

---

# BOLLETTINO UNIONE MATEMATICA ITALIANA

---

FRANCESCO MAZZOCCA

## Alcuni problemi di ricerca nelle geometrie di Galois

*Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. 4-B (2001),  
n.1, p. 45–69.*

Unione Matematica Italiana

[<http://www.bdim.eu/item?id=BUMI\\_2001\\_8\\_4B\\_1\\_45\\_0>](http://www.bdim.eu/item?id=BUMI_2001_8_4B_1_45_0)

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

---

*Articolo digitalizzato nel quadro del programma  
bdim (Biblioteca Digitale Italiana di Matematica)  
SIMAI & UMI*

<http://www.bdim.eu/>



## Alcuni problemi di ricerca nelle geometrie di Galois.

FRANCESCO MAZZOCCA (\*)

**Summary.** – *We present a survey on classical problems of Galois geometries. More precisely we discuss some problems and results about ovals, hyperovals, caps, maximal arcs and blocking sets in projective planes and spaces over Galois fields.*

Desideriamo innanzitutto ringraziare vivamente il Presidente, Alberto Conte, il Vice Presidente, Carlo Sbordone, la Commissione scientifica dell'UMI e il Comitato organizzatore del XVI congresso dell'UMI per l'onore che ci hanno concesso nell'invitarci a tenere questa conferenza.

Ci è stato esplicitamente chiesto un intervento non specialistico e di presentare dei risultati di carattere generale e facilmente comprensibili anche da persone non esperte nel nostro settore di ricerca. Naturalmente abbiamo fatto il possibile per attenerci a questo invito ed è in questo spirito che abbiamo organizzato l'esposizione. Chi volesse trovare risultati più profondi e aggiornati potrà avvalersi dell'ampia bibliografia riportata alla fine. Gli argomenti di cui tratteremo riguardano la *geometria sui campi di Galois*, che costituisce una delle aree più vaste ed importanti della combinatoria. Il suo interesse, al di là di quello intrinseco dovuto alla bellezza dei suoi risultati ed all'eleganza dei suoi metodi, è nato ed è in continuo crescendo a causa delle innumerevoli applicazioni, sia in altri campi della matematica che in teorie e discipline maggiormente coinvolte in problemi concreti.

La vastità della letteratura esistente ci ha costretti ad una drastica selezione tra i possibili argomenti da presentare. Abbiamo, così, limitato la nostra attenzione ad alcuni problemi classici, diversi dei quali non ancora completamente risolti, e tra questi abbiamo messo maggiormente in luce quelli più vicini ai nostri gusti e ai nostri interessi di ricerca.

(\*) Conferenza tenuta a Napoli il 18 settembre 1999 in occasione del XVI Congresso U.M.I.

## 1. – Caratteri di insiemi di punti in un piano proiettivo finito.

Siano  $\mathcal{P}$  ed  $\mathcal{L}$  rispettivamente gli insiemi dei punti e delle rette di un piano proiettivo finito  $\pi_q$  d'ordine  $q$  e sia  $X$  un insieme di punti di  $\pi_q$  con  $m$  elementi. Ricordiamo che  $\pi_q$  possiede lo stesso numero,  $q^2 + q + 1$ , di punti e di rette e che ogni retta contiene esattamente  $q + 1$  punti. Quando  $\pi_q$  è isomorfo al piano proiettivo sul campo di Galois  $GF(q)$  con  $q$  elementi si usa denotarlo con  $PG(2, q)$ ; ovviamente in questo caso  $q$  è potenza di un primo  $p$ , la caratteristica di  $GF(q)$ .

**DEFINIZIONE 1.1.** – Per ogni  $j = 1, 2, \dots, q + 1$ , si chiama *carattere  $j$ -esimo*, o *numero d'intersezione  $j$ -esimo*, di  $X$  il numero  $t_j = t_j(X)$  delle rette di  $\pi_q$  che intersecano  $X$  in esattamente  $j$  punti.

Siano  $j_0 < j_1 < \dots < j_s$  interi non negativi. L'insieme  $X$  si dice di *tipo*  $(j_0, j_1, \dots, j_s)$  se ogni retta di  $\pi_q$  interseca  $X$  in esattamente  $j_h$  punti, per qualche  $h = 0, 1, \dots, s$ . Si dice invece che  $X$  è di *classe*  $(j_0, j_1, \dots, j_s)$  se è di tipo  $(j_0, j_1, \dots, j_s)$  e risulta  $t_{j_h} \neq 0$ , per ogni  $h = 0, 1, \dots, s$ . ■

Una retta di  $\pi_q$  con un unico punto  $P$  in comune con  $X$  si dice *unisecante*, o anche *tangente* ad  $X$  in  $P$ . Una retta che interseca  $X$  in esattamente  $j > 1$  punti si dice *secante*, o  *$j$ -secante*. La proposizione che segue fornisce le relazioni fondamentali tra gli interi  $t_j$ ; esse sono note come *equazioni dei caratteri* di  $X$ .

**PROPOSIZIONE 1.2.** – Sia  $X$  un insieme di  $m$  punti di  $\pi_q$ . Allora i caratteri di  $X$  verificano le seguenti relazioni:

$$(1) \quad \begin{cases} \sum_{j=0}^{q+1} t_j &= q^2 + q + 1, \\ \sum_{j=1}^{q+1} j t_j &= m(q + 1), \\ \sum_{j=2}^{q+1} (j - 1) j t_j &= m(m - 1). \end{cases}$$

**ESEMPIO 1.3.** – Gli insiemi di classe  $(0, 1)$ ,  $(1, q + 1)$ ,  $(q + 1)$  sono rispettivamente i punti, le rette e l'insieme di tutti i punti di  $\pi_q$ . ■

**ESAMPIO 1.4.** – Un insieme  $X$  di punti di  $\pi_q$  si chiama *sottopiano* d'ordine  $m$  se è di tipo  $(0, 1, m + 1)$  e le intersezioni di  $X$  con le rette aventi  $m + 1$  punti in comune con  $X$  definiscono una struttura di piano proiettivo su  $X$ .

Se  $q$  è un quadrato, un sottopiano di  $\pi_q$  d'ordine  $\sqrt{q}$  si chiama *sottopiano di Baer*.

L'insieme  $X$  dei punti del piano  $PG(2, q^n)$  a coordinate in  $GF(q)$  è un sottopiano di  $PG(2, q^n)$  d'ordine  $q$  isomorfo a  $PG(2, q)$ . Nel caso  $n = 2$ ,  $X$  è un sottopiano di Baer.

Siano  $q$  un quadrato e  $X$  un insieme di  $q + \sqrt{q} + 1$  punti di  $\pi_q$ . Se  $X$  è di tipo  $(1, \sqrt{q} + 1)$ , allora  $X$  è un sottopiano di Baer di  $\pi_q$ . ■

PROPOSIZIONE 1.5. – *Sia  $X$  un sottopiano d'ordine  $m$  di  $\pi_q$  con  $m < q$ . Allora, se esiste una retta di  $\pi_q$  disgiunta da  $X$ , risulta*

$$q \geq m^2 + m.$$

*Se ogni retta di  $\pi_q$  è ad intersezione non vuota con  $X$ , allora  $q$  è un quadrato e  $X$  un sottopiano di Baer.*

Il problema fondamentale relativo ai caratteri dei sottoinsiemi di  $\pi_q$  può enunciarsi nel seguente modo.

PROBLEMA 1.6. – *Sia  $t = (t_0, t_1, \dots, t_{q+1})$  una successione di interi non negativi verificanti le (1). Stabilire se esistono in  $\pi_q$  insiemi di punti  $X$  con numeri di intersezione  $t_j$  e, in caso di risposta affermativa, classificarli tutti a meno di collineazioni.*

Diciamo subito che il problema, nella sua generalità, è di estrema difficoltà ed è risolto solo per pochissimi valori di  $t$ . Quasi sempre, pertanto, si richiede che  $X$ , oltre ad avere caratteri assegnati, verifichi anche delle ulteriori proprietà. Noi ci limiteremo ad esporre alcuni risultati soltanto nel caso  $\pi_q = PG(2, q)$ .

L'interesse per questo tipo di problematiche si è senza alcun dubbio sviluppato in seguito ai risultati ottenuti negli anni '50 da B. Segre relativamente alla sua teoria degli archi in un piano di Galois e, in particolare, a quelli relativi alla classificazione delle coniche.

Riportiamo, di seguito, alcune generalità sugli archi di un piano  $\pi_q$ .

DEFINIZIONE 1.7. – Un insieme di  $k$  punti di  $\pi_q$  a tre a tre non allineati prende il nome di *arco di ordine  $k$* , o  *$k$ -arco*. ■

Poiché le rette per un punto di  $\pi_q$  sono in numero di  $q + 1$ , si ha subito che per ogni  $k$ -arco risulta

$$(2) \quad k \leq q + 2.$$

Abbiamo, inoltre, tre possibili numeri d'intersezione non nulli:  $t_0, t_1, t_2$ .

ESEMPIO 1.8. – È ben noto che ogni forma quadratica irriducibile in tre variabili su  $GF(q)$  possiede esattamente  $q + 1$  punti razionali in  $PG(2, q)$ . Ne se-

gue che i  $q + 1$  punti di una conica non singolare di  $PG(2, q)$  costituiscono un  $(q + 1)$ -arco. ■

DEFINIZIONE 1.9. – Un  $k$ -arco si dice *completo* se non è contenuto in un  $(k + 1)$ -arco; nel caso contrario si dice *incompleto*. ■

Sia  $K$  un  $k$ -arco di  $\pi_q$ . Detti  $A$  un punto di  $K$  e  $B$  un punto non appartenente a  $K$ , introduciamo i seguenti parametri relativi a  $K$ :

$$(3) \quad \begin{cases} t &= \text{numero di tangenti a } K \text{ nel punto } A, \\ u_0(B) &= \text{numero delle rette per } B \text{ esterne a } K, \\ u_1(B) &= \text{numero delle rette per } B \text{ tangenti a } K, \\ u_2(B) &= \text{numero delle rette per } B \text{ secanti } K. \end{cases}$$

È un semplice esercizio provare la seguente proposizione.

