KATHY O'HARA'S CONSTRUCTIVE PROOF OF THE UNIMODALITY OF THE GAUSSIAN POLYNOMIALS

By Doron Zeilberger, Department of Mathematics, Drexel University, Philadelphia, PA19104.

Current Address (1990-): Department of Mathematics, Temple University, Philadelphia, PA19122. zeilberg@math.temple.edu

Appeared in: Amer. Math. Monthly 96 (1989), 590-602.

1.Introduction

Kathy O'Hara[6][7] has recently solved a long-standing open problem in combinatorics: to find a *direct combinatorial proof* that the "Gaussian polynomials"

$$G(b,a) := \frac{(1-q^{a+b})(1-q^{a+b-1})...(1-q^{a+1})}{(1-q^b)(1-q^{b-1})...(1-q)} \qquad (1)$$

are unimodal . A polynomial $p(q) = c_0 + c_1 q + ... + c_n q^n$ is *unimodal* if its coefficients are increasing up to a point and then they are decreasing: i.e. there is an integer r such that $c_0 \le c_1 \le ... \le c_r \ge c_{r+1} \ge ...c_n$. (The fact that $G(b,a)$ is a polynomial will be shown below .)

For example $G(2,2) = (1-q^4)(1-q^3)/(1-q^2)(1-q) = 1 + q + 2q^2 + q^3 + q^4$, which is indeed unimodal: $1 \le 1 \le 2 \ge 1 \ge 1$.

The best way to learn a topic is by teaching it. Similarly, the best way to understand a new proof is by writing an expository paper about it. This was the original motivation of the present paper. Once written, I thought that it would be nice if all the readers of this Monthly had the opportunity to savor this elegant proof. All the central ideas and constructions are O'Hara's, but I have made a few minor improvements and shortcuts that I believe to make the argument clearer. I would like to thank Kathy O'Hara for stimulating conversations and correspondence.

The unimodality of the Gaussian polynomials (1) received several 'fancy' proofs, the first one by Sylvester[13]. The most elementary proof before O'Hara's was that of Proctor[8] who only used linear algebra. The reader is urged to look up Proctor's beautiful paper[8] for the history and significance of this problem. I should also mention White's[15] elegant proof that uses Polya theory.

What does it mean to give a direct combinatorial proof? The coefficients of the Gaussian polynomials G(b,a) have a well known combinatorial interpretation. Namely, the coefficient of q^k in G(b,a), let us call it $c_k(b,a)$, equals the number of "partitions of k that have at most a parts and whose largest part is $\le b$ ". In other words, $c_k(b,a)$ equals the number of elements in the set

$$U_k(b,a) := \{p = (p_1, ..., p_a); 0 \le p_1 \le ... \le p_a \le b, p_1 + ... + p_a = k\}. \qquad (2)$$

For example $U_0(2,2)$=00, $U_1(2,2)$=01, $U_2(2,2)$=11, 02, $U_3(2,2)$=12, $U_4(2,2)$=22, whose number of elements are 1, 1, 2, 1, 1 respectively, the same as the coefficients of G(2,2).

The proof of this combinatorial interpretation is as follows ([2],3.2). $U_k(b,a)$ can be partitioned into two disjoint subsets: those elements p for which p_a ¡b, whose number is equal to the cardinality of $U_k(b-1,a)$, and those elements p for which $p_a = b$, whose number is equal to the cardinality of $U_{k-b}(b,a-1)$. Thus (for any finite set A, $|A|$ will denote its number of elements),

$$|U_k(b,a)| = |U_k(b-1,a)| + |U_{k-b}(b,a-1)|. \tag{3}$$

Now, it is readily checked that the Gaussian polynomials (1) satisfy the recurrence

$$G(b,a) = G(b-1,a) + q^b G(b,a-1),$$

which translates to the following recurrence in terms of the coefficients

$$c_k(b,a) = c_k(b-1,a) + c_{k-b}(b,a-1). \tag{4}$$

Since both $|U_k(b,a)|$ and $c_k(b,a)$ satisfy the same recurrence ((3) and (4) are identical), and their boundary values match (check!), they are identical.

In particular it follows from this combinatorial interpretation that $G(b,a)$ is indeed a polynomial, and that its degree is ab, since $U_k(b,a)$ is certainly empty for $k > ab$.

It is readily seen that the coefficients of $G(b,a)$ are symmetric with respect to the middle coefficient : $c_k = c_{ab-k}$. This also follows from the obvious bijection

$$U_k(b,a) \leftrightarrow U_{ab-k}(b,a),$$

given by

$$(p_1, ..., p_a) \leftrightarrow (b-p_a, ..., b-p_1).$$

It follows that in order to prove that G(b,a) is unimodal it is enough to show that

$$|U_k(b,a)| \leq |U_{k+1}(b,a)| \tag{5}$$

for every k in the range $0 \leq k < ab/2$.

A *direct combinatorial proof* of (5) will consist in exhibiting an *explicit* injection (one-to-one and into mapping) from $U_k(b,a)$ into $U_{k+1}(b,a)$ for $0 \leq k < ab/2$.

2.Posets

We will need some standard definitions and elementary results from the the theory of partially ordered sets (POSETS). All that we will need will be presented here, but the reader who wishes to know more about posets is referred to chapter 2 of Stanton and White's excellent textbook [12], and to Greene and Kleitman's well written survey article[4].

A *poset* $(P, \leq)$ is a set P with an order relation $\leq$ which has the following properties:

(i) a $\leq$a for all $a\epsilon P$, (ii) a$\leq$b and b$\leq$a implies a=b, and (iii) a$\leq$b and b$\leq$c implies a$\leq$c.

