A classification of strictly simple algebras with trivial subalgebras

Ágnes Szendrei

An algebra $\mathbf{A}$ is called *strictly simple* if $\mathbf{A}$ is simple and every proper subalgebra of $\mathbf{A}$ is trivial (i.e. one-element). Since each locally finite minimal variety is generated by a finite strictly simple algebra, it is hoped that they will be better understood by studying the structure of strictly simple algebras (cf. Problem 10 in [3]). In [16] and [17] we investigated finite simple algebras without proper subalgebras, and determined them, up to term equivalence, when all fundamental operations are surjective. The proof is based on a strong version of Rosenberg's primal algebra characterization theorem [10].

This paper starts the study of finite strictly simple algebras having trivial subalgebras with the analogue of the main result of [16]. We present a classification determining the maximal clones of all those finite strictly simple algebras with trivial subalgebras which do not generate a congruence permutable variety (Theorem 1; cf. also Corollary 2). The proof does not make use of (major parts of) the proof of Rosenberg's theorem. In fact, it is much simpler than the latter, which is shown also by the fact that, with some modifications, the proof given here works for infinite algebras (and local term operations replacing term operations) as well, provided they have at least two trivial subalgebras.

As a consequence of Theorem 1, we get for every finite set A and for every nonvoid subset U of A the full list of maximal subclones of the clone consisting of

This paper, though based partly on earlier results, was written while the author was a Humboldt fellow at the FB Mathematik, AG 1, Technische Hochschule Darmstadt. The excellent circumstances provided by the fellowship and by the THD are gratefully acknowledged. This research is partially supported also by Hungarian National Foundation for Scientific Research grant no. 1813.

all operations f on A with $f(u, \ldots, u) = u$ for all $u \in U$ (Corollary 2). We note that the special case $|U| = 1$ was proved earlier by D. Lau [5], and the case $U = A$ was also known before (see [15]). Further, we apply Theorem 1 to get a necessary and sufficient condition for a finite strictly simple algebra $\mathbf{A}$ having at least one trivial subalgebra and such that the fundamental operations of $\mathbf{A}$ are surjective to generate a congruence permutable variety (Corollary 3), and for a functionally complete algebra $\mathbf{A}$ with at least one trivial subalgebra to be quasiprimal (Corollary 6). It turns out that in both cases the condition involves only subalgebras of $\mathbf{A}^2$.

1. Main results

We adopt the convention that algebras are denoted by boldface capitals and their universes by the corresponding letters in italics. Two algebras are called *term equivalent* [*polynomially equivalent*], if they have the same clone of term [polynomial] operations. The clone of term operations of an algebra $\mathbf{A}$ is denoted by $\operatorname{Clo} \mathbf{A}$. For a set A and for $k \geq 1$, the nonvoid subsets of A^k will also be called *k-ary relations* (on A), and for an algebra $\mathbf{A}$ the universes of subalgebras of $\mathbf{A}$ will be called *subuniverses* of $\mathbf{A}$. (Hence a subuniverse is always nonempty.)

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 [7], [8].

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

$$t(x, y, z) = \begin{cases} z & \text{if } x = y, \\ x & \text{otherwise} \end{cases}$$

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, the quaternary relation

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

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

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

A k-ary relation B on A is called *totally reflexive* if it contains each k-tuple from A^k whose components are not pairwise distinct. Further, B is called *totally symmetric* if it is closed under permuting the components. (As a rule, "totally" is omitted if $k = 2$.) A totally reflexive, totally symmetric relation $B \subseteq A^k$ is called *central* if $B \neq A^k$ and there exists a $c \in A$ such that $(c, a_1, \ldots, a_{k-1}) \in B$ for all $a_1, \ldots, a_{k-1} \in A$. The set of all such elements c is called the *centre* of B. Observe that every unary relation is totally reflexive and symmetric, hence the unary central relations are exactly the nonvoid proper subsets of A. For a fixed subset U of A, a central relation will be called *U-central* if U is contained in its centre.

For an element $a \in A$ we set

$$X_a = (A \times \{a\}) \cup (\{a\} \times A).$$

As usual, a binary relation on A is called *irreflexive*, if none of the pairs (a, a), $a \in A$, belongs to it. For a fixed subset U of A, the binary relations of the form

$$X_u \cup Y \quad \text{with } u \in U \text{ and } Y \text{ an irreflexive binary relation on } A - U$$

will be called *U-crosses* on A.

The principal result of the paper is the following theorem.

THEOREM 1. *Let* $\mathbf{A}$ *be a finite strictly simple algebra having at least one trivial subalgebra, and let* U *be the set of all elements* u *of* $\mathbf{A}$ *for which* $\{u\}$ *is a trivial subalgebra of* $\mathbf{A}$. *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) *there is a* U*-central relation among the subuniverses of* $\mathbf{A}^k$ *for some* $k \geq 2$*;*

(d) *there is a bounded partial order among the subuniverses of* $\mathbf{A}^2$ *such that every element of* U *is a bound (consequently* $|U| \leq 2$*);*

(e) *there is a symmetric* U*-cross among the subuniverses of* $\mathbf{A}^2$.

We present some applications.

(A) Theorem 1 can be used to determine the maximal subclones of the clone $\mathcal{C}_U$ consisting of all operations f on A with $f(u, \ldots, u) = u$ for all $u \in U$. For a k-ary relation B and an operation f on A, f is said to *preserve* B if B is a subuniverse of the algebra $(A; f)^k$. The operations preserving a fixed relation B form a clone, which will be denoted by $\mathcal{P}_B$.

COROLLARY 2. *Let A be a finite set and U a nonvoid subset of A. The maximal subclones of $\mathcal{C}_U$ are exactly the clones $\mathcal{C}_U \cap \mathcal{P}_B$ where B is one of the following relations.*

(I) *B is a nonempty proper subset of A distinct from the singletons $\{u\}$, $u \in U$;*

(II) *B is a nontrivial equivalence relation on A such that $\{u\}$ is a singleton block of B for all $u \in U$;*

(III) *B is a permutation of A of prime order such that U is invariant under B, B has at most one fixed point in U and no fixed point in $A - U$;*

(IV) *$B = \{(a, b, a + b)\colon\ a, b \in A\}$ for an elementary Abelian 2-group $\widehat{A} = (A; +, 0)$, and $U = \{0\}$;*

(V) *B is a k-ary U-central relation ($k \geq 2$);*

(VI) *B is a bounded partial order such that every element of U is a bound (consequently $|U| \leq 2$);*

(VII) *B is a symmetric U-cross.*

The case $|U| = 1$ was proved earlier by D. Lau [5], while the case $U = A$ (when $\mathcal{C}_U = \mathcal{C}_A$ is the clone of all idempotent operations on A) was solved independently by several participants of the Séminaire de Mathématiques Supérieures on "Universal algebra and relations" (Montreal, 1984), among others R. W. Quackenbush and the author. In [15] the result is derived from a more general theorem on idempotent algebras. An interesting feature of this proof is that it works for infinite base sets as well, thus yielding a description for the so-called maximal locally closed subclones of $\mathcal{C}_A$. Keeping this in mind, we give a proof for Theorem 1 (and hence for Corollary 2) which can be modified with some effort to yield the infinite analogues as well, provided $|U| \geq 2$ (see the Rermark at the end of Section 2).

(B) We call an algebra *surjective* if all its fundamental operations are surjective. For example, every strictly simple groupoid (or, more generally, every strictly simple algebra with a single fundamental operation) is surjective, unless its operation is constant.

