Distribution Agreement

Jeremy McKibben-Sanders   April 25, 2010

Some Quotients of the Boolean Lattice are Symmetric Chain Orders

by

Jeremy McKibben-Sanders

Advisor: Dwight Duffus

Department of Mathematics and Computer Science

Dwight Duffus

Advisor

Robert Roth

Committee Member

Christopher Curran

Committee Member

April 25, 2010

Some Quotients of the Boolean Lattice are Symmetric Chain Orders

by

Jeremy McKibben-Sanders

Advisor Dwight Duffus

Abstract of

A thesis submitted to the Faculty of Emory College

of Emory University in partial fulfillment

of the requirements of the degree of

Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2010

Abstract

Some Quotients of the Boolean Lattice are Symmetric Chain Orders

by

Jeremy McKibben-Sanders

R. Canfield has conjectured that for all subgroups G of the symmetric group S_n, the quotient B_n/G of the boolean lattice B_n is a symmetric chain order. We provide a straightforward proof of K. K. Jordan's result that B_n/G is a symmetric chain order when G is generated by an n-cycle, and we present a simple algorithm for finding a symmetric chain decomposition of B_n/G, beginning from the well-known symmetric chain decomposition of B_n obtained by Greene and Kleitman. We also verify Canfield's conjecture when G is generated by a set of pairwise disjoint transpositions, and provide an algorithm for finding a symmetric chain decomposition of B_n/G in this case as well.

Some Quotients of the Boolean Lattice are Symmetric Chain Orders

by

Jeremy McKibben-Sanders

Advisor : Dwight Duffus

A thesis submitted to the Faculty of Emory College

of Emory University in partial fulfillment

of the requirements of the degree of

Bachelors of Sciences with Honors

Department of Mathematics and Computer Science

2010

Contents

List of Figures

1 Introduction

Combinatorics is a branch of discrete mathematics that finds many applications in the areas of algebra, probability, topology, and computer science. Countable discrete structures such as partially ordered sets and lattices play a crucial role in the study of set systems, leading to many well known results such as Sperner's theorem on maximum-sized unordered families in a power set, Dilworth's max-min theorem on chain partitions, and Hall's matching theorem. The study of the properties and structures found on the Boolean lattice in particular is a fascinating and broad topic, involving contributions from such diverse areas as graph theory, topology, and linear algebra.

This thesis concerns an important notion of symmetry in a partially ordered set - the existence of symmetric chain decompositions. In particular, we are interested in finding symmetric chain decompositions of certain quotients of the Boolean lattice structure.

1.1 Basic Terminology

We begin with some important definitions. A *partial order* is a relation on a set S which is reflexive, antisymmetric, and transitive. In other words, if we denote the relation on S by $\leq$, then it satisfies the following conditions:

(1) $\forall x \in S$, $x \leq x$ (reflexivity)

(2) $\forall x, y \in S$, if $x \leq y$ and $y \leq x$, then $x = y$ (antisymmetry).

(3) $\forall x, y, z \in S$, if $x \leq y$ and $y \leq z$ then $x \leq z$ (transitivity).

A set with a partial order $\leq$ is called a *partially ordered set*, or *poset*, and is denoted $(S, \leq)$. Two common examples are the power set of a set under containment, and the set of positive divisors of a positive number m under divisibility, denoted $(D(m), |)$. To be more explicit concerning the latter example, let m be a positive integer and let $D(m)$ be the set of its positive divisors. Then we can define a partial order $|$ on $D(m)$ in the following way. For $a, b \in D(m)$, we say that *a divides* b, or $a|b$, if $b = ac$ for some positive integer c. Then the relation $|$ defines a partial order on $D(m)$, so $(D(m), |)$ is a poset.

In fact, both of the previous examples of posets $(S, \leq)$ have the additional properties that:

(1) $\forall x, y \in S$, the *least upper bound* of x, y exists (denoted $x \vee y$).

(2) $\forall x, y \in S$, the *greatest lower bound* of x, y exists (denoted $x \wedge y$).

Note that $x \vee y$ is the unique minimum of the elements of S that are greater than or equal to both x and y. Similarly, $x \wedge y$ is the unique maximum of the elements of S that are less than or equal to both x and y. A poset with the above two properties is known as a *lattice*. For example, in the power set of a set ordered by containment, set union provides the least upper bound of two subsets, and set intersection provides the greatest lower bound. In $(D(m), |)$, the least common multiple of two divisors of m provides the least upper bound, and the greatest common divisor provides the greatest lower bound.

Let $(S, \leq)$ be a poset with $x, y \in S$. We say that $x < y$ if $x \leq y$ and $x \neq y$. A *chain* in $(S, \leq)$ is a set $\{x_1, x_2, \ldots, x_n\} \subseteq S$ such that $x_1 < x_2 < \cdots < x_n$. If $x, y \in S$ and $x \leq y$ or $y \leq x$ then x and y are *comparable*, otherwise x and y are said to be *incomparable.* An *antichain* in S is a non-empty subset of S such that no two of its elements are comparable. If $x < y$, then y *covers* x if there is no z in S such that $x < z < y$. A chain $x_1 < x_2 < \ldots x_n$ in $(S, \leq)$ is said to be *saturated* if x_{i+1} covers x_i for $i \in \{1, 2, \ldots, n-1\}$.

If there exists a unique element x in S such that $x \leq y$ for all $y \in S$, then we call x the zero element of $(S, \leq)$ and denote it by 0. We define the *length* of a chain to be one less than its cardinality, and we consider a poset to be *ranked* if for any $x < y$ all saturated chains from x to y have the same length. In a ranked poset, we define the *rank*(x) for $x \in S$ to be the length of a saturated chain from x to 0. For example, if the poset in question is the power set of a finite set under containment, then the empty set is 0 and the rank of a subset is simply the number of elements it contains.

1.2 Symmetric Chain Decompositions

In a ranked poset the saturated chain $x_1 < x_2 < \cdots < x_k$ is a *symmetric chain* if $r(x_1) + r(x_k) = r(S)$, where $r(S)$ is the maximum rank in S. A *symmetric chain decomposition* or *SCD* of S is a partition of S into symmetric chains $C_1, C_2, \ldots, C_k$. A ranked poset that possesses a symmetric chain decomposition is known as a *symmetric chain order* or *SCO.* A *maximal* chain in a ranked poset is a chain containing exactly one element of every rank. Clearly a maximal chain is always saturated, but a saturated chain is not necessarily maximal.

Of particular importance to us is the poset known as the *Boolean lattice*, denoted B_n, which is the power set of the set $[n] = \{1, 2, \ldots, n\}$ ordered by containment. Clearly B_n is a ranked poset, with $\emptyset$ being the zero element, and $rank(A)$ equal to the cardinality of A, as noted above.

