FOUR GENERATORS OF AN EQUIVALENCE LATTICE WITH CONSECUTIVE BLOCK COUNTS

Gábor Czédli*

University of Szeged, Bolyai Institute. Szeged, Aradi vértanúk tere 1, HUNGARY 6720, http://www.math.u-szeged.hu/~czedli/

e-mail: czedli@math.u-szeged.hu

Dedicated to my esteemed coauthors, Honorary Professors László Szabó on his seventy-fifth birthday and Lajos Klukovits on his eightieth birthday.

This paper is probably self-contained for those who know the concept of a lattice as an algebraic structure. Our goal is two-fold. First, we present a historical remark on the connection between equivalence lattices and quasiorder lattices. Second, we prove a new theorem, which corresponds to the title of the paper.

1 Introduction and a historical remark

We begin with some notations and well-known definitions. The set of *equivalences* (in other words, *equivalence relations*, that is, reflexive, symmetric, and transitive relations) of a set A will be denoted by $\mathrm{Equ}(A)$. With intersections and the transitive hulls of unions acting as meets and joins, respectively, $\mathrm{Equ}(A)$ is a *lattice*, the *equivalence lattice* of (or over) A; the notation $\mathrm{Equ}(A)$ will stand for this lattice, too. By the canonical bijective correspondence between equivalences and partitions of a set, $\mathrm{Equ}(A)$ is isomorphic to the *partition lattice* $\mathrm{Part}(A)$ of A, which consists of all partitions of A. We will often consider equivalences as partitions. For $X \subseteq Y$, we say that X is a *proper* subset of Y if $X \neq Y$. A *sublattice* or a *complete sublattice* of $\mathrm{Equ}(A)$ is a nonempty subset that is closed with respect to binary joins and meets or to arbitrary joins and meets, respectively. A subset X of $\mathrm{Equ}(A)$ is a *generating set* or a *complete-generating set* of $\mathrm{Equ}(A)$ if there is

*This research was supported by the National Research, Development and Innovation Fund of Hungary, under funding scheme K 138892.

no proper sublattice Y or a proper complete sublattice Y of $\mathrm{Equ}(A)$, respectively, such that $X \subseteq Y$. *Quasiorders* are reflexive and symmetric relations. The quasiorders of a set A form a lattice, the *quasiorder lattice* $\mathrm{Quo}(A)$ of A. Note that $\mathrm{Equ}(A)$ is a complete sublattice of $\mathrm{Quo}(A)$.

In the middle of the seventies, Henrik Strietz proved that for any finite set A with $|A| \geq 3$, $\mathrm{Equ}(A)$ is *four-generated*, that is, it has a four-element generating set; see Strietz [10]–[11]. Since Strietz's work, more than a dozen papers have been devoted to four-element (or small) generating sets of equivalence lattices and quasiorder lattices; for details, see the "References" section here and the bibliographic sections and the survey parts of the papers listed there. Hence, instead of giving another survey, we focus only on the connection between the small generating sets of $\mathrm{Equ}(A)$ and those of $\mathrm{Quo}(A)$. In one direction, we recall an important statement from [9, page 61]; see also Lemma 2.1 of [7], where the original lemma is recalled.

Lemma 1.1 (Kulin's Lemma)**.** *If A is an arbitrary set with at least three elements and S is a complete sublattice of* $\mathrm{Quo}(A)$ *such that* $\mathrm{Equ}(A)$ *is a proper subset of S, then $S = \mathrm{Quo}(A)$.*

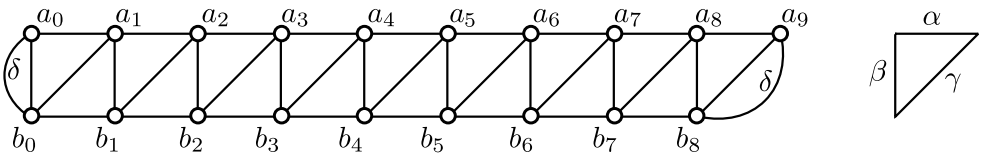

Figure 1: Zádori's construction for $|A| = 19$

In other directions, neither any connection nor the forthcoming Claim 1.4 has been published before. To present such a connection of historical value, let $|A| = 19$; the case of $|A| = 2k + 1 \geq 5$ would be similar. The construction visualized by Figure 1 is taken from Zádori [12].

Claim 1.2 ([12]; exemplifying the odd case of Zádori's construction)**.** *If $|A| = 19$, then* $\mathrm{Equ}(A)$ *has a four-element generating set.*

For later reference, we present Zádori's proof and his generating set.

