ISTITUTO DI MATEMATICA APPLICATA
FACOLTÀ DI INGEGNERIA
UNIVERSITA' DEGLI STUDI DE L'AQUILA

SEMINARIO DI GEOMETRIE COMBINATORIE

GIUSEPPE TALLINI

BLOCKING SETS NEI SISTEMI DI STEINER E d-BLOCKING SETS IN PG(r,q) ED AG(r,q)

QUADERNO N. 3
Maggio 1983

Centro Stampa "LA TECNICA"
L'AQUILA

QUADERNO N. 3

Maggio 1983

Pubblicazione realizzata con il contributo del Ministero della Pubblica Istruzione (fondi 60%) a cura di L. Berardi e di F. Eugeni dell'Istituto di Matematica Applicata dell'Universitá de L'Aquila. (depositato a norma di legge)

GIUSEPPE TALLINI

BLOCKING SETS NEI SISTEMI DI STEINER E d-BLOCKING SETS IN PG(r,q) ED AG(r,q)

INTRODUZIONE

Nel presente lavoro espongo risultati da me recentemente ottenuti sui blocking sets nei sistemi di Steiner e sui d-blocking sets negli spazi affini e proiettivi di Galois. Gli argomenti qui esposti sono stati oggetto di un ciclo di conferenze tenute nella primavera dell'83 presso l'Istituto di Matematica Applicata della Facolta` di Ingegneria dell'Universita` de L'Aquila. Ringrazio i professori L.Berardi e F.Eugeni che hanno curato la stesura del lavoro e l'Istituto di Matematica Applicata della Facolta` di Ingeneria che ha permesso la stampa del presente volume.

1. ALCUNE OSSERVAZIONI NEI SISTEMI DI STEINER

Richiamiamo brevemente per completezza la nozione di sistema di Steiner e le piu` importanti proprieta`.

Sia S un insieme finito non vuoto e $\mathscr{B}$ una famiglia propria e non vuota di parti di S dette blocchi. La coppia $(S,\mathscr{B})$ e` un sistema di Steiner $S(t,k,v)$ se sono verificate le seguenti condizioni:

(1.1) $\quad |S| = v \quad ; \quad \forall B \in \mathscr{B}\ , \quad |B| = k$

(1.2) Per t punti di S passa uno ed un sol blocco.

Supporremo nel seguito $t < k < v$.

Esempio 1. - Lo spazio proiettivo di Galois $PG(r,q)$, considerando come blocchi le rette, e` un $S(2,q+1,\theta_r)$.

Esempio 2. - Lo spazio affine di Galois $AG(r,q)$, considerando come blocchi le rette, e` un $S(2,q,q^r)$.

Esempio 3. - Lo spazio affine $AG(r,2)$, considerando come blocchi i piani, e` un $S(3,4,2^r)$.

Esempio 4. - In $PG(3,q)$ una (q^2+1)-calotta K (cioe` una uadrica ellittica se q e` dispari), considerando come blocchi le sezioni di K con piani non tangenti a K, e` un 3$(3,q+1,q^2+1)$.

Esempio 5. - Esiste un solo $S(5,8,24)$ a meno di isomorfismi. Il gruppo degli automorfismi di $S(5,8,24)$ e` il gruppo di Mathieu $M_{24}$, che e` un gruppo semplice sporadico.

Dato un $S(t,k,v)$, sia P un suo punto. Poniamo $S_P = S - \{P\}$ e consideriamo la famiglia $\mathcal{B}_P$ di parti di S_P definita da: $\mathcal{B}_P = \{B - \{P\} : B \in \mathcal{B}, P \in B\}$. La coppia $(S_P, \mathcal{B}_P)$ e` un $S(t-1, k-1, v-1)$ che prende il nome di contrazione o derivazione di $S(t,k,v)$ rispetto a P. Contraendo un $S(t,k,v)$ successivamente rispetto ai punti P_1, $P_2, \dots, P_s$, si ottiene un $S(t-s,k-s,v-s)$. Dato un $S(t,k,v)$, determiniamo $|\mathcal{B}|$. Sia N il numero delle coppie costituite da una t-pla di punti di S e da un blocco per essi. Si ha:

$$N = \binom{k}{t} |\mathcal{B}| = \binom{v}{t}$$

a cui

(1.3) $$r_0 = |\mathcal{B}| = \binom{v}{t} \Big/ \binom{k}{t}.$$

erivando rispetto ad $1,2,\dots,t$ punti di $S(t,k,v)$ si ottengono rispettivamente le:

$$r_1 = |\mathcal{B}_P| = \binom{v-1}{t-1} \Big/ \binom{k-1}{t-1}$$

$$r_2 = |\mathcal{B}_{P_1 P_2}| = \binom{v-2}{t-2} \Big/ \binom{k-2}{t-2}$$

....

$$r_{t-1} = |\mathcal{B}_{P_1 \dots P_{t-1}}| = \binom{v-t+1}{t-t+1} \Big/ \binom{k-t+1}{t-t+1} = \frac{v-t+1}{k-t+1}$$

$$r_t = |\mathcal{B}_{P_1 \dots P_t}| = 1,$$

che riassumiamo nella formula generale:

(1.4) $$r_s = |\mathcal{B}_{P_1 \dots P_s}| = \binom{v-s}{t-s} \Big/ \binom{k-s}{t-s}$$

Posto $r_0 = b = |\mathcal{B}|$, $r_1 = r$, dalla (1.4) per s=0 e s=1 si ottiene:

(1.5) $$vr = kb.$$

Perche` esista un $S(t,k,v)$ occorre che siano interi tutti gli r_s $(s=0,1,\dots,t-1)$. Per $t=2, k=3$ (sistemi di terne di Steiner) le condizioni necessarie precedenti sono anche sufficienti: un $S(2,3,v)$ esiste se, e solo se:

$$v \equiv 1 \text{ oppure } v \equiv 3 \bmod 6.$$

Si dice che un sistema $S(t,k,v)$ e` una estensione di una classe di $S(t-1,k-1,v-1)$, se la contrazione di $S(t,k,v)$ in un qualsiasi suo punto e` isomorfa ad un sistema della classe di $S(t-1,k-1,v-1)$. Piu` in generale si dice che $S(t,k,v)$ e` una estensione di grado s di una classe di $S(t-s,k-s,v-s)$, se la contrazione di $S(t,k,v)$ in una qualsiasi s-pla di punti e` isomorfa ad un sistema della classe.

Dato un $S(t,k,v)$, determiniamo le sue estensioni di grado t-2 proiettive, cioe` tali che per ogni (t-2)-pla di punti la contrazione, rispetto ad essi, sia un:

$$S(2,k-t+2,v-t+2) = S(2,q+1,q^2+q+1).$$

Deve necessariamente risultare:

$$k-t+2 = q+1, \quad v-t+2 = q^2+q+1,$$

da cui:

(1.6) $$k = q+t-1, \quad v = q^2+q+t-1.$$

Sostituendo nella (1.4) per $s=t-1, t-2, t-3$, i valori di v e k dati dalle (1.6) si ha:

7) $\binom{v-t+1}{1} / \binom{k-t+1}{1} = \theta_1$

8) $\binom{v-t+2}{2} / \binom{k-t+2}{2} = \theta_2$

9) $\binom{v-t+3}{3} / \binom{k-t+3}{3} = (q-1)(\theta_2 +4)+12/(q+2)$

endo essere tali numeri interi, segue che q+2 deve di-
ere 12. Allora, essendo $q \geq 2$, necessariamente risulta
,4,10, e, in forza delle (1.6), si ha:

10) q = 2   k=t+1; v=5+t; S(t,t+1,t+5)

11) q = 4   k=t+3; v=19+t; S(t,t+3,19+t)

12) q = 10   k=t+9; v=109+t; S(t,t+9,109+t)

Per t= 3 si ha:
q = 2 da' luogo all'S(3,4,8) = $AG_2(3,2)$ (rispetto ai
ni), unico a meno di isomorfismi;
q = 4 da' luogo all'S(3,6,22), anche esso unico, che
ottiene contraendo l'S(5,8,24) di Mathieu rispetto a
punti;
q = 10 da' luogo ad un S(3,12,112); la contrazione di
o rispetto ad un punto P e' un piano d'ordine 10 in
ogni blocco di S(3,12,112), non per P, e' una ovale;
ltra parte e' stato recentemente provato da Lam (cfr.
) che in un piano d'ordine 10, ammesso esistente, non
stono ovali. Ne segue che non esiste un S(3,12,112).
Per t=4, oltre i secondi membri delle (1.7), (1.8),
)), deve risultare intero anche il secondo membro
a (1.4) per s=t-4, cioe':

$$r_4 = \binom{v-t+4}{4} / \binom{k-t+4}{4}$$

ndo conto delle (1,6),...,(1,12), si ha:

q=2 ⟶ $r_4 = 2\cdot 3^2 \cdot 7/5$

q=4 ⟶ $r_4 = 23\cdot 11$; k=7 , v=23

c) q=10 ⟶ $r_4 = 113\cdot 28\cdot 37/13$

ne segue che un S(4,k,v), tale che la contrazione su due punti e' proiettiva, esiste solo se k=7, v=23.

