Four-generated direct powers of partition lattices and authentication

By Gábor Czédli

Dedicated to Professor László Zádori on his sixtieth birthday

Abstract. For an integer $n \geq 5$, H. Strietz (1975) and L. Zádori (1986) proved that the lattice $\mathrm{Part}(n)$ of all partitions of $\{1, 2, \ldots, n\}$ is four-generated. Developing L. Zádori's particularly elegant construction further, we prove that even the k-th direct power $\mathrm{Part}(n)^k$ of $\mathrm{Part}(n)$ is four-generated for many but only finitely many exponents k. E.g., $\mathrm{Part}(100)^k$ is four-generated for every $k \leq 3 \cdot 10^{89}$, and it has a four-element generating set that is not an antichain for every $k \leq 1.4 \cdot 10^{34}$. In connection with these results, we outline a protocol how to use these lattices in authentication and secret key cryptography.

1. Introduction

This paper is dedicated to László Zádori not only because of his birthday, but also because a nice construction from his very first mathematical paper is heavily used here. Our starting point is that Strietz [16, 17] proved in 1975 that

$$\left. \begin{array}{l} \text{the lattice } \mathrm{Part}(n) \text{ of all partitions of the (finite)} \\ \text{set } \{1, 2, \ldots, n\} \text{ is a four-generated lattice.} \end{array} \right\} \tag{1.1}$$

A decade later, Zádori [19] gave a very elegant proof of this result (and proved even more, which is not used in the present paper). Zádori's construction has opened lots of perspectives; this is witnessed by Chajda and Czédli [3], Czédli [4, 5, 6, 7], Czédli and Kulin [8], Kulin [12], and Takách [18].

Our goal is to generalize (1.1) from partition lattices to their direct powers; see Theorems 3.1 and 4.1 later. Passing from $\mathrm{Part}(n)$ to $\mathrm{Part}(n)^k$ has some content because of four reasons, which will be given with more details later; here we only mention these reasons tangentially. First, even the direct square of a four-generated lattice need not be four-generated. Second, if some direct power of a lattice is four-generated, then so are the original lattice and all of its other direct powers with smaller exponents; see Corollaries 3.2 and 4.2. Third, for each non-singleton finite lattice L, there is a (large) positive integer $k_0 = k_0(L)$ such that for every $k \geq k_0$, the direct power L^k is *not* four-generated; this explains that the exponent is not arbitrary in our theorems. We admit that we could not determine the set $\{k : \mathrm{Part}(n)^k$ is four-generated$\}$, that is, we could not find the least k_0; this task will probably remain unsolved for long. Fourth, a whole section of this paper is devoted to the applicability of complicated lattices with few generators in Information Theory.

Although this paper has some links to Information Theory, it is primarily a *lattice theoretical* paper. Note that only some elementary facts, regularly taught in graduate (and often in undergraduate) algebra, are needed about lattices. For those who know how to compute the join of two equivalence relations the paper is probably self-contained. If not, then a small part of each of the monographs Burris and Sankappanavar [1], Grätzer [10, 11], and Nation [13] can be recommended; note that [1] and [13] are freely downloadable at the time of writing.

Outline. The rest of the paper is structured as follows. Section 2 gives the rudiments of partition lattices and recalls Zádori's construction in details; these details will be used in the subsequent two sections. Section 3 formulates and proves our first result, Theorem 3.1, which asserts that $\mathrm{Part}(n)^k$ is four-generated for certain values of k. In Section 4, we formulate and prove Theorem 4.1 about the existence of a four-element generating set of order type $1 + 1 + 2$ in $\mathrm{Part}(n)^k$. Finally, Section 5 offers a protocol for authentication based on partition lattices and their direct powers; this protocol can also be used in secret key cryptography.

2. Rudiments and Zádori's construction

Below, we are going to give some details in few lines for the sake of those not familiar with partition lattices and, in addition, we are going to fix the corresponding notation. For a set A, a set of pairwise disjoint nonempty subsets of A is a *partition* of A if the union of these subsets, called *blocks*, is A. For example,

$$U = \{\{1,3\},\{2,4\},\{5\}\} \tag{2.1}$$

is a partition of $A = \{1,2,3,4,5\}$. For pairwise distinct elements $a_1,\dots,a_k$ of A, the partition of A with block $\{a_1,\dots,a_k\}$ such that all the other blocks are singletons will be denoted by $[\![a_1,\dots a_k]\!]^{\text{e}}$. Then, in our notation, U from (2.1) is the same as

$$[\![1,3]\!]^{\text{e}} + [\![2,4]\!]^{\text{e}}. \tag{2.2}$$

For partitions U and V of A, we say that $U \leq V$ if and only if every block of U is as subset of a (unique) block of V. With this ordering, the set of all partitions of A turns into a lattice, which we denote by $\mathrm{Part}(A)$. For brevity,

$$\mathrm{Part}(n) \text{ will stand for } \mathrm{Part}(\{1,2,\dots,n\}), \tag{2.3}$$

and also for $\mathrm{Part}(A)$ when A is a given set consisting of n elements. Associated with a partition U of A, we define an *equivalence relation* π_U of A as the collection of all pairs $(x,y) \in A^2$ such that x and y belong to the same block of U. As it is well known, the equivalence relations and the partitions of A mutually determine each other, and $\pi_U \leq \pi_V$ (which is our notation for $\pi_U \subseteq \pi_V$) if and only if $U \leq V$. Hence, the *lattice* $\mathrm{Equ}(A)$ *of all equivalence relations* of A (in short, the *equivalence lattice* of A) is isomorphic to $\mathrm{Part}(A)$. In what follows, we do not make a sharp distinction between a partition and the corresponding equivalence relation; no matter which of them is given, we can use the other one without warning. For example, (2.2) also denotes an equivalence relation associated with the partition given in (2.1), provided the base set $\{1,2,\dots,5\}$ is understood. So we define and denote equivalences as the partitions above but we prefer to work in $\mathrm{Equ}(A)$ and $\mathrm{Equ}(n) = \mathrm{Equ}(\{1,\dots,n\})$, because the lattice operations are easier to handle in $\mathrm{Equ}(A)$. For $\kappa,\lambda \in \mathrm{Equ}(A)$, the *meet* and the *join* of κ and λ, denoted by $\kappa\lambda$ (or $\kappa \cdot \lambda$) and $\kappa + \lambda$, are the intersection and the transitive hull of the union of κ and λ, respectively. The advantage of this notation is that the usual precedence rule allows us to write, say, $xy + xz$ instead of $(x \wedge y) \vee (x \wedge z)$. *Lattice terms* are composed from variables and join and meet operation signs in the usual way; for example, $f(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_3 + x_4) + (x_1 + x_3)(x_2 + x_4)$ is

a quaternary lattice term. Given a lattice L and $a_1, \ldots, a_k \in L$, the *sublattice generated* by $\{a_1, \ldots, a_k\}$ is denoted and defined by

$$[a_1, \ldots, a_k]_{\text{lat}} := \{f(a_1, \ldots, a_k) : a_1, \ldots, a_k \in L, \ f \text{ is a lattice term}\}. \qquad (2.4)$$

If there are pairwise distinct elements $a_1, \ldots, a_k \in L$ such that $[a_1, \ldots, a_k]_{\text{lat}} = L$ then L is said to be a *k-generated lattice*.

Almost exclusively, we are going to define our equivalence relations by (undirected simple, edge-colored) graphs. Every horizontal thin straight edge is α-colored but its color, α, is not always indicated in the figures. The thin straight edges of slope 1, that is the southwest-northeast edges, are β-colored while the thin straight edges with slope -1, that is the southeast-northwest edges, are γ-colored. Finally, the thin *solid* curved edges are δ-colored. (We should disregard the *dashed* ovals at this moment. Note that except for Figure 4, every edge is thin.) Figure 1 helps to keep this convention in mind. On the vertex set A, this figure and the other figures in the paper define an *equivalence* (relation) $\alpha \in \text{Equ}(A)$ in the following way: deleting all edges but the α-colored ones, the components of the remaining graph are the blocks of the partition associated with α. In other words, $\langle x, y \rangle \in \alpha$ if and only if there is an α-colored path from vertex x to vertex y in the graph, that is, a path (of possibly zero length) all of whose edges are α-colored. The equivalences β, γ, and δ are defined analogously. The success of Zádori's construction, to be discussed soon, lies in the fact of this visualization. Note that, to make our figures less crowded, the labels $\alpha, \ldots, \delta$ are not always indicated but

$$\text{our convention, shown in Figure 1, defines the color of the edges} \qquad (2.5)$$
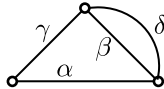
even in this case.

Figure 1. Standard notation for this paper

Let us agree upon the following notation:

$$\left. \begin{aligned} \sum_{\text{for all meaningful } x} [\![u_x, v_x]\!]^{\text{e}} \text{ will be denoted by} \\ [\![u_x, v_x]\!]^{\text{e}}_{\forall} \text{ or } \quad [\![u_y, v_y]\!]^{\text{e}}_{\forall}; \end{aligned} \right\} \qquad (2.6)$$

that is, each of x and y in subscript or superscript position will mean that a join is formed for all meaningful values of these subscripts or superscript. If only a part of the meaningful subscripts or superscripts are needed in a join, then the following notational convention will be in effect:

$$[\![\langle u^{(i)}, v^{(i)} \rangle : i \in I]\!]^{\mathrm{e}} \quad \text{stands for} \quad \sum_{i \in I} [\![u^{(i)}, v^{(i)}]\!]^{\mathrm{e}}. \tag{2.7}$$

For an integer $k \geq 2$ and the $(2k+1)$-element set

$$Z = Z(2k+1) := \{a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_{k-1}\},$$

we define

$$
\begin{aligned}
\alpha &:= [\![a_0, a_1, \ldots a_k]\!]^{\mathrm{e}} + [\![b_0, b_1, \ldots b_{k-1}]\!]^{\mathrm{e}} = [\![a_x, a_{x+1}]\!]^{\mathrm{e}}_{\forall} + [\![b_y, b_{y+1}]\!]^{\mathrm{e}}_{\forall} \\
\beta &:= [\![a_x, b_x]\!]^{\mathrm{e}}_{\forall} = [\![\langle a_i, b_i \rangle : 0 \leq i \leq k-1]\!]^{\mathrm{e}}, \\
\gamma &:= [\![a_{x+1}, b_x]\!]^{\mathrm{e}}_{\forall} = [\![\langle a_{i+1}, b_i \rangle : 0 \leq i \leq k-1]\!]^{\mathrm{e}}, \\
\delta &:= [\![a_0, b_0]\!]^{\mathrm{e}} + [\![a_k, b_{k-1}]\!]^{\mathrm{e}};
\end{aligned}
\tag{2.8}
$$

see Figure 2. Then the system $\langle Z(2k+1); \alpha, \beta, \gamma, \delta \rangle$ is called a $(2k+1)$-element *Zádori configuration*. Its importance is revealed by the following lemma.

