Numero 5 - 1992

RATIO MATHEMATICA

Atti del Convegno
Giornate di Geometrie Combinatorie
L'Aquila - Marzo 1991

a cura di

Franco Eugeni e Mario Gionfriddo

Comitato Organizzatore

Numero 5 - 1992

RATIO MATHEMATICA

Atti del Convegno
Giornate di Geometrie Combinatorie
L'Aquila - Marzo 1991

a cura di

Franco Eugeni e Mario Gionfriddo

Comitato Organizzatore

Indice

PERCHE' SI APPLICA PROPRIO LA MATEMATICA ? ALCUNI PENSIERI CONSIDERANDO LA CRITTOGRAFIA

ALBRECHT BEUTELSPECHER
Math. Institut, Arndtstr. 2 D-6300 Giessen, Germania

1. Introduzione

Le problematiche connesse con la protezione delle cose preziose o delle informazioni sono state sempre presenti e saranno anche un grande problema anzi una sfida nel futuro. Pertanto l'uomo ha sempre provato ad inventare meccanismi per garantire una tale sicurezza. C'e' un grande numero di tali meccanismi e la maggior parte di questi non ha niente a che fare con la crittologia. Consideriamo due di tali meccanismi non-crittografici in dettaglio.

La protezione delle cose preziose oppure di informazioni segrete si ottiene normalmente mediante l'uso di una **cassaforte**. Ogni cosa che e' dentro una cassaforte e' protetta fisicamente. Solo il proprietario puo' aprire la cassaforte mediante una chiave oppure mediante una combinazione di cifre. Se la cassaforte ha piu' di un lucchetto, si puo' anche realizzare il principio dei quattro-occhi: cioe' che almeno due persone autorizzate siano d'accordo prima che la cassaforte si apra.

Un tipo completamente diverso di sicurezza si trova nella **carta moneta**. Qui il problema non e' la segretezza, ma la autenticita': i biglietti di banca non devono essere duplicati e neanche falsificati! Per questo si sono inventate proprieta' fisiche molto sofisticate. L'autenticita' di un biglietto di banca si ottiene (per esempio) mediante una speciale filigrana, mediante lo stampare con precisione, con l'utilizzo di carta speciale, etc. Ma si e' sempre saputo di biglietti di banca falsificati. In particolare, considerando le fotocopiatrici a colori moderne, ci si deve chiedere se la sicurezza offerta dai biglietti di banca sia sufficiente nei prossimi secoli.

I meccanismi tradizionali per ottenere la sicurezza (tra i quali abbiamo parlato della cassaforte e delle proprieta' dei biglietti di banca) hanno le seguenti proprieta' caratteristiche:

1. Sono basati su *proprieta' fisiche invariabili*: non cambia ne'la chiave per una cassaforte, ne' la filigrana di un biglietto di banca. La invariabilita' di tali proprieta' e' (in un certo senso) un fatto positivo e fondamentale per la sicurezza.

2. La maggior parte dei meccanismi tradizionali e' basata su *proprieta'* che sono essenzialmente *note e non segrete*. E' chiaro che la chiave di una cassaforte oppure la combinazione delle cifre deve essere conservata in modo sicuro, ma le proprieta' di sicurezza per i biglietti di banca sono pubbliche e solo quelli che conoscono le proprieta' sono in grado di distinguere un biglietto di banca vero da uno falso.

Ovviamente la sicurezza ottenuta da tali meccanismi puo' essere misurata solo empiricamente. Esprimiamo questo fatto con cattiveria (in pari tempo in modo piu' banale): un sistema viene usato solo fino a quando non viene rotto. La storia delle banche mostra chiaramente che la storia della moneta e' una lotta tra i "buoni" (la gente che inventa i meccanismi per la sicurezza) e i "cattivi" (che trovano il modo di rompere i sistemi di sicurezza). Le banche inventano sempre nuovi meccanismi e ottengono un vantaggio - ma questo vantaggio non e' garantito nel tempo perche' nuovi sviluppi tecnologici (ad esempio l'invenzione della fotocopiatrice a colori) costituiscono un nuovo pericolo.

A tal punto ci chiediamo: il mondo e' necessariamente cosi'? Non e' possibile fare in modo completamente diverso? E' possibile inventare sistemi di sicurezza nei quali un bandito non ha alcuna possibilita' di fare cose indesiderate - precisamente non solo oggi, ma per sempre ed in eterno? Se avessimo tre desideri liberi, allora potremmo chiedere una sicurezza con le seguenti proprieta':

- Non e' basata esclusivamente su proprieta' fisiche statiche.
- Non e' verificata solo empiricamente, ma si basa su fondamenti teorici.
- E' senza limite.

Nelle fiabe i desideri si avverano sempre - anche nella vita questo puo' talvolta accadere: lo scopo della **crittologia** e' quello di inventare sistemi di sicurezza che offrano sicurezza illimitata, la quale possa essere provata dai matematici in modo

rigoroso!

A questo punto il lettore certamente si chiedera': perche' proprio la crittografia e' in grado di produrre una tale meraviglia e non le altre scienze? La risposta e' semplice: ... perche' la crittografia e' matematica! Ci si chiede ora: perche' la matematica e' buona? La matematica e' adatta perche' i fatti sono accettati solo se sono dimostrati!

E' vero che le dimostrazioni non sono sempre molto gradite agli allievi e studenti, ma sono il vero vantaggio della matematica rispetto ad altre discipline. Immaginiamo ad esempio di avere monete (forse "monete elettroniche") tali che la loro sicurezza sia ottenuta mediante meccanismi crittografici e supponiamo che tale sicurezza sia provata matematicamente. Allora nessuna banca deve avere paura di un futuro sviluppo tecnologico, poiche' la sicurezza non e' basata sulla tecnologia di oggi, ma accertata per sempre!

Esiste un altro vantaggio nelle tecniche crittografiche. Se i cattivi riescono, ad esempio, a falsificare la filigrana, non ha senso mettere due filigrane dentro la carta per aumentare la sicurezza. D'altro canto, se esiste un protocollo crittografico che garantisce una sicurezza di, diciamo, 2^{-64} (cioe' una chiave di 64 bit), spesso e' anche possibile costruire un protocollo dotato di sicurezza doppia (cioe' 2^{-65}). In altre parole usando meccanismi crittografici, si puo' avere un livello di sicurezza arbitrario ("sicurezza senza limite").

Lo scopo di questo lavoro e' quello di dare argomentazioni a favore di queste tesi e di discutere se queste sono utopiche oppure realistiche.

2. Tre Applicazioni crittografiche

2.1 Controllo d'accesso

Consideriamo il problema di come una macchina possa convincersi della identita' di una persona. Un tale problema si presenta in molte situazioni, non solo per l'accesso ad un grande computer, ma ad ogni sportello Bancomat. Il metodo usuale e' che l'utente sia autenticato mediante un segreto (ad esempio il PIN). L'utente

trasmette il suo segreto all'Automa, il quale verifica se il segreto esibito e' proprio quello corrispondente al nome dell'utente.

Questo e' un **metodo statico** (poiche' il PIN non cambia mai) e ha tutti gli svantaggi di un metodo statico. Poiche' il PIN non cambia mai, un nemico deve scoprire solo una volta il PIN e dopo, conoscendo il segreto, puo' giocare il ruolo dell'utente.

Ma questo metodo ha un aspetto positivo: una persona puo' provare la sua identita' ad un computer mostrando di essere in possesso di un certo segreto. L'aspetto negativo e' che il segreto puo' essere scoperto.

Presentiamo ora un protocollo semplice, che costituisce un miglioramento essenziale: il segreto non viene trasmesso, i dati trasmessi sono di carattere random e il nemico non puo' fare nulla. L'idea e' la seguente: il computer pone una certa domanda, l'utente fornisce una risposta che dipende dal suo segreto **k**; infine il computer confronta la risposta dell'utente con il risultato che esso ha computato (cfr. Fig. 1).

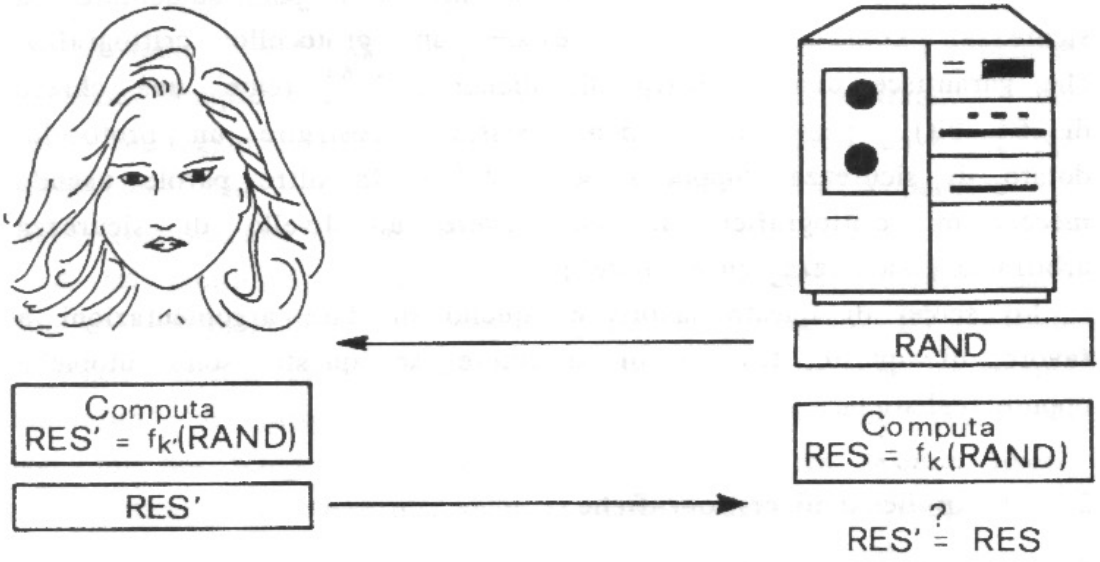


Fig. 1. Un protocollo challenge and response

Chiamiamo questo un protocollo **challenge and response**; il challenge e' un numero random RAND. Notiamo che f e' una funzione crittografica, che ha come input un "testo chiaro" RAND e una chiave k e ha come output una risposta RES := f_k(RAND).

Il nostro scopo qui non e' studiare le proprieta' che una tale

funzione f deve avere per essere adatta ad un protocollo challenge and response. Affermiamo solo che mediante l'uso di un protocollo semplice ed una funzione non complicata abbiamo ottenuto un progresso enorme: l'utente non deve scoprire il suo segreto, il computer si convince in *modo indiretto* che l'utente conosce il segreto k. Principalmente, un nemico non ha nessun vantaggio se ascolta la comunicazione.

Negli ultimi anni, tali protocolli challenge and response sono stati ampiamente sviluppati: i cosidetti protocolli "zero knowledge" hanno ottenuto un grado insuperabile di perfezione.

2.2 Funzioni unidirezionali

Per molte applicazioni crittografiche servono funzioni chiamate **unidirezionali**. Sono applicazioni che soddisfanno le seguenti proprieta' che a prima vista possono sembrare paradossali:

- E' facile computare f(x).
- La funzione f e' invertibile, ma dato un y, e' estremamente difficile trovare un x tale che sia f(x) = y.

Esistono delle funzioni unidirezionali? Nella vita quotidiana incontriamo "ampie carrettate" di tali funzioni: un esempio molto chiaro e significativo e' quello costituito da un elenco telefonico:

E' una cosa facilissima, usando un elenco telefonico, trovare il numero telefonico di una certa persona. Inversamente e' una grande perdita di tempo trovare il nome che corrisponde ad un numero dato. La ragione e' che per trovare un sol nome, si deve di fatto invertire tutta la guida telefonica.

Ci sono funzioni unidirezionali crittografiche? Questa e' una domanda difficilissima, che teoricamente non ha avuto ancora risposta. Nella ricerca si studiano funzioni che sono candidate ad essere funzioni unidirezionali: di conseguenza la matematica tocca livelli piu' elevati. Mediante l'uso di strutture matematiche si costruiscono potenziali funzioni unidirezionali. Gli oggetti piu' importanti per questi scopi sono i numeri primi p, precisamente "gli interi modulo p".

Nella crittografia il candidato principale a funzione unidirezionale e' la funzione esponenziale discreta. Che cosa e'? Per definirla ci serve (nel caso piu' semplice) un numero primo p (il modulo) e un intero b qualsiasi (la base). Si puo'

immaginare che la **funzione esponenziale discreta** ε_b sulla base b viene computata nei due passi seguenti:

Sia x un numero intero qualsiasi.

1*mo passo*: Computa b^x.

2*do passo*: Dividi b^x per p; il resto non-negativo si denota con $\varepsilon_b(x)$.

In poche parole: $\varepsilon_b(x) := b^x \bmod p$.

Si puo' credere che questa funzione sia molto simile alla funzione esponenziale reale ... e la funzione esponenziale reale e' una delle funzioni piu' studiate; in particolare ogni ingegnere conosce la sua funzione inversa e sa come trattarla. E poi?

Nella realta' - a parte la definizione - non vi e' alcuna somiglianza tra la funzione esponenziale reale continua e la funzione esponenziale discreta. La Fig. 2 mostra la difficolta' insita in una funzione esponenziale discreta.

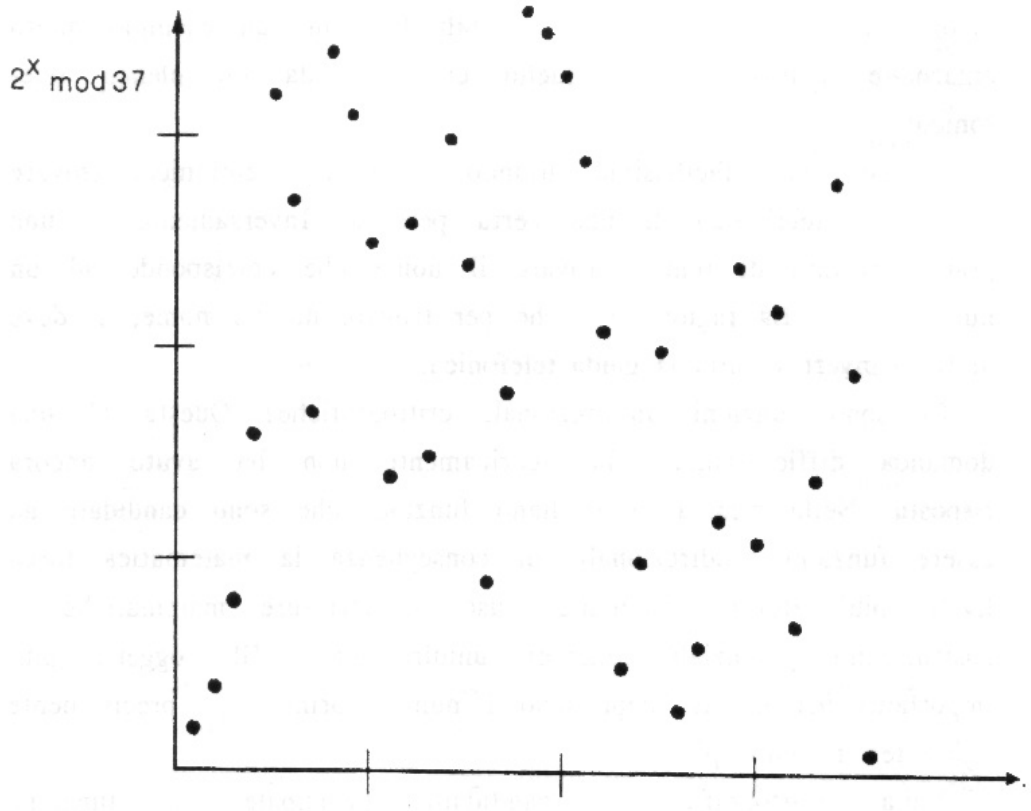


Fig. 2. Il fascino discreto della funzione esponenziale discreta (p = 37)

Chiaramente ci sono algoritmi migliori per computare la funzione esponenziale discreta; servono circa 2log p moltiplicazioni. Ma per invertire l'esponenziale discreto (cioe' per computare un **logaritmo discreto**) con i migliori algoritmi che possediamo servono circa $\sqrt{p}$ moltiplicazioni. Quindi la funzione esponenziale discreta puo' essere considerata come unidirezionale.

2.3 Segreti distributivi

In molte situazioni una informazione segreta deve essere distribuita tra molte persone cosi' da condividere anche la responsabilita' del segreto stesso. Presentiamo due esempi:

- Molte casseforti moderne utilizzano il "principio dei quattro occhi": solo se due persone autorizzate sono d'accordo ad aprire una cassaforte (con la chiave oppure con una combinazione di cifre), la cassaforte si apre.

Possiamo generalizzare il principio dei "quattrocchi" senza difficolta': desideriamo che un procedimento possa essere iniziato solo se due persone tra un numero totale di n autorizzate sono d'accordo. Questo metodo e' molto piu' flessibile del classico principio dei quattrocchi, poiche' basta che siano d'accordo due persone qualsiasi nell'insieme di tutti gli autorizzati.

- Nei sistemi crittografici spesso una chiave gioca un ruolo straordinario; usualmente una tale chiave si chiama **masterkey**. E' ovvio che la masterkey e' il tallone d'Achille del sistema, e dunque deve essere protetta meglio possibile. Ci sono due cose da osservare: una e' che il nemico non deve mai poter conoscere tutto il segreto, l'altra e' che gli impiegati leali devono essere protetti da falsi sospetti; quindi neanche un impiegato deve conoscere tutta la chiave - e questo deve poter essere dimostrato!

Per realizzare tutti questi scopi sono stati introdotti i **threshold schemes** come caso speciale degli **shared secret schemes**. In questo contesto il livello delle applicazioni della matematica e' altissimo: i threshold schemes offrono una sicurezza che puo' essere dimostrata in modo rigoroso!

In un **t-threshold scheme** il segreto viene diviso in molte parti (chiamati **segreti parziali**) tali che valgano le seguenti

proprieta':

- dato un sottoinsieme di t segreti parziali qualsiasi, il segreto puo' essere ricostruito facilmente;
- se sono noti t-1 segreti parziali o meno, il segreto non puo' essere ricostruito.

(E' chiaro che in un certo senso ogni segreto puo' essere ricostruito, per esempio, se il numero totale dei segreti possibili e' k, allora il segreto puo' essere "ricostruito" con una probabilita' di 1/k.)

Come esempio presentiamo il caso t = 2. Scegliamo una retta r in un piano (per gli esperti: in un piano proiettivo d'ordine q). Il segreto sia un punto K di r, scelto a caso. Per dividere il segreto K scegliamo una retta s diversa da r per il punto K. Infine scegliamo molti punti di s. Ognuno di questi punti e' un segreto parziale (cfr.Fig.3).

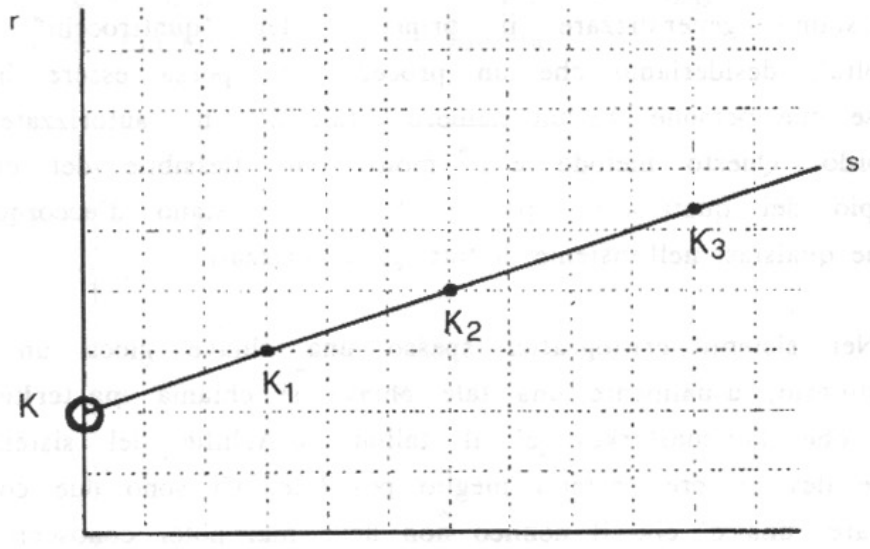


Fig. 3. Un threshold scheme con t = 2

Quando si vuole ricostruire il segreto, il sistema riceve alcuni punti; computa la retta s' per questi punti e computa l'intersezione di r ed s'. Questo punto K' e' il segreto ricostruito. Si confronti K' con K. Se sono uguali, la ricostruzione e' fatta.

Ora analizziamo la sicurezza di un tale 2-threshold scheme. Se la retta r ha almeno q+1 punti, la probabilita' di indovinare il segreto e' al piu' 1/(q+1). E' importante che questa probabilita' non aumenti per gli insider, cioe' per quelli che

conoscono qualche segreto parziale.

E' ben noto che per ogni potenza di un primo q esistono piani con la proprieta' che ogni retta ha precisamente $q+1$ punti (sono i piani di Galois costruiti mediante il campo di Galois con q elementi). Questo significa che e' possibile costruire t-threshold schemes per ogni livello di sicurezza desiderato.

Concludendo, questi sistemi offrono una sicurezza calcolabile; il fruitore sceglie numericamente la probabilita' che desidera e la matematica offre il sistema corrispondente! Inoltre, per avere una sicurezza abbastanza alta (ad esempio una probabilita' di 10^{-9}) servono solo "campi piccoli" (ordine di grandezza 2^{30}). Cio' significa che la implementazione non presenta nessuna difficolta'.

3. Conclusioni

Abbiamo cosi' mostrato che gli strumenti crittografici (cioe' matematici) raggiungono lo scopo desiderato che era appunto quello di avere una sicurezza misurabile, controllabile e dimostrabile. Distinguiamo i seguenti livelli

- sicurezza che puo' essere **analizzata in modo informale** (esempio: protocollo challenge and response);
- sicurezza che puo' essere **analizzata matematicamente** (esempio: la funzione esponenziale discreta);
- sicurezza che puo' essere **dimostrata matematicamente** (esempio: threshold schemes).

Dobbiamo ammettere che meccanismi la cui sicurezza e' dimostrabile, e contemporaneamente adatti per l'uso pratico sono per ora molto rari. Certamente lo scopo principale della crittografia per i prossimi anni sara' quello di sviluppare algoritmi e meccanismi che soddisfino entrambe le proprieta'.

Ma ripetiamo un'altra volta il messaggio di questo lavoro, come i Romani avrebbero detto: *In dubio pro matematica.*

Bibliografia

L. Berardi: Some remarks about an electronic signature derived from a generalized RSA-code. J. of Info. & Opti. Sci. 11 (1990), 189-194.

A. Beutelspacher, F. Eugeni: Geometrie finite e crittosistemi. Atti del II simposio nazionale so "stato e perspettive della ricerca crittografica in Italia". Roma, Novembre 1989.

B.K. Dass, F. Eugeni: How to share secrets: the idea of geometric threshold schemes. J. of Info. & Opti. Sci. 12 (1991), 3-11.

ISO Security Addendum ISO IS 7498/2: Open Systems Interconnection Reference Model - Part 2: Security Architecture

D. Chaum: Security without Identification: Transaction systems to Make Big Brother Obsolete. Comm. ACM 28 (1985), 1030-1044

D.W. Davies, W.L. Price: Security for Computer Networks. John Wiley & Sons, Chichester, 2nd edition 1989

A. Sgarro: Crittografia. Muzzio Editore, 1986.

G. Simmons: How to (really) share a secret. Advances of Cryptology - CRYPTO 88, Lecture Notes in Computer Science 403 (1989), 390-448.

G. Simmons: Authentication Theory / Coding Theory. Advances in Cryptology - CRYPTO 84, Lecture Notes in Computer Science 196 (1985), 411-432.

A. Shamir: How to share a secret. Comm. ACM 22 (1979), 612-613.

A LOCAL PROPERTY OF HAMILTONIAN MOON TOURNAMENTS (*)

Cosimo DI MITRI, Cosimo GUIDO

We prove that a hamiltonian tournament H_n, $n \geq 5$, is of Moon-type (i.e. its subtournaments are either hamiltonian or transitive) if and only if each hamiltonian 5-subtournament is too.

1. INTRODUCTION

Several properties of tournaments are known that are verified globally iff they are fulfilled by each subtournament of a given order.

It is well known, for example, that a tournament with at least 3 vertices is transitive iff each 3-subtournament T_3 is too.

Burzio and Demaria [3] proved that a hamiltonian tournament with at least 5 vertices is bineutral iff each hamiltonian k-subtournament is too, for some $5 \leq k \leq n$.

Other local properties of hamiltonian tournaments that are global properties too were studied by Demaria and Gianella [4], who proved the following:

- a hamiltonian tournament with at least 5 vertices has the minimum number, n-2, of 3-cycles iff every hamiltonian 5-subtournament has 3 3-cycles.
- a hamiltonian tournament with at least 6 vertices has only one spanning cycle iff every hamiltonian 6-subtournament has the same property.

---

* Work performed under the auspices of the Gruppo Nazionale di Topologia (MURST) and of the GNSAGA (CNR).

Burzio and Demaria [2] proved that a tournament with at least 4 vertices is of Moon-type (see next section for definitions) iff all of its 4-subtournaments are of the same type.

In this paper we prove that a hamiltonian tournament T_n, $n \geq 5$, is of Moon-type iff each hamiltonian 5-subtournament is too. (We remark that every Moon tournament is either hamiltonian or transitive).

2. PRELIMINARIES

In this section we give some definitions and well known results. See [1] and [5] for the definitions that we shall not refer to.

We denote by T_m a *tournament* of *order* m and by H_m a *hamiltonian* tournament of order m.

We often denote by T_m the set of labeled vertices of the tournament T_m.

C_r usually denotes a *cycle* of r vertices in a tournament, as well as the subtournament with the same vertices.

If (u,v) is an *arc* from the vertex u (called *predecessor*) to the vertex v (called *successor*) in T_m, then we write $u \longrightarrow v$.

$A \longrightarrow B$ means that each vertex of the subtournament A precedes all the vertices of the subtournament B in T_m.

We denote by Tr_m the *transitive* tournament of order m.

We say that a vertex v *cones* a subtournament R in T_m (or R is *coned* by v) iff either $v \longrightarrow R$ or $R \longrightarrow v$ in T_m. A subtournament R is *non-coned* if no vertex exists which cones R in T_m (see [2]).

We say that a subtournament S of T is an *e-component* of T, and its vertices are called *equivalent*, if S is coned by each vertex of T-S. Single vertices and T are trivial e-components.

Every tournament T_n can be partitioned (in a non-unique way) into disjoint e-components $S^1, S^2, \ldots, S^m$. In such a case the e-components $S^1, S^2, \ldots, S^m$ can be considered as the vertices ($v_1, v_2, \ldots, v_m$ respectively) of a tournament Q_m, so that T_n can be obtained as the *composition* $Q_m(S^1, S^2, \ldots, S^m)$ of the *quotient* Q_m with the e-components

$S^1, S^2, \ldots, S^m$.

In other words $T_n = S^1 \cup S^2 \cup \ldots \cup S^m$ and $a \longrightarrow b$ in T_n iff either $a \longrightarrow b$ in some S^j or $a \in S^h$, $b \in S^k$ and $v_h \longrightarrow v_k$ (i.e. $S^h \longrightarrow S^k$).

T_n is *simple* if it has no non-trivial e-component:

A subtournament R is called *shrinkable* in T_n if it is included in a non-trivial e-component of T_n (see [2]).

The *dual* (or *converse*) T^* of a tournament T has the same vertex-set as T, but every arc is reversed.

Moon [6] considered tournaments whose subtournaments are either hamiltonian or transitive; we call them *Moon tournaments* or tournaments of *Moon-type*.

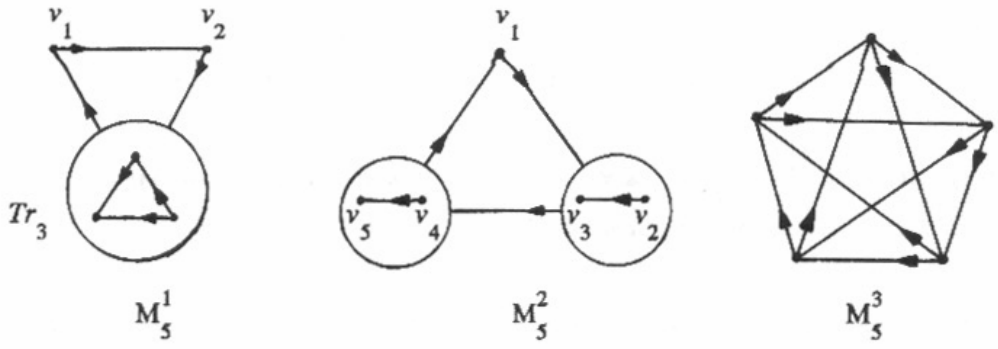
Burzio and Demaria (see [2] theorem 8) proved the following.

