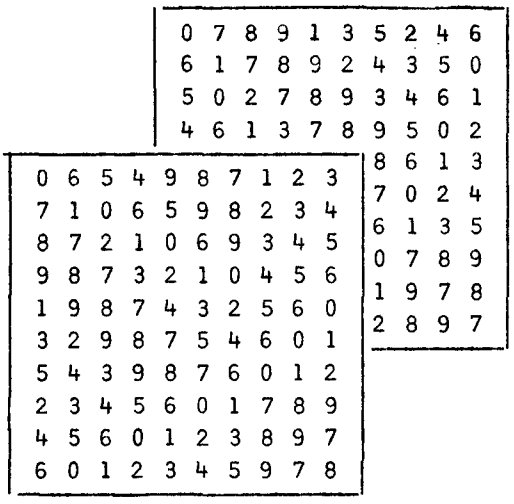
* *The research in this report was partially supported by the Air Force Office of Scientific Research Contract AFOSR-68-1415.*



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 0 | 6 | 5 | 4 | 9 | 8 | 7 | 1 | 2 | 3 |
| 7 | 1 | 0 | 6 | 5 | 9 | 8 | 2 | 3 | 4 |
| 8 | 7 | 2 | 1 | 0 | 6 | 9 | 3 | 4 | 5 |
| 9 | 8 | 7 | 3 | 2 | 1 | 0 | 4 | 5 | 6 |
| 1 | 9 | 8 | 7 | 4 | 3 | 2 | 5 | 6 | 0 |
| 3 | 2 | 9 | 8 | 7 | 5 | 4 | 6 | 0 | 1 |
| 5 | 4 | 3 | 9 | 8 | 7 | 6 | 0 | 1 | 2 |
| 2 | 3 | 4 | 5 | 6 | 0 | 1 | 7 | 8 | 9 |
| 4 | 5 | 6 | 0 | 1 | 2 | 3 | 8 | 9 | 7 |
| 6 | 0 | 1 | 2 | 3 | 4 | 5 | 9 | 7 | 8 |

C O M B I N A T O R I A L
M A T H E M A T I C S
Y E A R

*February 1969 - June 1970*

# CODES, PACKINGS AND THE CRITICAL PROBLEM*

*by*

T. A. Dowling

*Department of Statistics*
*University of North Carolina at Chapel Hill*

Institute of Statistics Mimeo Series No. 600.34

February, 1971

# Codes, Packings and the Critical Problem*

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

## 1. Introduction

A fundamental problem of finite projective geometry is to determine the maximum cardinality of a set of points such that no three points of the set are collinear, or more generally, the maximum number of points in a set, no $t$ of which lie in a subspace of dimension $t-2$. A set satisfying this latter property we call $t$-independent, and a maximal such set a $t$-packing. The problem has received considerable attention in recent years, not only from geometers, but from applied mathematicians and engineers as well, for "large" $t$-independent sets have important applications in coding theory, factorial designs in statistics, information retrieval systems, and a number of other areas.

Our purpose will be to establish the connection between the packing problem and a general combinatorial problem, called the critical problem [11], which includes, among others, the classical problems of determining the chromatic number of a graph or the minimum flow in a network.

The critical problem for a set of points in a projective geometry is to determine the minimum number of hyperplanes which "distinguish" the points of the set. Its solution depends only on the lattice of closed sets in the subgeometry. The characteristic polynomial of the lattice; a generalization of the concept of the chromatic polynomial of a graph, plays a fundamental role. The required minimal number of hyperplanes, called the *critical exponent* of the set, is the smallest power of the order of the field which is not a root of the polynomial.

* *The research in this report was partially supported by the Air Force Office of Scientific Research Contract AFOSR-68-1415.*

For the coding problem, the critical exponent of a certain subgeometry of projective geometry represents the minimal redundancy of a linear code with prescribed minimum distance. Enumerative formulae in terms of evaluations of the characteristic polynomial are given for the number of t-independent sets and t-independent spanning sets of any given cardinality.

## 2. Combinatorial Geometry

We summarize in this section some basic definitions and results of combinatorial geometry. A detailed treatment is given in [11].

A (finite) *pregeometry* $G(X)$ consists of a finite set $X$ together with a closure operator $A \to \bar{A}$ satisfying the *exchange property*: If $a,b \in X$, $A \subseteq X$ and $a \in \overline{A \cup b}$, $a \notin \bar{A}$, then $b \in \overline{A \cup a}$. A set $A$ is *closed* if $A = \bar{A}$. A set $B$ is *independent* if $b \notin \overline{B-b}$ for all $b \in B$. A *basis* of a set $A \subseteq X$ is a minimal subset $B$ of $A$ such that $\bar{B} = \bar{A}$; equivalently, a basis of $A$ is a maximal independent subset of $A$. A *basis of* $G(X)$ is a basis of $X$. All bases of any set $A$ have the same cardinality, called the *rank* of $A$. The *rank of* $G(X)$ is the rank of $X$. A $k$-*flat* is a closed set $A$ of rank $k$. In particular, a one-flat is a *point*, a two-flat a *line*, etc. If $G(X)$ is of rank $r$, an $(r-1)$-flat is a *copoint*, an $(r-2)$-flat a *coline*, etc. A set is *dependent* if not independent. A *circuit* is a minimal dependent set.