COROLLARY 3. *Let $\mathbf{A}$ be a finite, surjective, strictly simple algebra having at least one trivial subalgebra, and let U be the set of all elements u of $\mathbf{A}$ for which*

$\{u\}$ *is a trivial subalgebra of* $\mathbf{A}$. *Then* $\mathbf{A}$ *generates a congruence permutable variety if and only if none of the following relations* B *occurs among the subuniverses of* $\mathbf{A}^2$*:*

(α) B *is a* U*-cross;*

(β) B *is a binary* U*-central relation with centre* U, $|U| = 1$*;*

(γ) B *is a bounded partial order such that* U *is the 2-element set consisting of the bounds.*

This shows that for an algebra $\mathbf{A}$ satisfying the assumptions of Corollary 3, $\mathbf{A}$ generates a congruence permutable variety if and only if $\mathbf{A}^2$ has no subuniverse B with $|A| < |B| < |A|^2$. We note that none of the relations (α)–(γ) can be omitted in Corollary 3, as is shown by the following proposition.

PROPOSITION 4. *Let* $\mathbf{A}$ *be a finite set and* U *a nonvoid subset of* A. *For each of the binary relations* B *in* (α)–(γ)*, there exists an algebra* $\mathbf{A}$ *of finite type such that*

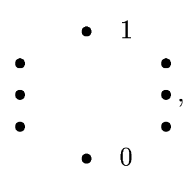
(i) $\mathbf{A}$ *is strictly simple and the trivial subalgebras of* $\mathbf{A}$ *are exactly the singletons* $\{u\}$, $u \in U$*;*

(ii) $\mathbf{A}$ *is surjective; and*

(iii) Δ *and* B *(and in case* (γ) *also* B^{-1}*) are the only subuniverses of* $\mathbf{A}^2$ *that are not direct products of subuniverses of* $\mathbf{A}$.

REMARKS. 1. If B is of type (α) or (β), then the algebra $\mathbf{A}$ satisfying the requirements of Proposition 4 can be chosen to be term equivalent to $(A; \mathcal{C}_U \cap \mathcal{P}_B)$.

2. If B is of type (γ), then the analogous claim is not true in general. In fact, if $|A| = 8$ and B is the partial order



then G. Tardos's proof [18] for the fact that $\mathcal{P}_B$ is not finitely generated yields also that $\mathcal{C}_{\{0,1\}} \cap \mathcal{P}_B$ is not finitely generated; hence $(A; \mathcal{C}_U \cap \mathcal{P}_B)$ is not term equivalent to any algebra of finite type.

(C) Recall that an algebra $\mathbf{A}$ is said to be *functionally complete* if it is finite and every operation on A is a polynomial operation of $\mathbf{A}$. Recently K. Kaarli [4] proved that every functionally complete algebra having no proper subalgebras is quasiprimal. If the algebra has trivial subalgebras, then the conclusion is no longer true; namely we have the following

PROPOSITION 5. *Let* $\mathbf{A}$ *be a finite set and* U *a nonvoid subset of* A. *For arbitrary* U*-cross* B *on* A, $\mathbf{A} = (A; \mathcal{C}_U \cap \mathcal{P}_B)$ *is a functionally complete algebra whose subalgebras are exactly the singletons* $\{u\}$, $u \in U$, *and* $\mathbf{A}$ *is not quasiprimal.*

It follows from Theorem 1 that every nonquasiprimal, functionally complete algebra having trivial subalgebras is a reduct of these algebras.

COROLLARY 6. *Let* $\mathbf{A}$ *be a functionally complete algebra having no nontrivial proper subalgebras. Assume* $\mathbf{A}$ *has a trivial subalgebra, and let* U *be the set of all elements* u *of* $\mathbf{A}$ *for which* $\{u\}$ *is a trivial subalgebra of* $\mathbf{A}$. *Then* $\mathbf{A}$ *is quasiprimal if and only if there is no symmetric* U*-cross among the subuniverses of* $\mathbf{A}^2$.

In a forthcoming paper we will apply Theorem 1 for the investigation of strictly simple Abelian algebras (i.e. strictly simple algebras satisfying the Term Condition).

2. Proof of Theorem 1

The cardinality of a set A is denoted by $|A|$. For convenience we identify every natural number n with the set $n = \{0, \ldots, n-1\}$. The full symmetric group on n is denoted by S_n.

We introduce some operators on relations that will be needed in the sequel. For $B \subseteq A^n$ and for $i_0, \ldots, i_{k-1} \in n$,

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

is the projection of B onto its components $i_0, \ldots, i_{k-1}$. In particular, if $I = \{i_0, \ldots, i_{k-1}\}$ is a subset of n with $i_0 < \ldots < i_{k-1}$, then we write $\mathrm{pr}_I B$ instead of $\mathrm{pr}_{(i_0,\ldots,i_{k-1})} B$. Furthermore, for any $\pi \in S_n$, we set $B^\pi = \mathrm{pr}_{(0\pi,\ldots,(n-1)\pi)} B$, i.e. B^π arises from B by permuting its components according to π. In particular, if $n = 2$ and π is the transposition, then we write B^{-1} instead of B^π.

For $B \subseteq A^n$ and for an equivalence relation ε on n, we set

$$B_\varepsilon = \{(x_0, \ldots, x_{n-1}) \in B \colon\ x_i = x_j \text{ whenever } (i,j) \in \varepsilon\}.$$

Let I_ε denote the subset of n consisting of the least elements of the blocks of ε, and put

$$\mathrm{eq}_\varepsilon B = \mathrm{pr}_{I_\varepsilon} B_\varepsilon.$$

In the subscript, instead of ε, it will often be more convenient to write the list of nonsingleton blocks of ε; e.g.

$$\mathrm{eq}_{01} B = \{(x_0, x_1 \dots, x_{n-2}) \in A^{n-1}\colon\ (x_0, x_0, x_1 \dots, x_{n-2}) \in B\}.$$

For $B \subseteq A^n$, $1 \le l < n$, and $a_l, \dots, a_{n-1} \in A$, we define the l-ary relation arising from B by 'fixing the jth component at a_j for $j = l, \dots, n-1$' as follows:

$$B(x_0, \dots, x_{l-1}, a_l, \dots, a_{n-1})$$

$$= \{(x_0, \dots, x_{l-1}) \in A^l\colon\ (x_0, \dots, x_{l-1}, a_l, \dots, a_{n-1}) \in B\}.$$

It is straightforward to check that if for some algebra $\mathbf{A}$, B is a subuniverse of $\mathbf{A}^n$, then the relations $\mathrm{pr}_I B$, B_ε, $\mathrm{eq}_\varepsilon B$ described above are also subuniverses of the corresponding powers of $\mathbf{A}$, provided they are nonempty. If, in addition, $\{a_j\}$ $(l \le j \le n-1)$ are singleton subalgebras of $\mathbf{A}$, then $B(x_0, \dots, x_{l-1}, a_l, \dots, a_{n-1})$ is a subuniverse of $\mathbf{A}^l$, provided it is nonempty.

With the foregoing notations, an n-ary relation B on A is totally reflexive if and only if $\mathrm{eq}_{ij} B = A^{n-1}$ for all $i, j \in m$, $i < j$, and totally symmetric if and only if $B^\pi \subseteq B$ for all $\pi \in S_n$. An n-ary relation B will be called *reflexive* if $\mathrm{eq}_{0\dots n-1} B = A$. It will be convenient to consider the permutations σ of A as binary relations $\{(x, x\sigma)\colon\ x \in A\}$, and conversely, to call every relation of this form a permutation. The identity permutation, considered as a binary relation (i.e. the diagonal of A^2) will be denoted by Δ.

