Università degli Studi di Teramo
Scuola di Dottorato in Astrofisica ed Informatica
XIX ciclo

Tesi di dottorato in Informatica

Blocking Sets nel complementare di Arrangiamenti di Iperpiani nello spazio Proiettivo

della

Dott.ssa Simona Settepanella

Relatore
Prof. Franco Eugeni

Direttore della Scuola di Dottorato
Prof. Franco Eugeni

Indice

Introduzione

In questa tesi ci occupiamo della *Teoria dei Blocking Sets* negli spazi affini e proiettivi. In particolare introduciamo, per la prima volta, lo studio di Blocking Sets nel complementare di un arrangiamento di iperpiani.

Un arrangiamento di iperpiani é un insieme di iperpiani nello spazio (proiettivo o affine).

Partendo dall'osservazione che lo spazio affine AG(n,q) non é altro che il complementare di PG(n,q) rispetto ad un particolare iperpiano, abbiamo studiato cosa accade nel caso piú generale in cui a PG(n,q) viene tolto un arrangiamento finito di iperpiani.

Ma prima di procedere alla descrizione dettagliata della tesi, diamo, in questa introduzione, alcuni interessanti cenni storici.

Sulla metá degli anni '40, specialmente per opera di eminenti statistici quali Bose e Fischer, mentre le geometrie di Galois muovevano i primi passi, le loro applicazioni nell'ambito della statistica teorica apparivano sempre piu' felici.

È oggi ben noto che l'*analisi fattoriale*, qualora non si possano sperimentare tutti i possibili trattamenti, conduce a costruire un piano di esperimenti. Ció puó essere interpretato nel modo piú corretto in termini di spazi di Galois o, piú in generale, in termini di block designs, ovvero disegni bilanciati

di blocchi (cfr. [24], [11], [12], [28], [43], [44]).

È del 1960 un articolo di G. Tallini [44] in cui questi aspetti della *Teoria di Galois* sono ben evidenziati; dello stesso periodo e' il libro di Pompilj e Dall'Aglio: *Piani di Esperimenti*, [24]. In questo contesto, relativamente ai block designs o, più in generale, ai grafi e multigrafi, punti fermi di riferimento nel panorama italiano sono F. Speranza e M. Gionfriddo (cfr. [41], [42], [29]).

Circa nello stesso periodo alcuni astronomi finlandesi, i cui nomi sono divenuti leggendari ai cultori delle Geometrie Finite, parliamo di G. Jarnefelt, P. Kustaanheimo e B. Qvist, si proposero di costruire un modello di spazio geometrico discontinuo e finito, che rappresentasse con maggiore aderenza il macrocosmo.

Un terzo filone di interesse applicato di grande attualità è quello della *Teoria dell'informazione.*

In questo secolo, denso di mutamenti rapidi e insospettati, è stato completamente rivoluzionato uno dei concetti fondamentali dell'economia: *la moneta.*

Infatti oggi la moneta è e va trattata come informazione, precisamente come informazione del credito che l'intera società concede al singolo, in base alla sua presunta produttività. Si capisce da questo punto di vista come possano allora presentarsi problemi notevoli di *crittografia, autenticazione* e la necessità di disporre di *codici rivelatori e correttori di errori.*

Per notizie dettagliate su queste teorie si rinvia al trattato di P. Quattrocchi e W. Heise ([30]).

Vi è un ultimo filone applicato di cui vogliamo parlare, ed è quello che ci interessa più da vicino: *la teoria dei giochi cooperativi.*

Questa teoria, sorta nel 1943 ad opera di Von Neumann e Morgenstern ([37]), si è andata sempre più affermando anche per molte previsioni fatte

da specialisti a proposito di coalizioni governative, strategie di investimenti, controllo di compagnie ecc...

Diciamo che un problema della teoria dei giochi è costituito dalle cosiddette coalizioni bloccate (cioè non vincenti e non perdenti) ovvero dai blocking sets. Specialmente da questo punto di vista le geometrie finite ci vengono in aiuto.

Molte strutture geometriche classiche quali subpiani di Baer oppure le *superfici e curve Hermitiane* caratterizzate da Maria Tallini Scafati, ovvero gli *unitals* di Buekhenout, Mets e L.A. Rosati sono blocking sets, anzi blocking sets notevoli.

Passiamo ora ad una descrizione particolare dei contenuti della tesi.

I primi tre capitoli hanno carattere introduttivo.

Nel primo vengono esposti i principali concetti della teoria classica degli spazi affini e proiettivi, nonchè le principali proprietà combinatorie degli spazi finiti. Inoltre vengono definiti i caratteri di un K-insieme con alcune loro proprietà.

Nel secondo capitolo si introduce la nozione di Blocking sets. Con una breve parentesi storica.

Nel terzo vengono esaminate le proprietà dei Blocking Sets nei piani e negli spazi affini e proiettivi. Con i principali risultati fino ad ora noti.

Nel quarto capitolo vengono esposti alcuni dei risultati originali della tesi. Vengono descritti:

- un algortimo che permette di costruire un insieme di punti di spazi proiettivi (ed affini) non contenente rette dello spazio;
- un algoritmo di verifica che controlla se tale insieme interseca tutte le rette dello spazio.

In particolare si nota come questo algoritmo produca blocking set negli spazi affini e proiettivi nei casi PG(3,5) ed AG(2,5).

Inoltre vengono descritti i risultati ottenuti per PG(4,5) e, di conseguenza, per PG(5,5).

Nel quinto capitolo si introduce la nuova teoria che e' la parte centrale di questa tesi: lo studio di blocking set nel complementare di un arrangiamento di iperpiani.

Infine nell'appendice viene riportato il codice sorgente dell'algortmo, scritto nel linguaggio semicompilato Axiom.

Capitolo 1

Generalità sugli spazi proiettivi ed affini

1.1 Spazi Proiettivi

Dato un insieme **S**, sia $\mathcal{B}$ un insieme di parti di **S** (chiameremo punti gli elementi di **S** e rette gli elementi di $\mathcal{B}$) tali che siano soddisfatti i seguenti assiomi:

1. dati due punti distinti P e Q, esiste una ed una sola retta PQ che li contiene entrambi;

2. ogni retta contiene almeno tre punti;

3. date due rette r ed s aventi un punto in comune P, siano A,B punti di r e C,D punti di s, con A,B,C,D,P tutti distinti. Allora le rette AC e BD hanno un punto in comune.

Si noti che due rette distinte non possono avere più di un punto in comune.

Chiameremo sottospazio di $\mathbf{S}$ ogni insieme $T \subset \mathbf{S}$ che soddisfi la condizione:

$$\text{dati} P, Q \in T \text{con} P \neq Q, \text{ allora } PQ \subseteq T. \tag{1.1}$$

Esempi di sottospazi sono l'insieme vuoto, tutti gli insiemi formati da un solo punto (questi insiemi saranno nel seguito identificati con il loro unico elemento, per cui parleremo dei punti di $\mathbf{S}$ come sottospazi), tutte le rette di $\mathbf{S}$ determina allora l'insieme $\mathcal{P}$ di tutti i sottospazi di $\mathbf{S}$: chiameremo spazio proiettivo la coppia $\mathbf{P}$=($\mathbf{S}$,$\mathcal{P}$) determinata in questo modo.

Per la (1.1) l'intersezione di due sottospazi è ancora un sottospazio; dato comunque un sottoinsieme U di $\mathbf{S}$ possiamo definire il sottospazio generato da U (indicato con $< U >$) come l'intersezione di tutti i sottospazi di $\mathbf{S}$ contenenti U). Dati due sottospazi T ed U si definisce: $T \vee U =< T \cup U >$. Abbiamo così che:

Teorema 1.1. *La coppia $(\mathcal{P}, \subseteq)$ è un reticolo complementato e modulare (quindi con dimensione), avente il vuoto come minimo ed $\boldsymbol{S}$ come massimo.*

Nel seguito faremo sempre l'ipotesi che $(\mathcal{P}, \subseteq)$ sia a catene limitate finite, cioè che, fissati comunque due sottospazi T ed U con $T \subseteq U$, non esista alcuna catena infinita del tipo $T \subset T_1 \subset \cdots \subset U$. Allora, dato un sottospazio T, ogni catena massimale $\emptyset \subset T_1 \subset \cdots \subset T$ è formata dallo stesso numero di sottospazi non vuoti, che si dice rango di T e si indica con rg(T). Definiamo quindi la dimensione di T come dim(T):= rg(T)-1 e la dimensione di $\mathbf{P}$ come la dimensione di $\mathbf{S}$.

Indicheremo con $\mathbf{P}_r$ uno spazio proiettivo di dimensione r e con $\mathbf{S}_h$ un generico sottospazio di dimensione h. Un sottospazio di dimensione 2 viene detto piano, un sottospazio di dimensione r-1 iperpiano.

Si dimostra facilmente che sottospazi della stessa dimensione hanno la stessa cardinalità. Quando $\mathbf{S}$ è un insieme finito diremo che $\mathbf{P}$ ha ordine q se ognuna delle sue rette ha cardinalità q+1 e scriveremo $\mathbf{P} = \mathbf{P}(r, q)$.

Dato un insieme di punti $T = \{P_0, P_1, \ldots, P_h\}$ diremo che esso è formato da punti indipendenti se, per ogni P_i, abbiamo che $\P_i \notin < T \setminus \{P_i\} >$. Un insieme di punti indipendenti che generano uno spazio vengono detti una base di quello spazio.

Dato uno spazio proiettivo $\mathbf{P_r}$ sia $\mathbf{P}' = (\mathbf{S}, \mathcal{P}')$ un altro spazio proiettivo tale che:

1. $\mathcal{S}' \subseteq \mathcal{S}$
2. per ogni retta $r' \in \mathcal{P}'$ esiste una retta $r \in \mathcal{P}$ tale che $r' \subseteq r$

allora $\mathbf{P}'$ si dice una subgeometria di $\mathbf{P}$. Ogni sottospazio di $\mathbf{P}$ è una subgeometria, ma l'inverso non è vero: ad esempio $\mathbf{P}$ con dim($\mathbf{P}$)=r ammette subgeometrie di dimensione r. In particolare se r=2 si dirà che $\mathbf{P}' \subset \mathbf{P}$ e' un subpiano di Baer se $\mathbf{P}'$ è una subgeometria di dimensione 2 massimale rispetto all'inclusione.

Abbiamo visto che il reticolo $(\mathcal{P}, \subseteq)$ è modulare; allora, dato $\mathbf{P} = (\mathbf{S}, \mathcal{P})$, il reticolo duale $(\mathcal{P}, \supseteq)$ è ancora un reticolo ed è il reticolo dei sottospazi di uno spazio proiettivo $\mathbf{P}^* = (\mathbf{S}^*, \mathcal{P}^*)$, che si dice spazio duale di $\mathbf{P}$. Si ha il seguente:

Teorema 1.2. ***Principio di dualità*** *Data una proprietà* $\tau = \tau(\mathbf{P_r}, \mathbf{S_{h_1}}, \ldots, \mathbf{S_{h_n}}, \subseteq, \vee, \cap)$ *concernente sottospazi di date dimensioni* $h_1, \ldots, h_n$ *di* $\mathbf{P_r}$ *e le loro inclusioni,intersezioni e congiungenti, che risulta vera per ogni* $\mathbf{P_r}$*, risulta vera anche la proprietà duale* $\tau^* = \tau(\mathbf{P_r}, \mathbf{S_{r-1-h_1}}, \ldots, \mathbf{S_{r-1-h_n}}, \supseteq, \cap, \vee)$.

Dati due spazi proiettivi, chiameremo collineazione tra i due spazi, una biiezione che mantiene l'allineamento dei punti.