Proof. For $p, q \in A$, the smallest equivalence collapsing p and q is an atom in $\mathrm{Equ}(A)$; we denote it by $\mathrm{at}(p, q)$. So $(x, y) \in \mathrm{at}(p, q)$ if and only if $x = y$ or $\{x, y\} = \{p, q\}$. Denote the elements of A as follows: $A = \{a_0, a_1, \ldots, a_9, b_0, b_1, \ldots, b_8\}$; see Figure 1. The figure defines a subset $X := \{\alpha, \beta, \gamma, \delta\}$ of the equivalence lattice $\mathrm{Equ}(A)$ as follows. Assume that the horizontal edges, the vertical edges, and the slanted straight edges of the graph are labeled

by α, β, and γ, respectively. To avoid a crowded figure, these labels are not indicated in the figure, but the triangle on the right reminds us of this convention. There are also two δ-labeled edges, which are drawn as curves. For $\epsilon \in X$, the figure defines ϵ as follows; walks of length zero are allowed.

$$\epsilon := \{(x, y) \in A^2 : \text{we can walk from } x \text{ to } y \text{ along } \epsilon\text{-colored edges}\}. \quad (1.1)$$

For example, $\{b_1, a_2\}$ is a block of γ and $\{b_0, \dots, b_8\}$ is a block of α. Let S be the sublattice generated by X. In Figure 2, where A is drawn three times, some equivalences are given by their non-singleton blocks. The meanings of these blocks, with different geometric orientations, line styles, and colors, are defined on the right of the figure. For example, $\rho_0 = \mathrm{at}(a_0, b_0)$ and $\lambda'_1 = \mathrm{at}(a_9, a_8) \vee \mathrm{at}(a_8, a_7) \vee \mathrm{at}(b_8, b_7)$. We can easily show that, in this order, ρ_0, ρ'_0, ρ''_0, ρ_1, ρ'_1, ρ''_1, ρ_2, ρ'_2, ρ''_2, ρ_3, ρ'_3, ρ''_3, ρ_4, ... belong to S, since each of them is expressible from the generators and the earlier ones. Indeed, $\rho_0 = \beta \wedge \delta$ and, for $i = 0, 1, 2, \dots$, we have that $\rho'_i = (\rho_i \vee \gamma) \wedge \alpha$, $\rho''_i = (\rho'_i \vee \beta) \wedge \gamma$, and $\rho_{i+1} = \big(((\rho''_i \vee \beta) \wedge \alpha) \vee \rho''_i\big) \wedge \beta$. The increasing sequences $(\rho_0, \rho_1, \rho_2, \dots)$, $(\rho'_0, \rho'_1, \rho'_2, \dots)$, and $(\rho''_0, \rho''_1, \rho''_2, \dots)$ are *right-going* in the sense that when the subscript increases by 1, the subscripted equivalence obtains a new "edge" on the right of the earlier edges. By interchanging the role of β and γ, we obtain three increasing "left-going" sequences $(\lambda_0, \lambda_1, \lambda_2, \dots)$, $(\lambda'_0, \lambda'_1, \lambda'_2, \dots)$, and $(\lambda''_0, \lambda''_1, \lambda''_2, \dots)$. Where a right-going sequence "reaches" the appropriate left-going one, the meet of the two sequences yields an atom of $\mathrm{Equ}(A)$. Namely, for $i \in \{0, 1, \dots, 8\}$, $\mathrm{at}(a_i, b_i) = \rho_i \wedge \lambda''_{8-i} \in S$, $\mathrm{at}(a_{i+1}, b_i) = \rho''_i \wedge \lambda_{8-i} \in S$, and $\mathrm{at}(a_i, a_{i+1}) = \rho'_i \wedge \lambda'_{8-i} \in S$. Furthermore, for $i \in \{0, \dots, 7\}$, $\mathrm{at}(b_i, b_{i+1}) = \big(\mathrm{at}(a_{i+1}, b_i) \vee \mathrm{at}(a_{i+1}, b_{i+1})\big) \wedge \alpha \in S$. Hence, for every edge (x, y) of the graph, $\mathrm{at}(x, y) \in S$. Therefore, the following lemma implies easily that X generates $\mathrm{Equ}(A)$. □

Lemma 1.3. *If* $3 \leq n \in \mathbb{N}^+ = \{1, 2, 3, \dots\}$, $A = \{a_0, a_1, \dots, a_{n-1}\}$, *and* $|A| = n$, *then* $\{\mathrm{at}(a_{i-1}, a_i) : i \in \{1, \dots, n-1\}\} \cup \{\mathrm{at}(a_{n-1}, a_0)\}$ *generates* $\mathrm{Equ}(A)$.

In some form, this easy lemma occurs in several papers; see, e.g., [3, Lemma 2.2] and [8, Lemma 2.5].

In 1995, the author visited Ivan Chajda at Palacký University in Olomouc. The research plan looked easy: by orienting the edges of the graph in Figure 1 in some way, we should find a small generating set of $\mathrm{Quo}(A)$. Our first construction was soon developed into a more sophisticated one, and so the first construction does not occur [1]. However, we need the first

