FOUR-GENERATED DIRECT POWERS OF PARTITION LATTICES AND AUTHENTICATION

GÁBOR CZÉDLI

Dedicated to professor László Zádori on his sixtieth birthday

Abstract. For an integer \( n \geq 5 \), let \( \text{Part}(n) \) denote the lattice of all partitions of the \( n \)-element set \( \{1, 2, \ldots, n\} \). This lattice, called a partition lattice or, alternatively, an equivalence lattice, was proved to be four-generated by H. Strietz in 1975 and by L. Zádori in 1986. It is L. Zádori’s particularly elegant construction that we develop further to prove that even the \( k \)-th direct power \( \text{Part}(n)^k \) of \( \text{Part}(n) \) is four-generated if the exponent \( k \) is “not too large”. While a trivial argument shows that this direct power cannot be four-generated for very large exponents \( k \), we prove that, for example, \( \text{Part}(100)^k \) is four-generated for every exponent \( k \leq 3 \cdot 10^{89} \). Also, we prove that \( \text{Part}(n)^k \) is generated by a four element subset that is not an antichain but here \( k \) is smaller; it is at most about \( 1.45 \cdot 10^{34} \) for \( n = 100 \). Last but not least, in connection with the fact that finite partitions lattices and some of their direct powers are complicated lattices generated by only four elements, 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 construction from his very first mathematical paper is heavily used here. Our starting point is that Strietz [16, 17] proved in 1975 that

\[
\text{the lattice } \text{Part}(n) \text{ of all partitions of the (finite) set } \{1, 2, \ldots, n\} \text{ is a four-generated lattice.} \tag{1.1}
\]

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 Takáč [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 \( \text{Part}(n) \) to \( \text{Part}(n)^k \) 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 is the original lattice; see Corollaries 3.2 and 4.2. Third, for each non-singleton finite lattice \( L \), there is a (large) positive integer \( k = k(L) \) such that

\[
\text{Date: April 29, 2020.}
\]

1991 Mathematics Subject Classification. 06C10.

Key words and phrases. Partition lattice, equivalence lattice, four-generated lattice, Stirling number of the second kind, Bell number, authentication, cryptography, commitment, semimodular lattice.
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 find all possible exponents; 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 prove our first result, Theorem 3.1, asserting that \( \text{Part}(n)^k \) 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 \( \text{Part}(n)^k \). 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

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,

\[
U = \{\{1, 3\}, \{2, 4\}, \{5\}\}
\]  

(2.1)

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

\[
[1, 3] + [2, 4].
\]  

(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 \( \text{Part}(A) \). For brevity,

\[
\text{Part}(n) \text{ will stand for } \text{Part}(\{1, 2, \ldots, n\}),
\]  

(2.3)

and also for \( \text{Part}(A) \) when \( A \) is a given set consisting of \( n \) elements. Associated with a partition \( U \) of \( A \), we define an **equivalence relation** \( \pi_U \) 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 \( \pi_U \leq \pi_V \) if and only if \( U \leq V \). Hence, the **lattice** \( \text{Equ}(A) \) of all equivalence relations of \( A \) (in short, the **equivalence lattice** of \( A \)) is isomorphic to \( \text{Part}(A) \). 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 \( \{1, 2, \ldots, 5\} \) is understood. So we define and denote equivalences as the partitions above but we
prefer to work in Equ\((A)\) and Equ\((n)\) = Equ\({1, \ldots, n}\)), because the lattice operations are easier to handle in Equ\((A)\). For \(\kappa, \lambda \in \text{Equ}(A)\), the meet and the join of \(\kappa\) and \(\lambda\), denoted by \(\kappa \land \lambda\) (or \(\kappa \cdot \lambda\)) and \(\kappa \lor \lambda\), are the intersection and the transitive hull of the union of \(\kappa\) and \(\lambda\), respectively. The advantage of this notation is that the usual precedence rule allows us to write, say, \(xy + xz\) instead of \((x \land y) \lor (x \land z)\).

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

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

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-coloured) graphs. Every horizontal thin straight edge is \(\alpha\)-colored, but this is not always indicated in the figures. The thin straight edges of slope \(-1\), that is the southeast-northwest edges, are \(\gamma\)-colored. Finally, the thin solid curved edges are \(\delta\)-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 \(\alpha\)-colored ones, the components of the remaining graph are the blocks of the partition associated with \(\alpha\). In other words, \((x, y) \in \alpha\) if and only if there is an \(\alpha\)-coloured path from vertex \(x\) to vertex \(y\) in the graph, that is, a path (of possibly zero length) all of whose edges are \(\alpha\)-colored. The equivalences \(\beta, \gamma,\) and \(\delta\) are defined analogously. The success of Zádorí’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 our convention, shown in Figure 1, defines the colour of the edges even in this case.

\begin{figure}[h]
\centering
\includegraphics[width=0.2\textwidth]{figure1}
\caption{Standard notation for this paper}
\end{figure}

Let us agree upon the following notation:

\[
\sum_{\text{for all meaningful } x} \left[ u_x, v_x \right]^* \text{ will be denoted by any of } \left[ u_x, v_x \right]_{x^*}, \left[ u_y, v_y \right]_{y^*}, \text{ and } \left[ u_z, v_z \right]_{z^*}; \tag{2.6}\]

that is, each of \(x, y\) and \(z\) 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:

\[
\left[ \left( u^{(i)}, v^{(i)} \right) : i \in I \right]^* \text{ stands for } \sum_{i \in I} \left[ u^{(x)}, v^{(x)} \right]^*; \tag{2.7}\]
For an integer \( k \geq 2 \) and the \((2^k + 1)\)-element set
\[
Z = Z(2k + 1) := \{a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_{k-1}\},
\]
we define
\[
\begin{align*}
\alpha &:= \left[\begin{array}{c} a_0, a_1, \ldots, a_k \end{array}\right] e + \left[\begin{array}{c} b_0, b_1, \ldots, b_{k-1} \end{array}\right] e \\
\beta &:= \left[\begin{array}{c} a_x, b_x \end{array}\right] e = \left[\begin{array}{c} \langle a_i, b_i \rangle : 0 \leq i \leq k - 1 \end{array}\right] e, \\
\gamma &:= \left[\begin{array}{c} a_{x+1}, b_x \end{array}\right] e = \left[\begin{array}{c} \langle a_{i+1}, b_i \rangle : 0 \leq i \leq k - 1 \end{array}\right] e, \\
\delta &:= \left[\begin{array}{c} a_0, b_0 \end{array}\right] e + \left[\begin{array}{c} a_k, b_{k-1} \end{array}\right] e;
\end{align*}
\]
see Figure 2. Then the system \( \langle Z(2k + 1); \alpha, \beta, \gamma, \delta \rangle \) is called a \((2^k + 1)\)-element \( \text{Zádori configuration} \). Its importance is revealed by the following lemma.