Proposition 1. *A tournament T_n, $n \geq 4$, is a Moon tournament iff each 4-subtournament in T_n is a Moon tournament, i.e. iff no 3-cycle is coned in T_n.*■

3. CHARACTERIZATION OF HAMILTONIAN MOON TOURNAMENTS

Proposition 1 allows us to determine easily the Moon tournaments in the set of the hamiltonian tournaments with 5 vertices, that are described, for example, in [5].

In fact the three hamiltonian tournaments $M_5^1 = C_3(v_1, v_2, Tr_3)$,



M_5^1 M_5^2 M_5^3

fig. 1

$M_5^2 = C_3(v_1,\{v_2,v_3\},\{v_4,v_5\})$ and M_5^3 (i.e. the regular tournament of order 5) of fig.1 are of Moon-type.

On the other hand $N_5^1 = C_3(v_1,v_2,C_3)$, N_5^2, N_5^3 described in fig.2 are the hamiltonian tournaments that are not of Moon-type, since each of them contains a coned 3-cycle.

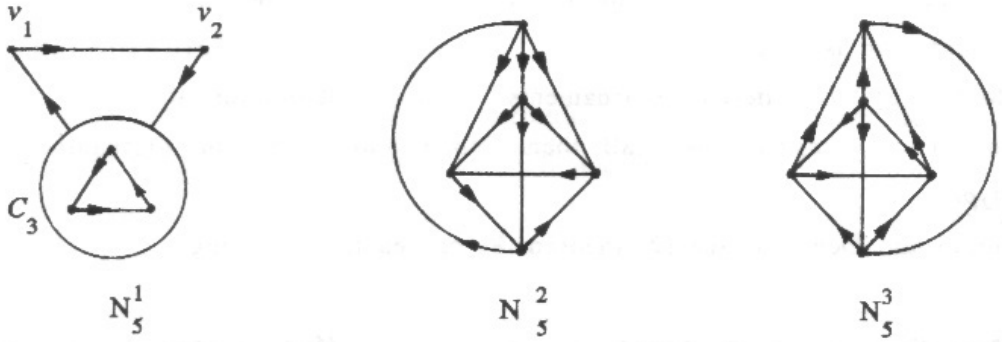


fig.2

Let us denote by $\mathcal{AH}$ the class of hamiltonian tournaments with at least 5 vertices whose hamiltonian 5-subtournaments are of Moon-type.

On the other hand let us denote by $\mathcal{MH}$ the class of hamiltonian Moon tournaments with at least 5 vertices.

We shall prove that $\mathcal{AH} = \mathcal{MH}$ (see proposition 4).

Remark 1. If T_n is of Moon-type then its dual tournament T_n^* is of Moon-type.

If $H_n \in \mathcal{AH}$, then its dual tournament $H_n^* \in \mathcal{AH}$.

Proposition 2. *If $H_n \in \mathcal{AH}$ and S is a non-trivial e-component of H_n, then S is a transitive subtournament of H_n.*

Proof. Since H_n is hamiltonian there exists a successor s of S and a predecessor p of S such as $s \longrightarrow p$.

Now if a 3-cycle C_3 were contained in S, then H_n would contain the hamiltonian subtournament $N_5^1 = C_3(s,p,C_3)$ which contradicts the assumption.■

Definition 1. *We say that a cycle C_r in a tournament T_n can be extended to a cycle C_s, $s>r$, in T_n if there exist cycles C_{r+1}, ...,C_{s-1} such that C_{i+1} can be obtained from C_i by inserting a new vertex between two consecutive vertices, for every $r \leq i \leq s-1$ (or equivalently C_i can be obtained from C_{i+1} by deleting a vertex, for every $r \leq i \leq s-1$).*

Proposition 3. *Let C_m be a cycle in T_n, $m<n$. C_m can be extended to a spanning cycle in T_n if and only if C_m is unshrinkable.*

Proof. If S were a non-trivial e-component of T_n and $C_m \subseteq S$, then each vertex $v \in T_n$-S would cone S hence no cycle contained in S could be extended outside S.

For the "if" part of the proof, the assumption allows us to consider a vertex $v_{m+1} \in T_n$-C_m that does not cone C_m, so that C_m can be extended to a cycle C_{m+1} containing v_{m+1} and, of course, C_{m+1} cannot be contained in any non-trivial e-component of T_n.

Therefore we can extend by induction C_m to a spanning cycle C_n in T_n.■

A trivial consequence of the preceding result is the following, that generalizes proposition 3 of [2].

Corollary 1. *A tournament is hamiltonian iff it contains an unshrinkable cycle.*■

Proposition 4. $\mathcal{AH} = \mathcal{MH}$.

Proof. The inclusion $\mathcal{MH} \subseteq \mathcal{AH}$ is immediate since every subtournament of a

Moon tournament is of Moon-type too.

Now let $H_n \in \mathcal{AH}$ and assume H_n is not of Moon-type.

If C_3 is any coned 3-cycle in H_n, then we deduce from proposition 2 that no non-trivial e-component of H_n can contain C_3 and consequently, by proposition 3, we can extend C_3 to some spanning cycle C_n in H_n.

If C_3 is coned by v in H_n we denote by $\mathcal{C}(C_3,v)$ the set of all minimal cycles in H_n that can be obtained by extending C_3 and contain v.

Let $\mathcal{C}$ denote the union of the family $\{\mathcal{C}(C_3,v) : C_3 \subseteq H_n, C_3 \text{ coned by } v, v \in H_n\}$.

Eventually let us consider a hamiltonian tournament $C_r \in \mathcal{C}$ having minimum lenght in $\mathcal{C}$, and let C_r be an extension of a 3-cycle C_3 coned by $v \in C_r$. Of course $r \geq 5$.

We may assume, by remark 1, that $v \longrightarrow C_3$.

If $C_r = (\ldots(C_3 \cup v_4) \cup \ldots \cup v_r)$, we must have $v_r = v$.

Otherwise, if $v_j = v$ then $3 < j < r$, $C_j = (\ldots(C_3 \cup v_4) \cup \ldots \cup v_j)$ would be a smaller cycle than C_r extending C_3 and containing v, so C_r could not belong to $\mathcal{C}(C_3,v)$.

Consequently $C_r - v$ is a cycle which extends C_3 and, since its lenght is smaller than the minimum r, $C_r - v$ cannot contain any vertex which cones C_3.

Now let x be a predecessor of v in $< C_r >$.

If x precedes exactly two vertices (resp. one vertex) of C_3, then $< x,v,C_3 >$ is isomorphic to N_5^2 (resp. N_5^3).

In any case H_n cannot belong to $\mathcal{AH}$, which is absurd.■

A trivial consequence of proposition 4 is the following.

Corollary 2. *Let H_n be a hamiltonian tournament. If every hamiltonian 5-subtournament of H_n is isomorphic to M_5^i for some $i=1,2,3$, then every non-hamiltonian subtournament of H_n is transitive.*■

Remark 2. We note that there exist tournaments with at least 6 vertices

that are not of Moon-type although their hamiltonian 5-subtournaments are of Moon-type.

Easy examples are provided by $T_6 = T_2(v, M_5^1)$.

REFERENCES

[1] BEINEKE L.W. and REID K.B., *Tournaments*, Selected Topics in Graph Theory, edited by Beineke L.W. and Wilson R.J., Academic Press, New York (1979).

[2] BURZIO M. and DEMARIA D.C., *Characterization of tournaments by coned 3-cycles*, Acta Univ.Carol.-Math.Phys., Vol.28 n.2 (1987), 25-30.

[3] BURZIO M. and DEMARIA D.C., *On a classification of hamiltonian tournaments*, Acta Univ.Carol.-Math.Phys., Vol.29 n.2 (1988), 3-14.

[4] DEMARIA D.C. and GIANELLA G.M., *On local properties of hamiltonian tournaments*, to appear.

[5] MOON J.W., *Topics on Tournaments*, Holt, Rinehart and Winston, New York (1968).

[6] MOON J.W., *Tournaments whose subtournaments are irreducible or transitive*, Canad.Math.Bull., Vol.21 n.1 (1979), 75-79.

Cosimo DE MITRI and Cosimo GUIDO

Department of Mathematics,University of Lecce, 73100 Lecce, Italy.

I PIANI DI MOBIUS, LAGUERRE E MINKOWSKI E LE QUADRICHE NON SINGOLARI DELLO SPAZIO PROIETTIVO FINITO

Giorgio FAINA
Dipartimento di Matematica - Università
Via Vanvitelli 1, 06100 Perugia

Inspired by the pioneering works of F. Buekenhout [3] and W. Benz [2] on the intrinsic characterizations of some non singular quadrics Q of a n-dimensional projective space, the aim of this paper is to emphasize the many interconnections between Benz geometries (i.e. Möbius, Laguerre and Minkowski planes) and nonsingular quadrics by surveying some recent characterization theorems of elliptic [6], parabolic [7] and hyperbolic [8] nonsingular quadrics of finite projective space PG(3,q) .

1. Introduzione

La caratterizzazione delle quadriche non singolari di uno spazio proiettivo finito è certamente uno degli argomenti più studiati nell'ambito delle Geometrie di Galois ed a tal fine, nel corso degli ultimi quaranta anni, sono state messe a punto varie teorie. Limitandoci alla trattazione di quelle più propriamente geometriche, gli approcci principali alla caratterizzazione delle quadriche finite non singolari sono due:

l'*approccio classico (o immerso)*, basato sulla caratterizzazione delle quadriche a partire da una coppia $(\mathcal{E},\mathcal{F})$, dove $\mathcal{E}$ è un opportuno sottoinsieme dell'insieme dei punti di PG(d,q) ed $\mathcal{F}$ è una famiglia di parti di $\mathcal{E}$ soggetta ad opportune condizioni algebriche o geometriche.

Questo lavoro è stato eseguito con il contributo del Ministero dell'Università e della Ricerca Scientifica e Tecnologica e del GNSAGA del CNR.

L' *approccio intrinseco*, basato sulla caratterizzazione delle quadriche a partire da una coppia $(\mathcal{E},\mathcal{F})$, dove $\mathcal{E}$ è un insieme astratto, non necessariamente immerso in uno spazio proiettivo, ed $\mathcal{F}$ è una famiglia o di partizioni di $\mathcal{E}$, o di permutazioni di $\mathcal{E}$ o di sottoinsiemi di $\mathcal{E}$, soggetta a condizioni tali da permettere l'immersione (anche impropria) di $\mathcal{E}$ nell'insieme dei punti sostegno di una quadrica non singolare di un'opportuno PG(d,q).

L' ***approccio classico*** si è evoluto in due direzioni ben distinte:

a) quella detta dell' ***iperpiano tangente***, che riguarda lo studio di coppie $(\mathcal{E},\mathcal{F})$ nelle quali $\mathcal{E}$ è soggetto a delle condizioni analoghe alla condizione di esistenza di un iperpiano tangente in ogni punto di una quadrica di PG(d,q). Gran parte dei risultati ottenuti con questo tipo di approccio sono stati un riflesso della sorprendente congettura di Kustaanheimo [12] del 1949 e della relativa dimostrazione data da B. Segre nel famoso seguente risultato [18].

TEOREMA 1.1. Se $\mathcal{O}$ è un'ovale (i.e. un insieme di q+1 punti a tre a tre non allineati) del piano proiettivo PG(2,q) di ordine dispari, allora $\mathcal{O}$ è una conica irriducibile.

Tale risultato fu immediatamente seguito da quello ottenuto da A. Barlotti [1] e, indipendentemente, da G. Panella [15], relativo alla classificazione delle quadriche ellittiche in PG(3,q), con q dispari.

TEOREMA 1.2. Se Ω è un ovoide (i.e. un insieme di q^2+1 punti a tre a tre non allineati) dello spazio proiettivo PG(3,q) di ordine dispari, allora Ω è una quadrica ellittica.

b) quella detta dei ***caratteri***, con la quale si affronta il problema della caratterizzazione delle quadriche a partire da sottoinsiemi di un PG(d,q) doddisfacenti ad opportune restrizioni sulla cardinalità delle loro intersezioni con certi sottospazi lineari r-dimensionali dello stesso spazio ambiente PG(d,q). Anche in questo caso, per meglio chiarire la problematica in discussione, citiamo due risultati ottenuti da F. Buekenhout [4] e J. Thas [20] rispettivamente.

Sia T un insieme di punti di uno spazio proiettivo $PG(d,q)$. Si dice che T è un *Tallini set* di $PG(d,q)$ se ogni retta che lo incontra in almeno tre punti è completamente contenuta in T. Una *tangente* di un Tallini set T è una retta che o interseca T in esattamente un punto oppure è completamente contenuta in T. Un *insieme quadratico (quadratic set)* è un Tallini set T con la seguente proprietà: per ogni punto A di T, l'insieme

$$T_A = \{B \mid B=A \text{ oppure } B \neq A \text{ e la retta } AB \text{ è tangente}\}$$

o coincide con l'insieme dei punti di un iperpiano oppure è l'insieme di tutti i punti.

TEOREMA 1.3. Un insieme quadratico di uno spazio proiettivo (non necessariamente finito) P o è una quadrica oppure è un ovoide di P.

In [20], Thas modifica la situazione del precedente Teorema provando che:

TEOREMA 1.4. In un PG(d,q) un insieme K di punti tale che ogni iperpiano lo incontri o in 1 oppure in m punti distinti, con $m \geq 2$, e che abbia almeno un iperpiano tangente o è una retta oppure è un ovoide di PG(d,q).

Il metodo generale *intrinseco* si è, anch'esso, sviluppato lungo due direzioni:

a) l'approccio *intrinseco relativo*, che consiste nello studio di coppie $(\mathfrak{E},\mathfrak{I})$ nelle quali $\mathfrak{E}$ è un sottoinsieme di punti di una struttura di incidenza $\mathcal{S}$ (ad es., un piano di Mobius, un piano di Laguerre, un piano di Minkowski, un quadrangolo generalizzato, uno spazio planare) ed ha come scopo quello di stabilire sotto quali condizioni su $\mathcal{S}$ e su $\mathfrak{I}$ è possibile estendere $\mathcal{S}$ ad un PG(d,q) in modo tale che $\mathfrak{E}$ risulti immerso (anche impropriamente) nell'insieme sostegno dei punti di una quadrica irriducibile di PG(d,q). Come al solito, per meglio chiarire la problematica relativa, ci soffermiamo su un significativo risultato ottenuto in questo ambito.

Sia (S,L) uno spazio di rette, cioè sia S un insieme i cui elementi chiameremo punti, L una famiglia di parti di S, i cui elementi

chiameremo rette, tale che ogni retta di L contenga almeno due punti e per due punti distinti passi una sola retta. Supponiamo che esista una famiglia P di sottospazi di (S,L) tale che: $|P|\geq 2$, ogni $\pi\in P$ contenga tre punti indipendenti e per tre punti indipendenti passi un sol elemento di P. La terna (S,L,P) prende il nome di spazio planare e gli elementi di P si dicono piani.

Si dice calotta di uno spazio planare (S,L,P) ogni insieme di punti a tre a tre non allineati. Una calotta H di uno spazio planare (S,L,P) si dice ovoide se:

per ogni $X\in H$, l'unione delle rette tangenti in X ad H costituisce un sottoinsieme t_X di S tale che per ogni coppia di punti distinti $Y,Z\in t_X$, la retta per Y e Z è contenuta in t_X e tale che ogni piano per X incontra t_X in una retta.

D'ora in avanti supporremo che lo spazio planare (S,L,P) abbia tutte le rette con uguale cardinalità $k\geq 2$ ed i piani con uguale cardinalità v. A partire da questi concetti è stata provata la seguente caratterizzazione degli ovoidi (cfr. [19]).

TEOREMA 1.5. Se in uno spazio planare (S,L,P) esiste un ovoide H , allora lo spazio planare coincide con PG(3,q) ed H è una quadrica ellittica se $q=k-1$ è dispari, oppure un ovoide di PG(3,q) se $q=k-1$ è pari.

b) l'***approccio intrinseco assoluto***. Tale approccio permette di fornire caratterizzazioni delle quadriche non singolari di PG(d,q) a partire da una coppia $(\mathfrak{E},\mathfrak{F})$ dove $\mathfrak{E}$ è un insieme astratto qualsiasi. La sua origine risale, implicitamente, al famoso lavoro di F. Buekenhout "Etude intrinséque des ovales", pubblicato nel 1966 (cfr. [3]), ed esplicitamente all'articolo di W. Benz, "Permutations and plane sections of a ruled quadric", pubblicato nel 1972 (cfr [2]).

Altre interessantissime ricerche inquadrabili in questo filone sono dovute a Korchmaros e Olanda [13] ed a Lo Re e Olanda [14]. In esse si caratterizzano gli ovoidi e le quadriche ellittiche di PG(3,q) e le quadriche iperboliche di PG(3,q), rispettivamente, a partire da un insieme astratto $\mathfrak{E}$ e da una famiglia di permutazioni involutorie di $\mathfrak{E}$. Questo tipo di approccio è il più recente, ed è ancora poco

approfondito. Ci sembra pertanto opportuno dedicare questo lavoro ad alcuni recentissimi risultati ottenuti, in questo ordine di idee, dallo stesso autore ed ancora in corso di pubblicazione.

2. I piani di Benz

Prima di passare in rassegna tali risultati, è necessario richiamare alcune definizioni della Teoria dei piani di Benz. Per quanto riguarda, invece, le più familiari definizioni e le principali proprietà relative alle quadriche non singolari di PG(3,q), faremo costante riferimento a [10] e [11].

Un *piano di Benz* è una terna ordinata $(\mathcal{P},\mathcal{B},R)$, dove $\mathcal{P}$ è un insieme astratto i cui elementi sono detti *punti*, $\mathcal{B}$ è una famiglia di parti di $\mathcal{P}$ i cui elementi sono detti *cerchi* ed R è una famiglia di relazioni di equivalenza su $\mathcal{P}$, tale che valgono in essa i seguenti assiomi (due punti X e Y di $\mathcal{P}$ si dicono dipendenti se esiste una relazione di equivalenza $\varrho\in R$ tale che $X\varrho Y$, altrimenti essi si dicono indipendenti):

(B1) per ogni terna di punti a due a due indipendenti $X,Y,Z\in\mathcal{P}$ esiste un unico cerchio $\gamma(X,Y,Z)\in\mathcal{B}$ che li contiene;

(B2) per ogni cerchio $\gamma\in\mathcal{B}$ e per ogni coppia di punti indipendenti $X,Y\in\mathcal{P}$, con $X\in\gamma$, esiste un unico cerchio $\beta(Y,\gamma,X)$ che contiene Y ed è tangente a γ in X (cioè interseca γ soltanto in X se $Y\notin\gamma$ e coincide con γ se $Y\in\gamma$);

(B3) per ogni punto $X\in\mathcal{P}$, per ogni cerchio $\gamma\in\mathcal{B}$ e per ogni relazione di equivalenza $\varrho\in R$ esiste esattamente un punto $Y\in\gamma$ tale che $X\varrho Y$;

(B4) per ogni coppia di punti $X,Y\in\mathcal{P}$ e per ogni coppia di differenti relazioni di equivalenza $\varrho,\varrho'\in R$ esiste esattamente un punto $Z\in\mathcal{P}$ tale che $X\varrho Z$ e $Z\varrho' Y$.

(B5) esistono quattro punti non appartenenti ad un medesimo cerchio ed a due a due indipendenti.

Nel caso in cui $R\equiv\emptyset$, un piano di Benz si dice piano di Möbius; in

tal caso gli assiomi (B3) e (B4) sono sovrabbondanti.

Nel caso in cui $|R|=1$, un piano di Benz si dice piano di Laguerre. In tal caso l'assioma (B4) è sovrabbondante.

Nel caso in cui $|R|=2$, un piano di Benz si dice piano di Minkowski.

4. Gli Ovoidi Generalizzati ed i Piani di Möbius

Sia Ω un ovoide di PG(3,q) ed r una qualsiasi retta esterna ad Ω. Al variare del piano π nel fascio di piani di asse r, resta individuata una partizione di Ω formata dagli insiemi $\pi\cap\Omega$. E' ben noto che ogni piano interseca Ω o in un unico punto oppure in $n+1$ punti distinti. E' altresì evidente che se π e π' sono due piani tali che $\pi\cap\pi'\cap\Omega=\emptyset$, allora i *cerchi* $\pi\cap\Omega$ e $\pi\cap\Omega'$ sono contenuti in una unica partizione di Ω, quella relativa al fascio di piani di asse la retta $\pi\cap\pi'$ esterna ad Ω.
Le nozioni di ovoide e di piano di Möbius sono strettamente legate tra loro. Infatti, la struttura di incidenza $I(\Omega)=(\mathcal{P},\mathcal{B},|)$, con $\mathcal{P}\equiv\Omega$, $\mathcal{B}\equiv\{\pi\cap\Omega : \pi$ piano di PG(3,q) non tangente ad $\Omega\}$ e $|=\in$, è un piano di Möbius (o inversivo) finito di ordine q. Un piano di Möbius isomorfo ad un $I(\Omega)$ è detto *ovoidale.*
Tutti i piani di Möbius finiti a noi noti sono ovoidali. In virtù del già citato Teorema 1.2 di Barlotti, ogni piano di Möbius finito di ordine q dispari che si conosca è isomorfo ad $I(\Omega)$, con Ω quadrica ellittica di un opportuno PG(3,q). Per q pari, invece, sono note due distinte classi di ovoidi: la quadrica ellittica e l'ovoide di Suzuki-Tits (cfr. [22]) e non è escluso che possano esistere altre classi di ovoidi. D'altro canto, è ben noto un teorema di P. Dembowski nel quale si prova che ogni piano di Möbius finito è ovoidale [5]. Pertanto, nel caso pari, l'ordine di un piano di Möbius è sempre della forma $q=2^h$.
A questo punto ci sembra naturale porsi il seguente problema:

dato un arbitrario insieme finito $\mathcal{E}$ ed una famiglia $\mathcal{F}$ di partizioni di $\mathcal{E}$, quali condizioni è necessario imporre su $\mathcal{F}$ affinché si possa definire su $\mathcal{E}$ una struttura di piano di Möbius (ovoidale o non) oppure di ovoide di un opportuno spazio proiettivo PG(3,q)?

In [6] sono stati dimostrati alcuni risultati inerenti a questo problema, ma prima di trattarli è necessario fornire alcune definizioni.

Siano $\mathcal{E}$ un insieme astratto finito ed $\mathfrak{Z}$ una famiglia di partizioni di $\mathcal{E}$. Si denoti con $\mathcal{B}$ la famiglia di tutti quei sottoinsiemi di $\mathcal{E}$ che appartengono ad almeno una partizione di $\mathfrak{Z}$. Nel seguito, gli elementi di $\mathcal{E}$ e di $\mathcal{B}$ saranno detti *punti* e *cerchi*, rispettivamente.

Onde evitare lo studio di casi banali, d'ora in avanti, denotata con v la cardinalità di $\mathcal{E}$ e fissato un intero positivo $n \geq 3$, supporremo che:

(2.1) ogni cerchio $\gamma \in \mathcal{B}$ contiene o uno o n punti;

(2.2) esistono in $\mathcal{B}$ due cerchi di cardinalità n (o n-cerchi) disgiunti e tali che la loro unione è propriamente contenuta in $\mathcal{E}$.

La coppia $(\mathcal{E},\mathfrak{Z})$ si dice *ovoide generalizzato di tipo n* (o, più brevemente, OG(n)) se valgono le seguenti proprietà:

(A.1) per ogni terna di punti distinti passa uno ed un solo cerchio;

(A.2) ogni coppia di cerchi disgiunti è contenuta in una ed una sola partizione;

In base alle osservazioni riportate all'inizio di questo numero, possiamo osservare quanto segue.

Se Ω è un ovoide (ad es., una quadrica ellittica non singolare) di PG(3,q), ad ogni retta r esterna ad Ω resta associato un fascio di piani ed ognuno di tali piani interseca Ω o in un punto oppure in n=q+1 punti distinti. Pertanto, ad ogni retta r esterna ad Ω resta associata una partizione $\mathcal{P}(r)$ di Ω stessa e, denotata con $\mathfrak{Z}$ la famiglia di tutte le partizioni $\mathcal{P}(r)$ ottenute al variare di r nell'insieme delle rette esterne ad Ω, la coppia $(\Omega,\mathfrak{Z})$ fornisce un esempio di OG(q+1).

Un esempio di OG(n) non derivabile da alcun ovoide proiettivo né da alcun piano di Möbius è, invece, il seguente: sia $\mathcal{E}$ un insieme di cardinalità 7 e sia $\mathcal{B}_3$ la famiglia di tutte le terne di punti distinti di $\mathcal{E}$. Inoltre, sia $\mathfrak{Z}$ la famiglia di tutte le partizioni di $\mathcal{E}$ formate da due terne disgiunte di $\mathcal{B}_3$ e dal residuo punto di $\mathcal{E}$ non contenuto in esse e la partizione di $\mathcal{E}$ formata da tutti i sottoinsiemi di $\mathcal{E}$ di cardinalità 1 sia anch'essa in $\mathfrak{Z}$. E' facile verificare che $(\mathcal{E},\mathfrak{Z})$ è un OG(3). Inoltre, poiché non esistono piani inversivi di cardinalità 7, tale struttura non

è derivabile da alcun ovoide proiettivo né da alcun piano inversivo ovoidale o non.

Esistono anche OG(n) tali che l'insieme degli 1-cerchi è vuoto. Si consideri, infatti, un qualsiasi insieme $\mathcal{E}$ di cardinalità 9 e si denoti con $\mathcal{B}$ la famiglia di tutte le terne non ordinate di punti di $\mathcal{E}$. Se $\mathcal{Z}$ denota la famiglia delle partizioni di $\mathcal{E}$ costituite da tre terne disgiunte di $\mathcal{Z}$, allora la coppia $(\mathcal{E},\mathcal{Z})$ è un esempio di OG(3) con $\mathcal{B}_1=\emptyset$. Anche in questo esempio $(\mathcal{E},\mathcal{Z})$ non è derivabile da alcun ovoide proiettivo né da alcun piano inversivo ovoidale o non.

Al fine di snellire la successiva trattazione denoteremo con:

$\mathcal{B}_n$ la famiglia di tutti gli n-cerchi di $\mathcal{B}$

$\mathcal{B}_1$ la famiglia di tutti i cerchi di $\mathcal{B}$ aventi cardinalità 1 (o 1-cerchi)

$\mathcal{Z}(\gamma)$ la famiglia delle partizioni di $\mathcal{Z}$ che contengono un fissato cerchio γ di $\mathcal{B}$

$\mathcal{B}(X)$ la famiglia dei cerchi di $\mathcal{B}$ che contengono un assegnato punto X di $\mathcal{E}$

Se in un OG(n) vale la successiva proprietà (A.3), diremo che esso è proiettivo e lo denoteremo con POG(n):

(A.3) esiste almeno un 1-cerchio $\{X\}$ tale che $|\mathcal{B}(X)|=|\mathcal{Z}\{X\}|+n$.

In [6] sono stati provati i seguenti risultati.

TEOREMA 3.1. Se $(\mathcal{E},\mathcal{Z})$ è un PGO(n), allora $(\mathcal{E},\mathcal{B}_n)$ è un piano di Mobius di ordine q=n-1.

LEMMA 3.2. Se $(\mathcal{E},\mathcal{Z})$ è un PGO(n), allora ogni partizione di $\mathcal{Z}$ contiene esattamente due 1-cerchi e ad ogni n-cerchio γ resta associata una permutazione involutoria $I(\gamma)$ dei punti di $\mathcal{E}$ che ha come punti uniti tutti e soli i punti di γ.

Denoteremo, d'ora in avanti, con Γ_n la famiglia di tutte le permutazioni involutorie $I(\gamma)$ di cui al precedente lemma.

Come è stato già ricordato, se q è pari, tutti i piani di Mobius di ordine q sono ovoidali e non si conoscono ancora piani inversivi non ovoidali di ordine q dispari (cfr [5], p. 254). Inoltre, (cfr. [1]), se q

è dispari, ogni ovoide proiettivo di PG(3,q) è l'insieme dei punti di una quadrica ellittica dello stesso PG(3,q).

