J. Aust. Math. Soc. **108** (2020), 332–340
doi:10.1017/S1446788720000014

A MINIMAL CONGRUENCE LATTICE REPRESENTATION FOR $\mathbb{M}_{p+1}$

ROGER BUNN, DAVID GROW, MATT INSALL and PHILIP THIEM

(Received 25 May 2017; accepted 20 November 2019; first published online 24 March 2020)

Communicated by M. Giudici

Abstract

Let p be an odd prime. The unary algebra consisting of the dihedral group of order $2p$, acting on itself by left translation, is a minimal congruence lattice representation of $\mathbb{M}_{p+1}$.

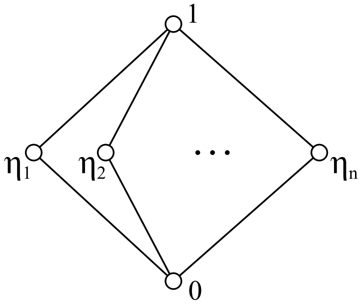
2010 *Mathematics subject classification*: primary 03G10, 06B15, 08A60, 08A62; secondary 06B15.

Keywords and phrases: universal algebra, congruence lattice representation.

1. Introduction

The finite lattice representation problem asks whether every finite lattice is isomorphic to the congruence lattice of a finite universal algebra. This problem is one of the oldest [12] and most important in universal algebra [1, 2, 4, 10, 14, 16]. Pálfy and Pudlák [15] have reduced the problem to the question, is every finite lattice isomorphic to an interval in the subgroup lattice of a finite group? Many believe this question has a negative answer [3], and much work has been directed toward finding a height-two lattice which has no such representation.

Consequently, the principal objects of this study will reside among the lattices $\mathbb{M}_n$ consisting of a least, a greatest, and n pairwise incomparable elements. That is, $\mathbb{M}_n = (M_n, \wedge, \vee)$ where $M_n = \{0, \eta_1, \ldots, \eta_n, 1\}$, $\eta_i \wedge \eta_j = 0$, and $\eta_i \vee \eta_j = 1$ if $1 \leq i < j \leq n$.



© 2020 Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

Definition 1.1. A lattice $\mathbb{L}$ is called finitely representable if there is a finite algebra $\mathbb{A} = (A, \mathfrak{F})$ such that $\mathbb{C}\mathrm{on}(\mathbb{A}) \cong \mathbb{L}$. In this case we write $\mathbb{L} \in \mathfrak{R}$ and call $\mathfrak{R}$ the class of finitely representable lattices. Define a function ϱ from $\mathfrak{R}$ into the natural numbers $\mathbb{N}$ by

$$\varrho(\mathbb{L}) = \min\{n \in \mathbb{N} : \mathbb{L} \cong \mathbb{C}\mathrm{on}(\mathbb{A}), |A| = n\}.$$

If $\mathbb{L} \in \mathfrak{R}$ then any algebra $\mathbb{A}$ for which $\mathbb{L} \cong \mathbb{C}\mathrm{on}(\mathbb{A})$ and $\varrho(\mathbb{L}) = |A|$ is called a minimal representing algebra for $\mathbb{L}$.

See [13] for a survey of those values of n for which it is known that $\mathbb{M}_n \in \mathfrak{R}$. Currently, $n = 16$ is the smallest value for which it is unknown if $\mathbb{M}_n$ is finitely representable [14]. For the particular case when $n = p + 1$ where p is prime, $\mathbb{M}_{p+1}$ is known to be finitely representable and the extant literature (e.g. [13] and [14]) uses a binary algebra with p^2 elements to represent $\mathbb{M}_{p+1}$. That is, $\varrho(\mathbb{M}_{p+1}) \leq p^2$. Our main result is the following theorem.

Theorem 1.2. *If p is an odd prime, then $\varrho(\mathbb{M}_{p+1}) = 2p$.*

In addition to obtaining optimal objects which are of intrinsic mathematical interest, the proof of the result for the infinite family $\mathbb{M}_{p+1}$ brings to the fore an interesting connection between the minimal representing algebras and automorphism groups of associated families of regular graphs (cf. [17]). Specifically, the geometric objects considered in our work are graphs, whereas previously the fundamental geometric structures used to obtain congruence lattice representations were vector spaces over finite fields. The operations in our case form subgroups of the automorphism groups of the graphs. On the other hand, the operations used for the previous representations constructed from vector spaces do not form subgroups of the automorphism groups of the vector spaces.