In fact, it was shown in 1951 by de Bruijn *et al.* that the lattice $(D(m), |)$ is a symmetric chain order [1]. This is of special interest to us because it is not hard to see that B_n is isomorphic to $D(m, |)$ when m is a square-free positive integer with n distinct prime factors, and hence B_n is a symmetric chain order for all positive integers n. To see that De Bruijn *et al.*'s result is true in the case of a square-free positive integer m, suppose that m has k distinct prime divisors $p_1, p_2, \ldots, p_k$. When $k = 1$ the result is clear, since 1 and p_1 are the only divisors of m and $D(p_1) = \{1, p_1\}$ can be partitioned into a single symmetric chain.

Now assume the theorem is true for some arbitrary number k, and suppose that m is a square-free number with $k + 1$ prime divisors. Then $m = m_1 p_{k+1}$, where m_1 has k prime divisors. Let $d_1, d_2, \ldots, d_h$ be a symmetric chain in the SCD of $D(m_1)$. Then it is clear that $d_1, d_2, \ldots, d_h, d_h p_{k+1}$ and $d_1 p_{k+1}, d_2 p_{k+1}, \ldots, d_{h-1} p_{k+1}$ form symmetric chains of $D(m)$, since

$$\begin{aligned} r(d_1 p_{k+1}) + r(d_{h-1} p_{k+1}) &= r(d_1) + r(d_h p_{k+1}) \\ &= r(d_1) + r(d_h) + r(p_{k+1}) \\ &= r(m_1) + r(p_{k+1}) \\ &= r(m) \end{aligned}$$

It's also easy to see that every divisor of m will be found in one such symmetric chain. The proof for all positive integers (including those that are not square-free) is similar.

1.3 Permutation groups

The *symmetric group* S_n is the group of all permutations of $[n]$ with function composition as the group operation. We use the usual cycle notation to denote permutations. For example, $\sigma = (1\ 2 \ldots n)$ is an n-cycle, and $\tau = (i\ j)$ is a transposition. We compose cycles from right to left, for instance, $(1\ 2\ 3\ 4)(1\ 3\ 2) = (1\ 4)(3)(2)$.

Given any subgroup G of the symmetric group S_n of all permutations of $[n]$, the *quotient* B_n/G has as its elements the equivalence classes

$$[A] = \{B \mid B = \sigma(A), \text{for some } \sigma \in G\},$$

$A \in B_n$, ordered by

$$[A] \leq [B] \iff X \subseteq Y \text{ for some } X \in [A] \text{ and } Y \in [B].$$

We will not prove that this relation defines a partial ordering on B_n/G, but it may be useful to at least verify that the relation $\leq$ on B_n/G is transitive. Let U, V, W be elements of B_n/G, and suppose $U \leq V$ and $V \leq W$. Then we can produce $X \in U$ and $Y_1 \in V$ such that $X \subseteq Y_1$, and we can produce $Y_2 \in V$ and $Z \in W$ such that $Y_2 \subseteq Z$. Since $Y_1, Y_2 \in V$, we can also produce $\sigma \in G$ such that $Y_1 = \sigma(Y_2)$, and clearly since $Y_2 \subseteq Z$, we have that $Y_1 = \sigma(Y_2) \subseteq \sigma(Z)$, with $\sigma(Z) \in W$. Therefore, $X \subseteq Y_1 \subseteq \sigma(Z)$, so $U \leq W$, and hence the relation is transitive.

1.4 The Main Result

In an unpublished manuscript, R. Canfield and S. Mason [2] made the following conjecture, which we have sought to prove in a few limited cases.

Conjecture 1. *If G is a subgroup of the symmetric group S_n acting on the set $[n]$, then the quotient poset B_n/G is a symmetric chain order.*

The following theorem, first proved by K. K. Jordan [7], shows that the conjecture is true in one special case.

Theorem 1.1. *Let $\sigma \in S_n$ be any n-cycle and let $G = \langle \sigma \rangle$ denote the subgroup of S_n generated by σ. Then the partially ordered set B_n/G is a symmetric chain order.*

In fact, a special case of this result had been proved before Jordan. In [5] Griggs, Killian, and Savage constructed a SCD of $B_p/\langle \sigma \rangle$ for p prime and $\sigma = (1\ 2\ \ldots p)$. They also asked if $B_n/\langle \sigma \rangle$ is a SCO for all n, which is answered affirmatively by Theorem 1.1.

We offer a new proof of Theorem 1.1. Our proof also provides a simple, straightforward method of finding a symmetric chain decomposition of B_n/G when G is generated by an n-cycle, beginning from the well-known SCD of B_n obtained by Greene and Kleitman [4].

1.5 Other Results

In addition to proving Canfield's conjecture in the case of groups generated by an n-cycle, we have also made the following observation, concerning groups generated by pairwise disjoint transpositions.

Theorem 1.2. *Let $\tau_1, \tau_2, \ldots, \tau_k \in S_n$ be k pairwise disjoint transpositions and let $G = \langle \tau_1, \tau_2, \ldots, \tau_k \rangle$ denote the subgroup of S_n generated by $\tau_1, \tau_2, \ldots, \tau_k$. Then the partially ordered set B_n/G is a symmetric chain order.*

Again, our proof provides a straightforward method of finding a symmetric chain decomposition of the relevant quotient of B_n, with the SCD of B_n obtained by Greene-Kleitman as the starting point.

2 An Important SCD of B_n

In this thesis, our main concern is the construction of symmetric chain decompositions for various quotients of B_n. Towards that end, it will be useful to present a construction of an SCD for B_n due to Greene and Kleitman [4]. But before doing so, we would like to note that there is another interpretation of elements of B_n, involving sequences of 0's and 1's. For each set $A \in B_n$, we associate a binary sequence called $\hat{A}$, where $\hat{A}$ contains a 1 in position i if $i \in A$, and otherwise $\hat{A}$ contains a 0 in position i. For example, if $A = \{1, 3, 4\} \in B_5$, then $\hat{A} = 10110$. This equivalent description of the elements of B_n will be very useful to us later on.

The Greene-Kleitman SCD is obtained by a "pairing" or "matching" procedure which can be describe inductively. Fix $A \subseteq [n]$. If $1 \notin A$ and $2 \in A$, pair 1 and 2; define $p_A(2) = 1$. Suppose that we considered $1, 2, \ldots k-1$. If $k \in A$ and there is some $j < k$, $j \notin A$ such that j is unpaired, then let $p_A(k)$ be the maximum such j and say $p_A(k)$ and k are *paired* or *matched*. Continue for all k in $[n]$. Let $R(A)$ be the set of all x for which $p_A(x)$ is defined, let $L(A) = \{p_A(x) \mid x \in R(A)\}$, and let

$P(A) = L(A) \cup R(A)$.

