SOLUTION OF TWO DIFFICULT COMBINATORIAL PROBLEMS WITH LINEAR ALGEBRA

ROBERT A. PROCTOR*
Department of Mathematics, University of California, Los Angeles, CA 90024

(i) *Pick six positive real numbers—any six positive real numbers. If you chose*

$$1, e, \pi, 4, \sqrt{67}, 98.6,$$

you're in trouble, because the object of this game is to have as many subsets as possible adding up to the same sum. For example, choosing

$$5, 6, 8, 9, 13, 14$$

yields three subsets with the same sum:

$$14 = 5 + 9 = 6 + 8.$$

The set

$$3, 4, 5, 6, 7, 8$$

has four subsets adding up to the same number:

$$7 + 8 = 3 + 4 + 8 = 3 + 5 + 7 = 4 + 5 + 6.$$

Choosing

$$1, 2, 3, 4, 5, 6$$

yields five subsets with the same sum:

$$4 + 6 = 1 + 3 + 6 = 1 + 4 + 5 = 2 + 3 + 5 = 1 + 2 + 3 + 4.$$

Is this the best possible? This problem can be more generally posed for n positive real numbers: *Then it seems that no collection does better than*

$$1, 2, 3, \ldots, n - 1, n.$$

Call this problem the **subset sum problem**.

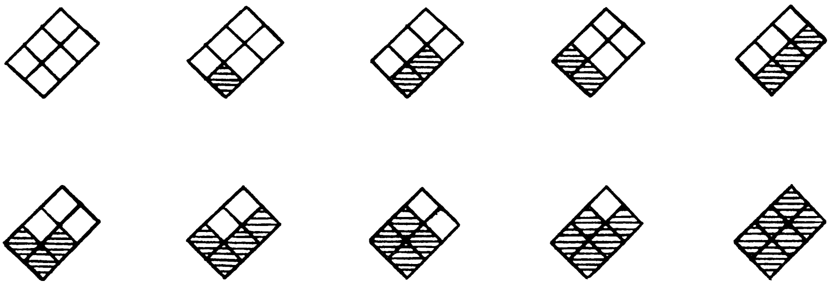

FIG. 1.

(*ii*) *Fix two positive integers m and n. Draw an $m \times n$ grid of squares "on tilt" as in Fig.* 1. *Now shade in some of the squares so that there are no unshaded squares below shaded squares—i.e., so that if the shaded squares were blocks in a rectangular frame, none would slide down. Call such a*

Author's autobiography: My research centers on the combinatorial study of discrete structures arising in Lie theory. When mathematics permits, my hobbies include country swing dancing, soccer, and surfing. I received my graduate education primarily at M.I.T., where my thesis adviser was Richard P. Stanley. I was also a visiting graduate student at the University of California at San Diego for one year, and this is when the ideas contained in this article arose. I am now a Hedrick Assistant Professor at the University of California at Los Angeles.

*Supported in part by an NSF Graduate Fellowship.

shading a **proper shading**. *As an index k runs from 0 to mn, count how many proper shadings there are with k shaded squares. For example, if $m = 2$ and $n = 3$, then the count is*

$$1, 1, 2, 2, 2, 1, 1$$

as k runs from 0 to 6. For $m = 2$ and $n = 4$, the count is

$$1, 1, 2, 2, 3, 2, 2, 1, 1.$$

And for $m = 3$ and $n = 4$ one counts

$$1, 1, 2, 3, 4, 4, 5, 4, 4, 3, 2, 1, 1.$$

It seems that the count always weakly increases until half of the squares have been shaded, and then weakly decreases until all of the squares have been shaded. In other words, there seem to be no "dips" in the count. It gets bigger, then smaller. Is this always true for any size grid? Call this the **grid shading problem**.

1. Introduction. *Letting the cats out of the bags, the answers to both of the questions above are what you would expect. The choice*

$$1, 2, 3, \ldots, n-1, n$$

is the best possible, and there are not any dips in the proper shading count for any values of m and n. Proving either of these answers correct is surprisingly hard. All known proofs of these results involve representations of Lie algebras or the symmetric group in some form. We'll give proofs phrased entirely in terms of elementary linear algebra. These proofs were obtained by translating the essential parts of Lie algebraic proofs into linear algebra. So knowledge of undergraduate linear algebra is the only background you'll need.

Let $p_0, p_1, \ldots, p_r$ be a sequence of numbers. If

$$p_0 \leqslant p_1 \leqslant \cdots \leqslant p_{h-1} \leqslant p_h \geqslant p_{h+1} \geqslant \cdots \geqslant p_{r-1} \geqslant p_r$$

for some h between 0 and r, then the sequence is said to be **unimodal**. The grid shading problem can now be succinctly stated: *Is the sequence of proper shading counts unimodal for all values of m and n?*

How did this problem and its solution arise? Unfortunately from a theatrical point of view, the grid shading problem first arose in the subject in which it was ultimately solved: Classical Invariant Theory. (Not a dashing rescue of some befuddled combinatorialists by the Lie algebra cavalry: The ancestors of modern day Lie representation theorists got themselves into and out of this one!) While finding all covariants of a binary quantic in the early 1850's, Arthur Cayley apparently took the unimodality of the grid shading counts completely for granted. At the same time, he accepted without proof the independence of a certain set of linear equations. In the words of James Sylvester, this crucial gap in Cayley's methods remained for "upwards of a quarter century." Then in 1878, "by aid of a construction drawn from the resources of Imaginative Reason," Sylvester "accomplished with scarcely an effort a task which (he) had believed lay outside the range of human power," and showed that Cayley's equations were in fact independent. The unimodality of the proper shading counts is an immediate consequence of the independence of these equations. Other proofs have appeared over the last century in various contexts, including representations of the symmetric group, Hodge theory, and representations of Lie algebras. But all of these proofs, including the one presented in this article, are related to the methods of Cayley and Sylvester. However, this being 1982, instead of using "a construction drawn from the resources of Imaginative Reason," we'll use a "trick" for our crucial step.

Upon hearing of this unimodality theorem and its mysterious proofs a few years ago, some combinatorialists decided to look for a more satisfying "combinatorial" proof: For each $k < mn/2$ (less than half of the squares shaded), explicitly describe a one-to-one map from the set of proper shadings with k squares shaded into the set of proper shadings with $k + 1$ squares shaded. This would imply that the proper shading count increases until half of the squares have been shaded. A simple symmetry argument then completes the proof. At first glance it seems like it should be easy to find such a proof, but to date such proofs have been found only for the cases where one of m or n is less than or equal to 5.