Numerical work by the authors on specific lattices $\mathbb{M}_n$ outside the $\mathbb{M}_{p+1}$ family suggests that this connection between minimal representing algebras and automorphism groups of regular graphs may be quite widespread. If so, it could significantly reduce the complexity of the search for a counterexample to the finite congruence lattice representation problem among the height-two lattices.

The rest of this paper is organized in the following manner. In Section 2 we introduce fundamental definitions and notation. In Section 3 we prove Theorem 3.4: if p is an odd prime then the dihedral group of order $2p$, acting on itself by left translation, forms a unary algebra whose congruence lattice is isomorphic to $\mathbb{M}_{p+1}$. Section 4 is devoted to demonstrating Theorem 4.6: if p is an odd prime and $\mathbb{A} = (A, \mathfrak{F})$ is a finite algebra such that $\mathbb{C}\mathrm{on}(\mathbb{A}) \cong \mathbb{M}_{p+1}$ then A has at least $2p$ elements. Theorem 1.2 is then is an immediate consequence.

2. Definitions and notation

For unexplained notation, definitions, and background results on universal algebras and lattices see [6, 7]. The reference [9] contains further information about graphs. For the elements of group theory, see [8].

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

Definition 2.1. Let A be a nonempty set. A nonempty subset θ of the cartesian product $A \times A$ is called an equivalence relation on A if θ is reflexive, symmetric, and transitive; that is, $(a, a) \in \theta$ for all $a \in A$, if $(a, b) \in \theta$ then $(b, a) \in \theta$, and if $(a, b) \in \theta$ and $(b, c) \in \theta$ then $(a, c) \in \theta$. The set $\mathsf{Eq}(A)$ of all equivalence relations on A forms a lattice, $\mathbb{E}\mathrm{q}(A)$, with meet operation defined by $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$ and join operation defined as follows: $(a, b) \in \theta_1 \vee \theta_2$ if and only if there exists a finite sequence $c_1, c_2, \ldots, c_n$ of elements of A such that $(c_i, c_{i+1}) \in \theta_1$ or $(c_i, c_{i+1}) \in \theta_2$ for $i \in \{1, 2, \ldots, n-1\}$ with $a = c_1$ and $b = c_n$. Furthermore, $\mathbb{E}\mathrm{q}(A)$ is a bounded lattice with least element the diagonal $\Delta = \{(a, a) : a \in A\}$ and greatest element $\nabla = A \times A$. If $S \subseteq A \times A$ then S^σ will denote the symmetric closure of S; that is, $S^\sigma = S \cup \{(b, a) : (a, b) \in S\}$.

Definition 2.2. Let $\mathbb{A} = (A, \mathfrak{F})$ be an algebra of type $\mathfrak{F}$ on a set A. A congruence θ on $\mathbb{A}$ is an equivalence relation on the set A with the following compatibility property: for every n-ary symbol $f \in \mathfrak{F}$ and $a_i, b_i \in A$, if $(a_i, b_i) \in \theta$ for $i \in \{1, 2, \ldots, n\}$ then $(f(a_1, a_2, \ldots, a_n), f(b_1, b_2, \ldots, b_n)) \in \theta$. The lattice $\mathbb{C}\mathrm{on}(\mathbb{A})$ is the set consisting of all congruences on $\mathbb{A}$ with the equivalence relation meet and join operations. If $(a, b) \in A \times A$ then $\theta(a, b)$ denotes the principal congruence in $\mathbb{C}\mathrm{on}(\mathbb{A})$ generated by (a, b). That is, $\theta(a, b)$ is the intersection of all the congruences in $\mathbb{C}\mathrm{on}(\mathbb{A})$ which contain (a, b). The θ-equivalence class $[x]_\theta$ of $x \in A$ is $\{a \in A | (a, x) \in \theta\}$.

