Algorithmic Problems for Amalgams of Finite Semigroups

Mark V. Sapir*

Abstract

We prove that there exist an amalgam of two finite 4-nilpotent semigroups such that the corresponding amalgamated product has undecidable word problem. We also show that the problem of embeddability of finite semigroup amalgams in any semigroups and the problem of embeddability of finite semigroup amalgams into finite semigroups are undecidable. We use several versions of Minsky algorithms and Slobodskoj's result about undecidability of the universal theory of finite groups.

1 Introduction

It is well known that any amalgam of two finite groups is embeddable into a group [16]. Moreover the free product with amalgamation of two finite groups and in general the fundamental group of any graph of finite groups is a virtually free group (Karras, Pietrowski, Solitar, [13]), so it is residually finite. Therefore any amalgam of finite groups is embeddable into a finite group.

On the other hand it is well known that not every amalgam of two finite semigroups is embeddable into a semigroup. A very simple example was found in 1957 by Kimura, see [2]. Here we present an even simpler (fewer elements) example. Let S be the 4-element semigroup $\{a, b, c, 0\}$ where $ab = c$ and all other products are equal to 0. This semigroup contains two subsemigroups $\{a, c, 0\}$ and $\{b, c, 0\}$ with zero product. Consider a disjoint copy $S' = \{a', b', c', 0'\}$ of S, and form an amalgam W of S and S' by identifying a with c', c with b' and 0 with $0'$. Suppose that W is embeddable into a semigroup H. Then in H, we have the following equalities:

$$a = c' = a'b' = a'c = a'ab = a'c'b = 0'b = 0b = 0.$$

Thus a and 0 get identified by any homomorphism from the amalgam W into a semigroup.

Ever since Kimura's example was discovered, one of the important problems in the theory of semigroups was to find necessary and sufficient conditions under which a given amalgam of semigroups is embeddable into a semigroup or a finite semigroup.

*This research was supported in part by NSF grants DMS 9623284, DMS 9203981.

I am not in a position to survey all 100+ papers about semigroup amalgams published since 1962 (see the book [11] and survey articles [12] and [10]). I mention only some of the results.

In 1962, Howie [11], [2] proved that, for example, every amalgam of semigroups $S \cup_U T$ where the common semigroup U is unitary in S and T is embeddable into a semigroup. Here being unitary in S means that for any two elements $s \in S, u \in U$ such that $us \in U$ or $su \in U$ we have $s \in U$.

One of the main tools in proving embeddability of amalgams is Isbell's zigzag theorem ([12] is a survey article of applications of this theorem).

Other tools were invented by T. Hall (he used representations of semigroups by transformations). In particular T. Hall [8] showed that any inverse semigroup is an amalgamation base, which means that any amalgam of two semigroups where the common subsemigroup is inverse embeds into a semigroup.

The class of embeddable amalgams of infinite semigroups is known to be "bad" from the algorithmic view point. Lallement [15] found an infinite system of formulas which is necessary and sufficient for a semigroup amalgam to be embeddable into a semigroup. He proved that no finite subsystem of this system of formulas can serve as a necessary and sufficient condition. Recently Dekov [3] generalized this result by proving that the class of embeddable amalgams of semigroups is not finitely axiomatizable. Recently Birget, Margolis and Meakin [1] proved that the amalgamated product of two finitely presented semigroups with solvable word problem and nice common subsemigroup may have undecidable word problem.

Nevertheless there was a hope that amalgams of finite semigroups are much nicer, and there is an algorithm to solve the word problem in the amalgamated product of two finite semigroups, and an algorithm to decide whether an amalgam of two finite semigroups embeds into a semigroup or embeds into a finite semigroups.

Hall and Putcha [9] proved that if the finite semigroup U is an amalgamation base in the class of finite semigroups then its J-classes are linearly ordered. This condition is also sufficient if U is inverse.

Some necessary and sufficient conditions on a finite semigroup amalgam to be embeddable into a finite semigroup were given by Okniński and Putcha [17]. They used representations of finite semigroups by matrices.

In this paper, we shall prove the following surprising results.

Theorem 1.1 *There exists an amalgam of two finite semigroups such that the word problem is undecidable in the corresponding free product with amalgamation.*

Theorem 1.2 *The problem of whether an amalgam of two finite semigroups is embeddable into a semigroup is undecidable.*

Theorem 1.3 *The problem of whether an amalgam of two finite semigroups is embeddable into a finite semigroup is undecidable.*

Remark 1. The proofs of these theorems show that one can assume that finite semigroups in each of them are 4-nilpotent (that is the product of every 4 elements is 0).

Remark 2. The proof of Theorem 1.3 shows that one can fix an easy 7-element semigroup U (the semigroup consisting of all upper triangular 4×4-matrix units and 0) such that the problem of embeddability of a finite amalgam of the form $S \cup_U T$ into a finite semigroup is undecidable. It is interesting to describe all semigroups U which have this property.

Remark 3. By taking semigroup rings over a finite field, one can easily deduce analogs of these three theorems for finite associative rings.