In what follows, we will need a concept generalizing the automorphisms of algebras. Before the definition we prove a lemma.

LEMMA 7. *Let A be a finite set. For a k-ary relation C on A $(k \ge 2)$, the following conditions are equivalent:*

(i) $|C| = |A|^{k-1}$, *and* $\mathrm{pr}_{k-\{i\}} C = A^{k-1}$ *for all* $i \in k$;

(ii) *for all $i \in k$, the projection mapping of C omitting the ith component is one-to-one and onto A^{k-1};*

(iii) *for every $j \in k$ there exists a $(k-1)$-ary operation Γ_C^j on A such that*

(1) $$C = \{(x_0, \dots, x_{j-1}, \Gamma_C^j(x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_{k-1}), x_{j+1}, \dots, x_{k-1})\colon$$
$$(x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_{k-1}) \in A^{k-1}\},$$

(2) $\Gamma_C^j(a_0, \dots, a_{i-1}, x, a_{i+1}, \dots, a_{j-1}, a_{j+1}, \dots, a_{k-1})$ *is a permutation of A for all $i \in k$, $i \ne j$, and for all elements $a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_{j-1}, a_{j+1}, \dots, a_{k-1} \in A$, and*

(3) *the identities*

$$\Gamma_C^i(x_0,\dots,x_{i-1},x_{i+1},\dots,x_{j-1},\Gamma_C^j(x_0,\dots,x_{i-1},x_i,x_{i+1},\dots,x_{j-1},$$

$$x_{j+1},\dots,x_{k-1}),x_{j+1},\dots,x_{k-1}) = x_i$$

hold for arbitrary distinct indices $i,j \in k$.

PROOF. The equivalence (i)⇔(ii) and the implication (iii)⇒(ii) are obvious, so assume (ii) holds for C. By symmetry it suffices to prove (1), (2) for $j = k-1$. Since the projection mapping $C \to \mathrm{pr}_{k-1} C = A^{k-1}$ is bijective, there is a uniquely determined operation Γ_C^{k-1} satisfying (1) (for $j = k-1$). Also, for arbitrary index $i \in (k-1)$ and for arbitrary fixed elements $a_0,\dots,a_{i-1},a_{i+1},\dots,a_{k-2} \in A$ the mapping

$$C(a_0,\dots,a_{i-1},x,a_{i+1},\dots,a_{k-2},y) \to A, \quad (x,y) \mapsto y$$

is bijective. Here

$$C(a_0,\dots,a_{i-1},x,a_{i+1},\dots,a_{k-2},y)$$

$$= \{(x,\Gamma_C^{k-1}(a_0,\dots,a_{i-1},x,a_{i+1},\dots,a_{k-2}))\colon\ x \in A\},$$

implying that the unary operation $\Gamma_C^{k-1}(a_0,\dots,a_{i-1},x,a_{i+1},\dots,a_{k-2})$ is a permutation of A. This proves (2).

To show (3) let, say, $i < j$, and consider the permutations

$$\pi(x) = \Gamma_C^i(a_0,\dots,a_{i-1},a_{i+1},\dots,a_{j-1},x,a_{j+1},\dots,a_{k-1}),$$

$$\sigma(x) = \Gamma_C^j(a_0,\dots,a_{i-1},y,a_{i+1},\dots,a_{j-1},a_{j+1},\dots,a_{k-1}).$$

Clearly,

$$C(a_0,\dots,a_{i-1},y,a_{i+1},\dots,a_{j-1},x,a_{j+1},\dots,a_{k-1})$$

$$= \{(\pi(x),x)\colon\ x \in A\} = \{(y,\sigma(y))\colon\ y \in A\}.$$

Thus π and σ are inverses of each other, proving the equality in (3) for

$$(x_0,\dots,x_{i-1},x_{i+1},\dots,x_{j-1},x_{j+1},\dots,x_{k-1})$$

$$= (a_0,\dots,a_{i-1},a_{i+1},\dots,a_{j-1},a_{j+1},\dots,a_{k-1}).$$

The latter is an arbitrary $(k-2)$-tuple, hence (3) follows.

DEFINITION. Let $\mathbf{A}$ be a finite algebra. For $k \geq 2$ a *k-automorphism* (or, if k is clear from the context, a *multi-automorphism*) of $\mathbf{A}$ is a subuniverse C of $\mathbf{A}^k$ satisfying the equivalent conditions of Lemma 7.

Note that the 2-automorphisms of $\mathbf{A}$ are just the automorphisms of $\mathbf{A}$. Further, the quaternary relation $Q_{\widehat{A}}$ occurring in the definition of an affine algebra $\mathbf{A}$ is a 4-automorphism of $\mathbf{A}$.

LEMMA 8. *Let B be a subuniverse of $\mathbf{A}^m$. If $\mathrm{pr}_I B$ is a multi-automorphism of $\mathbf{A}$ for some $I \subseteq m$, $|I| \geq 2$, then there exists $i \in m$ such that $|B| = |\mathrm{pr}_{m-\{i\}} B|$.*

PROOF. For simplicity, assume $I = k$, $2 \leq k \leq m$. Then

$$B \to \mathrm{pr}_{m-\{0\}} B, \quad (x_0, x_1, \ldots, x_{k-1}, x_k, \ldots, x_{m-1}) \mapsto (x_1, \ldots, x_{k-1}, x_k, \ldots, x_{m-1})$$

is bijective, since the component x_0 of B is uniquely determined by $x_1, \ldots, x_{k-1}$.

LEMMA 9. *Let $\mathbf{A}$ be a finite algebra, and let $m \geq 2$. Assume that every subuniverse of $\mathbf{A}^{m-1}$ has cardinality a power of $|A|$. If B is a subuniverse of $\mathbf{A}^m$ whose cardinality is not a power of $|A|$, then*

$$\mathrm{pr}_{m-\{i\}} B = A^{m-1} \text{ for all } i \in m. \tag{4}$$

PROOF. Note first that for every $l < m$, every subuniverse C of $\mathbf{A}^l$ has cardinality a power of $|A|$, since $A^{m-l-1} \times C$ is a subuniverse of $\mathbf{A}^{m-1}$ and its cardinality $|A|^{m-l-1}|C|$ is a power of $|A|$. In particular, the only subuniverses of $\mathbf{A}$ are A and singletons (if any).

We prove that $\mathrm{pr}_I B = A^{|I|}$ for all proper subsets I of m. First let, say, $I = \{i\}$. If $\mathrm{pr}_{\{i\}} B$ is distinct from A, then it is a singleton, implying that

$$B = (\mathrm{pr}_{\{i\}} B) \times (\mathrm{pr}_{m-\{i\}} B).$$

By assumption both factors have cardinality a power of $|A|$, hence so is B, a contradiction. Thus $\mathrm{pr}_{\{i\}} B = A$ for all $i \in m$.

Suppose our claim is false and let, say, k be a minimal proper subset of m such that $\mathrm{pr}_k B \neq A^k$. By the foregoing observation we have $k \geq 2$. So by the minimality of k, $\mathrm{pr}_{k-\{i\}} B = A^{k-1}$ for all $i \in k$. Since $k < m$, the subuniverse $\mathrm{pr}_k B$ has cardinality a power of $|A|$. Thus $|\mathrm{pr}_k B| = |A|^{k-1}$, whence $\mathrm{pr}_k B$ is a k-automorphism of $\mathbf{A}$. By Lemma 8 we conclude that $|B| = |\mathrm{pr}_{m-\{j\}} B|$ for some $j \in m$. However, by assumption the right hand side is a power of $|A|$, while the left hand side is not. This contradiction completes the proof.

