Unions of Equational Monadic Theories

Piotr Hoffman

Institute of Informatics, Warsaw University, Poland
piotrek@mimuw.edu.pl

Abstract. We investigate the decidability of unions of decidable equational theories. We focus on monadic theories, i.e., theories over signatures with unary symbols only. This allows us to make use of the equivalence between monoid amalgams and unions of monadic theories. We show that if the intersection theory is unitary, then the decidability of the union is guaranteed by the decidability of tensor products. We prove that if the intersection theory is a group or a group with zero, then the union is decidable. Finally, we show that even if the intersection theory is a 3-element monoid and is unitary, the union may be undecidable, but that it will always be decidable if the intersection is 2-element unitary. We also show that unions of regular theories, i.e., theories recognizable by finite automata, can be undecidable. However, we prove that they are decidable if the intersection theory is unitary.

Introduction

We consider the following question:

> If $\mathcal{S}$ and $\mathcal{T}$ are decidable equational theories, then under what assumptions is the union theory $\mathcal{S} \cup \mathcal{T}$ decidable as well?

The practical importance of this question is clear: our ability to combine decision procedures for $\mathcal{S}$ and $\mathcal{T}$ into a decision procedure for the union depends on it.

It is obvious that for the union $\mathcal{S} \cup \mathcal{T}$ to be decidable, something more is needed than just $\mathcal{S}$ and $\mathcal{T}$ being decidable themselves. Let Σ_S be the signature of $\mathcal{S}$ and Σ_T the signature of $\mathcal{T}$, and let $\Sigma_U = \Sigma_S \cap \Sigma_T$ be their intersection. As usual, we assume that any equation over Σ_U is a consequence of $\mathcal{S}$ iff it is a consequence of $\mathcal{T}$. This means that an intersection theory $\mathcal{U}$ over Σ_U exists which is conservatively extended by $\mathcal{S}$ and by $\mathcal{T}$.

Since 1974 it is known [1] that if Σ_U is empty, i.e., if $\mathcal{S}$ and $\mathcal{T}$ are built over disjoint signatures, then decidability of $\mathcal{S}$ and $\mathcal{T}$ implies the decidability of $\mathcal{S} \cup \mathcal{T}$. A few years ago it has been proved that if *effective $\mathcal{U}$-bases* of $\mathcal{S}$ and $\mathcal{T}$ exist, then the decidability of $\mathcal{S}$ and $\mathcal{T}$ implies the decidability of $\mathcal{S} \cup \mathcal{T}$ [2, 3].[1]

Following the ideas of [4], in our work we focus on *monadic* theories, that is, on theories over signatures in which all function symbols are unary (in fact, account is also taken of constants). This admittedly strong restriction makes the

[1] These results are succintly presented in Sect. 2.

research problem simpler, but far from trivial. It is therefore a perfect vehicle for testing ideas that may be later applied to theories in which symbols of arbitrary arities appear. As for theorems stating the *undecidability* of certain unions, there is of course no need to generalize them to non-monadic theories.

Three categories of results are presented in the paper. These are: results on unitary theories and links between unions and tensor products (Sect. 2), results on the decidability of unions built over group and group-like theories (Sect. 3), and results on the undecidability of certain unions (Sect. 4).

We start with Sect. 1, in which basic notions are defined. In Sect. 2 we first recall known results on theories over effective bases (Th. 1). We then show that if the intersection theory is unitary and the tensor products are decidable, then so is the union (Th. 2). In particular, unions of *regular* theories, that is, of theories recognizable by finite automata, are decidable if their intersection is unitary (Cor. 2). In Sect. 3 we show that a union of theories whose intersection is a group is decidable under certain liberal assumptions (Th. 3, Cor. 3); a similar result is proved for groups with zero (Th. 4). We start Sect. 4 by recalling [4] that a union of theories with unitary intersection may be undecidable (Th. 5). We then show that this is true even if one of those theories is regular with only 4 equivalence classes and the intersection is the theory of two boolean constants (Th. 6). We also prove that our example is minimal, i.e., if the intersection is unitary and regular with less than 3 equivalence classes, then the union is decidable (Prop. 3). Finally, we present a construction due to Sapir [5] which proves that even the union of two regular theories may be undecidable (Th. 7). We conclude by a discussion of the forms of assumptions that might guarantee decidability of theory unions and of possible generalizations of the obtained decidability results.

1 Unions of Theories and Amalgams of Monoids

In this paper we deal only with monadic theories. A *monadic signature* is a finite set Σ_S of unary function symbols. A *monadic theory* $\mathcal{S}$ is a set of equations of the form $t_1(x) = t_2(x)$, where t_1, t_2 are terms over Σ_S. In fact, signatures in which constants appear can be encoded as monadic signatures by adding, for all symbols f and all constants c, equations $c(f(x)) = c(x)$. Thus, our considerations are applicable to signatures with both nullary and unary symbols.

Any monadic theory $\mathcal{S}$ over Σ_S naturally defines a monoid S and a homomorphism $h_S : \Sigma_S^* \to S$ from the free monoid over the alphabet Σ_S onto S. The monoid S is simply the quotient of the free monoid Σ_S^* by an equivalence relation such that words w_1, w_2 over Σ_S are considered equivalent iff the terms they represent are equal in $\mathcal{S}$, and h_S is the canonical homomorphism. The neutral element 1 of S represents the equivalence class of the variable "x". The word w is said to *represent* the element $h_S(w) \in S$, and we will write w instead of $h_S(w)$. When speaking about any monoid S, we will tacitly assume that it is generated by a finite set Σ_S and that a canonical homomorphism $h_S : \Sigma_S^* \to S$ is given. A construction converse to the one presented above also exists [4], taking any monoid S and homomorphism h_S from Σ_S^* onto S to a monadic theory over Σ_S.

The above equivalence between monadic theories and monoids allows us to speak about theories in the language of monoids. Any notion concerning monadic theories has its counterpart in the world of monoids, and vice versa.

