

PARTE SECONDA

ELEMENTI DI GEOMETRIA SU CAMPI DI GALOIS

La geometria sui campi di Galois costituisce una delle aree piú vaste ed importanti della combinatoria. Il suo interesse, a parte quello intrinseco dovuto soprattutto alla bellezza ed all'eleganza dei risultati, é nato ed é in un continuo crescendo a causa delle innumerevoli e sorprendenti applicazioni, sia in diversi campi della matematica che in teorie maggiormente coinvolte in problemi piú concreti, come la statistica, la teoria dei codici e la teoria dei giochi. La vastità della letteratura esistente ci ha ovviamente costretti ad una forte selezione tra i possibili argomenti da presentare. Abbiamo cosí limitato la nostra attenzione ad alcuni problemi classici, molti dei quali non ancora completamente risolti, e tra questi abbiamo maggiormente approfondito quelli che possono affrontarsi con l'uso di tecniche polinomiali.

Nei capitoli che seguono avremo modo di studiare diverse applicazioni degli argomenti che esporremo alla teoria dei *disegni* e a quella dei *codici lineari*.

Capitolo 8

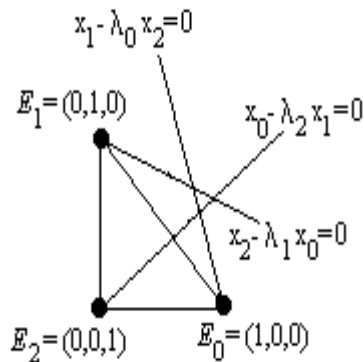
Archi e calotte di ordine massimo

8.1 Ovali ed iperovali in $PG(2, q)$

In questo paragrafo e nel successivo riterremo fissato un riferimento proiettivo $\mathfrak{R} = (E_0, E_1, E_2, E)$ di $PG(2, q)$. Denotate con (x_0, x_1, x_2) le coordinate proiettive di un generico punto di $PG(2, q)$, osserviamo che le rette distinte dagli assi coordinati e contenenti E_0, E_1, E_2 hanno 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 λ_j sarà detto *coordinata* in \mathfrak{R} della retta nell'equazione della quale compare.

Osserviamo ancora che, se consideriamo una retta ℓ_i per E_i di coordinata λ_i , per $i = 0, 1, 2$, allora ℓ_0, ℓ_1, ℓ_2 formano fascio se, e soltanto se

$$\det \begin{pmatrix} 0 & 1 & -\lambda_0 \\ -\lambda_1 & 0 & 1 \\ 1 & -\lambda_2 & 0 \end{pmatrix} = 1 - \lambda_0 \lambda_1 \lambda_2 = 0,$$

cioé se, e soltanto se,

$$\lambda_0 \lambda_1 \lambda_2 = 1. \quad (8.1)$$

Ne segue che, se un punto M non appartiene agli assi coordinati, le coordinate μ_0, μ_1, μ_2 delle rette passanti rispettivamente per M e E_0, E_1, E_2 verificano la relazione

$$\mu_0 \mu_1 \mu_2 = 1. \quad (8.2)$$

Nel seguito, se K é 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 $\alpha_j, \beta_j, \gamma_j$, $j = 1, 2, \dots, t$.

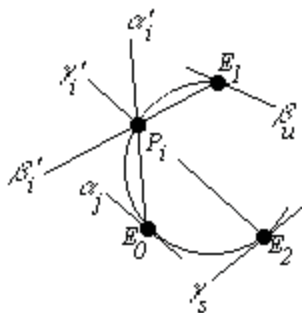
PROPOSIZIONE 8.1.1. (*lemma delle tangenti*) Sia K un k -arco di $PG(2, q)$ contenente i punti E_0, E_1, E_2 e siano $\alpha_j, \beta_j, \gamma_j$, $j = 1, 2, \dots, t$, rispettivamente le coordinate delle rette tangenti a K in E_0, E_1, E_2 . Allora risulta

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

In particolare, se Ω é un'ovale di $PG(2, q)$ e le tre rette tangenti nei punti E_0, E_1, E_2 hanno rispettivamente coordinate α, β, γ , risulta

$$\alpha \beta \gamma = -1. \quad (8.3)$$

DIMOSTRAZIONE. Denotiamo con P_i , $i = 1, 2, \dots, k-3$, i punti di K diversi da E_0, E_1, E_2 , e con $\alpha'_i, \beta'_i, \gamma'_i$ rispettivamente le coordinate delle rette per P_i e E_0, E_1, E_2 .