A *restriction* $G(S)$ of a pregeometry $G(X)$ is a pregeometry defined on a subset $S$ of $X$ with closure operator $A \to \bar{A} \cap S$. The independent sets in $G(S)$ are those subsets of $S$ independent in $G(X)$, and the rank function of $G(S)$ is the restriction of the rank function of $G(X)$ to subsets of $S$. A *contraction* $G(X)/S$ of $G(X)$ is a pregeometry defined on a subset $X-S$ of $X$ with closure operator $A \to \overline{A \cup S} - S$. The independent sets of $G(X)/S$ are those subsets $A \subseteq X-S$ such that $A \cup B$ is independent in $G(X)$ for some

(equivalently, for every) basis $B$ of $X-S$. A *minor* of $G(X)$ is any pregeometry defined on a subset of $X$ obtained by a sequence of restrictions and contractions. Any minor may be represented in the form $G(B)/A$ for $A \subseteq B \subseteq X$, that is, as a contraction of a restriction of $G(X)$. The minor $G(B)/A$ is equivalently the restriction of the contraction $G(X)/A$ to the set $B-A \subseteq X-A$.

A *combinatorial geometry* (briefly, a geometry) is a pregeometry $G(X)$ for which the empty set and all elements of $X$ are closed. Equivalently, a pregeometry is a geometry iff every two-element subset of $X$ is independent. Every pregeometry $G(X)$ has an *associated geometry* $G(X_0)$ whose points are the equivalence classes of $X-\bar{\phi}$ modulo the equivalence relation $a \sim b$ iff $\bar{a} = \bar{b}$. A restriction of a geometry $G(X)$ is a geometry, called a *subgeometry* of $G(X)$. A contraction of a geometry is not necessarily a geometry.

A (finite) *geometric lattice* is a finite lattice $L$ such that if $x,y \in L$, then $y$ covers $x$ (that is $x < z \leq y$ implies $z = y$) iff there exists a point (element covering 0, or atom) $p \in L$ such that $x \wedge p = 0$, $x \vee p = y$. The set $L(X)$ of closed sets of a pregeometry $G(X)$, ordered by inclusion, is a *geometric lattice*, called the *lattice of* $G(X)$. It is isomorphic to the lattice of the associated geometry. Conversely, every geometric lattice $L$ is the lattice of a geometry defined on the set of its points. The *rank* $r(x)$ of an element $x \in L(X)$ is well-defined as the length of all maximal chains from 0 to $x$, and is equal to the rank of the corresponding closed set in the (pre-) geometry $G(X)$.

For any flat $\bar{B}$ of $G(X)$, and subset $A \subset \bar{B}$, if $x$, $y$ denote the flats $\bar{A}$, $\bar{B}$ respectively in the lattice $L(X)$, then the interval $[x,y]$ of $L(X)$ is isomorphic to the lattice of the minor $G(\bar{B})/A$.

If $G(S)$ is a restriction of a (pre-) geometry $G(X)$, the lattice of $G(S)$ is isomorphic to the lattice $L(S)$ consisting of those flats of $G(X)$ which have a basis in the set $S$. The function $\rho: L(X) \to L(S)$ which sends

each flat $x$ to the largest flat contained in it with a basis in $S$ is called the *retract* from $L(X)$ to $L(S)$.

The *Möbius function* $\mu$ of a (locally finite) partially ordered set $P$ is the integer-valued function defined on $P\times P$ by $\mu(x,y) = 0$ if $x \not\leq y$, $\mu(x,x) = 1$, $\mu(x,y) = -\sum_{x\leq z<y} \mu(x,z)$ if $x < y$. By the *Möbius inversion formula* [20], if $f$, $g$ are real-valued functions on $P$ such that $g(x) = \sum_{y\geq x} f(y)$, then $f(x) = \sum_{y\geq x} \mu(x,y)g(y)$.

The *Whitney numbers* of a geometric lattice $L$ are of two kinds,

$$W_L(k) = \sum_{x\in L} \delta(r(x),k), \qquad \text{(Second kind)}$$

that is, the number of elements of rank $k$, and

$$w_L(k) = \sum_{x\in L} \mu(0,x)\ \delta(r(x),k) \qquad \text{(First kind)}.$$

The latter are the coefficients of the *characteristic polynomial* of $L$,

$$p_L(\nu) = \sum_{x\in L} \mu(0,x)\ \nu^{r(1)-r(x)}.$$

To illustrate, let $V_n = V_n(q)$ be the $n$-dimensional vector space over $GF(q)$. Then $V_n$ is a pregeometry, with closure operator $A \to sp(A)$, where $sp(A)$ is the subspace of $V_n$ spanned by the set $A \subseteq V_n$. The closed sets are thus the subspaces of $V_n$, and the independent sets are those sets $B$ linearly independent over $GF(q)$. The rank of a set $A$ is the dimension of $sp(A)$. The associated geometry of $V_n$ is the projective geometry $\mathbb{P}_n = \mathbb{P}_n(q)$ of rank $n$ (= projective dimension $n-1$, typically denoted $PG(n-1,q)$) over $GF(q)$. The lattice of subspaces of $V_n$, denoted $L_n = L(V_n)$, is isomorphic to the lattice of projective subspaces of $\mathbb{P}_n$. An interval $[x,y]$ of $L_n$ is isomorphic to $L_m$, $m = r(y)-r(x)$. The Whitney numbers of $L_n$ are

