ON A PROBLEM OF PÁLFY AND SAXL

WILLIAM DEMEO

Abstract. Among the oldest open questions in universal algebra is the following: which finite lattices are congruence lattices of finite algebras? In this note we consider a related problem about a special class of lattice, namely, the "diamonds" M_n, which are height-two modular lattice with n atoms. In [1], Péter Pálfy and Jan Saxl proved, using deep results from group theory, that if a finite algebra has a and congruence lattice isomorphic to M_n $(n > 3)$, and at least three atoms pairwise permute, then $n - 1$ is a power of a prime number. In the process, they also showed that if a G-set has an M_n $(n > 3)$ congruence lattice and at least 3 atoms pairwise permute, then all congruences permute.

Pálfy and Saxl leave open the following question: if a finite algebra has congruence lattice M_n $(n > 3)$, and if at least 3 atoms pairwise permute, does it follow that all congruences permute? In this note, we present some of the background required understand Pálfy and Saxl's question, including some tame congruence theory that dispenses with an "easy" case of the question. We then discuss a strategy that we hope will lead to a solution in the harder case.

1. Introduction

This paper mainly concerns lattices of the form displayed in Figure 1. In the

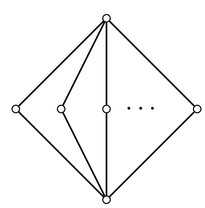


Figure 1. The lattice M_n has n "atoms" for a total of $n + 2$ elements.

paper [1], Péter Pálfy and Jan Saxl pose the following:

> Problem. Let $\mathbf{A}$ be a finite algebra with $\operatorname{Con}\mathbf{A} \cong M_n$, $n \geqslant 4$. If three nontrivial congruences of $\mathbf{A}$ pairwise permute, does it follow that every pair of congruences of $\mathbf{A}$ permute?

In this note we answer this question affirmatively for a special class of algebras—namely, those that live in a *Taylor variety*, which is a variety satisfying a nontrivial idempotent Malcev condition. Thereafter, we consider the general problem and give some examples to guide intuition and suggest some possible solution strategies.

Date: February 15, 2016.

1.1. **Notation.** Throughout, X denotes a finite set and $\mathrm{Eq}(X)$ denotes the lattice of equivalence relations on X. For $\alpha \in \mathrm{Eq}(X)$ and $x \in X$, we let x/α denote the equivalence class of α containing x, and X/α denotes the set of all equivalence classes of α. That is,

$$x/\alpha = \{y \in X : x \mathrel{\alpha} y\} \quad \text{and} \quad X/\alpha = \{x/\alpha : x \in X\}.$$

The largest and smallest equivalence relations on X are denoted by $1_X = X^2$ and $0_X = \{(x,x) : x \in X\}$, respectively. We say that α and β are *complementary* equivalence relations on X provided $\alpha \vee \beta = 1_X$ and $\alpha \wedge \beta = 0_X$.

We often refer to equivalence classes as "blocks." For a given $\alpha \in \mathrm{Eq}(X)$, the number of blocks of α is $|X/\alpha|$. The map $\varphi_\alpha : x \mapsto x/\alpha$ is a function from X into the power set $\mathscr{P}(X)$ with kernel $\ker \varphi_\alpha = \alpha$. The *block-size function* $x \mapsto |x/\alpha|$ is a function from X into $\{1, 2, \dots, |X|\}$.

We will often abuse notation and identify an equivalence relation with the corresponding partition of the set X. For example, if $X = \{0,1,2,3,4\}$, we identify the relation

$$\alpha = \{(0,0),(1,1),(2,2),(3,3),(4,4),(0,1),(1,0),(2,3),(3,2)\}$$

with the partition $|0,1|2,3|4|$, and will even write $\alpha = |0,1|2,3|4|$. Using this example to illustrate the notation above, we have $\varphi_\alpha(0) = 0/\alpha = \{0,1\} = 1/\alpha = \varphi_\alpha(1)$. Similarly, $\varphi_\alpha(2) = \{2,3\} = \varphi_\alpha(3)$, and $\varphi_\alpha(4) = 4/\alpha = \{4\}$. Thus, we have $X/\alpha = \{\{0,1\},\{2,3\},\{4\}\}$, so $|X/\alpha| = 3$ in this case.

We say that α has *uniform blocks* if all blocks of α have the same size; or, equivalently, the block-size function is constant: for all $x, y \in X$, $|x/\alpha| = |y/\alpha|$. In this case we will use $|x/\alpha|$ without specifying a particular x to denote this block size. Thus, if α has uniform blocks, then

$$|X| = |x/\alpha|\,|X/\alpha| \quad (\text{for all } x \in X).$$

We say that two equivalence relations with uniform blocks have *compatible uniform block structure* (CUBS) if the number of blocks of one is equal to the block size of the other. That is, α and β have CUBS iff $|x/\alpha||y/\beta| = |X|$ (for all x and y).

If α and β are binary relations on X, then the relation

$$\alpha \circ \beta = \{(x,y) \in X^2 : \exists z \,.\, x \mathrel{\alpha} z \mathrel{\beta} y\} \tag{1.1}$$

is called the *composition of* α *and* β. Obviously, $(x,y) \in \alpha \circ \beta$ iff $(y,x) \in \beta \circ \alpha$. If $\alpha \circ \beta = \beta \circ \alpha$, then we call α and β *permuting* relations and we say that α and β *permute*.

In this paper, we are mostly concerned with the set $\mathrm{Eq}(X)$ of equivalence relations on X. $\mathrm{Eq}(X)$ is a lattice if we define, for $\alpha, \beta \in \mathrm{Eq}(X)$, the meet $\alpha \wedge \beta$ to be the usual intersection of sets α and β and the join $\alpha \vee \beta$ to be the equivalence relation generated by α and β, that is, the smallest equivalence relation containing both α and β. It is not too difficult to prove that $\alpha \vee \beta$ is equal to

$$\alpha \vee \beta = (\alpha \circ \beta) \cup (\alpha \circ \beta \circ \alpha) \cup (\alpha \circ \beta \circ \alpha \circ \beta) \cup \cdots$$

and that $\alpha \circ \beta \subseteq \alpha \vee \beta$, with equality if and only if α and β permute. Note that, if α and β do not permute, then the relation $\alpha \circ \beta$ is not symmetric, and therefore is not an equivalence relation. Nonetheless, we will abuse the notation $x/\alpha \circ \beta$ in such cases, and define

$$x/\alpha \circ \beta := \{y \in X : \exists z \,.\, x \mathrel{\alpha} z \mathrel{\beta} y\} \;\text{ and }\; \alpha \circ \beta \backslash x := \{y \in X : \exists z \,.\, y \mathrel{\alpha} z \mathrel{\beta} x\}.$$

Although these are not necessarily equivalence classes, they are well-defined subsets of X. From the definition (1.1) it is clear that $(x,y) \in \alpha \circ \beta$ if and only if $y \in z/\beta$ for some $z \in x/\alpha$. Thus, for every $x \in X$,

$$x/\alpha \circ \beta = \bigcup_{z \in x/\alpha} z/\beta. \tag{1.2}$$

Furthermore, α and β are permuting equivalence relations iff for each $x \in X$ we have $x/\alpha \circ \beta = \alpha \circ \beta \backslash x$.

We conclude this subsection with one more definition that is nonstandard but is quite useful for our application. If Γ is a set of equivalence relations, we say that Γ consists of *pairwise-permuting pairwise-complements* (PPPC) if the following conditions hold for all $\gamma \neq \delta$ in Γ:

(i) $\gamma \vee \delta = 1_X$;
(ii) $\gamma \wedge \delta = 0_X$;
(iii) $\gamma \circ \delta = \delta \circ \gamma$.

1.2. **Basic observations.**

Lemma 1. Suppose α and β are complementary equivalence relations on X. Then α and β permute if and only if they have CUBS. That is,

$$\alpha \circ \beta = 1_X \quad \Longleftrightarrow \quad (\forall x)(\forall z)\ |x/\alpha||z/\beta| = |X|. \tag{1.3}$$

Corollary 1. Suppose α_1, α_2, α_3 are pairwise complementary equivalence relations on the finite set X. Then α_1, α_2, α_3 pairwise permute if and only if they have uniform blocks of size $\sqrt{|X|}$. That is,

$$(\forall i)(\forall j)\,(i \neq j \longrightarrow \alpha_i \circ \alpha_j = 1_X) \quad \Longleftrightarrow \quad (\forall i)(\forall x)\,|x/\alpha_i| = \sqrt{|X|}.$$

In this case, $|x/\alpha_i| = |X/\alpha_i|$.

Proof of Lemma 1. Suppose α and β are complementary equivalence relations. Then, since $\alpha \wedge \beta = 0_X$, the union in (1.2) is disjoint; we denote this by writing

$$x/(\alpha \circ \beta) = \coprod_{z \in x/\alpha} z/\beta. \tag{1.4}$$

Also, since $\alpha \circ \beta = \alpha \vee \beta = 1_X$, we have $x/(\alpha \circ \beta) = X$ for every $x \in X$. Thus the union in (1.4) is all of X, so every block of β appears in this union. It follows that the size of the block x/α is exactly the number $|X/\beta|$ of blocks of β. That is, $|x/\alpha| = |X/\beta|$. As x was arbitrary, α has uniform blocks of size $|X/\beta|$. Observe that, since α has uniform blocks, we have

$$|x/\alpha|\,|X/\alpha| = |X|. \tag{1.5}$$

The same argument with the roles of α and β swapped gives $|x/\beta| = |X/\alpha|$. Thus, for all $x, z \in X$ we have

$$|x/\alpha|\,|z/\beta| = |x/\alpha|\,|X/\alpha| = |X/\beta|\,|X/\alpha|.$$

This and (1.5) imply $|x/\alpha|\,|z/\beta| = |X|$, as desired.

