Серия «Математика»
2025. Т. 53. С. 141—155

Онлайн-доступ к журналу:
http://mathizv.isu.ru

И З В Е С Т И Я
Иркутского государственного университета

Research article

УДК 512.62
MSC 06B99, 06C10
DOI https://doi.org/10.26516/1997-7670.2025.53.141

Four-element Generating Sets with Block Count Widths at Most Two in Partition Lattices

Gábor Czédli[1]✉

[1] University of Szeged, Bolyai Institute, Szeged, Hungary
✉ czedli@math.u-szeged.hu

Abstract: The partitions of a finite set form a so-called *partition lattice*. Henrik Strietz proved that this lattice has a four-element generating set; his paper has been followed by a dozen others. Two recent papers of the present author indicate that small generating sets of these lattices can be applied in *cryptography*. The *block count* of a partition is the number of its blocks. Given a four-element set of partitions, list the block counts of its members in increasing order. Then subtract the first (i.e., the smallest) block count from all four to obtain the components of a four-dimensional vector. This vector and its last component are called the *block count type* and the *block count width*, respectively, of the given four-element set in question. There are exactly ten block count types of width at most two. We prove that for any partition lattice over a finite base set with at least eight elements, each of the ten block count types of width at most two is the block count type of a four-element *generating set* of the partition lattice; moreover, we give a lower bound of the number of these generating sets.

Keywords: equivalence lattice, four-element generating set, partition lattice, many small generating sets

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

For citation: Czédli G. Four-element Generating Sets with Block Count Widths at Most Two in Partition Lattices. *The Bulletin of Irkutsk State University. Series Mathematics*, 2025, vol. 53, pp. 141–155.
https://doi.org/10.26516/1997-7670.2025.53.141

Научная статья

Четырехэлементные порождающие множества с шириной блоков не более двух в решетках разбиений

Г. Цедли[1✉]

[1] Сегедский университет, Институт Бойяи, Сегед, Венгрия
✉ czedli@math.u-szeged.hu

Аннотация: Разбиения конечного множества образуют так называемую *решетку разбиений*. Хенрик Штриец доказал, что эта решетка имеет четырехэлементное порождающее множество; его статья была продолжена дюжиной других. Две недавние статьи автора показывают, что малые порождающие множества этих решеток могут быть применены в *криптографии*. *Количество блоков* разбиения — это количество его блоков. Дано четырехэлементное множество разбиений, перечислите количество блоков его элементов в порядке возрастания. Затем вычтите первое (т. е. наименьшее) количество блоков из всех четырех, чтобы получить компоненты четырехмерного вектора. Этот вектор и его последний компонент называются *типом количества блоков* и *шириной количества блоков* данного четырехэлементного множества. Существует ровно десять типов количества блоков шириной не более двух. В данном исследовании доказывается, что для любой решетки разбиений над конечным базовым множеством, содержащим не менее восьми элементов, каждый из десяти типов количества блоков шириной не более двух является типом количества блоков четырехэлементного *порождающего множества* решетки разбиений; более того, дается нижняя граница числа этих порождающих множеств.

Ключевые слова: решётка эквивалентностей, четырёхэлементное порождающее множество, решётка разбиений, множество малых порождающих множеств

Благодарности: Работа выполнена при финансовой поддержке OTKA K 138892, Венгрия

Ссылка для цитирования: Czédli G. Four-element Generating Sets with Block Count Widths at Most Two in Partition Lattices // Известия Иркутского государственного университета. Серия Математика. 2025. Т. 53. С. 141–155.
https://doi.org/10.26516/1997-7670.2025.53.141

Dedication

This paper is dedicated to Professor **Sándor Radeleczki**, an esteemed coauthor of mine, on his sixty-fifth birthday.

1. Introduction

The present writing is intended to be self-contained modulo an average MSc curriculum. Even though this introductory section can contain some concepts known only by experts, the notions needed in the statements and their proofs will be defined in due course.

Recent developments show that some lattices like partition lattices could have applications in (the algebraic methods of) computer science and information processing, namely, in cryptography; see [2] and mainly [3]. Even though [3] would probably need further development and analysis before implementation, it is an important constituent of our motivation.

The second part of the motivation for this paper lies in the rich literature on the topic, which is worth continuing. By an old result of Strietz [6], finite partition lattices with at least five elements can be generated by four of their elements. His result has been followed by more than half a dozen papers devoted to four-element generating sets of partition lattices and also by half a dozen papers devoted to the closely related topic of four-element (or small) generating sets of quasiorder lattices. To keep the size of the References section limited, here we mention only Zádori's pioneering 1986 paper [7] and Kulin [5], as their methods influenced many other papers. The rest of the literature is surveyed in [1], [3], and [4] (with overlappings).

We know from [4] that many four-element generating sets of a given partition lattice can be constructed feasibly; let X denote the collection of these four-element generating sets. However, the statistical analysis presented in [4] shows with high confidence level (but does not prove rigorously) that the collection of four-element generating sets is much larger than X. Since the cryptographic applicability depends on the size of X, any argument that increases X makes sense; this idea also belongs to our motivation.

Next, we fix some notations and recall some well-known concepts.

Notations. *As it is usual in lattice theory,* $X \subset Y$ *denotes that* X *is a* proper subset *of* Y*, that is,* $X \subseteq Y$ *and* $X \neq Y$*.*

For a set A*, let* $\mathrm{Part}(A)$ *stand for the collection of all partitions of* A*. That is,* $B \in \mathrm{Part}(A)$ *if and only if* B *is a set of pairwise disjoint nonempty subsets of* A *such that* A *is the union of the members of* B*.*

For a natural number $n \in \mathbb{N}^+ := \{1, 2, 3, \dots\}$*, let* $[n] := \{1, 2, \dots, n\}$*. Instead of* $\mathrm{Part}([n])$*, we will often write* $\mathrm{Part}(n)$*.*

Let $\{S_i : i \in K\}$ be a finite collection of nonempty sets. We say that $\bigcup_{i\in K} S_i$ is a *connected overlapping union* if either $|K| = 1$, or $|K| > 1$ and the following two conditions hold:

1) for each $i \in K$, there is a $j \in K \setminus \{i\}$ such that $S_i \cap S_j \neq \emptyset$, and
2) there is no nonempty proper subset I of K such that $S_i \cap S_j = \emptyset$ for every $i \in I$ and $j \in K \setminus I$.