In contrast to the grid shading problem, the story behind the subset sum problem *does* have something of a dramatic twist. Since this problem was of genuinely combinatorial origins, its solution was almost necessarily by accident: No one in his right mind would consider using the cohomology of projective algebraic varieties! However, this was the technique which led to the first solution of this problem. First proposed by that grandmaster of intriguing combinatorial problems himself, Paul Erdős, and Leo Moser in 1963, no progress was made on the problem until 1969. At that time, Bernt Lindström reduced the problem to showing that a certain family of partially ordered sets have the "Sperner" property. Completely unaware of both the original problem and Lindström's reduction, Richard Stanley showed in 1978 that this family of partially ordered sets do have the Sperner property. Stanley's methods used the hard Lefschetz theorem of algebraic geometry, which concerns the effect of multiplication by the cohomology class corresponding to a hyperplane section in the cohomology ring of a projective algebraic variety. However, the solution was not complete until these two pieces were combined. The connection was made by Larry Harper during a phone call with Stanley, the original purpose of which was to discuss a house sublet during a sabbatical leave! The Lie algebraic solution from which our proof is derived is closely related to Stanley's algebraic geometric solution.

The solutions presented here proceed as follows: We'll associate a family of partially ordered sets to each problem, and then show how the questions at hand can be translated into properties of the partially ordered sets. Next we'll associate vector spaces with linear operators to each partially ordered set. Everything will then be reduced to showing that the linear operators have the largest ranks possible. The solutions will be completed by proving this with a trick borrowed from the representation theory of Lie algebras.

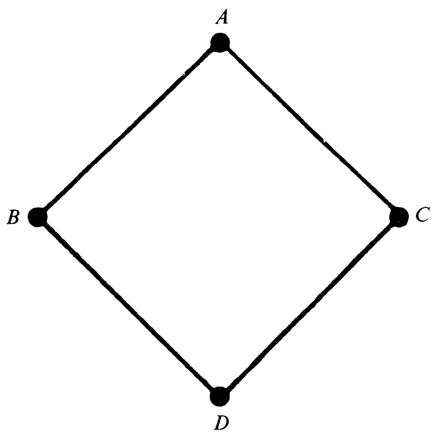

FIG. 2.

2. Poset Formulation. A **finite partially ordered set** ("**poset**" for short) is just a finite set upon which an ordering relation $\leqslant$ has been defined. As indicated by the word "partial," it is not necessary for any two elements to be related by $\leqslant$. For example, Fig. 2 shows what a poset describing the logical dependence of four chapters in a textbook might look like: Chapter A must precede Chapters B and C, and Chapters B and C must precede Chapter D, but neither Chapter B nor Chapter C must precede the other.

For any fixed values of m and n, there's a natural partial ordering of the various proper shadings of an $m \times n$ grid: Order the proper shadings "by containment." See Fig. 3 for the case $m = 2$ and $n = 2$. Given a proper shading, let a_1 be the number of squares shaded in its top right

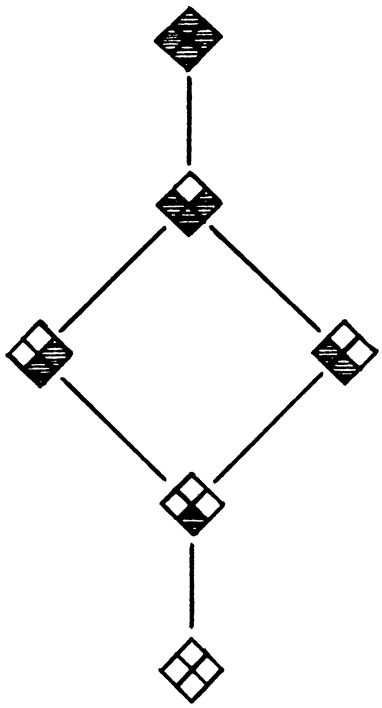

FIG. 3.

row, a_2 the number shaded in the next row,..., and a_n the number shaded in the bottom left row. Note that

$$0 \leqslant a_1 \leqslant a_2 \leqslant \cdots \leqslant a_{n-1} \leqslant a_n \leqslant m.$$

Let the n-tuple

$$\mathbf{a} = (a_1, a_2, \ldots, a_n)$$

denote this shading. It's easy to see that there's a 1-1 correspondence between the collection of all such n-tuples and the set of all proper shadings of the $m \times n$ grid. Now the poset of proper shadings can be officially described:

$$\mathbf{a} \leqslant \mathbf{b}$$

if and only if

$$a_1 \leqslant b_1, \quad a_2 \leqslant b_2, \quad \ldots, \quad a_n \leqslant b_n.$$

We'll call this poset ***L(m, n)***. Fig. 4 shows $L(3,3)$.

Whenever one element of a poset lies immediately above another element, we'll say that the first element **covers** the second. For example, the element $(1,2,3)$ covers the element $(1,1,3)$ in $L(3,3)$. A poset P which can be split up into $r+1$ subsets

$$P_0, P_1, P_2, \ldots, P_{r-1}, P_r$$

such that elements in P_k cover *only* elements in P_{k-1} is called **ranked**. (The smallest example of a poset which cannot be ranked has a diagram which is a pentagon.) If we let p_k denote the number of elements in the **kth rank** P_k, the sequence of numbers

$$p_0, p_1, p_2, \ldots, p_{r-1}, p_r$$

lists the sizes of the ranks of P. If this sequence is unimodal, we'll call P a **rank unimodal** poset.