To prove the converse, suppose α and β have CUBS. Then $|x/\alpha|\,|y/\beta| = |X|$, so $|y/\beta| = |x/\alpha|^{-1}|X| = |X/\alpha|$, for all $x, y \in X$. Therefore,

$$\big|x/(\alpha \circ \beta)\big| = \Big|\coprod_{y \in x/\alpha} y/\beta\Big| = \sum_{y \in x/\alpha} |y/\beta| = \sum_{y \in x/\alpha} |X/\alpha| = |x/\alpha|\,|X/\alpha| = |X|,$$

for all $x \in X$. This proves $\alpha \circ \beta = 1_X$, as desired. □

Proof of Cor. 1. Let $\alpha_1, \alpha_2, \alpha_3$ be pairwise complementary equivalence relations. ($\Rightarrow$) Assume $\alpha_1, \alpha_2, \alpha_3$ are pairwise permuting (hence, PPPC). Then, by Lemma 1,

$$\begin{aligned}
|x/\alpha_1|\,|x/\alpha_2| &= |X|\\
|x/\alpha_1|\,|x/\alpha_3| &= |X|\\
|x/\alpha_2|\,|x/\alpha_3| &= |X|.
\end{aligned}$$

By the third of these equations, we have $|x/\alpha_3| = |x/\alpha_2|^{-1}|X|$. Substituting this into the second equation gives $|x/\alpha_1|\,|x/\alpha_2|^{-1}|X| = |X|$, or $|x/\alpha_2| = |x/\alpha_1|$. Substituting this into the first equation gives $|x/\alpha_1| = \sqrt{|X|}$. This can finally be substituted back into the second and third equations to arrive at $|x/\alpha_2| = \sqrt{|X|} = |x/\alpha_3|$.
($\Leftarrow$) The right-to-left direction follows immediately from the right-to-left direction in (1.3). $\square$

Define the set $\mathcal{S} \subseteq \operatorname{Eq}(X)$ as follows:

$$\mathcal{S} = \{\alpha \in \operatorname{Eq}(X) : (\forall x)\ |x/\alpha| = \sqrt{|X|} = |X/\alpha|\}.$$

From Corollary 1 we see that the Pálfy-Saxl problem can be rephrased as follows:

> Problem. Let $\mathbf{A}$ be a finite algebra with $\operatorname{Con}\mathbf{A} \cong M_n$, $n \geqslant 4$. If the set $\mathcal{S}$ contains three atoms of $\operatorname{Con}\mathbf{A}$, does it follow that $\mathcal{S}$ contains every atom of $\operatorname{Con}\mathbf{A}$?

To prove that the answer is "yes," it suffices to show that whenever $M_n \cong L \leqslant \operatorname{Eq}(X)$ has 3 atoms in $\mathcal{S}$ and an atom β with $|x/\beta| < \sqrt{|X|}$, then L is not a congruence lattice.

1.3. **Clones and tolerances.** Let $\mathbf{A} = \langle A, \dots\rangle$ be an algebra with congruence lattice $\operatorname{Con}\langle A, \dots\rangle$. Recall that a *clone* on a non-void set A is a set of operations on A that contains the projection operations and is closed under compositions. The *clone of term operations* of the algebra $\mathbf{A}$, denoted by $\operatorname{Clo}\mathbf{A}$, is the smallest clone on A containing the basic operations of $\mathbf{A}$. The *clone of polynomial operations* of $\mathbf{A}$, denoted by $\operatorname{Pol}\mathbf{A}$, is the clone generated by the basic operations of $\mathbf{A}$ and the constant unary maps on A. The set of n-ary members of $\operatorname{Pol}\mathbf{A}$ is denoted by $\operatorname{Pol}_n\mathbf{A}$. It often simplifies matters to shift our attention away from the basic operations of $\mathbf{A}$ and focus instead on $\operatorname{Clo}\mathbf{A}$ or $\operatorname{Pol}\mathbf{A}$, or even $\operatorname{Pol}_1\mathbf{A}$. If our primary interest is the congruence lattice $\operatorname{Con}\mathbf{A}$, this is not a limitation because of the following fact: $\operatorname{Con}\langle A, \dots\rangle = \operatorname{Con}\langle A, \operatorname{Clo}\mathbf{A}\rangle = \operatorname{Con}\langle A, \operatorname{Pol}\mathbf{A}\rangle = \operatorname{Con}\langle A, \operatorname{Pol}_1\mathbf{A}\rangle$. For proof, see e.g. [4, Theorem 4.18].

A reflexive, symmetric, compatible binary relation $T \subseteq A^2$ is called a *tolerance of* $\mathbf{A}$. Any congruence relation of an algebra is a tolerance, and the transitive closure of any tolerance is a congruence relation. We call a tolerance of $\mathbf{A}$ *connected* if its transitive closure is all of A^2. As a compatible and binary relation, a tolerance induces a subalgebra of $\mathbf{A}^2$, so we often denote a tolerances with boldface letters, as in $\mathbf{T} \leqslant \mathbf{A}^2$. If we have a pair $(\mathbf{u}, \mathbf{v}) \in A^m \times A^m$ of m-tuples of A, then we write $\mathbf{u}\ \underline{\mathbf{T}}\ \mathbf{v}$ just in case $\mathbf{u}(i)\ \mathbf{T}\ \mathbf{v}(i)$ for all $i \in \underline{m}$.

1.4. **Centralizers and Abelian Algebras.** We will need some basic facts about abelian algebras. Let $\mathbf{A} = \langle A, F^{\mathbf{A}}\rangle$ be an algebra. Suppose $\mathbf{S}$ and $\mathbf{T}$ are tolerances on $\mathbf{A}$. An $\mathbf{S},\mathbf{T}$-*matrix* is a 2×2 array of the form

$$\begin{bmatrix} t(\mathbf{a},\mathbf{u}) & t(\mathbf{a},\mathbf{v}) \\ t(\mathbf{b},\mathbf{u}) & t(\mathbf{b},\mathbf{v}) \end{bmatrix},$$

where t, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$, $\mathbf{v}$ have the following properties:

(i) $t \in \operatorname{Clo}_{\ell+m} \mathbf{A}$,
(ii) $(\mathbf{a},\mathbf{b}) \in A^\ell \times A^\ell$ and $\mathbf{a} \mathrel{\underline{\mathbf{S}}} \mathbf{b}$,
(iii) $(\mathbf{u},\mathbf{v}) \in A^m \times A^m$ and $\mathbf{u} \mathrel{\underline{\mathbf{T}}} \mathbf{v}$.

Let δ be a congruence relation of $\mathbf{A}$. If the entries of every $\mathbf{S},\mathbf{T}$-matrix satisfy

$$t(\mathbf{a},\mathbf{u}) \mathrel{\delta} t(\mathbf{a},\mathbf{v}) \quad\Longleftrightarrow\quad t(\mathbf{b},\mathbf{u}) \mathrel{\delta} t(\mathbf{b},\mathbf{v}), \tag{1.6}$$

then we say that $\mathbf{S}$ *centralizes* $\mathbf{T}$ *modulo* δ and we write $\mathsf{C}(\mathbf{S},\mathbf{T};\delta)$. That is, $\mathsf{C}(\mathbf{S},\mathbf{T};\delta)$ holds iff (1.6) holds *for all* ℓ, m, t, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$, $\mathbf{v}$ satisfying properties (i)–(iii). The condition $\mathsf{C}(\mathbf{S},\mathbf{T};0_{\mathbf{A}})$ is sometimes called the $\mathbf{S},\mathbf{T}$-*term condition*, and when it holds we say that $\mathbf{S}$ *centralizes* $\mathbf{T}$, and write $\mathsf{C}(\mathbf{S},\mathbf{T})$. A tolerance $\mathbf{T}$ is called *abelian* if $\mathsf{C}(\mathbf{T},\mathbf{T})$. An algebra $\mathbf{A}$ is called *abelian* if $1_{\mathbf{A}}$ is abelian.

Remark. An algebra $\mathbf{A}$ is abelian iff $\mathsf{C}(1_{\mathbf{A}},1_{\mathbf{A}})$ iff

$$\forall \ell \in \{0,1,2,\dots\},\quad \forall m \in \{1,2,\dots\},\quad \forall t \in \operatorname{Clo}_{\ell+m}\mathbf{A},\quad \forall (a,b) \in A^\ell \times A^\ell,$$
$$\ker t(a,\cdot) = \ker t(b,\cdot).$$

1.5. **Facts.** We now collect some useful facts about centralizers of congruence relations. These facts are well-known and easy to prove. (See, for example, [2].)