Un siffatto S(4,7,23) puo' ottenersi contraendo rispetto ad un punto l'S(5,8,24) di Mathieu. Esso e' unico.

Per t=5, da quanto detto nel caso t=4, segue che un S(5,k,v), tale che la contrazione su 3 punti e' proiettiva, necessariamente e' tale che la contrazione in un punto e' un S(4,7,23). Di conseguenza deve essere k=8, v=24. Esiste (cfr. Esempio 5) un tale S(5,8,24) ed e' unico.

Per $t \geq 6$, se S(t,k,v) e' una estensione proiettiva di grado t-2, allora necessariamente deve essere una estensione di grado t-5 dell'S(5,8,24).

Proviamo che una tale estensione non esiste per t=6 e pertanto neanche per $t>6$, (poiche' l'esistenza di un S(t,k,v), con $t>6$, implicherebbe, contraendo rispetto a t-6 punti, l'esistenza di un S(6,k,v)).

In un eventuale S(6,k,v), la cui contrazione semplice e' un S(5,8,24), e' necessariamente k=9, v=25. Segue allora dalla (1.4):

$$r_0 = 25\cdot 23\cdot 11/3$$

che non e' intero.

Si ha allora:

I. Un S(t,k,v) e' una estensione proiettiva di grado t-2 solamente nei seguenti casi:

a) se t=3, esistono: l'S(3,4,8) isomorfo ad $AG_2(3,2)$ (rispetto ai piani); l'S(3,6,22), per esempio la contrazione di grado 2 dell'S(5,8,24);

b) se t=4, esiste l'S(4,7,23), per esempio la contrazione dell'S(5,8,24).

c) se t=5, esiste l'S(5,8,24).

d) se $t \geq 6$, non esistono sistemi di Steiner che siano estensioni di un piano proiettivo.

In particolare osserviamo che:

Dato un S(2,k,v), se esiste un blocco $B \in \mathcal{B}$ tale che ogni altro blocco $B' \in \mathcal{B}$ lo interseca, allora S(2,k,v) e' un piano proiettivo.

Infatti il numero dei blocchi per un punto $P(\notin B)$ coincide con il numero dei punti di B, allora $v=k(k-1)+1 = k^2-k+1$. Posto $k = q+1$, si ha $v= q^2+q-1$, onde $S(2,k,v)= S(2,q+1,q^2+q+1)$.

Proviamo che:

II. Sia $S(t,k,v)$, $t\geq 3$, un sistema di Steiner diverso da $S(5,8,24)$, $S(4,7,23)$, $S(3,6,22)$, $S(3,4,8)$. Allora, preso comunque un blocco $B \in \mathscr{B}$ e fissati t-2 punti $P_1, P_2, \ldots, P_{t-2}$ di B, esiste un blocco $B' \in \mathscr{B}$ che interseca B solo nei t-2 punti fissati.

Dimostrazione. La contrazione di $S(t,k,v)$ rispetto ai t-2 punti fissati e' un $S(2,k-t+2,v-t+2)$ che non e' un piano proiettivo, altrimenti, per la Prop. I, l'$S(t,k,v)$ dovrebbe coincidere con uno dei sistemi di Steiner esclusi per ipotesi. Esiste quindi un blocco di $S(2,k-t+2,v-t+2)$ che non incontra $B-\{P_1,\ldots, P_{t-2}\}$ e quindi esiste un $B'\in\mathscr{B}$ tale che $B'\cap B = \{P_1,\ldots, P_{t-2}\}$.

Sia ora A un (k+1)-arco (ovvero un insieme di k+1 punti a tre a tre non allineati) di un $S(2,k,v)$. Il numero delle 2-secanti e' $k(k+1)/2$. Per ogni punto $P \in A$ passano k rette 2-secanti e quindi r_1-k rette tangenti (ove $r_1=(v-1)/(k-1)$, si noti che e' sempre $r_1-k\geq 0$, il segno di eguaglianza avendosi se, e solo se, l'$S(2,k,v)$ e' un piano proiettivo); ne segue che il numero delle tangenti ad A e':

(1.13) $$(k+1)\,(r_1-k)\ .$$

Il numero t_0 delle rette esterne ad A e':

(1.14) $$t_0 = v(v-1)/k(k-1) - \binom{k+1}{2} -(r_1-k)(k+1)\ .$$

La condizione $t_0>0$, come subito si verifica, equivale a:

(1.15) $$2v^2-2v(1+k+k^2) + (k^4+k^2+2k)>0\ .$$

Per $k\geq 3$ risulta (Δ essendo il discriminante della (1.15)):

(1.16) $$\Delta=-k^4+2k^3+k^2-2k+1< 0\ .$$

Quindi $t_0>0$ per ogni k con $k\geq 3$, di conseguenza esistono sempre rette esterne ad un (k+1)-arco di $S(2,k,v)$.

Considerato ora un k-arco, in luogo delle (1.13), (1.14), (1.15), (1.16) si hanno rispettivamente le:

(1.17) $$k(r_1-k+1) = n^{ro} \text{ delle tangenti al k-arco}$$

(1.18) $$t_0=v(v-1)/k(k-1) - \binom{k}{2} -(r_1-k+1)k$$

(1.19) $$2v^2-2v(1+k^2) + k^2(k^2-2k+3)>0$$

(1.20) $$\Delta=-k^4+4k^3-4k^2+1 < 0 \quad \text{per } k\geq 3\ .$$

Ne segue che anche un k-arco di un $S(2,k,v)$ ammette rette esterne.

Proviamo che:

III. In $S(3,k,v)$, fissato comunque un blocco $B\in\mathscr{B}$ ed un punto $P\in S-B$, per P passa almeno un $B'\in\mathscr{B}$ con $B\cap B'=\emptyset$ (anzi il numero di tali blocchi e' t_0, dato dalla (1.14)).

Dimostrazione. In $S(3,k,v)$ si consideri un blocco B ed un punto $P\in S-B$ e si contragga l'$S(3,k,v)$ rispetto a P. Nella contrazione $S_P(2,k-1,v-1)$ l'insieme B e' un ((k-1)+1)-arco. Infatti ogni blocco di $S(3,k,v)$ incontra B in al piu' due punti, e cosi' ogni blocco per P, cioe' ogni retta di $S(2,k-1,v-1)$ incontra B in al piu' due punti. Poiche' il ((k-1)+1)-arco di S_P ammette rette esterne, esiste un blocco B' per P che non incontra B.

IV. In $S(t,k,v)$, $t\geq 4$, per ogni $B\in\mathscr{B}$ e per ogni $P_1, P_2, \ldots, P_{t-3}\in B$, esiste $B'\in\mathscr{B}$ tale che $B\cap B'= \{P_1,P_2,\ldots,P_{t-3}\}$.

Dimostrazione. In $S(t,k,v)$ si consideri un $B\in\mathscr{B}$ e t-3 punti $P_1,P_2,\ldots,P_{t-3}$ di B. Contraendo rispetto a $P_1,P_2,\ldots,P_{t-3}$ si ottiene un $S(3, k-t+3, v-t+3)$ e $B-\{P_1,\ldots,P_{t-3}\}$ e' un blocco di tale contrazione. Per la Prop. III esiste qualche blocco $B'-\{P_1,\ldots,P_{t-3}\}$ di $S(3,k-t+3,v-t+3)$, con $B'\in\mathscr{B}$ tale che

$$(B'-\{P_1,\ldots,P_{t-3}\})\cap(B-\{P_1,\ldots,P_{t-3}\})=\emptyset,$$

ovvero tale che $B\cap B' = \{P_1,P_2,\ldots,P_{t-3}\}$.

2. BLOCKING SETS NEI SISTEMI DI STEINER

Sia $(S,\mathscr{B})$ un sistema di Steiner $S(t,k,v)$ con $2\leq t<k<v$. Dicesi blocking set di $(S,\mathscr{B})$ un sottoinsieme C di S tale che ogni $B\in\mathscr{B}$ abbia qualche punto in comune con C e con S-C. Il complementare S-C di un blocking set C di $(S,\mathscr{B})$ e\` ancora un blocking set. Un blocking set C di $(S,\mathscr{B})$ dicesi irriducibile se per ogni punto $P\in C$ si ha che $C-\{P\}$ non e\` un blocking set, cioe\` se per ogni $P\in C$ passa almeno un $B\in\mathscr{B}$ unisecante C. In caso contrario C si dice riducibile. Si noti che C e\` riducibile se, e solo se, esiste un $P\in C$ tale che in $S_P(t-1,k-1,v-1)$ l'insieme $C-\{P\}$ e\` un blocking set. E\` evidente che ogni blocking set di $(S,\mathscr{B})$ contiene qualche blocking set irriducibile.

