A variety where the set of subalgebras of finite simple algebras is not recursive

Stanislav Kublanovsky and Mark Sapir

May 27, 1996

Abstract

We construct a finitely based variety of algebras with two binary operations where the set of subalgebras of finite simple algebras is not recursive.

It is easy to see that the set of finite simple algebras in any finitely based variety is recursive. In this article we are interested in the problem when a finite algebra in a variety is embeddable into a finite simple algebra in this variety.

Every finite group is embeddable into a finite simple group (the group of even permutations on a finite set). Thus our problem is decidable in the variety of all groups. The classification of finite simple groups and the result of Weigel [5] that any infinite set of finite simple non-Abelian groups generates the variety of all groups shows that our problem is decidable in any finitely based variety of groups.

Our problem is decidable for the variety of associative rings. Indeed, simple finite rings are rings of matrices over a finite field. Thus a finite associative ring is embeddable into a finite simple ring if and only if it has prime characteristics. Similarly, one can show that the problem is decidable in any finitely based variety of associative rings.

Finite congruence simple semigroups are exactly finite simple groups or aperiodic 0-simple semigroups over the trivial group whose sandwich matrices have no equal columns and no equal rows (see [1]). Every completely 0-simple semigroup over the trivial group can be embedded into a finite congruence simple semigroup. Thus the set of subsemigroups of finite congruence simple semigroups coincides with the union of the set of all finite groups and the set of subsemigroups of finite aperiodic 0-simple semigroups. It follows from the main theorem of [3] that the second set is recursive (because the universal theory of the trivial group is decidable). Thus the set of subsemigroups of congruence simple finite semigroups is recursive. The same result holds for any finitely based variety of semigroups.

In this article we find a finitely based variety of universal algebras where the set of subalgebras of simple finite algebras is not recursive.

More precisely the main result of the paper is the following theorem.

Theorem 1 *Let $\mathcal{V}$ be the variety of algebras with two binary operations $*$ and $+$ given by the following identities:*

1. $(x*y)*z = x*(y*z)$

2. $x+y = y+x$

3. $(x*(u+v)*y)*(x*(u+v)*y) = x*u*y*x*(u+v)*y$

Then there is no algorithm to decide whether a given finite algebra in $\mathcal{V}$ is embeddable into a simple finite algebra in $\mathcal{V}$. In other words the set of subalgebras of finite simple algebras in $\mathcal{V}$ is not recursive.

We will omit $*$ in the terms of the variety $\mathcal{V}$. So instead of $x*y$ we will write simply xy.

Recall that a semigroup is called 0-simple if it does not contain ideals except for S itself and possibly $\{0\}$. A semigroup S with 0 is called nil-semigroup if every element in S in some power is equal to 0. Recall also that if I is an ideal of S then the Rees factor-semigroup S/I consists of elements $\{I\}$ and $\{a\}$ for all $a \in S \backslash I$ with the obvious multiplication). The corresponding congruence on S is called a Rees congruence.

Our proof of Theorem 1 is based on the following lemma.

Lemma 1 *Let S be a finite simple algebra in $\mathcal{V}$. Then considered as a semigroup $(S,*)$ the algebra S has an ideal I such that I is 0-simple and the Rees factor semigroup S/I is a nil-semigroup.*

Proof. Let S be a finite simple algebra in $\mathcal{V}$. Without loss of generality assume that $|S| > 1$. Let I be a 0-minimal ideal of the semigroup $(S,*)$ (i.e. I is a non-zero ideal which contains no proper ideals of S except possibly 0). It is well known [1] that I is a 0-simple semigroup or a semigroup with zero product. Let us define the following sequence of of subsets I_n of S ($n = 0, 1, ...$): $I_0 = I$, $I_{n+1} = S^1(I_n + S)S^1$ for every $n \geq 0$. Here S^1 is the semigroup S with identity element adjoint.

Let $\bar{I} = \cup_{n=0}^{\infty} I_n$. From the definition of $\bar{I}$, it follows that $\bar{I}+S \subseteq \bar{I}$ and $S^1\bar{I} = \bar{I}S^1 = I$. This means that $\bar{I}$ is an ideal with respect to the both operations, $+$ and $*$. Then the Rees equivalence relation σ corresponding to $\bar{I}$ is a congruence on the algebra $(S,*,+)$. Since $|I| > 1$, σ does not coincide with the diagonal. Thus σ is the universal relation. So $S = \bar{I}$ because $(S,*,+)$ is simple.