Definition 2.3. Let $\mathbb{K}$ and $\mathbb{L}$ be lattices. A mapping $\varphi : K \to L$ which preserves the lattice operations (i.e. $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$ and $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$ for all $x, y \in K$) is called a homomorphism. In addition, if $\mathbb{K}$ and $\mathbb{L}$ are bounded lattices then we will insist such a homomorphism preserves the least and greatest elements: $\varphi(0_{\mathbb{K}}) = 0_{\mathbb{L}}$ and $\varphi(1_{\mathbb{K}}) = 1_{\mathbb{L}}$. If the homomorphism is bijective then it is called an isomorphism and we write $\mathbb{K} \cong \mathbb{L}$; if it is merely injective then it is called an embedding and we write $\mathbb{K} \hookrightarrow \mathbb{L}$.

Definition 2.4. For each integer $n > 2$, the dihedral group $\mathbb{D}_n$ of order $2n$ consists of all distance-preserving mappings of a regular polygon with n sides onto itself.

Remark 2.5. Equivalently, $\mathbb{D}_n$ is the finite group whose generators a and b have orders n and 2, respectively, and $ba = a^{-1}b$. Therefore

$$D_n = \{a^i b^j : 0 \leq i \leq n-1, 0 \leq j \leq 1\},$$

and hence $|D_n| = 2n$. Also $\mathbb{D}_n$ can be characterized as the automorphism group of an n-element cycle. As is standard in group theory, the notation $\langle a_1, \ldots, a_n \rangle$ will denote the subuniverse of a given group generated by the set of elements $\{a_1, \ldots, a_n\}$. For example, $D_n = \langle a, b \rangle$. We will abuse notation and denote the subuniverse generated by $\{a_1, \ldots, a_n\}$ and the corresponding subgroup itself by this same notation: $\langle a_1, \ldots, a_n \rangle$.

3. The algebra $(D_p, T(\mathbb{D}_p))$ and its congruence lattice

In this section the symbol $\mathbb{G}$ will always denote a group, with underlying set G. The identity of $\mathbb{G}$ will be represented by e.

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

DEFINITION 3.1. If $g \in G$, then define τ_g, the left translation by g operator, to be the mapping from G into G given by $\tau_g(x) = gx$ for all $x \in G$. Denote by $T(\mathbb{G}) = \{\tau_g : g \in G\}$ the subuniverse of the transitive group of permutations acting on the set G and form the unary algebra $\langle G, T(\mathbb{G})\rangle$. If ξ is a congruence in $\mathbb{C}\mathrm{on}\langle G, T(\mathbb{G})\rangle$, let $S_\xi = \{x \in G : (e, x) \in \xi\}$. If $\mathbb{K}$ is a subgroup of $\mathbb{G}$, let $\chi_K = \{(a, ax) : a \in G, x \in K\}$.

The next two lemmas are part of a special case of [15, Lemma 3]. They are well known and proofs can be found in [11, Lemma 4.20] and [5, Lemma 1.5A].

LEMMA 3.2. *Let $\xi \in \mathrm{Con}\langle G, T(\mathbb{G})\rangle$ and let $\mathbb{K}$ be a subgroup of $\mathbb{G}$. Then $\mathbb{S}_\xi$ is a subgroup of $\mathbb{G}$, χ_K is a congruence in $\mathbb{C}\mathrm{on}\langle G, T(\mathbb{G})\rangle$, $\chi_{S_\xi} = \xi$, and $S_{\chi_K} = K$.*

LEMMA 3.3. *If $\mathbb{H}$ and $\mathbb{K}$ are subgroups of $\mathbb{G}$ with $H \subseteq K$ then $\chi_H \subseteq \chi_K$. If η and ξ are congruences in $\mathbb{C}\mathrm{on}\langle G, T(\mathbb{G})\rangle$ with $\eta \subseteq \xi$ then $S_\eta \subseteq S_\xi$.*

THEOREM 3.4. *If p is an odd prime then $\mathbb{C}\mathrm{on}\langle D_p, T(\mathbb{D}_p)\rangle \cong \mathbb{M}_{p+1}$.*