Lemma 2.1 (Zádori [19]). *For $k \geq 2$, $[\alpha, \beta, \gamma, \delta]_{\mathrm{lat}} = \mathrm{Equ}(Z(2k+1))$, that is, the four partitions in (2.8) of the Zádori configuration generate the lattice of all equivalences of $Z(2k+1)$. Consequently,*

$$[\alpha, \beta, \gamma, [\![a_0, b_0]\!]^{\mathrm{e}}, [\![a_k, b_{k-1}]\!]^{\mathrm{e}}]_{\mathrm{lat}} = \mathrm{Equ}(Z(2k+1)). \tag{2.9}$$
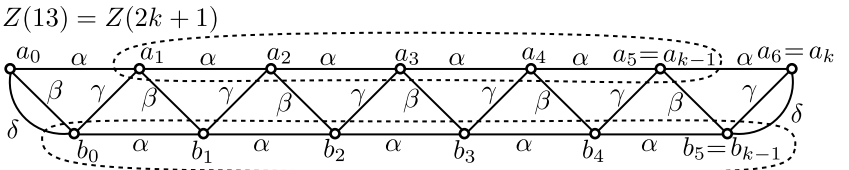

Figure 2. The Zádori configuration of odd size $2k+1$ with $k = 6$

We shall soon outline the proof of this lemma since we are going to use its details in the paper. But firstly, we formulate another lemma from Zádori [19], which has also been used in Czédli [4, 5, 6] and in other papers like Kulin [12]. We are going to recall its proof only for later reference.

Lemma 2.2 ("Circle Principle"). *If $d_0, d_1, \ldots, d_{n-1}$ are pairwise distinct elements of a set A and $0 \le u < v \le n-1$, then*

$$\llbracket d_u, d_v \rrbracket^{\mathrm{e}} = \big(\llbracket d_u, d_{u+1} \rrbracket^{\mathrm{e}} + \llbracket d_{u+1}, d_{u+2} \rrbracket^{\mathrm{e}} + \cdots + \llbracket d_{v-1}, d_v \rrbracket^{\mathrm{e}} \big) \cdot \big(\llbracket d_v, d_{v+1} \rrbracket^{\mathrm{e}} \\
+ \cdots + \llbracket d_{n-2}, d_{n-1} \rrbracket^{\mathrm{e}} + \llbracket d_{n-1}, d_0 \rrbracket^{\mathrm{e}} + \llbracket d_0, d_1 \rrbracket^{\mathrm{e}} + \cdots + \llbracket d_{u-1}, d_u \rrbracket^{\mathrm{e}} \big) \tag{2.10}$$

holds in $\mathrm{Equ}(A)$. *If, in addition, $A = \{d_0, d_1, \ldots, d_{n-1}\}$, then* $\mathrm{Equ}(A)$ *is generated by*

$$\{ \llbracket d_{n-1}, d_0 \rrbracket^{\mathrm{e}} \} \cup \bigcup_{0 \le i \le n-2} \{ \llbracket d_i, d_i + 1 \rrbracket^{\mathrm{e}} \}.$$

PROOF OF LEMMA 2.2. (2.10) is trivial. The second half of the lemma follows from the fact that for a finite A, the lattice $\mathrm{Equ}(A)$ is *atomistic*, that is, each of its elements is the join of some atoms.   □

PROOF OF LEMMA 2.1. On the set $\{\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta}\}$ of variables, we are going to define several quaternary terms recursively. But first of all, we define the quadruple

$$\overline{\boldsymbol{\mu}} := \langle \overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta} \rangle \tag{2.11}$$

of four variables in order to abbreviate our quaternary terms $t(\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta})$ by $t(\overline{\boldsymbol{\mu}})$. We let

$$\left. \begin{aligned}
g_0(\overline{\boldsymbol{\mu}}) &:= \overline{\beta}\,\overline{\delta} \ (\text{i.e.,} = \overline{\beta} \wedge \overline{\delta}), \\
h_{i+1}(\overline{\boldsymbol{\mu}}) &:= ((g_i(\overline{\boldsymbol{\mu}}) + \overline{\gamma})\overline{\alpha} + g_i(\overline{\boldsymbol{\mu}}))\overline{\gamma} \text{ for } i \ge 0, \\
g_{i+1}(\overline{\boldsymbol{\mu}}) &:= ((h_{i+1}(\overline{\boldsymbol{\mu}}) + \overline{\beta})\overline{\alpha} + h_{i+1}(\overline{\boldsymbol{\mu}}))\overline{\beta} \text{ for } i \ge 0, \\
H_0(\overline{\boldsymbol{\mu}}) &:= \overline{\gamma}\,\overline{\delta}, \\
G_{i+1}(\overline{\boldsymbol{\mu}}) &:= ((H_i(\overline{\boldsymbol{\mu}}) + \overline{\beta})\overline{\alpha} + H_i(\overline{\boldsymbol{\mu}}))\overline{\beta} \text{ for } i \ge 0, \\
H_{i+1}(\overline{\boldsymbol{\mu}}) &:= ((G_{i+1}(\overline{\boldsymbol{\mu}}) + \overline{\gamma})\overline{\alpha} + G_{i+1}(\overline{\boldsymbol{\mu}}))\overline{\gamma} \text{ for } i \ge 0.
\end{aligned} \right\} \tag{2.12}$$

For later reference, let us point out that

$$\left. \begin{aligned}
&\text{in (2.12), } \delta \text{ is used only twice: to} \\
&\text{define } g_0(\overline{\boldsymbol{\mu}}) \text{ and to define } H_0(\overline{\boldsymbol{\mu}}).
\end{aligned} \right\} \tag{2.13}$$

Next, in harmony with (2.8) and Figure 2, we let

$$\boldsymbol{\mu} := \langle \alpha, \beta, \gamma, \delta \rangle. \tag{2.14}$$

Clearly,

$$\beta\delta = \llbracket a_0, b_0 \rrbracket^{\mathrm{e}} \ \text{ and } \ \gamma\delta = \llbracket a_k, b_{k-1} \rrbracket^{\mathrm{e}}. \tag{2.15}$$

An easy induction shows that

$$
\left.\begin{aligned}
g_i(\boldsymbol{\mu}) &:= [\![\langle a_j, b_j\rangle : 0 \le j \le i]\!]^{\mathrm{e}} \text{ for } 0 \le i \le k-1, \\
h_i(\boldsymbol{\mu}) &:= [\![\langle a_j, b_{j-1}\rangle : 1 \le j \le i]\!]^{\mathrm{e}} \text{ for } 1 \le i \le k, \\
H_i(\boldsymbol{\mu}) &:= [\![\langle a_{k-j}, b_{k-1-j}\rangle : 0 \le j \le i]\!]^{\mathrm{e}} \text{ for } 0 \le i \le k-1, \\
G_i(\boldsymbol{\mu}) &:= [\![\langle a_{k-j}, b_{k-j}\rangle : 1 \le j \le i]\!]^{\mathrm{e}} \text{ for } 1 \le i \le k.
\end{aligned}\right\} \tag{2.16}
$$

Next, for certain edges $\langle u, v\rangle$ of the graph given in Figure 2, we define a corresponding lattice term $e_{u,v}(\overline{\boldsymbol{\mu}})$ as follows.

$$
\left.\begin{aligned}
e_{a_i,b_i}(\overline{\boldsymbol{\mu}}) &:= g_i(\overline{\boldsymbol{\mu}}) \cdot G_{k-i}(\overline{\boldsymbol{\mu}}), \quad \text{for } 0 \le i \le k-1, \\
e_{a_i,b_{i-1}}(\overline{\boldsymbol{\mu}}) &:= h_i(\overline{\boldsymbol{\mu}}) \cdot H_{k-i}(\overline{\boldsymbol{\mu}}), \quad \text{for } 1 \le i \le k \\
e_{a_i,a_{i+1}}(\overline{\boldsymbol{\mu}}) &:= \overline{\alpha} \cdot (e_{a_i,b_i}(\overline{\boldsymbol{\mu}}) + e_{a_{i+1},b_i}(\overline{\boldsymbol{\mu}})), \quad \text{for } 0 \le i \le k-1, \\
e_{b_i,b_{i+1}}(\overline{\boldsymbol{\mu}}) &:= \overline{\alpha} \cdot (e_{a_{i+1},b_i}(\overline{\boldsymbol{\mu}}) + e_{a_{i+1},b_{i+1}}(\overline{\boldsymbol{\mu}})), \quad 0 \le i \le k-2.
\end{aligned}\right\} \tag{2.17}
$$

The first two equalities below follow from (2.16), while the third and the fourth follow from the first two.

$$
\left.\begin{aligned}
e_{a_i,b_i}(\boldsymbol{\mu}) &= [\![a_i, b_i]\!]^{\mathrm{e}}, \quad \text{for } 0 \le i \le k-1, \\
e_{a_i,b_{i-1}}(\boldsymbol{\mu}) &= [\![a_i, b_{i-1}]\!]^{\mathrm{e}} \quad \text{for } 1 \le i \le k \\
e_{a_i,a_{i+1}}(\boldsymbol{\mu}) &= [\![a_i, a_{i+1}]\!]^{\mathrm{e}} \quad \text{for } 0 \le i \le k-1, \\
e_{b_i,b_{i+1}}(\boldsymbol{\mu}) &= [\![b_i, b_{i+1}]\!]^{\mathrm{e}}, \quad 0 \le i \le k-2.
\end{aligned}\right\} \tag{2.18}
$$

Finally, let

$$
\langle d_0, d_1, \ldots, d_{n-1}\rangle := \langle a_0, a_1, \ldots, a_k, b_{k-1}, b_{k-2}, \ldots, b_0\rangle. \tag{2.19}
$$