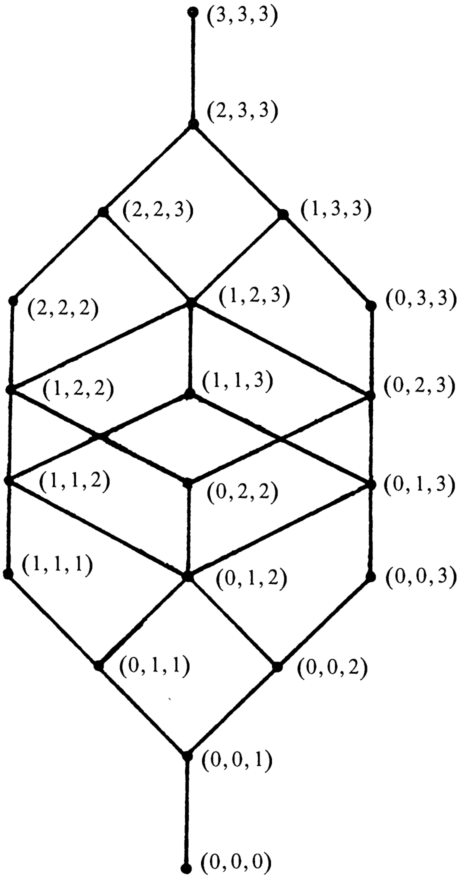

FIG. 4. $L(3,3)$.

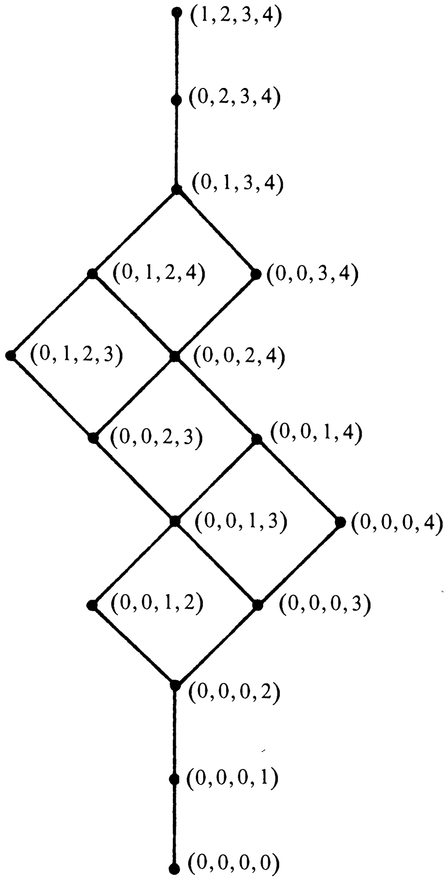

FIG. 5. $M(4)$.

In the posets $L(m, n)$, the 0th rank consists of just the empty grid. As we generate all proper shadings by adding one shaded square at a time, note that all the grids with k squares shaded will lie in the kth rank of $L(m, n)$. So the size of the kth rank of $L(m, n)$ is the number of proper shadings of an $m \times n$ grid with k squares shaded. Therefore the grid shading problem can be restated as: *Show that the posets $L(m, n)$ are rank-unimodal for all values of m and n.*

There's a family of posets closely related to the $L(m, n)$ whose structures play a crucial role in the solution of the subset sum problem. Let ***M(n)*** denote the set of all n-tuples of integers

$$\mathbf{b} = (b_1, b_2, \ldots, b_n)$$

such that

$$0 = b_1 = \cdots = b_j < b_{j+1} < b_{j+2} < \cdots < b_n \leqslant n$$

where j is some integer $0 \leqslant j \leqslant n$. For example, if $n = 3$, there are eight such 3-tuples:

$$(0,0,0), \quad (0,0,1), \quad (0,0,2), \quad (0,0,3),$$
$$(0,1,2), \quad (0,1,3), \quad (0,2,3), \quad (1,2,3).$$

Now define a partial ordering on the set $M(n)$ exactly as we did for $L(m, n)$:

$$\mathbf{a} \leqslant \mathbf{b}$$

if and only if

$$a_1 \leqslant b_1, \quad a_2 \leqslant b_2, \quad \ldots, \quad a_n \leqslant b_n.$$

See Fig. 5 for a picture of $M(4)$.

The 0th rank of $M(4)$ consists of the 4-tuple $(0,0,0,0)$. As we move upward in the poset, we see that each succeeding rank consists of 4-tuples whose entries add up to a sum 1 greater than the sums of the 4-tuples in the preceding rank. Therefore the kth rank of $M(4)$ consists of 4-tuples which add up to k. For example, the 5th rank of $M(4)$ consists of $(0,0,2,3)$ and $(0,0,1,4)$. It is not hard to see that this is true for the ranks of any $M(n)$.

Now recall that the subset sum problem concerned the sums of the elements of subsets of a set of n positive real numbers. In particular, it was claimed that the set

$$N = \{1,2,3,\ldots, n-1, n\}$$

had at least as many subsets adding up to a common sum as did any other set of n positive real numbers. If we look back at our definition of $M(n)$, we see that there is a 1-1 correspondence between its n-tuples and the subsets of the set N. Note that under this correspondence, the entries of the n-tuple add up to the same sum as the elements of the subset do. So two subsets of N will add up to the same number k if and only if both of their corresponding n-tuples lie in the kth rank of $M(n)$. Therefore the largest collection of subsets of N with equal sums will be found by taking the subsets which correspond to the n-tuples lying in the largest rank of $M(n)$.

Now remember that what we want to show is that no other set S of n positive real numbers will do better than the set N. Take any such set S and list its elements in increasing order:

$$S = \{s_1, s_2, s_3, \ldots, s_{n-1}, s_n\},$$
$$s_1 < s_2 < s_3 < \cdots < s_{n-1} < s_n.$$

If

$$A = \{s_{i_1}, s_{i_2}, \ldots, s_{i_q}\}, \quad i_1 < i_2 < \cdots < i_q,$$

is a subset of S, then define

$$\mathbf{a} = (0,0,\ldots,0,i_1,i_2,\ldots,i_q)$$

to be a corresponding element of $M(n)$. It will no longer be true for S (as it was for N) that two subsets corresponding to n-tuples in the same rank of $M(n)$ will have equal sums. However, the following *will* be true:

$$\mathbf{a} < \mathbf{b} \quad \text{in } M(n)$$

implies that

$$\Sigma(A) < \Sigma(B),$$

where $\Sigma(A)$ and $\Sigma(B)$ denote the sums of the subsets of S corresponding to the n-tuples **a** and **b**. To see this, just write the elements of S above the entries of **a** and **b** to which they correspond. For example, if

$$S = \{\sqrt{2}, 11, 10\pi, 55\}$$

and

$$A = \{1,3\} \quad \text{and} \quad B = \{1,2,4\},$$

then write

$$\begin{array}{cccc} & & \sqrt{2} & 10\pi \\ (0, & 0, & 1, & 3) \end{array} \quad \text{and} \quad \begin{array}{cccc} & \sqrt{2} & 11 & 55 \\ (0, & 1, & 2, & 4). \end{array}$$

Observe that the element of S written above the ith entry of **a** will be less than the element of S written above the ith element of **b**. Therefore the sum of the elements in A will be less than the sum of the elements in B.

