RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

LARRY D. SHATOFF

Binary multiples of combinatorial geometries

Rendiconti del Seminario Matematico della Università di Padova, tome 48 (1972), p. 95-104

<http://www.numdam.org/item?id=RSMUP_1972__48__95_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 48 (1973)

BINARY MULTIPLES OF COMBINATORIAL GEOMETRIES

LARRY D. SHATOFF *)

Introduction.

A *pregeometry* G on a set S is a closure relation $A \to \overline{A}$ on S satisfying the properties:

(i) For any a, $b \in S$ and for any $A \subseteq S$, if $a \in \overline{A \cup b}$ and $a \notin \overline{A}$, then $b \in \overline{A \cup a}$;

(ii) For any $A \subseteq S$ there exists a finite set $B \subseteq A$ such that $\overline{B} = \overline{A}$.

A *combinatorial geometry* (or *geometry*) on the set S is a pregeometry such that

(iii) $\overline{\emptyset} = \emptyset$ and $\overline{a} = a$, any $a \in S$.

A closed sef ot a pregeometry is called a *flat*. This, and all further terminology is that of [1].

Many authors refer to pregeometries as matroids and to combinatorial geometries as simple matroids. If we wish to indicate that S is the underlying set of G we write $G(S)$.

It is known that the flats of a pregeometry, ordered by inclusion, form a geometric lattice with point set $\{\overline{a} : a \in S, \overline{a} \neq \overline{\emptyset}\}$. Conversely, if L is a geometric lattice with S as its point set, the closure relation $\overline{A} = \{a \in S : a \leq \sup A\}$, defines a combinatorial geometry on S. With any pregeometry we therefore canonically associate the combinatorial geometry determined by its lattice of flats. The Pregeometry and its

---

*) Indirizzo dell'A.: Colgate University, Dept. of Math. Hamilton, New York 13346, U.S.A.

associated geometry have isomorphic lattices of closed sets. [See 1, Chapter 2].

Let $G(S)$ be a pregeometry and $B \subseteq S$. The *subgeometry* on B is that geometry determined by the closure relation $C \to \overline{C} \cap B$, $C \subseteq B$.

With any pregeometry $G(S)$ we associate a rank function defined on the power set of S. The rank of $A \subseteq S$, $r(A)$, is one less than the cardinality of a maximal chain from $\overline{\emptyset}$ to $\overline{A}$ in the lattice of flats of G. The rank function is submodular: $r(A \cup B)+r(A \cap B) \leq r(A)+r(B)$, any A, $B \subseteq S$. A flat A *covers* flat B is $r(A)=r(B)+1$. Suppose $r(S)=n$. If A is a flat with $r(A)=1$, 2, $n-1$, or $n-2$, then A is called a *point*, *line*, *copoint*, or *coline*, respectively.

$A \subseteq S$ is *independent* in $G(S)$ if $r(A)=|A|$, the cardinality of A. A set is *dependent* if it is not independent.

Important examples of combinatorial geometries are projective geometries. Given a projective geometry on the set of points S, the lattice of flats (points, lines, etc.) form a geometric lattice, and this defines a combinatorial geometry. We will refer to these combinatorial geometries as *projective geometries*. If a combinatorial geometry is isomorphic to a subgeometry of a projective geometry over the field $GF(2)$, it is called *binary*. Tutte has characterized binary geometries as follows [3, p. 164, (2.6)].

THEOREM 1 (Tutte). $G(S)$ is binary if and only if there are at most three copoints covering any coline in $G(S)$.