Take any $n \geq 0$. Let $a \in I_{n+1}$. We will show that $a^6 \in I_n$. By definition, a can be represented in the form $a = x(u+v)y$ where $x, y \in S^1$, $u \in I_n$, $v \in S$. Then

$$\begin{aligned}
&a^6 = [x(u+v)yx(u+v)yx(u+v)y][x(u+v)yx(u+v)yx(u+v)y] = \\
&x_1(u+v)y_1x_1(u+v)y_1 \text{ (for some } x_1 \text{ and } y_1 \text{ from } S) = x_1uy_1x_1(u+v)y_1 \\
&\text{ (we used the identity 3)} \in SuS
\end{aligned}$$

By definition I_n is an ideal of $(S,*)$, we have that $SuS \subseteq I_n$. Thus $a^6 \in I_n$.

The fact proved in the previous paragraph implies that S/I is a nil-semigroup with respect to the operation $*$. (indeed, if $a \in I_n$ then $a^{6^n} \in I$). Now if I is a 0-simple semigroup then the statement of our lemma is true. If I is a semigroup with zero product then S is a nil-semigroup, so S is an extension of a trivial semigroup by a nil-semigroup and again the statement of the lemma is true. The lemma is proved.

Consider the class of finite semigroups $\mathcal{R}$ which consists of Rees ideal extensions of finite nil-semigroups by the four element semigroup $\{e, f, g, 0\}$ where $e^2 = e, f^2 = f, g^2 = g$ and all other products are equal to 0. The proof of the following result can be extracted from [3]. Nevertheless for the sake of completeness we present the proof here.

Proposition 1 *The problem of whether a given semigroup from $\mathcal{R}$ is embeddable into a finite 0-simple semigroup is undecidable.*

Proof. 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*.

By a theorem of T. Evans [2], 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 [4] 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 group from $\mathcal{V}$.

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 may 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 the following problem is undecidable:

> Given a finite symmetric partial group A, decide whether or not A is embeddable into a group from $\mathcal{V}$.

Let B be a partial group and let A be embedded into B. Let A^2 be the set of all products $x \cdot y$ where $x, y \in A$. We shall call B *extension* of A *or rank* 2 if:

- The element $1 \in A$ is the identity element for B.
- $B = A \cup A^2$
- A product $x \cdot y$ where $x, y \in B$ is undefined unless $x, y \in A$ or $1 \in \{x, y\}$.

It is clear that there are only finitely many extensions of rank 2 of any finite partial group A and all of them may 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 2 is embeddable into G.

Thus the following problem is undecidable:

> Given a finite symmetric partial group A and an extension $B > A$ of rank 2, decide whether or not B is embeddable into a group from $\mathcal{V}$.

Let C be any partial group and let $B_n(C)$ be the set $\mathbf{n} \times C \times \mathbf{n}$ (where $\mathbf{n}$ stands for the set $\{1, 2, \ldots, n\}$) with the following partial operation:

$$(\ell, g, r)(\ell', g', r') = \begin{cases} (\ell, gg', r') & \text{if } r = \ell' \text{ and } gg' \text{ is defined ;} \\ 0 & \text{if } r \neq \ell'. \end{cases}$$

It is clear that for every group G the partial groupoid $B_n(G)$ is a 0-simple semigroup. In fact it is the so called Brandt semigroup, see [1].

Lemma 2 *If a partial group A is embeddable into a group G then there exists an extension of A of rank 2 such that $B_n(A')$ is embeddable into the Brandt semigroup $B_n(G)$.*

Proof. It is enough to compare the definitions of $B_n(G)$ and $B_n(C)$.

Now let A be a finite partial group, let A' be extension of A of rank 2. Let us define the following subsemigroup $S = S(A, A') \subset B_3(A')$.

$$\begin{aligned} &S = (\{1\} \times A \times \{2\}) \cup (\{2\} \times A \times \{3\}) \cup (\{1\} \times A' \times \{3\}) \\ &\cup\{(1,1,1)\} \cup \{(2,1,2)\} \cup \{(3,1,3)\} \cup \{0\}; \end{aligned}$$

Notice that the semigroup $S(A, A')$ is an extension of a nilpotent semigroup

$$S_1(A, A') = (\{1\} \times A \times \{2\}) \cup (\{2\} \times A \times \{3\}) \cup (\{1\} \times A' \times \{3\}) \cup \{0\}$$

and $S \backslash S_1$ consists of three idempotents $(1,1,1)$ and $(2,1,2)$ and $(3,1,3)$ which we shall call e_1, e_2 and e_3 respectively. It is easy to check that e_1 is a left unit for $\{1\} \times A \times \{2\}$ and for $\{1\} \times A' \times \{3\}$, e_2 is a left unit for $\{2\} \times A' \times \{3\}$ and a right unit for $\{1\} \times A \times \{2\}$ and e_3 is a right unit for $\{2\} \times A \times \{3\}$ and $\{1\} \times A' \times \{3\}$. In particular, $S(A, A') \in \mathcal{R}$.