Acknowledgements. This paper is inspired by my conversations with Tom Hall during my visit to Monash University, Australia, in the Summer of 1994. I am grateful to Tom for the invitation, for suggesting the problem, and for very helpful discussions. The theorems 1, 2, 3 were proved soon after I returned from Australia and I gave a couple of lectures in Lincoln, Nebraska, explaining the proofs in 1994. I have been busy with other projects and did not have time to publish anything. About a year ago Marcel Jackson notified me that he also independently proved Theorems 1.2, 1.3. He deduced both theorems from the results of a paper by Kublanovsky and myself [7]. His proofs are not published either. My proof of Theorem 1.2 uses Minsky algorithms and is of course independent of [7] because [7] appeared two years later. My first proof of Theorem 1.3 also used Minsky machines, but this proof is much more complicated and is not presented here.

2 Minsky's Algorithms

We start with definitions of two forms of Minsky algorithms [14]. The first form works with glasses and coins.

Consider two glasses. We assume that these glasses are of infinite height. Suppose also that we have infinitely many coins. A *program* is a numbered sequence of instructions.

An *instruction* has one of the following forms:

- Put a coin in the glass # n and go to instruction # j, $n = 1$ or 2;
- If the glass # n is not empty then take a coin from this glass and go to instruction # j otherwise go to instruction # k, $n = 1$ or 2.
- Stop.

A program starts working with the instruction number 1 and empty second glass and ends when it comes to the Stop instruction which will always have number 0.

We say that a program calculates a function $f(m)$ if, starting with m coins in the first glass and empty second glass, we end up with $f(m)$ coins in the first glass and empty second glass.

A configuration of a Minsky algorithm is a triple (m, k, n), where m is the number of coins in the first glass, n is the number of coins in the second glass, and k is the number of the instruction we are executing.

Another useful variant of Minsky algorithms works with a number of the form 2^m3^n instead of glasses.

An *instruction* has one of the following forms:

- Multiply the number by 2 and go to instruction # j.
- Multiply the number by 3 and go to instruction # j.
- If the number is even then divide it by 2 and go to instruction # j otherwise go to instruction # k.
- If the number is divisible by 3 then divide it by 3 and go to instruction # j otherwise go to instruction # k.
- Stop.

A program starts working with the instruction number 1 and a number of the form 2^m and ends when it comes to the Stop instruction which will always have number 0. As in the previous case, the configuration when the algorithm deals with number 2^m3^n and executes the command number k can be denoted by the triple (m, k, n).

It is clear that these two modifications of Minsky algorithms are equivalent. Minsky's theorem states that for every recursive function $f(n)$ there exists a Minsky algorithm which for every number n transforms the configuration $(2^n, 1, 0)$ to $(2^{f(n)}, 0, 0)$ if n belongs to the domain of f or works indefinitely long without coming to a stop configuration if n is not in this domain.

We shall need another, the third, kind of Minsky algorithms. These are algorithms of the first form simulating algorithms of the second form. I used similar algorithms in [18].

Let M be any algorithm of the second form. We create a new algorithm M' using the following method.

The start command adds a coin in the first glass.

1 *Add a coin to the first glass and go to* 1.1.

Let α be the instruction number i in M. We put several instructions with numbers i.1, i.2,... into M'.

If α has the form "multiply by 2 and go to instruction j" then we add instructions

$i.1$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.2$ *otherwise go to instruction* $i.4$.

$i.2$ *Add a coin to the second glass and go to* $i.3$.

$i.3$ *Add a coin to the second glass and go to* $i.1$.

$i.4$ *If the second glass is not empty then remove a coin from the second glass and go to instruction* $i.5$ *otherwise go to instruction* $j.1$.

$i.5$ *Add a coin to the first glass and go to* $i.4$.

If the algorithm starts with a configuration $(k, i.1, 0)$, then it first removes the coins from the first glass, and puts $2k$ coins to the second glass, moving to the configuration $(0, i.4, 2k)$, then it transfers coins from the second glass into the first glass, moving to the configuration $(2k, j.1, 0)$. Thus indeed this algorithm simulates multiplication by 2.

If α has the form "multiply by 3 and go to instruction j" then we add instructions

$i.1$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.2$ *otherwise go to instruction* $i.5$.

$i.2$ *Add a coin to the second glass and go to* $i.3$.

$i.3$ *Add a coin to the second glass and go to* $i.4$.

$i.4$ *Add a coin to the second glass and go to* $i.1$.

$i.5$ *If the second glass is not empty then remove a coin from the second glass and go to instruction* $i.6$ *otherwise go to instruction* $j.1$.

$i.6$ *Add a coin to the first glass and go to* $i.4$.

This algorithm simulates multiplication by 3.

One can easily write algorithms simulating the other three types of instructions of Minsky algorithms of the second form.

Nevertheless for the sake of comppleteness we present them here.

If α has the form "if the number is divisible by 2 then divide by 2 and go to instruction number j, otherwise go to instruction number k" then we add instructions

$i.1$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.2$ *otherwise go to instruction* $i.5$.

$i.2$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.3$ *otherwise go to instruction* $i.6$.

$i.3$ *Add a coin to the second glass and go to* $i.1$.

$i.4$ *If the second glass is not empty then take a coin from the second glass and go to* $i.5$ *otherwise goto* $j.1$.

$i.5$ *Add a coin to the first glass and go to* $i.4$.

$i.6$ *If the second glass is not empty then take a coin from the second glass and go to* $i.7$ *otherwise goto* $k.1$.

$i.7$ *Add a coin to the first glass and go to* $i.8$.

$i.8$ *Add a coin to the first glass and go to* $i.6$.

