GENERATING THE DIRECT POWERS OF A BOOLEAN LATTICE WITH AN EXTRA 0

Gábor Czédli*

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

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

1 Introduction

In this paper the author gives an account on the progress after his online talk at the 15th International Summer-School Conference "Problems Allied to Universal Algebra and Model Theory", Novosibirsk–Erlagol, June 21, 2023. The content of this talk is covered by [4] together with its references and, at the time of writing, the slides of the talk are available from the author's website. Furthermore, we present some new results; see Theorem 2.3 and Corollary 2.4, exemplified by (4.1) and (4.2).

For a natural number $n \in \mathbb{N}_0 = \mathbb{N}^+ \cup \{0\} = \{0, 1, 2, \dots\}$, let $B_n = (B_n; \vee, \wedge)$ denote the 2^n-element Boolean lattice. As we make no difference between two isomorphic algebraic structures, we often think of B_n as the powerset lattice $\mathsf{P}([n]) = (\mathsf{P}([n]); \cup, \cap)$ of the set $[n] := \{1, 2, \dots, n\}$ or as the direct power B_1^n. A subset X of a finite lattice L *generates* L if each element of L can be obtained by applying a lattice term (built from joins and meets) to appropriate elements of X.

$$\text{Let } \gamma(L) \text{ denote the least number } n \in \mathbb{N}_0 \text{ such that there is an } n\text{-element subset of } L \text{ that generates } L. \tag{1.1}$$

In [3] and [4], we have pointed out that large lattices L with many small generating subsets give rise to authentication and cryptographic protocols. If $\gamma(L)$ is small but L is large, then L has many small generating subsets and it is a candidate to be the underlying lattice of the protocols described in [3] and [4]; this constitutes one of our motivations. Another motivation

*This research was supported by the National Research, Development and Innovation Fund of Hungary, under funding scheme K 138892. Version of October 15, 2023

is supplied by more than a dozen papers devoted to small generating sets of certain lattices; in addition to the survey parts of [3] and [4], here we mention only an early result by Gelfand, and Ponomarev [9], which was quoted by Zádori [16] when he proved an analogous result.

As usual, we refer to *partially ordered sets* by their widely spred synonym, *posets*. For posets $X_0 = (X_0; \leq_{X_0})$, $X = (X; \leq_X)$, and $Y = (Y; \leq) = (Y; \leq_Y)$ such that $X \subseteq Y$, $\leq_X$ is the intersection of X^2 with $\leq_Y$, and X is isomorphic to X_0, we are going to call X a *copy* of X_0 in Y. For $y_1, y_2 \in Y$, let $y_1 \parallel y_2$ stand for the conjunction of $y_1 \not\leq y_2$ and $y_2 \not\leq y_1$. If X and X' are copies of X_0 in Y such that $x \parallel x'$ for all $x \in X$ and $x' \in X'$, then X and X' are said to be *incomparable copies* or, in other words, *unrelated copies* of X_0 in Y. Note that Y is often a lattice in which, as usual, $y \leq y'$ means that $y = y \wedge y'$.

$$\text{Denote by } \sigma(X_0, Y) \text{ the maximum number of pairwise incomparable copies of } X_0 \text{ in } Y. \tag{1.2}$$

As B_0 is the singleton poset, Sperner's classical theorem asserts that, for $n \in \mathbb{N}_0$, $\sigma(B_0, B_n) = \binom{n}{\lfloor n/2 \rfloor}$; see [15]. As for our notation, the lower number in the binomial coefficient is the *lower integer part* of $\frac{n}{2}$; note at this point that $\lceil x \rceil$ will stand for the *upper integer part* of x. Note also that γ and σ in (1.1) come (1.2) from *g*enerating and *S*perner, respectively. Results on $\sigma(X_0, Y)$ are called *Sperner theorems* (not to be confused with Sperner's theorem); see, e.g., Dove and Griggs [8], Griggs, Stahl, and Trotter [11], and Katona and Nagy [12] for examples, and see also [5] and [6], which came to existence after the afore-mentioned conference talk.

In [4] and the conference talk, we proved that $\gamma(B_k)$ is the smallest $n \in \mathbb{N}_0$ such that $k \leq \binom{n}{\lfloor n/2 \rfloor}$. In other words, $\gamma(B_1^k) = \min\{n \in \mathbb{N}_0 : k \leq \sigma(B_0, B_n)\}$. Hence, we can easily determine $\gamma(B_n)$ for, say, $n = 10^{3000}$ while the trivial algorithm that lists all subsets and checks which of them are generating ones would not be feasible even for $n = 20$. For a finite lattice D, $J(D)$ stands for a *poset of join-irreducible elements* of D; an element is *join-irreducible* if it covers exactly one element, and the order (relation) of $J(D)$ is the restriction of the order of D to $J(D)$. The main result of [5] extends the second formulation of the just-mentioned result on Boolean lattices to all finite distributive lattices as follows.

$$\text{For any finite distributive lattice } D \text{ and } k \in \mathbb{N}^+, \ \gamma(D^k) \text{ is the least } n \in \mathbb{N}^+ \text{ such that } k \leq \sigma(J(D), B_n). \tag{1.3}$$

The "conference talk result" on $\gamma(B_k)$" is a consequence (1.3) and Sperner's theorem. For any finite poset X, Dove and Griggs [8] and, independently,

Katona and Nagy [12] determined $\sigma(X, B_n)$ asymptotically as $n \to \infty$. Katona and Nagy [12] and, recently, [5] have determined $\sigma(X, B_n)$ for some particular posets X while, for some other particular posets X, [5] and [6] have supplied estimates for $\sigma(X, B_n)$ that are reasonable even when n is small. For $n \in \mathbb{N}_0$,

$$\begin{array}{l}\text{let } B_{n,0} \text{ denote the } (2^n+1)\text{-element lattice that}\\ \text{we obtain by adding a new least element to } B_n.\end{array} \tag{1.4}$$

So $B_n = B_{n,0} \setminus \{0\}$ is a 2^n-element sublattice (in fact, a filter) of $B_{n,0}$. For $J(B_{1,0})$, which is the 2-element chain, Griggs, Stahl, and Trotter [11, Theorem 2] (valid for all finite chains) applies; so we know that $\sigma(B_{1,0}, B_n) = \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ for $i \in \{0, 1\}$. For the value of $\sigma(J(B_{2,0}), B_n)$, Katona and Nagy [12] give a conjecture, which we are going to recall later. Only estimates are proved for $\sigma(J(B_{3,0}), B_n)$ in [5] but, for many k's,

$$\text{even these estimates are sufficient to obtain } \gamma(B_{3,0}^k) \text{ exatly;} \tag{1.5}$$

for example, if $k = 3 \cdot 10^{606}$, then $\gamma(B_{3,0}^k) = 2023$. In the next section, letting r be any positive integer larger than 1, we give estimates that are sufficient to obtain information on $\gamma(B_{r,0}^k)$ and, if $r \leq 4$, to determine it in many cases.