**Lemma 2.1** (Zádori [19]). For \( k \geq 2 \), \( [\alpha, \beta, \gamma, \delta]_{\text{lat}} = \text{Equ}(Z(2k + 1)) \), that is, the four partitions the Zádori configuration generate the lattice of all equivalences of \( Z(2k + 1) \). Consequently,
\[
[\alpha, \beta, \gamma, \delta, [\alpha_0, b_0], [a_k, b_{k-1}]]_{\text{lat}} = \text{Equ}(Z(2k + 1)).
\]

**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] that has been used also in Czédli [4, 6, 4] and in other papers like Kulin [12]. We are going to recall its proof only for later reference.

**Lemma 2.2** ("Circle Principle"). If \( d_0, d_1, \ldots, d_{n-1} \) is a repetition-free enumeration of an \( n \)-element finite set \( A \) and \( n \geq 3 \), then \( \text{Equ}(A) \) is generated by
\[
\{[d_{n-1}, d_0]^e\} \cup \bigcup_{0 \leq i \leq n-2} \{[d_i, d_i+1]^e\}.
\]

**Proof of Lemma 2.2.** The lemma follows from the easy fact that for any two subscripts \( u \) and \( v \) with \( 0 \leq u < v \leq n - 1 \),
\[
\begin{align*}
[d_u, d_v]^e = \left( [d_u, d_{u+1}]^e + [d_{u+1}, d_{u+2}]^e + \cdots + [d_{v-1}, d_v]^e \right) \cdot \left( [d_d, d_{v+1}]^e \right) + \cdots + \left( [d_{n-2}, d_{n-1}]^e + [d_{n-1}, d_0]^e \right) \cdot \left( [d_d, d_1]^e \right) + \cdots + \left( [d_{u-1}, d_u]^e \right) \cdot \left( [d_d, d_{v-1}]^e \right). \tag{2.10}\n\end{align*}
\]

**Proof of Lemma 2.1.** On the set \( \{\pi, \beta, \gamma, \delta\} \) of variables, we are going to define several quaternary terms recursively. But first of all, we define the quadruple
\[
\overline{\pi} := (\overline{\pi}, \overline{\beta}, \overline{\gamma}, \overline{\delta}) \tag{2.11}
\]
of four variables with the purpose of abbreviating our quaternary terms \( t(\overline{\alpha, \beta, \gamma, \delta}) \) by \( t(\overline{\mu}) \). We let

\[
\begin{align*}
g_0(\overline{\mu}) &:= \overline{\beta \delta} \quad \text{(i.e. = \( \overline{\beta} \land \delta \)),} \\
h_{i+1}(\overline{\mu}) &:= ((g_i(\overline{\mu}) + \overline{\gamma})\overline{\alpha} + g_i(\overline{\mu}))\overline{\gamma} \text{ for } i \geq 0, \\
g_{i+1}(\overline{\mu}) &:= ((h_{i+1}(\overline{\mu}) + \overline{\beta})\overline{\alpha} + h_{i+1}(\overline{\mu}))\overline{\beta} \text{ for } i \geq 0, \\
H_0(\overline{\mu}) &:= \overline{\tau}, \\
G_{i+1}(\overline{\mu}) &:= ((H_i(\overline{\mu}) + \overline{\beta})\overline{\alpha} + H_i(\overline{\mu}))\overline{\beta} \text{ for } i \geq 0, \\
H_{i+1}(\overline{\mu}) &:= ((G_{i+1}(\overline{\mu}) + \overline{\gamma})\overline{\alpha} + G_{i+1}(\overline{\mu}))\overline{\gamma} \text{ for } i \geq 0.
\end{align*}
\]

(2.12)

For later reference, let us point out that

\[
\text{In (2.12), } \delta \text{ is used only twice: to define } g_0(\overline{\mu}) \text{ and to define } H_0(\overline{\mu}).
\]

(2.13)

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

\[ \overline{\mu} := (\alpha, \beta, \gamma, \delta). \]

(2.14)

Clearly,

\[ \beta \delta = [a_0, b_0] \text{ and } \gamma \delta = [a_k, b_{k-1}]. \]

(2.15)

An easy induction shows that

\[
\begin{align*}
g_i(\overline{\mu}) &:= \llbracket (a_i, b_j) : 0 \leq j \leq i \rrbracket \text{ for } 0 \leq i \leq k - 1, \\
h_i(\overline{\mu}) &:= \llbracket (a_i, b_{j-1}) : 1 \leq j \leq i \rrbracket \text{ for } 1 \leq i \leq k, \\
H_i(\overline{\mu}) &:= \llbracket (a_{k-j}, b_{k-1-j}) : 0 \leq j \leq i \rrbracket \text{ for } 0 \leq i \leq k - 1, \\
G_i(\overline{\mu}) &:= \llbracket (a_{k-j}, b_{k-j}) : 1 \leq j \leq i \rrbracket \text{ for } 1 \leq i \leq k.
\end{align*}
\]

(2.16)

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

\[
\begin{align*}
e_{a_i,b_i}(\overline{\mu}) &:= g_i(\overline{\mu}) \cdot G_{k-i}(\overline{\mu}), \quad \text{for } 0 \leq i \leq k - 1, \\
e_{a_i,b_{i-1}}(\overline{\mu}) &:= h_i(\overline{\mu}) \cdot H_{k-i}(\overline{\mu}), \quad \text{for } 1 \leq i \leq k \\
e_{a_i,a_{i+1}}(\overline{\mu}) &:= \overline{\alpha} \cdot (e_{a_i,b_i}(\overline{\mu}) + e_{a_{i+1},b_i}(\overline{\mu})), \quad \text{for } 0 \leq i \leq k - 1, \\
e_{b_i,b_{i+1}}(\overline{\mu}) &:= \overline{\alpha} \cdot (e_{a_{i+1},b_i}(\overline{\mu}) + e_{a_{i+1},b_{i+1}}(\overline{\mu})), \quad 0 \leq i \leq k - 2.
\end{align*}
\]

(2.17)