LEMMA 10. *Let* $\mathbf{A}$ *be a finite algebra having a trivial subalgebra* $\{0\}$*, and assume that for some* $m \geq 3$ *every subuniverse of* $\mathbf{A}^{m-1}$ *has cardinality a power of* $|A|$*. Let* B *be a subuniverse of* $\mathbf{A}^m$ *such that* $|B|$ *is not a power of* $|A|$*, and let*

$$B' = B(x_0, \ldots, x_{m-2}, 0),$$

$$\bar{B} = \{(x_0, \ldots, x_{m-1}) \in A^m\colon \text{ there is a } y \in A \text{ such that}$$

$$(x_{m-2}, x_1, \ldots, x_{m-3}, y) \in B' \text{ and } (x_0, \ldots, x_{m-3}, y, x_{m-1}) \in B\}.$$

If $B' \neq A^{m-1}$*, then*

(i) B' *is an* $(m-1)$*-automorphism of* $\mathbf{A}$*;*

(ii) $\bar{B}$ *is a subuniverse of* $\mathbf{A}^m$*,*

$$\bar{B} = \{(x_0, \ldots, x_{m-1}) \in A^m\colon (x_0, \ldots, x_{m-3}, \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \ldots, x_{m-3}), x_{m-1}) \in B\},$$

and we have

$$(x_0, \ldots, x_{m-2}, 0) \in \bar{B} \quad \text{if and only if} \quad x_0 = x_{m-2};$$

(iii) *the mapping*

$$\varphi\colon \bar{B} \to B, \quad (x_0, \ldots, x_{m-1}) \mapsto (x_0, \ldots, x_{m-3}, \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \ldots, x_{m-3}), x_{m-1})$$

is bijective, and hence $|\bar{B}| = |B|$*.*

PROOF. (i) By Lemma 9 (4) holds, and therefore

(5) $$\mathrm{pr}_{(m-1)-\{i\}} B' = A^{m-2} \quad \text{for all} \quad i \in (m-1).$$

Since B' is obviously a subuniverse of $\mathbf{A}^{m-1}$, $|B'|$ is a power of $|A|$, implying $|B'| = |A|^{m-2}$ (as $B' \neq A^{m-1}$). This proves (i).

(ii) It is straightforward to check that $\bar{B}$ is a subuniverse of $\mathbf{A}^m$, and in view of (i), the equality for $\bar{B}$ holds. For $x_0, \ldots, x_{m-2} \in A$ we have $(x_0, \ldots, x_{m-2}, 0) \in \bar{B}$ if and only if

$$(x_0, \ldots, x_{m-3}, \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \ldots, x_{m-3})) \in B',$$

or equivalently,

$$x_0 = \Gamma_{B'}^{0}(x_1, \ldots, x_{m-3}, \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \ldots, x_{m-3})).$$

However, by Lemma 7 the right hand side is x_{m-2}, proving the last claim in (ii).

(iii) Fixing $x_0, \dots, x_{m-3}, x_{m-1}$ arbitrarily, we know that the mapping $x_{m-2} \mapsto \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \dots, x_{m-3})$ of the remaining component is a permutation of A, hence φ is one-to-one. For arbitrary m-tuple $(x_0, \dots, x_{m-3}, y, x_{m-1}) \in B$ there exists $x_{m-2} \in A$ such that $y = \Gamma_{B'}^{m-2}(x_{m-2}, x_1, \dots, x_{m-3})$, so that $(x_0, \dots, x_{m-3}, x_{m-2}, x_{m-1}) \in \bar{B}$, proving that φ is onto.

LEMMA 11. *Let* $\mathbf{A}$ *be a finite algebra having a trivial subalgebra* $\{0\}$, *and assume that for some* $m \geq 3$ *every subuniverse of* $\mathbf{A}^{m-1}$ *has cardinality a power of* $|A|$. *If* B *is a subuniverse of* $\mathbf{A}^m$ *whose cardinality is not a power of* $|A|$, *then*

(i) $B(x_0, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_{m-1}) = A^{m-1}$ *for all* $i \in m$, *and*

(ii) B *is totally reflexive.*

PROOF. We use the notations of the previous lemma.

(i) By symmetry it suffices to show that $B' = A^{m-1}$. Suppose $B' \neq A^{m-1}$. Consider the subuniverse $C = \mathrm{pr}_{\{0,m-2,m-1\}} \bar{B}$ of $\mathbf{A}^3$. Using (4), (5) one can easily see that

$$\mathrm{pr}_{\{0,1\}} C = \mathrm{pr}_{\{0,2\}} C = \mathrm{pr}_{\{1,2\}} C = A^2.$$

Furthermore, by the property of $\bar{B}$ established in Lemma 10 (ii), $(a, b, 0) \in C$ if and only if $a = b$. Thus $C \neq A^3$. If $3 \leq m-1$, then by the assumption on the subuniverses of $\mathbf{A}^{m-1}$ we get that $|C| = |A|^2$, and hence C is a 3-automorphism of $\mathbf{A}$. Now it follows from the bijectivity of φ in Lemma 10 (iii) that the projection

$$B \to \mathrm{pr}_{m-\{0\}} B, \quad (x_0, x_1, \dots, x_{m-1}) \mapsto (x_1, \dots, x_{m-1})$$

is bijective. By Lemma 9 we have $\mathrm{pr}_{m-\{0\}} B = A^{m-1}$, implying $|B| = |A|^{m-1}$, which contradicts the assumptions of the lemma.

It remains to settle the case $m = 3$. Replacing B with $\bar{B}$ (which is now equal to C) we may assume without loss of generality that $B(x, y, 0) = \Delta$, in other words,

$$(x, y, 0) \in B \Leftrightarrow x = y. \tag{6}$$

Then, clearly, $B(0, x, y) \neq A^2$, which implies by Lemma 10 (i) (with the components interchanged) that $B(0, x.y)$ is a permutation. Hence the subuniverse $\mathrm{eq}_{01} B$ of $\mathbf{A}^2$ contains only one pair with first component 0 (namely $(0, 0)$), yielding that $\mathrm{eq}_{01} B \neq A^2$. However, $A \times \{0\} \subseteq \mathrm{eq}_{01} B$, therefore by the assumption on the subuniverses of $\mathbf{A}^2$ we conclude that equality holds here, that is,

$$(x, x, y) \in B \Leftrightarrow y = 0. \tag{7}$$

Now let

$$R = \{(x, y) \in A^2\colon\ (c, d, x), (c, d, y) \in B \text{ for some } c, d \in A\}.$$

Clearly, R is a subuniverse of $\mathbf{A}^2$, $\Delta \subseteq R$ since $\mathrm{pr}_{\{2\}} B = A$, and $R \neq A^2$ since $(0, y) \in R$ holds only if $y = 0$. Indeed, if $(0, y) \in R$, then $(c, d, 0), (c, d, y) \in B$ for some $c, d \in A$, hence applying (6) and (7) we get $c = d$ and $y = 0$. Thus $R = \Delta$, which means that the projection

$$B \to \mathrm{pr}_{\{0,1\}} B, \quad (x, y, z) \mapsto (x, y)$$

is bijective. By Lemma 9 we have $\mathrm{pr}_{\{0,1\}} B = A^2$, yielding $|B| = |A|^2$, which contradicts the assumptions of the lemma. This completes the proof of (i).