For example, $\{1, 2\} \cup \{2, 3\} \cup \{3, 4\}$ is a connected overlapping union but $\{1, 2\} \cup \{2, 3\} \cup \{4, 5\} \cup \{5, 6\}$ is not. The forthcoming description of the join in a partition lattice might look unusual but it has the advantage of showing how one can compute it. Hence, for those familiar with other definitions, it is trivial that our definition is equivalent to the standard ones.

Definition 1. *For $B \in \mathrm{Part}(A)$, the members of B are called the* blocks *of B. For $X, Y, U, V \in \mathrm{Part}(A)$,*

$$X \le Y \overset{\text{def}}{\iff} \textit{each block of } X \textit{ is a subset of some block of } Y;$$
$$U = X \wedge Y \overset{\text{def}}{\iff} \textit{the blocks of } U \textit{ are exactly the nonempty } E \cap F \textit{ where } E \textit{ is a block of } X \textit{ and } F \textit{ is a block of } Y;$$
$$V = X \vee Y \overset{\text{def}}{\iff} \textit{the blocks of } V \textit{ are exactly the maximal connected overlapping unions of sets belonging to } X \cup Y.$$

Then $\wedge$ and $\vee$ are operations on $\mathrm{Part}(A)$, and the structure $(\mathrm{Part}(A), \wedge, \vee)$ is the partition lattice of A. *As usual, we write $\mathrm{Part}(A)$ rather than writing $(\mathrm{Part}(A), \wedge, \vee)$. In particular, if $n \in \mathbb{N}^+$ and $A = [n]$, then $\mathrm{Part}(n) := \mathrm{Part}([n])$ stands for the* partition lattice *of $\{1, \dots, n\}$.*

Definition 2. *For a set A, a nonempty subset S of $\mathrm{Part}(A)$ is a* sublattice *of $\mathrm{Part}(A)$ if for any $X, Y \in S$, both $X \wedge Y$ and $X \vee Y$ are in S. A subset G of $\mathrm{Part}(A)$ is a* generating set *of $\mathrm{Part}(A)$ or, in other words, G* generates *$\mathrm{Part}(A)$ if there is no proper sublattice S of $\mathrm{Part}(A)$ such that $G \subseteq S$. For $k \in \mathbb{N}^+$, $\mathrm{Part}(A)$ is* k-generated *if it is generated by a k-element subset.*

With reference to Strietz [6], we have already mentioned that for $3 \le n \in \mathbb{N}^+$, $\mathrm{Part}(n)$ is four-generated. Note that Strietz also proved that $\mathrm{Part}(n)$ is not three-generated for $3 \le n \in \mathbb{N}^+$.

2. Methods

In addition to using or developing some lemmas proved in earlier papers, an integral part of our method is the following notation of the elements of $\mathrm{Part}(A)$ and (in particular) $\mathrm{Part}(n)$ for a finite set A and $n \in \mathbb{N}^+$. Namely, for $X \in \mathrm{Part}(A)$, we denote X by listing its non-singleton blocks and the elements of these blocks in the lexicographic order. We separate the blocks by semicolons. Within a block, we can separate the elements by commas; these commas are often dropped when no ambiguity threatens. For example,

$$\mathrm{pt}(bd) = \{\{a\}, \{b, d\}, \{c\}\} \in \mathrm{Part}(\{a, b, c, d\}), \tag{2.1}$$
$$\mathrm{pt}(bd) = \{\{a\}, \{b, d\}, \{c\}, \{e\}\} \in \mathrm{Part}(\{a, b, c, d, e\}), \tag{2.2}$$
$$\mathrm{pt}(be; cd) = \{\{a\}, \{b, e\}, \{c, d\}\} \in \mathrm{Part}(\{a, b, c, d, e\}),$$
$$\mathrm{pt}(11, 14; 12, 13) = \{\{11, 14\}, \{12, 13\}\} \in \mathrm{Part}(\{11, 12, 13, 14\}),$$
$$\mathrm{pt}() = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\} \in \mathrm{Part}(6).$$

The acronym pt in the notation comes from **p**ar**t**ition; we can add A or n, rather than $[n]$, to it as a subscript. The advantage of our notation is that for any $n \in \mathbb{N}^+$,

$$\text{if } A \subseteq B, \text{ then } \mathrm{Part}(A) \text{ is a sublattice of } \mathrm{Part}(B) \tag{2.3}$$

in the natural way exemplified by (2.1) and (2.2). For $X \subseteq \mathrm{Part}(n)$, the *sublattice generated by* X consists of those partitions that can be obtained from the members of X by using meets and joins in a finite number of steps. The following easy lemma is Lemma 2.5 from [4].

Lemma 1 ("Circle Principle"). *For $2 \le n \in \mathbb{N}^+$ and an n-element set A, and let $a_1, a_2, \dots, a_n$ be the elements of A. If each of $\mathrm{pt}(a_1a_2)$, $\mathrm{pt}(a_2a_3)$, $\mathrm{pt}(a_3a_4)$, …, $\mathrm{pt}(a_{n-1}a_n)$, and $\mathrm{pt}(a_na_1)$ belongs to the sublattice generated by X, then X generates $\mathrm{Part}(A)$.*

To *find* the generating sets occurring in Lemmas 4–23, we used a variant of the mini-package "equ2024p" of programs developed by the author; it is available from the author's website[1]. (This explains how the components of $\vec{\alpha}$ in Lemmas 4–23 will be listed.) On the other hand, finding computer-free and *humanly readable proofs* of the fact that the four-element sets in these lemmas are *generating* sets required to add a lot of human effort. This fact can be (and has been) verified in two independent ways. First, "equp2024reduced.exe" in the mini-package can be used to verify whether a four-element subset of $\mathrm{Part}(n)$, for $n \le 9$, is a generating set. Second, even though the humanly readable proofs that we present are long and technical, it is substantially faster to verify them than to find a rigorous verification of the correctness of the computer program.