Another class of combinatorial geometries comes from Boolean algebras. Let S be a finite set. For every $A \subseteq S$, define $\overline{A}=A$. This closure relation determines a combinatorial geometry in which every set is both closed and independent. The lattice of closed sets of S is simply the Boolean algebra of subset of S, and we will refer to this combinatorial geometry as the *Boolean algebra* on S. An n-set is a set of cardinality n. Let S be an n-set and $2 \leq k \leq n$. If $A \subseteq S$, let $\overline{A}=A$ when $|A| < k$ and $\overline{A}=S$ when $|A| \geq k$. This closure relation defines a combinatorial geometry in which every j-set, $j<k$, is closed. Since the collection of flats of this combinatorial geometry is the same as the collection of flats of rank less than k of the Boolean algebra on S, together with S itself, we call it the *rank k Boolean truncation* on S.

Multiples of Geometries.

A function f defined on the collection of subsets of a set S is *submodular* if it satisfies these conditions:

f is integer valued;

$A \subseteq B$ implies $f(A) \leq f(B)$, any $A, B \subseteq S$;

$f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$, any $A, B \subseteq S$.

THEOREM 2 (Edmonds). If f is a submodular function on a set S, then the subsets $A \subseteq S$ such that $f(A') \geq |A'|$ for all nonempty $A' \subseteq A$ form the independent sets of a pregeometry on S. This pregeometry is a combinatorial geometry if and only if all two-element sets are independent.

This theorem is apparently due to Edmonds. A proof appears in [1, Prop. 7.3].

Suppose k is a positive integer. Since the rank function r of a pregeometry is submodular, we see that the function kr, defined by $(kr)(A) = k \cdot r(A)$ is also submodular. If r is the rank function of pregeometry $G(S)$, we denote by kG or $kG(S)$ the pregeometry determined by the function kr. Note that as long as $\overline{\emptyset} = \emptyset$, kG is a combinatorial geometry for $k \geq 2$. The *sequence of multiples* of G is the sequence of pregeometries (kG), where k takes on positive integer values. Each pregeometry k G is called a multiple of G. $A \subseteq S$ is *k-indipendent* if it is independent in kG. $A \subseteq S$ is *k-closed* if it is closed in kG.

Suppose $G(S)$ is a finite pregeometry. That is, S is finite. Then there exists an integer n such that if $k \geq n$, $kG = nG$. Clearly there exists sufficiently large n such that $nr(A - \overline{\emptyset}) \geq |A - \overline{\emptyset}|$, all $A \subseteq S$. Then every set which is disjoint from $\overline{\emptyset}$ is n-independent (and k-independent for $k \geq n$). Thus the lattice of flats of kG, $k \geq n$ is simply the Boolean algebra of subsets of $S - \emptyset$. The smallest number n such that nG is a Boolean algebra has been investigated in another context by Edmonds, [2].

Let $G(S)$ be a projective geometry. When are the multiples of G binary geometries? We show that kG is binary only when $k = 1$ and G is binary, or when kG is a Boolean truncation of rank one less than the cardinality of S, or when kG is a Boolean algebra. We prove this

result first for projective planes and then use induction for the general case. We will make use of the following well known results on projective geometries.

THEOREM 3. If G is a projective geometry, any two copoints intersect in a coline. For any projective geometry there is an integer $n \geq 2$ such that:

i) every flat of rank q contains exactly $1+n+ \ldots +n^{q-1}$ points;

ii) any coline is covered by exactly $n+1$ copoints;

iii) G has rank q then G has exactly $1+n+ \ldots +n^{q-1}$ copoints.

The number n is the order of G. Notice that the rank of a flat is one more than its dimension in the projective geometry. (Thus a projective plane has rank 3).

THEOREM 4. If G is a projective geometry of order n and rank $q \geq 4$, and if A is a copoint of G, then the subgeometry of G on A is a projective geometry of order n and rank $q-1$.

Binary multiples.

LEMMA 1. If $G(S)$ is the rank n Boolean truncation on S then G is binary if and only if $n=|S|-1$ or $n=|S|$.

PROOF. If G is the rank n Boolean truncation, any $(n-2)$-set is a coline and any $(n-1)$-set is a copoint. Therefore there are $|S|-(n-2)$ copoints covering a given coline. By Theorem 1, G is binary if and only if $|S|-(n-2) \leq 3$. That is, if and only if $n \geq |S|-1$, and so $n=|S|-1$ or $n=|S|$.

