

Dowling Group Geometries and the Critical Problem

GEOFF WHITTLE

*Mathematics Department, University of Tasmania,
GPO Box 252C, Hobart, Tasmania 7001*

Communicated by W. R. Pulleyblank

Received August 27, 1987

This paper relates the critical problem of Crapo and Rota ["On the Foundations of Combinatorial Theory: Combinatorial Geometries," M.I.T. Press, Cambridge, MA, 1970] to Dowling group geometries. If A is a finite group, $Q_r(A)$ is the rank- r Dowling group geometry over A , and M is a rank- r matroid embeddable as a minor of $Q_r(A)$, then it is shown that the critical exponent of M over A is well defined and is determined by an evaluation of the characteristic polynomial of M . Classes of tangential k -blocks obtained from Dowling group geometries are also displayed. A consequence of the theory is that for the first time all cases of Hadwiger's conjecture can be stated as critical problems. © 1989 Academic Press, Inc.

1. INTRODUCTION

For a finite group A and positive integer r , Dowling [7] (but see also [6, 8]) defines a rank- r geometry associated with A , denoted $Q_r(A)$. The class of such geometries forms the *Dowling group geometries over A* . These geometries are interesting in a number of respects, not least because they have a double aspect. They not only generalise matroids of complete graphs (Dowling constructs them via a generalization of the partition lattice), but they also have many properties in common with projective geometries over finite fields.

Zaslavsky [19–21] highlights the former aspect by showing that minors of Dowling group geometries over A are the matroids of gain graphs with gains in the group A . It should be noted that if A is the trivial group then minors of $Q_r(A)$ are the cycle matroids of graphs while if A is the group of order 2 then minors of $Q_r(A)$ are the matroids of signed graphs.

The latter aspect is dramatically illustrated by Kahn and Kung [9] where it is shown that if \mathcal{C} is a nondegenerate variety of finite combinatorial geometries then \mathcal{C} is either the class of projective geometries over a fixed finite field or the class of Dowling group geometries over a fixed finite group.

(iv) if $r \geq 3$ then $Q_r(A)$ is a representable over a finite field of order q if and only if A is cyclic and m divides $q - 1$.

(v) $Q_r(A)$ has $((m + 1)^r - 1)/m$ hyperplanes.

Proof. Parts (i), (ii), (iii), and (iv) are all proved in [7] while (v) can be shown either from a straightforward induction argument or else from the formula for the Whitney numbers of the second kind of $Q_r(A)$ given in the erratum to [7].

2. THE CRITICAL EXPONENT OF MATROIDS REPRESENTABLE OVER A GROUP

Let M be a matroid and let G be a geometry. Then M is said to be *representable over G* if \bar{M} is isomorphic to a minor of G . If ϕ is such an isomorphism then \bar{M} is said to be *embedded in G* by ϕ . We denote by $\phi(M)$ the image of the ground set of M in the ground set of G under ϕ . For most applications it will be the case that M *spans* G ; that is, \bar{M} is isomorphic to a spanning subgeometry of G . If \mathcal{C} is a class of geometries then we define M to be *representable over \mathcal{C}* if \bar{M} is representable over a member of \mathcal{C} . Of course the above definitions coincide with the usual ones in the case that \mathcal{C} is the class of projective geometries over a finite field.

Let A be a finite group. We say that M is *representable over A* if M is representable over $Q_r(A)$ for some positive integer r .

If M is a rank r matroid representable over A then it is readily seen that M is representable over $Q_r(A)$. That is, if M is representable over A then M can be embedded as a *spanning* subgeometry of a Dowling group geometry over A . If ϕ is such an embedding define $N(M, \phi, A, k)$ to be the number of k -tuples of hyperplanes (H_1, \dots, H_k) of $Q_r(A)$ which distinguish $\phi(M)$. (A k -tuple of hyperplanes is said to *distinguish* a set S if $(\bigcap_{i=1}^k H_i) \cap S = \emptyset$). It is the task of this section to show that $N(M, \phi, A, k)$ is independent of the map ϕ .