PROPOSIZIONE 1.10. – *L'intero  $t$  non dipende dal punto  $A$  e risulta*

$$(4) \quad \begin{cases} t = q + 2 - k, \\ t_0 = \frac{q(q-1)}{2} + \frac{t(t-1)}{2}, \quad t_1 = kt, \quad t_2 = \frac{k(k-1)}{2}, \\ u_1(B) + 2u_2(B) = k. \end{cases}$$

*In particolare, nel caso  $k = q + 1$ , risulta*

$$(5) \quad t = 1, \quad t_0 = \frac{q(q-1)}{2}, \quad t_1 = q + 1, \quad t_2 = \frac{q(q+1)}{2}.$$

PROPOSIZIONE 1.11. – *Se  $q$  è dispari, il massimo numero di punti di un arco di  $\pi_q$  è  $q + 1$ .*

PROPOSIZIONE 1.12. – *Se  $q$  è pari, le tangenti ad un  $(q + 1)$ -arco  $K$  di  $\pi_q$  passano tutte per uno stesso punto (il nucleo di  $K$ ).*

OSSERVAZIONE 1.13. – Quando  $q$  è pari, ogni  $(q + 1)$ -arco di  $PG(2, q)$  è incompleto e può completarsi, aggiungendo il nucleo, in unico modo in un  $(q + 2)$ -arco. In particolare, una conica non singolare di  $PG(2, q)$  è un  $(q + 1)$ -arco completo se, e soltanto se,  $q$  è dispari. ■

DEFINIZIONE 1.14. – I  $(q + 1)$ -archi e, nel caso  $q$  pari, i  $(q + 2)$ -archi di  $\pi_q$  si chiamano rispettivamente *oval*i e *iperoval*i. ■

## 2. – Le ovali di $PG(2, q)$ , $q$ dispari.

In un articolo del 1949 [50] G. Jarnefelt e P. Kustaanheimo congetturarono che ogni ovale di  $PG(2, q)$ , con  $q$  dispari, fosse una conica. Molti geometri dell'epoca ritennero la congettura azzardata, tant'è che Marshall Hall Jr, nella sua recensione dell'articolo per il Mathematical Review (14,1008d), scrisse: «*The reviewer finds the conjecture implausible*». Fu questo, forse, il motivo per cui Beniamino Segre prese a studiare il problema, ottenendo uno dei suoi risultati più belli e famosi: la veridicità della congettura di Jarnefelt-Kustaanheimo. Quando lo stesso Marshall Hall Jr. recensì il risultato di Segre [69], ancora per il Mathematical Review (17,72g), scrisse: «*The fact that this conjecture seemed implausible to the reviewer seems to have been at least a partial incentive to the author to undertake this work. It would be very gratifying if further expressions of doubt were as fruitful.*»

L'argomento di Segre è abbastanza lineare e si presta ad essere descritto brevemente. A tale scopo, fissiamo un riferimento proiettivo  $\Re = (E_0, E_1, E_2, E)$  di  $PG(2, q)$ . Denotate con  $(x_0, x_1, x_2)$  le coordinate proiettive di punto in  $PG(2, q)$ , le rette distinte dagli assi coordinati e contenenti  $E_0, E_1, E_2$  avranno rispettivamente equazione del tipo

$$x_1 - \lambda_0 x_2 = 0, \quad x_2 - \lambda_1 x_0 = 0, \quad x_0 - \lambda_2 x_1 = 0,$$

con  $\lambda_j \in F_q^*$ . Ognuno di tali  $\lambda_j$  sarà detto *coordinata* in  $\Re$  della retta nell'equazione della quale compare.

Nel seguito, se  $K$  è un  $k$ -arco di  $PG(2, q)$ , supporremo sempre che  $E_0, E_1, E_2$  appartengano a  $K$  e che le rette tangenti a  $K$  nei punti  $E_0, E_1, E_2$  abbiano rispettivamente coordinate  $\alpha_j, \beta_j, \gamma_j, j = 1, 2, \dots, t$ . Proprietà elementari di geometria e dei campi di Galois permettono di provare le seguenti due proposizioni.

**PROPOSIZIONE 2.1 (lemma delle tangenti).** – *Sia  $K$  un  $k$ -arco di  $PG(2, q)$  contenente i punti  $E_0, E_1, E_2$  e siano  $\alpha_j, \beta_j, \gamma_j, j = 1, 2, \dots, t$ , rispettivamente le coordinate delle rette tangenti a  $K$  in  $E_0, E_1, E_2$ . Allora risulta*

$$\prod_{j=1}^t \alpha_j \beta_j \gamma_j = -1.$$

*In particolare, se  $\Omega$  è un'ovale di  $PG(2, q)$  e le tre rette tangenti nei punti  $E_0, E_1, E_2$  hanno rispettivamente coordinate  $\alpha, \beta, \gamma$ , risulta*

$$(6) \quad \alpha\beta\gamma = -1.$$

**PROPOSIZIONE 2.2.** – *Sia  $\Omega$  un'ovale di  $PG(2, q)$  con  $q$  dispari e consideriamo tre suoi punti, che non è restrittivo identificare con  $E_0, E_1, E_2$ . Siano,*

*inoltre,  $l_0, l_1, l_2$  rispettivamente le tangenti ad  $\Omega$  nei tre punti assegnati. Allora, posto*

$$T_0 = l_1 \cap l_2, \quad T_1 = l_2 \cap l_0, \quad T_2 = l_0 \cap l_1,$$

*le rette  $E_0 T_0, E_1 T_1, E_2 T_2$  formano fascio.*

**PROPOSIZIONE 2.3** (teorema di B. Segre [68, 69]). – *Ogni ovale  $\Omega$  di  $PG(2, q)$ , con  $q$  dispari, è una conica.*

**DIMOSTRAZIONE.** – Mantenendo le notazioni usate per la precedente proposizione, possiamo supporre che il punto unitario  $E$  del riferimento  $\Re$  coincida con il punto di intersezione delle rette  $E_0 T_0, E_1 T_1, E_2 T_2$ ; così abbiamo  $\alpha = \beta = \gamma = -1$  e le rette  $l_0, l_1, l_2$  hanno tutte coordinata uguale a  $-1$ , cioè hanno rispettivamente equazione

$$x_1 + x_2 = 0, \quad x_2 + x_0 = 0, \quad x_0 + x_1 = 0.$$

Inoltre le rette  $E_0 T_0, E_1 T_1, E_2 T_2$  hanno rispettivamente equazione

$$x_1 - x_2 = 0, \quad x_2 - x_0 = 0, \quad x_0 - x_1 = 0$$

e risulta

$$T_0 = (-1, 1, 1), \quad T_1 = (1, -1, 1), \quad T_2 = (1, 1, -1).$$

Sia ora  $M = (m_0, m_1, m_2)$  un punto di  $\Omega$  diverso da  $E_0, E_1, E_2$  e sia

$$\mu_0 x_0 + \mu_1 x_1 + \mu_2 x_2 = 0$$

l'equazione dell'unica retta  $l$  tangente ad  $\Omega$  in  $M$ ; osserviamo che ogni  $\mu_i$  è diverso da zero perché nessuno dei punti  $E_i$  appartiene ad  $l$ . In forza della prop. 2, relativamente al triangolo  $ME_1 E_2$ , abbiamo che le rette congiungenti i punti  $M, E_1, E_2$  rispettivamente con i punti  $T_0 = l_1 \cap l_2, A_2 = l_2 \cap l, A_1 = l \cap l_1$  sono concorrenti in un punto  $W$ .

I punti  $A_1, A_2$  hanno coordinate

$$A_1 = (-\mu_1, \mu_0 - \mu_2, \mu_1), \quad A_2 = (-\mu_2, \mu_2, \mu_0 - \mu_1),$$

le rette  $E_1 A_2, E_2 A_1$  hanno rispettivamente equazione

$$(\mu_0 - \mu_1)x_0 + \mu_2 x_2 = 0, \quad (\mu_0 - \mu_2)x_0 + \mu_1 x_1 = 0$$

e, quindi,  $W$  ha coordinate

$$W = (\mu_1 \mu_2, (\mu_2 - \mu_0) \mu_2, \mu_1 (\mu_1 - \mu_0)).$$

Allora, essendo  $W$  allineato con  $M$  e  $T_0$ , abbiamo

$$(\mu_0 - \mu_1 - \mu_2)[\mu_1(m_0 + m_1) - \mu_2(m_0 + m_2)] = 0.$$

Osserviamo che è  $\mu_0 - \mu_1 - \mu_2 \neq 0$ , altrimenti il punto  $T_0 = (-1, 1, 1)$  appar-

terrebbe ad  $l$  e per esso passerebbero tre tangenti ad  $\Omega$  e ciò, si vede subito, non è possibile. Deve dunque essere

$$\mu_1(m_0 + m_1) = \mu_2(m_0 + m_2)$$

e, ragionando allo stesso modo con riferimento ai triangoli  $M, E_0, E_2$  e  $M, E_0, E_1$ ,

$$\mu_2(m_1 + m_2) = \mu_0(m_1 + m_0), \quad \mu_0(m_0 + m_2) = \mu_1(m_1 + m_2).$$