In harmony with (2.10), we define the following term

$$
\left.\begin{aligned}
e_{d_u,d_v}(\overline{\boldsymbol{\mu}}) :={}& \big(e_{d_u,d_{u+1}}(\overline{\boldsymbol{\mu}}) + e_{d_{u+1},d_{u+2}}(\overline{\boldsymbol{\mu}}) + \cdots + e_{d_{v-1},d_v}(\overline{\boldsymbol{\mu}})\big) \\
&\cdot \big(e_{d_v,d_{v+1}}(\overline{\boldsymbol{\mu}}) + \cdots + e_{d_{n-2},d_{n-1}}(\overline{\boldsymbol{\mu}}) + e_{d_{n-1},d_0}(\overline{\boldsymbol{\mu}}) \\
&\quad + e_{d_0,d_1}(\overline{\boldsymbol{\mu}}) + \cdots + e_{d_{u-1},d_u}(\overline{\boldsymbol{\mu}})\big)
\end{aligned}\right\} \tag{2.20}
$$

for $0 \le u < v \le n-1 = 2k$. Combining (2.10), (2.18), and (2.20), we obtain that

$$
e_{d_u,d_v}(\boldsymbol{\mu}) = [\![d_u, d_v]\!]^{\mathrm{e}}. \tag{2.21}
$$

Based on (2.13), note at this point that in (2.12), (2.17), and (2.20), δ is used only twice: to define $g_0(\overline{\boldsymbol{\mu}})$ and to define $H_0(\overline{\boldsymbol{\mu}})$. Consequently, taking (2.15) also into account, we conclude that

$$\left.\begin{array}{l}\text{equality (2.21) remains valid if } \delta, \text{ the fourth component of}\\ \boldsymbol{\mu}, \text{ is replaced by any other partition whose meet with } \beta\\ \text{and that with } \gamma \text{ are } [\![a_0, b_0]\!]^e \text{ and } [\![a_k, b_{k-1}]\!]^e, \text{ respectively.}\end{array}\right\} \quad (2.22)$$

Since every atom of $\mathrm{Equ}(Z(2k + 1))$ is of the form (2.21) and $\mathrm{Equ}(Z(2k + 1))$ is an atomistic lattice, $[\alpha, \beta, \gamma, \delta]_{\mathrm{lat}} = \mathrm{Equ}(Z(n))$. In virtue of (2.22) and since $\overline{\delta}$ has been used only twice, (2.9) also holds, completing the proof of Lemma 2.1. $\quad\square$
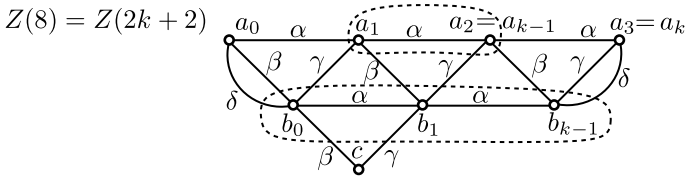

Figure 3. A configuration for even size $2k + 2$ with $k = 3$

Next, for $k \geq 2$, we add a new vertex c, a β-colored edge $\langle b_0, c \rangle$, and a γ-colored edge $\langle b_2, c \rangle$ to $Z(2k + 1)$ to obtain $Z(2k + 2)$, see Figure 3. This configuration is different from what Zádori [19] used for the even case; our approach by Figure 3 is simpler and fits better to our purposes. Again, the dashed curved edges of Figure 3 should be disregarded until otherwise is stated.

Lemma 2.3. *For $n = 2k + 2 \geq 6$, we have that $\mathrm{Equ}(Z(n)) = [\alpha, \beta, \gamma, \delta]_{\mathrm{lat}}$.*

PROOF. With the short terms $\overline{\alpha}^* = \overline{\alpha}$, $\overline{\beta}^* := \overline{\beta}(\overline{\alpha} + \overline{\delta})$, $\overline{\gamma}^* := \overline{\gamma}(\overline{\alpha} + \overline{\delta})$, and $\overline{\delta}^* := \overline{\delta}$, we define $\overline{\boldsymbol{\mu}}^* := \langle \overline{\alpha}^*, \overline{\beta}^*, \overline{\gamma}^*, \overline{\delta}^* \rangle$. For each term t defined in (2.12) and (2.17), we define a term t^* as $t^*(\overline{\boldsymbol{\mu}}) := t(\overline{\boldsymbol{\mu}}^*)$. We also need the corresponding partitions $\alpha^* := \alpha$, $\beta^* := \beta(\alpha + \delta)$, $\gamma^* := \gamma(\alpha + \delta)$, $\delta^* := \delta$, and the quadruple $\boldsymbol{\mu}^* := \langle \alpha^*, \beta^*, \gamma^*, \delta^* \rangle$. Apart from the singleton block $\{c\}$, they are the same as the partitions considered in Lemma 2.1 for $Z(2k + 1)$. Hence, it follows that (2.16), (2.18), and (2.21) hold with $\boldsymbol{\mu}^*$ instead of $\boldsymbol{\mu}$. In other words, they hold with $\boldsymbol{\mu}$ if the terms t are replaced by the corresponding terms t^*. In particular, (2.21) is reworded as follows:

$$e_{x,y}^*(\boldsymbol{\mu}) = [\![x, y]\!]^e \quad \text{for all } x, y \in Z(n) \setminus \{c\}. \quad (2.23)$$

So if we define (without defining their "asterisk-free versions" $e_{a_0,c}$ and $e_{a_2,c}$) the terms

$$e^*_{a_0,c}(\boldsymbol{\mu}) := \overline{\beta} \cdot \left(\overline{\gamma} + e_{a_0,a_2}(\boldsymbol{\overline{\mu}^*})\right) \text{ and } e^*_{a_2,c}(\boldsymbol{\mu}) := \overline{\gamma} \cdot \left(\overline{\beta} + e_{a_0,a_2}(\boldsymbol{\overline{\mu}^*})\right), \qquad (2.24)$$

then it follows easily that

$$e^*_{a_0,c}(\boldsymbol{\mu}) = [\![a_0, c]\!]^{\mathrm{e}} \text{ and } e^*_{a_2,c}(\boldsymbol{\mu}) = [\![a_2, c]\!]^{\mathrm{e}}; \qquad (2.25)$$

remark that in addition to (2.23), (2.25) also belongs to the scope of (2.22). Let

$$\langle d_0, d_1, \ldots, d_{n-1} \rangle := \langle a_0, c, a_2, a_3, \ldots, a_k, b_{k-1}, b_{k-2}, \ldots, b_1, a_1, b_0 \rangle. \qquad (2.26)$$

Similarly to (2.20) but now based on (2.26) rather than (2.19), we define the following term (without defining its "non-asterisked" f_{d_u,d_v} version)

$$\left. \begin{aligned} f^*_{d_u,d_v}(\boldsymbol{\overline{\mu}}) := & \left(e^*_{d_u,d_{u+1}}(\boldsymbol{\overline{\mu}}) + e^*_{d_{u+1},d_{u+2}}(\boldsymbol{\overline{\mu}}) \cdots + e^*_{d_{v-1},d_v}(\boldsymbol{\overline{\mu}})\right) \\ & \cdot \left(e^*_{d_v,d_{v+1}}(\boldsymbol{\overline{\mu}}) + \cdots + e^*_{d_{n-2},d_{n-1}}(\boldsymbol{\overline{\mu}}) + e^*_{d_{n-1},d_0}(\boldsymbol{\overline{\mu}})\right. \\ & \left. + e^*_{d_0,d_1}(\boldsymbol{\overline{\mu}}) + \cdots + e^*_{d_{u-1},d_u}(\boldsymbol{\overline{\mu}})\right) \end{aligned} \right\} \qquad (2.27)$$

for $0 \le u < v < n$. By Lemma 2.2, (2.23), (2.25), and (2.27), we obtain that

$$f^*_{x,y}(\boldsymbol{\mu}) = [\![x, y]\!]^{\mathrm{e}} \quad \text{for all } x \ne y \in Z(n). \qquad (2.28)$$

The remark right after (2.25) allows us to note that

$$(2.28) \text{ also belongs to the scope of } (2.22). \qquad (2.29)$$

Finally, (2.28) implies Lemma 2.3 since $\mathrm{Equ}(Z(n))$ is atomistic. □

3. Generating direct powers of partition lattices

Before formulating the main result of the paper, we recall some notations and concepts. The lower integer part of a real number x will be denoted by $\lfloor x \rfloor$; for example, $\lfloor \sqrt{2} \rfloor = 1$ and $\lfloor 2 \rfloor = 2$. The set of positive integer numbers will be denoted by $\mathbb{N}^+$. For $n \in \mathbb{N}^+$, the number of partitions of the n-element set $\{1, 2, \ldots, n\}$, that is, the size of $\mathrm{Part}(n) \cong \mathrm{Equ}(n)$ is the so-called n-th *Bell number*; it will be denoted by $\mathrm{Bell}(n)$. The number of partitions of n objects with exactly r blocks is denoted by $S(n, r)$; it is the *Stirling number of the second*

kind with parameters n and r. Note that $S(n,r) \geq 1$ if and only if $1 \leq r \leq n$; otherwise $S(n,r)$ is zero. Clearly, $\mathrm{Bell}(n) = S(n,1) + S(n,2) + \cdots + S(n,n)$. Let

$$\mathrm{Max}S(n) \text{ denote the maximal element of the set } \{S(n,r) : r \in \mathbb{N}^+\}. \qquad (3.1)$$

We know from Rennie and Dobson [15, page 121] that

$$\log \mathrm{Max}S(n) = n \log n - n \log\log n - n + O\left(n \cdot \frac{\log\log n}{\log n}\right). \qquad (3.2)$$

Hence, $\mathrm{Max}S(n)$ is quite large; see Tables (3.3)–(3.5) and (3.9) for some of its values; note that those given in exponential form are only rounded values. Some rows occurring in these tables, computed by Maple V. Release 5 (1997) under Windows 10, will be explained later.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{Max}S(n)$	1	1	3	7	25	90	350	1 701	7 770	42 525	246 730	1 379 400
$m(n)$				1	1	3	3	21	21	175	175
$m_*(n)$							1	1	1	1	2	2

(3.3)

n	13	14	15	16	17
$\mathrm{Max}S(n)$	9 321 312	63 436 373	420 693 273	3 281 882 604	25 708 104 786
$m(n)$	2 250	2 250	31 500	31 500	595 350
$m_*(n)$	2	2	9	9	9

(3.4)

n	18	19	20
$\mathrm{Max}S(n)$	1 974 624 834 000	1 709 751 003 480	15 170 932 662 679
$m(n)$	595 350	13 216 770	13 216 770
$m_*(n)$	9	49	49

(3.5)

n	21	22	23	24	25
$m(n)$	330 419 250	330 419 250	10 492 193 250	10 492 193 250	$3.40 \cdot 10^{11}$
$m_*(n)$	49	49	625	625	625