If $a \leq b$ and $a \neq b$, we write $a < b$. We say that *b covers a* if $a < b$ and there is no c such that $a < c < b$. We shall write $a \rightarrow b$ for "b covers a". A poset is *ranked* if each element $a\epsilon P$ can be assigned a non-negative integer, $rank(a)$, so that $a \rightarrow b$ implies $rank(b) = rank(a) + 1$. The set $L_i = \{a\epsilon P; rank(a) = i\}$ is called the *set of rank i*, or a *level set.*

A good way to visualize a poset P is in terms of its *Hasse diagram*of the poset and the cover relations are indicated by edges: $a \rightarrow b$ is denoted by an edge from a to b. By the transitivity of the order relation (property (iii)) these cover relations completely imply the order relation on P. Figures 1(a) and 1(b) illustrate examples of Hasse diagrams of a ranked and a non-ranked poset respectively.

&&&&&&&&&&&&&&&&&&&&(figure 1 here)

A finite ranked poset is *rank unimodal* if the numbers $w_i = |L_i|$ (sometimes called the *Whitney numbers*of the posets) satisfy, for some k: $w_0 \leq w_1 \leq ... \leq w_k \geq w_{k+1} \geq ....$ A poset is *rank symmetric* if there is an integer m such that $w_i = 0$ for $i > m$ and $w_i = w_{m-i}$. We will call this integer m the *rank of P*: $rank(P) := m$.

A *maximal symmetric chain* in a rank symmetric poset is a sequence of elements $(a_1, ..., a_r)$, such that $a_1 \rightarrow a_2 \rightarrow ... \rightarrow a_r$, and $rank(a_1) + rank(a_r) = rank(P)$, (i.e. the middle rank of the chain coincides with the middle rank of the poset .) A *maximal symmetric chain decomposition* (SCD) of a rank symmetric poset P, is a partition of the set P into a disjoint union of maximal symmetric chains:

$$P = \cup_{i=1}^{L} C_i.$$

Every chain in an SCD of a rank symmetric poset of rank m must contain exactly one element of the middle rank [m/2]. Thus the number of chains ,L, in an SCD is equal to the cardinality of the middle rank , $w_{[m/2]}$.

Let us illustrate all these notions in terms of a simple example: B_3, the three dimensional Boolean lattice. It consists of the $2^3 = 8$ 0-1 vectors with 3 components: 000, 001, 010, 100, 011, 101, 110, 111. The order is defined by $(a, b, c) \leq (a', b', c')$ if and only if $a \leq a'$, $b \leq b'$, $c \leq c'$. The rank is defined by rank(a,b,c)= a+b+c. The level sets are L_0= 000, L_1= 001,010,100, L_2=011,101,110, and L_3=111. Their cardinalities are respectively w_0=1, w_1=3, w_2=3, and w_3=1. Thus B_3 is rank unimodal: $1 \leq 3 = 3 \geq 1$, and rank symmetric of rank 3 : $w_i = w_{3-i}$. It also has an SCD, consisting of the 3 (= w_1) chains: 000 $\rightarrow$ 001 $\rightarrow$ 011 $\rightarrow$ 111, 010 $\rightarrow$ 110, 100 $\rightarrow$ 101.

&&&&&&&&&&&&&&&&&&&&(figure 2 here)

Every SCD induces an injection $L_k \rightarrow L_{k+1}$, for $k < m/2$, given by

$$p \rightarrow successor \quad of \quad p \quad in \quad the \quad chain \quad "to" \quad which \quad p \quad belongs. \tag{6}$$

In particular the property of having an SCD implies rank unimodality and , because the chains are *symmetric*, also rank-symmetry. In fact , it also implies something else. A ranked poset has the *Sperner property*if the maximal size of an *antichain* (a set of elements of P that are pairwise *unrelated*) equals the size of the largest level set, $w_{[m/2]}$. A poset that possesses an SCD is Sperner.

This follows from the facts that the largest level set is certainly an antichain (as are all level sets), and every conceivable antichain can have at most one representative from every one of the $w_{[m/2]}$ chains.

3. Young's Lattice U(b,a)

How does this tie in with the problem of the unimodality of the Gaussian polynomials? It is readily seen that the sets of partitions $U_k(b,a)$ introduced at the beginning are the level sets of the poset $U(b,a)$ consisting of all partitions with $\leq a$ parts and whose parts are $\leq b$:

$$U(b,a) := \{p = (p_1, ..., p_a); 0 \leq p_1 \leq ... \leq p_a \leq b\},$$

where the rank of an element p in U(b,a) is defined to be the sum of its parts: $rank(p) = p_1 + ... + p_a$. The *natural* order relation is $p \leq q$ if and only if $p_i \leq q_i$ for $i = 1, ..., a$. Under this order U(b,a) is called Young's lattice. The problem of proving the unimodality of the Gaussian polynomials is thus equivalent to showing that the poset U(b,a) is rank-unimodal. Furthermore, an explicit construction of an SCD for U(b,a) would imply, by (6), a constructive proof of this unimodality.

More generally, Given a partition λ, the Young lattice Y_λ, corresponding to λ is defined to be the set of all partitions p such that $p \leq \lambda$, with the same definition of $\leq$ and *rank* as before. The U(b,a) are the special cases of $\lambda = b^a$ (b repeated a times). U(b,a) is rank-unimodal, but what about Y_λ for general λ ? Of course Y_λ is no longer rank symmetric, but it appears to be rank unimodal for small λ. For example for $\lambda = 12$, Y_{12}=00, 01, 02, 11 , 12 , and L_0= 00, L_1=01, L_2 = 02, 11 , L_3= 12. So w_0= 1, w_1=1, w_2=2, and w_3=1, and since $1 \leq 1 \leq 2 \geq 1$, Y_{12} is rank unimodal.

The same phenomenon turns out to be true for much larger λ, so it was reasonable to conjecture that Y_λ, although obviously not rank symmetric, is nevertheless rank unimodal. It came as a great surprise when Dennis Stanton[11] , assisted by computer, found a counterexample: for λ= (4,4,8,8), Y_λ is *not* rank-unimodal. Furthermore, Stanton proved something that no computer can do by itself: he found *infinite* families of counterexamples, the simplest one being $(4, 4, 2k, 2k)$ for $k \geq 4$.

