Acta Sci. Math., 49 (1985), 29—48

Submaximal clones with a prime order automorphism

I. G. ROSENBERG and Á. SZENDREI

1. Introduction

This research was done during the second author's stay at the Centre de recherche de mathématiques appliquées, Université de Montréal. The financial assistance provided by the NSERC Canada operating grant A-9128, and Ministère de l'Education du Québec, FCAR grant E-539 is gratefully acknowledged.

Let $\mathfrak{L}$ denote the lattice of clones over a finite set A, $|A|\geqq 3$. A clone $C\in\mathfrak{L}$ is called *submaximal* if it is covered by a maximal clone. Although the full list of maximal clones has been known for more than twenty years [14], [15], so far the submaximal clones have not been intensively studied, except for $|A|=3$. In that case all submaximal clones are known. The description was completed by D. LAU [8], making use of some earlier results [10], [3], [21] (also [1]) for the first three types of maximal clones (cf. Theorem 2.1 below). For arbitrary finite A, the first author started to investigate the maximal subclones of $\operatorname{Pol} B$ where $\emptyset\neq B\subset A$ [17]. D. LAU [9] found all maximal subclones of $\operatorname{Pol} B$ when $|B|=1$. Recently the second author determined the maximal subclones of $\operatorname{Pol} s^{\bullet}$ when $|A|$ is prime and s is a cyclic permutation of A [23]. The aim of this paper is to solve the corresponding problem in the general case, i.e., to determine all maximal subclones of $\operatorname{Pol} s^{\bullet}$ where s is a fixed point free permutation of A with $s^p=\mathrm{id}$ (p prime).

In general, the submaximal clones seem to be interesting for the following reasons. The largely unknown lattice $\mathfrak{L}$ has intervals with antichains of cardinality $2^{\aleph_0}$ situated far down from the top. It is not unreasonable to assume that $\mathfrak{L}$ is nicer near the top, and therefore the submaximal clones are good candidates. The problem of determining certain submaximal clones also came up in the second author's study of shortest maximal chains in $\mathfrak{L}$ [24]. Given a maximal clone M one can ask for a primality or completeness criterion for M: under what conditions does the clone $\bar{F}$ generated by some $F\subseteq M$ coincide with M? In case M is finitely

Received April 6, 1983.

generated, a full list of clones maximal in M would provide a general criterion, because then $\bar{F}=M$ if and only if F is contained in no clone maximal in M. An application could be a characterization of Sheffer operations for M (i.e., $f\in M$ such that $\overline{\{f\}}=M$). V. B. Kudrjavcev [7] and P. Schofield [22] proved that they exist exactly for maximal clones determined by permutations, equivalences, or unary relations (equivalently, these clones form a unique irredundant cover of the clone of all operations), but the examples provided have many variables. It would be interesting to have simple criteria of the type G. Rousseau [20] gave for $\mathcal{O}$, which, in its turn, could lead to the question: what is the minimum number of functional values whose knowledge can guarantee that an operation is Sheffer ($k+2$ for $\mathcal{O}$ [18])? Finally, the submaximal clones may be of interest on their own, e.g., as a source of examples and counter-examples.

2. Preliminaries and main result

Let A be a finite set, $|A|\geqq 2$. Denote by $\mathcal{O}$ the set of (finitary) operations on A. A *clone* over A is the set of polynomials [5] of some algebra with base set A, i.e., a subset of $\mathcal{O}$ containing the projections and closed with respect to superposition. It is well known that an operation is a polynomial of some algebra $(A;F)$ if and only if it preserves all subalgebras of finite powers of $(A;F)$. This permits one to describe clones by means of "invariant relations" in the following sense: Relations are simply subsets of finite powers of A; the subsets of A^h $(0<h<\aleph_0)$ are called h-ary relations. The set of relations is denoted by $\mathcal{R}$. An operation f is said to *preserve* an h-ary relation ϱ if ϱ is a subalgebra of $(A;f)^h$. For a set of relations $R\subseteqq\mathcal{R}$, let $\mathrm{Pol}\,R$ consist of all operations preserving every relation from R, and for $F\subseteqq\mathcal{O}$ let $\mathrm{Inv}\,F$ consist of all relations preserved by every operation from F. It is well known and easy to check that Pol and Inv determine a Galois connection between the subsets of $\mathcal{O}$ and $\mathcal{R}$, with closure operators $F\mapsto\mathrm{Pol}\,\mathrm{Inv}\,F$ on $\mathcal{O}$ and $R\mapsto[R]=\mathrm{Inv}\,\mathrm{Pol}\,R$ on $\mathcal{R}$. In view of the above remark the closed sets of operations are exactly the clones. The closed sets of relations are called *relational algebras* [11, 1.1.8]. The set of relational algebras, ordered by inclusion, is a lattice $\mathfrak{L}^*$, which is dually isomorphic to the lattice $\mathfrak{L}$ of clones on A (the mutually inverse dual isomorphisms are $R\mapsto\mathrm{Pol}\,R$ and $F\mapsto\mathrm{Inv}\,F$).

The relational algebras $[R]$ can be described in various ways [2], [4], [11], but for our purposes we shall use the following [11, 2.1]: an h-ary relation ϱ belongs to $[R]$ if and only if there exists a first order formula $\Phi(x_0, \dots, x_{h-1})$ (with free variables $x_0, \dots, x_{h-1}$) built up from $\exists$, $\wedge$ and relation symbols from $R\cup\{=\}$ such that

$$\varrho = \{(a_0, \dots, a_{h-1})\in A^h\colon\ \Phi(a_0, \dots, a_{h-1})\ \text{ holds true}\}.$$

Simple but useful special cases are, for example, the direct product of relations, the relational product ($\circ$) of two binary relations, the intersection of relations of the same arity, the permutation of the components of a relation, in particular, taking the inverse ($^{-1}$) of a binary relation, or the projection of a relation onto some of its components, e.g., taking the domain (i.e., first projection) or range (second projection) of a binary relation.

It is well known [11, 4.1.3] that the lattice of clones over A is dually atomic and has a finite number of dual atoms, which are termed *maximal clones*. We shall need their explicit description found in [14], [15] (see also [11, 5.2.2], [12]), therefore we recall some definitions.

To every, say n-ary, operation f we can associate the $(n+1)$-ary relation $f^{\bullet}$ consisting of all $(n+1)$-tuples $(a_0, \ldots, a_{n-1}, f(a_0, \ldots, a_{n-1}))$ with $a_0, \ldots, a_{n-1} \in A$. For $F \subseteq \mathcal{O}$ we set $F^{\bullet} = \{f^{\bullet}: f \in F\}$. If $(A; +)$ is an abelian group, the quaternary relation $(x_0 - x_1 + x_2)^{\bullet}$ is referred to as the *affine relation* determined by $(A; +)$. An h-ary relation ϱ is called *central* if $\varrho \neq A^h$, ϱ is totally reflexive (i.e., contains all h-tuples having repeated components), totally symmetric (i.e., invariant under all permutations of components), and the *center* $\{a \in A: \{a\} \times A^{h-1} \subseteq \varrho\}$ of ϱ is nonempty. A family $T = \{\vartheta_0, \ldots, \vartheta_{m-1}\}$ of equivalence relations on A is said to be h-regular, if each ϑ_i $(0 \leqq i < m)$ has $h (\geqq 3)$ blocks, and $\bigcap (B_i: 0 \leqq i < m)$ is nonempty for arbitrary blocks B_i of ϑ_i $(0 \leqq i < m)$. The relation λ_T determined by T consists of all h-tuples whose components meet at most $h-1$ blocks of each ϑ_i $(0 \leqq i < m)$. The relations of the form λ_T will be called *regular* (or *h-regular*, where h is the arity). The equality relation, denoted ω, and the full relation A^2 on A are termed *trivial* equivalence relations.

Theorem 2.1 ([14], [15]). *Let A be a finite set, $|A| \geqq 2$. The maximal clones on A are the clones* Pol ϱ *where ϱ is one of the following relations*:

(O) *a bounded order,*

(P) *a relation $g^{\bullet}$ where g is a fixed point free permutation with $g^p = \mathrm{id}$ (p prime),*

(A) *an affine relation determined by an elementary abelian p-group (p prime),*

(E) *a nontrivial equivalence relation,*

(C) *a central relation,*

(R) *a regular relation.*

These relations will be called *atomic*. In view of the dual isomorphism between the lattices of clones and relational algebras, it is clear that the atomic relations are the generators of the atoms in the lattice of relational algebras.

The aim of this paper is to describe the maximal subclones of Pol $s^{\bullet}$ where $s^{\bullet}$ is an atomic relation of type (P), $s^p = \mathrm{id}$. For the formulation of the main theorem we introduce some notation and definitions. Denote by Θ the equivalence relation consisting of all pairs $(a, b) \in A^2$ with $a = s^i(b)$ for some $0 \leqq i < p$. An h-ary relation ϱ will be termed *Θ-closed* if $(b_0, ..., b_{h-1}) \in \varrho$ whenever $(a_0, ..., a_{h-1}) \in \varrho$ and $(a_i, b_i) \in \Theta$ for all $0 \leqq i < h$. In other words, ϱ Θ-closed means that ϱ is the full inverse image of a relation on the quotient set A/Θ (consisting of the blocks of Θ) under the natural mapping $A \to A/\Theta$ sending every $a \in A$ into the block containing it. In particular,

(a) an equivalence relation ϱ is Θ-closed if and only if $\Theta \subseteq \varrho$,

(b) a regular relation λ_T with $T = \{\vartheta_0, ..., \vartheta_{m-1}\}$ is Θ-closed if and only if $\Theta \subseteq \vartheta_0 \cap ... \cap \vartheta_{m-1}$, and

(c) a central relation is Θ-closed if and only if it is the inverse image of a central relation on A/Θ.