TEOREMA 3.3. Se $(\mathcal{E},\mathfrak{F})$ è un PGO(n), con q=n-1 pari, allora $q=2^h$ per un opportuno intero $h\geq 2$ e l'insieme $\mathcal{E}$ è un ovoide proiettivo di PG(3,q).

TEOREMA 3.4. Se $(\mathcal{E},\mathfrak{F})$ è un PGO(n), con q=n-1 dispari, tale che per ogni coppia di punti distinti di $\mathcal{E}$ ogni involuzione di Γ_n che li scambia è permutabile con ogni involuzione di Γ_n che li fissa, allora $\mathcal{E}$ è un ovoide proiettivo (i.e. una quadrica ellittica) di PG(3,q).

4. Coni generalizzati e Piani di Laguerre

Sia Ω un ovale del piano proiettivo π=PG(2,q). Sia V un punto di PG(3,q)$\setminus\pi$ e sia Σ il cono che proietta Ω da V. Le nozioni di cono e di piano di Laguerre sono strettamente legate tra loro. Infatti, siano: $\mathcal{P}\equiv\Sigma\setminus\{V\}$, $\mathcal{B}_1$ l'insieme di tutti i generatori di Σ, $\mathcal{B}_2$ la famiglia degli insiemi ottenuti intersecando Σ con i piani di PG(3,q) non contenenti V ed | sia la naturale incidenza. E' facile dimostrare che la struttura di incidenza $L(\Omega):=(\mathcal{P},\mathcal{B},|)$, con $\mathcal{B}=\mathcal{B}_1\cup\mathcal{B}_2$, è un piano di Laguerre di ordine q. Un piano di Laguerre isomorfo ad un $L(\Omega)$ è anche detto *ovoidale*. Se l'ovale Ω è una conica irriducibile, allora ogni piano di Laguerre isomorfo a $L(\Omega)$ è detto *classico*. Tutti i piani di Laguerre finiti a noi noti sono ovoidali. Dal teorema 1.1 discende immediatamente che ogni piano di Laguerre finito di ordine dispari è classico.

Si osservi, inoltre, che: posto $\mathcal{E}=\Sigma\setminus\{V\}$, ad ogni retta di PG(3,q) esterna ad $\mathcal{E}$ corrisponde una partizione di $\mathcal{E}$ stesso e, come nel numero precedente, è naturale porsi il seguente problema:

dato un arbitrario insieme finito $\mathcal{E}$ ed una famiglia $\mathfrak{F}$ di partizioni di $\mathcal{E}$, quali condizioni è necessario imporre su $(\mathcal{E},\mathfrak{F})$ affinché si possa definire su $\mathcal{E}$ una struttura di piano di Laguerre (ovoidale o non) oppure di cono quadrico di un opportuno spazio proiettivo PG(3,q)?

In [7] sono stati dimostrati alcuni risultati inerenti a questo problema, ma prima di trattarli è necessario fornire alcune definizioni.

Siano $\mathcal{E}$ un insieme astratto finito ed $\mathfrak{I}$ una famiglia di partizioni di $\mathcal{E}$. Si denoti con $\mathcal{B}$ la famiglia di tutti quei sottoinsiemi di $\mathcal{E}$ che appartengono ad almeno una partizione di $\mathfrak{I}$. Nel seguito, gli elementi di $\mathcal{E}$ e di $\mathcal{B}$ saranno detti *punti* e *cerchi*, rispettivamente. Due punti X e Y di $\mathcal{E}$ si diranno *dipendenti* se non esiste alcun cerchio di $\mathcal{B}$ che li contiene simultaneamente. Se X ed Y sono dipendenti denoteremo ciò con il seguente simbolo: $X||Y$.

Come nel caso degli OG(n), onde evitare lo studio di casi banali, d'ora in avanti supporremo che valgano anche in questo numero le condizioni (2.1) e (2.2).

La coppia $(\mathcal{E},\mathfrak{I})$ si dice *cono generalizzato di tipo n* (o, più brevemente, CG(n)) se valgono le seguenti proprietà:

(A.1) per ogni terna di punti a due a due indipendenti passa uno ed un solo cerchio;

(A.2) ogni coppia di cerchi disgiunti è contenuta in una ed una sola partizione;

(A.3) comunque si fissino un cerchio γ ed un punto $X\in\mathcal{E}\setminus\gamma$, esiste in γ esattamente un punto X_γ tale che $X_\gamma||X$.

Un CG(n) si dice proiettivo, e si denota con PCG(n), se in esso vale la seguente proprietà:

(A.4) Esiste almeno una coppia di punti indipendenti che è contenuta in esattamente $s=n-1$ cerchi.

Osserviamo, innanzitutto, che (A.4) è indipendente dagli altri assiomi. Infatti, sia $\mathcal{E}:=\{X_1,X_2,X_3,Y_1,Y_2,Y_3,Z_1,Z_2,Z_3\}$, con $|\mathcal{E}|=9$, e sia $\mathcal{B}$ la famiglia di tutte le terne di punti di $\mathcal{E}$ del tipo $\{X_i,Y_j,Z_k\}$, $i,j,k=1,2,3$. Sia, infine, $\mathfrak{I}$ la famiglia delle partizioni di $\mathcal{E}$ ognuna delle quali è costituita da tre terne disgiunte di $\mathcal{B}$. E' facile verificare che $(\mathcal{E},\mathfrak{I})$ verifica (A.1), (A.2) ed (A.3) con $m=1$ ed $n=3$ ma anche che $s=3\neq n-1$.

Invece, a partire da un cono quadrico di PG(3,q), si ottiene un esempio di PCG(n), con $n=q+1$. Infatti, sia Σ un cono quadrico di

vertice V in PG(3,q). Posto $\mathcal{E}=\Sigma\setminus\{V\}$, ad ogni retta dello spazio esterna a Σ corrisponde in modo naturale una partizione di $\mathcal{E}$ stesso individuata dalle intersezioni con $\mathcal{E}$ dei singoli piani del fascio di asse la retta stessa. Denotata con $\mathfrak{Z}$ la famiglia delle partizioni di $\mathcal{E}$ ottenibili nel modo anzidetto, è facile verificare che $(\mathcal{E},\mathfrak{Z})$ è un CG(n), con n=q+1 ed s=n-1=q.

In accordo con la terminologia adottata sui piani di Laguerre, sui piani di Laguerre ovoidali e sui piani di Laguerre classici, in [7] sono stati dimostrati i seguenti risultati:

TEOREMA 4.1. Se $(\mathcal{E},\mathfrak{Z})$ è un PCG(n), allora esiste una partizione $\mathfrak{L}$ di $\mathcal{E}$ tale che la struttura di incidenza $(\mathcal{E}, \mathfrak{L}\cup\mathfrak{B}, I)$, dove con I si indica la naturale relazione d'incidenza, è un piano di Laguerre.

Un CG(n) si dice *regolare* se soddisfa le due seguenti condizioni:

(TF) Per ogni terna di coppie (X_i,γ_i), con $X_i\in\mathcal{E}$, $X_i\in\gamma_i$, $X_1\neq X_2\neq X_3\neq X_1$, i=1,2,3, tali che almeno due dei punti X_i sono indipendenti e nessun cerchio tangente a γ_i in X_i è tangente anche a γ_j in X_j per $i\neq j$, esiste un punto $Y\in\mathcal{E}\setminus\{X_1,X_2,X_3\}$ tale che i cerchi β_i, i=1,2,3, dove β_i è l'unico cerchio per Y tangente in X_i a γ_i, sono a due a due tangenti in Y.

(DF) Per ogni coppia (X_1,γ_1), (X_2,γ_2), con X_1 ed X_2 indipendenti e tali che nessun cerchio è tangente sia a γ_1 in X_1 che a γ_2 in X_2, e tale che fissato un qualsiasi punto Y, indipendente sia con X_1 che con X_2, e denotata con $\partial(Y)$ la famiglia dei punti di $\mathcal{E}$ dipendenti con Y, esiste in $\partial(Y)$ un punto Z tale che i cerchi β_1 e β_2, dove β_i è l'unico cerchio per Z tangente a γ_i in X_i (i=1,2), sono tangenti tra loro.

TEOREMA 4.2. Se $(\mathcal{E},\mathfrak{Z})$ è un PCG(n) regolare, con n dispari, allora esiste una partizione $\mathfrak{L}$ di $\mathcal{E}$ tale che la struttura di incidenza $(\mathcal{E}, \mathfrak{L}\cup\mathfrak{B}, I)$, dove con I si indica la naturale relazione d'incidenza, è un piano di Laguerre classico.

COROLLARIO Se $(\mathcal{E},\mathfrak{Z})$ è un PCG(n) regolare con n dispari, allora $\mathcal{E}$ coincide con l'insieme dei punti di un cono quadrico di

PG(3,q), con q=n-1, privato del suo vertice ed ogni cerchio di $\mathcal{B}$ coincide con l'insieme intersezione di un opportuno piano di PG(3,q), non passante per il vertice del cono, ed $\mathcal{E}$.

5. Iperbolodi generalizzati e piani di Minkowski

Siano H una quadrica iperbolica di PG(3,q), $\mathcal{P}:=H$, $\mathcal{B}_1=\mathcal{B}_1' \cup \mathcal{B}_1''$, dove $\mathcal{B}_1'$ e $\mathcal{B}_2'$ sono le due famiglie di generatori di H, $\mathcal{B}_2$ la famiglia delle intersezioni di H con i piani non tangenti ad H stesso ed $|$ la naturale relazione d'incidenza. Allora la struttura di incidenza $M(H)=(\mathcal{P},\mathcal{B}_1 \cup \mathcal{B}_2,|)$ è un piano di Minkowski di ordine q. Ogni piano di Minkowski isomorfo ad un $M(H)$ si dice *classico*.

Ricordiamo che in [17] è stata dimostrata l'esistenza di piani di Minkowski di ordine n dispari che sono non classici. Invece, in [9] ed indipendentemente in [16], è stato dimostrato che ogni piano di Minkowski di ordine pari è classico. Perciò nel caso pari l'ordine di un piano di Minkowski è sempre della forma $n=2^h$.

Si osservi, inoltre, che: posto $\mathcal{E}=H$, ad ogni retta r di PG(3,q) esterna ad $\mathcal{E}$ corrisponde una partizione di $\mathcal{E}$ stesso generata dai piani del fascio di asse la stessa retta r.

A questo punto, come nei numeri precedenti, è naturale porsi l'analogo seguente quesito:

dato un arbitrario insieme finito $\mathcal{E}$ ed una famiglia $\mathcal{F}$ di partizioni di $\mathcal{E}$, quali condizioni è necessario imporre su $(\mathcal{E},\mathcal{F})$ affinché si possa definire su $\mathcal{E}$ una struttura di piano di Minkowski (classico o non) oppure di quadrica iperbolica di un opportuno spazio proiettivo PG(3,q)?

Prima di affrontare tale questione, diamo alcune definizioni. Come nei numeri precedenti, siano $\mathcal{E}$ un insieme astratto finito ed $\mathcal{F}$ una famiglia di partizioni di $\mathcal{E}$. Si denoti con $\mathcal{B}$ la famiglia di tutti quei sottoinsiemi di $\mathcal{E}$ che appartengono ad almeno una partizione di $\mathcal{F}$. Inoltre, come nei numeri precedenti, si definiscano le nozioni di punto, di cerchio, di dipendenza tra due punti così come si

suppongano soddisfatte le (2.1) e (2.2).

La coppia $(\mathcal{E},\mathfrak{I})$ si dice *iperboloide generalizzato di tipo n* (o, più brevemente, IG(n)) se valgono le seguenti proprietà:

(A.1) per ogni terna di punti a due a due indipendenti passa uno ed un solo cerchio;

(A.2) ogni coppia di cerchi disgiunti è contenuta in una ed una sola partizione;

(A.3) comunque si fissino un cerchio γ ed un punto $X\in\mathcal{E}\setminus\gamma$, esistono in γ esattamente due punti $X_{1\gamma}$ e $X_{2\gamma}$ tali che $X_{1\gamma}\|X\|X_{2\gamma}$.

Nel seguito, per brevità, spesso indicheremo con $\gamma(X)$ la famiglia dei punti del cerchio γ indipendenti rispetto ad un fissato punto $X\notin\gamma$.

Un IG(n) si dice proiettivo, e si denota con PIG(n), se in esso vale la seguente proprietà:

(A.4) Esiste almeno una coppia di punti indipendenti che è contenuta in esattamente s=n-2 cerchi.

Se H è una quadrica iperbolica non-singolare di PG(3,q), la coppia $(H,\mathfrak{I})$, dove $\mathfrak{I}$ indica la famiglia delle partizioni dell'insieme dei punti che costituiscono H individuate da tutte le rette esterne ad H stesso, ci fornisce un esempio di PIG(n) con n=q+1.

In virtù di (A.3), fissato un qualsiasi cerchio $\gamma\in\mathcal{B}$, si può definire almeno una applicazione

$$\varphi(\gamma):\mathcal{E}\setminus\gamma\rightarrow\gamma\times\gamma$$

tale che ad ogni punto X del dominio faccia corrispondere una coppia ordinata $(X_{1\gamma},X_{2\gamma})$ di punti di γ dipendenti con X stesso.

Allora, fissate una qualsiasi partizione $\mathcal{P}\in\mathfrak{I}$ ed una qualsiasi famiglia $\Psi=\{\varphi(\beta)\mid\beta\in\mathcal{P}\}$ di applicazioni, denoteremo con $r_i(\Psi)(X)$, [o, se il contesto lo permetterà, semplicemente con $r_i(X)$] l'insieme $\{X_{i\beta}\mid\beta\in\mathcal{P},\ X\notin\beta\}\cup\{X\}$, i=1,2, dove $(X_{1\beta},X_{2\beta})=\varphi(\beta)(X)$.

Un PIG(n), $(\mathcal{E},\mathfrak{I})$, si dice *regolare* se ogni $\varphi(\gamma)$ è iniettiva ($\gamma\in\mathcal{B}$) e se, rispetto ad almeno una partizione $\mathcal{P}\in\mathfrak{I}$, esiste una famiglia $\Psi=\{\varphi(\gamma)\mid\gamma\in\mathcal{P}\}$ tale che $r_i(\Psi)(X)=r_i(\Psi)(X_{i\partial})$ per ogni $\partial\in\mathcal{P}$.

A partire dal concetto di iperboloide generalizzato appena introdotto, in [8] sono stati dimostrati i seguenti risultati:

Teorema 5.1. Se $(\mathcal{E},\mathfrak{I})$ è un PIG(n) regolare, allora esiste in $\mathcal{E}$ una famiglia $\Sigma=\Sigma_1\cup\Sigma_2$ di sottoinsiemi tale che la struttura d'incidenza $(\mathcal{E},\Sigma\cup\mathcal{B},|)$, dove con | si indica la naturale relazione d'incidenza, è un piano di Minkowski di ordine q=n-1.

Dal Teorema 5.1 e dal fondamentale Teorema di W. Heise [9] e N. Percsy [16], segue immediatamente che vale il seguente

Teorema 5.2. Se $(\mathcal{E},\mathfrak{I})$ è un PIG(n) regolare con q=n-1 pari,allora $(\mathcal{E},\Sigma\cup\mathcal{B},I)$ è un piano di Minkowski classico ed $\mathcal{E}$ è l'insieme dei punti di una quadrica iperbolica di PG(3,q).

Dato un PIG(n) regolare e fissato un qualsiasi cerchio $\gamma\in\mathcal{B}$ ed un qualsiasi punto $X\in\mathcal{E}\setminus\gamma$, se esiste un punto $Y\in\mathcal{E}\setminus\gamma$ tale che, con riferimento ad una particolare Ψ, $X_1\gamma=Y_2\gamma$ e $X_2\gamma=Y_1\gamma$, allora diremo che X ed Y sono *opposti* rispetto a γ. Se X e Y sono opposti rispetto a γ allora essi sono indipendenti. Infatti, se X||Y, allora si avrebbe che o $X_1\gamma=Y_1\gamma$ o $X_2\gamma=Y_1\gamma$ e quindi che $X_1\gamma=X_2\gamma$ il che è *assurdo. Vale allora anche il seguente*

Teorema 5.3. Sia $(\mathcal{E},\mathfrak{I})$ un PIG(n) regolare e tale che per ogni coppia di punti X, Y di $\mathcal{E}$ tra loro opposti rispetto ad un fissato cerchio $\gamma\in\mathcal{B}$ e per ogni cerchio ∂, contenente sia X che Y, si verifichi che, se $Z\in\partial$, allora esiste un punto $U\in\partial$ opposto a Z rispetto a γ.

Allora la struttura d'incidenza $(\mathcal{E},\Sigma\cup\mathcal{B},I)$ è un piano di Minkowski di ordine q=n-1 ed $\mathcal{E}$ è l'insieme dei punti di una quadrica iperbolica di PG(3,q).

BIBLIOGRAFIA

1. BARLOTTI, A., Un'estensione del teorema di Segre-Kustaanheimo, *Boll. Un. Mat. Ital.* **10** (1955), 498-506.
2. BENZ, W., Permutations and plane sections of a ruled quadric, *Symposia Math.*, Academic Press, New York, **5** (1971), 325-339.
3. BUEKENHOUT, F., Etude intrinsèque des ovales, *Rend. Mat. Appl.* **25** (1966), 333-393.
4. BUEKENHOUT, F., Ensembles quadratiques des espaces projectifs, *Math. Z.* **110** (1969), 306-318.
5. DEMBOWSKI, P., Finite geometries, Springer Berlin, 1968.
6. FAINA, G., Ovoidi generalizzati, *Rend. Sem. Mat. Univ. Politec. Torino* **46** (1988), 247-257.
7. FAINA, G., On embeddable Laguerre Planes, preprint.
8. FAINA, G., Generalized Minkowski planes, preprint.
9. HEISE, W., Minkowski-Ebenen gerader Ordnung, *J. Geom.* **5** (1974), 83.
10. HIRSCHFELD, J.W.P., Projective Geometries over Finite Fields, Clarendon Press, Oxford 1979.
11. HIRSCHFELD, J.W.P., Finite Projective Spaces of Three Dimensions, Clarendon Press, Oxford 1985.
12. JARNEFELT, G. and KUSTAANHEIMO, P., An observation on finite geometries, *Skan. Math. Kong. Trondheim* **11** (1949), 166-182.
13. KORCHMAROS, G. and OLANDA, D., On egglike inversive planes, *J. of Geom.* **21** (1983), 53-58.
14. LO RE, P.M. and OLANDA, D., On Embeddable Minkowski Planes, *J. Geom.* **21** (1983), 138-145.
15. PANELLA, G., Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, *Boll. Un. Mat. Ital.* **10** (1955), 507-513.
16. PERCSY, N., Announcement at Finite Geometries Session, Oberwolfach 1974.

RECENTI RISULTATI SUI GRUPPI DI AUTOMORFISMI DI ALCUNE NOTEVOLI STRUTTURE GEOMETRICHE

Gabor KORCHMAROS

Lo studio delle stutture geometriche discrete, prevalentemente di natura combinatoria, riveste una certa importanza nella teoria dei gruppi di permutazioni. In quest'ambito, sono tuttora in corso ricerche, ci è sembrato pertanto utile presentare una rassegna dei risultati esposti nei lavori elencati nella Bibliografia.

1. Le 3-reti

Un quasigruppo $(X,\cdot)$ consiste notoriamente di un insieme X e di una operazione binaria $\cdot$ definita su X e tale che comunque presi due elementi $a,b \in X$, ciascuna delle equazioni $a\cdot x=b$ e $y\cdot a=b$ ha una e una sola soluzione. Un cappio è un quasigruppo dotato di un elemento unità e. Una 3-rete $\mathcal{N}$ è una struttura geometrica che consiste di un insieme $\mathbf{P}$ di punti e di una famiglia $\mathbf{L}$ di parti di $\mathbf{P}$, che si dicono *rette*, soddisfacenti le seguenti proprietà:

1) $\mathbf{L}$ *è suddivisa in 3 sottofamiglie disgiunte* $\mathbf{L}_i$ $(i=1,2,3)$;
2) *ogni punto appartiene ad una e una sola retta di ciascuna sottofamiglia;*
3) *due rette di sottofamiglie diverse hanno esattamente un punto in comune;*
4) *esistono tre rette appartenenti a tre sottofamiglie diverse e non contenenti uno stesso punto.*

È naturale dire che due rette di una stessa sottofamiglia hanno la "stessa direzione" oppure che "sono parallele". Ad ogni quasigruppo $(X,\cdot)$ si può associare una 3-rete in modo che i punti siano le coppie ordinate di elementi di X e le 3 sottofamiglie siano formate dai seguenti sottoinsiemi di punti:

$g_h = \{ (x,g) \mid g \text{ costante}, x \in X\}$, rette orizzontali;
$g_v = \{ (g,y) \mid g \text{ costante}, y \in X\}$, rette verticali;
$g_t = \{ (x,y) \mid x \cdot y = g; \text{ con } g \text{ costante } x,y \in X\}$, rette trasversali.

Viceversa, ogni 3-rete può essere coordinatizzata mediante un quasigruppo. Quelli che coordinatizzano una stessa 3-rete costituiscono una classe di isotopia la quale contiene sempre un cappio.

Per l'ordine di una 3-rete si intende l'ordine di un (qualsiasi) quasigruppo che la coordinatizza.

Una collineazione di una 3-rete è una permutazione dei punti che mandi rette in rette. Le collineazioni di una 3-rete costituiscono un gruppo contenente un sottogruppo normale (di indice ≤ 6) che conserva ciascuna direzione (cioè manda rette parallele in rette parallele).

Una teoria generale delle 3-reti con particolare riguardo ai gruppi di collineazioni è stata sviluppata da Barlotti e Strambach [1], la quale è stata ulteriormente approfondita per una importante classe di 3-reti particolari, dette 3-reti involutorie con identità.

Definizione 1. - *Una 3-rete N si dice involutoria se gode della seguente proprietà configurazionale:*

> *la retta trasversale contenente il punto (a,b) contiene anche il punto (b,a).*

Si può verificare che una 3-rete è involutoria con identità se e solo se è coordinatizzabile mediante un cappio commutativo di esponente 2. Nel caso in cui tale cappio sia un gruppo (quindi un 2-gruppo abeliano elementare), la 3-rete associata è immergibile in un piano di Galois e prende il nome di 3-rete involutoria classica con identità. Una sua caratterizzazione in termini gruppali è data dal seguente teorema:

Teorema 1. ([10] Theorem 5) *Una 3-rete involutoria con identità è classica se e soltanto se ammette un gruppo di automorfismi che:*

(1) *contenga un sottogruppo normale risolubile,*

(2) *conservi le direzioni,*

(3) *muti in sé una retta trasversale e operi sui punti di essa come un gruppo di permutazioni 2-volte transitivo.*

Notiamo che l'ipotesi (1) è essenziale in quanto vi sono 3-reti involutorie con identità che non sono classiche pur dotate di un gruppo di automorfismi che godono di entrambe le proprietà (2) e (3).

2. Le $\begin{bmatrix} X \\ t \end{bmatrix}$- geometrie con parallelismo

Continueremo a denotare con X un insieme finito di cardinalità n. Per analogia alle abituali notazioni di calcolo combinatorio, useremo il simbolo $\binom{X}{t}$ per indicare la famiglia dei t-insiemi di X (ossia i sottoinsiemi formati da esattamente t ($1<t<n$) punti). Osserviamo che $|\binom{X}{t}| = \binom{n}{t}$. Seguendo P. Cameron [3], introduciamo la nozione di parallelismo in $\binom{X}{t}$:

Definizione 2. - *Un parallelismo di* $\binom{X}{t}$ *è una relazione di equivalenza in* $\binom{X}{t}$ *soddisfacente la seguente proprietà:*

comunque presi un punto $P \in X$ *e un t-insieme* $b \in \binom{X}{t}$ *esiste un unico t-insieme* $c \in \binom{X}{t}$ *contenente* P *e parallelo a* b.

Ricordiamo che per un noto teorema dovuto a Baranyai (vedi [3] p. 5), una $\binom{X}{t}$-geometria con parallelismo esiste se e solo se t divide n. Un automorfismo di una $\binom{X}{t}$-geometria con parallelismo è una permutazione su X che manda coppie di t-insiemi paralleli in coppie di t-insiemi paralleli. An automorfismo si dice stretto se ogni t-insieme e la sua immagine sono paralleli. Gli automorfismi stretti costituiscono un sottogruppo normale del gruppo degli automorfismi. Tale sottogruppo è piuttosto ristretto: per $t>2$ è addirittura banale mentre per $t=2$ è isomorfo ad un 2-gruppo abeliano elementare che opera su X come un gruppo di permutazioni semire-

golare. Il caso di t=2 riveste particolare importanza anche per il fatto che è una generalizzazione della nozione classica di spazio affine sopra GF(2).

Una proprietà che nasce in modo naturale nell'ambito di tali geometrie è la proprietà del parallelogramma (cfr. [3] p.19): Comunque presi tre t-insiemi $a,b,c \in \binom{X}{t}$ tali che $a \| b$, $a \neq b$ e $c \subseteq a \cup b$, risulta $c \| (a \cup b)-c$. Conviene notare che se t=2 la proprietà di parallelogramma asserisce che se una coppia di lati opposti di un quadrangolo sono paralleli, lo stesso vale per l'altra coppia di lati opposti. È curioso che la proprietà del parallelogramma non caratterizzi gli spazi affini sopra GF(2) nell'ambito delle $\binom{X}{t}$ geometrie con parallelismo. Esiste comunque una unica eccezione data dalla $\binom{X}{4}$-geometria con il parallelismo sestetto sopra un insieme X di cardinalità 24. Poiché il gruppo degli automorfismi di tale geometria è isomorfo al gruppo di Mathieu M_{24}, si ha il

Teorema 2. ([3], p.21)- *Il gruppo degli automorfismi di una* $\binom{X}{t}$*-geometrie con parallelismo soddisfacente la proprietà del parallelogramma è isomorfo ad* ASL(m,2) *oppure a* M_{24}.

3. Le colorazione del grafo completo con il minor numero di colori

Si dice grafo completo il grafo in cui ogni coppia di vertici è congiunta da uno spigolo. Se ad ogni spigolo di un grafo completo si dà un colore si ha una colorazione di spigoli. Ci limiteremo a considerare colorazioni del grafo completo su un numero n pari di vertici che usino n-1 colori e che abbiano la proprietà che mai due spigoli uscenti da uno stesso vertice sono equicolorati. Tali colorazioni di spigoli sono dette *minime* in quanto occorrono ad ogni modo almeno n-1 colori perché un grafo completo abbia una colorazione che goda della suddetta proprietà. Avvertiamo che nei lavori [6] e [9] si adopera il termine di uno-fattorizzazione anziché colorazione minima di spigoli, ma la differenza è formale. (cfr. [3], §IV p.63).

Un automorfismo di una colorazione di spigoli è una permutazione dei vertici che mandi spigoli equicolorati in spigoli equicolorati. Una colorazione minima di spigoli di un grafo completo è detta k-transitiva se ammette un gruppo di automorfismi che operi sui vertici come un gruppo di permutazioni k-volte transitivo.

Lo studio delle colorazioni minime di spigoli k-volte ($k \geq 2$) transitive ha avuto inizio negli anni Settanta ad opera di Cameron ed è stato completato recentemente con l'uso della classificazione dei gruppi semplici finiti.

Teorema 3 ([4]) - *Classificazione completa delle colorazioni k-transitive ($k \geq 2$) minime di spigoli del grafo completo su n vertici:*

1) una classe infinita di colorazioni 3-transitive minime di spigoli: $n=2^m$ $(m=1,2,\ldots)$ *e il gruppo degli automorfismi è isomorfo ad* $ASL(m,2)$.

2) cinque esempi di tipo sporadico:

n	k	*gruppo degli automorfismi*
4	4	S_4 ($\cong PGL(2,4)$)
6	3	S_5 ($\cong PGL(2,5)$)
8	2	$PSL(2,7)$
12	2	$PSL(2,11)$
28	2	$P\Gamma L(2,8)$

Esistono invece per tutti i valori di n, delle colorazioni 1-transitive minime di spigoli del grafo completo su n vertici. In proposito, riportiamo due risultati su colorazioni cicliche (sono così chiamate le colorazioni dotate di un gruppo ciclico di automorfismi che opera sui vertici come un gruppo 1-transitivo di permutazioni.

