely, we will consider two theories E_1 and E_2 that satisfy the following assumptions for $i = 1, 2$, which we fix for the rest of the section:

- E_i is a non-trivial equational theory of some countable signature Σ_i;
- $\Sigma := \Sigma_1 \cap \Sigma_2$ is a set of constructors for E_i;
- ${E_1}^{\Sigma} = {E_2}^{\Sigma}$;
- E_i admits a Σ-base closed under variable renaming.

Let $E := E_1 \cup E_2$. It is proven in [BT02] that, under the assumptions above, $E^{\Sigma} = {E_1}^{\Sigma} = {E_2}^{\Sigma}$. In the following then, we will also use E^{Σ} to refer indifferently to ${E_1}^{\Sigma}$ or ${E_2}^{\Sigma}$.

The combination procedure will use two kinds of substitutions that we call, after [TR02], *identifications* and Σ-*instantiations*. Given a set of variables U, an *identification of U* is a substitution defined by partitioning U, electing a representative for each block in the partition, and mapping each element of U to the representative in its block. A Σ-*instantiation of U* is a substitution that maps some elements of U to non-variable Σ-terms and the other elements to themselves. For convenience, we will assume that the variables occurring in the terms introduced by a Σ-instantiation are *always fresh*.

4.1 The Combination Procedure

The combination procedure takes as input a positive existential $(\Sigma_1 \cup \Sigma_2)$-formula $\exists \mathbf{w}.\ \varphi(\mathbf{w})$ and outputs, non-deterministically, a pair of sentences: a positive Σ_1-sentence and a positive Σ_2-sentence. The procedure consists of the following steps.

1. **Convert into DNF.**
   Convert the input's matrix φ into the disjunctive normal form $\psi_1 \vee \cdots \vee \psi_n$ and choose a disjunct ψ_j.

2. **Convert into Separate Form.**
   Let S be the set obtained by purifying as described in Section 2 the set of all the equations in ψ_j. For $i = 1, 2$, let $\varphi_i(\mathbf{v}, \mathbf{u}_i)$ be the conjunction of all Σ_i-equations in S,[8] with $\mathbf{v}$ listing the variables in $\mathcal{V}ar(\varphi_1) \cap \mathcal{V}ar(\varphi_2)$ and $\mathbf{u}_i$ listing the remaining variables of φ_i.

3. **Instantiate Shared Variables.**
   Choose a Σ-instantiation ρ of $\mathcal{V}ar(\mathbf{v}) = \mathcal{V}ar(\varphi_1) \cap \mathcal{V}ar(\varphi_2)$.

4. **Identify Shared Variables.**
   Choose an identification ξ of $\mathcal{V}ar(\varphi_1\rho) \cap \mathcal{V}ar(\varphi_2\rho) = \mathcal{V}ar(\mathbf{v}\rho)$. For $i = 1, 2$, let $\varphi'_i := \varphi_i\rho\xi$.

5. **Partition Shared Variables.**
   Group the elements of $V_{\mathrm{s}} := \mathcal{V}ar(\mathbf{v}\rho\xi) = \mathcal{V}ar(\varphi'_1) \cap \mathcal{V}ar(\varphi'_2)$ into the tuples $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$, with $2 \leq 2m \leq |V_{\mathrm{s}}| + 1$, so that each element of V_{s} occurs exactly once in the tuple $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$.[9]

6. **Generate Output Pair.**
   Output the pair of sentences

$$\exists \mathbf{v}_1\, \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{v}_{2m-1}\, \forall \mathbf{v}_{2m}\, \exists \mathbf{u}_1.\ \varphi'_1,$$
$$\forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ \varphi'_2.$$

Ignoring inessential differences and our restriction to functional signatures, this combination procedure differs from the one by Baader and Schulz [BS95] only for

[8]Where Σ-equations are considered arbitrarily as either Σ_1- or Σ_2-equations.

[9]Note that some of the subtuples $\mathbf{v}_i$ may be empty.

the presence of Step 3. Note however that for component theories with disjoint signatures, the case considered in [BS95], Step 3 is vacuous because Σ is empty. In that case then the procedure above reduces to that in [BS95]. Correspondingly, our requirements on the two component theories also reduce to that in [BS95], which simply asks that E_1 and E_2 be non-trivial. In fact, as observed earlier, when Σ is empty it is always a set of constructors for E_i ($i = 1, 2$), with the whole $T(\Sigma_i, V)$ being a Σ-base closed under renaming. Moreover, ${E_1}^{\Sigma}$ is equal to ${E_2}^{\Sigma}$ because they both coincide with the theory $\{v \equiv v \mid v \in V\}$.

An important thing to notice about Step 3 in the procedure above is that, contrary to the other non-deterministic steps of the procedure, its non-determinism is not finitary. The reason is that in general there are infinitely-many possible Σ-instantiations to choose from. This means that, without further restrictions, the combination procedure above cannot be used as a decision procedure. One viable, albeit strong, restriction for obtaining a decision procedure is described in the next subsection.

Like the one it extends, this combination procedure is sound and complete in the following sense.

Theorem 4.1 (Soundness and Completeness) *For all possible inputs sentences $\exists \mathbf{w}.\ \varphi(\mathbf{w})$ for the combination procedure, $E_1 \cup E_2 \models \exists \mathbf{w}.\ \varphi(\mathbf{w})$ iff there is a possible output (γ_1, γ_2) such that $E_1 \models \gamma_1$ and $E_2 \models \gamma_2$.*

We will prove this result in Section 4.4. Before, we describe the extended decidability results the new procedure leads to.

4.2 Decidability Results

With our combination procedure we are able to properly extend the following combined decidability results of [BS95].

Theorem 4.2 *For $i = 1, 2$, let F_i be a non-trivial equational theory of countable signature Ω_i, where Ω_1 and Ω_2 are disjoint. If the positive theories of F_1 and of F_2 are decidable, then the positive theory of $F_1 \cup F_2$ is also decidable.*

The extension of course is obtained by relaxing the requirement that the signatures of the component theories be disjoint. We show in the following that the result above also applies to theories sharing constructors, provided that the equivalence relation defined by the theories over the constructor terms is *bounded* in a sense described below.

Definition 4.3 *Let E be an equational Ω-theory. We say that equivalence in E is* finitary modulo renaming *iff there is a finite subset R of $T(\Omega, V)$ such that for all $s \in T(\Omega, V)$ there is a term $t \in R$ and a renaming σ such that $s =_E t\sigma$. We call R a set of* E-representatives.

When Ω in the above definition is empty, equivalence in E is trivially finitary—with any singleton set of variables being a set of E-representatives. The same is true if Ω is a finite set of constant symbols. In that case, a set of E-representatives consists of one variable and all the constants of Ω. For a simple non-trivial example consider the theory $E := \{\forall x.\ x \equiv \mathsf{s}(\mathsf{s}(\mathsf{s}(x)))\}$ and $\Omega := \{\mathsf{0}, \mathsf{s}\}$. One set of E-representatives is $\{\mathsf{0}, \mathsf{s}(\mathsf{0}), \mathsf{s}(\mathsf{s}(\mathsf{0})), v, \mathsf{s}(v), \mathsf{s}(\mathsf{s}(v))\}$ where v is any element of V.

Whenever E^Σ, the Σ-restriction of the theories E_1 and E_2 fixed earlier, is finitary modulo renaming, the decidability of the positive theories of E_1 and of E_2 yields the decidability of the positive theory of $E_1 \cup E_2$. Similarly to [BS95], we will show this result via a boot-strapping process that starts with a combination result immediately based on the combination procedure's soundness and completeness.

Proposition 4.4 *Assume equivalence in E^Σ is finitary modulo renaming. If the positive theories of E_1 and of E_2 are both decidable, then the positive $\exists$-theory of $E_1 \cup E_2$ is also decidable.*

Proof. Let R be a set of E^Σ-representatives. By Theorem 4.1, the validity in $E_1 \cup E_2$ of a positive $\exists$-sentence $\exists \mathbf{v} \varphi(\mathbf{v})$ is reducible to the validity in E_1 of a positive sentence γ_1 and the validity in E_2 of a positive sentence γ_2, where (γ_1, γ_2) is one of the possible outputs of the combination procedure on input $\varphi(\mathbf{v})$. We can prove the claim then by showing that such a reduction is effective. For that, it is enough to show that each step of the combination procedure is *finitary*[10] and executable in finite time, which is easily done for all steps but Step 3. Step 3 is clearly executable in finite time; but is not finitary when Σ contains function symbols of non-zero arity because then there are infinitely-many instantiations into Σ-terms. However, since E^Σ is finitary modulo renaming, Step 3 is readily made finitary without loss of completeness. In fact, it is enough to choose only instantiations of the shared variables into a variant of terms in the (finite) set R. Each such variant is obtained from a term $t \in R$ by simply replacing t's variables with fresh ones. □

Lemma 4.5 *Let $i \in \{1, 2\}$ and let E_3 be the empty Σ_3-theory for some countably-infinite signature Σ_3 disjoint with Σ_i. If the positive theory of E_i is decidable, then the positive theory of $E_i \cup E_3$ is also decidable.*

[10] In the sense that it can have only finitely many alternative executions—recall that the procedure is non-deterministic.

Proof. Assume that positive theory of E_i is decidable. We know from Proposition 2.9 that the positive theory of E_3 is decidable. Since Σ_i and Σ_3 are disjoint, we can immediately conclude by Theorem 4.2 that the positive theory of $E_i \cup E_3$ is also decidable. □

We are now ready for our main decidability result.

Theorem 4.6 *For $i = 1, 2$, let E_i be a non-trivial equational theory of countable signature Σ_i such that*

- $\Sigma := \Sigma_1 \cap \Sigma_2$ *is a set of constructors for E_i;*
- E_i *admits a Σ-base closed under variable renaming;*
- ${E_1}^{\Sigma} = {E_2}^{\Sigma}$*;*
- *equivalence in ${E_i}^{\Sigma}$ is finitary modulo renaming.*

If the positive theories of E_1 and of E_2 are both decidable, then the positive theory of $E := E_1 \cup E_2$ is also decidable.

Proof. Assume that the positive theories of E_1 and of E_2 are both decidable. Let Σ_3 be a signature disjoint with both Σ_1 and Σ_2 and consisting of (countably) infinitely-many function symbols of arity n, for all $n > 0$. Clearly, given any positive $(\Sigma_1 \cup \Sigma_2)$-sentence γ, it is possible to Skolemize its universally quantified variables so that its Skolemized version $\hat{\gamma}$ is a $(\Sigma_1 \cup \Sigma_2 \cup \Sigma_3)$-sentence.