Ora, posto

$$\delta = \frac{\mu_2}{m_0 + m_1},$$

abbiamo

$$\mu_0 = \delta(m_1 + m_2), \quad \mu_1 = \delta(m_2 + m_0), \quad \mu_2 = \delta(m_0 + m_1)$$

e, sostituendo tali valori nella relazione

$$\mu_0 m_0 + \mu_1 m_1 + \mu_2 m_2 = 0,$$

che esprime l'appartenenza del punto  $M$  alla retta  $l$ , otteniamo

$$m_0(m_1 + m_2) + m_1(m_2 + m_0) + m_2(m_0 + m_1) = 0,$$

cioè

$$2(m_1 m_2 + m_2 m_0 + m_0 m_1) = 0.$$

Dall'essere  $q$  dispari otteniamo

$$m_1 m_2 + m_2 m_0 + m_0 m_1 = 0$$

e da ciò segue subito che  $\Omega$  coincide con la conica di equazione

$$x_1 x_2 + x_2 x_0 + x_0 x_1 = 0,$$

il nostro asserto. ■

**OSSERVAZIONE 2.4.** – La caratterizzazione delle coniche ottenuta da B. Segre con la prop. 2.3 ha dato impulso ad un interessante campo di ricerca: *caratterizzare mediante opportune proprietà d'incidenza le varietà algebriche notevoli*. Un matematico che ha dato enormi contributi in quest'ambito è stato *Giuseppe Tallini*, prematuramente scomparso nell'aprile del 1995. Di Lui citiamo soltanto l'articolo [78], nel quale si trovano esposti molti risultati suoi e della sua scuola. Per ulteriori approfondimenti su questa problematica si rimanda anche a [43], [44], [45]. ■

### 3. – Le iperovali di $PG(2, q)$ , $q$ pari.

Il teorema di B. Segre, prop. 2.3, non vale nel caso che  $q$  sia pari. In tale ipotesi, infatti, possiamo considerare un'iperovali  $\Omega = \Gamma \cup \{C\}$ , ove  $\Gamma$  è una conica non degenera e  $C$  il suo nucleo. Allora, detto  $M$  un punto di  $\Gamma$ , l'insieme  $\Omega \setminus \{M\}$  è un'ovale avente  $q$  punti in comune con  $\Gamma$  e quindi non può essere una conica non appena è  $q > 5$ .

Quando  $q$  è pari, le iperovali che si ottengono aggregando ad una conica non degenera il proprio nucleo si dicono *regolari*. La validità del teorema di B. Segre nel caso  $q$  dispari potrebbe indurre a pensare che, quando  $q$  è pari, le uniche iperovali sono quelle regolari; ciò, purtroppo, non è vero. Esistono, infatti, iperovali non regolari e il primo esempio fu trovato in  $PG(2, 16)$  nel 1958 da L. Lunelli e M. Sce [54] mediante l'uso di un calcolatore.

Le iperovali di  $PG(2, q)$ ,  $q$  pari, si caratterizzano mediante opportuni *polinomi di permutazione*, cioè polinomi  $f \in GF(q)[x]$  le cui funzioni polinomiali sono permutazioni degli elementi di  $GF(q)$ . Anche in questo caso il risultato di partenza si deve a B. Segre.

**PROPOSIZIONE 3.1** (B. Segre [70, 74]). – *Siano  $q$  pari e  $f \in GF(q)[x]$  un polinomio verificante le seguenti proprietà:*

- (i)  *$f$  è di permutazione, di grado non superiore a  $q - 1$  e  $f(0) = 0$ ,  $f(1) = 1$ ;*
- (ii) *per ogni  $a \in GF(q)$ ,  $g_a(x) = [f(x + a) + f(x)]/x$  è un polinomio di permutazione con  $g_a(0) = 0$ .*

*Allora l'insieme*

$$(7) \quad \Omega(f) = \{(f(t), t, 1) : t \in GF(q)\} \cup \{(1, 0, 0), (0, 1, 0)\}$$

*è un'iperovali di  $PG(2, q)$ . Viceversa, se  $\Omega$  è un'iperovali di  $PG(2, q)$ , esisto-  
no un riferimento di  $PG(2, q)$  e un polinomio  $f \in GF(q)[x]$  con le proprietà (i),  
(ii) tali che  $\Omega = \Omega(f)$ .*

I polinomi che verificano le condizioni (i), (ii) del precedente teorema vengono chiamati *o-polinomi*. La classificazione delle iperovali di  $PG(2, q)$  è dunque ricondotta alla ricerca dei polinomi  $f(x)$  di cui alla prop. 3 e questo problema è estremamente difficile e tuttora aperto e molto studiato. Per una interessante panoramica sull'argomento si consiglia [30]. Al momento, oltre ad alcuni esempi sporadici, sono note sette classi infinite di iperovali in  $PG(2, 2^r)$ . Per ciascuna di tali iperovali riportiamo di seguito un o-polinomio  $f(x)$  che la individua:

- *Iperovals regolari:*  $f(x) = x^2$ ;
- *Iperovals di traslazione* [70]:  $f(x) = x^{2^n}$ , con  $MCD(n, r) = 1$ ;

- *Iperovalì di B. Segre* [74, 55]:  $f(x) = x^6$ , nel caso  $r$  dispari;
- *Iperovalì di Glynn I* [40]:  $f(x) = x^{3\sigma+4}$ , nel caso  $r$  dispari e  $\sigma = 2^{(r+1)/2}$ ;
- *Iperovalì di Glynn II* [40]:  $f(x) = x^{\sigma+\lambda}$ , nel caso  $r$  dispari,  $\sigma = 2^{(h+1)/2}$ ,  $\lambda = 2^m$  se  $r = 4m - 1$  e  $\lambda = 2^{3m+1}$  se  $r = 4m + 1$ ;
- *Iperovalì di Payne* [60]:  $f(x) = x^{1/6} + x^{3/6} + x^{5/6}$ , nel caso  $r$  dispari;
- *Iperovalì di Subiaco* [31]:  $f(x) = \frac{d^2(x^4 + x) + d^2(1 + d + d^2)(x^3 + x^2)}{(x^2 + dx + 1)^2} + x^{1/2}$ , con  $T_r(1/d) = 1$  e  $d^2 + d + 1 \neq 0$ .

È da notare che le iperovalì di Payne e di Subiaco sono state scoperte mediante sofisticate tecniche della teoria dei *flock* di un cono quadratico, teoria che, come è noto, è strettamente correlata a quelle dei *quadrangoli generalizzati* e dei *piani di traslazione*. Un raffinamento di queste tecniche ha recentemente portato W. Cherowitzo, C. M. O'Keefe e T. Penttila alla scoperta di nuove iperovalì, le *iperovalì di Adelaide*, la cui costruzione, non ancora pubblicata, è per ora descritta soltanto in un preprint [32].

#### 4. – Insiemi di classe $(0, n)$ in $PG(2, q)$ .

Le iperovalì di  $PG(2, q)$  sono caratterizzate dall'essere insiemi di punti di classe  $(0, 2)$  e, come abbiamo visto, esistono soltanto nel caso  $q$  sia pari. È quindi naturale chiedersi se in  $PG(2, q)$  esistano insiemi di classe  $(0, n)$ ,  $n$  essendo un intero positivo maggiore di 2 e minore di  $q + 1$ . Gli insiemi di questo tipo d'ordine  $k$  sono detti  $(k; n)$ -archi massimali e, con semplici considerazioni aritmetiche, si vede che  $k = (n - 1)q + n$  e  $n$  divide  $q$ .

ESEMPIO 4.1. – Sia  $l$  una retta di  $PG(2, q)$ . Il piano affine  $PG(2, q) \setminus l$  è evidentemente un esempio di  $(q^2; q)$ -arco massimale. Non è difficile rendersi conto che ogni insieme di classe  $(0, q)$  in  $PG(2, q)$  è necessariamente del tipo precedente. Questi esempi di  $(k; n)$ -archi massimali sono detti *banali*. ■

Quando  $q$  è pari si possono costruire  $(k; n)$ -archi massimali, per ogni divisore  $n$  di  $q$ . Vale, infatti, il seguente teorema.

PROPOSIZIONE 4.2 (R. H. F. Denniston [36]). – *Si supponga che  $q$  sia pari. Introdotto in  $PG(2, q)$  un riferimento proiettivo, si consideri il fascio di coniche  $F_a$  di equazione*

$$x_0^2 + ax_0x_1 + x_1^2 + tx_2^2 = 0,$$

ove  $t \in GF(q)$  è un parametro e  $a$  è un elemento di  $GF(q)$  per cui il polinomio  $x^2 + ax + 1$  sia irriducibile su  $GF(q)$ . Si considerino, inoltre, un divisore  $n = 2^h$  di  $q$  ed un sottogruppo additivo  $H$  di  $GF(q)$  d'ordine  $n$ . Allora l'unione delle coniche di  $F_a$  ottenute al variare del parametro  $t$  nel sottogruppo  $H$  è un  $(k; n)$ -arco massimale.

Quando  $q$  è dispari, il problema di stabilire l'esistenza o meno di  $(k; n)$ -archi massimali si presenta molto complicato. Il primo risultato al riguardo, dovuto a A. Cossu [33], stabilisce la non esistenza di  $(k; 3)$ -archi massimali in  $PG(2, 9)$ , il primo caso significativo. Successivamente, J. A. Thas ha provato in [81] la non esistenza di  $(k; 3)$ -archi massimali in  $PG(2, 3^h)$ , per ogni intero  $h > 2$  e, nello stesso lavoro, ha congetturato la non esistenza di  $(k; n)$ -archi massimali non banali nel caso  $q$  dispari. Questa congettura, quotata come «*most wanted problem*» delle geometrie di Galois da T. Penttila e G. F. Royle [62], solo recentemente è stata definitivamente chiusa dal seguente teorema.