It is not hard to show that this is the case if A is cyclic with $O(A) = q - 1$ where q is a prime power. In this case we see by Theorem 1.1(iv) and (v) that $Q_r(A)$ is representable over $GF(q)$ and has $(q^r - 1)/(q - 1)$ hyperplanes. If $Q_r(A)$ is identified with a subgeometry of $PG(r - 1, q)$ then since $PG(r - 1, q)$ also has $(q^r - 1)/(q - 1)$ hyperplanes, the hyperplanes of $Q_r(A)$ and $PG(r - 1, q)$ are in one-to-one correspondence. It follows routinely from this observation that the number of k -tuples of hyperplanes of $Q_r(A)$ which distinguish an embedding of M in $Q_r(A)$ is equal to the number of k -tuples of hyperplanes of $PG(r - 1, q)$ which distinguish the induced embedding of M in $PG(r - 1, q)$. But this number is independent of the embedding.

For an arbitrary finite group our argument must be more subtle since we do not have an ambient projective space in which to embed $Q_r(A)$.

LEMMA 2.1. *Let A be a group of order m and let B be a basis of $Q_r(A)$. Then the number of k -tuples of hyperplanes of $Q_r(A)$ which distinguish the points of B is given by*

$$\frac{1}{m^k} \sum_{j=0}^k (-1)^j \binom{k}{j} ((m+1)^{k-j} - 1)^r.$$

Proof. Let B' be a proper subset of B with $|B'| = k$. A hyperplane H of $Q_r(A)$ contains B' if and only if $H \setminus B'$ is a hyperplane of $Q_r(A)/B'$. But by Theorem 1.1(i), $Q_r(A)/B' \cong Q_{r-k}(A)$ and therefore the number of k -tuples of hyperplanes (H_1, \dots, H_k) of $Q_r(A)$ with the property that $B' \subseteq \bigcap_{i=1}^k H_i$ is equal to the number of k -tuples of hyperplanes of $Q_{r-k}(A)$. But $Q_{r-k}(A)$ has $((m+1)^{r-k} - 1)/m$ hyperplanes and therefore $[((m+1)^{r-k} - 1)/m]^k$ k -tuples of hyperplanes; that is, there are $[((m+1)^{r-k} - 1)/m]^k$ k -tuples of hyperplanes (H_1, \dots, H_k) of $Q_r(A)$ with the property that $\bigcap_{i=1}^k H_i \supseteq B'$.

It then follows from the principle of inclusion-exclusion that the number of k -tuples of hyperplanes of $Q_r(A)$ which distinguish B is equal to

$$\begin{aligned} & \left[\frac{(m+1)^r - 1}{m} \right]^k - \sum_{i=1}^r (-1)^{i+1} \binom{r}{i} \left[\frac{(m+1)^{r-i} - 1}{m} \right]^k \\ &= \sum_{i=0}^r (-1)^i \left[\frac{(m+1)^{r-i} - 1}{m} \right]^k \binom{r}{i}. \end{aligned}$$

Routine manipulation and a change of index of summation shows the above sum to be equal to

$$\frac{1}{m^k} \sum_{j=0}^k (-1)^j \binom{k}{j} ((m+1)^{k-j} - 1)^r.$$

THEOREM 2.2. *Let A be a group of order m and let M be a rank r loopless matroid representable over A . Then the number $N(M, \phi, A, k)$ of k -tuples of hyperplanes of $Q_r(A)$ which distinguish an embedding ϕ of M in $Q_r(A)$ is given by*

$$N(M, \phi, A, k) = \frac{1}{m^k} \sum_{j=0}^k (-1)^j \binom{k}{j} P(M; (m+1)^{k-j}).$$

Proof. Since M is loopless, $P(M; \lambda) = P(\bar{M}; \lambda)$ and we may therefore assume without loss of generality that M is a geometry.

COROLLARY 2.3. *If A is a group of order m and M is a matroid representable over A , then $c(M; A)$ is equal to the least positive integer k for which $P(M; (m+1)^k) > 0$.*

Proof. The result follows immediately if M has a loop so assume that M is loopless. Let $N(M, A, k) = N(M, \phi, A, k)$ where ϕ is an arbitrary embedding of M in $Q_r(A)$. If $c(M; A) = 1$ then $0 < N(M, A, 1) = P(M; m+1)/m$ so $P(M; m+1) > 0$. Assume $c(M; A) = k$ where $k > 1$. Then $N(M, A, 1) = 0$ so $P(M; (m+1)) = 0$ and inductively by Theorem 2.2, $P(M; (m+1)^p) = 0$ for $1 \leq p < k$. Now

$$N(M, A, k) = \frac{1}{m^k} \sum_{j=0}^k (-1)^j \binom{k}{j} P(M; (m+1)^{k-j}) = \frac{1}{m^k} P(M; (m+1)^k).$$

But $N(M, A, k) > 0$ so $P(M; (m+1)^k) > 0$.