Poiché ogni retta per il punto E_i é tangente o secante K , abbiamo che

$$F_q^* = \{\alpha_1, \dots, \alpha_t, \alpha'_1, \dots, \alpha'_{k-3}\} = \\ \{\beta_1, \dots, \beta_t, \beta'_1, \dots, \beta'_{k-3}\} = \{\gamma_1, \dots, \gamma_t, \gamma'_1, \dots, \gamma'_{k-3}\}.$$

Allora dalla 4.3 segue che

$$-1 = \prod_{\alpha \in F_q^*} \alpha \prod_{\beta \in F_q^*} \beta \prod_{\gamma \in F_q^*} \gamma = \prod_{\alpha, \beta, \gamma \in F_q^*} \alpha \beta \gamma = \prod_{j=1}^t \alpha_j \beta_j \gamma_j \prod_{i=1}^{k-3} \alpha'_i \beta'_i \gamma'_i$$

e, essendo (cfr. 8.2)

$$\alpha'_i \beta'_i \gamma'_i = 1, \text{ per ogni } i,$$

risulta

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

come volevamo dimostrare. □

PROPOSIZIONE 8.1.2. *Siano Ω un'ovale di $PG(2, q)$ con q dispari, P_0, P_1, P_2 tre punti di Ω e ℓ_0, ℓ_1, ℓ_2 rispettivamente le tangenti ad Ω nei tre punti assegnati. Allora, posto*

$$T_0 = \ell_1 \cap \ell_2, \quad T_1 = \ell_2 \cap \ell_0, \quad T_2 = \ell_0 \cap \ell_1,$$

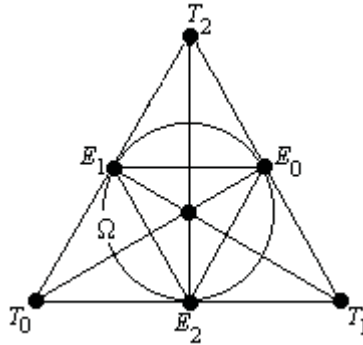
le rette P_0T_0, P_1T_1, P_2T_2 formano fascio.

DIMOSTRAZIONE. Non é restrittivo supporre che P_0, P_1, P_2 siano rispettivamente uguali ai punti fondamentali del riferimento E_0, E_1, E_2 . In queste ipotesi, dette α, β, γ le coordinate rispettivamente di ℓ_0, ℓ_1, ℓ_2 , abbiamo

$$T_0 = (\gamma, 1, \beta\gamma), \quad T_1 = (\gamma\alpha, \alpha, 1), \quad T_2 = (1, \alpha\beta, \beta)$$

e le rette E_0T_0, E_1T_1, E_2T_2 hanno rispettivamente equazione

$$x_2 - \beta\gamma x_1 = 0, \quad x_0 - \gamma\alpha x_2 = 0, \quad x_1 - \alpha\beta x_0 = 0.$$



Allora l'asserto segue dalle 8.1 e 8.3. □

PROPOSIZIONE 8.1.3. *(teorema di B.Segre) Ogni ovale Ω di $PG(2, q)$, con q dispari, é una conica.*

DIMOSTRAZIONE. Mantenendo le notazioni usate per la precedente proposizione, possiamo supporre che il punto unitario E del riferimento \mathfrak{R} coincida con il punto di intersezione delle

rette E_0T_0, E_1T_1, E_2T_2 ; cosí 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_0T_0, E_1T_1, E_2T_2 hanno rispettivamente equazione