PROPOSIZIONE 4.3 (S. Ball, A. Blokhuis, F. Mazzocca [3]). – Il piano  $PG(2, q)$ ,  $q$  dispari, non contiene  $(k; n)$ -archi massimali,  $1 < n < q$ .

Il risultato è stato ottenuto con moderne tecniche polinomiali nell'ambito della cosiddetta *teoria di Rédei* [64], sviluppata negli ultimi anni soprattutto da A. Blokhuis e T. Szőnyi.

Chiudiamo il paragrafo segnalando che in [51] sono stati ottenuti diversi risultati anche riguardo l'esistenza e la classificazione degli insiemi di classe  $(0, 2, t)$ ,  $t > 2$ .

## 5. – Ovoidi in $PG(3, q)$ .

I problemi sugli archi precedentemente studiati ammettono una naturale generalizzazione in  $PG(3, q)$ , lo spazio proiettivo tridimensionale sul campo di Galois  $GF(q)$ .

DEFINIZIONE 5.1. – Un insieme di  $k$  punti di  $PG(3, q)$  si chiama di *calotta di ordine  $k$* , o  *$k$ -calotta*, se i suoi punti sono a tre a tre non allineati. ■

Poiché le rette per un punto di  $PG(3, q)$  sono in numero di  $q^2 + q + 1$ , si ha subito che per ogni  $k$ -calotta risulta

$$(8) \quad k \leq q^2 + q + 2.$$

DEFINIZIONE 5.2. – Una  $k$ -calotta si dice *completa* se non è contenuta in una  $(k + 1)$ -calotta; nel caso contrario si dice *incompleta*. ■

ESEMPIO 5.3. – L'insieme dei  $q^2 + 1$  punti di una quadrica ellittica di  $PG(3, q)$  è una  $(q^2 + 1)$ -calotta completa. ■

ESEMPIO 5.4. – L'insieme dei punti di  $PG(3, 2)$  non appartenenti ad un piano fissato è una 8-calotta completa. Da notare che, in questo caso, l'ordine della calotta è il massimo consentito dalla (8). ■

Sia  $\mathcal{K}$  una  $k$ -calotta di  $PG(3, q)$ . Una retta  $l$  di  $PG(3, q)$  interseca  $\mathcal{K}$  in 0, 1, o 2 punti; in corrispondenza di queste tre possibilità,  $l$  si dirà *esterna*, *tangente* o *secante* a  $\mathcal{K}$ . Un piano  $PG(2, q)$  di  $PG(3, q)$  interseca  $\mathcal{K}$  in 0, 1, o  $s > 1$  punti; in quest'ultimo caso gli  $s$  punti formano un  $s$ -arco di  $PG(2, q)$ . In corrispondenza dei tre casi descritti il piano  $PG(2, q)$  si dirà *esterno*, *tangente* o *secante*  $\mathcal{K}$ .

OSSERVAZIONE 5.5. – Sia  $q$  pari. Allora una  $k$ -calotta  $\mathcal{K}$  di  $PG(3, q)$  è priva di rette tangenti se, e soltanto se,  $q = 2$ ,  $k = 8$  e  $\mathcal{K}$  è il complementare di un piano. ■

PROPOSIZIONE 5.6. – Siano  $q > 2$  e  $\mathcal{K}$  una  $k$ -calotta di  $PG(3, q)$ . Allora risulta

$$k \leq q^2 + 1.$$

Nel caso  $k = q^2 + 1$ , ogni piano secante  $\mathcal{K}$  interseca  $\mathcal{K}$  in un  $(q + 1)$ -arco e ogni punto  $P \in \mathcal{K}$  appartiene ad un unico piano tangente  $\mathcal{K}$ , il quale risulta l'unione delle  $q + 1$  rette per  $P$  tangenti a  $\mathcal{K}$ .

DEFINIZIONE 5.7. – Una calotta di  $PG(3, q)$ ,  $q > 2$ , con  $q^2 + 1$  punti prende il nome di *ovoide*. ■

Nel caso  $q$  dispari, ogni ovoide  $\Omega$  di  $PG(3, q)$  individua una polarità di  $PG(3, q)$  i cui punti assoluti sono esattamente quelli di  $\Omega$ . Usando, allora, il teorema di B. Segre (prop. 2), è possibile ottenere la seguente classificazione degli ovoidi, trovata indipendentemente da A. Barlotti [4] e G. Panella [57].

PROPOSIZIONE 5.8. – Se  $q$  è dispari, ogni ovoide di  $PG(3, q)$  è una quadrica ellittica.

Nel caso  $q$  pari, fissato un ovoide  $\mathcal{K}$  di  $PG(3, q)$ , si possono considerare la funzione biunivoca  $\psi$  che ad ogni piano  $PG(2, q)$  di  $PG(3, q)$  associa il punto

$P_{PG(2, q)}$  di  $PG(3, q)$  definito da

$$P_{PG(2, q)} = \begin{cases} PG(2, q) \cap \mathcal{K}, & \text{se } |PG(2, q) \cap \mathcal{K}| = 1 \\ \text{nucleo dell'ovale } PG(2, q) \cap \mathcal{K}, & \text{se } |PG(2, q) \cap \mathcal{K}| = q + 1. \end{cases}$$

La funzione  $\varphi$  inversa della  $\psi$  è una polarità di  $PG(3, q)$  [71] che, risultando  $P \in \varphi(P)$ , per ogni  $P \in PG(3, q)$ , è nulla. Ne segue che, pur potendo associare a  $\mathcal{K}$  la polarità  $\varphi$ , questa non individua univocamente l'ovoide  $\mathcal{K}$ , a differenza di quanto accade nel caso  $q$  dispari. È questo il motivo per cui la prop. 5 è falsa nel caso  $q$  pari. Il primo esempio di ovoide diverso da una quadrica ellittica fu trovato in  $PG(8, 3)$  da *B. Segre* nel 1959 [71]. Nel 1962 *J. Tits* ha trovato un esempio per ogni  $q$  potenza dispari di 2 [83]. Nel caso  $q = 8$  l'esempio di Tits coincide con quello di Segre [37].

È opportuno notare che gli ovoidi di Tits sono legati ad una interessante interpretazione geometrica del gruppo semplice di Suzuki; vale, infatti, il seguente teorema.

PROPOSIZIONE 5.9. – (*J. Tits* [82, 84]). – *Per un ovoide di Tits  $\Omega$  di  $PG(3, q)$  valgono le seguenti proprietà:*

- *Lo stabilizzatore di  $\Omega$  nel gruppo proiettivo  $PGL(4, q)$  è il gruppo di Suzuki  $Sz(q)$ ;*
- *$Sz(q)$  è doppiamente transitivo sui punti di  $\Omega$  e transitivo su quelli di  $PG(3, q) \setminus \Omega$ .*

*Esistono ovoidi diversi dalle quadriche ellittiche e da quelli di Tits?* È questo uno dei problemi più affascinanti delle geometrie su campi di Galois. Al momento, tranne che per piccoli valori di  $q$ , sembra si sia ancora lontani da una risposta. C'è da osservare che, nello studio di questo problema, potrebbero essere di grande aiuto opportune caratterizzazioni degli ovoidi noti. Esistono, in quest'ambito, molti risultati; di questi ne riportiamo solo uno, molto bello e recentemente ottenuto dal giovane matematico australiano *M. Brown*.

PROPOSIZIONE 5.10 ([19]). – *Sia  $\Omega$  un ovoide di  $PG(3, q)$ ,  $q$  pari, ed esista un piano secante  $\Omega$  in una conica. Allora  $\Omega$  è una quadrica ellittica.*

È da ricordare che il primo risultato sull'argomento si deve a *A. Barlotti* [4], il quale provò che se tutti i piani secanti  $\Omega$  tagliano  $\Omega$  in una conica, allora  $\Omega$  è una quadrica ellittica. Successivamente *B. Segre* [71] provò lo stesso teorema nell'ipotesi che i piani secanti in coniche fossero almeno  $(q^3 - q^2 + 2q)/2$ . Alla luce di questi primi risultati, quello di Brown è ancora più sorprendente!

## 6. – $(k, d)$ -calotte in $PG(n, q)$ .

Questo paragrafo è dedicato ad una generalizzazione dei concetti esposti nei precedenti. Denotiamo con  $PG(n, q)$  lo spazio proiettivo di dimensione  $n$  sul campo di Galois  $GF(q)$ .

**DEFINIZIONE 6.1.** – Un insieme  $K$  di  $k$  punti di  $PG(n, q)$ ,  $n > 1$ , si chiama  $(k, d)$ -calotta, o *calotta di specie  $d$* , di  $PG(n, q)$  se verifica le seguenti proprietà:

- (i)  $K$  è un generatore di  $PG(n, q)$ ,
- (ii) i punti di  $K$  sono a  $d + 1$  a  $d + 1$  indipendenti,
- (iii)  $K$  contiene  $d + 2$  punti dipendenti. ■

Le  $(k, n)$ -calotte di  $PG(n, q)$  prendono più propriamente il nome di *archi*, o  $k$ -archi, ed è chiaro che sono una generalizzazione degli archi piani. Le  $(k, n - 1)$ -calotte generalizzano invece le calotte di  $PG(3, q)$ .

Una  $(k, d)$ -calotta  $K$  si dice *completa* se non è contenuta in una  $(k + 1, d)$ -calotta e il massimo numero di punti di una calotta di specie  $d$  si denota con  $M_d(n, q)$ .