$$W_{L_n}(k) = \begin{bmatrix} n \\ k \end{bmatrix},$$

the Gaussian coefficients [14], defined as

$$\begin{bmatrix} n \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1},$$

and

$$w_{L_n}(k) = (-1)^k q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}.$$

The characteristic polynomial of $L_n$ is

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

Restrictions to subsets $S \subseteq V_n$ represent more typical examples of pregeometries. Although we shall be concerned only with pregeometries (geometries) of this type, it should be emphasized that not every pregeometry (geometry) is representable as a restriction of a vector space (projective geometry).

## 3. The Packing Problem

Let $\mathbb{P}_r$ be the projective geometry of rank $r$ over a finite field $GF(q)$. A set $T$ of points of $\mathbb{P}_r$ is *t-independent* if $|T| \geq t$ and every t-element subset of $T$ is independent, where $2 \leq t \leq r$. The *t-packing problem* for $\mathbb{P}_r$ is to determine the maximum cardinality of a t-independent set in $\mathbb{P}_r$. We denote this number by $N(r,t)$, and call a t-independent set of cardinality $N(r,t)$ a *t-packing* of $\mathbb{P}_r$.

Of course, the analogous problem could be posed for any combinatorial geometry $G$. For example, if $G$ is the bond geometry [20] of the complete graph $K_p$, the t-packing problem amounts to determining the maximum number of edges in a graph with $p$ vertices containing no circuits of length $t$ or less. In a classical paper of extremal graph theory, Turan [31] proved that $[p^2/4]$ is the

maximum number when $t = 3$, and that the extremal graph is unique. For $t \geq 4$, this problem is apparently still unsolved.

Various cases of the packing problem for $\mathbb{P}_r$ have been investigated by a number of Italian geometers, including Segre [21-27], Barlotti [1-4] and Tallini [29-30], and by Bose [5-9], who noted its connection with coding theory and experimental design, and numerous others.

In the terminology [4] of projective geometers, a t-independent set (which is not (t+1)-independent) of cardinality k is a k-*set of kind* t-1, a k-*arc* if t=r, a k-*cap* if $r \geq 4$, $t = 3$. An *oval* is a k-arc of maximum cardinality in a projective plane (not necessarily desarguesian); a k-cap of maximum cardinality is an *ovaloid*. The geometrical structure of ovals and ovaloids in lower dimensions is fairly well understood. An irreducible conic in a desarguesian plane $\mathbb{P}_3$ is a (q+1)-arc [23]. If q is odd, it is an oval, and every oval is a conic [21]. For q even a conic may be extended to an oval, with q+2 points [18]. An elliptic quadric is a $q^2+1$-cap in $\mathbb{P}_4$ [17], an ovaloid if $q > 2$ [5, 28, 18]. For odd q, every ovaloid is an elliptic quadric [1]. A comprehensive survey is given in [4].

A t-independent set in $\mathbb{P}_r$ has an obvious matrix-theoretic interpretation. Given a (homogeneous) coordinatization of $\mathbb{P}_r$ and any set S of n points, let a *matrix of* S be any $r \times n$ matrix over GF(q) each of whose columns is a coordinate vector of a point $a \in S$. Clearly there are $(q-1)^n n!$ different matrices of S. The matrix of a t-independent set has the property that every subset of t or fewer columns is independent over GF(q). A matrix with the latter property we call t-*independent* as well.

A few elementary observations on the behavior of N(r,t) may be made. Obviously, $N(r,2) = (q^r-1)/(q-1)$, since every two point subset of the point set of a projective geometry (or of any geometry) is independent. Also, given

a t-packing of a copoint $H$ of $\mathbb{P}_r$, any single point not in $H$ can be added to yield a t-independent set in $\mathbb{P}_r$. Since a copoint is isomorphic to $\mathbb{P}_{r-1}$,

$$N(r,t) \geq N(r-1,t) + 1.$$

A t-independent set is clearly (t-1)-independent, so

$$N(r,t) \leq N(r,t-1).$$

If $T$ is a t-packing $(t \geq 3)$ in $\mathbb{P}_r$ and $a \in T$, then in the contraction $\mathbb{P}_r/a$, with associated geometry $\mathbb{P}_{r-1}$, $T-a$ is a (t-1)-independent set. Hence

$$N(r,t) \leq N(r-1,t-1) + 1. \tag{3.1}$$

If $q = 2$ and $t$ is odd, this becomes an equality:

$$N(r,2s+1) = N(r-1,2s), \qquad q = 2, \tag{3.2}$$

which is easily proved by adding a column of zeros, then a row of ones, to a 2s-independent matrix, thereby reversing the inequality (3.1).