A *finite presentation* of a monoid S is a finite set of equations $w = w'$ ($w, w' \in \Sigma_S^*$) such that S is the quotient of Σ_S^* by those equations. These equations are called the *defining relations* of S. A monadic theory $\mathcal{S}$ directly corresponds to a set of defining relations, so if $\mathcal{S}$ is finite, then the monoid S is finitely presented.

The *word problem* is said to be decidable in a monoid S if one can, given words w, w' over Σ_S, decide whether $w = w'$ in S (that is, formally, whether $h_S(w) = h_S(w')$). The corresponding problem for theories is deciding whether an equation $t_1(x) = t_2(x)$ is a consequence of a theory $\mathcal{S}$.

The word problem is said to be *regular* in S if the language of words $e \in (\Sigma_S \cup \{=\})^*$ of the form "$w_1 = w_2$" such that $w_1 = w_2$ holds in S is regular. Regularity has a simple characterization in terms of monoids:

Lemma 1. *The word problem is regular in a monoid S iff S is finite.* $\square$

In the world of theories, the regularity of a theory means that a finite automaton exists which for any term t computes an index $i(t)$ such that $t_1 = t_2$ is a consequence of the theory iff $i(t_1) = i(t_2)$.

Assume theories $\mathcal{U}$, $\mathcal{S}$ and $\mathcal{T}$ over signatures $\Sigma_U \subseteq \Sigma_S, \Sigma_T$ are given such that $\mathcal{S}$ and $\mathcal{T}$ are conservative extensions of $\mathcal{U}$. This requirement means that any equation over Σ_U is a consequence of $\mathcal{U}$ iff it is a consequence of $\mathcal{S}$, and also iff it is a consequence of $\mathcal{T}$. We are interested in the theory $\mathcal{S} \cup \mathcal{T}$ over $\Sigma_S \cup \Sigma_T$.

The corresponding notions in the world of monoids are amalgam and amalgamated product.

A *monoid amalgam* $[U \subseteq S, T]$ is a triple of monoids such that $S \cap T = U$. The monoid U is called the *core* of the amalgam. The amalgam is *finitely presented* if U, S and T are. We assume that Σ_S and Σ_T extend Σ_U.

For any monoid amalgam one can consider the pushout $\mu : S \to P, \nu : T \to P$ in the category of monoids of the span of inclusions $i : U \to S$ and $j : U \to T$. This is called the *amalgamated product*. The amalgamated product can be defined as follows. Consider a (one-step) relation $\Leftrightarrow$ on $(S \cup T)^+$ defined by the rewrite rules $s \cdot s' \Leftrightarrow ss'$ and $t \cdot t' \Leftrightarrow tt'$ for all $s, s' \in S$ and $t, t' \in T$. [2] Let P be the quotient of $(S \cup T)^+$ by the reflexive-transitive closure $\Leftrightarrow^*$, and let $\mu : S \to P$ be defined by $\mu(s) = [s]_{\Leftrightarrow^*}$ and $\nu : T \to P$ by $\nu(t) = [t]_{\Leftrightarrow^*}$, for all $s \in S$ and $t \in T$. Then P, μ, ν form an amalgamated product of the amalgam $[U \subseteq S, T]$.

An equation $w = w'$ on words w, w' over $\Sigma_S \cup \Sigma_T$ holds *in the amalgam* if $h_P(w) = h_P(w')$. The *word problem in the amalgam* is the problem of deciding whether $w = w'$ in the amalgam, for given $w, w' \in (\Sigma_S \cup \Sigma_T)^*$. We have:

Lemma 2. *For any words w, w' over $\Sigma_S \cup \Sigma_T$, $w = w'$ in the amalgam iff $w \cdot 1 \Leftrightarrow^* w' \cdot 1$.* $\square$

[2] For words over $S \cup T$ we use the symbol "$\cdot$" to represent concatenation, so that $s \cdot s'$ is a two-letter word, while ss' is a one-letter word. For other free monoids concatenation is just represented by juxtaposition.

Note that the unit "1" above is introduced in case w or w' are empty.

A monoid amalgam $[U \subseteq S, T]$ precisely corresponds to a pair of theories $\mathcal{S}$ and $\mathcal{T}$ conservatively extending a theory $\mathcal{U}$. The union $\mathcal{S} \cup \mathcal{T}$ precisely corresponds to the amalgamated product P. In particular:

Proposition 1. *If $\mathcal{S}$ and $\mathcal{T}$ conservatively extend $\mathcal{U}$, then an equation $t_1 = t_2$ is a consequence of $\mathcal{S} \cup \mathcal{T}$ iff the corresponding word equation $w_1 = w_2$ holds in the amalgam $[U \subseteq S, T]$.* □

Therefore we may, instead of the original problem of theory unions, consider the following problem:

> If $[U \subseteq S, T]$ is an amalgam of monoids with decidable word problems, then under what assumptions is the word problem in the amalgam decidable as well?

2 Unitary and Tensor-Defined Amalgams

The relationship between the core U of an amalgam $[U \subseteq S, T]$ and the monoids S and T has a major influence on the difficulty of the amalgam's word problem. One notion that describes this relationship and which we will use intensively is that of a *unitary* submonoid. A submonoid U of S is unitary in S, if, for all $u \in U$ and $s \in S$, $su \in U$ or $us \in U$ imply $s \in U$.

The unitariness of U in S means that if we take an element of $S \setminus U$ and multiply it, on either side, by elements of U, then this product will always fall in $S \setminus U$. Note however, that it may well happen that the product of two elements of $S \setminus U$ falls in U. On the level of theories, unitariness means that if a certain term t over Σ_S is "new", that is it is not equal to any term over Σ_U modulo the theory $\mathcal{S}$, then its composition with an "old" term, that is one over Σ_U, will be "new" as well. Again, note that it may still happen that the composition of two "new" terms is "old", that is that it can be proved equal to a term over Σ_U.