Uno dei problemi fondamentali nello studio delle  $(k, d)$ -calotte di  $PG(n, q)$  è quello di valutare l'intero  $M_d(n, q)$ . Esso fu esplicitamente introdotto per la prima volta da *R. C. Bose* e *J. N. Srivastava* [17] in relazione a certe questioni di statistica studiate da *R. A. Fisher* ([38], [39]); successivamente lo stesso *Bose* ([15], [16], [17]) intuì le sue possibili applicazioni e connessioni con le teorie dei *disegni di esperimenti* e dei *codici* e gli diede il nome di *packing problem*. Segnaliamo che lo studio delle  $(k, d)$ -calotte è di fondamentale importanza nella teoria dei codici lineari. Purtroppo non abbiamo qui lo spazio per evidenziare le connessioni tra questi due campi. Ricordiamo soltanto che il cosiddetto *problema fondamentale della teoria dei codici lineari* è equivalente a quello del calcolo degli interi  $M_d(n, q)$ .

Il calcolo di  $M_d(n, q)$  è ancora oggi uno dei più studiati e difficili problemi combinatori della geometria su campi di Galois; al momento si conoscono risultati definitivi solo per valori particolari di  $d, n$  e  $q$ . Nel caso più semplice,  $d = 1$ , si richiede soltanto di trovare il massimo numero di punti di  $PG(n, q)$  a due a due distinti e quindi è

$$M_1(n, q) = |PG(n, q)| = q^n + q^{n-1} + \dots + q + 1.$$

Nel caso  $d = 2$ ,  $q = 2$ , si può provare che i punti non appartenenti ad un fissato iperpiano di  $PG(n, q)$  formano una calotta di specie 2 col massimo numero possibile di punti ([15], [72]), così è

$$M_2(n, 2) = 2^n.$$

Il caso  $d = 2$ ,  $q > 2$  è stato trattato nei paragrafi precedenti per le dimensioni  $n = 2, 3$  e non sono noti altri risultati in dimensioni superiori se non per  $(n, q) = (4, 3), (5, 3)$ ; più precisamente si ha (*G. Pellegrino* [61], *R. Hill* [42])

$$M_2(4, 3) = 20, \quad M_2(5, 3) = 56.$$

Per comodità del Lettore riportiamo la tabella dei valori di  $M_d(n, q)$  finora trovati.

| $n$   | $q$            | $d$ | $M_d(n, q)$           |
|-------|----------------|-----|-----------------------|
| $> 1$ |                | 1   | $\frac{q^{n+1}}{q-1}$ |
| $> 1$ | 2              | 2   | $2^n$                 |
| 2     | <i>pari</i>    | 2   | $q+2$                 |
| 2     | <i>dispari</i> | 2   | $q+1$                 |
| 3     | $> 2$          | 2   | $q^2+1$               |
| 4     | 3              | 2   | 20                    |
| 5     | 3              | 2   | 56                    |

Passiamo ora allo studio di  $M_n(n, q)$ , cioè del massimo numero di punti che può contenere un arco di  $PG(n, q)$ . Osserviamo che i punti fondamentali di un riferimento di  $PG(n, q)$  formano un arco, quindi è

$$M_n(n, q) \geq n + 2.$$

È possibile provare che tale disuguaglianza è in effetti una uguaglianza nel caso  $n \geq q - 1$ . Quando è  $2 < n < q - 1$ , risulta

$$M_n(n, q) \geq q + 1,$$

come mostra il seguente esempio.

ESEMPIO 6.2. – Sia  $X$  l'insieme dei  $q + 1$  punti di  $PG(n, q)$  appartenenti ad una *curva razionale normale*. Fissato un riferimento  $\Re = (E_0, E_1, \dots, E_n, E)$ , per esempio, non è restrittivo supporre

$$X = \{(1, t, t^2, \dots, t^n) : t \in GF(q)^*\} \cup \{E_n\}.$$

Si verifica che i punti di una tale curva di  $PG(n, q)$  sono a  $n + 1$  a  $n + 1$  indipendenti e quindi  $X$  è un arco. Nel caso della dimensione  $n = 2$ , tali archi sono esattamente le coniche non degeneri di  $PG(2, q)$ . ■

Quando è  $2 < n < q - 1$  non si conoscono esempi di  $k$ -archi con  $k > q + 1$  ad eccezione del caso  $n = q - 2$  con  $q$  pari; in tal caso risulta (J. A. Thas [80])

$$M_{q-2}(q-2, q) = q + 2.$$

Concludiamo questo paragrafo riportando una vecchia congettura che, sebbene molto accreditata e studiata, non è stata ancora provata.

CONGETTURA 6.3. – Siano  $n > 2$  e  $q > 2$ . Allora risulta

$$M_n(n, q) = \begin{cases} n + 2, & \text{se } n \geq q - 1; \\ n + 2, & \text{se } n = q - 2, q \text{ pari}; \\ q + 1, & \text{negli altri casi.} \end{cases}$$

## 7. – Blocking sets.

Siano  $X$  un insieme finito non vuoto ed  $\mathcal{F}$  una famiglia di sottoinsiemi di  $X$ .

DEFINIZIONE 7.1. – Un insieme  $B$  di elementi di  $X$  prende il nome di *blocking set* rispetto ad  $\mathcal{F}$ , o  $\mathcal{F}$ -blocking set, se  $B$  non contiene elementi di  $\mathcal{F}$  e ogni elemento di  $\mathcal{F}$  ha intersezione non vuota con  $B$ .

Un  $\mathcal{F}$ -blocking set  $B$  si dice *minimale* se  $B \setminus \{b\}$  non è un blocking set, per ogni elemento  $b \in B$ . Si dice invece che  $B$  è di *ordine minimo* se  $X$  non contiene  $\mathcal{F}$ -blocking set con un numero di punti minore di quello di  $B$ . ■

DEFINIZIONE 7.2. – Se  $X$  è l'insieme dei punti di un piano affine o proiettivo finito  $\pi$ , un blocking set rispetto alla famiglia di tutte le rette di  $\pi$  si chiama *blocking set di  $\pi$* . ■

Nel seguito esporremo alcuni risultati relativi ai blocking set dei piani affini e proiettivi su un campo di Galois.

Fissati  $X$  e la famiglia  $\mathcal{F}$ , uno dei problemi fondamentali della teoria dei blocking set è quello di *calcolare il minimo ordine di un  $\mathcal{F}$ -blocking set e descrivere la struttura degli  $\mathcal{F}$ -blocking set di minima cardinalità*. Tale problema, e la stessa nozione di blocking set, trovano le loro motivazioni iniziali in una serie di conferenze tenute a Princeton agli inizi degli anni '50 da L. S. Shapley allo scopo di generalizzare le teorie di J. von Neumann e O. Morgenstern contenute nel loro famoso libro del 1947 dal titolo *Theory of games and economic behavior* [56]. Le idee sviluppate da Shapley si rivelarono particolarmente utili ed interessanti nel caso in cui la famiglia  $\mathcal{F}$  era l'insieme di tutti i sottospazi di fissata dimensione in uno spazio affine o proiettivo su un campo di Galois. Nacque così l'esigenza di studiare i blocking set negli spazi affini e proiettivi e

il primo articolo sull'argomento, che si deve a *M. Richardson* [65], risale al 1956. In questo lavoro viene per la prima volta posto esplicitamente il problema di calcolare la minima cardinalità di un blocking set rispetto alla famiglia dei sottospazi di una fissata dimensione in  $PG(n, q)$  e, per quanto riguarda i piani, viene provato che 6 è il minimo numero di punti di un blocking set di  $PG(2, 3)$ . Più di dieci anni dopo, queste tematiche vennero riprese da *J. di Paola*, che in [58], [59] determinò gli ordini minimi dei blocking set nei piani proiettivi d'ordine 4, 5, 7, 8, 9 e, nei casi 3, 4, 5, 9 descrisse anche la struttura dei blocking set corrispondenti. Lo studio dei blocking set ha poi assunto l'aspetto di una vera e propria teoria con i primi lavori e risultati di *A. A. Bruen* [20], [21]. Per maggiori informazioni sui legami tra la teoria dei giochi e quella dei blocking set si consiglia l'articolo [6].

ESEMPIO 7.3. – Sia  $\alpha_n$  un piano affine finito d'ordine  $n$ . L'unione  $X$  di due rette distinte e incidenti di  $\alpha_n$  ha ordine  $2n - 1$  ed è ad intersezione non vuota con ogni retta. ■

ESEMPIO 7.4. – Sia  $\alpha_n$  un piano affine finito d'ordine  $n$ . Siano  $l, m$  due rette distinte e incidenti di  $\alpha_n$ ,  $a$  un punto non appartenente ad  $l \cup m$ . Siano  $a_m$  la proiezione di  $a$  su  $l$  nella direzione di  $m$  e  $a_l$  la proiezione di  $a$  su  $m$  nella direzione di  $l$ . Detto  $b$  un punto della retta  $a_m a_l$  diverso da  $a_m$  e  $a_l$ , l'insieme

$$B = (l \setminus \{a_m\}) \cup (m \setminus \{a_l\}) \cup \{a, b\}$$

è un blocking set minimale di  $\alpha_n$  con  $2n - 1$  punti. ■

ESEMPIO 7.5. – Sia  $\pi_n$  un piano proiettivo finito d'ordine  $n$ . Se  $n$  è un quadrato, i sottopiani di Baer di  $\pi_n$  sono blocking set minimali d'ordine  $n + \sqrt{n} + 1$ . In particolare,  $PG(2, q)$  è un blocking set minimale di  $PG(2, q^2)$  d'ordine  $q^2 + q + 1$ . ■

