

Triply transitive algebras

LÁSZLÓ SZABÓ

To the memory of András Huhn

In [7] P. SCHOFIELD proved that if G is a triply transitive permutation group on an at least four element finite set M and f is a surjective operation on M depending on at least two variables then the clone F generated by $G \cup \{f\}$ either equals the set of all operations on M or $F \subseteq L$ where L is a maximal clone of quasilinear operations on M . The aim of this paper is to improve this result by proving that the inclusion $F \subseteq L$ is actually an equality (Theorem 8).

In [6] R. PÖSCHEL described all finite relationally incomplete homogeneous relation algebras. As an application of our theorem we also improve this result by giving all at least four element finite relationally incomplete relation algebras having triply transitive automorphism groups (Theorem 9).

2. Preliminaries

Let M be a nonempty set. The set of all n -ary operations on M will be denoted by $O_M^{(n)}$ ($n \geq 1$), and we set $O_M = \bigcup_{n \geq 1} O_M^{(n)}$. An operation $f \in O_M$ is *idempotent* if for every $a \in M$ we have $f(a, \dots, a) = a$; f is *nontrivial* if it is not a projection. If f depends on at least two variables and takes on all values from M then it is called *essential*.

For $h \geq 1$ the set of h -ary relations on M (i.e. subsets of M^h) will be denoted by $R_M^{(h)}$; furthermore we set $R_M = \bigcup_{h \geq 1} R_M^{(h)}$. An operation $f \in O_M^{(n)}$ is said to *preserve* a relation $\varrho \in R_M^{(h)}$ if ϱ is a subalgebra of the h -th direct power of the algebra $\langle M; f \rangle$. For $R \subseteq R_M$ the symbol $\text{Pol } R$ denotes the set of all operations from O_M preserving

Received June 24, 1986, and in revised form October 27, 1986.

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

each relation in R , and for $F \subseteq O_M$ the symbol $\text{Inv } F$ denotes the set of all relations from R_M preserved by each operation in F . The correspondences $R \rightarrow \text{Pol } R$ and $F \rightarrow \text{Inv } F$ establish a Galois connection between the subsets of R_M and the subsets of O_M . For $F \subseteq O_M$ and $R \subseteq R_M$ we set $\langle F \rangle = \text{Pol } \text{Inv } F$ and $[R] = \text{Inv } \text{Pol } R$.

By a *clone of operations* on M we mean a subset $F \subseteq O_M$ which contains the projections and is closed with respect to superposition. It is known (cf. e.g. [5]) that, for finite M , a subset $F \subseteq O_M$ is a clone if and only if $F = \langle F \rangle$. By a *clone of relations* we mean a subset $R \subseteq R_M$ satisfying the equality $R = [R]$. We remark that for finite M there exists also an internal definition for $[R]$, namely $[R]$ is the set of all relations which are definable by a first order formula in which only \exists , \wedge , $=$, and relations (i.e. predicates) of R occur. For more details cf. [5].

By a *relation algebra* on the set M we mean a pair $\langle M; R \rangle$ where $R \subseteq R_M$. We say that $\langle M; R \rangle$ is nontrivial if $\text{Pol } R \neq O_M$. A permutation π on M is an *automorphism* of $\langle M; R \rangle$ if $q\pi \subseteq q$ and $q\pi^{-1} \subseteq q$ for every $q \in R$. The symbol $\text{Aut } \langle M; R \rangle$ denotes the group of all automorphisms of $\langle M; R \rangle$.

If f is an n -ary operation on M then f^* denotes the $(n+1)$ -ary relation $\{(a_1, \dots, a_n, f(a_1, \dots, a_n)) \mid a_1, \dots, a_n \in M\}$. Two relation algebras $\langle M; R_1 \rangle$ and $\langle M; R_2 \rangle$ are *equivalent* if $[R_1] = [R_2]$.