Proposition 1 will immediately follow from Lemma 2 and the following lemma.

Lemma 3 *If S is a subsemigroup of a finite 0-simple semigroup over a group G then A is embeddable into G.*

Proof. Let ϕ be an embedding from $S(A, A')$ into a finite 0-simple semigroup M. By the theorem of Sushkevich [1] $M = M^0(G; L, R, P)$ where G is a group, L, R are finite sets, and P is a $|L| \times |R|$-matrix over $G \cup \{0\}$, $M^0(G; L, R, P) = L \times G \times R \cup \{0\}$ and the operation in M is defined as follows:

$$(\ell, g, r)(\ell', g', r') = \begin{cases} (\ell, gP(r, \ell')g', r') & \text{if } P(r, \ell') \neq 0; \\ 0 & \text{if } P(r, \ell') = 0. \end{cases}$$

We have that $\phi(e_i)$ is idempotent for $i = 1, 2, 3$. Since ϕ is an embedding, $\phi(e_i) \neq 0$, $i = 1, 2, 3$.

Let $\phi(e_i) = (\ell_i, g_i, r_i)$.

Since $e_1(1, a, 2)e_2 = (1, a, 2)$, $e_2(2, a, 3)e_3 = (2, a, 3)$ and $e_1(1, a', 3)e_3 = (1, a', 3)$ for every $a \in A$ and every $a' \in A'$ we have that

$$(\ell_1, g_1, r_1)\phi(1, a, 2)(\ell_2, g_2, r_2) = \phi(1, a, 2),$$

$$(\ell_2, g_2, r_2)\phi(2, a, 3)(\ell_3, g_3, r_3) = \phi(2, a, 3),$$
$$(\ell_1, g_1, r_1)\phi(1, a', 3)(\ell_3, g_3, r_3) = \phi(1, a, 3).$$

Therefore

$$\phi(1, a, 2) = \begin{cases} (\ell_1, f(a), r_2), \\ 0 \end{cases},$$

$$\phi(2, a, 3) = \begin{cases} (\ell_2, g(a), r_3), \\ 0 \end{cases},$$

$$\phi(1, a', 3) = \begin{cases} (\ell_1, h(a'), r_3), \\ 0 \end{cases}$$

for some (possibly partial) functions $f, g : A \to G$ and $h : A' \to G$.

Notice that since $e_2e_2 = e_2 \neq 0$, $P(r_2, l_2) \neq 0$. It is known (see [1]) that if we multiply all entries of a row (a column) of the matrix P by any element $x \in G$ from the left (right) and obtain a new matrix P' then the semigroups $M^0(G; L, R, P)$ and $M^0(G; L, R, P')$ are isomorphic. Thus we can assume that the entry $P(r_2, l_2)$ of the matrix P is equal to 1.

Since $\phi(\{1\} \times A \times \{3\}) \neq \{0\}$ there exists $z \in A$ such that $\phi(1, z, 3) \neq 0$. Since $z = 1 \cdot z = z \cdot 1$ we have that

$$0 \neq \phi(1, z, 3) = \phi(1, 1, 2)\phi(2, z, 3) = \phi(1, z, 2)\phi(2, 1, 3). \tag{1}$$

We also have that for every $c \in A'$, $a \in A$, $\phi(1, c, 3) \neq 0$, $\phi(1, a, 2) \neq 0$ and $\phi(2, a, 3) \neq 0$. Therefore

$$\phi(1, a, 2) = (\ell_1, f(a), r_2), \phi(2, a, 3) = (\ell_2, g(a), r_3), \phi(1, b, 3) = (\ell_1, h(b), r_3)$$

for every $a \in A, b \in A'$. Hence the functions f, g, h are everywhere defined.

For every $a, b \in A$ we have

$$(\ell_1, f(a), r_2)(\ell_2, g(b), r_3) = (\ell_1, f(a)g(b), r_3).$$

On the other hand since ϕ is a homomorphism we must have

$$(\ell_1, f(a), r_2)(\ell_2, g(b), r_3) = (\ell_1, h(ab), r_3).$$

Notice that here we used the fact that ab is defined in A'.