Teorema 4. ([5]).- *Condizione necessaria e sufficiente affinché esista una colorazione ciclica minima del grafo completo su* n *vertici è che* n *sia una potenza di 2 ad esponente* ≥ 3.

Teorema 5. ([8]) - *Se il grafo completo su* n *vertici ammette una colorazione ciclica minima di spigoli tale che il relativo gruppo ciclico di automorfismi conservi un colore, allora* $n \not\equiv 0 \pmod 8$.

4. I sistemi di terne di Steiner

Un sistema di Steiner S(t,k,v) consiste di un insieme non vuoto X di cardinalità v (i cui elementi saranno detti punti) e di una famiglia di parti di X, detti blocci, ciascuna di cardinalità t tale che k punti distinti appartengano ad uno e un sol blocco. Tale nozione risale al 1844 ed è una delle più antiche nel campo della Combinatoria. Studi approfonditi di natura gruppale sui sistemi di Steiner sono stati effettuati soprattutto negli anni 30; vale la pena di ricordare l'importante caratterizzazione dei gruppi di Mathieu come gruppi di automorfismi di certi sistemi di Steiner. In anni recenti, l'interesse è rivolto principalmente al caso t=3, k=2, cioè ai sistemi di terne di Steiner. Sono state date diverse caratterizzazioni degli spazi affini sopra GF(3) e quelli proiettivi sopra GF(2) in termini di sistemi di terne di Steiner. Ci limitiamo a riportare un risultato di rilievo che riposa sulla classificazione dei gruppi semplici.

Teorema 6. ([4], [6], [7]) - *Tutti e soli di sistemi di terne di Steiner 2-volte transitivi sono gli spazi affini sopra* GF(3) *e gli spazi proiettivi sopra* GF(2).

5. Gli insiemi di permutazioni strettamente transitivi

Come è noto, un gruppo $\mathcal{G}$ di permutazioni sopra un insieme finito X si dice k-volte transitivo se prese comunque due k-ple di elementi distinti di X, $(x_1,\ldots,x_k)$, $(y_1,\ldots,y_k)$, esiste un ele-

elementi distinti di X, $(x_1,\ldots,x_k)$, $(y_1,\ldots,y_k)$, esiste un elemento $g\in G$ tale che $g(x_i)=y_i$, $i=1,2,\ldots,k$. Nel caso in cui vi sia, per ogni due k-ple, un unico tale elemento g, il gruppo $\mathcal{G}$ si chiama gruppo di permutazioni strettamente k-transitivo su X.

Lo studio dei gruppi di permutazioni k-volte strettamente transitivi, già ampiamente svolto nell'ambito della teoria dei gruppi, è stato esteso, sin dagli anni Sessanta, al caso più generale degli insiemi di permutazioni, ossia al caso in cui $\mathcal{G}$ sia un insieme (non necessariamente un gruppo) di permutazioni su X. Gli insiemi di permutazioni k-volte transitivi corrispondono per k=2 ai piani affini e per k=3 ai piani di Minkowski. Se $\mathcal{G}$ è un gruppo, la struttura geometrica corrispondente è molto particolare: per k=2 la struttura delle coordinate è un quasicorpo associativo, per k=3 un piano affine derivato è un piano di Galois o di André. Inoltre, se $k\geq 4$ e il gruppo generato da $\mathcal{G}$ non contiene il gruppo alterno A_X su X, allora l'insieme $\mathcal{G}$ è necessariamente un laterale di un opportuno sottogruppo del gruppo simmetrico S_X su X; tale sottogruppo coincide allora con uno dei seguenti gruppi: S_X, A_X, il gruppo M_{11} di Mathieu (k=4, $|X|=11$), il gruppo M_{12} di Mathieu (k=5, $|X|=12$). Quest'ultimo risultato, dovuto a L.A. Rosati, è un corollario della classificazione dei gruppi semplici finiti e la non-esistenza di piani affini di ordine 21 o 22. Gli insiemi di permutazioni strettamente 1-transitivi costituiscono una famiglia molto vasta e con caratteri di estrema generalità. È possibile tuttavia conseguire risultati significativi su particolari insiemi di permutazioni strettamente 1-transitivi. Questo è il caso degli insiemi di permutazioni involutorie strettamente 1-transitivi con identità che chiameremo brevemente PIIST.

Definizione 3. - *Un insieme di permutazioni* $(\mathcal{G},X)$ *sopra un insieme* X *si dice un insieme PIIST se*

(2) $$g(g(x))=x, \text{ per ogni } x\in X \text{ e per ogni } g\in\mathcal{G};$$

(3) $$id_X\in\mathcal{G}.$$

Osserviamo che ogni 2-gruppo abeliano elementare, riguardato nella sua rappresentazione Cayleiana, risulta essere un insieme PIIST.

Analogamente al caso dei gruppi di permutazioni, due insiemi PIIST $(X_1,\mathcal{G}_1)$ e $(X_2,\mathcal{G}_2)$ si dicono simili se vi sono due biiezioni α $(X_1\to X_2)$ e β $(\mathcal{G}_1\to \mathcal{G}_2)$ tali che $\alpha(g_1(x_1))=(\beta g_1)(\alpha(x_1))$, per ogni $x_1\in X_1$ e $g_1\in\mathcal{G}_1$. Due insiemi PIIST si dicono isomorfi se hanno lo stesso insieme sostegno e sono simili. In altri termini, si pone $(X,\mathcal{G}_1)\cong(X,\mathcal{G}_2)$ se sussite $\alpha\ {}^1\mathcal{G}_1\alpha=\mathcal{G}_2$ per una opportuna permutazione α su X. Dato un insieme PIIST $(X,\mathcal{G})$, un automorfismo è una permutazione γ su X tale che $\gamma\ {}^1\mathcal{G}\gamma=\mathcal{G}$; gli automorfismi costituiscono un gruppo di permutazioni su X che coincide ovviamente con il normalizzante $\mathcal{N}(\mathcal{G})$ di $\mathcal{G}$ in S_X. Osserviamo che se un insieme PIIST è un gruppo (e in tal caso necessariamente abeliano elementare di ordine $n=2^m$ con $|X|=n$), il gruppo degli automorfismi è isomorfo ad ASL(m,2) ed opera su X allo stesso modo di ASL(m,2) nello spazio affine di dimensione m sopra GF(2).

È facile vedere che se n=2 o n=4, gli insiemi PIIST su n oggetti sono fra loro isomorfi. Questo vale ancora per n=6, ma non per $n\geq 8$. In [11] si dà una classificazione completa degli insiemi PIIST su 8 oggetti: Vi sono esattamente sei classi di isomorfismo, ciascuna è caratterizzata dal suo gruppo di automorfismi. Ci limitiamo a riportare gli ordini dei rispettivi gruppi: 1344, 96, 64, 42, 24, 16.

6. Equivalenze fra casi particolari delle strutture geometriche precedentemente considerate

Le strutture geometriche su cui ci siamo soffermati sono collocate in aree diverse nell'ambito della Combinatoria. Fra esse esistono tuttavia significativi legami, il più notevole è l'equivalenza della nozione di colorazione minima di spigoli del grafo completo su n vertici con ciascuna delle seguenti nozioni:

$\binom{X}{2}$-*geometria con parallelismo.* Dato un insieme X, è chiaro che la sola differenza tra la $\binom{X}{2}$-geometria e il grafc completo i cui vertici sono gli elementi di X consiste nel chiamare i 2-sottoinsiemi di X col nome di spigoli. In particolare, 2-sottoinsiemi paralleli e spigoli equicolorati hanno lo stesso significato. Vi è pertanto una corrispondenza intrinseca fra le colorazioni minime di spigoli di un grafo completo e le $\binom{X}{2}$-geometrie con parallelismo sopra l'insieme X dei vertici del grafo. Si vede anche che i rispettivi gruppi di automorfismi coincidono.

3-rete involutoria con identità. Fissato un vertice *e*, ad ogni colorazione minima di spigoli resta associato un cappio commutativo $(X,\cdot)$ di esponente 2, se si introduce la seguente operazione "$\cdot$" sull'insieme sostegno X formato dai vertici:

(1) *per ogni* $a \in X$, $a \cdot a = e$;

(2) *per ogni* $a \in X - \{e\}$, $a \cdot e = a = e \cdot a$;

(3) *per ogni due* $a, b \in X - \{e\}$ *distinti,* $a \cdot b = c$ *se gli spigoli* $\{e,c\}$ *e* $\{a,b\}$ *sono equicolorati.*

Viceversa, ogni cappio commutativo $(X,\cdot)$ di esponente 2 dà luogo ad una colorazione minima di spigoli del grafo completo i cui vertici sono gli elementi di X. Poiché ogni 3-rete involutoria con identità è coordinatizzabile mediante un cappio commutativo di esponente 2, vi è una corrispondenza fra le colorazioni minime di spigoli del grafo completo su n vertici e le 3-reti involutorie con identità di ordine n. Mediante tale corrispondenza, è possibile definire un isomorfismo fra il gruppo Γ degli automorfismi della colorazione e il gruppo quoziente G/T dove G è il gruppo delle collineazioni della 3-rete che conservano le direzioni e mutano in sé una la retta e_t trasversale, e T è il sottogruppo costituito delle collineazioni che fissano ogni punto di e_t. Inoltre, Γ opera sui vertici del grafo allo stesso modo di G/T sui punti di e_t.

Insieme PIIST. Ad ogni colore di una colorazione minima di spigoli del grafo completo si può associare una permutazione involutoria sull'insieme dei vertici X nel modo seguente: Se $\{x_i, y_i\}$

sono gli (n-1)/2 spigoli di tale colore, le trasposizioni $(x_i y_i)$ sono disgiunte, quindi il loro prodotto è una permutazione involutoria su X. Gli n-1 colori danno così luogo ad altrettante permutazioni involutorie le quali con l'aggiunta dell'identità di X costituiscono un insieme PIIST. Questo ragionamento si inverte, sicché vi è una corrispondenza biunivoca fra le colorazioni minime di spigoli del grafo completo su n vertici e gli insiemi PIIST di ordine n. In quest'ordine di idee si vede anche l'isomorfismo fra i rispettivi gruppi di automorfismi.

Conviene notare infine che certe colorazioni minime di spigoli del grafo completo corrispondono *ai sistemi di terne di Steiner.* Più precisamente, se il cappio associato è totalmente simmetrico, vale a dire

(4) *per ogni* $a,b \in X$, $a\cdot(a\cdot b)=b$,

si ottiene un sistema di terne si Steiner considerando come punti i vertici distinti da e e come rette le terne $\{a,b,a\cdot b\}$ di vertici per ogni $a\neq b$ e $a\neq e\neq b$. Viceversa, ad ogni sistema di terne di Steiner si può associare un cappio commutativo totalmente simmetrico di esponente 2, quindi una particolare colorazione minima di spigoli di un grafo completo. Il gruppo degli automorfismi di una colorazione siffatta che fissano il vertice e, risulta isomorfo al gruppo degli automorfismi del corrispondente sistema di terne di Steiner.

In forza dei legami ora illustrati, i teoremi precedentemente riportati restano validi e potranno essere riformulati in ciascuna delle strutture equivalenti. Ci limitiamo ad enuniciare il Teorema 3 in termini di 3-reti e di insiemi PIIST:

Teorema 7. *Classificazione completa delle 3-reti involutorie con identità dotate di un gruppo* Γ *di automorfismi soddisfacente alle seguenti condizioni:*

(5) Γ *conserva le direzioni,*

(6) Γ *muta in sé una retta trasversale e operi sui punti di essa come un gruppo di permutazioni 2-volte transitivo.*

i) *la classe infinita delle 3-reti involutorie classiche con identità,*
ii) *tre 3-reti involutorie con identità di ordine rispettivamente 6, 12 e 28.*

Teorema 8. *Classificazione completa degli insiemi PIIST* $(\mathcal{G},X)$ *tali che il normalizzatore di* $\mathcal{G}$ *nel gruppo simmetrico su* X *sia doppiamente transitivo su* X.

i) *la classe infinita dei gruppi PIIST (ossia i 2-gruppi abeliano elementari);*
ii) *tre insiemi PIIST di ordine rispettivamente 6, 12 e 28.*

In [2] è stato compiuto il primo importante passo in direzione della classificazione di tutte le 3-reti che godano delle condizioni poste nel Teorema 7. In proposito, si è rivelato molto utile introdurre la nozione di 3-*rete irriducibile rispetto alle proprietà* (5) *e* (6). Si richiede che la 3-rete non contenga delle sotto 3-reti proprie (con eccezione al più delle 3-reti di ordine 2) dotate della stesse proprietà gruppali, nel senso che il sottogruppo Σ di Γ che muta in sé una sotto 3-rete di ordine >2 non sia doppiamente transitivo sui punti della retta trasversale situati su tale sotto 3-rete.

Teorema 9. ([2] Proposition 1.1) *Classificazione completa delle 3-reti irriducibili rispetto alle proprietà* (5) *e* (6):

i) *la classe delle 3-reti classiche coordinatizzate con gruppi di ordine primo dispari;*
ii) *tre 3-reti di ordine rispettivamente 4, 6 e 12.*

BIBLIOGRAFIA

[1] A. Barlotti and K. Strambach, The Geometry of Binary Systems, *Advances in Mathematics* **43** (1983), 1-105.

[2] A. Bonisoli, On 2-Transitive 3-Nets, *Journal of Geometry*, 41 (1991), 42-57.

[3] P.J. Cameron, *Parallelisms of Complete Desings*, London Math. Society Lecture Note Series 23, Cambridge University Press (1976).

[4] P.J. Cameron and G. Korchmáros, One-factorization of complete graphs with a doubly transitive automorphism group, *Bulletin of the London Mathematical Society, in corso di pubblicazione.*

[5] M. Hall, Steiner triple systems with a doubly transitive automorphism group, *Journal of Combinatorial Theory* **A38** (1985), 192-202.

[6] A. Hartman and A. Rosa, Cyclic one-factorizations of the complete graph, *European Journal of Combinatorial Theory* 6 (1985), 45-49.

[7] W.M. Kantor, Homogeneous designs and geometric lattices, *Journal of Combinatorial Theory* **A38** (1985), 66-74.

[8] J.D. Key - E.E. Shult, Steiner triple systems with doubly transitive automorphism group: A corollary to the classification for finite simple groups *Journal of Combinatorial Theory* **A36** (1984), 105-110.

[9] G. Korchmáros, Cyclic one-factorizations with an invariant one-factor of the complete graph, *Ars Combinatoria* 27 (1989), 133-138.

[10] G. Korchmáros and D. Saeli, Commutative loops of exponent 2 and involutorial 3-nets with identity, *Geometriae Dedicata* 28 (1988), 259-276.

[11] D. Saeli, Sugli insiemi di permutazioni involutorie con identità strettamente transitivi e i loro gruppi di automorfismi, preserving an oval of a finite projective plane, in Combinatorics'88 (Proc. International Conference on Incidence Geometries and Combinatorial Structures, Ravello 23-28 May 1988) vol. II pp. 391-411 (1991).

Lavoro eseguito nell'ambito dell'attività di ricerca del GNSAGA.

Indirizzo dell'autore:

Università degli Studi della Basilicata
Dopartimento di Matematica
via Nazario Sauro 85
85100 POTENZA

JOIN GEOMETRIES : UN APPROCCIO SINTETICO ALLA CONVESSITA'

Antonio LEONELLI
Facoltà di Scienze MM.FF.NN., Università di Viterbo

Gli insiemi convessi hanno come noto un ruolo centrale nei problemi di ottimizzazione. Essi intervengono ad esempio come insiemi soluzione di un sistema di disequazioni lineari in n variabili reali. Le caratteristiche geometriche di tali insiemi interessano, in tali applicazioni, piu' che altro per le loro conseguenze algebriche: si pensi al ruolo che i vertici di un poliedro giocano nella ricerca del massimo di un funzionale lineare. Anche per questo motivo l'approccio classico allo studio degli insiemi convessi e' stato quello di far uso delle coordinate, immergendosi in $\mathbb{R}^n$. La natura geometrica di tali problemi consente, pero', di darne delle dimostrazioni per via *sintetica*, anziche' analitica, cioe' senza far uso delle coordinate. Un modo molto generale per trattare la convessita' per via sintetica, che permette anche di semplificare alcune dimostrazioni e per di piu' fornisce modelli anche fuori della geometria euclidea, e' quello introdotto da Prenowitz, consistente nella geometria dei *Join Spaces*. Un *join space* e' un insieme munito di una iperstruttura, chiamata *prodotto join*, soddisfacente a opportuni assiomi suggeriti dall'operazione geometrica elementare consistente nell'assegnare ad ogni coppia di punti di uno spazio euclideo l'insieme dei punti del segmento che li congiunge. In questo modo, per un sottoinsieme di X l'essere convesso equivale all'essere stabile rispetto al prodotto join. I pochi assiomi stabiliti da Prenowitz permettono, come ora vedremo, di sviluppare una teoria della convessita' che fa ritrovare, senza far uso delle coordinate, i piu' importanti teoremi sugli insiemi convessi.

1. Definizioni ed esempi.

Sia X un insieme e $\cdot : X\times X \longrightarrow 2^X$ una iperoperazione su X. Se $A, B \subseteq X$, l'operazione si estende a coppie di insiemi, ponendo :

$$A\cdot B = \cup \{ a\cdot b \mid a\in A,\ b\in B \}$$

Per brevita' si omettera' il punto (come di abitudine, in Algebra) e si identifichera' ogni singleton $\{a\}$ con il suo unico elemento a.

Se l'iperoperazione e' commutativa, allora e' univocamente determinata l'*operazione inversa*, definita da :

$$(1.1) \qquad \frac{a}{b} = \{ x\in X \mid a \in b\cdot x \} .$$

Anch'essa viene estesa a coppie di insiemi allo stesso modo del prodotto.

1.1. <u>Definizione.</u>

La coppia $(X,\cdot)$ e' detta uno *spazio join* se soddisfa gli assiomi :

j1. $ab \neq \emptyset$, $\forall\ a, b \in X$.

j2. $ab = ba$, $\forall\ a, b \in X$. (proprieta' commutativa).

j3. $a(bc) = (ab)c$, $\forall\ a, b, c \in X$ (proprieta' associativa).

j4. $\forall\ a, b, c, d \in X$, $\frac{a}{b} \approx \frac{c}{d} \Longrightarrow a\cdot d \approx b\cdot c$, dove $\approx$ indica la relazione di incidenza.

j5. $\forall\ a, b \in X$, $\frac{a}{b} \neq \emptyset$.

j6. $aa = a$, $\frac{a}{a} = a \ \forall\ a \in X$, (idempotenza) .

In uno spazio join, l'iperprodotto di due elementi (o sottoinsiemi) e' detto *prodotto join* (o semplicemente *join*), mentre l'operazione inversa prende il nome di *estensione*. Il perche' di tali denominazioni sara' chiaro non appena si considereranno alcuni esempi.

Per il prodotto join e per l'estensione valgono le seguenti *proprieta' di monotonia* :

$$S \subseteq T \quad e \quad S' \subseteq T' \Longrightarrow SS' \subseteq TT' \quad e \quad \frac{S}{S'} \subseteq \frac{T}{T'} .$$

Osserviamo che, in letteratura, una iperstruttura soddisfacente j1, j2, j3 e' detta un *semi-iperguppo commutativo*. Per *iperguppo* si intende, invece, un semi-iperguppo che soddisfa anche la cosiddetta proprieta' di *riproducibilita'* :

1.2) $aX = X = Xa \quad , \forall\, a \in X$.

Si vede facilmente che (1.2) equivale a j5 e, quindi, uno spazio join e' un iperguppo commutativo.

Pertanto, l'assioma che caratterizza gli spazi join, nell'ambito degli ipergruppi e' j4 , il cui aspetto formale ricorda una ben nota regola dell'algebra elementare. Tale assioma assume un ben preciso significato geometrico non appena si considerino alcuni esempi di spazi join associati a note strutture geometriche.

1.2. <u>Esempio</u> (join vettoriale).

Si consideri uno spazio vettoriale V su un campo ordinato K (si pensi, per fissare le idee, ad $\mathbb{R}^n$ su $\mathbb{R}$). Presi due elementi a, b di V , si ponga $ab = \{ (1-\lambda)a + \lambda b \mid \lambda \in K \}$. ab e' il segmento aperto congiungente a e b , se a e b sono distinti, altrimenti si riduce al punto a . Il prodotto di tre elementi, comunque associati, e' il triangolo che li ha come vertici (eventualmente degenere in un segmento se i punti sono allineati) privato della frontiera. Pertanto, gli assiomi j1, j2, j3 sono evidentemente soddisfatti. Per verificare gli assiomi j4 e j5 , occorre vedere cos'e' l'estensione $\frac{a}{b}$ di due elementi. Dalla (1.1) segue facilmente che, se a e b sono distinti, $\frac{a}{b}$ e' la semiretta aperta con origine a , contenuta nella retta individuata da a e b e non contenente b ; con immagine suggestiva si potrebbe dire che e' l'ombra di a proiettata da b . Se, invece, a = b , allora $\frac{a}{b}$ e' ridotta al singolo punto a , pertanto l'estensione di due elementi e' comunque non vuota e j5 e' soddisfatto.

Il significato di j4 , in questo esempio, e' il seguente : se la semiretta $\frac{a}{b}$ incide la semiretta $\frac{c}{d}$ allora il segmento ad deve essere incidente al segmento bc , come in

effetti avviene.

1.3. Esempio (join *box*).

Si consideri in $\mathbb{R}^2$ l'iperprodotto definito da :

$$(a_1, a_2)\cdot(b_1, b_2) = (a_1 b_1)\times(a_2 b_2)$$

dove $a_i b_i$ $(i=1,2)$ e' il join vettoriale di a_i e b_i in $\mathbb{R}$ e $\times$ indica il prodotto cartesiano. Se i due punti sono sulla stessa retta orizzontale o verticale, il loro join e' un intervallo aperto su tale retta ; se sono in posizione obliqua, il loro join e' il rettangolo aperto coi lati paralleli agli assi che ha i due punti come vertici di una sua diagonale. Si puo' generalizzare questo esempio, prendendo in luogo di $\mathbb{R}^2$ il prodotto cartesiano di due o piu' spazi join qualsiasi ed, in particolare, $\mathbb{R}^n$, $\forall\, n \in \mathbb{N}$.

1.4. Esempio (spazio *triode*).

Sia X l'unione di tre semirette distinte del piano euclideo aventi lo stesso punto origine p , privata di p . Dati $a, b \in X$ il prodotto join ab e' cosi' definito: se $a=b$ allora $ab = a$; se $a\neq b$ ed entrambi i punti appartengono alla stessa semiretta, allora ab e' il segmento aperto su quella semiretta con estremi a e b ; se, infine, i due punti appartengono a semirette differenti, allora $ab = ap \cup pb$. X con tale iperprodotto e' uno spazio join.

1.5. Controesempio.

Consideriamo uno spazio di rette $(S, \mathcal{L})$ dove $L_{a,b} \in \mathcal{L}$ e' la retta che congiunge a con b , se $a \neq b$. Definiamo un iperprodotto al seguente modo :

$$x\cdot y = \begin{cases} \{x\} & \text{se } x = y \\ L_{x,y} & \text{se } x \neq y \end{cases}$$

L'operazione inversa, in tal caso, e' cosi' caratterizzata :
Se $a \neq b$, si ha :

$$x \in \frac{a}{b} \iff a \in b\cdot x = \begin{cases} \{b\} & \text{se } b=x \\ L_{b,x} & \text{se } b\neq x \end{cases} \quad ; \quad \text{essendo } a \neq b ,$$

non puo' essere $a \in \{b\}$, cioe' non puo' essere $b = x$; pertanto,

$x \in \frac{a}{b}$; se $x \prec b$, allora $a \in L^{x,b}$, cioè, $L^{x,b} = L^{a,b}$ e

quindi $\frac{a}{b} = L^{a,b} - \{b\}$. Se $a = b$, allora $a \in a \cdot x$ e questo succede per ogni x , cioè $\frac{a}{a} = X$. Si ha in questo caso una specie di "forma indeterminata" , in analogia alla classica $\frac{0}{0}$ in $\mathbb{R}$. Valgono gli assiomi i1, i2, i3, i5 . Non vale, però, l'assioma i4 (se una retta ha almeno tre punti); infatti, se $a \prec b$, si ha $\frac{a}{b} \lesssim \frac{b}{a}$ ma aa non ha punti in comune con bb.

1.6. Esempio (spazi proiettivi).

Per quanto appena detto, Prenowitz e Jantosciak per poter dare una caratterizzazione degli spazi proiettivi in termini di struttura join hanno dovuto introdurre un elemento neutro e e porre :

$$a \cdot b = \begin{cases} \{a,e\} & \text{, se } a = b \\ L^{a,b} - \{a,b\} & \text{, se } a \prec b \end{cases}$$

In tal modo sono soddisfatti tutti gli assiomi di uno spazio join tranne le due proprietà di idempotenza, espresse dall'assioma i6. Per questo motivo, quest'ultimo assioma e' stato trascurato da Prenowitz e Jantosciak, in alcune esposizioni della loro teoria cf.[8]), riuscendo così ad inserire tra le join geometries non solo l'importante classe degli spazi proiettivi, ma pertino quella dei gruppi abeliani.

In questa esposizione, focalizzata sulla trattazione degli insiemi convessi, abbiamo preferito conservare l'assioma i6 , perche' essenziale per una buona teoria della convessita'.

Nel seguito, sottointenderemo che gli insiemi considerati sono tutti contenuti in un fissato spazio join X .

2. Sottoinsiemi convessi e lineari.

2.1. <u>Definizione</u>.

Un insieme **A** e' detto *convesso* se e solo se

(2.1) $ab \in A \ , \ \forall \ a, b \in A \ .$

Nell'esempio 1.2., gli insiemi convessi nel senso della Def.2.1. sono esattamente gli insiemi convessi in senso usuale. Dal punto di vista algebrico, i sottoinsiemi convessi in uno spazio join sono quelli stabili rispetto al prodotto join. Si ha, ovviamente, che **A** e' convesso se e solo se $AA \subseteq A$. Perche' valga l'uguaglianza occorre che sia $A \subseteq AA$ e questo accade certamente se si postula l'idempotenza del join sugli elementi, cioe' la prima parte di j6. Si osservi che postulare l'idempotenza sui punti equivale a supporre che i punti siano convessi, come appare naturale. Come e' evidente, l'intersezione di una famiglia di convessi di uno spazio join e' ancora un insieme convesso. E' quindi possibile definire l'*involucro convesso* di un sottoinsieme S (che sara' indicato con [S]) come l'intersezione di tutti i sottoinsiemi convessi di X contenenti S . In particolare, l'involucro convesso di un punto e' il punto stesso, grazie a j6.
Non e' difficile convincersi che l'involucro convesso di un insieme S e' l'unione di tutti i prodotti join finiti di elementi di S . Seguendo la terminologia consolidata nel caso di $\mathbb{R}^n$, si dice che S *genera* **A** (*in senso convesso*) se **A** e' l'involucro convesso del sottoinsieme S , . Se S e' finito, allora **A** e' detto un *politopo*. E' facile convincersi che i politopi in senso usuale di $\mathbb{R}^n$ sono esattamente i politopi della struttura join vettoriale ; in particolare, in $\mathbb{R}^2$, sono i poligoni limitati.

Particolarmente importante e', come noto, il concetto di *punto estremo* di un insieme convesso. Esso puo' essere dato in modo molto semplice nell'ambito generale di uno spazio join, al seguente modo :

2.2. Definizione.

Se A e' un insieme convesso, un punto $a \in A$ e' detto un *estremo* di A se si ha :

$$\forall\, x, y \in A \qquad a \in xy \longrightarrow x = a = y \,.$$

In altri termini, a e' un punto estremo del convesso A se e solo se $A-\{a\}$ e' ancora convesso.

E' evidente che un punto estremo di A non e' contenuto neanche nel join di tre o piu' punti distinti di A .

Anche in questo ambito cosi' generale valgono alcuni noti teoremi sui punti estremi di convessi in $\mathbb{R}^n$.

2.3. Teorema.

$a \in A$ e' un punto estremo del convesso $A \subseteq X$ se e solo se a appartiene a ogni insieme di generatori di A .

Dimostrazione.