A similar routine argument shows that $P(M; (m+1)^k) > 0$ whenever $k > c(M; q)$.

The extent to which the theory of critical exponents over finite groups mimics that of critical exponents over finite fields is remarkable. For example we have, as a routine consequence of Theorem 2.2 and Corollary 2.3,

COROLLARY 2.4. *If the rank r matroid M is representable over the finite group A of order m and $c(M; A) = k$ then the number of sets of k -hyperplanes of $Q_r(A)$ which distinguish an embedding of M in $Q_r(A)$ is equal to $P(M; (m+1)^k)/m^k k!$*

This generalises a result of Brylawski [1, Theorem 9.5].

Other results on critical exponents can be similarly generalised. For example a result of Brylawski [2], namely that loopless principal transversal matroids have critical exponent at most two for any field over which they can be represented, is routinely generalisable. The analogous result for transversal matroids [16] is not quite so routinely generalisable. It would be of considerable interest to know exactly which results on critical exponents over finite fields generalise to critical exponents over groups.

One reason for studying the critical problem is to provide a general setting in which to place graph colouring problems. But a weakness of the traditional approach is that not all graph colouring problems could be stated as critical problems. The five colourable graphs are exactly the graphs whose matroids are affine (that is, have critical exponent one) over $GF(5)$ so the question as to which graphs are five colourable can be stated as a critical problem over a field. Not so the question as to which graphs are six colourable. Noting that $M(K_n)$ is representable over every finite group we can now state all such graph colouring problems as critical problems: a graph is k -colourable if and only if it is affine over every group of order

COROLLARY 3.5. *Let A be a finite cyclic group of order m and let q be a prime power such that m divides $q - 1$. If $r = (q^k - 1)/m + 1$, then $Q_r(A)$ is a tangential k -block over $GF(q)$.*

Consider K_r , the complete graph on r vertices. There are two geometries one can naturally associate with K_r . The first is a geometry on the edges of K_r and is the traditional cycle matroid of K_r , that is, $M(K_r)$. This is isomorphic to the Dilworth truncation of the free matroid F_r on r points. The second corresponds to taking the same Dilworth truncation together with F_r . Here the vertices form a basis of the geometry and the edges of the graph correspond to the intersection of the lines generated by this basis with a hyperplane in general position. The fact that this latter geometry is isomorphic to $M(K_{r+1})$ means that the above distinction is easily overlooked. (For good introductions to Dilworth truncations and their connection with geometries of complete graphs see Brylawski [4], Mason [10], or Crapo and Rota [5, Chap. 7]).

Now when Dowling group geometries are interpreted as geometries of gain graphs they seem to be most naturally interpreted as geometries on the vertices and edges of gain graphs. The subsets S and S' of $Q_r(A)$ correspond, respectively, to the vertices and edges of the associated gain graph. (See Kahn and Kung [9, Sect. 7] for a good explanation of this point). That is, to the extent that Dowling group geometries generalise geometries on graphs, they generalise geometries on the vertices and edges of graphs. How then to generalise the usual geometry on the edges of K_r ? One simply deletes S from the ground set of $Q_r(A)$ and considers $Q_r(A) \setminus S$. Thus motivated we define $Q'_r(A)$ by $Q'_r(A) = Q_r(A) \setminus S$. It turns out that these geometries also provide a rich class of tangential blocks.

LEMMA 3.6. *If the order of A is greater than one and $r > 1$, then $r(Q'_r(A)) = r(Q_r(A))$.*

Proof. By Corollary 2.3, $c(Q_r(A) \setminus S; A) = 1$. That is, there exists a hyperplane H of $Q_r(A)$ missing S . Let $\{i, j\} \subseteq S$. Then since $\{i, j, \alpha_{ij}\}$ is a circuit of $Q_r(A)$ for all $\alpha \in A$ and $O(A) > 1$, $\text{cl}_{Q_r(A)}(\{i, j\}) \setminus \{i, j\}$ contains at least two points. But at most one of these (in fact exactly one) belongs to H and therefore there exists $\alpha \in A$ such that $\alpha_{ij} \notin H$. But $\{H \cup \alpha_{ij}\} \subseteq S'$ and $r(H \cup \alpha_{ij}) = r = r(Q_r(A))$ and the result follows.