Let us go back to the rank unimodality of U(b,a), which we saw was equivalent to the unimodality of the Gaussian polynomials G(b,a). The rank unimodality itself was first established by Sylvester[13], as a spin-off of a deep theorem in the theory of invariants. But what about a *constructive proof*, or better still, an explicit construction of an SCD for U(b,a) ? As we saw, such an SCD would imply the Sperner property.

Even the mere existence of an SCD for U(b,a) is still an open problem. However to deduce the Sperner property, as well as rank unimodality, you don't quite need a *symmetric* chain decomposition. It is enough to have a *maximal chain decomposition all whose chains pass through the largest level set*from algebraic geometry, proved the *existence* of such a chain decomposition for the poset U(b,a) as well as for some other posets, among them the posets M(n) of all *strict* partitions whose largest part is $\leq$ n:

$$M(n) := \{p = (p_1, ..., p_i); 0 \leq i \leq n, 0 < p_1 < ... < p_i \leq n\},$$

with the same rank and order relation definitions as for U(b,a).

Stanley's proofs for U(b,a) and M(n) were subsequently simplified by Proctor[8]. Incidentally, the

Spernerity of M(n) , that Stanley discovered almost as an afterthought , trying to apply the "hard Lefschetz" hammer to as many nails as possible, turned out to be equivalent to a long standing conjecture of Erdos and Moser. Stanley found out about it, quite by accident, from Larry Harper, during a phone call whose original purpose was to discuss a house sublet during a sabbatical leave! (see Proctor[8] for this fascinating story of serendipity).

However, Both Stanley's proof and Proctor's simplifications were non-constructive, existence, proofs. It is still an open problem to find an explicit construction of an SCD for U(b,a), (or even that of a non-symmetric decomposition as above) . To date such a construction is only known when a or b are either 3 or 4 (see Lindstrom[5], West[14], Riess[9]).

In order to get a constructive proof of the unimodality of $G(b, a)$ we would have to define explicit injections $U_k(b, a) \rightarrow U_{k+1}(b, a)$ for $k < ba/2$. However the existence of an SCD in Young's lattice U(b,a) would entail that these injections, given by (6), are "nice": they map each partition of k not just to an *arbitrary* partition of k+1, but to one that is *covered by it*Perhaps this is asking for too much?

It turns out that the problem of constructing not necessarily "nice" injections can be formulated in terms of an SCD for a modified poset. Just change the order relation! Now that "everything goes", we can define a new order:

$p < q$ if and only if $rank(p) < rank(q)$,

and an SCD with respect to this new order will still yield explicit injections $U_k \rightarrow U_{k+1}$.

¿From now on we will forget all about the natural order and will tacitly assume that U(b,a) is equipped with this new, trivial, order.

&&&&&&&&&&&&&&&&&&&&&&&&&(Fig. 3 here)

4. Three Lemmas

We will need three simple lemmas.

LEMMA 1: Let P be a rank-symmetric ranked poset of rank m and let us define $\bar{P}$ to be the same poset (i.e. the same set and the same order relation), but with the rank defined by

$$r\bar{a}nk(p) = rank(p) + \alpha,$$

for some integer α. Then $\bar{P}$ is a rank-symmetric ranked poset of rank $m + 2\alpha$.

(We say that $\bar{P}$ is the *shift of P by α.*)

PROOF: We have $w_i = \bar{w}_{\alpha+i}$. Thus $w_i = w_{m-i}$ implies $\bar{w}_{\alpha+i} = \bar{w}_{m-i+\alpha} = \bar{w}_{(m+2\alpha)-(\alpha+i)}$.

A mapping $\pi : P \rightarrow Q$ between two posets P and Q is a *rank preserving, order preserving bijection* if:

(i) π is a bijection between P and Q as sets, (ii) rank (π(p))= rank(p), and (iii) if $p \leq p'$ then $\pi(p) \leq \pi(p')$.

LEMMA 2 : Let P and Q be ranked posets. Let $\pi : P \rightarrow Q$ be a rank preserving, order preserving bijection from P to Q, then if P has an SCD, so does Q. Furthermore, if we know π explicitly, and the SCD for P is explicit, then the SCD for Q can be constructed explicitly.

PROOF: If $P = unionfrom1toLC_i$ is an SCD for P, then $Q = unionfrom1toL\pi(C_i)$ is an SCD for Q.

If P and Q are posets then their *cartesian product* $(P \times Q, \leq)$ is defined by

$$P \times Q = \{(p, q); p\epsilon P, q\epsilon Q\},$$

and the order relation is defined by $(p, q) \leq (p', q')$ if and only if $p \leq p'$ and $q \leq q'$. If P and Q are ranked, then $P \times Q$ is made into a ranked poset by defining the rank by $rank(p, q) = rank(p) + rank(q)$. Of course $(p, q) \rightarrow (p', q')$ if and only if either $p \rightarrow p'$ and $q = q'$ or $p = p'$ and $q \rightarrow q'$.

LEMMA 3 ([3]): If P and Q are rank-symmetric ranked posets, of rank m and m' respectively, and we know how to construct SCDs for both P and Q, then there is an explicit way to construct an SCD for $PtimesQ$, and $P \times Q$ is a ranked, rank-symmetric poset of rank m+m'.