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

\[
\begin{align*}
e_{a_i,b_i}(\overline{\mu}) &= \llbracket a_i, b_i \rrbracket, \quad \text{for } 0 \leq i \leq k - 1, \\
e_{a_i,b_{i-1}}(\overline{\mu}) &= \llbracket a_i, b_{i-1} \rrbracket, \quad \text{for } 1 \leq i \leq k \\
e_{a_i,a_{i+1}}(\overline{\mu}) &= \llbracket a_i, a_{i+1} \rrbracket, \quad \text{for } 0 \leq i \leq k - 1, \\
e_{b_i,b_{i+1}}(\overline{\mu}) &= \llbracket b_i, b_{i+1} \rrbracket, \quad 0 \leq i \leq k - 2.
\end{align*}
\]

(2.18)

Finally, let

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

(2.19)

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

\[
\begin{align*}
e_{d_0,d_n}(\overline{\mu}) &:= \left( e_{d_0,d_{n+1}}(\overline{\mu}) + e_{d_{n+1},d_{n+2}}(\overline{\mu}) + \cdots + e_{d_{n-1},d_n}(\overline{\mu}) \right) \cdot \left( e_{d_0,d_{n+1}}(\overline{\mu}) \right) \\
&\quad + \cdots + e_{d_{n-2},d_{n-1}}(\overline{\mu}) + e_{d_{n-1},d_0} + e_{d_0,d_1} + \cdots + e_{d_{n-1},d_n}(\overline{\mu}).
\end{align*}
\]

(2.20)
for $0 \leq u < v \leq 2k + 1$. Combining (2.10), (2.18), and (2.20), we obtain that

$$e_{d_u,d_v}(\mu) = [d_u,d_v]^\ast.$$  

(2.21)

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

equality (2.21) remains valid if $\delta$, the fourth component of $\mu$, is replaced by any other partition whose meet with $\beta$ and that with $\gamma$ are $[a_0,b_0]^\ast$ and $[a_k,b_{k-1}]^\ast$, respectively. 

(2.22)

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

\[\begin{array}{c}
Z(8) = Z(2k + 2) = [a_0,a_1,a_2,a_3] = [a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8]
\end{array}\]

\[\begin{array}{c}
\text{Figure 3. A configuration for even size } 2k + 2 \text{ with } k = 3
\end{array}\]

Next, for $k \geq 2$, we add a new vertex $c$, a $\beta$-colored edge $\langle b_0,c \rangle$, and a $\gamma$-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 $\text{Equ}(Z(n)) = [\alpha,\beta,\gamma,\delta]_{\text{lat}}$.

Proof. With the short terms $\alpha^\ast := \alpha, \beta^\ast := \beta(\alpha + \delta), \gamma^\ast := \gamma(\alpha + \delta), \delta^\ast := \delta$, we define $\overline{\mu}^\ast := (\alpha^\ast,\beta^\ast,\gamma^\ast,\delta^\ast)$. For each term $t$ defined in (2.12) and (2.17), we define a term $t^\ast$ as $t^\ast(\overline{\mu}) := t(\overline{\mu})$. We also need the corresponding partitions $\alpha^\ast := \alpha, \beta^\ast := \beta(\alpha + \delta), \gamma^\ast := \gamma(\alpha + \delta), \delta^\ast := \delta$, and the quadruple $\mu^\ast := (\alpha^\ast,\beta^\ast,\gamma^\ast,\delta^\ast)$.

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 $\mu^\ast$ instead of $\mu$. In other words, they hold with $\mu$ if the terms $t$ are replaced by the corresponding terms $t^\ast$. In particular, (2.21) is reworded as follows:

$$e^\ast_{x,y}(\mu) = \llbracket x,y \rrbracket^\ast \text{ for all } x,y \in Z(n) \setminus \{c\}.$$  

(2.23)

So if we define (without defining their “*free versions” $e_{a_0,c}$ and $e_{a_2,c}$) the terms

$$e^\ast_{a_0,c}(\overline{\mu}) := \beta \cdot (\gamma + e_{a_0,a_2}(\overline{\mu}^\ast)) \quad \text{and} \quad e^\ast_{a_2,c}(\overline{\mu}) := \gamma \cdot (\beta + e_{a_0,a_2}(\overline{\mu}^\ast)),$$

(2.24)

then it follows easily that

$$e^\ast_{a_0,c}(\mu) = [a_0,c]^\ast \quad \text{and} \quad e^\ast_{a_2,c}(\mu) = [a_2,c]^\ast;$$  

(2.25)

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

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

(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)

$$f^*_{d_u,d_v}(\mu) := (e^*_{d_{u+1},d_{u+2}}(\mu) + \cdots + e^*_{d_{n-1},d_n}(\mu)) \cdot (e^*_{d_{0+1},d_{0+2}}(\mu) + \cdots + e^*_{d_{n-1},d_n}(\mu))$$

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

$$f^*_{x,y}(\mu) = \llbracket x,y \rrbracket$$

for all $x \neq y \in Z(n)$. (2.28)

The remark right after (2.25) allows us to note that (2.28) also belongs to the scope of (2.22). (2.29)

Finally, Lemma 2.2 and (2.28) imply Lemma 2.3. □

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 Part($n$) $\equiv$ Equ($n$) is the so-called $n$-th Bell number; it will be denoted by 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, Bell($n$) $= S(n,1) + S(n,2) + \cdots + S(n,n)$. Let

$$\text{MaxS}(n)$$

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

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

$$\log \text{MaxS}(n) = n \log n - n \log \log n - n + O \left( n \cdot \frac{\log \log n}{\log n} \right).$$

(3.2)

Hence, MaxS($n$) is quite large; see Tables (3.3)–(3.9) for some of its values; note that those given in exponential form are only rounded values. These tables were computed by Maple V. Release 5 (1997) under Windows 10.
Let $n \geq 5$ be an integer, let $k := \lfloor(n-1)/2\rfloor$, and let 
\[ m = m(n) := \text{MaxS}(k) \cdot \text{MaxS}(k-1). \] (3.10)

Then $\text{Part}(n)^m$ or, equivalently, $\text{Equ}(n)^m$ 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.

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 $\text{Part}(n)^t$ is four-generated. In particular, $\text{Part}(n)$ 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 $\text{Part}(n)^m \rightarrow \text{Part}(n)^t$, defined by $\langle x_1, \ldots, x_m \rangle \mapsto \langle x_1, \ldots, x_t \rangle$, sends a 4-element generating set into at most 4-element generating set, Theorem 3.1 applies.