LEMMA 3.7. *Let A be a group of order m where $m > 1$. Then if $r > 1$,*

$$P(Q'_r(A); \lambda) = (\lambda - (r - 1)(m - 1)) \sum_{i=1}^{r-1} (\lambda - 1 - (i - 1)m).$$

Proof. Consider $Q_r(A)$. Let $T \subset S$ and $i \in S \setminus T$. We first show that $Q_r(A) \setminus T/i \cong Q_{r-1}(A)$. Each line containing i and another element of S

(say j) contains at least one other point (in fact at least two). These are the points of the form α_{ij} where $\alpha \in A$. Therefore deleting T from $\overline{Q_r(A)}/i$ only deletes single elements from nontrivial parallel classes. That is, $\overline{Q_r(A)}/i \setminus T \cong \overline{Q_r(A)}/i$. But $\overline{Q_r(A)}/i \cong Q_{r-1}(A)$ and $Q_r(A)/i \setminus T = Q_r(A) \setminus T/i$ so $\overline{Q_r(A) \setminus T}/i \cong Q_{r-1}(A)$.

We now show by induction that for $T \subseteq S$,

$$P(Q_r(A) \setminus T; \lambda) = P(Q_r(A); \lambda) + |T| P(Q_{r-1}(A); \lambda).$$

If $|T| = 1$ the equality certainly holds so assume that it holds for all subsets T' of T with $|T'| < |T|$ and let $i \in T$. By Lemma 3.6, i is not a coloop of $Q_r(A) \setminus (T \setminus i)$ so $P(Q_r(A) \setminus T; \lambda) = P(Q_r(A) \setminus (T \setminus i); \lambda) + P(Q_r(A) \setminus (T \setminus i)/i; \lambda)$. But we have shown that $\overline{Q_r(A) \setminus (T \setminus i)}/i \cong Q_{r-1}(A)$ and therefore $P(Q_r(A) \setminus (T \setminus i)/i; \lambda) = P(Q_{r-1}(A); \lambda)$. Combining this observation with the induction assumption we obtain the desired equality. Setting $T = S$ we obtain

$$\begin{aligned} P(Q'_r(A); \lambda) &= P(Q_r(A); \lambda) + rP(Q_{r-1}(A); \lambda) \\ &= \prod_{i=1}^r (\lambda - 1 - (i-1)m) + r \prod_{i=1}^{r-1} (\lambda - 1 - (i-1)m) \\ &= (\lambda - (r-1)(m-1)) \prod_{i=1}^{r-1} (\lambda - 1 - (i-1)m). \end{aligned}$$

THEOREM 3.8. *Let A be a group of order m and let A' be a subgroup of A of order n . If $k \geq 1$ and $r = ((m+1)^k - 1)/n + 2$ then $Q'_r(A')$ is a tangential k -block over A .*

Proof. If $n = 1$ then $Q'_r(A') \cong M(K_{(m+1)^k+1})$ which is a tangential k -block over A by Theorem 3.4 so assume that $n > 1$.

Certainly $Q'_r(A')$ is representable over A and by Lemma 3.7, $P(Q'_r(A'); (m+1)^k) = 0$. It only remains to show that for a proper nonempty flat F of $Q'_r(A')$, $P(Q'_r(A')/F; (m+1)^k) > 0$. We first show that for $x \in S'$, $P(Q'_r(A')/x; (m+1)^k) > 0$.