PROOF. It follows from the previous two lemmas that the congruence lattice of $\langle G, T(\mathbb{G})\rangle$ is isomorphic to the lattice of all subgroups of $\mathbb{G}$. Now let p be an odd prime. The elements of D_p may be presented as permutations of the set $A = \{0, 1, \ldots, p-1\}$ given by

$$\{e, \sigma, \sigma^2, \ldots, \sigma^{p-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{p-1}\},$$

where above $e = \mathrm{id}_A$, $\sigma = (0, 1, \ldots, p-1)$, and $\tau = (1, p-1)(2, p-2)\cdots((p-1)/2, (p+1)/2)$. The nontrivial subgroups of $\mathbb{D}_p$ have $S = \{\sigma^k : 0 \le k < p\}$ as their subuniverses and $T_j = \{e, \tau\sigma^j\}$ for $0 \le j < p$ so the subgroup lattice of $\mathbb{D}_p$ has the form $\mathbb{M}_{p+1}$. □

4. A lower bound for $\varrho(\mathbb{M}_{p+1})$

The following two lemmas are well known and have straightforward proofs. We include the proofs for completeness.

LEMMA 4.1. *If $\mathbb{C}\mathrm{on}\langle D_n, T(\mathbb{D}_n)\rangle \cong \mathbb{M}_l$ for some integers $n > 2$ and $l > 1$, then n is prime.*

PROOF. Suppose not: suppose $n = uv$ where u and v are integers such that $1 < u, v < n$. Write $D_n = \langle a, b\rangle$ where $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$. Then

$$\langle e\rangle \subsetneq \langle a^u\rangle \subsetneq \langle a\rangle \subsetneq D_n,$$

so Lemmas 3.2 and 3.3 imply $\chi_{\langle a^u\rangle}$ and $\chi_{\langle a\rangle}$ are congruences in $\mathbb{C}\mathrm{on}\langle D_n, T(\mathbb{D}_n)\rangle$ such that

$$\Delta = \chi_{\langle e\rangle} \subsetneq \chi_{\langle a^u\rangle} \subsetneq \chi_{\langle a\rangle} \subsetneq \chi_{D_n} = \nabla.$$

But this contradicts $\mathbb{C}\mathrm{on}\langle D_n, T(\mathbb{D}_n)\rangle \cong \mathbb{M}_l$. □

LEMMA 4.2. *Let $\langle \mathfrak{F}, \circ\rangle$ be a group of permutations acting transitively on a set A. Then for each congruence $\theta \in \mathrm{Con}\langle A, \mathfrak{F}\rangle$, the cardinalities of all θ-equivalence classes are the same.*

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

Proof. Let θ be a congruence in $\mathbb{C}\mathrm{on}(A, \mathfrak{F})$. Note that $[\sigma(a)]_\theta = \sigma[[a]_\theta]$ for all $\sigma \in \mathfrak{F}$ and all $a \in A$. The desired conclusion is then immediate since $(\mathfrak{F}, \circ)$ acts transitively on A. □

Next we introduce a loopless, undirected graph in which edges are two-element sets. This graph will be crucial in demonstrating Theorem 4.6.

Definition 4.3. Let $\mathbb{A} = (A, \mathfrak{F})$ be an algebra for which there exist distinct congruences θ_1 and θ_2 in $\mathbb{C}\mathrm{on}(A, \mathfrak{F})$ such that

(1) $\theta_1 \wedge \theta_2 = \Delta$; and

(2) all equivalence classes modulo θ_j $(j = 1, 2)$ have cardinality 2.

Define a graph $\Gamma(\mathbb{A}, \theta_1, \theta_2) = (A, \mathcal{E})$ by setting

$$\mathcal{E} = \{[x]_{\theta_1} : x \in A\} \cup \{[y]_{\theta_2} : y \in A\}.$$

For the convenience of the reader, the following observation is labelled as a lemma.

Lemma 4.4. *The graph $\Gamma(\mathbb{A}, \theta_1, \theta_2)$ of Definition 4.3 is a loopless graph, each vertex of which has degree 2, and possesses the property that if $\{x, y\}$ and $\{y, z\}$ belong to $\mathcal{E}$, $x \neq z$, and $(x, y) \in \theta_1$ then $(y, z) \in \theta_2$.*

The next lemma is fundamental to the proof of Theorem 4.6.