We list below all known values [4] of $N(r,t)$ for which at least one of $r$, $t$, $q$ is arbitrary.

$$N(r,2) = (q^r-1)/(q-1),$$

$$N(3,3) = \begin{cases} q+1, & q \text{ odd} \\ q+2, & q \text{ even} \end{cases}$$

$$N(4,3) = q^2+1, \qquad q > 2$$

$$N(r,3) = 2^{r-1}, \qquad q = 2$$

$$N(r,r) = r+1, \qquad q = 2.$$

Various upper and lower bounds for $N(r,t)$ are known for special cases [3, 9, 26, 27, 29]. Bounds for general $r$, $t$ are most easily expressed in

terms of a related function $R(n,t)$ defined in Section 4, and will be given there.

Note that iteration of (3.1) yields

$$(3.3) \qquad N(r,t) \leq \frac{q^{r-t+2}-1}{q-1} + t - 2.$$

A t-independent set in $\mathbb{P}_r$ can be equivalently defined as a subgeometry $G(T)$ of $\mathbb{P}_r$ such that every $(t-1)$-element subset of points is closed. Thus the lattice $L(T)$ is isomorphic to the Boolean algebra $B(T)$ up to rank (= cardinality) $t-1$. This property permits an enumeration of the number of k-flats of $\mathbb{P}_r$ meeting $T$ in a given j-element subset, by Möbius inversion on the set $P$ of subsets of $T$ with $t-1$ or fewer elements, for all $0 \leq j \leq k \leq t-1$, as follows.

For $A \in P$, let $g_k(A)$ be the number of k-flats of $\mathbb{P}_r$ containing $A$, and $f_k(A)$ the number of k-flats of $\mathbb{P}_r$ intersecting $T$ in $A$. Then for $k \leq t-1$,

$$g_k(A) = \sum_{B \supseteq A} f_k(B),$$

which yields, by the Möbius inversion formula,

$$(3.4) \qquad f_k(A) = \sum_{B \supseteq A} \mu(A,B)\, g_k(B).$$

If $B \in P$ is of cardinality $\ell$, then the closure of $B$ in $\mathbb{P}_r$ is an $\ell$-flat, so $g_k(B) = \begin{bmatrix} r-\ell \\ k-\ell \end{bmatrix}$. For a set $A$ of cardinality $j$, the number of $B \in P$ of cardinality $\ell$ containing $A$ is $\binom{n-j}{\ell-j}$, and since the interval $[A,B]$ of $P$ is a Boolean algebra, $\mu(A,B) = (-1)^{\ell-j}$. Thus (3.4) becomes, if $|A| = j$,

$$(3.5) \qquad f_k(A) = \sum_{\ell=j}^{k} (-1)^{\ell-j} \begin{bmatrix} r-\ell \\ k-\ell \end{bmatrix} \binom{n-j}{\ell-j}.$$

The right-hand side of (3.4) is independent of $A$. We denote it by $\phi_{jk}(n)$, to emphasize its dependence on $n$.

THEOREM 1. Let $T$ be a t-independent set in $\mathbb{P}_r$ of cardinality $n$, and let $0 \le j \le k \le t-1$. Then the number of k-flats intersecting $T$ in any given j-element subset is

$$\phi_{jk}(n) = \sum_{\ell=j}^{k} (-1)^{\ell-j} \begin{bmatrix} r-\ell \\ k-\ell \end{bmatrix} \binom{n-j}{\ell-j}.$$

COROLLARY. The number of k-flats not meeting $T$ is

$$\phi_{0k}(n) = \sum_{\ell=0}^{k} (-1)^{\ell} \begin{bmatrix} r-\ell \\ k-\ell \end{bmatrix} \binom{n}{\ell}.$$

Note that $\phi_{0k}(n)$ is a polynomial in $n$ of degree $k$. Some obvious necessary conditions for the existence of a t-independent set of cardinality $n$ are

$$\phi_{0k}(m-1) \ge \phi_{0k}(m) \ge 0 \tag{3.6}$$

for all $m \le n$ and $k \le t-1$. The upper bound for $N(r,t)$ based solely on this observation appears to be larger than (3.3). Nevertheless, the sequence $(\phi_{0k}: 0 \le k \le t-1)$ provides some information which may be useful. Geometrical arguments establishing the non-existence of order ideals in $\mathbb{P}_r$ with $\phi_{0k}(n)$ flats of rank $k$ would imply the non-existence of a t-independent set of cardinality $n$.

To take a simple example, in $\mathbb{P}_3(3)$, with $t=3$, (3.8) is satisfied for $n = 5$, and $\phi_{00}(5) = 1$, $\phi_{01}(5) = 8$, $\phi_{02}(5) = 3$. Since three concurrent lines contain 10 points, and three non-concurrent lines 9 points, a 5-arc in $\mathbb{P}_3(3)$ is impossible.

