

* This research was supported in part by the Air Force Office of Scientific Research under Contract AFOSR-68-1415.

A q -ANALOG OF THE PARTITION LATTICE

by

T. A. Dowling
Department of Statistics
University of North Carolina at Chapel Hill
Institute of Statistics Mimeo Series No. 779

November, 1971

A q -ANALOG OF THE PARTITION LATTICE

T. A. Dowling
University of North Carolina at Chapel Hill

1. INTRODUCTION

The set of all partitions of a finite set, when ordered by refinement, is a well-known geometric lattice enjoying a number of structural properties. Every upper interval of a partition lattice is a partition lattice, and every interval is a direct product of partition lattices. The partitions with a single non-trivial block form a Boolean sublattice of modular elements, and the Whitney numbers are the familiar Stirling numbers. Because of these and other structural properties, the partition lattices occupy a middle ground between the highly structured modular geometric lattices (projective geometries), and arbitrary geometric lattices (combinatorial geometries), exhibiting some of the consequences of the departure from modularity while still retaining enough of the structure to facilitate their study.

We describe in this article for any prime power q a class of geometric lattices, here called q -partition lattices, which share a number of the properties of partition lattices. There is a natural order- and rank- preserving map from the q -partition lattice to the partition lattice of the same rank, which reduces to an isomorphism when $q = 2$. We examine the interval structure of the q -partition lattice and obtain a representation of it as the lattice

* *The research reported here was partially supported by the Air Force Office of Scientific Research under Contract AFOSR-68-1415.*

of a subgeometry of a projective geometry over the q -element field. The characteristic polynomial and Möbius function are obtained, and a Stirling-like identity and recursion derived for the Whitney numbers of the q -partition lattice. We conclude with an application to the enumeration of factorial designs using the geometrical formulation of the design problem developed by Professor Bose in his classical 1947 paper [1].

2. PRELIMINARIES

We summarize in this section a number of results and definitions needed later [4,7].

An (partially) *ordered set* (P, \leq) is a set P together with a reflexive, anti-symmetric, transitive relation on P , written $x \leq y$. When the order relation is implicit, we write simply P for (P, \leq) . An ordered set (P, \leq) is *finite* if P is a finite set. All ordered sets considered here are finite. The *direct product* of two ordered sets P, Q is the set $P \times Q$ with order $(u, v) \leq (x, y)$ iff $u \leq x$ in P and $v \leq y$ in Q . An *interval* $[x, y]$ of an ordered set P is the ordered subset $[x, y] = \{z \in P \mid x \leq z \leq y\}$ (with the order relation of P), defined for all $x, y \in P$ such that $x \leq y$. An element y *covers* x in P if $y > x$ and $[x, y]$ consists only of the two elements x, y . A subset $C = \{x_i \mid i \in [0, n]\}$ of P is a *chain* if it is *totally ordered*: $x_0 < x_1 < \dots < x_n$. The *length* of C is n , one less than its cardinality. C is a *maximal chain* in $[x, y]$ iff $x_0 = x$, $x_n = y$, and x_i covers x_{i-1} , $i \in [1, n]$. P satisfies the *chain condition* if all maximal chains in any interval $[x, y]$ are of the same length. If P has a *zero element* 0 ($0 \leq x$ for all $x \in P$), and satisfies the chain condition, the *rank* of an element $x \in P$, denoted $r(x)$, is the length of a maximal chain in $[0, x]$. If P has a unit

element 1 ($1 \geq x$ for all $x \in X$), and satisfies the chain condition, the *corank* of $x \in P$ is the length of a maximal chain in $[x, 1]$.

Let P have a 0 and 1 . An *atom* (*coatom*) is an element covering 0 (covered by 1). P is a *lattice* iff any two elements x, y have a unique minimal upper bound $x \vee y$, called their *join*, and a unique maximal lower bound $x \wedge y$, called their *meet*.

If P, Q are ordered sets, a function $\phi: P \rightarrow Q$ is *order-preserving* iff $x \leq y$ implies $\phi(x) \leq \phi(y)$. If both P, Q satisfy the chain condition, ϕ is *rank-preserving* if $r(\phi(x)) = r(x)$ for all $x \in P$. P and Q are *isomorphic*, written $P \cong Q$, iff there is a bijection $\phi: P \rightarrow Q$ such that ϕ, ϕ^{-1} are both order-preserving. If Q is a lattice and $\phi: P \rightarrow Q$ is an isomorphism of ordered sets, then P is a lattice and $\phi(x \vee y) = \phi(x) \vee \phi(y)$, $\phi(x \wedge y) = \phi(x) \wedge \phi(y)$, i.e. ϕ is a *lattice isomorphism*. An *anti-isomorphism* of two ordered sets P, Q is a bijection $\phi: P \rightarrow Q$ such that both ϕ, ϕ^{-1} are *order-inverting*.

A (finite) lattice L is *geometric* when y covers x iff $y = x \vee p$ for some atom p of L . A geometric lattice satisfies the chain condition, and its rank function satisfies the semimodular inequality: $r(x \vee y) + r(x \wedge y) = r(x) + r(y)$. Elements of rank $1, 2, r(1)-2, r(1)-1$, are called *points, lines, colines, copoints*, respectively.

A (finite) *combinatorial geometry* $G = G(S)$ is a finite set S together with a closure operator $A \mapsto \bar{A}$ on S satisfying the *exchange property*: $a \in \overline{A \cup b}$, $a \notin \bar{A}$ implies $b \in \overline{A \cup a}$, and such that the empty set and all elements of S , called *points*, are closed. An *independent set* is a set $B \subseteq S$ such that $\overline{B-b} \neq \bar{B}$ for all $b \in B$. All maximal independent subsets of any set $A \subseteq S$, called *bases* of A , have the same cardinality, called the *rank* of A . A basis of G is a basis of S , and the rank of G is the rank of S . A

subgeometry H of G is a subset T of S with closure operator $A \mapsto \bar{A} \cap T$.

A set $A \subseteq T$ is independent in H iff it is independent in G .

If $G(S)$ is a combinatorial geometry, the set of closed sets of G , ordered by inclusion, is a geometric lattice $L(G)$ whose points are the elements of S .