ESEMPIO 7.6. – Sia  $\pi_n$  un piano proiettivo finito d'ordine  $n$ . Se  $n$  è un quadrato, gli archi hermitiani di  $\pi_n$ , cioè gli  $(n\sqrt{n} + 1)$ -insiemi di classe  $(1, \sqrt{n} + 1)$ , sono blocking set minimali. In particolare le curve hermitiane  $H(2, q)$  di  $PG(2, q)$  risultano archi hermitiani e, quindi, sono blocking set minimali d'ordine  $q\sqrt{q} + 1$ . ■

DEFINIZIONE 7.7. – Sia  $X$  un insieme non vuoto di punti di  $AG(2, q)$ . Un punto  $a \notin X$  prende il nome di *nucleo* di  $X$  se ogni retta passante per  $a$  è ad intersezione non vuota con  $X$ . L'insieme dei nuclei di  $X$  si denota con  $N(X)$ . ■

OSSERVAZIONE 7.8. – Sia  $X$  un insieme non vuoto di punti di  $AG(2, q)$ . Risulta  $N(X) = AG(2, q) \setminus X$  se, e soltanto se,  $X$  è un blocking set di  $AG(2, q)$ . ■

OSSERVAZIONE 7.9. – Sia  $a$  un nucleo di un insieme  $X$  di punti di  $AG(2, q)$ . Allora ogni retta per  $a$  interseca  $X$  esattamente in un punto se, e soltanto se,  $|X| = q + 1$ . ■

Descriviamo un procedimento, dovuto ad *A. Blokhuis*, che permette di calcolare la migliore limitazione per il numero di nuclei che può avere un insieme di punti  $X$ .

Sia  $AG(2, q)$  il piano affine ottenuto da  $PG(2, q)$  eliminando i punti di una sua fissata retta  $l_\infty$  e denotiamo con  $(x, y)$  le coordinate affini di punto in  $AG(2, q)$  in un riferimento proiettivo  $\{E_0, E_1, E_2, E\}$  di  $PG(2, q)$  nel quale la retta  $l_\infty$  abbia equazione  $x_2 = 0$ .

Sia  $GF(q^2) = GF(q)[j]$  il campo di Galois ottenuto aggiungendo a  $GF(q)$  una radice  $j$  di un polinomio di secondo grado  $f(x) \in GF(q)[x]$  irriducibile su  $GF(q)$  e, con abuso di notazione e di linguaggio, identifichiamo i punti di  $AG(2, q)$  con gli elementi di  $GF(q^2)$  mediante la seguente funzione biunivoca

$$P = (x, y) \in AG(2, q) \rightarrow x + jy \in GF(q^2).$$

È allora possibile provare il seguente teorema.

PROPOSIZIONE 7.10 (*A. Blokhuis* [10]). – Sia  $x = (x_1, x_2, \dots, x_{q+n})$ ,  $0 < n \leq q$ , una successione di  $q + n$  elementi di  $GF(q^2)$  contenente tutte le  $q + 1$  radici  $(q + 1)$ -esime dell'unità di  $GF(q^2)$ . Allora risulta

$$\sigma_n(x) = \sum_{0 < j_1 < j_2 < \dots < j_n} x_{j_1} x_{j_2} \dots x_{j_n} = 0.$$

A questo punto supponiamo  $X = \{x_1, x_2, \dots, x_{q+n}\}$  con  $n \leq q$  e consideriamo il polinomio  $F_X(t) \in GF(q^2)[t]$  definito da

$$F_X(t) = \sigma_n((t - x_1)^{q-1}, (t - x_2)^{q-1}, \dots, (t - x_{q+n})^{q-1}).$$

Il coefficiente di  $t^{n(q-1)}$  in  $F_X(t)$  è

$$\binom{q+n}{n},$$

che, come si prova facilmente, non è un multiplo di  $p$ , la caratteristica di  $GF(q)$ ; pertanto  $F_X(t)$  ha grado  $n(q-1)$ .

Detto  $a$  un nucleo di  $X$ , osserviamo che  $(x - a)^{q-1}$  è una radice  $(q + 1)$ -esima dell'unità in  $GF(q^2)$ . Allora, poiché ogni retta per  $a$  ha almeno un punto su

$X$ , si ha che la successione

$$((a - x_1)^{q-1}, (a - x_2)^{q-1}, \dots, (a - x_{q+n})^{q-1})$$

contiene tutte le radici  $(q+1)$ -esime dell'unità di  $GF(q^2)$  e la prop. 7.10 assicura che è  $F_X(a) = 0$ . Resta così provato che ogni nucleo di  $X$  è una radice del polinomio  $F_X(t)$  e quindi il numero di tali punti non può superare il grado di  $F_X(t)$ , cioè  $n(q-1)$ . Abbiamo, così, il seguente teorema.

PROPOSIZIONE 7.11 (A. Blokhuis [10]). – Sia  $X$  un insieme di  $q+n$  punti di  $AG(2, q)$  con  $n > 0$ . Allora risulta

$$|N(X)| \leq n(q-1).$$

Come corollari della prop. 7.11 si hanno subito i due seguenti teoremi.

COROLLARIO 7.12 (teorema di A. Blokhuis-H. A. Wilbrink [14]). – Se  $X$  è un insieme di  $q+1$  punti di  $AG(2, q)$  risulta

$$|N(X)| \leq q-1.$$

COROLLARIO 7.13 (teorema di R. Jamison [49]). – Se  $B$  è un blocking set di  $AG(2, q)$  risulta

$$|B| \geq 2q-1.$$

OSSERVAZIONE 7.14. – Il corollario 7.12 stabilisce che il massimo numero di nuclei di un insieme  $X$  di  $q+1$  punti di  $AG(2, q)$  è  $q-1$ . Un esempio di insieme  $X$  tale che  $|N(X)| = q-1$  si ottiene prendendo  $X = l \cup \{a\}$ , ove  $l$  è una retta e  $a$  un punto non appartenente ad  $l$ . Tale insieme, infatti, ha per nuclei tutti e soli i  $q-1$  punti della retta per  $a$  parallela ad  $l$  e diversi da  $a$ . A parte quelli appena descritti, si conosce soltanto un altro esempio in  $AG(2, 5)$  di insieme con  $q+1$  punti dotato di  $q-1$  nuclei e una congettura tuttora aperta vuole che questi siano gli unici possibili ([11], [12], [13], [55]). ■

OSSERVAZIONE 7.15. – Il corollario 7.13 dice che un blocking set di ordine minimo in  $AG(2, q)$  deve avere  $2q-1$  punti e la 7.4 prova che tali blocking set esistono. Il problema di descrivere tutti i blocking set di ordine minimo in  $AG(2, q)$  è tuttora aperto. ■

OSSERVAZIONE 7.16. – La limitazione di cui al corollario 7.13 per il numero di punti di un blocking set di  $AG(2, q)$  non vale in generale in un piano non desarguesiano. Per esempio, A. A. Bruen e M. J. de Resmini hanno costruito in [23] un blocking set d'ordine 16 per un piano affine non desarguesiano d'ordine 9. Al momento, per quanto riguarda i piani affini non desarguesiani, non è

nota alcuna limitazione significativa per il minimo numero di punti di un blocking set. ■

È da notare che il corollario 7.12 dà anche una elegante caratterizzazione delle rette esterne ad un insieme con almeno  $q$  punti, generalizzando a sottospazi arbitrari di  $PG(2, q)$  alcuni noti risultati sulle coniche di A. A. Bruen-J. A. Thas [24] e B. Segre-G. Korchmaros [76].

**PROPOSIZIONE 7.17.** – *In  $PG(2, q)$  siano  $X$  un insieme di punti d'ordine maggiore di  $q - 1$  ed  $L$  un insieme di punti disgiunto da  $X$ . Allora  $L$  è una retta esterna ad  $X$  se, e solo se, ogni retta incidente  $X$  interseca  $L$  in esattamente un punto.*

Passiamo, ora, a trattare i blocking set di un piano proiettivo finito  $\pi_n$  d'ordine  $n$ . Osserviamo che, se  $B$  è un blocking set in  $\pi_n$  e  $l$  una retta, risulta

$$|B \cap l| \leq |B| - n.$$

In particolare, se è  $|B| = n + k$ , allora ogni retta di  $\pi_n$  interseca  $B$  in al più  $k$  punti.

**DEFINIZIONE 7.18.** – Sia  $B$  un blocking set di  $\pi_n$  d'ordine  $n + k$ . Una retta  $l$  che intersechi  $B$  in  $k$  punti si chiama *retta di Rédei*. Un blocking set per il quale esista almeno una retta di Rédei prende il nome di *blocking set di Rédei*. ■

**ESEMPIO 7.19.** – Un sottopiano di Baer di  $\pi_n$  è un blocking set di Rédei e ogni retta secante è di Rédei. ■

**ESEMPIO 7.20.** – Un arco hermitiano di  $\pi_n$  non ammette rette di Rédei. ■

**ESEMPIO 7.21.** – Siano  $l$  una retta di  $\pi_n$ ,  $\alpha = \pi_n \setminus \{l\}$  e  $X$  un insieme di  $n$  punti non allineati di  $\alpha$ . Si denoti con  $D(X)$  l'insieme dei punti di  $l$  appartenenti ad almeno una retta secante  $X$  e si supponga  $D(X) \neq l$ .

L'insieme

$$B(X) = X \cup D(X)$$

è un blocking set minimale di  $\pi_n$  e  $l$  è una sua retta di Rédei. Il blocking set  $B(X)$  si chiama blocking set di Rédei associato ad  $X$ . Inoltre, ogni blocking set di Rédei minimale di  $\pi_n$  è del tipo precedentemente descritto. ■

Quello che segue può ritenersi il primo risultato significativo della teoria geometrica dei blocking set.