If α has the form "if the number is divisible by 3 then divide by 3 and go toinstruction number j, otherwise go to instruction number k" then we add instructions

$i.1$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.2$ *otherwise go to instruction* $i.5$.

$i.2$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.3$ *otherwise go to instruction* $i.7$.

$i.3$ *If the first glass is not empty then remove a coin from the first glass and go to instruction* $i.4$ *otherwise go to instruction* $i.7$.

$i.4$ *Add a coin to the second glass and go to* $i.1$.

$i.5$ *If the second glass is not empty then take a coin from the second glass and go to* $i.6$ *otherwise goto* $j.1$.

$i.6$ *Add a coin to the first glass and go to* $i.5$.

$i.7$ *If the second glass is not empty then take a coin from the second glass and go to* $i.8$ *otherwise goto* $k.1$.

$i.8$ *Add a coin to the first glass and go to* $i.9$.

$i.9$ *Add a coin to the first glass and go to* $i.10$.

$i.10$ *Add a coin to the first glass and go to* $i.7$.

The stop command is translated in the following way:

0.1 *If the first glass is not empty then remove a coin from the first glass and go to* 0.1 *otherwise go to* 0.2.

0.2 *If the second glass is not empty then remove a coin from the second glass and go to* 0.2 *otherwise go to 0.*

0 Stop

The following two statements are obvious.

Lemma 2.1 *a) If M computes a function $f(n)$ then the new algorithm M' computes the function $f'(n) : 2^n - 1 \to 0$ with domain consisting of all numbers $2^n - 1$ for which n belongs to the domain of f. In particular* 0 *belongs to the domain of f if and only if it belongs to the domain of M'.*

b) Instruction number 1 in M' is of the form "add a coin to the first glass" and cannot be executed in the middle of any computation, that is there are no instructions in M' containing "go to 1".

If M is a Minsky algorithm, then we say that two configurations (m, j, n) and (m', j', n') are M-equivalent if M transforms them to the same configuration (m'', j'', n'').

Lemma 2.2 *Suppose that we have a pair of computations of M':*

$$(0, i, 0) \to (m_1, i_1, n_1) \to \ldots \to (m_k, i_k, n_k) = (m, j, n),$$

$$(0, i', 0) \to (m'_1, i'_1, n'_1) \to \ldots \to (m'_k, i'_k, n'_k) = (m, j, n)$$

then in each of these computations, we need to check if glass 1 is empty and if glass 2 is empty, and at the time of the check the corresponding glass turns out to be empty.

We shall call Minsky algorithms M' satisfying the conditions of Lemmas 2.1 and 2.2 *proper.*

Since there is no algorithm to decide whether 0 belongs to the domain of a recursive function, Lemmas 2.1 and 2.2 imply

Lemma 2.3 *a) There exists a proper Minsky algorithm with undecidable halting problem.*

b) It is impossible to decide given a proper Minsky algorithm whether the function it calculates has 0 in its domain.

3 An Interpretation of Minsky's Algorithms

Let M be a proper Minsky algorithm, computing a function $f(n)$. Let $N+1$ be the number of instructions in M and let us numerate the instructions by numbers from 0 to N where instruction 1 is the first instruction and instruction 0 is Stop. Let us define two finite 4-nilpotent semigroups $S(M)$ and $T(M)$. $S(M)$ is generated by the union of the set $\{a, \bar{b}, q_i, p_i \mid i = 0, \ldots, N\}$ and a set $U(M)$ which will be defined later; $T(M)$ is generated by the union of the set $\{A, b, \bar{a}, B\}$ and the same set $U(M)$. The set $U(M)$ consists of 0 (which acts as zero in both $S(M)$ and $T(M)$), the elements q_0, q_1 and the elements $u_{i,j}$, $i = 0, \ldots, N$, $j = 1, \ldots, k(i)$ (for some $k(i)$ defined below), which correspond to instructions in M. Let us define this correspondence and defining relations between elements of $S(M)$ and $T(M)$.

Pick an integer $i = 0, \ldots, N$.

If the instruction number i in M has the form: *Put a coin in the glass* $\#\ 1$ *and go to instruction* $\#\ j$ then $U(M)$ contains elements $u_{i,1}, u_{i,2}$, so $k(i) = 2$, and we have the following relations

Relations in $S(M)$	Relations in $T(M)$
$q_i = a u_{i,1} p_i$	$u_{i,1} = b u_{i,2}$
$u_{i,2} p_i = q_j$	

If the instruction number i in M has the form: *Put a coin in the glass # 2 and go to instruction # j* then $U(M)$ contains elements $u_{i,1}, u_{i,2}$, so $k(i) = 2$, and we have the following relations

Relations in $S(M)$	Relations in $T(M)$
$q_i = p_i u_{i,1} \bar{a}$	$u_{i,1} = u_{i,2} \bar{b}$
$p_i u_{i,2} = q_j$	

If the instruction number i in M has the form: *If the glass # 1 is not empty then take a coin from this glass and go to instruction # j otherwise go to instruction # k* then $U(M)$ contains elements $u_{i,1}, u_{i,2}, u_{i,3}$, so $k(i) = 3$, and we have the following relations

Relations in $S(M)$	Relations in $T(M)$
$q_i = u_{i,1} p_i$	$b u_{i,1} = u_{i,2}$
$a u_{i,2} p_i = q_j$	$A u_{i,1} = A u_{i,3}$
$u_{i,3} p_i = q_k$	