## 4. THE CODING PROBLEM

Let $F = GF(q)$. In the vector space $F^n$ $(\simeq V_n)$ let $w(a)$, $a = (a_1, a_2, \ldots, a_n)^T$, denote the number of non-zero coordinates $a_i$ of $a$. Then $w$ is a norm on $F^n$, called *Hamming weight*, inducing the metric $d$

(*Hamming distance*) on $F^n$ defined by $d(a,b) = w(a-b)$, that is, the number of indices $i$ such that $a_i \neq b_i$. An $(n,k)$-*linear code of distance* $t+1$ [16] is a $k$-dimensional subspace $C$ of $F^n$ such that $d(a,b) \geq t+1$ for all $a,b \in C$, $a \neq b$. The *redundancy* of an $(n,k)$-code is its codimension $r = n-k$. An $(n,k)$-code of distance $t+1$ is *optimal* if $k$ is maximal for given $n$, $t$; equivalently, if its redundancy is minimal. We denote by $R(n,t)$ the redundancy of an optimal code. The *coding problem* is to determine $R(n,t)$.

Suppose $C$ is any subspace of $F^n$ such that $d(a,b) \geq t+1$ for all $a \neq b$ in $C$. Then for $a \neq 0$, $w(a) = d(a,0) \geq t+1$. Thus $C$ contains no elements of the $t$-*ball*

$$S_{n,t} = \{e: \ 1 \leq w(e) \leq t\}.$$

Conversely, if $C$ is a subspace such that $C \cap S_{n,t} = \phi$, then $d(a,b) \geq t+1$ for $a \neq b$ in $C$, for $d(a,b) = w(a-b)$ and $a,b \in C$ imply $a-b \in C$, so $a-b \notin S_{n,t}$. Thus an $(n,k)$-linear code of distance $t+1$ is equivalently a $k$-dimensional subspace of $F^n$ containing no elements of the $t$-ball $S_{n,t}$.

Let $C$ be an $(n,n-r)$-code of distance $t+1$. If $M$ is an $r \times n$ matrix with $\operatorname{Ker} M = C$, then $C \cap S_{n,t} = \phi$ implies $Me \neq 0$ for all $e \in S_{n,t}$. By the definition of $S_{n,t}$, it follows that $M$ is $t$-independent. Conversely, given an $r \times n$ $t$-independent matrix $M$, its kernel, of dimension at least $n-r$, can contain no elements of $S_{n,t}$. Thus there exists an $(n,n-r)$ code of distance $t+1$ iff there exists in $\mathbb{P}_r$ an $n$-point $t$-independent set.

This result, first noted by Bose [5] in connection with an analogous problem, accounts for the importance of the packing problem in coding theory. A consequence is that each of $R(n,t)$, $N(r,t)$, regarded as functions of $n$, $r$ respectively, for fixed $t$, determines the other completely by the relation

$$R(n,t) \leq r \iff N(r,t) \geq n.$$

Thus

$$R(n,t) = \min\{r: N(r,t) \geq n\}, \tag{4.1}$$

$$N(r,t) = \max\{n: R(n,t) = r\}, \tag{4.2}$$

the equality in brackets above being justified by the fact that $R(n,t)$ is a unit-increasing function of $n$,

$$R(n+1,t) = R(n,t) + \epsilon, \qquad \epsilon \in \{0,1\}.$$

From (3.1) and (4.1) we obtain

$$R(n,t) \geq R(n-1,t-1) + 1, \tag{4.3}$$

which becomes an equality if $t$ is odd and $q = 2$, by (3.2) and (4.1):

$$R(n,2s+1) = R(n,2s) + 1, \qquad (q = 2).$$

A number of lower bounds for $R(n,t)$ are known. The Rao-Hamming bound [16, 19] is

$$R(n,2s) \geq \{\log_q B(n,s)\},$$

$$R(n,2s+1) \geq \{\log_q (B(n,s)+\binom{n-1}{s}(q-1)^{s+1})\},$$

where

$$B(n,m) = \sum_{i=0}^{m} \binom{n}{i}(q-1)^i .$$

This, of course, gives implicitly an upper bound for $N(r,t)$.

The Varshimov-Gilbert upper bound [16] for $R(n,t)$ is of a similar form:

$$R(n,t) \leq \{\log_q (1+B(n-1,t-1))\}. \tag{4.4}$$

The upper bounds given below for $t = 2s$ are derived from codes constructed by

Bose and Ray-Chaudhuri [7, 8], and Hoequenghem [15]: The bounds for $t = 2s+1$ are obtained from these, using (3.2) and (3.1):

$$(4.5) \qquad R(n,2s) \le s\{\ell og_2(n+1)\} \quad (q = 2)$$
$$R(n,2s+1) \le s\{\ell og_2 n\} + 1 \quad (q = 2).$$

$$(4.6) \qquad R(n,2s) \le 2s\{\ell og_q(n+1)\}$$
$$R(n,2s+1) \le (2s+2)\{\ell og_q(n+1)\} - 1.$$

These provide lower bounds for $N(r,t)$.

## 5. Connection with the Critical Problem

A sequence $(L_1,L_2,\ldots,L_r)$ of linear functionals on $V_n$ is said to *distinguish* a (spanning) set $S \subseteq V_n-\{0\}$ if for every $a \in S$ there exists an $L_i$ such that $L_i(a) \neq 0$. The *critical problem* for the set $S$, as formulated by Crapo and Rota [11], is to determine the minimum length $c = c(S)$ of a sequence of linear functionals distinguishing $S$. The integer $c = c(S)$ is called the *critical exponent* of $S$.