Now, let us describe the inductive pairing procedure on elements of B_n in terms of the binary sequences defined above. Let $A \in B_n$, and consider the sequence $\hat{A}$. Moving from left to right in the sequence, when we come to a 0 it becomes (possibly temporarily) unmatched. When we come to a 1 it either matches with the rightmost unmatched 0, or if there are no unmatched 0's, it becomes permanently unmatched. At the end of this procedure, matched 1's in $\hat{A}$ will correspond to the elements of $R(A)$, matched 0's will correspond to the elements of $L(A)$, the the set of all matched 1's and 0's will correspond to $P(A)$.

Now that the pairing procedure has been fully described, the Greene-Kleitman symmetric chain partition of $B(n)$ can be defined as follows. For all $A \in B_n$, let $\tau(A) = A \cup \{z\}$ where $z = \min([n] - (A \cup L(A)))$ provided that $[n] - (A \cup L(A)) \neq \emptyset$; otherwise $\tau(A)$ is undefined. It is straightforward to argue that the following inverts this mapping: $\tau^{-1}(B) = B - \{z\}$ where $z = \max(B - R(B))$ provided that $B - R(B) \neq \emptyset$; otherwise $\tau^{-1}(B)$ is undefined.

For all $A \in B_n$ such that $R(A) = A$, let $\mathcal{C}(A) = \{A, \tau(A), \tau^2(A), \ldots, \tau^k(A)\}$, with $|[n] - (A \cup L(A))| = k$. (Examination of Figures 1 and 2 shows that the sets A for which $A = R(A)$ are exactly the minimum elements of the SCD of B_5.) We shall show that given $S = \{\mathcal{C}(A) | A \in B_n, A = R(A)\}$, S defines a symmetric chain decomposition of B_n.

We can also describe τ by its action on the binary sequences corresponding to elements of B_n. Observe that τ acts on $A \in B_n$ by replacing the leftmost unmatched 0 in $\hat{A}$ with a 1. This is identical to the above description, in which it was said that

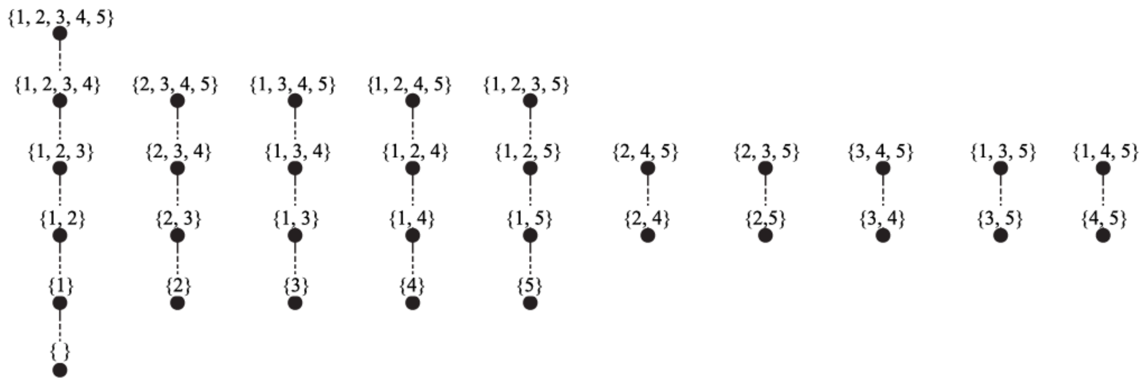

Figure 1: The Greene-Kleitman SCD of B_5

$\tau(A)$ is the union of A and the minimal element of $[n] - (A \cup L(A))$. Also, we can describe τ^{-1} as replacing the rightmost unmatched 1 in $\hat{A}$ with a 0. We are now ready to prove the following theorem.

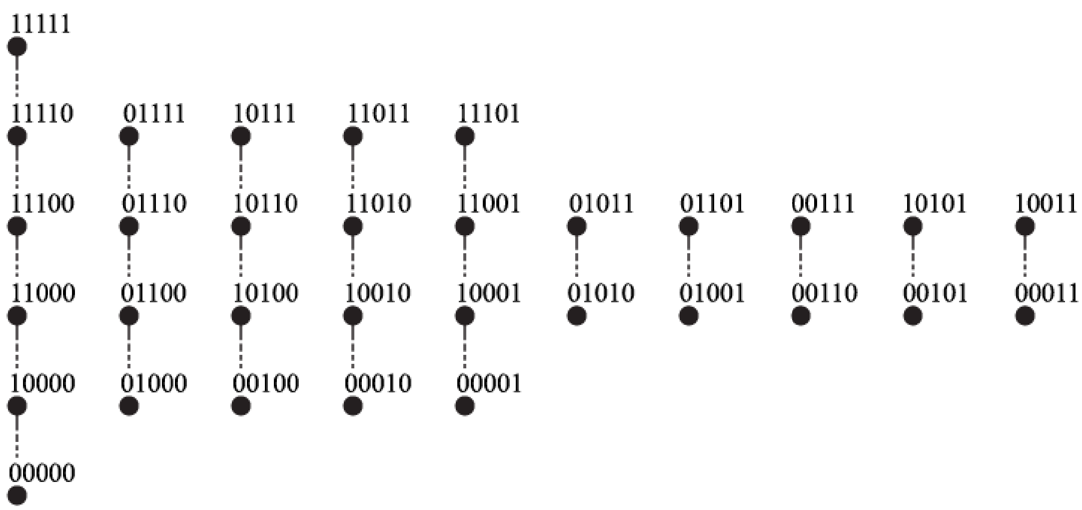

Figure 2: The Greene-Kleitman SCD of B_5 in terms of $(0,1)$-sequences

Theorem 2. *(Greene and Kleitman [4]) For $A \in B_n$ with $A = R(A)$, let $\mathcal{C}(A) = \{A, \tau(A), \tau^2(A), \ldots, \tau^k(A)\}$ where $k = |[n]-(A \cup L(A))|$. The following is a symmetric chain decomposition of B_n:*

$$S = \{\mathcal{C}(A) | A \in B_n, A = R(A)\}$$

Proof of Theorem 2: Pick $A \in B_n$ such that $A = R(A)$, so that

$$\mathcal{C}(A) = \{A, \tau(A), \tau^2(A), \ldots, \tau^k(A)\} \in S.$$

First we must show that $\mathcal{C}(A)$ is symmetric. Observe that

$$\begin{aligned}
r(A) + r(\tau^k(A)) &= |A| + |\tau^k(A)| \\
&= |R(A)| + (|R(A)| + k) \\
&= 2|R(A)| + |[n] - (A \cup L(A))| \\
&= 2|R(A)| + n - |A| - |L(A)| = 2|R(A)| + n - 2|R(A)| \\
&= n
\end{aligned}$$

since $|A| = |R(A)| = |L(A)|$. Hence $\mathcal{C}(A)$ is symmetric.