We will also need notions describing computational aspects of the relationship between the core U and S or T: if U is a submonoid of S, then *U-membership is decidable* in S if verifying whether $w \in U$ in S is decidable for all $w \in \Sigma_S^*$, and it is *computable* if additionally a word $w' \in \Sigma_U^*$ may then be computed such that $w = w'$ in S. Thus, on the level of theories, decidability of U-membership means that it is decidable whether a given term over Σ_S is "old", that is whether it is equal to some term over Σ_U; computability then means that the term over Σ_U is also computable. We have:

Lemma 3. *If S has a decidable word problem, U is a submonoid of S, and U-membership is decidable, then U-membership is computable.*

Proof. If $w \in \Sigma_S^*$ and $w \in U$, then it suffices to enumerate all $w' \in \Sigma_U^*$ and for each in turn check $w = w'$ in S, which is decidable. □

An amalgam $[U \subseteq S, T]$ with amalgamated product P, μ, ν is said to be *weakly embeddable* if μ and ν are injective (that is, if S and T embed in P). It is said to be *embeddable* if additionally for all $s \in S$, $t \in T$, we have that $\mu(s) = \nu(t)$ implies $s = t \in U$ (that is, if $S \cup T$ embeds in P). On the level of theories, weak embeddability means that both $\mathcal{S}$ and $\mathcal{T}$ are conservatively extended by the union $\mathcal{S} \cup \mathcal{T}$; in other words, two terms over Σ_S (Σ_T, resp.) are equal modulo $\mathcal{S} \cup \mathcal{T}$ iff they are equal modulo $\mathcal{S}$ ($\mathcal{T}$, resp.). Embeddability adds to this the requirement that $\mathcal{S}$ and $\mathcal{T}$ are *jointly* conservatively extended by $\mathcal{S} \cup \mathcal{T}$; in other words, if two terms, t_1 over Σ_S and t_2 over Σ_T, are equal modulo $\mathcal{S} \cup \mathcal{T}$, then there must be a term t over Σ_U such that $t_1 = t$ modulo $\mathcal{S}$ and $t = t_2$ modulo $\mathcal{T}$. The importance of embeddability for describing unions of monadic theories has been discussed in detail in [4]. The results [2, 3] on decidability of unions require the amalgams to be embeddable (see Lem. 4 point 3 below). We now succintly present those results.

If U is a submonoid of S, then a *U-base* of S is a set $G \subseteq S$ such that all elements $s \in S$ have a unique decomposition as $s = gu$, where $g \in G$, $u \in U$. The base is *effective* if g and u (or rather their representations, i.e., words over Σ_S and Σ_U) may be computed. A *U-cobase* is defined analogously. We have:

Lemma 4. *The following implications hold:*

1. *If S has a U-base and U-cobase, then U is unitary in S.*
2. *If G is a U-base of S, then $G \cap U = \{1\}$.*
3. *If S and T have U-bases, then $[U \subseteq S, T]$ is embeddable.*
4. *If S has a decidable word problem, then any U-base G of S such that G-membership is decidable in S is effective.*
5. *If S has a decidable word problem and an effective U-base, then U-membership is decidable in S.*

Proof. Claims 1 and 2 have been proved in [4]. Claim 3 has been proved in [2] (Prop. 4.14 and Lem. 4.18). Claim 4 holds because one may simply enumerate all pairs $(w, w') \in \Sigma_S^* \times \Sigma_U^*$ and check whether $w \in G$ and $ww' = s$ in S. Claim 5 holds because given $w \in \Sigma_S^*$ one may compute $g \in G$ and $u \in U$ such that $gu = w$ and then check whether $g = 1$ in S. □

The following theorem is a translation of the main result of Baader/Tinelli and Fiorentini/Ghilardi into the language of monoids. Note however that their result is not restricted to monadic theories. A simple proof may be found in [4]:

Theorem 1. *For any amalgam $[U \subseteq S, T]$, if:*

- *S and T have decidable word problems,*
- *there exist effective U-bases (or U-cobases) of S and T,*

then the amalgam has a decidable word problem. □

We now turn to a notion stronger than embeddability, namely *tensor-definedeness*.

A *stripe* is a word from $(S \cup T)^+$ which consists either of just one letter (in particular, it may be a letter from U), or of interleaved elements of $S \setminus U$ and

$T \setminus U$. It is natural to try to check whether an equality $w = w'$ holds in the amalgam by reducing w to a stripe W and w' to a stripe W' and then checking whether $W = W'$. Indeed, any word can be reduced to a stripe (though this stripe need not be unique):

Lemma 5. *For any amalgam $[U \subseteq S, T]$, if U-membership is decidable in S and T, and if S and T have decidable word problems, then for any word $w \in (\Sigma_S \cup \Sigma_T)^*$ a stripe W can be computed such that $w = W$ in the amalgam.* □

However, checking whether two stripes are equal in the amalgam need not be trivial. In general, it is not true that if two stripes W and W' are equal in the amalgam, then they must be of the same length and that then the ith letters of W and W' must be equal in S or, resp., T. For example, if U is the free monoid on one generator a, S extends U with a generator b satisfying $ab = ba = 1$, and T extends U with a generator c satisfying $ac = ca = 1$, then $W = b(cc)$ has length 2 and $W' = bcb$ has length 3, but $W = b(cc) = bc1c = bc(ba)c = bcb(ac) = bcb1 = bcb = W'$ in the amalgam.

The word problem is *n-decidable* in the amalgam if the problem of checking $W = W'$ in the amalgam is decidable for all stripes $W, W' \in (S \cup T)^+$ of length $\leq n$.

The notion of *n-tensor* $S \otimes_U T \otimes_U \ldots$ is intended to reflect the idea of proving equivalence by using words in which no more than n separate "blocks" from S exist. Formally, this tensor is defined as follows. Let $\sim_n$ be the least symmetric relation on *interleaved* words of length n, i.e., on words $w = x_1 \cdot \ldots \cdot x_n$ such that $x_1 \in S$, $x_2 \in T$, $x_3 \in S$, etc., satisfying the conditions:

$$w \cdot su \cdot t \cdot w' \sim_n w \cdot s \cdot ut \cdot w'$$

for all $s \in S$, $t \in T$, $u \in U$ and $w \in (S \cdot T)^k$, $w' \in (S \cdot T)^l$ (for $n = 2k + 2l + 2$) or $w' \in (S \cdot T)^l \cdot S$ (for $n = 2k + 2l + 3$), and

$$w \cdot tu \cdot s \cdot w' \sim_n w \cdot t \cdot us \cdot w'$$

for all $s \in S$, $t \in T$, $u \in U$ and $w \in (S \cdot T)^k \cdot S$, $w' \in T \cdot (S \cdot T)^l$ (for $n = 2k + 2l + 4$) or $w' \in (T \cdot S)^l$ (for $n = 2k + 2l + 3$). The *n-tensor* $\sim_n^*$ is the reflexive-transitive closure of $\sim_n$. The n-tensor $T \otimes_U S \otimes_U \ldots$ is defined analogously and also denoted by $\sim_n^*$. The n-tensor is *decidable* if one can decide whether $w \sim_n^* w'$ for given interleaved words $w, w' \in (S \cup T)^n$, the letters of which are given as words over Σ_S and Σ_T.