Conversely, every geometric lattice L defines a combinatorial geometry $G(S)$ on its set S of points by $A \rightarrow \bar{A} = \{p \in S \mid p \leq \bigvee_{a_i \in A} a_i\}$. If $H = H(T)$ is a subgeometry of $G = G(S)$, the lattice $L(H)$ consists of all elements $x \in L(G)$ such that $x = \bigvee_{a_i \in A} a_i$ for some subset $A \subseteq T$.

3. THE LATTICE OF PARTITIONS

A *partition* of a finite set X with n elements is a set $\pi = \{X_i \mid i \in [1, k]\}$ of disjoint, nonempty subsets of X , such that $X = \bigcup_{i=1}^k X_i$. The subsets X_i are the *blocks* of π . There is an obvious correspondence between partitions of X and equivalence relations defined on X , wherein the blocks of the partition are the equivalence classes.

The set Π_n of all partitions of X may be ordered by *refinement*: $\pi \leq \sigma$ iff each σ -block is a union of π -blocks. With this order, Π_n is a lattice, with zero element the partition consisting of n singleton blocks, corresponding to the identity relation on X , and unit element the partition 1 consisting of the single block X , corresponding to the universal relation on X .

The join and meet in Π_n of two partitions $\pi = \{X_i \mid i \in [1, k]\}$, $\tau = \{Y_j \mid j \in [1, \ell]\}$ may be easily found from the *intersection graph* $I(\pi, \sigma)$, a bipartite graph with vertices X_i, Y_j ($i \in [1, k], j \in [1, \ell]$) and edges $X_i Y_j$ iff $X_i \cap Y_j$ is nonempty. A block of $\pi \wedge \sigma$ is an intersection $X_i \cap Y_j$, for each

edge $X_i Y_j$, and a block of $\pi \vee \sigma$ is a union $\cup X_i$ over all X_i in a connected component of $I(\pi, \sigma)$.

The partition lattice is a geometric lattice, with rank function $r(\pi) = n - k(\pi)$, where $k(\pi)$ is the number of blocks of π .

4. THE q -PARTITION LATTICE Q_n

Let $IP_{n-1}(F)$ be a projective geometry of dimension $n-1$ over a finite field $F = GF(q)$, and let S be the set of points of IP_{n-1} . Given any independent set B in S , we may associate with each point $a \in \bar{B}$, the subspace spanned by B , a unique subset $B(a)$ of B , defined by

$$B(a) = \{b \in B \mid a \in \overline{B - b}\}.$$

$B(a)$ is the minimal subset of B whose closure contains a . We call $B(a)$ the B -support of a , $a \in \bar{B}$.

Let IP_{n-1} be coordinatized over F , i.e. each point $a \in S$ is represented by a non-zero list $\underline{a} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in F^n$ so that a subset $B = \{b_i \mid i \in [1, k]\}$ of S is independent iff the corresponding set $\{\underline{b}_i \mid i \in [1, k]\}$ of coordinate lists is linearly independent in F^n . We follow the usual convention of associating with every point $a \in S$ the set of all non-zero scalar multiples of its coordinate list. Thus every list $\underline{a} \in F^n - \{0\}$ represents a point of S , with two lists representing the same point iff they are scalar multiplier of each other

Then if $B = \{b_i \mid i \in [1, k]\}$ is an independent set, with $\{\underline{b}_i \mid i \in [1, k]\}$ a set of coordinate lists of the b_i , \bar{B} is the set of all points $a \in S$ such that for some $\lambda_i \in S$, $i \in [1, k]$, $\underline{a} = \sum_{i=1}^k \lambda_i \underline{b}_i$, where \underline{a} is a coordinate list of a . We shall find it convenient to denote this relationship by writing

$a = \sum_{i=1}^k \lambda_i b_i$, with the understanding implicit in all such expressions that a set of coordinate lists of the b_i is fixed, so that the λ_i are uniquely determined up to a constant scalar multiple. Thus $a = \sum_{i=1}^k \lambda_i b_i$, $a' = \sum_{i=1}^k \lambda'_i b_i$ implies $a = a'$ iff there is a $\kappa \in F^* = F-0$ such that $\lambda'_i = \kappa \lambda_i$ for all $i \in [1, k]$. In particular, $a = \kappa a$, $\kappa \in F^*$. Then $a = \sum_{i=1}^k \lambda_i b_i$ is a point of \bar{B} , and $B(a) = \{b_i \in B \mid \lambda_i \neq 0\}$. We shall frequently find it convenient to write the expression $\sum_{i=1}^k \lambda_i b_i$ as $\sum \lambda_i b_i$ ($b_i \in B(a)$) so that all the coefficients λ_i are non zero. More generally, if B_1 is a nonempty subset of $B(a)$, then $\sum \lambda_i b_i$ ($b_i \in B_1$) is the point $\sum \kappa_i b_i$, where $\kappa_i = \lambda_i$, $b_i \in B_1$, and $\kappa_i = 0$, $b_i \notin B_1$.

Let $X = \{x_i \mid i \in [1, n]\}$ be a basis of \mathbb{P}_{n-1} . We define a *q-partition* of X (briefly, a *q-partition*) as a set A of points for which the X -supports $X(a)$, $a \in A$, are disjoint sets. Thus if $A = \{a_i \mid i \in [1, k]\}$ is a *q-partition* of X , and $\underline{\alpha}_i$ is a coordinate list of a_i , then no two $\underline{\alpha}_i$ have non zero elements in the same position. Equivalently, the matrix with rows $\underline{\alpha}_i$ is a $k \times n$ *column-monomial matrix* over F , with no zero rows. Two $k \times n$ column-monomial matrices represent the same *q-partition* A iff one is obtainable from the other by a permutation of rows and multiplication of rows by non zero scalars, i.e. by premultiplication by a $k \times k$ *monomial* matrix.

It is clear that every *q-partition* A of X is an independent set, and that any subset of a *q-partition* is one also. In particular, X is a *q-partition*, as is the empty set. We denote by Q_n the set of all *q-partitions* of X . For $A \in Q_n$, let $k(A)$ be the cardinality of A , and let

$$(1) \quad X(A) = \bigcup_{a \in A} X(a), \quad X_0(A) = X - X(A).$$

Then $\{X(a) \mid a \in A\}$ is a partition of $X(A)$ into $k(A)$ blocks. However, $X_0(A)$ may be empty. We may remedy this by adjoining to $X_0(A)$ the empty

subspace z (or any element not in x). Then $A \in Q_n$ yields a partition

$$(2) \quad \pi(A) = \{X(a) \mid a \in A\} \cup \{X_0(A) \cup z\}$$

of $X \cup z$ into $k(A)+1$ blocks.