An equivalence relation ε will be called *transversal to s* if $s \in \mathrm{Pol}\, \varepsilon$ and $\varepsilon \cap \Theta = \omega$, i.e., s maps each block of ε onto another block of ε. A unary relation μ is *transversal to s* if $(\mu \times \mu) \cap \Theta \subseteq \omega$, i.e., $s^i(x) \notin \mu$ whenever $x \in \mu$, $1 \leqq i < p$.

In order to determine one type of maximal subclones of $\mathrm{Pol}\, s^\cdot$ we need a result from group theory. For two primes q, r such that $q^n \equiv 1 \pmod r$ and n is the least positive integer with this property, we denote by $\mathfrak{G}(q, r)$ the group of linear functions $ax+b$ on $GF(q^n)$ with $a, b \in GF(q^n)$ and $a^r = 1$. Clearly, $|\mathfrak{G}(q, r)| = q^n r$.

Responding to our inquiry, P. P. Pálfy proved the following fact:

Proposition 2.2. *A finite group has a maximal subgroup of order p (p prime) if and only if it is isomorphic to one of the groups listed below:*

(i) *an abelian group of order pq (q prime),*

(ii) $\mathfrak{G}(p, q)$ *for a prime q with* $p \equiv 1 \pmod q$,

(iii) $\mathfrak{G}(q, p)$ *for a prime* $q \neq p$.

Proof. The sufficiency being obvious, take a finite group $\mathfrak{G}$ which has a maximal subgroup $\mathfrak{H}$ with $|\mathfrak{H}| = p$. To show that $\mathfrak{G}$ is isomorphic to one of the groups (i)—(iii) the only nontrivial case to consider is $|\mathfrak{G}| = pn$ with n composite and $n \not\equiv 0 \pmod p$. Then $\mathfrak{H}$ is not normal, implying by the maximality of $\mathfrak{H}$ that $\mathfrak{H}$ coincides with its normalizer. Hence $\mathfrak{G}$ is a Frobenius group to $\mathfrak{H}$ [6, V.8.1]. Moreover, again by the maximality of $\mathfrak{H}$, the usual permutation representation of $\mathfrak{G}$ [6, V.8.2] is primitive, yielding that the Frobenius kernel of $\mathfrak{G}$ is elementary abelian [6, V.8.19]. Now it is easy to see that every proper subgroup of $\mathfrak{G}$ is abelian, and hence our statement follows from [13, Satz 4].

Now we define permutation groups on A as follows. For a group $\mathfrak{G}$ whose order divides $|A|$, consider a partition of A into $|\mathfrak{G}|$-element blocks $A_0, ..., A_{l-1}$ $(l|\mathfrak{G}| = |A|)$, and select arbitrary bijections $\varphi_i\colon A_i \to \mathfrak{G}$ $(0 \leqq i < l)$. Clearly, the permutations π_g $(g \in \mathfrak{G})$ of A defined by $\pi_g(x) = \varphi_i^{-1}(g \cdot \varphi_i(x))$ for every $0 \leqq i < l$ and $x \in A_i$ form a group, which will be called a *semiregular representation of* $\mathfrak{G}$

on A. (Note that a semiregular representation of $\mathfrak{G}$ on A exists only if $|\mathfrak{G}|$ divides $|A|$.)

After these preparations we are in a position to state our main result:

Theorem 2.3. *Let* A *be a finite set,* $|A| \geqq 2$, *and let* s *be a fixed point free permutation of* A *with* $s^p = \mathrm{id}$ *(*p *prime). Then the maximal subclones of* $\mathrm{Pol}\, s^{\bullet}$ *are the clones* $\mathrm{Pol}\,\{s^{\bullet}, \varrho\}$ *where* ϱ *is one of the following relations:*

(P_s) *a relation* $g^{\bullet}$ *such that* g *is a permutation of* A *and* $\{s, g\}$ *generates a semiregular representation of a group from Proposition 2.2,*

(A_s) *an affine relation determined by an elementary abelian* p*-group* $(A; +)$ *such that there exists an element* $c \in A$ *with* $s(x) = x + c$ *for every* $x \in A$,

(E_s) *a nontrivial equivalence relation that is either* Θ*-closed or transversal to* s,

(C_s) *a* Θ*-closed central relation or a nonempty unary relation transversal to* s,

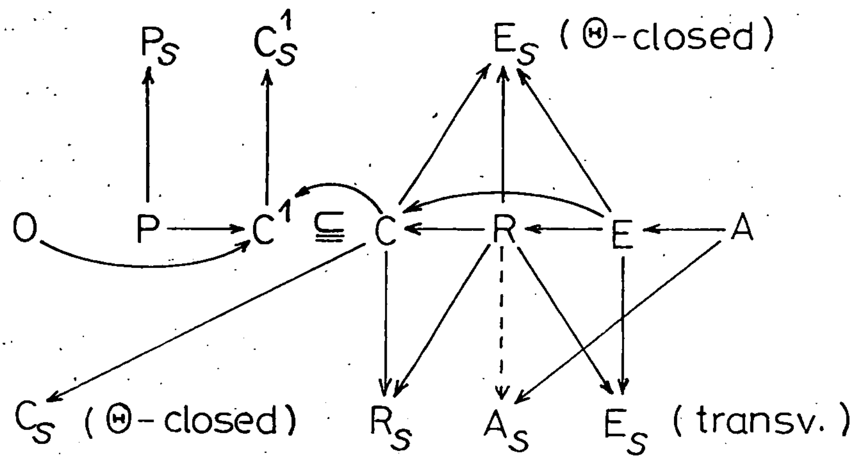
(R_s) *a* Θ*-closed regular relation.*

Corollary 2.4. *An algebra* $(A; F)$ *admitting* s *as an automorphism is polynomially equivalent to* $(A;\ \mathrm{Pol}\, s^{\bullet})$ *if and only if none of the relations* (P_s)—(R_s) *occurs among the subalgebras of finite powers of* $(A; F)$.

The proof of Theorem 2.3 naturally splits into two parts: one has to verify on the one hand that the clones listed in the theorem are indeed maximal in $\mathrm{Pol}\, s^{\bullet}$, and on the other hand, that the list is complete, i.e., all maximal subclones are found. Since $\mathrm{Pol}\, s^{\bullet}$ is finitely generated [11, 4.3.26] and hence the lattice of its subclones is dually atomic, the latter is equivalent to showing that every proper subclone of $\mathrm{Pol}\, s^{\bullet}$ is contained in $\mathrm{Pol}\,\{s^{\bullet}, \varrho\}$ for some relation ϱ listed in Theorem 2.3. In terms of relational algebras this statement can be formulated as follows:

Theorem 2.5. *Let* A *be a finite set,* $|A| \geqq 2$, *and let* s *be a fixed point free permutation of* A *with* $s^p = \mathrm{id}$ *(*p *prime). Then every relational algebra properly including* $[s^{\bullet}]$ *contains a relation of one of the types* (P_s)—(R_s).

The detailed (and rather lengthy) proof of Theorem 2.5 will be presented in the next section. Here we sketch only the main idea. The first step is to observe that any relational algebra properly including $[s^{\bullet}]$ contains either an atomic relation outside $[s^{\bullet}]$, or a relation $g^{\bullet}$ of type (P_s) such that $g^p = s$ (see Proposition 3.3), which explains also the surprising similarity between Theorems 2.1 and 2.3. Therefore in the rest of the proof it suffices to show for each type of atomic relation $\varrho \notin [s^{\bullet}]$, that $[s^{\bullet}, \varrho]$ contains a relation listed in Theorem 2.3. The proof will be constructive, the steps being illustrated by the arrows in the diagram below, except for one case (dotted arrow) when we use an argument for the operations preserving the relations in question (see Lemma 3.13 and Remark 2 after it).



Here C^1 and C_s^1 denote the unary relations of types C and C_s, respectively.

The maximality of the clones Pol $\{s^{\bullet}, \varrho\}$ in Pol $s^{\bullet}$ if ϱ runs over the relations (P_s)—(R_s) will be proved in Section 4. In the language of relational algebras this part of Theorem 2.3 has the following reformulation:

Theorem 2.6. *Let A be a finite set, $|A|\geqq 2$, and let s be a fixed point free permutation of A with $s^p=\mathrm{id}$ (p prime). Then for every relation ϱ of type* (P_s)—(R_s) *the relational algebra* $[s^{\bullet}, \varrho]$ *covers* $[s^{\bullet}]$.