2 Results

Definition 2.1. If X is a finite poset and f and g are $\mathbb{N}^+ \to \mathbb{N}_0$ functions such that $f(n) \leq \sigma(X, B_n) \leq g(n)$ for all $n \in \mathbb{N}^+$, then (f, g) is a *pair of estimates* of the function $\sigma(X, B_n)$. If, in addition, $n_0 \in \mathbb{N}_0$ and $g(n) \leq f(n+1)$ for all $n \in \mathbb{N}^+ \setminus [n_0]$, then we say that (f, g) is a *pair of reasonable estimates* of $\sigma(X, B_n)$ on $\mathbb{N}^+ \setminus [n_0]$. If $n_0 = 0$, then we drop it; the case when the common domain of f, g, and $\sigma(X, B_n)$ is of the form $\{r, r+1, r+2, \dots\}$ is analogous.

The following fact is trivial, it was used (in a more involved terminology) in [5] and [6], and it will be exemplified later in the proof of Corollary 2.4.

Fact 2.2. *Assume that D is a finite distributive lattice and (f, g) is a pair of reasonable estimates of $\sigma(J(D), B_n)$. Then for any $2 \leq k \in \mathbb{N}^+$, if $n = n_k$ denotes the smallest integer such that $k \leq f(n)$, then $\gamma(D^k) \in \{n-1, n\}$.*

Next, to ease the notation in what follows,

$$\begin{array}{l}\text{for } r \in \mathbb{N}^+, \text{ let } F^{(r)} := J(B_{r,0}); \text{ it consits of a smallest}\\ \text{element } z \text{ and } r \text{ maximal elements, } u_1, \dots, u_r.\end{array} \tag{2.1}$$

Before defining some functions below, let us emphasize that, by convention, $\binom{x}{y} = \frac{x!}{y!(x-y)!} \in \mathbb{N}^+$ if $x, y \in N_0$ such that $x \le y$ but

$$\binom{x}{y} := 0 \quad \text{in any other case like } y < 0 \text{ or } x < y. \tag{2.2}$$

In addition to $r \in \mathbb{N}^+$, let p be an integer parameter. For $n \in \mathbb{N}^+$, we define

$$f_r^{(p)}(n) := \sum_{i=0}^{\lfloor n/r \rfloor - 1} \sum_{\substack{(w_2,\dots,w_r)\in\{0,\dots,i\}^{r-1} \\ w_2+\cdots+w_r=i}} \frac{i!}{w_2!\dots w_r!} \times \\ \times \binom{n-(i+1)r}{1-p+\lfloor (n-r)/2 \rfloor - 2w_2 - 3w_3 - \cdots - rw_r} \cdot \prod_{\beta=2}^{r} \binom{r}{\beta}^{w_\beta} \tag{2.3}$$

$$\text{and} \qquad f_r(n) := \max\{f_r^{(p)}(n) : p \in \{-r, -r+1, \dots, r\}\}. \tag{2.4}$$

We define the counterpart $g_r(n)$ of $f_r(n)$ only for $r \in \{2,3,4\}$; note that only $g_4(n)$ is new since $g_2(n)$ and $g_3(n)$ are taken from [5]. So let

$$g_2(n) := \Big\lfloor \Big(1 + \frac{2n - 3\lfloor n/2 \rfloor - 1}{2n - \lfloor n/2 \rfloor - 1}\Big) \cdot \binom{n-2}{\lfloor (n-2)/2 \rfloor} \Big\rfloor, \tag{2.5}$$

$$g_3(n) := \Big\lfloor \frac{n}{3n - 2 - 2\lfloor n/2 \rfloor} \cdot \binom{n-1}{\lfloor (n-1)/2 \rfloor} \Big\rfloor, \text{ and} \tag{2.6}$$

$$g_4(n) := \Big\lfloor \frac{\lceil n/2 \rceil}{4n - 3\lfloor n/2 \rfloor - 3} \cdot \binom{n}{n/2} \Big\rfloor. \tag{2.7}$$

Note that $f_r(n)$ is defined in a simpler way in [5] than here. For $r \in \{2,3\}$, all the three parts of the theorem below have been proved in [5]. Further comments on the relation of this theorem to earlier results and methods will be enlightened in the last paragraph of Section 4.

Theorem 2.3. *Let $r, n \in \mathbb{N}^+$ such that $2 \le r \le n$.*

(A) *$f_r(n) \le \sigma(F^{(r)}, B_n)$.*

(B) *Keeping r fixed, $f_r(n)$ is asymptotically $\sigma(F^{(r)}, B_n)$, that is, we have that $\lim_{n\to\infty} \sigma(F^{(r)}, B_n)/f_r(n) = 1$.*

(C) *For $r \in \{2,3\}$ and $n \in \mathbb{N}^+ \setminus [r]$, and also for $r = 4$ and $n \in \mathbb{N}^+ \setminus [6]$, (f_r, g_r) is a reasonable pair of estimates of $\sigma(F^{(r)}, B_n)$ in the sense of Definition 2.1 and, furthermore, $g_r(n)$, $f_r(n)$, and $\sigma(F^{(r)}, B_n)$ are asymptotically equal.*

To make the connection between this theorem and the title of the paper conspicuous, we formulate the following corollary right here.

