Revised version, August 1990

The primal algebra characterization theorem revisited

Ágnes Szendrei

The aim of this note is to present a strong version of I. G. Rosenberg's primal algebra characterization theorem that was found while studying simple algebras without proper subalgebras having the additional property that their fundamental operations are surjective. The investigation of these algebras, which was inspired by a recent paper of C. Bergman and R. McKenzie [1], will be completed in a forthcoming paper [20].

It seems, however, that the new version of Rosenberg's theorem to be discussed here is of independent interest as well. It sheds some light on the following strange phenomenon occurring in the proof (but remainimg hidden in the final formulation) of Rosenberg's theorem [12]: certain algebras semi-affine with respect to elementary Abelian 2-groups come up in the proof at some point after semi-affine algebras had already seemed to have been taken care of. Starting from R. W. Quackenbush's proof [11] we now show that all these 'exceptional' algebras are isomorphic to reducts of matrix powers of 2-element unary algebras; moreover, all other semi-affine algebras whose powers admit no subalgebras falling into any of the remaining five classes of Rosenberg's theorem are in fact affine.

1. The main result

For a set A and for $k \geq 1$, the nonvoid subsets of A^k will often 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 $\mathbf{A}$. We adopt the convention that algebras are denoted by boldface capitals and their

Research partially supported by Hungarian National Foundation for Scientific Research grant no. 1813.

universes by the corresponding letters in italics. We identify every natural number n with the set $n = \{0, \dots, n-1\}$. For a set N, let T_N, S_N, and C_N denote the full transformation monoid on N, the full symmetric group on N and the set of (unary) constant operations on N, respectively. We denote by id_N, or shortly id, the identity mapping on N. 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 $\mathrm{Pol}\,\mathbf{A}$ the clone of term operations, the set of unary term operations, and the clone of polynomial operations of $\mathbf{A}$, respectively.

Recall that a finite algebra is said to be *primal* if every operation on its universe is a term operation. As is well known, I. G. Rosenberg's theorem [12] characterizes primal algebras $\mathbf{A}$ by the nonexistence of six kinds of relations among the subuniverses of finite powers of $\mathbf{A}$. Equivalently, for every finite algebra $\mathbf{A}$ which is not primal, some finite power of $\mathbf{A}$ has a subuniverse falling into one of six classes of relations. Four of these classes are as follows:

(1) bounded partial orders on A,

(2) permutations of A (considered as binary relations) having cycles of equal prime length and no fixed points,

(3) equivalence relations distinct from A^2 and the diagonal Δ,

(4) quaternary relations of the form

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

for some elementary Abelian p-group $\widehat{A} = (A;+)$ (p prime).

We say that an algebra $\mathbf{A}$ is *semi-affine with respect to an Abelian group* $\widehat{A}$ if $\mathbf{A}$ and $\widehat{A}$ have the same universe and the quaternary relation $Q_{\widehat{A}}$ is a subuniverse of $\mathbf{A}^4$. Furthermore, $\mathbf{A}$ is said to be *affine with respect to* $\widehat{A} = (A;+)$ if it is semi-affine with respect to $\widehat{A}$ and, in addition, $x - y + z$ is a term operation of $\mathbf{A}$. It is well known and easy to see (cf. [19; 2.1, 2.7– 2.8]) that the algebras that are semi-affine, or affine, with respect to $\widehat{A}$ are closely 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 1.1. *Let* $\mathbf{A}$ *be an algebra and* $\widehat{A}$ *an Abelian group on its universe.*

(i) $\mathbf{A}$ *is semi-affine with respect to* $\widehat{A}$ *if and only if* $\mathbf{A}$ *is a reduct of the algebra* $(A; \mathrm{Pol}\,({}_{(\mathrm{End}\,\widehat{A})}\widehat{A}))$*;*

(ii) $\mathbf{A}$ *is affine with respect to* $\widehat{A}$ *if and only if* $\mathbf{A}$ *is polynomially equivalent to a module* ${}_R\widehat{A}$ *for some subring* R *of* $\mathrm{End}\,\widehat{A}$*.*

To describe the remaining two classes of relations we need some definitions. A k-ary relation B on A is called *totally reflexive* if it contains each k-tuple from A^k whose coordinates are not pairwise distinct. Further, B is called *totally symmetric* if it is closed under permuting the coordinates. A totally reflexive, totally symmetric relation $B \subseteq A^k$ is called *central* if $B \neq A^k$ and there exists $c \in A$ such that $(c, a_1, \ldots, a_{k-1}) \in B$ for all $a_1, \ldots, a_{k-1} \in A$. The fifth class is

(5) central relations on A.

Observe that every unary relation is totally reflexive and symmetric, hence the unary central relations are exactly the nonvoid proper subsets of A.

Let $k \geq 3$. A family $T = \{\Theta_0, \ldots, \Theta_{m-1}\}$ $(m \geq 1)$ of equivalence relations on A is called *k-regular* if each Θ_i $(0 \leq i \leq m-1)$ has exactly k blocks and $\Theta_T = \Theta_0 \cap \ldots \cap \Theta_{m-1}$ has exactly k^m blocks. A relation on A is called *k-regular* if it is of the form

$$\lambda_T = \{(a_0, \ldots, a_{k-1}) \in A^k\colon \text{ for all } i \ (0 \leq i \leq m-1),$$
$$a_0, \ldots, a_{k-1} \text{ are not pairwise incongruent modulo } \Theta_i\}$$

for a k-regular family T of equivalence relations on A. They form the sixth class:

(6) k-regular relations on A $(k \geq 3)$.

Note that k-regular relations are both totally reflexive and totally symmetric.

Matrix powers of unary algebras are examples of algebras admitting a subuniverse belonging to class (6). For the notion and the history of matrix powers of arbitrary algebras the reader is referred to [21], [5]. 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 given mappings $\sigma\colon m \to m$, $\mu\colon m \to n$ and for $g_0, \ldots, g_{m-1} \in \mathrm{Clo}_1\,\mathbf{C}$ let us define an operation $h^\sigma_\mu[g_0, \ldots, g_{m-1}]$ on C^m as follows: for $x_i = (x_i^0, \ldots, x_i^{m-1}) \in C^m$ $(0 \leq i \leq n-1)$, put

$$h^\sigma_\mu[g_0,\dots,g_{m-1}](x_0,\dots,x_{n-1})=(g_0(x^{0\sigma}_{0\mu}),\dots,g_{m-1}(x^{(m-1)\sigma}_{(m-1)\mu})).$$

The *m-th matrix power* of $\mathbf{C}$, denoted $\mathbf{C}^{[m]}$, is the algebra with universe C^m and with all $h^\sigma_\mu[g_0,\dots,g_{m-1}]$ 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, $\operatorname{Clo}\mathbf{C}^{[m]}$ consists of all operations of the form $h^\sigma_\mu[g_0,\dots,g_{m-1}]$ as above. Clearly, every term operation of $\mathbf{C}^{[m]}$ depends on at most m variables. It is straightforward to check that if $|C|=k\geq 3$ and T consists of the kernels of the m projections $C^m\to C$, then T is a k-regular family of equivalences on C^m (with $\Theta_T=\Delta$), and λ_T is a subuniverse of $(\mathbf{C}^{[m]})^k$.

