Simple surjective algebras having no proper subalgebras

Ágnes Szendrei

Abstract

We prove that every finite, simple, surjective algebra having no proper subalgebras is either quasiprimal or affine or isomorphic to an algebra term equivalent to a matrix power of a unary permutational algebra. Consequently, it generates a minimal variety if and only if it is quasiprimal. We show also that a locally finite, minimal variety omitting type **1** is minimal as a quasivariety if and only if it has a unique subdirectly irreducible algebra.

1. Introduction

This note was inspired by C. Bergman's and R. McKenzie's recent paper [1] whose main result is that every locally finite, minimal, congruence modular variety is minimal as a quasivariety. To this end the authors find all finite simple algebras without proper subalgebras, which generate a congruence distributive variety and have the property that the set of unary term operations forms a group. Here we extend this description in two aspects: we drop the requirement that the algebras generate a congruence distributive variety, and replace the assumption that the unary term operations form a group by the much weaker condition that the algebra is *surjective*, i.e. all fundamental operations are surjective. It turns out that besides quasiprimal algebras and affine algebras, the only algebras satisfying the assumptions are the matrix powers of some unary permutational algebras (Theorem 3.4). The proof makes essential use of an improved version of I. G. Rosenberg's primal algebra characterization theorem found in [16].

We present some applications of Theorem 3.4 as well: we specialize it to algebras with a single fundamental operation (Corollary 3.5), and find all strictly simple algebras in which unary term operations form a group, but there is no restriction on the generated variety (Corollary 3.10). Furthermore, we apply Theorem 3.4 to show that a finite, simple, surjective algebra having no proper subalgebras — in particular, a finite simple groupoid without proper subgroupoids — generates a minimal variety if and only if it is quasiprimal (Theorem 4.2, Corollary 4.3). Finally, Corollary 3.10 makes it possible to extend the main result of [1] as follows: A locally finite, minimal variety omitting type **1** is minimal as a quasivariety if and only if it has a unique subdirectly irreducible algebra (Theorem 4.4).

In Section 2 we also get some Słupecki-type results on matrix powers of unary algebras.

2. Reducts of matrix powers of unary algebras

We adopt the convention that algebras are denoted by boldface capitals and their universes by the corresponding letters in italics. We identify every natural number n with the set $n = \{0, \ldots, n-1\}$. For a set N, let T_N, S_N denote the full transformation monoid and the full symmetric group on N, respectively. We denote by id the identity mapping of each set. The cardinality of a set A is denoted by $|A|$. For an algebra $\mathbf{A}$ we denote by $\mathrm{Clo}\,\mathbf{A}$, $\mathrm{Clo}_1\,\mathbf{A}$, and $\mathrm{Clo}_{\mathrm{surj}}\,\mathbf{A}$ the clone of term operations, the set of unary term operations, and the set of surjective term operations of $\mathbf{A}$, respectively.

For the notion and the history of matrix powers of arbitrary algebras the reader is referred to [17]. Here we need the concept only for unary algebras. To recall the definition, let $\mathbf{C} = (C; F)$ be a unary algebra and let $m \geq 1$. For some mappings $\mu\colon m \to n$, $\sigma \in T_m$ and for $g_0, \ldots, g_{m-1} \in \mathrm{Clo}_1\,\mathbf{C}$ let us define an operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ on C^m as follows: for $x_i = (x_i^0, \ldots, x_i^{m-1}) \in C^m$ $(0 \leq i \leq n-1)$,

$$h_\mu^\sigma[g_0, \ldots, g_{m-1}](x_0, \ldots, x_{n-1}) = (g_0(x_{0\mu}^{0\sigma}), \ldots, g_{m-1}(x_{(m-1)\mu}^{(m-1)\sigma})).$$

The mappings μ and σ will be referred to as the *variable mapping* and *component mapping*, respectively. If $g_0 = \ldots = g_{m-1} = \mathrm{id}$, then we will write h_μ^σ instead of $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$. The *m-th matrix power* of $\mathbf{C}$, denoted $\mathbf{C}^{[m]}$, is the algebra with universe C^m and with all $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ as fundamental operations. It is easy to see that $\mathbf{C}^{[m]}$ has no other term operations than its fundamental operations; that is to say, $\mathrm{Clo}\,\mathbf{C}^{[m]}$ consists of all operations of the form $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ as above (cf. Corollary 2.5). Clearly, every term operation of $\mathbf{C}^{[m]}$ depends on at most m variables. $\mathrm{Clo}\,\mathbf{C}^{[m]}$ has a useful generating system, too (see [17]):

Claim 2.1. $\mathrm{Clo}\,\mathbf{C}^{[m]}$ *is generated by the m-ary operation* $h_{\mathrm{id}}^{\mathrm{id}}$ *(the so-called diagonal operation), the unary operation* $h_{m\to 1}^\gamma$ *with γ the cyclic permutation* $(0\ 1\ \ldots\ m-1)$, *and the fundamental operations of the m-th direct power of $\mathbf{C}$.*

Recall that a transformation monoid $G \subseteq T_N$ (in particular, a permutation group $G \subseteq S_N$) is called *transitive* if the unary algebra $(N; G)$ has no proper subalgebras. A permutation group $G \subseteq S_N$ is said to *act primitively* on N if $(N; G)$ is simple and $|G| > 1$ (if $|N| = 2$). Clearly, primitivity implies transitivity.

The main result of this section is the following theorem.

Theorem 2.2. *Let $\mathbf{A}$ be a simple surjective algebra such that $\mathbf{A}$ is isomorphic to a reduct of $(N; S_N)^{[m]}$ for some finite set N $(|N| \geq 2)$ and for some $m \geq 1$. If m is chosen minimal with respect to the existence of such an isomorphism, then $\mathbf{A}$ is isomorphic to an algebra term equivalent to $(N; G)^{[m]}$ for some permutation group G on N which acts primitively on N if $|N| > 2$.*

We introduce some notation. For a set A and for $\varphi \in T_A$ we denote by $\ker \varphi$ the kernel of φ. For $B \subseteq A^n$ and for $I = \{i_0, \ldots, i_{k-1}\} \subseteq n$, $i_0 < \ldots < i_{k-1}$, the projection of B onto its components in I is

$$\mathrm{pr}_I\, B = \{(x_{i_0}, \ldots, x_{i_{k-1}}) \colon (x_0, \ldots, x_{n-1}) \in B\}.$$

Throughout this section N is a fixed set, $|N| \geq 2$. Unless stated otherwise, N is not assumed to be finite. If $\mathbf{A} = (N^m; F)$ is a reduct of $(N; T_N)^{[m]}$, then $T_\mathbf{A}$ will denote the collection of all component mappings of unary term operations of $\mathbf{A}$, that is,

$$T_\mathbf{A} = \{\sigma \in T_m \colon h_{m\to 1}^\sigma[g_0, \ldots, g_{m-1}] \in \mathrm{Clo}_1\,\mathbf{A} \text{ for some } g_0, \ldots, g_{m-1}\}.$$

Clearly,

$$T_{\mathbf{A}} = \{\sigma \in T_m \colon h_\mu^\sigma[g_0, \ldots, g_{m-1}] \in \mathrm{Clo}\,\mathbf{A} \text{ for some } \mu \text{ and } g_0, \ldots, g_{m-1}\}.$$

Furthermore, we set

$$\varepsilon_{\mathbf{A}} = \bigcap (\ker \mu \colon h_\mu^\sigma[g_0, \ldots, g_{m-1}] \in \mathrm{Clo}_{\mathrm{surj}}\,\mathbf{A} \text{ for some } \sigma \text{ and } g_0, \ldots, g_{m-1}).$$

Lemma 2.3. (i)   If $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ is a surjective operation of $(N; T_N)^{[m]}$, then $g_0, \ldots, g_{m-1}$ are surjective.

(ii)   For finite N, every surjective reduct of $(N; T_N)^{[m]}$ is a reduct of $(N; S_N)^{[m]}$.

(iii)   An operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ of $(N; S_N)^{[m]}$ is surjective if and only if $\ker \mu \cap \ker \sigma$ is the equality relation.