Now let $\Sigma_2' := \Sigma_2 \cup \Sigma_3$ and consider the Σ_2'-theory $E_2' := E_2 \cup E_3$ where E_3 is the empty theory of signature Σ_3. The theories E_1 and E_2' satisfy all the initial assumptions satisfied by E_1 and E_2. In fact, they are both non-trivial equational theories with a countable signature. The intersection of their signatures, which coincides with Σ, is a set of constructors for both, and they both admit a Σ-base closed under renaming. For E_1 this holds by assumption; for E_2', it holds by Proposition 3.7. Finally the Σ-restrictions of E_1 and E_2' coincide, given that ${E_2'}^{\Sigma} = {E_2}^{\Sigma}$, as one can easily see.

By Lemma 4.5 we also have that the positive theory of E_2' is decidable. Therefore, we can apply Proposition 4.4 to E_1 and E_2' and conclude that the positive $\exists$-theory of the $(\Sigma_1 \cup (\Sigma_2 \cup \Sigma_3))$-theory $E_1 \cup E_2' = E_1 \cup (E_2 \cup E_3)$ is decidable. The claim then follows from the fact that, for every positive $(\Sigma_1 \cup \Sigma_2)$-sentence and its Skolemized version $\hat{\gamma}$, $E_1 \cup E_2 \models \gamma$ iff $E_1 \cup E_2 \models \hat{\gamma}$ (by Lemma 2.1) and $E_1 \cup E_2 \models \hat{\gamma}$ iff $E_1 \cup E_2 \cup E_3 \models \hat{\gamma}$ (by construction of $\hat{\gamma}$ and E_3). □

4.3 An example

The reader may rightly wonder whether Theorem 4.6 is indeed a proper extension of Theorem 4.2, as it is not evident that there are in fact component theories satisfying all the requirements in Theorem 4.6. We discuss a simple but illustrative example of one such theory in this subsection.

Example 4.7 *Consider the signature* $\Omega := \{0, \mathsf{s}, +\}$ *and, for some* $n > 1$*, the equational theory* E_n *axiomatized by the identities*

$$x + (y + z) \equiv (x + y) + z, \quad (2)$$

$$x + y \equiv y + x, \quad (3)$$

$$x + \mathsf{s}(y) \equiv \mathsf{s}(x + y), \quad (4)$$

$$x + \mathsf{0} \equiv x, \quad (5)$$

$$\mathsf{s}^n(x) \equiv x. \quad (6)$$

where as usual $\mathsf{s}^n(x)$ *stands for the* n*-fold application of* s *to* x*. We show below that, for* E_n *and the subsignature* $\Sigma := \{\mathsf{0}, \mathsf{s}\}$ *of* Ω*, all the assumptions of Theorem 4.6 are satisfied.*

Proposition 4.8 *Let* Ω, E_n, Σ *be as in Example 4.7. Then the following holds.*

1. E_n *is non-trivial.*
2. *Equivalence in* E_n^Σ *is finitary modulo renaming.*
3. Σ *is a set of constructors for* E_n *with a* Σ*-base closed under renaming.*
4. *The positive theory of* E_n *is decidable.*

Proof. (1) Immediate consequence of the fact that $n > 1$ and the non-negative integers modulo n are a model of E_n.

(2) This point follows from the fact that every Σ-term contains at most one variable and every term in $T(\Sigma, \{v\})$ is equivalent in ${E_n}^\Sigma$ to a term in

$$\{\mathsf{s}^m(\mathsf{0}) \mid 0 \leq m < n\} \cup \{\mathsf{s}^m(v) \mid 0 \leq m < n\}.$$

(3) To prove this point we will implicitly appeal to standard results about term rewriting systems modulo an equational theory. The reader is referred to [JK86, BN98] for more details about them.

Let AC denote the equational theory defined by the first two axioms of E_n. It is not hard to show that orienting the remaining axioms from left to right yields a canonical term rewriting system R modulo AC. Consequently, every Ω-term t has a computable R-normal form $t{\downarrow}$, and normal forms of E_n-equivalent terms are equivalent modulo AC. We show that the set

$$G \;:=\; \{r \mid r \in T(\Omega, V) \text{ and } r{\downarrow} \text{ is a variable or starts with } +\},$$

is a Σ-base for E_n. Note that the normal form of each element of G is either a variable or a sum of variables. If π is a renaming and $r \in T(\Omega, V)$, then $(r\pi){\downarrow} = (r{\downarrow})\pi$. This, together with the fact that the set $\{t \mid t \text{ is a variable or starts with } +\}$ is closed under renaming, implies that G is closed under renaming.

Now, the first property required by Definition 3.2 is satisfied by G by definition since $v{\downarrow} = v$ for all $v \in V$. For the second property, let t be an arbitrary Ω-term. Its R-normal form $t{\downarrow}$ is either a Σ-term (and thus a term in $T(\Sigma, G)$), or some term $\mathsf{s}^m(r)$ where $0 \leq m < n$ and r starts with $+$. Since the subterm r of the normal form $t{\downarrow}$ is itself in normal form, we know that $r \in G$. It follows that $t =_{E_n} t{\downarrow} = \mathsf{s}^m(r) \in T(\Sigma, G)$.

To prove that G satisfies the third property of Σ-bases, it is enough to show the only-if direction since the if-direction is trivial. Thus, consider two E_n-equivalent elements t_1, t_2 of $T(\Sigma, G)$. For $i = 1, 2$, t_i is either (i) an element of $T(\Sigma, \emptyset)$ or (ii) of the form $t_i = \mathsf{s}^{m_i}(r_i)$ where $m_i \geq 0$ and $r_i \in G$. In the second case, $r_i{\downarrow}$ is a variable or a sum of variables. Since a term in $T(\Sigma, \emptyset)$ obviously cannot be E_n-equivalent to a term containing variables, either the first case holds for both terms, or the second case holds for both terms. In the first case, the third property of Σ-bases obviously holds since nothing is abstracted. In the second case, let v_1, v_2 be variables such that $v_1 = v_2$ iff $r_1 =_{E_n} r_2$. We must show that $\mathsf{s}^{m_1}(v_1) =_{E_n} \mathsf{s}^{m_2}(v_2)$.

To this purpose, we consider the R-normal forms of t_1, t_2. We claim that $t_i{\downarrow} = \mathsf{s}^{k_i}(r_i{\downarrow})$ where k_i is the remainder obtained when dividing m_i by n. Obviously, this term can be obtained from $t_i = \mathsf{s}^{m_i}(r_i)$ by applying the rewrite rules of R. In addition, since $r_i{\downarrow}$ is a variable or a sum of variables, no rule of R applies to $\mathsf{s}^{k_i}(r_i{\downarrow})$, which proves the claim. Since t_1, t_2 were assumed to be E_n-equivalent, their normal forms are equivalent modulo AC. This implies that $k_1 = k_2$ and $r_1{\downarrow} =_{AC} r_2{\downarrow}$. Consequently $m_1 \equiv m_2 \pmod{n}$ and $r_1 =_{E_n} r_1{\downarrow} =_{E_n} r_2{\downarrow} =_{E_n} r_2$. The second identity implies that $v_1 = v_2$ and the first that $\mathsf{s}^{m_1}(v_1) =_{E_n} \mathsf{s}^{m_2}(v_1)$. This completes the proof that G satisfies the third property of Σ-bases.

In conclusion, we have shown that G satisfies all requirements of Definition 3.2 and so is a Σ-base of E_n.

(4) From general results in [BS96] on positive theories and unification problems we know that the positive theory of E_n is decidable iff E_n-unification with linear constant restrictions is decidable. We prove this point then by sketching a decision

procedure for E_n-unification with linear constant restrictions. But first, we restrict our attention to unification with constants.

Assume that t_1, t_2 are two Ω-terms containing exactly the variables $v_1, \ldots, v_\ell$ (for some $\ell \geq 0$) and additional constant symbols from a set $C := \{\mathsf{c}_1, \ldots, \mathsf{c}_{\ell'}\}$, disjoint with Ω. It is easy to see that t_1, t_2 are E_n-unifiable iff there is an E_n-unifier σ of t_1, t_2 such that $v_j\sigma \in T(\Omega \cup C, \emptyset)$ for all $j \in \{1, \ldots, \ell\}$.

Let σ be a substitution into ground $(\Omega \cup C)$-terms. Without loss of generality we may assume that the terms t_1, t_2 as well as the terms $v_j\sigma$ are all in R-normal form. Under this assumption, it is easy to see that, modulo AC, t_i is of the form

$$t_i = \mathsf{s}^{m_i}(\sum_{j=1}^{\ell} a_{i,j}\, v_j + \sum_{k=1}^{\ell'} b_{i,k}\, \mathsf{c}_k),$$

where $a_{i,j}\, v_j$ and $b_{i,k}\, \mathsf{c}_k$ above abbreviate respectively the sum

$$\underbrace{v_j + \ldots + v_j}_{a_{i,j} \text{ times}} \quad \text{and} \quad \underbrace{\mathsf{c}_k + \ldots + \mathsf{c}_k}_{b_{i,k} \text{ times}}$$

for some $a_{i,j}, b_{i,k} \geq 0$.[11] Analogously, for every $j \in \{1, \ldots, \ell\}$ the term $x_j\sigma$ is of the form

$$x_j\sigma = \mathsf{s}^{p_j}(\sum_{k=1}^{\ell'} d_{j,k}\, \mathsf{c}_k).$$

Now consider the term $(t_i\sigma)\!\downarrow$ for $i = 1, 2$, which has the form $\mathsf{s}^{n_i}(r_i)$ where r_i is either a single constant from $C \cup \{\mathsf{0}\}$ or a sum of constants from C. It is not hard to show that σ is an E_n-unifier of t_1 and t_2 iff (1) $n_1 = n_2$ and (2) for each $k \in \{1, \ldots, \ell'\}$, the constant c_k occurs in r_1 the same number of times it occurs in r_2. In turn, these two conditions respectively hold iff

1. the tuple $(p_1, \ldots, p_\ell)$ solves the equation

$$a_{1,1}\, y_1 + \cdots + a_{1,\ell}\, y_\ell + m_1 = a_{2,1}\, y_1 + \cdots + a_{2,\ell}\, y_\ell + m_2$$

   in the variables y_j over the non-negative integers modulo n, and

2. for each $k \in \{1, \ldots, \ell'\}$, the tuple $(d_{1,k}, \ldots, d_{\ell,k})$ solves the equation

$$a_{1,1}\, x_{1,k} + \cdots + a_{1,\ell}\, x_{\ell,k} + b_{1,k} = a_{2,1}\, x_{1,k} + \cdots + a_{2,\ell}\, x_{\ell,k} + b_{2,k}$$

   in the variables $x_{j,k}$ over the non-negative integers.

