MINIMUM-SIZED GENERATING SETS OF THE DIRECT POWERS OF FREE DISTRIBUTIVE LATTICES

GÁBOR CZÉDLI

Dedicated to the memory of George F. McNulty

ABSTRACT. For a finite lattice L, let $\mathrm{Gm}(L)$ denote the least n such that L can be generated by n elements. For integers $r > 2$ and $k > 1$, denote by $\mathrm{FD}(r)^k$ the k-th direct power of the free distributive lattice $\mathrm{FD}(r)$ on r generators. We determine $\mathrm{Gm}(\mathrm{FD}(r)^k)$ for many pairs (r, k) either exactly or with good accuracy by giving a lower estimate that becomes an upper estimate if we increase it by 1. For example, for $(r, k) = (5, 25\,000)$ and $(r, k) = (20,\ 1.489 \cdot 10^{1789})$, $\mathrm{Gm}(\mathrm{FD}(r)^k)$ is 300 and 6000, respectively. To reach our goal, we give estimates for the maximum number of pairwise unrelated copies of some specific posets (called full segment posets) in the subset lattice of an n-element set. In addition to analogous earlier results in lattice theory, a connection with cryptology is also mentioned among the motivations.

1. INTRODUCTION

This work belongs mainly to *lattice theory* but it also belongs to *extremal combinatorics*. The paper is more or less self-contained; those familiar with M.Sc. level mathematics and the concept of distributive lattices can read it easily.

The search for small generating sets has belonged to lattice theory for long; for example, in chronological order, see Gelfand and Ponomarev [9], Strietz [17], Zádori [19, 20], Chajda and Czédli [2], Takách [18], Kulin [13], Czédli and Oluoch [7], and Ahmed and Czédli [1]. See also the surveying parts and the bibliographic sections in [1] and Czédli [3] for further references. If a large lattice L can be generated by few elements, then this lattice has many small generating sets. Czédli [3] and [5] have recently observed that these lattices can be used for cryptography; for a further note on this topic, see Remark 5.3. This fact and the results on small generating sets of lattices in the above-mentioned and some additional papers constitute the *lattice theoretic motivation* of the paper.

There is a *motivation* coming from *extremal combinatorics*, too. The first result on the maximum number $\mathrm{Sp}(U, n)$ of pairwise unrelated (in other words, incomparable) copies of a poset U in the powerset lattice of an n-element finite set was published by Sperner [16] ninety-five years ago. While U is the singleton poset in Sperner's theorem, the *Sperner theorem* (that is, the Sperner *type* theorem) in Griggs, Stahl, and Trotter [11] determines $\mathrm{Sp}(U, n)$ for any finite chain U. For some other finite posets, similar results were obtained by Katona and Nagy [12]

1991 *Mathematics Subject Classification.* Primary 06D99, secondary 05D05.

Key words and phrases. Free distributive lattice, minimum-sized generating set, small generating set, direct power, Sperner theorem, 3-crown poset, cryptography.

This research was supported by the National Research, Development and Innovation Fund of Hungary, under funding scheme K 138892. **November 8, 2023**.

and Czédli [6]. In general, the exact value of $\mathrm{Sp}(U,n)$ is rarely known. On the other hand, Katona and Nagy [12] and, independently from them, Dove and Griggs [8] determined the *asymptotic* value of $\mathrm{Sp}(U,n)$. Their celebrated result asserts that for any finite poset U,

$$\mathrm{Sp}(U,n) \sim \frac{1}{|U|}\binom{n}{\lfloor n/2\rfloor}, \text{ that is, } \lim_{n\to\infty}\frac{1}{|U|}\binom{n}{\lfloor n/2\rfloor}\cdot \mathrm{Sp}(U,n)^{-1}=1. \tag{1.1}$$

By the main result of [6], the lattice theoretic motivation and the combinatorial one are strongly connected; see (2.4) later, which we are going to quote from [6]. Here we only mention that in order to get closer to what the title of the paper promises, we need to determine $\mathrm{Sp}(U,n)$ for some rather special posets U.

The asymptotic result (1.1) may suggest that for our special posets U, we can obtain $\mathrm{Sp}(U,n)$ or at least some of its estimates simply by copying what Dove and Griggs [8] or Katona and Nagy [12] did. However, we have three reasons not to follow this plan. First, while several constructions and considerations can lead to the asymptotically same result, we cannot expect a similar experience when dealing with small values of n. Furthermore, concrete (non-asymptotic) calculations and considerations are often harder and their asymptotic counterparts do not offer too much help. For example, while we know for any fixed $a,b\in\mathbb{Z}$ (the set of integers) that, with our vertical-space-saving permanent notation $f_{\mathrm{Sp}}(n) := \binom{n}{\lfloor n/2\rfloor}$,

$$\binom{n+a}{\lfloor n/2\rfloor+b} \sim 2^a\cdot\binom{n}{\lfloor n/2\rfloor} = 2^a f_{\mathrm{Sp}}(n) \quad \text{as } n\to\infty \tag{1.2}$$

and so we can simply work with $2^a f_{\mathrm{Sp}}(n)$ in asymptotic considerations, we have to work with $\binom{n+a}{\lfloor n/2\rfloor+b}$ in concrete calculations, which is more difficult. (Note at this point that both Dove and Griggs [8] and Katona and Nagy [12] use (1.2).) Second, even though a general construction could be specialized to our particular posets U, we cannot expect to exploit the peculiarities of our U's in this way. Third, an easy-to-read construction with a short and easy argument will hopefully be interesting for the reader, partially because these details are necessary to explain and perform the computations.

Hence, the construction we are going to give for lower estimates is different from those in Dove and Griggs [8] and Katona and Nagy [12]. At some places in the proofs, we are going to point out the difference from [8]; the difference from [12] is clearer. Note that our construction gives better lower estimates for our particular posets U than any of the Dove-Griggs and the Katona-Nagy construction would give, at least for small values of n. (For $n\to\infty$, that is, asymptotically, all the three constructions yield the same lower estimate.) On the other hand, let us emphasize the similarities. While many calculations in this paper are new, most of the ideas in our construction occur in Dove and Griggs [8] and Katona and Nagy [12]; more details will be mentioned right after the proof of Proposition 3.2.

Even though our result allows a big gap between the lower estimate and the upper estimate of $\mathrm{Sp}(U,n)$, this result will suffice to determine the least number n of elements that generate the direct powers $\mathrm{FD}(3)^k$ of $\mathrm{FD}(3)$ with quite a good accuracy, and we can give reasonable estimates on n in case of $\mathrm{FD}(r)^k$.

FIGURE 1. FD(3) and the 3-crown $W_3 = \mathrm{FSP}(3,0,3) \cong \mathrm{J}(\mathrm{FD}(3))$

2. Basic facts and notations

Except for $\mathbb{N}^+ := \{1,2,3,\dots\}$, $\mathbb{N}_0 := \{0\} \cup \mathbb{N}^+$, $\mathbb{N}^{\geq 3} := \{3,4,5,\dots\} = \mathbb{N}^+ \setminus \{1,2\}$ and their subsets, all sets and structures in the paper will be assumed to be *finite*. (Sometimes, we repeat this convention for those who read only a part of the paper.) For $r \in \mathbb{N}^{\geq 3}$, the *free distributive lattice on r generators* is denoted by $\mathrm{FD}(r)$; for $r = 3$, it is drawn on the left of Figure 1. A lattice element with exactly one lower cover is called *join-irreducible*. For a lattice L, the *poset* (that is, the *partially ordered set*) of the join-irreducible elements of L is denoted by $\mathrm{J}(L)$. For $L = \mathrm{FD}(3)$, $\mathrm{J}(L)$ consists of the black-filled elements and it is also drawn separately on the right of the figure. For a set H, the *powerset lattice* of H is $(\{Y : Y \subseteq H\}; \cup, \cap)$; it (or its support set) is denoted by $\mathrm{Pow}(H)$. For $n \in \mathbb{N}_0$, the set $\{1,2,\dots,n\}$ is denoted by $[n]$; note that $[0] = \emptyset$. For x, y in a poset, in particular, for $x, y \in \mathrm{Pow}([n])$, we write $x \parallel y$ to denote that neither $x \leq y$ nor $y \leq x$ holds; in $\mathrm{Pow}([n])$, "$\leq$" is "$\subseteq$". For a poset U, a *copy* of U in $\mathrm{Pow}([n])$ is a subset of $\mathrm{Pow}([n])$ that, equipped with "$\subseteq$", is order isomorphic to U. Two copies of U in $\mathrm{Pow}([n])$ are *unrelated* if for all X in the first copy and all Y in the second copy, $X \parallel Y$. Let us repeat that for $n \in \mathbb{N}_0$ and a poset U, we let

$$\begin{aligned}\mathrm{Sp}(U,n) := \max\{k : \text{there exist } k \text{ pairwise} \\ \text{unrelated copies of } U \text{ in } \mathrm{Pow}([n])\}.\end{aligned} \tag{2.1}$$