If the instruction number i in M has the form: *If the glass # 2 is not empty then take a coin from this glass and go to instruction # j otherwise go to instruction # k* then $U(M)$ contains elements $u_{i,1}, u_{i,2}, u_{i,3}$, so $k(i) = 3$, and we have the following relations

Relations in $S(M)$	Relations in $T(M)$
$q_i = p_i u_{i,1}$	$u_{i,1} \bar{b} = u_{i,2}$
$p_i u_{i,2} \bar{a} = q_j$	$u_{i,1} B = u_{i,3} B$
$p_i u_{i,3} = q_k$	

Let us call all these relations the *main* relations of $S(M)$ (resp. $T(M)$).

We also add to $S(M)$ (resp. $T(M)$) all relations of the form $w = 0$ where w is any word in generators of $S(M)$ (resp. $T(M)$) which is not a subword of any word participating in the main relations, and the words Aq_1B and Aq_0B. For example, $a\bar{a} = aq_i = q_i\bar{a} = 0$ in $S(M)$, $Ab = AB = 0$ in $T(M)$. Thus the semigroups generated by $U(M)$ in both in $S(M)$ and in $T(M)$ are semigroups with zero product.

We have described all defining relations of $S(M)$ and $T(M)$. It is easy to see that $S(M)$ (resp. $T(M)$) consists of subwords of the words participating in the main relations and 0 and subwords of Aq_1B, Aq_0B. Some of these subwords are equal in $S(M)$ or in $T(M)$. But it is easy to describe these equalities. Indeed no defining relation of $S(M)$ (resp. $T(M)$) apply to proper subwords of the sides of the main relations of $S(M)$ (resp. $T(M)$). Thus if s and t are different words which are not equal to 0 in $S(M)$ (resp. $T(M)$) then s is equal to t in $S(M)$ (resp. $T(M)$) if and only if s and t are sides of the main defining relations of $S(M)$ (resp. $T(M)$) or subwords of Aq_1B or Aq_0B and there is a sequence of defining relations or their inverses: $s = r_1, r_1 = r_2, \ldots, r_n = t$. Now a simple inspection of the main defining relations of $S(M)$ and $T(M)$ gives the following statements.

Lemma 3.1 *Let s and t be two distinct words in the alphabet of generators of $S(M)$. Then s and t are equal in $S(M)$ if and only if one of the following three conditions hold.*

1. *s and t are not subwords of the sides of the main relations of $S(M)$ (in this case $s = t = 0$);*
2. *$s = t$ or $t = s$ is one of the main defining relations of $S(M)$;*
3. *$s = q_i$ and $t = q_i$ are among the main defining relations of $S(M)$ for some i.*

Lemma 3.2 *Let s and t be two distinct words in the alphabet of generators of $T(M)$. Then s and t are equal in $T(M)$ if and only if one of the following two conditions hold.*

1. *s and t are not subwords of the sides of the main relations of $T(M)$ and not subwords of Aq_1B, Aq_0B (in this case $s = t = 0$);*
2. *$s = t$ is one of the main defining relations of $T(M)$ or is obtained from such a relation by multiplying by A on the left or by B on the right.*

In particular no two distinct generators of $U(M)$ are equal in $S(M)$ or $T(M)$. Therefore the semigroups $S(M)$ and $T(M)$ form an amalgam with the intersection $S(M) \cap T(M) = U(M)$, a semigroup with zero product (no products of length 2 of generators of $U(M)$ is a subwordr of a defining relation of $S(M)$ or $T(M)$, or Aq_1B, Aq_0B, so each such product is equal to 0. Notice also that all words of length ≥ 4 are equal to 0 in $S(M)$ and in $T(M)$ (because the words in the main defining relations have lengths ≤ 3), so these semigroups are 4-nilpotent.

4 The word problem in $S(M) *_{U(M)} T(M)$

Notice that the semigroup $S(M) *_{U(M)} T(M)$ is given by the union of defining relations of $S(M)$ and $T(M)$.

The following lemma can be proved by a simple expection.

Lemma 4.1 *The presentation of $S(M) *_{U(M)} T(M)$ has no overlaps.*

We can consider a presentation of any semigroup as a rewriting system. If s and t are words in the generators of the semigroup, we shall write $s \Rightarrow t$ if this rewriting system rewrites s to t in several steps. The number of steps is denoted by $|s \Rightarrow t|$ and can be equal to 0. If s can be rewritten to t in 1 step, we shall write $s \to t$. The following lemma is probably well known.

Lemma 4.2 *If a presentation of a semigroup S does not have overlaps then for every two words s and t in the generators of S, $s = t$ in S if and only if there exists a word w, such that $s \Rightarrow w$ and $t \Rightarrow w$.*

Proof. Indeed, suppose that $s = t$ in S. Then there exists a sequence of words $w_1, ..., w_n$ such that

$$s \Rightarrow w_1, w_2 \Rightarrow w_1, w_2 \Rightarrow w_3, ..., t \Rightarrow w_n. \tag{1}$$

Here all words are considered different, so the first and/or the last transition may be omitted if $s \equiv w_1$ or $t \equiv w_n$.