Proof. The range of the operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ is

$$R = \{(g_0(x_{0\mu}^{0\sigma}), \ldots, g_{m-1}(x_{(m-1)\mu}^{(m-1)\sigma})) \colon x_i = (x_i^0, \ldots, x_i^{m-1}) \in N^m,\ 0 \le i \le n-1\}.$$

Thus (i), and hence also (ii) are obvious. To show (iii) let $g_0, \ldots, g_{m-1}$ be permutations. If there exist indices $i < j$ ($0 \le i, j \le m-1$) with $(i, j) \in \ker \mu \cap \ker \sigma$, that is with $i\mu = j\mu$ and $i\sigma = j\sigma$, then

$$\mathrm{pr}_{\{i,j\}}\, R = \{(g_i(x_{i\mu}^{i\sigma}), g_j(x_{j\mu}^{j\sigma})) \colon x_{i\mu}^{i\sigma} = x_{j\mu}^{j\sigma} \in N\} = \{(y, g_j g_i^{-1}(y)) \colon y \in N\},$$

hence $R \ne N^m$. Otherwise, $x_{0\mu}^{0\sigma}, \ldots, x_{(m-1)\mu}^{(m-1)\sigma} \in N$ can be selected independently, implying that $R = N^m$.

It is straightforward to check that the operations of $(N; T_N)^{[m]}$ are composed as follows:

Lemma 2.4. For an n-ary operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ and for k-ary operations $h_{\nu_l}^{\tau_l}[f_{0l}, \ldots, f_{m-1,l}]$ ($l = 0, \ldots, n-1$) of $(N; T_N)^{[m]}$ we have

$$h_\mu^\sigma[g_0, \ldots, g_{m-1}](h_{\nu_0}^{\tau_0}[f_{00}, \ldots, f_{m-1,0}](x_0, \ldots, x_{k-1}), \ldots$$
$$\ldots, h_{\nu_{n-1}}^{\tau_{n-1}}[f_{0,n-1}, \ldots, f_{m-1,n-1}](x_0, \ldots, x_{k-1}))$$

$$= h_\mu^\sigma[g_0, \ldots, g_{m-1}]((f_{00}(x_{0\nu_0}^{0\tau_0}), \ldots, f_{m-1,0}(x_{(m-1)\nu_0}^{(m-1)\tau_0})), \ldots$$
$$\ldots, (f_{0,n-1}(x_{0\nu_{n-1}}^{0\tau_{n-1}}), \ldots, f_{m-1,n-1}(x_{(m-1)\nu_{n-1}}^{(m-1)\tau_{n-1}})))$$

$$= (g_0 f_{0\sigma,0\mu}(x_{0\sigma\nu_{0\mu}}^{0\sigma\tau_{0\mu}}), \ldots, g_{m-1} f_{(m-1)\sigma,(m-1)\mu}(x_{(m-1)\sigma\nu_{(m-1)\mu}}^{(m-1)\sigma\tau_{(m-1)\mu}})).$$

Corollary 2.5. *For arbitrary submonoid G of T_N,*

$$\mathrm{Clo}\,(N;G)^{[m]} = \{h_\mu^\sigma[g_0, \ldots, g_{m-1}]: n \geq 1, \mu: m \to n, \sigma \in T_m, g_0, \ldots, g_{m-1} \in G\}.$$

Proof. The left hand side clearly contains the projections, and by the previous lemma it is closed under composition. Therefore, by the definition of $(N;G)^{[m]}$ the claim follows.

We start to investigate some reducts of $(N;T_N)^{[m]}$. Note that by Corollary 2.5 every term operation of a reduct $\mathbf{A}$ of $(N;T_N)^{[m]}$ is of the form $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ for some $n \geq 1$, $\mu: m \to n$, $\sigma \in T_m$, and $g_0, \ldots, g_{m-1} \in T_N$. Moreover, if $\mathbf{A}$ is a reduct of $(N;S_N)^{[m]}$, then for every term operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ we have also $g_0, \ldots, g_{m-1} \in S_N$.

Lemma 2.6. *Let $\mathbf{A}$ be a reduct of $(N;T_N)^{[m]}$.*
  (i)   *If $\mathbf{A}$ is surjective, then*

$$T_\mathbf{A} = \{\sigma \in T_m: h_\mu^\sigma[g_0, \ldots, g_{m-1}] \in \mathrm{Clo}_{\mathrm{surj}}\,\mathbf{A} \text{ for some } \mu \text{ and } g_0, \ldots, g_{m-1}\}.$$

  (ii)   *If $\mathbf{A}$ is simple, then $T_\mathbf{A}$ is a transitive submonoid of T_m.*

Proof. (i) Since the fundamental operations of $\mathbf{A}$ are surjective, it follows that every term operation of $\mathbf{A}$ arises from a surjective term operation by identification of variables. The identification of variables changes merely the variable mapping, which implies the equality.

(ii) We write T for $T_\mathbf{A}$. Applying composition for elements of $\mathrm{Clo}_1\,\mathbf{A}$ we see that T is closed under multiplication. Because of the projection in $\mathrm{Clo}_1\,\mathbf{A}$, T contains the identity mapping. Now let I be a subset of m that is closed under all transformations in T. Then the equivalence relation $\equiv$ on N^m defined by

$$x \equiv y \quad \text{if and only if} \quad \mathrm{pr}_I\, x = \mathrm{pr}_I\, y$$

is a congruence of $\mathbf{A}$. Since $\mathbf{A}$ is simple, we conclude that $I = \emptyset$ or $I = m$, proving the transitivity of T.

Lemma 2.7. *Let* $\mathbf{A}$ *be a reduct of* $(N; S_N)^{[m]}$ *such that* $\mathbf{A}$ *is surjective.*

(i) $\varepsilon_{\mathbf{A}}$ *is invariant under* $T_{\mathbf{A}}$, *that is,* $(i, j) \in \varepsilon_{\mathbf{A}}$ *implies* $(i\sigma, j\sigma) \in \varepsilon_{\mathbf{A}}$ *for all* $\sigma \in T_{\mathbf{A}}$.

(ii)   *If* $\varepsilon_{\mathbf{A}}$ *is the equality relation on* m, *then* $\mathbf{A}$ *has an* m-*ary term operation whose variable mapping is bijective (that is, it depends on all of its* m *variables).*

Proof. Let us write T, ε instead of $T_{\mathbf{A}}$, $\varepsilon_{\mathbf{A}}$, respectively.

(i) Assume $(i, j) \in \varepsilon$, and using Lemma 2.6 (i) select a surjective term operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ of $\mathbf{A}$ with component mapping σ. It suffices to show that $(i\sigma, j\sigma) \in \ker \nu$ for the variable mapping ν of each surjective term operation of $\mathbf{A}$. Consider the composition in Lemma 2.4 for $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ and for arbitrary operations $h_{\nu_l}^{\tau_l}[f_{0l}, \ldots, f_{m-1,l}] \in \mathrm{Clo}_{\mathrm{surj}}\, \mathbf{A}$ $(l = 0, \ldots, n-1)$ such that the variable mappings ν_l have pairwise disjoint ranges. (Replacing the variable mapping with another one of the same kernel is equivalent to renaming the variables.) Thus $\nu = \nu_{i\mu}(= \nu_{j\mu})$ runs over the variable mappings of all surjective term operations of $\mathbf{A}$. Furthermore, the disjointness condition ensures that the composition is surjective. In the variable mapping of the composition i and j are sent to $i\sigma\nu$ and $j\sigma\nu$, respectively. Since $(i, j) \in \varepsilon$, we have $i\sigma\nu = j\sigma\nu$, implying $(i\sigma, j\sigma) \in \ker \nu$, as required.

(ii) Let $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ be a surjective term operation of $\mathbf{A}$ such that $\ker \mu$ is minimal. We are done if we prove that $\ker \mu$ is the equality relation on m. Suppose this claim fails, and let $h_\nu^\tau[f_0, \ldots, f_{m-1}]$ be an arbitrary surjective term operation of $\mathbf{A}$. Consider the composition in Lemma 2.4 with $\tau_l = \tau$, $f_{il} = f_i$ for all $l = 0, \ldots, n-1$, $i = 0, \ldots, m-1$, and with $\nu_0, \ldots, \nu_{n-1}$ such that their ranges are pairwise disjoint and $\ker \nu_l = \ker \nu$ for all $l = 0, \ldots, n-1$. Thus the composition is surjective. By the choice of $\nu_0, \ldots, \nu_{n-1}$, for the variable mapping κ of the composition we have $\ker \kappa \leq \ker \mu$. Thus the minimality of $\ker \mu$ implies that $\ker \kappa = \ker \mu$. Consequently, for every block B of $\ker \mu$, κ is constant on B. Clearly, for $b \in B$, $b\kappa = b\sigma\nu_{r_B}$ where r_B is the unique element of $B\mu$. Therefore ν_{r_B}, and hence also ν, is constant on $B\sigma$. Since this holds for all variable mappings ν of surjective term operations of $\mathbf{A}$, we get that $B\sigma$ is contained in a block of

6

ε. However, $|B| = |B\sigma|$ for all blocks B of $\ker\mu$, as $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ is surjective, and therefore Lemma 2.3 implies that $\ker\mu \cap \ker\sigma$ is the equality relation. This contradicts the assumption that ε is the equality relation, completing the proof.