According to the sentence containing (1.2), we often write $\mathrm{C_b}(n,k)$ instead of $\binom{n}{k}$; especially in text environment and if n or k are complicated or subscripted expressions. The notation "$\mathrm{Sp}(-,-)$" and "$\mathrm{C_b}(-,-)$" come from Sperner and binomial coefficient, respectively. As usual, $\lfloor\ \rfloor$ and $\lceil\ \rceil$ denote the lower and upper *integer part* functions; for example, $\lfloor 5/3 \rfloor = 1$ and $\lceil 5/3 \rceil = 2$. With our notations, Sperner's theorem [16] asserts that for every $n \in \mathbb{N}_0$,

$$\text{if } U \text{ is the 1-element poset, then } \mathrm{Sp}(U,n) = \binom{n}{\lfloor n/2 \rfloor} =: f_{\mathrm{Sp}}(n). \tag{2.2}$$

Recall that a subset X a lattice $L = (L; \vee, \wedge)$ is a *generating set* of L if for every Y such that $X \subseteq Y \subseteq L$ and Y is closed with respect to $\vee$ and $\wedge$, we have that $Y = L$. We denote the *size of a minimum-sized generating set* of L by

$$\mathrm{Gm}(L) := \min\{|X| : X \text{ is a generating set of } L\}. \tag{2.3}$$

For $k \in \mathbb{N}^+$, the k-th *direct power* L^k of L consists of the k-tuples of elements of L and the lattice operations are performed componentwise. With our notations, the main result of Czédli [6] asserts that

$$\begin{aligned}&\text{for } 2 \leq k \in \mathbb{N}^+ \text{ and a finite distributive lattice } L,\ \mathrm{Gm}(L^k)\\ &\text{is the smallest } n \in \mathbb{N}^+ \text{ such that } k \leq \mathrm{Sp}(\mathrm{J}(L), n).\end{aligned} \tag{2.4}$$

It is also clear from [6] that for each finite distributive lattice L, the functions $k \mapsto \mathrm{Gm}(L^k)$ and $n \mapsto \mathrm{Sp}(\mathrm{J}(L), n)$ mutually determine each other, but we do not need this fact in the present paper. The following definition is crucial in the paper.

Definition 2.1. For $0 \leq a < b \leq r \in \mathbb{N}_0$ such that $a + 2 \leq b$, the *full segment poset* $\mathrm{FSP}(r, a, b)$ is the poset U defined (up to isomorphism) by the conjunction of the following two rules.

(a) r is the smallest integer such that U is embeddable into $\mathrm{Pow}([r])$;
(b) the subposet $\{X \in \mathrm{Pow}([r]) : a < |X| < b\}$ of $\mathrm{Pow}([r])$ is order isomorphic to U.

Even though $0 \leq a$ in Definition 2.1 could be replaced by by $-1 \leq a$, we do not do so since the case $a = -1$ would need a different (in fact, easier) treatment; see [6]. Let U be a finite poset, $s \in \mathbb{N}^+$, and denote $\{s, s+1, s+2, \dots\}$ by $\mathbb{N}^{\geq s}$. If $f_1, f_2 \colon \mathbb{N}^{\geq s} \to \mathbb{N}_0$ are functions such that $f_1(n) \leq \mathrm{Sp}(U, n) \leq f_2(n)$ for all $n \in \mathbb{N}^{\geq s}$, then (f_1, f_2) is a *pair of estimates* of the function $\mathrm{Sp}(U, -)$ on $\mathbb{N}^{\geq s}$; in particular, f_1 is a *lower estimate* while f_2 is an *upper estimate* of $\mathrm{Sp}(U, -)$. A reasonably good property of pairs of estimates of $\mathrm{Sp}(U, -)$ is defined as follows:

$$\begin{aligned}&\text{for } s \in \mathbb{N}^+, \text{ a pair } (f_1, f_2) \text{ of estimates is } \textit{separated}\\ &\text{on } \mathbb{N}^{\geq s} \text{ if } f_2(n) \leq f_1(n+1) \text{ for all } n \in \mathbb{N}^{\geq s}.\end{aligned} \tag{2.5}$$

The following fact is a trivial consequence of (2.4) and for $k \geq 2$, it is implicit in Czédli [6]; see around (5.23) and (5.24) in [6].

Observation 2.2. *Let D be a finite distributive lattice. Denote the poset $\mathrm{J}(D)$ by U, and let $s \in \mathbb{N}^+$. Let (f_1, f_2) be a separated pair of estimates of $\mathrm{Sp}(U, -)$ on $\mathbb{N}^{\geq s}$ such that f_1 (the lower estimate) is strictly increasing on $\mathbb{N}^{\geq s}$. Then, for each $k \in \mathbb{N}^+$ such that $f_1(s) < k$, (f_1, f_2) determines $\mathrm{Gm}(D^k)$, see (2.3), "with accuracy $1/2$" as follows: Letting n be the unique $n \in \mathbb{N}^+$ such that $f_1(n) < k \leq f_1(n+1)$, either $k \leq f_2(n)$ and $\mathrm{Gm}(D^k) \in \{n, n+1\}$ or $f_2(n) < k$ and $\mathrm{Gm}(D^k) = n + 1$.*

The term "accuracy $1/2$" comes from the fact that the distance between the never exact estimate $n + 1/2$ and $\mathrm{Gm}(D^k)$ is always $1/2$.

3. Lower estimates

The easy proof of the following lemma raises the possibility that the lemma might belong to the folklore even though the author has never met it.

Lemma 3.1. *For $2 \leq r \in \mathbb{N}^+$, $\mathrm{J}(\mathrm{FD}(r)) \cong \mathrm{FSP}(r, 0, r)$; see Definition 2.1.*

Proof. Denote by $\{x_1, \dots, x_r\}$ the set of free generators of $\mathrm{FD}(r)$. Call a subset J of $[r]$ *nontrivial* if $\emptyset \neq J \neq [r]$, and let $\mathrm{Pow}_{\mathrm{nt}}([r]) = \bigl(\mathrm{Pow}_{\mathrm{nt}}([r]); \subseteq\bigr)$ stand for the poset formed by the nontrivial subsets of $[r]$. For $J \in \mathrm{Pow}_{\mathrm{nt}}([r])$, let m_J be the meet $\bigwedge_{i \in J} x_i$, and define $X := \{m_J : J \in \mathrm{Pow}_{\mathrm{nt}}([r])\}$. As $X \subseteq \mathrm{FD}(r)$, $X = (X; \leq)$ is a subposet of $\mathrm{FD}(r)$.

First, we show that the map $\varphi\colon \mathrm{Pow}_{\mathrm{nt}}([r]) \to X$ defined by $J \to m_J$ is a dual order isomorphism. The tool wee need is very simple: Since $\mathrm{FD}(r)$ is free, it follows that whenever $J, K \in \mathrm{Pow}_{\mathrm{nt}}([r])$ and $m_J = m_K$, then $m_J(\vec{y}) = m_K(\vec{y})$ for all $\vec{y} = (y_1, \dots, y_r) \in \{0,1\}^r$, and similarly for "$\leq$" instead of "$=$". The implication $J \subseteq K \Rightarrow m_J \geq m_K$ is obvious. For the sake of contradiction, suppose that $m_J \geq m_K$ for some $J, K \in \mathrm{Pow}_{\mathrm{nt}}([r])$ but $J \nsubseteq K$. Pick a $j \in J \setminus K$, and let $\vec{y} \in \{0,1\}^r$ be the vector for which $y_j = 0$ but $y_i = 1$ for all $i \in [r] \setminus \{j\}$. Then $m_K = \vec{y} = 1$ since the j-th component of $\vec{y}$ does not occur in the meet but $m_J = 0$, contradicting $m_J \geq m_K$. This proves that "$\geq$" in X and "$\subseteq$" in $\mathrm{Pow}_{\mathrm{nt}}([r])$ correspond to each other. In particular, φ is a bijective map as the equality of two elements or subsets can be expressed by these relations. Thus, φ is a dual order isomorphism. The composite of φ and the selfdual automorphism of $\mathrm{Pow}_{\mathrm{nt}}([r])$ defined by $J \mapsto [r] \setminus J$ is an order isomorphism, proving that $X \cong \mathrm{FSP}(r, 0, r)$.

Next, to complete the proof, it suffices to show that $\mathrm{J}(\mathrm{FD}(r)) = X$. Using the tool (with $\vec{y}$) mentioned earlier, observe that $1 = x_1 \vee \dots \vee x_r \notin \mathrm{J}(\mathrm{FD}(r))$ and for every $J \in \mathrm{Pow}_{\mathrm{nt}}([r])$, $m_J \notin \{0,1\}$. By distributivity, each element of $\mathrm{FD}(r) \setminus \{0,1\}$ is the join of meets of some generators or, in other words, a disjunctive normal form of the generators. Clearly, neither the empty meet, nor the empty join, nor the meet of all generators is needed here, whereby there is at least one joinand and each of the joinands is of the form m_J with $J \in \mathrm{Pow}_{\mathrm{nt}}([r])$. As one joinand is sufficient for the elements of $\mathrm{J}(\mathrm{FD}(r))$, we obtain that $\mathrm{J}(\mathrm{FD}(r)) \subseteq X$.