Sia S un insieme di generatori di A , cioe' $[S] = A$. Se a e' un punto di A , allora $a \in A = [S]$, quindi esistono $s_1, \ldots, s_n \in S$ tali che $a \in s_1 \cdot \ldots \cdot s_n$. Allora, se a e' estremo, deve essere $a = s_1 = \ldots = s_n$, cioe' $a \in S$.

Viceversa, se a non e' estremo, allora $S-\{a\}$ genera ancora A. Infatti, essendo a non estremo, esistono due punti distinti $x, y \in A$ tali che $a \in xy$. Sia $x = s_1 \cdot \ldots \cdot s_n$, $y = s_{n+1} \cdot \ldots \cdot s_m$, dove gli s_i sono punti opportuni di S , dei quali due almeno distinti, altrimenti $x = y$. Allora, $a \in s_1 \cdot \ldots \cdot s_m$. Supponiamo che gli s_i siano tutti distinti (basta raggruppare quelli uguali e usare l'idempotenza) , allora se $a = s_1$, si ha :

$a \in \frac{a}{a} \subseteq s_2 \cdot \ldots \cdot s_m$ e i fattori del prodotto sono tutti distinti da a , pertanto $a \in [S-\{a\}]$.

Poiche' $[S-\{a\}] \supseteq (\, S-\{a\}\,) \cup \{a\} = S$, ne segue $[S-\{a\}] = A$. ∎

Dal Teorema segue che i punti estremi di un politopo sono in numero finito, dato che un politopo e' finitamente generato. Essi sono detti in tal caso anche *vertici*, come usuale in $\mathbb{R}^n$.

Si da' anche una nozione di *indipendenza convessa* al seguente

modo :

2.4. Definizione.

Un insieme finito S e' detto *indipendente in senso convesso* o, brevemente, C-*indipendente*, se ogni due suoi sottoinsiemi disgiunti hanno involucri convessi disgiunti. I punti di S sono detti, allora, C-*indipendenti* tra loro.

2.5. Teorema.

Sia S un n-insieme C-dipendente di uno spazio join, allora i politopi generati dagli (n-1)-sottoinsiemi di S hanno un punto in comune.

Dimostrazione.

Essendo S C-dipendente, esistono sottoinsiemi disgiunti S_1 e S_2 di S tali che $[S_1]$ incide $[S_2]$ in almeno un punto p. Ogni politopo generato da n-1 punti di S contiene uno degli insiemi $[S_1]$, $[S_2]$ e quindi contiene p ■

2.6. Definizione.

Dato un insieme S , se esiste una massima cardinalita' finita tra quelle dei suoi sottoinsiemi C-indipendenti , essa e' detta il C-*rango* di S ed e' indicata con $r_C(S)$ ..

2.7. Teorema.

Sia L un insieme lineare di C-rango $n \geq 1$ e siano $A_1, \ldots, A_{n+1}$ sottoinsiemi convessi di L , ogni n dei quali incidenti tra loro, allora $A_1 \cap \ldots \cap A_{n+1} \neq \emptyset$.

Dimostrazione.

Sia B_j $(j=1,\ldots,n+1)$ l'intersezione degli n insiemi A_i con $i \neq j$, allora per l'ipotesi e' $B_j \neq \emptyset$, $\forall$ $j = 1,\ldots,n$. Se $p_j \in B_j$ $\forall$ $j=1,\ldots,n$, $A_i \geq \{ p_1,\ldots,p_{i-1},p_{i+1},\ldots,p_{n+1} \}$, quindi $A_i \geq [p_1,\ldots,p_{i-1},p_{i+1},\ldots,p_{n+1}]$. Poiche' il C-rango di L e' n , gli n+1 punti p_j sono C-dipendenti e quindi i politopi $[p_1,\ldots,p_{i-1},p_{i+1},\ldots,p_{n+1}]$ hanno almeno un punto in comune ■

I convessi che sono stabili anche rispetto alla estensione sono, nel caso di $\mathbb{R}^n$, esattamente i sottoinsiemi lineari, quelli cioe' ottenibili come soluzioni di sistemi di equazioni lineari. Questo fatto e' all'origine della :

2.8. Definizione.

Un sottoinsieme A di uno spazio join e' detto *lineare* se e solo se :

(2.2) $\quad ab \subseteq A \ , \quad \frac{a}{b} \subseteq A \ , \ \forall\, a, b \in A \ .$

Pertanto, gli insiemi lineari sono particolari insiemi convessi. Si dimostra, facendo uso degli assiomi j1-j5 , che nella (2.2) la prima condizione e' conseguenza della seconda e cioe' che A e' lineare se e solo se $\frac{A}{A} \subseteq A$.

L'insieme vuoto e l'intero spazio sono lineari e, grazie alla seconda parte di j6 , lo sono anche i singoli punti .

I sottoinsiemi lineari di uno spazio join sono essi stessi spazi join rispetto al prodotto indotto.

Come e' evidente, l'intersezione di una famiglia di insiemi lineari e' lineare e questo consente di definire l'*involucro lineare* di un sottoinsieme S (o *insieme lineare generato da* S) come l'intersezione $\langle S \rangle$ di tutti i sottoinsiemi lineari contenenti S . Gli elementi di S sono detti *generatori* di $\langle S \rangle$. Scriveremo, per brevita', $\langle S,T \rangle$ in luogo di $\langle S \cup T \rangle$.

L'involucro lineare di un insieme S si esprime in termini di involucro convesso al seguente modo :

$$(2.3) \qquad \langle S \rangle = \frac{[S]}{[S]}$$

ed inoltre $\langle S \rangle$ e' l'unione di tutti i sottoinsiemi del tipo $\frac{s_1 \cdot \ldots \cdot s_m}{t_1 \cdot \ldots \cdot t_n}$ (s_i , $t_j \in S$; m, n $\in \mathbb{N}$) .

Si puo' dare una definizione di lineare indipendenza al modo seguente :

2.9. Definizione.

Un insieme S e' detto linearmente indipendente (brevemente, L-indipendente) o libero se si ha : $\forall\, a \in S \;,\; a \notin \langle S-\{a\} \rangle$.

Anche in questo contesto piu' ampio, gli insiemi linearmente indipendenti hanno la seguente caratterizzazione, ben nota in Algebra Lineare :

2.10. Teorema.

Sia S un insieme finito. S e' linearmente indipendente se e solo se nessun sottoinsieme proprio di S genera $\langle S \rangle$.

Dimostrazione.

Sia S L-indipendente . Se $x \in S$ e $\langle S \rangle = \langle S-\{x\} \rangle$, allora x e' L-dipendente da S , contro l'ipotesi.

Sia S insieme minimale di generatori di $\langle S \rangle$; se S fosse L-dipendente, esisterebbe $x \in S$ tale che $x \in \langle S-\{x\} \rangle$ e allora $\langle S \rangle = \langle S-\{x\} , x \rangle = \langle S-\{x\} \rangle$, contro l'ipotesi ■

2.11. Definizione.

Dato un insieme S , se esiste una massima cardinalita' finita tra quelle dei suoi sottoinsiemi L-indipendenti, essa e' detta L-rango di S ed indicata con $r_L(S)$. ,

Si dimostra che la L-indipendenza implica la C-indipendenza e che, quindi, per ogni insieme S si ha $r_L(S) \geq r_C(S)$. Non e' vero, in generale, il viceversa.

Dalla definizione 2.11. segue che in ogni spazio join l'insieme vuoto ha L-rango zero e i punti hanno L-rango 1 . Negli spazi $\mathbb{R}^n$ con il join vettoriale, le rette hanno L-rango 2 , i piani L-rango 3 e, in generale, i sottospazi affini di dimensione n hanno L-rango n+1 . Per dare un concetto di dimensione che coincida con quello usuale nel caso del join vettoriale basta quindi chiamare dimensione di un insieme lineare N , di L-rango finito, il numero $\dim N = r_L(N) - 1$.

Sempre in analogia con l'Algebra Lineare, si da' la

seguente definizione :

2.12. Definizione.

Si chiama *base* di un insieme lineare L ogni suo sottoinsieme di generatori linearmente indipendenti.

Se L e' finitamente generato, esso ha certamente una base : un qualsiasi suo insieme minimale di generatori (in virtu' del Teorema 2.10.).

Non e' detto, pero', che due basi di uno stesso insieme lineare finitamente generato abbiano lo stesso numero di elementi. Si consideri, infatti, la struttura join *box* su $\mathbb{R}^3$. In tale spazio una qualunque coppia di punti distinti in posizione obliqua e' una base dell'intero spazio, ma anche i tre punti (1,0,0) , (0,1,0) e (0,0,1) costituiscono una base per tale spazio join. Non si puo', quindi, parlare di identita' tra dimensione di un insieme lineare e numero di elementi di una sua base, come avviene in Algebra Lineare. Per ottenere una buona teoria della dimensione, occorre aggiungere l'ulteriore assioma, detto *di scambio* :

EX. Se $b \in \langle S,a \rangle$, $b \notin \langle S \rangle$ allora $\langle S,a \rangle = \langle S,b \rangle$,
$\forall$ a, b $\in$ X , S $\subseteq$ X .

2.13. Definizione.

Uno spazio join soddisfacente EX e' detto uno *spazio (join) di scambio*.

Se, come naturale, per *retta* in uno spazio join si intende un insieme lineare generato da due punti distinti, allora in uno spazio di scambio si ha che per due punti distinti passa una e una sola retta : la retta $\langle a,b \rangle$. Si dimostra, anzi (cf.[10]), che tale proprieta' e' equivalente all'assioma di scambio. Pertanto uno spazio join e' di scambio se e solo se lo spazio geometrico avente le rette come blocchi ha la struttura di uno spazio di rette (*linear space*).

Lo spazio join *box* (esempio 1.3.) non e' di scambio. Si considerino, infatti, due punti di $\mathbb{R}^2$ aventi la stessa ordinata $k \in \mathbb{R}$. Allora l'nsieme di equazione $y = k$ e' una retta rispetto alla struttura join *box* , essendo un insieme lineare generato dai due punti dati. Essa non e' pero' l'unica retta contenente i due punti, dato che l'intero $\mathbb{R}^2$ e', rispetto alla struttura *box*, anch'esso una retta, essendo l'involucro lineare di una qualunque coppia di suoi punti che siano in posizione *obliqua* rispetto agli assi (cioe', aventi coordinate omologhe distinte).

Lo spazio *triode* (esempio 1.4.) e' uno spazio di scambio perche' l'intero spazio e' l'unica retta in esso esistente.

Dal Teorema di scambio seguono risultati analoghi a quelli classici sulle basi degli spazi vettoriali. Infatti, si ha (cf.[10]) :

2.14. Teorema.

Se L ha una base finita, allora tutte le basi di L hanno la stessa cardinalita'.

2.15. Teorema (formula di Grassmann).

Se L e M sono sottoinsiemi lineari di dimensione finita si ha :

$$\dim \langle L,M \rangle \leq \dim L + \dim M - \dim L \cap M$$

e, se L incide M , allora vale l'uguaglianza.

3. Spazi ordinati e teoremi classici sui convessi.

I tre teoremi classici di Radon, Helly e Caratheodory possono essere generalizzati all'ambito degli spazi join, se si introduce l'ulteriore *assioma dell'ordine* :

OR. $\forall$ a, b, c $\in$ X punti distinti di una retta vale una delle tre relazioni :

(3.1) $\quad a \in bc \quad , \quad b \in ac \quad , \quad c \in ab$

3.1. Definizione.

Uno spazio join soddisfacente OR e' detto uno *spazio (join) ordinato*.

E' evidente che $\mathbb{R}^n$, con il join vettoriale, e' uno spazio ordinato.

Lo spazio *triode*, invece, (Esempio 1.4.) non e' ordinato. Per rendersene conto, basta prendere i punti a, b, c uno per ciascuna delle tre semirette che costituiscono lo spazio. I tre punti appartengono alla stessa retta, perche' l'intero spazio e' una retta (nella struttura di spazio-join), ma nessuno di essi appartiene al join degli altri due.

Anche gli spazi $\mathbb{R}^n$ con il join *box* (Esempio 1.3.) non sono ordinati, come si puo' vedere direttamente o tenendo conto del fatto che ogni spazio ordinato e' anche di scambio, come mostrato dal seguente Teorema :

3.2. Teorema.

In uno spazio ordinato, se a e b sono punti distinti, $\langle a,b\rangle$ e' l'unica retta contenente a e b e si ha :

(3.2) $$\langle a,b\rangle = ab \cup \frac{a}{b} \cup \frac{b}{a} \cup a \cup b .$$

Dimostrazione.

Sia L una retta contenente a e b . Essendo L lineare, certamente $L \supseteq \langle a,b\rangle \supseteq ab \cup \frac{a}{b} \cup \frac{b}{a} \cup a \cup b$ . . Sia $x \in L$. Se $x=a$ oppure $x=b$, allora $x \in \langle a,b\rangle$. Sia $x \neq a, b$. Allora $x, a, b \in L$ e OR implica : $x \in ab$ oppure $a \in xb$ oppure $b \in xa$. In ogni caso, $x \in ab \cup \frac{a}{b} \cup \frac{b}{a} \cup a \cup b \subseteq \langle a,b\rangle$. Cosi', $L \subseteq ab \cup \frac{a}{b} \cup \frac{b}{a} \cup a \cup b \subseteq \langle a,b\rangle$, da cui l'uguaglianza dei tre insiemi ■

Il Teorema ammette la seguente generalizzazione all'involucro lineare di un n-insieme, con $n \in \mathbb{N}$ qualsiasi:

3.3. Teorema.

In uno spazio ordinato, $\langle a_1, \ldots, a_n\rangle$ e' l'unione di tutti gli insiemi esprimibili nelle seguenti forme :

(I) $a_{i_1} \cdot \ldots \cdot a_{i_r}$, $1 \le i_1 < \ldots < i_r \le n$;

(II) $\dfrac{a_{i_1} \cdot \ldots \cdot a_{i_r}}{a_{j_1} \cdot \ldots \cdot a_{j_s}}$, $1 \le i_1 < \ldots < i_r \le n$; $1 \le j_1 < \ldots < j_s \le n$;

con $i_h \neq j_k$ per $h \neq k$.

Per quanto riguarda l'involucro convesso di un n-insieme in uno spazio ordinato, vale la seguente *formula di espansione dei politopi* : se $p \in [a_1,\ldots,a_n]$, allora
$[a_1,\ldots,a_n]=[p,a_2,\ldots,a_n]\cup[a_1,p,a_3,\ldots,a_n]\cup\ldots\cup[a_1,\ldots,a_{n-1}, p]$.

3.4. Teorema.

In uno spazio ordinato, n punti sono C-indipendenti se e solo se sono L-indipendenti.

Dimostrazione.

Sappiamo che in ogni spazio join la L-indipendenza implica la C-indipendenza. Per il viceversa occorre far uso del fatto che lo spazio e' ordinato.

Siano $a_1,\ldots,a_n$ L-dipendenti, allora e', ad esempio, $a_n \in \langle a_1,\ldots,a_{n-1}\rangle$. Per il Teorema 3.3., $a_n \approx a_{i_1} \cdot \ldots \cdot a_{i_r}$, oppure $a_n \approx \dfrac{a_{i_1} \cdot \ldots \cdot a_{i_r}}{a_{j_1} \cdot \ldots \cdot a_{j_s}}$, con le stesse limitazioni del Teorema 3.3. per gli indici. Nel secondo caso, si ha : $a_n a_{j_1} \ldots a_{j_s} \approx a_{i_1} \ldots a_{i_r}$. Pertanto, in entrambi i casi, si ha una relazione di incidenza di due prodotti join fatti con sottoinsiemi disgiunti di $\{a_1, \ldots, a_n\}$ e, quindi, quest'ultimo e' C-dipendente ■

L'equivalenza tra C-indipendenza e L-indipendenza caratterizza gli spazi ordinati. Si dimostra infatti che uno spazio join e' ordinato se e solo se vale tale equivalenza.

Poiche' L-rango e C-rango sono la stessa cosa, nell'ambito degli spazi ordinati si parla semplicemente di *rango* .

3.5. Corollario.

In uno spazio ordinato, ogni n+1 punti di un insieme lineare di rango n (cioe' di dimensione n-1) sono C-dipendenti.

3.6. Teorema (di Radon).

In uno spazio ordinato X , sia S un insieme di n+1 punti di un insieme lineare di dimensione n-1 , allora esistono sottoinsiemi disgiunti S_1 , S_2 di S tali che $[S_1] \approx [S_2]$.

Dimostrazione.

E' un corollario del Corollario 3.5. ■

3.7. Teorema (di Helly).

In uno spazio ordinato X , sia L un insieme lineare di dimensione $n-1 \geq 0$ e siano $A_1,\ldots,A_{n+1}$ sottoinsiemi convessi di L , ogni n dei quali incidenti fra loro, allora tutti gli n+1 sottoinsiemi A_i hanno un punto in comune.

Dimostrazione.

E' una immediata conseguenza dei Teoremi 2.7. e 3.4. ■

3.8. Teorema.

Se S e' un n-insieme linearmente dipendente di uno spazio ordinato, allora [S] e' l'unione dei politopi generati dagli (n-1)-sottoinsiemi di S .

Dimostrazione.

Per ogni $p \in [S] = [a_1,\ldots,a_n]$, la formula di espansione dei politopi da'

$[a_1,\ldots,a_n]=[p,a_2,\ldots,a_n]\cup[a_1,p,a_3,\ldots,a_n]\cup\ldots\cup[a_1,\ldots,a_{n-1}, p]$.

Essendo S L-dipendente, quindi C-dipendente, gli addendi dell'unione al secondo membro dell'uguaglianza hanno un punto in comune. Scegliendo tale punto come p nell'uguaglianza, esso e' ridondante in ogni addendo dell'unione ■

Un politopo generato da n punti linearmente indipendenti e' detto un *simplesso*.

3.9. Corollario.

In uno spazio ordinato, ogni politopo P e' esprimibile come unione finita di simplessi i cui vertici sono in P .

Dimostrazione.

Usando termini diversi, Il Teorema 3.8. afferma che, in uno spazio ordinato, se un politopo ha n vertici e non e' un simplesso, esso e' l'unione dei politopi generati da n-1 suoi vertici. Se questi politopi sono tutti simplessi, la dimostrazione e' completata ; in caso contrario si procede per induzione ■

Il Corollario afferma, in altri termini, che ogni punto di un politopo P , in uno spazio ordinato, e' contenuto in un simplesso con vertici in P .

3.10. Teorema.

In uno spazio ordinato, sia A un insieme convesso di rango r . Sia S un insieme di C-generatori di A . Allora A e' l'unione di una famiglia di simplessi di rango non superiore ad r ciascuno dei quali ha tutti i vertici in S .

Dimostrazione.

Se $x \in [S] = A$, esiste un sottoinsieme finito F di S tale che $x \in [F]$. [F] e' un politopo di rango al piu' r ■

3.11. Teorema (di Caratheodory).

Sia L un insieme lineare di dimensione n-1 in uno spazio ordinato. Sia $S \subseteq L$. Allora $x \in [S]$ se e solo se x e' in un prodotto-join di al piu' n punti di S .

Dimostrazione.

Se x e' in un prodotto-join di n punti di S , allora certamente $x \in [S]$. Sia, viceversa, $x \in [S]$. Poiche' L ha dimensione n-1 e, quindi, rango n, il rango di [S] e' al piu' n . Allora, per il Teorema 3.10., [S] e' l'unione di una famiglia di simplessi di rango al piu' n , aventi vertici in S . x appartiene, quindi, ad un simplesso di rango al piu' n ,

generato cioe' da al piu' n punti di S ; ne segue che x appartiene ad un prodotto-join formato con alcuni di questi punti ■

Chi ha presente la formulazione classica del Teorema di Caratheodory puo' riconoscere che il Teorema 3.11. e' una sua generalizzazione semplicemente osservando che , nel caso del join vettoriale, un punto p appartiene al prodotto join di n punti se e solo se p e' esprimibile come combinazione convessa degli stessi.

Concludiamo con una elegante caratterizzazione, in termini del prodotto-join, dell'involucro convesso di un sottoinsieme di un insieme lineare di data dimensione.

3.12. Teorema.

In uno spazio ordinato, sia S un sottoinsieme dell'insieme lineare non vuoto L di dimensione n-1 . Allora $[S] = S^n$, dove il secondo membro indica il prodotto join di S con se stesso n volte (potenza n-esima nell'ipergruppo).

Dimostrazione.

Sia $x \in [S]$. Per il Teorema 3.11. esistono m punti, con $m \leq n$, di S : $a_1, \ldots, a_m$ tali che $x \in a_1 \ldots a_m$ Quest'ultimo insieme e' contenuto in S^n in virtu' dell'idempotenza del join. Pertanto, $[S] \subseteq S^n$. Il viceversa segue dal fatto che $[S] \supseteq S \cup S^2 \cup \ldots \cup S^n \cup \ldots$ ■

I risultati esposti in questo articolo possono dare solo una prima idea del lavoro svolto per decenni dal fondatore della teoria, Walter Prenowitz, e dai suoi collaboratori, in particolare James Jantosciak. Essi, con l'uso delle sole operazioni di join e di estensione hanno introdotto con successo nozioni di Topologia, collegandole a quelle di *faccia* e di *iperpiano tangente*, e hanno applicato le tecniche delle *join Geometries* anche alla teoria dei coni, alle geometrie descrittive e sferiche, argomenti per i quali si rimanda alla bibliografia.

BIBLIOGRAFIA

[1] *V.W.Bryant, R.J.Webster*, Generalizations of the theorems of Radon, Helly and Caratheodory. Monatsh.Math.73 (1969), 309-315.

[2] *B.Grünbaum*, Convex Polytopes, New York, Interscience (1967).

[3] *W.Prenowitz*, Descriptive Geometries as Multigroups, Trans. Amer. Math. Soc.59 (1946), 333-380.

[4] *W.Prenowitz*, Partially Ordered Fields and Geometries, Amer. Math. Monthly 53 (1946), 439-449.

[5] *W.Prenowitz*, Spherical Geometries and Multigroups, Canad.J.Math. 2 (1950), 100-119.

[6] *W.Prenowitz*, Projective Geometries as Multigroups, Amer.J.Math. 65 (1943), 235-256.

[7] *W.Prenowitz*, A Contemporary Approach to Classical Geometry, Amer.Math.Monthly 68 (1961),no.1 part II.

[8] *W.Prenowitz, J.Jantosciak*, Geometries and Join Spaces, J.reine und ang. Math.(1972), 100-128.

[9]*W.Prenowitz, J.Jantosciak*, Basic Concepts of Geometry. New York, Blaisdell (1965).

[10] *W.Prenowitz, J.Jantosciak*, Join Geometries, A Theory of Convex Sets and Linear Geometry, UTM , Springer-Verlag (1979).

[11] *A.Seidenberg*, Lectures on Projective Geometry. Princeton 1962.

[12] *A.Zirakzadeh*, A Model for Finite Projective Spaces with Three Points on Every Line, Amer.Math.Monthly 76 (1969), 774-778.

CLUSTERING CON MASSIMA SEPARAZIONE SU UN ALBERO

M. MARAVALLE, Facoltà di Economia e Commercio
Università degli Studi dell'Aquila
B. SIMEONE, Dip. di Statistica, Probabilità e Statistiche Applicate
Università "La Sapienza" - Roma

ABSTRACT

The present paper deals with the following problem: given a tree with n vertices and a dissimilarity d_{ij} for each pair (i,j) of vertices, partition its set of vertices into p classes such that each class induces a subtree and the split of the partition is maximized. Applications include paging of hierarchical data bases and districting of a tree-like distribution or communication network. We describe an $O(n^3)$ *greedy* algorithm for finding an optimal partition.

KEYWORDS : separation, trees, greedy algorithm.

1. INTRODUZIONE

Lo scopo fondamentale della *cluster analysis* è quello di classificare un insieme di oggetti in sottoinsiemi, o clusters, seguendo due criteri antitetici: OMOGENEITA' (oggetti dello stesso gruppo dovrebbero essere simili) e SEPARAZIONE (oggetti di gruppi differenti dovrebbero essere dissimili fra loro).

In questo articolo verrà trattato solo il secondo criterio. Si indichino gli n oggetti da classificare con i numeri 1,2,....,n, cosi' che l'insieme di oggetti sia immediatamente identificabile con l'insieme standard $V \equiv \{1,2,.....,n\}$. Si supponga che venga fornito un indice di dissimilarità d_{ij} per ogni coppia (i,j) di oggetti. Sia $\pi \equiv \{ C_1,C_2,....,C_p\}$ un'arbitaria partizione di V in p sottoinsiemi (*gruppi o clusters*), dove $1 \leq p \leq n$.

Una comune misura di separazione è il divario (split) . Il *divario* di π viene definito come il minimo indice di dissimilarità fra due oggetti appartenenti a clusters differenti :

$$s(\pi)=\min \{ d_{ij} : i \in C_h , j \in C_k , h \neq k \} . \qquad (1)$$

Come hanno dimostrato Delattre ed Hansen (1980) , il ben noto algoritmo del legame singolo dà luogo, per ciascun valore di p=1,2,.....,n, ad una partizione in p classi con massimo divario. Dal punto di vista pratico, però, non tutte le partizioni possono essere considerate come "accettabili". Per esempio se gli oggetti fossero città di una certa regione, verrebbe usualmente richiesto che ciascun gruppo sia formato da città geograficamente contigue. Se gli oggetti fossero "records" in un data base relazionale, ciascun record dovrebbe essere relazionalmente accessibile da ciascun altro record dello stesso gruppo e cosi' via.

Situazioni di questo tipo possono essere trattate in modo naturale con modelli di questo tipo : gli n oggetti da classificare vengono identificati come vertici di un grafo G , e una partizione $\pi \equiv \{ C_1,C_2,....,C_p\}$ dell'insieme V dei vertici di G viene dichiarata *ammissibile* se, per ciascun k=1,2.....,p il sottografo $G(C_k)$ indotto da C_k e' connesso (Per quanto riguarda la terminologia dei grafi ci si riferisce a Cerasoli, Eugeni e Protasi 1988). Per una rassegna sui metodi di clustering vincolato si può consultare Murtagh 1985.

Si indichi con $\Pi_p(G)$ l'insieme di tutte le partizioni ammissibili di V. Si cerca una $\overline{\pi} \in \Pi_p(G)$ tale che

$$s(\overline{\pi}) = \max [\, s(\pi) : \pi \epsilon \Pi_p(G)] \,. \qquad (2)$$

Data la partizione $\pi \epsilon \Pi_p(G)$, uno spigolo di G è chiamato *interno* (rispetto a π) se è uno spigolo di un qualsiasi sottografo $G(C_k)$; altrimenti lo spigolo è chiamato *esterno*.

In questo lavoro si considera il caso particolare in cui il grafo è un albero $T \equiv (V,E)$. Questo caso si presenta, ad esempio, allorché si abbia a che fare con un data base gerarchico, o con una rete di distribuzione o di comunicazione ad albero (gasdotto, rete locale, ecc.). Nel caso di un albero una partizione ammissibile è caratterizzata nel modo che segue: se si "tagliano" (cioè si eliminano) p-1 spigoli scelti arbitrariamente, si ottiene una foresta con p componenti connesse $C_1,C_2,....,C_p$. Allora $\pi \equiv \{ C_1,C_2,....,C_n\}$ è una partizione ammissibile di V in p gruppi. Per contro, ciascuna partizione $\pi \epsilon \Pi_p(T)$ può essere ottenuta in questo modo. Invero ci sono esattamente $p-1$ spigoli esterni rispetto a π : tagliandoli si ottiene precisamente π . Esiste pertanto una corrispondenza biunivoca tra insiemi di $p-1$ spigoli e partizioni ammissibili di V in p clusters. Se $X \subseteq E$ ed $|X| = p-1$, si indicherà con π_X la corrispondente partizione ammissibile.

Nel paragrafo 2 viene descritto un algoritmo *ghiotto* (greedy) per trovare una partizione $\pi \epsilon \Pi_p(T)$ con divario massimo. La complessità computazionale dell'algoritmo è $O(n^3)$, dove n e' il numero di vertici dell'albero T.

2. L'ALGORITMO

Questo paragrafo è dedicato alla descrizione di un algoritmo che, dato un albero $T=(V,E)$ con n vertici, una matrice di dissimilarità simmetrica $D_{nxn}= [d_{ij}]$, e un intero p , $1 \le p \le n$, permetta di calcolare una partizione $\pi \epsilon \Pi_p(T)$ avente massimo divario.
L'algoritmo consiste di tre fasi.