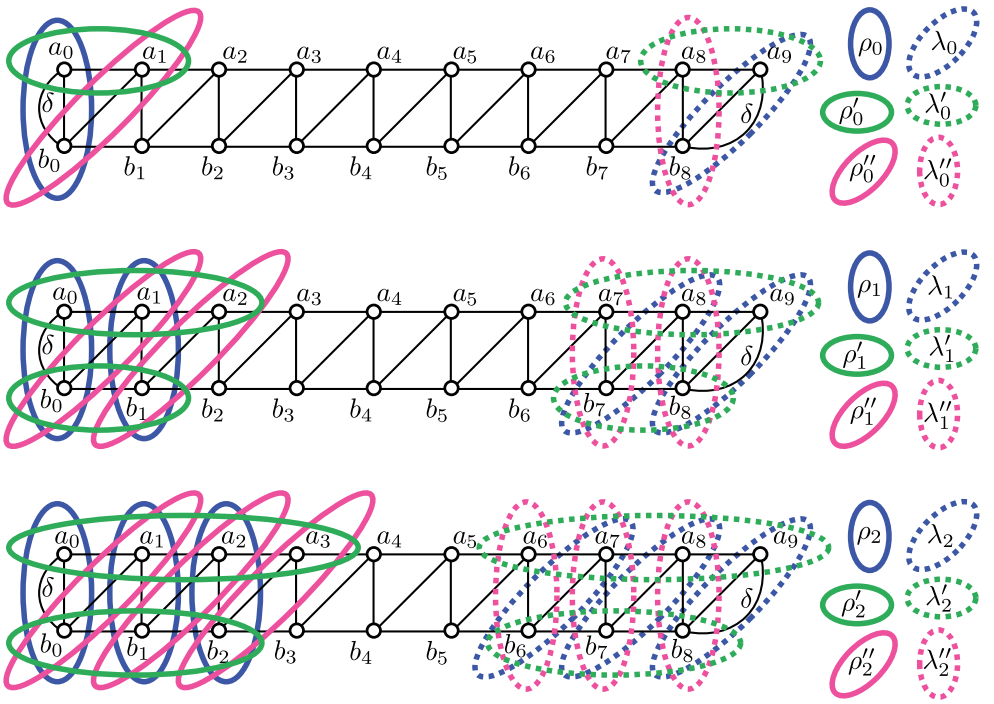

Figure 2: Right-going and left-going sequences

construction[1] here even though [1] contains a stronger result and we have an even stronger one nowadays.

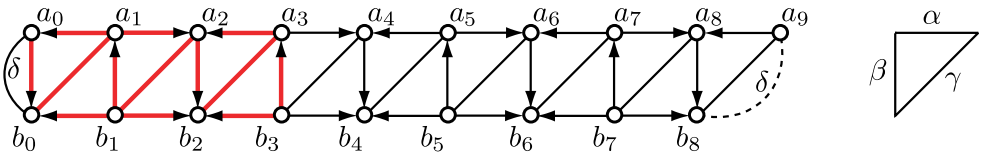

Figure 3: Generating a quasiorder lattice

Let $A = \{a_0, a_1, \ldots, a_9, b_0, b_1, \ldots, b_8\}$ be the 19-element set drawn in Figure 3, which is quite similar to Figure 1. Some edges are directed by arrowheads, some others are not. The figure defines a set $Y_0 = \{\alpha, \beta, \gamma, \delta\}$ of quasiorders of A by (1.1) with the only modification that we cannot walk along a directed edge in the opposite direction. Along an undirected edge, we can walk in both directions. At present, it makes no difference whether an edge is red and thick or not. For example, $(a_3, a_2), (a_3, a_4) \in \alpha$, $(a_3, b_2), (b_2, a_3) \in \gamma$, but $(b_4, a_4) \notin \beta$ and $(a_2, a_3), (a_3, a_7) \notin \alpha$. For $\epsilon \in Y_0$,

[1] Its exact details have been lost but the idea of Claim 1.4 is the same.

denote $\epsilon^{-1} = \{(y,x) : (x,y) \in \epsilon\} \in \mathrm{Quo}(A)$ the *inverse* of ϵ. Note that γ and δ are equivalences, and so $\gamma^{-1} = \gamma$ and $\delta^{-1} = \delta$. Let $Y := Y_0 \cup \{\epsilon^{-1} : \epsilon \in Y_0\} = \{\alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \delta\}$.

Claim 1.4. *The six-element set Y generates* $\mathrm{Quo}(A)$.

Outline of the proof. For $x, y \in A$, $\mathrm{qu}(x,y)$ denotes the smallest quasiorder containing (x,y). Let S stand for the sublattice generated by Y. Since $f\colon \mathrm{Quo}(A) \to \mathrm{Quo}(A)$ defined by $\mu \mapsto \mu^{-1}$ is an automorphism of $\mathrm{Quo}(A)$ and Y is f-closed, S is also closed with respect to forming inverses. In particular, whenever $\mathrm{qu}(x,y)$ is in S, then so is $\mathrm{qu}(y,x)$; this fact will be used without further explanation. Let us compute; each containment "$\in S$" below follows from the earlier ones and $Y \subseteq S$:

$$\mathrm{qu}(a_0,b_0) = \beta \wedge \delta \in S, \tag{1.2}$$
$$\mathrm{qu}(a_1,b_0) = (\alpha \vee \mathrm{qu}(a_0,b_0)) \wedge \gamma \in S, \text{ by (1.2)}, \tag{1.3}$$
$$\mathrm{qu}(a_1,a_0) = \alpha \wedge (\mathrm{qu}(a_1,b_0) \vee \mathrm{qu}(b_0,a_0)) \in S \text{ by (1.3) and (1.2)}, \tag{1.4}$$
$$\mathrm{qu}(b_1,a_1) = (\alpha \vee \mathrm{qu}(b_0,a_1)) \wedge \beta \in S \text{ by (1.3)}, \tag{1.5}$$
$$\mathrm{qu}(b_1,b_0) = \alpha \wedge (\mathrm{qu}(b_1,a_1) \vee \mathrm{qu}(a_1,b_0)) \in S \text{ by (1.5) and (1.3)}, \tag{1.6}$$
$$\mathrm{qu}(b_1,a_2) = \gamma \wedge (\mathrm{qu}(b_1,a_1) \vee \alpha) \in S \text{ by (1.5)}, \tag{1.7}$$
$$\mathrm{qu}(a_1,a_2) = \alpha \wedge (\mathrm{qu}(a_1,b_1) \vee \mathrm{qu}(b_1,a_2)) \in S \text{ by (1.5) and (1.7)}, \tag{1.8}$$
$$\mathrm{qu}(a_2,b_2) = \beta \wedge (\mathrm{qu}(a_2,b_1) \vee \alpha) \in S \text{ by (1.7)}, \tag{1.9}$$
$$\mathrm{qu}(b_1,b_2) = \alpha \wedge (\mathrm{qu}(b_1,a_2) \vee \mathrm{qu}(a_2,b_2)) \in S \text{ by (1.7) and (1.9)}, \tag{1.10}$$
$$\mathrm{qu}(a_3,b_2) = \gamma \wedge (\alpha \vee \mathrm{qu}(a_2,b_2)) \in S \text{ by (1.9)}, \tag{1.11}$$
$$\mathrm{qu}(a_3,a_2) = \alpha \wedge (\mathrm{qu}(a_3,b_2) \vee \mathrm{qu}(b_2,a_2)) \in S \text{ by (1.11) and (1.9)}, \tag{1.12}$$
$$\mathrm{qu}(b_3,a_3) = \beta \wedge (\alpha \vee \mathrm{qu}(b_2,a_3)) \in S \text{ by (1.11)}, \tag{1.13}$$
$$\mathrm{qu}(b_3,b_2) = \alpha \wedge (\mathrm{qu}(b_3,a_3) \vee \mathrm{qu}(a_3,b_2)) \in S \text{ by (1.13) and (1.11)}, \tag{1.14}$$

and so on. Computations (1.2)–(1.14) and the fact that S is closed with respect to forming inverses show that for each thick and red edge (x,y) of the graph, $\mathrm{qu}(x,y)$ and $\mathrm{qu}(y,x)$ are in S. The figure and (1.2)–(1.14) also show how we can proceed further to the right. Hence, $\mathrm{qu}(x,y)$ and $\mathrm{qu}(y,x)$ are in S for every edge (x,y) of the graph. Thus, the straightforward counterpart of Lemma 1.3 for quasiorder lattices completes the proof of Claim 1.4. □

In the proof above, δ was needed only in the first step, (1.2). This step and the whole proof still work if we omit the dashed curve in Figure 3 and replace δ by the equivalence $\mathrm{at}(a_0,b_0)$. Now we do not need a left-going sequence of quasiorders. Hence, and this was a surprise in 1995, we do not need the figure to end on the right. So A can be $\{a_i : i \in \mathbb{N}_0\} \cup \{b_i : i \in \mathbb{N}_0\}$,

where $\mathbb{N}_0 = \{0, 1, 2, \dots\}$; this was the moment when an *infinite base set* came into the picture.

Infinite base sets required new techniques, first for quasiorder lattices, see [1]. The new techniques were soon adapted to infinite equivalence lattices; see, e.g., [2]. Later, it appeared that these techniques are useful for finite equivalence lattices; see [3] and [8]. Due to the results of these two papers, a connection with cryptography has been discovered; see [3] and, mainly, [4]. This connection and many earlier results on four-element generating sets motivate Section 2, where a new four-element generating set is constructed. To summarize our historical remark: In some sense, most papers mentioned so far and the present one grew from the unpublished proof of Claim 1.4.

Finally, to conclude this section, note that we can obtain a four-element generating set of $\mathrm{Quo}(A)$ for $|A| = 19$, that is, a stronger result, as follows. (However, this argument does not show how to step from the class of finite equivalence and quasiorder lattices to that of the infinite ones.) Going after [7] and using Figure 1, add a new δ-curve, a directed one, from a_1 to a_2. That is, we change δ to $\delta \vee \mathrm{qu}(a_1, a_2)$. By the proof of Claim 1.2, we obtain all members of $\mathrm{Equ}(A)$ from $X := \{\alpha, \beta, \gamma, \delta\}$. Thus, X generates $\mathrm{Quo}(A)$ by (Kulin's) Lemma 1.1.