If $n \geq 1$ and q is a prime power then $V(n, q)$ denotes the n -dimensional vector space over the field $GF(q)$. In this note by a *linear operation* over $V(n, q)$ we mean an operation of the form $\sum_{i=1}^m x_i A_i + v$ where $v \in V(n, q)$ and the A_i ($1 \leq i \leq m$) are linear transformations of $V(n, q)$. Clearly, such an operation depends on its i -th variable if and only if $A_i \neq 0$, and is surjective if and only if $V(n, q)$ is spanned by its subspaces $\text{Im } A_i$, $i=1, \dots, m$. The set of all linear operations over $V(n, q)$ will be denoted by $ACL(n, q)$; and as usual $AGL(n, q)$ resp. $GL(n, q)$ denote the set of all linear permutations resp. the set of all linear permutations fixing the zero vector $0 \in V(n, q)$.

Let us denote by \mathcal{A}_n ($n \geq 1$) the alternating group of degree n . It is well known (see e.g. [3]) that $GL(4, 2) \cong \mathcal{A}_8$, and thus $GL(4, 2)$ contains subgroups isomorphic to \mathcal{A}_7 .

We need the following results.

Proposition 1 ([3], [4]). *If G is a subgroup of $GL(4, 2)$ and $G \cong \mathcal{A}_7$ then G is doubly transitive on $V(4, 2) \setminus \{0\}$, moreover, for any two triples u_1, u_2, u_3 and v_1, v_2, v_3 of linearly independent vectors in $V(4, 2)$ there is exactly one permutation $A \in G$ such that $u_i A = v_i$, $i=1, 2, 3$. Consequently, if T is the group of all translations on $V(4, 2)$ then $G \ltimes T$ is a triply transitive proper subgroup of $AGL(4, 2)$.*

Consider the elements of $GL(4, 2)$ as 4×4 matrices over $GF(2)$ in a fixed basis of $V(4, 2)$. Let G be a subgroup of $GL(4, 2)$ with $G \cong \mathcal{A}_7$. Consider the subgroup

G^* of $GL(4, 2)$, given by $G^* = \{A^* \mid A \in G\}$ where A^* is the transpose of A . Then clearly $G^* \cong \mathcal{A}_7$. Combining this fact with Proposition 1 we immediately get the following statement.

Proposition 2. *Let G be a subgroup of $GL(4, 2)$ with $G \cong \mathcal{A}_7$, and consider the elements of $GL(4, 2)$ as 4×4 matrices over $GF(2)$ in a fixed basis of $V(4, 2)$. Then for any numbers $1 \leq i_1 < i_2 < i_3 \leq 4$ and for any linearly independent 4-dimensional row (column) vectors $u_{i_1}, u_{i_2}, u_{i_3}$ over $GF(2)$ there is exactly one element $A \in G$ such that the i -th row (column) of A coincides with u_i for $i = i_1, i_2, i_3$.*

Theorem A (CAMERON and KANTOR [1]). *If H is a triply transitive proper subgroup of $AGL(n, 2)$ then $n=4$ and H is $\mathcal{A}_7 \rtimes T$ in $AGL(4, 2)$. Moreover, if G is a doubly transitive proper subgroup of $GL(n, 2)$ (on $V(n, 2) \setminus \{0\}$) then $n=4$ and G is \mathcal{A}_7 in $GL(4, 2)$.*

Theorem B (SZABÓ and SZENDREI [9]). *If $|V(n, q)| \geq 3$ then $\langle AGL(n, q) \cup \{f\} \rangle = ACL(n, q)$ for every essential operation $f \in ACL(n, q)$.*

Theorem C (SCHOFIELD [7]). *If M is a finite set, $|M| \geq 4$, G is a triply transitive permutation group on M and $f \in O_M$ is an essential operation, then either $\langle G \cup \{f\} \rangle = O_M$ or $|M| = 2^n$ for some $n \geq 2$ and $\langle G \cup \{f\} \rangle \subseteq ACL(n, 2)$.*

3. Lemmas

In this section we give some preparatory lemmas.

Lemma 3 (SCHOFIELD [7]). *If H is a triply transitive permutation group and f is an essential operation on an at least four element finite set M then $\langle H \cup \{f\} \rangle$ contains all constant operations and an operation taking on m values for some m with $2 \leq m < |M|$.*

From now on in this section let G denote a subgroup of $GL(4, 2)$ isomorphic to \mathcal{A}_7 , and let A, A_1, A_2 be unary linear operations on $V(4, 2)$ fixing the zero vector 0. For any unary linear operation X fixing 0, the symbol $G(X)$ denotes the set of all unary linear operations generated by $G \cup \{X\}$.