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].

CLAIM 1.2. *A finite algebra $\mathbf{A}$ is quasiprimal if and only if the ternary discriminator*

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

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

Note that each algebra whose term operations are all operations admitting a relation of class (2), or similarly, a unary relation of class (5) is quasiprimal. Also, every primal algebra is obviously quasiprimal.

Now we are in a position to state the main result of the paper.

THEOREM 1.3. *Let $\mathbf{A}$ be a finite simple algebra having no proper subalgebra. 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 isomorphic to a reduct of $(2;T_2)^{[m]}$ for some integer $m\geq 1$;*

(d) *there is a k-regular relation among the subuniverses of $\mathbf{A}^k$ for some $k\geq 3$;*

(e) *there is a central relation among the subuniverses of $\mathbf{A}^k$ for some $k\geq 2$;*

(f) *there is a bounded partial order among the subuniverses of* $\mathbf{A}^2$.

2. The 'exceptional' algebras

As was mentioned in the introduction, the core of the proof of Theorem 1.3 is the analysis of those semi-affine algebras that come up so unexpectedly in the proof of Rosenberg's theorem. This is done in this section.

Recall that in [6] an algebra $\mathbf{A}$ is said to be *strongly Abelian* if for all $n \geq 1$, for every n-ary term operation f of $\mathbf{A}$ and for arbitrary elements $u, v \in A$ and $a_i, b_i, c_i \in A$ $(1 \leq i \leq n-1)$,

$$f(u, a_1, \ldots, a_{n-1}) = f(v, b_1, \ldots, b_{n-1}) \quad \text{implies} \quad f(u, c_1, \ldots, c_{n-1}) = f(v, c_1, \ldots, c_{n-1}).$$

For $B \subseteq A^n$ and for $0 \leq i_0, \ldots, i_{k-1} \leq n-1$,

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

is the *projection* of B onto its coordinates $i_0, \ldots, i_{k-1}$. 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 $\mathrm{pr}_{i_0,\ldots,i_{k-1}} B$.

THEOREM 2.1. *Let* $\mathbf{A}$ *be a finite algebra which is strongly Abelian and semi-affine with respect to an Abelian group. Assume no finite power* $\mathbf{A}^k$ $(k > 2)$ *of* $\mathbf{A}$ *has a totally reflexive, totally symmetric subuniverse distinct from* A^k. *Then* $\mathbf{A}$ *is isomorphic to a reduct of* $(2; T_2)^{[m]}$ *for some integer* $m \geq 1$.

Proof. Let $\mathbf{A}$ satisfy the assumptions, and let $\widehat{A} = (A; +)$ be an Abelian group such that $\mathbf{A}$ is semi-affine with respect to $\widehat{A}$. For arbitrary Abelian group operation $+$ we will denote by d_+ the ternary operation defined by $d_+(x, y, z) = x - y + z$. First we prove the following claim.

Claim (a). For some $m \geq 1$ and some subalgebra $(N; d_+)$ of $(A; d_+)$, there exist a subdirect subalgebra $(W; d_+)$ of $(N; d_+)^m$ and an isomorphism $\varphi\colon (A; d_+) \to (W; d_+)$

which is simultaneously an isomorphism between $\mathbf{A}$ and the subalgebra $\mathbf{W}$ on W of a reduct of $(N; C_N)^{[m]}$.

We use the idea of [6; 13.3]. Let N be a minimal set in $\mathbf{A}$, and e a unary polynomial of $\mathbf{A}$ with $e^2 = e$ and $e(A) = N$. Let $F = \{f_0 = e, f_1, \ldots, f_{m-1}\}$ be the family of all unary polynomial operations of $\mathbf{A}$ with range N. By the basics of tame congruence theory [6; 2.8.4], for any distinct elements $x, y \in A$ there exists $f_i \in F$ such that $f_i(x) \neq f_i(y)$. Thus the assignment

$$x \mapsto (f_0(x), \ldots, f_{m-1}(x)) \quad (x \in A)$$

defines a bijective mapping of A onto a subdirect subset W of N^m. Let us denote this mapping by φ. Computing in $\mathbf{A}$ and $\widehat{A}^m$, and taking into account that $\mathbf{A}$ is semi-affine with respect to $\widehat{A}$, we get for arbitrary elements $x, y, z \in A$ that

$$d_+(x,y,z)\varphi = (x - y + z)\varphi = (f_0(x - y + z), \ldots, f_{m-1}(x - y + z))$$
$$= (f_0(x) - f_0(y) + f_0(z), \ldots, f_{m-1}(x) - f_{m-1}(y) + f_{m-1}(z))$$
$$= (f_0(x), \ldots, f_{m-1}(x)) - (f_0(y), \ldots, f_{m-1}(y)) + (f_0(z), \ldots, f_{m-1}(z))$$
$$= x\varphi - y\varphi + z\varphi = d_+(x\varphi, y\varphi, z\varphi).$$

Thus N is closed under d_+, and $(W; d_+)$ is a subdirect subalgebra of $(N; d_+)^m$ isomorphic to $(A; d_+)$ via φ.

Consider now any, say n-ary, fundamental operation g of $\mathbf{A}$. Since $\mathbf{A}$ is strongly Abelian, by tame congruence theory [6; Claim (3) in 5.6], the polynomial operations $f_i g$ $(0 \leq i \leq m-1)$ of $\mathbf{A}$ depend on at most one variable. Furthermore, they are constant or map onto N. Thus there exist mappings $\sigma\colon m \to m$, $\mu\colon m \to n$ such that

$$f_i g(x_0, \ldots, x_{n-1}) = g_i(f_{i\sigma}(x_{i\mu}))$$

with $g_i \in C_N \cup \{\mathrm{id}\}$ for all i $(0 \leq i \leq m-1)$. Hence for arbitrary elements $(f_0(x_j), \ldots, f_{m-1}(x_j)) \in W$ $(x_j \in A,\ 0 \leq j \leq n-1)$ we have

$$g((f_0(x_0), \ldots, f_{m-1}(x_0))\varphi^{-1}, \ldots, (f_0(x_{n-1}), \ldots, f_{m-1}(x_{n-1}))\varphi^{-1})$$

$$= g(x_0, \ldots, x_{n-1}) = (g(x_0, \ldots, x_{n-1})\varphi)\varphi^{-1}$$

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

$$= h^\sigma_\mu[g_0, \ldots, g_{m-1}]((f_0(x_0), \ldots, f_{m-1}(x_0)), \ldots, (f_0(x_{n-1}), \ldots, f_{m-1}(x_{n-1})))\varphi^{-1}.$$

This shows that if we make correspond to every basic operation g of $\mathbf{A}$ the operation $h^\sigma_\mu[g_0, \ldots, g_{m-1}]$ with σ, μ and $g_0, \ldots, g_{m-1}$ as described above, then φ is an isomorphism between $\mathbf{A} = (A; g, \ldots)$ and the subalgebra $\mathbf{W} = (W; h^\sigma_\mu[g_0, \ldots, g_{m-1}], \ldots)$ of a reduct of $(N; C_N)^{[m]}$. This proves Claim (a).