The upshot of all this is: *In order for two subsets of S to have equal sums, they must correspond to incomparable elements of* $M(n)$. (Two elements x and y of a poset are said to be **incomparable** if $x \nleq y$ and $y \nleq x$.) This tells us that the largest collection of subsets of S with equal sums can be no larger than the largest collection of mutually incomparable elements of $M(n)$. A little experimentation for small values of n seems to indicate that the largest collection of mutually incomparable elements of $M(n)$ is never larger than the biggest rank of $M(n)$. If we could prove this to be true for all n, then we'd be done, as the following summary indicates:

Largest collection of subsets of S with equal sums
is no larger than the
Largest collection of mutually incomparable elements of $M(n)$
which is conjectured to be no larger than the
Largest rank of $M(n)$
which is equal in size to the
Largest collection of subsets of N with equal sums.

Any ranked poset which has no collection of mutually incomparable elements larger than its largest rank is said to be **Sperner**. The above argument has reduced the subset sum problem to: *Show that the posets* $M(n)$ *are Sperner for all values of* n.

The methods we'll use in this article will actually show all $L(m, n)$ and $M(n)$ to be both rank unimodal and Sperner. Here's one way to show that a ranked poset P has these properties. Suppose the ranks of P are

$$P_0, P_1, P_2, \dots, P_{r-1}, P_r$$

and suppose we want to show that the sequence of rank sizes is unimodal with a peak at $k = h$. Assume for the time being that to each element x in a rank P_k with $k < h$, we can assign an element y from the rank P_{k+1} such that $x < y$ and such that no element y from the rank P_{k+1} is used more than once when all of the elements of rank P_k have been taken care of. If we can do this, we'll say that we have a **matching** of rank P_k into rank P_{k+1}. Also suppose that we can do the reverse process for each pair of ranks P_k and P_{k-1} when $k > h$ (i.e., find a 1-1 map from P_k into P_{k-1} such that if w in P_{k-1} is assigned to x in P_k, then $w < x$). The following lemma asserts that we will have solved both of our problems if we can find such matchings for $L(m, n)$ and $M(n)$.

LEMMA. *Let P be a ranked poset with* $r + 1$ *ranks. If rank* P_k *can be matched into rank* P_{k+1} *for* $k < h$ *and rank* P_k *can be matched into rank* P_{k-1} *for* $k > h$, *then the poset P is rank unimodal and Sperner.*

Proof. As before, let p_k be the number of elements in the kth rank. The matching conditions clearly imply that $p_k < p_{k+1}$ for $k < h$ and that $p_{k-1} > p_k$ for $k > h$. Thus the sequence of rank sizes is unimodal about $k = h$.

Picture the matchings as special edges in the diagram of P. (See Fig. 6.) Glue the various matchings together and obtain "chains" of elements of the poset which stream into the rank P_h from above, and below. (A **chain** is a subset of a poset in which any two elements are related by $\leqslant$. Chains can be visualized as ascending or descending sequences of elements in the diagram of the poset.) Every element of P lies on one of these chains. Now take any set of mutually incomparable elements in P and plot them on the diagram of P. Each of these elements lies on one of the chains. By the definition of incomparable, no two can lie on one chain. But there are exactly as many chains as there are elements in the biggest rank P_h. Therefore there can't be more elements in this mutually incomparable subset than there are elements in the largest rank P_h. So the poset P must be Sperner, as desired.

3. Linear Algebra Formulation. So far we have translated the original two problems into the question of whether certain matchings exist in the posets $L(m, n)$ and $M(n)$. The proof of the

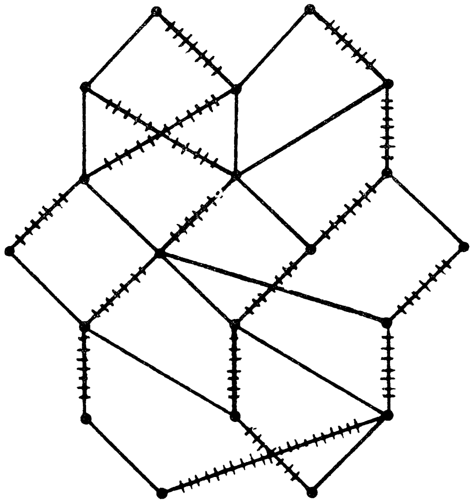

FIG. 6.

existence of such matchings, the heart of the solutions, is in the next section. To get there from here, we must first describe the role that linear algebra plays. In this section we'll work with an arbitrary ranked poset P with ranks

$$P_0, P_1, P_2, \dots, P_{r-1}, P_r.$$

Suppose that the elements of P are $a, b, \dots, e$. Let $\tilde{P}$ denote the vector space over the complex numbers which has a basis consisting of vectors $\tilde{a}, \tilde{b}, \dots, \tilde{e}$ which correspond to the elements of P. Under this set-up, $\tilde{P}_k$ will denote the subspace of $\tilde{P}$ spanned by those basis elements which correspond to elements in rank P_k. We'll call $\tilde{P}_k$ the **kth rank subspace** of $\tilde{P}$. Note that

$$\dim \tilde{P}_k = p_k,$$

the number of poset elements in the rank P_k.

Now define the **order operator** of P to be the linear operator X on $\tilde{P}$ given by:

$$X\tilde{a} = \Sigma_{b \text{ covers } a} \tilde{b}.$$

Unofficially: When X acts on a poset element, it produces the sum of poset elements covering that element. Note that

$$X(\tilde{P}_k) \subseteq \tilde{P}_{k+1}.$$

So let's define X_k to be the linear transformation from $\tilde{P}_k$ to $\tilde{P}_{k+1}$ obtained by restricting X to $\tilde{P}_k$. The matrix for X_k with respect to the poset element bases for $\tilde{P}_k$ and $\tilde{P}_{k+1}$ is a $p_{k+1} \times p_k$ matrix consisting of 0's and 1's. The locations of the 1's describe which elements of P_{k+1} cover which elements of P_k.