Lemma 4. *If $\text{Im } A \neq V(4, 2)$, then there is a B in G such that $\text{Im } BA = \text{Im } A$ and $(BA)^2 = BA$.*

Proof. Let $\dim(\text{Im } A) = n (\leq 3)$ and let u_1, \dots, u_n be a basis of $\text{Im } A$. Choose elements $v_1, \dots, v_n \in V(4, 2)$ such that $v_i A = u_i, i = 1, \dots, n$. It is easy to see that v_1, \dots, v_n are linearly independent, and therefore, by Proposition 1, there is a $B \in G$ such that $u_i B = v_i (i = 1, \dots, n)$. Then $u_i BA = u_i (i = 1, \dots, n)$ showing that $\text{Im } BA = \text{Im } A$ and $(BA)^2 = BA$.

Lemma 5. *Suppose $A^2=A$, $\text{Im } A \neq V(4, 2)$, and let U be a proper subspace of $\text{Im } A$ with $|U| \geq 2$. Then there is a $B \in G(A)$ such that $\text{Im } BA = U$ and $(BA)^2 = BA$.*

Proof. First consider the case when $\dim(\text{Im } A) = 3$ and $\dim U = 2$. Let u_1, u_2, u_3, u_4 be a basis of $V(4, 2)$ such that u_1, u_2 and u_1, u_2, u_3 are bases of U and $\text{Im } A$, respectively, and $u_4 \in \text{Ker } A$. By Proposition 1, there is a $C \in G$ such that $u_1 C = u_1, u_2 C = u_2$ and $u_3 C = u_4$. Then we have $u_1 A C A = u_1, u_2 A C A = u_2, u_3 A C A = 0$ and $u_4 A C A = 0$. Therefore if $AC = B$ then $\text{Im } BA = U$ and $(BA)^2 = BA$.

Now suppose that $\dim(\text{Im } A) = 2$ and $\dim U = 1$. Choose a basis u_1, u_2, u_3, u_4 of $V(4, 2)$ such that u_1 and u_1, u_2 are bases of U and $\text{Im } A$, respectively, and $u_3, u_4 \in \text{Ker } A$. Again by Proposition 1, there is a $C \in G$ such that $u_1 C = u_1$ and $u_2 C = u_3$. Now if $B = AC$ then we have $\text{Im } BA = U$ and $(BA)^2 = BA$.

Finally the statement in the case $\dim(\text{Im } A) = 3$ and $\dim U = 1$ follows from the previous two cases.

Lemma 6. *If $\text{Im } A \neq V(4, 2)$, and U is a subspace of $V(4, 2)$ such that $\dim U = \dim(\text{Ker } A)$ then there is a $B \in G$ such that $\text{Im } BA = \text{Im } A$ and $\text{Ker } BA = U$.*

Proof. Let u_1, \dots, u_n and v_1, \dots, v_n be bases of U and $\text{Ker } A$, respectively. Since $1 \leq n \leq 3$, by Proposition 1 there is a $B \in G$ such that $u_i B = v_i, i = 1, \dots, n$. Then $\text{Im } BA = \text{Im } A$ and $\text{Ker } BA = U$.

Lemma 7. *Suppose that $\text{Im } A_1, \text{Im } A_2 \neq V(4, 2)$, and $\text{Im } A_1 \not\subseteq \text{Im } A_2$, $\text{Im } A_2 \not\subseteq \text{Im } A_1$. Then there are $B_1 \in G(A_1)$ and $B_2 \in G(A_2)$ such that $\text{Im}(B_1 A_1 + B_2 A_2) = \text{Im } A_1 + \text{Im } A_2$.*