Lemma 4.5. *Let $\mathbb{A} = (A, \mathfrak{F})$ be a finite unary algebra with at least three elements and let $(\mathfrak{F}, \circ)$ be a group of permutations acting transitively on A. Suppose there exist distinct congruences θ_1 and θ_2 in $\mathbb{C}on(\mathbb{A})$ such that all equivalence classes modulo θ_j $(j = 1, 2)$ have cardinality 2, $\theta_1 \wedge \theta_2 = \Delta$, and $\theta_1 \vee \theta_2 = \nabla$. Then $k = |A|$ is even and $(\mathfrak{F}, \circ)$ is isomorphic to the dihedral group $\mathbb{D}_{k/2}$.*

Proof. Since A is finite,

$$|A| = \left| \bigcup_{\varepsilon \in A/\theta_1} \varepsilon \right| = \sum_{\varepsilon \in A/\theta_1} |\varepsilon| = 2|A/\theta_1|,$$

so $k = |A|$ is an even integer. Let $(A, \mathcal{E})$ be the graph constructed in Definition 4.3 and fix an element $x_1 \in A$. For each $j \in \{1, \dots, k-1\}$, let x_{j+1} be the unique member of $A \setminus \{x_1, \dots, x_j\}$ such that the doublet $\{x_j, x_{j+1}\}$ is

$$[x_j]_{\theta_1} \text{ if } j \text{ is odd, and } [x_j]_{\theta_2} \text{ if } j \text{ is even.}$$

Note that $\{x_k, x_1\} \in \mathcal{E}$; in fact, $\{x_k, x_1\} = [x_1]_{\theta_2}$.

The rest of the proof consists of showing the following:

(1) the elements of $A = \{x_1, x_2, \dots, x_k\}$ are the vertices of the graph;

(2) the only edges in the graph are between x_i and x_{i+1} for $1 \leq i \leq k$;

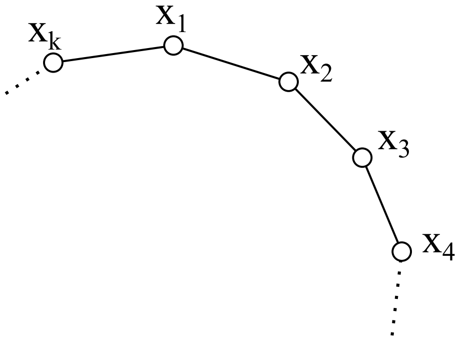
(3) $(x_{2j-1}, x_{2j}) \in \theta_1$ and $(x_{2j}, x_{2j+1}) \in \theta_2$ for $1 \leq j \leq k/2$;

(4) the graph $(A, \mathcal{E})$ is a cycle.

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

(In (2) and (3) we have used the notation $x_{k+1} = x_1$.)

The component of the graph $(A, \mathcal{E})$ that includes x_1 as a vertex is a cycle because A is finite and the graph is of degree 2. We will show that under the conditions $\theta_1 \wedge \theta_2 = \Delta$, and $\theta_1 \vee \theta_2 = \nabla$, this is the only component of the graph $(A, \mathcal{E})$; that is, $(A, \mathcal{E})$ is a cycle.



Let m be the smallest positive integer such that $x_{m+1} \in \{x_1, x_2, \ldots, x_m\}$. Assume, by way of contradiction, that $x_{m+1} \neq x_1$. Let $x_{m+1} = x_j$, where $1 < j < m$. Note that $[x_j]_{\theta_1} \cup [x_j]_{\theta_2} = \{x_{j-1}, x_j, x_{j+1}\}$. But $x_m \in [x_j]_{\theta_1} \cup [x_j]_{\theta_2}$ with $x_m \neq x_j$ and $x_m \neq x_{j-1}$ by minimality of m. Hence $x_m = x_{j+1}$. If $(x_j, x_m) = (x_j, x_{j+1}) \in \theta_1$ then $(x_m, x_j) = (x_m, x_{m+1}) \in \theta_2$. Thus $(x_j, x_m) \in \theta_1 \cap \theta_2 = \Delta$, so $x_j = x_m$, a contradiction. A similar argument when $(x_j, x_m) \in \theta_2$ also yields a contradiction. Thus $x_{m+1} = x_1$, so $(x_m, x_1) \in \theta_2$.