We denote $w_0 \equiv s$, $w_{n+1} = t$. We assume that n is minimal possible. If $n = 1$ we are done. Suppose $n > 1$. Then there exists $i > 1$ such that the words w_{i-1}, w_i and w_{i+1} are distinct, and $w_i \Rightarrow w_{i-1}$ and $w_i \Rightarrow w_{i+1}$.

For each of these "bad" i we denote the maximal number among $|w_i \Rightarrow w_{i-1}|$ and $|w_i \Rightarrow w_{i+1}|$ by $h(i)$. The maximal number among all $h(i)$ is denoted by h. We can assume that h is the smallest possible.

Take one of the "bad" i's. Then for some different words x and y we have $w_i \to x$, $w_i \to y$ and $|x \Rightarrow w_{i-1}| < |w_i \to w_{i-1}|$ and $|y \Rightarrow w_{i+1}| < |w_i \Rightarrow w_{i+1}|$. Since there are no overlaps between relations participating in the transitions $w_i \to x$ and $w_i \to y$, there exists a word z such that $x \to z$ and $y \to z$ (z is obtained from x using the same relation which was used to get y from w_i). Now replace parts $w_i \Rightarrow w_{i-1}$ and $w_i \Rightarrow w_{i+1}$ in our sequence (1) by

$$x \Rightarrow w_{i-1}, x \to z, y \to z, y \Rightarrow w_{i+1}.$$

Of course, if, for example, $x \equiv w_{i-1}$ we do not include the transition $x \Rightarrow w_{i-1}$ in our sequence: we keep all words in our sequence different.

If we apply this operation to all "bad" i in (1), we obviously lower our parameter h. This contradicts the assumption that h is minimal possible. Thus there are no "bad" i in the sequence (1), and it has one of the forms:

$$s \Rightarrow w, t \Rightarrow w,$$

$$s \Rightarrow t,$$

$$t \Rightarrow s.$$

The lemma is proved. □

Now we return to the semigroup $S(M) *_{U(M)} T(M)$ and from now on we shall consider the presentation of $S(M) *_{U(M)} T(M)$ defined above and the corresponding rewriting system. Lemmas 4.1 and 4.2 immediately imply

Lemma 4.3 *Two words s and t are equal in $S(M) *_{U(M)} T(M)$ if and only if there exists a word w such that $s \Rightarrow w$ and $t \Rightarrow w$.*

Consider the following set S of all words of the form $W(m,i,n) \equiv A(ab)^m q_i(\bar{a}\bar{b})^n B$, $m,n = 0,1,...$ and all words obtained from them by applying relations of $S(M) *_{U(M)} T(M)$.

¿From the definition of the presentation of $S(M) *_{U(M)} T(M)$, it is clear that if M transforms the configuration (m,i,n) into $(0,0,0)$ then $W(m,i,n) \Rightarrow W(0,0,0)$, and so $W(m,i,n) = W(0,0,0)$ in $S(M) *_{U(M)} T(M)$. On the other hand suppose that $W(m,i,n) = W(0,0,0)$ in $S(M) *_{U(M)} T(M)$. Then by Lemma 4.3 there exists a word W such that $W(m,i,n) \Rightarrow W$, $W(0,0,0) \Rightarrow W$. But there are no defining relations of $S(M) *_{U(M)} T(M)$ which can be applied to $W(0,0,0)$. Therefore $W(0,0,0) \equiv W$ and $W(m,i,n) \Rightarrow W(0,0,0)$.

This proves the following

Lemma 4.4 *$W(m,i,n) = W(0,0,0)$ in $S(M) *_{U(M)} T(M)$ if and only if M transforms (m,i,n) to $(0,0,0)$.*

Now we are able *to prove Theorem 1.1.* Take any proper Minsky algorithm with undecidable halting problem (by Lemma 2.3 such an algorithm exists). Then by Lemma 4.4 the amalgamated product $S(M) *_{U(M)} T(M)$ of two finite 4-nilpotent semigroups $S(M)$ and $T(M)$ has undecidable word problem.

Remark. It follows from Lemma 4.5 below that if 0 does not belong to the domain of the function computed by M, then the amalgam $S(M) \cup_{U(M)} T(M)$ embeds into $S(M) *_{U(M)} T(M)$. Thus there exists an embeddable amalgam of two finite 4-nilpotent semigroups such that the corresponding amalgamated product has undecidable word problem.

Lemma 4.5 *If 0 does not belong to the domain of the function computed by a proper Minsky algorithm M then the amalgam $S(M) \cup_{U(M)} T(M)$ is embeddable into $S(M) *_{U(M)} T(M)$.*

Proof. Suppose that 0 does not belong to the domain of the function computed by M. We need to check that subwords of the words involving in the main relations $S(M)$ and $T(M)$ and subwords of Aq_1B and Aq_0B cannot be equal to other such subwords unless they are equal in $S(M)$ or $T(M)$.

Since no relation of $S(M) *_{U(M)} T(M)$ applies to a proper subword of a word involved in a relation of $S(M) *_{U(M)} T(M)$, we can consider only the parts of the relations of $S(M) *_{U(M)} T(M)$ and subwords of Aq_1B, Aq_0B.

It is easy to see that if w is a part of a relation α and neither w nor the other part of the relation is q_i (for any i) then there exists at most one other word t such that $w \Rightarrow t$. This and Lemma 4.3 immediately imply that w cannot be equal to a word t in $S(M) *_{U(M)} T(M)$ unless it is equal to t in $S(M) \cup_{U(M)} T(M)$.