3. Proof of Theorem 2.5

First we introduce some notation. For a positive integer n, $\mathbf{n}$ will denote the set $\{0, \ldots, n-1\}$. We can assume without loss of generality that $A=\mathbf{k}$ (hence p divides k) and the cycles of s are $(tp, tp+1, \ldots, tp+p-1)$, $0\leqq t<k/p$. It will be convenient to write $x\oplus i$ and $x\ominus i$ instead of $s^i(x)$ and $s^{p-i}(x)$, respectively ($x\in\mathbf{k}$, $i\in\mathbf{p}$). In particular, restricted to $\mathbf{p}$, $\oplus$ and $\ominus$ are addition and subtraction modulo p. For an h-ary relation ϱ and $c=(c_0, \ldots, c_{h-1})\in\mathbf{p}^h$ we will denote by $\varrho\oplus c$ the relation consisting of all h-tuples $(a_0\oplus c_0, \ldots, a_{h-1}\oplus c_{h-1})$ with $(a_0, \ldots, a_{h-1})\in\varrho$. The following is obvious:

Lemma 3.1. *For every h-ary relation ϱ and $c\in\mathbf{p}^h$ we have* $[\varrho\oplus c, s^{\bullet}]=[\varrho, s^{\bullet}]$.

To check whether a relation belongs to $[s^{\bullet}]$ or not, we shall often need an explicit description of the members of $[s^{\bullet}]$. For later applications we formulate a slightly more general statement.

Lemma 3.2. *Let G be a permutation group on $\mathbf{k}$ in which no nonidentity permutation has fixed points. Then, up to a rearrangement of its components, every nonvoid* *member of* $[G^\bullet]$ *is a direct product of relations of the form*

(1) $$\{(a, g_1(a), \ldots, g_{h-1}(a)) \colon a \in \mathbf{k}\}$$

with $h \geqq 1$ *and* $g_1, \ldots, g_{h-1} \in G$.

Proof. Let $\varrho \in [G^\bullet]$, $\varrho \neq \emptyset$, say ϱ is n-ary, and consider a formula $\Phi(x_0, \ldots, x_{n-1})$ with bound variables $x_n, \ldots, x_{m-1}$ $(m \geqq n)$, which defines ϱ. Since G consists of permutations, the matrix of Φ is essentially a set of equations of the form $x_j = g(x_i)$ with $0 \leqq i, j < m$ and $g \in G$. Let $\sim$ denote the least equivalence relation on $\{x_0, \ldots, x_{m-1}\}$ containing all such pairs (x_i, x_j). Then $\Phi(x_0, \ldots, x_{m-1})$ can be split into the conjunction of its "subformulas" $\Phi_B(x_i \colon i < n,\ x_i \in B)$ corresponding to the $\sim$-blocks B. Clearly, up to the order of its components, ϱ is the direct product of the relations determined by Φ_B. Moreover, each Φ_B defines a relation of the form (1), since the assumption on G and $\varrho \neq \emptyset$ imply that for any $i, j \in B$ there is exactly one $g \in G$ with $x_j = g(x_i)$.

In the special case when $G = \{\mathrm{id}\}$, the relations described in Lemma 3.2 are the so called *diagonal relations*. The members of $[\omega] = [\mathrm{id}^\bullet]$, i.e., the relations which are empty or diagonal are termed *trivial relations*. Clearly, a relation is trivial if and only if it is preserved by every operation.

Now we can prove that "almost all" relational algebras properly including $[s^\bullet]$ contain an atomic relation outside $[s^\bullet]$.

Proposition 3.3. *Let R be a relational algebra such that* $R \supset [s^\bullet]$, *and every atomic relation in R belongs to* $[s^\bullet]$. *Then R contains a relation* $g^\bullet$ *for some permutation g with* $g^p = s$.

Proof. We will need the following property of R.

Claim. An h-ary $(h \geqq 1)$ relation $\xi \in R$ is diagonal whenever it contains an h-tuple $(a, \ldots, a)$ for some $a \in \mathbf{k}$. In particular, every nontrivial binary relation $\beta \in R$ is irreflexive (i.e., $\beta \cap \omega = \emptyset$).

To prove the claim assume $(a, \ldots, a) \in \xi$ $(a \in \mathbf{k})$. It is easy to see that this implies $(a, \ldots, a) \in \xi'$ for all $\xi' \in [\xi]$. Therefore $[\xi]$, and hence also $R(\supseteq [\xi])$, contains an atomic relation with the same property, unless ξ is diagonal. This shows that ξ is diagonal, as stated.

Now let $\varrho \in R \setminus [s^\bullet]$ be of minimum arity, say t. We prove that $t=2$. Clearly, $t \geqq 2$ since otherwise ϱ would be a nontrivial unary relation, and hence would be atomic. Suppose $t > 2$ and let ϱ' denote the projection of ϱ onto its first $t-1$ components. By the minimality of t and $\varrho' \in [\varrho]$ it follows that $\varrho' \in [s^\bullet]$. Applying Lemma 3.2 for the permutation group generated by s we get that either $\varrho' = \mathbf{k}^{t-1}$, or ϱ' (and hence also ϱ) has a binary projection, say onto the i-th and j-th components $(0 \leqq i < j < t-1)$, which is of the form $(s^l)^\bullet$ for some $0 \leqq l < p$. In the latter case ϱ

belongs to the relational algebra generated by $s^{\bullet}$ and the $(t-1)$-ary projection of ϱ omitting the j-th component. However, in view of the minimality of t, both of these relations belong to $[s^{\bullet}]$, yielding $\varrho\in[s^{\bullet}]$. This contradiction shows that $\varrho'=\mathbf{k}^{t-1}$. Hence we have $(0, \ldots, 0, u)\in\varrho$ for some $u\in\mathbf{k}$. By the minimality of t, the binary relation $\eta\in[\varrho]$ consisting of all pairs $(a, b)\in\mathbf{k}^2$ with $(a, \ldots, a, b)\in\varrho$ belongs to $[s^{\bullet}]$. Clearly, $\eta\neq\emptyset$, therefore u can be chosen so that $u\in\mathbf{p}$. Set $d=(0, \ldots, 0, \ominus u)$, and form $\varrho\oplus d$. Obviously, $(0, \ldots, 0)\in\varrho\oplus d\in R$ and, by Lemma 3.1, $\varrho\oplus d$ is not diagonal. This contradiction proves that $t=2$, i.e., ϱ is binary.

Now form the relation $\sigma=\varrho\circ\varrho^{-1}\in[\varrho]$. Clearly, σ is reflexive $(\omega\subseteq\sigma)$, since the domain and range of ϱ equal $\mathbf{k}$. Hence σ is diagonal. Suppose $\sigma=\mathbf{k}^2$. We prove by induction on $2\leqq n\leqq k$ that for each n-element subset $\{a_0, \ldots, a_{n-1}\}$ of $\mathbf{k}$ there is an element $b\in\mathbf{k}$ such that $(a_i, b)\in\varrho$ for all $0\leqq i<n$. By assumption this holds for $n=2$. Suppose it is true for some $2\leqq h<k$, and take the relation

$$\tau = \{(a_0, \ldots, a_h)\colon (a_0, b), \ldots, (a_h, b)\in\varrho \quad \text{for some} \quad b\in\mathbf{k}\}.$$

By construction $\tau\in[\varrho]$, and by the inductive assumption τ is totally reflexive. Thus τ is diagonal. Hence, in view of $h\geqq 2$, $\tau=\mathbf{k}^{h+1}$. This concludes the proof by induction. In particular, for $n=k$ we obtain that there is an element e such that $(a, e)\in\varrho$ for each $a\in\mathbf{k}$. Then $(e, e)\in\varrho$, contradicting the irreflexivity of ϱ.

Thus $\sigma=\varrho\circ\varrho^{-1}=\omega$. A similar argument for ϱ^{-1} yields $\varrho^{-1}\circ\varrho=\omega$, whence we get that $\varrho=f^{\bullet}$ for a permutation f of $\mathbf{k}$. Let m be the least positive integer with $f^m=\mathrm{id}$. It is easy to see that R contains all powers $(f^l)^{\bullet}=f^{\bullet}\circ\ldots\circ f^{\bullet}$ $(0\leqq l<m)$ of $f^{\bullet}$. Thus from the assumptions that $f^{\bullet}\notin[s^{\bullet}]$ and every atomic relation in R belongs to $[s^{\bullet}]$, we get that the nonidentity powers of f are fixed point free, $m>p$ is a power of p, and $(f^{m/p})^{\bullet}\in[s^{\bullet}]$. Therefore some power g of $f^{m/p}$ has the required property $g^p=s$.

From now on we can assume that $R\setminus[s^{\bullet}]$ contains an atomic relation ϱ. Clearly, it suffices to prove the assertion of Theorem 2.5 for the relational algebra $[s^{\bullet}, \varrho]$. The various types of atomic relations will be considered separately.

Proposition 3.4. *For a nontrivial unary relation γ the relational algebra $[s^{\bullet}, \gamma]$ contains a nontrivial Θ-closed unary relation, or a nonempty unary relation transversal to s.*

Proof. Consider a nontrivial unary relation $\mu\in[s^{\bullet}, \gamma]$ of least possible size, and set $\mu_i=\mu\oplus i$ for $0<i<p$. Clearly, for each $0<i<p$ the relation $\mu\cap\mu_i$ belongs to $[s^{\bullet}, \gamma]$, and therefore, by the minimality, it is either μ or $\emptyset$. Since p is prime, μ is Θ-closed whenever $\mu\cap\mu_i=\mu$ for some $0<i<p$. If $\mu\cap\mu_1=\ldots=\mu\cap\mu_{p-1}=\emptyset$, then μ is transversal to s.

Proposition 3.5. *For a bounded order* $\leqq$ *the relational algebra* $[s^{\bullet}, \leqq]$ *contains a nontrivial unary relation.*

Proof. Let o and e be the least and greatest elements of $\leqq$. Set $\gamma = \{a \in \mathbf{k}\colon a \leqq (a \oplus 1)\}$. Obviously, $o \in \gamma$ and $e \notin \gamma$, showing that $\gamma \in [s^{\bullet}, \leqq]$ is nontrivial.