[11] When every $a_{i,j}$ is zero, the summation $\sum_{j=1}^{\ell} a_{i,j}\, v_j$ stands for the constant $\mathsf{0}$.

Since the solvability of linear equations over the non-negative integers (and over the non-negative integers modulo n) is decidable, this shows that E_n-unification with constants is decidable.

For unification with (linear) constant restrictions, we must handle additional unifier constraints of the sort "constant c_k must not occur in the image of variable x_j"—see [BS96] for more details on unification with (linear) constant restrictions. Now, a constraint like that is satisfied exactly when $d_{j,k}$ above is zero. Thus, to satisfy a given set of (linear) constant restrictions one can simply replace the appropriate variable $x_{j,k}$ by zero in the linear equations above before solving them. It follows then that E_n-unification with linear constant restrictions is decidable, and therefore so is the positive theory of E_n. □

We illustrate the proof of point 4 of the proposition above by showing how it works on a specific example. Assume we want to unify the terms $v_1 + \mathsf{s}(v_1) + \mathsf{c}_1$ and $\mathsf{s}(v_2) + \mathsf{s}(\mathsf{c}_2)$ modulo the theory E_3. In addition, assume we have a constant restriction stating that c_2 must not occur in the image of v_2. The respective normal forms of the two terms to be unified are

$$t_1 := \mathsf{s}(v_1 + v_1 + \mathsf{c}_1) \quad \text{and} \quad t_2 := \mathsf{s}^2(v_2 + \mathsf{c}_2).$$

Therefore, we must solve three linear equations. One for the constant c_1:

$$2x_{1,1} + 1 = x_{2,1};$$

one for the constant c_2:

$$2x_{1,2} = x_{2,2} + 1;$$

and finally one (modulo 3) for s:

$$2y_1 + 1 \equiv y_2 + 2 \pmod{3}.$$

First, let us consider the unification problem without the constant restriction. Then

$$x_{1,1} = 1, \quad x_{2,1} = 3$$

is a solution of the first equation;

$$x_{1,2} = 1, \quad x_{2,2} = 1$$

is a solution of the second equation; and

$$y_1 = 2, \quad y_2 = 0$$

is a solution (modulo 3) of the third equation. These solutions yield the substitution

$$\sigma \;:=\; \{v_1 \mapsto \mathsf{s}^2(\mathsf{c}_1+\mathsf{c}_2),\ v_2 \mapsto \mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_2\}.$$

This substitution is indeed an E_3-unifier of t_1, t_2 since

$$\begin{aligned} t_1\sigma &= \mathsf{s}(\mathsf{s}^2(\mathsf{c}_1+\mathsf{c}_2)+\mathsf{s}^2(\mathsf{c}_1+\mathsf{c}_2)+\mathsf{c}_1) \\ &=_{E_3} \mathsf{s}^5(\mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_2+\mathsf{c}_2) \\ &=_{E_3} \mathsf{s}^2(\mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_1+\mathsf{c}_2+\mathsf{c}_2) \\ &= t_2\sigma. \end{aligned}$$

Note, however, that this unifier does not satisfy the constant restriction "c_2 must not occur in the image of v_2." To account for this restriction, we must find a solution of the equation

$$2x_{1,2} = x_{2,2} + 1$$

for which $x_{2,2} = 0$. However, such a solution obviously does not exist in the non-negative integers. Consequently, the unification problem does not have a solution under this restrictions.

Finally, let us illustrate the connection to validity of positive formulae in E_3. The single constant restriction "c_2 must not occur in the image of v_2" is induced by the linear ordering $\mathsf{c}_1 < v_2 < \mathsf{c}_2 < v_1$.[12] According to the results in [BS96] the solvability of the E_3-unification problem for t_1, t_2 under this linear constant restriction is equivalent to the validity in E_3 of the positive formula

$$\forall w_1 \exists v_2 \forall w_2 \exists v_1.\ \mathsf{s}(v_1+v_1+w_1) \equiv \mathsf{s}^2(v_2+w_2).$$

This formula is obtained from the unification problem by translating free constants into universally quantified variables and variables into existentially quantified variables, and ordering the quantifiers according to the linear ordering on the variables and free constants of the problem. Since, as we have seen, the E_3-unification problem with the linear constant restriction induced by $\mathsf{c}_1 < v_2 < \mathsf{c}_2 < v_1$ is not solvable, the above formula is not valid in E_n. In contrast, the formula

$$\forall w_1 \forall w_2 \exists v_2 \exists v_1.\ \mathsf{s}(v_1+v_1+w_1) \equiv \mathsf{s}^2(v_2+w_2)$$

is valid since the corresponding unification problem is the same as the one for the previous formula but without any constant restriction, and that problem is solvable.

[12] The linear constant restriction induced by this linear ordering on the variables and free constants of the problem says that constants that are greater than a variable must not occur in its image.

4.4 Correctness of the Procedure

We prove below that our combination procedure is sound and complete for the kind of component theories specified at the beginning of this section. In [BS95], the soundness and completeness proof relies on a particular free model of the union theory. This model is constructed explicitly, as an amalgamation of a free model of one component theory with a free model of the other component theory. The amalgamation construction and the proofs that use the resulting amalgamated model—called the *free amalgamated product* in [BS95]—are fairly complex.

An important technical contribution of this work is to construct an appropriate free model of the union theory also in the case where the theories share constructors. For this, it has turned out to be useful to consider first a simpler sort of amalgamated model for the union theory: one obtained as a *fusion* (defined below) of the free models of the two component theories. Contrary to Baader and Schulz's free amalgamated product, our fusion model is not free in the union theory. However, it admits a subalgebra that is so, which suffices for our purposes.

Definition 4.9 (Fusion [BT02, TR02]) *A $(\Omega_1 \cup \Omega_2)$-algebra $\mathcal{F}$ is a* fusion *of a Ω_1-algebra $\mathcal{A}_1$ and a Ω_2-algebra $\mathcal{A}_2$ iff $\mathcal{F}^{\Omega_1}$ is Ω_1-isomorphic to $\mathcal{A}_1$ and $\mathcal{F}^{\Omega_2}$ is Ω_2-isomorphic to $\mathcal{A}_2$.*

It is shown in [TR02] that two algebras $\mathcal{A}_1$ and $\mathcal{A}_2$ have fusions exactly when they are isomorphic over their shared signature. There it is also shown that fusions of algebra are related to unions of theories as follows.

Proposition 4.10 *For $i = 1, 2$, let $\mathcal{T}_i$ be an Ω_i-theory. For all $(\Omega_1 \cup \Omega_2)$-algebras $\mathcal{A}$, $\mathcal{A}$ is a model of $\mathcal{T}_1 \cup \mathcal{T}_2$ iff $\mathcal{A}$ is a fusion of a model of $\mathcal{T}_1$ and a model of $\mathcal{T}_2$.*

A Fusion Model for $E_1 \cup E_2$

In the following, we will construct a model of $E = E_1 \cup E_2$ as a fusion of the free models of the theories E_1 and E_2 fixed earlier, whose shared signature Σ was a set of constructors for both. We start by fixing, for $i = 1, 2$,

- a free model $\mathcal{A}_i$ of E_i with a countably infinite basis X_i,[13]
- a bijective valuation α_i of V onto X_i,
- a Σ-base G_i of E_i closed under variable renaming, and
- the set $Y_i := [\![G_i]\!]^{\mathcal{A}_i}_{\alpha_i}$.

[13] Such a model exists by Proposition 2.5.

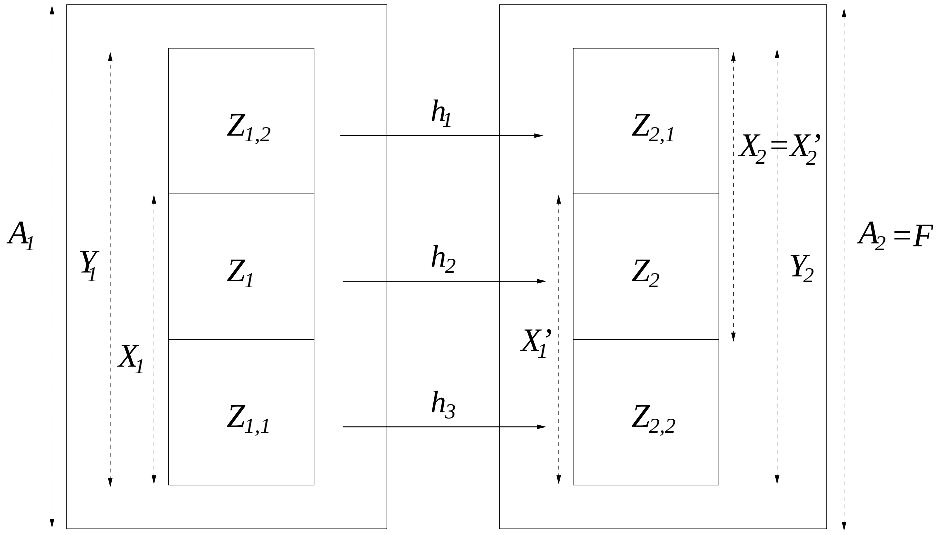

Figure 1: The Fusion $\mathcal{F}$ of $\mathcal{A}_1$ and $\mathcal{A}_2$.

We know from Corollary 3.4 that $X_i \subseteq Y_i$ and ${\mathcal{A}_i}^{\Sigma}$ is free in $E^{\Sigma} = {E_1}^{\Sigma} = {E_2}^{\Sigma}$ over Y_i. Observe that $\mathcal{A}_i$ is countably infinite, given our assumption that X_i is countably infinite and Σ_i is countable. As a consequence, Y_i is countably infinite as well.