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

e risulta

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

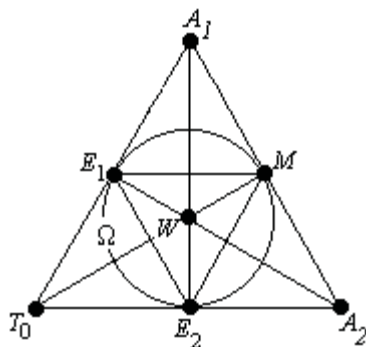
Sia ora $M = (m_0, m_1, m_2)$ un punto di Ω diverso da E_0, E_1, E_2 e sia

$$\mu_0x_0 + \mu_1x_1 + \mu_2x_2 = 0$$

l'equazione dell'unica retta ℓ tangente ad Ω in M ; osserviamo che ogni μ_i é diverso da zero perché nessuno dei punti E_i appartiene ad ℓ . In forza della 8.1.2 relativamente al triangolo ME_1E_2 , abbiamo che le rette congiungenti i punti M, E_1, E_2 rispettivamente con i punti $T_0 = \ell_1 \cap \ell_2, A_2 = \ell_2 \cap \ell, A_1 = \ell \cap \ell_1$ 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_1A_2, E_2A_1 hanno rispettivamente equazione

$$(\mu_0 - \mu_1)x_0 + \mu_2x_2 = 0, \quad (\mu_0 - \mu_2)x_0 + \mu_1x_1 = 0$$

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

$$\det \begin{pmatrix} \mu_1\mu_2 & (\mu_2 - \mu_0)\mu_2 & \mu_1(\mu_1 - \mu_0) \\ m_0 & m_1 & m_2 \\ -1 & 1 & 1 \end{pmatrix} = 0,$$

cioé

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

Osserviamo che é $\mu_0 - \mu_1 - \mu_2 \neq 0$, altrimenti il punto $T_0 = (-1, 1, 1)$ appartenerebbe ad ℓ e per esso passerebbero tre tangenti ad Ω , contro la 7.3.9. 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

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

cioé

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

Dividendo per 2 l'ultima uguaglianza, cosa possibile perché q é dispari, otteniamo

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

e da ciò segue subito che Ω coincide con la conica di equazione

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

come volevamo dimostrare. □

Il teorema appena provato non vale nel caso che q sia pari. In tale ipotesi, infatti, possiamo considerare un'iperovalle $\Omega = \Gamma \cup \{C\}$, ove Γ é una conica non degenera e C il suo nucleo. Allora,

detto M un punto di Γ , l'insieme $\Omega \setminus \{M\}$ é un'ovale avente q punti in comune con Γ e quindi non può essere una conica non appena é $q > 5$; infatti, due coniche distinte e non degeneri hanno al piú quattro punti in comune.

Quando q é pari, le iperovali che si ottengono aggregando ad una conica non degenerare il proprio nucleo si dicono *regolari*. Il primo esempio di iperovale non regolare fu trovato in $PG(2, 16)$ nel 1958 da *L.Lunelli* e *M.Sce* [58] mediante l'uso di un calcolatore.

ESERCIZIO 8.1.4. *Provare che tutte le iperovali di $PG(2, 2)$ e $PG(2, 4)$ sono regolari.*

Nel caso q pari, le iperovali di $PG(2, q)$ si caratterizzano mediante opportuni *polinomi di permutazione*, cioè polinomi $f \in GF(q)[x]$ le cui funzioni polinomiali sono permutazioni di $GF(q)$.

PROPOSIZIONE 8.1.5. (*B.Segre*, [75], [79]) *Siano q pari e $f \in GF(q)[x]$ un polinomio verificante le seguenti proprietà:*

- (i) *f é di permutazione, ridotto e $f(0) = 0, f(1) = 1$;*
- (ii) *per ogni $\alpha \in GF(q)$, $g_\alpha(x) = [f(x + \alpha) + f(\alpha)]/x$ é un polinomio di permutazione con $g_\alpha(0) = 0$.*

Allora l'insieme

$$\Omega(f) = \{(f(t), t, 1) : t \in GF(q)\} \cup \{(1, 0, 0), (0, 1, 0)\} \quad (8.4)$$