To show that converse inclusion by way of contradiction, suppose that $m_J \in X \setminus \mathrm{J}(\mathrm{FD}(r))$. Then m_J is the join of some elements of $\mathrm{J}(\mathrm{FD}(r))$ that are smaller than m_J. These elements are of the form m_{I_j} as $\mathrm{J}(\mathrm{FD}(r)) \subseteq X$. This fact and dual isomorphism proved in the previous paragraph imply that there are $I_1, \dots, I_t \in \mathrm{Pow}_{\mathrm{nt}}([r])$ such that $J \subset I_1$, …, $J \subset I_t$ and $m_J = m_{I_1} \vee \dots \vee m_{I_t}$. This equality holds as an identity in the two-element lattice $\{0,1\}$. However, if we define $\vec{y} \in \{0,1\}^r$ by $y_s := 1$ if $s \in J$ and $y_s = 0$ otherwise, then $m_J(\vec{y}) = 1$ but each of the joinands and so the join are 0. This contradiction completes the proof. □

For $1 \leq a < b \leq r \in \mathbb{N}^+$ such that $a + 2 \leq b$ and $n \in \mathbb{N}^{\geq r}$, $\vec{v}$ will denote a vector $(v_0, \dots, v_a; v_b, \dots, v_r)$, so there is gap in the index set of the components. Let $p \in \{-r, -r+1, \dots, r\}$ be a parameter, and let us agree that a binomial coefficient $\mathrm{C_b}(x_1, x_2)$ is 0 unless $x_1, x_2 \in \mathbb{N}_0$ and $0 \leq x_2 \leq x_1$. With these conventions, define

$$\begin{aligned} f^{(p)}_{r,a,b}(n) := \sum_{i=0}^{\lfloor n/r \rfloor - 1} \sum_{\substack{\vec{v} \in \{0,\dots,i\}^{r+a-b+2} \\ v_0+\dots+v_a+v_b+\dots+v_r = i}} \frac{i!}{v_0! \dots v_a! \cdot v_b! \dots v_r!} \times \\ \times \binom{n-(i+1)r}{p + \lfloor (n-r)/2 \rfloor - 0v_0 - 1v_1 - \dots - av_a - bv_b - \dots - rv_r} \times \\ \times \binom{r}{0}^{v_0} \dots \binom{r}{a}^{v_a} \cdot \binom{r}{b}^{v_b} \dots \binom{r}{r}^{v_r}, \qquad \text{and} \end{aligned} \tag{3.1}$$

$$f_{r,a,b}(n) := \max\{f^{(p)}_{r,a,b}(n) : p \in \{-r, -r+1, \dots, r-1, r\}\}. \tag{3.2}$$

Proposition 3.2. *For $r \in \mathbb{N}^{\geq 3}$ and $0 \leq a < b \leq r \in \mathbb{N}^+$ such that $a + 2 \leq b$, $f_{r,a,b}(n)$ is a lower estimate of $\mathrm{Sp}(\mathrm{FSP}(r,a,b), n)$ on $\mathbb{N}^{\geq r}$.*

The proof below shows that Proposition 3.2 would still hold if we replaced $\{-r, -r+1, \ldots, r-1, r\}$ with $\mathbb{Z}$ but we do not have any example where $\mathbb{Z}$, which would make practical computations longer, is better than $\{-r, -r+1, \ldots, r-1, r\}$.

Proof. It suffices to show that for any $p \in \mathbb{Z}$, $f^{(p)}_{r,a,b}(n) \leq \mathrm{Sp}(\mathrm{FSP}(r,a,b),n)$. Take an n-element set M, and denote the quotient $\lfloor n/r \rfloor$ by q. Fix q pairwise disjoint subsets $M_0, \ldots, M_{q-1}$ of M, we call them *blocks*, and let $M_q := M \setminus (M_0 \cup \cdots \cup M_{q-1})$. Let $h := p + \lfloor (n-r)/2 \rfloor$. For $j \in \{0, \ldots, q-1\}$, a subset X of the block M_j is called *small* if $|X| \leq a$. Similarly, if $|X| \geq b$, then X is *large* while in the remainder case when $a < |X| < b$, we say that X is *medium-sized*. By an *extremal subset* of M_j we mean a subset that is large or small; so "extremal" is the opposite of "medium-sized". For a subset B of M, $B \cap M_i$ is often denoted by B_i. We say that $(i, B) \in \{0, \ldots, q-1\} \times \mathrm{Pow}(M)$ is a *fundamental pair* if

(F1) $|B| = h$, and

(F2) $B_i = \emptyset$ and for each $j \in \{0, \ldots, i-1\}$, B_j is extremal (that is, small or large).

Four examples are given in Figure 2, where $n = 54$, $r = 8$, $a = 3$, $b = 6$, $q = 6$, and $h = 26$. In each of the four parts of this figure, the green-filled solid ovals[1] represent extremal subsets of the appropriate M_j's, $j \in \{0, \ldots, i-1\}$, the red dotted oval is a medium-sized subset of M_i, and there is no condition on the subsets represented by magenta-filled solid ovals. Hence, in each of the four examples, the *set component* (that is, the second component, which was denoted by B) of the fundamental pair is the union of the color-filled solid ovals. The *index component* (that is, the first component) is indicated at the top of the figure. Each color-filled solid oval contains the number of elements of the subset B_j that this oval represents. Note, however, that a red dotted oval (regardless the number it contains) in the picture of (i, B) means that $B_i = \emptyset$. (The red dotted ovals will be explained right after (3.3).) Note also that, witnessed by $i = 5$ and $i = 4$ in the figure, the set component does not determine the index component.

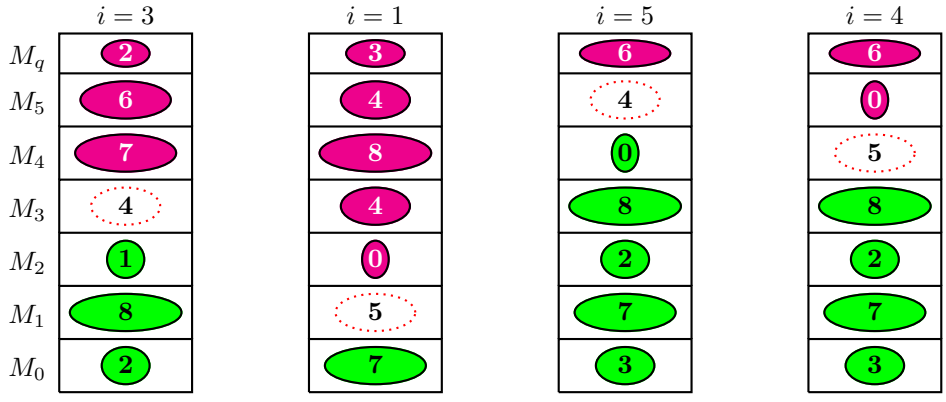

FIGURE 2. Illustrating the proof of Proposition 3.2 with $\mathrm{FSP}(8,3,6)$; $h = 26$, $n = 54$; in each fundamental pair, the set component is the union of the color-filled solid ovals.

[1]Note for a grayscale version: the green-filled ovals contain black numbers in their interiors while the ovals with white numbers are magenta-filled.

For a fundamental pair (i, B), let

$$U(i, B) := \{B \cup X : X \subseteq M_i \text{ and } a < |X| < b\}. \tag{3.3}$$

Clearly, $U(i, B)$ is a copy of $\mathrm{FSP}(r, a, b)$. The role of a red dotted oval in Figure 2 is to represent one of the sets X in (3.3). Now that we have defined our construction, we have to prove that the number of fundemental pairs is $f^{(p)}_{r,a,b}(n)$ and for different fundamental pairs (i, B) and (i', B'), $U(i, B)$ and $U(i', B')$ are unrelated.

To obtain a fundamental pair (i, B), first we choose $i \in \{0, \dots, q-1\}$; this explains the outer summation sign in (3.1). Then for each $j \in \{0, \dots, a, b, \dots, r\}$ we chose the number v_j of the j-element green-filled solid ovals. As there are i green-filled solid ovals, the choice of the vector formed from these v_j's is not quite arbitrary; this explains the subscript of the inner summation sign in (3.1). For example, on the right (that is, in the $i = 4$ part) of Figure 2, $\vec{v} = (v_0, \dots, v_3; v_6, v_7, v_8) = (0, 0, 1, 1; 0, 1, 1)$. The fraction in (3.1) is the multinomial coefficient showing how many ways v_0 zeros, v_1 1's, $\dots$, v_a a's, v_b $b's$, $\dots$, v_r r's can be ordered. On the right of the figure, this is how many ways the numbers 3, 7, 2, 8 can be written below the red dotted oval (the figure shows only one of these ways). As there is no stipulation on the magenta-filled solid ovals, the binomal coefficient in the middle of (3.1) gives the number of possible unions of the magenta-filled solid ovals, that it, it shows how many ways the system of these ovals can be chosen.