The amalgam is *tensor-defined* if for any stripes W and W' we have $W = W'$ in the amalgam iff W and W' are of the same length, say n, and $W \sim_n^* W'$. Thus, a tensor-defined amalgam is one in which the checking the equality of two stripes does not require one to use interleaved words longer than the longer of the two stripes. This is a form of bound on the space requirements for proving equality in the amalgam. By Lem. 5, a stripe equivalent to a given word may be easily computed, and therefore the word problem in tensor-defined amalgams is reduced to the problem of deciding the tensors.

The easy proof of the following lemma may be found on the author's webpage[3]:

Lemma 6. *The following implications hold for any amalgam $[U \subseteq S, T]$ of monoids with decidable word problems:*

1. *If U-membership is decidable in S and T, then the word problem in the amalgam is decidable iff it is n-decidable for all n.*
2. *If U-membership is decidable in S and the amalgam is embeddable, then it has a 1-decidable word problem.*
3. *If the amalgam is tensor-defined, then for any $n > 0$, if for all $k \leq n$ both its k-tensors are decidable, then it has an n-decidable word problem.* □

This leads us to the following corollary, which essentially says that tensor-defined unions of theories that are recognized by finite automata are decidable (though they need not be recognizable by finite automata themselves):

Corollary 1. *If an amalgam $[U \subseteq S, T]$ of finite monoids is tensor-defined, then it has a decidable word problem.*

Proof. In an amalgam of finite monoids, all n-tensors are finite relations and are therefore decidable. So is U-membership. Since the amalgam is tensor-defined, by points 1 and 3 of Lem. 6 it has a decidable word problem. □

The notion of tensor-definedeness of an amalgam is abstract and it may be difficult to verify whether an amalgam is or is not tensor-defined. Fortunately, the following proposition gives us a powerful method for showing tensor-definedeness.

Proposition 2. *The following implications hold for any amalgam $[U \subseteq S, T]$:*

1. *If for all defining relations $w = w'$ of S either $w, w' \in \Sigma_U^*$, or $w, w' \in \Sigma_S^* \setminus \Sigma_U^*$, then U is unitary in S.*
2. *If U is unitary in S and T, then the amalgam is tensor-defined.*
3. *If the amalgam is tensor-defined, then it is embeddable.*

Proof. In the proof of point 2, for any words $w \Leftrightarrow^* w'$, we show, by induction on the length of the proof of this equivalence, that if w reduces to a stripe W and w' to a stripe W', then W and W' must be of the same length, say k, and $W \sim_k^* W'$ holds. This proof is quite cumbersome, and may be found, together with the easy proofs of points 1 and 3, on the author's webpage. □

From the above proposition, we can infer the following corollaries:

Theorem 2. *If $[U \subseteq S, T]$ is an amalgam such that:*

- *U-membership is decidable in S and T,*
- *U is unitary in S and T,*
- *the tensors of the amalgam are decidable,*

[3] In the appendix of the paper at `http://www.mimuw.edu.pl/~piotrek/RTA2006-full.ps.gz`

then the amalgam has a decidable word problem.

Proof. By Prop. 2, the amalgam is tensor-defined. By point 3 of Lem. 6, it thus has an n-decidable word problem for all n. By point 1 of the same lemma, it then has a decidable word problem. $\square$

Corollary 2. *If $[U \subseteq S, T]$ is an amalgam such that:*

- *U is unitary in S and T,*
- *S and T are finite,*

then the amalgam has a decidable word problem. $\square$

3 Amalgams with Group-Like Cores

Results presented in Sect. 4 show that even for very simple monoids S and T the amalgam $[U \subseteq S, T]$ can have an undecidable word problem. Thus forcing U to be "small" will not make the amalgam decidable. However, it turns out that if U has a sufficiently "complete" structure, then the amalgam will have a decidable word problem for arbitary (decidable) S and T. This is quite remarkable and suggests that in the quest for decidability one should, instead of ensuring that the communication between S and T via U is difficult, rather try to ensure that any multi-step communication between them can be reduced to single-step communication.

If U is a submonoid of S, then *right U-quotients may be computed in S* if for any $s, s' \in S$ the set of all $u \in U$ satisfying $s = s'u$ is finite and may be computed (strictly speaking the s, s' are represented by words in Σ_S^* and the u by words in Σ_U^*). On the level of theories, the computability of right quotients means that for any two terms t and t' over Σ_S the set of terms t_U over Σ_U satisfying $t(x) = t_U(t'(x))$ modulo $\mathcal{S}$ contains only finitely many terms which are pairwise not equal modulo $\mathcal{U}$, and, moreover, that this set is computable.

Theorem 3. *If $[U \subseteq S, T]$ is an amalgam such that:*

- *S and T have decidable word problems,*
- *U is a group,*
- *right U-quotients are computable in S and in T,*

then the amalgam has a decidable word problem.