Now we need to show that the elements of S are disjoint, and so it suffices to show that τ is one-to-one. Here it should be noted that all unmatched 0's in $\hat{A}$ for $A \in B_n$ are to the right of all unmatched 1's, lest they be matched. Hence if i is the position of the leftmost unmatched 0 in $\hat{A}$, then i is also the position of the rightmost unmatched 1 in $\tau(\hat{A})$. Recall that we described τ^{-1} as changing the rightmost unmatched 1 to a 0.

Therefore, for all $A \in B_n$ such that $[n] - (A \cup L(A)) \neq \emptyset$, $\tau^{-1}(\tau(A)) = A$, and for all $A \in B_n$ such that $A - R(A) \neq \emptyset$, $\tau(\tau^{-1}(A)) = A$. Hence τ and τ^{-1} are one-to-one, and so the elements of S are disjoint symmetric chains.

The last thing we must show is that every element of B_n is in an element of S. Pick $A \in B_n$, and suppose that $\hat{A}$ contains k unmatched 1's. Then we must have $\tau^k(R(A)) = A$, since $P(A) = P(R(A))$, and τ^k simply replaces the leftmost k unmatched 0's in $R(A)$ with unmatched 1's. Hence $A \in \mathcal{C}(R(A))$, so A is contained in an element of S, and hence S is a symmetric chain decomposition of B_n. $\square$

We would like to show that the following lemma concerning the Greene-Kleitman pairing procedure is true, since it will be useful to us later on.

Lemma 3. *For all $A \in B_n$, for all $x \in R(A)$, $[p_A(x), x] \subseteq P(A)$; and $p_A(x)$ is the maximum y such that $1 \leq y < x$ and precisely half of the elements of the interval $[y, x]$ are in A.*

Proof of Lemma 3. Suppose that the first part of the lemma is not true. That is, there is a $y \in [p_A(x), x]$ such that $y \notin P(A)$. If $y \notin A$, then clearly the pairing procedure has been violated, since $p_A(x)$ could not have been the maximum unpaired element not in A when x was being considered for pairing. If $y \in A$, then $p_A(x)$ would have been unpaired when y was under consideration for pairing, making it impossible for y to remain unpaired. Hence $[p_A(x), x] \subseteq P(A)$.

Suppose it is not true that precisely half of the elements in the interval $[p_A(x), x]$ are in A. If there are more 1's than 0's in the interval on $\hat{A}$, then there must be an unpaired 1, since no 1 in the interval can be paired with a 0 outside of the interval, because that would imply that $p_A(x)$ was already paired before x was considered. However, it is not possible for an unpaired 1 to be in the interval by the first part of the lemma.

Similarly, suppose there are more 0's than 1's in the interval on $\hat{A}$. If a 0 is in the interval it cannot be paired with a 1 outside of the interval, since that would mean the 0 was unpaired when x was under consideration, so $p_A(x)$ would not have been the rightmost unpaired 0. Hence there must be an unpaired 0 in the interval, which is impossible by the first part of the lemma. Therefore, exactly half of the elements in the interval $[p_A(x), x]$ are in A.

Now suppose $p_A(x)$ is not the maximum y such that half of the elements of the interval $[y, x]$ are in A. Then there must be a smaller, minimal interval $[y, x]$ such that half of the elements of the interval are in A. Suppose that $y \notin A$. Then, as we have just shown, y must be paired with some $w \in [p_A(x), x]$, and exactly half of the elements of $[y, w]$ must be in A, and hence half of the elements of $[w + 1, x]$ must be in A, which is clearly impossible, since $[y, x]$ is the minimal interval with this property. Suppose that $y \in A$. Then there must be more 0's than 1's in the interval $[y + 1, x]$ on $\hat{A}$, and so there must be an unpaired 0 in $[p_A(x), x]$, which is impossible by the first part of the lemma. $\square$

We require one additional lemma, concerning the properties of the Greene-Kleitman SCD itself.

Lemma 4. *Let* $A \in B_n$, $A = R(A)$.

(1) $\mathcal{C}(A) = \{X \in B_n \mid R(X) = A\}$ *and* $p_X(a) = p_A(a)$ *for all* $X \in \mathcal{C}(A)$ *and for all* $a \in R(A)$;

(2) *if* $X \in \mathcal{C}(A)$, *then* $|\mathcal{C}(A)| = n - |P(X)| + 1$; *and,*

(3) $\min(\mathcal{C}(A)) = R(A)$, $\max(\mathcal{C}(A)) = [n] - L(A)$*; in fact,* $\mathcal{C}(A)$ *is the chain*

$$R(A) \subset R(A) \cup \{a_1\} \subset R(A) \cup \{a_1, a_2\} \subset \ldots \subset R(A) \cup \{a_1, a_2, \ldots a_t\} = [n] - L(A),$$

where $[n] - (R(A) \cup L(A)) = \{a_1 < a_2 < \ldots < a_t\}$.

Proof of Lemma 3, part (1). Part (1) follows easily from the definition of τ. It has already been said that τ replaces the leftmost unmatched 0 in $\hat{A}$ with a 1, which will also be unmatched in $\tau(\hat{A})$. Hence no paired elements of A are affected by the action of τ, so if $X \in B_n$ and $\tau(X)$ is defined, then clearly $R(X) = R(\tau(X))$, and hence part (1) follows easily from the definition of $\mathcal{C}(A)$.

Part (2). Part (2) simply states that $|\mathcal{C}(A)|$ in the Greene-Kleitman decomposition is equal to one plus the number of unpaired elements in any binary sequence $\hat{X}$ with X belonging to the chain. This follows from part (1), since by definition of $\mathcal{C}(A)$, $|\mathcal{C}(A)| = |[n] - (A \cup L(A))| + 1 = n - 2|R(A)| + 1$, and by part (1), $n - 2|R(A)| + 1 = n - 2|R(X)| + 1 = n - |P(X)| + 1$.