Nella fase 1 le $\mathcal{N} \equiv \binom{n}{2}$ coppie (i,j), $1 \le i<j \le n$, vengono ordinate in modo tale che

$$d_{i_1 j_1} \le d_{i_2 j_2} \le \ldots\ldots\ldots\ldots \le d_{i_{\mathcal{N}} j_{\mathcal{N}}}$$

Nella fase 2 a ciscuno spigolo è assegnata una etichetta (detta *rango* dello spigolo) con la seguente procedura in 5 passi:

Passo 1 : Si pone $k=1$ e $r=1$;

Passo 2 : Si genera l'insieme E_k degli spigoli del cammino (unico) su T con estremi i_k e j_k;

Passo 3 : Se tutti gli spigoli di E_k sono dotati di etichetta si va al Passo 5; altrimenti si assegna l'etichetta r a tutti gli spigoli di E_k che ne sono sprovvisti ;

Passo 4 : Si incrementa r di una unità;

Passo 5 : Se tutti gli spigoli di T sono stati etichettati, FINE ; altrimenti si incrementa k di una unità e si ritorna al Passo 2.

FINE

Nella fase 3 vengono eliminati i $p-1$ spigoli di T che hanno il rango più elevato. La partizione corrispondente risulterà avere il massimo divario. Un esempio della intera procedura viene riportato nel paragrafo 3.

Alla luce della fase 3 l'algoritmo può essere considerato *ghiotto* (greedy).

Allo scopo di implementare il Passo 2 della fase 2 è conveniente rappresentare l'albero T come un'arborescenza (*rooted tree*- viene utilizzata la terminologia di Aho,Hopcroft e Ullman 1975). Come radice dell'arborescenza viene scelto un vertice qualsivoglia di T. Ad eccezione della radice, ogni vertice i ha un unico predecessore *pred(i)*. Dunque l'arborescenza può essere rappresentata mediante la funzione pred($\bullet$) (indice dell predecessore). Usando l'indice del predecessore si può trovare l'antenato comune piú prossimo (*deepest common ancestor*) w_k di i_k e j_k . Il cammino (unico) che connette i_k a w_k è la concatenazione dei due cammini a ritroso (*backpaths*) da i_k a w_k e da j_k a w_k.

Prima di dimostrare la correttezza dell'algoritmo sarà utile introdurre alcune notazioni.

Per ogni $r=1,2,\ldots\ldots$ sia p(r) ilpiù piccolo indice k tale che esista almeno uno spigolo in E_k con rango r.

Per ogni $X \subseteq E$ sia $f(X) = s(\pi_X)$ e sia r(X) il minimo rango di uno spigolo in X.

La dimostrazione della correttezza dell'algoritmo si basa sul seguente lemma.

Lemma : Per tutti gli $X \subseteq E$ si ha:

$$f(X) = d_{i\,p(r(X))\,j\,p(r(X))} \qquad (3)$$

Dimostrazione. Sia $r=r(X)$. Per definizione di p(r) esiste almeno uno spigolo con rango r lungo il

cammino μ che collega i vertici $i_{p(r)}$ e $j_{p(r)}$; per di piu', tutti gli spigoli con rango r devono trovarsi sul cammino μ per come è definito il Passo 3. D'altra parte, f(X) è il divario della partizione ottenuto eliminando tutti gli spigoli in X. Tra questi spigoli ce ne sarà almeno uno con rango r . Poiche' questo spigolo è stato tagliato, i vertici $i_{p(r)}$ e $j_{p(r)}$ apparterrano a clusters differenti. Di conseguenza $f(X) \leq d_{i_{p(r)}j_{p(r)}}$

Supponiamo ora che $f(X) < d_{i_{p(r)}j_{p(r)}}$. Esiste un indice h tale che $f(X) = d_{i_h j_h}$.

Poichè la successione $\left\{ d_{i_k j_k} \right\}_{k=1,2.....}$ è non decrescente, si deve avere $h<p(r)$.

Per definizione di p(r), tutti gli spigoli lungo il cammino E_h devono avere rango $< r$. Ma almeno uno degli spigoli appartiene ad X, poichè i_h e j_h cadono in differenti clusters. Il rango di tale spigolo dovrebbe essere strettamente minore di $r=r(X)$ in contraddizione con quanto precedentemente detto. Riesce allora che

$$f(X) = d_{i_{p(r(X))}j_{p(r(X))}}$$

Teorema L'algoritmo è corretto e la sua complessità è dell'ordine di $O(n^3)$.

Dimostrazione Si noti dapprima che quando l'algoritmo termina tutti gli spigoli devono aver ricevuto un'etichetta. Allo scopo di trovare una partizione $\overline{\pi} \in \Pi_p(T)$ avente divario massimo, bisogna massimizzare f(X) tra tutti gli $X \subseteq E$ tali che $| X | = p - 1$. Perciò si deve massimizzare r(X) tra tutti gli $X \subseteq E$ tali che $| X | = p - 1$ (questo segue dalla (3) e dal fatto che la successione $\left\{ d_{i_{p(r)}j_{p(r)}} \right\}_{r=1,2.....}$ è non decrescente). Questo è precisamente quello che fa l'algoritmo nella fase 3. Conseguentemente l'algoritmo è corretto.

Passiamo ora ad analizzare la complessità dell'algoritmo. Nella Fase 1, l'ordinamento degli $\mathcal{N} \equiv \binom{n}{2}$ numeri d_{ij}, $1 \leq i<j \leq n$, richiede $O(n^2 \cdot \log_2 n)$ confronti. La complessità computazionale della Fase 2 è $O(n^3)$ poichè la generazione dell'insieme E_k nel Passo 2 richiede O(n) operazioni e bisigna generare al più $|\mathcal{N}|=O(n^2)$ insiemi E_k. Infine la Fase 3 richiede anch'essa O(n) confronti (si veda Aho,Hopcroft ed Ullman 1975). Quindi è possibile valutare globalmente la complessità computazionale dell'algoritmo che risulta $O(n^3)$.

3. UN ESEMPIO

Si consideri l'albero mostrato nella Fig. 1

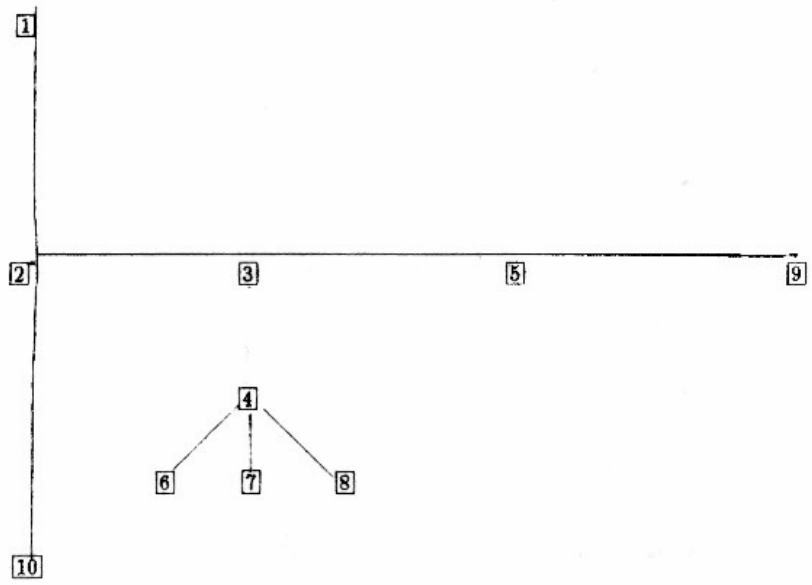


Fig.1 - Albero T.

Sia inoltre data la seguente matrice di dissimilarità $D_{jo,jo}$:

	1	2	3	4	5	6	7	8	9	10
1	0	15	23	12	45	68	90	13	24	37
2	15	0	21	39	22	77	85	4	71	45
3	23	21	0	24	69	40	25	83	27	38
4	12	39	24	0	29	34	55	86	19	28
5	45	22	69	29	0	36	8	59	47	66
6	68	77	40	34	36	0	20	50	18	54
7	90	85	25	55	8	20	0	25	20	60
8	13	4	83	86	59	50	25	0	49	23
9	24	71	27	19	47	18	20	49	0	15
10	37	45	38	28	66	54	60	23	15	0

In questo esempio si assumerà p=5.

La dissimilarità piu' piccola è $d_{2,8} = 4$. Allora tutti gli spigoli lungo il cammino con estremi 2 ed 8, cioè gli spigoli (2,3), (3,4),(4,8) avranno l'etichetta 1.

La dissimilarità successiva piu' piccola è $d_{5,7} = 8$. Gli spigoli lungo il cammino che ha come estremi 5 e 7 sono (3,5), (3,4) e (4,7). Lo spigolo (3,4) è stato già etichettato. Restano gli spigoli (3,5) e (4,7) che riceveranno l'etichetta 2.

Il successivo piu' piccolo indice di dissimilarità risulta $d_{1,4}$=12. Gli spigoli del cammino da 1 a 4 sono (1,2),(2,3) e (3,4). L'unico senza etichetta è lo spigolo (1,2) che prenderà il valore 3.

Il successivo più piccolo indice di dissimilarità risulta $d_{1,8} = 13$. Tutti gli spigoli lungo il cammino da 1 ad 8 sono etichettati.

Il successivo piu' piccolo indice di dissimilarità risulta $d_{9,10} = 15$. Gli spigoli lungo il cammino da 9 a 10 sono (5,9),(3,5),(2,3) e (2,10). Gli spigoli senza etichetta sono (5,9) e (2,10) che prenderanno l'etichetta 4.

Infine il piu' piccolo indice di dissimilarità risulta $d_{6,9} = 18$. Gli spigoli lungo il cammino da 6 a 9 sono (4,6),(3,4),(3,5) e (5,9). L'unico spigolo rimasto senza etichetta è (4,6) che prenderà il valore 5.

A questo punto l'algoritmo si interrompe poichè tutti gli spigoli sono stati etichettati.

Il numero posto accanto a ciascuno spigolo nella Fig.1 è il rango dello spigolo stesso.
I $p-1$ spigoli ($4=p-1$) di rango più elevato sono (4,6) con rango 5, (2,10) e (5,9) con rango 4, e (1,2) con rango 3.

Tagliando questi quattro spigoli si ottiene la partizione mostrata nella Fig.2.

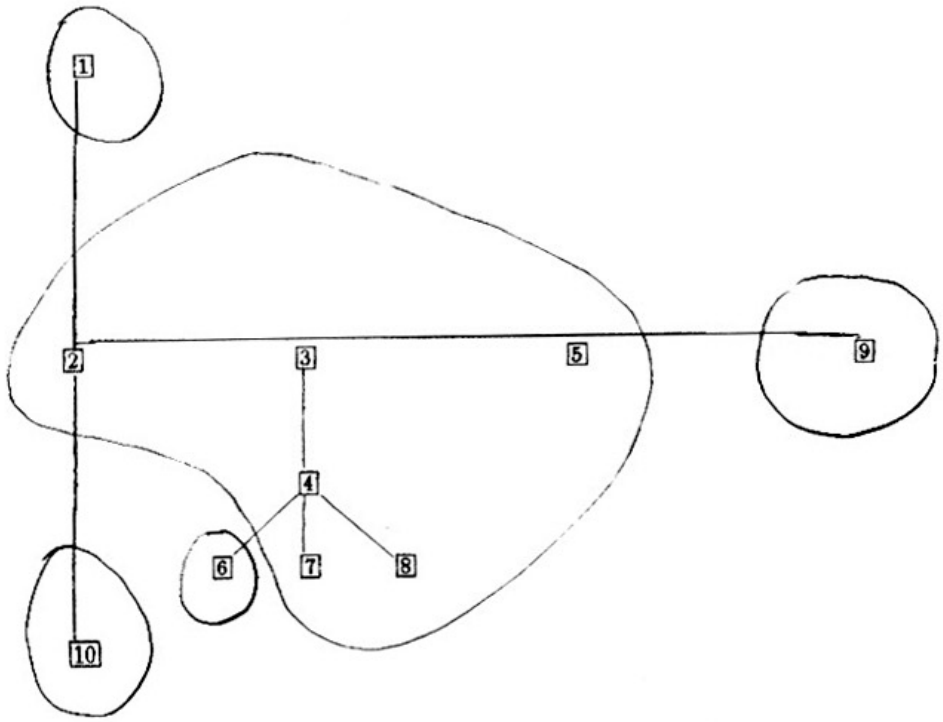


Fig.2 - Partizione in 5 gruppi .

Il *divario* di questa partizione è $d_{i_{p(3)}j_{p(3)}} = d_{1,4} = 12$, e nessuna partizione ammissibile può avere *divario* maggiore

BIBLIOGRAFIA

Aho A.V., Hopcroft J.E., Ullman J.D. (1975), *The design and analysis of computer algorithms* ,Addison Wesley, Reading.

Cerasoli M., Eugeni F. e Protasi M. (1988) *Elementi di matematica discreta*- Zanichelli - Bologna.

Delattre M., Hansen P., (1980)- *Bicriterion cluster analysis*. IEEE Trans. on Pattern Analysis and Machine Intelligence 2, n.4, 277-291 .

Murtagh, F. (1985) A Survey of Algorithms for contiguity-constrained clustering and related problems. *The Computer Journal*.28,82-88.

INTERSECTION PROBLEMS FOR STSs AND SQSs: A SHORT SURVEY (*)

Gaetano QUATTROCCHI
Dipartimento di Matematica - Università di Catania
Viale A. Doria, 6 - 95125 Catania - Italy

Abstract. We give a brief survey of the latest results on the block intersection problem for S(t,t+1,v) for t=2,3.

1. Definitions.

A t-*design* on v point is a pair (V,B) where V is a finite set of size v (called the *order* of the t-design) and B is a collection of k-subsets of V (called *blocks*) such that every t-subset of V is contained in exactly λ blocks of B. A t-design on v point is called an $S_\lambda(t,k,v)$. In the case $\lambda=1$, it is called a Steiner system S(t,k,v).

It is well-known that an S(2,3,v), or *Steiner triple system* STS(v), exists if and only if v≡1 or 3 (mod 6) and an S(3,4,v), or *Steiner quadruple system* SQS(v), exists if and only if v≡2 or 4 (mod 6) [27].

In an S(t,k,v) (V,B), $|B| = \binom{v}{t} / \binom{k}{t}$. If (V,B) is an STS(v) (SQS(v)) we will denote by $t_v = \frac{v(v-1)}{6}$ ($q_v = \frac{v(v-1)(v-2)}{24}$) the cardinality of B.

(*) Research supported by M.P.I.

A *parallel class* in an S(t,k,v) is a set of blocks that between them contain every point of V exactly once. A Steiner system is called *resolvable* if one can partition its blocks into parallel classes. Such a partition is called a *resolution*. Clearly, the number of blocks in a parallel class must equal v/k, and therefore k must divide v in any resolvable design. It is well-known that not every design with k a divisor of v is resolvable.

A resolvable S(2,3,v), called a *Kirkman triple system* KTS(v), exists if and only if v=3 mod 6 [76].

Hartman [32] proved that the necessary condition for the existence of a resolvable S(3,4,v) (i.e. v=4 or 8 (mod 12)) is also sufficient with the possible exception of twenty-three values of v.

Given an S(3,4,v) (V,B), if one chooses any point x∈P and deletes that point from the set P and from all blocks which contain it then the resulting system (V(x),B(x)), where V(x)=V-{x} and B(x)={b'=b-{x}/b∈B and x∈b}, will be an S(2,3,v-1). Such a triple system is said to be *derived* from the quadruple system and is called a *derived triple system* (DTS). It is easy to see that there exists a DTS of every possible order. However it is unknown whether or not every triple system is a DTS. See [6,68] for results on this topic.

A *partial system* S(t,k,v) is a pair (P,C) where P is a finite set of size n (called the order of the partial system) and C is a collection of k-subsets of P (called *blocks*) such that every

t-subset of P is contained in *at most* one block of C.

Two partial systems (P,C_1) and (P,C_2) are said to be *mutually balanced* if any given t-subset of P is contained in a block of C_1 if and only if it is contained in a block of C_2. Two mutually balanced partial systems are *disjoint* if they have no block in common.

A partial system (P,C) is *maximal* if there is no partial system (P,C′) with $C \subset C'$.

A *maximum partial system* is a maximal partial system with a maximum number of blocks.

A partial system with t=2 and k=3 (t=3 and k=4) is called a *partial triple system* (*partial quadruple system*).

The interested reader should consult the books [1,3,81] concerning design theory and [17,45] for more detailed results on Steiner systems.

2. The block intersection problem for STS and SQS.

Two Steiner systems (V,B_1) and (V,B_2) are said to *intersect in* k *blocks* provided $|B_1 \cap B_2|=k$. If k=0, (V,B_1) and (V,B_2) are said to be *disjoint*, and if $|B_1 \cap B_2|=1$ they are said to be *almost disjoint*. The existence of a pair of disjoint S(2,3,v)s of every order $v \geq 7$ has been shown by Doyen in [7]. Teirlinck [80] proved that if (V_1,B_1) and (V_2,B_2) are any two S(2,3,v)s, $v \geq 7$, and if V is any v-set, then there exist two disjoint S(2,3,v)s (V,B'_1), (V,B'_2) such that $(V_1,B_1) \simeq (V,B'_1)$ and $(V_2,B_2) \simeq (V,B'_2)$. Lindner [37,38] proved that there exists for every order $v \geq 3$ a pair of almost

disjoint S(2,3,v)s. In [43] the existence of large sets of mutually almost disjoint S(2,3,v)s is considered. A large set of S(2,3,v)s is a set $\{(V,B_i)/i\in I\}$ of S(2,3,v)s such that $\bigcup_{i\in I} B_i=\binom{V}{3}$, the set of all 3-subsets of V.

Etzion and Hartman have proved the existence of a pair of disjoint S(3,4,v)s for every admissible $v\geq 8$.

It is possible to consider the above results as particular cases of the following *block intersection problem for Steiner systems:* For every admissible v determine the set J(v) of all integers k such that there exists a pair of S(t,t+1,v) intersecting in k blocks.

For t=2 the set J(v) is completely determined [42]. More precisely, if $I(v)=\{0,1,\ldots,t_v-6\}\cup\{t_v-4,\ t_v=v(v-1)/6\}$, it is $J(v)=I(v)$ for every $v\equiv 1,3 \pmod 6 \geq 13$, $J(3)=\{1\}$, $J(7)=\{0,1,3,7\}$, and $J(9)=\{0,1,2,3,4,6,12\}$.

Many authors have studied the intersection problem for Steiner quadruple systems. The following results are known: Let $I(v)=\{0,1,2,\ldots,q_v-14\}\cup\left\{q_v-12,\ q_v-8, q_v=\frac{v(v-1)(v-2)}{24}\right\}$, $v\equiv 2,4 \pmod 6$. Then:

(1) $J(4)=1$, $J(2^n)=I(2^n)$ for every $n\geq 3$ [19,12,22,51].

(2) $J(10)=\{0,2,4,6,8,12,14,30\}$ [35], and

$J(5\cdot 2^n)=I(5\cdot 2^n)$ for every $n\geq 2$ [13,16,22,51].

(3) $J(14)\supseteq I(14)-\{48,50,52,57,58,60,62,63\ldots,79,83\}$ [54]; $76,77,79,83\notin J(14)$ [21]; and $J(7\cdot 2^n)=I(7\cdot 2^n)$ for every $n\geq 2$ [50,51].

(4) $J(v)=I(v)$ for every $v\equiv 4,8 \pmod{12}$ [52] (and independently

[10]).

The proof techniques of the above results use well-known constructions of S(3,4,2v). Very interesting constructions for S(3,4,v)s are known [27,29,30,31,36].

Recently a new construction (hextupling construction) for S(3,4,v)s is given in [25]. Applying the hextupling construction to the intersection problem, Colbourn and Hartman [33]: can show

$I(v)-\left\{0,\ldots,\frac{(v-2)(v-14)}{6}-1\right\}\subseteq J(v)$ for $v\equiv 2 \pmod{12}\geq 38$ and

$I(v)-\left\{0,\ldots,\frac{(v-10)}{6}-1\right\}\subseteq J(v)$ for $v\equiv 10 \pmod{12}\geq 46$.

At last in a remarkable paper , Hartman and Yehudai [33A] complete the determination of the sets of possible intersection sizes for Steiner quadruple systems of all admissible orders v except possibly v=14,16.

Let (V,B_1) and (V,B_2) be two Steiner systems such that $B_1\cap B_2=B\neq\emptyset$. If $X=\bigcup_{b\in B_1-B} b$, then (X,B_1-B) and (X,B_2-B) are two disjoint and mutually balanced (DMB) partial systems. If there does not exist a pair of DMB partial systems with k blocks, then $k\notin J(v)$.

As a consequence, many papers [11,14,15,18,22,23,24,46,47,48,49] have studied the existence of DMB partial systems.

If $J_R(v)$ denotes the set of all integers k such that there exists a pair of Kirkman triple systems intersecting in k blocks then $0,1\in J_R(v)$ for every admissible $v\geq 3$ [26,80] (see also [77]) and $I(v)-\{t_v-13,\ t_v-7,\ t_v-4\}\subseteq J_R(v)$ for $v=3^{n+1},5\cdot 3^n,7\cdot 3^n$ $(n\geq 2)$

[53].

To determine $J_R(v)$ for the other values of v is an open problem.

Since it is unknown whether or not every triple system is a DTS [68], the following question is of interest: Do the intersection problems for DTSs and for S(2,3,v)s have the same solution? The answer is yes for every admissible $v \leq 15$ [6] and for every $v \equiv 3,7 \pmod{12}$ [73]; but it is an open problem for $v \equiv 1,9 \pmod{12}$, $v \geq 21$.

Given an integer k such that $0 \leq k \leq t_v$ let us denote by D(v,k) the maximum number of STS(v)s that can be constructed on a v-set in such a way that any two of them have exactly k blocks in common, these k blocks being moreover in each of the D(v,k) systems. In [7] Doyen posed the problem of determining D(v,k). Clearly $D(v,k) \geq 2$ for every $k \in J(v)$. For k=0, D(v,0) denotes the maximum number of pairwise disjoint S(2,3,v)s. Then $D(v,0) \leq v-2$. If the equality sign holds, the v-2 Steiner triple systems form a *large set of disjoint* S(2,3,v)s. Clearly D(7,0)=2. Many papers have studied the parameter D(v,0) [77]. The best results on this topic are due to Lu Jia-Xi [55] who has shown D(v,0)=v-2 for all admissible v with the possible exception of v=141,283,506,789, 1051,2365. However Teirlinck writes in [80A] that Lu [55A] has completed these cases, so that D(v,0)=v-2 for all admissible $v \geq 9$.

In [59,61,62,63,70,71] the following values of the parameter D(v,k) are determined:

(1) If m=6 and v=9,13; or m=7 and v≥7; or m=8,9,11 and v=13,15; or m=12 and v=13; $D(v,t_v\text{-}m)=2$.

(2) If m=6 and v≥13; or m=9 and v≥9 v≠13,15; or m=10 and v≥19; or m=11 and v≥9 v≠13,15; or m=12 and v=15; or m=13 and v≥15; or m=14 and v=13,15,19; $D(v,t_v\text{-}m)=3$.

(3) If m=8 and v≥9 v≠13,15 or m=14 and v≥21, $D(v,t_v\text{-}m)=4$.

(4) $D(v,t_v\text{-}m)\leq 2\left\lfloor 3m/\left\lceil\left(1+\sqrt{1+24m}\right)/2\right\rceil\right\rfloor$; so that $D(v,t_v\text{-}t_w)=D(w,0)$ for any admissible w such that v≥2w+1. Therefore from [55,55A] it follows that $D(v,t_v\text{-}t_w)=w-2$ for w≥9.

It is possible to define the parameter D(v,k) for Steiner quadruple systems. For k=0 the following results are known: $D(2v,0)\geq v$ [39], $D(4v,0)\geq 3v$ [38], $D(2\cdot 5^m,0)\geq 5^m$ [67], $D(2n,0)\geq n$ where n=1 or 5 (mod 6) [69], $D(2^k n,0)\geq(2^k-1)n$ if k≥2 and there exists a set of 3n pairwise disjoint Steiner quadruple systems of order 4n with a certain structure [9A]. For k>0 it is proved in [20] that:

(1) $D\left(v,q_v - \frac{v^2(v-2)}{32}\right) \geq \frac{v}{2} - 1$ for every v=4,8 (mod 12).

(2) For every k∈N, k≥2, let w=min(λ∈N/λ≥4k, λ=2,4 (mod 6)). It follows that $D(2w,q_{2w}\text{-}k^2(2k-1))\geq 2k-1$ and $D(2v,q_w\text{-}k^2(2k-1)\geq 2k-1$, for v≥w, v=2,4 (mod 6).

(3) $D(v,q_v\text{-}8)=D(v,q_v\text{-}14)=D(v,q_v\text{-}15)=2$ for every $v=2^{n+2}$, $5\cdot 2^n$, $7\cdot 2^n$ and n≥2.

The block intersection problem can be generalized in the following way: Determine the sets $\bar{J}^m(v)$ ($J^m(v)$) of all integers k

such that there exists a collection of m (≥2) Steiner systems mutually intersecting in k blocks (in the same set of k blocks).

Clearly $\bar{J}^2(v)=J^2(v)=J(v)$ and $J^m(v)\subseteq\bar{J}^m(v)\subseteq J(v)$. Let $I^3(v)=\{0,1,\ldots,t_v-8\}\cup\{t_v-6,\ t_v\}$. The following results are proved in [64]: $J^3(v)=I^3(v)$ for every $v=1,3 \pmod 6$ $v\geq 19$, $J^3(7)=\{1,7\}$, $J^3(9)=\{0,1,3,4,12\}$, $J^3(13)=I^3_{13}-\{14,\ldots,18,20\}$ and $J^3(15)=I^3_{15}-\{24,\ldots,27\}$. I am not aware of any further results in this direction.

Let (V,B_1) and (V,B_2) be two $S(t,t+1,v)$ such that $|B_1\cap B_2|=k$. Clearly $(V,B_1\cup B_2)$ is an $S_2(t,t+1,v)$ having exactly k repeated blocks. Therefore the solution of the intersection problem proves the existence of $S_\lambda(t,t+1,v)$ (at least for certain values of v), with repeated blocks. See [4,61,65,72,78].

3. Steiner systems intersecting in a set with additional properties.

Let (V,B_1) and (V,B_2) be two $S(t,t+1,v)$s intersecting in exactly k blocks. One could require, as is done in [34], that $B_1\cap B_2$ contains an opportunely defined block set F and that $h=|F|+k$.

The *flower* [34] or *star* at a point x of a Steiner system is the set of all blocks containing x. The *flower intersection problem* for Steiner systems is the determination for each admissible v of the set $J^F(v)$ of all integers k such that there exists a pair of Steiner systems (V,B_1) and (V,B_2) of order v such that $|B_1\cap B_2|=|F|+k$, where F is the flower of a point $x\in V$. The following results are proved:

(1) Case t=2 (v=1,3 (mod 6)). Let $I^F(v)=\{0,1,\ldots,f_v-6\} \cup \left\{f_v-4, f_v - \frac{(v-1)(v-3)}{6}\right\}$. Then $J^F(3)=I^F(3)=\{0\}$, $J^F(7)=I^F(7)=\{0,4\}$, $J^F(9)=I^F(9)-\{1,4\}$, and $J^F(v)=I^F(v)$ for every $v\geq 13$ [34].

(2) Case t=3 (v=2,4 (mod 6)). Let $I^F(v)=\{0,1,\ldots,f_v-14\}\cup\left\{f_v-12, f_v-8, f_v= \frac{(v-1)(v-2)(v-4)}{24}\right\}$. Then $J^F(4)=\{0\}$, $J^F(8)=\{7\}$, $J^F(10)=\{0,18\}$, $I^F(16)-\{16\}\subseteq J^F(16)$ ($16\in J^F(16)$ is an open problem), and $J^F(v) = I^F(v)$ for every $v=4,8 \pmod{12}$, $v\geq 20$ [66,73].

We remark that the solution of the flower intersection problem gives a solution of the block intersection problem for other incidence structures. For example let (V,B) be a triple system and write B=F∪A where F is the flower at the point $x\in V$. Let $X=V-\{x\}$ and $G=\{\{a,b \mid \{a,b,x\}\in F\}$. Then (X,G,A) is a *group divisible design* (GDD) with group size 2 and block size 3, and (X,B-F) is a maximum partial system (MPT) of order $v=0,2 \pmod 6$.