It is proved in [11] that the critical exponent of $S$ depends only on the lattice $L(S)$ consisting of those subspaces of $V_n$ with a basis in $S$. In fact, more can be said:

Theorem *(Crapo-Rota)*. The number of sequences of linear functionals $(L_1,L_2,\ldots,L_r)$ of length $r$ on $V_n$ which distinguish the set $S$ is $p(q^r)$, where $p(\nu)$ is the characteristic polynomial of $L(S)$.

Corollary. The critical exponent $c$ for the set $S$ is determined by

$$p(q^r) = 0, \quad r = 0,1,\ldots,c-1$$
$$p(q^r) > 0, \quad r \ge c.$$

The critical problem embraces a number of well-known combinatorial problems. A classical example is the problem of coloring the vertices of a graph so that no two adjacent vertices receive the same color. The bond geometry of the graph, defined on the set of edges, has a representation in a vector space over any field. If $S$ is a representation of the geometry in $V_n = V_n(q)$, then the graph is colorable in $q^r$ colors iff $r \geq c(S)$, the critical exponent of $S$.

A sequence $\mu = (L_1, L_2, \ldots, L_r)$ of linear functionals clearly distinguishes $S$ iff no vector of $S$ is in the kernel of the linear transformation $\mu: V_n \to F^r$. Thus if $C$ is a subspace of dimension $k$ such that $C \cap S = \phi$, then any sequence $\mu = (L_1, L_2, \ldots, L_r)$ such that $\operatorname{Ker} \mu \subseteq C$ distinguishes $S$. This implies $r \geq n-k$, with equality iff $L_1, L_2, \ldots, L_r$ are independent in the dual space $V_n^*$ and $\operatorname{Ker} \mu = C$. It follows that if $k = k(S)$ is the maximum dimension of a subspace $C$ of $V_n$ such that $C \cap S$ is empty, then the critical exponent of $S$ is given by $c = n-k$.

The Crapo-Rota theorem and the foregoing remarks suggest that evaluations of the characteristic polynomial at powers of $q$ can be used to enumerate the subspaces of $V_n$ of each rank containing no points of $S$. This is indeed the case. The proof requires the following [10].

THEOREM *(Crapo)*. If $Q$ is the lattice of a subgeometry of a geometry with lattice $L$, then

$$\nu^{r_L(1)-r_Q(1)} p_Q(\nu) = \sum_{\substack{x \in L \\ \rho(x)=0}} p_{[x,1]}(\nu),$$

where $\rho: L \to Q$ is the retract.

We shall also need the identity:

$$(5.1) \qquad \sum_{i=0}^{m} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} m \\ i \end{bmatrix} \begin{bmatrix} m-i \\ j \end{bmatrix} = \delta_{jm}.$$

To prove (5.1), consider the number $g_j(x)$ of elements of corank $j$ above $x$ in $L_m$. Clearly

$$g_j(x) = \begin{bmatrix} m-r(x) \\ j \end{bmatrix} = \sum_{y \geq x} \delta(r(y), m-j).$$

By Möbius inversion,

$$\delta(r(x), m-j) = \sum_{y \geq x} \mu(x,y) \begin{bmatrix} m-r(y) \\ j \end{bmatrix}.$$

In particular, if $x = 0$,

$$\begin{aligned} \delta_{jm} &= \sum_{y \in L_m} \mu(0,y) \begin{bmatrix} m-r(y) \\ j \end{bmatrix} \\ &= \sum_{i=0}^{m} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} m \\ i \end{bmatrix} \begin{bmatrix} m-i \\ j \end{bmatrix}. \end{aligned}$$

THEOREM 2. If $S$ is a spanning set of $V_n$ not containing the zero, the number $a_{n-m}$ of subspaces of $V_n$ of dimension $n-m$ containing no points of $S$ is given by

$$\left( \prod_{i=0}^{m-1} (q^m - q^i) \right) a_{n-m} = \sum_{i=0}^{m} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} m \\ i \end{bmatrix} p(q^{m-i}), \tag{5.2}$$

where $p(\nu)$ is the characteristic polynomial of $L(S)$.

PROOF. The subspaces of $V_n$ containing no points of $S$ are the preimage of $0$ in the retract $\rho: L_n \to L(S)$. Since $[x,1] \simeq L_m$ for $x \in L_n$ of rank $n-m$, by Crapo's theorem,

$$p(\nu) = \sum_{m=0}^{n} a_{n-m} p_m(\nu), \tag{5.3}$$

where $p_m(\nu) = \prod_{i=0}^{m-1} (q^m - q^i)$ is the characteristic polynomial of $L_m$. Note that

$$\begin{bmatrix} m-i \\ j \end{bmatrix} = \frac{p_j(q^{m-i})}{p_j(q^j)}. \tag{5.4}$$