é un'iperovale di $PG(2, q)$. Viceversa, se Ω é un'iperovale di $PG(2, q)$, esistono 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 $PG(2, q)$ é dunque ricondotta alla ricerca dei polinomi $f(x)$ di cui alla 8.1.5 e questo problema é estremamente difficile e tuttora aperto. Per una interessante panoramica sull'argomento si consiglia [32]. Al momento, oltre ad alcuni esempi sporadici, sono note sette classi infinite di iperovali in $PG(2, 2^r)$; riportiamo di seguito gli o-polinomi $f(x)$ che le individuano:

- *Iperovals regolari:* $f(x) = x^2$;
- *Iperovals di traslazione:* $f(x) = x^{2^n}$, con $MCD(n, r) = 1$;
- *Iperovals di B.Segre:* $f(x) = x^6$, nel caso r dispari;
- *Iperovals di Glynn I:* $f(x) = x^{3\sigma+4}$, nel caso r dispari e $\sigma = 2^{(r+1)/2}$;
- *Iperovals di Glynn II:* $f(x) = x^{\sigma+\lambda}$, nel caso r dispari, $\sigma = 2^{(h+1)/2}$, $\lambda = 2^m$ se $r = 4m - 1$ e $\lambda = 2^{3m+1}$ se $r = 4m + 1$;
- *Iperovals di Payne:* $f(x) = x^{1/6} + x^{3/6} + x^{5/6}$, nel caso r dispari;
- *Iperovals di Subiaco:* $f(x) = \frac{d^2(x^4+x)+d^2(1+d+d^2)(x^3+x^2)}{(x^2+dx+1)^2} + x^{1/2}$, con $T_r(1/d) = 1$ e $d^2 + d + 1 \neq 0$.

8.2 Ovaloidi in $PG(3, q)$

Sia $PG(3, q)$ lo spazio proiettivo tridimensionale sul campo di Galois $GF(q)$.

DEFINIZIONE 8.2.1. Un insieme di k punti di $PG(3, q)$ prende il nome di *calotta di ordine k* , o *k -calotta*, se i suoi punti sono a tre a tre non allineati. \square

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

$$k \leq q^2 + q + 2. \quad (8.5)$$

DEFINIZIONE 8.2.2. Una k -calotta si dice *completa* se non è contenuta in una $(k+1)$ -calotta; nel caso contrario si dice *incompleta*. \square

ESEMPIO 8.2.3. L'insieme dei $q^2 + 1$ punti di una quadrica ellittica di $PG(3, q)$ è una $(q^2 + 1)$ -calotta massimale (cfr.6.6.18). \square

ESEMPIO 8.2.4. L'insieme dei punti di $PG(3, 2)$ non appartenenti ad un piano fissato è una 8-calotta massimale. Da notare che, in questo caso, l'ordine della calotta è il massimo consentito dalla (8.5). \square

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 π 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 π . In corrispondenza dei tre casi descritti il piano π si dirà *esterno*, *tangente* o *secante* \mathcal{K} .

PROPOSIZIONE 8.2.5. Siano q dispari 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} .

DIMOSTRAZIONE. Detti ℓ una retta secante \mathcal{K} e π_j , $j = 1, 2, \dots, q+1$, i piani per ℓ , denotiamo con n_j il numero dei punti di $\pi_j \cap \mathcal{K}$ non appartenenti ad ℓ . Poiché $\pi_j \cap \mathcal{K}$ è un $(n_j + 2)$ -arco di π_j , risulta

$$n_j \leq q - 1$$

e, tenendo presente che gli insiemi $\pi_j \setminus \ell$ formano una partizione di $PG(3, q) \setminus \ell$,

$$k - 2 = \sum_{j=1}^{q+1} n_j \leq (q+1)(q-1) = q^2 - 1, \quad (8.6)$$

cioè $k \leq q^2 + 1$.