**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 the 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 
\[ t > \text{Bell}(n) \cdot \text{Bell}(n-1) \cdot \text{Bell}(n-2) \cdot \text{Bell}(n-3), \] (3.11)
then $\text{Part}(n)^t$ is not four-generated. Thus, the exponent in Theorem 3.1 cannot be arbitrarily large.

| $n$ | 21 | 22 | 23 | 24 | 25 |
|-----|----|----|----|----|----|
| $m(n)$ | 330419250 | 330419250 | 10492193250 | 10492193250 | 3.40 \cdot 10^{14} |
| $m_n(n)$ | 49 | 49 | 625 | 625 | 625 |

| $n$ | 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} |
| $m_n(n)$ | 625 | 8100 | 8100 | 8100 | 8100 | 122500 |

| $n$ | 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} |
| $m_n(n)$ | 122500 | 122500 | 122500 | 2893401 | 2893401 | 2893401 |

| $n$ | 96 | 97 | 98 | 99 | 100 |
|-----|----|----|----|----|----|
| MaxS$(n)$ | 1.11 \cdot 10^{10} | 3.22 \cdot 10^{10} | 9.31 \cdot 10^{11} | 2.69 \cdot 10^{11} | 7.77 \cdot 10^{11} |
| $m(n)$ | 3.86 \cdot 10^{28} | 1.08 \cdot 10^{29} | 1.08 \cdot 10^{29} | 3.09 \cdot 10^{30} | 3.09 \cdot 10^{30} |
| $m_n(n)$ | 1.52 \cdot 10^{32} | 1.52 \cdot 10^{32} | 1.52 \cdot 10^{32} | 1.45 \cdot 10^{33} | 1.45 \cdot 10^{33} |
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 \(\text{Part}(n)^t\) 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 \(\text{Part}(n)^t\) is generated by some \(\{\alpha, \beta, \gamma, \delta\}\). Here \(\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)\) with all the \(\alpha_i \in \text{Part}(n)\), and similarly for \(\beta, \gamma, \) and \(\delta\). By the easy argument proving Corollary 3.2, we know that \(\{\alpha, \beta, \gamma, \delta\}\) generates \(\text{Part}(n)\) for all \(i \in \{1, \ldots, t\}\). Since \(\text{Part}(n)\) is not 3-generated by Zádorí [19], the quadruple \(\{\alpha_i, \beta_i, \gamma_i, \delta_i\}\) consists of pairwise distinct components. But there are only \(p\) such quadruples, whereby the pigeonhole principle yields two distinct subscripts \(i\) and \(j\) 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 \(\eta = (\eta_1, \ldots, \eta_t) \in [\alpha, \beta, \gamma, \delta]_{\text{lat}}\), we have that \(\eta_i = \eta_j\). Thus, \([\alpha, \beta, \gamma, \delta]_{\text{lat}} \neq \text{Part}(n)^t\), 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 \(L^2\) 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 \(\text{Equ}(Z(n))^m\) 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 \(\alpha = (\alpha_1, \ldots, \alpha_m), \beta = (\beta_1, \ldots, \beta_m), \gamma = (\gamma_1, \ldots, \gamma_m), \) and \(\delta = (\delta_1, \ldots, \delta_m)\) so that \(\{\alpha, \beta, \gamma, \delta\}\) generates \(\text{Equ}(Z(n))^m\). For every \(i \in \{1, \ldots, m\}, \alpha_i, \beta_i, \gamma_i, \gamma_i, \) and \(\delta_i\) 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 \(\delta_i\) is going to be more tricky. Let \(\delta_i := [a_0, b_i]^\# + [a_k, b_{k-1}]^\#\), as in Lemmas 2.1 and 2.3. Note that none of \(\alpha_i, \beta_i, \gamma_i, \) and \(\delta_i\) depends on \(i\). We know from Lemmas 2.1 and 2.3 that \(\{\alpha_i, \beta_i, \gamma_i, \delta_i\}\) generates \(\text{Equ}(Z(n))\). Therefore, for any two distinct elements \(u, v\) 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 \(\overline{u} := (\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta})\) such that, in virtue of (2.21) and (2.28),

\[
\begin{align*}
\text{depending on the parity of } n, \ f_{u,v} & \text{ is } c_{u,v} \text{ from the proof of Lemma 2.1 or it is } f_{u,v}^* \text{ from that of Lemma 2.3, and} \\
& f_{u,v}(\alpha_i, \beta_i, \gamma_i, \delta_i) = [u, v]^\# \in \text{Equ}(Z(n)).
\end{align*}
\]

By defining \(f_{u,v}\) to be the value of its four variables, the validity of (3.12) extends to the case \(u = v\), where \([u, u]^\#\) is understood as the least partition with all of its blocks being singletons.

Next, let \(U := \{a_1, a_2, \ldots, a_{k-1}\}\) and \(W := \{b_0, b_1, \ldots, b_{k-1}\}\); these sets are indicated by dashed ovals in Figures 2, 3, and 4. By the definition of \(\text{MaxS}(k-1)\), we can pick an integer \(r^t \in \mathbb{N}^+\) such that there are exactly \(\text{MaxS}(k-1)\) equivalences of \(U\) with exactly \(r^t\) blocks. (By a block of an equivalence we mean a block of the corresponding partition.) Let \(\mathcal{G}\) denote the set of these "\(r^t\)-block equivalences" of \(U\). Clearly, \(\mathcal{G}\) is an antichain in \(\text{Equ}(U)\) with size \(|\mathcal{G}| = \text{MaxS}(k-1)\). Similarly, \(\text{MaxS}(k)\) is the number of \(r^t\)-block equivalences for some \(r^t \in \mathbb{N}^+\) and the \(r^t\)-block equivalences of \(W\) form an antichain \(\mathcal{H} \subseteq \text{Equ}(W)\) such that \(|\mathcal{H}| = \text{MaxS}(k)\).
Observe that, in the direct product \( \text{Equ}(U) \times \text{Equ}(W) \),\n\( G \times H \) is an antichain. \hfill (3.13)
Since \( |G \times H| = |G| \cdot |H| = \text{MaxS}(k-1) \cdot \text{MaxS}(k) = m \), see (3.10), we can enumerate \( G \times H \) in the following repetition-free list of length \( m \) as follows:
\[ G \times H = \{ \langle \kappa_1, \lambda_1 \rangle, \langle \kappa_2, \lambda_2 \rangle, \ldots, \langle \kappa_m, \lambda_m \rangle \}. \] \hfill (3.14)
For each \( i \in \{1, \ldots, m\} \), we define \( \delta^i \) as follows:
\[ \delta^i := \text{the equivalence generated by } \delta_i \cup \kappa_i \cup \lambda_i; \] \hfill (3.15)
this makes sense since each of \( \delta_i, \kappa_i \) and \( \lambda_i \) is a subset of \( \mathbb{Z}(n) \times \mathbb{Z}(n) \). Clearly, for any \( x \neq y \in \mathbb{Z}(n) \), \( \langle x, y \rangle \in \alpha \delta^i \) if and only \( \langle x, y \rangle \in \kappa_i \cup \lambda_i \subseteq U^2 \cup W^2 \). This fact together with \( \kappa_i \cap \lambda_i \subseteq U^2 \cap W^2 = \emptyset \) yield that for any \( i, j \in \{1, 2, \ldots, m\} \),
\[ \text{if } i \neq j, \text{ then } \alpha \delta^i \text{ and } \alpha \delta^j \text{ are incomparable.} \] \hfill (3.16)