3. Our theorem

For $\mu \in \mathrm{Part}(n)$, let $\mathrm{nbl}(\mu)$ denote the ***n**umber of **bl**ocks* of μ. For example, $\mathrm{nbl}(\mathrm{prt}_7(25, 367)) = 4$ and $\mathrm{nbl}(\mathrm{prt}_8(25, 367)) = 5$.

Definition 3. *For a finite set A, let X be a four-element subset of $\mathrm{Part}(A)$. Denote the elements of X so that $X = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and the inequalities $\mathrm{nbl}(\alpha_1) \le \mathrm{nbl}(\alpha_2) \le \mathrm{nbl}(\alpha_3) \le \mathrm{nbl}(\alpha_4)$ hold. Then the* block count type *of X, denoted by $\mathrm{bctyp}(X)$, is defined to be the following vector:*

$$\mathrm{bctyp}(X) := \big(0, \mathrm{nbl}(\alpha_2) - \mathrm{nbl}(\alpha_1), \mathrm{nbl}(\alpha_3) - \mathrm{nbl}(\alpha_1), \mathrm{nbl}(\alpha_4) - \mathrm{nbl}(\alpha_1)\big).$$

The block count width *of X is $\mathrm{nbl}(\alpha_4) - \mathrm{nbl}(\alpha_1)$. If $X = \{\beta_1, \dots, \beta_4\}$ (without assuming any inequalities among the $\mathrm{nbl}(\beta_i)$s) generates $\mathrm{Part}(A)$, then $\vec{\beta}$ is called a* generating vector *and $\mathrm{bctyp}(\vec{\beta})$ is defined to be $\mathrm{bctyp}(X)$.*

[1] https://tinyurl.com/g-czedli/

The components of $\operatorname{bctyp}(X)$ above are in $\mathbb{N} := \{0\} \cup \mathbb{N}^+ = \{0, 1, 2, \dots\}$. If X is of block count width at most k, then $\operatorname{bctyp}(X) = (0, i_2, i_3, i_4)$ such that $0 \le i_2 \le i_3 \le i_4 \le k$. For $k = 2$, we will prove the converse: if $(0, i_2, i_3, i_4)$ satisfies these inequalities, then it is of the form $\operatorname{bctyp}(X)$; furthermore, this is witnessed by very many four-element generating sets X of $\operatorname{Part}(n)$. To be more precise, we formulate the result of the paper as follows; the lower integer part of a real number x will be denoted by $\lfloor x \rfloor$.

Theorem 1. *Whenever $i_2, i_3, i_4 \in \mathbb{N}$ such that $i_2 \le i_3 \le i_4 \le 2$ and $8 \le n \in \mathbb{N}^+$, then $\operatorname{Part}(n)$ has a four-element generating set X with block count type $(0, i_2, i_3, i_4)$. Furthermore, if $n \ge 10$, then $\operatorname{Part}(n)$ has at least*

$$\frac{2^{2\lfloor (n-8)/2 \rfloor - 3} \cdot (2\lfloor (n-8)/2 \rfloor - 1)!}{3 \cdot (2\lfloor (n-8)/2 \rfloor + 1)} \tag{3.1}$$

four-element generating sets X such that $\operatorname{bctyp}(X) = (0, i_2, i_3, i_4)$.

Remark 1. If m denotes the largest even integer such that $m \le n - 8$, then (3.1) turns into $2^{(m-3)} \cdot (m-1)!/(3m+3)$. This is a huge number. For example, for $n = 20$ and $n = 100$, (3.1) is 524 035 939 and (rounded to three decimal places in its exponential form) $2.999 \cdot 10^{164}$, respectively.

4. A lemma to support induction

The proof of Theorem 1 requires several lemmas. Although the present paper does not rely on the author's preprint https://tinyurl.com/czg-h4gen, we borrow the following concept from this preprint and the subsequent Lemma 2 is a slight generalization of a lemma in the preprint. The proof of Lemma 2 here is shorter than its precursor in the preprint. For a set A and $u_0 \ne u_1 \in A$, we denote the least element of $\operatorname{Part}(A)$, the greatest element of $\operatorname{Part}(A)$, and the partition with $\{u_0, u_1\}$ as the only non-singleton block by $0_{\operatorname{Part}(A)}$, $1_{\operatorname{Part}(A)}$, and $\operatorname{pt}(u_0, u_1)$ or $\operatorname{pt}(u_0 u_1)$, respectively.

Definition 4. *For a finite set A, $\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,1}, \alpha_{1,0} \in \operatorname{Part}(A)$, and $u_0, u_1 \in A$, we say that $\mathfrak{A} = (A; \alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1}; u_0, u_1)$ is an* eligible system *if it satisfies the following conditions:*

$$\{\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,1}, \alpha_{1,0}\} \text{ is a four-element generating set of } \operatorname{Part}(A), \tag{4.1}$$

$$\alpha_{0,0} \vee \alpha_{0,1} = 1_{\operatorname{Part}(A)}, \qquad \alpha_{0,0} \wedge \alpha_{0,1} = 0_{\operatorname{Part}(A)}, \tag{4.2}$$

$$\alpha_{1,i} \wedge \big(\alpha_{1,1-i} \vee \operatorname{pt}(u_0, u_1)\big) = 0_{\operatorname{Part}(A)} \qquad \text{for } i \in \{0,1\}, \text{ and} \tag{4.3}$$

$$\alpha_{1,0} \vee \alpha_{1,1} \vee \operatorname{pt}(u_0, u_1) = 1_{\operatorname{Part}(A)}. \tag{4.4}$$

With the vector $\vec{\alpha} := (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$, we often denote $\mathfrak{A}$ also by $(A; \vec{\alpha}; u_0, u_1)$. The vector $\vec{\alpha}$, the set $\{\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1}\}$, its block count *type, and* A *are called the* partition vector*, the* partition set*, the* block count type*, and the* base set *of* $\mathfrak{A}$*, respectively.*

By definition, the base sets of eligible systems are finite. The following lemma benefits from (2.3).