PROOF : Let $P = unionfromi = 1toLC_i$ and $Q = unionfromj = 1toMD_j$ be the SCDs for P and Q respectively. Then

$$P \times Q = \cup fromi = 1toL \cup fromj = 1toMC_i \times D_j.$$

Let $C_i = p_1 \rightarrow ... \rightarrow p_r$ and $D_j = q_1 \rightarrow ... \rightarrow q_s$. We claim that $C_i \times D_j$ can be decomposed into a union of min(r,s) maximal symmetric chains of $P \times Q$. Indeed, the following chains exhaust $C_i \times D_j$, $1 \leq l \leq min(r, s)$:

$$(p_1, q_l) \rightarrow ... \rightarrow (p_{r-l+1}, q_l) \rightarrow (p_{r-l+1}, q_{l+1}) \rightarrow ... \rightarrow (p_{r-l+1}, q_s). \tag{7}$$

These chains are symmetric, (and the rank of $P \times Q$ is m+m') since

$$rank(p_1, q_l) + rank(p_{r-l+1}, q_s) = rank(p_1) + rank(q_l) + rank(p_{r-l+1}) + rank(q_s) =$$
$$rank(p_1) + rank(q_1) + l - 1 + rank(p_r) - (l - 1) + rank(q_s) =$$
$$(rank(p_1) + rank(p_r)) + (rank(q_1) + rank(q_s)) = m + m'.""$$

A good way to picture these chains is as follows. Arrange $C_i \times D_j$ in rectangular form:

$$(p_1, q_1)(p_2, q_1)...(p_r, q_1)$$
$$(p_1, q_2)(p_2, q_2)...(p_r, q_2)$$

...

$$(p_1, q_s)\,(p_2, q_s)\,...(p_r, q_s) \quad ,$$

then the chains are obtained by successively "peeling off" the chain that is obtained by going from left to right along the top row and continuing all the way down the rightmost column.

&&&&&&&&&&&&&&&&&&&&&&&&&&&&(Fig. 4 here)

5. The Art of Constructing Symmetric Chain Decompositions

How does one go about constructing SCDs for a family of posets such as $U(b,a)$? One approach would be to discover a recursive decomposition that expresses $U(b,a)$ in terms of $U(b',a')$ for $b' < b$ or $a' < a$. This by itself is not hard. For example by the proof of the combinatorial interpretation of the Gaussian polynomials $G(b,a)$ given at the beginning , there is a bijection

$$U(b,a) \leftrightarrow U(b-1,a) \cup \tilde{U}(b,a-1),$$

where $\tilde{U}(b,a-1)$ is the poset $U(b,a-1)$ shifted by b.

However this decomposition is useless for our purposes, since neither $U(b-1,a)$ nor $\tilde{U}(b,a-1)$ have the same rank (as rank-symmetric posets) as the original poset $U(b,a)$. While $U(b,a)$ has rank ab, $U(b-1,a)$ has rank $a(b-1) = ab - b$, and $\tilde{U}(b,a-1)$ has rank $(a-1)b + 2b = ab + b$. In other words the chains of the first subposets, if they exist, would be "too high", while those of the second one would be "too low", while we need all the chains to be "smack in the middle". It follows that we can only use a decomposition of a poset into smaller subposets if all these smaller subposets are rank-symmetric posets *of the same rank as*the original poset.

Another possibility might have been to express U(b,a) as the cartesian product of smaller U(b',a'). For example, for the Boolean lattice B_n, we have $B_n = \{0,1\} \times B_{n-1}$, and applying lemma 3 recursively gives an SCD for B_n ([3]). This does not seem to be possible for $U(b,a)$. O'Hara's ingenuity consisted in *dividing and conquering*: She found a refinement of $U(b,a)$, a certain doubly indexed family of subposets, $U(b,a;m,d)$, that empirically also appeared to be rank-unimodal, rank-symmetric *and of the same rank , ab, as U(b,a)*. She then discovered a "structure theorem" for these smaller subposets, that expressed each of them in terms of the operations "union" and "cartesian product" of posets $U(b',a';m',d')$ for $a' < a$.

It was thus possible to use the three lemmas to recursively construct an SCD for each of these $U(b,a;m,d)$ in terms of those of smaller a. The base cases $a = -1, a = 0, and a = 1$ being trivial, this showed that each of these $U(b,a;m,d)$ had an SCD, and by taking union over all conceivable m and d, it was possible to construct an SCD for U(b,a) itself. We will now present the details.

6. O'Hara's Construction

Recall that

$$U(b,a) := \{p = (p_1, ..., p_a); 0 \leq p_1 \leq ... \leq p_a \leq b\}.$$

Henceforth, for convenience reason $p_i = 0$ for $i \leq 0$ and $p_i = b$ for $i > a$.

Define:

$$spread(p) := max\{p_i - p_{i-2}; 2 \leq i \leq a+1\}.$$

$$M(p) := \{2 \leq i \leq a+1; p_i - p_{i-2} = spread(p)\}.$$

Partition M(p) into

$$M(p) = \cup D_j$$

where the D_j are maximally connected intervals, and define the *degree* of p, $deg(p)$, by

$$deg(p) := \sum_j [\frac{|D_j|+1}{2}].$$

For example for a=13, b=10, and

p= 1 2 2 3 4 5 6 6 6 7 8 8 10 ,

spread(p)=2, M(p)= $2, 5, 6, 7, 11, 13, 14 = 2\ union\ 5, 6, 7\ union\ 11\ union\ 13, 14$; deg(p)=[(1+1)/2]+ [(3+1)/2]+ [(1+1)/2]+ [(2+1)/2]= 1+2+1+1=5.

Note that for p in U(b,a), $deg(p) \leq [(a+1)/2]$, $m \leq b$.

We now define the following subposets:

$$U(b, a; m, d) := \{p\epsilon U(b, a); spread(p) = m and deg(p) = d\}.$$

$$\bar{U}(b, a; m) = \{p\epsilon U(b, a); spread(p) \leq m\}.$$

We make the reasonable convention that U(b,0) contains a single partition: the "empty partition". If a is negative, then U(b,a) is the empty set. We will also make the convention that the cartesian product of the empty poset with a poset P , $\phi \times P$, is isomorphic to P, and its elements will be denoted by (-,p).

Everything would follow from the following theorem.