(3.6)

n	26	27	28	29	30	31
$m(n)$	$3.40 \cdot 10^{11}$	$1.29 \cdot 10^{13}$	$1.29 \cdot 10^{13}$	$5.91 \cdot 10^{14}$	$5.91 \cdot 10^{14}$	$2.67 \cdot 10^{16}$
$m_*(n)$	625	8100	8100	8100	8100	122500

(3.7)

n	32	33	34	35	36	37
$m(n)$	$2.67 \cdot 10^{16}$	$1.38 \cdot 10^{18}$	$1.38 \cdot 10^{18}$	$8.44 \cdot 10^{19}$	$8.44 \cdot 10^{19}$	$5.08 \cdot 10^{21}$
$m_*(n)$	122500	122500	122500	2893401	2893401	2893401

(3.8)

n	97	98	99	100	2020
$\mathrm{Max}S(n)$	$3.22 \cdot 10^{110}$	$9.31 \cdot 10^{111}$	$2.69 \cdot 10^{113}$	$7.77 \cdot 10^{114}$	$3.81 \cdot 10^{4398}$
$m(n)$	$1.08 \cdot 10^{87}$	$1.08 \cdot 10^{87}$	$3.09 \cdot 10^{89}$	$3.09 \cdot 10^{89}$	$5.52 \cdot 10^{3893}$
$m_*(n)$	$1.52 \cdot 10^{32}$	$1.52 \cdot 10^{32}$	$1.45 \cdot 10^{34}$	$1.45 \cdot 10^{34}$	$3.97 \cdot 10^{1700}$

$$(3.9)$$

The aim of this section is to prove the following theorem; (2.3) and (3.1) are still in effect.

Theorem 3.1. *Let $n \geq 5$ be an integer, let $k := \lfloor (n-1)/2 \rfloor$, and let*

$$m = m(n) := \mathrm{Max}S(k) \cdot \mathrm{Max}S(k-1). \qquad (3.10)$$

Then $\mathrm{Part}(n)^m$ *or, equivalently,* $\mathrm{Equ}(n)^m$ *is four-generated. In other words, the m-th direct power of the lattice of all partitions of the set $\{1, 2, \ldots, n\}$ is generated by a four-element subset.*

Some values of $m(n)$ are given in Tables (3.3)–(3.9). Before proving this theorem, we formulate some remarks and corollaries and we make some comments.

Corollary 3.2. *Let n and m as in Theorem 3.1. Then for every integer t with $1 \leq t \leq m$, the direct power $\mathrm{Part}(n)^t$ is four-generated. In particular, $\mathrm{Part}(n)$ in itself is four-generated.*

The second half of Corollary 3.2 shows that Theorem 3.1 is a stronger statement than the Strietz–Zádori result; see (1.1) in the Introduction. This corollary follows quite easily from Theorem 3.1 as follows.

PROOF OF COROLLARY 3.2. Since the natural projection from $\mathrm{Part}(n)^m$ to $\mathrm{Part}(n)^t$, defined by $\langle x_1, \ldots, x_m \rangle \mapsto \langle x_1, \ldots, x_t \rangle$, sends a 4-element generating set into an at most 4-element generating set, Theorem 3.1 applies. $\qquad \square$

Remark 3.3. We cannot say that $m = m(n)$ in Theorem 3.1 is the largest possible exponent. First, because the proof that we are going to present relies on a particular construction and we do not know whether there exist better constructions for this purpose. Second, because we use Stirling numbers of the second kind to give a lower estimate of the size of a maximum-sized antichain in partition lattices, and we know from Canfield [2] that this estimate is not sharp. However, this fact would not lead to a reasonably esthetic improvement of Theorem 3.1.

Remark 3.4. If n and t are positive integers such that $n \geq 4$ and

$$t > \mathrm{Bell}(n) \cdot \mathrm{Bell}(n-1) \cdot \mathrm{Bell}(n-2) \cdot \mathrm{Bell}(n-3), \qquad (3.11)$$

then $\mathrm{Part}(n)^t$ is not four-generated. Thus, the exponent in Theorem 3.1 cannot be arbitrarily large.

The product occurring in (3.11) is much larger than $m(n)$ in (3.10). Hence, there is a wide interval of integers t such that we do not know whether $\mathrm{Part}(n)^t$ is four-generated or not.

PROOF OF REMARK 3.4. Let p denote the product in (3.11). For the sake of contradiction, suppose that $t > p$ but $\mathrm{Part}(n)^t$ is generated by some $\{\alpha, \beta, \gamma, \delta\}$. Here $\alpha = \langle \alpha_1, \alpha_2, \ldots, \alpha_t \rangle$ with all the $\alpha_i \in \mathrm{Part}(n)$, and similarly for β, γ, and δ. By the easy argument proving Corollary 3.2, we know that $\{\alpha_i, \beta_i, \gamma_i, \delta_i\}$ generates $\mathrm{Part}(n)$ for all $i \in \{1, \ldots, t\}$. Since $\mathrm{Part}(n)$ is not 3-generated by Zádori [19], the quadruple $\langle \alpha_i, \beta_i, \gamma_i, \delta_i \rangle$ consists of pairwise distinct components. But there are only p such quadruples, whereby the the pigeonhole principle yields two distinct subscripts i and $j \in \{1, \ldots, t\}$ such that $\langle \alpha_i, \beta_i, \gamma_i, \delta_i \rangle = \langle \alpha_j, \beta_j, \gamma_j, \delta_j \rangle$. Hence, for every quaternary lattice term f, we have that $f(\alpha_i, \beta_i, \gamma_i, \delta_i) = f(\alpha_j, \beta_j, \gamma_j, \delta_j)$. This implies that for every $\eta = \langle \eta_1, \ldots, \eta_t \rangle \in [\alpha, \beta, \gamma, \delta]_{\mathrm{lat}}$, we have that $\eta_i = \eta_j$. Thus, $[\alpha, \beta, \gamma, \delta]_{\mathrm{lat}} \neq \mathrm{Part}(n)^t$, which is a contradiction proving Remark 3.4.   □

Remark 3.5. For a four-generated finite lattice L, the direct square L^2 of L need not be four-generated. For example, if L is the distributive lattice generated freely by four elements, then there exists no $t \geq 2$ such that L^t is four-generated.

PROOF. Let $t \geq 2$, and let L be the free distributive lattice on four generators. Observe that L^t is distributive. So if L^t was four-generated, then it would be a homomorphic image of L and $|L|^t = |L^t| \leq |L|$ would be a contradiction.   □

PROOF OF THEOREM 3.1. Since the notation of the elements of the base set is irrelevant, it suffices to show that $\mathrm{Equ}(Z(n))^m$ is four-generated. No matter if n is odd or even, we use the notation k, a_i and b_j as in Figures 2 and 3. We are going to define $\vec{\alpha} = \langle \alpha_1, \ldots, \alpha_m \rangle$, $\vec{\beta} = \langle \beta_1, \ldots, \beta_m \rangle$, $\vec{\gamma} = \langle \gamma_1, \ldots, \gamma_m \rangle$, and $\vec{\delta}^\sharp = \langle \delta^\sharp_1, \ldots, \delta^\sharp_m \rangle$ so that $\{\vec{\alpha}, \vec{\beta}, \vec{\gamma}, \vec{\delta}^\sharp\}$ generates $\mathrm{Equ}(Z(n))^m$. For every $i \in \{1, \ldots, m\}$, α_i, β_i, and γ_i are defined as in Figures 2 and 3, that is, as in the proofs of Lemmas 2.1 and 2.3. However, the definition of the equivalences $\delta^\sharp_i$ is going to be more tricky. Let $\delta_i := [\![a_0, b_0]\!]^{\mathrm{e}} + [\![a_k, b_{k-1}]\!]^{\mathrm{e}}$, as in Lemmas 2.1 and 2.3. Note that

$$\text{none of } \alpha_i := \alpha, \ \beta_i := \beta, \ \gamma_i := \gamma, \text{ and } \delta_i := \delta \text{ depends on } i. \qquad (3.12)$$

We know from Lemmas 2.1 and 2.3 that $\{\alpha_i, \beta_i, \gamma_i, \delta_i\}$ generates $\mathrm{Equ}(Z(n))$. Therefore, for any two distinct elements u and v of $Z(n)$, we can pick a quaternary lattice term $f_{u,v} = f_{u,v}(\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta})$ with variables $\overline{\mu} := \langle \overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta} \rangle$ such

that, in virtue of (2.21) and (2.28),

$$\left. \begin{array}{l} \text{depending on the parity of } n,\ f_{u,v} \text{ is } e_{u,v} \text{ from the proof} \\ \text{of Lemma 2.1 or it is } f_{u,v}^{*} \text{ from that of Lemma 2.3, and} \\ f_{u,v}(\alpha_i, \beta_i, \gamma_i, \delta_i) = [\![u, v]\!]^{\text{e}} \in \text{Equ}(Z(n)). \end{array} \right\} \qquad (3.13)$$

By defining $f_{u,u}$ to be the meet of its four variables, the validity of (3.13) extends to the case $u = v$, where $[\![u, u]\!]^{\text{e}}$ is understood as the least partition, that is, the partition with all of its blocks being singletons.