Claim (b). $|N| = 2$.

Let $|N| = t$. The elements of W will be written in the form $w = (w^0, \ldots, w^{m-1})$. Consider the following subset of W^t:

$$B = \{(w_0, \ldots, w_{t-1}) \in W^t\text{: for all } i \ (0 \leq i \leq m-1),$$
$$w^i_0, \ldots, w^i_{t-1} \text{ are not pairwise distinct}\}.$$

Clearly, B is totally reflexive and totally symmetric. Since W is a subdirect subset of N^m, therefore W has elements $v_0, \ldots, v_{t-1}$ such that $v^0_0, \ldots, v^0_{t-1}$ are pairwise distinct, and hence $(v_0, \ldots, v_{t-1}) \notin B$. Thus $B \neq W^t$. It is straightforward to check that B is a subuniverse of $\mathbf{W}^t$. In fact, if we apply a basic operation $h^\sigma_\mu[g_0, \ldots, g_{m-1}]$ of $\mathbf{W}$ to some elements $(w_{l,0}, \ldots, w_{l,t-1}) \in B$ $(l = 0, \ldots, n-1)$, then we get

$$((g_0(w^{0\sigma}_{0\mu,0}), \ldots, g_{m-1}(w^{(m-1)\sigma}_{(m-1)\mu,0})), \ldots, (g_0(w^{0\sigma}_{0\mu,t-1}), \ldots, g_{m-1}(w^{(m-1)\sigma}_{(m-1)\mu,t-1}))).$$

In view of $g_0, \ldots, g_{m-1} \in C_N \cup \{\mathrm{id}\}$, this clearly belongs to B. Since $\mathbf{A} \cong \mathbf{W}$, by the assumptions on $\mathbf{A}$ we conclude that $t = 2$, completing the proof of Claim (b).

Without loss of generality we identify $(N; d_+)$ with $(2; d_+)$, where $2 = \{0, 1\}$ and $+$ is addition modulo 2. Thus we get that for some integer $m \geq 1$, there exist a subdirect subalgebra $(W; d_+)$ of $(2; d_+)^m$ and an isomorphism $\varphi\colon (A; d_+) \to (W; d_+)$ which is simultaneously an isomorphism between $\mathbf{A}$ and the subalgebra $\mathbf{W}$ on W of a reduct of $(2; T_2)^{[m]}$. Assume m is chosen minimal with respect to the existence of such $\mathbf{W}$ and φ.

For $l = 0,1$ let $\bar{H}_l$ denote the family of all nonvoid subsets $I \subseteq m$ such that

$$\sum_{i \in I} w^i = l \quad \text{for all} \quad w = (w^0, \dots, w^{m-1}) \in W,$$

and put $\bar{H} = \bar{H}_0 \cup \bar{H}_1$. Since $(W; d_+)$ is a subalgebra of $(2; d_+)^m$ where $(2; d_+)$ is a simple idempotent Mal'tsev-algebra, it is not hard to show that these equalities determine W as follows (cf. [19; Lemma 4.4 and Remark on p. 98]):

$$W = \{(w^0, \dots, w^{m-1}) \in 2^m \colon \sum_{i \in I} w^i = l \text{ for all } I \in \bar{H}_l,\ l = 0,1\}.$$

Clearly, we have a similar description for all projections of W as well.

We are done if we prove that $\bar{H} = \emptyset$. Assume $\bar{H} \neq \emptyset$. Let H denote the set of minimal members of $\bar{H}$ (with respect to inclusion), and set $H_l = \bar{H}_l \cap H$ $(l = 0,1)$. Let $q = \min\{|I| \colon I \in H\}$. As W is a subdirect subset of 2^m, we have $q \geq 2$.

Notice that $\bar{H} \cup \{\emptyset\}$ is closed under symmetric difference. Indeed, if, say, $I \in \bar{H}_{l_I}$ and $J \in \bar{H}_{l_J}$, then

$$\sum_{i \in I} w^i = l_I \quad \text{and} \quad \sum_{j \in J} w^j = l_J \quad \text{for all} \quad w = (w^0, \dots, w^{m-1}) \in W,$$

implying that

$$\sum_{k \in (I \cup J) - (I \cap J)} w^k = \sum_{i \in I} w^i + \sum_{j \in J} w^j = l_I + l_J \quad \text{for all} \quad w = (w^0, \dots, w^{m-1}) \in W,$$

whence $(I \cup J) - (I \cap J) \in \bar{H}$.

Consequently, for arbitrary sets $I, J \in \bar{H}$ with $I \subset J$ we have $I, J - I \in \bar{H}$. This yields that every set in $\bar{H}$ is the disjoint union of sets in H. Thus

$$W = \{(w^0, \dots, w^{m-1}) \in 2^m \colon \sum_{i \in I} w^i = l \text{ for all } I \in H_l,\ l = 0,1\}.$$

Moreover, by the minimality of the members of H we get the following fact.

Claim (c). For arbitrary set $J \subseteq m$,

$$\operatorname{pr}_J W = 2^{|J|} \quad \text{if and only if} \quad I \not\subseteq J \quad \text{for all} \quad I \in H;$$

in particular,

$$\operatorname{pr}_J W = 2^{|J|} \quad \text{for all} \quad J \subseteq m \quad \text{with} \quad |J| < q.$$

We distinguish two cases.

CASE 1: $q > 2$. First we establish a property of the basic operations of $\mathbf{W}$.

Claim (d). Let $h = h_\mu^\sigma[g_0, \ldots, g_{m-1}]$ (with $\sigma\colon m \to m$, $\mu\colon m \to n$, $g_0, \ldots, g_{m-1} \in T_2$) be a basic operation of $\mathbf{W}$. Then for every set $I \in H$ with $|I| = q$, one of the following conditions holds:

(i) g_i is constant for some $i \in I$,

(ii) $g_i \in S_2$ for all $i \in I$, and there exist distinct indices $i, i' \in I$ with $i\mu = i'\mu$, $i\sigma = i'\sigma$,

(iii) $g_i \in S_2$ for all $i \in I$, μ is constant on I and $\{i\sigma\colon\ i \in I\}$ is a q-element set belonging to H.

Let $I \in H_l$, $|I| = q$, and assume (i), (ii) fail. Then $g_i(x) = x + c_i$ with $c_i \in 2$ for all $i \in I$. Furthermore, for arbitrary subset I' of I such that μ is constant on I', the elements $i\sigma$ $(i \in I')$ are pairwise distinct. As W is closed under h, we have

$$\text{(8)} \qquad \sum_{i \in I} (u_{i\mu}^{i\sigma} + c_i) = l \quad \text{for all} \quad u_j = (u_j^0, \ldots, u_j^{m-1}) \in W \ (0 \le j \le n-1).$$

Suppose μ is not constant on I. Then for arbitrary $r \in \{i\mu\colon\ i \in I\}$ we have that $|\{i \in I\colon\ i\mu = r\}| < q$ and the elements $i\sigma$ $(i \in I,\ i\mu = r)$ are pairwise distinct. Applying the second part of Claim (c) for the sets $J_r = \{i\sigma\colon\ i \in I, i\mu = r\}$ $(r \in \{i\mu\colon\ i \in I\})$ we get

$$\{(u_{i\mu}^{i\sigma})_{i \in I}\colon\ u_0, \ldots, u_{n-1} \in W\} = 2^{|I|},$$

contradicting (8). Thus μ is constant on I. It follows now that $|\{i\sigma\colon\ i \in I\}| = q$. Furthermore, by (8) we get that $\operatorname{pr}_{\{i\sigma\colon\ i \in I\}} W \neq 2^{|I|}$. By the first part of Claim (c) and by the minimality of q we conclude that $\{i\sigma\colon\ i \in I\} \in H$, completing the proof of Claim (d).