1.2 Spazi Affini

Dato uno spazio proiettivo $\mathbf{P} = (\mathbf{S}, \mathcal{P})$ di dimensione r sia Π un fissato iperpiano di $\mathbf{P}$ (iperpiano all'infinito). Chiameremo spazio affine associato allo spazio proiettivo $\mathbf{P}$ la coppia $\mathbf{A} = (\mathbf{S}, \mathcal{P}')$, ove $\mathcal{S}' = \mathbf{S} \setminus \Pi$ e $\mathcal{P}' = \{T \setminus \Pi | T \in \mathcal{P}\}$. Di nuovo chiamiamo $\mathcal{S}'$ l'insieme dei punti e $\mathcal{P}'$ l'insieme dei sottospazi di $\mathbf{A}$. Abbiamo altresì che l'intersezione di due sottospazi è ancora un sottospazio, mentre è possibile definire la somma di due sottospazi in modo analogo al caso proiettivo.

Teorema 1.3. *L'insieme* $(\mathcal{P}', \subseteq, \cap, \vee)$ *risulta un reticolo sopramodulare (e quindi con dimensione) con* $dim(\mathcal{P}') = dim(\mathcal{P})$. *Se* $dim(\mathcal{P}') > 1$ *il reticolo non è sottomodulare.*

Indicheremo nel seguito con $\mathbf{A}_h$ un sottospazio affine di dimensione h.

Dato un $\S_h \in \mathcal{P}$, esso determina un $\mathbf{A}_h =_S b_h \setminus \Pi \in \mathcal{P}'$ ed un $\mathbf{S}_{h-1} =_S b_h \cap \Pi \in \mathcal{P}$ disgiunti. Chiameremo sottospazio all'infinito (o improprio) di $\mathbf{A}_h$ l'$\mathbf{S}_{h-1}$ corrispondente. In particolare, se $\mathbf{P} = \mathbf{P}(r, q)$ avremo che ogni retta di $\mathbf{P}$ intersecherà l'iperpiano all'infinito in un punto, quindi le rette di $\mathbf{A}$ avranno cardinalità q (diremo quindi che $\mathbf{A}$ ha ordine q).

Possiamo introdurre nell'insieme $\mathcal{P}'_h$ (insieme dei sottospazi di dimensione h) la relazione di parallelismo:

$$T_1 \parallel T_2 \Leftrightarrow T_1 \text{ e } T_2 \text{ hanno lo stesso sottospazio all'infito} \tag{1.2}$$

che risulta essere una relazione di equivalenza; più in generale, dati due qualsiasi sottospazi affini T_1 e T_2 diremo che i sottospazi sono paralleli se uno dei

rispettivi sottospazi all'infinito è incluso nell'altro (in questo caso la relazione non è più transitiva).

Negli spazi affini possiamo definire i concetti di dipendenza ed indipendenza di punti, subgeometria di uno spazio e collineazione tra spazi in modo analogo alle rispettive definizioni per gli spazi proiettivi.

1.3 spazi lineari sopra campi

Siano $\mathbf{W} = \mathbf{W}(r+1, \mathbb{K})$ uno spazio vettoriale di dimensione r+1 sopra un campo $\mathbb{K}$, $\mathbf{W}^* = \mathbf{W} \setminus \{\mathbf{0}\}$ $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. Definita in $\mathbf{W}^*$ la seguente relazione:

$$\mathbf{u} \equiv \mathbf{v} \Leftrightarrow \mathbf{u} = a\mathbf{v}; a \in \mathbb{K}^* \tag{1.3}$$

Si vede facilmente che la relazione $\equiv$ è di equivalenza, e che le classi di equivalenza determinate da essa sono i sottospazi 1-dimensionali di $\mathbf{W}$, privati dello $\mathbf{0}$. Porremo allora $\mathbf{S} = \mathbf{W}^* / \equiv$ e chiameremo punti gli elementi di $\mathbf{S}$. Un punto $\mathbf{P}$ sarà spesso denotato con $\mathbf{P}(\mathbf{w})$, dove $\mathbf{w} \in \mathbf{W}^*$ è un rappresentante di $\mathbf{P}$. Possiamo quindi introdurre la funzione:

$$\varphi : \mathbf{W}^* \longrightarrow \mathbf{S}; \mathbf{w} \longmapsto \mathbf{P}(\mathbf{w}). \tag{1.4}$$

Poniamo $\mathcal{P} = \{\varphi(\mathbf{V}) | \mathbf{V} < \mathbf{W}\}$, $\mathcal{B} = \{\varphi(\mathbf{V}) | \mathbf{V} < \mathbf{W}; dim(\mathbf{V}) = 1\}$; si verifica facilmente che la famiglia $\mathcal{B}$ verifica gli assiomi $P_1 - P_3$ e che:

Teorema 1.4. *La coppia* $\mathbf{P} = (\mathbf{S}, \mathcal{P})$ *così definita risulta essere uno spazio proiettivo.*

Chiameremo $\mathbf{P}''$ spazio proiettivo lineare di dimensione r sul campo $\mathcal{K}''$. Si noti che se $\mathbf{W}$ ha dimensione r+1 su $\mathbb{K}$ allora $\mathbf{P}$ ha dimensione r.

Dato che ogni spazio vettoriale $\mathbf{W}$ di dimensione r+1 su un campo $\mathbb{K}$ è isomorfo allo spazio vettoriale $\mathbf{K^{r+1}}$, abbiamo il seguente:

Teorema 1.5. *Dato un campo $\mathbb{K}$ esiste, a meno di isomorfismi, uno ed un solo spazio proiettivo su $\mathbb{K}$ per ogni dimensione r.*

Denoteremo con $\mathbf{PG}(r, \mathbb{K})$ tale spazio; se $\mathbb{K} = GF(q)$ scriveremo $\mathbf{P} = \mathbf{PG}(r, q)$; a volte scriveremo anche $\mathbf{P} = \mathbf{P}(\mathbf{W})$.

Denotato con $\mathcal{S}(\mathbf{W})$ il reticolo di tutti i sottospazi di $\mathbf{W}$, la funzione φ prima definita determina una corrispondente funzione:

$$\Phi : \mathcal{S}(\mathbf{W}) \longrightarrow \mathcal{P}; \mathbf{V} \longmapsto \varphi(\mathbf{V}). \tag{1.5}$$

che è un isomorfismo di reticoli. In particolare per ogni sottospazio $\mathbf{V} \subseteq \mathbf{W}$ si ha:

$$\dim_P(\Phi(\mathbf{V})) = \dim_K(\mathbf{V}) - 1. \tag{1.6}$$

Proposizione 1.1. *In $\mathbf{PG}(r, \mathbb{K})$ due punti $P(\mathbf{u})$, $P(\mathbf{v})$ sono indipendenti se e solo se i rispettivi rappresentanti $\mathbf{u}$, $\mathbf{u}$, sono indipendenti.*

Sia $\mathbf{W} = \mathbf{W}(r+1, \mathbb{K})$, e $\{P_0 = P(\mathbf{w}_0), P_1 = P(\mathbf{w}_1), \ldots, P_{r+1} = P(\mathbf{w}_{r+1})\}$ un insieme di r+2 punti di $\mathbf{P}(\mathbf{W})$, ad r+1 ad r+1 indipendenti. Dato che i $\mathbf{w}_0, \ldots, \mathbf{w}_r$ sono una base di $\mathbf{W}$, potremo scrivere $\mathbf{w}_{r+1} = \sum_{i=0}^{r} a_i \mathbf{w}_i$ con gli a_i univocamente determinati da $\mathbf{w}_{r+1}$. Il sistema $\{a_0\mathbf{w}_0, \ldots, a_r\mathbf{w}_r\}$ rappresenta ancora i punti $\{P_0, \ldots, P_r\}$, ed è tale che, dato un qualsiasi punto $P = P(\mathbf{w})$, possiamo scrivere $\mathbf{w}$ come combinazione lineare dei $a_i\mathbf{w}_i$. Dove i coefficienti sono determinati a meno di un fattore di proporzionalità $c \neq 0$ e dipendono solamente dai punti P_i e non dai loro rappresentanti: essi si dicono coordinate proiettive omogenee rispetto al riferimento $\{P_0, \ldots, P_{r+1}\}$. Diciamo quindi che in uno spazio lineare $\mathbf{P}(\mathbf{W})$ è dato un riferimento proiettivo

$\mathcal{R}$ quando sono dati r+2 punti $\{P_0, \ldots, P_{r+1}\}$ ad r+1 ad r+1 indipendenti e scriveremo $\mathcal{R}(P_0, \ldots, P_{r+1})$. I punti $P_0, \ldots, P_r$ si dicono punti fondamentali del riferimento ed hanno coordinate $(1, 0, \ldots, 0), \ldots (0, \ldots, 1)$, mentre P_{r+1} si dice punto unità del riferimento ed ha coordinate $(1, \ldots, 1)$.

Inoltre un cambiamento di coordinate in $\mathbf{W}$ ($X' = \mathbf{A}X$ con X, X' vettori colonna e $\mathbf{A} \in GL(r+1, \mathbb{K})$) determina un cambiamento di coordinate proiettive omogenee in $\mathbf{P}(\mathbf{W})$ ($X'a = \mathbf{A}X$ con $a \in \mathbb{K}^*$).

Un sottospazio $\mathbf{S}_h \in \mathbf{PG}(r, \mathbb{K})$ sarà descritto dalle soluzioni di un sistema di equazioni del tipo $\mathbf{H}X = 0$ con $\mathbf{H} \in M(r-h, r+1, \mathbb{K})$ matrice di rango r-k. In particolare un iperpiano sarà determinato da una equazione del tipo: $\sum_{i=0}^{r} u_i x_i = 0$.

Dati due spazi proiettivi $\mathbf{P}$ e $\mathbf{P}' = \mathbf{PG}(r, \mathbb{K})$, una applicazione lineare di $\mathbb{K}^{r+1}$ in se determina una trasformazione lineare proiettiva da $\mathbf{P}$ in $\mathbf{P}'$ che è una collineazione.

Più in generale,dato un automorfismo σ di $\mathbb{K}$, definiamo un'applicazione semilineare di $\mathbb{K}^{r+1}$ in se una biiezione f tale che $f(a\mathbf{u} + b\mathbf{v}) = \sigma(a)f(\mathbf{u}) + \sigma(b)f(\mathbf{v})$. L'applicazione proiettiva corrispondente verrà detta trasformazione semilineare proiettiva.

Quando $\mathbf{P} = \mathbf{P}'$ abbiamo che:

1. l'insieme di tutte le collineazioni di $\mathbf{PG}(r, \mathbb{K})$ è un gruppo;

2. l'insieme di tutte le trasformazioni semilineari proiettive di $\mathbf{PG}(r, \mathbb{K})$ é anch'esso un gruppo e verrà denotato con $P\Gamma L(r+1, \mathbb{K})$;

3. l'insieme di tutte le proiettività di $\mathbf{PG}(r, \mathbb{K})$ risulta un gruppo detto gruppo lineare generale proiettivo e denotato con $PGL(r+1, \mathbb{K})$.

È chiaro che $PGL(r+1, \mathbb{K}) \subseteq P\Gamma L(r+1, \mathbb{K})$. Inoltre abbiamo che:

Teorema 1.6. ***(teorema fondamentale della geometria proiettiva)*** *Il gruppo delle collineazioni di uno spazio proiettivo* $\mathbf{PG}(r, \mathbb{K})$ *in sè coincide con il gruppo* $P\Gamma L(r+1, \mathbb{K})$.

Dato uno spazio proiettivo $\mathbf{PG}(r, \mathbb{K})$ e fissato un suo iperpiani Π, lo spazio affine a lui associato sarà denotato con $\mathbf{AG}(r, \mathbb{K})$.