Proposition 1. Let $\sigma: Q_n \rightarrow L_n$ be the map $A \mapsto \bigvee_{a_i \in A} a_i$ from the set of q -partitions of X to the lattice of subspaces of \mathbb{P}_{n-1} . Then the relation

$$(3) \quad A \geq B \text{ iff } \sigma(A) \leq \sigma(B)$$

defines an order on Q_n . So ordered, Q_n satisfies the chain condition with rank function $r(A) = n - k(A)$. The map $\pi: Q_n \rightarrow \Pi_{n+1}$, defined by (2), is surjective and preserves order and rank. If $q = 2$, π is an isomorphism.

Proof: Suppose $\sigma(A) \leq \sigma(B)$. Then $A \subseteq \bar{B}$, so every $a \in A$ can be written $a = \sum \lambda_i b_i$ ($b_i \in B(a)$), hence $X(a) = \bigcup X(b_i)$ ($b_i \in B(a)$). The remaining block $X_0(A) \cup z$ of $\pi(A)$ must then be the union of $X_0(B) \cup z$ and the blocks $X(b_i)$ contained in no $X(a)$. Thus $\pi(B) \leq \pi(A)$, so $\sigma(A) = \sigma(B)$ implies $\pi(A) = \pi(B)$, and each $B(a)$ is a singleton, i.e. $A = B$. σ is therefore injective, so the relation defined by (3) is anti-symmetric, hence an order on Q_n . It is evident from the above that $A > B$ in Q_n iff A can be obtained from B by a sequence of single point deletions and/or replacement of two points b'_i, b'_j of B ($B \leq B' < A$) by a third point $b'_i + \lambda b'_j$ on the line joining b'_i and b'_j . Each such operation decreases cardinality by one, so the length of all maximal chains in $[B, A]$ is $k(B) - k(A)$. Thus Q_n satisfies the chain condition and has rank function $r(A) = k(X) - k(A) = n - k(A)$. Since $\pi(A)$ has $k(A)+1$ blocks, the rank of $\pi(A)$ is $(n+1) - (k(A)+1) = n - k(A)$, so π preserves rank. Given any partition $\tau = \{X_0 \cup z, X_1, \dots, X_k\}$ of $X \cup z$, let $a_i = \sum x_j$ ($x_j \in X_i$), for each $i \in [1, k]$. Then $\pi(A) = \tau$, where $A = \{a_i \mid i \in [1, k]\}$, so π is surjective. If $q = 2$, A is the only preimage

of τ , hence π is a bijection. Clearly π^{-1} is order-preserving.

□

Remark: One could define a G -partition of a basis X of a combinatorial geometry G in the analogous way. It can be shown that σ is injective, so (3) defines an order, while the chain condition holds iff G has no trivial lines.

Corollary 1. A covers B in Q_n iff

$$A = B - b_i$$

or

$$A = B - \{b_i, b_j\} \cup \{b_i + \lambda b_j\}$$

for some $b_i, b_j \in B$, $\lambda \in F^*$.

Corollary 2. Each element of rank $n-k$ in Q_n is covered by

$$\binom{k}{1} + (q-1)\binom{k}{2}$$

elements of rank $n-k+1$.

Remark: The partial order defined by (3) can easily be described in terms of representative matrices of q -partitions. If M_A, M_B are representative matrices of A, B , respectively, then $A \geq B$ iff there is a $k(B) \times k(A)$ column-monomial matrix P such that $M_A = PM_B$. An equivalent definition, independent of dimension, can be obtained by adding $n-k(A)$ zero rows in arbitrary positions to any representative matrix of each element $A \in Q_n$. The $n \times n$ column-monomial matrices over F form a semigroup S_n under multiplication, containing as a maximal subgroup the group M_n of monomial matrices. Then $A \geq B$ iff there is a $P \in S_n$ such that $N_A = PN_B$, i.e. iff $N_A \in S_n N_B$, so $A \geq B$ if $S_n N_A \subseteq S_n N_B$. Two matrices $N_1, N_2 \in S_n$ generate the same

principal left ideal of S_n iff there is an $M \in M_n$ such that $N_1 = MN_2$. But this is precisely the requirement that N_1, N_2 represent the same q -partition, so Q_n is *anti-isomorphic* to the set of principal left ideals of S_n , ordered by inclusion.

Our next two propositions concern the interval structure of Q_n .

Proposition 2. If $B \in Q_n$ is of cardinality k , then $[B, 1] \cong Q_k$.

Proof: In Q_n , $A \geq B$ iff $A \subseteq \bar{B}$. But $A \in Q_n$, $A \subseteq \bar{B}$ imply the subsets $B(a)$, $a \in A$, are disjoint, so A is a q -partition of B . Conversely, every q -partition of B is a q -partition of X in $[B, 1]$. The closure in \bar{B} is that of \mathbb{P}_{n-1} , so this correspondence preserves order, and the subgeometry on \bar{B} is isomorphic to \mathbb{P}_{k-1} . □

Proposition 3. Let $A = \{a_\ell \mid \ell \in [1, k]\} \in Q_n$, and let $|X_0(A)| = n_0$, $|X(a_\ell)| = n_\ell$, $\ell \in [1, k]$. Then

$$[0, A] \cong Q_{n_0} \times \Pi_{n_1} \times \Pi_{n_2} \times \dots \times \Pi_{n_k}.$$

Proof: Let $X_0 = X_0(A)$, $X_\ell = X(a_\ell)$, $\ell \in [1, k]$. Suppose $a_\ell = \sum_{x_1 \in X_\ell} \kappa_1 x_1$. Then $B \leq A$ iff $\pi(B) \leq \pi(A)$ and $a_\ell \in \bar{B}_\ell$ for all $\ell \in [1, k]$, where $B_\ell = \{b \in B \mid X(b) \subseteq X_\ell\}$. But given only the $\pi(B)$ -blocks not in $X_0 \cup Z$, the subsets B_ℓ , $\ell \in [1, k]$, are uniquely determined by the a_ℓ . Namely, if $X_{\ell m}$ are the $\pi(B)$ -blocks contained in X_ℓ , then $b_{\ell m} = \sum_{x_1 \in X_{\ell m}} \kappa_1 x_1$ ($x_1 \in X_{\ell m}$). To the set $\cup B_\ell$ ($\ell \in [1, k]$), as determined by the blocks of $\pi(B)$ not in $X_0 \cup Z$, an arbitrary q -partition B_0 of X_0 can be added to obtain a $B \in [0, A]$. The order in $[0, A]$ is clearly the product of the orders in the blocks X_ℓ , $\ell \in [1, k]$, and the set X_0 . It is evident from the above that the order in X_ℓ is that of Π_{n_ℓ} , while that of X_0 is Q_{n_0} . □