Next, we define
the “zigzagged circle” \( \langle d_0, d_1, \ldots, d_{n-1} \rangle \) \hfill (3.17)
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 consist of the thick 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
\[
\tilde{g}^{(j)}_{d_p, d_{p+1}}(\overline{\mu}) := f_{d_p, d_{p+1}}(\overline{\mu}) \cdot \prod_{\langle d_p, x \rangle \in \alpha \delta^j} (\tau \delta + f_{x, d_{p+1}}(\overline{\mu})) \cdot \prod_{\langle y, d_{p+1} \rangle \in \alpha \delta^j} (f_{d_{p+1}, y}(\overline{\mu}) + \tau \delta). \] \hfill (3.18)
The assumption on \( p \) means that (3.18) defines \( g_{dp,dp+1}^{(j)}(\mathcal{R}) \) for each straight edge of the zigzagged circle. We claim that for all \( j \in \{1,\ldots,m\} \) and \( p \in \{0,1,\ldots,2k-1\} \),

\[
g_{dp,dp+1}^{(j)}(\alpha_j,\beta_j,\gamma_j,\delta_j) = [dp,dp+1]^j. \tag{3.19}
\]

In order to show (3.19), observe that \( \beta_i \delta_i = \beta_i \delta_i = [a_b,0]^n \) and \( \gamma_i \delta_i = \gamma_i \delta_i = [a_k,b_k-1]^n \). These equalities, (2.22), (2.29), and (3.12) yield that for any \( u,v \in Z(n), i \in \{1,\ldots,m\}, p \in \{0,1,\ldots,2k-1\} \),

\[
f_{u,v}(\alpha_i,\beta_i,\gamma_i,\delta_i) = [u,v]^n \quad \text{and, in particular,}
\]

\[
f_{dp,dp+1}(\alpha_i,\beta_i,\gamma_i,\delta_i) = [dp,dp+1]^j. \tag{3.20}
\]

Combining (3.18) and (3.21), we obtain the “\( \leq \)” part of (3.19). In order to turn this inequality to an equality, we have to show that the pair \( \langle dp,dp+1 \rangle \) belongs to \( \alpha\delta_j + f_x,dp+1(\alpha_j,\beta_j,\gamma_j,\delta_j) \) for every \( \langle dp,x \rangle \in \alpha\delta_j \), and it also belongs to \( f_{dp+y}(\alpha_j,\beta_j,\gamma_j,\delta_j) + \alpha\delta_j \) for every \( \langle y,dp+1 \rangle \in \alpha\delta_j \). But this is trivial since \( \langle x,dp+1 \rangle \in f_x,dp+1(\alpha_j,\beta_j,\gamma_j,\delta_j) \) in the first case by (3.20), and similarly trivial in the second case. We have shown (3.19).

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

\[
\text{if } i \neq j, \text{ then there exists a } p \in \{0,1,\ldots,2k-1\} \text{ such that } g_{dp,dp+1}^{(j)}(\alpha_i,\beta_i,\gamma_i,\delta_i) = \Delta := 0_{\text{Equ}(Z(n))}. \tag{3.22}
\]

In order to prove (3.22), assume that \( i \neq j \). For an equivalence \( \gamma \in \text{Equ}(Z(n)) \) and \( x \in Z(n) \), the \( \gamma \)-block \( \{y \in Z(n) : (x,y) \in \gamma\} \) of \( x \) will be denoted by \( x/\gamma \). We know from (3.16) that \( \alpha\delta_j \not\subseteq \alpha\delta_j \). Hence, there is an element \( x \in Z(n) \) such that \( x/(\alpha\delta_j) \not\subseteq x/(\alpha\delta_j) \). Since \( c/(\alpha\delta_j) = \{c\} = c/(\alpha\delta_j) \) for \( n \) even, \( x \) is distinct from \( c \). Hence, \( x \) is one of the endpoints of a straight edge \( \langle dp,dp+1 \rangle \) of the zigzagged circle. This is how we can select a \( p \in \{0,1,\ldots,2k-1\} \), that is, a straight edge \( \langle dp,dp+1 \rangle \) of the zigzagged circle (3.17) such that

\[
dp/(\alpha\delta_j) \not\subseteq dp/(\alpha\delta_i) \quad \text{or} \quad dp+1/(\alpha\delta_j) \not\subseteq dp+1/(\alpha\delta_i). \tag{3.23}
\]

Now, we are going to show that this \( p \) satisfies the requirement of (3.22). We can assume that the first part of the disjunction given in (3.23) holds, because the treatment for the second half is very similar. Pick an element

\[
z \in dp/(\alpha\delta_j) \text{ such that } z \not\in dp/(\alpha\delta_i). \tag{3.24}
\]

Because of (3.21) and the first condition in (3.18),

\[
g_{dp,dp+1}^{(j)}(\alpha_i,\beta_i,\gamma_i,\delta_i) \leq [dp,dp+1]^j. \tag{3.25}
\]

We claim that

\[
\langle dp,dp+1 \rangle \not\subseteq g_{dp,dp+1}^{(j)}(\alpha_i,\beta_i,\gamma_i,\delta_i). \tag{3.26}
\]

Suppose the contrary. Then, using (3.18) and \( \langle dp,z \rangle \in \alpha\delta_j \), we have that

\[
\langle dp,dp+1 \rangle \in \alpha\delta_i + f_{z,dp+1}(\alpha_i,\beta_i,\gamma_i,\delta_i) \overset{(3.20)}{=} \alpha\delta_i + [z,dp+1]^j. \tag{3.27}
\]