It remains to consider the case when two words w_1, w_2 belong to the set consisting of all q_i and all subwords of Aq_1B or Aq_0B containing q_1 or q_0. Suppose that two such words are equal in $S(M) *_{U(M)} T(M)$. Then by Lemma 4.3 $w_1 \Rightarrow w$ and $w_2 \Rightarrow w$ for some word w. Suppose first that $w_1 = q_i$, $w_2 = q_j$. Then we have two sequences of applications of relations of $S(M) *_{U(M)} T(M)$:

$$q_i \to s_1 \to s_2 \to \ldots \to s_m = w, \tag{2}$$

$$q_j \to t_1 \to t_2 \to \ldots \to t_n = w. \tag{3}$$

Then we have the following corresponding sequences

$$Aq_iB \to As_1B \to As_2B \to \ldots \to As_mB = AwB, \tag{4}$$

$$Aq_jB \to At_1B \to At_2B \to \ldots \to At_nB = AwB. \tag{5}$$

Let us denote the set of relations of $S(M) *_{U(M)} T(M)$ which correspond to the instruction number k by R_k. It is easy to see that letters p, u with indices appearing in different R_i are different, and that the left part of every relation in R_i except the first one contains either u or p. An easy induction shows that every word in the sequences (2)-(5) contains at most one u-letter and at most one p- or q-letter. Therefore for every word in these sequences, only one of the main relations can apply. If we have a word of the form $A(ab)^m q_i(\bar{a}\bar{b})^n B$ then the only relation which can be applied to this word is the first relation of R_i, and we must keep applying relations of R_i in the natural order, until we get a word of the form $A(ab)^{m'} q_j(\bar{a}\bar{b})^{n'} B$. The relations of R_i are chosen in such a way that in this case the Minsky algorithm M transforms (m, i, n) to (m', i', n') in one step. Therefore we can assign a configuration (m, i, n) of the Minsky algorithm M to any word in the sequences (4), (5) in the following way: we assign (m, i, n) to the word of the form $A(ab)^m q_i(\bar{a}\bar{b})^n B$ and to each word not of this form, obtained from it by applying a sequence of relations from R_i. Then the sequences of configurations corresponding to the sequences (4) and (5) have the following form:

$$[(0,i,0),...,(0,i,0)],[(m_1,i_1,n_1),...,(m_1,i_1,n_1)],...,[(m_k,i_k,n_k),...,(m_k,i_k,n_k)],$$

$$[(0,j,0),...,(0,j,0)],[(m'_1,i'_1,n'_1),...,(m'_1,i'_1,n'_1)],...,[(m'_\ell,i'_\ell,n'_\ell),...,(m'_\ell,i'_\ell,n'_\ell)];$$

I combined equal configurations corresponding to the blocks of applications of relations from R_s in square brackets. If we take one representative of each square bracket, we get two computations of the Monsky algorithm M:

$$(0, i, 0) \to (m_1, i_1, n_1) \to \ldots \to (m_k, i_k, n_k),$$

$$(0, j, 0) \to (m'_1, i'_1, n'_1) \to \ldots \to (m'_\ell, i'_\ell, n'_\ell)].$$

Since sequences (4), (5) end with the same word w, we have $(m_k, i_k, n_k) = (m'_\ell, i'_\ell, n'_\ell)$. Since M is proper, in each of these computations we need to check if the glass 1 is empty and if the glass 2 is empty and at the time of the check these glasses turn out to be empty. It is easy to see that in this situation the corresponding sets of relations R_i include relations of containing A (if we check the first glass) and B (if we check the second glass) in their left sides, and we need to apply these relations. So relations involving A and B are applied in (4) and in (5). But the relations applied in sequences (2) (resp. (3) are the same as relations applied in (4) (resp. (5). Thus relations involving A and B are applied in (2) and (3). But letters A and B cannot appear as a result of application of any relation of $S(M) *_{U(M)} T(M)$, and the first words in these sequences do not contain A and B, a contradiction.

An almost identical argument works in any case when w_1 or w_2 do not belong to $\{Aq_1B, Aq_0B\}$. Therefore it remains to consider the case $w_1 = Aq_1B$, $w_2 = Aq_0B$ (the situation when $w_1 = Aq_0B$, $w_2 = Aq_1B$ is of course similar). In this case as before we have corresponding computations of M:

$$(0,1,0) \to ... \to (m,i,n)$$
$$(0,0,0) \to ... \to (m,i,n).$$

Since $(0,0,0)$ is the stop configuration of M, we have $(m,i,n) = (0,0,0)$, and so 0 belongs to the domain of the function computed by M, a contradiction. This proves that if 0 does not belong to the function computed by M, then the amalgam $S(M) \cup_{U(M)} T(M)$ embeds into $S(M) *_{U(M)} T(M)$.

On the other hand if 0 belongs to this domain then we have a computation $(0,1,0) \to ... \to (0,0,0)$, and as before $Aq_1B = W(0,1,0) \Rightarrow W(0,0,0) = Aq_0B$ in $S(M) *_{U(M)} T(M)$. Both Aq_1B and Aq_0B are elements of $T(M)$ which are different in $T(M)$ (no relation of $T(M)$ applies to any of these words). So in this case the amalgam $S(M) \cup_{U(M)} T(M)$ does not embed into any semigroup.