PROPOSIZIONE 7.22 (A. A. Bruen [20, 21]). – Se  $B$  è un blocking set di  $\pi_n$ , risulta

$$|B| \geq n + \sqrt{n} + 1 ,$$

l'uguaglianza avendosi se, e soltanto se,  $n$  è un quadrato e  $B$  un sottopiano di Baer.

Notiamo che esiste anche una limitazione superiore per il numero di punti di un blocking set minimale. Essa è fornita dal seguente teorema.

PROPOSIZIONE 7.23. – (A. A. Bruen-J. A. Thas [25]). – Se  $B$  è un blocking set minimale di  $\pi_n$ , risulta

$$|B| \leq n\sqrt{n} + 1 ,$$

l'uguaglianza avendosi se, e soltanto se,  $n$  è un quadrato e  $B$  un arco hermitiano.

Il teorema di Bruen (prop. 7.22) fornisce la migliore limitazione inferiore per il numero dei punti di un blocking set in un piano proiettivo finito d'ordine quadrato  $n$ . Trovare limitazioni nel caso  $n$  non sia un quadrato è un problema molto difficile ed è possibile ottenere qualche risultato soltanto se si considerano classi particolari di piani. Per esempio, nel caso il piano sia coordinabile su un campo finito, usando la teoria dei polinomi lacunosi di Rédei [64], è stato stabilito il seguente risultato.

PROPOSIZIONE 7.24 (A. Blokhuis [10]). – Siano  $q > 2$  e  $B$  un blocking set di  $PG(2, q)$ . Allora risulta

$$|B| \geq \begin{cases} p + \frac{p+3}{2} & \text{se } q = p \\ p^{2e} + p^e + 1 & \text{se } q = p^{2e}, e > 0 \\ p^{2e+1} + p^{e+1} + 1 & \text{se } q = p^{2e+1}, e > 0 . \end{cases}$$

Descriviamo, per finire, alcuni metodi per costruire blocking set minimali.

ESEMPIO 7.25. – In  $GF(q)$ , con  $q$  dispari, denotiamo con  $Q$  l'insieme dei suoi quadrati non nulli. Consideriamo in  $PG(2, q)$  l'insieme

$$B = \{(0, 1, -s), (-s, 0, 1), (1, -s, 0) : s \in Q\} \cup \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

e osserviamo che, se una retta interseca i lati del triangolo fondamentale nei punti  $(0, 1, -a)$ ,  $(-b, 0, 1)$ ,  $(1, -c, 0)$ , allora  $abc = 1 \in Q$ . Ne segue che almeno uno fra  $a$ ,  $b$ ,  $c$  è un quadrato in  $GF(q)$ ; da ciò segue che  $B$  è un blocking

set e si ha subito che

$$(9) \quad |B| = q + \frac{q+3}{2}.$$

Il blocking set appena costruito risulta di Rédei e prende il nome di *triangolo proiettivo*. ■

ESEMPIO 7.26. – Siano  $x_0, x_1, x_2$  coordinate proiettive di  $PG(2, q)$ ,  $l_\infty$  la retta di equazione  $x_2 = 0$  e  $AG(2, q) = PG(2, q) \setminus l_\infty$ . Per ogni funzione

$$f: GF(q) \rightarrow GF(q),$$

si consideri il grafico  $X_f$  di  $f$  in  $AG(2, q)$ , si ponga cioè

$$X_f = \{(a, f(a)) : a \in GF(q)\}.$$

Poiché  $D(X_f)$  è in corrispondenza biunivoca con l'insieme dei coefficienti angolari delle rette di  $AG(2, q)$  secanti  $X_f$ , il suo ordine è pari al numero di elementi dell'insieme

$$\left\{ \frac{f(a) - f(b)}{a - b} : a, b \in GF(q), a \neq b \right\}.$$

Ora, nell'ipotesi  $D(X_f) \neq l_\infty$ , poiché  $|X_f| = q$ , si può considerare il blocking set di Rédei  $B(X_f)$  associato a  $X_f$  e risulta

$$(10) \quad |B(X_f)| = q + |D(X_f)|.$$

Ne segue che i blocking set di Rédei minimali di  $PG(2, q)$  aventi  $l_\infty$  come retta di Rédei e non contenenti il punto  $(0, 1, 0)$  sono tutti del tipo  $B(X_f)$ .

OSSERVAZIONE 7.27. – Sia  $q = q_1^m$  e denotiamo con  $T = T_{q_1}$  la traccia di  $GF(q)$  su  $GF(q_1)$ , cioè

$$T: a \in GF(q) \rightarrow a + a^{q_1} + a^{q_1^2} + \dots + a^{q_1^{m-1}} \in GF(q_1) (\subset GF(q)).$$

In  $AG(2, q)$  sia  $X$  il grafico della funzione  $y = T(x)$  e sia  $B(X)$  il blocking set di Rédei di  $PG(2, q)$  associato a  $X$ . Allora risulta

$$(11) \quad |B(X)| = q + \frac{q}{q_1} + 1.$$

Le 7.25 e 7.27 provano che le limitazioni per il numero di punti di un blocking set trovate con la 7.24 sono le migliori possibili nei casi  $q = p$  e  $q = p^3$ ,  $p$  primo. Nel caso  $q = p^{2e+1}$ , con  $e > 1$ , non è noto se esistano o meno in  $PG(2, q)$  blocking set con  $p^{2e+1} + p^{e+1} + 1$  punti. Il Lettore interessato ad altri risultati sull'argomento può consultare [10].

## REFERENCES

- [1] E. ARTIN, *Geometric Algebra*, Interscience, 1957.
- [2] E. F. ASSMUS - E. F. KEY, *Designs and their Codes*, Cambridge Tracts in Mathematics, **103**, Cambridge University Press, 1992.
- [3] S. BALL - A. BLOKHUIS - F. MAZZOCCA, *Maximal arcs in Desarguesian planes of odd order do not exist*, Combinatorics, **17** (1997), 31-41.
- [4] A. BARLOTTI, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. U.M.I., **10**, Serie III (1955), 498-506.
- [5] L. BERARDI, *Algebra e teoria dei codici correttori*, Collana di matematica e statistica, Franco Angeli, 1994.
- [6] L. BERARDI - F. EUGENI, *Blocking sets e teoria dei giochi: origini e problematiche*, Atti Sem. Fis., Univ. Modena, **34** (1988), 165-196.
- [7] A. BEUTELSPACHER, *Einführung in die endliche geometrie*, vol. I, II, Wiessensnftsverlag, 1983.
- [8] A. BEUTELSPACHER - U. ROSENBAUM, *Projective Geometry*, Cambridge University Press, 1998.
- [9] N. L. BIGGS - A. T. WHITE, *Permutation Groups and Combinatorial Structures*, London Mathematical Society, Lecture Note Series, **33**, Cambridge University Press, 1979.
- [10] A. BLOKHUIS, *Blocking sets in Desarguesian planes*, Combinatorics, Paul Erdos is Eighty (vol. 2), Bolyai Society Mathematical Studies, Keszthely (Ungheria), 1-20, 1993.
- [11] A. BLOKHUIS - F. MAZZOCCA, *On maximal sets of nuclei in  $PG(2, q)$  and quasi-odd sets in  $AG(2, q)$* , Advances in finite geometries and designs, Oxford University Press, 35-46, 1991.
- [12] A. BLOKHUIS - F. MAZZOCCA, *Special point sets in  $PG(n, q)$  and the structure of sets with the maximal number of nuclei*, J. Geom., **41** (1991), 33-41.
- [13] A. BLOKHUIS - F. MAZZOCCA, *Lifts of nuclei in finite projective spaces*, L.M.S. Lecture Note Series, **191** (1993), 31-36.
- [14] A. BLOKHUIS - H. A. WILBRINK, *A characterization of exterior lines of certain sets of points in  $PG(2, q)$* , Geom. Dedicata, **23** (1987), 253-254.
- [15] R. C. BOSE, *Mathematical Theory of the Symmetrical Factorial Design*, Sankhya, **8** (1947), 107-166.
- [16] R. C. BOSE, *On some connections between the design of experiments and information theory*, Bull. Inst. Internat. Statist., **38** (1964), 257-271.
- [17] R. C. BOSE - J. N. SRIVASTAVA, *On a bound useful in the theory of factorial designs and error correcting codes*, Ann. Math. Statist., **35** (1964), 408-414.
- [18] A. E. BROUWER - A. SCHRIJVER, *The blocking number of an affine space*, J. of Combin. Theory (A), **24** (1978), 251-253.
- [19] M. R. BROWN, *Ovoids of  $PG(3, q)$ ,  $q$  even, with a conic section*, J. London Math. Soc., to appear.
- [20] A. A. BRUEN, *Baer subplanes and blocking sets*, Bull. Amer. Math. Soc., **76** (1970), 342-344.
- [21] A. A. BRUEN, *Blocking sets in finite projective planes*, SIAM J. of Appl. Math., **21** (1971), 380-392.
- [22] A. A. BRUEN, *Nuclei of sets of  $q + 1$  points in  $PG(2, q)$  and blocking sets of Rédei type*, J. of Combin. Theory (A), **55** (1990), 130-132.