Part (3). To see that $\min(\mathcal{C}(A)) = R(A)$ and $\max(\mathcal{C}(A)) = [n] - L(A)$, observe that if $\tau(A)$ is defined then $A \leq \tau(A)$. Hence out of the set $\mathcal{C}(A) = \{A, \tau(A), \ldots, \tau^k(A)\}$, where $|[n] - (A \cup L(A))| = k$ and $A - R(A) = \emptyset$, it is clear that A is the minimum element, and $A = R(A)$. Similarly, $\tau^k(A)$ is the maximum element, and the binary sequence defined by $\tau^k(A)$ contains no unpaired 0's. Hence $\tau^k(A) = [n] - L(A)$.

The second statement of part (3) follows easily from the definition of τ and $\mathcal{C}(A)$.

$\square$

3 Proof of the Main Result

Without loss of generality, we take the usual order on $[n]$ and let $\sigma = (1\ 2\ \ldots\ n)$. Now let $C_1, C_2, \ldots, C_t$, where $t = \binom{n}{\lfloor n/2 \rfloor}$, be the symmetric chains in the Greene-Kleitman decomposition, ordered by decreasing length. Theorem 1.1 is established by finding a family $\mathcal{C} = \{C'_{i_1}, C'_{i_2}, \ldots C'_{i_m}\}$, with $(i_1, i_2, \ldots, i_m)$ a subsequence of $(1, 2, \ldots, t)$, that satisfies these conditions:

(1) for all $1 \leq j \leq m$, $C'_{i_j} \subseteq C_{i_j}$ and is a symmetric chain in B_n;

(2) for all $1 \leq r < s \leq m$ and for all $A \in C'_{i_r}, B \in C'_{i_s}$, $A \notin [B]$; and,

(3) for all $[X]$ there is some $Y \in [X]$ such that $Y \in C'_{i_j}$ for some j.

We see that **(1) - (3)** imply Theorem 1.1 once we realize that each symmetric chain of B_n defines a symmetric chain in the quotient B_n/G and that each $[X] \in B_n/G$ belongs to exactly one of the symmetric chains of B_n/G induced by the chains in $\mathcal{C}$.

A procedure that provides a family $\mathcal{C}$ satisfying **(1) - (3)** is based on the following two lemmas. Before that, note that given a symmetric chain C in B_n and $X \in C$ with $|X| \leq \lfloor n/2 \rfloor$, we define X^* to be the member of C with $|X^*| = n - |X|$. Also, for any $Y \in C$, let $\tau(Y)$ denote its successor in C, if it exists, and $\tau^{-1}(Y)$ be its predecessor, if it exists, as introduced in section 2.

The first lemma was proved in [3].

Lemma 5. *For $i = 1, 2, \ldots, t$ and for all $X \in C_i$ with $|X| \leq \lfloor n/2 \rfloor$, $(\sigma(X))^* = \sigma(X^*)$.*

Lemma 6. *Let $w \in \{1, 2, \ldots, t\}$, and let $A \in C_w$ with $|A| \leq \lceil n/2 \rceil$. Suppose that there is some $B \in [A]$ such that $B \in C_j$ for some $j < w$. Then there is some $k < w$ and $D \in C_k$ such that $D \in [\tau^{-1}(A)]$, provided that $\tau^{-1}(A)$ is defined.*

Let us use these facts to describe an inductive procedure for obtaining the set $\mathcal{C} = \{C'_{i_1}, C'_{i_2}, \ldots C'_{i_m}\}$ satisfying **(1) - (3)**.

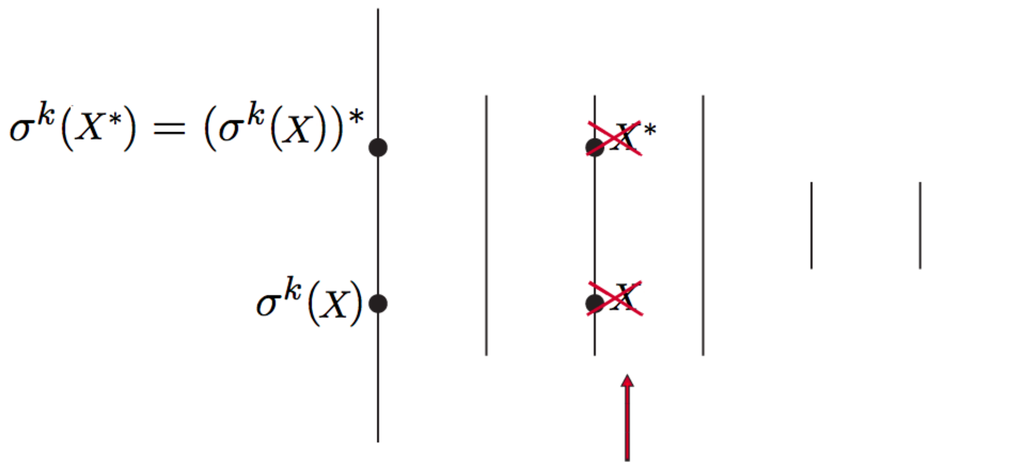

Figure 3: An illustration of Lemma 5. The vertical lines represent symmetric chains in the Greene-Kleitman SCD of B_n.

First, let $i_1 = 1$ and $C'_{i_1} = C_1$. Now suppose that we have already obtained $C'_{i_1}, C'_{i_2}, \ldots, C'_{i_k}$ satisfying **(1)** and **(2)**, and that we wish to obtain $C'_{i_{k+1}}$. To do so, attempt to choose i least in $\{i_k + 1, \ldots, t\}$ such that for some $X \in C_i$,

$$[X] \cap \left(\bigcup_{j=1}^{k} C_{i_j}\right) = \emptyset \tag{3.1}$$

and set $i_{k+1} = i$. If it is not possible to choose such an i then $m = k$ and the procedure is complete. Now let

$$C'_{i_{k+1}} = \{Y \in C_{i_{k+1}} \mid [Y] \cap (\bigcup_{j=1}^{k} C'_{i_j}) = \emptyset\}. \tag{3.2}$$

We know that if $Y \in C'_{i_{k+1}}$, with $|Y| \leq \lfloor n/2 \rfloor$ then $Y^* \in C'_{i_{k+1}}$, by Lemma 5 (refer to Figure 3). Also, if $Z \in C_{i_{k+1}}$ and $Y \subseteq Z \subseteq Y^*$ where $Y \in C'_{i_{k+1}}$ then $Z \in C'_{i_{k+1}}$ by Lemma 6 and Lemma 5 (refer to Figure 4). Thus, $C'_{i_{k+1}}$ is symmetric in B_n and **(1)** holds.