Siano m,n rispettivamente il minimo ed il massimo numero di punti che C ha in comune con B, al variare di B in $\mathscr{B}$. Si dira\` in tal caso anche che C e\` un $(c;m,n)$-insieme di $S(t,k,v)$ $(c=|C|,\ 1\leq m\leq n\leq k-1)$. Si definisce carattere di indice i di C il numero t_i dei blocchi che incontrano C in i punti esattamente $(i=m,\dots,n)$.
Computando in due modi diversi le coppie costituite da s punti di C e da un blocco per essi, si ha:

$$(2.1)\qquad \sum_{i=m}^{n}\binom{i}{s}t_i=r_s\binom{c}{s}\qquad (s=m,\dots,n).$$

In particolare, per s=0,1,2 si ha:

$$(2.2)\qquad \left|\begin{array}{l}\sum_{i=m}^{n}t_i=r_0\\ \sum_{i=m}^{n}it_i=cr_1\\ \sum_{i=m}^{n}i(i-1)t_i=c(c-1)r_2\end{array}\right.$$

e quindi, sostituendo la $(2.2)_{II}$ in $(2.2)_{III}$, si ottiene:

$$(2.3)\qquad \sum_{i=m}^{n}i^2t_i=c\,[\,r_2(c-1)+r_1]\ .$$

Proviamo che:

V. In $S(t,k,v)$ non esistono blocking sets intersecati da ogni blocco in un numero costante di punti, ovvero ad un sol carattere rispetto ai blocchi, di conseguenza necessariamente $m<n$.

Dimostrazione. Se m=n, cioe\` se ogni blocco incontra C in m punti, deve essere $m>1$, altrimenti si avrebbe m=1, c=1, $t_1=r_0=r_1$ e cio e\` assurdo. Se e\` $m>1$, dalla (1.4) si ha:

$$t_m=r_0,\ mt_m=r_1c,\ m(m-1)\cdot t_m=c(c-1)r_2\longrightarrow$$

$$\longrightarrow mr_0=r_1c\ ,\ (m-1)r_1=(c-1)r_2\longrightarrow$$

$$\longrightarrow c=mr_0/r_1=mv/k\ ;\ c-1=(m-1)r_1/r_2=(m-1)(v-1)/(k-1)\longrightarrow$$

$$\longrightarrow k^2-k(v+m)+mv=0\longrightarrow k=v \text{ ovvero } k=m,$$

e tali relazioni sono entrambe assurde, essendo $t<k<v$ e $m<k$.

Dalle $(2.2)_I$ e $(2.2)_{II}$, per differenza si ha:

$$0<\sum_{i=m}^{n}(i-1)t_i=r_1c-r_0\ ,$$

ovvero, essendo per la (1.5) $v/k=r_0/r_1$, ed essendo il complementare S-C ancora un blocking set, si ha:

$$(2.4)\qquad v/k<c<v-v/k\ .$$

Sia C un blocking set di $S(t,k,v)$. Sussistono le implicazioni seguenti:

$(2.5)_I$ $|C|\leq k-(t-3)\Rightarrow$ C possiede t+1 punti indipendenti

$(2.5)_{II}$ $k\geq 2t-3\Rightarrow|C|\geq t+1$.

La $(2.5)_I$ segue dalla Prop. IV. Proviamo la $(2.5)_{II}$.

Se $t=2$ e` $|C|>2$. Sia $t\geq 3$ e $k\geq 2t-3$, onde $k-(t-3)\geq t$; supposto $|C|\leq t$, C e` contenuto in un blocco B ed esistono $t-3$ punti $P_1,\dots,P_{t-3}$ di B non in C. Per la Prop. IV esiste allora un blocco $B'\in\mathcal{B}$ tale che $B'\cap B=\{P_1,\dots P_{t-3}\}$, onde $B'\cap C=\emptyset$; ma allora C non e` un blocking set, contro l'ipotesi.

Proviamo ora che:

VI. In un $S(t,k,v)$, con $t<k<v$ e $t\leq 5$, ogni blocking set C non puo` essere contenuto tutto in un blocco, cioe` C contiene $t+1$ punti indipendenti.

Dimostrazione. L'asserto e` ovvio pet $t=2$. Per $t=3$ segue dalla Prop. III. Per $t=4$, se fosse C contenuto in un blocco B, esisterebbe $P\in B-C$; in forza della Prop. IV esisterebbe allora un blocco B' tale che $B\cap B'=\{P\}$ e quindi $B'\cap C=\emptyset$, onde C non sarebbe un blocking set. Supponiamo dunque $t=5$ e sia B un blocco contenente C. Se esistessero due punti P_1, P_2 in $B-C$, per la Prop.IV esisterebbe un blocco B' tale che $B\cap B'=\{P_1,P_2\}$, cioe` $B'\cap C=\emptyset$, onde C non sarebbe un blocking set. Ne segue allora che esiste un punto P di B tale che $C=B-\{P\}$.

Contraendo l'$S(5,k,v)$ rispetto a 3 suoi punti si ha un $S(2,k-3,v-3)$; per esso deve aversi:

$$(\alpha_1)\quad \begin{cases} v-4\geq (k-4)(k-3) \\ v-4=(k-4)(k-3) \Leftrightarrow S(2,k-3,v-3) \text{ e\` proiettivo} \end{cases}$$

Si scelgano in $S(5,k,v)$ tre punti Q_1,Q_2,Q_3 fuori di B (certamente esistenti altrimenti sarebbe $v\leq k-2$ e cio` e` in contrasto con la (α_1)). I blocchi per Q_1, Q_2, Q_3, P sono in numero di $r_4=(v-4)/(k-4)$; ciascuno di essi incontra $C=B-\{P\}$ in un punto almeno, perche` C e` un blocking set, e blocchi distinti incontrano $C=B-\{P\}$ in punti distinti. Ne segue che e` (anche in forza di (α_1) e della Prop. I):

$$(\alpha_2)\quad \begin{cases} k-1\geq |C|\geq (v-4)/(k-4)\geq k-3 \\ (v-4)/(k-4)=k-3 \Leftrightarrow S(5,k,v)=S(5,8,24) \end{cases}$$

Osserviamo che nell'$S(5,8,24)$ dato un blocco B esistono 30 blocchi ad intersezione vuota con B (basta risolvere il sistema (2.1) dei caratteri relativo all'8-insieme B), ne segue che $C=B-\{P\}$ non e` un blocking set in $S(5,8,24)$.

Essendo $r_4=(v-4)/(k-4)$ un intero e l'$S(5,k,v)$ diverso dall'$S(5,8,24)$, dovra` necessariamente aversi:

$$(\beta_1)\qquad (v-4)/(k-4)=k-1,$$

ovvero

$$(\beta_2)\qquad (v-4)/(k-4)=k-2.$$

Se vale la (β_1) si ha (cfr.(1.4)):

$$r_3=\binom{v-3}{2}\Big/\binom{k-3}{2}=(k-1)(v-3)/(k-3)=k^2-3k+1+2/(k-3)$$

onde $k-3$ deve dividere 2, cioe` $k=4$ ovvero $k=5$ e cio` e` assurdo essendo $k>t=5$.
Se vale la (β_2) si ha:

$$r_1=\binom{v-1}{4}\Big/\binom{k-1}{4}=(k-3)(k-5)(k^2-6k+16)+30-60/(k-1)$$

onde $k-1$ deve dividere 60, cioe` deve essere $k=6,7,11,13,16,21,31,61$; corrispondentemente i valori di v sono, in forza della $(\beta_2)$, i seguenti $v=12,19,67,103,172,327,787,3367$. Per tali valori di $(k,v)$ l'unico sistema di Steiner esistente e` l'$S(5,6,12)$, in quanto per gli altri valori delle coppie (k,v) l'r_0 corrispondente non e` intero.

Siamo dunque condotti ad esaminare se in $S(5,6,12)$ il 5-insieme $C=B-\{P\}$ e` un blocking set. Mostreremo che non lo e`, provando che ogni 5-insieme C di $S(5,6,12)$ ammette qualche blocco esterno. Dalle (2.1) -che valgono per un qualsiasi $(c;m,n)$-insieme di un $S(t,k,v)$- si ha (tenuto conto che attualemnte risulta $c=5$, $m\geq 0$, $n\leq 5$, $r_0=132$, $r_1=66$, $r_2=30$, $r_3=12$, $r_4=4$):

$$\begin{cases} t_0+t_1+t_2+t_3+t_4+t_5=132 \\ t_1+2t_2+3t_3+4t_4+5t_5=330 \\ 2t_2+6t_3+12t_4+20t_5=600 \\ 6t_3+24t_4+60t_5=720 \\ 24t_4+120t_5=480 \\ 120t_5=120 \end{cases}$$

risolvendo tale sistema otteniamo

$$t_5=1,\quad t_4=15,\quad t_3=50,\quad t_2=50,\quad t_1=15,\quad t_0=1.$$

Essendo $t_0=1$ si ha che esiste un blocco esterno a C, ne segue l'asserto.