Next, let

$$U := \{a_1, a_2 \ldots, a_{k-1}\} \text{ and } W := \{b_0, b_1, \ldots, b_{k-1}\}; \qquad (3.14)$$

these sets are indicated by dashed ovals in Figures 2, 3, and 4. By the definition of $\text{Max}S(k-1)$, we can pick an integer $r' \in \mathbb{N}^+$ such that there are exactly $\text{Max}S(k-1)$ equivalences of U with exactly r' blocks. (By a block of an equivalence we mean a block of the corresponding partition.) Let $\mathcal{G}$ denote the set of these "r'-block equivalences" of U. Clearly, $\mathcal{G}$ is an antichain in $\text{Equ}(U)$ with size $|\mathcal{G}| = \text{Max}S(k-1)$. Similarly, $\text{Max}S(k)$ is the number of r''-block equivalences for some $r'' \in \mathbb{N}^+$ and the r''-block equivalences of W form an antichain $\mathcal{H} \subseteq \text{Equ}(W)$ such that $|\mathcal{H}| = \text{Max}S(k)$. Observe that, in the direct product $\text{Equ}(U) \times \text{Equ}(W)$,

$$\mathcal{G} \times \mathcal{H} \text{ is an antichain.} \qquad (3.15)$$

Since $|\mathcal{G} \times \mathcal{H}| = |\mathcal{G}| \cdot |\mathcal{H}| = \text{Max}S(k-1) \cdot \text{Max}S(k) = m$, see (3.10), we can enumerate $\mathcal{G} \times \mathcal{H}$ in the following repetition-free list of length m as follows:

$$\mathcal{G} \times \mathcal{H} = \{\langle \kappa_1, \lambda_1 \rangle, \langle \kappa_2, \lambda_2 \rangle, \ldots, \langle \kappa_m, \lambda_m \rangle\}. \qquad (3.16)$$

For each $i \in \{1, \ldots, m\}$, we define $\delta^{\sharp}{}_i$ as follows:

$$\delta^{\sharp}{}_i := \text{the equivalence generated by } \delta_i \cup \kappa_i \cup \lambda_i; \qquad (3.17)$$

this makes sense since each of δ_i, κ_i and λ_i is a subset of $Z(n) \times Z(n)$. Clearly, for any $x \neq y \in Z(n)$, $\langle x, y \rangle \in \alpha\delta^{\sharp}{}_i$ if and only $\langle x, y \rangle \in \kappa_i \cup \lambda_i \subseteq U^2 \cup W^2$. This fact together with $\kappa_i \cap \lambda_i \subseteq U^2 \cap W^2 = \emptyset$ and (3.15) yields that for any $i, j \in \{1, 2, \ldots, m\}$,

$$\text{if } i \neq j, \text{ then } \alpha\delta^{\sharp}{}_i \text{ and } \alpha\delta^{\sharp}{}_j \text{ are incomparable.} \qquad (3.18)$$

Next, we define

$$\text{the "zigzagged circle" } \langle d_0, d_1, \ldots, d_{n-1} \rangle \qquad (3.19)$$
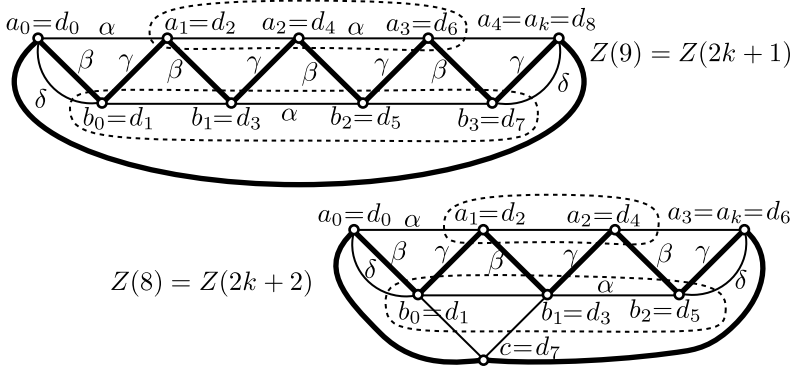
Figure 4. "zigzagged circles"

as follows; see also the thick edges and curves in Figure 4. (Note that the earlier meaning of the notation $d_0, d_1, \ldots$ is no longer valid.) For $i \in \{0, \ldots, k-1\}$, we let $d_{2i} := a_i$ and $d_{2i+1} := b_i$. We let $d_{2k} = a_k$ and, if $n = 2k+2$ is even, then we let $d_{n-1} = c$. Two consecutive vertices of the zigzagged circle will always be denoted by d_p and d_{p+1} where $p, p+1 \in \{0, 1, \ldots, n-1\}$ and the addition is understood modulo n. The zigzagged circle has one or two *thick curved edges*; they are $\langle a_0, a_k \rangle$ for $n = 2k+1$ odd and they are $\langle a_0, c \rangle$ and $\langle c, a_k \rangle$ for $n = 2k+2$ even; the rest of its edges are *straight thick edges*. So the zigzagged circle consists of the thick (straight and curved) edges, whereby the adjective "thick" will often be dropped.

Next, we define some lattice terms associated with the edges of the zigzagged circle. Namely, for $j \in \{1, \ldots, m\}$ and for $p \in \{0, 1, \ldots, 2k-1\}$, we define the quaternary term

$$
\begin{aligned}
g^{(j)}_{d_p,d_{p+1}}(\overline{\boldsymbol{\mu}}) := f_{d_p,d_{p+1}}(\overline{\boldsymbol{\mu}}) \cdot \prod_{\langle d_p,x \rangle \in \alpha\delta^{\sharp}_j} \left(\overline{\alpha}\overline{\delta} + f_{x,d_{p+1}}(\overline{\boldsymbol{\mu}}) \right) \\
\cdot \prod_{\langle y,d_{p+1} \rangle \in \alpha\delta^{\sharp}_j} \left(f_{d_p,y}(\overline{\boldsymbol{\mu}}) + \overline{\alpha}\overline{\delta} \right).
\end{aligned}
\tag{3.20}
$$

The assumption on p means that (3.20) defines $g^{(j)}_{d_p,d_{p+1}}(\overline{\boldsymbol{\mu}})$ for each straight edge of the zigzagged circle. We claim that for all $j \in \{1, \ldots, m\}$ and $p \in \{0, 1, \ldots, 2k-1\}$,

$$
g^{(j)}_{d_p,d_{p+1}}(\alpha_j, \beta_j, \gamma_j, \delta^{\sharp}_j) = [\![d_p, d_{p+1}]\!]^{\mathrm{e}}.
\tag{3.21}
$$

In order to show (3.21), observe that $\beta_i \delta^{\sharp}_i = \beta_i \delta_i = [\![a_0, b_0]\!]^{\mathrm{e}}$ and $\gamma_i \delta^{\sharp}_i = \gamma_i \delta_i = [\![a_k, b_{k-1}]\!]^{\mathrm{e}}$. These equalities, (2.22), (2.29), and (3.13) yield that for any $u, v \in$

$Z(n)$, $i \in \{1, \ldots, m\}$, and $p \in \{0, 1, \ldots, 2k-1\}$,

$$f_{u,v}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i) = [\![u, v]\!]^e \text{ and, in particular,} \tag{3.22}$$

$$f_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i) = [\![d_p, d_{p+1}]\!]^e. \tag{3.23}$$

Combining (3.20) and (3.23), we obtain the "$\leq$" part of (3.21). In order to turn this inequality to an equality, we have to show that the pair $\langle d_p, d_{p+1} \rangle$ belongs to $\alpha\delta^\sharp_j + f_{x, d_{p+1}}(\alpha_j, \beta_j, \gamma_j, \delta^\sharp_j)$ for every $\langle d_p, x \rangle \in \alpha\delta^\sharp_j$, and it also belongs to $f_{d_p, y}(\alpha_j, \beta_j, \gamma_j, \delta^\sharp_j) + \alpha\delta^\sharp_j$ for every $\langle y, d_{p+1} \rangle \in \alpha\delta^\sharp_j$. But this is trivial since $\langle x, d_{p+1} \rangle \in f_{x, d_{p+1}}(\alpha_j, \beta_j, \gamma_j, \delta^\sharp_j)$ in the first case by (3.22), and similarly trivial in the second case. We have shown (3.21).

Next, we claim that for any $i, j \in \{1, \ldots, m\}$,

$$\left. \begin{array}{l} \text{if } i \neq j, \text{ then there exists a } p \in \{0, 1, \ldots, 2k-1\} \\ \text{such that } g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i) = \Delta := 0_{\mathrm{Equ}(Z(n))}. \end{array} \right\} \tag{3.24}$$

In order to prove (3.24), assume that $i \neq j$. For an equivalence $\varepsilon \in \mathrm{Equ}(Z(n))$ and $x \in Z(n)$, the ε-*block* $\{y \in Z(n) : \langle x, y \rangle \in \varepsilon\}$ of x will be denoted by x/ε. We know from (3.18) that $\alpha\delta^\sharp_j \not\leq \alpha\delta^\sharp_i$. Hence, there is an element $x \in Z(n)$ such that $x/(\alpha\delta^\sharp_j) \not\subseteq x/(\alpha\delta^\sharp_i)$. Since $c/(\alpha\delta^\sharp_j) = \{c\} = c/(\alpha\delta^\sharp_i)$ for n even, x is distinct from c. Hence, x is one of the endpoints of a straight edge $\langle d_p, d_{p+1} \rangle$ of the zigzagged circle. This is how we can select a $p \in \{0, 1, \ldots, 2k-1\}$, that is, a straight edge $\langle d_p, d_{p+1} \rangle$ of the zigzagged circle (3.19) such that

$$d_p/(\alpha\delta^\sharp_j) \not\subseteq d_p/(\alpha\delta^\sharp_i) \quad \text{or} \quad d_{p+1}/(\alpha\delta^\sharp_j) \not\subseteq d_{p+1}/(\alpha\delta^\sharp_i). \tag{3.25}$$

Now, we are going to show that this p satisfies the requirement of (3.24). We can assume that the first part of the disjunction given in (3.25) holds, because the treatment for the second half is very similar. Pick an element

$$z \in d_p/(\alpha\delta^\sharp_j) \text{ such that } z \notin d_p/(\alpha\delta^\sharp_i). \tag{3.26}$$

Because of (3.23) and the first meetand in (3.20),

$$g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i) \leq [\![d_p, d_{p+1}]\!]^e. \tag{3.27}$$

We claim that

$$\langle d_p, d_{p+1} \rangle \notin g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i). \tag{3.28}$$

Suppose the contrary. Then, using (3.20) and that $\langle d_p, z \rangle \in \alpha\delta^\sharp_j$ by (3.26), we have that

$$\langle d_p, d_{p+1} \rangle \in \alpha\delta^\sharp_i + f_{z, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp_i) \overset{(3.22)}{=} \alpha\delta^\sharp_i + [\![z, d_{p+1}]\!]^e. \tag{3.29}$$

According to (3.29), there exists a *shortest* sequence $u_0 = d_{p+1}$, u_1, ..., u_{q-1}, $u_q = d_p$ such that for every $\ell \in \{0, 1, \ldots, q-1\}$, either $\langle u_\ell, u_{\ell+1}\rangle \in \alpha\delta^\sharp{}_i$, which is called a *horizontal step*, or $\langle u_\ell, u_{\ell+1}\rangle \in [\![z, d_{p+1}]\!]^e$, which is a *non-horizontal step*. There is at least one non-horizontal steps since d_p and d_{p+1} are in distinct α-blocks. A non-horizontal step means that $\{u_\ell, u_{\ell+1}\} = \{z, d_{p+1}\}$, so $\{z, d_{p+1}\}$ is the only "passageway" between the two nonsingleton α-blocks. Hence, there exists exactly one non-horizontal step since our sequence is repetition-free. This step is the first step since we have taken a shortest sequence. Hence, $u_1 = z$ and all the subsequent steps are horizontal steps. Hence, $\langle z, d_p\rangle = \langle u_1, d_p\rangle \in \alpha\delta^\sharp{}_i$. Thus, $z \in d_p/(\alpha\delta^\sharp{}_i)$, contradicting the choice of z in (3.26). This contradiction yields (3.28). Finally, (3.28) together with (3.27) implies (3.24).