(ii) Let $i < j \in m$. By (i) the subuniverse $\mathrm{eq}_{ij} B$ of $\mathbf{A}$ contains every $(m-1)$-tuple with one component 0, whence $|A|^{m-2} < |\mathrm{eq}_{ij} B| \leq |A|^{m-1}$. The assumption on the cardinalities of subuniverses of $\mathbf{A}^{m-1}$ yields that $\mathrm{eq}_{ij} B = A^{m-1}$. Hence B is totally reflexive, as claimed.

Now we look at the subuniverses of $\mathbf{A}^2$.

LEMMA 12. *Let $\mathbf{A}$ be a finite, strictly simple algebra having at least one trivial subalgebra. If B is a subuniverse of $\mathbf{A}^2$ such that $\mathrm{pr}_{\{0\}} B = \mathrm{pr}_{\{1\}} B = A$ and $|A| < |B|$, then there exists an element $0 \in A$ such that $\{0\}$ is a trivial subalgebra of $\mathbf{A}$ and $B(x, 0) = A$ or $B(0, x) = A$.*

PROOF. Let U be the set of all elements $u \in A$ such that $\{u\}$ is a trivial subalgebra of $\mathbf{A}$. For arbitrary $u \in U$, $B(x, u)$ and $B(u, x)$ are subuniverses of $\mathbf{A}$, hence each of them is A or a singleton contained in U. Assume that, in contrary to our claim, $B(x, u)$ and $B(u, x)$ are singletons for all $u \in U$. Then $B \cap U^2$ is a permutation of U. Hence

$$C = \{(x, y) \in A^2\colon\ (x, z), (y, z) \in B \text{ for some } z \in A\}$$

is a reflexive, symmetric subuniverse of $\mathbf{A}^2$ such that $C(x, u) = C(u, x) = \{u\}$ for all $u \in U$. Further, $C \neq \Delta$, since equality here together with $\mathrm{pr}_{\{0\}} B = \mathrm{pr}_{\{1\}} B = A$ would imply that B is a permutation of A, contradicting $|B| > |A|$. Therefore the transitive closure of C is a congruence of $\mathbf{A}$ distinct from Δ, in which every element of U forms a singleton block. However, this is impossible, as $\mathbf{A}$ is simple.

LEMMA 13. *Let $\mathbf{A}$ be a finite algebra such that every proper subalgebra of $\mathbf{A}$ is trivial, and let $\{0\}$ be a fixed trivial subalgebra. If $\mathbf{A}^2$ has a subuniverse B*

such that $\operatorname{pr}_{\{0\}} B = \operatorname{pr}_{\{1\}} B = A$, $|A| < |B|$, $B(x,0) = \{0\}$, *then either some finite power* $\mathbf{A}^k$ *of* $\mathbf{A}$ *has a totally reflexive, totally symmetric subuniverse distinct from* A^k *and* Δ *(if* $k = 2$*), or there exists an element* $e \in A - \{0\}$ *such that* $B(x,e) = A$.

PROOF. For $k \geq 1$ let

$$R_k = \{(x_0, \ldots, x_{k-1}) \in A^k\colon \text{ there exists an } a \in A \text{ with } (x_i, a) \in B \text{ for all } i \in k\}.$$

Clearly, $R_1 = A$ and $\Delta \subseteq R_2$ as $\operatorname{pr}_{\{0\}} B = A$; moreover, $R_2 \neq \Delta$ since otherwise $\operatorname{pr}_{\{0\}} B = \operatorname{pr}_{\{1\}} B = A$ would imply that B is a permutation of A, contradicting $|B| > |A|$.

Let $|A| = n$, $A = \{a_0, \ldots, a_{n-1}\}$. If $R_n = A^n$, then there exists an element $e \in A$ such that $(a_i, e) \in B$ for all $i \in n$, that is, $B(x,e) = A$. Otherwise, let $k \geq 2$ be the least integer such that $R_k \neq A^k$. Since $R_{k-1} = A^{k-1}$, therefore R_k is totally reflexive. Clearly, R_k is totally symmetric. Furthermore, it is easily seen to be a subuniverse of $\mathbf{A}^k$. As we have seen before, $R_2 \neq \Delta$, so the proof is complete.

LEMMA 14. *Let* $\mathbf{A}$ *be a finite, strictly simple algebra having at least one trivial subalgebra, and let* U *be the set of all elements* $u \in A$ *such that* $\{u\}$ *is a trivial subalgebra of* $\mathbf{A}$. *Assume no finite power* $\mathbf{A}^k$ $(k \geq 2)$ *of* $\mathbf{A}$ *has a totally reflexive, totally symmetric subuniverse distinct from* A^k *and* Δ *(if* $k = 2$*).*

(i) *If* B *is a non-reflexive subuniverse of* $\mathbf{A}^2$ *such that* $\operatorname{pr}_{\{0\}} B = \operatorname{pr}_{\{1\}} B = A$ *and* $|A| < |B|$, *then* B *is a* U*-cross.*

(ii) *If* B *is a reflexive subuniverse of* $\mathbf{A}^2$ *with* $|A| < |B| < |A|^2$, *then its transitive closure is a bounded partial order on* A *such that every element of* U *is a bound.*

PROOF. (i) By Lemma 12, there exists an element $0 \in U$ such that, say, $B(0,x) = A$. Since B is not reflexive, the subuniverse $\operatorname{eq}_{01} B$ of $\mathbf{A}$ is a singleton, namely $\{0\}$, as $(0,0) \in B$. Thus $B(x,0) \supseteq \{0\}$. Supposing equality holds here we would get from Lemma 13 that there exists an element $e \in A$ with $B(x,e) = A$. Then $(e,e) \in B$, implying $e = 0$, whence $B(x,0) = A$.

Thus $X_0 \subseteq B$. For arbitrary element $u \in U - \{0\}$, the subuniverses $B(u,x)$ and $B(x,u)$ of $\mathbf{A}$ contain 0 and do not contain u, hence $B(u,x) = B(x,u) = \{0\}$. Therefore the relation $Y = B - X_0$ is contained in $(A-U)^2$. Since $\operatorname{eq}_{01} B = \{0\}$, Y is irreflexive on $A - U$. Thus B is a U-cross.

(ii) Again by Lemma 12, there exists an element $0 \in U$ such that, say, $B(0,x) = A$. Since $B \cap B^{-1}$ is a reflexive, symmetric subuniverse of $\mathbf{A}^2$, we have

$B \cap B^{-1} = \Delta$, that is, B is *antisymmetric*. Hence $B(x, 0) = \{0\}$. Let $\hat{B}$ be the transitive closure of B. It is easy to check that $\hat{B}$ is a subuniverse of $\mathbf{A}^2$, $B \subseteq \hat{B}$, and $\hat{B}(0, x) = A$, $\hat{B}(x, 0) = \{0\}$. By the same reason as above, $\hat{B}$ is antisymmetric. Thus $\hat{B}$ is a partial order with least element 0. Applying Lemma 13 for $\hat{B}$ we get that it has a greatest element e as well. If there existed an element $u \in U$ such that $u \neq 0, e$, then $\hat{B}(x, u)$ would be a proper, nontrivial subuniverse of $\mathbf{A}$, as it contains $0, u$, and fails to contain e. This completes the proof.