Corollary 2.4 ([5]). (A) *Let $r, k \in \mathbb{N}^+ \setminus \{1\}$. If n denotes the smallest natural number such that $k < f_r(n)$, then $\gamma(B^k_{r,0}) \leq n$; in particular, the direct power $B^k_{r,0}$ has an n-element generating set.*

(B) *Let $r \in \{2, 3, 4\}$ and $6 \leq k \in \mathbb{N}^+$. Again, let n be the smallest natural number such that $k < f_r(n)$. Then either $g_r(n-1) < k$ and $\gamma(B^k_{r,0}) = n$, or $k \leq g_r(n-1)$ and $\gamma(B^k_{r,0}) \in \{n-1, n\}$.*

3 Proofs

Proof of Theorem 2.3. Let A be an n-element set and denote $\lfloor n/r \rfloor$ by q. Partition A into (pairwise disjoint) r-element subsets $A_0, \ldots A_{q-1}$ and an $(n - r\lfloor n/r \rfloor)$-element remainder set A_q. (If r divides r, then $A_q = \emptyset$ and the partition is $\{A_0, \ldots, A_{q-1}\}$.) The elements of A_i will be denoted by $u^{(i)}_1$, $\ldots$, $u^{(i)}_r$. For a given $i \in \{0, \ldots, q-1\}$ and $(w_2, \ldots, w_r) \in \{0, \ldots, i\}^{r-1}$ such that $w_2 + \cdots + w_r = i$, pick a vector $\vec{s} := (s_0, \ldots, s_{i-1}) \in \{2, \ldots, r\}^i$ such that w_2 many components of $\vec{s}$ equal 2, w_3 many equal 3, $\ldots$, $|\{\iota : s_\iota = r\}| = w_r$. There are $\frac{i!}{w_2! \ldots w_r!}$ ways to pick such an $\vec{s}$, and this is why $\frac{i!}{w_2! \ldots w_r!}$ occurs in (2.3). For $\alpha \in \{0, \ldots, i-1\}$, pick an s_α-element subset B_α of A_α; this can be done in $\binom{r}{s_\alpha}$ many ways. Observe that $\prod_{\alpha=0}^{i-1} \binom{r}{s_\alpha}$ is the same as $\prod_{\beta=2}^{r} \binom{r}{\beta}^{w_\beta}$ in (2.3), whence the latter shows how many ways $(B_0, \ldots, B_{i-1})$ can be chosen. Letting $z := 1 - p + \lfloor (n-r)/2 \rfloor$, we also pick a $(z - 2w_2 - 3w_3 - \cdots - rw_r)$-element subset B_i of $A_{i+1} \cup \cdots \cup A_q$. Note that

$$|B_i| = z - 2w_2 - 3w_3 - \cdots - rw_r = z - s_0 - s_1 - \cdots - s_{i-1}. \tag{3.1}$$

Since $A_{i+1} \cup \cdots \cup A_q = A \setminus (A_0 \cup \ldots A_i)$ consists of $n - (i+1)r$ elements, the first binomial coefficient in (2.3) shows how many ways we can choose B_i. (As (2.2) shows, "no way" is possible but it does not disturb our argument.) Now let $\vec{B} := (B_0, \ldots, B_i)$. We call any vector obtained in this way an *eligible set vector*. For a given $\vec{s}$, the second line of (2.3) shows how many ways we can pick $\vec{B}$ while its first line shows how many ways i and $(w_2, \ldots, w_r)$ can be chosen. Furthermore, $\vec{B}$ determines $\vec{s} = (|B_0|, \ldots, |B_{i-1}|)$, $(w_2, \ldots, w_r)$, and i, whereby it follows that (2.3), that is $f^{(p)}_r(n)$, is the number of eligible set vectors.

For an eligible set vector $\vec{B}$, let $Z_{\vec{B}}$ be the union of the components of $\vec{B}$. Then

$$\begin{aligned} &B_0 = Z_{\vec{B}} \cap A_0, \ldots, B_{i-1} = Z_{\vec{B}} \cap A_{i-1}, B_i = Z_{\vec{B}} \cap (A_{i+1} \cup \cdots \cup A_q), \\ &\text{so the sets } B_0, \ldots, B_i \text{ are pairwise disjoint and their union is } Z_{\vec{B}}. \end{aligned} \tag{3.2}$$

Since $\vec{B}$ determines i (the number of its components minus 1), we can write that $i = i(\vec{B})$. With $i = i(\vec{B})$, we define, for $\rho \in [r]$,

$$U_{\vec{B}}^{(\rho)} := Z_{\vec{B}} \cup \{u_\rho^{(i)}\}. \text{ Let } F_{\vec{B}}^{(r)} := \big\{Z_{\vec{B}}, U_{\vec{B}}^{(1)}, \ldots, U_{\vec{B}}^{(r)}\big\}. \tag{3.3}$$

It follows from (3.2) that for any $\rho \in [r]$,

$$\begin{array}{l}\text{the sets } B_0, \ldots, B_i, \text{ and } \{u_\rho^{(i)}\} \text{ are pair-}\\ \text{wise disjoint and their union is } U_{\vec{B}}^{(\rho)}.\end{array} \tag{3.4}$$

It is clear by (3.1) and (3.2) that[1]

$$|Z_{\vec{B}}| = z, \text{ so it does not depend on } \vec{B}. \tag{3.5}$$

Since $Z_{\vec{B}} \cap A_i = \emptyset$, $F_{\vec{B}}^{(r)}$ is copy of $F^{(r)}$. Thus, in order to show that $f_r^{(p)}(n)$ is a lower bound of $\sigma(F^{(r)}, B_n)$, it suffices to show that whenever $\vec{C}$ is an eligible set vector different from $\vec{B}$, then $F_{\vec{B}}^{(r)}$ and $F_{\vec{C}}^{(r)}$ are unrelated. To do so, let $j := i(\vec{C})$, the number of components of $\vec{C}$ minus 1; then we can write that $\vec{C} = (C_0, \ldots, C_j)$. Assume that $X \in F_{\vec{B}}^{(r)}$ and $Y \in F_{\vec{C}}^{(r)}$; our task it to show that $X \parallel Y$. Depending on i and j, there are two cases to consider: either $i = j$ or, by symmetry, $i < j$.

Case 1 (where $i = j$). As $\vec{B} \neq \vec{C}$, there is an $\alpha \in \{0, \ldots, i\}$ such that $B_\alpha \neq C_\alpha$. If $B_\alpha \parallel C_\alpha$, then $X \cap A_\alpha = B_\alpha \parallel C_\alpha = Y \cap A_\alpha$ implies that $X \parallel Y$ provided that $\alpha < i$. Changing "$\cap A_\alpha$" to "$\cap (A_{i+1} \cup \cdots \cup A_q)$", we draw the same conclusion if $\alpha = i$. Hence, we can assume that B_α and C_α are comparable, say, $B_\alpha \subset C_\alpha$. Then $|B_\alpha| < |C_\alpha|$, which together with $|B_0| + \cdots + |B_i| = |Z_{\vec{B}}| = z = |Z_{\vec{C}}| = |C_0| + \cdots + |C_i|$ yield a subscript $\beta \in \{0, \ldots, i\} \setminus \{\alpha\}$ such that $|C_\beta| < |B_\beta|$. Now $X \subseteq Y$ would lead to $B_\beta = X \cap A_\beta \subseteq Y \cap A_\beta = C_\beta$, contradicting the inequality $|C_\beta| < |B_\beta|$ while $Y \subseteq X$ would similarly violate that $|B_\alpha| < |C_\alpha|$. Thus, $X \parallel Y$ and $F_{\vec{B}}^{(r)}$ is unrelated to $F_{\vec{C}}^{(r)}$, completing Case 1.