According to (3.27), there exists a shortest sequence \( u_0 = dp+1, u_1, \ldots, u_{q-1} \), \( u_q = dp \) such that for every \( \ell \in \{0,1,\ldots,q-1\} \) either \( \langle u_{\ell},u_{\ell+1} \rangle \in \alpha\delta_i \), which is called a horizontal step, or \( \langle u_{\ell},u_{\ell+1} \rangle \in [z,dp+1]^j \), which is a non-horizontal step. There is at least one non-horizontal steps since \( dp \) and \( dp+1 \) are in distinct \( \alpha \)-blocks. A non-horizontal step means that \( \{u_{\ell},u_{\ell+1}\} = \{z,dp+1\} \), so \( \{z,dp+1\} \) is the only “passageway” between the two nonsingleton \( \alpha \)-blocks. Hence, there exists exactly
one non-horizontal step since our sequence is repetition-free. Clearly, this step is the first step. Hence, \( v_1 = z \) and all the subsequent steps are horizontal steps. Hence, \( \langle z, d_p \rangle = \langle v_1, d_p \rangle \in \alpha \delta^j \). Thus, \( z \in d_p / (\alpha \delta^j) \), contradicting the choice of \( z \) in (3.24). This contradiction yields (3.26). Finally, (3.26) together with (3.25) imply (3.22).

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

\[
h_{d_q,d_{q+1}}^{(j)}(\vec{\mu}) := f_{d_q,d_{q+1}}(\vec{\mu}) \cdot \prod_{p=0}^{2k-1} (f_{d_q,d_{p+1}}(\vec{\mu}) + g_{d_p,d_{p+1}}^{(j)}(\vec{\mu}) + f_{d_{p+1},d_{q+1}}(\vec{\mu}))
\]

(3.28)

We claim that, for \( q \in \{ 0, 1, \ldots, n - 1 \} \) and \( i, j \in \{ 1, \ldots, m \} \),

\[
h_{d_q,d_{q+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) = \begin{cases} \|d_q, d_{q+1}\|, & \text{if } i = j, \\ \Delta = 0_{\text{Equ}(Z(n))}, & \text{if } i \neq j, \end{cases}
\]

(3.29)

where \( q + 1 \) in subscript position is understood modulo \( n \). In virtue of (3.19), (3.20), and (3.21), the validity of (3.29) is clear when \( i = j \). So, to prove (3.29), we can assume that \( i \neq j \). Since \( h_{d_q,d_{q+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) \leq \|d_q, d_{q+1}\| \) by (3.20) and (3.21), it suffices to show that \( \langle d_q, d_{q+1}\rangle \notin h_{d_q,d_{q+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) \). Suppose the contrary. Then we obtain from (3.20) and (3.28) that for all \( p \in \{ 0, 2k - 1 \} \),

\[
\begin{aligned}
\langle d_q, d_{q+1}\rangle &\in \|d_q, d_{p}\| + g_{d_p,d_{p+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) + \|d_{p+1}, d_{q+1}\| \quad \text{and} \\
\langle d_q, d_{q+1}\rangle &\in \|d_q, d_{p+1}\| + g_{d_p,d_{p+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) + \|d_p, d_{q+1}\|.
\end{aligned}
\]

(3.30)

(3.31)

Now we choose \( p \) according to (3.22); then \( g_{d_p,d_{p+1}}^{(j)}(\alpha, \beta, \gamma, \delta^j_i) \) can be omitted from (3.30) and (3.31). Therefore, if \( p = q \), then both (3.30) and (3.31) assert that \( \langle d_q, d_{q+1}\rangle \in \Delta \), a contradiction. If \( \|d_p, d_{p+1}, d_q, d_{q+1}\| = 4 \), then both (3.30) and (3.31) give a contradiction again. If \( \|d_p, d_{p+1}, d_q, d_{q+1}\| = 3 \), then exactly one of (3.30) and (3.31) gives a contradiction. Hence, no matter how \( p \) and \( q \) are related, we obtain a contradiction. This proves the \( i \neq j \) part of (3.29). Thus, (3.29) has been proved.

Finally, let \( K := [\alpha, \beta, \gamma, \delta^j_i]_{\text{lat}} \); it is a sublattice of \( \text{Equ}(Z(n))^m \) and we are going to show that \( K = \text{Equ}(Z(n))^m \). Let \( j \in \{ 1, \ldots, m \} \). By (3.29),

\[
\langle \Delta, \ldots, \Delta, \|d_q, d_{q+1}\|, \Delta, \ldots, \Delta \rangle \in K, \text{ for all } q \in \{ 0, \ldots, n - 1 \}.
\]

(3.32)

Since the sublattice

\[
S_j := \{ \Delta \} \times \{ \Delta \} \times \text{Equ}(Z(n)) \times \{ \Delta \} \times \{ \Delta \}
\]

with the non-singleton factor at the \( j \)-the place is isomorphic to \( Z(n) \), it follows from (3.32) and Lemma 2.2 that \( S_j \subseteq K \), for all \( j \in \{ 1, \ldots, m \} \). Therefore, since every element of \( \text{Equ}(Z(n))^m \) is of the form \( s^{(1)} \cup s^{(2)} \cup \ldots \cup s^{(m)} \) with \( s^{(1)} \in S_1, \ldots, s^{(m)} \in S_m \), we obtain that \( \text{Equ}(Z(n))^m \subseteq K \). Consequently, \( \text{Equ}(Z(n))^m = K = \)
[α, β, γ, δ]_{lat} is a four-generated lattice, as required. The proof of Theorem 3.1 is complete. □

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 \( \text{Part}(n) \) 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

\[
m_* = m_*(n) := \max \left( \lfloor (k - 1)/2 \rfloor, 1, \max S(\lfloor (k - 1)/2 \rfloor)^2 \right)
\]

Then \( \text{Part}(n)^m_* \) or, equivalently, \( \text{Equ}(n)^m_* \) 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](image)