Lemma 2. *Let* $\mathfrak{A} = (A; \alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1}; u_0, u_1)$ *be an eligible system, and let* $k \in \{0,1\}$*. Let* a' *be an element outside* A*, and let* $A' := A \cup \{a'\}$*. For* $i \in \{0,1\}$*, we define*

$$\alpha'_{0,i} := \alpha_{1,i} \vee \mathrm{pt}(u_i, a') \in \mathrm{Part}(A') \quad \text{and} \quad \alpha'_{1,i} := \alpha_{0,i} \in \mathrm{Part}(A'), \tag{4.5}$$

and let $u'_k := u_k$ *and* $u'_{1-k} = a'$*. Then*

$$\mathfrak{A}' = (A'; \alpha'_{0,0}, \alpha'_{0,1}, \alpha'_{1,0}, \alpha'_{1,1}; u'_0, u'_1)$$

is also an eligible system.

Proof of Lemma 2. Let S denote the sublattice of $\mathrm{Part}(A')$ generated by $\{\alpha'_{i,j} : i, j \in \{0,1\}\}$. Then (4.2) applied to $\mathrm{Part}(A)$ and the fact that $\mathrm{Part}(A)$ is a sublattice of $\mathrm{Part}(A')$ yield that

$$1_{\mathrm{Part}(A)} = \alpha_{0,0} \vee \alpha_{0,1} = \alpha'_{1,0} \vee \alpha'_{1,1} \in S. \tag{4.6}$$

Hence, using Definition 1, we obtain that $\alpha_{i,j} = 1_{\mathrm{Part}(A)} \wedge \alpha'_{1-i,j} \in S$ for all $i, j \in \{0,1\}$. Thus, (4.1) implies that $\mathrm{Part}(A) \subseteq S$; in particular, $\mathrm{pt}(u_0, u_1) \in S$. For $i \in \{0,1\}$, we claim that

$$\mathrm{pt}(u_i, a') = \alpha'_{0,i} \wedge \big(\alpha'_{0,1-i} \vee \mathrm{pt}(u_0, u_1)\big) \in S. \tag{4.7}$$

It suffices to deal with the equality in (4.7). For $i \in \{0,1\}$, let $U_i \subseteq A$ be the (unique) $\alpha_{1,i}$-block of u_i; see Figure 1. (Note that $|U_i| = 1$ is not excluded.) By Definition 1 and (4.5), $U'_i := U_i \cup \{a'\}$ is the $\alpha'_{0,i}$-block of u_i; see the figure. We claim that $U_0 \cap U_1 = \emptyset$. Suppose the contrary, and let $x \in U_0 \cap U_1$. Then $(x, u_i) \in \alpha_{1,i} \wedge \big(\alpha_{1,1-i} \vee \mathrm{pt}(u_0, u_1)\big)$, and so (4.3) yields that $x = u_i$ for both $i \in \{0,1\}$. This contradicts that $u_0 \neq u_1$, and we conclude that $U_0 \cap U_1 = \emptyset$. Thus, the figure visualizes the relation between U_0 and U_1 correctly, and so (4.7) follows by Definition 1.

Next, the inclusion $\mathrm{Part}(A) \subseteq S$, (4.7), and Lemma 1 imply that $S = \mathrm{Part}(A')$, that is, $\mathfrak{A}'$ satisfies (4.1). Let $i \in \{0,1\}$. As (4.3) holds for $\mathfrak{A}$, $\alpha_{1,0} \wedge \alpha_{1,1} = 0_{\mathrm{Part}(A)}$. Since the blocks of $\alpha'_{0,i}$ are those of $\alpha_{1,i}$ except that U'_i replaces U_i, the just-mentioned equality, the already established $U_0 \cap U_1 = \emptyset$, and Definition 1 imply that the second half of (4.2) holds for $\mathfrak{A}'$. The first half of (4.2) follows similarly from $\{u_0, u_1\} \subseteq U'_0 \cup U'_1$ and the property (4.4) of $\mathfrak{A}$. The blocks of $\alpha'_{1,i}$ are those of $\alpha_{0,i}$ and the singleton block $\{a'\}$. Hence, the property (4.2) of $\mathfrak{A}$ and Definition 1 imply that $\mathfrak{A}'$ satisfies (4.3). Similarly, as every block of $\alpha_{0,i}$ is a block of $\alpha'_{1,i}$, (4.4) for $\mathfrak{A}'$ follows from the property (4.2) of $\mathfrak{A}$, completing the proof of Lemma 2. $\square$

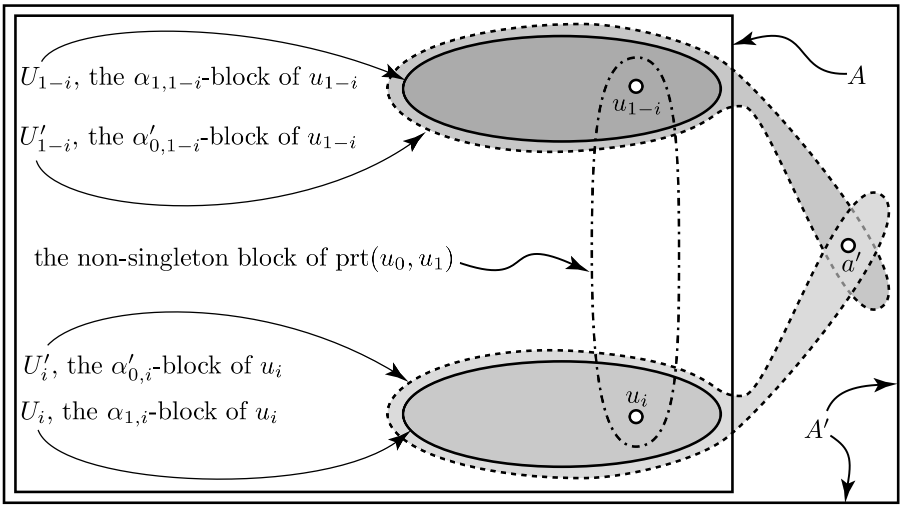

Figure 1. Illustrating the proof of the equality in (4.7)