If $x \in S'$ then $x = \alpha_{ij}$ for $\{i, j\} \subseteq S$. Now $r = (((m+1)^k - 1)/n) + 2$ and $k \geq 1$ so $r \geq 3$ and there exists $k \in S$ with $i \neq k \neq j$. One routinely shows that for such a k , $\{\alpha_{ij}, k\}$ is a rank 2 flat of $Q_r(A')$ and therefore $\{k\}$ is a rank one flat of $Q_r(A')/\alpha_{ij}$. Therefore $\overline{Q_r(A')/\alpha_{ij} \setminus k}$ is a proper loopless minor of $\overline{Q_r(A')/\alpha_{ij}}$. But $\overline{Q_r(A')/\alpha_{ij}} \cong Q_{r-1}(A')$ and by Theorem 3.4, $Q_{r-1}(A')$ is a tangential k -block over A so $P(\overline{Q_r(A')/\alpha_{ij} \setminus k}; (m+1)^k) > 0$. Since $Q'_r(A')/\alpha_{ij} = Q_r(A')/\alpha_{ij} \setminus S$ it follows that $P(Q'_r(A')/\alpha_{ij}; (m+1)^k) > 0$. Now let F be a proper nonempty flat of $Q'_r(A')$. Let $x \in F$. Then since $\overline{Q'_r(A')/x}$ is isomorphic to a proper loopless minor of $Q_{r-1}(A')$ so is $\overline{Q'_r(A')/F}$. Therefore $P(Q'_r(A')/F; (m+1)^k) > 0$ and the result follows.

Again we obtain as an immediate consequence of Theorem 3.8 in the light of Proposition 3.2,

COROLLARY 3.9. *Let A be a finite cyclic group of order m and let q be a prime power such that m divides $q - 1$. If $r = ((q^k - 1)/m) + 2$, then $Q'_r(A)$ is a tangential k -block over $GF(q)$.*

The class of geometries $\{Q'_r(A); r \text{ a positive integer and } A \text{ a finite group}\}$ is unusual in that it forms a large class of geometries whose members all have completely factorisable characteristic polynomials but whose members are nonetheless typically not supersolvable.

THEOREM 3.10. *If $r \geq 3$, $m \geq 2$, and A is a group of order m , then $Q'_r(A)$ has no modular hyperplanes unless both $r = 3$ and $m = 2$.*

Proof. By [7, Theorem 2(b) and Corollary 2.2], a connected hyperplane of $Q_r(A)$ is either isomorphic to $Q_{r-1}(A)$, in which case it contains all but one element of S , or it is isomorphic to $M(K_r)$, in which case it is disjoint from S . It is easily seen that for $r \geq 3$ and $m \geq 2$, the connected hyperplanes of $Q'_r(A)$ are exactly the restrictions of connected hyperplanes of $Q_r(A)$ to S' . One routinely shows that $Q'_r(A)$ is connected and modular hyperplanes of connected geometries are connected so the only candidates for modular hyperplanes of $Q'_r(A)$ are the restrictions of connected hyperplanes of $Q_r(A)$ to S' .

Let H be a connected hyperplane of $Q_r(A)$ isomorphic to $Q_{r-1}(A)$ and let H' be its restriction to S' . Let i be the point of S not on H and let j be an element of S distinct from i . Since $i \notin H$ and $j \in H$, $\{\alpha_{ij}, \alpha \in A\} \cap H = \emptyset$. Since $m \geq 2$, $r(\{\alpha_{ij}, \alpha \in A\}) = 2$ and $\text{cl}_{Q_r(A)}(\{\alpha_{ij}; \alpha \in A\}) \cap H = j$. But $j \notin H'$ so $\text{cl}_{Q'_r(A)}(\{\alpha_{ij}; \alpha \in A\}) \cap H' = \emptyset$. A modular hyperplane must meet every rank 2 flat so H' is therefore not modular in $Q'_r(A)$.

Now assume that $H \cong M(K_r)$ and assume that $r \geq 4$. Since $H \cap S = \emptyset$, H is both a hyperplane of $Q_r(A)$ and of $Q'_r(A)$. Also since $H \cap S = \emptyset$ we see that for distinct points i and j of S , H contains at most (in fact exactly) one point of $\text{cl}_{Q_r(A)}\{i, j\} = \{i, j\} \cup \{\alpha_{ij}; \alpha \in A\}$. Now $m \geq 2$ so there exists $\alpha \in A$ such that $\alpha_{ij} \notin H$. Let h, i, j , and k be distinct points of S and let α_{hi} and β_{jk} be points of S' with $\{\alpha_{hi}, \beta_{jk}\} \cap H = \emptyset$. Then $\{\alpha_{hi}, \beta_{jk}\}$ is a trivial line of $Q_r(A)$ and of $Q'_r(A)$ (no three-point circuit of $Q_r(A)$ contains $\{\alpha_{hi}, \beta_{jk}\}$). So $\text{cl}_{Q'_r(A)}(\{\alpha_{hi}, \beta_{jk}\}) \cap H = \emptyset$ and H is therefore not modular in $Q'_r(A)$.