Now let $Z_{i,2} := Y_i \setminus X_i$ for $i = 1, 2$, and let $\{Z_{1,1}, Z_1\}$ be a partition of X_1 such that Z_1 is countably infinite and $|Z_{1,1}| = |Z_{2,2}|$.[14] Similarly, let $\{Z_{2,1}, Z_2\}$ be a partition of X_2 such that $|Z_{2,1}| = |Z_{1,2}|$ and Z_2 is countably infinite (see Figure 1). Then consider 3 arbitrary bijections

$$h_1 \colon Z_{1,2} \longrightarrow Z_{2,1}, \quad h_2 \colon Z_1 \longrightarrow Z_2, \quad h_3 \colon Z_{1,1} \longrightarrow Z_{2,2},$$

as shown in Figure 1. Observing that $\{Z_{i,1}, Z_i, Z_{i,2}\}$ is a partition of Y_i for $i = 1, 2$, it is immediate that $h_1 \cup h_2 \cup h_3$ is a well-defined bijection of Y_1 onto Y_2. Since ${\mathcal{A}_i}^{\Sigma}$ is free in E^{Σ} over Y_i for $i = 1, 2$, we have that $h_1 \cup h_2 \cup h_3$ extends uniquely to a (Σ)-isomorphism h of ${\mathcal{A}_1}^{\Sigma}$ onto ${\mathcal{A}_2}^{\Sigma}$.

The isomorphism h induces a fusion of $\mathcal{A}_1$ and $\mathcal{A}_2$, whose main the properties are listed in the following lemma taken from [BT02].

Lemma 4.11 *There is a fusion $\mathcal{F}$ of $\mathcal{A}_1$ and $\mathcal{A}_2$ having the same universe as $\mathcal{A}_2$ and such that*

1. *h is a (Σ_1)-isomorphism of $\mathcal{A}_1$ onto $\mathcal{F}^{\Sigma_1}$;*

[14] This is possible because $Z_{2,2}$ is countable (possibly finite).

2. the identity map of A_2 is a (Σ_2)-isomorphism of $\mathcal{A}_2$ onto $\mathcal{F}^{\Sigma_2}$;

3. $\mathcal{F}^{\Sigma_1}$ is free in E_1 over $X_1' := Z_{2,2} \cup Z_2$;

4. $\mathcal{F}^{\Sigma_2}$ is free in E_2 over $X_2' := Z_{2,1} \cup Z_2$;

5. $\mathcal{F}^{\Sigma}$ is free in E^{Σ} over $Y_2 = Z_{2,1} \cup Z_2 \cup Z_{2,2}$;

6. $Y_2 = [\![G_2]\!]^{\mathcal{F}^{\Sigma_2}}_{\alpha_2} = [\![G_1]\!]^{\mathcal{F}^{\Sigma_1}}_{h \circ \alpha_1}$.

We will now consider the theory $E = E_1 \cup E_2$ again, together with the algebras $\mathcal{F}$, $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{A}$ where:

- $\mathcal{F}$ is the fusion of $\mathcal{A}_1$ and $\mathcal{A}_2$ from Lemma 4.11;
- $\mathcal{F}_i := \mathcal{F}^{\Sigma_i}$ for $i = 1, 2$;[15]
- $\mathcal{A}$ is the subalgebra of $\mathcal{F}$ generated by Z_2.

Both $\mathcal{F}$ and $\mathcal{A}$ are models of E. In fact, $\mathcal{F}$ is a model of E by Proposition 4.10 for being a fusion of a model of E_1 and a model of E_2, whereas $\mathcal{A}$ is a model of E by Lemma 2.3, as E is equational for being the union of two equational theories.

We prove below that $\mathcal{A}$ is a free model of E. To do that we will use the following sets of terms and their properties.

Definition 4.12 **($G_1^\infty, G_2^\infty, G^\infty$)** *For $i = 1, 2$ let $G_i^\infty := \bigcup_{n=0}^\infty G_i^n$ where $\{G_i^n \mid n \geq 0\}$ is the family of sets defined as follows:*

$$\begin{array}{lcll} G_i^0 & := & V & \\ G_i^{n+1} & := & G_i^n \cup \{r(r_1, \ldots, r_m) & \mid \; r(v_1, \ldots, v_m) \in G_i \setminus V, \\ & & & \quad r \neq_E v \text{ for all } v \in V, \\ & & & \quad r_j \in G_k^n \text{ with } k \neq i, \text{ for all } j = 1, \ldots, m, \\ & & & \quad r_j \neq_E r_{j'} \text{ for all distinct } j, j' = 1, \ldots, m\}. \end{array}$$

The set G^∞ is the union $G_1^\infty \cup G_2^\infty$.

It is easy to see that, for $i = 1, 2$, the set G_i^1 defined above consists of all the variables plus the terms of G_i that are not equivalent in E_i to a variable. Every element of G_i^n has a stratified recursive algebra. A term in $G_i^1 \setminus G_i^0$ has just one layer. A term $r(\mathbf{r})$ in $G_i^n \setminus G_i^{n-1}$ has n layers. Layer 1, the top layer, is made of the term r only; layer 2 is made of all the terms that are at layer 1 in an element of $\mathbf{r}$; and so on. Furthermore, terms in the same layer all belong to either G_1 or G_2, and

[15] These algebras are defined just for notational convenience.

if the terms in one layer are in G_i then the non-variable terms in the next layer are not in G_i.

As proved in [BT02], the sets $G_1^\infty, G_2^\infty, G^\infty$ satisfy the following two properties.

Lemma 4.13 *Let $i \in \{1, 2\}$. For any bijection α of V onto Z_2 the following holds:*

1. $[\![G_i^\infty \setminus V]\!]_\alpha^{\mathcal{F}} \subseteq Z_{2,i}$;
2. *for all $t_1, t_2 \in G_i^\infty \setminus V$, if $[\![t_1]\!]_\alpha^{\mathcal{F}} = [\![t_2]\!]_\alpha^{\mathcal{F}}$ then $t_1 =_E t_2$.*

Proposition 4.14 *The set G^∞ is Σ-base of $E = E_1 \cup E_2$.*

Note that the above proposition entails by Theorem 3.3 that Σ is a set of constructors for E. Using these two properties we can now show that $\mathcal{A}$ is a free model of E.

Proposition 4.15 *$\mathcal{A}$ is free in E over Z_2.*

Proof. We have seen that $\mathcal{A}$, the subalgebra of $\mathcal{F}$ generated by Z_2, is a model of E. Let $t_1, t_2 \in T(\Sigma_1 \cup \Sigma_2, V)$ such that $(\mathcal{A}, \alpha) \models t_1 \equiv t_2$ for some injective valuation α of $\mathcal{V}ar(t_1 \equiv t_2)$ into Z_2. By Proposition 2.6 it is enough to show that $t_1 =_E t_2$.

We know from Lemma 2.2 that $(\mathcal{F}, \alpha) \models t_1 \equiv t_2$ as well because $t_1 \equiv t_2$ is a quantifier-free formula and $\mathcal{A}$ is a subalgebra of $\mathcal{F}$ containing the elements of $\alpha(\mathcal{V}ar(t_1 \equiv t_2))$. Let us assume—with no loss of generality by Proposition 4.14 and Definition 3.2—that for each $i = 1, 2$, t_i has the form $s_i(\mathbf{r}_i)$ where s_i is a Σ-term and $\mathbf{r}_i$ consists of elements of $G^\infty = G_1^\infty \cup G_2^\infty$. Let us also assume that the tuple $\mathbf{r}_1, \mathbf{r}_2$ contains at least one term from G_1^∞ (if all the components of $\mathbf{r}_1, \mathbf{r}_2$ are from G_2^∞ the proof is symmetrical).

Let $t_1' \equiv t_2'$ be the Σ_1-equation obtained from $t_1 \equiv t_2$ by means of the following abstraction process. For each $i = 1, 2$ and r' in $\mathbf{r}_i$,

- if $r' \in G_2^\infty \setminus V$, then r' is replaced by a fresh variable;
- if $r' \in G_1^\infty \setminus V$, then r' has the form $r(r_1, \ldots, r_n)$ where r_j is an element of G_2^∞ for all $j \in \{1, \ldots, n\}$ (cf. Definition 4.12); in that case, each $r_j \in G_2^\infty \setminus V$ is replaced by a fresh variable.

Furthermore, the new variables are chosen so that every two abstracted terms are replaced by the same variable iff they are equivalent in E. By Lemma 4.13, $[\![r']\!]_\alpha^{\mathcal{F}} \in Z_{2,2}$ and $[\![r']\!]_\alpha^{\mathcal{F}} \neq [\![r'']\!]_\alpha^{\mathcal{F}}$ for all abstracted terms r', r'' such that $r' \neq_E r''$. It is then not hard to see that it is possible to extend α to an injective valuation β of

$\mathcal{V}ar(t'_1 \equiv t'_2)$ into $X'_1 = Z_2 \cup Z_{2,2}$ such that $(\mathcal{F}, \beta) \models t'_1 \equiv t'_2$. With such a β, we have that $(\mathcal{F}_1, \beta) \models t'_1 \equiv t'_2$, given that $t'_1 \equiv t'_2$ is a Σ_1-formula.

Recalling that, by Lemma 4.11, $\mathcal{F}_1$ is free in E_1 over X'_1, we can conclude by Proposition 2.6 that $t'_1 =_{E_1} t'_2$, which entails that $t'_1 =_E t'_2$ because $E = E_1 \cup E_2$. Now, it is easy to see that, by construction of $t'_1 \equiv t'_2$, there is a substitution σ such that $t_1 =_E t'_1\sigma$ and $t_2 =_E t'_2\sigma$. From this it follows immediately that $t_1 =_E t_2$. □

Corollary 4.16 *Where α is any bijection of V onto Z_2, let $Y := [\![G^\infty]\!]^{\mathcal{A}}_\alpha$. Then the following holds:*

1. *$Y \subseteq Y_2$;*
2. *$\mathcal{A}^\Sigma$ is free in E^Σ over Y;*

Proof. (1) Recall that $G^\infty := G_1^\infty \cup G_2^\infty \supseteq V$. Let $t \in G^\infty$ and observe that $[\![t]\!]^{\mathcal{A}}_\alpha = [\![t]\!]^{\mathcal{F}}_\alpha$ because $\mathcal{A}$ is the subalgebra of $\mathcal{F}$ generated by Z_2 and α is a bijection of V onto Z_2. Now, if $t \in V$ then, by construction of α, $[\![t]\!]^{\mathcal{A}}_\alpha = \alpha(t) \in Z_2 \subseteq Y_2$. If $t \in G_i^\infty \setminus V$ then, by Lemma 4.13, $[\![t]\!]^{\mathcal{A}}_\alpha \in Z_{2,i} \subseteq Y_2$.

(2) By Proposition 4.15, Proposition 4.14 and Corollary 3.4. □

For the rest of this section we will fix

- a bijection α of V onto Z_2 and
- the corresponding set $Y := [\![G^\infty]\!]^{\mathcal{A}}_\alpha$.