Sia C un blocking set di S(t,k,v), supponiamo che C sia un (c;m,n)-insieme. Indicati con t_i i caratteri di C, valgono le (2.2) e (2.3). Se M ed N sono due interi arbitri con $M\le m$ ed $N\ge n$, risulta:

(2.6) $$0\le \sum_{i=m}^{n} (N-i)(i-M)t_i = -\{c^2 r_2 - c[(N+M-1)r_1 + r_2] + MNr\}.$$

Posto:

$$f(c) = c^2 r_2 - c[(N+M-1)r_1 + r_2] + MNr_0 ,$$

risulta

(2.7) $$f(c)\le 0$$

ed

(2.8) $$f(c) = 0 \rightleftharpoons N=n,\ M=m \text{ e C di tipo } (m,n).$$

Risulta inoltre necessariamente:

(2.9) $$\Delta = [r_2+(n+m-1)r_1]^2 - 4mnr_0 r_2 \ge 0.$$

Proviamo che:

VII. In S(2,k,v) ogni blocking set C, che sia un(c;m,n)-insieme, e' tale che:

(2.10) $$1\le m\le n-2 ,$$

ne segue che $n\ge 3$.

Dimostrazione. Per ogni punto $P\in S-C$ risulta ovviamente $mr_1 \le c$; se $c=mr_1$, ogni blocco incontra C in m punti, e cio' e' assurdo per la Prop.V. Dunque:

$$mr_1+1\le c.$$

Per ogni $P\in C$ si ha ovviamente:

$$c-1\le (n-1)\, r_1 ,$$

cioe'

$$c\le (n-1)r_1+1.$$

Se $c=(n-1)r_1+1$, ogni blocco per P risulta n-secante, di conseguenza, contenendo ogni blocco un punto di C, ogni blocco di S(2,k,v) risulta n-secante, e cio' e' assurdo per la Prop.V. Allora:

$$c\le (n-1)r_1 .$$

Dunque

$$mr_1+1\le c\le (n-1)r_1 ,$$

ne segue

$$mr_1+1\le (n-1)r_1,\ \text{onde}\ (n-m-1)r_1\ge 1,$$

ovvero $n-m-1\ge 1$, da cui la (2.10).

Come corollario della Prop. VII si ha:

VIII. In S(2,3,v) non esistono blocking sets, e quindi in $S(3,4,v)$ ogni blocking set e\` irriducibile. In particolare in $PG(r,2)$, $AG(r,2)$ ed $AG(r,3)$, $r \geq 2$, rispetto alle rette, non esistono blocking sets; mentre in $AG(r,2)$, $r \geq 3$, rispetto ai piani, ogni blocking set e\` irriducibile.

Proviamo che:

IX. In $S(2,4,v)$ ogni $(c;m,n)$-blocking set e\` tale che $m=1$, $n=3$.

Dimostrazione. Dalla Prop. VII per $k=4$, essendo $1 \leq m \leq \leq n-2 \leq k-3$ (in quanto $n \leq k-1$), si ha $n \leq 3$, onde $n=3, m=1$.

X. Fissati m,n,k tali che $k > 4mn/[4mn-(m+n-1)^2]$, $n < (\sqrt{m}+1)^2$, esiste un v_0, zero positivo del polinomio:

$$P(v) = v^2\{k\,[(m+n-1)^2 -4mn] +4mn\} + +2v\,[k^2(m+n-1)-k(m^2+n^2-m-n)-2mn] +k(m+n-k)^2 \tag{2.11}$$

tale che in ogni $S(2,k,v)$ con $v > v_0$ non esistono $(c;m,n)$-insiemi.

Dimostrazione. Dalla (2.7) e (2.9), per $t=2$, nel qual caso e\` $r_2=1$, risulta:

$$\begin{cases} \Delta = [1+(n+m-1)r_1]^2 -4mnr_0 \geq 0 \\ [1+(m+n-1)r_1 - \sqrt{\Delta}]/2 \leq c \leq [1+(m+n-1)r_1 + \sqrt{\Delta}]/2. \end{cases} \tag{2.12}$$

Per la (2.8) nella $(2.12)_{II}$ vale il segno di eguaglianza se, e solo se, C e\` di tipo (m,n). Essendo per $t=2$:

$$r_1 = (v-1)/(k-1) \quad , \quad r_0 = v(v-1)/k(k-1) \quad ,$$

risulta:

$$\Delta k(k-1)^2 = v^2\{k\,[(m+n-1)^2-4mn] + 4\,mn\} + +2v\,[k^2(m+n-1)-k(m^2+n^2-m-n)-2mn]+k(m+n-k)^2 \;:=\; P(v).$$

Osserviamo che e\`:

$$(m+n-1)^2 -4mn = [n-(\sqrt{m}+1)^2]\,[n-(\sqrt{m}-1)^2],$$

da cui, essendo $n-(\sqrt{m}-1)^2>0$, si ha:

$$(m+n-1)^2 -4mn < 0 \iff n < (\sqrt{m}+1)^2 ,$$

e quindi:

$$k\,[(m+n-1)^2 -4mn] +4mn < 0 \iff n < (\sqrt{m}+1)^2 ,$$

$$k > 4mn/[4mn-(m+n-1)^2] .$$

Ne segue che l'equazione $P(v)=0$ ha una sola radice positiva v_0; dunque per $v > v_0$ e\` $P(v) < 0$ e quindi $\Delta < 0$. Di conseguenza in $S(2,k,v)$ per $v > v_0$ non possono esistere $(c;m,n)$-insiemi C.

Dalla Prop. X per $m=1$, $n=3$, $k=5$ si ha:

XI. In $S(2,5,v)$ non esistono $(c;m,n)$-blocking sets con $m=1$, $n=3$ per ogni $v > 26$.

Dalle (2.12) e dalla Prop. IX si ha:

XII. In $S(2,4,v)$ ogni blocking set C e\` tale che:

$$(v-\sqrt{v})/2 \leq |C| \leq (v+\sqrt{v})/2 , \tag{2.13}$$

i segni di eguaglianza valendo se, e solo se, C e\` di tipo $(1,3)$.

Si consideri una n-secante s di un $(c;m,n)$-insieme C $(1 \leq m < n \leq k-1)$ di $S(2,k,v)$, e sia $Q \in s \setminus C$. Ciascuna retta per Q, diversa da s, incontra C in almeno un punto; ne segue che e\` $c \geq (r_1-1)+n$ e quindi:

$$c = (r_1-1)+h \;,\quad h \geq n. \tag{2.14}$$

Poniamo successivamente:

$$r_1 = q+1 \tag{2.15}$$

$$a = (r_1-k)/k, \tag{2.16}$$

i ha che

2.17) $a=0 \rightleftarrows S(2,k,v)$ e` un piano proiettivo di ordine q.

XIII. Sia C un blocking set di $S(2,k,v)$, $2 < k < v$, he sia un $(c;m,n)$-insieme. Risulta, tenuto conto delle 2.13), (2.14), (2.15):

2.18) $|C| = q+h \geq q+[-a+2+\sqrt{(a-2)+4(q-1)}]/2$,

l segno di eguaglianza valendo se, e solo se, $h=n$, $m=1$ e e` di tipo $(1,n)$.

La (2.18), come e` facile provare, equivale alla iseguaglianza di Bruen-Thas (cf.[3]).Si noti che per $a=0$ i ritrovano le diseguaglianze di Bruen (cfr.[1] ,[2])per blocking sets di un piano proiettivo.

Dimostrazione. Dalle (2.6) e (2.7) per $N=h$, $M=1$, $=q+1$, essendo $c=q+h$ ed $r_0=q^2+q+1-qa$, si ha:

$$q[q-(h-1)^2-ha] = -\sum_{i=m}^{n}(h-i)(i-1)t_i \leq 0 ;$$

uindi:

2.19) $q = r_1-1 \leq (h-1)^2+ha$

2.20) $q = (h-1)^2+ha \rightleftarrows m=1,\ h=n,\ t_i=0 \quad i=2,\dots,n-1$

$\rightleftarrows$ C e` di tipo $(1,n)$ con $|C| = q+n$.

alla (2.19) si ha:

$$h \leq [-a+2+\sqrt{(a-2)^2+4(q-1)}]/2 ,$$

quindi l'asserto.

Proviamo che:

XIV, Sia C un blocking set di $S(3,k,v)$ che sia un $:;m,n)$-insieme. Allora:

2.21) $r_2 < c < v-r_2$.

Dimostrazione. Per un blocking set C di $S(3,k,v)$ si ha evidentemente:

$$r_2 \leq mr_2 \leq c .$$

Supponiamo $c=r_2$ (allora $m=1$). Cio` accade se,e solo se,ogni blocco con due punti fuori di C incontra C in un punto. Ne segue che ogni blocco per due punti di C incontra S-C in un punto, quindi $|S-C| = r_2$, onde $v-c=r_2$, di conseguenza $c=r_2= v/2$. Ma dalla eguaglianza

$$c = r_2=(v-2)/(k-2)=v/2$$

si ha:

$$(k-4)v+4=0 ,$$

che e` assurda, essendo $k \geq 4$, ne segue l'asserto.

In $S(3,4,v)$ si ha $r_2=(v-2)/(k-2)=(v-2)/2$, quindi la (2.21) diviene:

$$v/2-1 < |C| < v/2+1$$

onde $|C|=v/2$. Allora se in un $S(3,4,v)$ esiste un blocking set C, necessariamente $|C|=v/2$, di conseguenza esso e` irriducibile insieme al suo complementare.