Let $q \in A$. The pair $(x_1, q) \in \nabla = \theta_1 \vee \theta_2$ so there is a path from x_1 to q of the form

$$(x_1, y_1) \in \theta_1, (y_1, y_2) \in \theta_2, (y_2, y_3) \in \theta_1, \ldots, (y_{n-1}, y_n) = (y_{n-1}, q) \in \theta_2$$

or

$$(x_1, y_1) \in \theta_2, (y_1, y_2) \in \theta_1, (y_2, y_3) \in \theta_2, \ldots, (y_{n-1}, y_n) = (y_{n-1}, q) \in \theta_1.$$

It follows that $y_1 \in \{x_1, x_2, x_m\}$ and immediately $y_i \in \{x_1, \ldots, x_m\}$ for all i. Consequently, $q \in \{x_1, \ldots, x_m\}$, $k = m$, and $A = \{x_1, x_2, \ldots, x_k\}$.

To show that $(\mathfrak{F}, \circ)$ is isomorphic to $\mathbb{D}_{k/2}$, we will first show that up to isomorphism, $(\mathfrak{F}, \circ)$ is a subgroup of $\mathbb{D}_k$. Since the graph $(A, \mathcal{E})$ is a cycle, we may identify the elements of A with the vertices in a regular k-gon in the obvious manner. Let $\sigma \in \mathfrak{F}$ and $(x_i, x_{i+1}) \in \theta_l$; then $(x_m, x_n) = (\sigma(x_i), \sigma(x_{i+1})) \in \theta_l$, so $n \in \{m+1, m-1\}$. Thus σ maps adjacent vertices in the graph $(A, \mathcal{E})$ to adjacent vertices. That is, $(\mathfrak{F}, \circ)$ is (isomorphic to) a subgroup of $\mathbb{D}_k$, the group of all distance-preserving mappings of a regular k-gon onto itself.

We will now show that $\mathbb{D}_{k/2} \cong (\mathfrak{F}, \circ)$. We begin by noting that the rotation in D_k that maps x_1 to x_2 does not belong to $\mathfrak{F}$. For suppose $\mu \in \mathfrak{F}$ and $\mu(x_1) = x_2$. Then $(x_1, x_2) \in \theta_1$ implies $(x_2, \mu(x_2)) = (\mu(x_1), \mu(x_2)) \in \theta_1$. Hence $\mu(x_2) = x_1$ so μ cannot be a rotation in D_k since $k > 2$. Next, we claim that the reflection in D_k that maps x_1 to x_2 is the only element of $\mathfrak{F}$ that maps x_1 to x_2. Since $(\mathfrak{F}, \circ)$ acts transitively, there exists $\sigma \in \mathfrak{F}$ such that $\sigma(x_1) = x_2$. But a previous argument shows that $\sigma(x_2) = x_1$.

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

A simple induction argument then shows $\sigma(x_i) = x_{k+3-i}$ and $\sigma(x_{k+3-i}) = x_i$ for all $2 \le i \le 1 + (k/2)$. That is, σ is the unique reflection in D_k that maps x_1 to x_2. It is not hard to see that the rotation in D_k which maps x_1 to x_3 belongs to $\mathfrak{F}$. For by transitivity of $(\mathfrak{F}, \circ)$ acting on A, there exists $\rho \in \mathfrak{F}$ such that $\rho(x_1) = x_3$. Suppose $\rho : A \to A$ is a reflection in D_k. Then $\rho^2 = \mathrm{id}_A$, so $\rho(x_3) = x_1$ and $\rho(x_2) = x_2$. But $(x_2, x_3) \in \theta_2$ implies $(\rho(x_2), x_1) = (\rho(x_2), \rho(x_3)) \in \theta_2$. Therefore $\rho(x_2) = x_k$ and hence $x_2 = x_k$, contradicting $k > 2$. Since $(x_1, x_2) \in \theta_1$, it follows that $(x_3, \rho(x_2)) = (\rho(x_1), \rho(x_2)) \in \theta_1$. Thus, $\rho(x_2) = x_4$. A simple induction shows that ρ is the unique rotation in D_k that maps x_1 to x_3. In particular, it follows that $\rho^{k/2} = \mathrm{id}_A$ and $\rho^i \neq \mathrm{id}_A$ for all $0 < i < k/2$. Next, let τ denote the unique rotation in D_k that maps x_1 to x_2. Observe that the order of τ is k and recall that σ is a reflection, so its order is 2. We claim that $\sigma\tau = \tau^{-1}\sigma$. This follows from the fact that if $1 \le i \le k$, then