Corollary 1. Let $B \leq A$ in Q_n , where $A = \{a_\ell | \ell \in [1, k]\}$. Let $|B_0(A)| = m_0$, $|B(a_\ell)| = m_\ell$, $\ell \in [1, k]$. Then

$$[B, A] \simeq Q_{m_0} \times \Pi_{m_1} \times \Pi_{m_2} \times \dots \times \Pi_{m_k}.$$

Corollary 2. If $a_\ell = \sum \kappa_i x_i$ ($x_i \in X_\ell$), $A = \{a_\ell | \ell \in [1, k]\}$, the atoms of $[0, A]$ are

$$X - \{x_i, x_j\} \cup \{\kappa_i x_i + \kappa_j x_j\}.$$

for all $x_i, x_j \in X_\ell$, $\ell \in [1, k]$, and

$$X - x_i, \quad X - \{x_i, x_j\} \cup \{x_i + \lambda x_j\},$$

for all $x_i, x_j \in X_0$, $\lambda \in F^*$.

Corollary 3. Let $A = \{a\}$ be a copoint of Q_n . If $X(a) = X$, $[0, A] \simeq \Pi_n$, while if $X(a) = \{x_i\}$, $[0, A] \simeq Q_{n-1}$.

We prove in §5 that Q_n is isomorphic to the lattice of a subgeometry of \mathbb{P}_{n-1} . The next proposition (and its corollary) is not required for that proof, but we include it to describe the nature of joins and meets in Q_n .

Proposition 4. Q_n is a lattice.

Proof. Let $A, B \in Q_n$. Since π preserves order, $\pi(C) \geq \pi(A) \vee \pi(B)$ and $\pi(D) \leq \pi(A) \wedge \pi(B)$ for any upper bound C and lower bound D of $A, B \in Q_n$. Let $\pi(A) \vee \pi(B) = \{X_\ell | \ell \in [1, m]\} \cup \{X_0 \cup z\}$. Suppose $\{X_\ell | \ell \in [1, p]\}$ where $p \leq m$, are the blocks of $\pi(A) \vee \pi(B)$ for which there exists a point $c_\ell \in \bar{A}_\ell \cap \bar{B}_\ell$ with X -support X_ℓ , where A_ℓ, B_ℓ are the subsets of A, B , respectively, with $X(A_\ell) = X_\ell$, $X(B_\ell) = X_\ell$. Then clearly $C = \{c_\ell | \ell \in [1, p]\}$ is a minimal upper bound of A, B in Q_n . To show that $A \vee B$ exists, we must prove that the c_ℓ are uniquely defined. For a fixed $\ell \in [1, p]$, let $A_\ell = \{a_i | i \in [1, r]\}$,

$B_\ell = \{b_j | j \in [1, s]\}$. Suppose there are two points c_ℓ, c'_ℓ in $\bar{A}_\ell \cap \bar{B}_\ell$ with X-support X_ℓ . Then

$$\begin{aligned} c_\ell &= \sum_{i=1}^r \kappa_i a_i = \sum_{j=1}^s \lambda_j b_j, \\ c'_\ell &= \sum_{i=1}^r \kappa'_i a_i = \sum_{j=1}^s \lambda'_j b_j, \end{aligned}$$

say, where all coefficients are non-zero. Let $a_i = \sum \alpha_{iu} x_u$, $b_j = \sum \beta_{jv} x_v$. If $x \in X_\ell$, say $x = x_t$, and x_t is contained in the X-supports of $a_i \in A_\ell$, $b_j \in B_\ell$, then the coefficient of x_t in c_ℓ, c'_ℓ is

$$\kappa_i \alpha_{it} = \lambda_j \beta_{jt}, \quad \kappa'_i \alpha_{it} = \lambda'_j \beta_{jt}$$

respectively. Thus $\kappa_i / \lambda_j = \kappa'_i / \lambda'_j$, so $\kappa'_i / \kappa_i = \lambda'_j / \lambda_j$ whenever $X(a_i) \cap X(b_j)$ is nonempty. Since x_ℓ is a block of $\pi(A) \vee \pi(B)$, the intersection graph of the $X(a_i)$, $i \in [1, r]$, and the $X(b_j)$, $j \in [1, s]$ is connected. Thus all the ratios κ'_i / κ_i , λ'_j / λ_j are equal, so $c_\ell = c'_\ell$ and $A \vee B = C$.

The blocks of $\pi(A) \wedge \pi(B)$ are the nonempty intersections of the blocks of $\pi(A)$ with the blocks of $\pi(B)$. Let $a = \sum \kappa_i x_i$ ($x_i \in X(a)$), $b = \sum \lambda_j x_j$ ($x_j \in X(b)$) be arbitrary points of A, B respectively, and let Y_ℓ be a block of $\pi(A) \wedge \pi(B)$ such that $z \in Y_\ell$. We define a q-partition D of X as follows. If $Y_\ell = X_0(A) \cap X(b)$, let D contain the point $\sum \lambda_j x_j$ ($x_j \in Y_\ell$), while if $Y_\ell = X(a) \cap X_0(B)$, let D contain the point $\sum \kappa_i x_i$ ($x_i \in Y_\ell$). Finally, if $Y_\ell = X(a) \cap X(b)$, then partition Y_ℓ into the blocks $Y_{\ell m}$ defined by the equivalence relation $E: x_i E x_j$ iff $\lambda_i / \kappa_i = \lambda_j / \kappa_j$. For each $Y_{\ell m}$ let D contain the point $\sum \lambda_i x_i$ ($x_i \in Y_{\ell m}$). It is clear (see the proof of Proposition 3) that D is the unique maximal upper bound of A, B in Q_n , i.e. $D = A \wedge B$.