LEMMA 15. *Let $\mathbf{A}$ be a finite, strictly simple algebra having at least one trivial subalgebra, and let U be the set of all elements $u \in A$ such that $\{u\}$ is a trivial subalgebra of $\mathbf{A}$. Assume some finite power $\mathbf{A}^m$ $(m \geq 2)$ of $\mathbf{A}$ contains a totally reflexive, totally symmetric subuniverse distinct from A^m and Δ (if $m = 2$). If m is chosen minimal with this property and B is a totally reflexive, totally symmetric subuniverse of $\mathbf{A}^m$ distinct from A^m and Δ (if $m = 2$), then B is U-central.*

PROOF. For arbitrary $u \in U$, $B(x_0, \ldots, x_{m-2}, u)$ is a totally reflexive, totally symmetric subuniverse of $\mathbf{A}^{m-1}$. If $m = 2$, then Lemma 12 combined with the symmetry of B implies $X_0 \subseteq B$ for some $0 \in U$. Thus $B(x_0, u) = A$ is obvious if $u = 0$, and in view of $0, u \in B(x_0, u)$ it follows also if $u \neq 0$. If $m \geq 3$, then the minimality of m yields that $B(x_0, \ldots, x_{m-2}, u) = A^{m-1}$. Hence in either case B is central and u belongs to the centre of B. Thus B is U-central.

Now we are in a position to conclude the proof of Theorem 1. Let $\mathbf{A}$ be a finite strictly simple algebra having at least one trivial subalgebra, and let U be the set of all elements u of $\mathbf{A}$ for which $\{u\}$ is a trivial subalgebra of $\mathbf{A}$. If each subuniverse of each finite power of $\mathbf{A}$ has cardinality a power of A, then, by a result of R. W. Quackenbush [9] $\mathbf{A}$ generates a congruence permutable variety, and hence by a theorem of R. McKenzie [6] (cf. also [13], [2]) one of conditions (a), (b) holds for $\mathbf{A}$. If some finite power $\mathbf{A}^m$ $(m \geq 2)$ of $\mathbf{A}$ contains a totally reflexive, totally symmetric subuniverse distinct from A^m and Δ (if $m = 2$), then by Lemma 15, (c) holds for $\mathbf{A}$. So assume no finite power $\mathbf{A}^k$ $(k \geq 2)$ of $\mathbf{A}$ has a totally reflexive, totally symmetric subuniverse distinct from A^k and Δ (if $k = 2$), and some power $\mathbf{A}^m$ of $\mathbf{A}$ has a subuniverse B with $|B|$ not a power of $|A|$. Suppose m is chosen minimal with respect to the existence of such B. We have $m \geq 2$, as $\mathbf{A}$ has no nontrivial proper subalgebras. Were $m \geq 3$, we would get from Lemma 11 (ii) that B is totally reflexive, and hence the subuniverse $\bigcap(B^\pi \colon \pi \in S_n)$ of $\mathbf{A}^m$ is totally reflexive and totally symmetric, which is impossible. Thus $m = 2$. Now by Lemma

9 the hypotheses of Lemma 14 (i) or (ii) are satisfied. Hence applying the lemma, and in case (i) taking $B \cap B^{-1}$, we see that (d) or (e) holds for $\mathbf{A}$.

REMARK. Observe that the role of Lemma 13, where we made essential use of the finiteness of $\mathbf{A}$, is restricted merely to the proof of Lemma 14. However, if $|U| \geq 2$, then both of the claims (i), (ii) in Lemma 14 can be proved directly, without any assumption on the totally reflexive, totally symmetric subuniverses of finite powers of $\mathbf{A}$. (It suffices to look at the subuniverses $B(x,u)$, $B(u,x)$ ($u \in U$) of $\mathbf{A}$.)

Apart from this, finiteness is apparently crucial throughout the section because of the arguments using the cardinalities of subuniverses of finite powers of $\mathbf{A}$. However, applying multi-automorphisms, one can modify these arguments so that they work for infinite algebras as well. Namely, for not necessarily finite algebras, multi-automorphisms can be defined by the equivalent conditions (ii) and (iii) in Lemma 7. Lemmas 9–10, 12, 14 (for $|U| \geq 2$) go through, with occasional slight changes in the proofs, for all algebras having no nontrivial proper subalgebras, if one takes for m the least positive integer for which $\mathbf{A}^m$ has a subuniverse B such that

(*) $B \neq A^m$, $\mathrm{pr}_{\{i\}} B = A$ for all $i \in m$, and $\mathrm{pr}_I B$ is not a multi-automorphism of $\mathbf{A}$ for any subset $I \subseteq m$, $|I| \geq 2$.

For Lemma 11 we have to assume, in addition, that none of the projection mappings $B \to \mathrm{pr}_{m-\{i\}} B = A^{m-1}$, $i \in m$, is bijective. The following claim shows that should this fail for the B we started with, we can always replace it with another subuniverse of $\mathbf{A}^m$ having the required property.

CLAIM. *Let B be a subuniverse of $\mathbf{A}^m$ ($m \geq 2$) such that $\mathrm{pr}_{m-\{i\}} B = A^{m-1}$ for all $i \in m$, and the projection mapping $B \to \mathrm{pr}_{(m-1)} B = A^{m-1}$ is bijective, while the projection mapping $B \to \mathrm{pr}_{m-\{0\}} B = A^{m-1}$ is not bijective. Then for the subuniverse*

$$B^* = \{(x_0, x_0', x_1, \dots, x_{m-2}) \in A^m\text{: there is a } y \in A \text{ such that}$$

$$(x_0, x_1, \dots, x_{m-2}, y), (x_0', x_1, \dots, x_{m-2}, y) \in B\}$$

of $\mathbf{A}^m$, none of the projection mappings $B^* \to \mathrm{pr}_{m-\{i\}} B^* = A^{m-1}$, $i \in m$, is bijective, and $B^* \neq A^m$.

Lemma 8 becomes superfluous, and Lemma 15 remains valid without change. Finally, if no finite power $\mathbf{A}^m$ of $\mathbf{A}$ has a subuniverse B satisfying (*), then, instead of

Quackenbush's theorem [9], one can apply the results of [14] on locally paraprimal algebras, and hence conclude that **A** is either locally quasiprimal, or locally affine.

In this manner, if $|U| \geq 2$, then Theorem 1 can be extended to infinite algebras as well.

3. Proofs of the corollaries

(A) First we prove that every proper subclone of $\mathcal{C}_U$ is contained in $\mathcal{P}_B$, or equivalently, for every algebra $\mathbf{A}$ with $\operatorname{Clo}\mathbf{A} \subset \mathcal{C}_U$, B is a subuniverse of the corresponding power of **A**, for at least one of the relations B in (I)–(VII). So assume **A** is an algebra such that $\operatorname{Clo}\mathbf{A} \subset \mathcal{C}_U$. If **A** has a proper subalgebra distinct from the singletons $\{u\}$, $u \in U$, then its universe B clearly satisfies (I). If **A** is not simple, say B is a nontrivial congruence of **A**, then either (II) holds for B, or for some $u \in U$, the block $B(x,u)$ of B containing u is a subuniverse of **A** as described in (I).

From now on we assume that **A** is strictly simple and the trivial subalgebras of **A** are exactly $\{u\}$, $u \in U$. So we can apply Theorem 1. If (a) holds, then **A** has a nontrivial automorphism (as it has no nontrivial proper subalgebras), and hence it has an automorphism σ of prime order. Clearly, σ carries trivial subalgebras into trivial subalgebras, hence U is invariant under σ. Furthermore, since the fixed points of σ form a subalgebra in **A**, it follows that σ has at most one fixed point, and the fixed point (if any) belongs to U. Thus σ is as described in (III).