In $S(3,k,v)$ sia C un $(c;m,n)$-insieme con $1 \leq m < n \leq 3$. Dalle (2.1) si ha:

$$(2.22)\quad \left|\begin{array}{l} t_1+t_2+t_3=r_0 \\ t_1+2t_2+3t_3=cr_1 \\ 2t_2+6t_3=c(c-1)r_2 \\ 6t_3=c(c-1)(c-2) . \end{array}\right.$$

Dalle ultime tre di (2.22) si ottengono i valori:

$$(2.23)\qquad \begin{cases} t_3 = c(c-1)\ (c-2)/6 \\ t_2 = c(c-1)\ (r_2-c+2)/2 \\ t_1 = cr_1 - c(c-1)(c-2)/2 - c(c-1)(r_2-c+2), \end{cases}$$

che, sostituiti nella prima delle (2.22), danno:

$$c^3-3c^2(1+r_2)+c(2+3r_2+6r_1)-6r_0=0,$$

dalla quale, sostituendo i valori di r_i, si ottiene:

$$(2.24)\qquad k(k-1)(k-2)c^3-3c^2(v+k-4)k(k-1)+ck[2(k-1)(k-2)+$$
$$+3(v-2)(k-1)+6(v-1)(v-2)]-6v(v-1)(v-2)=0.$$

Inoltre, dovendo essere $t_2 \geq 0$, dalla $(2.23)_{II}$ e dalla (2.21) si ha:

$$(2.25)\qquad r_2+1 \leq c \leq r_2+2.$$

Osserviamo inoltre che contraendo l'S(3,k,v) in un punto $P \notin C$ si ottiene un $S_P(2,k-1,v-1)$ e in esso C e` un (c;m,n)-insieme con $1 \leq m < n \leq 3$; ma per la Prop.X, se $k-1>4$, si ha che si puo` trovare un v_0-1 tale che per ogni $v-1>v_0-1$ in $S_P(2,k-1,v-1)$ non esistono siffatti (c;m,n)-insiemi. Concludendo si ha che:

XV. In S(3,k,v) sia C un (c;m,n)-insieme con $1 \leq m < n \leq 3$. Allora necessariamente e` $c=r_2+1$ ovvero $c=r_2+2$, inoltre c deve soddisfare la (2.24). Infine se e` $k>5$ si puo` trovare un intero v_0 tale che per ogni $v>v_0$ in S(3,k,v) non esistono tali (c;m,n)-insiemi.

Per k=4, la (2.24) diventa:

$$(2.26)\qquad 4c^3-6c^2v+2c(2v^2-3v+2)-v^3+3v^2-2v=$$
$$=(c-v/2)(4c^2-4vc+2v^2-6v+4)=0\ .$$

Dalla (2.26) si ritrova $c=v/2$, (essendo $c=v/2$ l'unica soluzione intera di (2.26)) .
Sostituendo $c=v/2$ in (2.23), si ha:

$$(2.27)\qquad \begin{cases} t_1=v(v-2)(v-4)/48=\binom{c}{3} \\ t_2=v(v-2)/8=\binom{c}{2} \\ t_3=v(v-2)(v-4)/48=\binom{c}{3} \end{cases}$$

Contraendo l'S(3,4,v) in un punto Q del blocking set C, si ottiene un $S_Q(2,3,v)$ ed in esso l'insieme $A=C-\{Q\}$ risulta un (v/2-1)-arco.
Per ogni $P\in A$ in $S_Q(2,3,v)$ passano v/2-2 rette secanti e quindi (v-2)/2-(v/2-2) rette tangenti, cioe` per ogni $P\in A$ passa una sola retta tangente. Ne segue che le tangenti ad A sono in numero di $|A|=v/2-1$. Poiche` il numero delle secanti di A e` (v-2)(v-4)/8, si ha che il numero delle rette esterne di A e`:
$(v-1)(v-2)/6-(v-2)/2-(v-2)(v-4)/8 = (v-2)(v-4)/24$.

Concludendo:

XV. Se C e` un blocking set di un S(3,4,v), risulta $|C|=v/2$, i numeri dei blocchi 1-secanti, 2-secanti, 3-secanti sono dati dalle (2.27). Inoltre per ogni punto P di C i numeri u_1, u_2, u_3, dei blocchi per P rispettivamente 1-secanti, 2-secanti, 3-secanti sono dati da:

$$(2.28)\qquad \begin{cases} u_1=(v-2)(v-4)/24 \\ u_2=(v-2)/2 \\ u_3=(v-2)(v-4)/8 \end{cases}$$

In AG(3,2) isomorfo a S(3,4,8) gli unici blocking sets, rispetto ai piani, sono evidentemente costituiti da quaterne di punti indipendenti (essendo $c=v/2=4$).

In AG(r,2) con $r\geq 4$ non esistono blocking sets rispetto ai piani. Infatti, se ne esistesse uno, S, esso sarebbe intersecato da ogni sottospazio 3-dimensionale A_3 di AG(r,2) in 4 punti (in quanto l'intersezione deve essere un blocking set rispetto ai piani di A_3). Ma allora S sarebbe ad un sol carattere rispetto agli A_3, di conseguenza, cfr. [14], $S=\emptyset$ oppure $S=AG(r,2)$; cio` e` escluso.

Ne segue:

XVI. In $AG(r,2)$ blocking sets, rispetto ai piani, esistono solo se $r=3$, nel qual caso sono dati da una quaterna di punti indipendenti.

3. GENERALITA' SUI d-BLOCKING SETS DI AG(r,q) E PG(r,q)

In $AG(r,q)$ o in $PG(r,q)$ definiamo d-blocking set un sottoinsieme K tale che ogni d-sottospazio S_d $(1 \le d \le r)$ abbia qualche punto in comune con K e qualche punto in comune con il complementare di K. Evidentemente il complementare di un d-blocking set e` ancora un d-blocking set. Inoltre ogni h-sottospazio $S_h$, con $h \ge d$, incontra un d-blocking set ancora in un d-blocking set. Infine ogni (d-1)-blocking set e` un d-blocking set. Un d-blocking set si dira` proprio se non e` un (d-1)-blocking set, cioe` se contiene un $S_{d-1}$ ovvero ammette un $S_{d-1}$ esterno. Un d-blocking set $K$ dicesi irriducibile se per ogni $P \in K$ passa almeno un $S_d$ che incontra $K$ solo in $P$, cioe` se per ogni $P \in K$ l'insieme $K-\{P\}$ non e` un d-blocking set. Evidentemente ogni d-blocking set e` contenuto in uno irriducibile.

Recentemente F.Mazzocca e G.Tallini hanno provato che: (cfr. [7])

XVII. Dati gli interi $q(=p^h$, con p primo) e $d(\ge 1)$ esistono un intero $b_p(d,q)$ e un intero $b_a(d,q)$ tale che in $PG(r,q)$ un d-blocking set esiste se, e solo se, e` $r \le b_p(d,q)$, in $AG(r,q)$ un blocking set esiste se, e solo se, e` $r \le b_a(d,q)$.

Il problema dell'esistenza dei d-blocking set in $PG(r,q)$ o in $AG(r,q)$, in forza della Prop.XVII, e` fortemente collegato alla determinazione degli interi $b_p(d,q)$ e $b_a(d,q)$.

Proviamo che:

(3.1) $$b_a(d,q) \le b_p(d,q).$$

Ragionando per assurdo, supponiamo che sia $b_a(d,q) > b_p(d,q)$. Posto $r-1 = b_p(d,q)$, sara` $b_a(d,q) \ge r$, quindi in $AG(r,q)$ esiste qualche d-blocking set $K'$. Poiche` e` $b_p(d,q)=r-1$, nell'iperpiano improprio $PG(r-1,q)$ di $AG(r,q)$ esiste qualche d-blocking set $K''$. In $PG(r,q)=AG(r,q) \cup PG(r-1,q)$ l'insieme $K=K' \cup K''$ e` evidentemente un d-blocking set, quindi deve essere $b_p(d,q) \ge r$ e cio` e` assurdo essendo $b_p(d,q) = r-1$.

Poiche` in $AG(r,q)$ ogni d-blocking set e` anche un (d+1)-blocking set $(1 \le d \le r-1)$ si ha:

(3.2) $$b_a(d,q) \le b_a(d+1,q)$$

Osserviamo che ogni d-blocking set di un iperpiano di $PG(r,q)$ e` un (d+1)-blocking set di $PG(r,q)$, ne segue che e`:

(3.3) $$b_p(d,q) \le b_p(d+1,q)-1$$

Dalla (1.3) segue induttivamente che:

(3.4) $$b_p(d,q) \ge b_p(1,q)+d-1.$$

In $AG(d+1,q)$, con $d \ge 2$, $d+1$ rette per un punto O indipendenti (cioe` congiunte da $AG(d+1,q)$) costituiscono un d-blocking set (come subito si prova); si ha dunque che:

(3.5) $$b_a(d,q) \ge d+1, \quad d \ge 2 .$$

Nel seguito ci occuperemo dei d-blocking set con $d \ge 2$ (per il caso $d=1$ cfr. [12]).

4. ESEMPI DI d-BLOCKING SETS

Esempio I: Subspazi di Baer $PG(r,q)$ in $PG(r,q^2)$.