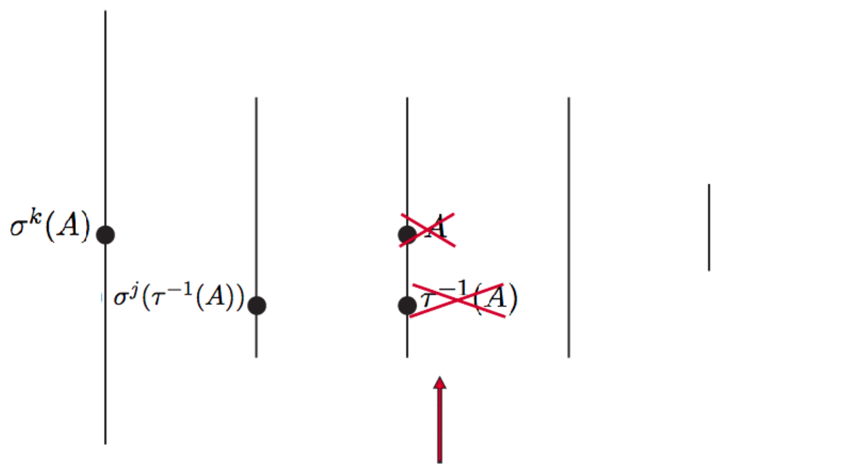

Figure 4: An illustration of Lemma 6. The vertical lines represent symmetric chains in the Greene-Kleitman SCD of B_n.

It is immediate from equation (3.2) that property **(2)** holds. It is also easily seen from equation (3.1) and equation (3.2) that property **(3)** holds.

Proof of Lemma 5. The proof is divided into cases depending upon which of $R(X) \subseteq X \subseteq X^*$ contain n. It is not possible that $n \in X - R(X)$, because $|X| \leq \lfloor n/2 \rfloor$ means that for some $y < n$ precisely half the elements of $[y, n]$ are in X, and, hence,

$n \in R(X)$ by Lemma 3. Consequently, we have three cases to consider. In each case, we argue that

$$R(\sigma(X^*)) = R(\sigma(X)),$$

apply Lemma 4, part (1) to see that $\sigma(X^*)$ and $(\sigma(X))^*$ are both members of $\mathcal{C}(\sigma(X))$, and conclude $\sigma(X^*) = (\sigma(X))^*$ since these sets both have cardinality $n - |\sigma(X)|$.

Case 1: $n \notin X^*$

Since $n \in [n] - L(X) = \max(\mathcal{C}(X))$ and $n \notin X^*$, $X \neq \min(\mathcal{C}(X)) = R(X)$. Thus, we can choose $y = \min(X - R(X))$. If $y = 1$ then $p_{\sigma(X)}(2) = 1 = p_{\sigma(X^*)}(2)$. For each $z \in R(X)$, $\sigma(z) = z + 1 \in R(\sigma(X))$ and each $z + 1 \in R(\sigma(X))$ has $z \in R(X)$ apart from $z + 1 = 2$. Thus,

$$\begin{aligned} R(\sigma(X)) &= \sigma(R(X)) \cup \{2\} && \text{since } p_{\sigma(X)}(2) = 1, \\ &= \sigma(R(X^*)) \cup \{2\} && \text{by Lemma 4, part (1),} \\ &= R(\sigma(X^*)) && \text{since } p_{\sigma(X^*)}(2) = 1. \end{aligned}$$

If $y > 1$ we claim that $[1, y-1] \subseteq P(X)$. Note that $y - 1 \in X$ as otherwise $y \in R(X)$ with $p_X(y) = y-1$, contradicting the choice of y. By the minimality of y, $y-1 \in R(X)$ and, by Lemma 3, $[p_X(y-1), y-1] \subseteq P(X)$. Continue in the same manner, with $p_X(y-1) - 1$ in place of y and thereby verify the claim that $[1, y-1] \subseteq P(X)$. The argument is just about the same except we use the fact that $[1, y-1] \subseteq P(X)$ and $1 \notin X$, so, $p_{\sigma(X)}(y+1) = 1$:

$$R(\sigma(X^*)) = \sigma(R(X^*)) \cup \{y+1\} = \sigma(R(X)) \cup \{y+1\} = R(\sigma(X)).$$

Case 2: $n \in R(X)$

Every element of $R(\sigma(X))$ is in $\sigma(R(X))$ and every element of $\sigma(R(X))$, except for 1, is in $R(\sigma(X)$. Thus,

$$R(\sigma(X)) = \sigma(R(X)) - \{1\} = \sigma(R(X^*)) - \{1\} = R(\sigma(X^*)).$$

Case 3: $n \in X^* - X$

Since $n \in X^* - X$, Lemma 4, part (3) shows that $X^* = \max(\mathcal{C}(X)) = [n] - L(X)$ and, thus, $X = \min(\mathcal{C}(X)) = R(X)$.

If $z + 1 \in R(\sigma(X))$ then $z \in X = R(X)$, so $R(\sigma(X)) \subseteq \sigma(R(X))$. Conversely, $1 \notin \sigma(R(X))$, and any $z + 1 \in \sigma(R(X))$ is obviously a member of $R(\sigma(X))$. Thus, $R(\sigma(X)) = \sigma(R(X))$. Similarly, since $n \notin R(X)$, it follows that $R(\sigma(X^*)) = \sigma(R(X^*))$. Hence, $R(\sigma(X^*)) = R(\sigma(X))$. $\square$

Proof of Lemma 6. As before, let $C_1, C_2, \ldots, C_t$, where $t = \binom{n}{\lfloor n/2 \rfloor}$, be the symmetric chains in the Greene-Kleitman decomposition, ordered by decreasing length. Let $A \in C_w$ with $|A| \leq \lceil \frac{n}{2} \rceil$. Without loss of generality, let $\sigma = (1\ 2\ \ldots\ n)$, and suppose that there exists a $j < w$ such that $B \in C_j$ and $B \in [A]$. Hence there is an integer m such that $B = \sigma^m(A)$.

It would suffice to show that if $\tau^{-1}(A)$ is defined, then there is a $k < w$ such that $D \in C_k$ and $D \in [\tau^{-1}(A)]$. As described earlier, it is useful to interpret A as a binary sequence $\hat{A}$ of length n, with $1's$ corresponding to elements of $[n]$ contained in A and $0's$ corresponding to all other elements of $[n]$. Clearly by Lemma 4, part (3) $\hat{A}$ must contain unpaired 1's, since $\tau^{-1}(A)$ is defined, so let i be the position of the rightmost unpaired 1 in $\hat{A}$. As noted before, $B = \sigma^m(A)$, and we will assume without loss of generality that $-(i-1) \leq m \leq n-i$, $m \neq 0$. We must consider two cases:

Case 1: The 1 at position $i+m$ in $\hat{B}$ is paired.