Lemma 2. *Let $\mathbf{A}$ be an algebra with congruences $\alpha,\beta,\gamma,\alpha',\beta' \in \operatorname{Con}(\mathbf{A})$, and let $\mathbf{B}$ be a subalgebra of $\mathbf{A}$. Then,*

(1) $\mathsf{C}(\alpha,\beta;\alpha\wedge\beta)$;
(2) if $\mathsf{C}(\alpha,\beta;\gamma)$ and $\mathsf{C}(\alpha,\beta;\gamma')$, then $\mathsf{C}(\alpha,\beta;\gamma\wedge\gamma')$;
(3) if $\mathsf{C}(\alpha,\beta;\gamma)$ and $\mathsf{C}(\alpha',\beta;\gamma)$, then $\mathsf{C}(\alpha\vee\alpha',\beta;\gamma)$;
(4) if $\mathsf{C}(\alpha,\beta;\gamma)$ and $\alpha' \leqslant \alpha$, then $\mathsf{C}(\alpha',\beta;\gamma)$;
(5) if $\mathsf{C}(\alpha,\beta;\gamma)$ and $\beta' \leqslant \beta$, then $\mathsf{C}(\alpha,\beta';\gamma)$;
(6) if $\mathsf{C}(\alpha,\beta;\gamma)$ and $\gamma \leqslant \gamma'$, then $\mathsf{C}(\alpha,\beta;\gamma')$;
(7) if $\mathsf{C}(\alpha,\beta;\delta)$ holds in $\mathbf{A}$, then $\mathsf{C}(\alpha\cap B^2,\beta\cap B^2;\delta\cap B^2)$ holds in $\mathbf{B}$;
(8) if $\delta' \leqslant \delta$, then $\mathsf{C}(\alpha,\beta;\delta)$ holds in $\mathbf{A}$ iff $\mathsf{C}(\alpha/\delta',\beta/\delta';\delta/\delta')$ holds in $\mathbf{A}/\delta'$.

Remark. By (1), if $\alpha\wedge\beta = 0_{\mathbf{A}}$, then $\mathsf{C}(\beta,\alpha)$ and $\mathsf{C}(\alpha,\beta)$. By (6), if an algebra $\mathbf{A}$ is abelian, then $\mathsf{C}(1_{\mathbf{A}},1_{\mathbf{A}};\theta)$ for all $\theta \in \operatorname{Con}(\mathbf{A})$, so in this case (8) implies that $\mathsf{C}(1_{\mathbf{A}/\theta},1_{\mathbf{A}/\theta})$ for every $\theta \in \operatorname{Con}(\mathbf{A})$.

Lemma 3. *If $\operatorname{Clo}\mathbf{A}$ is trivial (i.e., generated by the projections), then $\mathbf{A}$ is abelian.*

If the congruence lattice $\operatorname{Con}(\mathbf{A})$ has a 0,1-sublattice of shape M_n with $n \geqslant 3$, then $\mathbf{A}$ is abelian, as the next result shows.[1] For proof, see the Appendix.

Lemma 4. *If α_1, α_2, $\alpha_3 \in \operatorname{Con}(\mathbf{A})$ are pairwise complements, then $\mathsf{C}(1_{\mathbf{A}},\alpha_i)$ for each $i = 1,2,3$. If, in addition, $\mathbf{A}$ is idempotent with a Taylor term operation, then $\mathsf{C}(1_{\mathbf{A}},1_{\mathbf{A}})$; that is, $\mathbf{A}$ is abelian.*

---

[1]A "0,1-sublattice of shape M_n with $n \geqslant 3$" is a height-two modular sublattice with top $1_{\mathbf{A}}$, bottom $0_{\mathbf{A}}$, and at least 3 atoms.

Here is another well known and easily derivable fact: $\mathbf{A}$ is abelian if and only if the diagonal of $\mathbf{A} \times \mathbf{A}$ is a class of a congruence of $\mathbf{A} \times \mathbf{A}$. We denote the diagonal of A by $D(A) := \{(a, a) : a \in A\}$.

Lemma 5. An algebra $\mathbf{A}$ is abelian if and only if there is some $\theta \in \operatorname{Con}(\mathbf{A}^2)$ that has the diagonal set $D(A)$ as a congruence class.

Lemma 5 can be used to prove that if there is a congruence of $\mathbf{A}_1 \times \mathbf{A}_2$ that has the graph of a bijection as a block, then both $\mathbf{A}_1$ and $\mathbf{A}_2$ are abelian algebras. This is the content of Lemma 6. (See Appendix Section A for proof.)

Lemma 6. Suppose $\rho : A_1 \to A_2$ is a bijection and suppose the graph $\{(x, \rho x) \mid x \in A_1\}$ is a block of some congruence $\beta \in \operatorname{Con}(A_1 \times A_2)$. Then both $\mathbf{A}_1$ and $\mathbf{A}_2$ are abelian.

1.6. **Prelude to tame congruence theory.** Suppose $e \in \operatorname{Pol}_1 \mathbf{A}$ is a unary polynomial satisfying $e^2(x) = e(x)$ for all $x \in A$. Define $B = e(A)$ and $F_B = \{ef|_B \mid f \in \operatorname{Pol}_1 \mathbf{A}\}$, and consider the unary algebra $\mathbf{B} = \langle B, F_B\rangle$. (In the definition of F_B, we could have used $\operatorname{Pol} \mathbf{A}$ instead of $\operatorname{Pol}_1 \mathbf{A}$, and then our discussion would not be limited to unary algebras. However, we are mainly concerned with congruence lattices, so we lose nothing by restricting the scope in this way.)

Péter Pálfy and Pavel Pudlák prove in [5, Lemma 1] that the restriction mapping $|_B$, defined on $\operatorname{Con} \mathbf{A}$ by $\alpha|_B = \alpha \cap B^2$, is a lattice epimorphism of $\operatorname{Con} \mathbf{A}$ onto $\operatorname{Con} \mathbf{B}$. In [6], Ralph McKenzie developed the foundations of what would become tame congruence theory, and the Pálfy-Pudlák lemma played a seminal role in this development. In his presentation of the lemma, McKenzie introduced the mapping $\widehat{\ }$ defined on $\operatorname{Con} \mathbf{B}$ as follows:

$$\widehat{\beta} = \{(x, y) \in A^2 \mid \text{ for all } f \in \operatorname{Pol}_1 \mathbf{A},\ (ef(x), ef(y)) \in \beta\}. \tag{1.7}$$

Throughout this paper, whenever $\mathbf{A} = \langle A, \dots\rangle$ and $\mathbf{B} = \langle B, \dots\rangle$ are algebras with $B = e(A)$ for some $e^2 = e \in \operatorname{Pol}_1 \mathbf{A}$, we take $\widehat{\ }\colon \operatorname{Con} \mathbf{B} \to \operatorname{Con} \mathbf{A}$ to mean the map defined in (1.7). It is not hard to see that the codomain of $\widehat{\ }$ is indeed $\operatorname{Con} \mathbf{A}$. For example, if $(x, y) \in \widehat{\beta}$ and $g \in \operatorname{Pol}_1 \mathbf{A}$, then for all $f \in \operatorname{Pol}_1 \mathbf{A}$ we have $(efg(x), efg(y)) \in \beta$, so $(g(x), g(y)) \in \widehat{\beta}$.

For each $\beta \in \operatorname{Con} \mathbf{B}$, let $\beta^* = \operatorname{Cg}^{\mathbf{A}}(\beta)$. That is, ${}^*\colon \operatorname{Con} \mathbf{B} \to \operatorname{Con} \mathbf{A}$ is the congruence generation operator restricted to the set $\operatorname{Con} \mathbf{B}$. The following lemma concerns the three mappings, $|_B$, $\widehat{\ }$, and *. The third statement of the lemma, which follows from the first two, will be useful in the later sections of the paper.

Lemma 7 (Lemma 2.1 of [7])**.**
- (i) ${}^*\colon \operatorname{Con} \mathbf{B} \to \operatorname{Con} \mathbf{A}$ is a residuated mapping with residual $|_B$.
- (ii) $|_B\colon \operatorname{Con} \mathbf{A} \to \operatorname{Con} \mathbf{B}$ is a residuated mapping with residual $\widehat{\ }$.
- (iii) For all $\alpha \in \operatorname{Con} \mathbf{A}$, for all $\beta \in \operatorname{Con} \mathbf{B}$,
$$\beta = \alpha|_B \quad \Longleftrightarrow \quad \beta^* \leqslant \alpha \leqslant \widehat{\beta}.$$
In particular, $\beta^*|_B = \beta = \widehat{\beta}|_B$.

The proof is straightforward once we recall the definition of a residuated mapping. However, as we will only make use of item (iii), we relegate the proof of Lemma 7 to Section A.1 of the appendix.

The lemma above was inspired by the two approaches to proving [5, Lemma 1]. In the original paper * is used, while McKenzie uses the $\widehat{\ }$ operator. Both β^* and $\widehat{\beta}$

are mapped onto β by the restriction map $|_B$, so the restriction map is indeed onto $\operatorname{Con}\mathbf{B}$. By combining the two approaches, our version of the lemma highlights the fact that the interval

$$[\![\beta^*, \widehat{\beta}]\!] = \{\alpha \in \operatorname{Con}\mathbf{A} \mid \beta^* \leqslant \alpha \leqslant \widehat{\beta}\}$$

is precisely the set of congruences for which $\alpha|_B = \beta$. In other words, the $|_B$-inverse image of β is $[\![\beta^*, \widehat{\beta}]\!]$. This fact plays a central role in the theory developed in this paper. For the sake of completeness, we conclude this section by verifying that [5, Lemma 1] can be obtained from the lemma above.

Corollary 2 (cf. [5, Lemma 1])**.** The mapping $|_B \colon \operatorname{Con}\mathbf{A} \to \operatorname{Con}\mathbf{B}$ is onto and preserves meets and joins.