**Proof.** Combining Zádori’s 1986 idea, see [19] with that of the proof or Theorem 3.1, the proof is straightforward and, thus, would be boring to the reader. Hence, and also because of saving space, we only outline the proof. With our earlier conventions, we define \( \alpha, \beta, \gamma, \) and \( \delta \) as in Section 3, but we let \( \delta := \{a_0, a_k\}^\ast + \{b_0, b_{k-1}\}^\ast \). 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. Since

\[
\{a_0, b_0\}^\ast = (\beta + \delta) \quad \text{and} \quad \{a_k, b_{k-1}\}^\ast = (\gamma + \delta),
\]

we obtain that \( [\alpha, \beta, \gamma, \delta]_{lat} = \text{Equ}(Z(n)) \) both for \( n \) odd and \( n \) even in the same way as in Section 3. (For \( n \) odd, also in the same way as Zádori [19].) Instead of taking the same \( U \) and \( W \) as in the proof of Theorem 3.1, now we let \( U := \{a_i : 1 \leq i \leq k - 2 \text{ and } i \text{ is odd} \} \) and \( W := \{b_i : 1 \leq i \leq k - 2 \text{ and } i \text{ is odd} \} \). The point with this \( U \) and \( W \) is that we are going to extend \( \delta \) by equivalences of \( U \) and \( W \) as in the proof of Theorem 3.1 but we want to keep the validity of (4.2). For (4.2), it was important that the distance \( k \) between \( a_0 \) and \( a_k \) and the distance \( k - 1 \) between \( b_0 \) and \( b_{k-1} \) are of distinct parities. Since the distance between any two elements of \( U \) is even, the same holds for \( W \), and since \( (U \cup W) \times \{a_0, b_0, a_k, b_{k-1}\} \) will remain disjoint from the extended \( \delta \), the validity of (4.2) will not be in danger. The rest of the proof is practically the same as in case of Theorem 3.1, but there is a little modification for \( n \) small. Namely, if \( t := \lfloor (k - 1)/2 \rfloor = 2 \), then \( \text{Equ}(t) \) is a chain and \( \max S(t)^2 = 1 \). However, we can easily take a 2-element antichain in \( \text{Equ}(2) \times \text{Equ}(2) \) in this case. □
Next, we state a counterpart of Corollary 3.2, which clearly holds.

**Corollary 4.2.** Let \( n \) and \( m \ast \) as in Theorem 4.1. Then for every integer \( t \) with \( 1 \leq t \leq m \ast \), the direct power \( \text{Part}(n)^t \) 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 a Bank and conversely; online, of course. We need 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 lattice by Pudlák and Tůma [14]. Also, they are large lattices described by very little data. For example, we can take

\[
L = \text{Part}(201), \text{ its size is } |\text{Part}(201)| = 3.18 \cdot 10^{277},
\]

or

\[
L = \text{Part}(10)^{55}, \text{ its size is } |\text{Part}(10)^{55}| = 3.47 \cdot 10^{278}.
\]

Although these two lattices seem to be similar is several aspects, let us point out a possible advantage of \( \text{Part}(10)^{55} \): while it is time-consuming to compute the join of two partitions in \( \text{Part}(201) \) and parallel computation seems not to help much,

\[
\text{joins can easily be computed componentwise in } \text{Part}(10)^{55} \text{ if parallel computation is allowed.}
\]

András and the Bank chooses two small integer parameters \( p, q \geq 4 \), the suggested value is \( p = q = 8 \) or larger; this can be public. Also, András and the Bank agrees upon a \( p \)-tuple \( \vec{s} = (s_1, s_2, \ldots, s_p) \in L^p \). 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 \( \vec{s} \) is that of the PIN (personal identification number) of a bank card.

Every time András and the Bank begins to communicate, András selects a random vector \( \vec{w} = (w_1, w_2, \ldots, w_q) \) of long and complicated \( p \)-ary lattice terms. (If the Bank thinks that \( \vec{w} \) is not complicated enough, then it can insist of choosing another \( \vec{w} \) or there can be a software that automatically filters out those \( \vec{w} \) that are not complex enough.) After that András sends his \( \vec{w} \) to the Bank, the Bank sends

\[
\vec{w}(\vec{s}) := (w_1(s_1, \ldots, s_p), \ldots, w_q(s_1, \ldots, s_p))
\]

\(^1\)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).
back to András. András also computes $\overline{\varpi}(\overline{s})$ and compares it with what the Bank has sent; if they are equal then András can be sure that he communicates with the Bank rather then with an Adversary. Note that it is easy and fast to compute $\overline{\varpi}(\overline{s})$ from $\overline{\varpi}$ and $\overline{s}$. The Bank verifies similarly if it is communicating with András. That is, the Bank sends a randomly chosen complicated and long $q$-tuple $\overline{\varpi}'$ of $p$-ary lattice terms to András and checks if András can send $\overline{\varpi}'(\overline{s})$.

At each occasion, new $\overline{\varpi}$ and $\overline{\varpi}'$ are chosen randomly, so even if the Adversary intercepts the communication, he cannot use the old values of $\overline{\varpi}(\overline{s})$ and $\overline{\varpi}'(\overline{s})$. So the Adversary’s only chance to interfere is to extract the secret $\overline{s}$ from $\overline{s} := \overline{\varpi}(\overline{s})$ and $\overline{\varpi}$ (or from $\overline{\varpi}'(\overline{s})$ and $\overline{\varpi}'$). However, extracting $\overline{s}$ from $\overline{s} = \overline{\varpi}(\overline{s})$ and $\overline{\varpi}$ seems to be hard. (This problem is in NP and hopefully it is not in $\mathcal{P}$.)

The Adversary cannot test all possible $p$-tuples $\overline{s}' \in L^p$ since there are astronomically many such tuples. The usual iteration technique that would work to find the root of a function $\mathbb{R}^p \to \mathbb{R}$ is not applicable since it is very unlikely that two elements of $L$ are comparable, simply because the length of $L$ is small. It is even more 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 lover and upper covers and so there are many ways to represent it as the join of two elements (in case the outmost operation in $w_1$ is a join) or the meet of two elements (in case the outmost operation is a meet). Each of these several directions splits into several sub-directions 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 followed, which is not feasible.

Some caution by András and the Bank is necessary when choosing the secret common authentication code $\overline{s}$. This $\overline{s}$ should be chosen so that $[s_1, s_2, \ldots, s_p]_{\text{lat}}$ should be very large. One possibility to ensure that $s_1, s_2, \ldots, s_p$ generates $L$ is to extend a four-element generating set form Sections 2–4 to a $p$-element subset of $L$. If $L = \text{Part}(201)$, then one can pick a permutation $\tau$ of the set $\{1, 2, \ldots, n\}$; this $\tau$ induces an automorphism $\tau$ of $\text{Part}(201)$ in the natural way, and $\{\tau(\alpha), \tau(\beta), \tau(\gamma), \tau(\delta)\}$ with $\alpha, \ldots, \delta$ from Section 2 is a four-element generating set of $\text{Part}(201)$. If $L = \text{Part}(10)^{55}$, then in addition to a permutation of $\{1, 2, \ldots, 10\}$, there are many ways to select a 55-element antichain as a subset of the 175-element maximum-sized antichain that occurs in (3.13). In both cases, András and the Bank can easily pick one of the astronomically many four-element generating sets described in the present paper. They can extend this four-element set to a $p$-element one in many ways, and there are four-element generating sets described neither in the present paper, nor in Strietz [17].