Proof. Because U is a group, U is unitary in S and T. For if $su \in U$ for $s \in S$ and $u \in U$, then $s = (su)u^{-1} \in Uu^{-1} \subseteq U$. A similar argument works for us and for T. Hence, by Prop. 2, the amalgam is tensor-defined. Note that U-membership is decidable in S and T, since for any $w \in \Sigma_S^*$ or $w \in \Sigma_T^*$ we can check whether there exists $u \in U$ such that $w = 1u$; but this holds iff $w \in U$. By points 1 and 3 of Lem. 6, it thus suffices to show that the m-tensor is decidable for all $m \geq 1$

Consider any interleaved word $W = s_1 \cdot t_1 \cdot \ldots \cdot s_n \cdot t_n$ of length m and assume $m = 2n$. We claim that any word W' equivalent to W in the tensor is of the form

$$(s_1u_1) \cdot (u_1^{-1}t_1u_2) \cdot (u_2^{-1}s_2u_3) \cdot \ldots \cdot (u_{2n-1}^{-1}t_n)$$

for some $u_1, \ldots, u_{2n-1} \in U$.

Suppose to the contrary. Let k be the least number of steps used to prove that W and W' are equivalent in the tensor. Of course $k > 0$. Assume W' is obtained from some W_0 in one step and W_0 from W in $k-1$ steps. For W and W_0 the claim holds, that is, $W_0 = (s_1 u_1) \cdot (u_1^{-1} t_1 u_2) \cdot (u_2^{-1} s_2 u_3) \cdot \ldots \cdot (u_{2n-1}^{-1} t_n)$. The step from W_0 to W' is either of the form $\ldots \cdot su \cdot t \cdot \ldots \sim_{2n} \ldots \cdot s \cdot ut \cdot \ldots$, where $su = u_{2i-2}^{-1} s_i u_{2i-1}$ and $t = u_{2i-1}^{-1} t_i u_{2i}$, or $\ldots \cdot s \cdot ut \cdot \ldots \sim_{2n} \ldots \cdot su \cdot t \cdot \ldots$, where $s = u_{2i-2}^{-1} s_i u_{2i-1}$ and $ut = u_{2i-1}^{-1} t_i u_{2i}$, or of analogical forms with the roles of s and t swapped. In the former case we have $s = u_{2i-2}^{-1} s_i (u_{2i-1} u^{-1})$ and $ut = u u_{2i-1}^{-1} t_i u_{2i} = (u_{2i-1} u^{-1})^{-1} t_i u_{2i}$. In the latter case we have $su = u_{2i-2}^{-1} t_i (u_{2i-1} u)$ and $t = u^{-1} u_{2i-1}^{-1} t_i u_{2i} = (u_{2i-1} u)^{-1} t_i u_{2i}$. This proves the claim. Analogical claims hold for $m = 2n+1$ and for the second tensor.

Now, all we have to do in order to decide whether

$$s_1 \cdot t_1 \cdot s_2 \cdot \ldots \sim_m^* s_1' \cdot t_1' \cdot s_2' \cdot \ldots$$

is check whether there exist $u_1, u_2, \ldots \in U$ such that

$$\begin{aligned} s_1' &= s_1 u_1 \\ t_1' &= u_1^{-1} t_1 u_2 \\ s_2' &= u_2^{-1} s_2 u_3 \\ &\vdots \end{aligned}$$

By assumption, we can compute a finite set of all possible choices for u_1, that is, all $u_1 \in U$ satisfying $s_1' = s_1 u_1$. If this set is empty, then the above system of equations is unsatisfiable. Otherwise for each choice in turn we repeat the whole procedure for the (shorter) list of equations

$$\begin{aligned} u_1 t_1' &= t_1 u_2 \\ s_2' &= u_2^{-1} s_2 u_3 \\ &\vdots \end{aligned}$$

with unknowns $u_2, u_3, \ldots \in U$. □

Of course, a dual version of the above theorem holds for left U-quotients.

In certain cases, the assumption that right U-quotients are computable can easily be done away with. This is the case if U is finite, since one then can simply enumerate all elements of $u \in U$ and check which of them satisfy $s = s'u$. Thus:

Corollary 3. *If $[U \subseteq S, T]$ is a monoid amalgam such that:*

- *S and T have decidable word problems,*
- *U is a finite group,*

then the amalgam has a decidable word problem. □

This corollary is especially remarkable, since it guarantees the decidability of $[U \subseteq S, T]$ solely based on the form of U.

The assumption that U is a group is satisfied in many standard cases. Consider a signature with three unary symbols `pred`, `succ` and `neg`, satisfying the equations:

$$
\begin{array}{ll}
\texttt{pred}(\texttt{succ}(x)) = x & \qquad \texttt{neg}(\texttt{succ}(x)) = \texttt{pred}(\texttt{neg}(x)) \\
\texttt{succ}(\texttt{pred}(x)) = x & \qquad \texttt{neg}(\texttt{pred}(x)) = \texttt{succ}(\texttt{neg}(x)) \\
\texttt{neg}(\texttt{neg}(x)) = x &
\end{array}
$$

The monoid U defined by these equations is indeed a group, since all the generators can be inverted. Thus, if right quotients are computable in S and T, *any* amalgam with U as core will have a decidable word problem if S and T do.

Note however that if we add 0 to the above group, that is, if we add an unary symbol `0` and the equations:

$$\texttt{0}(\texttt{succ}(x)) = \texttt{0}(\texttt{pred}(x)) = \texttt{0}(\texttt{neg}(x)) = \texttt{0}(\texttt{0}(x)) = \texttt{0}(x) = \texttt{neg}(\texttt{0}(x))$$

then the monoid U_{nat} defined by these equations is no longer a group.[4] Rather, it is the group U with a right zero `0` adjoined, which aditionally satisfies $\texttt{0}\,\texttt{neg} = \texttt{0}$. Therefore Th. 3 cannot be applied here. The same is true for the monoid U_{bool} defined by equations

$$\texttt{f}(\texttt{f}(x)) = \texttt{f}(\texttt{t}(x)) = \texttt{f}(x) \qquad\qquad \texttt{t}(\texttt{f}(x)) = \texttt{t}(\texttt{t}(x)) = \texttt{t}(x)$$

over the generators `f` and `t`. The monoid U_{bool} contains an identity and two right zeros, and is not a group.

Unfortunately, it is not in general true that an amalgam of decidable monoids in which the core is a group with adjoined zero or right zeros must have a decidable word problem. In fact, in the next section we prove that there exists a monoid T with decidable word problem, such that the word problem of the amalgam $[U_{bool} \subseteq U_{bool} \cup \{0\}, T]$ is undecidable!