Assumendo che Π abbia equazione $x_0 = 0$, tutti i punti dello spazio affine avranno coordinata $x_0 \neq 0$ e quindi potranno essere rappresentati mediante una r-upla di coordinate proiettive non omogenee $(y_1, \ldots, y_r)$ con $y_i = x_i/x_0$. A partire da questa osservazione si ottine che i vettori e i laterali di $\mathbf{W} = \mathbb{K}^r$ costituiscono rispettivamente i punti e i sottospazi di $\mathbf{AG}(r, \mathbb{K})$. Inoltre si ha che ogni sottospazio è rappresentato da un sistema di equazioni $\mathbf{H}X = a$ con $\mathbf{H} \in M(r-h, r, \mathbb{K})$, matrice di rango r-h.

Chiameremo affinità tra due spazi affini una biiezione data dalla formula $Y' = \mathbf{M}Y + a$ con $M \in GL(r, \mathbb{K})$ ed $a \in \mathbb{K}$. L'insieme di tutte le affinità di $\mathbf{AG}(r, \mathbb{K})$ si dice gruppo lineare affine e viene denotato con $AGL(r, \mathbb{K})$.

1.4 Spazi Finiti, k-insiemi e caratteri

In uno spazio proiettivo $\mathbf{P}(r, q)$ il numero dei punti è dato da $\Theta_{r,q} = \sum_{i=0}^{r} q^i$ che coincide anche con il numero degli iperpiani (per dualità).

Mentre il numero degli spazi di dimensione d è dato da $\gamma_{r,d,q} = \Pi_{i=0}^{d} \frac{\Theta_{r-i,q}}{\Theta_{d-i,q}}$.

Analogamente nel caso affine si ha che il numero dei punti di $\mathbf{A}(r, q)$ è q^r e quello dei sottospazi di dimensione d è $q^{r-d}\gamma_{r-1,d-1,q}$.

Dato uno spazio proiettivo o affine $(\mathbf{S}, \mathcal{P})$ ed un intero k con $0 < k \leq |\mathbf{S}|$, chiameremo k-insieme in $\mathbf{S}$ un generico insieme K di cardinalità k. Indicheremo inoltre con $\mathcal{P}_d$ la famiglia dei sottospazi $\mathbf{S}_d$ e con ρ_d la cardinalità di un $\mathbf{S}_d$.

Dato un k-insieme K, per ogni intero i con $0 \leq i \leq \rho_d$ esso determina la famiglia $\mathcal{P}_{d,i} = \{\mathbf{S}_d \in \mathcal{P}_d \text{ t.c. } |\mathbf{S}_d \cap K| = i\}$. È evidente che $\mathcal{P}_d = \bigcup_{i=0}^{\rho_d} \mathcal{P}_{d,i}$.

Rimangono quindi determinati $\rho_d + 1$ interi $t_0^d, \ldots, t_{\rho_d}^d$ che si dicono caratteri di K rispetto alla dimensione d. Diremo che K è di classe $[m_1, \ldots, m_h]$ se $t_i^d = 0$ per $i \notin \{m_1, \ldots m_h\}$; diremo inoltre che K è di tipo $(m_1, \ldots, m_h)$ se vale l'ulteriore condizione che $t_i^d \neq 0$ per $i \in \{m_1, \ldots m_h\}$

Nel seguito porremo $m^d = \min\{t_i^d | t_i^d \neq 0\}$ e $n^d = \max\{t_i^d | t_i^d \neq 0\}$; ometteremo inoltre gli indici relativi alla dimensione dove questo non dia luogo ad ambiguità.

In particolare si ha che se un insieme K di uno spazio affine o proiettivo $\mathbf{S}_r$ ha un solo carattere non nullo per una certa dimensione $0 < d < r$, allora K è vuoto oppure è tutto lo spazio. Valgono inoltre i seguenti:

Teorema 1.7. *Sia* $\mathbf{P} = \mathbf{P}(r, q)$ *uno spazio proiettivo e K un k-insieme di* $\mathbf{P}$. *Allora i caratteri di K soddisfano le equazioni:*

$$\sum_{i=0}^{n^d} t_i^d = \gamma_{r,d} \tag{1.7}$$

$$\sum_{i=1}^{n^d} i t_i^d = k\gamma_{r-1,d-1} \tag{1.8}$$

$$\sum_{i=2}^{n^d} i(i-1) t_i^d = k(k-1)\gamma_{r-2,d-2} \tag{1.9}$$

Teorema 1.8. *Sia* $\mathbf{A} = \mathbf{A}(r, q)$ *uno spazio affine e K un k-insieme di* $\mathbf{A}$. *Allora i caratteri di K soddisfano le equazioni:*

$$\sum_{i=0}^{n^d} t_i^d = q^{r-d}\gamma_{d-1,r-1} \tag{1.10}$$

$$\sum_{i=1}^{n^d} i t_i^d = k\gamma_{d-1,r-1} \tag{1.11}$$

$$\sum_{i=2}^{n^d} i(i-1) t_i^d = k(k-1)\gamma_{d-2,r-2} \tag{1.12}$$

Per i risultati enunciati in questo capitolo si possono consultare [1], [10], [31], [32], [45], [49].

Capitolo 2

Generalità sui Blocking Sets

2.1 Definizioni

Data una coppia $(\mathbf{S}, \mathcal{P})$ in cui $\mathbf{S}$ è un insieme e $\mathcal{P}$ l'insieme delle parti di $\mathbf{S}$, si definisce *Blocking Set* di $\mathbf{S}$ un sottoinsieme T di $\mathbf{S}$ tale che:

1. per ogni $r \in \mathcal{P}$ è $r \cap T \neq \emptyset$;

2. non esiste $r \in \mathcal{P}$ con $r \subseteq T$.

In particolare $(\mathbf{S}, \mathcal{P})$ può essere uno spazio proiettivo od affine in cui $\mathbf{S}$ è l'insieme dei punti e $\mathcal{P}$ l'insieme dei sottospazi di data dimensione.

È immediato notare che se T è un blocking set lo è anche il suo complemnentare.

In questa tesi ci occuperemo esclusivamente di blocking sets negli spazi affini e proiettivi e, prevalentemente, di blocking sets rispetto alle rette.

Un blocking set si dice *minimale* se per ogni suo punto P, l'insieme $T \setminus P$ non è più un blocking set.

Osserviamo che un blocking set T è minimale se e solo se per ogni suo punto passa almeno una unosecante.

2.2 Introduzione storica

Abbiamo accennato, nell'introduzione, che la genesi del concetto di blocking set si deve a Von Neumann e Morgenstein (rif [37]). Vediamo più nel dettaglio come è nato.

Nel loro lavor Von neumann e Morgenstein definiscono un gioco semplice su n persone nel modo seguente. Dato un insieme $\mathbf{S} = \{1, \ldots, n\}$ chiameremo *giocatori* i suoi elementi e *coalizioni* i suoi sottoinsiemi. Sia $\mathcal{P}$ l'insieme delle parti di $\mathbf{S}$; se $\mathcal{K} \in \mathcal{P}$ porremo:

$\mathcal{K}^+ = \{X \in \mathcal{P} | \exists K \in \mathcal{K}, K \subseteq X\}$ ($\mathcal{K}^+$ è la classe di tutte le coalizioni che hanno come sottoinsieme una coalizione di $\mathcal{K}$)

$\mathcal{K}^* = \{X \in \mathcal{P} | \exists K \in \mathcal{K}, X = S \setminus K\}$ ($\mathcal{K}^8$ è la classe di tutti i complementari delle coalizioni di $\mathcal{K}$).

Siano $\mathcal{W} \subseteq \mathcal{P}$ la classe di tutte le coalizioni vincenti ed $\mathcal{L} = \mathcal{P} \setminus \mathcal{W}$ la classe di tutte le coalizioni perdenti: lo scopo del gioco per gli n giocatori è appunto quello di formare una coalizione vincente.

Perchè il gioco abbia senso sono però richieste queste condizioni su $\mathcal{W}$ e $\mathcal{L}$:

1. $\mathcal{W} = \mathcal{W}^+$;
2. $\mathcal{W} \cap \mathcal{W}^* = \emptyset$;
3. $\mathcal{L} \cap \mathcal{L}^* = \emptyset$;
4. $\mathcal{W}$ deve contenere tutte le coalizioni formate da n-1 giocatori.

La prima condizione esprime il fatto che se ad una coalizione vincente vengono aggiunti dei giocatori, la nuova coalizione dovrà essere naturalmente ancora vincente; la quarta, inessenziale per i nostri scopi, evita che un solo giocatore possa vincere senza bisogno di coalizzarsi; la seconda e la terza insieme servono ad evitare che l'insieme di tutti i giocatori possa dividersi in due coalizioni entrambe vincenti o entrambe perdenti: si possono riformulare queste due condizioni nel modo seguente:

data una coalizione K, se $K \in \mathcal{W}$ allora $\mathbf{S} \setminus K \in \mathcal{L}$ e viceversa.

Va infine notato che, a causa della prima, il gioco risulta determinato quando sia dato insieme $\mathcal{W}^m$ delle coalizioni vincenti minimali; a causa delle prime due condizioni ogni coalizione minimale deve intersecare tutte le altre.

Secondo la descrizione in [37], quindi, il gioco finisce sempre con una coalizione vincente ed una perdente; i successivi sviluppi della teoria, però, pur mantenendo la seconda condizione hanno lasciato cadere la terza, sicchè è possibile che i giocatori si dividano in due coalizioni entrambe perdenti ottenendo quindi un risultato di parità: si definisce allora l'insieme $\mathcal{B} = \mathcal{L} \cap \mathcal{L}^*$ delle *coalizioni bloccanti*: se $\mathcal{B} = \emptyset$ il gioco è detto *forte* ed è un gioco nel senso di Von Neumann e Morgenstein.

Una *blocking coalition* (coalizione bloccante) corrisponde al nostro concetto di blocking set, in quanto deve intersecare tutte le coalizioni vincenti minimali (altrimenti la complementare sarebbe vincente), ma non deve contenerne nessuna (altrimenti sarebbe essa stessa vincente).

In [37] è indirettamente dimostrato che non esistono blocking sets in $\mathbf{PG}(2,2)$: infatti, nel tentativo di classificare tutti i possibili giochi in base al numero di giocatori, si esibisce, nel caso n=7, un gioco in cui l'insieme $\mathcal{W}^m$ è dato dalle rette di $\mathbf{PG}(2,2)$.

Nel 1956 M. Richardson pubblicò un articolo (vedi) in cui si definiva *gioco*

proiettivo finito un gioco su $n = \Theta_{r,q}$ giocatori in cui l'insieme $\mathcal{W}^m$ è dato da tutti i sottospazi di $\mathbf{PG}(r,q)$ di dimensione d, dove $d = r/2$ se r è pari e $d = (r+1)/2$ se r è dispari; veniva esaminato poi il caso $r = 2$ dimostrando esatta la congettura di Von Neumann (non esistono giochi proiettivi forti se $r = 2$ e $q \geq 3$, cioè esiste una blocking coalition in $\mathbf{PG}(2,q)$ se $q \geq 3$) e trovando alcuni limiti per la cardinalità di una blocking coalition.

I principali problemi che si ponevano erano laricerca del minimo possibile per la cardinalità di una blocking coalition in un dato spazio e del minimo e massimo possibili per la cardinalità dell'intersezione di una blocking coalition con una coalizione vincente minimale: fondamentale fu, a questo proposito, il lavoro di J. Di Paola sulle blocking coalition nei t-disegni e nei piani proiettivi: in vengono trovate le cardinalità minime per le blocking coalition nei piani proiettivi di ordine ≥ 9.