For $j \in \{0, \dots, a, b, \dots, r\}$, a j-element subset (green-filled solid oval) of an r-element block M_t can be chosen in $\mathrm{C_b}(r, j)$ ways. As there are v_j such subsets and there are several values of j, the product in the last row of (3.1) is the number how many ways the systems of the green-filled solid ovals can be chosen. Therefore, $f^{(p)}_{r,a,b}(n)$ is the number of fundamental pairs as required.

Next, let $(i, B) \neq (i', B')$ be distinct fundamental pairs, $Y = B \cup X \in U(i, B)$, and $Y' = B' \cup X' \in U(i', B')$. For the sake of contradiction, suppose that $Y \subseteq Y'$. If we had that $i = i'$, then $B = (M \setminus M_i) \cap Y \subseteq (M \setminus M_i) \cap Y' = (M \setminus M_{i'}) \cap Y' = B'$, which together with $|B| = h = |B'|$ would give that $B = B'$ and so $(i, B) = (i', B')$, a contradiction. Hence, $i \neq i'$. Observe that $Y \subseteq Y'$ gives that $M_j \cap Y \subseteq M_j \cap Y'$ for all $j \in \{0, \dots, q\}$. Furthermore, $M_j \cap Y = B_j$ for $j \neq i$ while $M_i \cap Y = X$. Similarly, $M_j \cap Y' = B'_j$ for $j \neq i'$ while $M_{i'} \cap Y' = X'$. Hence, $B_j \subseteq B'_j$ and so $|B_j| \leq |B'_j|$ for $j \in \{0, \dots, q\} \setminus \{i, i'\}$, implying that

$$z := \sum_{j \in \{0,\dots,q\} \setminus \{i,i'\}} |B_j| \leq \sum_{j \in \{0,\dots,q\} \setminus \{i,i'\}} |B'_j| =: z'. \tag{3.4}$$

As X is medium-sized, B'_i is extremal, and $X = M_i \cap Y \subseteq M_i \cap Y' = B'_i$, we have that B'_i is large, that is, $b \leq |B'_i|$. Hence, (3.4) gives that $z' + b \leq z' + |B'_i| = |B'|$. Similarly, X' is medium-sized, $B_{i'}$ is extremal, and $B_{i'} = M_{i'} \cap Y \subseteq M_{i'} \cap Y' = X'$, whence $B_{i'}$ is small, that is, $|B_{i'}| \leq a$. Thus, $|B| = z + |B_{i'}| \leq z + a$. Combining the inequalities $a < b$, $|B| \leq z + a$, $z' + b \leq |B'|$, and (3.4), we obtain that

$$|B| \leq z + a < z + b \leq z' + b \leq |B'|.$$

This strict inequality contradicts (F1), completing the proof of Proposition 3.2. □

Several ideas and ingredients of the proof above, like the way of partitioning the base set into blocks, are contained in Dove and Griggs [8] and Katona and Nagy [12]. However, even if the construction given in [8] was tailored to our particular

posets U, (F1) would fail. The following assertion says that the lower estimate given in Proposition 3.2 is *asymptotically* as good as possible.

Proposition 3.3. *For $r \in \mathbb{N}^{\geq 3}$ and $0 \leq a < b \leq r \in \mathbb{N}^+$ such that $a+2 \leq b$, $f_{r,a,b}(n)$ and, for any fixed $p \in \mathbb{Z}$, $f^{(p)}_{r,a,b}(n)$ are asymptotically $\mathrm{Sp}(\mathrm{FSP}(r,a,b),n)$ as $n \to \infty$.*

Proof. With $s := |\mathrm{FSP}(r,a,b)|$, $s = 2^r - \binom{r}{0} - \cdots - \binom{r}{a} - \binom{r}{b} - \cdots - \binom{r}{r}$. Let κ be a real number such that $\kappa < 1$ but $1-\kappa$ is very little. As we have that $\sum_{i=0}^{\infty}((2^r-s)/2^r)^i = 2^r/s$, we can pick an $n_0 \in \mathbb{N}^+$ such that

$$\kappa \cdot 2^r/s \leq \sum_{i=0}^{\lfloor n/r \rfloor -1} ((2^r-s)/2^r)^i \leq \frac{1}{\kappa} 2^r/s \text{ for all } n \text{ such that } n \geq n_0. \tag{3.5}$$

It suffices to deal with $f^{(p)}_{r,a,b}$ for a fixed $p \in \mathbb{Z}$. Using (1.2), we can pick an $n_1 \geq n_0$ such that

$$\begin{aligned} &\kappa \cdot f_{\mathrm{Sp}}(n) \cdot 2^{-(i+1)r} \\ &\quad \leq \binom{n-(i+1)r}{p + \lfloor (n-r)/2 \rfloor - 0v_0 - 1v_1 - \cdots - av_a - bv_b - \cdots - rv_r} \\ &\quad \leq \frac{1}{\kappa} \cdot f_{\mathrm{Sp}}(n) \cdot 2^{-(i+1)r} \end{aligned} \tag{3.6}$$

for all $n \geq n_1$. Let us define an auxiliary function for $n \geq n_1$ and apply the multinomial theorem to it as follows.

$$\begin{aligned} f_{\mathrm{aux}}(n) &:= \sum_{i=0}^{\lfloor n/r \rfloor -1} \sum_{\substack{\vec{v} \in \{0,\ldots,i\}^{r+a-b+2} \\ v_0+\cdots+v_a+v_b+\cdots+v_r = i}} \frac{i!}{v_0!\ldots v_a! \cdot v_b! \ldots v_r!} \times \\ &\quad \times f_{\mathrm{Sp}}(n) \cdot 2^{-(i+1)r} \binom{r}{0}^{v_0} \ldots \binom{r}{a}^{v_a} \cdot \binom{r}{b}^{v_b} \ldots \binom{r}{r}^{v_r} \qquad (3.7) \\ &= \frac{f_{\mathrm{Sp}}(n)}{2^r} \sum_{i=0}^{\lfloor n/r \rfloor -1} (2^r)^{-i} \Big(\binom{r}{0} + \cdots + \binom{r}{a} + \binom{r}{b} + \cdots + \binom{r}{r} \Big)^i \\ &= \frac{f_{\mathrm{Sp}}(n)}{2^r} \sum_{i=0}^{\lfloor n/r \rfloor -1} \Big(\frac{2^r - s}{2^r} \Big)^i. \qquad (3.8) \end{aligned}$$

Comparing (3.1), (3.6), and (3.7), we obtain that $\kappa f_{\mathrm{aux}}(n) \leq f^{(p)}_{r,a,b}(n) \leq \kappa^{-1} f_{\mathrm{aux}}(n)$ holds for all $n \geq n_1$. Applying (3.5) to the sum in (3.8), it follows that $\kappa f_{\mathrm{Sp}}(n)/s \leq f_{\mathrm{aux}}(n) \leq \frac{1}{\kappa} f_{\mathrm{Sp}}(n)/s$. Substituting this pair of inequalities into the previous one, we have that $\kappa^2 f_{\mathrm{Sp}}(n)/s \leq f^{(p)}_{r,a,b}(n) \leq \kappa^{-2} f_{\mathrm{Sp}}(n)/s$ for all $n \geq n_0$. Letting $\kappa \to 1$, it follows that $f^{(p)}_{r,a,b}(n)$ is asymptotically $f_{\mathrm{Sp}}(n)/s$. So is $\mathrm{Sp}(\mathrm{FSP}(r,a,b),n)$ by Dove and Griggs [8] and Katona and Nagy [12]. By transitivity, we obtain the required asymptotic equality. The proof of Proposition 3.3 is complete. □

4. Pairs of estimates

For $n \in \mathbb{N}^{\geq 3}$, take the following "discrete 4-dimensional simplex"

$$\begin{aligned} H_4(n) := \{(t,x_1,x_2,x_3) \in \mathbb{N}_0^4 : x_1 > 0,\ x_2 > 0,\ x_3 > 0, \\ t + x_1 + x_2 + x_3 \leq n\}. \end{aligned} \tag{4.1}$$

Remembering that $[3] := \{1, 2, 3\}$, define the function $f_{3,4}\colon H_4(n) \to \mathbb{N}_0$ by

$$\begin{aligned} f_{3,4}(t, x_1, x_2, x_3) = &\sum_{j\in[3]} (t + x_j)! \cdot (n - t - x_j)! \\ &+ \sum_{\{j,u\}\subseteq[3],\ j\neq u} (t + x_j + x_u)! \cdot (n - t - x_j - x_u)! \\ &- \sum_{(j,u)\in[3]\times[3],\ j\neq u} (t + x_j)! \cdot x_u! \cdot (n - t - x_j - x_u)!\,, \end{aligned} \tag{4.2}$$

and let

$$M_n := \min\{f_{3,4}(t, x_1, x_2, x_3) : (t, x_1, x_2, x_3) \in H_4(n)\}. \tag{4.3}$$

We also define the following three functions:

$$g_r(n) := \left\lfloor \frac{1}{2} f_{\mathrm{Sp}}(n + 2 - r) \right\rfloor, \tag{4.4}$$

$$g_3^*(n) := \lfloor n!/M_n \rfloor, \text{ where } M_n \text{ is given in (4.3), and} \tag{4.5}$$

$$\begin{aligned} g_3^{**}(n) = \Big\lfloor n! \cdot \Big(&3 \cdot \lfloor n/2 \rfloor! \cdot \lceil n/2 \rceil! + 3 \cdot \lfloor (n + 2)/2 \rfloor! \cdot \lceil (n - 2)/2 \rceil! \\ &-6 \cdot \lfloor n/2 \rfloor! \cdot \lceil (n - 2)/2 \rceil! \Big)^{-1} \Big\rfloor \end{aligned} \tag{4.6}$$

Next, based on the notations and concepts given in (2.1), (2.5), Definition 2.1, (4.4), (4.5), and (4.6), we can formulate the main result of the paper.