If $r = 3$, then $H \cong M(K_3)$. Assume that $m > 2$. There exists α and β in A such that $H = \{\alpha_{12}, \beta_{23}, \alpha\beta_{13}\}$. Let $\alpha' \neq \alpha$ and $\beta' \neq \beta$ be elements of A . If $\alpha'\beta' \neq \alpha\beta$ then $\{\alpha'_{12}, \beta'_{23}, \alpha'\beta'_{13}\}$ is a line of $Q'_3(A)$ not meeting H and H is therefore not modular. Assume then that $\alpha'\beta' = \alpha\beta$. Since $m \geq 3$ there exists $\alpha'' \in A$ distinct from α and α' and therefore $\alpha''\beta' \neq \alpha'\beta'$. That is,

$\{\alpha''_{12}, \beta'_{23}, \alpha''\beta'_{13}\}$ is a line of $Q'_3(A)$ not meeting H and again we see that H is not modular.

The exceptional case is $Q'_3(A)$ where $O(A) = 2$. It is straightforward to argue geometrically that $Q'_3(A) \cong M(K_4)$ and therefore does have a modular hyperplane. But perhaps a nicer way to show this is to note that by Theorem 3.8, $Q'_3(A)$ is a rank 3 tangential 1-block over $GF(3)$ and Walton and Welsh [14] show that the only rank 3 tangential 1-block over $GF(3)$ is $M(K_4)$. (See also Zaslavsky [19, Fig. 1].)

In [17] it is shown that the class of tangential k -blocks over $GF(q)$ with modular hyperplanes is tractable and in [18] it is shown that this is an extensive class. Difficulties with the critical problem arise, in part, from the existence of tangential k -blocks without modular hyperplanes. It is an immediate consequence of Theorems 3.8 and 3.10 that there exists a tangential k -block over the finite group A of order $m > 1$ which contains no modular hyperplanes for all positive integers k apart from the case $k = 1$ and $m = 2$. In particular there exist tangential k -blocks over $GF(q)$ which contain no modular hyperplanes whenever q is a prime power greater than 2 except when $k = 1$ and $q = 3$. Using a construction based on $M^*(P_{10})$ (the cocycle matroid of the Petersen graph) it is also possible to show that there exist tangential k -blocks over $GF(2)$ without modular hyperplanes for all $k > 1$. This result will appear elsewhere.

We finish with an example. By Theorem 3.8, if A has order 3 then $Q'_3(A)$ is a tangential 1-block over $GF(4)$. Walton and Welsh [14] mention that $AG(2, 3)$ is a tangential 1-block over $GF(4)$. It is left to the reader to perform the routine verification that $Q'_3(A) \cong AG(2, 3)$.

REFERENCES

1. T. H. BRYLAWSKI, A decomposition for combinatorial geometries, *Trans. Amer. Math. Soc.* **171** (1972), 235–282.
2. T. H. BRYLAWSKI, An affine representation for transversal geometries, *Stud. Appl. Math.* **54** (1975), 143–150.
3. T. H. BRYLAWSKI, Modular constructions for combinatorial geometries, *Trans. Amer. Math. Soc.* **203** (1975), 1–44.
4. T. H. BRYLAWSKI, Coordinatizing the Dilworth truncation, in "Matroid Theory" (L. Lovasz and A. Recski, Eds.), Colloquia Mathematica Societas Janos Bolyai, Vol. 40, North-Holland, Amsterdam, 1985.
5. H. H. CRAPO AND G.-C. ROTA, "On the Foundations of Combinatorial Theory: Combinatorial Geometries," M.I.T. Press, Cambridge, MA, 1970.
6. DOUBILET, G.-C. ROTA, AND R. STANLEY, On the foundations of combinatorial theory (VI): The idea of generating function, in "Proc. Sixth Berkeley Sympos. on Mathematical Statistics and Probability, Berkeley, CA. 1970/1971," Vol. 11, pp. 276–318, Probability Theory, Univ. of California Press, Berkeley, CA, 1972.
7. T. A. DOWLING, A class of geometric lattices based on finite groups, *J. Combin. Theory Ser. B* **14** (1973), 61–86; erratum, *J. Combin. Theory Ser. B* **15** (1973), 211.