Lemma 3. *Assume that the base set of an eligible system $\mathfrak{A}'$ has at least three elements. Then there exists at most one eligible system $\mathfrak{A}$ and at most one $k \in \{0, 1\}$ such that $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ in the way described by Lemma 2.*

Proof. Assume that $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ and the notations used in Lemma 2 are in effect. It follows from (4.6) and the sentence right after (4.6) that $\mathfrak{A}'$ determines $1_{\mathrm{Part}(A)}$ and the $\alpha_{i,j}$s. As $1_{\mathrm{Part}(A)}$ dSuppose the contraryetermines A and a', so does $\mathfrak{A}'$. Finally, k is determined by the condition that $u'_k \in A$. □

5. Twenty more lemmas

The possible triplets of $(i_2, i_3, i_4) \in \mathbb{N}^3$ with $i_2 \le i_3 \le i_4 \le 2$ are the following:

$$\begin{aligned} &(0,0,0),\ (0,0,1),\ (0,0,2),\ (0,1,1),\ (0,1,2),\\ &(0,2,2),\ (1,1,1),\ (1,1,2),\ (1,2,2),\ (2,2,2). \end{aligned} \tag{5.1}$$

The corresponding cases for the "smallest" possible even values and odd values of n will be taken care of by consecutive pairs of the following twenty lemmas; their order corresponds to (5.1). Here "smallest" means that "the smallest we have found and probably the smallest". In some cases, simple arguments show that "smallest" is indeed the smallest, but we do not include these arguments in the paper. The twenty proofs are so similar that reading all of them would be boring; furthermore, space considerations do not allow us to include all of them in the journal version of the paper. Hence, only one of the twenty lemmas is proved in the present section. The remaining ones are proved in the Appendix of the *extended version* of the paper; see https://tinyurl.com/czg-4gw2 or https://www.arxiv.org/. Note that the first two lemmas out of the twenty could be replaced by similar lemmas occurring in the already-mentioned preprint https://tinyurl.com/czg-h4gen. The components of $\vec{\alpha}$ will be displayed so that the $\alpha_{0,i}$s are listed from northwest to southeast and the $\alpha_{1,i}$s from northeast to southwest.

Lemma 4. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(14; 37; 56), \qquad \alpha_{1,0} = \mathrm{pt}(15; 23; 46),$$
$$\alpha_{1,1} = \mathrm{pt}(12; 367), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(26; 457).$$

Then $([7]; \vec{\alpha}; 1, 4)$ *is an eligible system with block count type* $(0, 0, 0, 0)$.

Lemma 5. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(168; 237), \qquad \alpha_{1,0} = \mathrm{pt}(178; 345),$$
$$\alpha_{1,1} = \mathrm{pt}(12; 467; 58), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(135; 26; 47).$$

Then $([8]; \vec{\alpha}; 2, 3)$ *is an eligible system with block count type* $(0, 0, 0, 0)$.

Lemma 6. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(16; 234), \qquad \alpha_{1,0} = \mathrm{pt}(12; 45),$$
$$\alpha_{1,1} = \mathrm{pt}(134; 56), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(14; 26; 35).$$

Then $([6]; \vec{\alpha}; 2, 6)$ *is an eligible system with block count type* $(0, 0, 0, 1)$.

Lemma 7. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(146; 27; 35), \qquad \alpha_{1,0} = \mathrm{pt}(26; 34; 57),$$
$$\alpha_{1,1} = \mathrm{pt}(15; 247; 36), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(123; 47; 56).$$

Then $([7]; \vec{\alpha}; 1, 3)$ *is an eligible system with block count type* $(0, 0, 0, 1)$.

Lemma 8. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(123; 45), \qquad \alpha_{1,0} = \mathrm{pt}(35),$$
$$\alpha_{1,1} = \mathrm{pt}(15; 246), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(14; 25; 36).$$

Then $([6]; \vec{\alpha}; 1, 2)$ *is an eligible system with block count type* $(0, 0, 0, 2)$.

Lemma 9. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(12; 37; 456), \qquad \alpha_{1,0} = \mathrm{pt}(13; 67),$$
$$\alpha_{1,1} = \mathrm{pt}(156; 23; 47), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(157; 234).$$

Then $([7]; \vec{\alpha}; 2, 4)$ *is an eligible system with block count type* $(0, 0, 0, 2)$.

Lemma 10. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(12;34;56), \qquad \alpha_{1,0} = \mathrm{pt}(13;26),$$
$$\alpha_{1,1} = \mathrm{pt}(24;56), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(146;35).$$

Then $([6];\vec{\alpha};1,2)$ *is an eligible system with block count type* $(0,0,1,1)$.

Lemma 11. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(124;37;56), \qquad \alpha_{1,0} = \mathrm{pt}(237;46),$$
$$\alpha_{1,1} = \mathrm{pt}(256;34), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(13;25;467).$$

Then $([7];\vec{\alpha};1,2)$ *is an eligible system with block count type* $(0,0,1,1)$.

Lemma 12. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(15;234;67), \qquad \alpha_{1,0} = \mathrm{pt}(36;45),$$
$$\alpha_{1,1} = \mathrm{pt}(12;47;56), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(126;35;47).$$

Then $([7];\vec{\alpha};1,3)$ *is an eligible system with block count type* $(0,0,1,2)$.