Proof. Given $\beta \in \operatorname{Con}\mathbf{B}$, each $\theta \in \operatorname{Con}\mathbf{A}$ in the interval $[\![\beta^*, \widehat{\beta}]\!]$ is mapped to $\theta|_B = \beta$, so $|_B$ is clearly onto. That $|_B$ preserves meets is obvious, so we just check that $|_B$ is join preserving. Since $|_B$ is order preserving, we have, for all $S \subseteq \operatorname{Con}\mathbf{A}$,

$$\bigvee \theta|_B \leqslant \left(\bigvee \theta\right)|_B,$$

where joins are over all $\theta \in S$. The opposite inequality follows from (A.7) above. Indeed, by (A.7) we have

$$\left(\bigvee \theta\right)|_B \leqslant \bigvee \theta|_B \quad\iff\quad \bigvee \theta \leqslant \left(\bigvee \theta|_B\right)^{\widehat{}}$$

and the last inequality holds by another application of (A.7): if $\eta \in S$, then

$$\eta \leqslant \left(\bigvee \theta|_B\right)^{\widehat{}} \quad\iff\quad \eta|_B \leqslant \bigvee \theta|_B.$$

$\square$

2. Tame Congruence Theory

In this section we review some basic definitions and results of *tame congruence theory*, as developed by David Hobby and Ralph McKenzie in [3]. We then remark on some consequences of this theory that is useful for our application. In particular, we will see that if $\mathbf{A}$ is a finite algebra whose congruence lattice is M_n, for some $n > 2$, then $\mathbf{A}$ is Abelian. (Note how this improves upon 4.) Moreover, we will see that when $n-1$ is not a prime power, $\operatorname{Con}\mathbf{A} \cong M_n$ implies that $\mathbf{A}$ is *strongly Abelian.*

2.1. **Tight lattices.**

In this section we define the class of "tight" lattices ([3, Definition 1.6]) and the class of "tame" congruences. Later we apply these concepts to congruence lattices of shape M_n.

Definition 1. Let L be any lattice.

(1) By a *meet endomorphism* of L we mean a function $\mu : L \to L$ satisfying, for all $x, y \in L$, $\mu(x \wedge y) = \mu(x) \wedge \mu(y)$. A *join endomorphism* is defined dually.
(2) Departing from standard terminology, we call a function $\mu : L \to L$ *increasing* iff $\mu(x) \geqslant x$ for all $xinL$, and *strictly increasing* if $\mu(x) > x$ for all $x \in L$ except the largest element of L. The concepts of *decreasing* and of *strictly decreasing* function on L are defined dually.

(3) By a *polarity* of L we mean a pair (σ, μ) such that σ is a decreasing join endomorphism of L, μ is an increasing meet endomorphism of L, and $\sigma\mu(x) \leqslant x \leqslant \mu\sigma(x)$ for all x in L.

Let L be any lattice with 0 and 1. A homomorphism $f : L \to L'$ is called 0,1-*separating* iff $f^{-1}\{f(0)\} = \{0\}$ (f *separates* 0) and $f^{-1}\{f(1)\} = \{1\}$ (f *separates* 1). We say that L is 0,1-*simple* iff $|L| > 1$ and every nonconstant homomorphism $f : L \to L'$ is 0,1-separating.

Definition 2. A lattice L is called *tight* iff L is finite, $|L| > 1$, and if ρ is any tolerance of L containing $\langle 0, a\rangle$ for some $a > 0$, or containing $\langle b, 1\rangle$ for some $b < 1$, then $\rho = L^2$.

Lemma 8 (Lemma 1.7 of [3])**.** A finite lattice L is tight iff L is 0,1-simple and every strictly increasing meet endomorphism of L is constant (i.e., L^2 is the only connected tolerance of L).

Lemma 9 (Lemma 1.8 of [3])**.** For any lattice L with 0 and 1, such that $|L| > 1$, the following are equivalent.

(1) L is 0,1-simple.
(2) L has a largest congruence $\theta \neq L^2$, and this congruence satisfies $1/\theta = \{1\}$ and $0/\theta = \{0\}$.

From Lemma 8, it easily follows that for every $n \geqslant 2$, the lattice M_n is tight.

2.2. **Tame quotients.** All algebras considered will be assumed to be finite. The concept of a minimal set relative to a pair of congruences is fundamental.

Definition 3 (Definition 2.5 of [3])**.** Let $\mathbf{A}$ be a finite algebra and let $\alpha < \beta$ be two congruences of $\mathbf{A}$. Define $U_{\mathbf{A}}(\alpha, \beta)$ to be the set of all sets of the form $f(A)$ where $f \in \mathrm{Pol}_1 \mathbf{A}$ and $f(\beta) \nsubseteq \alpha$. Define $M_{\mathbf{A}}(\alpha, \beta)$ to be the set of all minimal members of $U_{\mathbf{A}}(\alpha, \beta)$. Call the members of $M_{\mathbf{A}}(\alpha, \beta)$ the α, β-*minimal sets* of $\mathbf{A}$.

Observe that $M_{\mathbf{A}}(\alpha, \beta)$ is non-empty and for each α, β-minimal set U, we have $\alpha|_U \neq \beta|_U$. By a *quotient* in a lattice L, we mean simply a pair $\langle x, y\rangle$ of elements of L with $x < y$. We often refer to such a pair as "the quotient $x < y$ in L." A *prime quotient* is a covering relation $x \prec y$ in L; that is, if $x \leqslant z \leqslant y$, then either $z = x$ or $z = y$. The interval lattice $[\![x, y]\!]$ associated with a quotient $x < y$ is the sublattice of L consisting of all elements z such that $x \leqslant z \leqslant y$.

Definition 4. For a finite algebra $\mathbf{A}$, a quotient $\alpha < \beta$ in $\mathrm{Con}\,\mathbf{A}$ is called *tame* if there exists $V \in M_{\mathbf{A}}(\alpha, \beta)$ and a unary $e^2 = e \in \mathrm{Pol}_1 \mathbf{A}$ such that $e(A) = V$ and such that $[\![\alpha, \beta]\!] \to [\![\alpha|_V, \beta|_V]\!]$ is a 0,1-separating lattice homomorphism.

Theorem 1 (Thm. 2.11 of [3])**.** *If $\alpha < \beta$ is a quotient in $\mathrm{Con}\,\mathbf{A}$ such that $[\![\alpha, \beta]\!]$ is tight, then $\alpha < \beta$ is tame.*

Let $\alpha < \beta$ be a quotient in $\mathrm{Con}\,\mathbf{A}$. If $A \in M_{\mathbf{A}}(\alpha, \beta)$, then we call $\mathbf{A}$ *minimal relative to* $\alpha < \beta$, or simply α, β-*minimal*.

Lemma 10 (Lemma 2.13 of [3])**.** If $\alpha < \beta$ is a quotient in $\mathrm{Con}\,\mathbf{A}$, then the following hold.

(1) $\mathbf{A}$ is α, β-minimal iff for all $f \in \mathrm{Pol}_1 \mathbf{A}$, either f is a permutation of $\mathbf{A}$ or $f(\alpha) \subseteq \beta$.

(2) If $\mathbf{A}$ is α,β-minimal then $\alpha<\beta$ is tame.
(3) If $\alpha<\beta$ is tame and $U\in M_{\mathbf{A}}(\alpha,\beta)$ then the algebra $\mathbf{A}|_U$ is $\alpha|_U,\beta|_U$-minimal.

In item (3), "tameness" can be replaced by "there exists $e^2=e\in\operatorname{Pol}_1\mathbf{A}$ with $U=e(A)$."

A finite algebra $\mathbf{A}$ is called *minimal* if $\mathbf{A}$ is $0_A,1_A$-minimal, equivalently, $|A|>1$ and every nonconstant $f\in\operatorname{Pol}_1\mathbf{A}$ is a permutation. A finite algebra $\mathbf{A}$ is called *E-minimal* if $|A|>1$ and every nonconstant $e^2=e\in\operatorname{Pol}_1\mathbf{A}$ is the identity.

2.3. **The types of tame quotients.** We are now ready to define and study the five types of tame congruence quotients. In this section we delineate the distinct characters of these types, primarily in relation to the "polynomial structure" of an algebra. Later, we consider the congruence lattice of an algebra as a labeled graph, where all of the prime quotients are labeled with their respective types. We then consider the ways in which this labeling is influenced by the unlabeled congruence lattice, construed purely as an abstract lattice.

Definition 5 (Definition 5.1 of [3])**.**

(1) Let $\alpha<\beta$ be a tame quotient of congruences in a finite algebra $\mathbf{A}$. Let $U\in M_{\mathbf{A}}(\alpha,\beta)$. We define the *type* of $\alpha<\beta$, written $\operatorname{typ}(\alpha,\beta)$, to be the type of $\mathbf{A}|_U$ relative to $\alpha|_U<\beta|_U$.
(2) Let $\gamma<\lambda$ be any quotient of congruences in a finite algebra $\mathbf{A}$. Then we let $\operatorname{typ}\{\gamma,\lambda\}$ denote the set $\{\operatorname{typ}(\alpha,\beta):\gamma\leqslant\alpha\prec\beta\leqslant\lambda\}$.
(3) Let $\mathbf{A}$ be any finite algebra. We call $\mathbf{A}$ *tame* iff the quotient $0_A<1_A$ is tame. If $\mathbf{A}$ is tame, we put $\operatorname{typ}\mathbf{A}=\operatorname{typ}(0_A,1_A)$.
(4) Let $\mathbf{A}$ be any finite algebra. By $\operatorname{typ}\{\mathbf{A}\}$ we denote the set $\operatorname{typ}\{0_A,1_A\}$ of types.