In $PG(r,q^2)$ si consideri un subspazio di Baer $PG(r,q)$. Ogni sottospazio d-dimensionale S_d, con $2d \ge r$, di $PG(r,q^2)$ e` tale che:

$$S_d \cap PG(r,q) \ne \emptyset \text{ e } S_d \cap (PG(r,q^2)-PG(r,q)) \ne \emptyset .$$

Infatti se S_d e` a coefficienti in $GF(q)$ $(\subseteq GF(q^2))$ risulta $|S_d \cap PG(r,q)| = \theta(d,q)$ e $|S_d \cap (PG(r,q^2)-PG(r,q))| = \theta(d,q^2)-\theta(d,q) > 0$; se $S_d$ e` a coefficienti in $GF(q^2)-$

$\subseteq GF(q)$, sia $\bar{S}_d$ il complesso coniugato di S_d, allora $S_d \cap \bar{S}_d \subseteq PG(r,q)$ e $\dim S_d \cap \bar{S}_d \geq 0$ (essendo $2d \geq r$), onde S_d ha qualche punto in comune con $PG(r,q)$ e qualche punto in comune con il complementare. Ne segue che $PG(r,q)$ e' un d-blocking set di $PG(r,q^2)$ se $r \leq 2d$.

Esempio II: Quadriche non singolari di PG(2d,q).

E' noto,(cfr. [8], [11]) che in PG(2d,q) due quadriche non singolari sono proiettivamente equivalenti e se Q_0 e' una tale quadrica, risulta:

(4.1) $$|Q_0| = \theta_{2d-1} ,$$

inoltre gli spazi di dimensione massima situati su Q_0 sono degli S_{d-1}. Se $d \geq 2$ ogni S_d incontra allora Q_0 in una quadrica dell'S_d, onde $Q_0 \cap S_d \neq \emptyset$ (perche' $d \geq 2$) e $S_d \not\subseteq Q_0$. Ne segue che Q_0 e' un d-blocking set proprio (perche' Q_0 contiene degli S_{d-1}) onde $b_p(d,q) \geq 2$, se $d \geq 2$.

Esempio III: Quadriche non singolari di PG(2d+1,q).

E' noto (cfr. [8], [11]) che in PG(2d+1,q) esistono due soli tipi proiettivamente distinti di quadriche non singolari: quelle iperboliche e quelle ellittiche. Sia Q_+ una quadrica iperbolica. E' noto, [11], allora che:

(4.2) $$|Q_+| = \theta_{2d} + q^d$$

e che gli spazi di dimensione massima su Q_+ sono degli S_d. Ne segue che, se e' $d \geq 1$, ogni S_{d+1} incontra Q_+ in una quadrica dell'S_{d+1}, onde $Q_+ \cap S_{d+1} \neq \emptyset$ (perche' $d+1 \geq 2$) e $S_{d+1} \not\subseteq Q_+$. Quindi Q_+ e' un (d+1)-blocking set proprio (perche' Q_+ contiene degli S_d).

Sia Q_- una quadrica ellittica. E' noto, [11], allora che:

(4.3) $$|Q_-| = \theta_{2d} - q^d$$

e che gli spazi di dimensione massima su Q_- sono degli S_{d-1}. Ne segue che, se e' $d \geq 2$, ogni S_d incontra Q_- in una quadrica di S_d, onde $Q_- \cap S_d \neq \emptyset$ (perche' e' $d \geq 2$) e $S_d \not\subseteq Q_-$.

Quindi Q_- e' un d-blocking set proprio (perche' Q_- contiene degli S_{d-1}), onde:

(4.4) $$b_p(d,q) \geq 2d+1, \qquad d \geq 2$$

Esempio IV: I k-insiemi di tipo $(1,n)_{r-1}$ di PG(r,q), $r \geq 3$.

E' noto che, [10], [15], un k-insieme di tipo $(1,n)_{r-1}$ rispetto agli iperpiani in PG(r,q), $r \geq 3$, e' necessariamente una retta ovvero e' $r=3$ e K e' una (q^2+1)-calotta (e quindi una quadrica ellittica se q e' dispari), comunque in ogni caso e' $n=q+1$. Un tale insieme e' un (r-1)-blocking set di PG(r,q).

Esempio V: Fibrazioni non totali in PG(3,q).

Sia $\mathcal{F}$ una fibrazione non totale in PG(3,q), cioe' tale che $1 \leq |\mathcal{F}| \leq q^2$. Posto $F = \bigcup_{f \in \mathcal{F}} f$, ogni piano α e' tale che $\alpha \cap F \neq \emptyset$, inoltre e' $\alpha \not\subseteq F$ (in quanto $|\mathcal{F}| \leq q^2$). Dunque F e' un 2-blocking set di PG(3,q).

Esempio VI: Forme hermitiane di PG(r,q).

Sia $GF(q) = G_q$ un campo di Galois con q quadrato.

L'applicazione $x \in G_q \longrightarrow x^{\sqrt{q}} \in G_q$ e' allora un automorfismo involutorio di G_q che dicesi coniugio e si pone

$\bar{x} = x^{\sqrt{q}}$. In PG(r,q) chiamasi forma hermitiana (cfr. [9], [11], [13]) il luogo H dei punti le cui coordinate soddisfano l'equazione:

(4.5) $$\sum_{ij}^{0,r} a_{ij} x_i \bar{x}_j = 0 , \quad \text{con } a_{ij} = \bar{a}_{ji} .$$

Si prova che ogni retta o appartiene ad H ovvero incontra H in un sol punto (retta tangente) o in $n = \sqrt{q}+1$ punti, cioe' H e' di tipo $(1,n,q+1)_1$. Un punto P di H dicesi singolare se ogni retta per esso o appartiene ad H ovvero e' tangente in P ad H. Se H e' non singolare (cioe' se non contiene punti singolari) allora $\det \|a_{ij}\| \neq 0$ e viceversa.

Se H e' singolare, l'insieme dei punti singolari e' un sottospazio S_h e H e\` un cono proiettante da tale $S_h$ una forma hermitiana non singolare di un $S_{r-h-1}$ sghembo con l'$S_h$. Lo studio delle forme hermitiane si riconduce cosi\` a quello delle forme hermitiane non singolari.

Se H e\` non singolare, la biezione tra PG(r,q) e PG*(r,q) di equazione:

(4.6) $$u = A\bar{X} \quad , \qquad A = \| a_{ij} \|$$

prende il nome di polarita\` associata ad H. Essa gode della proprieta\` di reciprocita\`. Scelto l'(r+1)-simplesso fondamentale del riferimento coincidente con un (r+1)-simplesso autopolare rispetto ad H ed opportunamente il punto unitario, l'equazione di H diventa:

$$\sum_{i=0}^{r} x_i \bar{x}_i = 0$$

onde le forme hermitiane non singolari sono tutte proiettivamente equivalenti.

Se $P \in H$, l'iperpiano polare di P coincide con l'iperpiano tangente in P ad H, cioe\` con l'unione delle rette per P tangenti o appartenenti ad H. Tale iperpiano $\tau_P$ incontra H in una forma hermitiana che ammette come unico punto singolare P e quindi che proietta da P una forma hermitiana non singolare di un $S_{r-2} \subset \tau_P$ con $P \notin S_{r-2}$. Da cio\` segue che, denotato con $h_{r,q}$ il numero dei punti di una forma hermitiana non singolare di PG(r,q) si ha:

(4.7) $$h_{r,q} = \sqrt{q}\, q^{r-1} + q h_{r-2,q} + 1$$

da cui induttivamente otteniamo:

(4.8) $$h_{2d,q} = \theta_{d-1} (1 + q^d \sqrt{q})$$

(4.9) $$h_{2d+1,q} = \theta_d (1 + q^d \sqrt{q}).$$

Inoltre si ha che gli spazi di dimensione massima situati su H sono degli S_{d-1} se r=2d e degli S_d se r=2d+1. Ne segue che, se e\` r=2d, ogni $S_d$ incontra H in una forma hermitiana dell'$S_d$, onde $H \cap S_d \neq \emptyset$ e $S_d \not\subseteq H$, cioe\` H e\` un d-blocking set proprio. Se e\` r=2d+1 ogni S_{d+1} incontra H in una forma hermitiana dell'S_{d+1}, onde e\` $H \cap S_{d+1} \neq \emptyset$ e $S_{d+1} \not\subseteq H$, cioe\` H e\` un (d+1)-blocking set proprio.

Esempio VII: Quadriche in AG (3,q) e in AG(4,q) .