Now let $t = 2^{q-1}$ and define a subset B of W^t as follows:

$$B = \{(w_0, \ldots, w_{t-1}) \in W^t\colon \text{ for all } I \in H \text{ with } |I| = q,$$
$$\operatorname{pr}_I w_0, \ldots, \operatorname{pr}_I w_{t-1} \text{ are not pairwise distinct}\}.$$

Clearly, B is totally reflexive and totally symmetric. By the second part of Claim (c) we have $|\mathrm{pr}_I W| = 2^{q-1} = t$ for all $I \in H$ with $|I| = q$. Thus, for arbitrary fixed set $I_0 \in H$ with $|I_0| = q$ there exist elements $v_0, \ldots, v_{t-1} \in W$ such that $\mathrm{pr}_{I_0} v_0, \ldots, \mathrm{pr}_{I_0} v_{t-1}$ are pairwise distinct, yielding $(v_0, \ldots, v_{t-1}) \notin B$. Thus $B \neq W^t$. We prove that B is a subuniverse of $\mathbf{W}^t$. For arbitrary fundamental operation $h = h^\sigma_\mu[g_0, \ldots, g_{m-1}]$ ($\sigma\colon m \to m$, $\mu\colon m \to n$, $g_0, \ldots, g_{m-1} \in T_2$), and for arbitrary elements $(w_{l,0}, \ldots, w_{l,t-1}) \in B$ ($l = 0, \ldots, n-1$), the result of h on these elements is

$$(9) \qquad ((g_0(w^{0\sigma}_{0\mu,0}), \ldots, g_{m-1}(w^{(m-1)\sigma}_{(m-1)\mu,0})), \ldots, (g_0(w^{0\sigma}_{0\mu,t-1}), \ldots, g_{m-1}(w^{(m-1)\sigma}_{(m-1)\mu,t-1}))).$$

Let $I \in H$ with $|I| = q$. Note that $|\mathrm{pr}_I W| = 2^{q-1} = t$ and, in view of $q > 2$ and Claim (c), we have $\mathrm{pr}_{i,j} W = 2^2$ for all $i, j \in I$, $i \neq j$. Now apply Claim (d). In case (i) the projections of the t m-tuples in (9) to I cannot exhaust $\mathrm{pr}_I W$ (and hence are not pairwise distinct), because they have a constant coordinate. In the remaining cases let, say, $g_i(x) = x + c_i$ ($c_i \in 2$, $i \in I$). If (ii) holds, then again the projections of the t m-tuples in (9) to I cannot exhaust $\mathrm{pr}_I W$ (and hence are not pairwise distinct), because the i-th and i'-th coordinates sum up to the constant $c_i + c_{i'}$. Finally, in case (iii), the projections of the t m-tuples in (9) to I, equal, for some l ($0 \leq l \leq n-1$), the projections of the t m-tuples appearing in $(w_{l,0}, \ldots, w_{l,t-1})$ ($\in B$) to $\{i\sigma\colon\ i \in I\}$, with the constant tuple $(c_i)_{i \in I}$ added. Thus (9) belongs to B, proving that B is a subuniverse of $\mathbf{W}^t$. However, since $t = 2^{q-1} > 2$ and $\mathbf{W} \cong \mathbf{A}$, this contradicts our assumptions on $\mathbf{A}$.

CASE 2: $q = 2$. Since $\bar{H} \cup \{\emptyset\}$ is closed under symmetric difference, the relation $\equiv$ on m defined by

$$i \equiv j \quad \text{if and only if} \quad i = j \quad \text{or} \quad \{i, j\} \in H$$

is an equivalence relation. Let $B_0, \ldots, B_{s-1}$ be the blocks of $\equiv$, and assume without loss of generality that $i \in B_i$ ($0 \leq i \leq s-1$). Let $W' = \mathrm{pr}_{\{0,\ldots,s-1\}} W$, let π denote the projection mapping $W \to W'$, and let $\alpha\colon m \to s$ be defined by $i\alpha = j$ whenever $i \in B_j$. Then there exist elements $a_0 = \ldots = a_{s-1} = 0$ and $a_s, \ldots, a_{m-1} \in 2$ such that

$$W = \{(x^{0\alpha} + a_0, \ldots, x^{(s-1)\alpha} + a_{s-1}, x^{s\alpha} + a_s, \ldots, x^{(m-1)\alpha} + a_{m-1}\colon\ (x^0, \ldots, x^{s-1}) \in W'\}.$$

Obviously, π is an isomorphism $(W; d_+) \to (W'; d_+)$. For every basic operation $h = h^\sigma_\mu[g_0, \ldots, g_{m-1}]$ ($\sigma: m \to m$, $\mu: m \to n$, $g_0, \ldots, g_{m-1} \in T_2$), say $g_i(x) = \kappa_i x + c_i$ ($\kappa_i, c_i \in 2$, $0 \le i \le m-1$), and for arbitrary elements $w'_j = (w^0_j, \ldots, w^{s-1}_j) \in W'$ $(0 \le j \le n-1)$,

$$\begin{aligned} & h(w'_0\pi^{-1}, \ldots, w'_{n-1}\pi^{-1}) \\ &= h((w_0^{0\alpha} + a_0, \ldots, w_0^{(m-1)\alpha} + a_{m-1}), \ldots, (w_{n-1}^{0\alpha} + a_0, \ldots, w_{n-1}^{(m-1)\alpha} + a_{m-1})) \\ &= (\kappa_0(w_{0\mu}^{0\sigma\alpha} + a_{0\sigma}) + c_0, \ldots, \kappa_{m-1}(w_{(m-1)\mu}^{(m-1)\sigma\alpha} + a_{(m-1)\sigma}) + c_{m-1}) \\ &= (\kappa_0(w_{0\mu}^{0\sigma\alpha} + a_{0\sigma}) + c_0, \ldots, \kappa_{s-1}(w_{(s-1)\mu}^{(s-1)\sigma\alpha} + a_{(s-1)\sigma}) + c_{s-1})\pi^{-1} \\ &= h^\tau_\nu[f_0, \ldots, f_{s-1}](w'_0, \ldots, w'_{n-1})\pi^{-1} \end{aligned}$$

with $\tau = \sigma\alpha|_s: s \to s$, $\nu = \mu|_s: s \to n$ and $f_i(x) = \kappa_i(x + a_{i\sigma}) + c_i$ for all i $(0 \le i \le s-1)$. Thus the isomorphism $\varphi\pi: (A; d_+) \to (W'; d_+)$ is simultaneously an isomorphism between $\mathbf{A} = (A; g, \ldots)$ and the subalgebra $(W'; h^\tau_\nu[f_0, \ldots, f_{s-1}], \ldots)$ of a reduct of $(2; T_2)^{[s]}$. Clearly, $s < m$, since $H \neq \emptyset$. This contradicts the minimality of m, and completes the proof.