2 A new four-element generating set with a special property

The *block count* of an equivalence $\mu \in \mathrm{Equ}(A)$ is the number $\mathrm{blnum}(\mu)$ of blocks of (the partition corresponding to) μ. We say that $X = \{\mu_1, \mu_2, \mu_3, \mu_4\}$ is a *four-element generating set of* $\mathrm{Equ}(A)$ *with consecutive block counts* if X generates $\mathrm{Equ}(A)$ and $\mathrm{blnum}(\mu_{1+i}) = \mathrm{blnum}(\mu_1) + i$ for $i \in \{1, 2, 3\}$. We are going to prove the following theorem.

Theorem 2.1. *If the number of elements of a finite set A is six or it is at least eight, then* $\mathrm{Equ}(A)$ *has a four-element generating set with consecutive block counts.*

Similar properties (namely, "same block counts" and "the difference between the block counts ≤ 2") have been studied in [5] and [6]; the property we consider in this section is more difficult to fulfill. Despite some similarities with [5] and [6] in the approach, the present paper remains self-contained.

Remark 2.2. We know that if $|A| < 6$, then $\mathrm{Equ}(A)$ has no four-element generating set with consecutive block counts; we guess the same for $|A| = 7$.

A pair (μ, ν) of elements of $\mathrm{Equ}(A)$ is *complementary* if $\mu \vee \nu = \mathbf{1}_A$, the top element of $\mathrm{Equ}(A)$, and $\mu \wedge \nu = \mathbf{0}_A$, the bottom element of $\mathrm{Equ}(A)$.

Definition 2.3 ([5]). A 7-tuple $\mathbf{A} = (A; \alpha, \beta, \gamma, \delta; u, v)$ is called an *eligible system* if A is a nonempty set, $\{\alpha, \beta, \gamma, \delta\}$ is a generating set of $\mathrm{Equ}(A)$, and the pairs (α, δ), $\bigl(\beta, \gamma \vee \mathrm{at}(u, v)\bigr)$, and $\bigl(\beta \vee \mathrm{at}(u, v), \gamma\bigr)$ are complementary.

For $\rho \subseteq (A')^2$, $\overline{\mathrm{eq}}'(\rho)$ will denote the smallest equivalence of A' that includes ρ. For distinct elements $x, y \in A'$, let $\mathrm{at}'(x, y) := \overline{\mathrm{eq}}'(\{(x, y)\})$. The lattice operations in $\mathrm{Equ}(A')$ will be denoted by $\vee'$ and $\wedge'$.

Lemma 2.4. *Let* $\mathbf{A}$ *be an eligible system with components denoted as in Definition 2.3. Assume that* $u', v' \notin A$ *and* $u' \neq v'$. *Let* $A' := A \cup \{u', v'\}$, $\alpha' := \overline{\mathrm{eq}}'(\alpha) \vee' \mathrm{at}'(u, u')$, $\beta' := \overline{\mathrm{eq}}'(\beta) \vee' \mathrm{at}'(u, v')$, $\gamma' := \overline{\mathrm{eq}}'(\gamma) \vee' \mathrm{at}'(v, v')$, $\delta' := \overline{\mathrm{eq}}'(\delta) \vee' \mathrm{at}'(u', v')$. *Then* $\mathbf{A}' := (A'; \alpha', \beta', \gamma', \delta'; u', v')$ *is an eligible system, too. Furthermore, if* $\Phi := \{\alpha, \beta, \gamma, \delta\}$ *is of consecutive block counts, then so is* $\Phi' := \{\alpha', \beta', \gamma', \delta'\}$.

Proof. The situation is visualized in Figure 4, where the blocks of some elements, all important elements from our perspective, are drawn. The three blocks drawn by solid lines are blocks of some members of $\Phi \subseteq \mathrm{Equ}(A)$. The seven blocks drawn in non-solid line styles (dotted and various kinds of dashed) are blocks of the equivalences belonging to $\Phi' \subseteq \mathrm{Equ}(A')$. The figure uses different line styles or distinct colors for the blocks of different equivalences, but we use the same color for $\epsilon \in \Phi$ and ϵ'. Note that the geometrically large blocks on the left could be singletons and, on the other hand, $u/\alpha := \{x : (x, u) \in \alpha\}$ and v/γ can be but need not be disjoint. Not all blocks of all ϵ and ϵ' are drawn for $\epsilon \in \Phi$. However, for any $x \in A$ and $\epsilon \in \Phi$, if the block x/ϵ is not drawn, then $x/\epsilon = x/\epsilon'$. The last sentence of Lemma 2.4 follows from the trivial fact that $\mathrm{blnum}(\epsilon') = 1 + \mathrm{blnum}(\epsilon)$ holds for every $\epsilon \in \Phi$. Applying a lemma from [5] twice (in a "twisted way" and in a "straight way"), we could derive the rest of Lemma 2.4 from [5]. To keep the paper self-contained, we give a different and direct proof.

The existence of an $x \in u/\beta \wedge v/\gamma$ would violate the conjunction of $\beta \wedge (\gamma \vee \mathrm{at}(u, v)) = \mathbf{0}_A$ and $\gamma \wedge (\beta \vee \mathrm{at}(u, v)) = \mathbf{0}_A$ —call them the *meet conditions* for β and γ— and $u \neq v$. Thus, u/β and v/γ are disjoint.