LEMMA 2. Let $G(S)$ be a combinatorial geometry of rank q. Suppose $A \subseteq S$ is a $(q+k)$-set, k a positive integer, and every q-subset of A is a basis of G. Then there is coline of G which is covered by at least $k+2$ copoints.

PROOF. Suppose $A=\{a_1, a_2, \ldots, a_{q+k}\}$. Let $B=\overline{\{a_1, a_2, \ldots, a_{q-2}\}}$. B is a coline of G. For every j such that $q-1 \leq j \leq q+k$, let $B_j = \overline{\{a_1, \ldots, a_{q-2}, a_j\}}$. Then $B_{j-1}, \ldots, B_{q+k}$ are distinct copoints covering B.

LEMMA 3. Let $(G(S)$ be a projective geomerty of order n and rank 3. If $k \geq \frac{n+1}{2}$ then kG is a Boolean truncation of rank

$$\min \{3k,\ 1+n+n^2\}.$$

PROOF. Let $A \subseteq S$ be a set such that $|A| = \min \{3k,\ 1+n+n^2\}$. It suffices to show that every such set is a basis for kG. Denote the rank function of G by r. Let $A' \subseteq A$. If $A' = \emptyset$ or if A' is a 1-set, clearly $kr(A') \geq |A'|$. If $2 \leq |A'| \leq n+1$ then $r(A')$ is 2 or 3, and so $kr(A') \geq 2k \geq n+1 \geq |A'|$ by the hypotheses. If

$$n+1 \leq |A'| \leq \min \{3k,\ 1+n+n^2\}$$

then $r(A')=3$, and so $kr(A')=3k \geq |A'|$. Thus every such A is a k-independent set. If $B \subseteq S$ is a $(3k+1)$-set, then since $3k+1 > n+1$ we have $r(B)=3$. Since $kr(B)=3k < |B|$, B is not k-independent. Thus every A with $|A| = \min \{3k,\ 1+n+n^2\}$ is a basis for kG.

THEOREM 5. Let $G(S)$ be a projective plane of order n. kG is binary if and only if $k \geq \frac{n^2+n}{3}$ or both $k=1$ and $n=2$.

PROOF. For $n=2$, 3 and 4, the multiples can be found and the theorem shown to hold.

Now we let $n \geq 5$. Consider two cases, according to the size of k. First let $k \geq \frac{n+1}{2}$. By Lemma 3, kG is a Boolean truncation of rank $\min \{3k,\ 1+n+n^2\}$. Thus by Lemma 1, it is binary if and only if $3k \geq (n^2+n+1)-1$; that is, if and only if $k \geq \frac{n^2+n}{3}$. Next let $1 < k < \frac{n+1}{2}$. If A is a line, $kr(A)=2k<n+1=|A|$. Thus A is not k-independent. If A is any $2k$-set then $r(A)=2$ or 3, and so $kr(A) \geq 2k = |A|$. A is thus k-independent. Suppose A is a $3k$-set no $(2k+1)$-subset of which is contained in a line. Such a set is k-independent; for if $A' \subseteq A$ and $|A'| \leq 2k$ then A' is k-independent, and if $|A'| \geq 2k$ we have $r(A')=3$ by the hypothesis and so $kr(A')=3k \geq |A'|$. Clearly no $(3k+1)$-set can be independent, and so A is a basis for kG. We now construct a set of $3k+2$ elements every $3k$-subset of which is a basis