Case 2 (where $i < j$). As $Y \cap A_i = C_i$ has at least two elements but $X \cap A_i$ is either the empty set or it is a singleton set of the form $\{u_\rho^{(i)}\}$, we have that $Y \nsubseteq X$. For the sake of contradiction, suppose that $X \subset Y$. As $Z_{\vec{B}} \subseteq X$, we also have that $Z_{\vec{B}} \subset Y$. Let $Z_{\vec{B}}^{\text{up}} = Z_{\vec{B}} \cap (A_{i+1} \cup \cdots \cup A_q) = B_i$, $Z_{\vec{B}}^{\text{mid}} = Z_{\vec{B}} \cap A_i$, and $Z_{\vec{B}}^{\text{dn}} = Z_{\vec{B}} \cap (A_0 \cup \cdots \cup A_{i-1})$. Using i again rather than j, let

[1] In addition to the fact that we do not use iteration and our construction is simpler, this is where our proof differs from that in Dove and Griggs, where several "layers" are populated.

$Y^{\rm up} = Y \cap (A_{i+1} \cup \cdots \cup A_q)$, $Y^{\rm mid} = Y \cap A_i$, $Y^{\rm dn} = Y \cap (A_0 \cup \cdots \cup A_{i-1})$. Clearly, $Z_{\vec{B}}^{\rm up} \subseteq Y^{\rm up}$, $Z_{\vec{B}}^{\rm mid} \subseteq Y^{\rm mid}$, and $Z_{\vec{B}}^{\rm dn} \subseteq Y^{\rm dn}$. These inequalities together with the equalities $Z_{\vec{B}} = Z_{\vec{B}}^{\rm up} \cup Z_{\vec{B}}^{\rm mid} \cup Z_{\vec{B}}^{\rm up}$ and $Y = Y^{\rm up} \cup Y^{\rm mid} \cup Y^{\rm dn}$ imply that $Y \setminus Z_{\vec{B}} \supseteq Y^{\rm mid} \setminus Z_{\vec{B}}^{\rm mid} = C_i \setminus \emptyset = C_i$. Hence, $|Y| - |Z_{\vec{B}}| = |Y \setminus Z_{\vec{B}}| \geq |C_i| \geq 2$. This contradicts (3.5) since $|Y|$ differs from $|Z_{\vec{C}}|$ (and thus from $|Z_{\vec{B}}|$) by at most 1. The contradiction we have obtained shows that $X \parallel Y$, completing Case 2.

Having just seen that $F_{\vec{B}}^{(r)}$ and $F_{\vec{C}}^{(r)}$ are unrelated, we have proved that, for every meaningful p, $f_r^{(p)}(n)$ is a lower bound of $\sigma(F^{(r)}, B_n)$. So is the maximum $f_r(n)$ of these $f_r^{(p)}(n)$'s, proving part (A) of Theorem 2.3.

The proof of part (B) uses the previous notation $z := 1 - p + \lfloor (n - r)/2 \rfloor$ and the folkloric fact[2] that for any integers α and β, $\binom{n-\alpha}{\lfloor (n-\alpha)/2 \rfloor - \beta}$ is asymptotically $\binom{n}{\lfloor n/2 \rfloor} \cdot 2^{-\alpha}$. So for every fixed $i \in \mathbb{N}^+$ and each small positive real number ϵ,

$$\begin{aligned} &(1-\epsilon)\binom{n-(i'+1)r}{z-2w_2-3w_3-\cdots-rw_r} \\ &\qquad < 2^{-(i'+1)r}\binom{n}{\lfloor n/2 \rfloor} < \qquad \text{for } i' \in \{0,1,\ldots,i\} \qquad (3.6) \\ &(1+\epsilon)\binom{n-(i'+1)r}{z-2w_2-3w_3-\cdots-rw_r} \end{aligned}$$

holds for all but finitely many n. Letting

$$\kappa(n) := \sum_{i=0}^{\lfloor n/r \rfloor - 1} \sum_{\substack{(w_2,\ldots,w_r) \in \{0,\ldots,i\}^{r-1} \\ w_2+\cdots+w_r = i}} \frac{i!}{w_2! \ldots w_r!} 2^{-(i+1)r} \binom{n}{\lfloor n/2 \rfloor} \prod_{\beta=2}^{r} \binom{r}{\beta}^{w_\beta}$$

and applying (3.6) to the inner summation in (2.3), it follows that

$$(1-\epsilon) f_p^{(r)}(n) \leq \kappa(n) \leq (1+\epsilon) f_p^{(r)}(n). \qquad (3.7)$$

[2]This folkloric fact was used by, say, Dove and Griggs [8], Katona and Nagy [12], and [5, 6]

Using the multinomial theorem and $\sum_{\beta=0}^{r}\binom{r}{\beta}=2^r$, we obtain that

$$\kappa(n)=\frac{1}{2^r}\binom{n}{\lfloor n/2\rfloor}\sum_{i=0}^{\lfloor n/r\rfloor-1}\frac{1}{2^{ir}}\sum_{\substack{(w_2,\dots,w_r)\in\{0,\dots,i\}^{r-1}\\ w_2+\dots+w_r=i}}\frac{i!}{w_2!\dots w_r!}\prod_{\beta=2}^{r}\binom{r}{\beta}^{w_\beta}$$

$$=\frac{1}{2^r}\binom{n}{\lfloor n/2\rfloor}\sum_{i=0}^{\lfloor n/r\rfloor-1}\frac{1}{2^{ir}}\Big(\sum_{\beta=2}^{r}\binom{r}{\beta}\Big)^i$$

$$=\frac{1}{2^r}\binom{n}{\lfloor n/2\rfloor}\sum_{i=0}^{\lfloor n/r\rfloor-1}\frac{1}{2^{ir}}(2^r-r-1)^i=\frac{1}{2^r}\binom{n}{\lfloor n/2\rfloor}\sum_{i=0}^{\lfloor n/r\rfloor-1}\Big(\frac{2^r-r-1}{2^{ir}}\Big)^i.$$