$$\tau\sigma\tau(x_i) = \tau\sigma(x_{i+1}) = \tau(x_{k+3-(i+1)}) = \tau(x_{k+2-i}) = x_{k+3-i} = \sigma(x_i).$$

Consequently, $D_k = \langle \tau, \sigma \rangle$. Since $\tau^2 = \rho$, it follows that $\sigma\rho = \sigma\tau^2 = \tau^{-2}\sigma = \rho^{-1}\sigma$. Because $o(\rho) = k/2$ and $o(\sigma) = 2$, we have

$$\mathbb{D}_{k/2} \cong \langle \rho, \sigma \rangle \le (\mathfrak{F}, \circ) \lneq \mathbb{D}_k.$$

Furthermore, $[\langle \rho, \sigma \rangle : \mathbb{D}_k] = 2$, so $\langle \rho, \sigma \rangle$ is a maximal proper subgroup of $\mathbb{D}_k$. Thus $\langle \rho, \sigma \rangle = (\mathfrak{F}, \circ)$. □

Theorem 4.6. *If p is an odd prime and $\mathbb{A} = (A, \mathfrak{F})$ is a finite algebra such that $\mathbb{C}on(\mathbb{A}) \cong \mathbb{M}_{p+1}$, then A has at least $2p$ elements.*

Proof. Let $\mathbb{A} = (A, \mathfrak{F})$ be an algebra such that $\mathbb{C}on(\mathbb{A}) \cong \mathbb{M}_{p+1}$ and $\rho(\mathbb{M}_{p+1}) = |A|$. By Theorem 1 of Pálfy and Pudlák [15], we may assume that $\mathbb{A}$ is a unary algebra and $(\mathfrak{F}, \circ)$ is a group of permutations acting transitively on the set A.

We assert that there must be at least two distinct congruences in $\mathbb{C}on(\mathbb{A})$ in which all the congruence class sizes are equal to 2. For $1 \le i \le p + 1$, let ξ_i denote the $p + 1$ distinct congruences in $\mathrm{Con}(\mathbb{A}) \setminus \{\Delta, \nabla\}$. Suppose there were just one such congruence, say ξ_1, which had all congruence equivalence classes of size equal to 2. Fix an element $x_1 \in A$ and count the number of elements in $[x_1]_{\xi_i}$ for each $1 \le i \le p + 1$. There exists only one other element in $[x_1]_{\xi_1}$ besides x_1; label it x_2. For each $2 \le i \le p + 1$, there exist at least two other distinct elements in $[x_1]_{\xi_i}$ different from x_1; label them x_{2i-1} and x_{2i}. This produces a list of elements $x_1, x_2, x_3, x_4, \ldots, x_{2p+1}, x_{2p+2}$ in A. Since $\xi_i \wedge \xi_j = \Delta$ for $i \neq j$, it follows that all these elements in A are distinct. Consequently, A has at least $2p + 2$ elements, contradicting minimal cardinality of the representing algebra for $\mathbb{M}_{p+1}$ in light of Theorem 3.4. A similar argument shows that if no congruence among $\xi_1, \xi_2, \xi_3, \ldots, \xi_{p+1}$ had all congruence classes of size 2 then $|A| \ge 2p + 3$, again a contradiction.