Clearly $m > 0$, since in order for the 1 at position i in $\hat{A}$ to become paired in $\hat{B}$ an additional 0 must have appeared at the beginning of the sequence to pair with it. We can also observe that by Lemma 3 all of the 1's to the right of the 1 at position $i+m$ in $\hat{B}$ must be paired, since they were paired in A. Now consider the binary sequence $\sigma^m(\tau^{-1}(\hat{A}))$ contained in some chain C_k. Clearly $\sigma^m(\tau^{-1}(\hat{A}))$ can be obtained by replacing the 1 at position $i+m$ in $\hat{B}$ with a 0. It follows from this that $\sigma^m(\tau^{-1}(A))$ must have one fewer pairs than B, since the additional 0 will be unpaired, while the 1 that it replaced was paired. Hence, by Lemma 4, part (2), $|C_k| > |C_j|$, so $k < j < w$, as desired.

Case 2: The 1 at position $i+m$ in $\hat{B}$ is unpaired.

If the 1 at position $i+m$ is the rightmost unpaired 1 in $\hat{B}$ then we are done, since in that case we have $\tau^{-1}(B) = \sigma^m(\tau^{-1}(A))$. So suppose instead that the rightmost unpaired 1 is at a position to the right of $i+m$, say at position $i+m+\ell$, $\ell > 0$. Clearly $m < 0$, since the 1 in position $i+m+\ell$ in $\hat{B}$ must have been in a position to the left of i in $\hat{A}$.

My claim is that, for some q, $\sigma^q(A)$ is the maximum element of its chain, and its chain is not a singleton, so $|\sigma^q(A)| > \left\lceil \frac{n}{2} \right\rceil$. This would contradict the fact that $|A| \leq \left\lceil \frac{n}{2} \right\rceil$, since $|\sigma^q(A)| = |A|$.

To see that this is true, we need to take a closer look at the transition from $\hat{B}$ to $\hat{A}$. We can think of this transition as a sequence of rightward shifts. After each "click" rightwards, the 1 at position $i+m$ in $\hat{B}$ and the 1 at position $i+m+\ell$ in $\hat{B}$ must remain unpaired (since the 1 at position $i+m$ in $\hat{B}$ is unpaired in $\hat{A}$), at least until the 1 at position $i+m+\ell$ in $\hat{B}$ moves from position n to position 1. Hence at some intermediate step from $\hat{B}$ to $\hat{A}$, the 1 at position $i+m+\ell$ in $\hat{B}$ is in position n, and is unpaired. Let's call this intermediate element $\sigma^q(A)$. Clearly $\sigma^q(A)$ is the maximum element of its chain, since the rightmost unpaired 1 is in position n, and hence there are no unpaired 0's (recall that all unmatched 0's must occur to the right of all unmatched 1's). We can also see that the chain containing $\sigma^q(A)$ is not a singleton, since $\sigma^q(A)$ contains an unmatched 1, and the binary sequence in a singleton chain must contain only pairs, by Lemma 4, part (2). Again, this contradicts the fact that $|A| \leq \lceil \frac{n}{2} \rceil$, since $|\sigma^q(A)| = |A|$. $\square$

4 Proof of Other Results

We now prove Theorem 1.2, which states that B_n/G is a SCO for G generated by a set of pairwise disjoint transpositions. As in the proof of Theorem 1.1, we proceed by removing entire chains from the standard Greene-Kleitman decomposition. We begin by showing that it holds in case $\tau_1 = (12), \tau_2 = (34), \ldots, \tau_k = (2k-1\ 2k)$ and applying the following lemma concerning permutation groups

Lemma 7. *For any positive integer n, these statements hold for the symmetric group S_n.*

(1) *Given k pairwise disjoint transpositions $\tau_1, \tau_2, \ldots, \tau_k \in S_n$, there is a permutation σ such that $\tau_1 = \sigma(12)\sigma^{-1}, \tau_2 = \sigma(34)\sigma^{-1}, \ldots, \tau_k = \sigma(2k-1\ 2k)\sigma^{-1}$.*

(2) *For any subgroup H of S_n generated by permutations $\rho_1, \rho_2, \ldots, \rho_k$, and any permutation σ, $\sigma H \sigma^{-1}$ is generated by $\sigma\rho_1\sigma^{-1}, \sigma\rho_2\sigma^{-1}, \ldots, \sigma\rho_k\sigma^{-1}$.*

(3) *For all subgroups H of S_n and for all $\sigma \in S_n$, the partially ordered set B_n/H is order-isomorphic to $B_n/\sigma H \sigma^{-1}$.*

Proof of Lemma 7. To see that part (1) is true, suppose that $\tau_i = (u_i, v_i), i = 1, 2, \ldots, k$, so that $\{u_1, v_1, u_2, v_2, \ldots, u_k, v_k\}$ is a set of $2k$ distinct elements in $[n]$. An elementary fact about conjugacy in S_n is that for all $\alpha, \rho \in S_n$, $\rho\alpha\rho^{-1}$ has the same cycle decomposition as α with a cycle $(\rho(i_1)\ \rho(i_2) \ldots \rho(i_\ell))$ for each cycle $(i_1\ i_2 \ldots i_\ell)$ of α (see, for instance, Theorem 2.63 of [9]). To obtain $\sigma \in S_n$ with the required property, we let

$$\sigma(1) = u_1, \sigma(2) = v_1, \sigma(3) = u_2, \sigma(4) = v_2, \ldots \sigma(2k-1) = u_k, v_k,$$

and let $\sigma(2k+1), \ldots, \sigma(n)$ be chosen so that σ is a permutation.

Part (2) is clearly a special case of a general fact about conjugates of finitely generated subgroups H of any group G.