Lemma 2.8. *Let* $\mathbf{A}$ *be a reduct of* $(N; S_N)^{[m]}$ *such that* $\mathbf{A}$ *is surjective,* $T_\mathbf{A}$ *is transitive on* m *and* $\varepsilon_\mathbf{A}$ *is the equality relation on* m.

(i) *For every transformation* $\tau \in T_m$, $\mathbf{A}$ *has a term operation with component mapping* τ *and variable mapping* $\nu = \mathrm{id}$.

(ii) *If* N *is finite, then the diagonal operation* $h_{\mathrm{id}}^{\mathrm{id}}$ *is a term operation of* $\mathbf{A}$.

Proof. (i) By renaming the variables if necessary we get from Lemma 2.7 (ii) that $\mathbf{A}$ has a term operation of the form $h_{\mathrm{id}}^\sigma[g_0, \ldots, g_{m-1}]$ for some $\sigma \in T_m$ and $g_0, \ldots, g_{m-1} \in S_N$. Let us compose this operation with some essentially unary term operations $h_{m \to \{i\}}^{\tau_i}[f_{0i}, \ldots, f_{m-1,i}]$ of $\mathbf{A}$ such that $i\sigma\tau_i = i\tau$ $(i = 0, \ldots, n-1)$ (the transitivity of $T_\mathbf{A}$ ensures the existence of such τ_i). Then the variable mapping of the composition is the identity, while the component mapping is τ.

(ii) By (i) $\mathbf{A}$ has a term operation of the form $h_{\mathrm{id}}^{\mathrm{id}}[g_0, \ldots, g_{m-1}]$ for some $g_0, \ldots, g_{m-1} \in S_N$. Identifying its variables we get the unary term operation $h_{m \to 1}^{\mathrm{id}}[g_0, \ldots, g_{m-1}]$ of $\mathbf{A}$, which is a permutation on N^m. Since N is finite, for some natural number k, we have

$$h_{m \to 1}^{\mathrm{id}}[g_0^{-1}, \ldots, g_{m-1}^{-1}] = (h_{m \to 1}^{\mathrm{id}}[g_0, \ldots, g_{m-1}])^k \in \mathrm{Clo}_1\, \mathbf{A}.$$

Thus

$$h_{\mathrm{id}}^{\mathrm{id}}(x_0, \ldots, x_{m-1}) = h_{m \to 1}^{\mathrm{id}}[g_0^{-1}, \ldots, g_{m-1}^{-1}](h_{\mathrm{id}}^{\mathrm{id}}[g_0, \ldots, g_{m-1}](x_0, \ldots, x_{m-1})) \in \mathrm{Clo}\,\mathbf{A},$$

proving the claim.

The next lemma makes it possible to take an isomorphic copy of the representation of $\mathbf{A}$ as a reduct of $(N; S_N)^{[m]}$, in which the unary term operations are easier to handle.

Lemma 2.9. *Let* $\pi_0, \ldots, \pi_{m-1} \in S_N$, *and let* π *be the permutation of* N^m *defined by*

$$\pi\colon N^m \to N^m, \quad (x^0, \ldots, x^{m-1}) \mapsto (\pi_0(x^0), \ldots, \pi_{m-1}(x^{m-1})).$$

Then π is an isomorphism of arbitrary reduct $\mathbf{A}$ of $(N; S_N)^{[m]}$ onto another reduct of $(N; S_N)^{[m]}$ if we make correspond to each fundamental operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ of $\mathbf{A}$ the operation

$$h_\mu^\sigma[\pi_0 g_0 \pi_{0\sigma}^{-1}, \ldots, \pi_{m-1} g_{m-1} \pi_{(m-1)\sigma}^{-1}].$$

Proof. Indeed, for $x_0, \ldots, x_{n-1} \in N^m$ we have

$$h_\mu^\sigma[g_0, \ldots, g_{m-1}](x_0, \ldots, x_{n-1})\pi$$

$$= (\pi_0 g_0(x_{0\mu}^{0\sigma}), \ldots, \pi_{m-1} g_{m-1}(x_{(m-1)\mu}^{(m-1)\sigma}))$$

$$= (\pi_0 g_0 \pi_{0\sigma}^{-1}(\pi_{0\sigma}(x_{0\mu}^{0\sigma})), \ldots, \pi_{m-1} g_{m-1} \pi_{(m-1)\sigma}^{-1}(\pi_{(m-1)\sigma}(x_{(m-1)\mu}^{(m-1)\sigma})))$$

$$= h_\mu^\sigma[\pi_0 g_0 \pi_{0\sigma}^{-1}, \ldots, \pi_{m-1} g_{m-1} \pi_{(m-1)\sigma}^{-1}](x_0\pi, \ldots, x_{n-1}\pi).$$

As in Claim 2.1, γ will denote the cyclic permutation $(0\ 1\ \ldots\ m-1)$ on m.

Lemma 2.10. Let $\mathbf{A}$ be a reduct of $(N; T_N)^{[m]}$ such that $h_{\mathrm{id}}^{\mathrm{id}}$ and $h_{m \to 1}^\gamma$ are term operations of $\mathbf{A}$. Then

$$G_\mathbf{A} = \{g \in T_N \colon h_{m \to 1}^{\mathrm{id}}[g, \ldots, g] \in \mathrm{Clo}_1 \mathbf{A}\}$$

is a transformation monoid on N, and $\mathbf{A}$ is term equivalent to $(N; G_\mathbf{A})^{[m]}$.

Proof. Let us write G instead of $G_\mathbf{A}$. That G is a submonoid of T_N is immediate from the definition. Since $h_{\mathrm{id}}^{\mathrm{id}}, h_{m \to 1}^\gamma \in \mathrm{Clo}\,\mathbf{A}$, it follows from Claim 2.1 that $\mathrm{Clo}\,(N; G)^{[m]} \subseteq \mathrm{Clo}\,\mathbf{A}$. To prove the reverse inclusion let $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ be a term operation of $\mathbf{A}$, and let $i \in m$. It suffices to show that $g_i \in G$, that is, $h_{m \to 1}^{\mathrm{id}}[g_i, \ldots, g_i] \in \mathrm{Clo}_1 \mathbf{A}$. This can be verified as follows. For arbitrary natural numbers k, l, let us compute the unary term operation $(h_{m \to 1}^\gamma)^k h_{m \to 1}^\sigma[g_0, \ldots, g_{m-1}](h_{m \to 1}^\gamma)^l$ of $\mathbf{A}$ (addition in the subscripts and superscripts is understood modulo m):

$$(h_{m \to 1}^\gamma)^k h_{m \to 1}^\sigma[g_0, \ldots, g_{m-1}](h_{m \to 1}^\gamma)^l((x^0, \ldots, x^{m-1}))$$

$$= (h_{m \to 1}^{\gamma})^k h_{m \to 1}^{\sigma}[g_0, \ldots, g_{m-1}]((x^l, x^{l+1}, \ldots, x^{l+m-1}))$$

$$= (h_{m \to 1}^{\gamma})^k ((g_0(x^{l+0\sigma}), g_1(x^{l+1\sigma}), \ldots, g_{m-1}(x^{l+(m-1)\sigma})))$$

$$= (g_k(x^{l+k\sigma}), g_{k+1}(x^{l+(k+1)\sigma}), \ldots, g_{k+m-1}(x^{l+(k+m-1)\sigma})).$$

For every $j \in m$, choosing $k = i - j$ and $l = j - i\sigma$, we see that $\mathbf{A}$ has a unary term operation u_j with

$$u_j(x) = (\ldots, \overbrace{g_i(x^j)}^{j\text{th component}}, \ldots).$$

Thus

$$h_{m \to 1}^{\mathrm{id}}[g_i, \ldots, g_i](x) = h_{\mathrm{id}}^{\mathrm{id}}(u_0(x), \ldots, u_{m-1}(x))$$

is indeed a term operation of $\mathbf{A}$.