András and the Bank should also be careful when selecting a $q$-tuple $\overline{\varpi} = \langle w_1, \ldots, w_q \rangle$ of complicated $p$-ary lattice terms. To exemplify our ideas, consider the (short) lattice term

$$x_4 \left( x_5 + \left( (x_1 x_8 + x_2 x_3)(x_4 x_5 + x_3 x_6) \right) + \left( x_2 x_8 + (x_3 x_4) x_7 \right) \right). \quad (5.4)$$

Now, to choose a random term $w_1$, we can begin with a randomly chosen variable. Then, we iterate the following, say, 300 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. However, the following questions arise.
Shall we pick the first occurrence of $x_4$, the first occurrence of $x_5$ and the (only) occurrence of $x_6$ in (5.4) with the same probability or should these probabilities depend (and how should they depend) on the “depths” of these occurrences, which are distinct? Should we always check whether the replacement immediately cancels be the absorption laws? For example, if $x_6$ in (5.4) is replaced by $x_3 + x_7$, then this replacement cancels, but it is easy to avoid such replacements. 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 $w_1(\overline{s}), \ldots, w_q(\overline{s})$ should be far from each other, from $0 = 0_L$, 1, and from $s_1, \ldots, s_p$. 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; it is a question what this constant should be for $L$ or for $L^q$. Since $L$ is of a small length, there is a danger that while we are building, say, $w_1$, then $w_1(\overline{s})$ becomes 0 or 1 quite early. Hence, while developing $w_1$ randomly, one can monitor $w_1(\overline{s})$ and interfere into the random process from time to time.

If $L$ is from (5.1) or (5.2), then $L$ is a semimodular lattice, so any two maximal chain 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

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

Since any two maximal chains of 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 $\text{length}([x, x+y])$.

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.

If authentication is not (or no longer) targeted and only $\overline{w}$ is transmitted, then $\overline{w}(\overline{s})$ described above is known only for András and the Bank. In the same way, they can easily convert $\overline{w}(\overline{s})$ into a string or a sequence of integers. Hence, András and the Bank can use $\overline{w}(\overline{s})$ as the secret key of a classical cryptosystem like Vernam’s. Such a 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.

We guess 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 $\overline{s}$.

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

\begin{table}
\begin{tabular}{|c|c|c|c|c|c|c|c|}
\hline
\text{n} & 4 & 5 & 6 & 7 & 8 & 9 \\
\hline
|Part($n$)| 15 & 52 & 203 & 877 & 4140 & 21447 \\
\hline
|\forall-sets| 6435 & 7.53 \cdot 10^9 & 6.22 \cdot 10^{10} & 8.41 \cdot 10^{12} & 2.13 \cdot 10^{16} & 9.91 \cdot 10^{23} \\
\hline
|tested| 100000 & 10000 & 10000 & 6000 & 1000 & 284 \\
\hline
|found| 89780 & 7690 & 7913 & 5044 & 848 & 248 \\
\hline
|\%| 89.78 & 76.90 & 79.13 & 84.01 & 84.80 & 90.19 \\
\hline
\end{tabular}
\end{table}
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 \( \text{Part}(n) \). 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 5.6 and 5.7. The second, third, fourth, fifth, and sixth rows in Tables 5.6 give the size of \( \text{Part}(n) \), the number of its 8-element subsets, the number of randomly selected 8-elements subsets, the number of those selects 8-elements subsets that generate \( \text{Part}(n) \), 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 5.7 is practically the same but the \( n \)-element subsets generating \( \text{Part}(n) \) are counted in it.

| \( n \) | 4  | 5  | 6  | 7  | 8  | 9  |
|------|----|----|----|----|----|----|
| \( |\text{Part}(n)| \) | 15 | 52 | 203| 877| 4140| 21147|
| \( |\text{\( \forall \)}-\text{sets}| \) | 1365·2·509·960·9.2·10^19| 7.73·10^18| 2.13·10^17| 2.33·10^16|
| \( |\text{tested}| \) | 100000 | 100000 | 10000 | 10000 | 1000 |
| \( |\text{found}| \) | 89780  | 1430 | 3918 | 6811 | 848 |
| \%  | 89.78| 14.30| 39.18| 68.11| 84.80|

(5.7)

Computing the last column of Table 5.6 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 5.6 and the last column of Table 5.7 is missing. After computing the columns for \( n = 4 \) and \( n = 5 \) in Tables 5.6 and 5.7, we expected that the number in the percentage row (the last row) would decrease as \( n \) 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 \( n = 201 \) and \( L \) is taken from (5.1).

**References**

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

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

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

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

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

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

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

[8] Czédli, G., Kulin, J.: 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 Jeremy M. White: Medians are below joins in semimodular lattices of breadth 2. http://arxiv.org/abs/1911.02124

[10] Grätzer, G.: General lattice theory, Birkhäuser, Basel-Stuttgart, 1978

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

[12] Kulin, J. (2016). Quasiorder lattices are five-generated. *Discuss. Math. Gen. Algebra Appl.* **36**: 59–70.
[13] Nation, J. B.: Notes on Lattice Theory. www.math.hawaii.edu/~jb/books.html
[14] Pudlák, P.; Tůma, J.: Every finite lattice can be embedded in a finite partition lattice. Algebra Universalis 10 (1980), 74–95.
[15] Rennie, B. C.; Dobson, A. J.: On Stirling numbers of the second kind. J. Combinatorial Theory 7 (1969), 116–121.
[16] Strietz H. (1975). Finite partition lattices are four-generated. In: Proc. Lattice Th. Conf. Ulm, 1975, pp. 257–259.
[17] Strietz H. (1977). Über Erzeugendenmengen endlicher Partitionverbände. Studia Sci. Math. Hungarica 12:1–17.
[18] Takách, G. (1996): Three-generated quasiorder lattices. Discuss. Math. Algebra Stochastic Methods 16: 81–98.
[19] Zádori, L. (1986) Generation of finite partition lattices. In: Lectures in universal algebra. (Proc. Colloq. Szeged, 1983) Colloq. Math. Soc. János Bolyai, Vol. 43. Amsterdam: North-Holland, pp. 573–586.