Now suppose (b) holds for **A**. It is well known that for an affine algebra **A** and for arbitrary element $0 \in A$ there exists an (unique) Abelian group $\widehat{A}$ with neutral element 0 such that **A** is affine with respect to $\widehat{A}$; namely, the operation $+$ of $\widehat{A}$ is defined by $x + y = p(x, 0, y)$ where p is the unique term operation of **A** satisfying Mal'tsev's identities $p(x, y, y) = p(y, y, x) = x$. Therefore there is no loss of generality in assuming that **A** is affine with respect to an elementary Abelian p-group (p prime) $\widehat{A} = (A; +, 0)$ such that $0 \in U$. Since $\{0\}$ is a subalgebra of **A**, **A** is a reduct of the module ${}_{(\operatorname{End}\widehat{A})}\widehat{A}$. Hence every fundamental operation of **A** is of the form

$$\sum_{i \in m} r_i x_i \quad (r_i \in \operatorname{End}\widehat{A},\ i \in m).$$

Now it is easy to verify that U is a subgroup of $\widehat{A}$. Further, if $|U| > 1$ and $u \in U - \{0\}$, then the mapping $A \to A$, $x \mapsto x + u$ is an automorphism of **A** satisfying the requirements in (III). If $U = \{0\}$ and $p > 2$, then selecting an integer $c > 1$

that is of prime order modulo p, we get that the mapping $A \to A$, $x \mapsto cx$ is an automorphism of $\mathbf{A}$ satisfying the requirements in (III). In the remaining case $U = \{0\}$, $p = 2$, the subuniverse $Q_{\widehat{A}}(x, 0, y, z)$ of $\mathbf{A}^3$ is as described in (IV).

Finally, if (c), (d), or (e) holds for $\mathbf{A}$, then we have nothing to prove: the same relations are listed in (V), (VI), (VII), respectively.

It is easy to see that for every relation B in (I)–(VII), $\mathcal{C}_U \cap \mathcal{P}_B$ is a proper subclone in $\mathcal{C}_U$. To prove their maximality in $\mathcal{C}_U$, it suffices now to verify that there are no proper inclusions between any two of them. In fact, the argument shows also that equality can hold only in the 'obvious' cases, namely when either both relations are of type (III) and are powers of each other, or both relations are of type (VI) and are inverses of each other.

So let B, B' be two distinct relations in (I)–(VII). We intend to prove that, except for the cases just mentioned,

$$(8) \qquad \mathcal{C}_U \cap \mathcal{P}_B \not\subseteq \mathcal{C}_U \cap \mathcal{P}_{B'}.$$

Consider the algebras $\mathbf{A} = (A; \mathcal{C}_U \cap \mathcal{P}_B)$ and $\mathbf{A}' = (A; \mathcal{C}_U \cap \mathcal{P}_{B'})$.

First let B be as described in (I) or (III). Then $\mathbf{A}$ is quasiprimal, and (8) holds for every B' which is not of type (I) or (III). So assume B', too, is as described in (I) or (III), and hence $\mathbf{A}'$ is also quasiprimal. Observe that in case (I) the algebras have no nontrivial automorphisms, and the proper subalgebras are exactly B [resp. B'] and $\{u\}$, $u \in U$; in case (III) the automorphisms are exactly the powers of B [resp. B'], and the algebras have no proper subalgebras other than $\{u\}$, $u \in U$. Thus (8) holds unless B, B' are both of type (III) and are powers of each other.

Now let B be of type (IV). Then $\mathbf{A}$ is term equivalent to the module ${}_{(\mathrm{End}\,\widehat{A})}\widehat{A}$, hence $\mathbf{A}$ is simple and has no proper subalgebras other than $\{0\}$. Moreover, as $\widehat{A}$ is a 2-group, $\mathbf{A}$ has no nontrivial automorphisms. This implies (8) unless B' is also of type (IV). In that case (8) follows by checking that the term operation $+$ of $\mathbf{A}$ does not preserve B' if $B' \neq B$.

The remaining cases can be handled in a uniform way. We illustrate the method on the case when B is of type (VII). So let B be a U-cross such that $X_0 \subseteq B$, $0 \in U$. We consider $n \times t$ matrices M with entries in A such that

(9) the rows are pairwise distinct, and
none of the vectors $(u, \ldots, u)$, $u \in U$, occurs among the rows.

The rows of M will be denoted by M_i, $i \in n$. If (9) holds for M, then for arbitrary

n-tuple $a = (a_0, \ldots, a_{n-1})$, we can define a t-ary operation on A as follows:

$$f_{M,a}(x_0, \ldots, x_{t-1}) = \begin{cases} a_i & \text{if } (x_0, \ldots, x_{t-1}) = M_i \text{ for some } i \in n, \\ u & \text{if } (x_0, \ldots, x_{t-1}) = (u, \ldots, u) \text{ for some } u \in U, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that if

$$(10) \qquad (a_i, a_j) \in B \quad \text{whenever} \quad (M_i, M_j) \in B^t,\ i, j \in n,\ i \neq j,$$

then $f_{M,a} \in \mathcal{C}_U \cap \mathcal{P}_B$. (For t-tuples $v, w \in A^t$, $(v, w) \in B^t$ denotes that v and w are componentwise in relation B.)

Now let B' be one of the relations in (I)–(VII) distinct from B, say B' is n-ary, and select a matrix M such that the set of columns of M is exactly B'. Clearly, (9) and (10) are now equivalent to requiring that

$$(9')_n \qquad \mathrm{pr}_{(i,j)} B' \not\subseteq \Delta \quad \text{for all} \quad i, j \in n,\ i \neq j,$$

$$\mathrm{pr}_{\{i\}} B' \neq \{u\} \quad \text{for all} \quad i \in n,\ u \in U,$$

and

$$(10')_n \qquad (a_i, a_j) \in B \quad \text{whenever} \quad \mathrm{pr}_{(i,j)} B' \subseteq B,\ i, j \in n,\ i \neq j,$$

respectively. Thus (9) holds, and (8) follows by verifying that we can always select an n-tuple $a \notin B'$ with (10), implying $f_{M,a} \in \mathcal{C}_U \cap \mathcal{P}_B$ and $f_{M,a} \notin \mathcal{P}_{B'}$.

A similar argument works also if B belongs to the families (II), (V) or (VI). We note that if B is of type (VI), then the existence of the required monotone operations $g_{M,a}$ such that $g_{M,a}(u, \ldots, u) = u$ for $u \in U$ and

$$g_{M,a}(M_i) = a_i \quad \text{for all} \quad i = 0, \ldots, n-1$$

follows from the fact that the rows of the matrices M corresponding to the relations B' in (I)–(VII) are pairwise incomparable under B (componentwise) unless B', too, is of type (VI) and $B' \subseteq B$. The details are left to the reader.

(B) The necessity in Corollary 3 is obvious. For the sufficiency we apply Theorem 1. Let $\mathbf{A}$ be a strictly simple algebra such that the trivial subalgebras are exactly $\{u\}$, $u \in U$, and $\mathbf{A}$ does not generate a congruence permutable variety. By Theorem 1 one of conditions (c)–(e) holds for $\mathbf{A}$. If, in addition, $\mathbf{A}$ is surjective, then we can apply the following well-known and easy lemma (cf. [11], [12]).