Proof. Let $U_1 \subseteq \text{Im } A_1$ and $U_2 \subseteq \text{Im } A_2$ be subspaces such that $U_1 \cap U_2 = \{0\}$ and $U_1 + U_2 = \text{Im } A_1 + \text{Im } A_2$. Then applying Lemmas 4 and 5 we get $C_1 \in G(A_1)$ and $C_2 \in G(A_2)$ such that $\text{Im } C_i A_i = U_i$ and $(C_i A_i)^2 = C_i A_i, i = 1, 2$. Since $U_1 \cap U_2 = \{0\}$, we have $\dim U_1 + \dim U_2 \leq 4$. Therefore $\dim(\text{Ker } C_1 A_1) \geq \dim U_2$. Now, by Lemma 6, there is a $D_1 \in G$ such that $\text{Im } D_1 C_1 A_1 = U_1$ and $\text{Ker } D_1 C_1 A_1 \supseteq U_2$. If we choose $B_1 = D_1 C_1$ and $B_2 = C_2$, then we have $\text{Im}(B_1 A_1 + B_2 A_2) = U_1 + U_2 = \text{Im } A_1 + \text{Im } A_2$. Indeed, it follows that $B_2 A_2 B_1 A_1 = 0$ and $(B_2 A_2)^2 = B_2 A_2$. Therefore, if E is the identity permutation, then we have

$$(E \circ B_2 A_2)(B_1 A_1 + B_2 A_2) = B_1 A_1 \text{ and } B_2 A_2(B_1 A_1 + B_2 A_2) = B_2 A_2.$$

4. Main theorem

Here we formulate and prove our main theorem.

Theorem 8. *If M is a finite set with $|M| \geq 4$, H is a triply transitive permutation group on M and $f \in O_M$ is an essential operation, then either $\langle H \cup \{f \rangle = O_M$, or $|M| = 2^n$ for some $n \geq 2$ and $\langle H \cup \{f \rangle = ACL(n, 2)$.*

Proof. Let M, H and f satisfy the assumptions of the theorem. If $\langle H \cup \{f \rangle \neq O_M$ then, by Theorem C, we have that $|M| = 2^n$ for some $n \geq 2$ and $\langle H \cup \{f \rangle \subseteq ACL(n, 2)$. We have to show that the latter inclusion is actually an equality. Let \bar{H} denote the group of all permutations belonging to $\langle H \cup \{f \rangle$.

If $\bar{H} = AGL(n, 2)$, then by Theorem B we have $\langle H \cup \{f \rangle = ACL(n, 2)$. Suppose that \bar{H} is a proper subgroup of $AGL(n, 2)$. Then applying Theorem A we get that $n = 4$, and if G denotes the subgroup of \bar{H} containing all permutations of H fixing the zero vector then $G \cong \mathcal{A}_7$.

Let s be the minimum of the arities of essential operations belonging to $\langle H \cup \{f \rangle$ and let g be an s -ary essential operation in $\langle H \cup \{f \rangle$. Since H is transitive, we can suppose that $g(0, \dots, 0) = 0$ and thus g has the form $\sum_{i=1}^s x_i A_i$. We show that $s = 2$. Suppose $s \geq 3$. If for some $j \in \{1, \dots, s\}$ there is a $k \in \{1, \dots, s\} \setminus \{j\}$ such that $\text{Im } A_j \subseteq \text{Im } A_k$ then $g(x_1, \dots, x_{k-1}, 0, x_{k+1}, \dots, x_s)$ is an $(s-1)$ -ary essential operation and it belongs to $\langle H \cup \{f \rangle$ by Lemma 3. This contradicts the assumption on s . Hence we have that $\text{Im } A_1, \text{Im } A_2 \neq V(4, 2)$, and $\text{Im } A_1 \not\subseteq \text{Im } A_2$ and $\text{Im } A_2 \not\subseteq \text{Im } A_1$. Then Lemma 7 yields a procedure for constructing an $(s-1)$ -ary essential operation, a contradiction. Hence $s = 2$, and $g(x_1, x_2) = x_1 A_1 + x_2 A_2$.