Successivamente A. Bruen (al quale si deve la sostituzione del termine blocking coalition con quello corrente di blocking set) insieme ad altri autori iniziò uno studio autonomo e sistematico dell'argomento, focalizzando l'attenzione sui piani proiettivi e riuscendo a trovare limitazioni per la cardinalità di un blocking set e per la cardinalità delle sue intersezioni con le rette del piano.

Un ulteriore sviluppo fu infine l'estensione dei problemi suddetti anche ai blocking sets nei piani affini e negli spazi affini e proiettivi a più dimensioni, avvenuta sopratutto per opera di G. Tallini (vedi , in cui si danno i primi teoremi di esistenza per blocking sets negli spazi affini, e) e di altri autori italiani.

Per altre informazioni circa i temi trattati in questa introduzione vedi , in cui vengono maggiormente approfonditi gli aspetti matematici della teoria dei giochi legati al concetto di blocking coalition. Un lavoro più recente (seb-

bene limitato ai soli piani proiettivi ed affini) è (1993), in cui sono riassunti i principali risultati, vengono presentate molte applicazioni della teoria dei blocking sets ad altri settori della matematica combinatoria (che non saranno qui esaminate) e viene fornita un'ampia bibliografia.

Va infine fatto notare che il termine *blocking set* non è usato in maniera univoca dai vari autori.

Coloro che usano la nostra terminologia chiamano *intersection set* un'insieme che soddisfa almeno la prima condizione (cioè un'insieme che interseca tutte le rette); altri autori chiamano invece blocking set il nostro intersection set, distinguendo tra trivial blocking set (insieme contiene qualche retta) e non-trivial blocking set (l'insieme corrispondente alla nostra definizione di blocking set).

inoltre, si usa comunemente il termine *t-blocking set* per indicare un insieme T che soddisfi la condizione

per ogni $r \in \mathcal{P}$ è $|r \cap T| \leq t$

e la condizione due definita prima (quindi i blocking sets propriamente detti sarebbero gli 1-blocking sets).

Anche il termine *minimale* non è adottato da tutti gli autori: per indicare lo stesso concetto sono usati anche *ridotto* ed *irriducibile*.

2.3 Insiemi di fissato tipo in un disegno. Caso dei blocking sets

Siano t, k, v, λ interi positivi con $2 \leq t < k < v$. Una coppia $(S, \mathcal{B})$, ove S è un v-insieme di elementi detti *punti* e $\mathcal{B}$ è una famiglia di parti di S detti blocchi, si dice un t-(v,k,λ) disegno se:

1. ogni blocco ha k punti;

2. ogni t-insieme è contenuto in esattamente λ blocchi.

Se $\mathcal{B}$ è la famiglia di tutti i k-sottoinsiemi, allora $(S, \mathcal{B})$ si dice completo, altrimenti incompleto.

Il numero r_s $(s = 0, 1, \ldots, t)$ dei blocchi contenenti un fissato s-insieme, è una costante data da:

$$r_s = \frac{\begin{pmatrix} v-s \\ t-s \end{pmatrix} \lambda}{\begin{pmatrix} k-s \\ t-s \end{pmatrix}} \tag{2.1}$$

Notiamo esplicitamente che ogni $t-(v,k,\lambda)$ disegno è in particolare un $s-(v,k,r_s)$ disegno, $s < t$.

Sia C un c-insieme di un $t-(v,k,\lambda)$ disegno $(S, \mathcal{B})$. Denotiamo con x_i il numero dei blocchi che sono i-secanti C con $0 \geq i \geq min\{c,k\}$. Contando le coppie (X, B), ove $|X| = s$ ed $X \subseteq B \cap C$ con $\mathcal{B}$, otteniamo le equazioni:

$$\sum_{i=s}^{k} \begin{pmatrix} i \\ s \end{pmatrix} x_i = \begin{pmatrix} c \\ s \end{pmatrix} r_s \tag{2.2}$$

ove $s = 0, 1, \ldots, t$; esse sono chiamate *equazioni cardinali* di un $|C|$-insieme.

Un problema interessante è quello di classificare un c-insieme avente dei determinati numeri di intersezione con i blocchi. Ricordiamo, dal primo capitolo, che un c-insieme C si dice di $classe[M]$ se $x_s = 0$ per ogni $s \in M$ e di $tipo(T)$ se inoltre $x_s \neq 0$ per ogni $s \in T$, dove M e T sono insiemi di interi non negativi.

Come esempio di un caratterizzazione di un insieme di dato tipo ricordiamo il *teorema di Segre*, affermante che un insieme di tipo $(0, 1, 2)$ in un piano proiettivo di ordine dispari è una conica.

Un c-insieme $C \subseteq S$ si dice una $\{c, m\}$-*calotta* (o anche *arco*) di $(S, \mathcal{B})$ se ciascun blocco incontra C in al più di m punti con $m < k$.

Il complementare di una $\{c, m\}$-*calotta* è incontrato in almeno $s = k - m$ punti e prende il nome di *intersection set di livello s*.

Con queste notazioni generali, un c-insieme C si dice *blocking set di livello (m,s)* se C è un m-intersection set ed S-C è un s-intersection set $(m, s > 1)$, cioè se per C si ha: $x_0 = x_1 = \cdots = x_{m-1} = x_{k-s+1} = \cdots = x_k = 0$.

Un blocking set di livello $(1, 1)$ si dice semplicemente blocking set. In una situazione così generale non vi sono molti risultati. Esiste una limitazione generale per la cardinalità di un blocking set in un $t - (v, k, \lambda)$ disegno, essenzialmente dovuto a David Drake.

Teorema 2.1. *Sia C un blocking set di un $t - (v, k, \lambda)$ disegno. Allora:*

$$|C| \geq v/2 - (1/2k)\sqrt{(v^2k^2 - 4v^2k + 4vk)}. \tag{2.3}$$

Drake in [25] prova il teorema per un $2 - (v, k, \lambda)$ disegno con $k \neq 3$. la prova er $k = 3$ appare in Eugeni-Mayer [27]. Inoltre è immediato constatare che, essendo la 2.3 indipendente da λ, basta applicarla allo stesso disegno pensato come un $2 - (v, k, r_{t-2})$ disegno. In [2] L. Berardi e A. Beutelspacher provano in particolare che:

Teorema 2.2. *In un $t - (v, k, \lambda)$ disegno completo esistono blocking sets di livello (l,m) se e solo se $v < 2k - (l + m)$. In questo caso ogni c-insieme con $v - k + l \leq c < k - m$ è un blocking set.*

Teorema 2.3. *Sia $\mathcal{D}$ un $2 - (v, 3, \lambda)$ disegno contenente blocking sets, allora $v = 4$, $\mathcal{D}$ è completo e i blocking sets sono i 2-insiemi.*

Teorema 2.4. *Sia $\mathcal{D}$ un $3 - (v, 4, \lambda)$ disegno contenente blocking sets C di livello (l,m), allora:*

1. *v è pari, l=m=1 e $|C| = v/2$;*

2. *v=5, $\lambda = 2$, $\mathcal{D}$ è completo e i blocking sets sono gli insiemi con 2 oppure 3 punti.*

I teoremi 2.3 e 2.4 sono stati ottenuti da Tallini in [48] nel caso $\lambda = 1$. Notiamo che esistono veramente pochi esempi di $3-(v,4,\lambda)$ disegni contenenti blocking sets.

Abbiamo informazioni solo nel caso di un $3-(v,4,1)$ disegno con $v = 8, 10, 14$.

Concludiamo questa sezione con un risultato che appare per la prima volta in [5] .

Sia $(S,\mathcal{B})$ un disegno. Definiamo la famiglia $\overline{\mathcal{B}} = \{S - B : B \in \mathcal{B}\}$. La coppia $(S,\overline{\mathcal{B}})$ è, come subito si prova un $t-(v,v-k,\lambda')$ disegno, con

$$\lambda' = \frac{\begin{pmatrix} v-k \\ t \end{pmatrix}\lambda}{\begin{pmatrix} k \\ t \end{pmatrix}} \tag{2.4}$$

detto, come ben noto, il *disegno complementare* di $(S,\mathcal{B})$.

Un blocking set C di $(S,\mathcal{B})$ si dice *regolare* se nè C nè S-C sono contenuti in un blocco di $\mathcal{B}$. Il seguente lemma è di immediata dimostrazione:

Lemma 2.1. *Un blocking set C di $(S,\mathcal{B})$ è regolare se e solo se C è un blocking set regolare di $(S,\overline{\mathcal{B}})$. In altre parole $(S,\mathcal{B})$ e $(S,\overline{\mathcal{B}})$ hanno gli stessi blocking sets regolari.*

A S. Innamorati [33] si devono i seguenti risultati:

Proposizione 2.1. *Ogni 5-insieme non contenuto in un blocco di un 4-(11,6,3) disegno ha esattamente un blocco esterno.*

Teorema 2.5. *Ogni 4-(11,6,3) disegno può essere immerso in uno ed un sol modo in un sistema di Steiner S(5,6,12).*

Capitolo 3

Blocking sets negli Spazi Proiettivi ed Affini

3.1 Blocking sets nei piani proiettivi

Abbiamo visto che in un piano proiettivo π_q di ordine q si chiama *blocking set* ogni insieme di punti non contenente rette, ma intersecato da ogni retta e che il complementare di un blocking set è ancora un blocking set.

Inoltre abbiamo visto nel precedente capitolo che un blocking set si dice *irriducibile* se esso non contiene propriamente blocking sets, ovvero per ogni punto passa almeno una tangente.

Proposizione 3.1. *In π_q esistono blocking sets se e solo se $q \geq 3$.*

Una dimostrazione di questo risultato si trova in [5] .

In [14], [15], [16] l'autore dimostra il seguente risultato

Teorema 3.1. *Sia C un blocking set di un piano proiettivo, allora*

$$q + \sqrt{q} + 1 \leq |C| \leq q^2 - \sqrt{q} \tag{3.1}$$

il segno uguale a sinistra (destra) valendo se e solo se C è un subpiano di Baer (il complemento di un subpiano di Baer).

Mentre in [20] [48] gli autori dimostrano separatamente che:

Teorema 3.2. *Sia C un blocking set irriducibile di un piano proiettivo finito, allora*

$$|C| \leq q\sqrt{q} + 1 \tag{3.2}$$

il segno uguale valendo se e solo se C è unital.

Quest'ultimo risultato è anche conseguenza di un lavoro di M. Tallini Scafati sulle curve Hermitiane [39], [40]. Si noti che gli ultimi due teoremi sono stati generalizzati per i disegni simmetrici (si veda [5] per approfondimenti).

Per quanto riguarda la minima cardinalità possibile e relativamente ai piccoli ordini si hanno le seguenti informazioni: per $q = 5, 7, 8$ le cardinalità minime possibili sono $6, 12, 13$ rispettivamente, come provato direttamente in Hirshefeld [32]. Introduciamo ora la funzione:

$$m(q) := \begin{cases} \sqrt{q} & \text{se } q = p^{2h} \text{ p primo} \\ (q+1)/2 & \text{se } q = p \\ p^{2h+1} - p^d & \text{se } q = p^{2h+1} \\ & \text{e } d := \max\{\delta : \delta | 2h+1, \delta \neq 2h+1\} \end{cases} \tag{3.3}$$

Osservazione 3.1. *I blocking sets in* $\mathbf{PG}(2,q)$ *di cardinalità q+1+m(q) sono i blocking sets di minima cardinalità nota. Se q è quadrato, essi realizzano proprio il minimo, negli altri casi non si sa se ce ne siano di più piccoli. Se q=p un esempio di blocking set con p+1+m(p) punti è un triangolo proiettivo mentre nel caso* $q = p^{2h+1}$ *un esempio è in [32]*

I seguenti teoremi riguardano essenzialmente il caso desarguesiano.