3. Proof of Theorem 1.3

First we introduce some notation that will be needed in the sequel. 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 coordinates according to π. For $n \ge 1$ and for an equivalence relation ε on n, put

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

These are called *diagonal relations*. The superscript is omitted if it is clear from the context. In the subscript it will often be more convenient to write, instead of ε, the list of nonsingleton blocks of ε; e.g. $\Delta^{(3)}_{01}$, $\Delta^{(4)}_{01|23}$, etc. Clearly $\Delta = \Delta^{(2)}_{01}$, and for ε the equality relation, $\Delta^{(n)}_\varepsilon = A^n$. With these notations one can easily see that an n-ary relation B on A is totally reflexive if and only if $\Delta^{(n)}_\varepsilon \subseteq B$ for every equivalence ε distinct from the equality relation, and totally symmetric if and only if $B^\pi \subseteq B$ for all $\pi \in S_n$.

For an algebra $\mathbf{A}$, a totally reflexive, totally symmetric subuniverse B of $\mathbf{A}^k$ will be called *trivial* if $B = A^k$ or (for $k = 2$) $B = \Delta$. Clearly, if $\mathbf{A}$ is finite and $k > |A|$, then every totally reflexive, totally symmetric subuniverse of $\mathbf{A}^k$ is trivial.

The proof of I. G. Rosenberg's primal algebra characterization theorem in [12] (see also [11]) yields the following fact.

LEMMA 3.1. [12] *Let $\mathbf{A}$ be a finite algebra. Assume some finite power $\mathbf{A}^k$ $(k \geq 1)$ of $\mathbf{A}$ has a nontrivial totally reflexive, totally symmetric subuniverse, and let k be the largest positive integer with this property. If B is a nontrivial totally reflexive, totally symmetric subuniverse of $\mathbf{A}^k$ and B is maximal with respect to inclusion, then B is either an equivalence relation, or a central relation, or a k-regular relation.*

The claims of the lemma below can be extracted from R. W. Quackenbush's proof for Rosenberg's primal algebra characterization theorem [11; Sections 4–6].

LEMMA 3.2. [11] *Let $\mathbf{A}$ be a finite algebra such that no finite power of $\mathbf{A}$ contains a nontrivial totally reflexive, totally symmetric subuniverse. Assume that some finite power $\mathbf{A}^m$ of $\mathbf{A}$ contains a subuniverse with cardinality not a power of $|A|$, and let m be the smallest positive integer with this property. If B is an arbitrary subuniverse of $\mathbf{A}^m$ such that $|B|$ is not a power of $|A|$, then $2 \leq m \leq 3$ and*

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

In particular,

(i) *if $m = 2$ and B is a maximal proper subuniverse of $\mathbf{A}^2$, then B is a bounded partial order, while*

(ii) *if $m = 3$ and $\Delta_{012} \subseteq B$, then for some permutation $\pi \in S_3$ we have $\Delta_{01} \cup \Delta_{02} \subseteq B^\pi$ and $\Delta_{12} \cap B^\pi = \Delta_{012}$, furthermore, there is an elementary Abelian 2-group $\widehat{A} = (A; +)$ such that $\mathbf{A}$ is semi-affine with respect to $\widehat{A}$.*

From Lemma 3.4 below it follows that the algebras described in Lemma 3.2 (ii) satisfy the assumptions of Theorem 2.1. For the proof we need a characterization of strongly Abelian algebras.

CLAIM 3.3. *An algebra* $\mathbf{A}$ *is strongly Abelian if and only if for all* $n \geq k \geq 1$, *for every* n*-ary term operation* f *of* $\mathbf{A}$ *and for arbitrary elements* $u_i, v_i \in A$ $(0 \leq i \leq k-1)$ *and* $a_j, b_j, c_j \in A$ $(k \leq j \leq n-1)$,

$$f(u_0, \ldots, u_{k-1}, a_k, \ldots, a_{n-1}) = f(v_0, \ldots, v_{k-1}, b_k, \ldots, b_{n-1})$$

implies

$$f(u_0, \ldots, u_{k-1}, c_k, \ldots, c_{n-1}) = f(v_0, \ldots, v_{k-1}, c_k, \ldots, c_{n-1}).$$

For $k = 1$ these implications are the same as in the definition, while for $k > 1$ they can be derived by induction.

LEMMA 3.4. *For an algebra* $\mathbf{A}$ *that is semi-affine with respect to an Abelian group* $\widehat{A}$, *the following conditions are equivalent:*

(i) $\mathbf{A}$ *is strongly Abelian,*

(ii) $\mathbf{A}^3$ *has a subuniverse* B *such that* $\Delta_{01} \cup \Delta_{02} \subseteq B$ *and* $\Delta_{12} \cap B = \Delta_{012}$.

Proof. (i)⇒(ii). Suppose $\mathbf{A}$ is strongly Abelian, and let B be the subuniverse of $\mathbf{A}^3$ generated by $\Delta_{01} \cup \Delta_{02}$. Hence B consists of all triples of the form

$$(f(a_0, \ldots, a_{k-1}, b_k, \ldots, b_{n-1}), f(a_0, \ldots, a_{k-1}, a_k, \ldots, a_{n-1}), f(b_0, \ldots, b_{k-1}, b_k, \ldots, b_{n-1}))$$

with $n \geq 1$, $0 \leq k \leq n$, f an n-ary term operation of $\mathbf{A}$ and $a_i, b_i \in A$ $(0 \leq i \leq n-1)$. If for an element of B the last two coordinates are equal, then all three coordinates are equal in view of Claim 3.3. Thus $\Delta_{12} \cap B \subseteq \Delta_{012}$, as required.

(ii)⇒(i). Assume (ii) holds and let f be an arbitrary term operation of $\mathbf{A}$; say f is n-ary. By Claim 1.1 (i)

$$f(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} r_i x_i + a \quad \text{for some} \quad n \geq 1,\ a \in A,\ r_0, \ldots, r_{n-1} \in \operatorname{End} \widehat{A}.$$

First we show that

$$\operatorname{Im} r_0 \cap \sum_{j=1}^{n-1} \operatorname{Im} r_j = \{0\}. \tag{7}$$

Consider an element $r_0a_0 = r_1a_1 + \ldots + r_{n-1}a_{n-1} \in \operatorname{Im} r_0 \cap \sum_{j=1}^{n-1} \operatorname{Im} r_j$. Since

$$(a_0, 0, a_0) \in B \quad \text{and} \quad (a_j, a_j, 0) \in B \quad \text{for all} \quad 0 < j \leq n-1,$$

therefore by applying f we get

$$(\sum_{j=0}^{n-1} r_ja_j + a,\ \sum_{j=1}^{n-1} r_ja_j + a,\ r_0a_0 + a) \in B.$$

The last two coordinates are equal by assumption, hence all coordinates are equal. Thus $r_0a_0 = 0$, proving (7).