First consider the case when $\text{Im } A_1 = V(4, 2)$ (the case $\text{Im } A_2 = V(4, 2)$ can be handled similarly). Then $x_1 + x_2 A_2 = x_1 A_1^{-1} A_1 + x_2 A_2 \in \langle H \cup \{f \rangle$. Applying Lemmas 4, 5 and Lemma 3, one can easily show that there is a unary operation $B \in \langle H \cup \{f \rangle$ fixing 0 such that $\dim(\text{Im } B) = 1$, $B^2 = B$ and $x_1 + x_2 B \in \langle H \cup \{f \rangle$. Choose a basis u_1, \dots, u_4 of $V(4, 2)$ such that u_1 and u_2, u_3, u_4 are bases of $\text{Im } B$ and $\text{Ker } B$ respectively. Let $C \in G$ be such that $u_1 + u_1 C, u_2, u_3, u_4$ is again a basis of $V(4, 2)$, and let E denote the identity permutation. Then $u_1(E + BC) = u_1 + u_1 C$ and $u_i(E + BC) = u_i, i = 2, 3, 4$, implying that $E + BC$ is a permutation, and thus $E + BC \in G$. Hence for $E, E + BC \in G$ we have $u_i E = u_i(E + BC), i = 2, 3, 4$. Therefore by Proposition 1 it follows that $E = E + BC$ implying $BC = 0$, a contradiction.

Finally consider the case when $\text{Im } A_1, \text{Im } A_2 \neq V(4, 2)$. Then Lemma 7 yields a procedure for constructing a binary operation $x_1 B_1 + x_2 B_2 \in \langle H \cup \{f \rangle$ such that $\text{Im}(B_1 + B_2) = V(4, 2)$. Then $B_1 + B_2 \in G$ and the operation $h(x_1, x_2) = (x_1 B_1 + x_2 B_2)(B_1 + B_2)^{-1}$ is idempotent. Consider the operations $h_0(x_1, x_2) = h(x_1, x_2)$ and $h_n(x_1, x_2) = h_{n-1}(h(x_1, x_2), x_2)$ if $n \geq 1$. It is easy to check that there is a $t \geq 0$ such that for $h_t(x_1, x_2) = x_1 C_1 + x_2 C_2$ we have either $C_1^2 = C_1$ or

$C_1^2=0$, $C_1 \neq 0$. Since h_i is idempotent, we have that $h_i(x_1, x_2) = x_1 C_1 + x_2(E - C_1)$. If $C_1^2=0$, then $(E - C_1)^2 = E$, which shows that $\text{Im}(E - C_1) = V(4, 2)$, and this case has been settled.

Now suppose that $C_1^2 = C_1$ and consider the operation $x_1 C_1 + x_2(E - C_1)$. Let $\dim(\text{Im } C_1) = k$ and $\dim(\text{Ker } C_1) = l$. Then clearly $1 \leq k, l$ and $k + l = 4$. Choose a basis u_1, \dots, u_4 of $V(4, 2)$ such that u_1, \dots, u_k and u_{k+1}, \dots, u_4 are bases of $\text{Im } C_1$ and $\text{Ker } C_1$. From now on consider the unary linear operations fixing 0 as 4×4 matrix over $GF(2)$ in the basis u_1, \dots, u_4 . Let D be a permutation belonging to $GL(4, 2) \setminus G$. Then, by Proposition 2, there are $D_1, D_2 \in G$ such that the first k columns of D and D_1 are equal, and the last l columns of D and D_2 are equal. Then it is easy to check that $D = D_1 C_1 + D_2(E - C_1)$ and thus $D \in G$, a contradiction. This completes the proof.

5. Application

An algebra $\langle M; F \rangle$ is said to be *homogeneous* if every permutation on M is an automorphism of $\langle M; F \rangle$. In [2] B. CSÁKÁNY proved that almost all at least two element nontrivial finite algebras are functionally complete. The exceptional algebras are equivalent to one of the following six algebras:

- (1) $\langle \{0, 1\}; s \rangle$ where $s(x) = x + 1 \pmod{2}$,
- (2) $\langle \{0, 1\}; m \rangle$ where $m(x, y, z) = x + y + z \pmod{2}$,
- (3) $\langle \{0, 1\}; t \rangle$ where $t(x, y, z) = x + y + z + 1 \pmod{2}$,
- (4) $\langle \{0, 1\}; d \rangle$ where $d(x, y, z) = xy + xz + yz \pmod{2}$,
- (5) $\langle \{0, 1, 2\}; l \rangle$ where $l(x, y, z) = x - y + z \pmod{3}$,
- (6) $\langle \{0, 1\}^2; m \rangle$.