However, a slight generalization of Th. 3 to groups with zero is possible. A *group with zero* is a monoid of the form $G \cup \{0\}$, where G is a group and 0 is a *zero*, that is, $0g = g0 = 00 = 0$ for all $g \in G$. As is proved below, the assumption that $0s \neq 0$ and $s0 \neq 0$ for all $s \in S \setminus U$ guarantees that U is unitary in S.

Theorem 4. *If $[U \subseteq S, T]$ is a monoid amalgam such that:*

- *S and T have decidable word problems,*
- *U is a group with zero (which we denote by 0),*
- *$0s \neq 0$ and $s0 \neq 0$ for all $s \in S \setminus U$, and a similar property holds for T,*
- *right U-quotients are computable in S and in T,*

then the amalgam has a decidable word problem.

Proof. The monoid U is unitary in S and T. For if $su \in U$ for some $s \in S$, $u \in U$, then either $u \neq 0$, and then $s = (su)u^{-1} \in Uu^{-1} \subseteq U$, or $u = 0$, and then we would have $s0 \in U$. But then $0 = (s0)0 = s(00) = s0$, which implies

[4] The idea of this example is taken from [2].

$s \in U$. Thus, for the same reasons as in the proof of Th. 3, it suffices to prove that for all $m \geq 1$ the m-tensor is decidable. Note that the element 0 may be computed, since one can enumerate all words $w \in \Sigma_U^*$, and check for which of them $w\sigma = \sigma w = w$ holds for all $\sigma \in \Sigma_U$. For any interleaved word $W = s_1 \cdot t_1 \cdot \ldots$ of length $m = 2n$, let $Z(W)$ be the word $s_1 x_1 \cdot x_1 t_1 y_1 \cdot y_1 s_2 x_2 \cdot \ldots$, where:

- $x_i = 0$ if there is some $1 \leq j \leq i$ such that $s_j 0 = s_j, 0t_j 0 = 0t_j, s_{j+1}0 = s_{j+1}, \ldots, 0t_{i-1}0 = 0t_{i-1}, s_i 0 = s_i$ or $1 \leq j < i$ such that $t_j 0 = t_j, s_{j+1}0 = s_{j+1}, \ldots, 0t_{i-1}0 = 0t_{i-1}, s_i 0 = s_i$,
- $x_i = 0$ if there is some $i < j \leq n$ such that $0s_j = s_j, 0t_{j-1}0 = t_{j-1}0, 0s_{j-1}0 = s_{j-1}0, \ldots, 0t_i 0 = t_i 0$ or $i \leq j \leq n$ such that $0t_j = t_j, 0s_j 0 = s_j 0, 0t_{j-1}0 = t_{j-1}0, 0s_{j-1}0 = s_{j-1}0, \ldots, 0t_i 0 = t_i 0$,
- otherwise $x_i = 1$,
- y_i is defined analogously.

We have $W \sim_m^* Z(W)$. Moreover, $W_1 \sim_m^* W_2$ iff $Z(W_1) \sim_m^* Z(W_2)$, since the first relation implies $Z(W_1) \sim_m^* W_1 \sim_m^* W_2 \sim_m^* Z(W_2)$ and vice versa.

Now consider the least symmetric relation $\approx_m$ on interleaved words of length m such that:

$$w \cdot su \cdot t \cdot w' \approx_m w \cdot s \cdot ut \cdot w'$$

for all $s \in S$, $t \in T$ and $u \in U$ such that $su0 \neq su$ and $0t \neq t$ and all $w \in (S \cdot T)^k$, $w' \in (S \cdot T)^l$ (for $n = k + l + 1$), and:

$$w \cdot tu \cdot s \cdot w' \approx_m w \cdot t \cdot us \cdot w'$$

for all $s \in S$, $t \in T$ and $u \in U$ such that $tu0 \neq tu$ and $0s \neq s$ and all $w \in (S \cdot T)^k \cdot S$, $w' \in T \cdot (S \cdot T)^l$ (for $n = k + l + 2$).

It can be proved that $W_1 \sim_m^* W_2$ iff $Z(W_1) \approx_m^* Z(W_2)$ and that similar results hold for the other tensor and for $m = 2n + 1$; it can also be proved that $\approx_m^*$ is decidable (for a proof of these claims see the author's webpage). Now, if we are to check whether $W_1 \sim_m^* W_2$, then all we have to do is compute $Z(W_1)$ and $Z(W_2)$ and then check whether $Z(W_1) \approx_m^* Z(W_2)$, which is decidable. □

4 Undecidability Results

In this section we prove results that explain why it is so hard to come up with methods for joining decision procedures even in the simple case of monadic theories. We show that even for amalgams of very simple monoids the word problem can be undecidable.

We start by recalling a fact proven in [4]. The proof itself is recast in terms of *2-counter machines*. This will allow us to show the similarities between the proofs of Th. 5, 6 and 7. Recall that a 2-counter machine consists of a finite set of instructions of three forms:

- "increment counter 1 (resp. 2) and jump to instruction i",
- "if counter 1 (resp. 2) is non-zero, decrement it and jump to instruction i; if it is zero, jump to instruction j",

– “stop”, which is always the last instruction.

Any 2-counter machine starts at instruction 1 with counter 1 set to n and counter 2 set to 0. The input n is considered accepted if “stop” is executed with both counters 0. 2-counter machines are Turing-complete [6]. By a *state* of M a triple (i, n, m) is understood, where i is the current instruction and n and m are the values of the counters. The transition relation of the machine is denoted by $\to^*$.

Theorem 5 ([4]). *A finitely presented amalgam $[U \subseteq S, T]$ exists such that:*

- *S and T have decidable word problems,*
- *U is unitary in S and T,*
- *U is the free monoid $(\mathbb{N}, +)$,*
- *S has a U-cobase,*

and the amalgam has an undecidable word problem.

