CISM COURSES AND LECTURES NO. 313
INTERNATIONAL CENTRE FOR MECHANICAL SCIENCES

GEOMETRIES, CODES AND CRYPTOGRAPHY

EDITED BY

G. LONGO/M. MARCHI/A. SGARRO

SPRINGER - VERLAG
WIEN - NEW YORK

INTERNATIONAL CENTRE FOR MECHANICAL SCIENCES

COURSES AND LECTURES - No. 313

GEOMETRIES, CODES AND CRYPTOGRAPHY

EDITED BY

G. LONGO
UNIVERSITY OF TRIESTE

M. MARCHI
UNIVERSITY OF UDINE

A. SGARRO
UNIVERSITY OF UDINE

SPRINGER - VERLAG WIEN - NEW YORK

Le spese di stampa di questo volume sono in parte coperte da contributi del Consiglio Nazionale delle Ricerche.

This volume contains 36 illustrations.

In order to make this volume available as economically and as rapidly as possible the authors' typescripts have been reproduced in their original forms. This method unfortunately has its typographical limitations but it is hoped that they in no way distract the reader.

ISBN 3-211-82205-4 Springer Verlag Wien-New York
ISBN 0-387-82205-4 Springer Verlag New York-Wien

PREFACE

Geometry is the art not to make calculations.

The International Centre for Mechanical Sciences has a long-standing tradition of advanced schools in coding theory and information theory, started as early as 1970 (cf the list of volumes in this series at the end of this book). In 1983 a rather exciting event took place, namely an advanced school on the new subject of cryptology (queer indeed, that the the century-long art of secret writing should be called new!). The 1983 meeting (cf volume n. 279 in this series) has by now entered the history of contemporary European cryptologic research, preceded as it is only by one similar event in Burg Feuerstein, Germany, in 1982, and followed by the 1984 workshop at the Sorbonne of Paris, which was the first of this sort to bear the by now well-established name of Eurocrypt.
So, in a way, the Udine meeting was Eurocrypt number zero, second in a list whose origin is curiously set at n= -1.

After this, CISM kept secretive for several years on the subject of coding, be it source coding, channel coding or ciphering. In 1989 the second editor, M. Marchi, who is a "pure" geometer, having heard about the spectacular success that finite (pure!) geometries were experiencing in the domain of authentication schemes (a very matter-of-fact subject nowadays, as it has so much to do with the proper handling of our credit cards), decided to appease his curiosity and contacted the third editor, A. Sgarro, an information theorist active in Shannon-theoretic cryptology. From their conversations the idea of this school originated; the first editor, G. Longo, himself an information theorist but also a writer, added his experience to their enthusiasm. The result was a delightful week during which students and researchers alike were given the opportunity to meet, to exchange ideas, to get along in their field, and, why not!, to make friends. About fifty people participated, coming from fifteen different countries. Geometers and coding *theorists (not necessarily distinct persons) worked shoulder to shoulder in the historical Palazzo del Torso, the beutiful 16th-century site of CISM; we are confident that these contacts helped to blur the largely artificial borders between "pure" and "applied" mathematics.*

While classes took place in the Palazzo del Torso, conversation groups could spread all over the charming town of Udine, which is a fertile crossroads of European cultures, situated as it is at the intersection of Latin, Germanic and Slav areas. We are particularly proud of this fact in this 1989 of wonders, which, we firmly hope, will open an age of thriving for what was often and rather bitterly called the old continent.

The editors: Giuseppe Longo, Mario Marchi, Andrea Sgarro

PART ONE

Geometries and Codes

CONTENTS

LECTURES ON GALOIS GEOMETRIES AND STEINER SYSTEMS

G. Tallini
Università La Sapienza, Roma, Italy

ABSTRACT

The paper consists of four lectures held at "Centre International des Sciences Meccaniques" of Udine (Italy), June 1989. Their content is the following. General concepts on Galois geometry and Steiner systems. The theory of h-sets in Steiner systems, with particular attention to Galois spaces. The theory of blocking sets, the even and odd type sets in a Steiner system. Applications to linear error correcting codes.

1. GALOIS SPACES

Let p be a prime, Z_p the field of the residue classes mod p, g(x) a polynomial with coefficients in Z_p, irreducible in Z_p and of degree h. We call *Galois field* of order $q = p^h$ the field $GF(q) = Z_p[x]/(g(x))$, algebraic extension of Z_p by the polynomial g(x). We prove that *every finite field has order $q = p^h$ (p a prime) and it is isomorphic to a Galois field.* Moreover, *for every prime p and integer h a Galois field of order $q = p^h$ exists and it is unique up to an isomorphism.*

For any integer $r \geq 2$ we denote by PG(r,q) *the projective space* of dimension r over GF(q). The points of PG(r,q) are therefore the ordered (r+1)-tuples of not all zero elements of GF(q), determined up to a non zero multiplicative factor in GF(q). A subspace S_d of dimension d in PG(r,q) is the set of points whose coordinates satisfy a system of r-d linear homogeneous independent equations.