Setting $\nu = q^{m-i}$ in (5.3) and substituting into the right-hand side of (5.2), and using (5.4) and (5.1), we obtain

$$\sum_{i=0}^{m} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} m \\ i \end{bmatrix} \sum_{j=0}^{n} a_{n-j} p_j(q^{m-i})$$

$$= \sum_{j=0}^{n} p_j(q^j) a_{n-j} \sum_{i=0}^{m} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} m \\ i \end{bmatrix} \begin{bmatrix} m-i \\ j \end{bmatrix}$$

$$= \sum_{j=0}^{n} p_j(q^j) a_{n-j} \delta_{jm}$$

$$= \left( \prod_{i=0}^{m-1} (q^m - q^i) \right) a_{n-m}.$$

We recall from Section 4 that an $(n,k)$-linear code of distance $t+1$ is a $k$-dimensional subspace of $F^n$ containing no vectors of the $t$-ball $S_{n,t}$, the latter consisting of all non-zero vectors with $t$ or fewer non-zero coordinates. (The set $S_{n,t}$ could be defined independently of coordinates in $V_n$ as the set of all vectors linearly dependent on $t$ or fewer elements of a given basis $B$ of $V_n$. Equivalently, $e \in S_{n,t}$ iff $e \in B$ or there exists a circuit $E$ of $V_n$ such that $|E| \leq t+1$ and $e \in E \subseteq Bue$.) The coding problem is to determine the minimum codimension $R(n,t)$ of a subspace of $F^n$ containing no vector of $S_{n,t}$. Thus the coding problem is the *critical problem for* $S_{n,t}$, and the critical exponent of $S_{n,t}$ is the redundancy $R(n,t)$ of an optimal code.

PROPOSITION 1. The redundancy $R(n,t)$ of an optimal code of length $n$ and distance $t+1$ is given by

$$p_{n,t}(q^r) = 0, \quad r = 0,1,\ldots,R(n,t) - 1$$
$$p_{n,t}(q^r) > 0, \quad r \geq R(n,t),$$

where $p_{n,t}(\nu)$ is the characteristic polynomial of the geometric lattice $L_{n,t}$ of subspaces of $F^n$ $(F = GF(q))$ with a basis in

$$S_{n,t} = \{e: \ 1 \leq w(e) \leq t\}.$$

COROLLARY The maximum cardinality of a t-independent set in $\mathbb{P}_r$ is

$$N(r,t) = max\{n: \ p_{n,t}(q^r) > 0\}.$$

Recall that any coordinatization of $V_n$ defines a coordinatization of the dual space $V_n^*$ such that each linear transformation $\mu: V_n \to F^r$ is represented by premultiplication by an $r \times n$ matrix, whose rows are the coordinates of the linear functionals of $V_n^*$ defining $\mu$. We can thus state

PROPOSITION 2. The number of $r \times n$ t-independent matrices over GF(q) is $p_{n,t}(q^r)$.

COROLLARY. The number of n-point t-independent sets in $\mathbb{P}_r$ is $p_{n,t}(q^r)/(q-1)^n n!$.

Set $m = r$ in (5.2), and note that $\prod_{i=0}^{r-1}(q^r - r^i)$ is the order of the full linear group $GL_r(q)$. Hence

PROPOSITION 3. The number of t-independent $r \times n$ matrices of rank $r$ over GF(q) is

$$\sum_{i=0}^{r} (-1)^i \, q^{\binom{i}{2}} \begin{bmatrix} r \\ 2 \end{bmatrix} p_{n,t}(q^{r-i}).$$

COROLLARY. The number of n-points t-independent sets spanning $\mathbb{P}_r$ is

$$\sum_{i=0}^{r} (-1)^r \, q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} p_{n,t}(q^{r-i})/(q-1)^n n! \ .$$

Of course, for these results to be of any use in attacking the coding or packing problem, the characteristic polynomials $p_{n,t}(\nu)$ must be determined. Without underestimating the difficulties encountered in evaluating the polynomials, it seems likely that an investigation of the structure of the geometric lattices $L_{n,t}$ might provide considerable insight into the problem. At present,

we can offer a general expression for the polynomials $p_{n,t}(\nu)$ only for $t = 2$, a somewhat trivial case for the packing problem.

The elements of $L_{n,2}$ [13] are those subspaces of $F^n$ which are the null spaces of column monomial matrices. The order relation is representable as a generalization to $GF(q)$ of the refinement order of the partition lattice, to which it reduces when $q = 2$. The characteristic polynomial of $L_{n,2}$ is

$$p_{n,2}(\nu) = \prod_{i=0}^{n-1} (\nu-1-i(q-1)).$$

This yields the critical exponent

$$R(n,t) = [\log_q((n-1)(q-1)+1)] + 1$$

and hence,

$$N(r,2) = \frac{q^r-1}{q-1}.$$

The lattice $L_{n,t}$ has the property that it is isomorphic to $L_n$ above rank $n-t$, as implied by

THEOREM 3. The retract $\rho: L_n \to L_{n,t}$ preserves all elements $x \in L_n$ of corank $t-1$ or less.

PROOF. Let $x$ be an element of $L_{n,t}$ of corank $k \leq t-1$. Without loss of generality, we can take $x$ as the kernel of a matrix of the form $M = (I_k, A)$, where $I_k$ is the identity of order $k$. Then if $B = (-A^T, I_{n-k})$, $MB^T = 0$, so the rows of $B$ are a basis of $x$, and since each row of $A^T$ has at most $k$ non-zero elements, each row of $B$ has at most $k+1 \leq t$ non-zero elements. Thus $x$ has a basis in $S_{n,t}$, so $\rho(x) = x$.