After these preparations we prove Theorem 2.2.

Proof of Theorem 2.2. We assume without loss of generality that $\mathbf{A} = (N^m; F)$ is a reduct of $(N; S_N)^{[m]}$. Recall that N is now finite. Let us write T, ε instead of $T_{\mathbf{A}}$, $\varepsilon_{\mathbf{A}}$, respectively. By Lemma 2.7 (i) ε is invariant under T.

First we show that ε is the equality relation on m. Let $I_0, \ldots, I_{s-1}$ be the blocks of ε, let us identify the set N^m with $N^{I_0} \times \ldots \times N^{I_{s-1}}$, and write its elements in the form $x = (x^0, \ldots, x^{m-1}) = (x^{I_0}, \ldots, x^{I_{s-1}})$ (i. e. $\mathrm{pr}_{I_j} x = x^{I_j}$). Consider a fundamental operation $h_{\mu}^{\sigma}[g_0, \ldots, g_{m-1}]$ of $\mathbf{A}$, say it is n-ary, and let $\bar{\sigma}: s \to s$, $\bar{\mu}: s \to n$ be the mappings defined by the following conditions: for $j \in s$, $I_j \mu = \{j\bar{\mu}\}$ and $I_j \sigma \subseteq I_{j\bar{\sigma}}$. Furthermore, for $j \in s$, let us consider the mappings

$$\bar{g}_j: N^{I_{j\bar{\sigma}}} \to N^{I_j}, \quad (y^l)_{l \in I_{j\bar{\sigma}}} \mapsto (g_l(y^{l\sigma}))_{l \in I_j}.$$

Then for arbitrary elements $x_0, \ldots, x_{n-1} \in N^m$ we have

$$h_{\mu}^{\sigma}[g_0, \ldots, g_{m-1}](x_0, \ldots, x_{n-1}) = (\bar{g}_0(x_{0\bar{\mu}}^{I_{0\bar{\sigma}}}), \ldots, \bar{g}_{s-1}(x_{(s-1)\bar{\mu}}^{I_{(s-1)\bar{\sigma}}})).$$

By surjectivity, all $\bar{g}_j$ are surjective, and hence $|I_j| \leq |I_{j\bar{\sigma}}|$ for all $j \in s$.

We show that $|I_0| = \ldots = |I_{s-1}|$. Let $J \subseteq s$ consist of all indices $j \in s$ for which $|I_j|$ is maximal. Let $\bar{T}$ denote the submonoid of T_s generated by the

mappings $\bar{\sigma}$ as σ runs over the component mappings of all fundamental operations of $\mathbf{A}$. Then, by the previous remark, J is closed under all transformations in $\bar{T}$. Hence the equivalence relation $\equiv$ on $N^{I_0} \times \ldots \times N^{I_{s-1}}$ defined by

$$x \equiv y \quad \text{if and only if} \quad x^{I_j} = y^{I_j} \quad \text{for all} \quad j \in J$$

is a congruence of $\mathbf{A}$. Since $\mathbf{A}$ is simple, we conclude that $J = s$, as required.

This yields a representation of $\mathbf{A}$ as a reduct of the matrix power $(N^{I_0}; S_{N^{I_0}})^{[s]}$. By the minimality of m we get $s = m$, whence $|I_0| = \ldots = |I_{s-1}| = 1$, that is ε is the equality relation.

Thus we get from Lemmas 2.6 (ii) and 2.8 that $h_{\text{id}}^{\text{id}}$ is a term operation of $\mathbf{A}$, and $\mathbf{A}$ has a term operation of the form $h_{\text{id}}^{\gamma}[g_0, \ldots, g_{m-1}]$ for some $g_0, \ldots, g_{m-1} \in S_N$. Now we apply Lemma 2.9 with $\pi_0 = \text{id}$ and $\pi_i = g_0 g_1 \ldots g_{i-1}$ for $i = 1, \ldots, m-1$. Then the operation corresponding to $h_{\text{id}}^{\gamma}[g_0, \ldots, g_{m-1}]$ is of the form $h_{\text{id}}^{\gamma}[\text{id}, \ldots, \text{id}, g]$ for some $g \in S_N$. It is easy to see that the diagonal operation corresponds to itself in this assignment. So we can assume that $\mathbf{A}$ is a reduct of $(N; S_N)^{[m]}$ such that the diagonal operation $h_{\text{id}}^{\text{id}}$ and $h_{\text{id}}^{\gamma}[\text{id}, \ldots, \text{id}, g]$ are term operations of $\mathbf{A}$.

We prove that h_{id}^{γ} is a term operation of $\mathbf{A}$, and hence so is $h_{m \to 1}^{\gamma}$. Indeed, identifying the variables of $h_{\text{id}}^{\gamma}[\text{id}, \ldots, \text{id}, g]$ we get that $q = h_{m \to 1}^{\gamma}[\text{id}, \ldots, \text{id}, g]$ is a unary term operation of $\mathbf{A}$. Clearly, $q^m = h_{m \to 1}^{\text{id}}[g, \ldots, g]$, so for some natural number k, $q^{mk} = h_{m \to 1}^{\text{id}}[g^{-1}, \ldots, g^{-1}]$. Thus

$$h_{\text{id}}^{\gamma}(x_0, \ldots, x_{m-1}) = h_{\text{id}}^{\gamma}[\text{id}, \ldots, \text{id}, g](x_0, \ldots, x_{m-2}, q^{mk}(x_{m-1}))$$

is a term operation of $\mathbf{A}$, as required.

Hence Lemma 2.10 applies to $\mathbf{A}$, yielding that $\mathbf{A}$ is term equivalent to $(N; G_{\mathbf{A}})^{[m]}$. Now $G_{\mathbf{A}}$ is a subgroup of S_N, as $\mathbf{A}$ is a reduct of $(N; S_N)^{[m]}$ and N is finite. Since $\text{Con}\, \mathbf{A} \cong \text{Con}\, (N; G_{\mathbf{A}})^{[m]} \cong \text{Con}\, (N; G_{\mathbf{A}})$ and $\mathbf{A}$ is simple, therefore $(N; G_{\mathbf{A}})$ is simple, so $G_{\mathbf{A}}$ acts primitively on N provided $|N| > 2$.

The proof of the theorem is complete.

We conclude this section with some Słupecki-type results which can be proved analogously to Theorem 2.2. They extend a theorem of B. Csákány [3]. I am indebted to L. Szabó for pointing out that the foregoing arguments can be applied in this direction.

Słupecki's theorem [12] and a strengthening of it due to A. A. Salomaa [11] states that for every finite set A with $|A| \geq 3$, the clone $\mathcal{C}$ of all operations on A satisfies the following conditions, respectively:

(Sł) the set of all unary operations in $\mathcal{C}$ together with any surjective operation in $\mathcal{C}$ depending on at least two of its variables forms a generating set for $\mathcal{C}$.

(Sa) the set of all permutations in $\mathcal{C}$ together with any surjective operation in $\mathcal{C}$ depending on at least two of its variables forms a generating set for $\mathcal{C}$.

It can be shown that the clones of matrix powers of unary permutational algebras have property (Sa), even if the base set is infinite.

Proposition 2.11. *Let N be a set and m an integer such that $|N| > 1$, $m > 1$. For arbitrary permutation group G on N, condition (Sa) is satisfied by the clone $\mathcal{C} = \mathrm{Clo}\,(N; G)^{[m]}$.*

Proof. Consider an arbitrary surjective operation f in $\mathcal{C}$ depending on at least two of its variables, and let $\mathbf{A}$ be the reduct of $(N; G)^{[m]}$ whose fundamental operations are f and all permutations in $\mathcal{C}$. Let us write T, ε instead of $T_{\mathbf{A}}$, $\varepsilon_{\mathbf{A}}$, respectively. Clearly, T is transitive; in fact, $S_m \subseteq T$. By construction $\mathbf{A}$ is surjective, therefore Lemma 2.7 (i) yields that ε is invariant under T. Furthermore, the operation f of $\mathbf{A}$ ensures that ε is not the full relation on m. Combining this with $S_m \subseteq T$ we conclude that ε is the equality relation on m.