Now, if $f(u, a_1, \ldots, a_{n-1}) = f(v, b_1, \ldots, b_{n-1})$ for some $u, v \in A$ and $a_j, b_j \in A$ $(1 \leq j \leq n-1)$, then $r_0(u - v) = \sum_{j=1}^{n-1} r_j(b_j - a_j)$, whence by (7) $r_0(u - v) = 0$, implying $f(u, c_1, \ldots, c_{n-1}) = f(v, c_1, \ldots, c_{n-1})$ for arbitrary elements $c_j \in A$ $(1 \leq j \leq n-1)$.

Combining the foregoing facts with a slight modification in the proof of [11; Proposition 6.1] to avoid ”falling back into class (2)”, we now complete the proof of Theorem 1.3.

Proof of Theorem 1.3. Let **A** satisfy the assumptions of the theorem. If some finite power of **A** contains a nontrivial totally reflexive, totally symmetric subuniverse, then by Lemma 3.1 and by the assumptions on **A** we have (d) or (e).

Assume now that no finite power of **A** contains a nontrivial totally reflexive, totally symmetric subuniverse, however, some finite power $\mathbf{A}^m$ of **A** contains a subuniverse with cardinality not a power of $|A|$. Let m be chosen minimal with this property. By Lemma 3.2 $m = 2$ or $m = 3$. If $m = 2$, Lemma 3.2 (i) immediately implies that (f) holds for **A**.

Suppose now that $m = 3$, and let B be a subuniverse of $\mathbf{A}^3$ such that $|B|$ is not a power of $|A|$. Define

$$C = \{(x, y)\colon\ (x, x, y) \in B\}.$$

Since $\operatorname{pr}_{0,1} B = A^2$, C is nonempty. Clearly, C is a subuniverse of $\mathbf{A}^2$. Since **A** has no proper subuniverse, $\operatorname{pr}_0 C = \operatorname{pr}_1 C = A$. By the minimality of m we have $|C| = |A|$ or $|C| = |A|^2$. In the latter case $C = A^2$ and $\Delta_{012} \subseteq B$. In the former case A has a permutation σ such that $C = \{(x, x\sigma)\colon\ x \in A\}$; in fact, σ is an automorphism of **A**. Thus

$$B' = \{(x, y, z) \in A^3\colon\ (x, y, z\sigma) \in B\}$$

is a subuniverse of $\mathbf{A}^3$ with $|B'| = |B|$ and $\Delta_{012} \subseteq B'$. Therefore $\mathbf{A}^3$ has a subuniverse satisfying the assumptions of Lemma 3.2 (ii), which together with Lemma 3.4 and Theorem 2.1 yields (c).

Finally, it remains to consider the case when each subuniverse of each finite power of $\mathbf{A}$ has cardinality a power of $|A|$. Then, by a result of R. W. Quackenbush [10] $\mathbf{A}$ generates a congruence permutable variety, and hence by a theorem of R. McKenzie [4] (cf. also [16], [2]) one of conditions (a), (b) holds for $\mathbf{A}$.

4. Some consequences

Now we look at some applications of Theorem 1.3. We specialize it to algebras whose fundamental operations are surjective or generate a variety satisfying a nontrivial congruence condition, and we get some functional completeness results as well.

An algebra $\mathbf{A}$ is said to be *functionally complete* if it is finite and every operation on A is a polynomial operation of $\mathbf{A}$. For an algebra $\mathbf{A}$, $V(\mathbf{A})$ will denote the variety generated by $\mathbf{A}$.

A. *Functionally complete algebras having no proper subalgebras*

Recently K. Kaarli [3] solved A. Foster's longstanding problem (see A. F. Pixley [7]) whether every functionally complete algebra $\mathbf{A}$ is categorical (i.e. $\mathbf{A}$ is the only subdirect irreducible in $V(\mathbf{A})$). He constructed an example showing that the answer is negative in general; however, what is more interesting, he proved that if the algebra $\mathbf{A}$ is assumed also to have no proper subalgebra, then the answer is affirmative, in fact $\mathbf{A}$ is quasiprimal.

None of the earlier Rosenberg-type completeness criteria were strong enough to imply this fact. Now Theorem 1.3 does the job.

COROLLARY 4.1. [3] *Every finite, functionally complete algebra having no proper subalgebra is quasiprimal.*

Proof. Let $\mathbf{A}$ be a finite algebra having no proper subalgebra, and assume $\mathbf{A}$ is functionally complete. Clearly, $\mathbf{A}$ is simple, therefore Theorem 1.3 applies. Since $\mathbf{A}$ is functionally complete, none of conditions (b)–(f) can hold for $\mathbf{A}$. Thus $\mathbf{A}$ is quasiprimal, as claimed.

B. *Surjective algebras*

We will call an algebra *surjective* if all its fundamental operations are surjective. The observation that for algebras with a single operation, or more generally, for surjective algebras, the family of “excluded relations” in the characterization of primality can be considerably reduced is due to G. Rousseau [15] and I. G. Rosenberg [13]. There are two facts underlying this phenomenon.

LEMMA 4.2. *Let $\mathbf{A}$ be a finite surjective algebra. If B is a subuniverse of $\mathbf{A}^n$ $(n \geq 1)$, then for arbitrary k $(0 \leq k \leq n-1)$,*

$$(B)_k = \{(x_0, \ldots, x_{k-1}) \in A^k\colon\ (x_0, \ldots, x_{n-1}) \in B \textit{ for all } x_k, \ldots, x_{n-1} \in A\}$$

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

The proof is straightforward. It is easy to see that for B a bounded partial order, $(B)_1$ is the singleton containing the least element, while for B a central relation, $(B)_1$ is the centre of B. Furthermore, for any k-regular family T of equivalence relations on A we have $(\lambda_T)_2 = \Theta_T$. Thus Lemma 4.2 immediately implies the following fact.

LEMMA 4.3. [15], [13] *Let $\mathbf{A}$ be a finite, simple, surjective algebra without proper subalgebras. Then*

(i) *there is no bounded partial order among the subuniverses of $\mathbf{A}^2$;*

(ii) *there is no central relation among the subuniverses of $\mathbf{A}^k$ for any k $(k \geq 2)$;*

(iii) *if λ_T is a subuniverse of $\mathbf{A}^k$ $(k \geq 3)$ for some k-regular family T of equivalences on A, then $\Theta_T = \Delta$.*

The second fact crucial in these considerations also originates from [15] and [13], though it was stated in a different terminology. It concerns the structure of surjective algebras admitting a k-regular relation λ_T with $\Theta_T = \Delta$.

LEMMA 4.4. [15], [13] *Let* $\mathbf{A}$ *be a finite surjective algebra. If, for some* $k \geq 3$, *there is a* k*-regular relation* λ_T *with* $|T| = m$ *and* $\Theta_T = \Delta$ *among the subuniverses of* $\mathbf{A}^k$, *then* $\mathbf{A}$ *is isomorphic to a reduct of* $(N; S_N)^{[m]}$ *for some* k*-element set* N.