Theorem 2 (Theorem 5.7 of [3])**.** *Let $\mathbf{A}$ be a finite algebra.*

(1) *Every prime congruence quotient of $\mathbf{A}$ is tame.*
(2) *For any quotient $\alpha<\beta$ of $\mathbf{A}$, the following are equivalent:*
  (i) *$\alpha<\beta$ is prime and nonabelian.*
  (ii) *$\alpha<\beta$ is tame and $\operatorname{typ}(\alpha,\beta)\in\{3,4,5\}$.*
(3) *A tame quotient $\alpha<\beta$ has type 1 iff it is strongly Abelian, and has type 2 iff it is Abelian but not strongly Abelian.*
(4) *For any quotient $\alpha<\beta$ of $\mathbf{A}$ that is not strongly Abelian, the following are equivalent:*
  (i) *$\alpha<\beta$ is tame.*
  (ii) *The interval lattice $[\![\alpha,\beta]\!]$ is tight.*
  (iii) *$[\![\alpha,\beta]\!]$ is 0,1-simple and complemented.*
  (iv) *$[\![\alpha,\beta]\!]$ admits a 0,1-separating homomorphism onto the congruence lattice of a vector space. (This homomorphism is essentially unique.)*

2.4. **Application to M_n.** We first note that, for $n\geqslant 2$, the lattice M_n is simple and tight. Suppose $\mathbf{A}$ is a finite algebra with $\operatorname{Con}\mathbf{A}\cong M_n$. Then $[\![0_A,1_A]\!]$ is tight, hence $0_A<1_A$ is tame. Since $0_A<1_A$ is not prime, by Theorem 2(2), $\operatorname{typ}(0,1)\notin\{3,4,5\}$. Thus, $\mathbf{A}$ is Abelian. Finally, if $\mathbf{A}$ is Abelian, but not strongly abelian, then by Theorem 2(4), M_n must be isomorphic to the congruence lattice of a vector space, hence $n-1$ is a prime power.

3. Graphical Compositions

Let X be a nonempty set. Given α, β, $\gamma \in \mathrm{Eq}(X)$, define the relation

$$W(\alpha, \beta; \gamma) := \{(x, y) \in X^2 : \exists (a, b) \in \gamma \,.\, x \;\alpha\; a \;\beta\; y \;\alpha\; b \;\beta\; x\}.$$

That is, $(x, y) \in W(\alpha, \beta; \gamma)$ iff there exists $(a, b) \in \gamma$ such that the relations in Figure 2 hold.

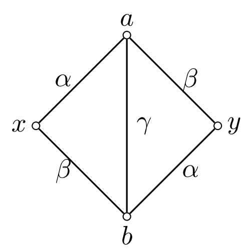


Figure 2. The Wheatstone Bridge defines the relation $W(\alpha, \beta; \gamma)$.

It is not hard to see that $W(\alpha, \beta; \gamma)$ is a *tolerance* (that is, a reflexive symmetric relation) on X. Also obvious is the fact that $W(\alpha, \beta; \gamma) = W(\beta, \alpha; \gamma)$.

Suppose α_1, α_2, and α_3 are PPPC in $\mathrm{Eq}(X)$, and let $\beta \in \mathrm{Eq}(X)$ be complementary to each α_i, so that $L = \{0_X, \alpha_1, \alpha_2, \alpha_3, \beta, 1_X\} \cong M_4$. (See Figure 3.)

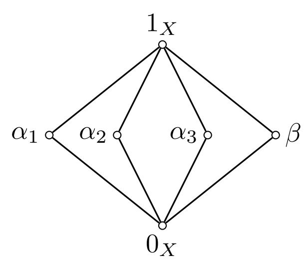


Figure 3. The lattice M_4.

Define the relation $\tau = \tau(\alpha_1, \alpha_2, \beta) \subseteq X \times X$ as $R(\alpha_1, \alpha_2, \beta) \subseteq X \times X$ as follows:

$$x \;\tau\; y \quad \longleftrightarrow \quad (\exists (a, b) \in \beta)\; x \;\alpha_1\; a \;\alpha_2\; y \;\alpha_1\; b \;\alpha_2\; x.$$

Graphically, $x \;\tau\; y$ if and only if there exist $a, b \in X$ satisfying the relations depicted in Figure 4. It is clear that τ is a *tolerance*, that is, a reflexive and symmetric binary relation. Let $f : X \to X$ be a unary operation and suppose that f is *compatible* with each relation $\theta \in \{\alpha_1, \alpha_2, \beta\}$, that is, $(u, v) \in \theta \longrightarrow (f(u), f(v)) \in \theta$. Then f is also compatible with τ.

Fact 3.1. If $L = \{0_X, \alpha_1, \alpha_2, \alpha_3, \beta, 1_X\} \cong M_4$, then

$$\alpha_1 \cap \tau(\alpha_1, \alpha_2, \beta) = 0_X = \alpha_2 \cap \tau(\alpha_1, \alpha_2, \beta),$$

$$\alpha_1 \cap \tau(\alpha_1, \alpha_3, \beta) = 0_X = \alpha_3 \cap \tau(\alpha_1, \alpha_3, \beta),$$

$$\alpha_2 \cap \tau(\alpha_2, \alpha_3, \beta) = 0_X = \alpha_3 \cap \tau(\alpha_2, \alpha_3, \beta).$$

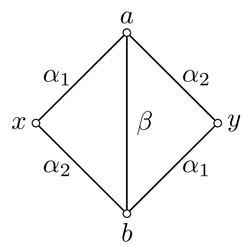


FIGURE 4. The Wheatstone Bridge which defines the relation $\tau(\alpha_1, \alpha_2, \beta)$ as follows: $(x, y) \in \tau(\alpha_1, \alpha_2, \beta)$ if and only if there exist $a, b \in X$ satisfying the relations in the diagram.

Proof. Fix $(x, y) \in \alpha_1 \cap \tau(\alpha_1, \alpha_2, \beta)$ and suppose a and b satisfy the diagram in Figure 4. Then $(x, y) \in \alpha_1$ implies $(a, b) \in \alpha_1 \wedge \beta = 0_X$, so $a = b$. Therefore, $(x, y) \in \alpha_1 \wedge \alpha_2 = 0_X$, so $x = y$. Proofs of the other identities are similar. $\square$

4. Functions Derived from Graphical Compositions

Let R^β_{12} be the relation on $X^2 \times X^2$ defined by

$$(a, b)\ R^\beta_{12}\ (x, y) \quad \longleftrightarrow \quad (a, b) \in \beta \ \text{ and } \ x\ \alpha_1\ a\ \alpha_2\ y\ \alpha_1\ b\ \alpha_2\ x.$$

Define R^β_{13} and R^β_{23} similarly. Graphically, $(a, b)\ R^\beta_{12}\ (x, y)$ holds if and only if the relations in Figure 4 are satisfied.

Lemma 11. Suppose α_i and α_j are complementary equivalence relations on X with uniform blocks of size $\sqrt{|X|}$. Then the relation R^β_{ij} restricted to $\beta \times X^2$ is a one-to-one function from β into X^2.

Proof. First we note that each pair $(a, b) \in \beta$ has at most one image. For if $(a, b)\ R^\beta_{ij}$ (x, y) and $(a, b)\ R^\beta_{ij}\ (u, v)$, then $(x, u) \in \alpha_i \wedge \alpha_j = 0_X$ and $(y, v) \in \alpha_i \wedge \alpha_j = 0_X$, so $(x, y) = (u, v)$.

Next, since both α_i and α_j have $\sqrt{|X|}$ blocks, and since each of these blocks has size $\sqrt{|X|}$, we see that each block of α_i intersects each block of α_j at exactly one point. That is, for all $a, b \in X$, the set $a/\alpha_i \cap b/\alpha_j$ is a singleton. Therefore, to each $(a, b) \in \beta$ there corresponds precisely one $(x, y) \in X^2$ such that $(a, b)\ R^\beta_{ij}\ (x, y)$ holds. Specifically, $\{x\} = a/\alpha_i \cap b/\alpha_j$ and $\{y\} = b/\alpha_i \cap a/\alpha_j$. Thus, R^β_{ij} is a function.

From now on, we let $R^\beta_{ij}((a, b))$ denote the image of (a, b) under R^β_{ij}; that is, $R^\beta_{ij}((a, b))$ denotes the ordered pair (x, y) satisfying $(a, b)\ R^\beta_{ij}\ (x, y)$.

Suppose $R^\beta_{ij}((a, b)) = R^\beta_{ij}((c, d))$. Then $(a, c) \in \alpha_i \wedge \alpha_j = 0_X$ and $(b, d) \in \alpha_i \wedge \alpha_j = 0_X$, so $(a, b) = (c, d)$. Therefore, R^β_{ij} is one-to-one. $\square$

If, in addition to the assumptions of Lemma 11, we assume that the image of β under R^β_{ij} is contained in β, then $R^\beta_{ij} : \beta \to \beta$ is a bijective involution. That is, R^β_{ij} is one-to-one and onto, and $R^\beta_{ij} \circ R^\beta_{ij}$ is the identity map.

5. Final piece of the puzzle

As above, suppose $L = \{0_X, \alpha_1, \alpha_2, \alpha_3, \beta, 1_X\} \cong M_4$ is a congruence lattice and suppose $\{\alpha_i\}_{i=1}^3$ is PPPC. Suppose $R^\beta_{ij} : \beta \to \beta$ holds for all $i, j \in \{1, 2, 3\}$.