Teorema 3.3. ***Teorema di Copertura*** *(L.Berardi e F. Eugeni [35]). In* $\mathbf{PG}(2,q)$ *per ogni intero* k *con* $q+1+m(q) \leq k \leq q^2 - m(q)$ *esiste almeno un blocking set di cardinalità* k*.*

Teorema 3.4. *(A. Blokhuis e A. Brouwer [35]). Sia* C *un blocking set di* $\mathbf{PG}(2,q)$ *con* $|C| = q+n$*,* $q \geq 7$ *dispari e* $n > 1$*. Supponiamo che* C *sia privo di rette* n*-secanti. Allora*

$$|C| > q + \sqrt{2q} + 1. \tag{3.4}$$

Se invece $q = 2^{2h+1}$ *risulta:*

$$|C| > 2^{2h+1} + 2^{h+1}. \tag{3.5}$$

Si ha, dai risultati precedenti,

Teorema 3.5. *Se* $q \geq 7$ *è dispari e non quadrato allora in* $\mathbf{PG}(2,q)$ *è':*

$$|C| > q + \sqrt{2q} + 1. \tag{3.6}$$

La dimostrazione di questo teorema si trova in [5].

Ci si può chiedere se esista un teorema di copertura per i blocking sets irriducibili C, per i quali sia $q + 1 + \sqrt{q} \leq |C| \leq q\sqrt{q} + 1$. Ad esempio se $q = 4$ per ogni cardinalità ammissibile 7, 8, 9 vi è un blocking set irriducibile [6]. Riguardo a questo problema Bruen e Silvermann [19] hanno provato che :

Teorema 3.6. *Sia* C *un blocking set in* $\mathbf{PG}(2,q)$ *con* q *quadrato e* $|C| = q + \sqrt{q} + 1 + t$ *dove* $0 < t < \sqrt{2q} - \sqrt{q} - 1/2q$*. Allora* C *contiene un subpiano di Baer (ed è quindi riducibile).*

Questo teorema esprime il fatto che per piccoli spostamenti dalla cardinalità di un subpiano di Baer, si hanno blocking sets riducibili.

Nel caso dei piani proiettivi è abbastanza semplice vedere che il complementare di un blocking set irriducibile è sempre riducibile (cf. [46], [48]).

Concludiamo evidenziando un interesante legame tra i blocking sets e k-archi complementi, costituito dal teorema di Bruen e Fischer [17]. Questo teorema è stato generalizzato nel caso ei disegni simmetrici da Eugeni ed Innamorati (cf. [26]).

Sia $\mathcal{K}$ un k-arco completo, cioè un insieme di punti di classe $[0, 1, 2]$ non propriamente immergibile in un altro arco. È noto che $|\mathcal{K}| \geq q + 2$, l'eguaglianza valendo se e solo se $\mathcal{K}$ è un *iperovale* (insieme di tipo $(0, 2)$). Si prova facilmente che:

Teorema 3.7. *Sia $\mathcal{K}$ un k-arco completo di un piano proiettivo π_q con $|\mathcal{K}| \leq q + 1$. Le corde di $\mathcal{K}$ formano nel piano duale un blocking set.*

Chiameremo *Blocking set derivato* da un k-arco un blocking set così costruito. Sussiste il seguente teorema caratterizzante i suddetti blocking sets.

Teorema 3.8. *(A. Bruen e C.Fisher [17]). Un blocking set C è derivato da un k-arco se e solo se valgono le seguenti condizioni:*

1. $|C| \leq k(k-1)/2$;
2. *il numero delle rette (k-1)-secanti è almeno k;*
3. *tre rette (k-1)-secanti non sono mai concorrenti.*

Una descrizione particolareggiata dei blocking sets in $\mathbf{PG}(2, q)$ per q piccolo può essere trovata nella tesi di laurea di N. Cassetta (cf. [21]).

3.2 Blocking sets nei piani affini.

Abbiamo visto che in $\mathbf{AG}(r,q)$ un blocking set è un insieme di punti incontrato da ogni spazio s-dimensionale in almeno un punto. Il seguente risultato è fondamentale per il seguito:

Teorema 3.9. *(R. Jamison [34], A. Brouwer-A. Schrijver [13]). Sia C un (r-1)-intersection set di* $\mathbf{AG}(r,q)$*, allora*

$$|C| \geq rq - (r-1). \tag{3.7}$$

Nel caso r=2, un intersection set ha, nel caso desarguesiano, almeno $sq-1$ punti. Segue che una siffatta limitazione vale anche per i blocking sets.

Osservazione 3.2. *Sia C un intersection set di un piano affine (desarguesiano o no) contenente una retta, allora* $|C| \geq 2q-1$*. (Basta considerare le q-1 parallele alla retta contenuta.)*

I piani affini $\mathbf{AG}(2,2)$ *ed* $\mathbf{AG}(2,3)$ *non hanno blocking sets, come si prova facilmente direttamente.*

In [3], completando un risultato di G. Tallini [47], è stato provato che $\mathbf{AG}(2,4)$ *contiene un unico tipo di blocking set: la parabola hermitiana (in* $\mathbf{PG}(2,4)$ *si fissa una curva hermitiana, che in questo caso è un triangolo privato dei vertici e si toglie una tangente, ottenendo un 8-insieme in un piano affine: la parabola hermitiana).*

Se $q \geq 5$ si sa che:

Teorema 3.10. *(L. Berardi e F. Eugeni [3]). In* $\mathbf{AG}(2,q)$*,* $q \geq 5$*, esistono blocking sets con c punti se e solo se* $2q-1 \leq c \leq (q-1)^2$*.*

Bruen e de Resmini in [18] hanno costruito nel piano di Hughes di ordine 9, non desarguesiano, blocking sets di cardinalità inferiore a 2q-1. Il problema generale di una limitazione nei piani non desarguesiani è completamente aperto.

Una descrizione particolareggiata dei blocking sets in $\mathbf{AG}(2,q)$ per q piccolo può essere trovata nella tesi di laurea di N. Cassetta (cf. [21]).

3.3 Blocking sets negli spazi affini e proiettivi

In questo paragrafo $\Sigma = \Sigma(r,q)$ denota uno spazio proiettivo o affine di dimensione r ed ordine q. Generalizzando la definizione data in precedenza, un insieme C di punti di Σ si chiama un *t-blocking set di livello l* se ogni sottospazio t-dimensionale di Σ ha almeno l punti in comune con C e $\Sigma \setminus C$.

Si dimostrano facilmente i seguenti risultati:

Proposizione 3.2. *In uno spazio affine o proiettivo di dimensione $r > 2$, l'intersezione tra un blocking set C e uno sottospazio S_d di dimensione $d > 1$ è un blocking set in S_d.*

Proposizione 3.3. *Sia S_{r-1} un iperpiano di $\mathbf{PG}(r,q)$ $(r > 2)$. Se C_1 è un blocking set in $\mathbf{AG}(r,q) = \mathbf{PG}(r,q) \setminus S_{r-1}$ e C_2 è un blocking set in S_{r-1}, allota $C_1 \cup C_2$ è un blocking set in $\mathbf{PG}(r,q)$.*

Corollario 3.1. *Se esistono blocking sets in $\mathbf{PG}(r,q)$ ed in $\mathbf{AG}(r+1,q)$ allora esistono blocking sets in $\mathbf{PG}(r+1,q)$.*

Usando la teoria di Ramsey è stato provato che:

Teorema 3.11. *(F. Mazzocca- G. Tallini [36]). Esiste una funzione b(t,q) che dipende solo da t,q e dalla natura affine o proiettiva, tale che $\Sigma(r,q)$ contiene t-blocking sets se e solo se $r \leq b(t,q)$.*

È facile provare che in $\mathbf{AG}(r,2)$, $\mathbf{AG}(r,3)$ e $\mathbf{PG}(r,2)$ non vi sono blocking sets, in $\mathbf{AG}(r,4)$ e $\mathbf{PG}(r,3)$ vi sono solo se $r=2$, in $\mathbf{AG}(r,5)$ vi sono blocking set (cf. [23]) mentre per $\mathbf{PG}(r,4)$ N. Cassetta in [22] dimostra che esistono blocking sets solo se $r=2$, provando che $\mathbf{PG}(3,4)$ non ha blocking set. In particolare questo chiude il caso $\mathbf{AG}(3,q)$ e $\mathbf{PG}(3,q)$ essendo noto che $\mathbf{AG}(3,q)$ ammette blocking set per $q>5$ e $\mathbf{PG}(3,q)$ per $q>4$.

Un altro risultato generale è il seguente:

Teorema 3.12. *(A. Beutelspacher-F. Eugeni [9]). Se $q \geq 2^r$, allora in $\mathbf{AG}(r,q)$ ed in $\mathbf{PG}(r,q)$ esistono t-blocking sets.*

Un risultato intermedio é il seguente:

Teorema 3.13. *Se $\mathbf{AG}(r,q)$ contiene un blocking set di livello 2^h, allora $\mathbf{AG}(r+1,q)$ contiene un blocking set di livello 2^{h-1}.*

Capitolo 4

Un algoritmo per la ricerca di Blocking sets

4.1 Risultati noti

Dal capitolo precedente si ottengono, per l'esistenza di Blocking sets in $PG(r,q)$ e $AG(r,q)$ rispettivamente, le due tabelle qui sotto.

Da queste tabelle si osserva che il problema dell'esistenza di Blocking sets

$q \diagdown r$	2	3	4	5	6	7	...
2	no	no	no	no	no	no	...
3	si	no	no	no	no	no	...
4	si	no	no	no	no	no	...
5	si	si	?	?	?	?	...
7	si	si	?	?	?	?	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabella 4.1: Esistenza di Blocking sets in PG(r,q)

$q \diagdown r$	2	3	4	5	6	7	...
2	no	no	no	no	no	no	...
3	no	no	no	no	no	no	...
4	si	no	no	no	no	no	...
5	si	si	?	?	?	?	...
7	si	si	?	?	?	?	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabella 4.2: Esistenza di Blocking sets in AG(r,q)

è ancora un problema aperto e di difficile soluzione.

In questo capitolo descriveremo l'algoritmo che ci ha permesso di trovare ulteriori Blocking sets in $PG(3, q)$ per $q > 4$.

4.2 Descrizione dell'algoritmo

La procedura che descriviamo può essere riassunta nei seguenti passi:

1. la prima funzione ha in entrata due numeri interi che rappresentano, rispettivamente, q ed r in $PG(r, q)$. Il risultato è una lista *ordinata* di tutti i punti di $PG(r, q)$.

   Chiameremo questa lista $PGrq$ ($AGrq$) e indicheremo con $\sharp PGrq$ la sua cardinalità.

2. La seconda funzione ha in entrata le liste $PGrq$; una lista data dai quozienti modulo q (si suppone di essere in $\mathbb{Z}_q$), cioè una lista di liste tale che la i-esima lista contiene nella j-esima posizione i/j modulo q; quindi gli interi q ed r.

In uscita questa funziona dà una matrice di tutte le rette di $PG(r,q)$.

In particolare la matrice ha $\sharp PGrq$ righe e $(q-1)*\sharp PGrq$ colonne; la i-esima colonna rappresenta il punto P_i di $PG(r,q)$ che si trova in posizione i nella lista $PGrq$. Infine per $1 \leq i < j \leq \sharp PGrq$ le entrate $(q-1)*(j-1)+1,\ldots,(q-1)*j$ della i-esima colonna sono le posizioni occupate in $PGrq$ dai punti della retta di $PG(r,q)$ passante per P_i e P_j.

Ovviamente tutte le altre entrate sono 0.

Chiameremo $MRettePGrq$ questa matrice.