□

Corollary. Q_n is a geometric lattice.

Proof: By Corollary 1 of Proposition 1, A covers B iff $A = B - b_r$, or $A = B - \{b_r, b_s\} \cup \{b_r + \lambda b_s\}$. In the first case, $A = BV(X - x_1)$ for any $x_1 \in X(b_r)$, while in the second case $A = BV(X - \{x_1, x_j\} \cup \{x_1 + \lambda x_j\})$ for any $x_1 \in X(b_r)$, $x_j \in X(b_s)$.

□

5. REPRESENTATION OF Q_n

In the lattice L_n of subspaces of \mathbb{P}_{n-1} , let $X^* = \{x^*_i \mid i \in [1, n]\}$ be the set of copoints defined by $x^*_i = \bigvee x_j$ ($x_j \in X - x_i$). X^* is the dual basis of X ; every copoint $c \in L$ may be written as $c = \sum \kappa_i x^*_i$ such that $a = \sum \lambda_i x_i$ is a point, then $a \leq c$ iff $\sum \kappa_i \lambda_i = 0$. The dual of a point $a = \sum \kappa_i x_i$ is the copoint $a^* = \sum \kappa_i x^*_i$, and the dual of a copoint $c = \sum \lambda_i x^*_i$ is the point $c^* = \sum \lambda_i x_i$. The pair of bijections $a \mapsto a^*$, $c \mapsto c^*$ extend to an antiisomorphism $*$: $L_n \rightarrow L_n$;

$$(\bigwedge a_i)^* = \bigwedge a_i^*, \quad (\bigwedge c_i)^* = \bigvee c_i^*.$$

Recall the injection $\sigma: Q_n \rightarrow L_n$ defined by $\sigma(A) = \bigvee a_i$ ($a_i \in A$). The elements of Q_n are independent sets, so

$$r_L(\sigma(A)) = k(A) = n - r_Q(A).$$

Since $A \geq B$ in Q_n iff $\sigma(A) \leq \sigma(B)$, the image of Q_n under σ is antiisomorphic to Q_n . Thus the image R_n of the composite map $\sigma^* = * \circ \sigma: Q_n \rightarrow L_n$ is isomorphic to Q_n . Further,

$$r_L(\sigma^*(A)) = n - r_L(\sigma(A)) = r_Q(A),$$

so the rank of an element in R_n is its rank in L_n . We now prove that R_n is the lattice of a subgeometry of \mathbb{P}_{n-1} .

Proposition 5. Q_n is a geometric lattice, isomorphic to its image R_n under the map $\sigma^*: Q_n \rightarrow L_n$. R_n is the lattice of the subgeometry of \mathbb{P}_{n-1} on the point set

$$S_2 = \{a \in S \mid |X(a)| \leq 2\},$$

consisting of X and all points $x_i + \lambda x_j$ on the lines joining two points of X .

Proof: We have only to show that S_2 is the σ^* -image of the atoms of Q_n , and that a subspace U is in R_n iff it contains a basis in S_2 .

The σ^* -image of $A = \{a_\ell \mid \ell \in [1, k]\} \in Q_n$ is $\bigvee b_r$ ($r \in [1, n-k]$) where $\{b_r \mid r \in [1, n-k]\}$ is any independent set such that $b_r \leq a^*_\ell$ for all $r \in [1, n-k]$, $\ell \in [1, k]$. Consider now the image of the atoms of Q_n . The dual of x_1 is x^*_1 and that of $x_i + \lambda x_j$ is $x^*_i + \lambda x^*_j$. A point $a = \bigvee \kappa_\ell x_\ell$ is the σ^* -image of $X - x_i$ iff $\kappa_\ell = 0$ for all $\ell \neq i$. Thus

$$(4) \quad \sigma^*(X - x_i) = x_i.$$

The point $a = \bigvee \kappa_\ell x_\ell$ is the σ^* -image of $X - \{x_i, x_j\} \cup \{x_i + \lambda x_j\}$ iff $\kappa_\ell = 0$ for all $\ell \neq i, j$, and $\kappa_i + \lambda \kappa_j = 0$. Hence

$$(5) \quad \sigma^*(X - \{x_i, x_j\} \cup \{x_i + \lambda x_j\}) = x_i - \lambda^{-1} x_j,$$

so S_2 is the set of points of P_n .

Let $A = \{a_\ell \mid \ell \in [1, k]\} \in Q_n$, where $a_\ell = \bigvee \kappa_i x_i$ ($x_i \in X_\ell = X(a_\ell)$). By Corollary 1 of Proposition 3, (4), and (5), the points of $[0, \sigma^*(A)]$ in P_n are

$$(6) \quad \kappa_i^{-1} x_i - \kappa_j^{-1} x_j \quad (x_i, x_j \in X_\ell),$$

$$(7) \quad x_i, \quad x_i + \lambda x_j \quad (x_i, x_j \in X_0 = X_0(A)).$$

Fix a point, say x_ℓ , in X_ℓ , for each $\ell \in [1, k]$, and let

$$T_\ell = \{x_\ell - \kappa_\ell \kappa_i^{-1} x_j \mid x_j \in X_\ell, x_j \neq x_\ell\}.$$

Then $T = T_1 \cup T_2 \cup \dots \cup T_k \cup X_0$ is independent and of cardinality $n-k = r_L(\sigma^*(A))$, so T is a basis of $\sigma^*(A)$ in S_2 .

It remains to show that for every $U \in L_n$, $U \cap S_2$ is of the form given by (6) and (7). Let U be a subspace, and let $X_0 = \{x_i \mid x_i \in U\}$. Then $x_i + \lambda x_j \in U$ for all $\lambda \in F^*$, $x_i, x_j \in X_0$. If $X_0 = X$, $u = 1 = \sigma^*(1)$, so assume $X - X_0$ is nonempty. Let $x_i \in X - X_0$. If $x_i + \lambda x_j \in U$, and $x_j \in X_0$, then $x_i \in U$, so $x_i \in X_0$, a contradiction. Hence every point $x_i + \lambda x_j$ in U has either $x_i, x_j \in X_0$ or $x_i, x_j \in X - X_0$. If $x_i + \lambda x_j, x_i + \kappa x_j \in U$, $\lambda \neq \kappa$, then $x_i, x_j \in U$, so $x_i, x_j \in X_0$. We conclude that for every pair $x_i, x_j \in X - X_0$, there is at most one point $x_i + \lambda x_j$ in U on the line joining x_i and x_j .