Adding to this calculation that $\sum_{i=0}^{\infty}\Big(\frac{2^r-r-1}{2^r}\Big)^i=\sum_{i=0}^{\infty}\Big(1-\frac{r+1}{2^r}\Big)^i=\frac{2^r}{r+1}$, we obtain that

$$(1-\epsilon)\kappa(n)\le\frac{1}{2^r}\binom{n}{\lfloor n/2\rfloor}\frac{2^r}{r+1}\le(1+\epsilon)\kappa(n). \tag{3.8}$$

Combining (3.7) with (3.8), we have that

$$(1-\epsilon)^2 f_r^{(p)}(n)\le\frac{1}{r+1}\binom{n}{\lfloor n/2\rfloor}\le(1+\epsilon)^2 f_r^{(p)}(n) \tag{3.9}$$

for all but finitely many n. Letting ϵ tend to 0, (3.9) implies that $f_r^{(p)}(n)$ is asymptotically $\frac{1}{r+1}\binom{n}{\lfloor n/2\rfloor}$. Applying Katona and Nagy [12, Theorem 1.1] or Dove and Griggs [8, Theorem 1.4] to our poset $F^{(r)}$, we know that $\sigma(F^{(r)},B_n)$ is asymptotically $\frac{1}{r+1}\binom{n}{\lfloor n/2\rfloor}$, too. Hence, part (B) of the theorem follows by transitivity.

Next, we turn our attention to the upper bounds. As the case $r\in\{2,3\}$ has been settled in [5], we restrict ourselves to the case $r=4$. For $4\le n\in\mathbb{N}^+$, let our base set $A:=|n]=\{1,2,\dots,n\}$ and let $k:=\sigma(F^{(4)},B_n)$. As it happened first in Lubell [13] and then in Griggs, Stahl, and Trotter [11], [5], and [6], and with some terminological change, in Bollobás [2], Dove and Griggs [8], and Katona and Nagy [12], we also define a set of permutations of $[n]$ as follows. For $X\subseteq A$,

$$\begin{aligned}&\text{let } \Psi(X) \text{ consist of all those permutations } \vec{\pi}=\\ &(\pi_1,\dots,\pi_n) \text{ that satisfy } \{\pi_1,\dots,\pi_{|X|}\}=X.\end{aligned} \tag{3.10}$$

All the just listed papers use the obvious fact that for $X\parallel Y\in\mathsf{P}([n])$, we have that $\Psi(X)\cap\Psi(Y)=\emptyset$. However, our situation needs some preparation.

Let $W \subseteq \mathsf{P}([n])$ be a copy of $F^{(4)}$, and pick an order isomorphism $\varphi\colon F^{(4)} \to W$. (There are $4! = 24$ such isomorphisms but no matter which one we take.) We call W a *cover-preserving copy* of $F^{(4)}$ if for all $x, y \in F^{(4)}$, if y covers x (in notation, $x \prec y$), then $\varphi(x) \prec \varphi(y)$. While this definition reflects generality, note that W_i is a cover-preserving copy of $F^{(4)}$ if and only if it is of the form

$$W_i = \{Z_i, Z_i \cup \{u_1^{(i)}\}, Z_i \cup \{u_2^{(i)}\}, Z_i \cup \{u_3^{(i)}\}, Z_i \cup \{u_4^{(i)}\}\} \tag{3.11}$$

where none of the elements $u_1^{(i)}$, $u_2^{(i)}$, $u_3^{(i)}$, and $u_4^{(i)}$ is in the set $Z_i \in \mathsf{P}(A)$ and these four elements are pairwise distinct. The key of our argument is the following statement, for the sake of which we interrupt the proof of Theorem 2.3.

Lemma 3.1. *If there are m pairwise unrelated copies of $F^{(4)}$ in B_n, then there are m pairwise unrelated* cover-preserving *copies of $F^{(4)}$ in B_n, too.*

Note here that this lemma fails for $F^{(r)}$ if $r \geq 5$. (For $r = 5$, this is witnessed by a 5-element antichain in B_4 together with the bottom element.) This is why Part (C) of Theorem 2.3 is restricted to $r \leq 4$.

Proof of Lemma 3.1. As the first step in the argument, recall that the *convex hull* of an $X \subseteq \mathsf{P}(A)$ is $\mathrm{Cnv}(X) := \{R \in \mathsf{P}(A) : \exists S, T \in X \text{ such that } S \subseteq R \subseteq T\}$. Clearly, if X and Y are unrelated members of $\mathsf{P}(A)$, then $\mathrm{Cnv}(X)$ and $\mathrm{Cnv}(Y)$ are also unrelated; this fact was heavily used in Dove and Griggs [8] and in Katona and Nagy [12]. Assume that $W_1, \ldots, W_m$ are pairwise unrelated copies of $F^{(4)}$ in $\mathsf{P}(A)$. If each of them is of the form (3.11), then there is nothing to prove. So assume that W_i is not of this form for some $i \in [m]$. Then $W_i = \{Z_i, Z_i \cup U_1^{(i)}, Z_i \cup U_2^{(i)}, Z_i \cup U_3^{(i)}, Z_i \cup U_4^{(i)}\}$ for some sets $U_1^{(i)}, \ldots, U_4^{(i)} \in \mathsf{P}(A)$ that are disjoint from Z_i and form an antichain. Letting $U := U_1^{(i)} \cup U_2^{(i)} \cup U_3^{(i)} \cup U_4^{(i)}$, the sets $U_1^{(i)}, \ldots, U_4^{(i)} \in \mathsf{P}(A)$ are also in $\mathsf{P}(U)$ and they are pairwise unrelated. Hence, it follows from Sperner's theorem, see the sentence right after (1.2), that $|U| \geq 4$. Hence, we can simply take four distinct elements $u_1^{(i)}, u_2^{(i)}, u_3^{(i)}, u_4^{(i)} \in U$ and then

$$W_i' := \{Z_i, Z_i \cup \{u_1^{(i)}\}, Z_i \cup \{u_2^{(i)}\}, Z_i \cup \{u_3^{(i)}\}, Z_i \cup \{u_4^{(i)}\}\}$$

is such a copy of $F^{(4)}$ that is included in $\mathrm{Cnv}(W_i)$. Thus, we can change W_i to W_i', and we can do so for the rest of subscripts, one by one, until all the m copies of $F^{(4)}$ become cover-preserving. These copies remain pairwise unrelated, completing the proof of Lemma 3.1. □