THEOREM:(*The O'Hara Structure Theorem*)

Let a,b,m,d, be positive integers. The mapping σ :

$$\sigma : \bar{U}(b - md, a - 2d; m - 1) \times U(ma + 2m - 2b, d) \to U(b, a; m, d),$$

to be defined below, is an order preserving bijection such that for every $q\epsilon\bar{U}(b - md, a - 2d; m - 1)$ and $r\epsilon U(ma + 2m - 2b, d)$, we have

$$rank(\sigma(q, r)) = rank(q, r) + 2bd - md(d + 1). \tag{8}$$

Before defining σ and proving the theorem (i.e. showing that σ does indeed what it is supposed to do), let us show how the theorem implies an algorithm for constructing an SCD for any U(b,a; m,d) and thus, by taking the union over all feasible m and d, for U(b,a). The cases $a = -1$ and $a = 0$

are trivial. $U(b,-1)$ *is* the empty set. $U(b,0)$ only contains one element, the empty partition, and thus has an SCD. The case a=1 is not much harder, all the $U(b,1;m,d)$ are empty except when $m=b$ and $d=1$, so $U(b,1)=U(b,1;b,1)$ and there is an SCD consisting of the single chain : $0\to 1\to ...\to b$.

We can assume , recursively,that we know how to construct an SCD for $\bar{U}(b-md,a-2d;m-1)$, since it is a union of certain $U(b',a';m',d')$ for $a'=a-2d<a$. We can also assume that we know how to construct an SCD for $U(ma+2m-2b,d)$, since $d\leq[(a+1)/2]<a$ for $a>1$. Thus, by lemma 3, we know how to construct an SCD for their cartesian product $\bar{U}(b-md,a-2d;m-1)\times U(ma+2m-2b,d)$. This poset has rank $(b-md)(a-2d)+(ma+2m-2b)d$, and when shifted by $2bd-md(d+1)$, lemma 1 tells us that it has rank $(b-md)(a-2d)+(ma+2m-2b)d+2(2bd-md-md^2)=ba$. The theorem tells us that σ is a rank preserving , order preserving bijection between this shifted poset and $U(b,a;m,d)$. It follows from lemma 2 that $U(b,a;m,d)$ has an SCD, and that its rank is ab . Since all the $U(b,a;m,d)$ have the same rank as $U(b,a)$, (i.e. ab), an SCD for U(b,a) is obtained by combining all the chains of the SCDs for the constituent U(b,a;m,d).

7. Proof of the O'Hara Structure Theorem

In order to prove the theorem we have to: (i)Define the mapping σ . (ii)Define its alleged inverse π . (iii)Prove that σ is well defined .

(iv)Prove that π is well defined . (v)Prove that the composition $\sigma\pi$ is the identity mapping on $U(b,a;m,d)$. (vi) Prove that the composition $\pi\sigma$ is the identity mapping on $\bar{U}(b-md,a-2d;m-1)\times U(ma+2m-2b,d)$. (vii)Prove that (8) is correct . (viii)Prove that σ is order preserving .

It is easier, pedagogically, to start with the definition of π. So we will perform the eight tasks above in the following order : (ii),(i), (iv), (iii), (v),(vi),(vii),(viii).

(ii) DEFINITION OF $\pi: U(b,a;m,d)\to\bar{U}(b-md,a-2d;m-1)\times U(ma+2m-2b,d)$.

Let $p=(p_1,...,p_a)$ be in $U(b,a;m,d)$. We will define $\pi(p)=(q(p),r(p))=(q,r)$.

Let

$$t+1=maxM(p)=max\{2\leq i\leq a+1;p_i-p_{i-2}=m\},$$

Define a partition $p'=(p'_1,...,p'_{a-2})$ by:

$$p'_i=\{\begin{matrix}p_i,1\leq i\leq t-2\\ p_{i+2}-m,t-1\leq i\leq a-2\end{matrix}$$

[we will show that $p'\epsilon U(b-m,a-2;m,d-1)$ when $d>1$ and $p'\epsilon\bar{U}(b-m,a-2;m-1)$ when $d=1$.]

Let,

$$q(p):=\{\begin{matrix}p',d=1\\ q(p'),d>1[recursively]\end{matrix}$$

and,

$$r' := \{ \begin{array}{c} empty, d=1 \\ r(p'), d>1 [recursively] \end{array}$$

[We will show that r' has $d-1$ parts].

$r(p) = r = (r_1, ..., r_d)$, is defined by:

$$r_i = \{ \begin{array}{c} p_t + p_{t+1} + m(a-t+1) - 2b, i=1 \\ r'_{i-1}, 2 \leq i \leq d. \end{array}$$

(ii) DEFINITION OF σ: $\bar{U}(b-md, a-2d; m-1) \times U(ma+2m-2b, d) \to U(b,a;m,d)$.

Let $q \epsilon \bar{U}(b-md, a-2d; m-1)$ and $r \epsilon U(ma+2m-2b, d)$, we will have to define $\sigma(q,r) = p$, say.

Let r' be the partition with $d-1$ parts obtained from r by deleting the first part: $r'_i = r_{i+1}$, for $1 \leq i \leq d-1$. [Obviously r' belongs to $U(ma+2m-2b, d-1)$].

Let

$$p' := \{ \begin{array}{c} q, d=1 \\ \sigma(q, r'), d>1 \end{array} .$$

[We will show that p' has $a-2$ parts.]

We will now define a certain integer t, $1 \leq t \leq a$. If r_1=0, let t=a. Otherwise let t be the [unique] integer that satisfies

$$p'_{t-1} + p'_t - mt < r_1 - m(a+2) + 2b \leq p'_{t-2} + p'_{t-1} - m(t-1). \tag{9}$$

We define $p = \pi(q,r)$ by

$$p_i = \{ p'_i, 1 \leq i \leq t-1$$

$$r_1 - p'_{t-1} - m(a-t+2) + 2b, i=t$$

$$p'_{i-2} + m, t+1 \leq i \leq a$$

(iv) PROOF THAT π IS WELL DEFINED

p' is a genuine partition, since $p'_{t-1} = p_{t+1} - m = p_{t-1} \geq p_{t-2} = p'_{t-2}$. Here we have used the fact that $t+1 \epsilon M(p)$, and thus $p_{t+1} - m = p_{t-1}$. Now it is readily seen that $M(p') = M(p) - \{t+1\}$ if t does not belong to $M(p)$ and $M(p') = M(p) - \{t, t+1\}$ if t belongs to $M(p)$. In either case $deg(p') = deg(p) - 1$ and $spread(p') = m$, if d ¿1, and $spread(p') < m$ if $d=1$.