Lemma 12. If $a\ \alpha_1\ z\ \beta\ w$, then one of the following holds:

(1) $(a, w) \in \alpha_2$,
(2) $(a, w) \in \alpha_3$,
(3) $(a, w) \in \beta$,
(4) $a/\alpha_2 \cap z/\alpha_3 \cap w/\alpha_1 \neq \emptyset$,
(5) $a/\alpha_3 \cap z/\alpha_2 \cap w/\alpha_1 \neq \emptyset$.

If Lemma 12 is true, then we can prove the following:

Theorem 3. *If $L = \{0_X, \alpha_1, \alpha_2, \alpha_3, \beta, 1_X\} \cong M_4$ is a congruence lattice with α_i PPPC, then β permutes with each α_i.*

Proof. We will show $\alpha_1 \circ \beta \subseteq \beta \circ \alpha_1$. Assume $a\ \alpha_1\ z\ \beta\ w$. We consider each of the cases in Lemma 12 in turn and, in each case, find b satisfying $a\ \beta\ b\ \alpha_1\ w$.

(1) If $(a, w) \in \alpha_2$, then let $b = z/\alpha_2 \cap w/\alpha_1$. Then $R^\beta_{12}(z, w) = (a, b)$ and since $R^\beta_{12} : \beta \to \beta$, we have $(a, b) \in \beta$, so $a\ \beta\ b\ \alpha_1\ w$, as desired.
(2) If $(a, w) \in \alpha_3$, then let $b = z/\alpha_3 \cap w/\alpha_1$. Use the same argument as in the first case, but replace R^β_{12} with R^β_{13}.
(3) If $(a, w) \in \beta$, then let $b = a$.
(4) If $a/\alpha_2 \cap z/\alpha_3 \cap w/\alpha_1 \neq \emptyset$, then let y denote the element in this set. Let $x = z/\alpha_1 \cap w/\alpha_3$, and let $b = x/\alpha_2 \cap y/\alpha_1$. Then $(R^\beta_{12} \circ R^\beta_{13})(z, w) = R^\beta_{12}(x, y) = (a, b)$, so $(a, b) \in \beta$. Now, $b\ \alpha_1\ y\ \alpha_1\ w$, so $a\ \beta\ b\ \alpha_1\ w$, as desired.
(5) If $a/\alpha_3 \cap z/\alpha_2 \cap w/\alpha_1 \neq \emptyset$, then let y denote this element, let $x = z/\alpha_1 \cap w/\alpha_2$, and let $b = x/\alpha_3 \cap y/\alpha_1$. Then $(R^\beta_{13} \circ R^\beta_{12})(z, w) = R^\beta_{12}(x, y) = (a, b)$, so $(a, b) \in \beta$. Now, $b\ \alpha_1\ y\ \alpha_1\ w$, so $a\ \beta\ b\ \alpha_1\ w$, as desired.

□

6. Proof of Lemma 3

Consider the relation θ_{ij} defined as follows:

$$x\ \theta_{ij}\ y \quad \longleftrightarrow \quad (\exists a, b)\ a\ \alpha_i\ x\ \alpha_j\ b\ \beta\ y\ \alpha_j\ a.$$

Easy arguments similar to those above establish that

$$\theta_{ij} \cap \alpha_i = \theta_{ij} \cap \alpha_j = \theta_{ij} \cap \beta = 0_X.$$

On the other hand, since L is a congruence lattice, it must be the case that the transtive closure of θ_{ij} is contained in L.

TODO: complete proof of Lemma 3 (if possible).

Appendix A. Miscellaneous Proofs

Lemma. 3. If $\mathrm{Clo}\,\mathbf{A}$ is trivial (i.e., generated by the projections), then $\mathbf{A}$ is abelian.

Proof. We want to show $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}})$. Equivalently, we must show that for all $t \in \operatorname{Clo} \mathbf{A}$ (say, $(\ell+m)$-ary) and all $a, b \in A^{\ell}$, we have $\ker t(a, \cdot) = \ker t(b, \cdot)$. We prove this by induction on the height of the term t. Height-one terms are projections and the result is obvious for these. Let $n > 1$ and assume the result holds for all terms of height less than n. Let t be a term of height n, say, k-ary. Then for some terms $g_1, \dots, q_k$ of height less than n and for some $j \leqslant k$, we have $t = p^k_j[q_1, q_2, \dots, q_k] = q_j$ and since q_j has height less than n, we have

$$\ker t(a, \cdot) = \ker g_j(a, \cdot) = \ker g_j(b, \cdot) = \ker t(b, \cdot).$$

□

In fact, it can be shown that $\mathbf{A}$ is *strongly abelian* in this case.

Lemma. 4. If α_1, α_2, $\alpha_3 \in \operatorname{Con}(\mathbf{A})$ are pairwise complements, then $\mathsf{C}(1_{\mathbf{A}}, \alpha_i)$ for each $i = 1, 2, 3$. If, in addition, $\mathbf{A}$ is idempotent and has a Taylor term operation, then $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}})$; that is, $\mathbf{A}$ is abelian.

Proof. The goal is to prove $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}})$. By Lemma 2 (1), we have $\mathsf{C}(\alpha_1, \alpha_2; \alpha_1 \wedge \alpha_2)$. Since $\alpha_1 \wedge \alpha_2 = 0_{\mathbf{A}}$, this means $\mathsf{C}(\alpha_1, \alpha_2)$. Similarly, $\mathsf{C}(\alpha_3, \alpha_2)$. Therefore, by Lemma 2 (3), we have $\mathsf{C}(\alpha_1 \vee \alpha_3, \alpha_2)$. This is equivalent to $\mathsf{C}(1_{\mathbf{A}}, \alpha_2)$, since $\alpha_1 \vee \alpha_3 = 1_{\mathbf{A}}$. The same argument *mutatis-mutandis* yields $\mathsf{C}(1_{\mathbf{A}}, \alpha_1)$ and $\mathsf{C}(1_{\mathbf{A}}, \alpha_3)$. Before proceding, note that $\mathsf{C}(\alpha_1, \alpha_1)$, by Lemma 2 (4). Now, if $\mathbf{A}$ is idempotent and has a Taylor term operation, then by **??** we have $\mathsf{C}(\alpha_1 \vee \alpha_2, \alpha_1 \vee \alpha_2; \alpha_2)$. That is, $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}}; \alpha_2)$. Similarly, $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}}; \alpha_3)$. By 2 (2) then, $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}}; \alpha_2 \wedge \alpha_3)$. That is, $\mathsf{C}(1_{\mathbf{A}}, 1_{\mathbf{A}})$. □

Lemma. 5. An algebra $\mathbf{A}$ is abelian if and only if there is some $\theta \in \operatorname{Con}(\mathbf{A}^2)$ that has the diagonal $D(A) := \{(a, a) : a \in A\}$ as a congruence class.

Proof. ($\Leftarrow$) Assume Θ is such a congruence. Fix $k < \omega$, $t^{\mathbf{A}} \in \operatorname{Clo}_{k+1} \mathbf{A}$, $u, v \in A$, and $\mathbf{x}, \mathbf{y} \in A^k$. We will prove the implication (1.6), which in the present context is

$$t^{\mathbf{A}}(\mathbf{x}, u) = t^{\mathbf{A}}(\mathbf{y}, u) \quad \Longrightarrow \quad t^{\mathbf{A}}(\mathbf{x}, v) = t^{\mathbf{A}}(\mathbf{y}, v).$$

Since $D(A)$ is a class of Θ, we have $(u, u)\ \Theta\ (v, v)$, and since Θ is a reflexive relation, we have $(x_i, y_i)\ \Theta\ (x_i, y_i)$ for all i. Therefore,

$$t^{\mathbf{A}\times\mathbf{A}}((x_1, y_1), \dots, (x_k, y_k), (u, u))\ \Theta\ t^{\mathbf{A}\times\mathbf{A}}((x_1, y_1), \dots, (x_k, y_k), (v, v)). \tag{A.1}$$

since $t^{\mathbf{A}\times\mathbf{A}}$ is a term operation of $\mathbf{A} \times \mathbf{A}$. Note that (A.1) is equivalent to

$$(t^{\mathbf{A}}(\mathbf{x}, u), t^{\mathbf{A}}(\mathbf{y}, u))\ \Theta\ (t^{\mathbf{A}}(\mathbf{x}, v), t^{\mathbf{A}}(\mathbf{y}, v)). \tag{A.2}$$

If $t^{\mathbf{A}}(\mathbf{x}, u) = t^{\mathbf{A}}(\mathbf{y}, u)$ then the first pair in (A.2) belongs to the Θ-class $D(A)$, so the second pair must also belong this Θ-class. That is, $t^{\mathbf{A}}(\mathbf{x}, v) = t^{\mathbf{A}}(\mathbf{y}, v)$, as desired.