Se $k = q^2 + 1$ e π é un piano con due punti distinti A, B su \mathcal{K} , diciamo ℓ la retta per A e B . Allora, ragionando come nella prima parte della dimostrazione, dalla 8.6 otteniamo $n_j = q - 1$, per ogni $j = 1, 2, \dots, q + 1$, e cioè

$$|\mathcal{K} \cap \pi| = q + 1.$$

Ora, sempre nell'ipotesi $k = q^2 + 1$, se π é un piano contenente due rette ℓ, m tangenti a \mathcal{K} in un punto P , esso deve essere tangente a \mathcal{K} ; altrimenti $\mathcal{K} \cap \pi$ sarebbe un $(q + 1)$ -arco di π con le rette ℓ, m entrambi tangenti in P e ciò é assurdo. L'asserto é cosí completamente provato. \square

PROPOSIZIONE 8.2.6. *Sia q pari. Allora una k -calotta \mathcal{K} di $PG(3, q)$ é priva di rette tangenti se, e soltanto se, $q = 2$, $k = 8$ e \mathcal{K} é il complementare di un piano (cfr.8.2.4).*

DIMOSTRAZIONE. Supponiamo \mathcal{K} priva di rette tangenti. Allora \mathcal{K} contiene esattamente $q^2 + q + 2$ punti e il numero delle rette secanti \mathcal{K} é

$$\binom{q^2 + q + 2}{2} = \frac{1}{2}(q^2 + q + 2)(q^2 + q + 1).$$

Poiché tale numero é minore di quello delle rette di $PG(3, q)$, abbiamo che esiste una retta ℓ esterna a \mathcal{K} e ogni piano π per ℓ o é esterno a \mathcal{K} o interseca la nostra calotta in un $(q + 2)$ -arco; infatti, se un punto P appartiene a $\pi \cap \mathcal{K}$, ogni retta di π per P interseca \mathcal{K} in esattamente due punti. Ne segue che $k = q^2 + q + 2$ é un multiplo di $q + 2$, cioè é del tipo

$$k = q^2 + q + 2 = (q - 2)(q + 2) + 4 + (q + 2) = h(q + 2),$$

con h intero positivo, e

$$(q - 2) + \frac{4}{q + 2} + 1 = h.$$

Allora $\frac{4}{q+2}$ é un intero e, di conseguenza, é $q = 2$ e $k = 8$.

A questo punto osserviamo che $PG(3, 2) \setminus \mathcal{K}$ é un insieme di sette punti contenente la retta congiungente due suoi punti distinti arbitrari e, quindi, é un piano (cfr.6.2.4). L'asserto é cosí completamente provato. \square

PROPOSIZIONE 8.2.7. *Siano q pari e \mathcal{K} una k -calotta di $PG(3, q)$ con $k \geq q^2 + 1$. Allora ogni retta tangente a \mathcal{K} é contenuta in almeno un piano che interseca \mathcal{K} in un $(q + 1)$ -arco.*

DIMOSTRAZIONE. Sia ℓ una retta tangente a \mathcal{K} in un suo punto P e osserviamo che ogni piano per ℓ interseca \mathcal{K} in al piú $q + 1$ punti. Se nessuno di tali piani incontrasse \mathcal{K} in $q + 1$ punti, avremmo

$$q^2 \leq k - 1 \leq (q - 1)(q + 1) = q^2 - 1,$$

il che é assurdo. \square

PROPOSIZIONE 8.2.8. *Siano $q > 2$ pari 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} .

DIMOSTRAZIONE. Supponiamo che \mathcal{K} sia massimale e (cfr.(8.5) e prop.8.2.6)

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

Scelto un punto $P \in \mathcal{K}$, siano ℓ una retta tangente a \mathcal{K} in P e π un piano per ℓ che intersechi \mathcal{K} in un $(q+1)$ -arco Ω (cfr.prop.8.2.7). Detto N il nucleo di Ω , osserviamo che esiste almeno una retta m per N secante \mathcal{K} , altrimenti $\mathcal{K} \cup \{N\}$ sarebbe una $(k+1)$ -calotta, contro la massimalit  di \mathcal{K} . Ora, la retta m non   contenuta in π e ogni piano per m contiene una retta tangente ad Ω e quindi a \mathcal{K} . Ne segue che ognuno di tali piani interseca \mathcal{K} in al pi  $q+1$ punti e quindi  

$$q^2 - 1 \leq k - 2 \leq (q-1)(q+1) = q^2 - 1, \quad (8.7)$$

da cui ricaviamo $k = q^2 + 1$. Ne segue che ogni calotta di $PG(3, q)$ contiene al pi  $q^2 + 1$ punti.