So $p' \epsilon U(b-m, a-2; m, d-1)$ if $d>1$ and $p' \epsilon \bar{U}(b-m, a-2; m-1)$ if $d=1$. If $d=1$, q is obviously in $\bar{U}(b-md, a-2d; m-1)$, and if $d>1$ it belongs, by the inductive hypothesis to $\bar{U}(b-m-m(d-1), a-2-2(d-1); m-1)$= $\bar{U}(b-md, a-2d; m-1)$.

Let $t'+1 = maxM(p')$. Of course $t' \leq t-2$. It remains to show that r is a genuine partition in $U(m(a+2)-2b,d)$. By the inductive hypothesis r' belongs to $U(m(a-2+2)-2(b-m),d-1) = U(m(a+2)-2b,d-1)$, and to show that r is a bona fide element of $U(m(a+2)-2b,d)$ we will have to show that:

when $d>1$: $0 \leq r_1 \leq r_2$, i.e. $0 \leq r_1 \leq r'_1$, i.e.

$$0 \leq p_t + p_{t+1} + m(a-t+1) - 2b \leq p'_{t'} + p'_{t'+1} + m((a-2)-t'+1) - 2(b-m); \tag{10}$$

when $d=1$, we have to show $r_1 \leq m(a+2)-2b$, i.e.

$$0 \leq p_t + p_{t+1} + m(a-t+1) - 2b \leq m(a+2) - 2b. \tag{11}$$

Making the convention that $t'=-1$ when $d=1$, (11) becomes encompassed by (10), so it suffices to prove (10), but for $d \geq 1$.

The left side of (10) is equivalent to:

$$(b-m) + b - p_t - p_{t+1} \leq m(a-t), \tag{10.a}$$

and the right side of (10) is equivalent to

$$p_t + p_{t+1} - p'_{t'} - p'_{t'+1} \leq m(t-t'). \tag{10.b}$$

Both of these inequalities follow easily from lemma 4 below . (10.a) follows upon taking $A=a$, $B=t$, and noting that $p_{a+1}=b$, and $p_a \leq b-m$. (10.b) follows upon taking $A=t$ and $B=t'$, and noting that since $t' \leq t-2$, $p'_{t'} = p_{t'}$ and $p'_{t'+1} = p_{t'+1}$.

LEMMA 4 : Let $A \geq B$, then

$$p_A + p_{A+1} - p_B - p_{B+1} \leq m(A-B).$$

PROOF: If $A-B$ is even then

$$p_A + p_{A+1} - p_B - p_{B+1} = [p_A - p_B] + [p_{A+1} - p_{B+1}] = [(p_A - p_{A-2}) + ... + (p_{B+2} - p_B)] +$$
$$[(p_{A+1} - p_{A-1}) + ... + (p_{B+3} - p_{B+1})] \leq m(A-B)/2 + m(A-B)/2 = m(A-B).$$

Similarly, if $A-B$ is odd:

$$p_A + p_{A+1} - p_B - p_{B+1} = [p_A - p_{B+1}] + [p_{A+1} - p_B] = [(p_A - p_{A-2}) + ... + (p_{B+3} - p_{B+1})] +$$
$$[(p_{A+1} - p_{A-1}) + ... + (p_{B+2} - p_B)] \leq m(A-B-1)/2 + m(A+1-B)/2 = m(A-B) \quad .$$

(iii) PROOF THAT σ IS WELL DEFINED

Let $q \epsilon \bar{U}(b-md, a-2d; m-1)$ and $r \epsilon U(m(a+2)-2b, d)$. We will prove that $p=\sigma(q,r)$ is indeed a partition that belongs to U(b,a;m,d).

Since $r' \epsilon U(m(a+2)-2b, d-1) = U(m(a-2+2)-2(b-m), d-1)$ and $q \epsilon \bar{U}(b-md, a-2d; m-1)$ $= \bar{U}((b-m)-m(d-1), (a-2)-2(d-1), m-1)$, it follows by the induction hypothesis, for $d>1$, that p' belongs to $U(b-m, a-2; m, d-1)$. If d=1, then of course p' belongs to $\bar{U}(b-m, a-2; m-1)$.

Now we claim that

$$p'_{a-1} + p'_a - ma \leq r_1 - m(a+2) + 2b \leq p'_{-1} + p'_0 - m(1-1)$$

i.e. (since $p'_{-1} = p'_0 = 0$ and $p'_{a-1} = p'_a = b-m$)

$$2b - m(a+2) \leq r_1 - m(a+2) + 2b \leq 0.$$

This is equivalent to $0 \leq r_1 \leq m(a+2) - 2b$, which is obvious.

Now it is readily seen that the closed (discrete) interval $[2b - m(a+2), 0]$ can be partitioned as follows into a union of a single point and half open intervals:

$$[2b-m(a+2), 0] = \{2b - m(a+2)\} \cup \cup from t = a to t = 1 (p'_{t-1} + p'_t - mt, p'_{t-2} + p'_{t-1} - m(t-1)],$$

So the t that was defined in the definition of σ is well defined. Now let us show that p is a genuine partition. We must show that $p_t \geq p_{t-1}$ and $p_{t+1} \geq p_t$, both of which follow easily from (9). Furthermore, $p_a = p'_{a-2} + m \leq b - m + m = b$, so $p \epsilon U(b,a)$. Also $t+1 \epsilon M(p)$, while t may or may not be in M(p).