Proposition 3.6. *Let f be a fixed point free permutation with* $f^q = \mathrm{id}$ *(q prime) such that* $f^{\bullet} \notin [s^{\bullet}]$. *Then the relational algebra* $[s^{\bullet}, f^{\bullet}]$ *contains either a nontrivial unary relation, or a binary relation* $g^{\bullet}$ *for some permutation g which together with s generates a semiregular representation of a group from Proposition 2.2.*

Proof. Denote by G the permutation group generated by s and f, and by S its subgroup generated by s. It is easy to see that the set of fixed points of each $g \in G$ belongs to $[s^{\bullet}, f^{\bullet}]$. Thus $[s^{\bullet}, f^{\bullet}]$ contains a nontrivial unary relation unless every nonidentity permutation from G is fixed point free. In that case consider a subgroup H of G properly containing S, and minimal with respect to this property. Clearly, S is a maximal subgroup of H. Thus H is a semiregular representation of a group $\mathfrak{H}$ which has a maximal subgroup of order p, i.e., $\mathfrak{H}$ is one of the groups listed in Proposition 2.2. It is easy to see that all relations $g^{\bullet} \in H^{\bullet} \setminus S^{\bullet} (\subseteq [s^{\bullet}, f^{\bullet}])$ meet the requirements.

When considering central relations and regular relations we will often use the following general result on Θ-closed relations:

Lemma 3.7. *Let Γ be a set of Θ-closed relations and let* $\sigma \in [\Gamma]$. *If the full relation is the single diagonal relation containing* σ, *then* σ *is* Θ*-closed.*

Proof. Consider a formula $\Phi(x_0, \dots, x_{h-1})$ with bound variables $x_h, \dots, x_{m-1}$ defining σ. Since there is no forcible repetition among the coordinates of σ, we may assume that the matrix of Φ contains no condition of the form $x_i = x_j$ (such conditions with at least one bound variable can be easily eliminated). Thus the matrix of Φ consists of conditions $(x_{i_0}, \dots, x_{i_{t-1}}) \in \varrho$ with $\varrho \in \Gamma$. All $\varrho \in \Gamma$ being Θ-closed, this implies that σ is also Θ-closed.

Proposition 3.8. *For an at least binary central relation* γ *the relational algebra* $[s^{\bullet}, \gamma]$ *contains one of the following relations: a nontrivial unary relation, a nontrivial* Θ*-closed equivalence relation, a* Θ*-closed central relation, or a* Θ*-closed regular relation.*

Proof. Let σ be a central relation from $[s^{\bullet}, \gamma]$ of least possible arity, say h. If $h = 1$, we are done. Now assume $h \geqq 2$, and define an $(h-1)$-ary relation $\sigma^* \in [s^{\bullet}, \gamma]$ to consist of all $(a_0, \dots, a_{h-2}) \in \mathbf{k}^{h-1}$ such that $(a_0, \dots, a_l, a_l \oplus i, a_{l+1}, \dots, a_{h-2}) \in \sigma$ for all $0 \leqq i < p$ and $0 \leqq l < h-1$. It is easy to see that σ^* inherits total reflexivity and total symmetry from σ. Moreover, σ^* contains every $(h-1)$-tuple with one component in the center of σ. Since σ^* is not a central relation (by the choice of σ), we get that $\sigma^*=\mathbf{k}^{h-1}$.

Denote by τ the h-ary relation consisting of all $(a_0, \ldots, a_{h-1})\in\mathbf{k}^h$ with $(a_0\oplus i_0, \ldots, a_{h-1}\oplus i_{h-1})\in\sigma$ for all $0\leqq i_0, \ldots, i_{h-1}<p$. The construction of τ and the total symmetry of σ guarantee that τ is also totally symmetric. Using $\sigma^*=\mathbf{k}^{h-1}$ it is easy to show that τ is totally reflexive. Finally, τ is a subrelation of σ, and is clearly Θ-closed. Consequently τ is nontrivial, so $[\tau]$ contains an atomic relation. By Lemma 3.7 this atomic relation is Θ-closed, hence it is either an equivalence relation, or a central relation, or a regular relation.

We now turn to the most sophisticated case, when ϱ is a regular relation. Our departure point is

Lemma 3.9. *For an h-regular relation ϱ the relational algebra $[s^{\cdot}, \varrho]$ contains either a central relation or a regular relation σ such that $s\in\operatorname{Pol}\sigma$.*

Proof. Form the relation $\tau\in[s^{\cdot}, \varrho]$ consisting of all $(a_0, \ldots, a_{h-1})\in\mathbf{k}^h$ with $(a_0\oplus i, \ldots, a_{h-1}\oplus i)\in\varrho$ for every $0\leqq i<p$. Clearly, $\tau\subseteq\varrho$ is totally reflexive and symmetric. Thus, in view of $h\geqq 3$, the relation τ is nontrivial. Furthermore, obviously, $s\in\operatorname{Pol}\tau$. Now we can make use of the following fact which is implicit in [15], [12].

Claim. Let $l\geqq 2$, and let ξ be an l-ary nontrivial, totally reflexive, totally symmetric relation. Then all less than l-ary relations from $[\xi]$ are trivial, and $[\xi]$ contains a totally reflexive, totally symmetric atomic relation (types (E), (C), or (R)).

By this claim, $[\tau]$ contains a central or regular relation σ of arity at least h. Clearly, $s\in\operatorname{Pol}\tau\subseteq\operatorname{Pol}\sigma$.

In what follows, we need to consider only the regular relations ϱ for which $s\in\operatorname{Pol}\varrho$. Let $\varrho=\lambda_T$ where $T=\{\vartheta_0, \ldots, \vartheta_{m-1}\}$ is an h-regular family of equivalence relations. Denote $\vartheta_0\cap\ldots\cap\vartheta_{m-1}$ by ε_T. It is not hard to see (cf. [19]) that $s\in\operatorname{Pol}\varepsilon_T$, i.e., s maps each block of ε_T onto a block of ε_T.

Lemma 3.10. *Let T be an h-regular family of equivalence relations such that $s\in\operatorname{Pol}\lambda_T$. If $h\neq p$ or $\varepsilon_T\cap\Theta\neq\omega$, then the relational algebra $[s^{\cdot}, \lambda_T]$ contains a nontrivial Θ-closed equivalence relation, a Θ-closed central relation, or a Θ-closed regular relation.*

Proof. First we show that $h<p$ and $\varepsilon_T\cap\Theta=\omega$ cannot hold simultaneously. Indeed, since T is h-regular, ε_T has exactly h^m blocks. Furthermore, taking into account $\varepsilon_T\cap\Theta=\omega$ we obtain that for each block B of ε_T the blocks B, $s(B), \ldots, s^{p-1}(B)$ are pairwise distinct. Thus the prime p divides h^m, implying $h\geqq p$.

Let σ consist of all h-tuples $(a_0, \ldots, a_{h-1})$ such that $(a_0 \oplus i_0, \ldots, a_{h-1} \oplus i_{h-1}) \in \lambda_T$ for arbitrary $0 \leqq i_0, \ldots, i_{h-1} < p$. Clearly, σ is totally symmetric and Θ-closed. We prove that $\sigma \neq \emptyset$. First let $h > p$. For each block B of Θ, every h-tuple $(b_0, \ldots, b_{h-1}) \in B^h$ belongs to σ because each $(b_0 \oplus i_0, \ldots, b_{h-1} \oplus i_{h-1})$ is in B^h and, in view of $|B| = p < h$, contains a repetition. Now let $\varepsilon_T \cap \Theta \neq \omega$. Since $s \in \mathrm{Pol}\,\{\varepsilon_T, \Theta\}$, there exists a block B of Θ which is contained in a block of ε_T. Again every $(b_0, \ldots, b_{h-1}) \in B^h$ belongs to σ because $(b_0 \oplus i_0, b_1 \oplus i_1) \in B^2 \subseteq \varepsilon_T$ for all $0 \leqq i_0, i_1 < p$. Taking into account that σ is Θ-closed, totally symmetric, and $\emptyset \neq \sigma \subseteq \lambda_T$, we get that σ is nontrivial. By Lemma 3.7 the set $[\sigma]$ contains a Θ-closed atomic relation, which must be either an equivalence relation, or a central relation, or a regular relation.