3. La terza funzione ha per entrate $PGrq$, la lista dei quozienti, gli interi q ed r e la matrice $MRettePGrq$.

   La risultante di questa funzione è una lista di interi che rappresentano le posizioni di alcuni punti particolari in $PGrq$. Ossia è un sottoinsieme di $PG(r,q)$ che chiamiamo *blocco*.

   Questo sottoinsieme viene costruito *ordinatamente* a partire dal primo punto della lista $PGrq$; progressivamente secondo l'ordine in $PGrq$ si prende il punto i-esimo P_i della lista e

   - se tutte le rette per P_i hanno almeno un punto in *blocco* si itera (ossia il punto viene scartato)
   - altrimenti si controlla se il punto completa una retta insieme ad altri punti che già sono in *blocco*,
   - se completa una retta si itera
   - altrimenti si aggiunge il punto a *blocco* e nella matrice $MRettePGrq$

vengono azzerate tutte le entrate corrispondenti a rette passanti per P_i.

In questo modo si garantisce che *blocco* non contenga nessuna retta.

Inoltre la matrice $MRettePGrq$ viene trasformata in una matrice $MnuovoPGrq$ che ha entrate nulle quasi-ovunque.

4. L'ultima funzione è una funzione di controllo, ha come entrate la matrice trasformata $MnuovoPGrq$, l'insieme *blocco* e q. L'uscita di questa funzione è un booleano 0 o 1, il risultato è 0 se tutte le rette di $PG(r,q)$ passano per almeno un punto in *blocco*, 1 altrimenti.

Da quanto detto si deduce che, se dal controllo si ottiene 0, allora *blocco* è un blocking set in $PG(r,q)$.

Utilizzando questo algoritmo si sono trovati un blocking sets in $PG(3,5)$ ed $AG(2,5)$.

Si osserva immediatamente che esso dipende strettamente dall'ordine con cui vengono presi i punti in $PG(r,q)$.

Quindi cambiando l'ordinamento si ottengono blocking set diversi e di diversa cardinalità.

Purtroppo questo algoritmo, sebbene fornisca molti esempi di Blocking set nel caso proiettivo, è solo una condizione necessaria, ma non sufficiente. Infatti il fatto di non trovare blocking set NON è in nessun modo una prova del fatto che non ne esistano.

Inoltre, mentre nel caso proiettivo l'algoritmo dà sempre ottimi risultati, l' analogo nel caso affine non fornisce risultati altrettanto interessanti. Infatti già nel caso di $AG(3,5)$ scegliendo casualmente l'ordine dei punti non si ottengono blocking set, pur essendo la loro esistenza nota a priori.

4.3 Ulteriori risultati in PG(4,5) e PG(5,5)

Nel caso di $PG(4,5)$ e $PG(5,5)$ il nostro algoritmo non fornisce nessun blocking set, almeno per gli ordinamenti scelti, che sono comunque solo una minoranza.

Per quanto detto questa non è una prova della NON esistenza di Blocking sets in $PG(4,5)$ e $PG(5,5)$ per cui si ha solo una congettura:

Congettura: La funzione $b(t,q)$ definita nel Teorema 3.11 è una funzione crescente e per $t=1$ si ha che

$$b(t,q) = q_{min} - 1 \text{ dove } q_{min} = min\{p | p \text{ primo e } p \leq q\}.$$

Dallo studio dei caratteri nel caso di $PG(4,5)$ e $PG(5,5)$ si sono comunque ottenuti interessanti risultati parziali.

Le uguaglianze 1.7 danno dei sistemi di equazioni con la seguente tavola di valori:

$$\begin{aligned} &\text{per } r=2 \text{ allora } \gamma_{r,d} = 31, \gamma_{r-1,d-1} = 6, \quad 9 \leq k \leq 22 \\ &\text{per } r=3 \text{ allora } \gamma_{r,d} = 806, \gamma_{r-1,d-1} = 31, \quad 31 \leq k \leq 125 \\ &\text{per } r=5 \text{ allora } \gamma_{r,d} = 508431, \gamma_{r-1,d-1} = 781, \quad 781 \leq k \leq 3125 \end{aligned} \tag{4.1}$$

dove k, come sempre, indica la cardinalità dell'insieme K considerato. In questi sistemi di equazioni supponiamo $t_0 = t_6 = 0$ e da ora in poi considereremo solo i caratteri t_i per $0 < i < 6$.

Ricordiamo inoltre che se K è un blocking set in $PG(r,q)$ allora lo è anche il suo complementare. In particolare, indicato con K^c il complementare di K vale la seguente relazione tra i caratteri:

$$t_i(K) = 0 \Leftrightarrow t_{q+1-i} = 0 \tag{4.2}$$

Risolvendo questi sistemi per ogni possibile cardinalità di K, otteniamo, nel caso di $PG(2,5)$, i seguenti risultati:

1. non ci sono soluzioni nel caso che ci siano più di 2 caratteri distinti nulli;

2. se $t_1 = t_4 = 0$ allora ci sono soluzioni se e solo se $k = 13, 15, 16, 18, 19, 21, 22$;
   In tutti gli altri casi in cui ci sono esattamente 2 caratteri nulli non ci sono soluzioni;

3. se $t_5 = 0$ o $t_4 = 0$ allora vi sono soluzioni se e solo se $8 < k < 18$;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_2 = 0$ o $t_1 = 0$ allora esistono soluzioni se e solo se $17 < k < 23$.

Dai conti sopra, tenendo conto della relazione 4.2 si ricava per $PG(2, 5)$:

1. non ci sono soluzioni nel caso che ci siano più di 1 carattere non nullo;

2. se $t_5 = 0$ o $t_4 = 0$ allora vi sono soluzioni se e solo se $8 < k < 14$;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_2 = 0$ o $t_1 = 0$ allora esistono soluzioni se e solo se $17 < k < 23$.
   In particolare i blocking set per $t_2 = 0$ o $t_1 = 0$ si ottengono come complementari di quelli per cui $t_5 = 0$ o $t_4 = 0$.

Per $PG(3, 5)$:

1. non ci sono soluzioni nel caso che ci siano più di 2 caratteri distinti nulli;

2. se $t_1 = t_4 = 0$ allora ci sono soluzioni se e solo se $k = i + 29$ per $i =$
   $39, 40, 42, 43, 45, 46, 48, 49, 51, 52, 54, 55, 57, 58, 60, 61, 63, 64, 66, 67, 69, 70, 72, 73, 75, 76,$
   $78, 79, 81, 82, 84, 85, 87, 88, 90$;
   In tutti gli altri casi in cui ci sono esattamente 2 caratteri nulli non ci sono soluzioni;

3. se $t_5 = 0$ ci sono soluzioni se e solo se $37 < k < 89$;
   se $t_4 = 0$ o $t_2 = 0$ ci sono soluzioni se e solo se $32 < k < 124$;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_1 = 0$ ci sono soluzioni se e solo se $67 < k < 120$;

Come per $PG(2, 5)$, anche nel caso di $PG(3, 5)$ dalla relazione 4.2 si ricava che:

1. non ci sono soluzioni nel caso che ci siano più di 1 carattere non nullo;

2. se $t_5 = 0$ allora vi sono soluzioni se e solo se $37 < k < 89$;
   se $t_4 = 0$ o $t_2 = 0$ ci sono soluzioni se e solo se $32 < k < 124$;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_1 = 0$ ci sono soluzioni se e solo se $67 < k < 119$; In particolare i blocking set per $t_2 = 0$ o $t_1 = 0$ si ottengono come complementari di quelli per cui $t_5 = 0$ o $t_4 = 0$.

Per $PG(4, 5)$ dai conti fatti per i casi precedenti e dalla relazione 4.2 si ottiene:

1. non ci sono soluzioni nel caso che ci sia più di 1 carattere nullo;

2. se $t_5 = 0$ allora ci sono soluzioni se e solo se k é compreso tra alcuni valori precisi;
   se $t_4 = 0$ o $t_2 = 0$ allora ci sono soluzioni se e solo se k é compreso tra alcuni valori precisi ;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_1 = 0$ ci sono soluzioni se e solo se k é compreso tra alcuni valori precisi.

Infine per $PG(5,5)$ da calcoli diretti, dai conti fatti per i casi precedenti e dalla relazione 4.2 si ottiene:

1. non ci sono soluzioni nel caso che ci sia più di 1 carattere nullo;

2. se $t_5 = 0$ allora ci sono soluzioni se e solo se $924 < k < 2201$;
   se $t_4 = 0$ o $t_2 = 0$ allora ci sono soluzioni se e solo se $825 < k < 3081$;
   se $t_3 = 0$ non ci sono soluzioni;
   se $t_1 = 0$ ci sono soluzioni se e solo se $1705 < k < 2982$.

Il caso in cui tutti i caratteri siano non nulli è ovviamente più complicato e laborioso.

Questi risultati non danno indicazioni sull'esistenza o meno di possibili blocking sets, ma, nel caso esistano, danno comunque una buona descrizione di come questi dovrebbero essere.

Capitolo 5

Blocking sets nel complementare di arrangiamenti di iperpiani

In questo capitolo, che è anche il capitolo centrale della tesi, diamo le linee principali di quella che è una nuova teoria all'interno dello studio dei Blocking Sets.

Questa ricerca è stata motivata da un duplice interesse.

Da una parte l'osservazione che essa è la naturale estensione di una ricerca che è già di notevole interesse: lo studio di Blocking Sets negli Spazi Affini.

Dall'altra l'interesse sempre maggiore dimostrato dalla comunità scentifica intorno alla teoria degli Arrangiamenti di Iperpiani.

5.1 Arrangiamenti di iperpiani in PG(n,q)

Chiamiamo Arrangiamento di iperpiani in $PG(n,q)$ un insieme $\mathcal{A} = \{H_1, \ldots, H_m\}$ di iperpiani di $PG(n,q)$.

Il complementare di un arrangiamento di iperpiani è l'insieme di punti:

$$M(\mathcal{A}) = PG(n,q) \setminus \cup_{i=1,\dots m} H_i$$

Per una trattazione di base completa sulla teoria degli arrangiamenti di iperpiani si rimanda a [38].

Un arrangiamento di iperpiani che riveste particolare interesse nella teoria classica è l'arrangiamento degli iperpiani di riflessione dello spazio. Questo arrangiamento è anche detto *arrangiamento delle trecce*.

Sia $PG(n+1,q)$ lo spazio proiettivo i cui punti sono le $n+2$-uple $(x_0, x_1, \dots, x_{n+1})$; l'arrangiamento delle trecce è l'arrangiamento $\mathcal{A}(A_{n,q}) = \{H_{i,j}\}_{1 \le i < j \le n+1}$ i cui iperpiani $H_{i,j}$ hanno equazione $\alpha_{i,j} : x_i - x_j = 0$.

I punti di $M(\mathcal{A}(A_{n,q}))$ sono tutti e soli i punti $(x_0, x_1, \dots, x_{n+1})$ di $PG\ (\ n+1\ ,\ q\ )$ tali che $x_i \neq x_j$ per ogni $1 \le i < j \le n+1$.

Per definizione, si osserva subito che il complementare $M(\mathcal{A}(A_{n,q}))$ è vuoto in $PG(n+1,q)$ se $q < n+1$. Quindi il problema sull'esistenza di Blocking Sets in $M(\mathcal{A}(A_{n,q}))$ ha interesse se e solo se $q \ge n+1$.

Nel prossimo capitolo studieremo alcune proprietà dei Blocking Sets nel complementare di un arrangiamento, potremo quindi dimostrare che per l'arrangiamento delle trecce vale la seguente:

Proposizione 5.1. *$M(\mathcal{A}(A_{n,q}))$ ammette Blocking Sets per ogni $q \ge n+1$*

5.2 Blocking sets nel complementare di arrangiamenti in PG(n,q)

In questa sezione ripercorriamo i risultati generali validi per blocking sets in spazi affini e proiettivi e dimostriamo che essi sono validi anche per il complementare.