A slight modification of the proof of Lemma 2.8 (ii) yields that the conclusion remains valid for $\mathbf{A}$ though at present N is not necessarily finite. This is because now $h^{\mathrm{id}}_{m \to 1}[g_0^{-1}, \ldots, g_{m-1}^{-1}] \in \mathrm{Clo}_1\,\mathbf{A}$ holds by the definition of $\mathbf{A}$. Thus $h^{\mathrm{id}}_{\mathrm{id}} \in \mathrm{Clo}\,\mathbf{A}$, and by assumption $h^{\gamma}_{m \to 1}$, $h^{\mathrm{id}}_{m \to 1}[g, \ldots, g]$ $(g \in G)$ are fundamental operations of $\mathbf{A}$. Hence Lemma 2.10 applies to $\mathbf{A}$ with $G_{\mathbf{A}} = G$, yielding $\mathrm{Clo}\,\mathbf{A} = \mathcal{C}$. This completes the proof.

The analogue of Słupecki's theorem holds for all matrix powers of finite unary algebras.

Corollary 2.12. *Let N be a finite set and m an integer such that $|N| > 1$, $m > 1$. For arbitrary transformation monoid U on N, condition (Sł) is satisfied by the clone $\mathcal{C} = \mathrm{Clo}\,(N; U)^{[m]}$.*

Proof. Consider an arbitrary surjective operation $f = h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ in $\mathcal{C}$ depending on at least two of its variables, and let $\mathcal{D}$ be the subclone of $\mathcal{C}$ generated by f and all unary operations in $\mathcal{C}$. The surjectivity of f implies that $g_0, \ldots, g_{m-1}$ are surjective. By the finiteness of N, it follows that $U \cap S_N$ is a permutation group on N and $g_0, \ldots, g_{m-1} \in U \cap S_N$. Thus by Proposition 2.11 the clone $\mathcal{C}_0 = \mathrm{Clo}\,(N; U \cap S_N)^{[m]}$ is generated by f and all permutations in $\mathcal{C}_0$. Hence $\mathcal{C}_0 \subseteq \mathcal{D}$, implying that $h_{\mathrm{id}}^{\mathrm{id}} \in \mathcal{D}$. By assumption $h_{m\to1}^\gamma$, $h_{m\to1}^{\mathrm{id}}[g, \ldots, g]$ $(g \in U)$ also belong to $\mathcal{D}$. Therefore Lemma 2.10 applies to the algebra $\mathbf{A} = (N^m; \mathcal{D})$, and we have $G_{\mathbf{A}} = U$, whence $\mathcal{D} = \mathrm{Clo}\,\mathbf{A} = \mathcal{C}$.

3. The main result

In this section we give a full description, up to term equivalence, for all finite, simple, surjective algebras having no proper subalgebras. Recall that a finite algebra $\mathbf{A}$ is called *quasiprimal* if every operation on A preserving the internal isomorphisms (i.e. isomorphisms between subalgebras) of $\mathbf{A}$ is a term operation of $\mathbf{A}$. The concept as well as the following characterization of quasiprimal algebras is due to A. F. Pixley [9], [10].

Claim 3.1. *A finite algebra $\mathbf{A}$ is quasiprimal if and only if the ternary discriminator*

$$t(a, b, c) = \begin{cases} c & \text{if } a = b \\ a & \text{otherwise} \end{cases} \quad (a, b, c \in A)$$

on A is a term operation of $\mathbf{A}$.

An algebra $\mathbf{A}$ is said to be *affine with respect to an Abelian group $\widehat{A}$* if $\mathbf{A}$ and $\widehat{A}$ have the same universe, $x - y + z$ is a term operation of $\mathbf{A}$, and

$$\{(a, b, c, d) \in A^4 \colon a - b + c = d\}$$

is a subuniverse of $\mathbf{A}^4$ (i.e., the fundamental operations of $\mathbf{A}$ commute with $x - y + z$). The algebras that are affine with respect to $\widehat{A}$ are well known to be related to the module $_{(\mathrm{End}\,\widehat{A})}\widehat{A}$ (i.e. $\widehat{A}$ considered as a module over its endomorphism ring $\mathrm{End}\,\widehat{A}$).

Claim 3.2. *Let* **A** *be an algebra and* $\widehat{A}$ *an Abelian group on its universe. The algebra* **A** *is affine with respect to* $\widehat{A}$ *if and only if* **A** *is polynomially equivalent to a module* $_R\widehat{A}$ *for some subring* R *of* End $\widehat{A}$.

In an earlier paper [16; Corollary 3.5] the following theorem was proved.

Theorem 3.3. [16]   *Let* **A** *be a finite, simple, surjective algebra having no proper subalgebras. Then one of the following conditions holds:*

(a)   **A** *is quasiprimal;*

(b)   **A** *is affine with respect to an elementary Abelian p-group (p prime);*

(c)   **A** *is isomorphic to a reduct of* $(N; S_N)^{[m]}$ *for a finite set* N $(|N| \geq 2)$ *and for some integer* $m \geq 1$.

If **A** satisfies condition (c), then Theorem 2.2 applies, and since **A** is assumed to have no proper subalgebras, the group G is primitive even if $|N| = 2$. Thus we get

Theorem 3.4. *Let* **A** *be a finite, simple, surjective algebra having no proper subalgebras. Then one of the following conditions holds:*

(a)   **A** *is quasiprimal;*

(b)   **A** *is affine with respect to an elementary Abelian p-group (p prime);*

(c)   **A** *is isomorphic to an algebra term equivalent to* $(N; G)^{[m]}$ *for some finite set* N $(|N| \geq 2)$*, some* $m \geq 1$*, and for some permutation group* G *on* N *which acts primitively on* N.

In the context of tame congruence theory, Theorem 3.4 can be restated as follows:

Let **A** *be a finite, simple, surjective algebra having no proper subalgebras. If* **A** *is of type* **1***, then* **A** *is isomorphic to an algebra term equivalent to* $(N; G)^{[m]}$ *for some primitive permutation group* G *on* N*; if* **A** *is of type* **2***, then* **A** *is affine, while if* **A** *is of type* **3***, then* **A** *is quasiprimal.* **A** *cannot be of type* **4** *or* **5***.*

Assume now that $\mathbf{A} = (A; f)$ is an algebra with a single fundamental operation. Clearly, if **A** has no proper subalgebras, then f must be surjective. Thus we can specialize Theorem 3.4 to algebras with a single fundamental operation.

Corollary 3.5. *Let* **A** *be a finite simple algebra with a single fundamental operation and with no proper subalgebras. Then one of the following conditions holds:*

(a)   **A** *is quasiprimal;*

(b)   **A** *is affine with respect to an elementary Abelian p-group (p prime);*

(c)   **A** *is isomorphic to an algebra term equivalent to* $(N; g)^{[m]}$ *for some set N of prime cardinality, some integer* $m \geq 1$, *and some cyclic permutation g of length* $|N|$ *on N.*

Proof. Apply Theorem 3.4. If (a) or (b) holds for **A**, then we have nothing to prove, so assume (c). Furthermore, assume without loss of generality that **A** is term equivalent to $(N; G)^{[m]}$, and let $f = h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ ($\mu\colon m \to n$, $\sigma \in T_m$, $g_0, \ldots, g_{m-1} \in G$) be the fundamental operation of **A**. The same argument as in the proof of Lemma 2.6 (ii) yields that no proper subset of m is closed under σ, and hence σ is a cyclic permutation of m. Rearranging the components we can assume that $\sigma = \gamma = (0 \; 1 \; \ldots \; m-1)$. Secondly, in the same way as in the proof of Theorem 2.2 when we applied Lemma 2.9, taking an isomorphic copy of **A** via an isomorphism π with $\pi_0 = \mathrm{id}$ and $\pi_i = g_0 \ldots g_{i-1}$ ($i = 1, \ldots, m-1$), we can assume that $f = h_\mu^\gamma[\mathrm{id}, \ldots, \mathrm{id}, g]$ for some $\mu\colon m \to n$ and $g \in G$. Observe that in both steps the clone of term operations of **A** remains equal to $\mathrm{Clo}\,(N; G)^{[m]}$. Hence G must be generated by the single permutation g. Thus the primitivity of G forces g to be a cycle and N to be of prime cardinality. This completes the proof.

We note that the description in Corollary 3.5 (c) of the simple algebras of type **1** having a single fundamental operation and no proper subalgebras is a special case of Theorem 4.8 in R. McKenzie's paper [7], which can be restated as follows.