We're now ready to state the next step of the solutions:

LEMMA. *Let P be a ranked poset with $r + 1$ ranks and order operator X. If there is some h such that the X_k are injective for $k < h$ and surjective for $k \geqslant h$, then P is rank unimodal and Sperner.*

Proof. Suppose $k < h$. Then X_k is injective and its matrix with respect to the poset basis has rank p_k. This matrix must have at least one nonzero $p_k \times p_k$ minor. The usual determinantal expansion of this minor into $p_k!$ terms must have at least one nonzero term. This term is the product of p_k 1's, where no two of these 1's lie in the same row or the same column of the matrix for X_k. Now the columns of the matrix for X_k are indexed by the elements of P_k and the rows by elements of P_{k+1}. Using the nonzero term of the nonzero minor, we can assign to each element in P_k a covering element from P_{k+1} in such a way that no element from P_{k+1} is used twice. In other words, we get a matching of P_k into P_{k+1}. The same method produces matchings of P_k into P_{k-1} when $k > h$ and X_{k-1} is surjective. Apply the lemma of the previous section to finish the proof.

4. Order Operators Have Maximal Ranks. In this section we'll complete the solutions of the two problems by showing that the order operators for the posets $L(m, n)$ and $M(n)$ satisfy the requirements of the lemma above. The construction used will seem somewhat unmotivated and *ad hoc* to anyone unfamiliar with representations of the Lie algebra $sl(2, \mathbb{C})$. However, the existence of such a construction is almost necessary in these circumstances—more on this in the last section.

Recall that the elements of $L(m, n)$ and $M(n)$ are being denoted by n-tuples

$$\mathbf{a} = (a_1, a_2, \ldots, a_n).$$

Also recall that the order operator X for any poset is defined by

$$X\tilde{\mathbf{a}} = \Sigma_{\mathbf{b}\text{ covers }\mathbf{a}}\tilde{\mathbf{b}}.$$

We'll need two other linear operators H and Y on the vector spaces $\tilde{L}(m, n)$ and $\tilde{M}(n)$. Set

$$H\tilde{\mathbf{a}} = [2(a_1 + a_2 + \cdots + a_n) - mn]\tilde{\mathbf{a}}$$

on $\tilde{L}(m, n)$, and

$$H\tilde{\mathbf{a}} = \left[2(a_1 + a_2 + \cdots + a_n) - \frac{n(n+1)}{2}\right]\tilde{\mathbf{a}}$$

on $\tilde{M}(n)$. Oh yes—we forgot to mention in Section 2 that if $\mathbf{b}$ covers $\mathbf{a}$ in either $L(m, n)$ or $M(n)$, then there is some index i such that $a_i = b_i - 1$ and $a_j = b_j$ when $j \neq i$. But no harm done, since only now do we need this fact: Define the third operator Y on either $L(m, n)$ or $M(n)$ by

$$Y\tilde{\mathbf{b}} = \Sigma_{\mathbf{b}\text{ covers }\mathbf{a}}c(\mathbf{a}, \mathbf{b})\tilde{\mathbf{a}},$$

where (assuming $a_i = b_i - 1$)

$$c(\mathbf{a}, \mathbf{b}) = (m + n - a_i - i)(a_i + i)$$

for $L(m, n)$, and $c(\mathbf{a}, \mathbf{b}) = n(n+1)/2$ if $a_i = 0$, otherwise $= (n - a_i)(n + a_i + 1)$ for $M(n)$. In passing, we culturally remark that each set of three operators defines a representation of $sl(2, \mathbb{C})$ on $\tilde{L}(m, n)$ or $\tilde{M}(n)$.

If you picture the posets $L(m, n)$ and $M(n)$ as in Figures 4 and 5, then the action of X raises vectors by one level, the action of H leaves vectors in their original levels, and the action of Y lowers vectors by one level. By now it should be apparent that the two cases $L(m, n)$ and $M(n)$ are very similar. To save ink, we'll usually refer only to $L(m, n)$ from now on. The rank subspaces of $\tilde{L}(m, n)$ will be denoted by

$$\tilde{L}_0, \tilde{L}_1, \ldots, \tilde{L}_k, \ldots, \tilde{L}_{mn}.$$

Now that we've dispensed with the reductions of the problems, definitions, notation, and preliminary observations, we're ready to get to work. What do we want to prove? Remember that X_k denotes the restriction of X to the rank subspace $\tilde{L}_k$ (or $\tilde{M}_k$ for $\tilde{M}(n)$).

LEMMA. *The linear transformations X_k for $\tilde{L}(m, n)$ are injective if $k < mn/2$ and surjective if $k \geq mn/2$. The linear transformations X_k for $\tilde{M}(n)$ are injective if $k < n(n+1)/4$ and surjective if $k \geq n(n+1)/4$.*

Once we prove this, the solutions are complete. The proof consists of two parts. The first part concerns the "commutation relations" between the three operators X, Y, and H. The second part constructs new bases for the vector spaces $\tilde{L}(m, n)$ and $\tilde{M}(n)$.

Getting on with the first part, we first claim that

$$HX - XH = 2X \quad \text{and} \quad HY - YH = -2Y.$$

These aren't hard to prove: Take $\mathbf{a}$ in L_k. Then

$$H\tilde{\mathbf{a}} = (2k - mn)\tilde{\mathbf{a}} \quad \text{and} \quad H(X\tilde{\mathbf{a}}) = (2k + 2 - mn)X\tilde{\mathbf{a}},$$

since $X\tilde{\mathbf{a}}$ is in $\tilde{L}_{k+1}$. Therefore

$$[HX - XH]\tilde{\mathbf{a}} = [2k + 2 - mn - (2k - mn)]X\tilde{\mathbf{a}} = 2X\tilde{\mathbf{a}}.$$

And similarly for the relation $HY - YH = -2Y$.