Resuming the proof of Theorem 2.3, Lemma 3.1 allows us to assume that all the W_i are cover-preserving copies, that is, (3.11) holds for all $i \in [k]$. For $i \in [k]$, based on (3.10), we let $\Phi_i := \bigcup_{X \in W_i} \Psi(X)$. For $i \neq j \in [k]$, $X \in W_i$, and $Y \in W_j$, we have that $\Psi(X) \cap \Psi(Y) = \emptyset$ by the fact mentioned right after (3.10). Hence, $\Phi_i \cap \Phi_j = \emptyset$. Letting $x_i := |Z_i|$, we know (either from Lubell [13] or by a trivial argument) that $|\Psi(Z_i)| = x_i!(n-x_i)!$. Similarly, $|\Psi(Z_i \cup \{u_j^{(i)}\})| = (x_i+1)!(n-x_i-1)!$ for $j \in [4]$. A permutation $(\pi_1, \ldots, \pi_n)$ belongs to both $\Psi(Z_i)$ and $\Psi(Z_i \cup \{u_j^{(i)}\})$ if and only if $(\pi_1, \ldots, \pi_{x_i})$ is a permutation of Z_i, this can happen in $x_i!$ many ways, $\pi_{x_i+1} = u_j^{(i)}$, and $(\pi_{x_i+2}, \ldots, \pi_n)$ is a permutation of $[n] \setminus (Z_i \cup \{u_j^{(i)}\})$, which can happen in $(n-x_i-1)!$ ways. Hence, $|\Psi(Z_i) \cap \Psi(Z_i \cup \{u_j^{(i)}\})| = x_i!(n-x_i-1)!$ for every $j \in [4]$. That is all we have to know in order to apply the inclusion-exclusion principle to obtain $|\Phi_i|$ since whenever $T \subseteq W_i$ is not a chain, then the sentence following (3.10) yields that $|\bigcap_{X \in T} \Psi(X)| = 0$. Thus, we obtain that

$$\begin{aligned} |\Phi_i| &= x_i!(n-x_i)! + 4(x_i+1)!(n-x_i-1) - 4x_i!(n-x_i-1)! \\ &= (n+3x_i)x_i!(n-x_i-1)! =: h_1(x_i) \end{aligned} \tag{3.12}$$

for every $i \in [k]$. We consider h_1 given in (3.12) an $\mathbb{N}_0 \to \mathbb{N}_0$ function. Straightforward computation shows that $h_1(x+1) - h_1(x) = h_2(x)x!(n-x-2)!$ with $h_2(x) = 6x^2+(9-n)x+(3+2n-n^2)$ provided that $0 \leq x \leq n-2$. The nonnegative root of h_2 is

$$x_0 = \frac{n-9+\sqrt{25n^2-66n+9}}{12}.$$

As $(5n-7)^2 - (25n^2-66n+9) = 40-4n < 0$ if $n \geq 11$, we have that $5n-7 < \sqrt{25n^2-66n+9}$ for $n \geq 11$. Similarly, $(5n-6)^2-(25n^2-66n+9) = 6n+27 > 0$ gives that $\sqrt{25n^2-66n+9} < 5n-6$ for $n \geq 2$. Using these two inequalities, we obtain that $(6n-16)/12 < x_0 < (6n-15)/12$ for $n \geq 11$. This implies that $x_0 < \lceil x_0 \rceil = \lfloor (n-1)/2 \rfloor$. Since h_2 is a quadratic function of x and so its graph is well known, the smallest $m \in \mathbb{N}_0$ for which $h_2(m)$ is positive, that is, $h_1(m+1) - h_1(m) > 0$, is $m = \lfloor (n-1)/2 \rfloor$. Therefore, the minimum value of $|\Phi_i| = h_1(x_i)$ is $h_1(\lfloor (n-1)/2 \rfloor)$ provided that $n \geq 11$. The same holds for $n \in \{4, \ldots, 10\}$; this follows by listing $h_1(0)$, $\ldots$, $h_1(n-1)$ for these small n's.

Since the Φ_i's, for $i \in [k]$, are pairwise disjoint subsets of the $n!$-element set of all permutations of $[n]$ and the minimum of $|\Phi_i|$ is $h_1(\lfloor (n-1)/2 \rfloor)$, it

follows that

$$\sigma(F^{(4)}, B_n) = k = \Big\lfloor \frac{k \cdot h_1(\lfloor (n-1)/2 \rfloor)}{h_1(\lfloor (n-1)/2 \rfloor)} \Big\rfloor = \Big\lfloor \frac{\sum_{i=1}^{k} h_1(\lfloor (n-1)/2 \rfloor)}{h_1(\lfloor (n-1)/2 \rfloor)} \Big\rfloor$$
$$\leq \Big\lfloor \frac{\sum_{i=1}^{k} |\Phi_i|}{h_1(\lfloor (n-1)/2 \rfloor)} \Big\rfloor \leq \Big\lfloor \frac{n!}{h_1(\lfloor (n-1)/2 \rfloor)} \Big\rfloor$$
$$= \Big\lfloor \binom{n}{\lfloor n/2 \rfloor} \frac{\lfloor n/2 \rfloor! (n - \lfloor n/2 \rfloor)!}{h_1(\lfloor (n-1)/2 \rfloor)} \Big\rfloor . \tag{3.13}$$

Let us focus on the last (complicated) fraction in (3.13). For $n = 2n$ even, (3.12) and (3.13) allow us to compute it as follows:

$$\frac{m!m!}{h_1(m-1)} = \frac{m!m!}{(2m + 3(m-1))(m-1)!m!}$$
$$= \frac{m(m-1)!m!}{(5m-3)(m-1)!m!} = \frac{m}{5m-3} = \frac{\lceil n/2 \rceil}{4n - 3\lfloor n/2 \rfloor - 3},$$

as (2.7) requires. Similarly, for $n = 2m + 1$ odd,

$$\frac{m!(m+1)!}{h_1(m)} = \frac{m!(m+1)!}{(2m+1+3m)m!m!} = \frac{m+1}{5m+1} = \frac{\lceil n/2 \rceil}{4n - 3\lfloor n/2 \rfloor - 3},$$

as required. We have shown that $g_4(n)$ is an upper bound of $\sigma(F^{(4)}, B_n)$.