Every tame algebra of type **1** *with a single fundamental operation which is not constant, is isomorphic to an algebra term equivalent to* $(N; g)^{[m]}$ *for some finite set N, some integer* $m \geq 1$, *and some permutation g on N.*

Problem 3.6. It would be interesting to have a common generalization of this result and the analogous description in Theorem 3.4 (c) of the simple surjective algebras of type **1** having no proper subalgebras.

In the next section we will need simple algebras without proper subalgebras in which unary term operations form a group. Obviously, if the unary term operations of some algebra $\mathbf{A}$ form a group, then $\mathbf{A}$ is surjective. Furthermore, for $m \geq 2$, the matrix powers $(N; G)^{[m]}$ with $|N| \geq 2$ and G an arbitrary permutation group on N possess unary term operations that are not permutations. Thus Theorem 3.4 immediately implies

Corollary 3.7. *Let* $\mathbf{A}$ *be a finite simple algebra having no proper subalgebras. If* $\mathrm{Clo}_1 \mathbf{A}$ *is a group, then one of the following conditions holds:*

(a) $\mathbf{A}$ *is quasiprimal;*

(b) $\mathbf{A}$ *is affine with respect to an elementary Abelian* p-*group* (p *prime);*

(c) $\mathbf{A}$ *is term equivalent to* $(A; G)$ *for some primitive permutation group* G *on* A.

Note that in case (c) of Theorem 3.4 and Corollaries 3.5, 3.7 it holds also that, conversely, all algebras appearing in the description satisfy the assumptions (up to term equivalence). Indeed, it is straightforward to check that the algebra $(N; G)^{[m]}$ with G a primitive permutation group on N is simple and has no proper subalgebras. By Claim 2.1 it is also term equivalent to a surjective algebra. Moreover, it is not hard to show (applying Claim 2.1 and adequate parts of the proofs of Corollary 3.5 and Theorem 2.2) that the algebras satisfying the stronger constraints of Corollary 3.5 (c) are also term equivalent to an algebra with a single fundamental operation.

Thus in case (c) Theorem 3.4 and Corollaries 3.5, 3.7, respectively, provide an explicit description, up to term equivalence, for the corresponding algebras. Using some known results an analogous description can be given in cases (a) and (b) as well.

Recall that a permutation group G on A is called *semiregular* if the identity permutation is the only member of G having fixed points, and *regular* if it is transitive and semiregular. An operation f is called *idempotent* if it satisfies the identity $f(x, \ldots, x) = x$, while an algebra is said to be *idempotent* if every fundamental operation (and hence every term operation) of the algebra is idempotent. For an algebra $\mathbf{A}$ we denote by $\mathrm{Clo}_{\mathrm{id}} \mathbf{A}$ the clone of idempotent term operations of $\mathbf{A}$.

Assume $\mathbf{A}$ satisfies the assumptions of Theorem 3.4. If $\mathbf{A}$ is quasiprimal, then

its term operations are exactly the operations preserving the automorphisms of **A** (as **A** has no proper subalgebras). Since the fixed points of each automorphism of **A** form a subalgebra, we conclude that Aut **A** is semiregular. For a permutation group G acting on A let $\mathcal{R}(G)$ denote the clone of all operations on A admitting all members of G as automorphisms. It is easy to see that if G is semiregular and not regular, then $\mathcal{R}(G)$ contains unary operations that are not permutations.

Combining all these facts we get

Claim 3.8. *If **A** is a surjective quasiprimal algebra without proper subalgebras [or, in particular, a quasiprimal algebra without proper subalgebras and with a single fundamental operation], then it is term equivalent to $(A; \mathcal{R}(G))$ for a semiregular permutation group G on A. Moreover if $\mathrm{Clo}_1 \mathbf{A}$ is a group, then **A** is term equivalent to $(A; \mathcal{R}(G))$ for a regular permutation group G on A.*

These descriptions are best possible. Indeed, it is not hard to show that for any semiregular permutation group G on A the algebra $(A; \mathcal{R}(G))$ is quasiprimal, has no proper subalgebras, and is term equivalent to an algebra with a single (surjective) fundamental operation. Furthermore, if G is regular, then its unary term operations are exactly the permutations commuting with all members of G, which form a regular permutation group on A.

The description of finite simple affine algebras appeared first in [2] (cf. [14; Chapter 2] for a direct proof): For every finite simple affine algebra **A** there exist a finite field K, a vector space $_K\widehat{A} = (A; +, K)$, and an endomorphism e of $_K\widehat{A}$ with $e^2 = e$ such that **A** is term equivalent to

$$(A;\ \mathrm{Clo}_{\mathrm{id}}\left(_{(\mathrm{End}\,_K \widehat{A})}\widehat{A}\right),\ e) \quad \text{or} \quad (A;\ \mathrm{Clo}_{\mathrm{id}}\left(_{(\mathrm{End}\,_K \widehat{A})}\widehat{A}\right),\ e,\ T(\widehat{A})).$$

Here $\mathrm{End}\,_K\widehat{A}$ stands for the endomorphism ring of $_K\widehat{A}$ and $T(\widehat{A})$ for the group $\{x + a :\ a \in A\}$ of translations of $\widehat{A}$. Clearly, if **A** has no proper subalgebras, then the first case cannot occur. If, in addition, **A** has a single fundamental operation, then it is easy to see that some nonidentity translation $x + b$ $(b \in A)$ is an automorphism of **A**, so the second case with $e = 0$ cannot occur either.

Thus we have

Claim 3.9. *If **A** is a simple, surjective, affine algebra without proper subalgebras [or, in particular, a simple affine algebra without proper subalgebras and with a single fundamental operation], then it is term equivalent to*

16

$(A;\ \text{Clo}_{\text{id}}\left(_{(\text{End}_K \widehat{A})}\widehat{A}\right), e,\ T(\widehat{A}))$ *for some vector space* $_K\widehat{A} = (A; +, K)$ *over a finite field* K *and some endomorphism* e *of* $_K\widehat{A}$ *with* $e^2 = e$ *[and* $e \neq 0$*]. Moreover if* $\text{Clo}_1 \mathbf{A}$ *is a group, then* $\mathbf{A}$ *is term equivalent to* $(A;\ \text{Clo}_{\text{id}}\left(_{(\text{End}_K \widehat{A})}\widehat{A}\right),\ T(\widehat{A}))$ *for some vector space* $_K\widehat{A} = (A; +, K)$ *over a finite field* K.

Again, these descriptions are best possible, as it is straightforward to check that all algebras $(A;\ \text{Clo}_{\text{id}}\left(_{(\text{End}_K \widehat{A})}\widehat{A}\right), e,\ T(\widehat{A}))$ above are simple, affine, have no proper subalgebras, and are term equivalent to a surjective algebra; moreover, if $e \neq 0$, then to an algebra with a single (surjective) fundamental operation. Furthermore, if e is missing (i.e. $e = \text{id}$), then $\text{Clo}_1 \mathbf{A} = T(\widehat{A})$.

Now we are in a position to give a full list of strictly simple algebras with unary term operations forming a group, thus improving Corollary 10 in [1]. Recall that an algebra is called *strictly simple* if it is simple and has no nontrivial (i.e. nonsingleton) proper subalgebras. Let $\mathbf{A}$ be a strictly simple algebra such that $\text{Clo}_1 \mathbf{A}$ is a group. As was noted in [1], either $\mathbf{A}$ is idempotent or $\mathbf{A}$ has no proper subalgebras. The latter case is settled above. In the first case Theorem 2.1 from [15] applies. For a permutation group G acting on A let $\mathcal{I}(G)$ denote the set of idempotent members of $\mathcal{R}(G)$. For $a \in A$ and for an integer $k \geq 2$ let $\mathcal{F}_k^a$ denote the clone of all operations f on A such that

$$X_k^a = \{(a_0, \ldots, a_{k-1}) \in A^k\colon a_i = a \text{ for at least one } i,\ 0 \leq i \leq k-1\}$$

is a subuniverse of $(A; f)^k$. Furthermore, we put $\mathcal{F}_\omega^a = \bigcap_{k=2}^\infty \mathcal{F}_k^a$. In case $|A| = 2$, we denote by $\mathcal{M}_{\text{id}}$ the clone of monotone, idempotent operations on A.