Let us combine Lemmas 4.3, 4.4 with Theorem 1.3, and observe that in Theorem 1.3 (c) for every surjective operation $h^\sigma_\mu[g_0, \dots, g_{m-1}]$ of $(2; T_2)^{[m]}$ we have $g_0, \dots, g_{m-1} \in S_2$. Thus we get the corollary below, which includes as special cases the main results of [17] and [18].

COROLLARY 4.5. *Let* $\mathbf{A}$ *be a finite, simple, surjective algebra having no proper subalgebra. 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);*

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

In the context of tame congruence theory, Corollary 4.5 can be restated as follows:

Let $\mathbf{A}$ *be a finite, simple, surjective algebra having no proper subalgebra. If* $\mathbf{A}$ *is of type* **1**, *then* $\mathbf{A}$ *is isomorphic to a reduct of* $(N; S_N)^{[m]}$ *for a nonsingleton finite set* N *and some integer* $m \geq 1$; *if* $\mathbf{A}$ *is of type* **2**, *then* $\mathbf{A}$ *is affine, while if* $\mathbf{A}$ *is of type* **3**, *then* $\mathbf{A}$ *is quasiprimal.**

C. *Algebras in varieties satisfying a nontrivial congruence condition*

By a *congruence condition* we mean an inclusion $p \subseteq q$ where p, q are terms using the operation symbols $\vee$, $\wedge$, and $\circ$ (interpreted as join, meet, and relation product of congruences, respectively). A congruence condition is *satisfied* in a variety if it holds for arbitrary congruences of each algebra in the variety, and is called *trivial*, if it is satisfied in every variety.

* For type **2** this result was announced at the Conference on Universal Algebra and Lattice Theory in Charleston (1984), but the proof, different from the one presented here, remained unpublished.

It is well known that congruence conditions are closely related to Mal'tsev conditions. Recall that a *strong Mal'tsev condition* is a condition of the form

$$(\exists f_0, \ldots, f_{r-1})(e_0 \wedge \ldots \wedge e_{s-1})$$

with $e_0, \ldots, e_{s-1}$ identities in the function symbols $f_0, \ldots, f_{r-1}$, which is said to be *satisfied* in a variety V if V has terms $f_0, \ldots, f_{r-1}$ such that $e_0, \ldots, e_{s-1}$ hold in V. A *Mal'tsev condition* is a property of the form $(\exists n)\, U_n$ where all U_n $(n = 0, 1, 2, \ldots)$ are strong Mal'tsev conditions, and a *weak Mal'tsev condition* is a property of the form $(\forall k)(\exists n)\, U_{k,n}$ where all $(\exists n)\, U_{k,n}$ $(k = 0, 1, 2, \ldots)$ are Mal'tsev conditions. A strong (–, weak) Mal'tsev condition is called *idempotent* if its identities imply the idempotent law $f_i(x, \ldots, x) = x$ for every function symbol f_i occurring, and is called *linear*, if functions are not substituted into one another on either side of each identity in the condition. A strong (–, weak) Mal'tsev condition is said to be *trivial* if it is satisfied in every variety.

By a result of A. F. Pixley [9] and R. Wille [22] every congruence condition is equivalent to an idempotent, linear, weak Mal'tsev condition. Thus every variety satisfying a nontrivial congruence condition satisfies a nontrivial idempotent, linear Mal'tsev condition. It is worth mentioning, though will not be used here explicitly, that by tame congruence theory [6; Theorem 9.6], for locally finite varieties the converse also holds.

For a locally finite variety V the following conditions are equivalent:

(i) *V omits type* **1***;*

(ii) *V satisfies a nontrivial congruence condition;*

(iii) *V satisfies a nontrivial idempotent, linear Mal'tsev condition.*

We will need a special case of the easy direction (iii)⇒(i).

CLAIM 4.6. *If $\mathbf{A}$ is isomorphic to a reduct of $(N; T_N)^{[m]}$ for a nonsingleton finite set N and for some integer $m \geq 1$, then $V(\mathbf{A})$ satisfies no nontrivial idempotent, linear Mal'tsev condition.*

The reader not familiar with [6] can prove this claim directly, by observing that all idempotent operations of $(N; T_N)^{[m]}$ are of the form $h_\mu^{\mathrm{id}}[\mathrm{id}, \ldots .\mathrm{id}]$ $(\mu\colon m \to n)$, hence for arbitrary fixed element $c \in N$, they restrict to the set $N \times \{c\}^{m-1}$ as projection operations.

For finite algebras admitting a k-regular relation we have the same conclusion as in Claim 4.6 (cf. [14]).

LEMMA 4.7. *Let $\mathbf{A}$ be a finite algebra. If, for some $k \geq 3$, there is a k-regular relation among the subuniverses of $\mathbf{A}^k$, then $V(\mathbf{A})$ satisfies no nontrivial idempotent, linear Mal'tsev condition.*

Proof. Let $T = \{\Theta_0, \dots, \Theta_{m-1}\}$ $(m \geq 1)$ be a k-regular family of equivalence relations on A, and assume λ_T is a subuniverse of $\mathbf{A}^k$. Suppose a nontrivial idempotent, linear Mal'tsev condition witnessed by the terms $f_0, \dots, f_{r-1}$ holds in $V(\mathbf{A})$. Consider the reduct $\mathbf{A}' = (A;\ f_0, \dots, f_{r-1})$ of $\mathbf{A}$. Since the operations $f_0, \dots, f_{r-1}$ of $\mathbf{A}'$ are idempotent, $\mathbf{A}'$ is a surjective algebra. Obviously, λ_T is a subuniverse of $(\mathbf{A}')^k$ as well. Therefore by Lemma 4.2 we get that $\Theta_T = (\lambda_T)_2$ is a congruence of $\mathbf{A}'$.

Let $\mathbf{B} = \mathbf{A}'/\Theta_T$ and $\Phi_i = \Theta_i/\Theta_T$ $(i = 0, \dots, m-1)$. Clearly, $\mathbf{B}$ is a surjective algebra such that $V(\mathbf{B})$ satisfies the same nontrivial idempotent, linear Mal'tsev condition as $V(\mathbf{A})$. Moreover, $U = \{\Phi_0, \dots, \Phi_{m-1}\}$ is a k-regular family of equivalences on B with $\Phi_U = \Delta$ such that λ_U is a subuniverse of $\mathbf{B}^k$. Thus by Lemma 4.4 $\mathbf{B}$ is isomorphic to a reduct of $(N; T_N)^{[m]}$ for some k-element set N. This contradicts Claim 4.6, completing the proof.

Combining Theorem 1.3 with Claim 4.6 and Lemma 4.7 we get

COROLLARY 4.8. *Let $\mathbf{A}$ be a finite simple algebra having no proper subalgebra. If $V(\mathbf{A})$ satisfies a nontrivial congruence condition, 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);*

(e) *there is a central relation among the subuniverses of $\mathbf{A}^k$ for some $k \geq 2$;*

(f) *there is a bounded partial order among the subuniverses of $\mathbf{A}^2$.*

In particular, for surjective algebras we have

COROLLARY 4.9. *Let* $\mathbf{A}$ *be a finite, simple, surjective algebra having no proper subalgebra. If* $V(\mathbf{A})$ *satisfies a nontrivial congruence condition, then either*

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

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

D. *Functional completeness*

For an algebra $\mathbf{A} = (A; F)$ let $\bar{\mathbf{A}} = (A; F \cup C_A)$, that is, $\bar{\mathbf{A}}$ arises from $\mathbf{A}$ by adding all constants as fundamental operations. Clearly, for $\mathbf{A}$ finite, $\mathbf{A}$ is functionally complete iff $\bar{\mathbf{A}}$ is primal iff $\bar{\mathbf{A}}$ is quasiprimal (as $\bar{\mathbf{A}}$ has neither proper subalgebras nor nontrivial automorphisms).