Se $k = q^2 + 1$, ogni punto di \mathcal{K} appartiene ad esattamente $q+1$ rette tangenti. Inoltre dalla 8.7 ricaviamo che ogni piano α per m interseca \mathcal{K} in un $(q+1)$ -arco Ω_α e l'unica retta per N tangente ad Ω_α   contenuta in π . Ne segue che N appartiene ad esattamente $q+1$ rette tangenti \mathcal{K} e queste sono le rette per N contenute in π .

Osserviamo esplicitamente che la (8.7)   stata provata nella sola ipotesi che m sia una retta per N secante \mathcal{K} e quindi, ragionando in modo analogo, si ha che ogni piano contenente una retta per N secante K interseca K in un $(q+1)$ -arco.

Sia ora ℓ' una retta tangente a \mathcal{K} in P diversa da ℓ e sia β il piano di ℓ e ℓ' . Tale piano non pu  contenere un punto $T \in \mathcal{K}$ diverso da P , altrimenti la retta NT , non essendo contenuta in π , sarebbe secante \mathcal{K} e $\mathcal{K} \cap \beta$ sarebbe un $(q+1)$ -arco di β per P con ℓ e ℓ' tangenti distinte in P , un assurdo. Ne segue che le $q+1$ rette tangenti a \mathcal{K} in P appartengono tutte al piano β .

Per completare la dimostrazione, rimanendo nell'ipotesi $k = q^2 + 1$, consideriamo un piano τ contenente due punti distinti A, B di \mathcal{K} e osserviamo che, poich  le $q+1$ rette tangenti a \mathcal{K} in A giacciono sullo stesso piano, ogni piano per la retta AB deve contenere esattamente $q+1$ punti di \mathcal{K} . □

Mettendo insieme i risultati 8.2.5 e 8.2.8, abbiamo il seguente teorema.

PROPOSIZIONE 8.2.9. *Se   $q > 2$ 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 8.2.10. Una $(q^2 + 1)$ -calotta di $PG(3, q)$, $q > 2$, prende il nome di *ovaloide*. □

PROPOSIZIONE 8.2.11. *Sia \mathcal{K} un ovaloide di $PG(3, q)$. Allora in $PG(3, q)$ non esistono piani esterni a \mathcal{K} .*

DIMOSTRAZIONE. Detto ν il numero dei piani π secanti \mathcal{K} in $q + 1$ punti, facciamo il doppio conteggio delle possibili coppie $(\pi, \{A, B, C\})$, ove $\{A, B, C\}$ é un insieme di tre punti scelti in $\pi \cap \mathcal{K}$. Abbiamo cosí

$$\nu \binom{q+1}{3} = \binom{q^2+1}{3},$$

da cui ricaviamo

$$\nu = q^3 + q.$$

L'asserto segue, allora, tenendo presente che dei $q^3 + q^2 + q + 1$ piani di $PG(3, q)$ ve ne sono esattamente $q^2 + 1$ tangenti a \mathcal{K} . \square

Nel caso q dispari, usando il teorema di Segre 8.1.3, é possibile ottenere la seguente classificazione degli ovaloidi, trovata indipendentemente da *A.Barlotti* [3] e *G.Panella* [65].

PROPOSIZIONE 8.2.12. *Se q é dispari, ogni ovaloide di $PG(3, q)$ é una quadrica ellittica.*

ESERCIZIO 8.2.13. *Provare che, se q é dispari, ogni ovaloide \mathcal{K} di $PG(3, q)$ individua una polaritá π_Ω di $PG(3, q)$ i cui punti assoluti sono esattamente quelli di Ω .*

OSSERVAZIONE 8.2.14. Nel caso q pari la prop.8.2.12 é falsa. Il primo esempio di ovaloide diverso da una quadrica ellittica fu trovato in $PG(3, 8)$ da *B.Segre* nel 1959 [76]. Nel 1962 *J.Tits* ha trovato un esempio per ogni q potenza dispari di 2 [89]. Nel caso $q = 8$ l'esempio di Tits coincide con quello di Segre [40].