Sia $\mathcal{A}_a = \{H_1, \ldots, H_m\}$ un arrangiamento di iperpiani in $AG(n,q)$ e sia

$$M_a(\mathcal{A}) = AG(n,q) \setminus \cup_{i=1,\ldots m} H_i$$

il complementare nello spazio affine.

Allora i risultati delle Proposizioni 3.2, 3.3 e del corollario 3.1 del terzo capitolo si estendono banalmente anche a Blocking Sets in $M(\mathcal{A}) \subset PG(n,q)$ ed $M_a(\mathcal{A}) \subset AG(n,q)$, utilizzando la stessa dimostrazione usata per il caso generale.

Leggermente più complesso è verificare che anche il Teorema di Mazzocca-Tallini (3.11) si estende al complementare di un arrangiamento. Si ha che vale il seguente:

Teorema 5.1. *Esiste una funzione $b(t,q)(\mathcal{A}(n,q))$ che dipende solo da t,q, dalla natura affine o proiettiva e dall'arrangiamento $\mathcal{A}(n,q)$ considerato, tale che $M(\mathcal{A}(n,q))$ contiene t-blocking sets se e solo se $r \leq b(t,q)(\mathcal{A}(n,q))$.*

Per poter dimostrare questo Teorema è necessario ripercorrere la dimostrazione data da Mazzocca-Tallini in [36] per l'analogo del Teorema 3.11 nel caso delle varietà algebriche di $PG(n,q)$ ed $AG(n,q)$.

Si osserva infatti che questa dimostrazione vale integralmente anche per il caso del complementare. Riportiamo qui, per completezza, la dimostrazione, adattata al caso di nostro interesse, cioè il caso di $M(\mathcal{A}(n,q))$.

Dimostrazione Teorema 5.1. Sia $d_{M(\mathcal{A}(n,q))}$ il massimo delle dimensioni dei sottospazi lineari contenuti in $M(\mathcal{A}(n,q))$. Per costruzione, essendo $M(\mathcal{A}(n,q))$ il complementare di un arrangiamento di iperpiani, si ha che $\{d_{M(\mathcal{A}(n,q))} : n \in \mathbb{N}\}$ è una successione crescente.

Supponiamo per assurdo che esista una successione $\{r_n : n \in \mathbb{N}\}$ di interi tali che, per ogni r_n esiste un h-blocking set $B(r_n)$ in $M(\mathcal{A}(n,q))$.

Sotto queste ipotesi, supponendo $d_{M(\mathcal{A}(r_n,q))} > h$, si ha che l'intersezione di $B(r_n)$ con una delle varietà lineari $S(r_n)$ di dimensione massima contenuta in $M(\mathcal{A}(r_n, q))$ dovrebbe essere un h-blocking set di $S(r_n)$. Ma questo è assurdo per il Teorema 3.11. Questo completa la dimostrazione .

5.3 Arrangiamenti in PG(n,q) che ammettono Blocking Sets nel loro complementare

Consideriamo l'arrangiamento delle trecce nello spazio affine $AG(n+1, q)$ ed indichiamo con $M_a(\mathcal{A}(A_{n,q}))$ il suo complementare. Alla dimostrazione della Proposizione 5.1 premettiamo i seguenti Lemmi.

Lemma 5.1. *Tutte e solo le rette in* $M_a(\mathcal{A}(A_{q,q}))$ *sono le* $(q-1)!$ *rette di equazione parametrica* $\underline{y} + t(\underline{x} - \underline{y})$ *con* $\underline{x} - \underline{y} = (1, \ldots, 1)$.

Dimostrazione. Banalmente tutte le rette passanti per un punto di $M_a(\mathcal{A}(A_{q,q}))$ e con vettore direttore $(1, \ldots, 1)$ sono contenute in $M_a(\mathcal{A}(A_{q,q}))$.

Viceversa, siano $\underline{x}, \underline{y} \in M_a(\mathcal{A}(A_{q,q}))$ tali che $\underline{x} - \underline{y} \neq (1, \ldots, 1)$. Allora, se $\underline{x} = (x_1, \ldots, x_{q+1})$ e $\underline{y} = (y_1, \ldots, y_{q+1})$, devono esistere due indici i, j tali che $x_i - y_i \neq x_j - y_j$. Posto:

$$t_0 = \frac{(y_j - y_i)}{(x_i - y_i) - (x_j - y_j)}$$

si ha che $t_0 \neq 0$ e il punto $P = \underline{y} + t_0(\underline{x} - \underline{y})$ ha l'entrata i-esima e l'entrata j-esima uguali, cioè entrambe pari a $\frac{x_i y_j - x_j y_i}{(x_i - y_i) - (x_j - y_j)}$. Ossia P è un punto che non appartiene ad $M_a(\mathcal{A}(A_{q,q}))$. Questo conclude la dimostrazione.

Lemma 5.2. *$M_a(\mathcal{A}(A_{q,q}))$ ammette Blocking Sets.*

Dimostrazione. Osservando che i punti in $M_a(\mathcal{A}(A_{q,q}))$ sono $q!$, la dimostrazione del Lemma è immediata conseguenza del Lemma 5.1. Infatti si ha che il numero di rette é di molto inferiore al numero di punti, da cui il blocking set puó essere costruito scegliendo, opportunamente, un punto per ogni retta.

Diamo ora la:

Dimostrazione della proposizione 5.1. La dimostrazione segue immediatamente dal lemma 5.2, dal teorema 5.1 e dal corollario 3.1.

Osservazione 5.1. *Notiamo che, come conseguenza della proposizione 3.2, se, dato un arrangiamento $\mathcal{A}$ in $PG(n,q)$ (o anche $AG(n,q)$), il complementare contiene un sottospazio che non ammette Blocking Sets, allora nemmeno $M(\mathcal{A})$ può averne.*

Osservazione 5.2. *Un'altra interessante osservazione riguarda il caso affine piano. In [3] gli autori dimostrano che in $AG(2,q)$, per $q \geq 5$, esiste sempre un blocking set di cardinalitá minima pari a $2q-1$.*

Un analogo risultato vale anche per il caso del complementare di un arrangiamento in $AG(2,q)$. In questo caso un arrangiamento $\mathcal{A}$ é composto di rette del piano. Da semplici osservazioni geometriche, si ha che se $\sharp\mathcal{A} = 1$ allora in $M(\mathcal{A})$ esiste un blocking set minimale di cardinalitá $q-1$. Infatti in questo caso $M(\mathcal{A})$ contiene tutte e sole le rette parallele alla retta in $\mathcal{A}$ e il blocking set minimale si ottiene prendendo un punto per ognuna di queste rette.

In generale se $\mathcal{A}$ é composto di r rette parallele allora $M(\mathcal{A})$ ammette un blocking set minimale di cardinalitá $q - r$.

Se in $\mathcal{A}$ ci sono due rette che si intersecano allora il problema diventa vuoto poiché $M(\mathcal{A})$ non contiene rette. Quest'ultima osservazione vale anche per $PG(2, q)$.

Questo nuovo approccio al problema dei Blocking Sets apre un numero notevole di problemi.

Intanto viene spontaneo chiedersi come si caratterizza in $PG(n, q)$ (ed in $AG(n, q)$) un arrangiamento *sbloccante minimale*; ossia un arrangiamento $\mathcal{A}$ tale che $PG(n, q)$ non ammette Blocking Sets, ma $M(\mathcal{A})$ si e tale che la sua cardinalità sia minima tra quelle degli arrangiamenti sbloccanti.

Viceversa, ci si chiede come si caratterizza un arrangiamento *bloccante*. Un esempio di arrangiamento bloccante è quello costituito dalla retta ad infinito in $PG(2, 3)$. Infatti è noto che $PG(2, 3)$ ammette Blocking Sets mentre $AG(2, 3)$ no.

Ancora ci si chiede che legame effettivo ci sia tra la teoria dei Blocking Sets classica e quella fatta sul complementare di un arrangiamento. Così come sarebbe interessante studiare gli eventuali punti di incontro tra lo studio dei blocking sets sul complementare e lo studio della teoria degli arrangiamenti su spazi finiti.

Si osserva infine che, quanto detto, é generalizzabile al caso in cui si consideri il complementare di un arrangiamento di sottospazi di dimensione qualsiasi.

Questo approccio permette anche di riscrivere in termini del tutto nuovi diversi problemi che sono giá oggetto di studio.

Appendice

In questo capitolo presentiamo l'algoritmo effettivo per il calcolo di Blocking sets in PG(n,q). L'algoritmo per il caso affine é praticamente identico.

L'algoritmo é scritto usando il linguaggio simbolico Axiom ed é diviso in 3 parti.

Nella prima parte si descrivono la funzione che dá i punti di PG(n,q) sotto forma di liste di numeri e la funzione che, assegnata la divisione in Z_q sotto forma di lista, costruisce la retta passante per due dati punti dello spazio proiettivo PG(n,q).

Nella seconda parte si costruisce un insieme di punti che ha la proprietá di non contenere nessuna retta.

Nella terza parte si verifica se l'insieme cosi' costruito é effettivamente un *blocking set*, verificando che interseca tutte le rette di PG(n,q).

Parte prima

Questa funzione riduce modulo q un vettore assegnato.

```
rimdupl:(List(List(INT)),INT) -> List(List(INT))
rimdupl(PG0,q) ==
```

```
        h:INT:=1
        while not(h=0) repeat
          l1:=PG0.h
          for t in 2..q-1 repeat
            l2:=[t*l1.i for i in 1..♯l1]
            l2r:=[divide(l2.i,q).remainder for i in 1..♯l1]
            PG0:=remove(l2r,PG0)
            c:=♯PG0
          if h<c then h:=h+1
          else h:=0
        PG0
```

Crea i punti di PG(n,q) sotto forme di liste normalizzate:

```
spazioPG:(INT,INT) -> List(List(INT))
spazioPG(q,n) ==
        L1:List(List(INT)):=[[0],[1]]
        L2:List(List(INT))
        L:List(List(INT))
        h:INT:=0
        l:List(INT)
        while h<n+1 repeat
          c:=♯ L1
          L:=nil
          for k in 1..c repeat
            l:=L1.k
            for i in 0..q-1 repeat
```

```
            l2:=concat(l,i)
            L:=concat(L,l2)
            l2:=nil
          L1:=L
          h:=♯ L1.1
        L
```

Divisione in Z_5, l=List(List(INT)) e l.i.j=i/j

l:List(List(INT)):=[[1,3,2,4],[2,1,4,3],[3,4,1,2],[4,3,2,1]]

Questo algoritmo costruisce la retta passante per i due punti p1 e p2 dello spazio proiettivo PG(n,q).
ND:=PF q (o ND:=INT) da assegnare volta volta prima di compilare.

```
rettapq:  (List(Vector(ND)),INT,INT,List(List(ND)),INT,INT) -> List(INT)
rettapq(PG,p1,p2,l,q,n) ==      retta:List(INT):=[p1,p2]
        ptp1:Vector(ND):=PG.p1
        ptp2:List(ND):=PG.p2
        ptt:Vector(ND)
        ptt1:PF 5
        for t in 1..q-1 repeat
          if t=1 then ptt:=ptp1-ptp2
          else ptt:=ptp2+t*(ptp1-ptp2)
          ptt1:=ptt.1
          if ptt1=1 then (retta:=concat(retta,position(ptt,PG));
iterate)
```

```
        if not(ptt1=0) then
          ptt:=1/ptt1*ptt
          retta:=concat(retta,position(ptt,PG))
        else for g in 1..q-1 repeat
          post:=position(g*ptt,PG)
          if post>0 then (retta:=concat(retta,post); break)
      retta
```

Quanto fatto vale solo su un campo finito Z_q con q primo, altrimenti bisogna aggiungere la divisione euclidea.