In the remaining case of $h = p$ and $\varepsilon_T \cap \Theta = \omega$ we have:

Lemma 3.11. *Let T be a p-regular set of equivalence relations such that $s \in \mathrm{Pol}\,\lambda_T$ and $\varepsilon_T \cap \Theta = \omega$. Then the elements $\vartheta_0, \ldots, \vartheta_{m-1}$ of T and the blocks B^i_j of ϑ_i $(0 \leqq i < m,\ 0 \leqq j < p)$ can be indexed in such a way that for some integers $0 \leqq l \leqq m/p$ and $0 \leqq q \leqq m - lp$ the following holds:*

(2)
$$s(B^i_j) = \begin{cases} B^{i\oplus 1}_j & \text{if } 0 \leqq i < lp \quad \text{and } 0 \leqq j < p, \\ B^i_j & \text{if } lp \leqq i < m-q \quad \text{and } 0 \leqq j < p, \\ B^i_{j\oplus 1} & \text{if } m-q \leqq i < m \quad \text{and } 0 \leqq j < p. \end{cases}$$

Proof. For the time being, denote by D^i_j $(0 \leqq j < p)$ the blocks of ϑ_i $(0 \leqq i < m)$. By the regularity of T, the blocks of ε_T are the sets $D_c = D^0_{c_0} \cap \ldots \cap D^{m-1}_{c_{m-1}}$ with $c = (c_0, \ldots, c_{m-1}) \in \mathbf{p}^m$. Since $s \in \mathrm{Pol}\,\varepsilon_T$, s induces a selfmap $\bar{s}$ of $\mathbf{p}^m$ by the equality $s(D_a) = D_{\bar{s}(a)}$, for every $a \in \mathbf{p}^m$. The fact $s \in \mathrm{Pol}\,\lambda_T$ implies that $\bar{s}$ is a *wreath function*, i.e., there are a permutation μ of $\mathbf{m}$ and permutations ν_i of $\mathbf{p}$ $(0 \leqq i < m)$ such that
$$\bar{s}(c_0, \ldots, c_{m-1}) = \big(\nu_0(c_{\mu(0)}), \ldots, \nu_{m-1}(c_{\mu(m-1)})\big)$$
for every $(c_0, \ldots, c_{m-1}) \in \mathbf{p}^m$ (see [20], [19]). Clearly, $s^p = \mathrm{id}$ implies $\bar{s}^p = \mathrm{id}$, and hence $\mu^p = \mathrm{id}$. Therefore we can assume without loss of generality that
$$\mu^{-1} = (0 \ldots p-1) \ldots \big((l-1)p \ldots lp-1\big)$$
for some $0 \leqq l \leqq m/p$. Thus, for every $0 \leqq i < lp$ and $0 \leqq j < p$, we have

(3)
$$s(D^i_j) = s\big(\bigcup (D_a\colon a \in \mathbf{p}^m,\ a_i = j)\big) = \bigcup (D_{\bar{s}(a)}\colon a \in \mathbf{p}^m,\ a_i = j) = D^{i\oplus 1}_{\nu_{i\oplus 1}(j)},$$

and, similarly, for every $lp \leqq i < m$ and $0 \leqq j < p$,

(4)
$$s(D^i_j) = D^i_{\nu_i(j)}.$$

Consequently, for $n=0, 1, \ldots$ we get

$$s^n(D_j^i) = \begin{cases} D^{i\oplus n}_{v_{i\oplus n}\cdots v_{i\oplus 1}(j)} & \text{if } 0 \leqq i < lp, \quad 0 \leqq j < p, \\ D^i_{v_i^n(j)} & \text{if } lp \leqq i < m, \quad 0 \leqq j < p. \end{cases}$$

The condition $s^p=\mathrm{id}$ obviously implies that

(5) $$v_{pt+p-1}\cdots v_{pt} = \mathrm{id} \quad \text{for every} \quad 0 \leqq t < l,$$

and $v_i^p=\mathrm{id}$ for every $lp\leqq i<m$. In the latter case, obviously, v_i is either a p-cycle, or the identity. Suppose the p-cycles are exactly $v_{m-q}, \ldots, v_{m-1}$ $(0\leqq q\leqq m-lp)$. Now set $B_j^{pt\oplus n}=D^{pt\oplus n}_{v_{pt\oplus n}\cdots v_{pt\oplus 1}(j)}$ for every $0\leqq t<l$, $0\leqq n<p$, $0\leqq j<p$, $B_j^i=D_j^i$ for every $lp\leqq i<m-q$, $0\leqq j<p$, and $B_j^i=D^{i}_{v_i^j(0)}$ for every $m-q\leqq i<m$, $0\leqq j<p$. Using (3)—(5) it is not hard to check that (2) holds.

Lemma 3.12. *Let T be a p-regular set of equivalence relations such that $s\in \mathrm{Pol}\,\lambda_T$, $\varepsilon_T\cap\Theta=\omega$, and* (2) *is satisfied. Then the equivalence relation $\bigcap(\vartheta_i\colon m-q\leqq i<m)$ is transversal to Θ, and belongs to $[s^\cdot, \lambda_T]$.*

Proof. Observe first that $q\geqq 1$. Indeed, $q=0$ would imply by (2) that $s(B)=B$ holds for the block $B=B_0^0\cap\ldots\cap B_0^{m-1}$ of ε_T, which is impossible, because $\varepsilon_T\cap\Theta=\omega$ and s has no fixed point. Setting $\vartheta=\bigcap(\vartheta_i\colon m-q\leqq i<m)$ we get from (2) that $s\in\mathrm{Pol}\,\vartheta$, and for every block D of ϑ, $s(D)\cap D=\emptyset$. Thus ϑ is transversal to Θ.

Let σ denote the binary relation consisting of all $(a, b)\in\mathbf{k}^2$ such that

(6) $$(a, a\oplus 1, \ldots, a\oplus(i-1), b, a\oplus(i+1), \ldots, a\oplus(p-1))\in\lambda_T$$

for every $0<i<p$. Clearly, $\sigma\in[s^\cdot, \lambda_T]$. We show that $\sigma^{-1}\circ\sigma=\vartheta$. First consider $(a, b)\in\mathbf{k}^2\setminus\vartheta$, say, $a\in B_u^t$, $b\in B_v^t$ for some $m-q\leqq t<m$ and $0\leqq u<v<p$. Then for $i=v-u$ the components of the p-tuple (6) belong to the blocks $B_u^t, B_{u\oplus 1}^t, \ldots$ $\ldots, B^t_{u\oplus(p-1)}$, respectively, hence (6) does not hold, so $(a, b)\notin\sigma$. Thus $\sigma\subseteq\vartheta$, and hence $\sigma^{-1}\circ\sigma\subseteq\vartheta$. Conversely, let $b\in B^0_{j_0}\cap\ldots\cap B^{m-1}_{j_{m-1}}$ and $a\in B_0^0\cap\ldots\cap B_0^{m-q-1}\cap$ $\cap B^{m-q}_{j_{m-q}}\cap\ldots\cap B^{m-1}_{j_{m-1}}$ for some $0\leqq j_0, \ldots, j_{m-1}<p$. Then, by (2), $a\oplus i\in B_0^0\cap\ldots\cap$ $\cap B_0^{m-q-1}$ for every $0\leqq i<p$. In view of $p\geqq 3$ this shows that (6) holds for $0<i<p$, i.e., $(a, b)\in\sigma$. Hence $\sigma^{-1}\circ\sigma\supseteq\vartheta$, completing the proof.

The equivalence relation $\bigcap(\vartheta_i\colon m-q\leqq i<m)$ is trivial if and only if $q=m$ and $\varepsilon_T=\omega$. This case is considered below.

Lemma 3.13. *Let T be a p-regular set of equivalence relations such that $\varepsilon_T=\omega$, $s\in\mathrm{Pol}\,\lambda_T$, and* (2) *holds with $q=m$. Then $[s^\cdot, \lambda_T]$ contains an affine relation determined by an elementary abelian p-group* $(\mathbf{k}; +)$ *such that there exists an element $c\in\mathbf{k}$ with $s(x)=x+c$ for every $x\in\mathbf{k}$.*

Proof. In view of $\varepsilon_T=\omega$ the mapping assigning to every $(j_0, ..., j_{m-1})\in\mathbf{p}^m$ the (unique) element of $B^0_{j_0}\cap...\cap B^{m-1}_{j_{m-1}}$ is a bijection between $\mathbf{p}^m$ and $\mathbf{k}$. We may identify $\mathbf{k}$ and $\mathbf{p}^m$ via this bijection. The set of equivalence relations corresponding to $T=\{\vartheta_0, ..., \vartheta_{m-1}\}$ is $Z=\{\zeta_0, ..., \zeta_{m-1}\}$ where ζ_i is defined by $(a, b)\in\zeta_i$ iff the i-th components of a and b coincide ($a, b\in\mathbf{p}^m$; $0\leqq i<m$). Furthermore, since (2) holds with $q=m$, the permutation t of $\mathbf{p}^m$ induced by s can be expressed as follows: $t(x)=x\oplus\bar{1}$ for every $x\in\mathbf{p}^m$, where $\bar{1}=(1, ..., 1)$, and $\oplus$ denotes the componentwise addition modulo p. We want to show that the affine relation α determined by $(\mathbf{p}^m; \oplus)$ belongs to $[t^{\bullet}, \lambda_Z]$, or, equivalently, $\mathrm{Pol}\,\{t^{\bullet}, \lambda_Z\}\subseteqq\mathrm{Pol}\,\alpha$.