Theorem 4.1. *For $3 \le r \le n \in \mathbb{N}^+$ and $p \in \{-r, -r + 1, \ldots, r - 1, r\}$, $g_r(n)$ is an upper estimate while*

$$f_{r,0,r}^{(p)}(n) := \sum_{i=0}^{\lfloor n/r \rfloor - 1} \sum_{j=0}^{i} \binom{i}{j} \binom{n - (i + 1)r}{p + \lfloor (n - r)/2 \rfloor - jr} \quad \textit{and} \tag{4.7}$$

$$f_{r,0,r}^{\flat}(n) := f_{r,0,r}^{(0)}(n) \tag{4.8}$$

are lower estimates of $\mathrm{Sp}(\mathrm{FSP}(r, 0, r), n) = \mathrm{Sp}(\mathrm{J}(\mathrm{FD}(r)), n)$ on $\mathbb{N}^{\ge r}$. In particular,

$$\textit{for all } n \in \mathbb{N}^{\ge r}, \quad f_{r,0,r}^{\flat}(n) \le \mathrm{Sp}(\mathrm{J}(\mathrm{FD}(r)), n) \le g_r(n). \tag{4.9}$$

For $r = 3$, in addition to the satisfaction of (4.9), $g_3^*(n)$ is also an upper estimate of $\mathrm{Sp}(\mathrm{J}(\mathrm{FD}(3)), n)$ on $\mathbb{N}^{\ge 3}$. For $n \in \{3, 4, \ldots, 300\}$, $g_3^*(n) = g_3^{**}(n) \le g_r(n)$; in fact, $g_3^{**}(n) < g_r(n)$ for $n \in \{5, 6, \ldots, 300\}$. The pair $(f_{3,0,3}^{\flat}, g_3)$ is separated for $n \in \mathbb{N}^{\ge 3}$, and so are the pairs $(f_{3,0,3}^{\flat}, g_3^{**})$ and $(f_{3,0,3}^{\flat}, g_3^*)$ for $n \in \{3, 4, \ldots, 300\}$. Finally, for $r \in \{3, 4, \ldots, 100\}$, the pair $(f_{r,0,r}^{\flat}, g_r)$ is separated on the set $\{r, r + 1, \ldots, 300\}$.

It took 952 seconds $\approx$ 16 minutes for a computer, see Footnote 2 later, to show that for $r \in \{3, \ldots, 200\}$ and $n \in \{r, \ldots 300\}$, $f_{r,0,r}^{\flat}(n)$ defined in (4.8) is the same as $f_{r,0,r}(n)$; see (3.2). Since $f_{r,0,r}^{\flat}(n)$ is easier to define and much easier to compute than $f_{r,0,r}(n)$, it is the former that occurs in Theorem 4.1. However, it will be clear from the proof that the theorem holds with $f_{r,0,r}$ in place of $f_{r,0,r}^{\flat}$.

Conjecture 4.2. We guess that $g_3^*(n) = g_3^{**}(n)$ for all $n \in \mathbb{N}^{\ge 3}$ and $g_3^{**}(n) < g_r(n)$ for all $\mathbb{N}^{\ge 6}$.

Example 5.4 in Section 5 will show that, combining Theorem 4.1 with Observation 2.2, we can determine $\mathrm{Gm}(\mathrm{FD}(3)^k)$ exactly in many cases and we can give a good approximation for $\mathrm{Gm}(\mathrm{FD}(r)^k)$ quite often.

Proof of Theorem 4.1. Substituting $(i-j, j)$ for (v_0, v_r) and observing that the multinomial coefficient becomes a binomial one, it is clear that $f^{(p)}_{r,0,r}$ in (4.7) is a particular case of (3.1). Hence, Lemma 3.1, (3.2), Proposition 3.2, and (4.8) yield the first inequality in (4.9).

By its definition (and Lemma 3.1), $\mathrm{FSP}(r,0,r) = \mathrm{J}(\mathrm{FD}(r)) \cong \mathrm{Pow}_{\mathrm{nt}}([r])$. In each of the intervals $[\{1\}, \{1,3,4,\dots,r\}]$ and $[\{2\}, \{2,3,4,\dots,r\}]$, take a maximal chain; denote these two chains by C' and C''. Clearly, C' and C'' are unrelated chains of length $r-2$ and $C' \cong C''$. Let $n \in \mathbb{N}^{\geq r}$. With $k := \mathrm{Sp}(\mathrm{FSP}(r,0,r), n)$, there are k pairwise unrelated copies of $\mathrm{Pow}_{\mathrm{nt}}([r]) \cong \mathrm{FSP}(r,0,r)$ in $\mathrm{Pow}([n])$. Therefore, there are $2k$ pairwise unrelated copies of C' in $\mathrm{Pow}([n])$. So $2k \leq \mathrm{Sp}(C', n)$. By Griggs, Stahl, and Trotter [11], $\mathrm{Sp}(C', n) = f_{\mathrm{Sp}}(n-(r-2))$. So $2k \leq f_{\mathrm{Sp}}(n+2-r)$, implying the second inequality in (4.9).

In the rest of the proof, $r := 3$. Let $\mathrm{Sym}(n)$ stand for the set of all permutations of $[n]$. For $\vec{\sigma} = (\sigma_1, \dots, \sigma_n) \in \mathrm{Sym}(n)$ and $i \in \{0, 1 \dots, n\}$, the i's *initial segment* of $\vec{\sigma}$ is $\mathrm{Is}(\vec{\sigma}, i) := \{\sigma_j : j \leq i\}$. For $X \in \mathrm{Pow}([n])$, the *permutation set* associated with X is $\mathrm{Ps}(X) := \{\vec{\sigma} \in \mathrm{Sym}(n) : X = \mathrm{Is}(\vec{\sigma}, |X|)\}$. The trivial fact that

$$\begin{aligned} &\text{if } X, Y \in \mathrm{Pow}([n]) \text{ are incomparable (in nota-} \\ &\text{tion, } X \parallel Y), \text{ then } \mathrm{Ps}(X) \cap \mathrm{Ps}(Y) = \emptyset \end{aligned} \tag{4.10}$$

was used first by Lubell [14], and then by Griggs, Stahl, and Trotter [11] and some other papers listed in the bibliographic section. To ease the notation, let $W_3 := \mathrm{FSP}(3,0,3)$ and denote its elements by A, B, C, X, Y, Z according to Figure 1. Let $k := \mathrm{Sp}(W_3, n)$, and let $W_3^{(1)}, \dots, W_3^{(k)}$ be pairwise unrelated copies of W_3 in $\mathrm{Pow}([n])$. For $W_3^{(i)}$, we use the notation $W_3^{(i)} = \{A_i, B_i, C_i, X_i, Y_i, Z_i\}$ in harmony with Figure 1; for example, $A_i \subset X_i$ and $A_i \parallel Z_i$, etc.. We claim that $W_3^{(1)}, \dots, W_3^{(k)}$ can be chosen so that, for all $i \in [k]$,

$$X_i = A_i \cup B_i, \quad Y_i = A_i \cup C_i, \quad Z_i = B_i \cup C_i, \tag{4.11}$$

$$A_i = X_i \cap Y_i, \quad B_i = X_i \cap Z_i, \quad C_i = Y_i \cap Z_i. \tag{4.12}$$

Assume that the first equality in (4.11) fails. Let $X_i' := A_i \cup B_i$ and define $W_3^{(i)\prime} := (W_3^{(i)} \setminus \{X_i\}) \cup \{X_i'\}$. If we had that $X_i' \subseteq Y_i$, then $B \subseteq X_i' \subseteq Y_i$ would be a contradiction. As $Y_i \subseteq X_i'$ would lead to $Y_i \subseteq X_i$ since $X_i' \subseteq X_i$, we conclude that $X_i' \parallel Y_i$. We obtain similarly that $X_i' \parallel Z_i$. So $\{X_i', Y_i, Z_i\}$ is an antichain, and now it follows easily that $W_3^{(i)\prime}$ is a copy of W_3. For $j \in [k] \setminus \{i\}$ and $E \in W_3^{(j)}$, $E \subseteq X_i'$ would lead to $E \subseteq X_i$ while $X_i' \subseteq E$ to $A_i \subseteq E$. So $E \nparallel X_i'$ would lead to contradiction. Hence, $W_3^{(i)\prime}$ and $W_3^{(j)}$ are unrelated, showing that we can change $W_3^{(i)}$ to $W_3^{(i)\prime}$. As there is an analogous treatment for Y_i and Z_i, and we can take $i = 1$, $i = 2$, …, $i = k$ one by one, (4.11) can be assumed.