The lemma is proved.

Now *Theorem 1.2* immediately follows from Lemmas 2.3 and 4.5.

5 Proof of Theorem 1.3

Although the formulation of Theorem 1.3 is similar to the formulation of Theorem 1.2, the proof presented here is completely different. We are going to use a construction which first appeared in [6] and then was used again in [7] to solve Rhodes' problem.

A set A with a partial binary operation $\cdot$ on it and a distinguished element 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in A$ will be called a *partial group* if it satisfies the *cancellation property*: $ac = bc \to a = b$ and $ca = cb \to a = b$.

By a theorem of T. Evans [4, 5] (see also Connection 2.2 in [14]), the problem of embeddability of finite partial algebras into algebras of a pseudo-variety is decidable if and only if the universal theory of this pseudo-variety is decidable. Since by a result of Slobodskoj [19] the universal theory of finite groups is undecidable, the following problem is undecidable:

> Given a finite partial group A, decide whether or not A is embeddable into a finite group.

Let us call a partial group A *symmetric* if for every $a \in A$ there exists a unique element $a' \in A$ such that $aa' = a'a = 1$. A partial group $B > A$ is called a symmetric extension of A if B is symmetric and for every element $b \in B$ either b or b' belongs to A. Thus the order of every symmetric extension of A does not exceed $2|A|$ so every finite partial group has only finitely many symmetric extensions and all of them can be effectively listed. It is clear that a partial group A is embeddable into a group if and only if one of its symmetric extensions is embeddable into this group. Therefore we have the following result.

Lemma 5.1 *There is no algorithm to decide whether a given finite symmetric partial group is embeddable into a finite group.*

Let B be a partial group and let A be embedded into B. For every $i = 1, 2 \ldots$ let us define a subset A^i of B. Let $A^0 = \{1\}$, $A^1 = A$ and for every $i > 1$ let $A^{i+1} = A^i \cdot A$. We shall call a partial group B an *extension* of A *or rank* k if:

- $B = \bigcup_{s=0}^{k} A^s$.
- for every numbers i and j between 0 and k such that $i + j \leq k$ and for every pair of elements $x \in A^i$ and $y \in A^j$ the product xy exists in B and belongs to A^{i+j}.
- all products $x \cdot y$ where $x \in A^i \backslash A^{i-1}$, $y \in A^j \backslash A^{j-1}$ and $i + j > k$ are undefined.
- for every $x \in A^i, y \in A^j, z \in A^m$ such that $i + j + m \leq k$ both $(xy)z$ and $x(yz)$ are defined and $(xy)z = x(yz)$.

It is clear that there are only finitely many extensions of rank k (for any fixed k) of any finite partial group A, and all of them can be effectively listed.

It is also clear that a partial group A is embeddable into a group G if and only if some extension of A of rank k is embeddable into G.

Now take any extension C of rank 3 of a finite symmetric partial group A.

With every such C we associate the following algebra

$$\begin{aligned}&S(C) = (\{1\} \times A \times \{2\}) \cup (\{2\} \times A \times \{3\}) \cup (\{3\} \times A \times \{4\})\\ &\cup(\{1\} \times (A^2 \cup A) \times \{3\}) \cup (\{2\} \times (A^2 \cup A) \times \{4\}) \cup (\{1\} \times C \times \{4\}) \cup \{0\}.\end{aligned}$$

with one binary operation: $(i, a, j)(j, b, k) = (i, ab, k)$ for every $a, b \in A$, $1 \leq i < j < k \leq 4$, other products are equal to 0.

It is easy to check that $S(C)$ is a 4-nilpotent semigroup. This construction first appeared in [6].

For every $i < j, i, j = 1, ..., 4$, let $e_{i,j} = (i, 1, j) \in S(C)$.

For every group G consider also the Brandt semigroup $B_4(G)$ [2] consisting of 0 and all triples (i, g, j) with $i, j = 1, 2, 3, 4, g \in G$ and multiplication

$$(i, g, j)(i', g', j') = \begin{cases} (i, gg', j') & \text{if } j = i'; \\ 0 & \text{otherwise.} \end{cases}$$

It is clear and well known that $B_4(1)$ is inside $B_4(G)$ for every G.

The following lemma is essentially Lemma 5 from [7]. I only replaced the part 2 of Lemma 5 in [7] by a stronger statement. The fact that this replacement is possible follows immediately from the proof of Lemma 5 in [7], see the first paragraph of that proof.

Lemma 5.2 *For every finite symmetric partial group A the following conditions are equivalent:*

1. *A is embeddable into a finite group.*

2. *There exists an extension C of A of rank 3 such that the semigroup $S(C)$ is embeddable into a finite Brandt semigroup $B_4(G)$ for some group G; under this embedding elements $(i,1,j)$ go to $(i,1,j)$ and 0 goes to 0.*

3. *There exists an extension C of A of rank 3 such that the semigroup $S(C)$ is embeddable into a finite semigroup T where $(2,1,3) = x(1,1,4)y$ for some $x, y \in T$.*

4. *There exists an extension C of A of rank 3 such that the semigroup $S(C)$ is embeddable into a finite semigroup T where $(1,1,4) = x(2,1,3)y$ and $(2,1,3) = x'(1,1,4)y'$ for some $x, x', y.y' \in T$, that is $(1,1,4)$ and $(2,1,3)$ are in the same $\mathcal{J}$-class of T.*

Notice that the set $U = \{(1,1,2),(2,1,3),(3,1,4),(1,1,3),(2,1,4),(1,1,4),0\}$ form the same 4-nilpotent subsemigroup in $B_4(1)$ and in $S(C)$ for every C. For every extension C of rank 3 of a finite symmetric partial group A, consider the amalgam $Z(C)$ of $S(C)$ and $B_4(1)$ where U is amalgamated.