Summarizing, we have

Corollary 3.10. *Let* $\mathbf{A}$ *be a finite, strictly simple algebra such that* $\text{Clo}_1 \mathbf{A}$ *is a group. If* $\mathbf{A}$ *has no trivial subalgebras, then* $\mathbf{A}$ *is term equivalent to one of the following algebras:*

(a) $(A; \mathcal{R}(G))$ *for a regular permutation group* G *on* A;

(b) $(A;\ \text{Clo}_{\text{id}}\left(_{(\text{End}_K \widehat{A})}\widehat{A}\right),\ T(\widehat{A}))$ *for some vector space* $_K\widehat{A} = (A; +, K)$ *over a finite field* K;

(c) $(A; G)$ *for a primitive permutation group* G *on* A.

If $\mathbf{A}$ *has trivial subalgebras, then* $\mathbf{A}$ *is idempotent, and it is term equivalent to one of the following algebras:*

(a°) $(A; \mathcal{I}(G))$ for a permutation group G on A such that every nonidentity member of G has at most one fixed point;

(b°) $(A; \text{Clo}_{\text{id}} (_{(\text{End}_K \widehat{A})} \widehat{A}))$ for some vector space $_K \widehat{A} = (A; +, K)$ over a finite field K;

(x°) $(A; \mathcal{I}(G) \cap \mathcal{F}_k^0)$ for some k $(2 \leq k \leq \omega)$, some element $0 \in A$, and some permutation group G on A such that 0 is the unique fixed point of every nonidentity member of G;

(m°)   a reduct of $(A; \mathcal{M}_{\text{id}})$ provided $|A| = 2$.

It is easy to see that all algebras listed in Corollary 3.10 are in fact strictly simple and have the property that their unary term operations form a group. An interesting consequence of Corollary 3.10 is that very few permutation groups can occur as $\text{Clo}_1 \mathbf{A}$ for a strictly simple algebra $\mathbf{A}$. Namely,

(i)   the one-element group $\{\text{id}\}$ (for idempotent $\mathbf{A}$),

(ii)   regular permutation groups (for quasiprimal or affine $\mathbf{A}$),

(iii)   primitive permutation groups (for essentially unary $\mathbf{A}$).

Corollary 3.11. *If $\mathbf{A}$ is a finite simple algebra having no proper subalgebras such that $\text{Clo}_1 \mathbf{A}$ is a group, then $\text{Clo}_1 \mathbf{A}$ is either regular or primitive.*

Clearly, if $\text{Clo}_1 \mathbf{A}$ is a transitive permutation group on A, then $\mathbf{A}$ has no proper subalgebras. Thus the following result from [8] is also a consequence of Corollary 3.10.

Corollary 3.12. [8]   *If G is a nonregular transitive permutation group on A and $\mathbf{A}$ is a simple algebra with $G = \text{Clo}_1 \mathbf{A}$, then $\mathbf{A}$ is term equivalent to $(A; G)$.*

4. Minimal varieties

It is well known, and easy to see that every locally finite minimal variety is generated by a strictly simple algebra. It is an open problem, in general, which finite, strictly simple algebras generate minimal varieties. Making use of Theorem 3.4 we can determine all finite, simple, surjective algebras having no proper subalgebras, which generate minimal varieties.

Lemma 4.1. *If $m \geq 1$ and $\mathbf{C} = (C; G)$ is a unary algebra such that G is a permutation group on C, $|G| > 1$, then $\mathbf{C}^{[m]}$ does not generate a minimal variety.*

Proof. Consider $\mathbf{C}^{[m]}$ as an indexed algebra (recall that all operations $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ with $\sigma \in T_m$, $\mu \colon m \to n$, $g_0, \ldots, g_{m-1} \in G$ are fundamental operations of $\mathbf{C}^{[m]}$), and let $\mathbf{U}$ be the reduct of $(2; \mathrm{id})^{[m]}$ which is of the same type as $\mathbf{C}^{[m]}$, and for every fundamental operation $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ of $\mathbf{C}^{[m]}$, the corresponding operation of $\mathbf{U}$ is h_μ^σ. Clearly, $\mathbf{U}$ is term equivalent to $(2; \mathrm{id})^{[m]}$.

We show that $\mathbf{U}$ is a homomorphic image of $\mathbf{C}^{[m]} \times \mathbf{C}^{[m]}$. Let $\varphi \colon C^m \times C^m \to 2^m$ be the mapping defined as follows: for any $a = (a^0, \ldots, a^{m-1})$ and $b = (b^0, \ldots, b^{m-1})$ in C^m, $(a, b)\varphi$ is the m-tuple whose ith component is

$$((a, b)\varphi)^i = \begin{cases} 1, & \text{if } a^i = b^i \\ 0, & \text{otherwise} \end{cases} \quad \text{for all} \quad i \ (0 \leq i \leq m - 1).$$

Clearly, φ is surjective. Let $h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ ($\sigma \in T_m$, $\mu \colon m \to n$, $g_0, \ldots, g_{m-1} \in G$) be an arbitrary fundamental operation of $\mathbf{C}^{[m]}$, and $(a_0, b_0), \ldots, (a_{n-1}, b_{n-1})$ arbitrary elements in $C^m \times C^m$. For any $i \ (0 \leq i \leq m - 1)$, we have

$$(h_\mu^\sigma[g_0, \ldots, g_{m-1}]((a_0, b_0), \ldots, (a_{n-1}, b_{n-1}))\varphi)^i = 1$$

$$\Leftrightarrow \quad g_i(a_{i\mu}^{i\sigma}) = g_i(b_{i\mu}^{i\sigma}) \quad \Leftrightarrow \quad a_{i\mu}^{i\sigma} = b_{i\mu}^{i\sigma} \quad \Leftrightarrow \quad ((a_{i\mu}, b_{i\mu})\varphi)^{i\sigma} = 1 \quad \Leftrightarrow$$

$$(h_\mu^\sigma((a_0, b_0)\varphi, \ldots, (a_{n-1}, b_{n-1})\varphi))^i = 1,$$

implying that φ is a homomorphism.

Thus $\mathbf{U}$ is a nonsingleton algebra belonging to the variety generated by $\mathbf{C}^{[m]}$. Since $\mathbf{C}^{[m]}$ has distinct fundamental operations for which the corresponding operations of $\mathbf{U}$ coincide (e. g. $h_{m \to 1}^{\mathrm{id}}$ and $h_{m \to 1}^{\mathrm{id}}[g, \ldots, g]$, $g \in G$, $g \neq \mathrm{id}$), therefore $\mathbf{U}$ generates a proper subvariety of $\mathbf{C}^{[m]}$. The proof of Lemma 4.1 is complete.

Note that the claim and proof of Lemma 4.1 is analogous to the well-known situation for affine algebras: if $\mathbf{A}$ is a simple affine algebra having no proper subalgebras, then $\mathbf{A}$ does not generate a minimal variety, as $\mathbf{A}^2$ has a homomorphic image generating a nontrivial proper subvariety of the variety generated by $\mathbf{A}$ ([6], [13]). Among the algebras occurring in Theorem 3.4 there remain only the

quasiprimal algebras, which do generate minimal varieties by Jónsson's lemma [5]. Thus we get

Theorem 4.2. *A finite, simple, surjective algebra having no proper subalgebras generates a minimal variety if and only if it is quasiprimal.*

Corollary 4.3. *A finite simple algebra with a single fundamental operation and with no proper subalgebras generates a minimal variety if and only if it is quasiprimal.*

Recently C. Bergman and R. McKenzie [1] proved that every locally finite, minimal, congruence modular variety is minimal as a quasivariety. Now we apply Corollary 3.10 to prove an extension of this result. Both the statement and the proof require some notions from tame congruence theory, for which the reader is referred to [4].

Theorem 4.4. *A locally finite, minimal variety omitting type $\mathbf{1}$ is minimal as a quasivariety if and only if it has a unique subdirectly irreducible algebra.*

The proof goes along the same lines as the proof for the congruence distributive case in [1; Theorem 12], which is based on

Lemma 4.5. [1] *Let $\mathbf{A}$ be a finite, strictly simple algebra. The variety $V(\mathbf{A})$ generated by $\mathbf{A}$ is a minimal quasivariety if and only if $V(\mathbf{A}) = \mathrm{SP}(\mathbf{A})$ and $\mathbf{A}$ embeds into every nontrivial subalgebra of $\mathbf{A}^2$.*

The two facts making it possible to weaken "congruence distributivity" to "omitting type $\mathbf{1}$" are Corollary 3.10 and the following deep result from tame congruence theory.