We set

$$\theta_d = \sum_{i=0}^{d} q^i . \qquad (1.1)$$

We prove:

I. - *In PG(r,q) a subspace S_d, $1 \leq d \leq r$, has θ_d points:*

$$|S_d| = \theta_d . \qquad (1.2)$$

In particular:

$$|PG(r,q)| = \theta_r \qquad (1.3)$$

II. - *The number of hyperplanes, S_{r-1}, of PG(r,q) is θ_r. It fol-*

lows that the number of S_{d-1}'s belonging to a S_d of $PG(r,q)$ is θ_d.

III. - *In $PG(r,q)$ the number of hyperplanes through a S_{r-d-1} is θ_d.*

IV. - *We denote by $\gamma_{r,d,q}$, $1 \leq d \leq r-1$, the number of subspaces S_d of $PG(r,q)$. It is:*

$$\gamma_{r,d,q} = \prod_{i=0}^{d} (\theta_{r-i}/\theta_{d-i}) \; . \tag{1.4}$$

V. - *In $PG(r,q)$ the number of S_d's through a given S_m, $m \geq 0$, is $\gamma_{r-m-1,d-m-1,q}$.*

2. STEINER SYSTEMS S(2,k,v)

A *Steiner system $S(2,k,v)$* (or a *2-$(v,k,1)$ design*) is a pair (S,L), where S is a set whose elements we call points and L is a family of parts of S whose elements we call lines such that:

$$|S| = v; \qquad \forall \ell \in L \Rightarrow |\ell| = k \; . \tag{2.1}$$

through two distinct points there is a unique line:

$$\forall P,Q \in S, P \neq Q \Rightarrow \exists ! \, \ell \in L: \; P,Q \in \ell \tag{2.2}$$

For example PG(r,q) with respect to its lines is a $S(2,q+1,\theta_r = \sum_{i=0}^{r} q^i)$.

We denote by F_p the set of lines of S(2,k,v) through a point P of S. It is:

$$\forall P \in S \; , \quad |F_p| = (v-1)/(k-1) \tag{2.3}$$

Counting in two different ways the pairs (P,ℓ) where $P \in S$, $\ell \in L$, $P \in \ell$, we have $v.|F_p| = |L|k$, then (see (2.3)):

$$|L| = v(v-1)/k(k-1)\ . \tag{2.4}$$

Therefore a necessary condition in order a $S(2,k,v)$ exists, is the following:

$$r = (v-1)/(k-1)\ , \quad b = v(v-1)/k(k-1) \tag{2.5}$$

are both integers.

If $P \in S$ and $\ell \in L$, $P \notin \ell$, we denote by u the number of lines through P not meeting the line ℓ (*parallel* to ℓ). It is:

$$u = r - k \tag{2.6}$$

We have:

$$0 \leq u = r - k = (v-1)/(k-1) - k \Longrightarrow v \geq k(k-1) + 1 = k^2 - k + 1$$

It is:

$$u = 0 \iff v = k^2 - k + 1 \iff [\forall \ell, \ell' \in L, \ell \neq \ell' \Rightarrow |\ell \cap \ell'| = 1] \iff \tag{2.7}$$
$$\iff S(2,k,k^2-k+1) \text{ is a projective plane of order } q=k-1,$$
$$S(2,k,k^2-k+1) = S(2,q+1,q^2+q+1) \iff |L| = |S| = q^2 + q + 1;$$
$$\forall P \in S,\ \forall \ell \in L,\ |\ell| = q+1 = |F_p|, \text{ for example } PG(2,q).$$

$$u = 1 \iff v = k^2 \iff [\forall P \in S, \forall \ell \in L, \exists ! \ell' \in L\text{: } P \in \ell', \ell' \cap \ell = \emptyset \tag{2.8}$$
$$(\ell' \text{ parallel to } \ell)] \iff S(2,k,k^2) \text{ is an affine plane of}$$

order k, for example AG(2,q), k = q.

We call *subspace* of S(2,k,v) a subset T of S such that:

$$P, Q \in T \implies \text{the line } PQ \subseteq T. \tag{2.9}$$

Obviously $\emptyset$, the points, the lines, S, are subspaces. Moreover every subspace T ($|T| \geq 2$) is a $S(2,k,v_T)$, with $v_T \leq v$ and, if $T \neq S$, $v_T = |T| \leq r$.