Questo programma costruisce, infine, la matrice la cui colonna i-esima è data dal punto P_i di PG(n,q) e lungo le colonne ci sono i (q-1) punti che costituiscono le rette passanti per il punto P_i e i punti P_j con $j > i$. Chiaramente i (q-1) punti della retta P_iP_j occuperanno le righe (q-1)*(j-1)+1..(q-1)*j.

```
RettePG:(List(Vector(ND)),List(List(INT)),INT,INT) -> Matrix(INT)
RettePG(PG,l,q,n) ==
      a:=♯PG
      diff:PositiveInteger:=q-1
      b:PositiveInteger:=a*diff
      M:Matrix(INT):=zero(b,a)
      r:List(INT)
      for j in 1..a repeat
        for i in j+1..a repeat
          r:=rettapq(PG,j,i,l,q,n)
          for t in 3..♯r repeat
            M((q-1)*(i-1)+(t-2),j):=r.t
```

```
        M
```

Parte seconda

Questa funzione costruisce, a partire dalla matrice delle rette di PG(n,q), un insieme che non contiene nessuna retta di PG(n,q).
Inoltre tarsforma la matrice di tutte le rette di PG(n,q) in una matrice con entrate nulle nelle posizioni corrispondenti a rette che intersecano l'insieme trovato.

```
blok:  (List(Vector(ND)),List(List(INT)),INT,INT,Matrix(INT)) ->
List(INT)
blok(PG,l,q,n,M) ==
        blocc:List(INT):=nil
        c:=ncols(M)
        r:=nrows(M)
        z:Vector Integer:=zero(r)
        rinb:List(List(List(INT))):=[[[],[]]]
        qk:INT
        nnc:=0
        ttt:List(INT)
        lll:List(INT):=[i for i in 1..c]
        for i in 1..c repeat
          output(i=,i)
          qk:=0
          nni:=i-nnc
          h:=ncols(M)
```

```
          cri:=#rinb
          if column(M,nni)=z then
          else
            for k in 1..cri repeat
              ptf:=rinb.k.2
              if member?(i,ptf)=true then if #ptf=1 then (qk:=1;
break)
            if qk=1 then iterate
            else
              bb:=#blocc
              blocc:=concat(blocc,i)
              if bb>0 then
                for k in 1..cri repeat
                  ptf:=rinb.k.2
                  if member?(i,ptf)=true then remove!(i,rinb.k.2)
                for qq in 1..bb repeat
                  retiq:=rettapq(PG,i,blocc.qq,l,q,n)
                  if retiq=nil then iterate
                  else
                    rinb:=concat(rinb,[retiq,setDifference(retiq,blocc)])
              ll:=setDifference(lll,blocc)
              for j in ll repeat
                post:=position(i,column(M,j))
                if post=0 then iterate
                else
                  ttt:=[post]
                  for ss in post+1..r repeat
```

```
                    if M(ss,j)=i then ttt:=concat(ttt,ss)
                for t in ttt repeat
                    rr1:=divide(t,q-1)
                    rr:=rr1.quotient
                    re:=rr1.remainder
                    if re=0 then rrq:=(rr-1)*(q-1)
                    else rrq:=rr*(q-1)
                    for k in 1..(q-1) repeat
                      M(rrq+k,j):=0
        blocc
```

Parte terza

Quest'ultima funzione controlla che il blocco costruito nella seconda parte sia un blocking set. Per fare questo prende la matrice M delle rette di PG(n,q) trasformata dalla funzione precedente. Se la nuova matrice ha alcune entrate opportune nulle questo significa che tutte le rette dello spazio intersecano l'insieme *blocco* che risulta essere, pertanto, un blocking set.

```
control:  (Matrix(INT),List(INT),INT) -> INT
control(M1,blocc,q) ==
        cck:INT:=0
        nc:=ncols(M1)
        M2:Matrix(INT):=transpose(matrix[column(M1,j) for j in blocc])
        z:List(INT):=nil
        for i in blocc repeat
          z:=append(z,[(q-1)*(i-1)+j for j in 1..q-1])
```

```
M:Matrix(INT):=matrix[row(M2,j) for j in z]
r:=nrows(M)
ncm:=ncols(M)
output(ncm,nr=,[ncm,r])
blc:=setDifference([i for i in 1..nc],blocc)
ncm:=#blocc
for j in 1..ncm repeat
  output(j=,j)
  for i in 1..ncm repeat
    output(i)
    ll:=[M((q-1)*(i-1)+k,j) for k in 1..q-1]
    if ll=[0 for h in 1..q-1] then iterate
    if #setDifference(ll,blc)<q-1 then iterate
    else (cck:=1;break)
  if cck=1 then
    output(i=,i)
    break
cck
```

Bibliografia

[1] E. Artin. *Geometric algebra*. Interscience, New York and London, 1957.

[2] L. Berardi and A. Beutelspacher. *On blocking sets in t-designs with blocks of small size*. Riv.Mat.Univ.Udine, **201**:1–17, 1989.

[3] L. Berardi and F. Eugeni. *On blocking sets in affine planes*. J. Geom, **22**:167–177, 1984.

[4] L. Berardi and F. Eugeni. *On the cardinality of blocking sets in PG(2,q)*. J. Geom, **22**:5–14, 1984.

[5] L. Berardi and F. Eugeni. *Blocking sets e teoria dei giochi*. Atti Sem. Mat. Fis. Univ. Modena, **34**:165–196, 1988.

[6] L. Berardi and F. Eugeni. *Blocking sets in projective plane of order four*. Ann. Discrete Math, **37**:43–50, 1988.

[7] L. Berardi and F. Eugeni. *Blocking sets and game theory*. Proc. of 1 Int. Conf. on Blocking Sets, (Giessen 1989), Mitt. Math. Sem. Giessen, **201**:1–17, 1991.

[8] L. Berardi, F. Eugeni, and O. Ferri. *Sui blocking sets nei sistemi di Steiner*. Boll.Un.Mat.Ital.Algebra e Geom., **1-D**:141–164, 1984.

[9] A. Beutelspacher and F. Eugeni. *On blocking sets in projective and affine spaces of large order*. Communicated in Oberwolfach, Rend.Mat., **4**:3–19, 1989.

[10] G. Birkhoof. *Lattice theory*. Amer.Math.Soc.Colloq.Pub., 1948. vol.25.

[11] R. Bose. *Mathematical theory of the symmetrical factorial design*. Sankhya, **8**:107–166, 1947.

[12] R. Bose and K. Kishen. *On the problem of confounding in the symmetrical factorial designe*. Sankhya, **5**:21–36, 1940.

[13] A. Brouwer and A. Schrijver. *The blocking number of an affine space*. J. Combin. Theory, **22**:253–266, 1977.

[14] A. Bruen. *Baer subplane and blocking sets*. Bull.Amer.Math.Soc., **76**:342–344, 1970.

[15] A. Bruen. *Blocking sets in projective plan*. Siam. J.Appl.Math, **21**:380–392, 1971.

[16] A. Bruen. *Arcs and multiple blocking sets*. Symposia Math. Acc. Press,INDAM, 1986. pp 15-29.

[17] A. Bruen and J. Fisher. *Blocking sets and complete k-arcs*. Pacific J. Math, **53**:73–84, 1974.

[18] A. Bruen and M. De Resmini. *Blocking sets in affine planes*. Ann. Discrete Math., **18**:13–15, 1983.

[19] A. Bruen and R. Silverman. *Arcs and blocking sets II*. Preprint, , 1986.

[20] A. Bruen and J. Thas. *Blocking sets*. Geometriae Dedicata, **6**:193–203, 1977.

[21] N. Cassetta. *Teoria dei blocking sets negli spazi proiettivi ed affini finiti*. Tesi di Laurea, 1995.

[22] N. Cassetta. *The non existence of blocking set in PG(3,4)*. Italian Journal of pure and appl. math., **3**:79–84, 1998.

[23] N. Cassetta. *A blocking set in AG(3,5)*. Italian Journal of pure and appl. math., **8**:9–17, 2000.

[24] G. Dall'Aglio and G. Pompilj. *Piano degli Esperimenti*. Einaudi, 1959.

[25] D. Drake. *Blocking sets in block designs*. J. Comb. Theory, **2**:459–462, 1985.

[26] F. Eugeni and S. Innamorati. *Arcs and blocking sets in symmetric designs*. Ars Combinatoria, **24**:29–40, 1987.

[27] F. Eugeni and E. Mayer. *On blocking sets of index two*. Prooc.in Annals of Discrete Math., **37**:169–176, 1988.

[28] R. Fisher. *The theory of confounding in factorial experiments in relation to the theory of groups*. Ann. Eugen. London, **11**:341–353, 1942.

[29] M. Gionfriddo. *A short survey on some generalized colourings of graphs*. Ars Combinatoria, , 1988.

[30] W. Heise and P. Quattrocchi. *Informations und Codierungs theorie*. Springer-Verlag, 1983.

[31] D. Hilbert. *Grundlagen der Geometrie.* Teubner,Leipzig und Berlin, 1899.

[32] J. Hirschfeld. *Projective geometries over finite fields.* Claredon Press, Oxford, , 1979.

[33] S. Innamorati. *Tesi di laurea e comunicazione personale.* .

[34] R. Jamison. *Covering finite fields with coset of subspaces.* J.Comb. Thoery, **22**:253–266, 1977.

[35] G. Korchmaros. *New examples of complete k-arcs in PG(2,q).* Europ.J.Combin., **4**:329–334, 1983.

[36] F. Mazzocca and G. Tallini. *On the nonexistence of blocking sets in PG(n,q) and A(n,q) for all large enough n.* Simon Stevin, **1**:43–50, 1985.

[37] J. Von Neumann and O. Morgenstein. *Theory of Games and Economic Behavior.* Princeton University Press, 1953.

[38] P. Orlik and H. Terao. *Arrangements of Hyperplanes*, volume 300. Springer-Verlag, 1992.

[39] M. Tallini Scafati. *Sui (k;n)-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri.* Nota I e II, Rend. Acc. Naz. Lincei, **8,40**:812–818 e 1020–1025, 1966.

[40] M. Tallini Scafati. *Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$.* Rend. Mat. Univ. Roma, **26**:273–303, 1967.

[41] F. Speranza. *Numero cromatico, omomorfismi e colorazioni di un grafo*. Ann. Mat. Pura Appl., **102**:359–367, 1975.

[42] F. Speranza. *Problemi di colorazione e d'omomorfismo di grafi*. Sem. Mat. Univ. Bari, **176**:1–5, 1980.

[43] G. Tallini. *Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria dell'informazione*. Rend. mat. Roma, **19**:379–400, 1960.

[44] G. Tallini. *Un'applicazione della geometria di Galois a questioni di statistica*. Rend. Acc. Naz. Lincei, **35**:479–485, 1963.

[45] G. Tallini. *Problemi e risultati sulle geometrie di Galois*. Ist.Mat.Univ.Napoli, 1973. Relaz. n. 30.

[46] G. Tallini. *k-insiemi e blocking sets in PG(r,q) e in AG(r,q)*. Quaderno n.1 Sem. Geom. Comb. Ist. Math. Appl. Univ. L'Aquila, :1–36, 1982.

[47] G. Tallini. *Blocking sets nei sistemi di Steiner e d-blocking sets in PG(r,q)*. Quaderno n.3 Sem. Geom. Comb. Ist. Math. Appl. Univ. L'Aquila, , 1983.

[48] G. Tallini. *On blocking sets in finite projective and affine spaces*. Annals of Discrete Math., **37**:433–450, 1988.

[49] O. Veblen and J. Young. *Projective geometry*. Ginn, Boston, 1916.