Fissato un ovaloide \mathcal{K} di $PG(3, q)$, sempre nell'ipotesi q pari, possiamo considerare la funzione biunivoca ψ che ad ogni piano π di $PG(3, q)$ associa il punto P_π di $PG(3, q)$ definito da

$$P_\pi = \begin{cases} P, & \text{se } |\pi \cap \mathcal{K}| = 1 \\ \text{nucleo di } \pi \cap \mathcal{K}, & \text{se } |\pi \cap \mathcal{K}| = q + 1 \end{cases}.$$

La funzione φ inversa della ψ é una polaritá di $PG(3, q)$ che, risultando $P \in \varphi(P)$, per ogni $P \in PG(3, q)$, é nulla. Ne segue che, pur potendo associare a \mathcal{K} la polaritá φ , questa non individua univocamente l'ovaloide \mathcal{K} , a differenza di quanto accade nel caso q dispari (cfr. 8.2.13). \square

ESERCIZIO 8.2.15. *Siano \mathcal{K} un ovaloide di $PG(3, q)$ e P un punto su \mathcal{K} . Siano \mathcal{P} l'insieme dei punti di \mathcal{K} diversi da P e \mathcal{L} l'insieme dei $(q + 1)$ -archi per P contenuti in \mathcal{K} e privati del punto P . Provare che $(\mathcal{P}, \mathcal{L})$ é un piano affine d'ordine q isomorfo ad $AG(2, q)$.*

8.3 (k, d) -calotte in $PG(n, q)$

Questo paragrafo é dedicato alla generalizzazione dei concetti esposti nei due precedenti.

DEFINIZIONE 8.3.1. 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 proprietá:

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

DEFINIZIONE 8.3.2. Una (k, d) -calotta K si dice *completa* se non é 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 $PG(n, q)$ é 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* [18] in relazione a certe questioni di statistica studiate da *R.A.Fisher* ([41], [42]); successivamente lo stesso *Bose* ([15], [16], [18]) intuí le sue possibili applicazioni e connessioni con le teorie dei *disegni di esperimenti* e dei *codici* e gli diede il nome di *packing problem*.

Il calcolo di $M_d(n, q)$ é ancora oggi uno dei piú 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 piú semplice, $d = 1$, si richiede soltanto di trovare il massimo numero di punti di $PG(n, q)$ a due a due distinti e quindi é

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

Nel caso $d = 2, q = 2$, si puó 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], [77]), cosí é

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

Il caso $d = 2, q > 2$ é stato trattato nei paragrafi precedenti per le dimensioni $n = 2, 3$ e non sono noti altri risultati in dimensioni superiori se non per $(n, q) = (4, 3), (5, 3)$; piú precisamente si ha (*G.Pellegrino* [68], *R.Hill* [47])

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

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

n	q	d	$M_d(n, q)$
> 1		1	$\frac{q^{n+1}-1}{q-1}$
> 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 é

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

Proveremo in seguito che tale disuguaglianza é in effetti una uguaglianza nel caso $n \geq q - 1$. Quando é $2 < n < q - 1$, risulta

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

come mostra il seguente esempio.

ESEMPIO 8.3.3. Un insieme X di $q + 1$ punti di $PG(n, q)$ si chiama *curva razionale normale* se esiste un riferimento $\mathfrak{R} = (E_0, E_1, \dots, E_n, E)$ nel quale risulta

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

Si verifica che i punti di ogni curva razionale normale X di $PG(n, q)$ sono a $n + 1$ a $n + 1$ indipendenti e quindi X é un arco. Nel caso della dimensione $n = 2$, tali archi sono esattamente le coniche non degeneri di $PG(2, q)$. \square

Quando é $2 < n < q - 1$ 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* [88])

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

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

CONGETTURA 8.3.4. *Siano $n > 2$ e $q > 2$. Allora risulta*

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