Applying Theorem 1.3 for $\bar{\mathbf{A}}$ and some techniques from part B we get a slight improvement on I. G. Rosenberg's result [13] on the functional completeness of surjective algebras.

COROLLARY 4.10. *For a finite, simple, surjective algebra* $\mathbf{A}$ *one of the following conditions holds:*

(a)′ $\mathbf{A}$ *is functionally complete;*

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

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

(e)′ *there is a central relation among the subuniverses of* $\mathbf{A}^2$;

(f) *there is a bounded partial order among the subuniverses of* $\mathbf{A}^2$.

Proof. Clearly, (a) for $\bar{\mathbf{A}}$ implies (a)′, (b) for $\bar{\mathbf{A}}$ implies (b) (cf. Claim 1.1 (ii)), and (f) for $\bar{\mathbf{A}}$ implies (f). Furthermore, (c) for $\bar{\mathbf{A}}$ implies (c) for $\mathbf{A}$, and since $\mathbf{A}$ is surjective, we have (cd) with $|N| = 2$. If (e) holds for $\bar{\mathbf{A}}$, say B is a central relation among the subuniverses of $\bar{\mathbf{A}}^k$, then B is a subuniverse of $\mathbf{A}^k$ as well. Since $\mathbf{A}$ is surjective, Lemma 4.2 yields that $(B)_2$ is a subuniverse of $\mathbf{A}^2$. It is easy to see that $(B)_2$ is a central relation, whence (e)′ follows. Finally, assume (d) for $\bar{\mathbf{A}}$. Then (d) holds for $\mathbf{A}$ as well, so in the same way as in part B (using the simplicity of $\mathbf{A}$) we conclude that (cd) holds with $|N| \geq 3$.

An application of Corollary 4.8 for $\bar{\mathbf{A}}$ immediately implies

COROLLARY 4.11. *Let* $\mathbf{A}$ *be a finite simple algebra such that* $V(\mathbf{A})$ *satisfies a nontrivial congruence condition. Then one of the following conditions holds:*

(a)′ $\mathbf{A}$ *is functionally complete;*

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

(e) *there is a central relation among the subuniverses of* $\mathbf{A}^k$ *for some* $k \geq 2$*;*

(f) *there is a bounded partial order among the subuniverses of* $\mathbf{A}^2$.

Note that if $\mathbf{A}$ is, in addition, surjective, then (e) can be replaced by (e)′ (see Corollary 4.10). Corollary 4.11 is a common generalization of the well-known theorem of R. McKenzie [4] (see also H. P. Gumm [2]) concerning finite simple algebras $\mathbf{A}$ with $V(\mathbf{A})$ congruence permutable — when (e), (f) cannot occur —, and the main result of I. G. Rosenberg [14], where $V(\mathbf{A})$ is assumed to be congruence distributive.

E. *Concluding remarks*

1. Conditions (a)–(f) in Theorem 1.3 are independent in the sense that for each one of the six conditions there exists an algebra $\mathbf{A}$ satisfying the assumptions of the theorem for which that condition holds and none of the remaining ones do. For (a)–(b) and (d)–(f) this is easy and quite well known, while for condition (c) the matrix powers $(2; S_2)^{[m]}$ $(m \geq 1)$ are appropriate. Indeed, it is straightforward to check (cf. e.g. [21], [5]) that $\mathrm{Clo}\,(2; S_2)^{[m]}$ is generated by the m-ary operation $h^{\mathrm{id}}_{\mathrm{id}}[\mathrm{id}, \ldots, \mathrm{id}]$ and unary operations $h^{\gamma}_{m\to 1}[\mathrm{id}, \ldots, \mathrm{id}]$, $h^{\mathrm{id}}_{m\to 1}[\tau, \ldots, \tau]$ where γ is the cyclic permutation $(0\,1\,\ldots\,m-1)$ and τ is the transposition $(0\,1)$. Hence $(2; S_2)^{[m]}$ is term equivalent to a surjective algebra. Clearly, (c) holds while (a) and (b) fail for $(2; S_2)^{[m]}$. Since $(2; S_2)^{[m]}$ has cardinality 2^m and it has a term operation depending on m variables, therefore it cannot be isomorphic to a reduct of $(N; S_N)^{[m']}$ with $|N| > 2$, $m' \geq 1$. In view of Lemmas 4.3 and 4.4 the properties established so far for $(2; S_2)^{[m]}$ imply the failure of conditions (d)–(f) as well.

2. It is easy to see that if $\mathbf{A} = (A; f)$ is an algebra with a single fundamental operation and it has no proper subalgebra, then f is surjective. Thus Corollaries 4.5 and 4.9 hold

true for every finite simple algebra **A** with a single fundamental operation and with no proper subalgebra.

3. The results in Corollaries 4.5, 4.10 can be further improved: namely, finite simple algebras satisfying condition (cd) can be described more explicitly, up to term equivalence, which has interesting consequences, for instance, on minimal varieties. This will be discussed in another paper [20].

References

[1] C. Bergman, R. McKenzie, Minimal varieties and quasivarieties, *J. Austral. Math. Soc. (Ser. A)* **48** (1990), 133–147.

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

[3] K. Kaarli, On varieties generated by functionally complete algebras, *Algebra Universalis*, to appear.

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

[5] 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.

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

[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] A. F. Pixley, Local Mal'cev conditions, *Canad. Math. Bull.* **15** (1972), 559–568.

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

[11] R. W. Quackenbush, A new proof of Rosenberg's primal algebra characterization theorem, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam, 1981; pp. 603–634.

[12] 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.

[13] 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.

[14] I. G. Rosenberg, Functionally complete algebras in congruence distributive varieties, *Acta Sci. Math. (Szeged)* **43** (1981), 347–352.

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

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

[17] Á. Szendrei, Demi-primal algebras, *Algebra Universalis* **18** (1984), 117–128.

[18] Á. Szendrei, Demi-primal algebras with a single operation, in: *Lectures in Universal Algebra* (Proc. Conf. Szeged, 1983), Colloq. Math. Soc. J. Bolyai, vol. 43, North-Holland, Amsterdam, 1986; pp. 509–531.

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

[20] Á. Szendrei, Simple surjective algebras having no proper subalgebras, *J. Austral. Math. Soc. (Ser. A)* **48** (1990), 434–454.

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

[22] R. Wille, *Kongruenzklassengeometrien,* Lecture Notes in Math. 113, Springer-Verlag,

Berlin, 1970.

Bolyai Institute
Aradi vértanúk tere 1
6720 Szeged, Hungary