Sia I un iperboloide iperbolico di AG(3,q) e sia π_∞ il piano improprio di AG(3,q) e C_∞ la conica all'infinito (non degenere) di I. Sia α un qualsiasi piano di AG(3,q) ed r_∞ la sua retta impropria. Se r_∞ e\` esterna a $C_\infty$ allora $I \cap \alpha$ e\` una ellisse (non degenere, essendo I a punti iperbolici) e quindi $|I \cap \alpha| = q+1$ e $|\alpha - I \cap \alpha| = q^2 - (q+1) > 0$ onde e\` $I \cap \alpha \neq \emptyset$ e $\alpha - I \cap \alpha \neq \emptyset$. Se $r_\infty$ e\` tangente a C_∞ in un punto P_∞ allora $I \cap \alpha$ o e\` una parabola (non degenere) e quindi $|I \cap \alpha| = q$ e $|\alpha - I \cap \alpha| = q^2 - q > 0$ onde $I \cap \alpha \neq \emptyset$ e $\alpha - I \cap \alpha \neq \emptyset$; oppure $I \cap \alpha$ e\` una conica degenere in due rette per P_∞ a coefficienti in GF(q) (essendo I a punti iperbolici) e quindi $|I \cap \alpha| = 2q$ e $|\alpha - I \cap \alpha| = q^2 - 2q$ onde e\` $I \cap \alpha \neq \emptyset$ e, se e\` $q > 2$, $\alpha - I \cap \alpha \neq \emptyset$. Se r_∞ e\` secante $C_\infty$, $I \cap \alpha \neq \emptyset$ e\` una iperbole non degenere e quindi $|I \cap \alpha| = q-1$ e $|\alpha - I \cap \alpha| = q^2 - q + 1 > 0$, onde $I \cap \alpha \neq \emptyset$ e $\alpha - I \cap \alpha \neq \emptyset$, oppure $I \cap \alpha$ degenera in due rette a coefficienti in GF(q) incidenti in un punto proprio e quindi risulta $|I \cap \alpha| = 2q-1$ e $|\alpha - I \cap \alpha| = q^2 - 2q + 1 = (q-1)^2 > 0$, onde $I \cap \alpha \neq \emptyset$ e $\alpha - I \cap \alpha \neq \emptyset$. Dunque, se e\` $q > 2$, in ogni caso $I \cap \alpha \neq \emptyset$ e $\alpha - I \cap \alpha \neq \emptyset$, cioe\`:
se $q > 2$ l'iperboloide iperbolico I e\` un 2-blocking set di AG(3,q) ed e\` $|I| = q^2 + q$.

In modo analogo si prova che:

In AG(3,q) ogni paraboloide iperbolico, P_i, o ellittico, P_e, e\` un 2-blocking set, qualsiasi sia $q \geq 2$ ed e\` $|P_i| = q^2 = |P_e|$. Mentre un iperboloide ellittico non e\` un 2-blocking set.

In AG(4,q) ogni quadrica non singolare non e\` un 2-blocking set ma, come facilmente si puo\` provare, e\` un 3-blocking set quindi proprio.

Esempio VIII: Iperboloide iperbolico in AG(2d-1,q) con $d \geq 2$ e $q > 2$.

In AG(2d-1,q) con $d \geq 2$ e $q > 2$, sia I un iperboloide iperbolico, cioe\` una quadrica iperbolica la cui quadrica all'infinito risulti una quadrica non singolare, onde e' $|I|=\theta_{2d-2}+q^{d-1}-\theta_{2d-3}$. Allora I contiene come spazi di dimensione massima degli S_{d-1}. Inoltre si puo' facilmente provare che ogni S_d di AG(2d-1,q) ha intersezione non vuota con I e con il suo complementare, se e' $d \geq 2$ e $q > 2$; ne segue che I e' un d-blocking set, onde e':

$$(4.10) \qquad b_a(d,q) \geq 2d-1, \quad d \geq 2,\ q > 2.$$

Esempio IX: Blocking set di A.Beutelspacher (cfr.[4]).

In $P=PG(3d-1,q^2)$ sia ω un sottospazio 2d-dimensionale di P e B un subspazio di Baer di ω. Posto $S=\omega-B$ proviamo che S e' un d-blocking set di $PG(3d-1,q^2)$. Se d=1, e' $P=\omega$ ed S e' il complementare del subpiano di Baer B che, come e' noto, e' un 1-blocking set. Possiamo dunque supporre $d \geq 2$. Sia U un qualsiasi sottospazio d-dimensionale di P. Se U e' contenuto in ω, esso ha almeno un punto in comune con B e almeno un punto in comune con $S=\omega-B$ (cfr. Es. I n.4). Se U non e' contenuto in ω allora ogni punto di $U-\omega$ non e' in S, mentre, essendo $\dim(U \cap \omega) \geq 1$, $U \cap \omega$ ha qualche punto in comune con S. Dunque in ogni caso e': $U \cap S \neq \emptyset$ e $U \cap (P-S) \neq \emptyset$, cioe' S e' un d-blocking set.

Esempio X. In P=PG(r,q) si consideri un sottospazio S_s con $r \leq d+s-1$ ed in S_s un d-blocking set H privo di rette esterne (per esempio, se q e' un quadrato r=3d-1 e s=2d, H sia una forma hermitiana di S_{2d} non singolare, cfr. Es. VI). Allora H e' un d-blocking set di PG(r,q). Infatti ogni S_d di S_s e' ad intersezione non vuota con H e con il suo complementare, se S_d non e' in S_s, allora $S_d \cap (P-H) \neq \emptyset$ inoltre $S_d \cap S_s = S_i$, con $i \geq d+s-r \geq 1$, onde $S_i \cap H \neq \emptyset$ (perche' H e' privo di rette esterne in S_s) e quindi $S_d \cap H \neq \emptyset$.

Esempio XI. In P=PG(3d-1,q), $d \geq 2$, si consideri un sottospazio S_{2d+1} e in esso una quadrica ellittica Q_-. Allora Q_- e' un d-blocking set di S_{2d+1} (cfr. Es. III). Proviamo che Q_- e' un d-blocking set in PG(3d-1,q). Basta mostrare che ogni S_d non contenuto in S_{2d+1} e' ad intersezione non vuota con Q_- (essendo ovviamente ad intersezione non vuota con $P-Q_-$), risulta $S_d \cap S_{2d+1}=S_i$, con $i \geq 2$, onde esiste un piano S_2 contenuto in S_i, ma allora $S_2 \cap Q \neq \emptyset$ e quindi

$S_d \cap Q_- (\supseteq S_i \cap Q_- \supseteq S_2 \cap Q_- \neq \emptyset)$ e' non vuoto. Si ha cosi' l'asserto. Ne segue che :

$$(4.11) \qquad b_p(d,q) \geq 3d-1.$$

5. LIMITAZIONI PER IL NUMERO DEI PUNTI DI UN d-BLOCKING SET DI AG(r,q) E PG(r,q)

Sia K un d-blocking set di AG(r,q), con $d \leq r-1$. Ogni sottospazio S_{d+1} incontra K in un d-blocking set $K_1=K \cap S_{d+1}$.

Lo spazio congiungente K_1 e' l'S_{d+1} (perche', se cosi' non fosse, K_1 apparterrebbe ad un S_d di S_{d+1}, ma allora un S_d' parallelo all'S_d in S_{d+1} avrebbe intersezione vuota con K_1 e cio' e' escluso). Ne segue che K_1 contiene d+2 punti indipendenti, siano essi $O_0, O_1, \ldots, O_{d+1}$. Denotato con π l'iperpiano di S_{d+1} congiungente i punti $O_1, O_2, \ldots, O_{d+1}$, ogni iperpiano di S_{d+1} parallelo a π, distinto da π e non passante per O_0, deve incontrare K_1 in almeno un punto diverso da $O_0, O_1, \ldots, O_{d+1}$.
Ne segue che e' $|K_1| \geq d+2+(q-2)$, cioe':

$$(5.1) \qquad |K_1| = |K \cap S_{d+1}| \geq d+q .$$

Supponiamo ora che il d-blocking set K ammetta qualche $\bar{S}_d$ tale che $|K \cap \bar{S}_d|=1$, per esempio che K sia irriducibile (cfr.n.3). Gli S_{d+1} per un tale $\bar{S}_d$ sono in numero di θ_{r-d-1}; ciascuno di essi incontra K, per la (5.1), in almeno d+q-1 punti fuori dell'$\bar{S}_d$. Pensando allora i punti di $K-\bar{S}_d$ distribuiti sugli S_{d+1} per $\bar{S}_d$ si ha:

$$|K| \geq \theta_{r-d-1}(q+d-1)+1$$

cioe':

$$|K| \geq \theta_{r-d}+(d-1)\theta_{r-d-1} .$$

Poiche' ogni d-blocking set di AG(r,q) contiene qualche d-blocking set irriducibile e il complementare di un d-blocking set e' un d-blocking set, si ha:

XVIII. Ogni d-blocking set K di AG(r,q) con $d \leq r-1$, e` tale che:

$$(5.2)\qquad \theta_{r-d}+(d-1)\theta_{r-d-1} \leq |K| \leq q^r -(\theta_{r-d}+(d-1)\theta_{r-d-1}).$$

Per $r=4$, $d=2$ e $q=2$ dalla (5.2) si ha l'assurdo $10 \leq |K| \leq 6$. Ne segue che in $AG(r,2)$, per $r \geq 4$, non esistono 2-blocking sets. Da cio` e dalla (3.5) si ha allora:

$$(5.3)\qquad b_a(2,2) = 3.$$

Si noti che per $r=3$, $d=2$, $q=2$ la (5.2) da`: $|K| = 4$, cioe` in $AG(3,2)$ l'unico 2-blocking set e` costituito da 4 punti indipendenti.