Now since

$$r_1 - m(a+2) + 2b \leq r_2 - m(a-2+2) + 2(b-m)$$

the " previous t", let us call it t', that was obtained in the previous step out of r_2, satisfies $t' \leq t-2$. (if $d=1$, then $t'=-1$.) Thus $M(p) = M(p') union \{t+1\}$ or $M(p) = M(p') union \{t, t+1\}$. (If d=1, M(p') is empty.) If $d>1$, deg(p)=deg(p')+1=d-1+1=d. Of course spread(p)=m, and if $d=1$, $deg(p)=1$, since $M(p)$ consists of either t or t t+1 , so in either case $p \epsilon U(b, a; m, d)$.

(vi) PROOF THAT $\pi\sigma$ IS THE IDENTITY

Let $p = \sigma(q,r)$. We have to show that $\pi(p) = (q,r)$. We have just seen that $M(p) = M(p') union$ t or $M(p) = M(p') union \{t, t+1\}$. In either case $t+1 = max M(p)$, so the " t obtained in doing $\pi(p)$", is the same as " the t obtained in doing $\sigma(q,r)$". By the inductive hypothesis, if $p' = \sigma(q, r')$, then $\pi(p') = (q, r')$.

Finally, " the r_1 obtained from $\pi(p)$" is

$$p_t + p_{t+1} + m(a-t+1) - 2b = r_1 - p'_{t-1} - m(a-t+2) + 2b + p'_{t-1} + m + m(a-t+1) - 2b = r_1,$$

as it should.

(v) PROOF THAT $\sigma\pi$ IS THE IDENTITY

Let $(q,r) = \pi(p)$, we have to show that $\sigma(q,r) = p$.

We have that $p_t + p_{t+1} = r_1 - m(a-t+1) + 2b$. But $p_{t+1} = p_{t-1} + m$, since $t + 1 \epsilon M(p)$. So $p_t = r_1 - m(a-t+2) + 2b - p_{t-1}$. Now t may or may not be in $M(p)$, thus $p_t - p_{t-2} \leq m$, which yields the right side of (9), and $t+2$ does not belong to $M(p)$, so $p_{t+2} - p_t < m$, which yields the left side of (9). Thus the "t obtained in doing $\sigma(\pi(p))$" is the same as the "t obtained in doing $\pi(p)$. The rest follows from the inductive hypothesis.

(vii) Proof That

$$rank\sigma(q,r) = rank(q,r) + 2bd - md - md^2. \tag{8}$$

We have

$$rank\sigma(q,r) = rank(p) = p_1 + ... + p_a = p'_1 + ... + p'_{t-1} +$$
$$(r_1 - p'_{t-1} - m(a-t+2) + 2b) + (p'_{t-1} + m) + ... + (p'_{a-2} + m) = rank(p') + r_1 + 2(b-m).$$

If $d = 1$, $p' = q$ and $r = r_1$, so

$$rank\sigma(q,r) = rank(q) + rank(r) + 2(b-m),$$

which agrees with (8) when $d = 1$.

When $d > 1$, using the inductive hypothesis gives:

$$ranksigma(q,r) = ranksigma(q,r') + r_1 + 2(b-m) =$$
$$rank(q) + rank(r') + 2(b-m)(d-1) - m(d-1)d + r_1 + 2(b-m) =$$
$$rank(q) + rank(r) + 2bd - md(d+1) = rank(q,r) + 2bd - md(d+1).""$$

(viii) PROOF THAT σ IS ORDER PRESERVING

Immediate from (vii). (Recall that the order we took on U(b,a) is the trivial one in which $p < q$ if and only if $rank(p) < rank(q)$.)

8. Examples

(i)Example of $\pi : U(5,5;2,2) \to \bar{U}(1,1;1) \times U(4,2)$.

Let $a=5$, $b=5$, $m=2$ and $d=2$, $p=12244$. Here $t=4$, and $r_1=4+4+2(5-4+1)-2(5)=2$; p'=122. Now $a=3, b=3$, $t=1$, and "r_1"$=r_2=1+2+2(3-1+1)-2(3)=3$; p''=("current p'")=0. So $q=0\epsilon\bar{U}(1,1;1)$ and $r=23\epsilon U(4,2)$. Summing up: $\pi(12244)=(0,23)$.

(ii) Example of $\sigma:\bar{U}(1,1;1)\times U(4,2)\to U(5,5;2,2)$.

Let us try and find $\sigma(0,23)$, and see if we get the input of (i) back.

We have $q=0$, $r=23$. We start with $a=3$, $b=3$, $d=1$, $m=2$. $2b-m(a+2)=-4$. The intervals $(p'_{t-1}+p'_t-mt, p'_{t-2}+p'_{t-1}-m(t-1)]$, for $t=1$ is $(-3,0]$, and since $r_1-m(a+2)+2b$= $3-2(3+2)+2(3)=-1$, and -1 falls in (-3,0], $t=1$. $p_1=3-0-2(3-1+2)+2(3)=1$; $p_2=2$, and $p_3=p'_1+2=2$. So the output from the first stage was $p=122$, which is the "current p'" of the second stage. Now $a=5, b=5, m=2$,and $r_1=2$, $2b-m(a+2)=2(5)-2(5+2)=-4$. The intervals $(p'_{t-1}+p'_t-mt, p'_{t-2}+p'_{t-1}-m(t-1)]$, for $t=5,4,3,2,1$ are respectively: $(-4,3],(-3,-2],(-2,-1],(-1,-1], and(-1,0]$. $r_1-m(a+2)+2b=2-4=-2$ falls in the interval $(-3,-2]$, so $t=4$. $p_1=1, p_2=2, p_{3=2}$, and $p_4=2-2-2(5-4+2)+2(5)=4$, $p_5=p'_3+m=2+2=4$. So $\sigma(0,23)=12244$.