Next, for $j \in \{1, 2, ..., m\}$ and $q \in \{0, 1, \ldots, n-1\}$, we define the following quaternary term

$$
\left.
\begin{aligned}
h^{(j)}_{d_q, d_{q+1}}(\overline{\boldsymbol{\mu}}) := \\
f_{d_q, d_{q+1}}(\overline{\boldsymbol{\mu}}) \cdot \prod_{p=0}^{2k-1} \big(f_{d_q, d_p}(\overline{\boldsymbol{\mu}}) + g^{(j)}_{d_p, d_{p+1}}(\overline{\boldsymbol{\mu}}) + f_{d_{p+1}, d_{q+1}}(\overline{\boldsymbol{\mu}})\big) \\
\cdot \prod_{p=0}^{2k-1} \big(f_{d_q, d_{p+1}}(\overline{\boldsymbol{\mu}}) + g^{(j)}_{d_p, d_{p+1}}(\overline{\boldsymbol{\mu}}) + f_{d_p, d_{q+1}}(\overline{\boldsymbol{\mu}})\big),
\end{aligned}
\right\}
\tag{3.30}
$$

where $q+1$ in subscript position is understood modulo n. We claim that, for $q \in \{0, 1, \ldots, n-1\}$ and $i, j \in \{1, \ldots, m\}$,

$$
h^{(j)}_{d_q, d_{q+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i) =
\begin{cases}
[\![d_q, d_{q+1}]\!]^e, & \text{if } i = j, \\
\Delta = 0_{\mathrm{Equ}(Z(n))}, & \text{if } i \neq j.
\end{cases}
\tag{3.31}
$$

In virtue of (3.21), (3.22), and (3.23), the validity of (3.31) is clear when $i = j$. So, to prove (3.31), we can assume that $i \neq j$. Since $h^{(j)}_{d_q, d_{q+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i) \leq [\![d_q, d_{q+1}]\!]^e$ by (3.22) and (3.23), it suffices to show that $\langle d_q, d_{q+1}\rangle$ does not belong to $h^{(j)}_{d_q, d_{q+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i)$. Suppose the contrary. Then we obtain from (3.22) and (3.30) that for all $p \in \{0, \ldots, 2k-1\}$,

$$
\langle d_q, d_{q+1}\rangle \in [\![d_q, d_p]\!]^e + g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i) + [\![d_{p+1}, d_{q+1}]\!]^e \text{ and}
\tag{3.32}
$$

$$
\langle d_q, d_{q+1}\rangle \in [\![d_q, d_{p+1}]\!]^e + g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i) + [\![d_p, d_{q+1}]\!]^e.
\tag{3.33}
$$

Now we choose p according to (3.24); then $g^{(j)}_{d_p, d_{p+1}}(\alpha_i, \beta_i, \gamma_i, \delta^\sharp{}_i)$ can be omitted from (3.32) and (3.33). Therefore, if $p = q$, then (3.32) asserts that $\langle d_q, d_{q+1}\rangle \in \Delta$,

a contradiction. Note that, due to $n \geq 5$, the equality $p = q$ is equivalent to $|\{d_p, d_{p+1}, d_q, d_{q+1}\}| = 2$, whence $|\{d_p, d_{p+1}, d_q, d_{q+1}\}| = 2$ has just been excluded. If $|\{d_p, d_{p+1}, d_q, d_{q+1}\}| = 4$, then each of (3.32) and (3.33) gives a contradiction again. If $|\{d_p, d_{p+1}, d_q, d_{q+1}\}| = 3$, then exactly one of (3.32) and (3.33) gives a contradiction. Hence, no matter how p and q are related, we obtain a contradiction. This proves the $i \neq j$ part of (3.31). Thus, (3.31) has been proved.

Finally, let $K := [\vec{\alpha}, \vec{\beta}, \vec{\gamma}, \vec{\delta}^\sharp]_{\mathrm{lat}}$; it is a sublattice of $\mathrm{Equ}(Z(n))^m$ and we are going to show that $K = \mathrm{Equ}(Z(n))^m$. Let $j \in \{1, \ldots, m\}$. It follows from (3.31) that

$$\langle \Delta, \ldots, \Delta, \underbrace{[\![d_q, d_{q+1}]\!]^{\mathrm{e}}}_{j\text{-th entry}}, \Delta, \ldots, \Delta \rangle \in K, \text{ for all } q \in \{0, \ldots, n-1\}. \qquad (3.34)$$

Since the sublattice

$$S_j := \{\Delta\} \times \cdots \times \{\Delta\} \times \mathrm{Equ}(Z(n)) \times \{\Delta\} \times \cdots \times \{\Delta\}$$

with the non-singleton factor at the j-th place is isomorphic to $Z(n)$, it follows from (3.34) and Lemma 2.2 that $S_j \subseteq K$, for all $j \in \{1, \ldots, m\}$. Therefore, since every element of $\mathrm{Equ}(Z(n))^m$ is of the form $s^{(1)} + s^{(2)} + \cdots + s^{(m)}$ with $s^{(1)} \in S_1, \ldots, s^{(m)} \in S_m$, we obtain that $\mathrm{Equ}(Z(n))^m \subseteq K$. Consequently, $\mathrm{Equ}(Z(n))^m = K = [\alpha, \beta, \gamma, \delta^\sharp]_{\mathrm{lat}}$ is a four-generated lattice, as required. The proof of Theorem 3.1 is complete. $\qquad\square$

4. $(1+1+2)$-generation

By a $(1+1+2)$-generating set or, in other words, *a generating subset of order type* $1+1+2$ we mean a four-element generating set such that exactly two of the four elements are comparable. Lattices having such a generating set are called $(1+1+2)$-*generated*. In his paper, Zádori [19] proved that for every integer $n \geq 7$, the partition lattice $\mathrm{Part}(n)$ is $(1+1+2)$-generated. In this way, he improved the result proved by Strietz [17] from $\{n : n \geq 10\}$ to $\{n : n \geq 7\}$. In this section, we generalize this result to direct powers by the following theorem; (2.3) and (3.1) are still in effect.

Theorem 4.1. *Let $n \geq 7$ be an integer, let $k := \lfloor (n-1)/2 \rfloor$, and let*

$$m_* = m_*(n) := \max\left(\lfloor (k-1)/2 \rfloor, \mathrm{Max}S(\lfloor (k-1)/2 \rfloor)^2 \right). \qquad (4.1)$$

Then $\mathrm{Part}(n)^{m_*}$ or, equivalently, $\mathrm{Equ}(n)^{m_*}$ is $(1+1+2)$-generated. In other words, the m_*-th direct power of the lattice of all partitions of the set $\{1, 2, \ldots, n\}$ has a generating subset of order type $1+1+2$.
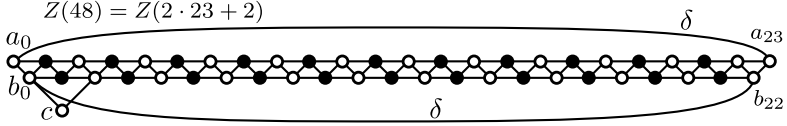
Figure 5. $Z(2k+2)$ for $k = 23$

PROOF. With our earlier conventions, we define α, β, and γ as in Sections 2 and 3, see also (3.12), but we let $\delta := [\![a_0, a_k]\!]^e + [\![b_0, b_{k-1}]\!]^e \in \mathrm{Equ}(Z(n))$. For $n = 47$, this is illustrated by Figure 5 if we omit vertex c. For $n = 48$, Figure 5 is a faithful illustration without omitting anything but taking (2.5) into account. Instead of working with U and W from (3.14), we define these two sets as follows.

$$U := \{a_i : 1 \leq i \leq k - 2 \text{ and } i \text{ is odd}\} \text{ and} \tag{4.2}$$

$$W := \{b_i : 1 \leq i \leq k - 2 \text{ and } i \text{ is odd}\}. \tag{4.3}$$

In Figure 5, $U \cup W$ is the set of black-filled elements. Let $r := \lfloor (k-1)/2 \rfloor$; note that $r = |U| = |W|$. Since $n \geq 7$, we have that $k \geq 3$ and $r \geq 1$. Let $\delta^\bullet$ be the equivalence on $Z(n)$ generated by $\delta \cup U^2 \cup W^2$. In other words, $\delta^\bullet$ is the equivalence with blocks $\{a_0, a_k, b_0, b_{k-1}\}$, U, and W such that the rest of its blocks are singletons. Let

$$t := 2 \cdot \lfloor (k+1)/2 \rfloor - 3 \text{ and } T := \{i : 1 \leq i \leq t \text{ and } i \text{ is odd}\}.$$

Based on Figure 5, we can think of T as the set of subscripts of the black-filled elements. The blocks of $\gamma + \delta^\bullet$ are the following:

$$\{a_0, a_k, b_0, b_{k-1}\} \cup \{a_i : i \in T\} \cup \{b_{i-1} : i \in T\},$$
$$\{a_{i+1} : i \in T\} \cup \{b_i : i \in T\}, \text{ and, if } k \text{ is even, } \{a_{k-1}, b_{k-2}\},$$

and, for n even, $\{c\}$. Hence, we obtain that

$$[\![a_0, b_0]\!]^e = \beta(\gamma + \delta^\bullet). \tag{4.4}$$

Similarly, the blocks of $\beta + \delta^\bullet$ are $\{c\}$, if n is even, and the following:

$$\{a_i : i \in T\} \cup \{b_i : i \in T\}, \ \{a_0, a_k, b_0, b_{k-1}, a_{k-1}\}.$$

and, for $i \in \{2, 3, \ldots, k-2\} \setminus T, \quad \{a_i, b_i\}$.