($\Rightarrow$) Assume $\mathbf{A}$ is abelian. We show $\operatorname{Cg}^{\mathbf{A}^2}(D(A)^2)$ has $D(A)$ as a block. Assume

$$((x, x), (c, c')) \in \operatorname{Cg}^{\mathbf{A}^2}(D(A)^2). \tag{A.3}$$

It suffices to prove that $c = c'$. Recall, Malcev's congruence generation theorem states that (A.3) holds iff

$$\exists\, (z_0, z_0'), (z_1, z_1'), \dots, (z_n, z_n') \in A^2$$
$$\exists\, ((x_0, x_0'), (y_0, y_0')), ((x_1, x_1'), (y_1, y_1')), \dots, ((x_{n-1}, x_{n-1}'), (y_{n-1}, y_{n-1}')) \in D(A)^2$$
$$\exists\, f_0, f_1, \dots, f_{n-1} \in F^*_{\mathbf{A}^2}$$

such that

$$\{(x,x),(z_1,z_1')\} = \{f_0(x_0,x_0'), f_0(y_0,y_0')\} \tag{A.4}$$
$$\{(z_1,z_1'),(z_2,z_2')\} = \{f_1(x_1,x_1'), f_1(y_1,y_1')\}$$
$$\vdots$$
$$\{(z_{n-1},z_{n-1}'),(c,c')\} = \{f_{n-1}(x_{n-1},x_{n-1}'), f_{n-1}(y_{n-1},y_{n-1}')\} \tag{A.5}$$

The notation $f_i \in F^*_{\mathbf{A}^2}$ means

$$\begin{aligned} f_i(x,x') &= g_i^{\mathbf{A}^2}((a_1,a_1'),(a_2,a_2'),\dots,(a_k,a_k'),(x,x')) \\ &= (g_i^{\mathbf{A}}(a_1,a_2,\dots,a_k,x), g_i^{\mathbf{A}}(a_1',a_2',\dots,a_k',x')), \end{aligned}$$

for some $g_i^{\mathbf{A}} \in \operatorname{Clo}_{k+1}\mathbf{A}$ and some constants $\mathbf{a} = (a_1,\dots,a_k)$ and $\mathbf{a}' = (a_1',\dots,a_k')$ in A^k. Now, $((x_i,x_i'),(y_i,y_i')) \in D(A)^2$ implies $x_i = x_i'$, and $y_i = y_i'$, so in fact we have

$$\{(z_i,z_i'),(z_{i+1},z_{i+1}')\} = \{f_i(x_i,x_i), f_i(y_i,y_i)\} \quad (0 \leqslant i < n).$$

Therefore, by Equation (A.4) we have either

$$(x,x) = (g_i^{\mathbf{A}}(\mathbf{a},x_0), g_i^{\mathbf{A}}(\mathbf{a}',x_0)) \quad \text{or} \quad (x,x) = (g_i^{\mathbf{A}}(\mathbf{a},y_0), g_i^{\mathbf{A}}(\mathbf{a}',y_0)).$$

Thus, either $g_i^{\mathbf{A}}(\mathbf{a},x_0) = g_i^{\mathbf{A}}(\mathbf{a}',x_0)$ or $g_i^{\mathbf{A}}(\mathbf{a},y_0) = g_i^{\mathbf{A}}(\mathbf{a}',y_0)$. By the abelian assumption, if one of these equations holds, then so does the other. This and and Equation (A.4) imply $z_1 = z_1'$. Applying the same argument inductively, we find that $z_i = z_i'$ for all $1 \leqslant i < n$ and so, by (A.5) and the abelian property, we have $c = c'$. □

Lemma. 6. Suppose $\rho : A_1 \to A_2$ is a bijection and suppose the graph $\{(x,\rho x) \mid x \in A_1\}$ is a block of some congruence $\beta \in \operatorname{Con}(A_1 \times A_2)$. Then both $\mathbf{A}_1$ and $\mathbf{A}_2$ are abelian.

Proof. Define the relation $\alpha \subseteq (A_1 \times A_1)^2$ as follows: for $((a,a'),(b,b')) \in (A_1 \times A_1)^2$,

$$(a,a')\ \alpha\ (b,b') \quad \iff \quad (a,\rho a')\ \beta\ (b,\rho b')$$

We prove that the diagonal $D(A_1)$ is a block of α by showing that $(a,a)\ \alpha\ (b,b')$ implies $b = b'$. Indeed, if $(a,a)\ \alpha\ (b,b')$, then $(a,\rho a)\ \beta\ (b,\rho b')$, which means that $(b,\rho b')$ belongs to the block and $(a,\rho a)/\beta = \{(x,\rho x) : x \in A_1\}$. Therefore, $\rho b = \rho b'$, so $b = b'$ since ρ is injective. This proves that $\mathbf{A}_1$ is abelian.

To prove $\mathbf{A}_2$ is abelian, we reverse the roles of A_1 and A_2 in the foregoing argument. If $\{(x,\rho x) \mid x \in A_1\}$ is a block of β, then $\{(\rho^{-1}(\rho x),\rho x) \mid \rho x \in A_2\}$ is a block of β; that is, $\{(\rho^{-1}y, y) \mid y \in A_2\}$ is a block of β. Define the relation $\alpha \subseteq (A_2 \times A_2)^2$ as follows: for $((a,a'),(b,b')) \in (A_2 \times A_2)^2$,

$$(a,a')\ \alpha\ (b,b') \quad \iff \quad (\rho^{-1}a,\rho a')\ \beta\ (\rho^{-1}b,\rho b').$$

As above, we can prove that the diagonal $D(A_2)$ is a block of α by using the injectivity of ρ^{-1} to show that $(a,a)\ \alpha\ (b,b')$ implies $b = b'$. □

A.1. **Residuation Lemma.**

Lemma. 7. (Lem. 2.1 of [7])

(i) $^*\colon \operatorname{Con}\mathbf{B} \to \operatorname{Con}\mathbf{A}$ is a residuated mapping with residual $|_B$.
(ii) $|_B\colon \operatorname{Con}\mathbf{A} \to \operatorname{Con}\mathbf{B}$ is a residuated mapping with residual $\widehat{\ }$.
(iii) For all $\alpha \in \operatorname{Con}\mathbf{A}$, for all $\beta \in \operatorname{Con}\mathbf{B}$,

$$\beta = \alpha|_B \quad \Longleftrightarrow \quad \beta^* \leqslant \alpha \leqslant \widehat{\beta}.$$

In particular, $\beta^*|_B = \beta = \widehat{\beta}|_B$.

Proof. We first recall the definition of *residuated mapping.* If X and Y are partially ordered sets, and if $f\colon X \to Y$ and $g\colon Y \to X$ are order preserving maps, then the following are equivalent:

(a) $f\colon X \to Y$ is a *residuated mapping* with *residual* $g\colon Y \to X$;
(b) $(\forall x \in X)(\forall y \in Y)\, f(x) \leqslant y \iff x \leqslant g(y)$;
(c) $g \circ f \geqslant \mathrm{id}_X$ and $f \circ g \leqslant \mathrm{id}_Y$,

where id_S denotes the identity map on the set S. The definition says that for each $y \in Y$ there is a unique $x \in X$ that is maximal with respect to the property $f(x) \leqslant y$, and the maximum is given by $x = g(y)$. Thus, (i) is equivalent to: $\forall \alpha \in \operatorname{Con}\mathbf{A}$, $\forall \beta \in \operatorname{Con}\mathbf{B}$,

$$\beta^* \leqslant \alpha \iff \beta \leqslant \alpha|_B. \tag{A.6}$$

This is easily verified, as follows: If $\beta^* \leqslant \alpha$ and $(x, y) \in \beta$, then $(x, y) \in \beta^* \leqslant \alpha$ and $(x, y) \in B^2$, so $(x, y) \in \alpha|_B$. If $\beta \leqslant \alpha|_B$ then $\beta^* \leqslant (\alpha|_B)^* \leqslant \operatorname{Cg}^{\mathbf{A}}(\alpha) = \alpha$.

Statement (ii) is equivalent to: $\forall \alpha \in \operatorname{Con}\mathbf{A}$, $\forall \beta \in \operatorname{Con}\mathbf{B}$,

$$\alpha|_B \leqslant \beta \iff \alpha \leqslant \widehat{\beta}. \tag{A.7}$$

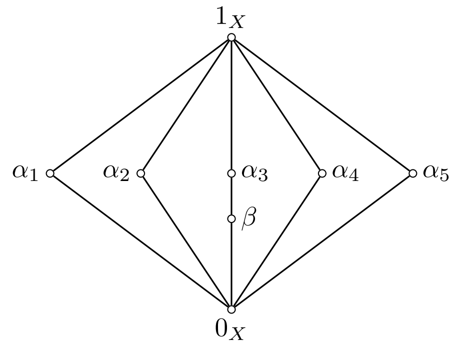
This is also easy to check. For, suppose $\alpha|_B \leqslant \beta$ and $(x, y) \in \alpha$. Then $(ef(x), ef(y)) \in \alpha$ for all $f \in \operatorname{Pol}_1\mathbf{A}$ and $(ef(x), ef(y)) \in B^2$, therefore, $(ef(x), ef(y)) \in \alpha|_B \leqslant \beta$, so $(x, y) \in \widehat{\beta}$. Suppose $\alpha \leqslant \widehat{\beta}$ and $(x, y) \in \alpha|_B$. Then $(x, y) \in \alpha \leqslant \widehat{\beta}$, so $(ef(x), ef(y)) \in \beta$ for all $f \in \operatorname{Pol}_1\mathbf{A}$, including $f = \mathrm{id}_A$, so $(e(x), e(y)) \in \beta$. But $(x, y) \in B^2$, so $(x, y) = (e(x), e(y)) \in \beta$.

Combining (A.6) and (A.7), we obtain statement (iii) of the lemma. $\square$

Appendix B. Example

Let X be a set. It is useful to represent partitions of X as lists of lists, and write them as (possibly nonrectangular) arrays, where each row represents a single block. We do this in the following example, which aids our intuition when thinking about the Palfy-Saxl problem.