Sia ora K un d-blocking set di $PG(r,q)$ che sia irriducibile e sia $\bar{S}_d$ un sottospazio tale che $|K \cap \bar{S}_d| = 1$. Ogni S_{d+1} per l'$\bar{S}_d$ incontra K in un d-blocking set $K_1 = K \cap S_{d+1}$ di S_{d+1} e risulta:

$$(5.4)\qquad \begin{cases} |K_1| = |K \cap S_{d+1}| \geq q+1 \\ |K_1| = q+1 \iff K_1 \text{ e` una retta.} \end{cases}$$

Pensando i punti di $K-\bar{S}_d$ distribuiti sugli S_{d+1} per l'$\bar{S}_d$ si ha allora:

$$(5.5)\qquad \begin{cases} |K| \geq q\,\theta_{r-d-1}+1 = \theta_{r-d} \\ |K| = \theta_{r-d} \iff \text{ogni } S_{d+1} \text{ per } \bar{S}_d \text{ incontra } K \end{cases}$$

in una retta.

Poiche` ogni d-blocking set di $PG(r,q)$ e` contenuto in un d-blocking set irriducibile ed il complementare di un d-blocking set e` un d-blocking set, si ha:

XIX. Ogni d-blocking set K di $PG(r,q)$, con $2 \leq d \leq r-1$, e` tale che:

$$(5.6)\qquad \theta_{r-d} \leq |K| \leq \theta_r - \theta_{r-d}\ ,$$

il segno di eguaglianza a sinistra avendosi se, e solo se, ogni S_{d+1} per un $\bar{S}_d$ che sia 1-secante K incontra K in una retta, quello a destra avendosi se, e solo se, ogni S_{d+1} per un $\bar{S}_d$ che sia 1-secante K incontra K nel complementare di una retta.

Osserviamo che, se $r < 2d$, ogni S_{r-d} e` un d-blocking set e quindi il segno di eguaglianza a sinistra della (5.6) e` raggiunto da un S_{r-d} e quello a destra dal complementare di un S_{r-d}.

Vogliamo ora generalizzare un risultato ottenuto in [12] (cfr.n.6). Sia K un k-insieme di $PG(r,q)$ che abbia il carattere $t_0 = t_0^d = 0$ e tale che $t_1 = t_1^d \geq k$ (in particolare K sia un d-blocking set irriducibile). Denotato con n il massimo numero di punti che un S_d ha in comune con K si ha (cfr. [12] n.1):

$$(5.7)\qquad \begin{cases} \sum_{i=1}^{n} t_i = \gamma_{r,d} \\ \sum_{i=1}^{n} i t_i = k\gamma_{r-1,d-1} \\ \sum_{i=1}^{n} i(i-1)t_i = k(k-1)\gamma_{r-2,d-2}\ . \end{cases}$$

Sottraendo dalla $(5.7)_I$ moltiplicata per n la $(5.7)_{II}$ si ottiene:

$$0 \leq \sum_{i=2}^{n-1} (n-i)t_i = n\gamma_{r,d} - k\gamma_{r-1,d-1} - (n-1)\,t_1\ ,$$

da cui:

$$n\gamma_{r,d} - k\gamma_{r-1,d-1} - (n-1)t_1 \geq 0\ ,$$

l'eguaglianza valendo se, e solo se, $t_2 = \ldots = t_{n-1} = 0$, cioe` se, e solo se, K e` di tipo $(1,n)_d$. Ne segue:

$$(n-1)k \leq (n-1)t_1 \leq n\gamma_{r,d} - k\gamma_{r-1,d-1}\ ,$$

da cui

$$(5.8)\qquad k \leq n\gamma_{r,d} \;/\; (n-1+\gamma_{r-1,d-1})\ .$$

Nella (5.8) il segno di eguaglianza vale se, e solo se, $t_1 = k$ e K e` di tipo $(1,n)_d$.

Se e\` $r=2$ (e quindi $d=1$), allora (cfr. [12] Prop. XXIII) $n=\sqrt{q}+1$, $k=q\sqrt{q}+1$ e il segno di eguaglianza nella (5.8) si ha quando K e\` un arco hermitiano. Se e\` $r \geq 3$, $d=r-1$ (cfr. [10] Prop. XXI), un k-insieme di tipo $(1,n)_{r-1}$ ha $n=q+1$ ed e\` necessariamente una retta oppure e\` $r=3$ e K e\` una (q^2+1)-calotta (e quindi, cfr. [10] Prop.V, una quadrica ellittica se q e\` dispari). Se infine e\` $r \geq 4$, $2 \leq d \leq r-2$ (cfr. [10] Prop. XX) non esistono k-insiemi di tipo $(1,n)_d$.

Esaminiamo i vari casi possibili.

Se K e\` una retta di PG(r,q), $r \geq 3$, si ha dalla (5.8), nella quale vale ora il segno di eguaglianza ed e\` $n=q+1$:

$$q+1 = n\,\theta_r / (n-1+\theta_{r-1}) = (q+1)\theta_r / (q+\theta_{r-1})$$

da cui segue l'assurdo $\theta_r = q+\theta_{r-1}$, $r \geq 3$.

Nel caso che K sia una (q^2+1)-calotta e\` $r=3$, $d=2$, $n=q+1$ e poiche\` la (5.8) diviene:

$$k \leq n\,\theta_3 / (n-1+\theta_2) = (q+1)\theta_3 / (q+\theta_2) = q^2+1 ,$$

si conclude che per $r \geq 3$, $2 \leq d = r-1$ l'eguaglianza nella (5.8) vale se, e solo se, K e\` una (q^2+1)-calotta di PG(3,q).

Rimane da esaminare il caso:

$$d=1 \text{ e } k = n\,\gamma_{r,d} / (n-1+\gamma_{r-1,d-1}) .$$

In tal caso risulta $k=n\gamma_{r,1} / (n-1+\theta_{r-1})$ se, e solo se, $t_1=k$ e K e\` di tipo $(1,n)_1$ e allora (cfr. [14]) risulta necessariamente $r=2$ e K un arco hermitiano.

Si e\` cosi\` provato che:

XX. In PG(r,q) sia K un k-insieme privo di S_d esterni (cioe\` $t_0^d = 0$) e tale che $t_1^d \geq k$ (per esempio un d-blocking set irriducibile) e sia $n = \max |S_d \cap K|$. Allora e\`

(5.9) $$k \leq n\,\gamma_{r,d} / (n-1+\gamma_{r-1,d-1}) ,$$

il segno di eguaglianza valendo se, e solo se, e\` $r=3$, $d=2$, $n=q+1$ e K e\` una (q^2+1)-calotta ovvero e\` $r=2$, $d=1$, $n=\sqrt{q}+1$ e K e\` un arco hermitiano.

BIBLIOGRAFIA

[1] A. Bruen, Baer subplanes and blocking sets, Bull. Amer. Math. Soc., 76 (1970), 342-344.

[2] A. Bruen, Blocking sets in finite projective planes, SIAM J. Appl. Math., 21 (1971), 380-392.

[3] A. Bruen, J.A. Thas, Blocking sets, Geometriae Dedicata, 6 (1977), 193-203.

[4] L.Berardi, A.Beutelspacher, F.Eugeni, On the (s,t;h)-blocking sets in finite projective and affine spaces (in preparazione).

[5] J.Doyen, A.Rosa, An updated bibliography and survey of Steiner systems, Annals of Discrete Math., 7 (1980), 317-349.

[6] C.Lam, Risultato comunicato privatamente da Hering.

[7] F.Mazzocca, G.Tallini, On the non existence of blocking sets in PG(n,q) and AG(n,q) for all large enough n, (to appear).

[8] B.Segre, Le geometrie di Galois, Ann.Mat.48 (1959), 1-97.

[9] B. Segre, Forme e geometrie hermitiane con particolare riguardo al caso finito, Ann.Mat.70 (1965), 1-202.

[10] G.Tallini, Problemi e risultati sulle geometrie di Galois, Relazione n.30 (1973), Istituto di Matematica dell'Universita\` di Napoli.

[11] G.Tallini, Spazi parziali di rette, Spazi polari, Geometrie subimmerse in Spazi proiettivi, Quaderno n. 14, Gennaio 1979, Seminario di Geometrie Combinatorie, Facolta` di Scienze,Universita` Roma.

[12] G.Tallini, k-insiemi e blocking sets in PG(r,q) e in AG(r,q), Quaderno n.1 (1982), Istituto di Matematica Applicata, Facolta` di Ingegneria,L'Aquila.

[13] M.Tallini Scafati, Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$, Rend. Mat. 26 (1967), 273-303.

[14] M.Tallini Scafati, Calotte di tipo (m,n) in uno spazio di Galois $S_{r,q}$, Rend. Acc. Naz. Lincei, 53 (1973), 71-81.

[15] J.A.Thas, A combinatorial problem, Geometriae Dedicata, 1(1973), 236-240.

Finito di stampare nel mese di Dicembre 1983
Centro Stampa "LA TECNICA"
T. Maurizi - Via dei Guelfi 13 - tel. 26277
L'AQUILA