Hence, it follows that

$$\llbracket a_k, b_{k-1} \rrbracket^{\mathrm{e}} = \gamma(\beta + \delta^{\bullet}). \tag{4.5}$$

In the proof of Theorem 3.1, based on (3.14), $\mathcal{G}$, $\mathcal{H}$, (3.15), and (3.16), we defined the equivalences $\delta^{\sharp}_1, \ldots, \delta^{\sharp}_m$ in (3.17). Now we define $\delta^{\sharp}_1, \ldots, \delta^{\sharp}_{m_*}$ exactly in the same way but we use (4.2) and (4.3) instead of (3.14), and we take into account that U and W are now smaller and we obtain m_* rather than m from them. Observe that

$$\llbracket a_0, b_0 \rrbracket^{\mathrm{e}} = \beta(\gamma + \delta) \quad \text{and} \quad \llbracket a_k, b_{k-1} \rrbracket^{\mathrm{e}} = \gamma(\beta + \delta). \tag{4.6}$$

Since $\delta \leq \delta^{\sharp}_j \leq \delta^{\bullet}$ for $j \in \{1, \ldots, m_*\}$, it follows from (4.4), (4.5), and (4.6) that

$$\llbracket a_0, b_0 \rrbracket^{\mathrm{e}} = \beta(\gamma + \delta^{\sharp}_j) \quad \text{and} \quad \llbracket a_k, b_{k-1} \rrbracket^{\mathrm{e}} = \gamma(\beta + \delta^{\sharp}_j) \tag{4.7}$$

for all $j \in \{1, \ldots, m_*\}$. Armed with (4.7) and all the previous preparations, the rest of the proof is the same as in case of Theorem 3.1 unless $r = 2$; these details are not repeated here. Observe that the only role of m in the proof of Theorem 3.1 is that we had to find an m-element antichain in $\mathrm{Equ}(U) \times \mathrm{Equ}(W)$. Similarly, if $r \neq 2$, then all what we have to do with m_* is to find an m_*-element antichain in $\mathrm{Equ}(U) \times \mathrm{Equ}(W)$. If $r \neq 2$, then we obtain such an antichain as the Cartesian product of an antichain of $\mathrm{Equ}(U)$ and that of $\mathrm{Equ}(W)$. If $r = 2$, then this method does not work since $\mathrm{Equ}(U)$ and $\mathrm{Equ}(W)$ are (two-element) chains but $m_* = 2$. However, $\mathrm{Equ}(U) \times \mathrm{Equ}(W)$ has an $m_* = 2$-element antichain even in this case. This completes the proof of Theorem 4.1. $\qquad \square$

Obviously, Theorem 4.1 implies the following counterpart of Corollary 3.2.

Corollary 4.2. *Let n and m_* be as in Theorem 4.1. Then for every integer t with $1 \leq t \leq m_*$, the direct power $\mathrm{Part}(n)^t$ is $(1 + 1 + 2)$-generated.*

5. Authentication and secret key cryptography with lattices

While lattice theory is rich with involved constructs and proofs, it seems not to have many, if any, applications in information theory. The purpose of this section is to suggest a protocol primarily for *authentication*; it is also good for *secret key cryptography*, and it could be appropriate for a *commitment protocol*.

Assume that during the authentication protocol that we are going to outline, András[1] intends to prove his identity to his Bank and conversely; online, of course. In order to do so, András and the Bank should find a lattice L with the following properties:

- $|L|$ is large,
- L has a complicated structure,
- the length of L is small (that is, all maximal chains of L are small),
- every non-zero element of L has lots of lower covers and dually,
- L can be given by and constructed easily from little data,
- and L is generated by few elements.

The first four properties are to make the Adversary's task difficult (and practically impossible) while the rest of these properties ensure that András and the Bank can handle L. It is not necessary that L has anything to do with partitions, but partitions lattices and their direct powers seem to be good choices. Partition lattices are quite complicated since every finite lattice can be embedded into a finite partition lattice by Pudlák and Tůma [14]. Also, they are large lattices described by very little data. For example, we can take

$$L = \mathrm{Part}(273), \text{ its size is } |\mathrm{Part}(273)| \approx 3.35 \cdot 10^{404}, \text{ or} \tag{5.1}$$

$$L = \mathrm{Part}(12)^{61}, \text{ its size is } |\mathrm{Part}(12)^{61}| \approx 1.27 \cdot 10^{404}. \tag{5.2}$$

Although these two lattices seem to be similar in several aspects, each of them has some advantage over the other. As opposed to $\mathrm{Part}(273)$,

$$\text{joins can easily be computed componentwise in } \mathrm{Part}(12)^{61} \text{ if parallel computation is allowed.} \tag{5.3}$$

On the other hand, using that $\mathrm{Part}(273)$ is a semimodular lattice and so any two of its maximal chains have the same length, it is easy to see that the longest chain in $\mathrm{Part}(273)$ is only of length 272 (that is, this chain consists of 273 element). Using semimodularity again, it follows easily that the longest chain in $\mathrm{Part}(12)^{61}$ is of length $61 \cdot 11 = 671$, so $\mathrm{Part}(273)$ seems to be more advantageous in this aspect. Based on data obtained by computer, to be presented in Tables (5.9) and (5.10), we guess that $\mathrm{Part}(273)$ has more p-element generating sets of an *unknown pattern* than $\mathrm{Part}(12)^{61}$. If so, then this can also be an advantage of $\mathrm{Part}(273)$ since a greater variety of p-element generating sets of unknown patterns makes the

---

[1] *András* is the Hungarian version of Andrew; as a famous lattice theorist with this first name, I mention my scientific advisor, András P. Huhn (1947–1985).

Adversary's task even more hopeless. It is probably too early to weigh all the pros and cons of (5.1), (5.2) and, say, Part$(113)^3$ with size $|\mathrm{Part}(113)|^3 \approx 1.51 \cdot 10^{405}$.

András and the Bank choose two small integer parameters $p, q \geq 4$, the suggested value is $p = q = 8$ or larger; these numbers can be public. Also, András and the Bank agree upon a p-tuple

$$\overline{s} = \langle s_1, s_2, \ldots, s_p \rangle \in L^p. \tag{5.4}$$

This $\vec{s}$ is the common authentication code for András and the Bank; only they know it and they keep it in secret. So far, the role of $\overline{s}$ is that of the PIN (personal identification number) of a bank card.

Every time András intends to send an authenticated message to the Bank, the Bank selects a vector $\overline{w} = \langle w_1, w_2, \ldots, w_q \rangle$ of long and complicated p-ary lattice terms randomly. (We are going to discuss after (5.7) how to select $\overline{w}$.) Then the Bank sends $\overline{w}$ to András. (If András thinks that $\overline{w}$ is not complicated enough, then he is allowed to ask for a more complicated $\overline{w}$ repeatedly until he is satisfied with $\overline{w}$.) Then, to prove his identity, András sends

$$\overline{w}(\overline{s}) := \langle w_1(s_1, \ldots, s_p), \ldots, w_q(s_1, \ldots, s_p) \rangle \tag{5.5}$$

to the Bank. (Preferably, in the same message that instructs the Bank to do something like transferring money, etc.) The Bank also computes $\overline{w}(\overline{s})$ and compares it with what András has sent; if they are equal then the Bank can be sure that he communicates with András rather than with an adversary. Note that it is easy and fast to compute $\overline{w}(\overline{s})$ from $\overline{w}$ and $\overline{s}$. Note also that, changing their roles, András can also verify (by another q-tuple $\overline{w}'$ of terms) that he communicates with the Bank rather than with the Adversary.

The point of the protocol is that while $\overline{s}$ can be used many times, a new $\overline{w}$ is chosen at each occasion. So even if the Adversary intercepts the communication, he cannot use the old values of $\overline{w}(\overline{s})$. So the Adversary's only chance to interfere is to extract the secret $\overline{s}$ from $\overline{r} := \overline{w}(\overline{s})$. However, extracting $\overline{s}$ from $\overline{r} := \overline{w}(\overline{s})$ and $\overline{w}$ seems to be hard. (This problem is in NP and hopefully it is not in P.) The Adversary cannot test all possible p-tuples $\overline{s}' \in L^p$ since there are astronomically many such tuples. The usual iteration technique to find a root of a function $\mathbb{R}^p \to \mathbb{R}$ is not applicable here since, in general,

$$\text{it is unlikely that two elements of } L \text{ are comparable,} \tag{5.6}$$

simply because the length of L is small but $|L|$ is large. It is also unlikely that two members of L^q are comparable. If the Adversary begins parsing, say, $r_1 := w_1(\overline{s})$,

then even the first step splits into several directions since $r_1 \in L$ has many lower and upper covers and so there are many possibilities to represent it as the join of two elements (in case the outmost operation sign in w_1 is $\vee$) or as the meet of two elements (in case the outmost operation sign is $\wedge$). Each of these several possibilities split into several cases at the next step, and this happens many times depending on the length of w_1. But w_1 is a long term, whence exponentially many sub-directions should be handled, which is not feasible.

Some caution is necessary when choosing the common secret authentication code $\overline{s}$. This $\overline{s}$ should be chosen so that $[s_1, s_2, \ldots, s_p]_{\text{lat}} = L$ or at least $[s_1, s_2, \ldots, s_p]_{\text{lat}}$ should be very large. One possibility to ensure that the set $\{s_1, s_2, \ldots, s_p\}$ generates L is to extend a four-element generating set from Sections 2–4 to a p-element subset of L. If $L = \text{Part}(273)$, then one can pick a permutation τ of the set $\{1, 2, \ldots, 273\}$; this τ induces an automorphism $\overline{\tau}$ of $\text{Part}(273)$ in the natural way, and $\{\overline{\tau}(\alpha), \overline{\tau}(\beta), \overline{\tau}(\gamma), \overline{\tau}(\delta)\}$ with $\alpha, \ldots, \delta$ from Section 2 is a four-element generating set of $\text{Part}(273)$. If $L = \text{Part}(12)^{61}$, then in addition to the permutations of $\{1, 2, \ldots, 12\}$, allowing different permutations in the direct factors, there are many ways to select a 61-element antichain as a subset of the 175-element maximum-sized antichain that occurs in (3.15). (Note that we obtained this number, 175, when computing the last column of (3.3).) In both cases, András and the Bank can easily pick one of the astronomically many four-element generating sets described in the present paper. A four-element generating set can be extended to a p-element one in many ways. It would be even better to pick a p-element generating set of an unknown pattern, but it is not clear at this moment how this would be possible.

András and the Bank should also be careful when selecting a q-tuple $\overline{w} = \langle w_1, \ldots, w_q \rangle$ of complicated p-ary lattice terms. They should avoid that, for $i \in \{1, \ldots, q\}$, the outmost operation symbol in w_i is $\wedge$ and $w_i(\overline{s})$ is meet irreducible (or it has only few upper covers), and dually, and similarly for most of the subterms of w_i. In particular, $w_i(\overline{s}) \in \{0, 1\}$ should not happen.