We have seen that, for $r \in \{2, 3, 4\}$, (f_r, g_r) is a pair of estimates of $\sigma(F^{(r)}, B_n)$. For $r \in \{2, 3\}$, [5] proves that this pair is reasonable. The very tedious details of showing exactly that (f_4, g_4) is a *reasonable* pair of estimates of the function $n \mapsto \sigma(F^{(4)}, B_n)$ would hardly be appetizing for the reader. Hence, we only outline the idea; asymptotic equalities will be denoted $\sim$. We have already shown that $f_4(n) \sim \sigma(F^{(4)}, B_n) \sim \frac{1}{r+1}\binom{n}{\lfloor n/2 \rfloor} = \frac{1}{5}\binom{n}{\lfloor n/2 \rfloor}$. Clearly, $g_4(n) \sim \frac{1}{5}\binom{n}{\lfloor n/2 \rfloor}$. Combining these asymptotic equalities with the folkloric fact mentioned in Footnote 2, we obtain that $f_4(n+1)/2 \sim g_4(n)$. Parsing the proofs of the asymptotic equalities involved, we can find an $n_0 \in \mathbb{N}^+$ such that the required inequality $g_4(n) \leq f_4(n+1)$ holds for all $n \geq n_0$. By our computer-generated data, see Section 4, it also holds for $n \in \{7, 8, \ldots, n_0 - 1\}$.

Modulo the previous paragraph, we have proved Theorem 2.3. □

Proof of Corollary 2.4. It is clear that the proof given in [5] works for any pair of reasonable estimates; see also Fact 2.2. Hence, no proof is necessary here. However, we enlighten the (trivial) idea by two examples, namely, by the direct powers $B_{4,0}^{2023}$ and $B_{4,0}^{2500}$. As Table 1 shows, $\sigma(F^{(4)}, B_{15}) \leq g_4(15) =$

1430 while $2448 = f_4(16) \leq \sigma(F^{(4)}, B_{16})$. Hence, the smallest n for which $2023 \leq \sigma(F^{(4)}, B_n)$ is $n = 16$. Applying (1.3) and taking $F^{(4)} \cong J(B_{4,0})$ into account, we obtain that $\gamma(B_{4,0}^{2023}) = 16$.

In case of 2500, we obtain from Table 1 only that $\sigma(F^{(4)}, B_{15}) \leq g_4(15) = 1430 < 2500$ and $2500 \leq 4696 = f_4(17) \leq \sigma(F^{(4)}, B_{17})$. Hence, the smallest n for which $2500 \leq \sigma(F^{(4)}, B_n)$ is either 16 or 17. Therefore, $\gamma(B_{4,0}^{2500}) \in \{16, 17\}$. □

4 Odds and ends

To obtain the data of this section, we used a computer algebraic program, namely, Maple V Release 5 Version 5.00 (November 27, 1997) of Waterloo Maple Inc. and a desktop computer with AMD Ryzen 7 2700X Eight-Core Processor 3.70 GHz. Our program that Maple executed is given in the (Appendix) Section 5.

n	4	5	6	7	8	9	10	11	12	13	14	15
$f_4(n)$	1	1	2	3	12	20	36	66	159	315	558	1113
$g_4(n)$	1	2	5	8	16	30	57	106	205	387	750	1430

n	16	17	18	19	20	21	22
$f_4(n)$	2 448	4 696	8 926	17 310	36 560	69 410	136 710
$g_4(n)$	2 782	5 336	10 418	20 082	39 309	76 076	149 226

n	23	24	25	26	27
$f_4(n)$	262 250	542 000	1 031 500	2 062 036	3 949 288
$g_4(n)$	289 731	569 296	1 108 260	2 180 770	4 254 790

n	28	29	30
$f_4(n)$	8 070 468	15 625 260	31 038 651
$g_4(n)$	8 382 573	16 385 653	32 316 150
$g_4(n)/f_4(n) \approx$	1.038 672 478	1.048 664 342	1.041 158 329

Table 1: Some values of $f_4(n)$ and $g_4(n)$.

Corollary 2.4 together with Table 2 yield that, say,

$$\gamma(B_{4,0}^{10^{299}}) = 1001 \tag{4.1}$$

(there is no misrpint here, the exponent of the 5-element lattice $B_{4,0}$ consists of 300 decimals). However, even Table 1 is sufficient for anything related

to our motivation, cryptography and authentication. Indeed, this table and Corollary 2.4 gives that, say,

$$\gamma(B_{4,0}^{30\,000\,000}) = 30. \tag{4.2}$$

This is a $5^{30\,000\,000}$-element lattice generated only by 30 elements; this lattice is (more than) large enough to provide crpytographic security.

The computation for Table 1 took only one second while that for Table 2 needed 215 minutes. A trivial algorithm based on excluding all the 29-element subsets and listing some 30-element subsets until a generating one is found could not prove that $\gamma(B_{4,0}^{30\,000\,000}) = 30$, which is now a simple consequence of the "one second table" (Table 1) and Corollary 2.4.

n	100	200	300
$f_4(n) \approx$	$2.022\,665 \cdot 10^{28}$	$1.813\,143 \cdot 10^{58}$	$1.876\,694 \cdot 10^{88}$
$g_4(n) \approx$	$2.042\,335 \cdot 10^{28}$	$1.821\,902 \cdot 10^{58}$	$1.882\,725 \cdot 10^{88}$
$\frac{g_4(n)}{f_4(n)} \approx$	1.009724683	1.004830944	1.003 213 720

n	400	500	600
$f_4(n) \approx$	$2.060\,285 \cdot 10^{118}$	$2.336\,007 \cdot 10^{148}$	$2.703\,240 \cdot 10^{178}$
$g_4(n) \approx$	$2.065\,246 \cdot 10^{118}$	$2.340\,504 \cdot 10^{148}$	$2.707\,574 \cdot 10^{178}$
$\frac{g_4(n)}{f_4(n)} \approx$	1.002 407 708	1.001 924 929	1.001 603 422

n	700	800	900
$f_4(n) \approx$	$3.172\,574 \cdot 10^{208}$	$3.761\,977 \cdot 10^{238}$	$4.496\,142 \cdot 10^{268}$
$g_4(n) \approx$	$3.176\,932 \cdot 10^{208}$	$3.766\,499 \cdot 10^{238}$	$4.500\,945 \cdot 10^{268}$
$\frac{g_4(n)}{f_4(n)} \approx$	1.001 373 942	1.001 201 923	1.001 068 186

n	1000	1001	1002
$f_4(n) \approx$	$5.407\,062 \cdot 10^{298}$	$1.080\,764 \cdot 10^{299}$	$2.160\,665 \cdot 10^{299}$
$g_4(n) \approx$	$5.412\,260 \cdot 10^{298}$	$1.081\,801 \cdot 10^{299}$	$2.162\,738 \cdot 10^{299}$
$\frac{g_4(n)}{f_4(n)} \approx$	1.000 961 231	1.000 960 076	1.000 959 310

Table 2: Some approximate values of $f_4(n)$ and $g_4(n)$.