of kG. By Lemma 2 this will show that there are at least four copoints covering some coline of kG, and so kG is not binary. Let us label the lines of G by L_1, L_2, ..., L_{1+n+n^2}. Construct the set A as follows. Select any $2k$ points from L_1. Select one point, a, from L_2-L_1. Select one point, b, from $L_3-(L_1 \cup L_2)$. If necessary, relabel the remaining lines so that the line determined by a and b is L_{1+n+n^2}. Now select one point from $L_4-(L_1 \cup L_2 \cup L_3 \cup L_{1+n+n^2})$, one point from $L_5-(L_1 \cup L_2 \cup L_3 \cup \cup L_4 \cup L_{1+n+n^2})$, ..., one point from $L_{k+3}-(L_1 \cup \ldots \cup L_{k+2} \cup L_{1+n+n^2})$. Thus $|A|=3k+2$. We must show that there are a sufficient number of lines and points in G to carry out this process. We need $k+4$ lines to construct A. G has $1+n+n^2$ lines. Since $k+4<\frac{n+1}{2}+4\leq 1+n+n^2$ for $n\geq 5$, there are enough lines. Any two lines meet in one point so at the last step we are eliminating $k+3$ points of L_{k+3} from our selection. Any line contains $n+1$ points. Thus we must have $(n+1)-(k+3)\geq 1$. That is, $n-k\geq 3$. But $k<\frac{n+1}{2}$, so $n-k>n-\left(\frac{n+1}{2}\right)=\frac{n}{2}-\frac{1}{2}\geq 2$ for $n\geq 5$. Therefore $n-k\geq 3$. We see then that the process for forming A is valid one. We claim that if B is a $(2k+1)$-subset of A then B is not contained in a line. If we select B so that at least two of its elements are in L_1, then the only line that could possibly contain B is L_1 (otherwise two lines would intersect in more than one point). Since $|L_1 \cap A|<2k+1$, we cannot select B completely from L_1; and so $|B \cap L_1|=0$ or 1. If $|B \cap L_1|=1$, then we must select the remaining $2k$ elements of B from the $k+2$ elements of $A \cap L_1^c$. This is only possible if $k=2$, in which case we select all the elements of $A \cap L_1^c$. But the only line containing a and b is L_{1+n+n^2}, and the element of A selected from L_4 is not in L_{1+n+n^2}. Thus B cannot be contained in a line. If $|B \cap L_1|=0$, then we must select $2k+1$ elements from the $k+2$ elements of $A \cap L_1^c$, clearly impossible. A is therefore a $(3k+2)$-set any $3k$-subset of which is a basis of kG. kG is therefore not binary if $1<k<\frac{n+1}{2}$. This completes the proof.

LEMMA 4. If n and q are integers such that $n\geq 2$ and $q\geq 4$, then unless $n=2$ and $q=4$,

$$n^{q-2}>\frac{n+n^2+\ldots+n^{q-2}}{q-1}+2.$$

If $n \geq 2$ and $q \geq 4$ then

$$n^{q-2} > \frac{1+n+ \ldots +n^{q-3}}{q-1} + 1.$$

If n and m are integers such that $n \geq 2$ and $m \geq 1$ then

$$\frac{1+n+ \ldots +n^m}{m+1} < \frac{n+n^2+ \ldots +n^{m+1}}{m+2}$$

and

$$\frac{1+n+ \ldots +n^m}{m+1} < \frac{1+n+ \ldots +n^{m+1}}{m+2}.$$

The proofs of these inequalities are not difficult.

LEMMA 5. Let $G(S)$ be a pregeometry, $S' \subseteq S$, and G' the subgeometry of G on S'. Then nG' is the same pregeometry as the subgeometry of nG on S', denoted $(nG)'$.

PROOF. Let r be the rank function of G. $A \subseteq S'$ is independent in nG, and thus in $(nG)'$, if and only if $nr(A') \geq |A'|$ for all $A' \subseteq A$. Since r restricted to S' is the rank function of G', this condition holds if and only if A is independent in nG'. Since $(nG)'$ and nG' have the same independent sets, $nG' = (nG)'$.

THEOREM 6. Let $G(S)$ be a projective geometry of order n and rank q. kG is binary if and only if $k \geq \frac{n^{q-1}+n^{q-2}+ \ldots +n}{q}$ or both $k=1$ and $n=2$.