Lemma 5.3 *For every finite symmetric partial group A the following conditions are equivalent:*

1. *A is embeddable into a finite group.*

2. *There exists an extension C of A of rank 3 such that the amalgam $Z(C)$ is embeddable into a finite semigroup.*

3. *There exists an extension C of A of rank 3 such that the amalgam $Z(C)$ is embeddable into a finite 0-simple semigroup.*

Proof. If A is embeddable into a finite group G then by Lemma 5.2 there exists an extension C of A of rank 3 embeddable such that $S(C)$ is embeddable into $B_4(G)$. Under this embedding the elements from U map onto the corresponding elements of $B_4(1)$ embedded in $B_4(G)$. Thus the whole amalgam $Z(C)$ is embedded into $B_4(G)$. Since $B_4(G)$ is 0-simple and finite, we get implication $1 \to 3$.

Implication $3 \to 2$ is obvious.

Suppose that for some extension C of rank 3 of a finite symmetric partial groupoid A the amalgam $S(C)$ is embedded into a finite semigroup T. The equality $(2,1,3) = (2,1,1)(1,1,4)(4,1,3)$ holds in $B_4(1)$. Therefore element $(2,1,3)$ is divisible by $(1,1,4)$

in T. By Lemma 5.2 this implies that A is embeddable into a finite group. This gives $2 \to 1$. The lemma is proved.

The *proof of Theorem 1.3* follows now immediately. Indeed, since the problem of embeddability of finite symmetric partial groups into finite groups is undecidable, there is no algorithm to decide whether an amalgam of the form $Z(C)$ is embeddable into a finite semigroup.

References

[1] J.-C. Birget, S. Margolis, J. Meakin, On the word problem for tensor products and amalgams of monoids, IJAC, to appear.

[2] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups.* Volume 1, 2, Amer. Math. Soc., Providence, 1961, 1967.

[3] Deko V. Dekov, The class of all embeddable semigroup amalgams is not finitely axiomatizable. J. Pure Appl. Algebra 125 (1998), no. 1-3, 135–139.

[4] T. Evans. On multiplicative systems defined by generators and relations. I. Normal form theorems. *Proc. Cambridge Phil. Soc*, 47:637–649, 1951.

[5] T. Evans. The word problem for abstract algebras. *J. London Math. Soc.*, 26:64–71, 1951.

[6] T. Hall, S. Kublanovsky, S. Margolis, M. Sapir, and P. Trotter. Decidable and undecidable problems related to finite 0-simple semigroups, , J. Pure and Applied Algebra, 119: 75-96, 1997

[7] S. Kublanovsky, M. Sapir, Potential divisibility in finite semigroups is undecidable, IJAC, 1999 (to appear).

[8] T. Hall, Amalgamation and inverse and regular semigroups. Trans. Amer. Math. Soc. 246 (1978), 395–406.

[9] T. E. Hall and M. S. Putcha. The potential J-relation and amalgamation bases for finite semigroups. Proc. AMS, 95 (1985), 3, 361–364.

[10] Peter M. Higgins, Epimorphisms and amalgams. Colloq. Math. 56 (1988), no. 1, 1–17.

[11] John M. Howie, *Fundamentals of semigroup theory.* London Mathematical Society Monographs. New Series, 12. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1995.

[12] John M. Howie, Isbell's zigzag theorem and its consequences. Semigroup theory and its applications (New Orleans, LA, 1994), 81–91, London Math. Soc. Lecture Note Ser., 231, Cambridge Univ. Press, Cambridge, 1996.

[13] A.Karrass, A.Pietrowski, D. Solitar, Finite and infinite cyclic extensions of free groups, J. Austr. Math. Soc.,16, 1973, 458-466.

[14] O.G. Kharlampovich and M.V. Sapir. Algorithmic problems in varieties. *Inter. J. Algebra Comput.*, 5 (1995), 4–5, 379–602.

[15] Gerard Lallement, Amalgamated products of semigroups: the embedding problem. Trans. Amer. Math. Soc. 206 (1975), 375–394.

[16] R. C. Lyndon and P. E. Schupp. *Combinatorial group theory.* Springer-Verlag, 1977.

[17] Jan Okniński, Mohan Putcha, Embedding finite semigroup amalgams. J. Austral. Math. Soc. Ser. A 51 (1991), no. 3, 489–496.

[18] M. V. Sapir, On the word problem in periodic group varieties. Internat. J. Algebra Comput. 1 (1991), no. 1, 115–126.

[19] A. M. Slobodskoi. Undecidability of the universal theory of finite groups. *Algebra i Logika*, 20(2):207–230, 1981.

Mark V. Sapir
Department of Mathematics
Vanderbilt University
Nashville, TN 37240
msapir@math.vanderbilt.edu
http://www.math.vanderbilt.edu/~msapir