- [23] A. A. BRUEN - M. J. DE RESMINI, *Blocking sets in affine planes*, Annals of Discrete Math., **18** (1983), 169-176.
- [24] A. A. BRUEN - J. A. THAS, *Flocks, chains and configurations in finite geometries*, Atti Accad. Naz. Lincei, Rend. Cl. Fis. e Mat., **59** (1975), 744-748.
- [25] A. A. BRUEN - J. A. THAS, *Blocking sets*, Geom. Ded., **6** (1977), 193-203.
- [26] P. J. CAMERON, *Four lectures on projective geometry*, in Finite Geometries, Lecture Notes in Pure and Applied Mathematics, **103** (1985), 27-65.
- [27] P. J. CAMERON - J. H. VAN LINT, *Designs, Graphs, Codes and their Links*, London Mathematical Society, Student Texts, **22**, 1991.
- [28] P. J. CAMERON - F. MAZZOCCA, *Bijections which preserve blocking sets*, Geom. Dedicata, **21** (1986), 219-229.
- [29] M. CERASOLI - F. EUGENI - M. PROTASI, *Elementi di matematica discreta*, Zanichelli, 1988.
- [30] W. CHEROWITZO, *Hyperovals in Desarguesian planes of even order*, Ann. Discrete Math., **37** (1988), 87-94.
- [31] W. CHEROWITZO - T. PENTTILÄ - I. PINNERI, *Flocks and ovals*, Geom. Dedicata, **60** (1996), 17-37.
- [32] W. CHEROWITZO - C. M. O'KEEFE - T. PENTTILÄ, *A unified construction of finite geometries in characteristic two*, Preprint.
- [33] A. COSSU, *Su alcune proprietà dei  $\{k, n\}$ -archi di un piano proiettivo sopra un corpo finito*, Rend. Mat. e Appl., **20** (1961), 271-277.
- [34] H. S. M. COXETER, *Projective geometry*, Springer, Second Edition, 1987.
- [35] P. DEMBOWSKI, *Finite geometries*, Springer-Verlag, 1968.
- [36] R. H. F. DENNISTON, *Some maximal arcs in finite projective planes*, J. Combinatorial Theory, **6** (1969), 317-319.
- [37] G. FELLEGERA, *Gli ovaloidi di uno spazio tridimensionale di Galois di ordine 8*, Atti Acc. Naz. Lincei, Rend. Cl. Sci. Mat., Fis., Nat., **32** (1962), 170-176.
- [38] R. A. FISHER, *The theory of confounding in factorial experiments in relation to the theory of groups*, Ann. Eugen. London, **11** (1942), 341-352.
- [39] R. A. FISHER, *A system confounding for factors with more than two alternatives giving completely orthogonal cubes and higher powers*, Ann. Eugen. London, **12** (1945), 283-290.
- [40] D. G. GLYNN, *Two new sequences of ovals in finite Desarguesian Planes of even order*, Combinatorial Mathematics X (Lecture Note in Math. 1036, Springer), edited by R. Casse, 217-229, 1983.
- [41] R. W. HAMMING, *Error detecting and error correcting codes*, Bell Syst. Tech. J., **29** (1950), 147-160.
- [42] R. HILL, *On the largest size of cap in  $S_{5,3}$* , Atti Accad. Naz. Lincei, Rend. Cl. Sc. Mat., Fis., Nat., **54** (1973), 378-384.
- [43] J. W. P. HIRSCHFELD, *Projective geometries over finite fields*, Oxford University Press, Oxford, 1979.
- [44] J. W. P. HIRSCHFELD, *Finite projective spaces of three dimensions*, Clarendon Press, Oxford, 1985.
- [45] J. W. P. HIRSCHFELD - J. A. THAS, *General Galois Geometries*, Oxford Mathematical Monographs, Oxford University Press, 1991.
- [46] D. R. HUGHES, *On  $t$ -designs and groups*, Amer. J. Math., **87** (1965), 761-768.
- [47] D. R. HUGHES - F. C. PIPER, *Projective planes*, Springer Verlag, 1973.
- [48] D. R. HUGHES - F. C. PIPER, *Design Theory*, Cambridge University Press, 1988.

- [49] R. JAMISON, *Covering finite fields with cosets of subspaces*, J. of Combin. Theory (A), **22** (1977), 253-266.
- [50] G. JÄRNEFELT - P. KUSTAANHEIMO, *An observation on finite geometries*, Comptes Rendus XI Congr. Math. Scand., Trondheim, 166-182, 1949.
- [51] G. KORCHMAROS - F. MAZZOCCA, *On  $(q + t)$ -arcs of type  $(0, 2, t)$  in a Desarguesian plane of order  $q(i)$* , Mathematical Proceedings of the Cambridge Philosophical Society, **108** (1990), 445-449.
- [52] C. W. H. LAM - L. THIEL - S. SWIERCZ - J. MCKAY, *The non-existence of ovals in a projective plane of order 10*, Discrete Math., **45** (1983), 319-321.
- [53] C. W. H. LAM - L. THIEL - S. SWIERCZ, *The non-existence of finite projective planes of order 10*, Canad. J. Math., **41** (1989), 1117-1123.
- [54] L. LUNELLI - M. SCE, *k-Archi completi nei piani proiettivi desarguesiani di rango 8 e 16*. Centro di Calcoli numerici, Politecnico di Milano, 1958.
- [55] F. MAZZOCCA, *Blocking sets with respect to special families of lines and nuclei of  $\theta_n$ -sets in finite  $n$ -dimensional projective and affine spaces*, Mitt. Math. Sem. Giessen, **201** (1991), 109-117.
- [56] J. VON NEUMANN - O. MORGENSTERN, *Theory of games and economic behavior*, Princeton, 1947.
- [57] G. PANELLA, *Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito*, Boll. U.M.I., **10**, Serie III (1955), 507-513.
- [58] J. DI PAOLA, *On a restricted class of block design games*, Canadian J. Math., **18** (1966), 225-236.
- [59] J. DI PAOLA, *On minimum blocking coalitions in small projective games*, SIAM J. of Appl. Math., **17** (1969), 378-392.
- [60] S. E. PAYNE, *A new infinite family of generalized quadrangles*, Congr. Numer., **49** (1985), 115-128.
- [61] G. PELLEGRINO, *Sul massimo ordine delle calotte in  $S_{4,3}$* , Matematiche (Catania), **25** (1970), 1-9.
- [62] T. PENTTILÄ - G. F. ROYLE, *Sets of type  $(m, n)$  in the affine and projective planes of order nine*, Designs, Codes and Cryptography, **6** (1995), 229-245.
- [63] B. QVIST, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fenn., Ser. A, **134**, 1952.
- [64] L. RÉDEI, *Lacunary polynomials over finite fields*, North Holland, Amsterdam, 1973.
- [65] M. RICHARDSON, *On finite projective games*, Proc. Amer. Math. Soc., **7** (1956), 458-465.
- [66] M. SCAFATI - G. TALLINI, *Geometria di Galois e teoria dei codici*, CISU, Roma, 1995.
- [67] B. SEGRE, *Lezioni di geometria moderna*, vol. I, Zanichelli, Bologna, 1948.
- [68] B. SEGRE, *Sulle ovali dei piani lineari finiti*, Atti Acc. Naz. Lincei, Rend. Cl. Sci. Mat., Fis., Nat., **17** (1954), 141-142.
- [69] B. SEGRE, *Ovals in finite projective planes*, Canad. J. Math., **7** (1955), 414-416.
- [70] B. SEGRE, *Sui  $k$ -archi nei piani finiti di caratteristica due*, Rev. Math. Pures Appl., **2** (1957), 289-300.
- [71] B. SEGRE, *On complete caps and ovaloids in three dimensional Galois spaces of characteristic two*, Acta Arith., **5** (1959), 315-332.
- [72] B. SEGRE, *Le geometrie di Galois*, Ann. Mat. Pura e Appl., **48** (1959), 1-97.
- [73] B. SEGRE, *Lectures on modern geometry*, Ed. Cremonese, Roma, 1961.

- [74] B. SEGRE, *Ovali e curve  $\sigma$  nei piani di Galois di caratteristica due*, Atti Acc. Naz. Lincei, Rend. Cl. Sci. Mat., Fis., Nat., **33** (1962), 785-790.
- [75] B. SEGRE - U. BARTOCCI, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith., **18** (1971), 423-449.
- [76] B. SEGRE - G. KORCHMAROS, *Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica*, Atti Accad. Naz. Lincei, Rend. Cl. Fis. e Mat., **62** (1977), 1-7.
- [77] G. TALLINI, *Sulle  $k$ -calotte di uno spazio lineare finito*, Ann. Mat., **42** (1956), 119-164.
- [78] G. TALLINI, *Partial line spaces and algebraic varieties*, Symposia Mathematica, **XXVIII** (1986), 203-217.
- [79] G. TALLINI, *Teoria dei  $k$ -insiemi in uno spazio di Galois. Teoria dei codici correttori*, Quaderno n. 64, Sem. Geom. Comb. Dip. Mat. Univ. Roma La Sapienza, 1985.
- [80] J. A. THAS, *Connection between the Grassmannian  $G_{k-1; n}$  and the set of the  $k$ -arcs of the Galois space  $S_{n, q}$* , Rend. Mat., **2** (1969), 121-134.
- [81] J. A. THAS, *Some results concerning  $\{(q+1)(n-1); n\}$ -arcs and  $\{(q+1)(n-1)+1; n\}$ -arcs in finite projective planes of order  $q$* , J. Comb Theory, Ser. A, **19** (1975), 228-232.
- [82] J. TITS, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki, **210**, 1960.
- [83] J. TITS, *Ovoides et groupes du Suzuki*, Arch. Math., **13** (1962), 187-198.
- [84] J. TITS, *Un propriété caractéristique des ovoides associés aux groupes de Suzuki*, Arch. Math., **17** (1966), 136-153.
- [85] V. D. TONCHEV, *Combinatorial Configurations*, Longman Scientific & Technical, 1988.

Dipartimento di Matematica, Seconda Università degli Studi di Napoli,  
Via Vivaldi 43 - 81100 Caserta, Italia  
e-mail: francesco.mazzocca@unina2.it