PROOF. Since there are $n+1$ copoints covering every coline, G is binary if and only if $n=2$ (Theorem 1). We can now let $k>1$. Because of the arithmetic details of the proof we first consider the case $n=2$ and $q=4$. In this case $G(S)$ has 15 points. Each copoint contains 7 points, each line contains 3 points. We may denote the elements of S by the 4-tuples (a_1, a_2, a_3, a_4), $a_i=0$ or 1, not all $a_i=0$, and let independence in G be linear independence. It is then possible to show that $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (1, 1, 0, 0), (1, 0, 1, 0), (0, 1, 1, 0), (0, 0, 0, 1), (0, 0, 1, 1), (0, 1, 1, 1), (1, 1, 1, 1)\}$ is a 10-set, any 8-subset of which is a basis of $2G$. Therefore by Lemma 2

and Theorem 1, $2G$ is not binary. $3G$ is the Boolean truncation of rank 12 on S, which is not binary Lemma 1. kG, $k \geq 4$, is a Boolean algebra. Thus we have kG binary if and only if $k \geq \frac{n^3+n^2+n}{4} = 3\frac{1}{2}$.

Now let $G(S)$ be a projective geometry of order n and rank q. We prove the theorem by induction on q. If $n \neq 2$, $q=3$ is the first step of the induction. The result is then that of Theorem 5. If $n=2$, then the case of $q=3$ is given by Theorem 5, and we let $q=4$ be the first step in the induction. Now assume the result holds for projective geometries of order n and rank $q-1$, $q \geq 4$ ($q \geq 5$ if $n=2$). We wish to show the result holds for G. Let G' be the subgeometry of G on some copoint of G. G' is a projective geometry of order n and rank $q-1$ (Theorem 4). Lemma 5 says that kG' is a subgeometry of kG, and so kG binary implies kG' binary, which by the induction hypothesis implies that $k \geq \frac{n+n^2+ \ldots +n^{q-2}}{q-1}$. Now of $k \geq \frac{1+n+ \ldots +n^{q-2}}{q-1}$, then every set of $1+n+ \ldots +n^{q-2}$ elements is k-independent. For if $|A| = 1+n+ \ldots +n^{q-2}$, then $r(A) \geq q-1$, and so $kr(A) \geq k(q-1) \geq |A|$. If $B \subseteq A$, $kr(B) \geq |B|$, for

$$\frac{|B|}{r(B)} \leq \frac{|\overline{B}|}{r(\overline{B})} \leq \frac{1+n+ \ldots +n^m}{m+1} \leq \frac{1+n+ \ldots +n^{q-2}}{q-1} \leq k$$

(for $m = r(\overline{B})-1$) by Lemma 4. This means that copoints of G are k-independent and so kG is a Boolean truncation. For kG to be binary we need all $(n+ \ldots +n^{q-1})$-sets to be k-independent (Lemma 1). This occurs if and only if $k \geq \frac{n+ \ldots +n^{q-1}}{q}$. This leaves only one case left to investigate: $k = \frac{n+n^2+ \ldots +n^{q-2}}{q-1}$. In this case, $k > \frac{1+n+ \ldots +n^{q-3}}{q-2}$ by Lemma 4, and so by an argument like that above, any $(1+n+ \ldots + +n^{q-3})$-set is k-independent. In fact, any $[(q-1)k]$-set is k-independent; for if A is a subset of such a set, and $1+n+ \ldots +n^{q-3} < |A| \leq \leq (q-1)k$, then $r(A) \geq q-1$ and so $kr(A) \geq k(q-1) = 1+ \ldots +n^{q-2} \geq \geq |A|$. A copoint (which is a $[(q-1)k+1]$-set) however is not k-independent. Analogous to the proof of Theorem 5 we conclude that a qk-set, no $[(q-1)k+1]$-subset of which is contained in a copoint of