Lemma 13. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(138;246;57), \qquad \alpha_{1,0} = \mathrm{pt}(235;46),$$
$$\alpha_{1,1} = \mathrm{pt}(26;37;458), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(12;356;478).$$

Then $([8];\vec{\alpha};1,2)$ *is an eligible system with block count type* $(0,0,1,2)$.

Lemma 14. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(167;234;58), \qquad \alpha_{1,0} = \mathrm{pt}(12;36;57),$$
$$\alpha_{1,1} = \mathrm{pt}(267;45), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(148;26;357).$$

Then $([8];\vec{\alpha};1,8)$ *is an eligible system with block count type* $(0,0,2,2)$.

Lemma 15. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(125;346;789), \qquad \alpha_{1,0} = \mathrm{pt}(267;34;89),$$
$$\alpha_{1,1} = \mathrm{pt}(158;239), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(147;238;569).$$

Then $([9];\vec{\alpha};1,4)$ *is an eligible system with block count type* $(0,0,2,2)$.

Lemma 16. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(26;35), \qquad \alpha_{1,0} = \mathrm{pt}(15;24),$$
$$\alpha_{1,1} = \mathrm{pt}(23;45), \ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(12;346).$$

Then $([6];\vec{\alpha};1,6)$ *is an eligible system with block count type* $(0,1,1,1)$.

Lemma 17. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(145;36), \qquad \alpha_{1,0} = \mathrm{pt}(16;245),$$
$$\alpha_{1,1} = \mathrm{pt}(17;26;35), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(13;257;46).$$

Then $([7];\vec{\alpha};1,3)$ *is an eligible system with block count type* $(0,1,1,1)$.

Lemma 18. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(16;24;35), \qquad \alpha_{1,0} = \mathrm{pt}(14;35),$$
$$\alpha_{1,1} = \mathrm{pt}(16;23;45), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(125;346).$$

Then $([6];\vec{\alpha};1,2)$ *is an eligible system with block count type* $(0,1,1,2)$.

Lemma 19. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(36;45), \qquad \alpha_{1,0} = \mathrm{pt}(126;57),$$
$$\alpha_{1,1} = \mathrm{pt}(17;24;35), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(15;23;467).$$

Then $([7];\vec{\alpha};2,3)$ *is an eligible system with block count type* $(0,1,1,2)$.

Lemma 20. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(16;45), \qquad \alpha_{1,0} = \mathrm{pt}(16;24),$$
$$\alpha_{1,1} = \mathrm{pt}(12;36;45), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(134;256).$$

Then $([6];\vec{\alpha};3,4)$ *is an eligible system with block count type* $(0,1,2,2)$.

Lemma 21. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(13;57), \qquad \alpha_{1,0} = \mathrm{pt}(12;34),$$
$$\alpha_{1,1} = \mathrm{pt}(156;47), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(17;236;45).$$

Then $([7];\vec{\alpha};1,3)$ *is an eligible system with block count type* $(0,1,2,2)$.

Lemma 22. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(12;36), \qquad \alpha_{1,0} = \mathrm{pt}(13;46),$$
$$\alpha_{1,1} = \mathrm{pt}(14;56), \text{ and } \qquad \alpha_{0,1} = \mathrm{pt}(16;2345).$$

Then $([6];\vec{\alpha};1,2)$ *is an eligible system with block count type* $(0,2,2,2)$.

Proof of Lemma 22. It is easy to see that (4.2)–(4.4) hold; so we present an argument only for (4.1). That is, we show that $\{\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1}\}$ generates Part(6). Let S denote the sublattice generated by this four-element subset of Part(6). Then the following partitions are all in S:

$$\alpha_{0,0} = \mathrm{pt}(12;36), \text{ as it is one of the generators,} \tag{5.2}$$

$$\alpha_{1,0} = \mathrm{pt}(13;46),\ \text{as it is one of the generators,} \tag{5.3}$$
$$\alpha_{1,1} = \mathrm{pt}(14;56),\ \text{as it is one of the generators,} \tag{5.4}$$
$$\alpha_{0,1} = \mathrm{pt}(16;2345),\ \text{as it is one of the generators,} \tag{5.5}$$
$$\mathrm{pt}(12346) = \mathrm{pt}(12;36) \vee \mathrm{pt}(13;46) \text{ by (5.2) and (5.3),} \tag{5.6}$$
$$\mathrm{pt}(124;356) = \mathrm{pt}(12;36) \vee \mathrm{pt}(14;56) \text{ by (5.2) and (5.4),} \tag{5.7}$$
$$\mathrm{pt}(13456) = \mathrm{pt}(13;46) \vee \mathrm{pt}(14;56) \text{ by (5.3) and (5.4),} \tag{5.8}$$
$$\mathrm{pt}(36) = \mathrm{pt}(12;36) \wedge \mathrm{pt}(13456) \text{ by (5.2) and (5.8),} \tag{5.9}$$
$$\mathrm{pt}(14) = \mathrm{pt}(14;56) \wedge \mathrm{pt}(12346) \text{ by (5.4) and (5.6),} \tag{5.10}$$
$$\mathrm{pt}(24;35) = \mathrm{pt}(16;2345) \wedge \mathrm{pt}(124;356) \text{ by (5.5) and (5.7),} \tag{5.11}$$
$$\mathrm{pt}(24;356) = \mathrm{pt}(36) \vee \mathrm{pt}(24;35) \text{ by (5.9) and (5.11),} \tag{5.12}$$
$$\mathrm{pt}(124;35) = \mathrm{pt}(14) \vee \mathrm{pt}(24;35) \text{ by (5.10) and (5.11),} \tag{5.13}$$
$$\mathrm{pt}(12) = \mathrm{pt}(12;36) \wedge \mathrm{pt}(124;35) \text{ by (5.2) and (5.13),} \tag{5.14}$$
$$\mathrm{pt}(56) = \mathrm{pt}(14;56) \wedge \mathrm{pt}(24;356) \text{ by (5.4) and (5.12),} \tag{5.15}$$
$$\mathrm{pt}(123;46) = \mathrm{pt}(13;46) \vee \mathrm{pt}(12) \text{ by (5.3) and (5.14),} \tag{5.16}$$
$$\mathrm{pt}(13;456) = \mathrm{pt}(13;46) \vee \mathrm{pt}(56) \text{ by (5.3) and (5.15),} \tag{5.17}$$
$$\mathrm{pt}(23) = \mathrm{pt}(16;2345) \wedge \mathrm{pt}(123;46) \text{ by (5.5) and (5.16),} \tag{5.18}$$
$$\mathrm{pt}(45) = \mathrm{pt}(16;2345) \wedge \mathrm{pt}(13;456) \text{ by (5.5) and (5.17).} \tag{5.19}$$