LEMMA 16. *Let* $\mathbf{A}$ *be a finite surjective algebra. If* B *is a subuniverse of* $\mathbf{A}^k$ $(k \geq 2)$, *then for arbitrary* l $(1 \leq l \leq n-1)$,

$$(B)_l = \{(x_0, \dots, x_{l-1}) \in A^l \colon (x_0, \dots, x_{k-1}) \in B \text{ for all } x_l, \dots, x_{k-1} \in A\}$$

is a subuniverse of $\mathbf{A}^l$ *provided it is not empty.*

Thus, if B is a U-central subuniverse of $\mathbf{A}^k$, then $(B)_1$, the centre of B, is a proper subuniverse of $\mathbf{A}$ containing U. Hence U is the centre of B and $|U| = 1$. Now $(B)_2$ is a U-central subuniverse of $\mathbf{A}^2$ with the same centre as B. If B is a bounded partial order, then $(B)_1$ and $(B^{-1})_1$ are the two singletons containing the bounds, hence $|U| = 2$. This completes the proof of Corollary 3.

For the proof of Proposition 4 we slightly modify the construction used at the end of the proof of Corollary 2. First let B be a U-cross with $X_0 \subseteq B$, $0 \in U$, or a binary U-central relation with centre $U = \{0\}$. Let B' be a binary relation on A satisfying $(9')_2$. We show that for $n = \max(|A|, 3) + 2$ and for some $t \geq |B'|$, there exists an $n \times t$ matrix M such that the set of columns of the submatrix of M consisting of the first two rows equals B', and

$$(M_i, M_j) \notin B^t \quad \text{for all} \quad i, j \in n,\ i \neq j,\ \{i, j\} \neq \{0, 1\}. \tag{11}$$

By the assumption on B' there exist $(b, b'), (c, c') \in B'$ such that $b \neq 0$, $c' \neq 0$. Hence there exist elements $d, d' \in A$ such that $d \neq b$, $d' \neq c'$ and one of the pairs (b, b), (d, b) and one of the pairs (c', c'), (d', c') fails to belong to B. Thus any matrix M whose first $2(n-2)$ colums are as shown below, and is such that the columns of the submatrix consisting of the first two rows equals B', otherwise arbitrary, satisfies the requirements.

$$\begin{pmatrix} b & b & b & \dots & b & b' & b' & b' & \dots & b' & \bullet & \dots & \bullet \\ c & c & c & \dots & c & c' & c' & c' & \dots & c' & \bullet & \dots & \bullet \\ d & b & b & \dots & b & d' & c' & c' & \dots & c' & & & \\ b & d & b & \dots & b & c' & d' & c' & \dots & c' & & & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & \\ b & b & b & \dots & d & c' & c' & c' & \dots & d' & & & \end{pmatrix}$$

In view of (11), for arbitrary n-tuple $a = (a_0, \dots, a_{n-1})$ with $(a_0, a_1) \in B$ provided $B' \subseteq B$, the operation $f_{M,a}$ belongs to $\mathcal{C}_U \cap \mathcal{P}_B$. Hence to each B' satisfying $(9')_2$ and distinct from B and A^2, there exists a surjective operation $f_{M,a}$ such that $f_{M,a} \in \mathcal{C}_U \cap \mathcal{P}_B$ and $f_{M,a} \notin \mathcal{P}_{B'}$. Thus the algebra $\mathbf{A}$ whose operations are these $f_{M,a}$ while B' runs over

(i) all binary relations $S \times A$ with $1 \leq |S| < |A|$, $S \neq \{u\}$ for all $u \in U$,

(ii) all nontrivial equivalences on A, and

(iii) all relations in (α)–(γ) distinct from B,

has the properties stated in the proposition.

A similar idea works also if B is a bounded partial order with bounds 0, 1. Now the last n rows of M are to be constructed so that they be incomparable (by the componentwise order) to the first two rows and to one another as well. They can always be chosen so that they consist of 0's and 1's. The role of $f_{M,a}$ is to be taken by monotone operations $g_{M,a}$ such that

$$g_{M,a}(0,\ldots,0) = 0, \quad g_{M,a}(1,\ldots,1) = 1,$$

and

$$g_{M,a}(M_i) = a_i \quad \text{for all} \quad i = 0,\ldots,n-1.$$

It can be shown that such a $g_{M,a}$ exists if for the n-tuple $a = (a_0,\ldots,a_{n-1})$ we have $(a_0,a_1) \in B$ provided $B' \subseteq B$, and $(a_0,a_1) \in B^{-1}$ provided $B' \subseteq B^{-1}$. The details are left to the reader.

To see the claim in the first remark, observe that for B a U-cross with $X_0 \subseteq B$, $0 \in U$, or a binary U-central relation with centre $U = \{0\}$, $\mathcal{C}_U \cap \mathcal{P}_B$ contains a majority operation, e.g. the one defined below:

$$m(x,y,z) = \begin{cases} x & \text{if } x = y \text{ or } x = z, \\ y & \text{if } y = z, \\ 0 & \text{otherwise.} \end{cases}$$

Adding this operation to $\mathbf{A}$, we get an algebra $\mathbf{A}'$, which inherits properties (i)–(iii) in Proposition 4, and has a majority operation as well. Hence by a theorem of K. A. Baker and A. F. Pixley [1] $\mathbf{A}'$ is term equivalent to $(A;\mathcal{C}_U \cap \mathcal{P}_B)$.

(C) The only nontrivial statement in Proposition 5 is that the algebra $\mathbf{A} = (A;\mathcal{C}_U \cap \mathcal{P}_B)$ is functionally complete. However, as we have seen in part (B), $\mathbf{A}$ has a majority operation, and the only reflexive subuniverses of $\mathbf{A}^2$ are Δ and A^2. Thus it follows from the theorem of K. A. Baker and A. F. Pixley [1] that $\mathbf{A}$ is functionally complete.

In Corollary 6 the necessity is obvious, while the sufficiency follows from Theorem 1 by observing that conditions (b)–(d) cannot hold for a functionally complete algebra.

References

[1] K. A. Baker, A. F. Pixley, Polynomial interpolation and the Chinese Remainder Theorem for algebraic systems, *Math. Z.* **143** (1975), 165–174.

[2] H. P. Gumm, Algebras in congruence permutable varieties: Geometrical properties of affine algebras, *Algebra Universalis* **9** (1979), 8–34.

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

[4] K. Kaarli, *Algebra Universalis*, submitted.

[5] D. Lau, Die maximale Klassen von $\mathrm{Pol}_k(0)$, *Rostock. Math. Kolloq.* **19** (1982), 29–47.

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

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

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

[9] R. W. Quackenbush, Algebras with minimal spectrum, *Algebra Universalis* **10** (1980), 117–129.

[10] I. G. Rosenberg, Über die funktionale Vollständigkeit in den mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen), *Rozpravy Československe Akad. Věd Řada Mat. Přírod. Věd* **80** (1970), 9–93.

[11] I. G. Rosenberg, Functional completeness of single generated or surjective algebras, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam, 1981; pp. 635–652.

[12] G. Rousseau, Completeness in finite algebras with a single operation, *Proc. Amer. Math. Soc.* **18** (1967), 1009–1013.

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

[14] Á. Szendrei, Locally para-primal algebras, in: *Contributions to General Algebra 5* (Proc. Conf. Salzburg, 1986), Verlag Hölder–Pichler–Tempsky, Wien, Verlag Teubner, Stuttgart, 1987; pp. 367–399.

[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] Á. Szendrei, Simple surjective algebras having no proper subalgebras, *J. Austral. Math. Soc.*, to appear.

[18] G. Tardos, A maximal clone of monotone operations which is not finitely generated, *Order* **3** (1986), 211–218.

Bolyai Institute
Aradi vértanúk tere 1
6720 Szeged, Hungary

Current address:
FB Mathematik, AG 1
Technische Hochschule Darmstadt
Schlossgartenstr. 7
6100 Darmstadt, Fed. Rep. Germany