By the two paragraphs above, Figure 4 faithfully represents the situation and contains all the details the proof needs. Hence, it is straightforward to verify that the three pairs in Definition 2.3 for $\mathrm{Equ}(A')$ are complementary. Let S and E denote the sublattice generated by Φ' in $\mathrm{Equ}(A')$ and the sublattice $\{\mu \in \mathrm{Equ}(A') : \text{ both } u'/\mu \text{ and } v'/\mu \text{ are singletons}\}$. Then $f\colon \mathrm{Equ}(A) \to E$ defined by $\mu \mapsto \overline{\mathrm{eq}}'(\mu)$ is a lattice isomorphism.

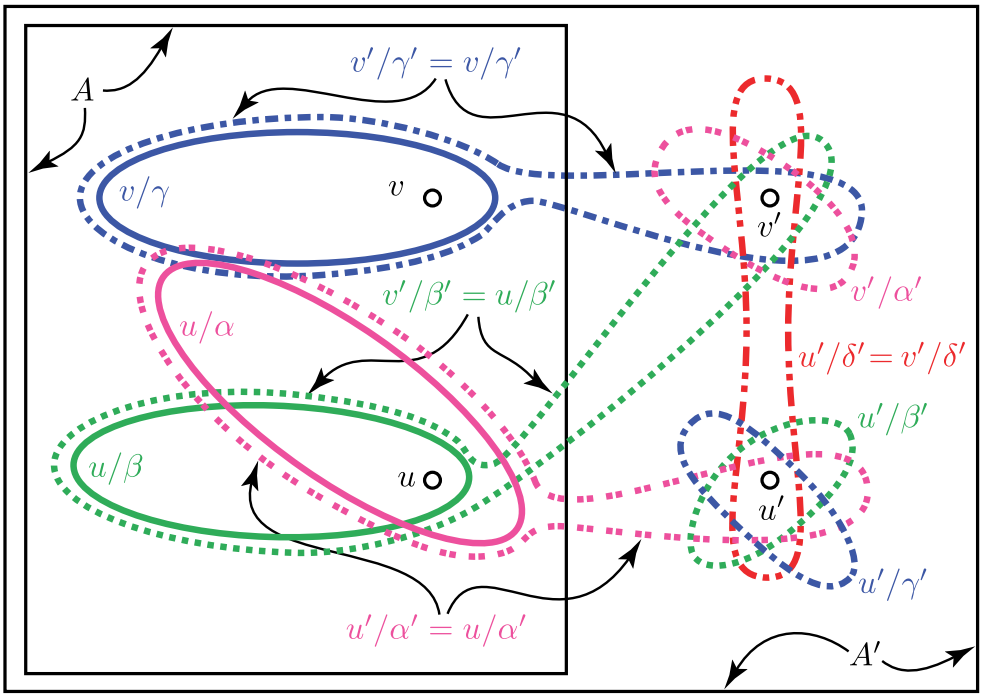

Figure 4: Illustrating the proof of Lemma 2.4

Observe that $\{u'\}$ is a singleton block of $\beta' \vee' \gamma'$. Furthermore, $\{v'\}$ is a singleton block of both α' and $\delta' \wedge' (\beta' \vee' \gamma')$. Thus $\{v'\}$ is a singleton block of $\alpha' \vee' \big(\delta' \wedge' (\beta' \vee' \gamma')\big)$. Therefore, with

$$\kappa := (\beta' \vee' \gamma') \wedge' \Big(\alpha' \vee' \big(\delta' \wedge' (\beta' \vee' \gamma')\big)\Big),$$

$|u'/\kappa| = |v'/\kappa| = 1$. Using the fact that $\epsilon \subseteq \epsilon'$ for all $\epsilon \in X$, the join condition $\beta \vee \mathrm{at}(u, v) \vee \gamma = \mathbf{1}_A$ for β and γ, and $(u, v) \in \beta' \vee' \gamma'$, we obtain that $A^2 \subseteq \beta' \vee' \gamma'$. By the previous two "$\subseteq$" inclusions, $\delta \subseteq \delta' \wedge' (\beta' \vee' \gamma')$. Using this fact, $\alpha \subseteq \alpha'$, and the join condition for the complementary pair (α, δ), we obtain that $A^2 \subseteq \kappa$. Combining this with $|u'/\kappa| = |v'/\kappa| = 1$, we have that $f(\mathbf{1}_A) = \kappa \in S$. Thus, for all $\epsilon \in \Phi$, $f(\epsilon) = f(\mathbf{1}_A) \wedge \epsilon' \in S$, whereby $f(\Phi) \subseteq S$. Since Φ generates $\mathrm{Equ}(A)$ and $f\colon \mathrm{Equ}(A) \to E$ is an isomorphism, we obtain that $E \subseteq S$. In particular, $\mathrm{at}'(u, v) = f(\mathrm{at}(u, v)) \in S$. As the following equalities are clear by the figure, we obtain further

elements of S as follows:

$$\mathrm{at}'(v,v') = (\mathrm{at}'(u,v) \vee' \beta') \wedge' \gamma' \in S, \tag{2.1}$$
$$\mathrm{at}'(v',u) = (\mathrm{at}'(u,v) \vee \mathrm{at}'(v,v')) \wedge' \beta' \in S,$$
$$\mathrm{at}'(v',u') = (\mathrm{at}'(v',u) \vee' \alpha') \wedge' \delta' \in S, \text{ and} \tag{2.2}$$
$$\mathrm{at}'(u',u) = \alpha' \wedge' (\mathrm{at}'(u',v') \vee' \mathrm{at}'(v',u)) \in S. \tag{2.3}$$