Next, we comment on the parameter p in (2.4). Experiencing with computer, we conjecture that for $r = 4$ and $n \geq 29$, the maximum is achieved at $p = 0$ if n is even and at $p = -1$ if n is odd. This has been verified for many values of n, the largest two being 1000 and 1001. (For $n \in \{1000, 1001\}$, the computer checked each p in $\{-10, -9, \ldots, 5\}$; this took 233 minutes.) For small n's (and still $r = 4$), the situation shows not much regularity; for

example, $p = 1$ gives the maximum for $n \in \{4, 5, \ldots, 8\}$ while $p = 0$ for $n \in \{16, 17, \ldots, 24\}$. Even if this conjecture fails for some (very large) n, we obtain a good (and asymptotically optimal) lower bound going after it.

We also guess that, for $r \in \{2, 3, 4\}$, $\sigma(F^{(r)}, B_n)$ is closer the $f_r(n)$ than to $g_4(n)$. For $r = 2$, as we have mentioned after (1.4), Katona and Nagy [12] conjectured that $\sigma(F^{(2)}, B_n) = f_2(n)$.

Calculating with (small) concrete numbers appears to be more difficult than doing it asymptotically. For example, while the folkloric fact mentioned in Footnote 2 provided a substantial simplification when proving the asymptotic part of our theorem, see around (3.6), we have no similar tool when n does *not* tend to ∞. In addition to (1.5), this is our excuse that, opposed to the asymptotic equalities proved in Dove and Griggs [8] and Katona and Nagy [12], the present paper deals only with estimates. On the other hand, let us emphasize that our proof contains many ideas taken from these two papers; we mentioned some of them while proving Theorem 2.3. Here we add that, like in the present paper, both [8] and [12] partition $A = [n]$ into r-element subsets, embed a poset (playing the role of $F^{(r)}$) into the powerset of one of these subsets, and modify these initial embeddings according to their strategies. However, there are differences, Footnote 1 mentions some of them. Computation shows that for a small n, our $f_r(n)$ is better (that is, larger) than what could be extracted from [12].

5 Appendix

We conclude the paper by presenting the Maple program that computed Tables 1 and 2; the limits (now 4 and 30) of the last "for" loop can be modified, of course. As our comment on the parameter p in the previous section indicates, the limit of the "for" loop with p could be "from -1 to 1" without changing the output of the program.

```
> restart; with(combinat, multinomial):
> time0:=time();
> fp4:=proc(n,p) local s,i,w2,w3,w4,z,r;
>  r:=4; z:=1-p+floor((n-r)/2); s:=0;
>  for i from 0 to floor(n/r)-1 do
>   for w2 from 0 to i do
>    for w3 from 0 to i-w2 do
>     w4:=i-w2-w3;
>     s:=s + multinomial(i,w2,w3,w4)*
>      binomial(n-(i+1)*r,z-2*w2-3*w3-4*w4)*
>      binomial(r,2)^w2*binomial(r,3)^w3*binomial(r,4)^w4;
```

```
>    od; #end of w3 loop
>   od; #end of w2 loop
>  od; #end of i loop
>  s:=s;
> end: #end of procedure fp4
>
> f4:=proc(n) local p,p0,b0,b,pfrom,pto; p0:=-1; b0:=0;
>  if n<50 then pfrom:=-10; pto:=10
>  else pfrom:=-4; pto:=2
>  fi;
>  for p from pfrom to pto do
>   b:=fp4(n,p);
>   if b>=b0 then b0:=b; p0:=p
>   fi;
>  od; #end of p cycle
>  # print(‘n=‘,n,‘ p=‘,p0,‘ f4(n)=‘,b0);
>     #print is invalidated after a test period
>  b:=b0;
> end: #end of procedure f4
>
> g4:=proc(n) local h; h:=floor(n/2);
>  floor( (ceil(n/2)/(4*n-3*h-3))*binomial(n,h) )
> end: #end of procedure g4
> #for n from 4 to 100 do f4(n): od:
> #for n from 4 to 100 do b:=f4(n) ;count:=0;
> # for p from -4 to 4 do if fp4(n,p)=b then count:=count+1 fi od;
> #  print(‘n=‘,n,‘          count=‘,count);
> # od:
>
> for n from 4 to 30 do lower:=f4(n): upper:= g4(n):
>  if lower>0 then ratio:=evalf(upper/lower)
>  else ratio:=undefined
>  fi :
>  print(‘n=‘, n, ‘ f4(n)=‘ ,lower, ‘ g4(n)=‘,
>      upper, ‘ ratio=‘, ratio);
>  if lower>10^6 then
>    print(‘lg(lower)=‘,evalf(log[10](lower)),
>      ‘lg(upper)=‘,evalf(log[10](upper)));
>  fi ;
> od:
> time1:=time();
> print(‘The total computation needed ‘, time1-time0,‘ seconds.‘);
```

References

[1] Anderson, I.: Combinatorics of Finite Sets. Dover Publications Inc., Mineola, New York, 2002.

[2] Bollobás, B.: Sperner systems consisting of pairs of complementary subsets. Journal of Combinatorial Theory (A) **15**, 363-366 (1973)

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

[4] G. Czédli: Generating Boolean lattices by few elements and a protocol for authentication and cryptography based on an NP-complete problem. arXiv:2303.10790 (extended version)

[5] 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

[6] G. Czédli: Minimum-sized generating sets of the direct powers of the free distributive lattice on three generators and a Sperner theorem. arXiv:2309.13783

[7] Dilworth, R. P.: A decomposition theorem for partially ordered sets. Ann. of Math. 51 (1951), 161–166.

[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)

[3] (Temporary note for the reviewer:) At the time of writing, see the menu item "Publications" in the author's website for a preprint.

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

[14] McKenzie, R.N., McNulty, G.F., Taylor, W.F.: Algebras, Lattices, Varieties. Vol. 1. Wadsworth & Brooks/Cole, Monterey, California, 1987

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

[16] Zádori, L.: Subspace lattices of finite vector spaces are 5-generated. Acta Sci. Math. (Szeged)[4] 74 (2008), 493–499

[4]At the time of writing, this paper and many other papers are freely available from the **old** site of the journal: http://www.acta.hu/ .