In particular, $\mathrm{pt}(14) \in S$ by (5.10), $\mathrm{pt}(45) \in S$ by (5.19), $\mathrm{pt}(56) \in S$ by (5.15), $\mathrm{pt}(63) \in S$ by (5.9), $\mathrm{pt}(32) \in S$ by (5.18), and $\mathrm{pt}(21) \in S$ by (5.14). Consequently, Lemma 1 completes the proof. □

Lemma 23. *Let* $\vec{\alpha} = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ *be given by*

$$\alpha_{0,0} = \mathrm{pt}(134;2567), \qquad \alpha_{1,0} = \mathrm{pt}(14;36;57),$$
$$\alpha_{1,1} = \mathrm{pt}(127;56),\ \textit{and} \qquad \alpha_{0,1} = \mathrm{pt}(15;24;37).$$

Then $([7];\vec{\alpha};1,3)$ *is an eligible system with block count type* $(0,2,2,2)$.

To conclude this section, note the following. The proof of Lemma 22 needed fourteen equations, (5.6)–(5.19). The proof of Lemma 14 needs forty-eight. The number of equations that the proof of any other lemma in this section needs is (strictly) between 14 and 48; the average is 26.5.

6. The rest of the proof of Theorem 1

Using our lemmas, now we can prove the theorem.

Proof of Theorem 1. Assume that $(A;\vec{\alpha};u_0,u_1)$ is an eligible system, a' and a'' are distinct elements outside A, $A' := A \cup \{a'\}$, and $A'' := A' \cup \{a''\}$. Let $(A';\vec{\alpha}';u'_0,u'_1)$ and $(A'';\vec{\alpha}'';u''_0,u''_1)$ be the eligible systems obtained from

$(A;\vec{\alpha};u_0,u_1)$ and $(A';\vec{\alpha}';u_0,u_1)$ applying Lemma 2, respectively. (Their dependence on the parameter k occurring in the lemma is irrelevant for a while.) For the $\alpha'_{i,j}$s in (4.5), we have that $\text{nbl}(\alpha'_{0,j}) = \text{nbl}(\alpha_{1,j})$ and $\text{nbl}(\alpha'_{1,j}) = \text{nbl}(\alpha_{0,j}) + 1$ for $j \in \{0,1\}$. Applying (4.5) to the primed αs, we obtain that $\text{nbl}(\alpha''_{i,j}) = \text{nbl}(\alpha_{i,j}) + 1$ for all $i,j \in \{0,1\}$. Therefore,

$$|A''| = |A| + 2 \text{ and } \text{bctyp}(A'';\vec{\alpha}'';u''_0,u''_1) = \text{bctyp}(A;\vec{\alpha};u_0,u_1). \tag{6.1}$$

For the rest of the proof, we fix a possible triplet (i_2,i_3,i_4) in the scope of the theorem. Lemmas 4–23, (5.1), and (6.1) yield two eligible systems

$$\mathfrak{A}_0 = ([8];\vec{\alpha};u_0,u_1) \text{ and } \mathfrak{B}_0 = ([9];\vec{\alpha}^*;u_0^*,u_1^*)$$

of block count type $(0,i_2,i_3,i_4)$. Depending on the parity of n, we start from $\mathfrak{A}$ or $\mathfrak{B}$ depending on whether n is even or odd, respectively. The repeated use of (6.1) gives that for any $n \geq 8$, $\text{Part}(n)$ has a four-element generating set X such that $\text{bctyp}(X) = (0,i_2,i_3,i_4)$. More effort is needed to prove that there are *many* such X.

Let $m := 2\lfloor (n-8)/2 \rfloor$. Observe that $m = n-8$ for n even and $m = n-9$ for n odd. Importantly, m is even. We will give the details on how to use $\mathfrak{A}_0$ for an even n, since $\mathfrak{B}_0$ could be used similarly for an odd n. We are going to construct $2^m \cdot m!$ eligible systems such that each of them is obtained from $\mathfrak{A}_0$ by using the constructive step offered by Lemma 2 m times and it has $[n]$ as its base set.

So $n \geq 10$ is even. Pick an m-dimensional vector $\vec{k} = (k_1,\dots,k_m)$ in $\{0,1\}^m$. Let $\vec{b} = (b_1,\dots,b_m)$ be a permutation of the set $[n] \setminus [8] = \{9,10,\dots,n\}$. So $[n] = [8] \cup \{(b_1,\dots,b_m\}$. Using k_1, b_1, and the (parenthesized) superscript 1 instead of k, a', and the prime symbol $'$, respectively, Lemma 2 yields an eligible system $\mathfrak{A}_1 = ([8] \cup \{b_1\};\vec{\alpha}^{(1)};u_0^{(1)},u_1^{(1)})$. In the next step, we use k_2, b_2, and the parenthesized 2. And so on; we use k_i, b_i, and (i) in the ith step to obtain $\mathfrak{A}_i = ([8] \cup \{b_1,\dots,b_i\};\vec{\alpha}^{(i)};u_0^{(i)},u_1^{(i)})$ from $\mathfrak{A}_{i-1}$. The base set of $\mathfrak{A}_m$ is $[n]$. Since we have made an even number of steps to obtain $\mathfrak{A}_m$ from $\mathfrak{A}_0$, Lemma 2 and (6.1) imply that the partition set of $\mathfrak{A}_m$ is a generating set of $\text{Part}(n)$ of block count type $(0,i_2,i_3,i_4)$. There are $2^m \cdot m!$ vectors $(\vec{k},\vec{b})$. So we can construct $2^m \cdot m!$ eligible systems in this way; call them the *constructed systems*. To show that they are pairwise distinct, it is sufficient to show that $\mathfrak{A}_m$ determines both $\vec{k}$ and $\vec{b}$.