Then we will consider, for $i = 1, 2$, the family $\{[\![G_i^n]\!]^{\mathcal{A}}_\alpha \mid n \geq 0\}$ of subsets of Y. Since $\mathcal{A}$ is the subalgebra of $\mathcal{F}$ generated by Z_2 and α is a valuation of V into Z_2, it is easy to see that $[\![G_i^n]\!]^{\mathcal{A}}_\alpha = [\![G_i^n]\!]^{\mathcal{F}}_\alpha$ for all $n \geq 0$. To simplify the notation then, in the following we will write just $[\![G_i^n]\!]$ in place of either $[\![G_i^n]\!]^{\mathcal{A}}_\alpha$ or $[\![G_i^n]\!]^{\mathcal{F}}_\alpha$.

Observe that $[\![G_1^0]\!] = [\![G_2^0]\!] = Z_2$ and $[\![G_i^n]\!] \subseteq [\![G_i^{n+1}]\!]$ for all $n \geq 0$ and $i = 1, 2$. Given that $[\![G_i^n]\!] \setminus Z_2 \subseteq [\![G_i^n \setminus V]\!]^{\mathcal{A}}_\alpha$, we can conclude by Lemma 4.13 that $[\![G_i^n]\!] \setminus Z_2 \subseteq Z_{2,i}$.[16] By Corollary 4.16 we have that

$$\bigcup_{n \geq 0} ([\![G_1^n]\!] \cup [\![G_2^n]\!]) = [\![\bigcup_{n \geq 0} (G_1^n \cup G_2^n)]\!] = [\![G_1^\infty \cup G_2^\infty]\!] = [\![G^\infty]\!] = Y.$$

Now consider the family of sets $\{C_i^n \mid n \geq 0\}$, depicted in Figure 2 along with $\{[\![G_i^n]\!] \mid n \geq 0\}$ and defined as follows:

$$\begin{aligned} C_i^0 &:= [\![G_i^0]\!], \\ C_i^{n+1} &:= [\![G_i^{n+1}]\!] \setminus [\![G_i^n]\!]. \end{aligned}$$

[16] This entails that $[\![G_1^m]\!] \setminus Z_2$ is disjoint with $[\![G_2^n]\!] \setminus Z_2$ for all $m, n > 0$.

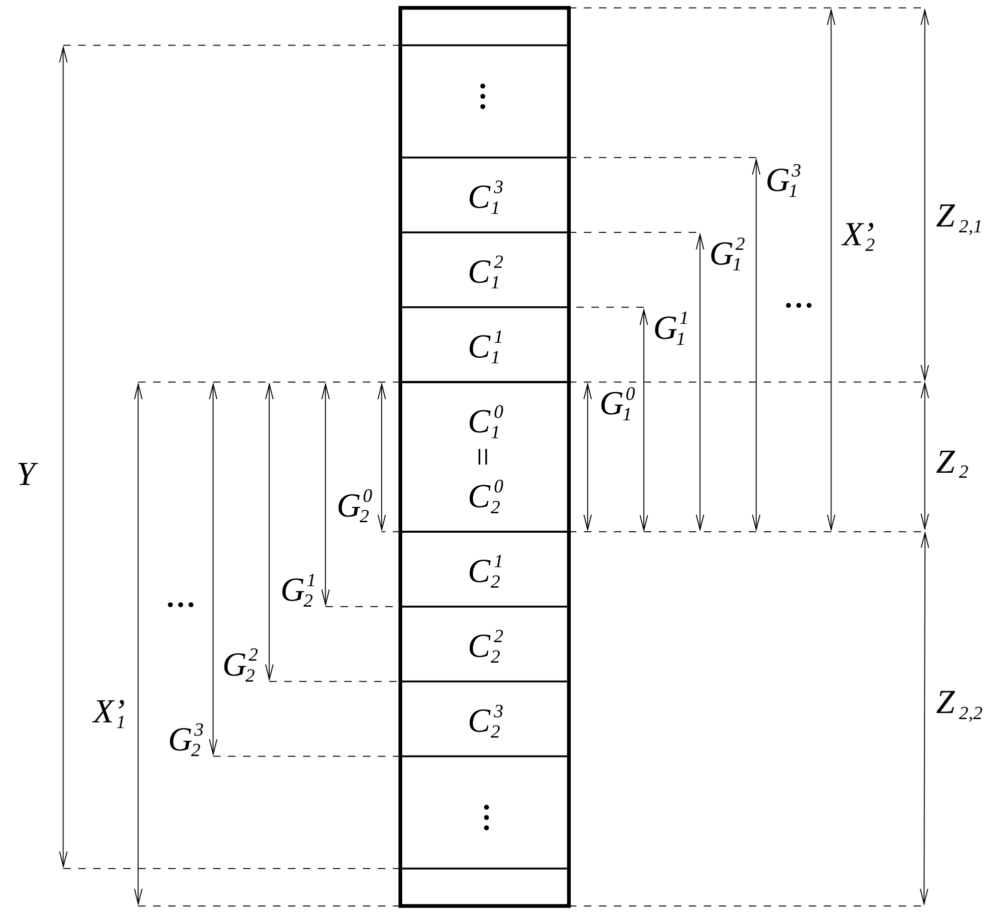

Figure 2: The families $\{[\![G_i^n]\!] \mid n \geq 0\}$ and $\{C_i^n \mid n \geq 0\}$.

First note that

$$\bigcup_{n \geq 0} (C_1^n \cup C_2^n) = \bigcup_{n \geq 0} ([\![G_1^n]\!] \cup [\![G_2^n]\!]) = Y.$$

Then note that, for all $n \geq 0$ and $i = 1, 2$, the elements of C_i^n are individuals of the algebras $\mathcal{F}_1$ and $\mathcal{F}_2$ (which have the same universe). By the above, $C_1^n \subseteq [\![G_1^n]\!] \subseteq Z_{2,1} \cup Z_2 = X_2'$; in other words, every element of C_1^n is a generator of $\mathcal{F}_2$. Similarly, $C_2^n \subseteq [\![G_2^n]\!] \subseteq Z_{2,2} \cup Z_2 = X_1'$, that is, every element of C_2^n is a generator of $\mathcal{F}_1$.

The family $\{C_i^n \mid n \geq 0\}$ satisfies the properties below, which will be useful in proving the completeness of the combination procedure.

Lemma 4.17 *For all distinct $m, n \geq 0$ the following holds.*

1. $C_i^m \cap C_i^n = \emptyset$ *for all* $i = 1, 2$;

2. C_1^{n+1} *is* Σ_1*-generated by* $[\![G_2^n]\!]$ *in* $\mathcal{F}_1$;

3. C_2^{n+1} *is* Σ_2*-generated by* $[\![G_1^n]\!]$ *in* $\mathcal{F}_2$.

Proof. Point 1 is immediate by construction of $\{C_i^n \mid n \geq 0\}$ and earlier observations on $\{[\![G_i^n]\!] \mid n \geq 0\}$ $(i = 1, 2)$. We prove Point 2 only, as the proof for Point 3 is symmetrical.

Let us start by observing that $C_i^{n+1} \subseteq [\![G_1^{n+1}]\!] \setminus [\![G_1^n]\!] \subseteq [\![G_1^{n+1} \setminus G_1^n]\!]_\alpha^{\mathcal{F}}$. From Definition 4.12 we know that for each $a \in [\![G_1^{n+1} \setminus G_1^n]\!]_\alpha^{\mathcal{F}}$ there is a term of the form $r(\mathbf{r})$ where $r \in G_1$ and $\mathbf{r} \in (G_2^n)^*$ such that $a = [\![r(\mathbf{r})]\!]_\alpha^{\mathcal{F}}$. Recalling that $[\![G_2^n]\!] \subseteq Z_{2,2} \cup Z_2 = X_1'$ and that $G_1 \subseteq T(\Sigma_1, V)$, we can conclude that a is Σ_1-generated by $[\![G_2^n]\!]$ in $\mathcal{F}$ and so in $\mathcal{F}_1$. □

To prove the correctness of the combination procedure, that is, to prove Theorem 4.1, we will use Proposition 4.21 below, relating satisfiability in the free model $\mathcal{A}$ of $E = E_1 \cup E_2$ to satisfiability in the free model $\mathcal{A}_1$ of E_1 and in the free model $\mathcal{A}_2$ of E_2, introduced at the beginning of this section. To prove Proposition 4.21 though we need three more lemmas.

Lemma 4.18 *Let* $i \in \{1, 2\}$. *If* f *is an automorphism of* $\mathcal{F}_i$ *such that* $f(X_i') \subseteq X_i'$, *then* $f(X_1' \cup X_2') \subseteq X_1' \cup X_2'$.

Proof. We start by considering $\mathcal{F}_2$ first. Let f be an automorphism of $\mathcal{F}_2$ such that $f(X_2') \subseteq X_2'$ and let $a \in X_1' \cup X_2'$. We show that $f(a) \in X_1' \cup X_2'$.

By Lemma 4.11, $X_1' \cup X_2' = Y_2 = [\![G_2]\!]_{\alpha_2}^{\mathcal{F}_2}$ where α_2 is a bijective valuation of the variables V onto X_2'. This means that there is a term $r \in G_2$ such that $a = [\![r]\!]_{\alpha_2}^{\mathcal{F}_2}$. Let σ be the substitution with domain $\mathcal{V}ar(r)$ such that $v\sigma = \alpha_2^{-1}(f(\alpha_2(v)))$ for all $v \in \mathcal{V}ar(r)$. Since $f(X_2') \subseteq X_2'$ and α_2, f are bijections, σ is well-defined and is a renaming. Since G_2 is closed under renaming by assumption, we then know that $r\sigma \in G_2$ as well, which entails that $[\![r\sigma]\!]_{\alpha_2}^{\mathcal{F}_2} \in X_1' \cup X_2'$. Let $\mathbf{v}$ be a tuple collecting the variables of r. The claim that $f(a) \in X_1' \cup X_2'$ then follows from the fact that $f(a) = f(r^{\mathcal{F}_2}(\alpha_2(\mathbf{v}))) = r^{\mathcal{F}_2}(f(\alpha_2(\mathbf{v}))) = r^{\mathcal{F}_2}(\alpha_2(\alpha_2^{-1}(f(\alpha_2(\mathbf{v}))))) = r^{\mathcal{F}_2}(\alpha_2(\mathbf{v}\sigma)) = [\![r\sigma]\!]_{\alpha_2}^{\mathcal{F}_2}$.