Let $X = \{0, 1, 2, \dots, 15\}$, and consider the equivalence relations $\alpha_1, \dots, \alpha_5$ and β, generating the following sublattice of $\operatorname{Eq}(X)$:



where $\alpha_1, \ldots, \alpha_5$, and β correspond to the following partitions of X:

$$
\begin{array}{ccc}
\alpha_1 & \alpha_2 & \alpha_3 \\
\begin{array}{llll}
[0 & 1 & 2 & 3] \\
[4 & 5 & 6 & 7] \\
[8 & 9 & 10 & 11] \\
[12 & 13 & 14 & 15]
\end{array}
&
\begin{array}{llll}
[0 & 4 & 8 & 12] \\
[1 & 5 & 9 & 13] \\
[2 & 6 & 10 & 14] \\
[3 & 7 & 11 & 15]
\end{array}
&
\begin{array}{llll}
[0 & 5 & 10 & 15] \\
[1 & 4 & 11 & 14] \\
[2 & 7 & 8 & 13] \\
[3 & 6 & 9 & 12]
\end{array}
\end{array}
$$

$$
\begin{array}{ccc}
\alpha_4 & \alpha_5 & \beta \\
\begin{array}{llll}
[0 & 7 & 9 & 14] \\
[1 & 6 & 8 & 15] \\
[2 & 5 & 11 & 12] \\
[3 & 4 & 10 & 13] \\
 & & & \\
 & & & \\
 & & &
\end{array}
&
\begin{array}{llll}
[0 & 6 & 11 & 13] \\
[1 & 7 & 10 & 12] \\
[2 & 4 & 9 & 15] \\
[3 & 5 & 8 & 14] \\
 & & & \\
 & & & \\
 & & &
\end{array}
&
\begin{array}{llll}
[0 & 5 & 10 & 15] \\
 & [1 & 4] & \\
 & [2 & 8] & \\
 & [3 & 12] & \\
 & [6 & 9] & \\
 & [7 & 13] & \\
 & [11 & 14] &
\end{array}
\end{array}
$$

The relations $\alpha_1, \ldots, \alpha_5$ are PPPC. Also, for each α_i, with $i \neq 3$, it's clear that β and α_i are nonpermuting complements. Here are some other facts that aid intuition.

Fact B.1. Each M_3 sublattice with all α's for atoms is a congruence lattice. In other words, if i, j, k are three distinct numbers in $\{1, 2, \ldots, 5\}$, then the sublattice $\{0_X, \alpha_i, \alpha_j, \alpha_k, 1_X\}$ is closed.

Fact B.2. Consider any M_4 having all α's for atoms. The closure is the M_5 lattice $\{0_X, \alpha_1, \ldots, \alpha_5, 1_X\}$.

Fact B.3. Each M_4 generated by β and three α's complementary to β is not closed. The closure will have many relations in it.

Regarding the last fact, I've forgotten how many relations are in the closure.

TODO: Check this; also check whether α_3 and the other omitted α always end up in the closure.

Fact B.4. The M_3 sublattice $\{0_X, \alpha_1, \alpha_2, \beta, 1_X\}$ is closed.

Fact B.5. The relation $\tau = \tau(\alpha_1, \alpha_2, \beta)$ defined via the Wheatstone Bridge (Figure 5) is a subset of β.

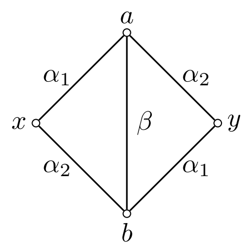


FIGURE 5. The Wheatstone Bridge which defines the relation $\tau(\alpha_1, \alpha_2, \beta)$ as follows: $(x, y) \in \tau(\alpha_1, \alpha_2, \beta)$ if and only if there exist $a, b \in X$ satisfying the relations in the diagram.

What follows is an informal discussion of the motivation that led to the relation β given in this example. (This and other parts of the Appendix are verbose and inelegant; all of this will be removed eventually.)

Regarding Fact B.5, β was constructed specifically to provide a nontrivial example where this fact might hold. That is, we wanted to know if an example existed in which β has smaller height than α_i (so that $|x/\beta| \leqslant |y/\alpha_i| < |X/\beta|$, and so β would not permute with α_1 and α_2), and such that $\tau(\alpha_1, \alpha_2, \beta) \subseteq \beta$, so that the Wheatstone Bridge of Figure 5 would not generate an equivalence relation that isn't already contained in $\{0_X, \alpha_1, \alpha_2, \beta, 1_X\}$.

To construct β, we started by assuming $0/\beta = \{0, 5, 10, 15\}$, which is the main diagonal of both α_1 and α_2. Then we considered the Wheatstone Bridge involving α_1 and α_2 and noticed that, if $\tau \subseteq \beta$, then β must contain all pairs that are at "opposite corners" (defined below) relative to pairs on the main diagonal $\{0, 5, 10, 15\}$.

By "opposite corners" we mean the following. Fix a pair in β, say, $(0, 10) \in \beta$, and consider the squares this pair generates in α_1 and α_2; that is, the squares with 0 and 10 at diagonal corners. We see that 2 and 8 appear at the remaining corners of such squares. We call the corners labeled 2 and 8 the "opposite corners" relative to 0 and 10.

The relation τ defined by the Wheatstone Bridge satisfies

$$0 \;\beta\; 10 \quad \longrightarrow \quad 2 \;\tau\; 8,$$

and, by symmetry of α_1 and α_2,

$$2 \;\beta\; 8 \quad \longrightarrow \quad 0 \;\tau\; 10.$$

Let us make this more general and precise. Recall the relation $\tau = \tau(\alpha_1, \alpha_2, \beta) \subseteq X \times X$ is defined by

$$x \;\tau\; y \quad \longleftrightarrow \quad (\exists (a, b) \in \beta)\; x \;\alpha_1\; a \;\alpha_2\; y \;\alpha_1\; b \;\alpha_2\; x. \tag{B.1}$$

Graphically, $x \;\tau\; y$ if and only if there exist $a, b \in X$ satisfying the relations depicted in Figure 5.

Let us order the elements of the equivalence classes of α_1 and α_2 according to the row-column arrangements given in the array representations above, and denote by $\alpha_1(i, j)$ the j-th element of the i-th equivalence class of α_1—that is $\alpha_1(i, j)$ is the element in row i and column j of the array representation of α_1.

Consider the Wheatstone Bridge diagram and note that, if (x, y) and (a, b) satisfy this diagram, so that (B.1) holds, then we have

$$x \in a/\alpha_1 \cap b/\alpha_2 \quad \text{and} \quad y \in b/\alpha_1 \cap a/\alpha_2. \tag{B.2}$$

Suppose $a = \alpha_1(i, j)$ and $b = \alpha_2(k, \ell)$. Then, by (B.2), x is the point where the i-th row of α_1 intersects the k-th row of α_2. But notice that, in this example, the array representing α_2 happens to be the transpose of the array representing α_1. Therefore, the k-th row of α_2 is the k-th column of α_1, so x is the element contained in the i-th row and k-th column of α_1, that is, $x = \alpha_1(i, k)$. Similarly, $y = \alpha_1(j, \ell)$. More generally, for all i, j, r, s in $\{1, 2, 3, 4\}$, we have

$$\alpha_1(i, j)\ \beta\ \alpha_1(r, s) \quad \longrightarrow \quad \alpha_1(i, s)\ \tau\ \alpha_1(j, r).$$

For example, looking at the array representing α_1, we see that if, say, $(2, 15)$ were to belong to β, then the pair $(3, 15)$ at the opposite corners must belong to $\tau(\alpha_1, \alpha_2, \beta)$.

References

[1] P. P. Pálfy and J. Saxl, "Congruence lattices of finite algebras and factorizations of groups," *Comm. Algebra*, vol. 18, no. 9, pp. 2783–2790, 1990, ISSN: 0092-7872.

[2] K. A. Kearnes and E. W. Kiss, "The shape of congruence lattices," *Mem. Amer. Math. Soc.*, vol. 222, no. 1046, pp. viii+169, 2013, ISSN: 0065-9266. DOI: 10.1090/S0065-9266-2012-00667-8. [Online]. Available: http://dx.doi.org/10.1090/S0065-9266-2012-00667-8.

[3] D. Hobby and R. McKenzie, *The structure of finite algebras*, ser. Contemporary Mathematics. Providence, RI: American Mathematical Society, 1988, vol. 76, pp. xii+203, Available from: math.hawaii.edu, ISBN: 0-8218-5073-3.

[4] R. N. McKenzie, G. F. McNulty, and W. F. Taylor, *Algebras, lattices, varieties. Vol. I.* Monterey, CA: Wadsworth & Brooks/Cole, 1987, pp. xvi+361, ISBN: 0-534-07651-3.

[5] P. P. Pálfy and P. Pudlák, "Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups," *Algebra Universalis*, vol. 11, no. 1, pp. 22–27, 1980, ISSN: 0002-5240. DOI: 10.1007/BF02483080.

[6] R. McKenzie, "Finite forbidden lattices," in *Universal algebra and lattice theory (Puebla, 1982)*, ser. Lecture Notes in Math. Vol. 1004, Berlin: Springer, 1983, pp. 176–205. DOI: 10.1007/BFb0063438.

[7] W. DeMeo, "Expansions of finite algebras and their congruence lattices," *Algebra Universalis*, vol. 69, pp. 257–278, 2013, Available from: github.com/williamdemeo/Overalgebras. DOI: 10.1007/s00012-013-0226-3.