Recall that Grätzer [10, Lemma 73] asserts that whenever a, b, c are elements of a lattice such that $\{a \vee b, a \vee c, b \vee c\}$ is a 3-element antichain, then this antichain generates an 8-element Boolean sublattice in which $\{a \vee b, a \vee c, b \vee c\}$ is the set of coatoms. Therefore, if we apply the dual of the procedure above (that is, if we replace A_i by $X_i \cap Y_i$, etc.), then we reach (4.12) without destroying the validity of (4.11). We have shown that both (4.11) and (4.12) can be assumed; so we assume them in the rest of the proof.

Let $T_i := X_i \cap Y_i \cap Z_i$. By (4.12), T_i is also the intersection of any two of A_i, B_i, and C_i. Hence, letting $A_i^\bullet := A_i \setminus T_i$, $B_i^\bullet := B_i \setminus T_i$, and $C_i^\bullet := C_i \setminus T_i$, it follows from

(4.11), (4.12), and $W_3^{(i)} \cong W_3$ that $A_i^\bullet$, $B_i^\bullet$, and $C_i^\bullet$ are pairwise disjoint subsets of $[n]$, none of them is empty, they are disjoint from T_i, and

$$\begin{aligned} &A_i = T_i \cup A_i^\bullet, \quad B_i = T_i \cup B_i^\bullet, \quad C_i = T_i \cup C_i^\bullet, \\ &X_i = T_i \cup A_i^\bullet \cup B_i^\bullet, \quad Y_i = T_i \cup A_i^\bullet \cup C_i^\bullet, \quad Z_i = T_i \cup B_i^\bullet \cup C_i^\bullet. \end{aligned} \tag{4.13}$$

For $i \in [k]$, we let

$$G_i := \mathrm{Ps}(A_i) \cup \mathrm{Ps}(B_i) \cup \mathrm{Ps}(C_i) \cup \mathrm{Ps}(X_i) \cup \mathrm{Ps}(Y_i) \cup \mathrm{Ps}(Z_i). \tag{4.14}$$

As each of $A_i,\ldots,Z_i$ is incomparable with each of $A_j,\ldots,Z_j$ provided that $i \neq j$, (4.10) together with (4.14) imply that

$$\text{for } i,j \in [k], \text{ if } i \neq j \text{ then } G_i \cap G_j = \emptyset. \tag{4.15}$$

It follows from (4.15), $G_1 \cup \cdots \cup G_k \subseteq \mathrm{Sym}(n)$, and $|\mathrm{Sym}(n)| = n!$ that

$$\sum_{i\in[k]} |G_i| \leq n! \ . \tag{4.16}$$

Next, for $i \in [k]$, we focus on $|G_i|$. Denote $|T_i|$, $|A_i^\bullet|$, $|B_i^\bullet|$, and $|C_i^\bullet|$ by t_i, a_i, b_i, and c_i, respectively. By (4.13), $|A_i| = t_i + a_i$, $|B_i| = t_i + b_i$, $|C_i| = t_i + c_i$, $|X_i| = t_i + a_i + b_i$, $|Y_i| = t_i + a_i + c_i$, and $|Z_i| = t_i + b_i + c_i$. Observe that $|\mathrm{Ps}(A_i)| = (t_i + a_i)! \cdot (n - t_i - a_i)!$ since what the first $|A_i| = t_i + a_i$ components of $\vec{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Ps}(A_i)$ form is set A_i and they can be arranged in $(t_i + a_i)!$ many ways while the rest of the components of $\vec{\sigma}$ in the last $n - t_i - a_i$ positions in $(n-t_i-a_i)!$ many ways. We obtain similarly that $|\mathrm{Ps}(B_i)| = (t_i+b_i)! \cdot (n-t_i-b_i)!$, $|\mathrm{Ps}(C_i)| = (t_i + c_i)! \cdot (n - t_i - c_i)!$, $|\mathrm{Ps}(X_i)| = (t_i + a_i + b_i)! \cdot (n - t_i - a_i - b_i)!$, $|\mathrm{Ps}(Y_i)| = (t_i+a_i+c_i)! \cdot (n-t_i-a_i-c_i)!$, and $|\mathrm{Ps}(Z_i)| = (t_i+b_i+c_i)! \cdot (n-t_i-b_i-c_i)!$. It follows from (4.10) that the intersection of any three of the six permutation sets considered above is empty since there is no 3-element chain in $W_3^{(i)}$. By (4.10) again, we need to take care of the intersections of two permutation sets associated with comparable members of $W_3^{(i)}$; there are six such intersections as the diagram of W_3 has exactly six edges; see Figure 1. One of the just-mentioned six intersections is $\mathrm{Ps}(A_i) \cap \mathrm{Ps}(X_i)$. For a permutation $\vec{\sigma} \in \mathrm{Ps}(A_i) \cap \mathrm{Ps}(X_i)$, (4.13) yields that there are $|A_i|! = (t_i + a_i)!$ possibilities to arrange the elements of A_i in the first $|A_i|$ places, $b_i!$ many possibilities to arrange the elements of $X_i \setminus A_i = B_i^\bullet$ in the next b_i places, and $(n - t_i - a_i - b_i)!$ possibilities for the rest of entries of $\vec{\sigma}$. Hence, $|\mathrm{Ps}(A_i) \cap \mathrm{Ps}(X_i)| = (t_i + a_i)! \cdot b_i! \cdot (n - t_i - a_i - b_i)!$, and analogously for the other five intersections of two permutation sets.

The considerations above imply that for $i \in [k]$, $|G_i| = f_{3,4}(t_i, a_i, b_i, c_i)$; see (4.2). As (t_i, a_i, b_i, c_i) is clearly in $H_4(n)$, (4.3) yields that $M_n \leq |G_i|$. This fact and (4.16) imply that $kM_n \leq \sum_{i\in[k]} |G_i| \leq n!$. Dividing by M_n and taking into account that $k \in \mathbb{N}^+$, we obtain that $\mathrm{Sp}(W_3, n) = k \leq \lfloor n!/M_n \rfloor = g_3^*(n)$, as required.

We only guess but could not prove that for all $n \in \mathbb{N}^{\geq 3}$, $f_{3,4}$ takes its minimum on $H_4(n)$ at $(\lfloor (n-2)/2 \rfloor, 1, 1, 1)$; see also Conjecture 4.2. However, we can reduce the computational difficulties by considering the following auxiliary function:

$$\begin{aligned} f_{3,3}(t,x,y) &= (t+x)! \cdot (n-t-x)! + (t+y)! \cdot (n-t-y)! \\ &\quad + 2(t+x+y)! \cdot (n-t-x-y)! - 2(t+x)! \cdot y! \cdot (n-t-x-y)! \\ &\quad - 2(t+y)! \cdot x! \cdot (n-t-x-y)! \ . \end{aligned} \tag{4.17}$$

The definition of $H_4(n)$, see (4.1), and

$$2f_{3,4}(t,x_1,x_2,x_3) = f_{3,3}(t,x_1,x_2) + f_{3,3}(t,x_2,x_3) + f_{3,3}(t,x_1,x_3)\,, \tag{4.18}$$

explain that we are interested in $f_{3,3}$ on the first one of the following two sets,

$$H_3(n) := \{(t,x,y) \in \mathbb{N}_0^3 : x > 0,\ y > 0,\ t + x + y \leq n-1\} \text{ and} \tag{4.19}$$

$$H_3'(n) := \{(t,x,y) \in \mathbb{N}_0^3 : x > 0,\ y \geq x,\ t + x + y \leq n-1\}. \tag{4.20}$$

In (4.19), the sum is only at most $n-1$ since the fourth variable of $f_{3,4}$, which does not occur in $f_{3,3}$, is at least 1. The progress is that $H_3(n)$ has much less elements than $H_4(n)$, and $H_3'(n)$ has even less; this is why we could reach 300 in Theorem 4.1. (Note that a priori, it was not clear that when $2f_{3,4}(t,x_1,x_2,x_3)$ takes its minimum value, then so do all of its summands in (4.18).) Observe that since $f_{3,3}$ is symmetric in its last two variables,

$$\min\{f_{3,3}(t,x,y) : (t,x,y) \in H_3(n)\} = \min\{f_{3,3}(t,x,y) : (t,x,y) \in H_3'(n)\}. \tag{4.21}$$

A straightforward Maple program[2], which benefits from (4.21), shows that

$$\begin{aligned}&\text{for } 3 \leq n \leq 300,\ f_{3,3} \text{ takes its minimum on the discrete}\\ &\text{tetrahedron } H_3(n) \text{ at } (t,x,y) = (\lfloor (n-2)/2 \rfloor, 1, 1).\end{aligned} \tag{4.22}$$

(Note that $f_{3,3}$ takes its minimum at two triples if n is even but only at a unique triple if n is odd.) If $n \in \{3,4,\ldots,300\}$ and $(\lfloor (n-2)/2 \rfloor, 1, 1, 1)$ is substituted for (t,x,y,z), then each of the three summands in (4.18) takes its minimal value by (4.22). This allows us to conclude that at $(t,x,y,z) = (\lfloor (n-2)/2 \rfloor, 1, 1, 1)$, $f_{3,4}$ takes its minimum on $H_4(n)$. Thus, for $n \in \{3,4,\ldots,300\}$ and for M_n from (4.3),

$$\begin{aligned}M_n = f_{3,4}(\lfloor (n-2)/2 \rfloor, 1, 1, 1) &= 3 \cdot \lfloor n/2 \rfloor! \cdot \lceil n/2 \rceil!\\ &+ 3 \cdot \lfloor (n+2)/2 \rfloor! \cdot \lceil (n-2)/2 \rceil! - 6 \cdot \lfloor n/2 \rfloor! \cdot \lceil (n-2)/2 \rceil!\,.\end{aligned} \tag{4.23}$$

Combining (4.5), (4.23), and (4.6), we obtain that $g_3^*(n) = g_3^{**}(n)$ for n belonging to the set $\{3,4,\ldots,300\}$, as required.