The proof for $\mathcal{F}_1$ is similar to the one above. It uses the fact that $X_1' \cup X_2' = [\![G_1]\!]_{h \circ \alpha_1}^{\mathcal{F}_1}$, again by Lemma 4.11, and G_1 is closed under renaming. □

Lemma 4.19 *Let* $i \in \{1, 2\}$. *Let* $\mathbf{a}_1 \in (X_1' \cup X_2')^*$ *and let* $\mathbf{x}_1$ *be any tuple of* $(X_i')^*$ *that* Σ_i*-generates* $\mathbf{a}_1$ *in* $\mathcal{F}_i$. *For every* Σ_i*-formula* $\varphi(\mathbf{v}_1, \mathbf{v}_2)$ *such that* $\mathcal{F}_i \models \exists \mathbf{v}_2\, \varphi(\mathbf{a}_1, \mathbf{v}_2)$, *there is a Σ-instantiation ρ of $\mathbf{v}_2$, a tuple $\mathbf{a}_2 \in (X'_1 \cup X'_2)^*$ and a tuple $\mathbf{z}_2 \in Z_2^*$ such that $\mathbf{a}_2$ is Σ_i-generated by $\mathbf{x}_1, \mathbf{z}_2$ in $\mathcal{F}_i$ and $\mathcal{F}_i \models (\varphi\rho)(\mathbf{a}_1, \mathbf{a}_2)$.*[17]

Proof. Let $\varphi(\mathbf{v}_1, \mathbf{v}_2)$ be a Σ_i-formula such that $\mathcal{F}_i \models \exists \mathbf{v}_2\, \varphi(\mathbf{a}_1, \mathbf{v}_2)$. Since $\mathcal{F}^\Sigma$ (and so ${\mathcal{F}_i}^\Sigma$) is Σ-generated by $Y_2 = X'_1 \cup X'_2$ by Lemma 4.11, there is a Σ-instantiation ρ of $\mathbf{v}_2$ and a tuple $\mathbf{b}_2 \in (X'_1 \cup X'_2)^*$ such that $\mathcal{F}_i \models (\varphi\rho)(\mathbf{a}_1, \mathbf{b}_2)$.

Since $\mathbf{b}_2$ is finite, $\mathbf{x}_1 \subseteq (X'_i)^*$, and $\mathcal{F}_i$ is Σ_i-generated by X'_i, there is a tuple $\mathbf{x}_2 \in (X'_i)^*$ disjoint from $\mathbf{x}_1$ and such that $\mathbf{x}_1, \mathbf{x}_2$ Σ_i-generates $\mathbf{b}_2$. Recalling that the subset Z_2 of X'_i is infinite, let f_0 be any bijection of X'_i onto itself that fixes $\mathbf{x}_1$ and moves $\mathbf{x}_2$ into Z_2.

From the fact that $\mathcal{F}_i$ is free over X'_i by Lemma 4.11 and from standard results about free algebras [Hod93], we know that every bijection of X'_i onto itself extends (univocally) to an automorphism of $\mathcal{F}_i$. Where f is the automorphism of $\mathcal{F}_i$ extending f_0, let $\mathbf{z}_2 := f(\mathbf{x}_2)$ and $\mathbf{a}_2 := f(\mathbf{b}_2)$. Note that $f(\mathbf{a}_1) = \mathbf{a}_1$ because $\mathbf{a}_1$ is Σ_i-generated by $\mathbf{x}_1$ and f is a Σ_i-automorphism that fixes $\mathbf{x}_1$.

Since $\mathbf{b}_2 \in (X'_1 \cup X'_2)^*$, we have by Lemma 4.18 that $\mathbf{a}_2 = f(\mathbf{b}_2) \in (X'_1 \cup X'_2)^*$. Using the fact that f is an automorphism, it is not hard to show that $\mathbf{a}_2$ is Σ_i-generated by $\mathbf{x}_1, \mathbf{z}_2$ and $\mathcal{F}_i \models (\varphi\rho)(\mathbf{a}_1, \mathbf{a}_2)$. □

Lemma 4.20 *Let $i, j \in \{1, 2\}$ with $i \neq j$, $a \in X'_1 \cup X'_2$ and $X \subseteq X'_i$. If a is Σ_i-generated by X in $\mathcal{F}_i$, then $a \in X \cup X'_j$.*

Proof. Ad absurdum, assume that $a \notin X \cup X'_j$. Then $a \in (X'_1 \cup X'_2) \setminus (X'_j \cup X) = X'_i \setminus X$. Recalling that $X \subseteq X'_i$, and X'_i is a set of generators for $\mathcal{F}_i$, this entails that $X'_i \setminus \{a\}$ is also a set of generators for $\mathcal{F}_i$. But that is impossible because X'_i, for being the basis of the free algebra $\mathcal{F}_i$, cannot be a redundant set of generators for $\mathcal{F}_i$, as one can easily show. □

Proposition 4.21 *Let $\varphi_i(\mathbf{v}, \mathbf{u}_i)$ be a conjunction of Σ_i-equations where $\mathbf{v}$ lists the elements of $\mathcal{V}ar(\varphi_1) \cap \mathcal{V}ar(\varphi_2)$ and, for $i = 1, 2$, $\mathbf{u}_i$ lists the elements of $\mathcal{V}ar(\varphi_i)$ not in $\mathbf{v}$. The following are equivalent.*

1. *There is a Σ-instantiation ρ of $\mathbf{v}$, an identification ξ of $\mathcal{V}ar(\mathbf{v}\rho)$ and a grouping $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$ of $\mathcal{V}ar(\mathbf{v}\rho\xi)$ with each element of $\mathcal{V}ar(\mathbf{v}\rho\xi)$ occurring exactly once in $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$ such that*

$$\begin{array}{lcl} \mathcal{A}_1 & \models & \exists \mathbf{v}_1\, \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{v}_{2m-1}\, \forall \mathbf{v}_{2m}\, \exists \mathbf{u}_1.\ (\varphi_1 \rho \xi) \quad \textit{and} \\ \mathcal{A}_2 & \models & \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ (\varphi_2 \rho \xi). \end{array}$$

[17] The tuple $\mathbf{x}_1$ exists because $\mathcal{F}_i$ is Σ_i-generated by X'_i by Lemma 4.11 and $\mathbf{a}_1$ is finite. In $(\varphi\rho)(\mathbf{a}_1, \mathbf{a}_2)$, $\mathbf{a}_2$ is a tuple of values assigned to the free variables of $\varphi\rho$.

2. $\mathcal{A} \models \exists \mathbf{v} \exists \mathbf{u}_1 \exists \mathbf{u}_2.\ (\varphi_1 \wedge \varphi_2)$.

Proof. ($1 \Rightarrow 2$) Let $\varphi_i' := \varphi_i \rho \xi$ for $i = 1, 2$. By Lemma 4.11 we have that

$$\begin{aligned} &\mathcal{F}_1 \models \exists \mathbf{v}_1\, \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{v}_{2m-1}\, \forall \mathbf{v}_{2m}\, \exists \mathbf{u}_1.\ \varphi_1'(\mathbf{v}_1, \dots, \mathbf{v}_{2m}, \mathbf{u}_1) \quad \text{and} \\ &\mathcal{F}_2 \models \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ \varphi_2'(\mathbf{v}_1, \dots, \mathbf{v}_{2m}, \mathbf{u}_2). \end{aligned}$$

By a special case of Lemma 4.19 (in which $\mathbf{v}_1$ there is empty), we know that there is a Σ-instantiation ρ_1 of $\mathbf{v}_1$, a tuple $\mathbf{a}_1 \in (X_1' \cup X_2')^*$ and a tuple $\mathbf{z}_1 \in Z_2^*$ such that $\mathbf{a}_1$ is Σ_1-generated by $\mathbf{z}_1$ and

$$\mathcal{F}_1 \models \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{u}_1.\ \varphi_1' \rho_1(\mathbf{a}_1, \mathbf{v}_2, \dots, \mathbf{u}_1).$$

By Lemma 4.20, we also know that every element of $\mathbf{a}_1$ is in $\mathbf{z_1} \cup X_2' = X_2'$.[18] Since $\mathbf{v}_1$ is universally quantified in φ_2', we have that

$$\mathcal{F}_2 \models \exists \mathbf{v}_2\, \cdots\, \exists \mathbf{u}_2.\ \varphi_2' \rho_1(\mathbf{a}_1, \mathbf{v}_2, \dots, \mathbf{u}_1).$$

Now, recall that $\mathcal{F}_2$ is free over X_2' which means that $\mathbf{a}_1$ is Σ_2-generated by itself in $\mathcal{F}_2$. By Lemma 4.19, there is a Σ-instantiation ρ_2 of $\mathbf{v}_2$, a tuple $\mathbf{a}_2 \in (X_1' \cup X_2')^*$ and a tuple $\mathbf{z}_2 \in Z_2^*$ such that $\mathbf{a}_2$ is Σ_2-generated by $\mathbf{a}_1, \mathbf{z}_2$ and

$$\mathcal{F}_2 \models \forall \mathbf{v}_3\, \cdots\, \exists \mathbf{u}_2.\ \varphi_2' \rho_1 \rho_2(\mathbf{a}_1, \mathbf{a}_2, \mathbf{v}_3, \dots, \mathbf{u}_1).$$

By Lemma 4.20, every element a of $\mathbf{a}_2$ is in $\mathbf{a}_1, \mathbf{z}_2 \cup X_1' = \mathbf{a}_1 \cup X_1'$. This means that every such a is either Σ_1-generated by itself in $\mathcal{F}_1$ (if $a \in X_1'$) or by $\mathbf{z}_1$ (if $a \in \mathbf{a}_1$). Let $\mathbf{a}_2'$ be a tuple collecting all the elements of $\mathbf{a}_2$ that are generated by themselves.

Since $\mathbf{v}_2$ is universally quantified in ψ_1 we have that

$$\mathcal{F}_1 \models \exists \mathbf{v}_3\, \cdots\, \exists \mathbf{u}_1.\ \varphi_1' \rho_1 \rho_2(\mathbf{a}_1, \mathbf{a}_2, \mathbf{v}_3, \dots, \mathbf{u}_1).$$

By Lemma 4.19, there is a Σ-instantiation ρ_3 of $\mathbf{v}_3$, a tuple $\mathbf{a}_3 \in (X_1' \cup X_2')^*$ and a tuple $\mathbf{z}_3 \in Z_2^*$ such that $\mathbf{a}_3$ is Σ_1-generated by $\mathbf{z}_1, \mathbf{a}_2', \mathbf{z}_3$ (and so by $\mathbf{z}_1, \mathbf{a}_2, \mathbf{z}_3$) in $\mathcal{F}_1$ and

$$\mathcal{F}_1 \models \forall \mathbf{v}_4\, \cdots\, \exists \mathbf{u}_1.\ \varphi_1' \rho_1 \rho_2 \rho_3(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{u}_1).$$

Iterating the argument above one can show that

$$\begin{aligned} &\mathcal{F}_1 \models \exists \mathbf{u}_1.\ \varphi_1' \rho_1 \cdots \rho_{2m}(\mathbf{a}_1, \dots, \mathbf{a}_{2m}, \mathbf{u}_1) \quad \text{and} \\ &\mathcal{F}_2 \models \exists \mathbf{u}_2.\ \varphi_2' \rho_1 \dots \rho_{2m}(\mathbf{a}_1, \dots, \mathbf{a}_{2m}, \mathbf{u}_2) \end{aligned}$$

where, for each $k \in \{1, \dots, m\}$,

[18] Abusing the notation a little we denote by $\mathbf{z_1} \cup X_2'$ the union of X_2' with the set of $\mathbf{z_1}$'s components. (Similarly, later on.)