More work is required to prove the third commutation relation:

$$XY - YX = H.$$

Again look at the effect of the operators on a basis vector $\tilde{\mathbf{a}}$ in $\tilde{L}_k$. Both $XY\tilde{\mathbf{a}}$ and $YX\tilde{\mathbf{a}}$ lie in $\tilde{L}_k$ and are thus linear combinations of the vectors $\tilde{\mathbf{d}}$ with $d_1 + d_2 + \cdots + d_n = k$. In terms of n-tuples, the effect of X is roughly described as adding 1 to each component of the n-tuple at a time. And Y subtracts 1 from each component at a time. So $\tilde{\mathbf{d}}$ appears in the expansion for $[XY - YX]\tilde{\mathbf{a}}$ exactly whenever there are indices i and j such that

$$d_i = a_i - 1 \quad \text{and} \quad d_j = a_j + 1.$$

If $i \neq j$, then the resulting terms in both $XY\tilde{\mathbf{a}}$ and $YX\tilde{\mathbf{a}}$ have coefficient $(m + n - a_i - i + 1)(a_i + i - 1)$ and thus cancel each other. Therefore $[XY - YX]\tilde{\mathbf{a}}$ is a scalar multiple of $\tilde{\mathbf{a}}$: the only contribution comes from adding then subtracting, or subtracting then adding 1 to the same component. Explicitly,

$$[XY - YX]\tilde{\mathbf{a}} = \Bigg\{ \sum_{\substack{1 \leqslant i \leqslant n \\ a_{i-1} < a_i}} (m + n - a_i - i + 1)(a_i + i - 1) - \sum_{\substack{1 \leqslant i \leqslant n \\ a_i < a_{i+1}}} (m + n - a_i - i)(a_i + i) \Bigg\}\tilde{\mathbf{a}}.$$

The summation conditions result from the requirement that the n-tuples must always satisfy

$$0 \leqslant a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n \leqslant m.$$

(And we have set $a_0 = 0$ and $a_{n+1} = m$.) A close look at these summations reveals that it's O.K. to drop the extra conditions on the summations—any new terms appearing will be zero or will cancel each other. So then

$$\begin{aligned}[XY - YX]\tilde{\mathbf{a}} &= \Bigg\{ \sum_{1 \leqslant i \leqslant n} [(m + n - a_i - i + 1)(a_i + i - 1) - (m + n - a_i - i)(a_i + i)] \Bigg\}\tilde{\mathbf{a}} \\ &= [2(a_1 + a_2 + \cdots + a_n) - mn]\tilde{\mathbf{a}} \\ &= H\tilde{\mathbf{a}}.\end{aligned}$$

Similar steps work for $M(n)$.

This brings us to the second part of the proof of the lemma. We are now ready to take advantage of one of the nicer features of linear algebra, the ability to change bases. Although changing bases will scramble the information currently contained in the matrix descriptions of the transformations X_i, the new basis will help us show that these transformations have the correct ranks. The lemma in Section 3 then provides for the unscrambling of the information back to its original form with the knowledge that the necessary matchings exist.

The construction given below replaces the poset basis used until now for $\tilde{L}(m, n)$ with a new basis which is depicted schematically in Fig. 7. Interpret this diagram as follows. The dots in the kth level of the diagram represent new basis vectors lying in the kth rank subspace $\tilde{L}_k$. And the new basis vectors lying in a vertical line are related by the recursion

$$w_{i+1} = Xw_i.$$

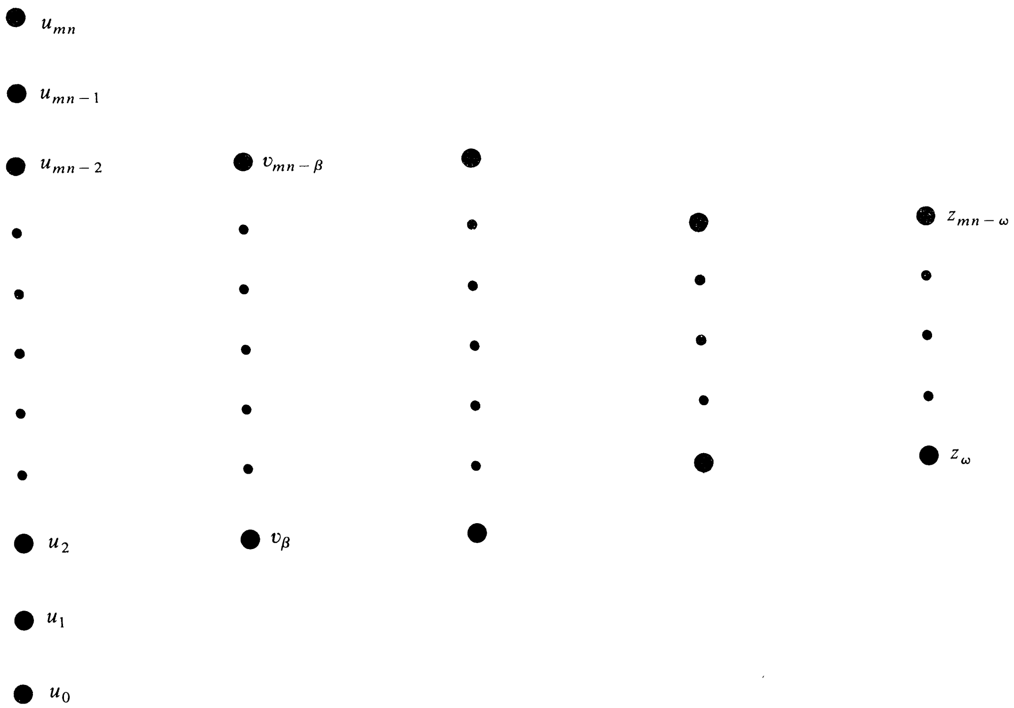

FIG. 7. New basis for $\tilde{L}(m, n)$.

Any sequence of vectors related in this manner is called a **string** of vectors. Our new basis will consist of a collection of strings of vectors with each string symmetric about the middle subspace(s).

Let the first member u_0 of the new basis be $\tilde{\mathbf{a}}_0$, where $\mathbf{a}_0$ is the only element of L_0. Let U be the subspace of $\tilde{L}(m, n)$ spanned by the various vectors obtained by acting on u_0 with all possible compositions of the operators X, Y, and H. For example, $5XYu_0 - 7XHXXu_0$ is a typical element of U. By repeatedly using the commutation relations

$$HX = XH + 2X, YH = HY + 2Y \quad \text{and} \quad YX = XY - H,$$

it's possible to express any composition of the operators X, Y, and H as a linear combination of terms of the form $X^iH^jY^k$. But $Yu_0 = 0$, and H^ju_0 is just a scalar multiple of u_0. So

$$u_0, u_1 = Xu_0, \quad u_2 = X^2u_0, \cdots$$

span the subspace U. Now u_0 is in $\tilde{L}_0$, u_1 is in $\tilde{L}_1$, etc. So these vectors lie in distinct disjoint subspaces of $\tilde{L}(m, n)$, implying that they are linearly independent. Therefore the string of vectors $u_0, u_1, \ldots$ forms a basis for U. But U is finite dimensional. Call the last vector in the string u_s.