Next, to show that the pair $(f_{3,0,3}^\flat, g_3) = (f_{3,0,3}^{(0)}, g_3)$ is separating, we need to show that $f_{3,0,3}^{(0)}(n+1) - g_3(n) \geq 0$ for all $n \in \mathbb{N}^{\geq 3}$. Depending on the parity of n, there are two cases. If n is of the form $n = 2m+2$ then, reducing the sum in (4.7) to its summands corresponding to $(i,j) = (0,0)$ and $(i,j) = (1,0)$,

$$\begin{aligned}2f_{3,0,3}^{(0)}(n+1) - 2g_3(n) &\geq 2\binom{2m}{m} + 2\binom{2m-3}{m} - \binom{2m+1}{m} \qquad (4.24)\\ &= \frac{2 \cdot (2m)!}{m! \cdot m!} + \frac{2 \cdot (2m-3)!}{m!(m-3)!} - \frac{(2m+1)!}{m!(m+1)!}\\ &= \frac{(2m-3)!}{m!(m+1)!} \cdot \alpha, \quad \text{where} \quad \alpha = 2(m+1)2m(2m-1)(2m-2)\\ &\quad +2(m+1)m(m-1)(m-2) - (2m+1)2m(2m-1)(2m-2)\\ &= 2m^4 + 4m^3 - 14m^2 + 8m = 2m(m+4)(m-1)^2. \qquad (4.25)\end{aligned}$$

[2]Maple V Release 5 (1997); this computer algebraic program ran on a desktop computer (AMD Ryzen 7 2700X Eight-Core Processor 3.70 GHz) in Windows XP environment simulated by Oracle VM VirtualBox 6.0 (2019) under Windows 10 Pro. The whole computation for (4.21) and the data in Section 5 took 7 hours and 16 minutes; (4.21) in itself needed about 7 hours. The program is available from the (Appendix) Section 6 of the extended arXiv:2309.13783 (or arXiv:2309.13783v2) version of the paper and, at the time of writing, from the author's website.

Hence, both α and the fraction multiplied by α are non-negative for $m \in \mathbb{N}^+$. Thus, $f^{(0)}_{3,0,3}(n+1) - g_3(n) \geq 0$ for $n \geq 4$ even. Similarly, for $n = 2m+1$ odd,

$$\begin{aligned} 2f^{(0)}_{3,0,3}(n+1) - 2g_3(n) &\geq 2\binom{2m-1}{m-1} + 2\binom{2m-4}{m-1} - \binom{2m}{m} \\ &= \frac{(2m-4)!}{m!m!} \cdot 2m^2(m-1)(m-2). \end{aligned}$$

Therefore, $f^{(0)}_{3,0,3}(n+1) - g_3(n) \geq 0$ for $2 \leq m \in \mathbb{N}^+$, that is, for $n \geq 5$ odd. For $n = 3$, $f^{(0)}_{3,0,3}(n+1) - g_3(n) \geq 0$ is trivial; see also 5.2. We have shown that $(f^\flat_{3,0,3}, g_3)$ is separated.

The already mentioned Maple program has computed $g_3(n)$, $g_3^*(n)$, and $g_3^{**}(n)$ for all $n \in \{3, 4, \ldots, 300\}$. This computation proves that $g_3^{**}(n) = g_3^*(n) \leq g_3(n)$ for all these n and $g_3^{**}(n) = g_3^*(n) < g_3(n)$ for $n \in \{5, 6, \ldots, 300\}$. These inequalities and that $(f^\flat_{3,0,3}, g_3)$ is separated imply that $(f^\flat_{3,0,3}, g_3^*)$ and $(f^\flat_{3,0,3}, g_3^{**})$ are separated on $\{3, 4, \ldots, 300\}$. The same Maple program has computed all the relevant $f^\flat_{r,0,r}(n+1)$ and $g_r(n)$, from which we conclude that for $r \in \{3, 4, \ldots, 100\}$, the pair $(f^\flat_{r,0,r}, g_r)$ is separated on the set $\{r, r+1, \ldots, 300\}$. The proof of Theorem 4.1 is complete. □

Some comments on this proof are appropriate here. While we could use quite a rough estimation in (4.24) when proving that $(f^\flat_{3,0,3}, g_3)$ is separating on the set $\mathbb{N}^{\geq 3}$, there is no similar possibility for $(f^\flat_{r,0,r}, g_r)$. Indeed, since $f^\flat_{r,0,r}(n+1) = g_r(n)$ for, say, $(r, n) = (20, 56)$ when $f^\flat_{20,0,20}(56+1) = 17\,672\,631\,900 = g_{20}(56)$, no estimation would be possible. As $g_r(n)$ is far from being asymptotically good, it is not worth putting more work into its investigation. While we could use Grätzer [10, Lemma 73] to reach a pleasant situation for $r = 3$, see (4.11) and (4.12),we have no similar tool for $r > 3$; this explains that Theorem 4.1 does not tell too much about upper estimates in case of $r > 3$. Finally, note that even though $f_{3,3}$ in (4.17) is simpler than $f_{3,4}$ in (4.2), the three-variate function $f_{3,3}$ is still too complicated. In particular, we know from computer-assisted calculations that $f_{3,3}$ has several "local minima" on the discrete tetrahedron $H_3(n)$ defined in (4.19); this is our excuse that we could verify Conjecture 4.2 only for $n \leq 300$ and only with a computer.

5. Odds and ends, including some computational results

Theorem 4.1 pays no attention to the case $r = 2$, which is trivial by the following remark. As in (4.4), $g_2(n) := \lfloor f_{\mathrm{Sp}}(n)/2 \rfloor = \lfloor \mathrm{C_b}(n, n/2)/2 \rfloor$.

Remark 5.1. For $n \in \mathbb{N}^{\geq 2}$, $\mathrm{Sp}(\mathrm{J}(\mathrm{FD}(2)), n) = g_2(n)$.

Proof. By Lemma 3.1 or trivially, $\mathrm{J}(\mathrm{FD}(2))$ is the two-element antichain. Hence, Remark 5.1 follows from Sperner's theorem; see (2.2). □

Corollary 5.2. *For $r \in \mathbb{N}^{\geq 3}$ and $k \in \mathbb{N}^{\geq 2}$, let $n \in \mathbb{N}^+$ be the smallest integer such that $k \leq f^\flat_{r,0,r}(n)$; see (4.8). Then for every distributive lattice D generated by r elements, the direct power D^k has an at most n-element generating set.*

Proof. Let k, D, and n be as in the corollary. Since $k \leq f^\flat_{r,0,r}(n)$ is included in the assumption and $f^\flat_{r,0,r}(n) \leq \mathrm{Sp}(\mathrm{J}(\mathrm{FD}(r)), n)$ by Theorem 4.1, it follows from (2.4) that $\mathrm{FD}(r)^k$ can be generated by an at most n element subset Y. Using that $\mathrm{FD}(r)$ is the *free* r-generated distributive lattice, we can pick a surjective (in other

words, onto) homomorphism $\varphi\colon \mathrm{FD}(r) \to D$. Then $\varphi^k\colon \mathrm{FD}(r)^k \to D^k$, defined by $(x_1, \dots, x_k) \mapsto (\varphi(x_1), \dots, \varphi(x_k))$, is also a surjective homomorphism. Thus, $\varphi^k(Y)$ generates D^k and $|\varphi^k(Y)| \leq |Y| \leq n$ proves Corollary 5.2. □

The just-proved corollary and the abundance of large lattices that are easy-to-describe and easy-to-work-with motivate the following extension of the cryptographic "protocol" outlined in Czédli [3] and, mainly, in [5]. The purpose of the quotient marks here is *to warn the reader*: none of our protocols is fully elaborated and, thus, it does not meet the requirements of nowadays' cryptology. In particular, neither a concrete method of choosing the master key according to some probabilistic distribution is given nor we have proved that the average case withstands attacks; we do not even say that we are close to meet these requirements. On the other hand, no rigorous average case analysis supports some widely used and, according to experience, safe cryptographic protocols like RSA and AES and, furthermore, many others rely ultimately on the *conjecture* that the complexity class **P** is different from **NP**. This is our excuse to tell a bit more about one of our motivations in Remark 5.3 below. For a lattice L and $\vec{h} = (h_1, \dots, h_k) \in L^k$, $\vec{h}$ is a (k-dimensional) *generating vector* of L if $\{h_1, \dots, h_k\}$ is a generating set of L.