Finally, since $E \subseteq S$ and we have (2.1), (2.2), and (2.3), Lemma 1.3 implies that $S = \mathrm{Equ}(A')$. This completes the proof of Lemma 2.4. □

Lemma 2.5. *With* $A = \{1, 2, \ldots, 6\}$,

$$\alpha := \mathrm{eq}(12; 3; 45; 6), \tag{2.4}$$
$$\beta := \mathrm{eq}(1; 2; 34; 5; 6), \tag{2.5}$$
$$\gamma := \mathrm{eq}(13; 24; 56), \text{ and} \tag{2.6}$$
$$\delta := \mathrm{eq}(146; 235), \tag{2.7}$$

$\mathbf{A} = (A; \alpha, \beta, \gamma, \delta; 4, 6)$ *is an eligible system with consecutive block counts.*

Proof. Let $\Phi := \{\alpha, \beta, \gamma, \delta\}$, and let S stand for the sublattice generated by S. The labels above the equality signs will indicate which members of S imply that the equivalences on the left of these equality signs belong to S.

$$\mathrm{eq}(12; 345; 6) \overset{(2.4)(2.5)}{=} \mathrm{eq}(12; 3; 45; 6) \vee \mathrm{eq}(1; 2; 34; 5; 6), \tag{2.8}$$
$$\mathrm{eq}(1234; 56) \overset{(2.5)(2.6)}{=} \mathrm{eq}(1; 2; 34; 5; 6) \vee \mathrm{eq}(13; 24; 56), \tag{2.9}$$
$$\mathrm{eq}(12; 3; 4; 5; 6) \overset{(2.4)(2.9)}{=} \mathrm{eq}(12; 3; 45; 6) \wedge \mathrm{eq}(1234; 56), \tag{2.10}$$
$$\mathrm{eq}(1; 2; 35; 4; 6) \overset{(2.7)(2.8)}{=} \mathrm{eq}(146; 235) \wedge \mathrm{eq}(12; 345; 6), \tag{2.11}$$
$$\mathrm{eq}(14; 23; 5; 6) \overset{(2.7)(2.9)}{=} \mathrm{eq}(146; 235) \wedge \mathrm{eq}(1234; 56), \tag{2.12}$$
$$\mathrm{eq}(1; 2; 345; 6) \overset{(2.5)(2.11)}{=} \mathrm{eq}(1; 2; 34; 5; 6) \vee \mathrm{eq}(1; 2; 35; 4; 6), \tag{2.13}$$
$$\mathrm{eq}(1356; 24) \overset{(2.6)(2.11)}{=} \mathrm{eq}(13; 24; 56) \vee \mathrm{eq}(1; 2; 35; 4; 6), \tag{2.14}$$
$$\mathrm{eq}(14; 235; 6) \overset{(2.11)(2.12)}{=} \mathrm{eq}(1; 2; 35; 4; 6) \vee \mathrm{eq}(14; 23; 5; 6), \tag{2.15}$$
$$\mathrm{eq}(1; 2; 3; 45; 6) \overset{(2.4)(2.13)}{=} \mathrm{eq}(12; 3; 45; 6) \wedge \mathrm{eq}(1; 2; 345; 6), \tag{2.16}$$
$$\mathrm{eq}(16; 2; 35; 4) \overset{(2.7)(2.14)}{=} \mathrm{eq}(146; 235) \wedge \mathrm{eq}(1356; 24), \tag{2.17}$$
$$\mathrm{eq}(13; 2456) \overset{(2.6)(2.16)}{=} \mathrm{eq}(13; 24; 56) \vee \mathrm{eq}(1; 2; 3; 45; 6), \tag{2.18}$$
$$\mathrm{eq}(126; 35; 4) \overset{(2.10)(2.17)}{=} \mathrm{eq}(12; 3; 4; 5; 6) \vee \mathrm{eq}(16; 2; 35; 4), \tag{2.19}$$

$$\mathrm{eq}(145;23;6) \overset{(2.12)(2.16)}{=} \mathrm{eq}(14;23;5;6) \vee \mathrm{eq}(1;2;3;45;6), \tag{2.20}$$

$$\mathrm{eq}(15;2;3;4;6) \overset{(2.14)(2.20)}{=} \mathrm{eq}(1356;24) \wedge \mathrm{eq}(145;23;6), \tag{2.21}$$