The family Σ of subspaces of (S,L) is a *closure system,* that is

$$\begin{cases} S \in \Sigma \\ \{T_i\}_{i \in \mathcal{I}}, \ T_i \in \Sigma \implies \bigcap_{i \in \mathcal{I}} T_i \in \Sigma \end{cases} \tag{2.10}$$

If $X \subseteq S$, the *closure*, $\bar{X}$, of X is the intersection of all subspaces containing X, that is the *minimal* subspace containing X.

A set $\mathcal{I}$ of points of S is called *independent* if:

$$x \in \mathcal{I} \implies x \notin \overline{(\mathcal{I} - \{x\})}. \tag{2.11}$$

A *base* of (S,L) is a *maximal independent* set of S.

(S,L) is a *matroid* if:

$$\forall X \subseteq S, \ \forall \mathcal{I}, \mathcal{I}' \text{ maximal independent contained in } X \implies \implies |\mathcal{I}| = |\mathcal{I}'|. \tag{2.12}$$

If (S,L) is a matroid we define:

$$\text{rank } X = |\mathcal{I}|, \ \mathcal{I} \text{ maximal independent of } X, \qquad \dim(S,L) = \text{rank } S - 1. \tag{2.13}$$

If (S,L) is a Galois space PG(r,q), the subspaces of (S,L) are the subspaces of PG(r,q). The closure of $X \subseteq S$ is its linear closure in PG(r,q). Moreover PG(r,q) is a matroid and dim(S,L) = r.

3. GENERAL CONCEPTS ABOUT h-SETS OF A S(2,k,v)

A h-set of S(2,k,v) = (S,L) is a subset H consisting of h points of S. We classify such sets with respect to their behaviour with the lines of (S,L).

We define *s-index character of H* the number t_s of lines meeting H in s points, $0 \leq s \leq k$. It is:

t_0 = Number of external lines to H,

t_1 = Number of tangent lines to H,

t_2 = Number of 2-secant lines to H,

t_s = Number of s-secant lines to H,

t_k = Number of lines belonging to H.

We prove:

I. - *The characters of a h-set of S(2,k,v) satisfy the following equations:*

$$\left|\begin{array}{l} \sum_{s=0}^{k} t_s = b = v(v-1)/k(k-1), \\ \sum_{s=0}^{k} s\, t_s = h\, r = h(v-1)/(k-1), \\ \sum_{s=0}^{k} s(s-1) t_s = h(h-1). \end{array}\right. \tag{3.1}$$

By $(3.1)_2$ and $(3.1)_3$ we have:

$$\sum_{s=0}^{k} s^2 t_s = h(h-1+r) = h[h-1 + (v-1)/(k-1)]. \qquad (3.2)$$

We say that H is an *m-character set*, if exactly m characters are different from zero. Let $(n_1, n_2, \ldots, n_r)$ be integers such that $0 \leq n_1 < < n_2 < \ldots < n_r \leq k$. We say that H is of *class* $[n_1, n_2, \ldots, n_r]$ if $t_n = 0$, $\forall\ n \neq n_1, n_2, \ldots, n_r$. We say that H is of *type* $(n_1, n_2, \ldots, n_m)$ if it is of class $[n_1, n_2, \ldots, n_m]$ and $t_{n_i} \neq 0$ $(i=1,2,\ldots,m)$.

The study of the h-sets of S(2,k,v) may be done by increasing the number of non-zero characters. We have:

II. - *If H has a unique character, either $H = \emptyset$ or $H = S$, that is non-trivial one-character sets don't exixt.*

Proof. If $H \neq \emptyset$, $H \neq S$, a point $P \in H$ and a point $Q \in S - H$ exist. Let be $n = |H \cap \ell|$, $\ell \in L$. If we range the points of H, different from P, on the r lines through P, we have $|H| = r(n-1)+1$. For Q we have similarly $|H| = r.n$, whence $rn = r(n-1)+1$, a contradiction (since $r \geq k > 1$).

Assume H has two characters, so that it is of type (m,n), with $0 \leq m < n \leq k$. By (3.1) we have:

$$\begin{cases} H \text{ of type } (m,n) \Longrightarrow t_m = (nb-hr)/(n-m),\ t_n = (hr-mb)/(n-m) \\ h^2 - h[1 + (n+m-1)r] + m\,n\,b = 0 \\ \Delta = [1 + (n+m-1)r]^2 - 4\,m\,n\,b \quad \text{is a square.} \end{cases} \qquad (3.3)$$

Moreover we prove:

III. - *Sets of type (0,k) don't exist. The sets of type (1,k) are the subspaces of S(2,k,v) such that every line meets them (we call such subspaces, Π, primes of S(2,k,v) and we have $|\Pi| = r$). The sets H of type (0,n), n <k, are such that:*

$$\begin{cases} |H| = h = (n-1)r + 1 , \\ P \notin H,\ \sigma_P = \#\, n\text{-secant lines through } P = r - (r-1)/n, \\ n \text{ divides } r-1. \end{cases} \tag{3.4}$$