Remark 5.3. In the *session key exchange protocol* given in Czédli [5][3], the secret master key known only by the communicating parties was a k-dimensional generating vector $\vec{h}$ of the 2^n-element Boolean lattice B_n. The point was that $\mathrm{Gm}(B_n)$, see (2.3), is small, and so there are very many k-dimensional generating vectors $\vec{h}$ if k is a few times, say, seven times larger than $\mathrm{Gm}(B_n)$. Here we suggest to add (A) or (B) to the protocol outlined in [5] and to work in a lattice different from B_n.

(A) Choose a medium-sized finite random poset U and an exponent $n \in \mathbb{N}^+$; for example, a 20-element random poset U and $n = 500$ are sufficient. (There are very many 20-element posets; see A000112 in Sloan [15]; the direct link is https://oeis.org/A000112.) By the well-known structure theorem of finite distributive lattices, see Grätzer [10, Theorem 107], U determines a finite distributive lattice D. Then replace B_n with D^n in the [5]-protocol so that, in addition to $\vec{h}$, U and n also belong to the secret master key.

(B) Choose a random poset U of size 100 or so. As in [4], this U determines the huge lattice $(\mathrm{Quo}^{\leq}(U); \subseteq)$ of quasiorders extending $\leq_U$; this lattice can be generated by few elements. Use this lattice instead of B_n. The poset U and a k-dimensional generating vector of $(\mathrm{Quo}^{\leq}(U); \subseteq)$ constitute the secret master key; otherwise the protocol is the same as in [5].

Next, we present some computational data, see Footnote 2; at the "≈" rows, the last decimals are correctly rounded.

n	298	299	300
$f^{\flat}_{3,0,3}(n) \approx$	$3.919\,720 \cdot 10^{87}$	$7.839\,440 \cdot 10^{87}$	$1.562\,662 \cdot 10^{88}$
$g_3^{**}(n) \approx$	$3.932\,918 \cdot 10^{87}$	$7.865\,747 \cdot 10^{87}$	$1.567\,888 \cdot 10^{88}$
$\frac{g_3^{**}(n)}{f^{\flat}_{3,0,3}(n)} \approx$	1.003 367 003	1.003 355 705	1.003 344 482

(5.1)

[3]At the time of writing, see (4.3) in https://arxiv.org/abs/2303.10790v3 .

$n=$	3	4	5	6	7	8
$f^\flat_{3,0,3}(n)$	1	1	2	3	6	11
$g^*_3(n)=g^{**}_3(n)$	1	1	2	4	7	13
$g_3(n)$	1	1	3	5	10	17
$n=$	9	10	11	12	13	14
$f^\flat_{3,0,3}(n)$	24	42	84	153	306	570
$g^*_3(n)=g^{**}_3(n)$	26	46	92	168	333	616
$g_3(n)$	35	63	126	231	462	858
$n=$	15	16	17	18	19	20
$f^\flat_{3,0,3}(n)$	1146	2145	4290	8100	16200	30786
$g^*_3(n)=g^{**}_3(n)$	1225	2288	4558	8580	17107	32413
$g_3(n)$	1716	3217	6435	12155	24310	46189

(5.2)

$n=$	4	5	6	7	8	9	10	11	12
$f^\flat_{4,0,4}(n)$	1	1	2	3	6	10	20	36	74
$g_4(n)$	1	1	3	5	10	17	35	63	126
$n=$	13	14	15	16	17	18	19	20	21
$f^\flat_{4,0,4}(n)$	134	268	496	992	1856	3712	7004	14014	26598
$g_4(n)$	231	462	858	1716	3217	6435	12155	24310	46189

(5.3)

$n=$	5	6	7	8	9	10	11	12	13
$f^\flat_{5,0,5}(n)$	1	1	2	3	6	10	20	35	70
$g_5(n)$	1	1	3	5	10	17	35	63	126
$n=$	14	15	16	17	18	19	20	21	22
$f^\flat_{5,0,5}(n)$	127	256	471	942	1758	3516	6620	13240	25095
$g_5(n)$	231	462	858	1716	3217	6435	12155	24310	46189

(5.4)

The computation for the following table took 306 seconds.

n	5 999	6 000
$f^\flat_{20,0,20}(n)\approx$	$7.445\,882\,708\,069\cdot 10^{1797}$	$1.489\,176\,541\,614\cdot 10^{1798}$
$g_{20}(n)\approx$	$1.488\,924\,847\,889\cdot 10^{1798}$	$2.977\,849\,695\,779\cdot 10^{1798}$

(5.5)

Next, we give some examples; each of them is based on (2.4), Observation 2.2, and one of the computational tables that will be specified.

Example 5.4. (A) By (5.2), $\mathrm{Gm}(\mathrm{FD}(3)^{30\,000})=20$; see (2.3). That is, the direct power $\mathrm{FD}(3)^{30\,000}$ can be generated by 20 elements but not by 19.

(B) By (5.3), $\mathrm{Gm}(\mathrm{FD}(4)^{20\,000})$ is either 20 or 21 but we do not know which one.

(C) By (5.4), $\mathrm{Gm}(\mathrm{FD}(5)^{25\,000})=22$.

(D) By (5.1), $\mathrm{Gm}(\mathrm{FD}(3)^{10^{88}})=300$ (the exponent in the direct power is 10^{88}).

(E) By (5.5), $\mathrm{Gm}(\mathrm{FD}(20)^{1.489\cdot 10^{1798}})=6\,000$ (the exponent is $1.489\cdot 10^{1\,798}$).

At the time of writing, we know from Sloan [15] (https://oeis.org/A000372) that in spite of lots of work by many contributors, the largest integer r for which $|\mathrm{FD}(r)|$ is known is $r=9$. We mention the following well-known folkloric lower fact:

$$2^{1024}=2^{2^{10}}\leq|\mathrm{FD}(20)|. \tag{5.6}$$

Indeed, the free Boolean lattice FB(10) on 10 generators consists of $2^{2^{10}}$ elements and it is lattice-generated by the free generators of FB(10) and their complements. So FB(10) as a distributive lattice is generated by 20 elements, implying (5.6).

Based on (5.6) and the paragraph above, the direct power in part (E) of Example 5.4 consists of an unknown but very large number of elements. However, only 306 seconds were needed to determine the least possible size of its generating sets.

References

[1] D. Ahmed and G. Czédli: (1+1+2)-generated lattices of quasiorders. Acta Sci. Math. (Szeged) 87 (2021), 415–427.[4]

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

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

[4] G. Czédli: Generating some large filters of quasiorder lattices. https://arxiv.org/abs/2302.13911

[5] G. Czédli: Generating Boolean lattices by few elements and exchanging session keys. arXiv:2303.10790

[6] G. Czédli: Sperner theorems for unrelated copies of some partially ordered sets in a powerset lattice and minimum generating sets of powers of distributive lattices. arXiv:2308.15625 .

[7] G. Czédli and L. Oluoch: Four-element generating sets of partition lattices and their direct products. Acta Sci. Math. (Szeged) 86, 405–448 (2020)

[8] Andrew P. Dove, Jerrold R. Griggs: Packing posets in the Boolean lattice. Order **32**, 429–438 (2015)

[9] Gelfand, I.M., Ponomarev, V.A.: Problems of linear algebra and classification of quadruples of subspaces in a finite dimensional vector space. Hilbert Space Operators, Coll. Math. Soc. J. Bolyai 5, Tihany, 1970.

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

[11] Griggs, J. R., Stahl, J., Trotter, W. T. Jr.: A Sperner theorem on unrelated chains of subsets. J. Combinatorial Theory, ser. A **36**, 124–127 (1984)

[12] Katona and Nagy: Incomparable copies of a poset in the Boolean lattice. Order **32**, 419–427 (2015)

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

[14] Lubell, D: A short proof of Sperner's lemma. J. Combinatorial Theory **1**, 299 (1966)

[15] Sloan, N. J. A.: The On-Line Encyclopedia of Integer Sequence. https://oeis.org/

[16] Sperner, E.: Ein Satz über Untermengen einer endlichen Menge. Math. Z. **27**, 544–548 (1928). DOI 10.1007/BF01171114

[17] H. Strietz: ̈ber Erzeugendenmengen endlicher Partitionverbände. Studia Sci. Math. Hungarica 12 (1977), 1–17. (in German)

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

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

[20] Zádori, L.: Subspace lattices of finite vector spaces are 5-generated. Acta Sci. Math. (Szeged) 74 (2008), 493–499.

Email address: czedli@math.u-szeged.hu

URL: http://www.math.u-szeged.hu/~czedli/

University of Szeged, Bolyai Institute. Szeged, Aradi vértanúk tere 1, HUNGARY 6720

[4] At the time of writing, [1], [7], and [20] are freely available from http://www.acta.hu/.