How long is this string of vectors? By the definition of U, none of the three operators X, Y, or H can move anything outside of the subspace U. Thus the restrictions of X, Y, and H to U are operators on U. Denote these operators on U by X', Y', and H'. Note for use below that the relation

$$H' = X'Y' - Y'X'$$

still holds. Now take u_k in $\tilde{L}_k$. Then

$$H'u_k = (2k - mn)u_k,$$

since u_k is a linear combination of the $\tilde{\mathbf{a}}$ with $a_1 + a_2 + \cdots + a_n = k$. So the trace of the operator H' can be easily computed:

$$\text{trace } H' = -mn + (2 - mn) + \cdots + (2s - mn).$$

We've finally arrived at the trick alluded to in the introduction: It's a simple fact that

$$\text{trace } AB = \text{trace } BA$$

for any two linear operators A and B. Apply this fact to the operators X' and Y':

$$\text{trace } X'Y' = \text{trace } Y'X'.$$

Then

$$\text{trace } H' = \text{trace } (X'Y' - Y'X') = 0,$$

implying

$$s = mn.$$

We conclude that the string of vectors

$$u_0, u_1, \ldots, u_{mn}$$

forms a basis for U.

Continue the construction of a new basis by letting β be the smallest index such that $U \cap \tilde{L}_\beta$ is not all of $\tilde{L}_\beta$. Pick any vector v_β in $\tilde{L}_\beta$ which is not in U. Let V denote the subspace spanned by all vectors resulting from all possible compositions of X, Y, and H acting on either u_0 or v_β. Since Yv_β must be in U, one can see that

$$v_\beta, \quad v_{\beta+1} = Xv_\beta, \quad v_{\beta+2} = X^2 v, \quad \cdots$$

together with the u_k's span V. If v_q is in U for some index q, then v_r is also in U for all $r \geqslant q$. Let v_t be the last vector in the second string which is not in U. By considering rank subspaces, it's easy to see that the only possible linear dependences among all of the u_k's and v_h's (with $\beta \leqslant h \leqslant t$) must occur between a u_k and a v_k in the same rank subspace $\tilde{L}_k$. But our choice of t prohibits any such degenerate relationships between members of the two strings. The union of the two strings therefore forms a basis for V. The trace trick can be used again to find that

$$t = mn - \beta.$$

So a basis for V is

$$u_0, u_1, \ldots, u_{mn}; \quad v_\beta, v_{\beta+1}, \ldots, v_{mn-\beta}.$$

Repeat this procedure, creating subspaces

$$U \subset V \subset W \subset \cdots \subset \tilde{L}(m, n).$$

Since $\tilde{L}(m, n)$ is finite dimensional, the process must eventually stop. Call the last subspace so constructed Z, and call the last basis vectors so chosen

$$z_\omega, z_{\omega+1}, \ldots, z_{mn-\omega}.$$

All the strings of vectors taken together form a new basis for $\tilde{L}(m, n) = Z$. The subset of these vectors with subscript k forms a basis for the rank subspace $\tilde{L}_k$. Finally note that each string of new basis vectors is symmetric about the middle rank subspace(s): If a string starts in $\tilde{L}_k$ with $k < mn/2$, then it ends in $\tilde{L}_{mn-k}$.

We're now ready to complete the proof of the lemma. If $k < mn/2$, then X_k takes all of the new basis vectors for $\tilde{L}_k$ to new basis vectors for $\tilde{L}_{k+1}$ because no strings end below the middle. So these X_k's are injective, as required. If $k \geqslant mn/2$, then X_k hits every new basis vector for $\tilde{L}_{k+1}$ with a new basis vector from $\tilde{L}_k$, since no strings start above the middle. And so these X_k's are surjective, as required.

We're done! Since this lemma was the last step in our solutions, we can conclude:

THEOREM. *The posets $L(m, n)$ and $M(n)$ are rank unimodal and Sperner. Therefore the proper* *grid shading counts for fixed m and n form a unimodal sequence, and no set of n positive real numbers has more subsets summing to a common sum than does the set* $N = \{1, 2, \ldots, n\}$.

5. Remarks. Our methods proved the existence of rank matchings for $L(m, n)$ and $M(n)$ satisfying the requirements of the lemma in Section 2, but did not explicitly construct such matchings. Some very nice matchings ("symmetric chain decompositions") have been found for $L(2, n)$, $L(3, n)$, $L(4, n)$, and $L(5, n)$ [Li2], [Rie], [Wes] (and K. Leeb and V. Strehl, unpublished). No rank matchings of any kind (not even ones possibly ignoring order relations) have been found for general $L(m, n)$ and $M(n)$.

The Lie representation constructions employed in this article may seem somewhat *ad hoc* and unnatural with respect to the combinatorial situation at hand. However, it can be shown [Pr1] that a ranked poset is rank unimodal, "rank symmetric," and "strongly Sperner" if and only if it "carries" a representation of $sl(2, \mathbb{C})$. **Rank symmetric** means $p_k = p_{r-k}$ and **strongly Sperner** means no union of N antichains is bigger than the union of the N largest ranks, for all $N \geqslant 1$. By **carry**, we mean that three operators X, Y, and H can be defined on the vector space associated with the poset as in this article, except that the operator X need not have all coefficients equal to 1 and the operator Y need not obey the order relations.

The computations required to determine whether a given ranked poset carries a representation of $sl(2, \mathbb{C})$ can be quite difficult. However, the computations become relatively simple in the context modelled the most closely after the situation in this article: distributive lattices, coefficients all equal to 1 for the operator X, and the operator Y respecting the order relations. Surprisingly, it is possible to prove [Pr3] that this version of our techniques can be applied to only one other infinite family of and two exceptional distributive lattices besides the $L(m, n)$ and $M(n)$. Dynkin-like diagrams play a crucial role in the classification procedure. The set of all of these diagrams also arises as the set of Dynkin-like diagrams corresponding to all quotients of semisimple Lie groups which are Hermitian symmetric spaces!