Consider an n-ary operation $f\in\mathrm{Pol}\,\{t^{\bullet}, \lambda_Z\}$. To f we associate the following m-tuple $(f_0, ..., f_{m-1})$ of nm-ary operations on $\mathbf{p}$: for $x=(x_0, ..., x_{n-1})\in(\mathbf{p}^m)^n$, $x_j=(x_{j0}, ..., x_{j,m-1})$ $(j=0, ..., n-1)$, and $\tilde{x}=(x_{00}, ..., x_{0,m-1}, ..., x_{n-1,0}, ..., x_{n-1,m-1})$ set $f(x)=(f_0(\tilde{x}), ..., f_{m-1}(\tilde{x}))$. The operations f_i are surjective on account of $f\in\mathrm{Pol}\,t^{\bullet}$. The condition $f\in\mathrm{Pol}\,\lambda_Z$ translates into $f_i\in\mathrm{Pol}\,\varkappa$ for all $0\leqq i<m$, where $\varkappa$ denotes the relation on $\mathbf{p}$ consisting of all p-tuples with at least one repetition. Taking into account the well-known fact [11, 2.2.4] that $\mathrm{Pol}\,\varkappa$ consists of all non-surjective or essentially unary operations, we infer that every f_i is essentially unary, i.e., $f_i(\tilde{x})=g_i(x_{u_i,v_i})$ for some $0\leqq u_i<n$, $0\leqq v_i<m$, and some selfmap g_i of $\mathbf{p}$ $(0\leqq i<m)$. In view of $f\in\mathrm{Pol}\,t^{\bullet}$ we have $g_i(y\oplus 1)=g_i(y)\oplus 1$ for all $y\in\mathbf{p}$ and $0\leqq i<m$, hence there exist $a_i\in\mathbf{p}$ such that $g_i(y)=y\oplus a_i$ for all $y\in\mathbf{p}$. Now it is easy to verify that $f\in\mathrm{Pol}\,\alpha$.

Remarks. 1. The clone $\mathrm{Pol}\,\{t^{\bullet}, \lambda_Z\}$ consists of the operations

$$a\oplus x_0E_0\oplus...\oplus x_{n-1}E_{n-1}$$

where $a\in\mathbf{p}^m$ and $E_l=(E_l(i,j))$ $(0\leqq l<n)$ are $m\times m$ matrices over $\mathbf{p}$ with all entries 0 or 1 such that each column contains at most one 1, and for every $0\leqq j<m$ there exists exactly one E_l $(0\leqq l<n)$ whose j-th column has a component 1. Indeed, it is straightforward to check that these operations do belong to $\mathrm{Pol}\,\{t^{\bullet}, \lambda_Z\}$. On the other hand, our argument in the proof of Lemma 3.13 shows that every $f\in\mathrm{Pol}\,\{t^{\bullet}, \lambda_Z\}$ has the required form with $a=(a_0, ..., a_{m-1})$ and the matrices $E_0, ..., E_{n-1}$ defined by $E_l(v_j, j)=1$ if $u_j=l$ and $E_l(i,j)=0$ otherwise. For comparison we note that the clone $\mathrm{Pol}\,\{t^{\bullet}, \alpha\}$ consists of the operations $a\oplus x_0A_0\oplus$ $\oplus...\oplus x_{n-1}A_{n-1}$ where $a\in\mathbf{p}^m$ and A_l $(0\leqq l<n)$ are $m\times m$ matrices over $\mathbf{p}$ satisfying $\bar{1}A_0\oplus...\oplus\bar{1}A_{n-1}=\bar{1}$.

2. An interesting feature of the proof of Lemma 3.13 is that $\alpha\in[t^{\bullet}, \lambda_Z]$ is shown by means of operations. There seems to be no easy way to construct α from $t^{\bullet}$ and λ_Z.

Summarizing Lemmas 3.9 through 3.13 we get:

Proposition 3.14. *For a regular relation λ_T the relational algebra* $[s^{\bullet}, \lambda_T]$ *contains one of the following relations: a central relation, a Θ-closed regular relation, a nontrivial equivalence relation which is either Θ-closed or transversal to s, or an affine relation determined by an elementary abelian p-group* $(\mathbf{k}; +)$ *such that there exists an element* $c \in \mathbf{k}$ *with* $s(x) = x + c$ *for all* $x \in \mathbf{k}$.

Proposition 3.15. *For a nontrivial equivalence relation ε the relational algebra* $[s^{\bullet}, \varepsilon]$ *contains either a central relation, or a regular relation, or a nontrivial equivalence relation which is Θ-closed or transversal to s.*

Proof. Let σ be a maximal nontrivial equivalence relation in $[s^{\bullet}, \varepsilon]$, and put $\sigma_i = \{a: (a, a \oplus i) \in \sigma\}$ for $0 < i < p$. Clearly, all σ_i belong to $[s^{\bullet}, \sigma] \subseteq [s^{\bullet}, \varepsilon]$, therefore if $\emptyset \neq \sigma_i \subset \mathbf{k}$ for some $0 < i < p$, we are done. The equality $\sigma_i = \mathbf{k}$ for some $0 < i < p$ implies that σ is Θ-closed. Thus it remains to consider the case when $\sigma_i = \emptyset$ for all $0 < i < p$, i.e., $\sigma \cap \Theta = \omega$. Denote by τ the binary relation consisting of all $(a, b) \in \mathbf{k}^2$ such that $(a, c), (c \ominus 1, b \ominus 1), (a \ominus 1, d \ominus 1), (d, b) \in \sigma$ for some $c, d \in \mathbf{k}$. Clearly, $\tau \in [s^{\bullet}, \sigma]$ is symmetric, and $\sigma \subseteq \tau$ (set $c = b, d = a$). Furthermore, $\tau \cap s^{\bullet} = \emptyset$, since $(a, a \oplus 1) \in \tau$ for some $a \in \mathbf{k}$ would imply the existence of an element $c \in \mathbf{k}$ with $(a, c) \in \sigma$ and $(c \ominus 1, a) \in \sigma$, yielding $(c \ominus 1, c) \in \sigma$ in contradiction to $\sigma \cap \Theta = \omega$. By the claim formulated in the proof of Lemma 3.9 the relational algebra $[\tau]$ contains a nontrivial equivalence relation, a nonunary central relation, or a regular relation. In the latter two cases, the claim of the proposition follows, so suppose $[\tau]$ contains a nontrivial equivalence relation λ. It is easy to show that every binary relation in $[\tau]$ distinct from ω contains τ. Hence $\sigma \subseteq \tau \subseteq \lambda$. Taking into account $\sigma, \lambda \in [s^{\bullet}, \varepsilon]$ and the maximality of σ we get that $\sigma = \lambda = \tau$. Thus for arbitrary $(a, b) \in \sigma$ we have $(a \oplus 1, b \oplus 1) \in \tau = \sigma$ (choose $c = a \oplus 1, d = b \oplus 1$), which proves that $s \in \mathrm{Pol}\, \sigma$, i.e., σ is transversal to s.

Proposition 3.16. *Let α be an affine relation determined by an elementary abelian p-group* $(\mathbf{k}; +)$ *(p prime). Then either there exists an element* $c \in \mathbf{k}$ *such that* $s(x) = x + c$ *for all* $x \in \mathbf{k}$, *or the relational algebra* $[s^{\bullet}, \alpha]$ *contains a nontrivial equivalence relation.*

Proof. Assume there is no $c \in \mathbf{k}$ with $s(x) = x + c$ for all $x \in \mathbf{k}$, that is, the set $U = \{(a \oplus 1) - a: a \in \mathbf{k}\}$ contains at least two elements. Note also that $0 \notin U$ as s is fixed point free. Hence $2 \leqq |U| \leqq k - 1$. Let ν denote the binary relation consisting of all $(a, b) \in \mathbf{k}^2$ such that $(a \oplus 1) - a + b = (b \oplus 1)$, or equivalently, $(a \oplus 1) - a = (b \oplus 1) - b$. Then $\nu \in [s^{\bullet}, \alpha]$ and ν is an equivalence relation with $|U|$ blocks.

4. Proof of Theorem 2.6

In order to show that for every relation ϱ listed in Theorem 2.3 the relational algebra $[s^{\bullet}, \varrho]$ indeed covers $[s^{\bullet}]$, we apply a more or less standard method, the main point being an explicit description of the members of $[s^{\bullet}, \varrho]$. With this at hand, it is already not hard to show that there is no relational algebra strictly between $[s^{\bullet}]$ and $[s^{\bullet}, \varrho]$. In fact, we can accomplish a bit more than that: we determine all relational subalgebras of $[s^{\bullet}, \varrho]$ (or, equivalently, all clones containing Pol $\{s^{\bullet}, \varrho\}$).

Making use of Lemma 3.2, type (P_s) is easy to settle.

Proposition 4.1. *Let g be a permutation such that $\{s, g\}$ generates a semiregular representation of a group $\mathfrak{G}$ from Proposition 3.1 on* **k**. *Then the lattice of relational subalgebras of $[s^{\bullet}, g^{\bullet}]$ is isomorphic to the lattice of subgroups of $\mathfrak{G}$.*

Proof. Let G denote the permutation group generated by $\{s, g\}$. It is clear that $[s^{\bullet}, g^{\bullet}]=[G^{\bullet}]$. Furthermore, in view of Lemma 3.2, every relational subalgebra of $[G^{\bullet}]$ is of the form $[H^{\bullet}]$ for some subgroup H of G. It follows also that $[H_1^{\bullet}]\neq [H_2^{\bullet}]$ for distinct subgroups H_1, H_2 of G.

To describe the relations in $[s^{\bullet}, \varrho]$ for the remaining four types (A_s)—(R_s), too, we proceed, as in the proof of Lemma 3.2, according to the following scheme: we consider a formula

$$\Phi(x_0, \dots, x_{h-1}) = \exists x_h \dots \exists x_{m-1} \Gamma(x_0, \dots, x_{m-1}) \tag{7}$$

determining a nonempty relation $\sigma\in[s^{\bullet}, \varrho]$, and then, utilizing the special properties of ϱ, we bring the matrix Γ of Φ to "canonical form", yielding the required description.