Define now a directed graph¹ D with vertex set $X - X_0$ such that for each point $x_i + \lambda x_j$ in U , D has one edge $x_i \xrightarrow{\lambda} x_j$ labelled λ and one edge $x_j \xrightarrow{\lambda^{-1}} x_i$ labelled λ^{-1} . Then any two vertices in D are joined by no edges or exactly two, with opposite orientations, and representing the same point.

Suppose that

$$x_\ell \xrightarrow{\lambda} x_j \xrightarrow{\kappa} x_i$$

is a path of length two in D . Then $(x_\ell + \lambda x_j) - \lambda(x_j + \kappa x_i) = x_\ell - \lambda \kappa x_i \in U$, so there is an edge $x_\ell \xrightarrow{-\kappa \lambda} x_i$ in D . We conclude that every connected component D_ℓ ,

¹ This idea, although similar to our original proof, is suggested in [9].

$\ell \in [1, k]$ say, is a complete graph. Let X_ℓ be the vertex set of D_ℓ . To complete the proof, we need only verify that the points $x_i \in X_\ell$ can be assigned labels $\kappa^{-1}_i \in F^*$ so that $x_i \xrightarrow{\lambda} x_j$ in D_ℓ implies $\lambda = -\kappa_i \kappa^{-1}_j$ (see (6)). Fix a point, say x_ℓ , in X_ℓ , and assign the label 1 to x_ℓ . To each $x_i \in X_\ell - x_\ell$ assign the label, say $-\kappa^{-1}_i$, of the edge $x_\ell \rightarrow x_i$. Then $x_\ell \xrightarrow{-\kappa^{-1}_i} x_i \xrightarrow{\lambda} x_j$ and $x_\ell \xrightarrow{-\kappa^{-1}_j} x_j$ imply $\kappa^{-1}_j = -\kappa^{-1}_i \lambda$, so $\lambda = -\kappa_i \kappa^{-1}_j$, as required. □

Remark: With the exception of Corollary 2 of Proposition 1, the assumed finiteness of F has not been used. Hence all our results to this point hold for an arbitrary field.

6. THE CHARACTERISTIC POLYNOMIAL AND WHITNEY NUMBERS OF Q_n

A *modular* element of a geometric lattice L with rank function r is an element $x \in L$ such that $r(x \vee y) + r(x \wedge y) = r(x) + r(y)$ for all $y \in L$. If x is a modular element, the map $z \mapsto x \vee z$ is an isomorphism $[x \wedge y, y] \simeq [x, x \vee y]$ with inverse $w \mapsto w \wedge y$, for any $y \in L$. Every point of a geometric lattice is a modular element.

Proposition 6. In the geometric lattice Q_n of q -partitions of X , the subset $M = \{A \mid A \subseteq X\}$ is a sublattice anti-isomorphic to the Boolean algebra $B(X)$. Every element of M is modular in Q_n .

Proof. If $A \in M$, $B \in Q_n$, the blocks of $\pi(A) \wedge \pi(B)$ not containing z are

$$(8) \quad \{a_i\}, \quad a_i \in A,$$

$$X(b) \cap (X-A), \quad b \in B, \quad X(b) \not\subseteq A,$$

and the blocks of $\pi(A) \vee \pi(B)$ not containing z are

(9) $X(b), \quad b \in B, \quad X(b) \subseteq A.$

It is clear (see the proof of Proposition 4) that $\pi(A \wedge B) = \pi(A) \wedge \pi(B)$ and $\pi(A) \vee \pi(B) = \pi(A \vee B)$. The total number of blocks in (8) and (9) is $k(A) + k(B)$, so $k(A) + k(B) = k(A \vee B) + k(A \wedge B)$. Thus since $r(C) = n - k(C)$, A is modular. If also $B \in M$, then $X(b) = \{b\}$, so $A \wedge B = A \cup B \in M$, $A \vee B = A \cap B \in M$. Thus M is a sublattice, and $A \mapsto X - A$ is an anti-isomorphism $M \cong B(X)$.

□

The *Möbius function* $\mu: L \times L \rightarrow Z$ of a finite partially ordered set L is defined recursively by $\mu(x, x) = 1$, $\mu(x, y) = 0$ if $x \not\leq y$, and $\mu(x, y) = -\sum_{z: x \leq z < y} \mu(x, z)$ if $x \leq y$ [7]. If L is a geometric lattice of rank n with rank function r , the *characteristic polynomial* of L is

$$p_L(v) = \sum_{x \in L} \mu(0, x) v^{n-r(x)}.$$

The characteristic polynomial extends to geometric lattices the notion of the chromatic polynomial of a graph. In particular, if L is the lattice of contractions [7] of a linear graph G with k components, then the chromatic polynomial of G is $\chi(v) = v^k p(v)$. The partition lattice Π_{n+1} is the lattice of contractions of the complete graph K_{n+1} with chromatic polynomial $v(v-1)\dots(v-n)$, so the characteristic polynomial of Π_{n+1} is $(v-1)(v-2)\dots(v-n) = (v-1)_{(n)}$. We may obtain the characteristic polynomial $p_n(v)$ of Q_n with the aid of the following special case of a theorem of Crapo ([3], Th.6, Cor.5): If L is a finite geometric lattice of rank n and c is a copoint of L , then

$$(10) \quad v p_{[0, c]}(v) = \sum_{x: x \wedge c = 0} p_{[x, 1]}(v),$$

where $p_{[a, b]}(v)$ is the characteristic polynomial of the interval $[a, b]$ of L .