Stanley was the first to prove that $L(m, n)$ and $M(n)$ have the strong Sperner property [St1]. The lemma in Section 3 is a simpler version of a lemma that he developed for this purpose. To show that the operator X satisfied the requirements of his lemma, Stanley first noted that bases for the cohomology rings of certain projective varieties (the Grassmannians for $L(m, n)$) can be labelled in a natural way with elements of $L(m, n)$ or $M(n)$. Then he observed that multiplication by a hyperplane section in the cohomology ring when viewed as a linear operator is exactly the operator X. Stanley completed his proofs with the hard Lefschetz theorem, a major theorem of algebraic geometry: This theorem states that the linear operator defined by multiplication with a hyperplane section produces a vector space isomorphism between "sister" cohomology groups.

In the cases of $L(m, n)$ and $M(n)$ (Stanley also treated many other posets), it is possible to replace the algebraic geometry in Stanley's proofs with representations of Lie algebras. This was done [Pr2] by combining combinatorial identifications of weights of representations by Hughes [Hug] with the construction of principal three dimensional subalgebras due to Dynkin [Dyn, p. 168] in the case of minuscule representations. This replacement yielded the Lie algebraic proofs from which the proofs given here were derived. The trace trick is a standard technique in representation theory [SaW, p. 278].

When the historical background for this article was being researched, after a little translation it was discovered that the vector spaces and operators used by Cayley [Cay] and Sylvester [Syl] for their problem in invariant theory were nearly the same as those used here for the poset $L(m, n)$. Cayley even used the same letters X, Y, and H! Although Sylvester's proof of the injectivity and the surjectivity of the operators X_i is different, it also uses the commutation relations between the three operators. For two other proofs of the unimodality of the grid shading sequences in the context of classical invariant theory, see Springer [Spr, Ex. 3.3.6(1)] and Elliott [Ell, p. 149].

The unimodality of the grid shading sequences has also been proved using representations of symmetric groups by White [Whi], Towber and Wagner [ToW], and Stanley [St2]. Stanley's proof is fairly simple, using nothing more sophisticated than general facts about representations of finite groups. He and Larry Harper [Har] have recently extended these methods to show that $L(m, n)$ is strongly Sperner. Their approach turns out to be a stronger version of some work of Pouzet [Pou]. The paper by Towber and Wagner shows that the symmetric group approach and the $s\mathrm{l}(2, \mathbb{C})$ approach are closely related.

The original conjecture of Erdős and Moser [Erd] actually concerned *any* $2n$ (or $2n + 1$) real numbers, rather than n positive real numbers. The answer is what one would expect:

$$-n, \quad -n+1, \quad \ldots, \quad -1, \quad 0, \quad 1, \quad \ldots, \quad n-1, \quad (n).$$

This conjecture was also first proved by Stanley [St1]. Roughly speaking, if $n = m + z + p$ specifies how many numbers are negative, zero, and positive, his proof consists of showing $M(m) \times M(z) \times M(p)$ to be Sperner (which can also be done with our methods) together with a short elementary argument showing that $z = 1$ and $n = p(\pm 1)$.

The reduction of the conjecture of Erdős and Moser for positive real numbers to the question of the Spernerity of $M(n)$ is due to Lindström [Li1].

I am indebted to my adviser Richard Stanley for encouragement and mathematical inspiration. I am also indebted to Bruce Sagan and several other people for constructive criticisms.

References

[Cay] A. Cayley, A Second Memoir upon Quantics, Coll. Math. Papers, vol. 2, Cambridge University Press, Cambridge, 1889, pp. 250–275.

[Dyn] E. B. Dynkin, Semisimple subalgebras of semisimple lie algebras, Amer. Math. Soc. Transl., Ser. 2, vol. 6 (1957) 111–244.

[Ell] E. B. Elliott, An Introduction to the Algebra of Quantics, Oxford University Press, London, 1913.

[Erd] P. Erdős, Extremal problems in number theory, Theory of Numbers, A. L. Whiteman, Editor, Amer. Math. Soc. Proc. Symp. Pure Math., vol. 8 (1965) 181–189.

[Hug] J. W. B. Hughes, Lie algebraic proofs of some theorems on partitions, Number Theory and Algebra, H. Zassenhaus, Editor, Academic Press, New York, 1977, 135–155.

[Li1] B. Lindström, Conjecture on a theorem similar to Sperner's, Combinatorial Structures and Their Applications, R. Guy, Editor, Gordon and Breach, New York, 1970, p. 241.

[Li2] ______, A partition of $L(3, n)$ into saturated symmetric chains, European J. Comb., 1 (1980) 61–63.

[Pr1] R. A. Proctor, Representations of $s\mathrm{l}(2, \mathbb{C})$ on posets and the Sperner property, SIAM J. Algebraic Discrete Methods, 3(1982)275–280.

[Pr2] ______, Bruhat lattices, plane partition generating functions, and minuscule representations, preprint.

[Pr3] ______, A Dynkin diagram classification of posets satisfying a combinatorial condition, in preparation.

[Rie] W. Riess, Zwei Optimierungsprobleme auf Ordnungen, Arbeitsberichte des Instituts für mathematische Maschinen und Datenverarbeitungen (Informatik) 2 (1978) no. 5 (April) Erlangen.

[SaW] A. Sagle and R. Walde, Introduction to Lie Groups and Lie Algebras, Academic Press, New York, 1973.

[Spr] T. A. Springer, Invariant Theory, Lecture Notes in Mathematics 585, Springer-Verlag, New York, 1977.

[St1] R. P. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, SIAM J. Algebraic Discrete Methods, 1 (1980) 168–184.

[St2] ______, Some aspects of groups acting on finite posets, J. Combin. Theory Ser. A, 32 (1982) 132–161.

[Syl] J. J. Sylvester, Proof of the Hitherto Undemonstrated Fundamental Theorem of Invariants, Coll. Math. Papers, vol. 3, Chelsea, New York, 1973, 117–126.

[ToW] J. Towber and B. Wagner, A new proof of a theorem in classical invariant theory, preprint.

[Wes] D. B. West, A symmetric chain decomposition of $L(4, n)$, European J. Combin., 1 (1980) 379–383.

[Whi] D. E. White, Monotonicity and unimodality of the pattern inventory, Advances in Math., 38 (1980) 101–108.

[Har] L. Harper, Morphisms for the strong Sperner property of Stanley and Griggs, preprint.

[Pou] M. Pouzet, Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations, Math. Z., 150 (1976) 117–134.