$$\mathrm{eq}(1;26;3;4;5) \overset{(2.18)(2.19)}{=} \mathrm{eq}(13;2456) \wedge \mathrm{eq}(126;35;4), \tag{2.22}$$

$$\mathrm{eq}(135;2;4;6) \overset{(2.11)(2.21)}{=} \mathrm{eq}(1;2;35;4;6) \vee \mathrm{eq}(15;2;3;4;6), \tag{2.23}$$

$$\mathrm{eq}(14;2356) \overset{(2.15)(2.22)}{=} \mathrm{eq}(14;235;6) \vee \mathrm{eq}(1;26;3;4;5), \tag{2.24}$$

$$\mathrm{eq}(13;2;4;5;6) \overset{(2.6)(2.23)}{=} \mathrm{eq}(13;24;56) \wedge \mathrm{eq}(135;2;4;6), \tag{2.25}$$

$$\mathrm{eq}(1;2;3;4;56) \overset{(2.6)(2.24)}{=} \mathrm{eq}(13;24;56) \wedge \mathrm{eq}(14;2356). \tag{2.26}$$

In particular, $\mathrm{at}(1,2) \in S$ by (2.10), $\mathrm{at}(2,6) \in S$ by (2.22), $\mathrm{at}(6,5) \in S$ by (2.26), $\mathrm{at}(5,4) \in S$ by (2.16), $\mathrm{at}(4,3) \in S$ by (2.5), and $\mathrm{at}(3,1) \in S$ by (2.25). Hence, Φ is a generating set by Lemma 1.3. Clearly, Φ is of consecutive block counts. It is easy to check that the pairs in Definition 2.3 are complementary. Thus, $\mathbf{A}$ is an eligible system, proving Lemma 2.5. □

The author has created a program package called "equ2024p", available from his website http://tinyurl.com/g-czedli/. This program package can also "prove" that Φ generates $\mathrm{Equ}(A)$, but verifying the programs is much more difficult than verifying the proofs of Lemmas 2.5 and (the next) 2.6.

Lemma 2.6. *With* $A = \{1, 2, \ldots, 9\}$,

$$\alpha := \mathrm{eq}(158;2;3;47;69), \tag{2.27}$$

$$\beta := \mathrm{eq}(1;23;4;56;78;9), \tag{2.28}$$

$$\gamma := \mathrm{eq}(135;268;4;79), \text{ and} \tag{2.29}$$

$$\delta := \mathrm{eq}(16;257;3489), \tag{2.30}$$

$\mathbf{A} = (A;\alpha,\beta,\gamma,\delta;1,4)$ *is an eligible system with consecutive block counts.*

The proof of this lemma is similar to but more than three times longer than the previous proof. As the reader would hardly enjoy such an amount of technicalities, the proof goes into the Appendix of the extended version of the paper; it is available at https://arxiv.org/abs/2410.15328 or https://doi.org/10.48550/arXiv.2410.15328.

Now, we are in the position to prove our theorem.

Proof of Theorem 2.1. Combine Lemmas 2.4, 2.5, and 2.6. □

References

[1] I. Chajda, G. Czédli, How to generate the involution lattice of quasiorders? Studia Sci. Math. Hungar., **32** (1996), 415–427.

[2] G. Czédli, Four-generated large equivalence lattices, Acta Sci. Math. (Szeged), **62** (1996), 47–69.

[3] G. Czédli, Four-generated direct powers of partition lattices and authentication, Publicationes Mathematicae (Debrecen), **99** (2021), 447–472. https://doi.org/10.5486/PMD.2021.9024

[4] G. Czédli, Generating Boolean lattices by few elements and exchanging session keys, Novi Sad Journal of Mathematics, https://doi.org/10.30755/NSJOM.16637 (online first)

[5] G. Czédli, A pair of four-element horizontal generating sets of a partition lattice, preprint.

[6] G. Czédli, Four-element generating sets with block count widths at most two in partition lattices, preprint.

[7] G. Czédli, J. Kulin, A concise approach to small generating sets of lattices of quasiorders and transitive relations, Acta Sci. Math. (Szeged), **83** (2017), 3–12. https://dx.doi.org/10.14232/actasm-016-056-2

[8] G. Czédli, L. Oluoch, Four-element generating sets of partition lattices and their direct products, Acta Sci. Math. (Szeged), **86** (2020), 405–448. https://doi.org/10.14232/actasm-020-126-7

[9] J. Kulin, Quasiorder lattices are five-generated. Discussiones Mathematicae — General Algebra and Applications, **36** (2016), 59–70. https://dx.doi.org/10.7151/dmgaa.1248

[10] H. Strietz: Finite partition lattices are four-generated. In: Proc. Lattice Theory Conf. Ulm, 1975, pp. 257–259.

[11] H. Strietz, Über Erzeugendenmengen endlicher Partitionenverbände, Studia Sci. Math. Hungar., **12** (1977), 1–17. (German)

[12] L. Zádori, Generation of finite partition lattices. In: Lectures in universal algebra. (Proc. Colloq. Szeged, 1983) Colloq. Math. Soc. János Bolyai, Vol. 43. Amsterdam: North-Holland, 1986, pp. 573–586.