# REFERENCES


[1] Barlotti, A. "Un' Estensione del Teorema di Segre-Kustaanheimo." *Boll. Un. Math. Ital.* (3) 10 (1955), 498-506.

[2] Barlotti, A. "Un' Osservasione sulle k-Calotte Degli Spazi Lineari Finite de Dimensione Tre." *Boll. Un. Mat. Ital., (3)* 11 (1956), 248-252.

[3] Barlotti, A. "Una Limitazione Superiore per il Numero di Punti Appartenenti a una k-Calotta C(k,0) di uno Spazio Lineare Finito." *Boll. Un. Math. Ital., (3)* 12 (1957), 67-70.

[4] Barlotti, A. "Some Topics in Finite Geometrical Structures," Institute of Statistics Mimeo Series No. 439, University of North Carolina, 1965.

[5] Bose, R. C. "Mathematical Theory of the Symmetrical Factorial Design." *Sankhyā*, 8 (1947), 107-166.

[6] Bose, R. C. "On Some Connections between the Design of Experiments and Information Theory." *Bull. Int. Stat. Inst., 38,* (1961).

[7] Bose, R. C. and D. K. Ray-Chaudhuri "On a Class of Error-Correcting Binary Group Codes." *Inf. and Control,* 3, (1960), 68-79.

[8] Bose, R. C. and D. K. Ray-Chaudhuri "Further Results on a Class of Error-Correcting Binary Group Codes." *Inf. and Control,* 3, (1960), 279-290.

[9] Bose, R. C. and J. N. Srivastava "On a Bound Useful in the Theory of Factorial Designs and Error-Correcting Codes." *Ann. Math. Stat., 35,* (1964), 408-414.

[10] Crapo, H. "Möbius Inversion in Lattices." *Arch. der Math. XIX,* (1968), 595-607.

[11] Crapo, H. and G.-C. Rota *Combinatorial Geometries,* MIT Press, Cambridge, Mass., 1970.

[12] Crapo, H. and G.-C. Rota "Geometric Lattices." *Trends in Lattice Theory.*

[13] Dowling, T. A. "A q-Partition Lattice." (in preparation).

[14] Goldman, J. and G.-C. Rota "The Number of Subspaces of a Vector Space." in *Recent Progress in Combinatorics,* edited by W. T. Tutte, Academic Press, (1969), 75-83.

[15] Hocquenghem, A. "Codes Correcteurs d'Erreurs." *Chiffres,* 2, (1959), 147-156.

[16] Peterson, W. W. *Error-Correcting Codes,* MIT Press, Cambridge, Mass., 1961.

[17] Primrose, E. I. F. "Quadrics in Finite Geometries." *Proc. Cambridge Philos. Soc. 47,* (1951), 299-304.

[18] Qvist, B. "Some Remarks Concerning Curves of Second Degree in the Finite Plane." *Ann. Acad. Sci. Fenn.,* Ser. A, I 134 (1952), 1-27.

[19] Rao, C. R. "Factorial Experiments Derivable from Combinatorial Arrangements of Arrays." *Suppl. J. Roy. Stat. Soc.,* 9 (1947), 128-139.

[20] Rota, G.-C. "On the Foundations of Combinatorial Theory I. Theory of Möbius Functions." *Z. Wahrscheinlichkeitstheorie und verw. Gebiete 2,* (1964), 340-368.

[21] Segre, B. "Sulle ovali nei piani lineari finiti." *Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)* 17 (1954), 141-152.

[22] Segre, B. "Ovals in a Finite Projective Plane." *Canad. J. Math.,* 7 (1955), 414-

[23] Segre, B. "Intorno alla geometria sopra un corpo di caratteristica due." *Rev. Fac. Sci. Univ. Istanbul* Ser. A., 21 (1956), 97-123.

[24] Segre, B. "Curve Razionali Normali e k-Archi Negli Spazi Finiti." *Ann. Mat. Pure. Appl. (4)* 39 (1955), 357-379.

[25] Segre, B. "Sui k-archi nei piani finiti di caratteristica 2." *Rev. Math. Pure Appl.* 2 (1957), 289-300.

[26] Segre, B. "Le geometrie di Galois." *Ann. Mat. Pura Appl. (4)* 48 (1959), 1-77.

[27] Segre, B. "On Complete Caps and Ovaloids in Three-Dimensional Galois Spaces of Characteristic Two." *Acta. Arith.* 5 (1959), 315-332.

[28] Seiden, E. "A Theorem in Finite Projective Geometry and an Application to Statistics." *Proc. Amer. Math. Soc.* 1 (1950), 282-286.

[29] Tallini, G. "Sulle k-Calotte di uno Spazio Lineare Finito." *Ann. Math. Pura. Appl. (4)* 42 (1956), 119-164.

[30] Tallini, G. "On Caps of Kind s in a Galois r-dimensional Space." *Acta. Arith.* 7 (1961), 19-28.

[31] Turán, P. "Eine Extremalanfgabe aus der Graphen Theorie." *Mat. Fiz. Lapok. 48* (1941), 436-452.