Proof. Let M be an N-instruction 2-counter machine. Let $U = \Box^*$, S be generated by $\Box$ and $\#$ satisfying the equation $\# = \#\Box$ and let T be generated by $\Box$, A, B, a, b and $q_1, \ldots, q_N$, satisfying the equations:

1. $ab = ba$, $aB = Ba$, $bA = Ab$, $AB = BA$,
2. $\Box q_i = q_j a$ (resp. $\Box q_i = q_j b$) if instruction i of M increments counter 1 (resp. 2) and jumps to instruction j,
3. $q_i a = \Box q_j$ (resp. $q_i b = \Box q_j$) and $q_i A = q_k A$ (resp. $q_i B = q_k B$) if instruction i of M decrements counter 1 (resp. 2) if it is non-zero and then jumps to instruction j, and otherwise jumps to instruction k.

The generators a and b represent single units on counters 1 and 2, while A and B represent the “end” or “zero” on counters 1 and 2. Note that we do not have relations $aA = Aa$ or $bB = Bb$, which guarantees that if A or B are read, then the counter must indeed be zero.

Obviously, U and S have decidable word problems. So does T, since for any word w of length k over Σ_T there is at most $(5+N)^k$ words equivalent to w. This is due to the fact that the defining relations of T preserve word length. By point 1 of Prop. 2, U is unitary in S and T. Finally, the U-cobase of S is $\#^*$.

We claim that $\#q_{i_1} a^{n_1} b^{m_1} AB = \#q_{i_2} a^{n_2} b^{m_2} AB$ in the amalgam iff there is a state (i, n, m) such that $(i_1, n_1, m_1) \to^* (i, n, m)$ and $(i_2, n_2, m_2) \to^* (i, n, m)$ in the machine M. This claim may be proved by induction on the number of defining relations of types 2 and 3 applied to derive the equality in the amalgam.

From the above claim we may infer that $\#q_1 a^k AB = \#q_N AB$ holds in the amalgam iff there is a state (i, n, m) such that $(1, k, 0) \to^* (i, n, m)$ and $(N, 0, 0) \to^* (i, n, m)$ in the machine M. But instruction N of the machine M is “stop”, and so $(N, 0, 0) \to^* (i, n, m)$ iff $i = N$ and $n = m = 0$. Thus $\#q_1 a^k AB = \#q_N AB$ in the amalgam iff $(1, k, 0) \to^* (N, 0, 0)$, which in turn holds iff the machine M accepts the number k. $\Box$

The amalgam produced above is, by Prop. 2, tensor-defined and embeddable. Actually, a much stronger result can be shown if one does not insist on S having a U-base or cobase. A monoid U is *right zero* if $uu' = u'$ for all $u, u' \in U$, $u' \neq 1$.

Theorem 6. *Let U be the 3-element right zero monoid and let S be the 4-element monoid obtained by adjoining a zero to U. There exists a finitely presented monoid T satisfying $S \cap T = U$ and such that:*

- *T has a decidable word problem,*
- *U is unitary in S and T,*

and the amalgam $[U \subseteq S, T]$ has an undecidable word problem.

Proof. Let M be an N-instruction 2-counter machine. Let $U = \{1, t, f\}$ with t and f right zeros, that is, with $ut = t$ and $uf = f$ for all $u \in U$. Let $S = U \cup \{0\}$ be U with a zero adjoined, that is, with $s0 = 0s = 0$ for all $s \in S$. Let T extend U with generators A, B, a, b and $q_1, \ldots, q_N$, satisfying the equations:

1. $ab = ba$, $aB = Ba$, $bA = Ab$, $AB = BA$,
2. $tq_i = fq_ja$ (resp. $tq_i = fq_jb$) if instruction i of M increments counter 1 (resp. 2) and jumps to instruction j,
3. $tq_ia = fq_j$ (resp. $tq_ib = fq_j$) and $tq_iA = fq_kA$ (resp. $tq_iB = fq_kB$) if instruction i of M decrements counter 1 (resp. 2) if it is non-zero and jumps to instruction j, and otherwise jumps to instruction k.

The monoid T has a decidable word problem, because for any word w over Σ_T, there is only a finite number of words w' over Σ_T such that $w = w'$ in T. Indeed, relations listed under point 1 just rearrange certain letters, and relations listed under points 2 and 3 cannot lead to new equivalent words if applied more than twice. As before, U is unitary in S and T by Prop. 2.

Similarily to the proof of the previous theorem, we claim that $0q_{i_1}a^{n_1}b^{m_1}AB = 0q_{i_2}a^{n_2}b^{m_2}AB$ in the amalgam iff there is a state (i, n, m) such that $(i_1, n_1, m_1) \to^* (i, n, m)$ and $(i_2, n_2, m_2) \to^* (i, n, m)$ in the machine M; this can be proved by induction on the number of defining relations of types 2 and 3 which have to be applied to derive $0q_{i_1}a^{n_1}b^{m_1}AB = 0q_{i_2}a^{n_2}b^{m_2}AB$. As before, this claim implies that $0q_1a^kAB = 0q_NAB$ holds in the amalgam iff the machine M accepts the number k, which is undecidable. □

One can actually show that U and S in the above theorem are minimal:

Proposition 3. *If $[U \subseteq S, T]$ is an amalgam such that:*

- *S and T have decidable word problems,*
- *U is unitary in S and T,*
- *U has less than 3 elements,*

then the amalgam has a decidable word problem.

Proof. If U has 1 element, then the amalgam is certainly decidable. If U has 2 elements, then either U is the 2-element group, or it is the trivial group with an adjoined zero. In the first case, the amalgam is decidable by Cor. 3. So assume that U is the trivial group with adjoined zero, that is, $U = \{1, 0\}$.

Since U is unitary in S, we cannot have $0s = 0$ or $s0 = 0$ for any $s \in S \setminus U$, and a similar property holds for T. Also, all right U-quotients are computable, since U is finite. Thus by Th. 4 the amalgam has a decidable word problem. □

As was the case for the amalgam constructed in Th. 5, the amalgam of Th. 6 is tensor-defined and embeddable. If the first of these properties is to be preserved and the amalgam is to have an undecidable word problem, then T must be infinite (see Cor. 1). However, if we do not insist on the amalgam being tensor-defined, then it is possible to construct an amalgam of *finite* monoids which itself has an undecidable word problem. We present an outline of the proof of Sapir [5] (Th. 1.1 and remark after Lem. 4.4). Our outline is much shorter than the original, and very similar to the proofs of Th. 5 and 6.