In these terms the flower intersection problem becomes the intersection problem for GDDs with group size 2 and block size 3. Moreover we can see the same flower intersection problem as the intersection problem for MPTs of order $v=0,2 \pmod 6$.

These problems are completely solved in [2] and [74] respectively. Also the flower intersection problem for MPTs of order $v=5 \pmod 6$ is solved in [74].

Lo Faro and Marino [54A,56] determine those pairs (k,v) $v=4$ or $8 \pmod{12}$ (with some possible exception for $v=20,28$) for which

there exists a pair of Steiner quadruple systems on the same v-set, the quadruples in one system containing two particular distinct points are the same as those in the other system containing that pair of points, and the two systems have otherwise exactly k triples in common.

A slightly different intersection problem was posed by Micale [58]: Determine the set $J_0(v)$ of all integers k such that there exists a pair of S(3,4,v)s having exactly k pairwise disjoint blocks in common.

Let $I_0(v) = \left\{ 0,1,\ldots, \left\lfloor \frac{v}{4} \right\rfloor \right\}$ ($\left\lfloor \frac{v}{4} \right\rfloor$ denotes the maximum integer $\leq \frac{v}{4}$), $v \equiv 2,4 \pmod 6$. It is known [35] that $J_0(10) = \{0\}$. In [58] it is proved that $J_0(v) = -I_0(v)$ for every $v = m \cdot 2^n$ with $n \geq 2$ and $m = 4,5,7$; $J_0(4) = 1$, $J_0(8) = \{0,2\}$ and $\{0,1,2\} \subseteq J_0(14) \subseteq \{0,1,2,3\}$.

In [75] it is proved that $J_0(v) = I_0(v)$ for every $v \equiv 4,8 \pmod{12}$, $v \geq 16$.

REFERENCES

[1] Th.Beth, D.Jungnickel and H.Lenz, Design Theory, Cambridge University Press (1986).

[2] R.A.R.Butler and D.G.Hoffman,Intersections of group divisible triple systems, preprint (1989).

[3] M.Cerasoli, F.Eugeni and M.Protasi, Elementi di Matematica Discreta, Zanichelli (1988).

[4] C.J. Colbourn, R.A. Mathon, A. Rosa and N. Shalaby, The fine structure of threefold triple systems: v=1,3 (mod 6),McMaster University, Preprint (1989).

[5] A.Cruse, On embedding imcomplete symmetric latin squares, J.Combinat. Theory (A) 16 (1974) 18-22.

[6] I.Diener, E.Schmitt and H.L.de Vries, All 80 Steiner triple systems on 15 elements are derived, Discrete Math. 55 (1985) 13-19.

[7] J.Doyen, Construction of disjoint Steiner triple systems, Proc. Amer. Math. Soc. 32 (1972), 409-416.

[8] J.Doyen and M.Vandensavel, Non-isomorphic Steiner quadruple systems, Bull. Soc. Math. Belg. 23 (1971) 393-410.

[9] K.Engel, Optimalitätsaussagen über Tripelsysteme, Rortock. Math. Kolloq. 17 (1981) 17-26.

[9A] T.Etzion and A.Hartman, Towards a large set of Steiner quadruple systems, IBM Technical report September 89.

[10] H.L.Fu, Intersection problem of Steiner systems S(3,4,2v), Discrete Math. 67 (1987) 241-247.

[11] M.Gionfriddo, On some particular disjoint and mutually balanced partial quadruple systems, Ars Combinatoria 12 (1981) 123-134.

[12] M.Gionfriddo, On the set J(v) for Steiner quadruple systems of order $v=2^n$ with $n\geq 4$, Discrete Math. 44 (1983) 155-160.

[13] M.Gionfriddo, On the block intersection problem for Steiner quadruple systems, Ars Combinatoria 15 (1983) 304-314.

[14] M.Gionfriddo, Some results on partial Steiner quadruple systems, Annals of Discrete Math. 18 (1983) 401-408.

[15] M.Gionfriddo, Construction of all disjoint and mutually balanced quadruple systems with 12, 14 or 15 blocks, Rend. Sem. Mat. Brescia 17 (1984) 343-354.

[16] M.Gionfriddo, Intersections of Steiner systems S(3,4,v) with $v=5\cdot 2^n$, J. Geometry 24 (1985) 103-111.

[17] M.Gionfriddo, Sui sistemi di Steiner, Quaderno n.9, Sem. Geom. Comb. Fac. Ingegneria L'Aquila (1986).

[18] M.Gionfriddo, On disjoint partial quadruple systems having seventeen blocks, J.Inf. & Optim. Sciences, 7 (1986) 129-136.

[19] M.Gionfriddo and C.C. Lindner, Construction of Steiner quadruple systems having a prescibed number of blocks in common, Discrete Math. 34 (1981) 31-42.

[20] M.Gionfriddo, A.Lizzio and M.C.Marino, On the maximum number of SQS(v) having a prescribed PQS in common, Annals of Discrete Math. 30 (1986) 251-262.

[21] M.Gionfriddo and G.Lo Faro, On Steiner systems S(3,4,14), Ars Combinatoria 21 (1986), 179-187.

[22] M.Gionfriddo and M.Marino, On Steiner systems S(3,4,20) and S(3,4,32), Utilitas Math. 25 (1984) 331-338.

[23] M. Gionfriddo and M.C.Marino, Construction of partial $S_2(3,4,v)$ with a prescribed number of blocks in common, J. Combinat. Inf. & Syst. Sciences 11 (1986) 33-38.

[24] M.Gionfriddo, S.Milici and V.Vacirca, On disjoint partial triple systems, Rend. Circolo Mat. Palermo (II) 33 (1984) 170-184.

[25] A.Granville and A.Hartman, Subdesigns in Steiner quadruple systems, preprint.

[26] J.I.Hall and J.I. Udding, On intersesction of pairs of Steiner triple systems, Indag. Math. 39 (1977) 87-100.

[27] H.Hanani, On quadruple systems, Canad. J.Math. 12 (1960) 145-157.

[28] F.Harary, Graph Theory (Addison - Wesley, Reading, MA 1969).

[29] A.Hartman, Tripling quadruple systems, Ars Combinatoria 10 (1980) 255-309.

[30] A.Hartman, A singular direct product for quadruple systems, Lecture Notes in Math. n.884, 211-220, Springer Verlag (1981).

[31] A.Hartman, A general recursive construction for quadruple systems, J. of Comb. Theory (A) 33 (1982), 121-134.

[32] A.Hartman, The existence od resolvable Steiner quadruple systems, J. of Combin. Theory (A) 44 (1987) 182-206.

[33] A.Hartman, C.J.Colbourn, Intersection and Supports of Quadruple Systems, preprint.

[33A] A.Hartman and Z.Yehudai, Intersections of Steiner quadruple

systems, preprint.

[34] D.G.Hoffman and C.C.Lindner, The flower intersection problem for Steiner triple systems, Annals of Discrete Math. 34 (1987) 243-248.

[35] E.S. Kramer and D.M. Mesner, Intersections among Steiner systems, J.Combin. Theory (A) 16 (1974) 273-285.

[36] H.Lenz, Tripling Steiner quadruple systems, Ars Combinatoria 20 (1985) 193-202.

[37] C.C.Lindner, Construction of Steiner triple systems having exactly one triple in common, Canad. J. Math. 26 (1974) 225-232.

[38] C.C.Lindner, A simple construction of disjoint and almost disjoint triple systems, J.Combinat. Theory (A) 17 (1974) 204-209.

[39] C.C.Lindner, A note on disjoint Steiner quadruple systems, Ars Combinatoria 3 (1977) 271-276.

[40] C.C.Lindner, On the Construction of pairwise disjoint Steiner quadruple systems, Ars Combinatoria 19 (1985) 153-156.

[41] C.C.Lindner and A. Rosa, Finite embedding theorems for partial Steiner quadruple systems, Bull. Soc. Math Belg. 27 (1975) 315-323.

[42] C.C.Lindner and A.Rosa, Steiner systems having a prescribed number of triples in common, Canad. J. Math. 27 (1975) 1166-1175; Corrigendum, Canad. J. Math. 30 (1978) 896.

[43] C.C.Lindner and A.Rosa, Construction of large sets of almost disjoint Steiner triple systems, Canad. J. Math. 27 (1975)

256-260.

[44] C.C.Lindner and A.Rosa, Steiner quadruple systems-a survey, Discrete Math. 21 (1978) 147-181.

[45] C.C.Lindner and A.Rosa (editors), Topics on Steiner systems, Annals of Discrete Math. 7 (1980).

[46] A.Lizzio, On Steiner systems S(3,4,10), Rend. Sem. Fac. Sci. Univ. Cagliari, 53 (1983) 69-79.

[47] A.Lizzio, M.C.Marino and F.Milazzo, Existence of S(3,4,v), $v=5\cdot 2^n$ and $n\geq 3$, with q_v-21 and q_v-25 blocks in common, Le Matematiche 37 (1982) 36-46.

[48] A.Lizzio and S.Milici, Constructions of disjoint and mutually balanced partial Steiner triple systems, Boll. UMI (6) 2-A (1983) 183-191.

[49] A.Lizzio and S.Milici, On some pairs of partial triple systems, Rend. Ist. Matem. Trieste 17 (1985) 21-29.

[50] G.Lo Faro, On the set J(v) for Steiner quadruple systems of order $v=7\cdot 2^n$ with $n\geq 2$, Ars Combinatoria 17 (1984) 39-47.

[51] G.Lo Faro, Steiner quadruple systems having a prescribed number of quadruples in common, Discrete Math. 58 (1986) 167-174.

[52] G.Lo Faro, On Block sharing Steiner quadruple systems, Annals of Discrete Math. 30 (1986) 297-302.

[53] G.Lo Faro, Kirkman triple systems having a prescribed number of triples in common, Ars Combinatoria 24B (1987) 9-21.

[54] G.Lo Faro and L.Puccio, Sull'insieme J(14) per sistemi di quaterne di Steiner, Acc. Gioenia 17 (1984) 221-237.

[54A] G.Lo Faro and M.C.Marino, On the set $J^E(v)$ for Steiner quadruple systems of order $v \equiv 4,8 \pmod{12}$, preprint.

[55] J.X. Lu, On large sets of disjoint Steiner Triple Systems VI, J.Combin. Theory (A) 37 (1984) 189-192.

[55A] J.X.Lu, On large sets of disjoint Steiner Triple Systems VII (unfinished manuscript due to the death of the author).

[56] M.C.Marino, Sistemi di quaterne di Steiner con particolari intersezioni, preprint (1989).

[57] E.Mendelsohn and A.Rosa, One-factorizations of the complete graph - a survey, J. Graph Theory 9 (1985) 43-65.

[58] B.Micale, Pairwise disjoint intersections among Steiner quadruple systems, J. Inform. & Optim. Sciences 9 (1988) 427-436.

[59] S.Milici, On the parameter $D(v,t_v-13)$ for Steiner triple systems, Annals Discrete Math. 30 (1986) 311-330.

[60] S.Milici, On the existence of $S_3(2,3,v)$ without two-times repeated blocks, preprint (1988).

[61] S.Milici and G.Quattrocchi, Alcune condizioni necessarie per l'esistenza di tre DMB PTS con elementi di grado 2, Le Matematiche, 38 (1983) 113-132.

[62] S.Milici and G.Quattrocchi $D(v,t_v-14)$ per sistemi di terne di Steiner, Le Matematiche 40 (1985) 93-105.

[63] S.Milici and G.Quattrocchi, Some results on the maximum number of STSs such that any two of them intersect in the same block-set, J. Inform. & Optim. Sc. 7 (1986) 291-302.

[64] S.Milici and G.Quattrocchi, On the intersection problem for three Steiner triple systems, Ars Combinatoria 24A (1987)

175-194.

[65] S.Milici and G.Quattrocchi, The spectrum of 3-times repeated blocks in a $S_3(2,3,v)$, J. Combin. Theory (A) **48** (1988) 117-128.

[66] S.Milici and G.Quattrocchi, The flower intersection problem for Steiner systems S(3,4,v), $v=4\cdot 2^n$, $5\cdot 2^n$, Ars Combinatoria, to appear.

[67] K.T.Phelps, A construction of disjoint Steiner quadruple systems, Proc. 8th S-E Conf. Combinatorics Graph Theory and computing, 559-567.

[68] K.T.Phelps, A survery of derived triple systems, Annals of Discrete Math. 7 (1980) 105-114.

[69] K.T.Phelps and A.Rosa, 2-Chromatic Steiner quadruple systems, Europ. J. Combinatorics 1 (1980) 253-258.

[70] G.Quattrocchi, Sul parametro D(13,14) per sistemi di terne di Steiner, Le Matematiche **39** (1984) 61-80.

[71] G.Quattrocchi, Sul massimo numero di DMB PTS aventi 12 blocchi ed immergibili in un STS, Riv. Mat. Univ. Parma **12** (4) (1986) 41-51.

[72] G.Quattrocchi, Threefold triple systems with blocks at most two-times repeated, Combinatorics 88, to appear.

[73] G.Quattrocchi, On the intersection of two S(3,4,2v) having a same derived triple system, Discrete Math. to appear.

[74] G.Quattrocchi, Intersections among maximum partial triple systems, J.Combin.,Inf.&Syst.Sc. 14 (1989) 192-201.

[75] G.Quattrocchi, On the set $J_0(v)$, for Steiner quadruple

systems, JMCC, to appear.

[76] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's schoolgirl problem, Proc. Sympos. Pure Math. 19 (Amer. Math. Soc., Providence, RI, 1971) 187-203.

[77] A.Rosa, Intersection properties of Steiner systems, Annals of Discrete Math. 7 (1980), 115-128.

[78] A.Rosa and D.G.Hoffman, The number of repeated blocks in twofold triple systems, J.Combin. Theory (A) 41 (1986) 61-88.

[79] J.Spencer, Maximal consistent families of triples, J. Combin. Theory 5 (1968) 1-8.

[80] L.Teirlinck, On making two Steiner triple systems disjoint, J. Combin. Theory (A) 23 (1977) 349-350.

[80A] L.Teirlinck, On the use of pairwise balanced designs and closure spaces in the construction of structures of degree at least 3, preprint.

[81] W.D.Wallis, Combinatorial designs, M.Dekoker (1988).

BLOKING SETS IN FINITE PLANES AND SPACES

Tamas SZONYI
Department of Computer Science, Eotvos University
H-1088, Budapest, Muzeum krt. 6.-8., Hungary

Abstract. We survey constructive and probabilistic results about the existence of blocking sets in higher dimensional spaces, blocking sets having few collinear points, and blocking sets in inversive planes.

1. Introduction

Blocking sets of projective planes were first introduced by di Paola in the sixties, and have been studied intensively since then. Let $\Pi(q)$ be a projective plane of order q. A subset S of $\Pi(q)$ is called a *blocking set* if S meets every line but contains no line. Using the same definition the notion of blocking set was extended to affine and projective spaces (see Mazzocca–Tallini [MT], Tallini [T]). Of course one can formulate the same condition in even more general structures such as hypergraphs and, surprisingly, blocking sets in hypergraphs and hypergraphs containing no blocking sets were studied by Erdős and others already at the beginning of sixties. They called a hypergraph having property B (after Bernstein) if there is a 2-colouring of the points without monochromatic edge. (Obviously any colour class in such a 2-colouring is just a blocking set in the hypergraph.) Today the name *2-colourable* is more common (and clearer) for these hypergraphs.

The aim of this short survey paper is to collect some interesting problems about blocking sets where the more general method gives stronger results than the explicit geometric constructions. For example, we tried to collect some easy applications of the probabilistic method and Lovász' bound concerning the ratio of the fractional and integral cover, as well as various refinements of Lovász' bound.

We concentrate only on the following problems: the existence problem of blocking sets in higher dimensional spaces, the existence of a blocking set having only few points on a line, and blocking sets in inversive planes. We survey the best results obtained by geometric constructions, and also the more general results for hypergraphs which are relevant. The main references about probabilistic results are the books Erdős–Spencer [ES], Spencer [S1] and Lovász [LL2].

This paper contains almost no new results, but some illustrative proofs are included. We hope that these results about hypergraphs are also interesting for geometers and can also orientate some future research.

I would like to end this introduction with my special thanks to **László Lovász, József Beck, Endre Boros and Zoltán Füredi**. I learnt the application of probabilistic methods in combinatorics (e.g. the use of Chernoff's inequality) from them.

2. Notation and preliminaries

Throughout the paper we use standard terminology ([F]). However as this survey is written to finite geometers, I would like to recall the terminology relevant to hypergraphs and probability theory. There are two technical comments on the notation, log denotes logarithm of base 2, and the end of the proof (or the absence of a proof) is marked by ∎.

Definition 2.1. A *hypergraph* $\mathcal{H}$ is a pair $(V(\mathcal{H}), E(\mathcal{H}))$, where $E(\mathcal{H})$ is a set of certain subsets of $V(\mathcal{H})$. We call the element of $V(\mathcal{H})$ *points*, while the elements of $E(\mathcal{H})$ *edges*. (So our definition does not allow repeated edges.) The *degree* of a point $P \in E(\mathcal{H})$ is just the number of edges that contain P. A hypergraph $\mathcal{H}$ is said to be *regular* (or: d-regular) if each point has the same degree d. More generally, if $A \subseteq V(\mathcal{H})$ then $deg(A)$ is the number of edges containing A. $\mathcal{H}$ is *uniform* (or: r-uniform) if every element of $E(\mathcal{H})$ has the same cardinality r. So, using the design theory terminology, a regular uniform hypergraph is just a 1-design.

So, for example the set of lines of a projective plane of order q form a hypergraph on q^2+q+1 points, which is $q+1$-regular and $q+1$-uniform. The set of lines of a space of three dimensions is still a $q+1$-uniform hypergraph, but the degree of a point is q^2+q+1, and the number of points is q^3+q^2+q+1.

Definition 2.2. The *covering number* of the hypergraph $\mathcal{H}$ is the minimum cardinality of points that intersect every edge of $\mathcal{H}$, and is denoted by $\tau(\mathcal{H})$.

For example, for any projective plane of order q, $\tau = q+1$ as it is easy to see that less than $q+1$ points cannot block every line, and a line is a set of $q+1$ points which intersects every line. Therefore this definition is not the same as the definition of a blocking set since our pointset might contain a line (sometimes the geometers call such a set an *intersection set*).

Definition 2.3. Let $\phi : V(\mathcal{H}) \longrightarrow \mathbf{R}^+$ be a mapping. If

$$\sum_{P \in E} \phi(P) \geq 1, \quad \text{for all} \quad E \in E(\mathcal{H}),$$

then we call ϕ a *fractional covering* of $\mathcal{H}$. The value

$$\min_{\phi} \sum_{P \in V(\mathcal{H})} \phi(P) = \tau^*$$

is called the *fractional covering number* of $\mathcal{H}$, where the minimum is taken over all fractional coverings.

For example, in case of regular and uniform hypergraphs, τ^* can easily be computed. It is not difficult to see that for a d-regular hypergraph,

$$|E(\mathcal{H})|/d \leq \tau^*.$$

On the other hand, $\tau^* \leq |V(\mathcal{H})|/r$ for r-uniform hypergraphs, as the mapping in which every point has weight $1/r$ is obviously a fractional covering. Counting incident point-hyperedge pairs yields

$$|V(\mathcal{H})| \cdot d = |E(\mathcal{H})| \cdot r$$

(which is just the standard equality for 1-designs), from which we immediately get

$$\tau^* = |V(\mathcal{H})|/r = |E(\mathcal{H})|/d$$

for d-regular r-uniform hypergraphs. For more details the reader is referred to [F, p.150].

A set that intersects every edge corresponds to a $0-1$ fractional covering, so we get immediately that $\tau^* \leq \tau$. On the other hand the difference between τ and τ^* is not too big as was proved by Lovász [LL1] (see also [LL2, 13.30]).

Theorem 2.4. (Lovász) If d denotes the maximum degree of the hypergraph $\mathcal{H}$ then

$$\tau(\mathcal{H}) \leq (1 + \log d)\tau^*(\mathcal{H}).$$

∎

Actually, this theorem was probably known before Lovász' paper, but he gave a greedy algorithm which produces intersection sets. The algorithm is the following: let us take first a point having maximum degree. This intersects some edges. Delete these edges and we get a hypergraph having fewer edges. Choose a point having maximum degree in this smaller hypergraph and iterate this process. We always end up with an intersection set. For example in case of a projective plane the first two points are arbitrary but the third is on the line determined by the first two. Then we always choose points of this line, so in the end we get a line which is an intersection set indeed. So in case of projective planes Lovász' greedy cover algorithm gives the best possible value.

Let us also include a very simple graph-version of this theorem.

Theorem 2.4'. Let G be a bipartite graph with bipartition $V(G) = L \cup U$. Suppose that the degree of every point of L is at least d. Then we can find a set B of at most $(|U| \log |L|)/d$ points of U such that each point of L is joined to at least one point of $B \subset U$. ∎

For every point $x \in L$ let

$$N(x) = \{\, y \in U \,:\, xy \text{ is an edge in } G \,\}$$

be the set of neighbours of x. Let $\mathcal{H}$ be the hypergraph with $V(\mathcal{H}) = U$, $E(\mathcal{H}) = \{N(x) : x \in L\}$. Of course we keep the repeated edges (which correspond to points with $N(x) = N(y)$) only once. Obviously the mapping $\phi(u) = 1/d$ $u \in U$ is a fractional covering, so $\tau^* \leq |U|/d$. Since the maximum degree of $\mathcal{H}$ is less than $|L|$, Theorem 2.4 gives this graph-version indeed.

There are other estimates on the ratio τ/τ^*, here we recall two of them. The first one was proved by Frankl and Rödl [FR] using the proof technique called the Rödl nibble (for an informal description see [S2]). This technique was originally used to show the existence of hypergraphs which are nearly designs. The result of [FR] says that sometimes the log-factor can be omitted from Theorem 2.4. Namely let our hypergraph be d-regular for some fixed d (having m vertices and n hyperedges), and suppose that it is almost uniform, i.e. each hyperedge has asymptotically $R = R(n)$ points. (Here $R(n)$ tends to infinity.) Moreover suppose that every two hyperedges intersect in only $o(R)$ points. Then there is an intersection set consisting of $\sim n/d$ points, which is obviously best possible. More precisely (with ε's and δ's) they proved the following fundamental result.

Theorem 2.5. ([FR]) Suppose $\varepsilon > 0$ is arbitrary, $\mathcal{H}$ is a d-regular hypergraph with a fixed d, $|E(\mathcal{H})| = n$, $a > 3$ is a real number. There exists a $\delta = \delta(\varepsilon) > 0$ such that if for some D one has $(1-\delta)D < |A| < (1+\delta)D$ for all $A \in V(\mathcal{H})$ and $|A \cap B| < D/(\log n)^a$ for all $A \neq B \in V(\mathcal{H})$, then for all $n > n_0(\delta)$,

$$\tau(\mathcal{H}) \leq n(1+\varepsilon)/d \quad \text{holds.}$$

∎

Of course this seems to be much better in geometric applications than Lovász' original result, since the intersection condition of Theorem 2.5 is quite natural in case of geometric problems (at least if the number of blocks is not exponential in D). However, the price is that the point-degrees are constant, which is quite restrictive in geometric problems. The $(\log n)^a$-factor in the intersection condition was eliminated by Pippenger and Spencer [PS], who strengthened and generalized the methods of Frankl and Rödl. As the affine plane $AG(2,q)$ satisfies all the conditions of Theorem 2.8 except that $d = q+1$ is not a constant, we see that some condition on the order of magnitude of d (compared to n) is indeed necessary.

The second refinement on Lovász' bound on τ/τ^* uses the notion of VC-dimension. The *Vapnik–Chervonenkis dimension* (or *VC-dimension*, for short) of a hypergraph $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ is the maximum size of a subset $A \subset V(\mathcal{H})$ with the property that every $B \subseteq A$ is a "trace" of an element of $E(\mathcal{H})$ on A, i.e. there exists an $E_B \in E(\mathcal{H})$ with $E_B \cap A = B$. For example if we take the lines of a projective space $PG(n,q)$ $(n \geq 2)$, then A itself is a trace, i.e. A is contained in a line r. Obviously, $|A| \leq 2$ as the

other lines intersect r in at most 1 point. Therefore the VC-dimension of this design is 2. Similarly, the VC-dimension of the design of hyperplanes of $PG(n,q)$ is n (and the points of a good A form a basis in a hyperplane).

A remarkable fact is that the number of edges in a hypergraph of small VC-dimension is polynomial in $|V(\mathcal{H})|$. Because of its importance, the theorem was rediscovered several times (by Sauer, Perles, Shelah, Vapnik–Chervonenkis). For the sake of simplicity we just refer to a recent survey [FP], where some proofs and all the references can be found.

Theorem 2.6. For any hypergraph with $|V(\mathcal{H})| = n$ and VC-dimension d,

$$|E(\mathcal{H})| \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{d}.$$

∎

Now let us see some theorems which relate the VC-dimension of $\mathcal{H}$ with the ratio $\tau^*(\mathcal{H})/\tau(\mathcal{H})$. Again we only state the first and then the best result, other results and applications can be found in [FP].

Theorem 2.7. (Haussler, Welzl [HW]) Let $\mathcal{H}$ be a hypergraph with VC-dimension d all of whose edges are of size at most $\varepsilon|V(\mathcal{H})|$ for some fixed $0 < \varepsilon < 1$. Then

$$\tau(\mathcal{H}) \leq \left[\frac{8d}{\varepsilon}\log\frac{8d}{\varepsilon}\right].$$

Theorem 2.8. (Komlós, Pach and Woeginger [KPW]) For any hypergraph $\mathcal{H}$ with VC-dimension d we have

$$\tau(\mathcal{H}) \leq d\tau^*(\mathcal{H})(\log\tau^*(\mathcal{H}) + 2\log\log\tau^*(\mathcal{H}) + 3),$$

provided that $\tau^*(\mathcal{H})$ is sufficiently large.

We do not mention here the other important parameters of a hypergraph and their connections (including many other results in the spirit of Theorems 2.4–2.8), but the reader is referred to the excellent survey [F] by Füredi.

From probability theory only basic facts are used (see Rényi [Ré]). The probability of the event A will be denoted by $Prob(A)$, the expectation and variance of a random variable ξ will be denoted by $E(\xi)$ and $D(\xi)$ respectively. The following lemma of Chernoff, which is an improvement on Chebytcheff's famous inequality for a particular class of random variables, plays a crucial role in various probabilistic results.

Theorem 2.9. (Chernoff) Let ξ_i $(i = 1, \dots n)$ be independent (discrete) random variables with $Prob(\xi_i = 1) = p$, $Prob(\xi_i = 0) = 1 - p$ $(i = 1, \dots n)$. Let $\eta = \xi_1 + \dots + \xi_n$ (which is a random variable having binomial distribution). Then

$$Prob\Big(|\eta - E(\eta)| \geq x \cdot D(\eta)\Big) \leq \exp\Big(\frac{-x^2}{2}\Big)$$

for every $x \geq 0$.

Actually, the proof of 2.9 is quite easy, one applies Chebytcheff's inequality for the random variable $\zeta = \exp(\xi_1 + \dots + \xi_n)$. (Of course $\exp(x)$ denotes e^x.)

3. Blocking sets in higher dimensional spaces

The fundamental question about blocking sets in higher dimensions is that of existence. Roughly speaking the results tell us that there are no blocking sets if the dimension is large compared to the order, but there do exist blocking sets if the dimension is small enough. For example if $q = 2$ then there are no blocking sets in the plane, i.e. in $PG(2, 2)$, but for $q > 2$ there are blocking sets in any projective plane of order q.

Using a geometric version of Ramsey's theorem due to Graham, Leeb, and Rothschild [GLR], Mazzocca and Tallini [MT] proved the following non-existence result.

Theorem 3.1. There exist $h_a = h_a(q)$ (and $h_p = h_p(q)$) such that there are no blocking sets in $AG(h, q)$ (or in $PG(h, q)$) for $h \geq h_a$ (or $h \geq h_p$).

(See also 14.23. of [LL2].) Mazzocca and Tallini also studied the relation between h_a and h_p. Unfortunately, these h's are very big compared to q.