Theorem 4.6. [4; Theorem 9.6] *For a locally finite variety V the following conditions are equivalent:*
  (i) *V omits type $\mathbf{1}$;*
  (ii) *V satisfies a nontrivial idempotent, linear Mal'tsev condition.*

Recall that a Mal'tsev condition is said to be *idempotent* if its identities imply the idempotent law $f(x, \ldots, x) = x$ for every term f occurring in it, and is called

linear, if terms are not substituted into one another on either side of each identity in the condition. A Mal'tsev condition is called *trivial* if it is satisfied in every variety.

Proof of Theorem 4.4. Let V be a locally finite, minimal variety omitting type **1**, and let **A** be a finite, strictly simple algebra in V (say, **A** is a nontrivial algebra of minimal cardinality in V). If V is minimal as a quasivariety, then we have $V = \mathrm{SP}(\mathbf{A})$ by Lemma 4.5, so **A** is the only subdirectly irreducible algebra in V. Conversely, assuming that **A** is the unique subdirectly irreducible algebra in V, we want to show that V is minimal as a quasivariety. By Lemma 4.5 it suffices to verify

Lemma 4.7. *For arbitrary finite, strictly simple algebra* **A** *in a variety omitting type* **1**, **A** *embeds into every nontrivial subalgebra of* $\mathbf{A}^2$.

Proof. The argument is a slight modification of the proof in [1; Theorem 12], so we give a brief sketch only.

Suppose the claim fails for some **A**, and let **A** be of minimal cardinality. That is to say, assume **A** is a strictly simple algebra such that

(i) the variety $V(\mathbf{A})$ generated by **A** omits type **1**,

(ii) there is a minimal subalgebra **R** of $\mathbf{A}^2$ such that **A** does not embed into **R**, and

(iii) for every strictly simple algebra **B** such that $|B| < |A|$ and $V(\mathbf{B})$ omits type **1**, **B** embeds into each nontrivial subalgebra of $\mathbf{B}^2$.

By Theorem 4.6 (i) is equivalent to requiring that there exists a nontrivial idempotent, linear Mal'tsev condition (M) satisfied in $V(\mathbf{A})$.

The first step of the proof is to show, using (ii), that **A** has no trivial subalgebras. For the details the reader is referred to [1].

Now if $\mathrm{Clo}_1 \mathbf{A}$ is a group, then we apply Corollary 3.10. Since no nontrivial idempotent, linear Mal'tsev condition can hold in a variety generated by a unary algebra, therefore condition (c) is excluded. Thus $\mathrm{Clo}_1 \mathbf{A}$ and $\mathrm{Aut}\,\mathbf{A}$ are regular permutation groups on A, and every minimal subalgebra of $\mathbf{A}^2$ is (the graph of) an automorphism of **A**. Hence every minimal subalgebra of $\mathbf{A}^2$ is isomorphic to **A**, contradicting (ii).

21

Therefore $\mathrm{Clo}_1\,\mathbf{A}$ is not a group, so $\mathbf{A}$ has a unary term operation g with $g^2 = g$ and $g(A) \neq A$. Let $B = g(A)$, $S = R \cap B^2$, and let $\mathbf{B}$ be the algebra with universe B whose operations are the restrictions $\tilde{f}|_B$ to B of all term operations $\tilde{f}(x_0, \ldots, x_{n-1}) = g(f(x_0, \ldots, x_{n-1}))$ $(n \geq 1)$ of $\mathbf{A}$. It was proved in [1] that $\mathbf{B}$ is strictly simple, S is a minimal subuniverse of $\mathbf{B}^2$, and $\mathbf{B} \ncong \mathbf{S}$. By (i), $\mathbf{A}$ has term operations $t_0, \ldots, t_k$ witnessing the satisfaction of the Mal'tsev condition (M) in $V(\mathbf{A})$. Then the operations $\tilde{t}_0|_B, \ldots, \tilde{t}_k|_B$ of $\mathbf{B}$ ensure the satisfaction of (M) in $V(\mathbf{B})$. The properties of $\mathbf{B}$ established so far contradict (iii). This completes the proof of the theorem.

The example $\mathbf{A} = (A; S_A)$ shows that the assumption on the type set of $V(\mathbf{A})$ cannot be omitted in Lemma 4.7.

When comparing Theorem 4.4 with the main result of [1] it is natural to ask what are the nonmodular minimal varieties omitting type $\mathbf{1}$ that are also minimal as quasivarieties. It can be shown that only some strictly simple algebras of type $\mathbf{5}$ can generate such varieties. This follows by combining one of the most striking results of tame congruence theory with a relatively easy fact (which is known to most of those working in the theory, though is not stated in [4]).

Theorem 4.8. [4; Theorem 10.4]   *Every residually small, locally finite variety omitting types $\mathbf{1}$ and $\mathbf{5}$ is congruence modular.*

Claim 4.9.   *Every type occurring in a variety occurs also as the type of the monolith of a finite subdirectly irreducible algebra in the variety.*

(The idea of the proof of Claim 4.9 is to show that for every finite algebra $\mathbf{A}$ and for every type $i \in \{\mathbf{1}, \ldots, \mathbf{5}\}$ occurring in the type set of $\mathbf{A}$, if $\alpha \prec \beta$ is a prime quotient of type i in the congruence lattice of $\mathbf{A}$ such that β is maximal with this property, then β is the unique upper cover of α, and hence $\mathbf{A}/\alpha$ is subdirectly irreducible with type i monolith.)

Thus we get

Corollary 4.10. *Let V be a locally finite, minimal variety which is minimal as a quasivariety. If the unique subdirectly irreducible algebra in V is of type $\mathbf{2}$, $\mathbf{3}$ or $\mathbf{4}$, then V is congruence modular.*

Acknowledgement. I am indebted to the referees for their useful comments on the original version of the paper.

References

[1] C. Bergman, R. McKenzie, Minimal varieties and quasivarieties, *J. Austral. Math. Soc.*, to appear.

[2] D. M. Clark, P. H. Krauss, Plain para primal algebras, *Algebra Universalis* **11** (1980), 365–388.

[3] B. Csákány, Completeness in coalgebras, *Acta Sci. Math. (Szeged)* **48** (1985), 75–84.

[4] D. Hobby, R. McKenzie, *The Structure of Finite Algebras (Tame Congruence Theory)*, Contemporary Mathematics, vol. 76, Amer. Math. Soc., Providence, R. I., 1988.

[5] B. Jónsson, Algebras whose congruence lattices are distributive, *Math. Scand.* **21** (1967), 110–121.

[6] R. McKenzie, On minimal, locally finite varieties with permuting congruence relations, Preprint, 1976.

[7] R. McKenzie, Finite forbidden lattices, in: *Universal Algebra and Lattice Theory* (Proc. Conf. Puebla, 1982), Lecture Notes in Math. 1004, Springer-Verlag, 1983; pp. 176–205.

[8] P. P. Pálfy, Á. Szendrei, Unary polynomials in algebras II, in: *Contributions to General Algebra* (Proc. Klagenfurt Conf., 1982), Verlag Hölder–Pichler–Tempsky, Wien, Verlag Teubner, Stuttgart, 1983; pp. 273–290.

[9] A. F. Pixley, Functionally complete algebras generating distributive and permutable classes, *Math. Z.* **114** (1970), 361–372.

[10] A. F. Pixley, The ternary discriminator function in universal algebra, *Math. Ann.* **191** (1971), 167–180.

[11] A. A. Salomaa, A theorem concerning the composition of functions of several variables ranging over a finite set, *J. Symbolic Logic* **25** (1960), 203–208.

[12] J. Słupecki, Completeness criterion for systems of many-valued propositional calculus, *C. R. des Séances de la Société des Sciences et des Lettres de Varsovie*

Cl. II **32** (1939), 102–109 (Polish); English translation: *Studia Logica* **30** (1972), 153–157.

[13] J. D. H. Smith, *Mal'cev Varieties,* Lecture Notes in Math. 554, Springer-Verlag, Berlin, 1976.

[14] Á. Szendrei, *Clones in Universal Algebra,* Séminaire de Mathématiques Supérieures, vol. 99, Les Presses de l'Université de Montréal, Montréal, 1986.

[15] Á. Szendrei, Idempotent algebras with restrictions on subalgebras, *Acta Sci. Math. (Szeged)* **51** (1987), 251–268.

[16] Á. Szendrei, The primal algebra characterization theorem revisited, *Algebra Universalis*, submitted.

[17] W. Taylor, The fine spectrum of a variety, *Algebra Universalis* **5** (1975), 262–303.

Bolyai Institute
Aradi vértanúk tere 1
6720 Szeged, Hungary