Therefore for every a, b in A we have

$$f(a)g(b) = h(ab).$$

From this, we can deduce that $f(1)g(a) = h(a) = f(a)g(1)$ for every $a \in A$. Therefore $f(a) = h(a)g(1)^{-1}$, $g(a) = f(1)^{-1}h(a)$ and $h(a)g(1)^{-1}f(1)^{-1}h(b) = h(ab)$. Thus

$$h(a)(g(1)^{-1}f(1)^{-1})h(b)(g(1)^{-1}f(1)^{-1}) = h(ab)(g(1)^{-1}f(1)^{-1}).$$

We can conclude that the mapping $\psi : A \to G$ which takes a to $h(a)(g(1)^{-1}f(1)^{-1})$ is a homomorphism of A. Since A is a partial group and ϕ is an embedding, ψ is also an embedding. Lemma 3 and Proposition 1 are proved.

It is easy to see that a semigroup S from $\mathcal{R}$ is embeddable into a Rees extension of a finite 0-simple ideal I by a nil-semigroup if and only if S is embeddable into I. Therefore we get the following result.

Lemma 4 *The problem whether a semigroup from $\mathcal{R}$ is embeddable into a Rees extension of a finite 0-simple semigroup by a nil-semigroup is undecidable.*

On every semigroup $S = (S, *)$ with 0 define a new operation $+$ by setting $x + x = x, x + y = 0$ for every $x \neq y$. Let $\hat{S}$ be the algebra $(S, *, +)$. It is easy to check that for every semigroup S with 0 the algebra $\hat{S}$ satisfies the identities 1, 2, 3 from Theorem 1, thus $\hat{S} \in \mathcal{V}$.

We shall need the following result.

Lemma 5 *If I is a 0-simple semigroup with 0 then $\hat{I}$ is a simple algebra.*

Proof. Indeed, let σ be a non-trivial congruence on $\hat{I}$. Let R be the class of σ containing 0. It is clear that R is an ideal of I. Since I is 0-simple, $R = 0$. Let $(a, b) \in \sigma$ and $a \neq b$. Then $(a + a, a + b) = (a, 0) \in \sigma$, so $a = 0$. Therefore every congruence class of $sigma$ is a singleton. Thus σ is the diagonal, a contradiction. The lemma is proved.

Now let S be a semigroup from $\mathcal{R}$. Suppose that $\hat{S}$ is embeddable into a finite simple algebra T from $\mathcal{V}$. By Lemma 1 $(T, *)$ is an extension of a 0-simple ideal I by a nil-semigroup. Hence S is embeddable into a nil-extension of a finite 0-simple semigroup.

Conversely, suppose that $S \in \mathcal{R}$ is embeddable into an extension of a finite 0-simple semigroup I by a nil-semigroup. Then, as we know, S is embeddable into I. Therefore $\hat{S}$ is embeddable into $\hat{I}$. By Lemma 5, $\bar{I}$ is a simple algebra, so $\bar{S}$ is embeddable into a finite simple algebra in $\mathcal{R}$.

Therefore the problem of whether a semigroup from $\mathcal{R}$ is embeddable into an extension of a finite 0-simple semigroup by a nil-semigroup, can be reduced to the problem of whether a finite algebra from $\mathcal{V}$ is embeddable into a finite simple algebra from $\mathcal{V}$. In order to complete the proof of Theorem 1, it remains to use Lemma 4. The theorem is proved.

Remark. Notice if S is a semigroup then the algebra $\bar{S}$ satisfies additional identities

4. $(x + y) + z = x + (y + z)$

5. $x + x = x$

This implies that in the variety given by identities $1 - 5$ the set of subalgebras of finite simple algebras is also not recursive. Both multiplication $*$ and addition $+$ in this variety are associative. The addition is commutative and idempotent.

Finally let us mention an open problem.

Problem 1 *Find a finitely based congruence distributive (modular) variety of algebras of finite type where the set of subalgebras of finite simple algebras is not recursive. Is there a locally finite variety with the same property?*

References

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

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

[3] T. Hall, S. Kublanovsky, S. Margolis, M. Sapir and P. Trotter. Decidable and undecidable problems related to finite 0-simple semigroups. , Journal of Pure and Applied Algebra, to appear.

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

[5] T. S. Weigel. Residual properties of free groups. III. Isr. J. Math. 77 (1992), 1–2, 65–81.

S. Kublanovsky
TPO Severnyj Ochag
Tarzhkovskaja, 5
St. Petersburg,
Russia, 197342 stas@north.spb.su

M. Sapir
Department of Mathematics and Statistics
Center for Communication and Information Science
University of Nebraska-Lincoln, Lincoln, Nebraska, USA, 68588
mvs@unlinfo.unl.edu