Proposition 7. The characteristic polynomial of Q_n is

$$(11) p_n(v) = \prod_{i=0}^{n-1} (v-1-(q-1)i) = (q-1)^n \binom{v-1}{q-1} (n).$$

Proof: We take as our c in (10) the copoint $C = \{x_1\}$ of Q_n . By Corollary 2, Proposition 3, $[0, C] \cong Q_{n-1}$. Since C is modular, $B \wedge C = 0$ iff $B = 0$ (i.e. $B = X$) or B is an atom of Q_n not in $[0, C]$. The number of such atoms is $1+(q-1)(n-1)$. By Proposition 2, $[B, 1] \cong Q_{n-1}$, for every atom $B \in Q_n$. Thus

$$(12) p_n(v) = (v-1-(q-1)(n-1)) p_{n-1}(v).$$

Since $p_1(v) = v-1$, we obtain (11). \square

Remark: Stanley [10,11] has recently investigated the class of geometric lattices containing a maximal chain $0 = x_0 < x_1 < \dots < x_n = 1$ of modular elements. Such lattices, called *supersolvable* lattices, have the property that all zeros of the characteristic polynomial are positive integers, namely,

$$p(v) = (v-\alpha_1)(v-\alpha_2)\dots(v-\alpha_n),$$

where α_i is the number of atoms of $[0, x_i]$ not in $[0, x_{i-1}]$. By Proposition 6, Q_n is supersolvable, with $\alpha_i = 1+(q-1)(i-1)$.

Corollary 1. Let μ be the Mobius function of Q_n , and let $\mu_n = \mu(0,1)$. Then

$$\begin{aligned} \mu_n &= (-1)^n \prod_{i=0}^{n-1} (1+(q-1)i) \\ &= (-(q-1))^n (1/(q-1))^{(n)}, \end{aligned}$$

where $x^{(k)} = x(x+1)\dots(x+k-1)$.

Proof: Set $v = 0$ in (11).

When $q = 2$, $\mu_n = (-1)^n n! = \mu'_{n+1}$ (say), where $\mu'_{n+1} = \mu(0,1)$ for the

partition lattice Π_{n+1} . Since the Mobius function is multiplicative on direct products, we obtain from Corollary 1 of Proposition 3,

Corollary 2. Let $B \leq A$ in Q_n , where $A = \{a_i | i \in [1, k]\}$, $B = \{b_j | j \in [1, m]\}$. Let $m_0 = |B_0(A)|$, $m_i = |B_0(a_i)|$, $i \in [1, k]$. Then

$$\begin{aligned} \mu(B, A) &= \mu_{m_0} \mu'_{m_1} \mu'_{m_2} \dots \mu'_{m_k} \\ &= (-1)^{m-k} (q-1)^{m_0} (1/(q-1))^{(m_0)} \prod_{i=1}^k (m_i-1)!. \end{aligned}$$

The *Whitney numbers* of a finite geometric lattice L of rank n are defined by

$$(13) \quad w(n, k) = \sum_{x: r(x)=n-k} \mu(0, x) \quad (\text{First kind}),$$

the coefficient of v^k in the characteristic polynomial, and

$$(14) \quad W(n, k) = \sum_{x: r(x)=n-k} 1, \quad (\text{Second kind}),$$

the number of elements of corank k . Some classical examples are the following.

If $L = B_n$, the lattice of subsets of an n -set,

$$w(n, k) = (-1)^{n-k} \binom{n}{k}, \quad W(n, k) = \binom{n}{k}.$$

If $L = L(V_n) \cong L(\mathbb{P}_{n-1})$, the lattice of subspaces of a vector (projective) space over $GF(q)$, then

$$w(n, k) = (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{k}_q, \quad W(n, k) = \binom{n}{k}_q,$$

where $\binom{n}{k}_q$ are the Gaussian coefficients [6],

$$(15) \quad \binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}.$$

Finally, if $L = \Pi_{n+1}$, the lattice of partitions of an n -set,

$$w(n,k) = s(n+1,k+1), \quad W(n,k) = S(n+1,k+1),$$

the Stirling numbers of the first and second kind, respectively. All of these, as well as the q -partition lattices Q_n , are classes of lattices which satisfy the hypotheses of the following proposition. Here $\delta(a,b) = 1$ or 0 according as $a = b$ or $a \neq b$.

Proposition 8. Let $\{P_n | n=0,1,\dots\}$ be a class of finite geometric lattices with the property that P_n is of rank n and $[x,1] \cong P_k$ for all $x \in P_n$ of corank k , $k \in [0,n]$, $n \in [0,\infty)$. Let $w(n,k)$, $W(n,k)$ be the Whitney numbers of P_n , $k \in [0,n]$. Then

$$(16) \sum_k W(n,k) w(k,m) = \delta(n,m),$$

and

$$(17) \sum_k w(n,k) W(k,m) = \delta(n,m).$$

The numbers $W(n,k)$, $w(n,k)$ then satisfy the inverse relations

$$(18) a_n = \sum_k W(n,k) b_k, \quad b_n = \sum_k w(n,k) a_k.$$

Proof: We use the identities $\delta(0,y) = \sum_{x \leq y} \mu(x,y) = \sum_{x \leq y} \mu(0,x)$.

Then

$$\begin{aligned} \sum_k W(n,k) w(k,m) &= \sum_{x \in P_n} \sum_{y: y \geq x} \mu(x,y) \delta(m,n-r(y)) \\ &= \sum_{y \in P_n} \delta(m,n-r(y)) \sum_{x: x \leq y} \mu(x,y) \\ &= \sum_{y \in P_n} \delta(m,n-r(y)) \delta(0,y) \\ &= \delta(n,m). \end{aligned}$$

Similarly,

$$\begin{aligned}
\sum_k w(n,k) W(k,m) &= \sum_{x \in P_n} \mu(0,x) \sum_{y: y \geq x} \delta(m, n-r(y)) \\
&= \sum_{y \in P_n} \delta(m, n-r(y)) \sum_{x: x \leq y} \mu(0,x) \\
&= \sum_{y \in P_n} \delta(m, n-r(y)) \delta(0,y) \\
&= \delta(n,m).
\end{aligned}$$

Then if $a_n = \sum_k W(n,k) b_k$,

$$\begin{aligned}
\sum_k w(n,k) a_k &= \sum_k w(n,k) \sum_m W(k,m) b_m \\
&= \sum_m b_m \sum_k w(n,k) W(k,m) \\
&= \sum_m b_m \delta_{nm} \\
&= b_n.
\end{aligned}$$

The converse is proved analogously. □

Corollary. The Whitney numbers $T(n,k)$, $t(n,k)$ of the q -partition lattice Q_n satisfy the inverse relations

$$\begin{aligned}
(q-1)^n \begin{pmatrix} v-1 \\ q-1 \end{pmatrix}_{(n)} &= \sum_k t(n,k) v^k, \\
v^n &= \sum_k T(n,k) (q-1)^k \begin{pmatrix} v-1 \\ q-1 \end{pmatrix}_{(k)}.
\end{aligned}$$

Proof: Set $a_n = v^n$ in (18). Then b_n is the characteristic polynomial (11). □

Note that on setting $q = 2$ and multiplying both equations above by v , we obtain the defining relations of the Stirling numbers.