The sets H' of type (m,k) are the complements of those of type (0,n = = k-m), whence:

$$\begin{cases} |H'| = v - (k-m-1)r - 1, \\ k - m \text{ divides } r - 1. \end{cases} \tag{3.4'}$$

IV. - *Every set of class* [0,1,k] *of* S(2,k,v) *is a subspace and conversely.*

We call *(h;m,n)-set* of S(2,k,v) a h-set H ($\neq \emptyset$,S) such that:

$$m = \min_{\substack{\ell \in L \\ \ell \cap H \neq \emptyset}} |\ell \cap H| , \qquad n = \max_{\ell \in L} |\ell \cap H| . \tag{3.5}$$

We have:

$$h \leq m + (r-1)n , \tag{3.6}$$

$$t_0 = 0,\ n < k \implies h \geq n + (r-1)m , \tag{3.7}$$

Let M,N be two integers such that $1 \leq M \leq m$, $n \leq N$. By (3.1), (3.2) for any (h;m,n)-set H of S(2,k,v) we have:

$$0 \leq \sum_M^N (N-s)(s-M)t_s = -MN \sum_M^N t_s + (M+N) \sum_M^N s\, t_s - \sum_M^N s^2 t_s =$$

$$= - MN(b-t_0) + (M+N)hr - h(h-1+r) =$$

$$= -h^2 + h[r(M+N-1) + 1] - MN(b-t_0)$$

that is:

$$0 \le \sum_{M}^{N} (N-s)(s-M)t_s = -h^2 + h[r(M+N-1) + 1] - MN(b-t_0) \tag{3.8}$$

It follows:

$$\begin{cases} MNt_0 \ge h^2 - h[r(M+N-1) + 1] + MNb \\ = \iff N = n,\ M = m,\ H \text{ is of class } [0,m,n], \end{cases} \tag{3.9}$$

whence:

$$t_0 = 0 \implies \begin{cases} h^2 - h[r(M+N-1) + 1] + MNb \le 0 \\ \text{the equality holds} \iff M=m, N=n,\ H \text{ is of type } (m,n) \end{cases} \tag{3.10}$$

$$t_0 = 0 \implies \begin{cases} \Delta = [r(M+N-1) + 1]^2 - 4MNb \ge 0 \\ \Delta = 0 \iff M=m, N=n, H \text{ is of type } (m,n), h=[r(m+n-1)+1]/2 \end{cases} \tag{3.11}$$

By (3.11), (3.10) it follows that:

V. - *In $S(2,k,v)$ sets of class $[1,2,3]$ don't exist, if $4v > k(3r+2)$. In particular in $S(2,q+1,q^2+q+1)$ and in $S(2,q,q^2)$ sets of class $[1,2,3]$ don't exist if $q \ge 5$.*

4. INTERSECTION SETS AND BLOCKING SETS IN S(2,k,v)

An *intersection set* of S(2,k,v) is a set H meeting every line in at least one point, that is such that $t_0 = 0$. It is:

$$H \text{ intersection set } \Longrightarrow \begin{cases} |H| \geq r\ , \\ |H| = r \iff H \text{ is of type } (1,k) \iff \\ \iff H \text{ is a prime} \end{cases} \tag{4.1}$$

A *blocking set* in S(2,k,v) is an intersection set not containing lines, that is such that $t_0 = t_k = 0$. Obviously, *if* B *is a blocking set, also* $S - B$ *it is*. It follows that (see (4.1)):

$$B \text{ blocking set } \Longrightarrow r < |B| < v - r \tag{4.2}$$

Our aim is to improve (4.2). Let be $n = \max_{\ell \in L} |\ell \cap B|$ and s a n-secant line to B. Let be $P \in s - B$. Each of the r-1 lines through P, different from s, meets B in at least one point, whence $|B| \geq r - 1 + n$. Set:

$$h = |B| = r - 1 + a, \quad a \geq n = \max_{\ell \in L} |\ell \cap B| \tag{4.3}$$

If in (3.10) we set $M = 1$, $N = a$, $h = |B| = r - 1 + a$, we get:

$$\begin{cases} (r-1+a)^2 - (r-1+a)(ra+1) + ab \leq 0 \\ = 0 \iff a = n,\ B \text{ is of type } (1,n) \end{cases} \tag{4.4}$$

Since $v = r(k-1) + 1$, $b = vr/k$, by (4.4) we get:

$$\begin{cases} ka^2 - a(3k-r) - k(r-2) \geq 0 \iff a \geq \alpha = 1 + \dfrac{k-r+\sqrt{(r-k)^2+4k(k-1)r}}{2k} \\ a = \alpha \iff a = \alpha = n,\ B \text{ is of type } (1,n). \end{cases} \tag{4.5}$$

By (4.3), (4.5) and since the complement of a blocking set is a block-