To do so, assume that $\mathfrak{A}_m$ is given, and let B_i denote the base set of $\mathfrak{A}_i$ for $i \in \{0,\dots,m\}$; in particular, $B_0 = [8]$ and $B_m = [n]$. By Lemma 3, $\mathfrak{A}_{m-1}$ and k_m are uniquely determined. Applying Lemma 3 to $\mathfrak{A}_{m-2}$ and $\mathfrak{A}_{m-1}$, we obtain that $\mathfrak{A}_{m-2}$ and k_{m-1} are uniquely determined, too. Next, the same lemma applied to $\mathfrak{A}_{m-3}$ and $\mathfrak{A}_{m-2}$ yields that $\mathfrak{A}_{m-3}$ and k_{m-2} are uniquely determined. And so on; after m applications of Lemma 3, we obtain that $\vec{k}$ and all the $\mathfrak{A}_i$, $i \in \{0,\dots,m\}$, are uniquely determined. For

$i \in [m]$, b_i is the unique element that belongs to (the base set of) $\mathfrak{A}_i$ but not to $\mathfrak{A}_{i-1}$. Hence, $\vec{b}$ is uniquely determined, too.

Next, we give an upper estimate of how many constructed systems $\mathfrak{A}_m$ give rise to the same generating set. First, $24 = 4!$ different generating vectors give the same four-element generating set. Second, we claim that $(u_0^{(m)}, u_1^{(m)})$ can be chosen in at most $m(m+1)$ ways. (We have added "at most" since the generating set can exclude some choices.) Indeed, there are (at most) $m(m-1)$ pairs $(u_0^{(m)}, u_1^{(m)})$ such that none of their components is in [8]. If $u_0^{(m)} \in [8]$, then $u_0^{(m)} = u_0$ and we can choose $u_1^{(m)}$ in (at most) m ways, and similarly if $u_1^{(m)} \in [8]$. So the number of possible pairs $(u_0^{(m)}, (u_1^{(m)})$ is at most $m(m-1) + m + m = m(m+1)$, indeed.

Finally, if we divide the number $2^m \cdot m!$ of the constructed systems by the just-obtained number $24m(m+1)$, then we obtain a lower estimate of the four-element generating sets of $\mathrm{Part}(n)$ with block count type $(0, i_2, i_3, i_4)$. Since this division results in the number given in (3.1), the proof of Theorem 1 is complete. □

7. Conclusion

We have discovered many new four-element generating sets of finite partition lattices. These generating sets have specific properties; see Definition 3 and Theorem 1. According to the statistical analysis presented in [4], it is highly probable that there are many more four-element generating sets of finite partition lattices than those presented in this paper and other papers. Therefore, it would be interesting to continue this research to find many additional four-element generating sets. In particular, we conjecture, though cannot currently prove, that the lower bound given in (3.1), which is based only on the number of four-element generating sets we have constructed, is far from being sharp. By exploring more four-element generating sets, we could increase the likelihood that (the extensions of) these sets will be applicable in cryptography. Another future task is to extend the corresponding ideas given in [2] and [3] to meet the requirements of modern cryptography.

References

1. Ahmed D., Czédli G. (1+1+2)-generated lattices of quasiorders. *Acta Sci. Math. (Szeged)*, 2021, vol, 87, pp. 415–427. https://doi.org/10.14232/actasm-021-303-1
2. Czédli G. Four-generated direct powers of partition lattices and authentication. *Publicationes Mathematicae (Debrecen)*, 2021, vol. 99, pp. 447–472. https://doi.org/10.5486/PMD.2021.9024

3. Czédli G. Generating Boolean lattices by few elements and exchanging session keys. *Novi Sad Journal of Mathematics.* https://doi.org/10.30755/NSJOM.16637
4. Czédli G., Oluoch L. Four-element generating sets of partition lattices and their direct products. *Acta Sci. Math. (Szeged)*, 2020, vol. 86, pp. 405–448. https://doi.org/10.14232/actasm-020-126-7
5. Kulin J. Quasiorder lattices are five-generated. *Discuss. Math. Gen. Algebra Appl.,* 2016, vol. 36, pp. 59–70.
6. Strietz H. Finite partition lattices are four-generated. *Proc. Lattice Th. Conf. Ulm,* 1975, pp. 257–259.
7. Zádori L. Generation of finite partition lattices. *Lectures in universal algebra: Proc. Colloq. Szeged, 1983. Colloq. Math. Soc. János Bolyai*, vol. 43, Amsterdam, North-Holland Publishing, 1986, pp. 573–586.

Об авторах

Цедли Габор, д-р физ.-мат. наук, почетный проф., Сегедский университет, Институт Бойяи, Сегед, Венгрия, czedli@math.u-szeged.hu, https://orcid.org/0000-0001-9990-3573

About the authors

Gábor Czédli, Dr. Sci.(Phys.-Math.), Emeritus Prof., University of Szeged, Bolyai Institute, Szeged, Hungary, czedli@math.u-szeged.hu, https://orcid.org/0000-0001-9990-3573

Поступила в редакцию / Received 10.10.2024
Поступила после рецензирования / Revised 18.11.2024
Принята к публикации / Accepted 19.11.2024