Proposition 4.2. *Let α be an affine relation determined by an elementary abelian p-group $(\mathbf{k}; +)$ such that there exists an element $c\in\mathbf{k}$ with $s(x)=x+c$ for all $x\in\mathbf{k}$. Then the relational subalgebras of $[s^{\bullet}, \alpha]$ form a 4-element Boolean lattice consisting of $[s^{\bullet}, \alpha]$, $[s^{\bullet}]$, $[\alpha]$, and $[\omega]$.*

Proof. Denote by L the set of operations $\beta_0 x_0+\dots+\beta_{l-1}x_{l-1}+\beta_l c$ on **k** where $0\leqq\beta_i<p$ $(0\leqq i\leqq l)$ and $\beta_0\oplus\dots\oplus\beta_{l-1}=1$, and consider a formula (7) determining a nonempty relation $\sigma\in[s^{\bullet}, \alpha]$. Since s and $x-y+z$ both belong to L, Γ is a solvable system of linear equations $x_j=f(x_{i_0}, \dots, x_{i_{l-1}})$ with $l\geqq 1$, $0\leqq j, i_0, \dots, i_{l-1}<m$, and $f\in L$. It is easy to see that every step of the usual elimination process yields equations of this form. Thus we can first eliminate all variables $x_h, \dots, x_{m-1}$, and then further elimination can express certain unknowns, say $x_t, \dots, x_{h-1}$, as linear functions (from L) of independent variables. Thus

$$\sigma = \{(a_0, \dots, a_{t-1}, f_t(a_0, \dots, a_{t-1}), \dots, f_{h-1}(a_0, \dots, a_{t-1})) \colon a_0, \dots, a_{t-1}\in\mathbf{k}\}$$

with $f_t, \dots, f_{h-1}\in L$.

Clearly, $[\sigma]=[f_t^\bullet, ..., f_{h-1}^\bullet]$. Now recall the well-known and easy fact (cf. [21], [1]) that L has exactly four subclones, namely, the clone of projections, the two clones generated by $x+c$, resp., $x-y+z$, and L itself, which is generated by $\{x+c, x-y+z\}$. Thus, for every $f\in L$ we have $[f^\bullet]=[\omega], [s^\bullet], [\alpha]$, or $[s^\bullet, \alpha]$, completing the proof.

For the rest of the proof it will be convenient to split Γ into a conjunction $\Gamma=\Gamma_1\wedge\Gamma_2$ such that Γ_1 collects all conditions involving ϱ and Γ_2 all conditions involving $=$ or $s^\bullet$. We will denote by $\sim$ the least equivalence relation on $\{x_0, ..., x_{m-1}\}$ such that $x_i\sim x_j$ whenever $x_i=x_j$ or $(x_i, x_j)\in s^\bullet$ appears in Γ_2, and $X_0, ..., X_{t-1}$ will denote the blocks of $\sim$. It is clear that if we fix one element x_{r_i} in each block X_i $(i=0, ..., t-1)$, then for arbitrary variable x_j $(0\leqq j<m)$ with $x_j\sim x_{r_i}$ there is an integer $0\leqq c_j<p$ such that Γ_2 implies

$$(x_{r_i}, x_j)\in(s^{c_j})^\bullet. \tag{8}$$

Since Φ determines a nonempty relation, and $(s^c)^\bullet\cap(s^d)^\bullet=\emptyset$ for all $0\leqq c<d<p$, the exponents c_j in (8) are uniquely determined. Thus Γ_2 is equivalent to the conjunction of the formulas (8) for all $0\leqq i<t$ and $x_j\sim x_{r_i}$, which will be denoted by Γ_2^*. Hence we can as well assume that Φ is given in the form

$$\Phi(x_0, ..., x_{h-1}) = \exists x_h ... \exists x_{m-1}(\Gamma_1(x_0, ..., x_{m-1})\wedge\Gamma_2^*(x_0, ..., x_{m-1})). \tag{7'}$$

The Θ-closed relations can be treated together.

Proposition 4.3. *Let ϱ be a Θ-closed equivalence relation, central relation, or regular relation. If ϱ is unary, then the relational subalgebras of $[s^\bullet, \varrho]$ are $[s^\bullet, \varrho]$, $[s^\bullet]$, $[s^\bullet\cap(\varrho\times\varrho)]$, $[\varrho]$, $[\omega]$, and hence they form a lattice isomorphic to $\mathfrak{N}_5$. Otherwise the relational subalgebras of $[s^\bullet, \varrho]$ form a 4-element Boolean lattice consisting of $[s^\bullet, \varrho]$, $[s^\bullet]$, $[\varrho]$, and $[\omega]$.*

Proof. Consider a formula (7′) determining a nonempty relation $\sigma\in[s^\bullet, \varrho]$. Select the variables $x_{r_i}\in X_i$ $(i=0, ..., t-1)$ so that x_{r_i} is free whenever X_i contains a free variable. We can assume without loss of generality that $X_0, ..., X_{q-1}$ $(q\leqq t, h)$ are exactly the blocks containing free variables, and $x_{r_i}=x_i$ $(i=0, ..., q-1)$. Since ϱ is Θ-closed, every condition $(x_{i_0}, ..., x_{i_{l-1}})\in\varrho$ in Γ_1 can be replaced by $(x_{j_0}, ..., x_{j_{l-1}})\in\varrho$ where $\{x_{j_0}, ..., x_{j_{l-1}}\}\subseteq\{x_{r_0}, ..., x_{r_{t-1}}\}$ and $x_{i_0}\sim x_{j_0}, ..., x_{i_{l-1}}\sim\sim x_{j_{l-1}}$. Clearly, $\exists x_{r_q}...\exists x_{r_{t-1}}\Gamma_1(x_{r_0}, ..., x_{r_{t-1}})$ determines a relation $\tau\in[\varrho]$, and σ is of the form

$$\sigma = \{(a_0, ..., a_{q-1}, a_{l_q}\oplus c_q, ..., a_{l_{h-1}}\oplus c_{h-1})\colon (a_0, ..., a_{q-1})\in\tau\}$$

with $0\leqq l_i<q$ for all $q\leqq i<h$.

Since the relation ϱ is atomic, either τ is trivial, or $[\tau]=[\varrho]$. Thus an easy argument shows that one of the following holds provided ϱ is at least binary: $[\sigma]=$

$=[s^{\bullet}, \varrho], [s^{\bullet}], [\varrho]$, or $[\omega]$. If ϱ is unary, we have one more possibility, namely $[\sigma]=$ $=[s^{\bullet}\cap(\varrho\times\varrho)]$.

It remains to consider equivalence relations and unary relations transversal to s.

Proposition 4.4. *Let ε be a nontrivial equivalence relation transversal to s. Then the relational subalgebras of $[s^{\bullet}, \varepsilon]$ are $[s^{\bullet}, \varepsilon]$, $[s^{\bullet}]$, $[\varepsilon\circ s^{\bullet}]$, $[\varepsilon]$, $[\omega]$, and hence they form a lattice isomorphic to $\mathfrak{N}_5$.*

Proof. Take a formula (7') determining a nonempty relation $\sigma\in[s^{\bullet}, \varepsilon]$, and define a graph $\mathbf{G}$ on the vertices $0, \ldots, t-1$ as follows: (u, v) is an edge of $\mathbf{G}$ if and only if there are $x\in X_u$ and $y\in X_v$ such that $(x, y)\in\varepsilon$ appears in Γ_1. Since ε is symmetric, $\mathbf{G}$ is undirected. In view of $s\in\operatorname{Pol}\varepsilon$, any condition $(x, y)\in\varepsilon$ in Γ_1 can be replaced by $(x', y')\in\varepsilon$ provided $(x, x')\in(s^i)^{\bullet}$ and $(y, y')\in(s^i)^{\bullet}$ are in Γ_2^* for some $0\leqq i<p$. Thus each vertex l of $\mathbf{G}$ can be labelled by a variable $x_{r_l}\in X_l$ in such a way that

$$\Gamma_1^* = \bigwedge\{(x_{r_i}, x_{r_j})\in\varepsilon\colon\ (i, j) \text{ is an edge of } \mathbf{G}\}$$

is equivalent to Γ_1. In fact, the labelling can proceed along the paths of $\mathbf{G}$. Circles (loops, multiple edges) do not cause the procedure to fail, because ε is symmetric, transitive, $\varepsilon\cap(s^i)^{\bullet}=\emptyset$ for every $0<i<p$, and by assumption, $\sigma\neq\emptyset$. Clearly, $\Gamma_1^*(x_0, \ldots, x_{m-1})$ determines a relation from $[\varepsilon]$, and hence σ is of the form $\sigma=\tau\oplus c$ with $\tau\in[\varepsilon]$ and $c\in\mathbf{p}^h$.