Thus there exist two distinct congruences θ_1 and θ_2 in $\mathbb{C}on(\mathbb{A})$ such that all equivalence classes modulo θ_j $(j = 1, 2)$ have cardinality 2. By Lemma 4.5, $|A| = k = |D_{k/2}| = |\mathfrak{F}|$. Consequently, the algebra $(A, \mathfrak{F})$ is isomorphic to $(D_{k/2}, T(\mathbb{D}_{k/2}))$. It follows that

$$\mathbb{M}_{p+1} \cong \mathbb{C}on(A, \mathfrak{F}) \cong \mathbb{C}on(D_{k/2}, T(\mathbb{D}_{k/2})).$$

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

Lemma 4.1 shows that $k/2 = q$ for some prime number q. Theorem 3.4 then implies $q = p$ and hence $|A| = k = 2p$. □

References

[1] J. Alm and J. Snow, ‘Lattices of equivalence relations closed under the operations of relation algebras’, *Algebra Univers.* **71** (2014), 187–190.

[2] M. Aschbacher, ‘Overgroups of primitive groups, II’, *J. Algebra* **322** (2009), 1586–1626.

[3] R. Baddely, ‘A new approach to the finite lattice representation problem’, *Period. Math. Hungar.* **36** (1998), 17–59.

[4] W. DeMeo, ‘Expansions of finite algebras and their congruence lattices’, *Algebra Universalis* **69** (2013), 257–278.

[5] J. D. Dixon and B. Mortimer, *Permutation Groups* (Springer, New York, 1996).

[6] G. Grätzer, *Universal Algebra*, 2nd edn (Springer, New York, 1979).

[7] G. Grätzer, *General Lattice Theory*, 2nd edn (Birkhäuser, Basel, 1998).

[8] M. Hall, *The Theory of Groups* (Macmillan, New York, 1959).

[9] F. Harary, *Graph Theory* (Addison-Wesley, Reading, MA, 1969).

[10] A. Lucchini, ‘Representation of certain lattices as intervals in subgroup lattices’, *J. Algebra* **164** (1994), 85–90.

[11] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices, Varieties*, Wadsworth & Brooks/Cole Mathematics Series, vol. I (Wadsworth & Brooks/Cole, Monterey, CA, 1987).

[12] G. F. McNulty, ‘A juggler’s dozen of easy problems’, *Algebra Universalis* **74** (2015), 17–34.

[13] P. P. Pálfy, ‘Intervals in subgroup lattices of finite groups’, in: *Groups ’93 Galway/St. Andrews, Vol. 2*, London Mathematical Society Lecture Note Series, 212 (Cambridge University Press, Cambridge, 1995), 482–494.

[14] P. P. Pálfy, ‘Groups and lattices’, in: *Groups ’01 St. Andrews/Oxford, Vol. 2*, London Mathematical Society Lecture Note Series, 305 (Cambridge University Press, Cambridge, 2003), 428–454.

[15] P. P. Pálfy and P. Pudlák, ‘Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups’, *Algebra Universalis* **11** (1980), 22–27.

[16] J. Snow, ‘A constructive approach to the finite congruence lattice representation problem’, *Algebra Universalis* **43** (2000), 279–293.

[17] M. G. Stone and R. H. Weedmark, ‘On representing $\mathbb{M}_n$’s by congruence lattices of finite algebras’, *Discrete Math.* **44** (1983), 299–308.

ROGER BUNN, Missouri State University,
901 South National Avenue, Springfield,
MO 65897, USA
e-mail: RogerBunn@missouristate.edu

DAVID GROW, Missouri University of Science and Technology,
202 Rolla Building, Rolla,
MO 65409-0020, USA
e-mail: grow@mst.edu

MATT INSALL, Missouri University of Science and Technology,
Mathematics & Statistics,
400 W 12th Street, Room 315 Rolla Building,
Rolla, MO 65409, USA
e-mail: insall@mst.edu

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press

PHILIP THIEM, Missouri University of Science and Technology,
202 Rolla Building, Rolla,
MO 65409-0020, USA
e-mail: ptt@mst.edu

https://doi.org/10.1017/S1446788720000014 Published online by Cambridge University Press