To justify part (3), we argue that the mapping $[A] \to [\sigma(A)]$ is an order-isomorphism of B_n/H onto $B_n/\sigma H \sigma^{-1}$. First, the mapping is well-defined and one-to-one because of this sequence of equivalences: for all $A, B \in B_n$,

$$\begin{aligned}
[A] = [B] \text{ in } B_n/H &\iff \rho(A) = B \text{ [for some } \ \rho \in H] \\
&\iff \sigma\rho\sigma^{-1}(\sigma(A)) = \sigma(B) \text{ [for some } \ \sigma\rho\sigma^{-1} \in \sigma H \sigma^{-1}] \\
&\iff [\sigma(A)] = [\sigma(B)] \text{ in } B_n/\sigma H \sigma^{-1}.
\end{aligned}$$

The mapping preserves order, as does its inverse, by almost the same reasoning: for all $A, B \in B_n$,

$$\begin{aligned}
[A] \leq [B] \text{ in } B_n/H &\iff \rho(A) \subseteq B \text{ [for some } \ \rho \in H] \\
&\iff \sigma\rho\sigma^{-1}(\sigma(A)) \subseteq \sigma(B) \text{ [for some } \ \sigma\rho\sigma^{-1} \in \sigma H \sigma^{-1}] \\
&\iff [\sigma(A)] \leq [\sigma(B)] \text{ in } B_n/\sigma H\sigma^{-1}.
\end{aligned}$$

The mapping is obviously onto. □

Now, let us see that the quotient B_n/G, where $G = \langle \tau_1, \tau_2, \ldots, \tau_k \rangle$, is a SCO with $\tau_1 = (12), \tau_2 = (34), \ldots, \tau_k = (2k-1\ 2k)$. First observe that for $A \subseteq [n]$ for which $2i-1 \notin A$ and $2i \in A$, then $2i \in R(A)$ and $p_A(2i) = 2i-1$. In words, $2i-1$ and $2i$ are paired in A. By Lemma 4, part (2), the same is true for all $X \in \mathcal{C}(R(A))$.

We select a subfamily of the Greene-Kleitman family $C_1, C_2, \ldots, C_t$, of symmetric chains, with $t = \binom{n}{\lfloor n/2 \rfloor}$. Let $\{j_1, j_2, \ldots, j_m\}$ be the set of those $j \in [t]$ such that: for all $A \in C_j$, $A \cap \{2i-1, 2i\} \neq 2i$, for each $i = 1, 2, \ldots k$. For each $B \notin \bigcup_{l=1}^{m} C_{j_l}$,

$$\begin{aligned}
B \in [B'] \text{ where } B' = (&B - \{2i \mid 2i \in B, 2i-1 \notin B, \ i = 1, 2, \ldots, k\}) \\
&\cup \{2i-1 \mid 2i \in B, 2i-1 \notin B, \ i = 1, 2, \ldots, k\}.
\end{aligned}$$

Moreover, B' is the unique element of $[B]$ in $\bigcup_{l=1}^{m} C_{j_l}$.

Create a symmetric chain decomposition of $B(n)/G$ by replacing each $A \in C_{i_l}$ by $[A]$, for $l = 1, 2, \ldots m$.

5 Closing Remarks

Although some small progress has been made towards proving Canfield's conjecture, in the end we have only shown that it is true in a few very special cases, namely, when G is generated by an n-cycle, and when G is generated by a set of disjoint transpositions. Other interesting subgroups of S_n for which the conjecture is still unproved include the 2-element reflection group $H = \langle \rho \rangle$, with $\rho = (1\ n)(2\ n-1)(3\ n-2)\ldots$, and the $2n$-element dihedral group.

While only a few cases have been proven, we believe there is positive evidence to show that the conjecture is true in general. In 1986, Pouzet and Rosenberg showed in [8] that the following is true. Let $P = B_n/G$. Then P is a ranked poset, and define $P_r = \{[S] \mid |S| = r\}$, the set of elements of P of rank r. Suppose $r \leq \frac{n}{2}$, and pick $s \geq r$ such that $r \leq n - s$. Then there exists a set of $|P_r|$ disjoint, saturated chains such that for each chain C in the set, $C \cap P_j \neq \emptyset, \forall j \in \{r, r+1, \ldots, s\}$. The existence of such chains, while not providing the needed symmetric chain decomposition of B_n/G, gives positive evidence for the possibility of its existence.

There are additional reasons to be hopeful that B_n/G is always a SCO, but presenting these requires some additional terminology. We can partition a ranked poset P into a set of disjoint subsets $P_0, P_1, \ldots, P_n$ such that if $x \in P_i$ and y covers x, then $y \in P_{i+1}$. Let $p_i = |P_i|$ for $i = 0, 1, \ldots, n$, and say that P is *rank symmetric* if $p_i = p_{n-i}$ for all i, and *rank unimodal* if, for some j,

$$p_0 \leq p_1 \leq \cdots \leq p_j \geq p_{j+1} \geq \cdots \geq p_n.$$

Recall that an antichain is a non-empty subset of P such that no two elements of the subset are comparable. Say that P is *k-Sperner* if there is no union of k antichains that is larger than the sum of the k largest ranks. Call P *strongly Sperner* if P is k-Sperner for all $k \in [n+1]$.

In 1980, R. Stanley showed in [10] (c.f. [8], [11]) that the quotient B_n/G is rank symmetric, rank unimodal, and strongly Sperner, all necessary conditions for a ranked poset to be a SCO. Finally, we say that a ranked poset P has the *LYM property* if, given an antichain A in P with m_i elements of rank i, we have

$$\sum_i \frac{m_i}{p_i} \leq 1.$$

Griggs showed in [6] that if P is rank symmetric, rank unimodal, and has the LYM property, then P is a SCO. In combination with Stanley's result stated above, we can conclude that for every G such that B_n/G has the LYM property, B_n/G is a SCO. As you can see, the evidence has been mounting for some time that B_n/G is always a SCO.

References

[1] N. G. de Bruijn, C. Tengbergen, and D. Kruyswijk, On the set of divisors of a number. *Nieuw Arch. Wiskd.* **23** (1951) 191-3.

[2] E.R. Canfield and S. Mason, When is a quotient of the boolean lattice a symmetric chain order? preprint (2006).

[3] D. Duffus, P. Hanlon and R. Roth, Matchings and hamiltonian cycles in some families of symmetric graphs, *Emory University Technical Reports* (1986).

[4] C. Greene and D. J. Kleitman, Strong versions of Sperner's theorem, *J. Combinatorial Theory A* **20** (1976) 80 - 88.

[5] J.R. Griggs, C.E. Killian, and C.D. Savage, Venn diagrams and symmetric chain decompositions in the boolean lattice, *Electronic J. of Combinatorics* **11** (2004) R2.

[6] J.R. Griggs, Sufficient conditions for a symmetric chain order, *Siam J. Appl. Math.* **32** (1977) 807-809.

[7] K. K. Jordan, The necklace poset is a symmetric chain order, *J. Combinatorial Theory A* (to appear).

[8] M. Pouzet and I.G. Rosenberg, Sperner properties for groups and relations. *Europ. J. Combinatorics* **7** (1986) 349-370.

[9] J. Rotman, *A First Course in Abstract Algebra*, Prentice-Hall, New Jersey (1996).

[10] R.P. Stanley, Weyl groups, the hard Lefschetz theorem and the Sperner property, *SIAM J. Alg. Disc. Math.* **7** (1980) 168-184.

[11] R.P. Stanley, Quotients of peck posets. *Order* **1** (1984) 29-34.