It is well known and easy to check that, up to the order of its components, τ is a direct product $\tau_0\times\ldots\times\tau_{q-1}$ where each τ_i arises from a relation

$$\{(a_0, \ldots, a_{k-1})\colon\ a_0\varepsilon a_1\varepsilon\ldots\varepsilon a_{k-1}\}$$

by repeating some components. Correspondingly, $\sigma=\sigma_0\times\ldots\times\sigma_{q-1}$ and every binary projection of each σ_i is equal to some $(s^c)^{\bullet}$ or some $(s^{-c})^{\bullet}\circ\varepsilon\circ(s^d)^{\bullet}$ $(0\leqq c, d<p)$. However, taking into account $s\in\operatorname{Pol}\varepsilon$ we get $\varepsilon=(s^{-c})^{\bullet}\circ\varepsilon\circ(s^c)^{\bullet}$ for all $0\leqq c<p$. Consequently, introducing the notation $\varepsilon_j=\varepsilon\circ(s^j)^{\bullet}$ $(0\leqq j<p)$ we have $(s^{-c})^{\bullet}\circ\varepsilon\circ$ $\circ(s^d)^{\bullet}=\varepsilon_{d\ominus c}$ and $\varepsilon_c\circ\varepsilon_d=\varepsilon_{c\oplus d}$ for all $0\leqq c, d<p$. This implies that $\varepsilon\in[\varepsilon_1]=[\varepsilon_2]=\ldots$ $\ldots=[\varepsilon_{p-1}]$. Hence a quick analysis of the various possibilities yields that $[\sigma]=$ $=[s^{\bullet}, \varepsilon](=[s^{\bullet}, \varepsilon_1])$, $[s^{\bullet}]$, $[\varepsilon_1]$, $[\varepsilon]$, or $[\omega]$, completing the proof.

A symmetric, transitive, binary relation will be called a *partial equivalence* (equivalence relation on a subset of the base set). The empty set is also considered a partial equivalence. The lattice of partial equivalences of $\mathbf{p}$ will be denoted by $\mathfrak{Q}_p$, and $\mathfrak{Q}_p^*$ will stand for the lattice arising from $\mathfrak{Q}_p$ by adding a new greatest element, and another element which is comparable only with the least element of $\mathfrak{Q}_p$.

Proposition 4.5. *Let μ be a nontrivial unary relation transversal to s, and let $\mu_i=\mu\oplus i$ $(0\leqq i<p)$, $\pi_{ij}=(\mu_i\times\mu_j)\cap(s^{j\ominus i})^{\bullet}$ $(0\leqq i,j<p)$. Then the relational subalgebras of $[s^{\bullet},\mu]$ are $[s^{\bullet},\mu]$, $[s^{\bullet}]$, and $[\pi_{ij}\colon (i,j)\in\xi]$ with $\xi\in\mathfrak{Q}_p$, and hence they form a lattice isomorphic to $\mathfrak{Q}_p^*$.*

Proof. A similar but simpler argument than in the previous proof yields again that every nonempty relation $\sigma\in[s^{\bullet},\mu]$ is of the form $\sigma=\tau\oplus c$ for some $\tau\in[\mu]$ and $c\in\mathbf{p}^h$. The well-known description of the relations in $[\mu]$ (see, e.g., [11, 2.2.2]) implies that σ is a direct product of relations of the form

$$\sigma'=\{(a\oplus c_0,\ldots,a\oplus c_{t-1})\colon a\in\nu\}$$

where $\nu=\mu$ or $\nu=\mathbf{k}$. Clearly, if $\nu=\mathbf{k}$, then $[\sigma']\subseteq[s^{\bullet}]$. If $\nu=\mu$, then $[\sigma']=[\pi_{c_0,c_l}\colon 0\leqq l<t]$. Taking into account that $[s^{\bullet},\pi_{ij}]=[s^{\bullet},\mu]$ for all $0\leqq i,j<p$, we get that there are the following three possibilities for a set of relations $R\subseteq[s^{\bullet},\mu]$:

(a) $[R]=[s^{\bullet},\mu]$,

(b) $[R]=[s^{\bullet}]$,

(c) $[R]=[\Pi]$ for some $\Pi\subseteq\{\pi_{ij}\colon 0\leqq i,j<p\}$.

In the last case it is easy to see that $[R]=[\pi_{mn}\colon (m,n)\in\xi]$ where ξ is the least partial equivalence on $\mathbf{p}$ such that $(i,j)\in\xi$ provided $\pi_{ij}\in\Pi$. The straightforward proof of the fact that the relational algebras listed in the proposition are indeed pairwise distinct is left to the reader.

Remarks. 1. The results above show that two clones $\operatorname{Pol}\{s^{\bullet},\varrho\}$ and $\operatorname{Pol}\{s^{\bullet},\varrho'\}$ where $\varrho\neq\varrho'$ are from the list in Theorem 2.3 coincide if and only if either both of ϱ and ϱ' are of type (P_s) such that the corresponding permutations and s generate the same permutation group, or both of ϱ and ϱ' are unary relations transversal to s such that $\varrho'=s^i(\varrho)$ for some $0<i<p$. This can be verified by comparing the sets of maximal clones containing $\operatorname{Pol}\{s^{\bullet},\varrho\}$, resp., $\operatorname{Pol}\{s^{\bullet},\varrho'\}$. (Apply Propositions 4.1—4.5 to determine the maximal clones, and make use of the well-known fact [16], [11, 4.3.23] that among the maximal clones, too, there are only some trivial coincidences.)

2. A similar argument shows also that for an atomic relation σ the clone $\operatorname{Pol}\{s^{\bullet},\sigma\}$ is maximal in $\operatorname{Pol}s^{\bullet}$ if and only if σ falls into one of the types (P_s)—(R_s) in Theorem 2.3.

References

[1] J. BAGYINSZKI and J. DEMETROVICS, The structure of the maximal linear classes in prime-valued logics, *C. R. Math. Rep. Acad. Sci. Canada*, **2** (1980), 209—213.

[2] V. G. BODNARČUK, L. A. KALUŽNIN, V. N. KOTOV and B. A. ROMOV, Galois theory for Post algebras. I—II, *Kibernetika*, **5** (1969), 1—10 and **5** (1969), 1—9 (Russian); English translation: *Cybernetics*, **5** (1969), 243—252 and 531—539.

[3] J. DEMETROVICS, L. HANNÁK and S. S. MARČENKOV, Closed classes of selfdual functions in P_3, *Diskret. Analiz*, **34** (1980), 38—73 (Russian); English summary: Some remarks on the structure of P_3, *C. R. Math. Rep. Acad. Sci. Canada*, **2** (1980), 215—219.

[4] D. GEIGER, Closed systems of functions and predicates, *Pacific J. Math.*, **27** (1968), 95—100.

[5] G. GRÄTZER, *Universal Algebra*, 2nd ed., Springer-Verlag (Berlin—Heidelberg—New York, 1979).

[6] B. HUPPERT, *Endliche Gruppen. I*, Grundlehren der math. Wissenschaften, B. 134, Springer-Verlag (Berlin—Heidelberg—New York, 1967).

[7] V. B. KUDRJAVCEV, The coverings of precomplete classes of k-valued logic, *Diskret. Analiz*, **17** (1970), 32—44. (Russian)

[8] D. LAU, Submaximale Klassen von P_3, *Elektron. Informationsverarb. Kybernet.*, **18** (1982), 227—243.

[9] D. LAU, Die maximalen Klassen von $\mathrm{Pol}_k(0)$, *Rostock. Math. Kolloq.*, **19** (1982), 29—47.

[10] H. MACHIDA, On closed sets of three-valued monotone logical functions, in: *Finite Algebra and Multiple-valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland (Amsterdam, 1981); pp. 441—467.

[11] R. PÖSCHEL and L. A. KALUŽNIN, *Funktionen- und Relationenalgebren. Ein Kapitel der diskreten Mathematik*, Math. Monographien, B. 15, VEB Deutscher Verlag der Wissenschaften (Berlin, 1979); and Math. Reihe, B. 79, Birkhäuser Verlag (Basel—Stuttgart, 1979).

[12] 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.

[13] L. RÉDEI, Das schiefe Produkt in der Gruppentheorie, *Comment. Math. Helvet.*, **20** (1947), 225—264.

[14] I. G. ROSENBERG, La structure des fonctions de plusieurs variables sur un ensemble fini, *C. R. Acad. Sci. Paris, Ser. A. B.*, **260** (1965), 3817—3819.

[15] I. G. ROSENBERG, Über die funktionale Vollständigkeit in den mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen), *Rozpravy Československé Akad. Věd, Řada Mat. Přírod. Věd*, **20** (1970), 3—93.

[16] I. G. ROSENBERG, Über die Verschiedenheit maximaler Klassen in P_k, *Rev. Roumaine Math. Pures Appl.*, **14** (1969), 431—438.

[17] I. G. ROSENBERG, Completeness, closed classes and relations in multiple-valued logics, in: *Proc. Intern. Sympos. on Multiple-valued Logics* (Morgantown, 1974); pp. 1—26.

[18] I. G. ROSENBERG, On generating large classes of Sheffer functions, *Aequationes Math.*, **17** (1978), 164—181.

[19] 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.

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

[21] A. SALOMAA, On infinitely generated sets of operations in finite algebras, *Ann. Univ. Turku., Ser. AI,* **74** (1963), 1—12.

[22] P. SCHOFIELD, Independent conditions for completeness of finite algebras with a single generator, *J. London Math. Soc.,* **44** (1969), 413—423.

[23] Á. SZENDREI, Algebras of prime cardinality with a cyclic automorphism, *Arch. Math. (Basel),* **39** (1982), 417—427.

[24] Á. SZENDREI, Short maximal chains in the lattice of clones over a finite set, *Math. Nachr.,* **110** (1983), 43—58.

(I. G. R.)
CENTRE DE RECHERCHE
DE MATHÉMATIQUES
UNIVERSITÉ DE MONTRÉAL
CASE POSTALE 6128, SUCC. "A"
MONTRÉAL, QUÉBEC H3C 3J7 CANADA

(Á. SZ.)
JÓZSEF ATTILA UNIVERSITY
BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
6720 SZEGED, HUNGARY