- ρ_{2k-1} and ρ_{2k} are Σ-instantiations of $\mathbf{v}_{2k-1}$ and $\mathbf{v}_{2k}$ respectively,
- $\mathbf{a}_{2k-1}$ is Σ_1-generated by $\mathbf{z}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{2k-2}, \mathbf{z}_{2k-1}$ in $\mathcal{F}_1$ and
- $\mathbf{a}_{2k}$ is Σ_2-generated by $\mathbf{a}_1, \mathbf{z}_2, \ldots, \mathbf{a}_{2k-1}, \mathbf{z}_{2k}$ in $\mathcal{F}_2$,

and all the elements of the "z" tuples are in Z_2.

Let $\rho = \rho_1 \cdots \rho_{2m}$. In a similar way one can show that

$$\mathcal{F}_1 \models \varphi_1' \rho \sigma_1(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_1) \quad \text{and}$$
$$\mathcal{F}_2 \models \varphi_2' \rho \sigma_2(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_2)$$

where

- σ_1 and σ_2 are Σ-instantiations of $\mathbf{u}_1$ and $\mathbf{u}_2$ respectively,
- $\mathbf{b}_1$ is Σ_1-generated by $\mathbf{z}_1, \mathbf{a}_2, \ldots, \mathbf{z}_{2n-1}, \mathbf{a}_{2m}, \mathbf{z}_{2n+1}$ in $\mathcal{F}_1$ for some $\mathbf{z}_{2n+1} \in Z_2^*$ and
- $\mathbf{b}_2$ is Σ_2-generated by $\mathbf{a}_1, \mathbf{z}_2, \ldots, \mathbf{a}_{2n-1}, \mathbf{z}_{2m}, \mathbf{z}_{2n+2}$ in $\mathcal{F}_2$ for some $\mathbf{z}_{2n+2} \in Z_2^*$.

In conclusion, recalling that $\mathcal{F}_i = \mathcal{F}^{\Sigma_i}$ for $i = 1, 2$, we have shown that

$$\mathcal{F} \models \varphi_1' \rho \sigma_1(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_1) \wedge \varphi_2' \rho \sigma_2(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_2).$$

By an simple induction argument we can show that the components of $\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_1, \mathbf{b}_2$ are all $(\Sigma_1 \cup \Sigma_2)$-generated by Z_2 in $\mathcal{F}$. Therefore, they are all individuals of $\mathcal{A}$, the subalgebra of $\mathcal{F}$ generated by Z_2. Since $\varphi_1' \rho \sigma_1 \wedge \varphi_2' \rho \sigma_2$ is quantifier-free, we have by Lemma 2.2 that

$$\mathcal{A} \models \varphi_1' \rho \sigma_1(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_1) \wedge \varphi_2' \rho \sigma_2(\mathbf{a}_1, \ldots, \mathbf{a}_{2m}, \mathbf{b}_2)$$

from which the claim easily follows.

($2 \Rightarrow 1$) Assume that $\mathcal{A} \models \exists \mathbf{v}, \mathbf{u}_1, \mathbf{u}_2.\ (\varphi_1(\mathbf{v}, \mathbf{u}_1) \wedge \varphi_2(\mathbf{v}, \mathbf{u}_2))$. Let α be the bijection of V onto Z_2 and Y the subset of Y_2 that we fixed after Corollary 4.16. Since the reduct $\mathcal{A}^{\Sigma}$ of $\mathcal{A}$ is Σ-generated by Y by Point 2 of the corollary, there certainly is a Σ-instantiation ρ of $\mathbf{v}$, an identification ξ of $\mathcal{V}ar(\mathbf{v}\rho)$, and an injective valuation β of $\mathbf{v}'$ into Y such that

$$(\mathcal{A}, \beta) \quad \models \quad \exists \mathbf{u}_1, \mathbf{u}_2.\ (\varphi_1'(\mathbf{v}', \mathbf{u}_1) \wedge \varphi_2'(\mathbf{v}', \mathbf{u}_2)),$$

where $\varphi_i' := \varphi_i \rho \xi$ for $i = 1, 2$, $\mathbf{v}'$ lists the the variables of $\mathbf{v}\rho\xi$. From this, recalling that $\mathcal{A}$ is $(\Sigma_1 \cup \Sigma_2)$-generated by Z_2 by construction and Y is included in Y_2, we can conclude that there is a tuple $\mathbf{a}$ of *pairwise distinct* elements of Y_2, all $(\Sigma_1 \cup \Sigma_2)$-generated by Z_2, such that

$$\mathcal{A} \models \exists \mathbf{u}_1, \mathbf{u}_2.\ \varphi_1'(\mathbf{a}, \mathbf{u}_1) \wedge \varphi_2'(\mathbf{a}, \mathbf{u}_2).$$

Since $\mathcal{A}$ is a subalgebra of $\mathcal{F}$ and $\varphi_1' \wedge \varphi_2'$ is quantifier-free, it follows by Lemma 2.2 that $\mathcal{F} \models \exists \mathbf{u}_1, \mathbf{u}_2.\ \varphi_1'(\mathbf{a}, \mathbf{u}_1) \wedge \varphi_2'(\mathbf{a}, \mathbf{u}_2)$ as well. Given that each φ_i' is a Σ_i-formula and $\mathbf{u}_1$ and $\mathbf{u}_2$ are disjoint, we have then that

$$\mathcal{F}_1 \models \exists \mathbf{u}_1.\ \varphi_1'(\mathbf{a}, \mathbf{u}_1) \quad \text{and} \quad \mathcal{F}_2 \models \exists \mathbf{u}_2.\ \varphi_2'(\mathbf{a}, \mathbf{u}_2). \tag{7}$$

We construct a partition of the elements of $\mathbf{a}$ that will induce a grouping of $\mathbf{v}'$ having the properties listed in Point 1 of the proposition. For that, we will use the families $\{C_1^n \mid n \geq 0\}$ and $\{C_2^n \mid n \geq 0\}$ of Lemma 4.17.

First, let $\mathbf{a}_1$ be a tuple collecting the components of $\mathbf{a}$ that are in $C_1^0 \cup C_1^1$. Then, for all $n > 1$, let $\mathbf{a}_n$ be a tuple collecting the components of $\mathbf{a}$ that are in C_1^n. Finally, for all $n > 0$, let $\mathbf{b}_n$ be a tuple collecting the components of $\mathbf{a}$ that are in C_2^n.[19]

Since $\mathbf{a}$ is a (finite) tuple of Y^* and $Y = \bigcup_{n \geq 0} (C_1^n \cup C_2^n)$ as observed earlier, there is a smallest $m \geq 0$ such that every component of $\mathbf{a}$ is in $\bigcup_{n=0}^m (C_1^n \cup C_2^n)$. Let $n \in \{0, \ldots, m-1\}$. By Lemma 4.17(3), $\mathbf{b}_{n+1}$ is Σ_2-generated by $[\![G_1^n]\!]$ in $\mathcal{F}_2$. Let Z_{n+1} be any finite subset of $[\![G_1^n]\!]$ that generates $\mathbf{b}_{n+1}$. Now recall that $\mathcal{F}_2$ is free over the countably-infinite set X_2'. We prove that $\mathbf{a}_1, \ldots, \mathbf{a}_m$, $\mathbf{b}_1, \ldots, \mathbf{b}_m$ and $Z_1, \ldots, Z_m$ satisfy Lemma 2.7.

To start with, we have that $\mathbf{a}_n \in (X_2')^*$ for all $n \in \{1, \ldots, m\}$ because $C_1^n \subseteq [\![G_1^n]\!] \subseteq X_2'$ by construction of C_1^n. From Lemma 4.17(1) it follows that the tuples $\mathbf{a}_n$ and $\mathbf{a}_{n'}$ are pairwise disjoint for all distinct $n, n' \in \{1, \ldots, m\}$, which means that all components of $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are distinct. Now let $n \in \{1, \ldots, m-1\}$. Observe that the set $Z_1 \cup \cdots \cup Z_n$ is included in $[\![G_1^{n-1}]\!] = C_1^0 \cup \cdots \cup C_1^{n-1}$ whereas every component of $\mathbf{a}_{n+1}$ belongs to C_1^{n+1}. It follows that no components of $\mathbf{a}_{n+1}$ are in $Z_1 \cup \cdots \cup Z_n$. Finally, where f is the bijection that maps, in order, the components of $\mathbf{a}$ to those of $\mathbf{v}'$, let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2m-1}, \mathbf{v}_{2m}$ be the rearrangement of $\mathbf{v}'$ corresponding to $\mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{a}_m, \mathbf{b}_m$ according to f. From (7) above we know that $\mathcal{F}_2 \models \exists \mathbf{u}_2.\ \varphi_2'(\mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{a}_m, \mathbf{u}_2)$. By Lemma 2.7 we can then conclude that $\mathcal{F}_2 \models \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ \varphi_2'$.

One can prove almost symmetrically that $\mathcal{F}_1 \models \exists \mathbf{v}_1 \forall \mathbf{v}_2 \cdots \exists \mathbf{v}_{2m-1} \forall \mathbf{v}_{2m} \exists \mathbf{u}_1.\ \varphi_1'$.[20] The claim then follows from the fact that $\mathcal{F}_i$ is Σ_i-isomorphic to $\mathcal{A}_i$ for $i = 1, 2$ by Lemma 4.11. □

[19] Each tuple above is meant to have no repeated components, and may be empty.

[20] The proof is not completely symmetric to the previous one because to use Lemma 2.7 again one must consider the tuples $\mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{b}_m, \mathbf{a}_m, \mathbf{b}_{m+1}$ and $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2m-1}, \mathbf{v}_{2m}, \mathbf{v}_{2m+1}$ where $\mathbf{b}_0$, $\mathbf{b}_{m+1}$, $\mathbf{v}_0$ and $\mathbf{v}_{2m+1}$ are all empty.