(iii) The O'Hara SCD for U(4,3)

We have:

$$U(4,3)=U(4,3;4,1)\cup U(4,3;3,1)\cup U(4,3;2,2)$$

(a)U(4,3;4,1)

$U(4,3;4,1)\equiv\bar{U}(0,1;3)\times U(12,1)=U(0,1)\times U(12,1)=0{\times}0\to 1\to 2\to ...\to 12$. $\bar{U}(0,1;3)\times U(12,1)$ consists of the single chain $(0,0)\to(0,1)\to...(0,12)$. Applying σ to it yields the SCD for $U(4,3;4,1)$ consisting of the single chain: $000\to 001\to 002\to 003\to 004\to 014\to 024\to 034\to 044\to 144\to 244\to 344\to 444$.

(b) U(4,3;3,1)

$U(4,3;3,1)\equiv\bar{U}(1,1;2)\times U(7,1)=U(1,1)\times U(7,1)=0\to 1\ \times\ 0\to 1\to ...\to 7$.

Applying the procedure of Lemma 3, we get the following SCD for $\bar{U}(1,1;2)\times U(7,1)$ consisting of the two chains:

$$(0,0)\to(1,0)\to(1,1)\to(1,2)\to(1,3)\to(1,4)\to(1,5)\to(1,6)\to(1,7),$$

and

$$(0,1)\to(0,2)\to(0,3)\to(0,4)\to(0,5)\to(0,6)\to(0,7).$$

Applying σ yields the following SCD for $U(4,3;3,1)$:

$$011\to 111\to 112\to 113\to 114\to 124\to 134\to 234\to 334$$

$$012\to 013\to 023\to 033\to 133\to 233\to 333.$$

(c)U(4,3;2,2)

$U(4,3;2,2) \equiv \bar{U}(0,-1;1) \times U(2,2) = \phi \times U(2,2) \equiv U(2,2)$.

An SCD for U(2,2) can be obtained recursively from the O'Hara construction, or better still, by inspection:

$$00 \to 01 \to 02 \to 12 \to 22,$$

$$11.$$

Applying σ yields the following SCD for U(4,3;2,2):

$$022 \to 122 \to 222 \to 223 \to 224,$$

$$123.$$

Combining (a),(b), and (c) , we get that the O'Hara algorithm produces the following SCD for U(4,3):

$$000 \to 001 \to 002 \to 003 \to 004 \to 014 \to 024 \to 034 \to 044 \to 144 \to 244 \to 344 \to 444$$

$$011 \to 111 \to 112 \to 113 \to 114 \to 124 \to 134 \to 234 \to 334$$

$$012 \to 013 \to 023 \to 033 \to 133 \to 233 \to 333$$

$$022 \to 122 \to 222 \to 223 \to 224$$

$$123$$

9. Prospects

I am sure that O'Hara's breakthrough will lead to further work in this area. It would be nice to find another decomposition of U(b,a) in which the analog of σ would be also order preserving with respect to the natural, Young's lattice, order. It would also be interesting to find an O'Hara-style constructive proof of Stanley's[10] result that the posets M(n) are rank-unimodal. This fact is equivalent to the unimodality of the polynomial $(1+t)(1+t^2)...(1+t^n)$.

More generally, Almkvist[1] conjectured that the polynomials

$$\prod_{v=1}^{n} \frac{1-t^{rv}}{1-t^v}$$

are unimodal when r is even and $r \geq 1$ and when r is odd and $n \geq 11$. Almkvist[1] developed an intersting analytical method that is capable, at least in principle, of proving this conjecture for every *specific* r. Assisted by computer, he proved his conjecture for $3 \leq r \leq 20$ and $r = 100, 101$. The conjecture is still open for general r. This is equivalent to the rank-unimodality of the poset of partitions in which each part can appear at most $r-1$ times, and whose largest parts are $\leq n$. An

O'Hara-style proof would be particularly gratifying since it would demonstrate that combinatorics is also capable of proving *new* results.

REFERENCES

1.Almkvist, Gert, *Proof of a conjecture about unimodal polynomials*, preprint. [Almkvist's address is : PL 500, S24300 Hoor, Sweden].

2.Andrews, George, "The Theory of Partitions", Addison-Wesley, Reading, Mass., 1976.

3.deBruijn,N.,Tenbergen,C. van E ., and Kruyswijk,D., *On the set of divisors of a number*, Nieuw Arch. Wisk.(2)**23** (1952), 191-193.

4.Greene, Curtis, and Kleitman, Daniel, *Proof techniques in the theory of finite sets*, in "Studies in Combinatorics", ed. by G.-C.Rota, Mathematical Association of America,1978, 22-79.

5.Lindstrom,B., *A partition of L(3,n) into saturated chains*, Europ. J. Comb. **1** (1980), 61-63.

6.O'Hara, Kathleen M., *Unimodality of Gaussian coefficients: a constructive proof*, research announcement, preprint, University of Iowa.

7.O'Hara, Kathleen M., *Unimodality of Gaussian coefficients: a constructive proof*, preprint, University of Iowa.

8.Proctor, Robert, *Solution of two difficult combinatorial problems with linear algebra*, Amer. Math. Monthly **89** (1982), 721-734.

9.Riess,W., *Zwei Optimierungprobleme auf Ordnungen*, Arbeitsberichte des Instituts fur mathematische Maschinen und Datenverarbeitungen **11** (1978), no. 5, Erlangen.

10.Stanley, Richard P., *Weyl groups, the hard Lefschetz theorem, and the Sperner property*, SIAM J. Algebraic and Discrete Methods, **1** (1980), 164-184.

11.Stanton, Dennis, *Unimodality and Young's lattice*, preprint, University of Minnesota.

12.Stanton, Dennis, and White, Dennis, "Constructive Combinatorics", Springer-Verlag, New York, 1986.

13.Sylvester, James J., *Proof of the hitherto undemonstrated fundamental theorem of invariants*, "Collected Math. Papers", vol. 3, Chelsea, New York, 1973, 117-126.

14.West, Dougless B., *A symmetric chain decomposition of L(4,n)*, Europ. J. Comb. **1** (1980), 379-383.

15.White, Dennis E., *Monotonicity and unimodality of the pattern inventory*, Advances in Math. **38** (1980), 101-108.

January 1988.