To exemplify our ideas that come below, consider the (short) lattice term

$$x_4\Big(x_5 + \big(((x_1x_8 + x_2x_3) \cdot (x_4x_5 + x_3x_6)) + (x_2x_8 + (x_3x_4)x_7)\big)\Big); \qquad (5.7)$$

there are 15 *occurrences* of variables in this term. That is, if we represented this term by a binary tree in the usual way, then this tree would have 15 leaves.

Now, to choose a random term w_1, we can begin with a randomly chosen variable. Then, we iterate the following, say, a thousand times: after picking an occurrence of a variable in the already constructed term randomly (we denote this occurrence by x_i), selecting two of the p variables, and picking one of the two

operations symbols, we replace x_i by the meet or the join of the two variables selected, depending on which operations symbol has been picked.

When choosing the two variables and the operation symbol mentioned above, we can exclude that the replacement immediately "cancels by the absorption laws". (Or, at least, we have to be sure that this does not happen too often.) For example, it seems to be reasonable to forbid that x_6 in (5.7) is replaced by $x_3 + x_7$. Although we can choose the occurrence mentioned in the previous paragraph according to the even distribution, it can be advantageous to go after a distribution that takes the *depths* of the occurrences into account somehow.

If $q = p$, which is recommended, then it is desirable that $\overline{w}(\overline{s})$ should be far from $\overline{s}$ and, in addition, each of the $w_1(\overline{s})$, ..., $w_q(\overline{s})$ should be far from each other, from $0 = 0_L$, 1, and from s_1, ..., s_p. By "far", we mean that the usual graph theoretical *distance* in the Hasse diagram of L or that of L^q is larger than a constant. Hence, while developing w_1 randomly, one can monitor $w_1(\overline{s})$ and interfere into the random process from time to time if necessary.

If L is from (5.1) or (5.2), then L is a semimodular lattice, so any two maximal chains of L consist of the same number of elements. In this case, the above-mentioned distance of $x, y \in L$ can be computed quite easily; see for example Czédli, Powers, and White [9, equation (1.8)]. Namely, the distance of x and y is

$$\text{distance}(x, y) = \text{length}([x, x + y]) + \text{length}([y, x + y]). \qquad (5.8)$$

Since any two maximal chains of $\text{Equ}(n)$ are of the same size, it follows easily that $\text{length}([x, x + y])$ is the difference of the number of x-blocks and the number of $(x + y)$-blocks, and similarly for $\text{length}([y, x + y])$.

Several questions about the strategy remains open but future experiments with computer programs can lead to satisfactorily answers. However, even after obtaining good answers, the reliability of the above-described protocol would still remain the question of belief in some extent. This is not unexpected, since many modern cryptographic and similar protocols rely on the belief that certain problems, like factoring an integer or computing discrete logarithms, are hard.

Besides authentication, our method is also good for *cryptography*. Assume that András and the Bank have previously agreed in $\overline{s}$; see (5.4). Then one of them can send a random $\overline{w}$ to the other. They can both compute $\overline{w}(\overline{s})$, see (5.5), but the Adversary cannot since even if he intercepts $\overline{w}$, he does not know $\overline{s}$. Hence, András and the Bank can use $\overline{w}(\overline{s})$ as the secret key of a classical cryptosystem like Vernam's. Such a secret key cannot be used repeatedly many times but András and the Bank can select a new $\overline{w}$ and can get a new key $\overline{w}(\overline{s})$ as often as they wish.

Next, we conjecture that András can lock a *commitment* $\overline{s}$ by making $\overline{w}(\overline{s})$ public. To be more precise, the protocol is that there is a Verifier who chooses $\overline{w}$, and then András computes $\overline{r} = \overline{w}(\overline{s})$ with the Verifier's $\overline{w}$ and makes this $\overline{r}$ public. From that moment, András cannot change his commitment $\overline{s}$, nobody knows what this $\overline{s}$ is, but armed with $\overline{w}$ and $\overline{r}$, everybody can check András when he reveals $\overline{s}$. Possibly, some stipulations should be tailored to $\overline{s}$ and $\overline{w}$ in this situation.

Finally, we have developed and used a computer program to see if there are sufficiently many 8-element generating subsets and n-element generating sets of $\mathrm{Part}(n)$. This program, written in Bloodshed Dev-Pascal v1.9.2 (Freepascal) under Windows 10 and partially in Maple V. Release 5 (1997), is available from the author's website; see the list of publications there. The results obtained with the help of this program are reported in Tables (5.9) and (5.10). The first, ..., sixth rows in Tables (5.9) give the size n of the base set, the size of $\mathrm{Part}(n)$, the number of 8-element subsets of $\mathrm{Part}(n)$, the number of randomly selected 8-element subsets, the number of those selected 8-element subsets that generate $\mathrm{Part}(n)$, and the percentage of these generating 8-element subsets with respect to the number of the selected 8-element subsets, respectively. These subsets were selected independently according to the uniform distribution; a subset could be selected more than once. Table (5.10) is practically the same but the n-element (rather than 8-element) subsets generating $\mathrm{Part}(n)$ are counted in it.

n	4	5	6	7	8	9
$|\mathrm{Part}(n)|$	15	52	203	877	4 140	21 147
$|\forall 8\text{-sets}|$		6435	$7.53 \cdot 10^8$	$6.22 \cdot 10^{13}$	$8.41 \cdot 10^{18}$	$2.13 \cdot 10^{24}$	$9.91 \cdot 10^{29}$
$|\text{tested}|$	100 000	10 000	10 000	6000	1000	284
$|\text{found}|$	89 780	7 690	7913	5044	848	248
%	89.78	76.90	79.13	84.01	84.80	90.19

$$(5.9)$$

n	4	5	6	7	8	9
$|\mathrm{Part}(n)|$	15	52	203	877	4 140	21 147
$|\forall n\text{-sets}|$		1365	$2\,598\,960$	$9.2 \cdot 10^{10}$	$7.73 \cdot 10^{16}$	$2.13 \cdot 10^{24}$	$2.33 \cdot 10^{33}$
$|\text{tested}|$	100 000	10 000	10 000	10000	1000	
$|\text{found}|$	89 780	1430	3918	6811	848	
%	89.78	14.30	39.18	68.11	84.80	

$$(5.10)$$

Computing the last column of Table (5.9) took 73 hours for a desktop computer with AMD Ryzen 7 2700X Eight-Core Processor 3.70 GHz; this explains

that no more 8-element subsets have been tested for Table (5.9) and the last column of Table (5.10) is partly missing. After computing the columns for $n = 4$ and $n = 5$ in Tables (5.9) and (5.10), we expected that the number in the percentage row (the last row) would decrease as n grows. To our surprise, the opposite happened. Based on these two tables, we guess that $p = n$ should be and even $p = 8$ could be appropriate in the protocol if $n = 273$ and L is taken from (5.1).

Chronology and comparison, added on July 20, 2020. The first version of the present paper was uploaded to `https://arxiv.org/abs/2004.14509` on April 29, 2020. A related *second paper* dealing with direct products rather than direct powers was completed and uploaded to `http://arxiv.org/abs/2006.14139` on June 25, 2020. (This second paper pays no attention to authentication and cryptography.) The present paper corrects few typos and minor imperfections but it is not significantly different from its April 29, 2020 version. Although a particular case of the second paper also tells something on four-generation of direct powers of finite partition lattices, the present paper, yielding larger exponents and paying attention to $(1+1+2)$-generation, tells more. For example, while the four-generability of $\mathrm{Part}(2020)^{10^{127}}$ is almost explicit in the second paper and the maximum we can extract from *that* paper is approximately the four-generability of $\mathrm{Part}(2020)^{10^{604}}$, the last column of Table (3.9) in the *present* paper guarantees a significantly larger exponent, $5.5194232 \cdot 10^{3893}$. (The corresponding value, $5.52 \cdot 10^{3893}$, from Table (3.9) was obtained by rounding up.)

References

[1] S. Burris and H.P. Sankappanavar, A Course in Universal Algebra, Vol. 78, Graduate Texts in Mathematics, *Springer-Verlag*, 1981, `http://www.math.uwaterloo.ca/~snburris/htdocs/ualg.htm`.

[2] E. R. Canfield, On a problem of Rota, *Advances in Math.* **20** (1978), 1–10.

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

[4] G. Czédli, Lattice generation of small equivalences of a countable set, *Order* **13** (1996), 11–16.

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

[6] G. Czédli, $(1+1+2)$-generated equivalence lattices, *J. Algebra* **221** (1999), 439–462.

[7] G. Czédli, Four-generated quasiorder lattices and their atoms in a four-generated sublattice, *Communications in Algebra* **45** (2017), 4037–4049.

[8] G. Czédli and J. Kulin, A concise approach to small generating sets of lattices of quasiorders and transitive relations, *Acta Sci. Math. (Szeged)* **83** (2017), 3–12.

[9] G. Czédli, C. Powers and J. M. White, Medians are below joins in semimodular lattices of breadth 2, *Order*, to appear, `http://arxiv.org/abs/1911.02124`.

[10] G. Grätzer, General Lattice Theory, *Birkhäuser, Basel-Stuttgart*, 1978.

[11] G. Grätzer, Lattice Theory: Foundation, *Birkhäuser Verlag, Basel*, 2011.

[12] J. Kulin, Quasiorder lattices are five-generated, *Discuss. Math. Gen. Algebra Appl.* **36** (2016), 59–70.

[13] J. B. Nation, Notes on Lattice Theory, `www.math.hawaii.edu/~jb/books.html`.

[14] P. Pudlák and J. Tůma, Every finite lattice can be embedded in a finite partition lattice, *Algebra Universalis* **10** (1980), 74–95.

[15] B. C. Rennie and A. J. Dobson, On Stirling numbers of the second kind, *J. Combinatorial Theory* **7** (1969), 116–121.

[16] H. Strietz, Finite partition lattices are four-generated, Proc. Lattice Th. Conf. Ulm, 1975, 257–259.

[17] H. Strietz, Über Erzeugendenmengen endlicher Partitionverbände, *Studia Sci. Math. Hungarica* **12** (1977), 1–17.

[18] G. Takách, Three-generated quasiorder lattices, *Discuss. Math. Algebra Stochastic Methods* **16** (1996), 81–98.

[19] L. Zádori, Generation of finite partition lattices, Lectures in universal algebra., Vol. 43, Proc. Colloq. Szeged, 1983, *North-Holland, Amsterdam*, 1986, 573–586.

BOLYAI INSTITUTE
UNIVERSITY OF SZEGED
H-6720 SZEGED, ARADI VÉRTANÚK TERE 1
HUNGARY

E-mail: czedli@math.u-szeged.hu
URL: `http://www.math.u-szeged.hu/~czedli/`