Theorem 7. *An amalgam $[U \subseteq S, T]$ exists such that:*

- *S and T are finite,*
- *the amalgam is embeddable,*

and the amalgam has an undecidable word problem.

Proof. Let M be an N-instruction 2-counter machine. Let U be generated by 0, and by α_i^1 and α_i^2 for any instruction i incrementing counter 1, β_i^1 and β_i^2 for i incrementing counter 2, $\aleph_i$, $\aleph_i^>$ and $\aleph_i^=$ for instruction i testing counter 1 on zero, and $\beth_i$, $\beth^>$ and $\beth^=$ for instruction i testing counter 2 on zero. Moreover, let $uu' = 0$ for all u, u' among the above generators.

Let S be additionally generated by a, b, $q_1, \ldots, q_N$ and $Q_1, \ldots, Q_{N-1}$. Let T be additionally generated by a', b', A and B. Let both be defined by the following relations (in addition to those defining U):

1. $q_i = a\alpha_i^1 Q_i$ in S, and $\alpha_i^1 = a'\alpha_i^2$ in T, and $\alpha_i^2 Q_i = q_j$ in S, if instruction i increments counter 1 and jumps to instruction j,
2. $q_i = Q_i\beta_i^1 b$ in S, and $\beta_i^1 = \beta_i^2 b'$ in T, and $Q_i\beta_i^2 = q_j$ in S, if instruction i increments counter 2 and jumps to instruction j,
3. $q_i = \aleph_i Q_i$ in S and:
   (a) $a'\aleph_i = \aleph_i^>$ in T and $a\aleph_i^> Q_i = q_j$ in S,
   (b) $A\aleph_i = A\aleph_i^=$ in T and $\aleph_i^= Q_i = q_k$ in S,
   if instruction i decrements counter 1 if it is non-zero and then jumps to instruction j, and otherwise jumps to instruction k,
4. $q_i = Q_i\beth_i$ in S and:
   (a) $\beth_i b' = \beth_i^>$ in T and $Q_i\beth_i^> b = q_j$ in S,
   (b) $\beth_i B = \beth_i^= B$ in T and $Q_i\beth_i^= = q_k$ in S,
   if instruction i decrements counter 2 if it is non-zero and then jumps to instruction j, and otherwise jumps to instruction k,
5. $ss' = 0$ in S and $tt' = 0$ in T for all products of generators s, s' of U and S or t, t' of U and T, except for those that appear in one of the above relations.

Both S and T extend U, since no two generators of U can be equated by applying the above relations. Also, both are finite. Finally, it can easily be verified that the amalgam is embeddable.

As before, one can prove that $A(aa')^{n_1}q_{i_1}(b'b)^{m_1}B = A(aa')^{n_2}q_{i_2}(b'b)^{m_2}B$ in the amalgam iff there is a state (i, n, m) of the machine M such that $(i_1, n_1, m_1) \to^* (i, n, m)$ and $(i_2, n_2, m_2) \to^* (i, n, m)$. This implies that $A(aa')^k q_1 B = Aq_N B$ iff $(1, k, 0) \to^* (N, 0, 0)$ in M, that is, iff k is accepted by M. $\square$

5 Conclusions

Results such as Th. 2, 3, 4 or 6 show that the approach via monoid amalgams, proposed in [4] where the weaker Th. 5 was proved, works in practice. Still, even in the realm of monadic theories, a great number of problems concerning the decidability of unions remains open. For example, unitariness is sufficient for the amalgam to be tensor-defined, but is certainly not necessary; a sufficient and necessary notion is not yet known. The decidability of n-tensors and the notion of n-decidability remain unexplored (though see [7]). Decidability of amalgams with "small" cores has been explored in this paper only in the unitary case. Decidability of amalgams with "complete" cores has been dealt with for groups and groups with zero; but certainly there are other classes of cores that are "complete" enough for amalgams over them to have decidable word problems.

Moreover, in none of the criteria employed in the context of combining theories (effective bases, unitariness, amalgams with group-like cores) does the relationship between the theories $\mathcal{S}$ and $\mathcal{T}$ appear directly; the only exception is tensor-definedeness. All the other criteria say something about $\mathcal{S}$, about $\mathcal{T}$, and about the intersection $\mathcal{U}$, but nothing about the relationship between $\mathcal{S}$ and $\mathcal{T}$. If we want to show the decidability of complex unions of theories, then it seems inevitable that our criteria refer directly to this relationship.

Of course, work is also, and maybe foremost, needed on applying the ideas developed for monadic theories to theories with symbols of arbitrary arities. It should then be possible to rather easily generalize the obtained results to many-sorted equational logic: most results of this paper can be reformulated in a many-sorted framework without any difficulty.

Finally, in the context of combining theories a number of interesting automata-theoretic questions arise. As we have seen, a union of regular theories may be undecidable. One is thus tempted to ask: When is it decidable (regular, automatic)? What about unions of automatic theories? What is the situation for relations other than equality? All these questions may also be posed for non-monadic theories, thus leading to problems for tree-automata.

References

1. Pigozzi, D.: The join of equational theories. Coll. Math. **30**(1) (1974) 15–25
2. Baader, F., Tinelli, C.: Deciding the word problem in the union of equational theories. Inf. Comp. **178**(2) (2002) 346–390
3. Fiorentini, C., Ghilardi, S.: Combining word problems through rewriting in categories with products. Th. Comp. Sci. **294** (2003) 103–149
4. Hoffman, P.: Union of equational theories: An algebraic approach. In: RTA'05. Volume 3467 of LNCS. (2005) 61–73
5. Sapir, M.V.: Algorithmic problems for amalgams of finite semigroups. J. Algebra **229**(2) (2000) 514–531
6. Minsky, M.: Computation: Finite and Infinite Machines. Prentice-Hall (1967)
7. Birget, J.C., Margolis, S., Meakin, J.: On the word problem for tensor products and amalgams of monoids. Intnl. J. Alg. Comp. **9** (1999) 271–294