Proposition 9. The numbers $T(n,k)$, $t(n,k)$ satisfy the recursions

$$(19) T(n,k) = T(n-1,k-1) + (1+(q-1)(k-1)) T(n-1,k)$$

$$(20) t(n,k) = t(n-1,k-1) - (1+(q-1)(n-1)) t(n-1,k).$$

Proof: Every q -partition of X of size k is obtainable either from a unique q -partition of $X-x_n$ of size $k-1$ by adding the point x_n , or from a unique q -partition B of $X-x_n$ of size $k-1$ by replacing some $b_i \in B$ by a point $b_i + \lambda x_n$ ($\lambda \in F^*$), or else is equal to a q -partition of $X-x_n$ of size k . This proves (19), while (20) follows from a comparison of the coefficients of v^k in (12). □

7. AN APPLICATION TO DESIGN

We conclude with an application to a problem of design in statistics. Consider an experiment in which n factors are to be observed, each factor at q levels, where q is a prime power. The q^n different combinations of levels of the factors are to be partitioned into q^{n-r} blocks of size q^r , in such a way that no t -factor or lower interaction is confounded with blocks. As Bose [1,2] has shown, the problem may be represented geometrically by representing the main effects of the n factors by the points of a basis X of \mathbb{P}_{n-1} over $GF(q)$. Each t -factor interaction is then represented by a point of X -weight (cardinality of its X -support) t . The design is specified by the choice of a subspace U of \mathbb{P}_{n-1} of dimension $n-r-1$, in which the points of U represent the interactions confounded with blocks in the design. Thus the design will confound no interactions of t or fewer factors iff U contains no points of

$$S_t = \{a \in S \mid |X(a)| \leq t\}.$$

For given n, t , it is desirable to maximize the dimension $n-r-1$ of U so as to minimize the block size q^r . Bose observed [2] that the problem is equivalent to that of finding an $(n, n-r)$ linear code over $GF(q)$ with minimum distance at least $t+1$.

The problem of determining the maximum k may be considered as a special case of the *critical problem of combinatorial geometry* [4]. It is shown in [4] that the number of lists (C_1, C_2, \dots, C_r) of projective hyperplanes such that no point of a given spanning set T of IP_{n-1} is in every C_i is $(q-1)^{-r} p(q^r)$, where $p(v)$ is the characteristic polynomial of the lattice $L(T)$ of closed sets in the subgeometry of IP_{n-1} on the point set T . This implies in particular that $p(q^r) = 0$ iff $r < c$, where $n-c-1$ is the maximum dimension of a subspace of IP_{n-1} containing no points of T . The integer c is called the critical exponent of T . We show in [5] by an application of Möbius inversion that the number N_{n-r} of $(n-r-1)$ -dimensional projective subspaces not meeting T is then given by

$$(21) \quad \left(\prod_{i=0}^{r-1} (q^r - q^i) \right) N_{n-r} = \sum_{i=0}^r (-1)^i q^{\binom{i}{2}} \binom{r}{i}_q p(q^{r-i}),$$

where $\binom{r}{i}_q$ is the Gaussian coefficient (15). The critical exponent of the set S_2 is well-known to be the smallest r such that $n \leq \binom{r}{1}_q = (q^r - 1)/(q - 1)$. We may, in addition, obtain the numbers N_{n-r} in this case, since $Q_n \cong L(S_2)$. We state this result as

Proposition 10. The number N_{n-r} of (q^n, q^r) factorial designs (i.e. n factors at q levels each, in q^{n-r} blocks of size q^r) such that no main effects or two-factor interactions are confounded is

$$N_{n-r} = \frac{\sum_{i=0}^{r-1} (-1)^i q^{\binom{i}{2}} \binom{r}{i}_q (q-1)^n \binom{q^r-1}{q-1}_{(n)}}{\prod_{i=0}^{r-1} (q^r - q^i)}$$

Note that $N_{n-r} = 0$ iff $n > \frac{q^r-1}{q-1}$. For the critical exponent c , we have the

Corollary. The number of (q^n, q^c) designs with minimum block size q^c , such that no main effects or two factor interactions are confounded, is

$$N_{n-c} = \frac{(q-1)^n \binom{q^c-1}{q-1}_{(n)}}{\prod_{i=0}^{c-1} (q^c - q^i)}$$

REFERENCES

- [1] Bose, R.C., "Mathematical Theory of the Symmetrical Factorial Design." *Sankhyā*, 8 (1947), 107-166.
- [2] Bose, R.C., "On Some Connections between the Design of Experiments and Information Theory." *Bull. Int. Stat. Inst.*, 38 (1961), 257-271.
- [3] Crapo, H., "Möbius Inversion in Lattices." *Arch. der Math.* XIX (1968), 595-607.
- [4] Crapo, H. and G.-C. Rota, *Combinatorial Geometries*, MIT Press, Cambridge, Mass., 1970.
- [5] Dowling, T.A., "Codes, Packings and the Critical Problem," in *Proceedings of the Conference on Combinatorial Geometry and Its Applications* (A. Barlotti, ed.), Perugia, Italy, 1971.
- [6] Goldman, J. and G.-C. Rota, "On the Foundations of Combinatorial Theory IV: Finite Vector Spaces and Eulerian Generating Functions." *Sudt. Appl. Math.* XLIX (1970), 239-258.
- [7] Rota, G.-C., "On the Foundations of Combinatorial Theory I: Theory of Möbius Functions." *Z. Wahrscheinlichkeitstheorie und verw. Gebiete*, 2 (1964), 340-368.

- [8] Rota, G.-C., "The Number of Partitions of a Set," *Am. Math. Monthly* 71 (1964), 498-504.
- [9] Rota, G.-C., P. Doubilet and R. Stanley, "The Idea of Generating Function," (to appear).
- [10] Stanley, R., "Modular Elements in Geometric Lattices," (to appear).
- [11] Stanley, R., "Supersolvable Semimodular Lattices," (to appear).