We can finally prove Theorem 4.1.

Proof of Theorem 4.1. Let $\exists \mathbf{w}.\ \varphi(\mathbf{w})$ be a $(\Sigma_1 \cup \Sigma_2)$-formula taken as input by the procedure. Recall that $\mathcal{A}$, $\mathcal{A}_1$ and $\mathcal{A}_2$ are free models E, E_1 and E_2, respectively and all of them have an infinite basis. Since both $\exists \mathbf{w}.\ \varphi(\mathbf{w})$ and the sentences output by the procedure are positive sentences, by Lemma 2.8 it is enough to show that $\mathcal{A} \models \exists \mathbf{w}.\ \varphi(\mathbf{w})$ iff $\mathcal{A}_1 \models \gamma_1$ and $\mathcal{A}_2 \models \gamma_2$ for some possible output (γ_1, γ_2) of the procedure.

Let $\psi_1(\mathbf{w}) \vee \cdots \vee \psi_n(\mathbf{w})$ be a disjunctive normal form of $\varphi(\mathbf{w})$. Clearly, $\mathcal{A} \models \exists \mathbf{w}.\ \varphi(\mathbf{w})$ iff $\mathcal{A} \models \exists \mathbf{w}.\ \psi_j(\mathbf{w})$ for some $j \in \{1, \ldots, n\}$. Now, such ψ_j is a possible output of Step 1 of the procedure, so let $\varphi_1(\mathbf{v}, \mathbf{u}_1)$ and $\varphi_2(\mathbf{v}, \mathbf{u}_2)$ be the formulae produced by Step 2 when given ψ_j as input.

It is easy to show that $\mathcal{A} \models \exists \mathbf{w}.\ \psi_j(\mathbf{w})$ iff $\mathcal{A} \models \exists \mathbf{v}\, \exists \mathbf{u}_1\, \exists \mathbf{u}_2.\ (\varphi_1 \wedge \varphi_2)$. By Proposition 4.21, $\mathcal{A} \models \exists \mathbf{v}\, \exists \mathbf{u}_1\, \exists \mathbf{u}_2.\ (\varphi_1 \wedge \varphi_2)$ iff there is a Σ-instantiation ρ of $\mathbf{v}$, an identification ξ of $\mathcal{V}ar(\mathbf{v}\rho)$ and a grouping $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$ of $V_{\mathrm{s}} := \mathcal{V}ar(\mathbf{v}\rho\xi) = \mathcal{V}ar(\varphi_1\rho\xi) \cap \mathcal{V}ar(\varphi_2\rho\xi)$, with each element of V_{s} occurring exactly once in $\mathbf{v}_1, \ldots, \mathbf{v}_{2m}$ such that

$$\begin{array}{lcl} \mathcal{A}_1 & \models & \exists \mathbf{v}_1\, \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{v}_{2m-1}\, \forall \mathbf{v}_{2m}\, \exists \mathbf{u}_1.\ (\varphi_1\rho\xi) \quad \text{and} \\ \mathcal{A}_2 & \models & \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ (\varphi_2\rho\xi). \end{array}$$

Since the tuple $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2m-1}, \mathbf{v}_{2m}$ is a permutation of V_{s}, we can assume without loss of generality that $2 \leq 2m \leq |V_{\mathrm{s}}| + 1$. In fact, one can easily show that if $2m > |V_{\mathrm{s}}| + 1$ then for some $j \in \{2, \ldots, 2m-1\}$ the tuple $\mathbf{v}_j$ must be empty. In that case, $\mathbf{v}_j$ can be eliminated and the tuples $\mathbf{v}_{j-1}$ and $\mathbf{v}_{j+1}$—which have the same quantifier in each formula above—can be concatenated. To conclude the proof then, it is enough it observe that the pair

$$(\ \exists \mathbf{v}_1\, \forall \mathbf{v}_2\, \cdots\, \exists \mathbf{v}_{2m-1}\, \forall \mathbf{v}_{2m}\, \exists \mathbf{u}_1.\ (\varphi_1\rho\xi), \quad \forall \mathbf{v}_1\, \exists \mathbf{v}_2\, \cdots\, \forall \mathbf{v}_{2m-1}\, \exists \mathbf{v}_{2m}\, \exists \mathbf{u}_2.\ (\varphi_2\rho\xi)\ )$$

is indeed a possible output of the combination procedure. □

5 Related and Further Research

The combination procedure as well as the proof of correctness are modeled on the corresponding procedure and proof in [BS95]. The only extension to the procedure is Step 3, which takes care of the shared symbols. In the proof, one of the main obstacles to overcome was to find an amalgamation construction that works in the non-disjoint case. Several of the hard technical results used in the proof depend on results from our previous work on combining decision procedures for the word problem [BT02].

The definition of the sets G_i, which are vital for proving that the constructed algebra $\mathcal{A}$ is indeed free, is also borrowed from there. It should be noted, however, that this definition can also be seen as a generalization to the non-disjoint case of a syntactic amalgamation construction originally due to Schmidt-Schauß [SS89]. As already mentioned in the introduction, the notion of constructors used here is taken from [BT02, TR02].

The only other work on combining unification algorithms in the non-disjoint case is due to Domenjoud, Ringeissen and Klay [DKR94]. The main differences with our work are that (i) their notion of constructors is much more restrictive than ours (as shown in [BT02]); and (ii) they combine algorithms computing complete sets of unifiers, and thus their method cannot be used for combining decision procedures.

Our combined decidability results are limited to theories sharing constructors whose equational theory is finitary modulo renaming. We believe that the notion of constructors is as general as one can get, a conviction that is supported by the work on combining decision procedures for the word problem and for universal theories [BT02, TR02]. The stronger limitation on the applicability of our decidability result is the restriction to constructors whose theory is finitary modulo renaming. Thus, the main thrust of further research will be to remove or at least relax this restriction. For example, one could try to replace it by additional algorithmic requirements on the theories to be combined or on the constructor theory. For this, the work in [DKR94], which assumes algorithms computing complete sets of unifiers for the component theory, could be a starting point.

The combination results in [BS95] apply not only to equational theories, but to arbitrary *atomic* theories, i.e., theories over signatures containing additional relation symbols and axiomatized by a set of (universally quantified) atomic formulae. For simplicity we have considered just equational theories in this paper. However, all notions, results and proofs given here extend virtually unchanged to atomic theories sharing at most function symbols. When the theories also share relation symbols, one needs an appropriate extension of the notion of constructors that takes relation symbols into account (see [TR02]). By using that extended notion of constructors all the main results given here should continue to hold, with most of the proofs carrying over with minimal changes.

It is interesting to observe that the results presented here (as well as those in [BS95]) extend even beyond atomic theories. Apart from having to share constructor symbols (or no symbols at all), the only essential model-theoretic requirements on the component theories are that (1) their set of models is closed under substructures and (2) they admit a free model with countably infinitely-many generators. The largest class of first order-theories satisfying these two requirements is that of non-trivial universal Horn theories [Mak87]. This means that, *mutatis mutandis*, our results also apply to the union of non-trivial universal Horn theories sharing constructors. An alternative argument supporting this claim comes from the following two observations. First, a non-trivial universal Horn theory and its atomic theory have the same positive consequences. Second, the atomic theory of the union $\mathcal{T}_1 \cup \mathcal{T}_2$ of two universal Horn theories $\mathcal{T}_1, \mathcal{T}_2$ sharing constructors is logically equivalent to the union of the atomic theory of $\mathcal{T}_1$ and the atomic theory of $\mathcal{T}_2$. The first observation is an immediate consequence of fact that a Horn theory and its atomic theory have the same free models, and free models are canonical for positive consequences. The second one can be proved using a fusion construction like the one in Section 4.4.

References

[BN98] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, United Kingdom, 1998.

[BS92] Franz Baader and Klaus U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. In D. Kapur, editor, *Proceedings of the 11th International Conference on Automated Deduction*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 50–65. Springer-Verlag, 1992.

[BS95] Franz Baader and Klaus U. Schulz. Combination of constraint solving techniques: An algebraic point of view. In *Proceedings of the 6th International Conference on Rewriting Techniques and Applications, RTA'95*, volume 914 of *Lecture Notes in Computer Science*, pages 50–65. Springer-Verlag, 1995.

[BS96] Franz Baader and Klaus U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. *Journal of Symbolic Computation*, 21(2):211–243, February 1996.

[BT02] Franz Baader and Cesare Tinelli. Deciding the word problem in the union of equational theories. *Information and Computation*, 2002. (to appear) Preprint available at `ftp.cs.uiowa.edu/pub/tinelli/papers/BaaTin-IC-02.ps.gz`.

[DKR94] Eric Domenjoud, Francis Klay, and Christophe Ringeissen. Combination techniques for non-disjoint equational theories. In A. Bundy, editor, *Proceedings of the 12th International Conference on Automated Deduction*, *Nancy (France)*, volume 814 of *Lecture Notes in Artificial Intelligence*, pages 267–281. Springer-Verlag, 1994.

[Hod93] Wilfrid Hodges. *Model Theory*, volume 42 of *Enclyclopedia of mathematics and its applications*. Cambridge University Press, 1993.

[JK86] Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal on Computing*, 15(4):1155–1194, 1986.

[Mah88] M. J. Maher. Complete axiomatizations of finite, rational and infinite trees. In *LICS'88: Proceedings 3rd Symposium on Logic in Computer Science*, pages 348–357, Edinburgh, UK, June 1988.

[Mak87] J. A. Makowsky. Why Horn formulas matter in computer science: Initial structures and generic examples. *Journal of Computer and System Sciences*, 34:266–292, 1987.

[NO79] Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Trans. on Programming Languages and Systems*, 1(2):245–257, October 1979.

[Pig74] Don Pigozzi. The join of equational theories. *Colloquium Mathematicum*, 30(1):15–25, 1974.

[SS89] Manfred Schmidt-Schauß. Unification in a combination of arbitrary disjoint equational theories. *Journal of Symbolic Computation*, 8(1–2):51–100, July/August 1989. Special issue on unification. Part II.

[Sti81] Mark E. Stickel. A unification algorithm for associative commutative functions. *Journal of the ACM*, 28(3):423–434, 1981.

[TR02] Cesare Tinelli and Christophe Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 2002. (to appear) Preprint available at `ftp.cs.uiowa.edu/pub/tinelli/papers/TinRin-TCS-02.ps.gz`.