G, is a basis for kG. We now construct a set A of $qk+2$ elements every qk-subset of which is a basis for kG. By Lemma 2 and Theorem 1, this will show that kG is not binary. Consider the $n+1$ copoints covering a fixed coline of G. Label them C_0, C_1, ..., C_n. Select the elements of A as follows. Let the $1+n+ \ldots +n^{q-3}$ points of the fixed coline be in A. Select any $(n^{q-2}-1)$ remaining elements of C_0 for A. We now have $(q-1)k$ points for A. Recall that C_0, C_1, ..., C_n each contain n^{q-2} different points not in the fixed coline. Let $\{x\}$ denote the samllest integer greater than or equal to x. Select $\left\{\frac{k+2}{n}\right\}$ points for A from each of the copoints C_1, ..., C_n. Select only points not in the fixed coline. This is possible by Lemma 4. Eliminating any excess points from C_1, ..., C_n, we have a set A such that $|A|=qk+2$. To show that every qk-subset of A is a basis, let B be a $[(q-1)k+1]$-subset of A. We show B is contained in no copoint of G. If $|B \cap C_0| \geq 2+n+ \ldots + +n^{q-3}$, then C_0 would be the only copoint containing these points. For if C was a copoint also containing them, then $|C \cap C_0| \geq 2+n+ + \ldots +n^{q-3}$. This contradicts Theorem 5. Thus we may suppose $|B \cap C_0| \leq 1+n+ \ldots +n^{q-3}$. We must select the other n^{q-2} points of B from the $k+2=\frac{n+ \ldots +n^{q-2}}{q-1}+2$ points of A not in C_0. But by Lemma 4 this is impossible unless $n=2$ and $q=4$. However, when $n=2$ we have assumed $q \geq 5$. The existence of the desired set A is thus guaranteed, and the proof is complete.

Let G be a projective geometry with sequence of multiples G, $2G$, ..., mG, where m is the smallest integer such that mG is a Boolean algebra. mG, of course, is binary, as is G when $n=2$. We have shown that the only other multiple that can possibly be binary is $(m-1)G$. It is not hard to see that $(m-1)G$ is binary if and only if $k= = \frac{n+ \ldots +n^{q-1}}{q}$ is an integer (where G has order n, rank q). In this case $m-1=k$. The following theorem shows that there are many geometries for which $(m-1)G$ actually is binary.

THEOREM 7. Let $q \geq 3$ be a prime number, and $n \geq 2$ be an integer. $k=\frac{n+n^2+ \ldots +n^{q-1}}{q}$ is an integer if and only if q and $n-1$ are relatively prime.

PROOF. Suppose $(n-1,\ q)=1$. We know $n^q \equiv n \pmod{q}$ by Fermat's Theorem. Also, $n^q \equiv n \pmod{(n-1)}$. Thus $n^q \equiv n \pmod{[q(n-1)]}$. Since $k=\dfrac{n^q-n}{q(n-1)}$, k is an integer.

Now suppose $(n-1,\ q)\neq 1$. Then $n \equiv 1 \pmod{q}$. Therefore $n^p \equiv 1 \pmod{q}$, $1 \leq p < q-1$, and so $n+n^2+ \ \ldots \ +n^{q-1} \equiv q-1 \pmod{q}$. Thus k is not an integer.

REFERENCES

[1] CRAPO, H. H. - ROTA, G.-C.: On the Foundations of *Combinatorial Theory: Combinatorial Geometries*, preliminary edition, M.I.T. Press, 1970.

[2] EDMONDS, J. R.: *Minimum Partition of a matroid into Independent Sets*, Journal of Research of the National Bureau of Standards, 69B (1965), 67-72.

[3] TUTTE, W. T.: *A homotopy theory for matroids, I, II*, Trans. of the Amer. Math. Soc., 88 (1958), 144-174.

Manoscritto pervenuto in redazione il 29 marzo 1972.