The result above was improved in [8] as follows: An at least four element nontrivial finite algebra with triply transitive automorphism group is either functionally complete or equivalent to the algebra $\langle \{0, 1\}^n; m \rangle$ for some $n \geq 2$.

A relation algebra $\langle M; R \rangle$ is said to be *relationally complete* if $[R \cup \{\{a\} \mid a \in M\}] = R_M$. As an analogue of Csákány's result R. PÖSCHEL [6] proved the following: Almost all at least two element finite nontrivial homogeneous relation algebras are relationally complete. The exceptional relation algebras are equivalent to one of the following five relation algebras:

- (1') $\langle \{0, 1\}; s' \rangle$,
- (2') $\langle \{0, 1\}; m' \rangle$,
- (3') $\langle \{0, 1\}; t' \rangle$,
- (4') $\langle \{0, 1, 2\}; l' \rangle$,
- (5') $\langle \{0, 1\}^2; m' \rangle$.

Now we apply Theorem 9 to get the analogue of the result in [8] formulated above for relation algebras, which is an improvement of Pöschel's result.

Theorem 9. *An at least four element nontrivial finite relation algebra with triply transitive automorphism group is either relationally complete or equivalent to the relation algebra $\langle\{0, 1\}^n; m'\rangle$ for some $n \geq 2$.*

Proof. Let $\langle M; R \rangle$ be a relation algebra satisfying the assumptions of the theorem. If $\langle M; R \rangle$ is not relationally complete, then

$$\begin{aligned} R_M \neq [R \cup \{\{a\} \mid a \in M\}] &= \text{Inv Pol } (R \cup \{\{a\} \mid a \in M\}) = \\ &= \text{Inv } (\text{Pol } R \cap \text{Pol } (\{\{a\} \mid a \in M\})) = \text{Inv } (I \cap \text{Pol } R) \end{aligned}$$

where clearly $I = \text{Pol } (\{\{a\} \mid a \in M\})$ is the set of all idempotent operations in O_M . It follows that $I \cap \text{Pol } R$ contains a nontrivial operation f which is evidently essential.

Now $\text{Aut } \langle M; R \rangle \cup \{f\} \subseteq \text{Pol } R$ and $\text{Pol } R \neq O_M$. Therefore, by Theorem 9, we have that there is an $n \geq 2$ such that $|A| = 2^n$ and $\text{Pol } R = \text{AGL}(n, 2)$. It is well-known (cf. e.g. [5]) that $\text{Inv } (\text{AGL}(n, 2)) = [m']$. Hence $\text{Inv Pol } R = [m']$, which was to be proved.

References

- [1] P. J. CAMERON and W. M. KANTOR, 2-transitive and antiflag transitive collineation groups of finite projective spaces, *J. Algebra*, **60** (1979), 384—422.
- [2] B. CSÁKÁNY, Homogeneous algebras are functionally complete, *Algebra Universalis*, **11** (1980), 149—158.
- [3] B. HUPPERT, *Endliche Gruppen. I*, Springer-Verlag (Berlin—Heidelberg—New York, 1967).
- [4] P. P. PÁLFY, personal communication.
- [5] R. PÖSCHEL and L. A. KALUŽNIN, *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften (Berlin, 1979).
- [6] R. PÖSCHEL, Homogeneous relational algebras are relationally complete, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland (Amsterdam, 1981); pp. 587—601.
- [7] P. SCHOFIELD, Complete subsets of mappings over a finite domain, *Proc. Camb. Phil. Soc.*, **62** (1966), 597—611.
- [8] L. SZABÓ and Á. SZENDREI, Almost all algebras with triply transitive automorphism group are functionally complete, *Acta Sci. Math.*, **41** (1979), 391—402.
- [9] L. SZABÓ and Á. SZENDREI, Słupecki-type criteria for quasilinear functions over a finite dimensional vector space, *Elektron. Informácionverarb. und Kybernet.*, **17** (1981), 601—611.

BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
6720 SZEGED, HUNGARY