On the other hand, when the dimension is small blocking sets exist. First let us summarize the known constructions, then we will see that the probabilistic argument gives a much better bound for the dimension h_p. As we mentioned earlier, in $PG(2, q)$ blocking sets exist, when $q > 2$. In $PG(3, q)$, Rajola [R] showed that blocking sets exist for $q > 4$. For $q = 2, 3$ there are no blocking sets in $PG(3, q)$. The case $q = 4$ is still open, partial results can be found in Metsch [M]. Using a recursive construction, Beutelspacher and Eugeni [BE] showed that for $q \geq 2^h$ there do exist blocking sets in $AG(h, q)$. In $PG(3, q)$ Blokhuis and Fisher (private communication) gave the following example. Consider $AG(3, q)$ as $GF(q^3)$ and let S be the set of squares in $GF(q^3)$. Then S, regarded as a point set of $AG(3, q)$ is a blocking set for $q \geq 5$. (So this is another proof of Rajola's result.) Hirschfeld and Szőnyi [HSz] generalized this example and improved the bound $2^h \leq q$ to $h^2 - 1 \leq q$.

On the other hand, using probabilistic arguments much more is known for more general structures.

Theorem 3.2. (Erdős–Hajnal, [EH]) Let $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ be an n-uniform hypergraph with $|E(\mathcal{H})| \leq 2^{n-1}$. Then there is a subset $B \subset V(\mathcal{H})$ which intersects every edge, but contains no edge; in other words $\mathcal{H}$ is 2-colourable.

Sketch of the proof. List the edges, let $E(\mathcal{H}) = \{E_1, \ldots, E_m\}$. Colour the points with two colours at random, independently of each other and with probability $1/2$. If A_i denotes the event that E_i is monochromatic, then it is easy to see that $Prob(A_i) = 2^{-n+1}$. So the probability of having a monochromatic edge is

$$Prob(A_1 + \ldots A_m) < \sum_{i=1}^{m} Prob(A_i) = \frac{m}{2^{n-1}} \leq 1.$$

For the details we refer to [ES, p.19], [S1, p. 8] or [LL, 13.41.].

Using the geometric language this is a theorem about the existence of blocking sets. Although this result is quite good it can be improved. In general, Beck [Be] proved that every hypergraph on n points and with m edges has a blocking set if $m < 2^{n-1}n^{1/3-\epsilon}$. Beck's proof uses a very clever refinement of the probabilistic method, the "deletion method". Roughly speaking, one takes a random configuration and proves that it is bad in only a few places. Then these bad spots can be deleted and after this "small modification" the object has the desired property. More details on applications of the deletion method can be found in [S1, Lecture 2]. On the other hand this result is basically sharp as there are hypergraphs with m edges having no blocking sets, where $m = cn^2 \cdot 2^n$ (see [LL2, 13.42.]).

For the particular case when the edges of the hypergraph are either disjoint or have exactly one point in common, Erdős and Lovász [EL] proved the following theorem.

Theorem 3.3. (Erdős–Lovász) Let $\mathcal{H}$ be an r-uniform hypergraph having n points and m edges and suppose that two edges have at most one point in common. Then
(a) If $n \leq 2^{r-4}$, then there is a blocking set in $\mathcal{H}$ (in other words, $\mathcal{H}$ is 2-colorable).
(b) If $m \leq 4^{r-4}/r^3$, then there is a blocking set in $\mathcal{H}$.

(See also [LL2, 13.44].) This theorem is essentially sharp, as Erdős and Lovász [EL] proved that there do exist r-uniform hypergraphs with $m < cr^4 4^r$ hyperedges, which are not 2-colourable and any two edges intersect in at most 1 point.

The proof of (b) is based on the same idea as the proof of Theorem 3.2. The cornerstone is the following probabilistic lemma, which is now called "Lovász' local lemma".

Theorem 3.4. (Lovász' local lemma) Let G be a (finite) graph with maximum degree d and vertices $v_1, \ldots, v_n$. Let us associate an event A_i with v_i $(i = 1, \ldots, n)$ and suppose that A_i is independent of the set

$$\{A_j \ : \ (v_i, v_j) \notin E(G)\}.$$

Also suppose $Prob(A_i) \leq 1/(4d)$. Then

$$Prob(\bar{A}_1 \cdot \ldots \cdot \bar{A}_n) > 0.$$

∎

(In the proof of Theorem 3.3 the vertices of G are the hyperedges of $\mathcal{H}$ and A_i is the event that the hyperedge is monochromatic.)

Theorem 3.4 is a sieve method improving on the usual counting sieve if there is much independence among the events $A_1, \ldots, A_n$. The common feature of Lovász' local lemma and the deletion method is that they help us in finding (or at least in proving the existence of) rare points, i.e. it works even when the set of good points is very small. We saw another similar method, the Rödl nibble, in Section 2. An asymmetric version and various applications of the local lemma can be found in [S1, Lecture 8].

Let us see what Theorem 3.3 gives us for projective spaces. In $PG(n,q)$ we have roughly q^n points, q^{2n-2} lines. So as long as $q^{2n-2} \leq 4^{q-4}/q^3$ blocking sets exist. Taking logarithms of base 2 on both sides we get

$$(2n-2)\log q \leq 2(q-4) - 3\log q,$$

so for $n \leq \dfrac{q-4}{\log q} - \dfrac{1}{2}$ there do exist blocking sets in $PG(n,q)$, and this bound is much better than the bounds obtained from the various constructions.

Let us make some "philosophical" comments on the fact that the construction is much worse than the probabilistic method. The reason is that the constructions want to produce "regular" blocking sets. For example, the blocking sets in [HSz] have the property that every line intersects them in roughly $q/2$ points, at least when the dimension is small compared to q. (Other constructions produce blocking sets which are not regular in this sense but e.g. they contain q points on a line etc.) This procedure can be simulated using random selection. If one chooses each point independently with probability $1/2$, then what we get is a blocking set having roughly $q/2$ points on each line. This selection works if the dimension $n \leq \sqrt{q}/2$, which can be seen using Chernoff's inequality. So the essential difference is that in the proof of Theorem 3.2 every subset was taken into account, i.e. they had a chance of being chosen, while the constructions choose among "regular" or extremely irregular subsets.

4. Blocking sets with small line intersections

In this chapter we are dealing with blocking sets whose intersection with each line contains a limited number of points. We say that a projective plane π has property $B(c)$ if there is a blocking set S whose intersection with each line of π contains less than c points. For a blocking set B, $c(B)$ denotes the maximum number of collinear points of B. Before the results let us mention that the obvious examples of blocking

sets (Baer-subplanes, unitals, and blocking sets contained in the union of three lines) are very bad regarding $c(B)$, i.e. $c(B) = \sqrt{q} + 1$ or $c(B) \geq (q+1)/2$ in these cases.

Erdős has asked whether there exists an absolute constant c such that every projective plane has property $B(c)$. Instead of a constant c, Erdős, Silverman, and Stein [ESS] proved the following result.

Theorem 4.1. (Erdős–Silverman–Stein) Every projective plane of order n has property $B(c \log n)$, if n is sufficiently large and $c > 2e$.

Sketch of the proof. (I learnt the idea of this proof from Zoltán Füredi. We will only concentrate on showing the existence of a blocking set B with $c(B) \leq c \log n$, but not on the best value of c.) Let us denote the number of points (as usual) by v, the number of blocks by b, and the size of a line by k. Let us select the points independently at random with probability $p = (C \log k)/k$. Then first of all the expected number of points will be $p \cdot v \sim (C \cdot v \log k)/k$. Then list all the lines (blocks) $L_1, \ldots, L_b$ and concentrate on one line L_1, say. Let the points of L_1 be $P_1, \ldots, P_k$. Because of the independent selection to each point P_i $(i = 1, \ldots, k)$ there corresponds a random $0-1$-variable ξ_i which takes the value 1 iff the point is selected, and these independent random variables satisfy the conditions of Theorem 2.9 (Chernoff's inequality) with $p = (C \log k)/k$. Then the value of $\eta_1 = \xi_1 + \ldots + \xi_k$ is just the number of points selected on the line L_1. As η_1 has binomial distribution its expected value $E(\eta_1) = kp = C \log k$, its variance is $D(\eta_1) = \sqrt{kp(1-p)} \leq \sqrt{C \log k}$. So Chernoff's inequality gives (for $x \geq 0$) that

$$Prob\Big(|\eta_1 - E(\eta_1)| \geq x \cdot D(\eta_1)\Big) \leq \exp\Big(\frac{-x^2}{2}\Big).$$

We are going to apply this for $x = c^* \sqrt{\log k}$, where the new constant $c^* < C$. This is good a choice because then $xD(\eta_1)$ is less than $E(\eta_1)$. Therefore we will certainly bound using the previous inequality the probability that no points or more than $2C \log k$ points of L_1 are selected. The actual bound is at most

$$\exp((-x^2)/2) = \exp(((-c^{*2})/2) \log k) = k^{((-c^{*2})/2)}.$$

One can do this similarly for each line L_i. If B denotes the set of chosen points then $|B \cap L_i| = \eta_i$ and therefore

$$Prob\Big(|B \cap L_i| < (C - c^*) \log k, \quad \text{or} \quad |B \cap L_i| > C^* \log k\Big) \leq k^{((-c^{*2})/2)}.$$

Using the obvious bound for the probability of the sum of events we get immediately that

$$Prob\Big(\exists i : |B \cap L_i| < (C - c^*) \log k, \text{ or } |B \cap L_i| > C + c^*) \log k\Big) \leq b k^{((-c^{*2})/2)}.$$

In our case $b < k^2$ so if $c^* > 2$ then this probability is strictly less than 1, which means that there exists a B for which

$$(C-2) \log k \leq |B \cap L_i| \leq (C+2) \log k, \quad \forall i = 1, \ldots, b.$$

The only thing we needed was $C > c^*$, i.e. for $C > 4$ one can choose a c^* for which this proof works. ∎

First of all remark that in [ESS] the value of the constant is better. Our second remark is that the same computation can be done if we find a constant r so that $k^r > b$, which shows that blocking sets with small line intersections do exist in more general block designs. (Actually from this proof one gets $4r \log k$ as an upper bound for the number of points lying on one block.) Finally let us remark that Abbott and Liu [AL] improved this result for the special case of Galois planes $PG(2,q)$, q is an odd prime power, and proved that the condition on c may be replaced by $c > 2/\log 2$.

On the other hand, Ughi [U] proved that in $PG(2,q)$, q odd, from the union of c conics one can never get a blocking set, where c is a constant and q is large enough compared to c. Let us remark here that Ughi also proved that there are $c \log q$ suitably chosen conics that form a blocking sets. This is clear from Theorem 2.4' if we apply it for the following bipartite graph: points of the "upper" level U are the irreducible conics, points of the "lower" level L are the lines of $PG(2,q)$, a conic and a line being adjacent exactly when they are not disjoint. Here there are roughly q^2 points of the lower and q^5 of the upper level, while the degree of points of L is at least roughly $(q^5 - q^3)/2$ (roughly half of the conics intersect a given line in two points over $GF(q)$). Now Theorem 2.4' shows that one can choose at most $2\log(q^2+q+1)$ conics such that they intersect each line. (Actually Ughi's proof was based on a counting argument and was essentially the same as this.)

For particular classes of planes there are constructions showing the existence of blocking sets having at most 4 points on a line.

Theorem 4.2. (Bruen–Fisher, [BF]) $PG(2,3^r)$ has property $B(5)$. ∎

This result was generalized by Boros [Bo], who proved that in the plane $PG(2,p^r)$, $p > 2$ prime, there is a blocking set S of size $2p^r$ having not more than $p+1$ points on a line. In other words, the plane $PG(2,p^r)$, $p > 2$ has property $B(p+2)$. Let us remark that Theorem 4.2 is better than Theorem 4.1 only if r is very big compared to p.

Theorem 4.3. (Illés–Szőnyi–Wettl, [ISzW]) The plane $PG(2,2^r)$ has property $B(6)$ if r is even, and $B(7)$ if r is odd. ∎

In the case r is even the proof is similar to the constructions of Bruen–Fisher and Boros, while in the case r odd we proved that the union of three suitably chosen conics form a blocking set. This also shows that in the result of Ughi the condition q odd was necessary indeed.

5. Blocking sets in inversive planes

Of course blocking sets can be studied in various geometric structures. In case of projective and affine planes we know something about blocking sets. A natural next step would be to study blocking sets in an inversive plane as these are one-point extensions of affine planes. As usual we will concentrate on classical (i.e. Miquelian) inversive planes. Let $M(q)$ be such an inversive plane of order q and B be a blocking set (or better: intersection set) in $M(q)$. As $M(q)$ is a 3-design on q^2+1 points, it is a $q+1$-uniform, q^2+q-regular hypergraph, so by the remark after DEfinition 2.3 we get that $\tau^* = (q^2+1)/(q+1)$, which also yields a lower bound for the value of τ. This general bound on τ can be improved.

Take a point $P \notin B$ and form the point-residual of $M(q)$ with respect to P. This is the desarguesian affine plane $AG(2,q)$, and B has to block all the lines of $AG(2,q)$. Then by a result of Jamison [J] and Brouwer–Schrijver [BSch] one has $|B| \geq 2q-1$. Let us remark that the same lower bound is true for arbitrary inversive planes.

Theorem 5.1. (Bruen–Rothschild [BR]) If S is a blocking set in any inversive plane of order q, then $|S| \geq 2q$ for $q \geq 9$, and $|S| \geq 2q-1$ for $q \neq 3$. ∎

So we have a lower bound on $|B|$ but essentially no constructions are known. From Lovász' theorem (Theorem 2.4) one gets that there are intersection sets with cardinality $|B| \leq Cq\log q$.

Another approach would be to use random selection. In the previous section we formulated the proof of Theorem 4.1 in such a way that there is a blocking set intersecting every block in at most $c\log q$ points, if there is a fixed r for which $b < k^r$. In our case $k = q+1$, $b = (q^2+1)(q+1)q$, so this condition is satisfied with $r = 3$. This again gives the existence of a blocking set of size $Kq\log q$.

Finally, one can also show the existence of an intersection set consisting of $C\log q$ circles by using Theorem 2.4.' for the following graph: the point of the lower level are circles, the points of the upper level are again circles and we join two circles if they have non-empty intersection. What is the degree of a point in this graph? There are $\binom{q+1}{2}\cdot q$ circles intersecting the given circle in two points and other $(q+1)q$ circles intersecting it in one points. The total number of circles is $\binom{q^2+1}{3}/\binom{q+1}{3} = (q^2+1)q$. Therefore the minimum degree is roughly half the number of points, and Theorem 2.4' gives the existence of roughly $3\log q$ circles which intersect every other circle. So this is again an intersection set having about $Cq\log q$ points. It might be interesting to note that in this last construction we really need $c\log q$ circles as the following theorem shows.

Theorem 5.2. Suppose that the union of k circles of an inversive plane intersects every circle. Then $k > c\log q$, for a suitable constant $c > 0$.

Sketch of the proof. List the circles $C_1, \ldots C_k$ of our intersection set. Consider a point P which does not belong to the union of these circles. Then in particular we have to block all the circles through P. These are exactly the lines of a (classical) affine plane,

the point-residual of the inversive plane. Using coordinates on this affine plane let the equation of C_i be $(x-a_i)^2 - k(y-b_i)^2 = r_i$, where k is a fixed non-square of $GF(q)$. Take a point $A(a,b)$ of the affine plane and consider the lines through A. Such a line does not intersect C_i if and only if a certain quadratic polynomial $f_i(m)$ is a non-square, where m denotes the slope of the line. Without computation we can guess what these polynomials are. Namely the the zeroes of $f_i(m)$ correspond to the slopes of the tangents of C_i passing through A, so $f_i(m) = k_i(m-m_{i,1})(m-m_{i,2})$, where $m_{i,1}$ and $m_{i,2}$ denote the slopes of the tangents (which belong to $GF(q^2)$). (We can exclude the possibility that there is a vertical tangent through A; as C_i has two vertical tangents so if A does not lie on any of these $2k$ lines, then the polynomials $f_i(m)$ are quadratic polynomials indeed.) Also we can suppose that $A \notin C_i$ $(i = 1,\dots,k)$, so these polynomials have no multiple roots. We are going to apply Lemma 1 of [Sz]. In order to do this, it is sufficient that no two polynomials $f_i(m)$ have a common root. But a common root of f_i and f_j corresponds to a common tangent to C_i and C_j passing through A. There are at most 4 common tangents to each pair (i,j) so this condition excludes at most $(k-1)k/2$ tangents, which cover at most $qk(k-1)/2$ points of the plane. So the total number of excluded points is $k(q+1) + 2kq + qk(k-1)/2$. This is much less than the number of points, so we can find a point A, such that for the polynomials $f_i(m)$ $(i = 1,\dots,k)$ all conditions of Lemma 1 of [Sz] are satisfied. Therefore we find at least

$$\frac{q}{2^k} - k(\sqrt{q}+1)$$

values of m with $f_i(m)$ being a non-square for every $i = 1,\dots,k$. Geometrically this means that there is a line through A which does not intersect $C = \cup_i C_i$, that is C is not an intersection set, if $k \le (1/2 - \varepsilon)\log q$. ∎

Remark. Actually the same proof shows that Ughi's result (see [U]) is essentially sharp in the sense that if we want to block all the lines of a projective plane by the union of some conics then we really need about $c\log q$ conics. As we already remarked in the previous section, this theorem does not extend to planes of even order (cf. the remarks after Theorem 4.3).

6. References

[AL] Abbott, H.L. and Liu, A.: Property of B(s) and projective planes, *Ars Combinatoria* **20** (1985), 217–220.

[Be] Beck, J.: On 3-chromatic hypergraphs, *Discrete Math.* **24** (1978), 127–137.

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

[BeE] Beutelspacher, A. and Eugeni, F.: On blocking sets in projective and affine spaces of large order, *Rend. di Mat. (Roma)* **6**, (1986), 587–595.

[Bo] Boros, E.: $PG(2,p^s)$, $p>2$ has property B(p+2), *Ars Combinatoria* **25** (1988), 111–114.

[BSch] Brouwer, A.E. and Schrijver, A.: The blocking number of an affine space, *J. Comb. Theory (A)* **24** (1978), 251–253.

[B1] Bruen, A.A.: Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[B2] Bruen, A.A.: Blocking sets in finite projective planes, *SIAM. J. Appl. Math.* **21** (1971), 380–392.

[BF] Bruen, A. and Fisher, J.C.: Blocking sets and complete arcs, *Pacific J. Math.* **53** (1974), 73–84.

[BR] Bruen, A. and Rothschild, B.L.: Lower bounds on blocking sets, *Pacific J. Math.* **118** (1985), 303–311.

[BT] Bruen, A.A. and Thas, J.A.: Blocking sets, *Geom. Ded.* **6**, (1977), 193–203.

[D] Di Paola, J.W.: The shape of minimum blocking sets in small planes, *Ars Combinatoria* **20-B** (1985), 15–26.

[EH] Erdős, P. and Hajnal, A.: On a property of families of sets, *Acta Math. Hung.* **12** (1961), 87–123.

[EL] Erdős, P. and Lovász, L.: Problems and results on 3-chromatic hypergraphs and some related qusetions, in: *Infinite and Finite Sets*, Coll. Math. Soc. J. Bolyai **10**, Bolyai–North-Holland (1974), 609–627.

[ESS] Erdős, P., Silverman, R. and Stein, A.: Intersection properties of families of sets of nearly the same size, *Ars Comb.* **15** (1983), 247–259.

[ES] Erdős, P. and Spencer, J.: *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974.

[FR] Frankl, P. and Rödl, V.: Near Perfect Covers in Graphs and Hypergraphs, *Eur. J. Comb.* **6** (1985), 317–326.

[F] Füredi, Z.: Matchings and Covers in Hypergraphs, *Graphs and Combin.* **4** (1988), 115–206.

[FP] Füredi, Z. and Pach, J.: Traces of finite sets, extremal problems and geometric applications, in: *Extremal problems in combinatorics, Visegrád, Hungary 1991*, to appear.

[GLR] Graham, R.L., Leeb, K. and Rothschild, B.L.: Ramsey's theorem for a class of categories, *Adv. in Math.* **8** (1972), 417–433.

[HW] Haussler, D. and Welzl, E.: ε-nets and simple range queries, *Discr. Comput. Geom.* **2** (1987), 127–151.

[H] Hirschfeld, J.W.P.: *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1976.

[HSz] Hirschfeld, J.W.P. and Szőnyi, T.: Constructions of large minimal blocking sets and (k,n)-arcs in Galois-planes, *Europ. J. Comb.* **12** (1991), 499–511.

[ISzW] Illés, T., Szőnyi, T. and Wettl, F.: Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97–107.

[IM] Innamorati, S. and Maturo, A.: On irreducible blocking sets in projective planes, *Ratio Math.* **2** (1991), 151–155.

[J] Jamison, R.E.: Covering finite fields by cosets of subspaces, *J. Comb. Theory (A)* **22** (1977), 253–266.

[KPW] Komlós, J., Pach, J. and Woeginger, G.: Almost tight bounds for ε-nets, *Discr. Comput. Geometry* **7** (1992), to appear.

[LL1] Lovász, L.: On the ratio of optimal integral and fractional covers, *Discrete Math.* **13** (1975), 383–390.

[LL2] Lovász, L.: *Combinatorial problems and exercises*, Akadémiai Kiadó, Budapest, 1979.

[MT] Mazzocca, F. and Tallini, G.: On the non-existence of blocking sets in $PG(n,q)$ and $AG(n,q)$ for all large enough n, *Simon Stevin* **1** (1985), 43–50.

[M] Metsch, K.: Blocking sets in $PG(3,4)$?, *Mitt. Math. Sem. Giessen* **201** (1991), 119–131.

[PS] Pippenger, N. and Spencer, J.: Asymptotic Behavior of the Chromatic Index for Hypergraphs, *J. Comb. Theory A* **51** (1989), 24–42.

[R] Rajola, S.: A blocking set in $PG(3,q)$, $q \geq 5$, *Annals of Discrete Math.* **37** (1988), 391–394.

[Rö] Rödl, V.: Proof of the Erdős–Hanani conjecture, *European. J. of Comb.* **6** (1985), 69–78.

[Ré] Rényi, A.: *Probability Theory*, Akadémiai Kiadó, Budapest, 1970.

[S1] Spencer, J.: *Ten lectures on the probabilistic method*, SIAM Publication, 1987.

[S2] Spencer, J.: The probabilistic method, Chapter for *The Handbook of Combinatorics* (ed. by: R.L. Graham, M. Grötschel, L. Lovász), North-Holland, to appear.

[Sz] Szőnyi, T.: Note on the existence of large minimal blocking sets in PG(2,q), *Combinatorica* **12** (1992), to appear.

[T] Tallini, G.: Blocking sets in projective and affine spaces, *Ann. Discr. Math.* **37** (1988),433–450.

[U] Ughi, E.: On (k,n)-blocking sets which can be obtained as a union of conics, *Geom. Ded.* **26** (1988), 241–245.

A GEOMETRIC INTERPRETATION OF THE FIGUEROA PLANES

Rita VINCENTI
Dipartimento di Matematica - Università degli Studi - Perugia

In [3] Grundhöfer gives a synthetic construction of a Figueroa plane of order q^3 starting from $PG(2,q^3)$ which is independent on the algebraic point of view of the action of a Singer group, as Figueroa [1] used in the original construction.

In this paper, we analyze at first the action of the collineation α of order h of $PG(2,q^h)$, $q=p^r$, p,h primes, $p,h>2$, fixing $PG(2,q)$ pointwise. If $h=5,7$ we prove that α admits three kinds of point and line orbits, as in the case $h=3$. The group of the collineations of $PG(2,q^h)$ which fix $PG(2,q)$, acts trasitively on the points and on the lines of $\mathcal{P}_3$ and $\mathcal{L}_3$ respectively, precisely when $h=3$.

In Sec.3, we analyze the Grundhöfer construction by a geometric point of view and we obtain that a Figueroa plane of order q^3 can be represented starting from $PG(2,q^3)$ leaving invariant the incidence relation and replacing the subset $\mathcal{L}_3$ of the lines by a new subset $\mathcal{L}_3^*$, any new line $r^* \in \mathcal{L}_3^*$ consisting of a subset of the old line r, union a subset of an algebraic curve defined by r.

1. PRELIMINARY RESULTS.

Let $F=GF(q^h)$ be a Galois field , $q=p^r$, p,h primes , $p,h>2$.
The field F can be regarded as an extension $K(w)$ of $K=GF(q)$, where w is a root of a polynomial $f(x)\in K[X]$, deg $f=h$, f irreducible over K.
Let $\tilde{\alpha} : x \mapsto x^q$ be the automorphism of F fixing the subfield K elementwise. Then $o\tilde{\alpha} = h = |\langle \tilde{\alpha} \rangle|$.
Denote by $\Pi = PG(2,q^h)$ the desarguesian plane over F and by $\Pi_o = PG(2,q)$ the subplane of Π coordinatized by K with respect to a chosen coordinate system for Π so that a point P of Π has homogeneous coordinates (x,y,z), $x,y,z\in F$, and a fixed line l_∞ has equation $z=0$; denote by α the collineation of Π defined by $(x,y,z)\alpha = (x\tilde{\alpha}, y\tilde{\alpha}, z\tilde{\alpha})$.
Express $\Pi=(\mathcal{P},\mathcal{L}, I)$ as an incidence structure such that $\Pi_o=(\mathcal{P}_o,\mathcal{L}_o, I_o)$ where $\mathcal{P}_o\subset\mathcal{P}$, $\mathcal{L}_o\subset\mathcal{L}$, $I_o = I/\mathcal{P}_o\times\mathcal{L}_o$, $I=\in$.
Let $\theta s = \{s, s\alpha, s\alpha^2, \ldots, s\alpha^{h-1}\}$ be the orbit of the element $s\in\mathcal{P}\cup\mathcal{L}$ under the action of the group $\langle\alpha\rangle$.

LEMMA 1.1- i) the group $\langle\alpha\rangle$ is planar and fixes precisely the points of $\mathcal{P}_o$ (the lines of $\mathcal{L}_o$);
ii) $\forall s\in\mathcal{P}\cup\mathcal{L}$, $|\theta s| = h$ if and only if $s\notin\mathcal{P}_o\cup\mathcal{L}_o$;
iii) $r\supset\theta P$ for some $P\in r$ if and only if $r\in\mathcal{L}_o$ ($P\in\bigcap\theta r$ for some $r\ni P$ if and only if $P\in\mathcal{P}_o$).

Proof:

A point $P=(x,y,z)$ is in $\mathcal{P}_o$ if and only if
$X=xz^{-1}$, $Y=yz^{-1}$ are in K when $z\neq 0$ or
$X=xy^{-1}$ or $Y=x^{-1}y$ are in K when $z=0$.
A point P is fixed by α if and only if
$(x\tilde{\alpha}, y\tilde{\alpha}, z\tilde{\alpha}) = (\lambda x, \lambda y, \lambda z)$; equivalently, $X\tilde{\alpha}=X$ and $Y\tilde{\alpha}=Y$, that is, if and only if X,Y are elements of K. Hence α fixes precisely the points of Π_o. The dual argument holds for the lines.

A point P of is fixed by $\alpha^i\in\langle\alpha\rangle$ where $i=1,\ldots,h$ if and only if $X\tilde{\alpha}^i = X$, $Y\tilde{\alpha}^i = Y$; the elements X,Y must belong to a field M such that $K\leq M<F$ $|M:F| = s$, s/h . Therefore $s=1$ and P is a point of Π_o . The dual arguments hold for the lines.

Let $s \in \mathcal{P} \cup \mathcal{L}$; then $|\theta s| \leq h$. We have $|\theta s| < h$ if and only if there exist i, j such that $1 \leq i < j < h-1$ and $s\alpha^i = s\alpha^j$, or, $s\alpha^{j-i} = s$, that is (by i)) , if and only if $s \in \mathcal{P}_0 \cup \mathcal{L}_0$. Furthermore,

$\theta P \subset r$ if and only if $r = P\ P\alpha = P\alpha P\alpha^2 = r$; that is, if and only if r is a fixed line under $\langle \alpha \rangle$; $P \in \bigcap \theta r$ if and only if P is a point fixed by $\langle \alpha \rangle$.

REMARK 1- From iii) it follows that $h/p^{rh}-p^r$.

LEMMA 1.2- Three points of θP are collinear if and only if there exist i,j such that $1 \leq i < j < h$ and $P, P\alpha^i, P\alpha^j$ are collinear.

Proof:

Let $P\alpha^k, P\alpha^m, P\alpha^n$ be three points of θP, $k<m<n$. Then $P\alpha^k$ $P\alpha^m, P\alpha^n \in r$ where $r \in \mathcal{L}$ if and only if $P, P\alpha^i, P\alpha^j \in r^{h-k}$ where $i=m+n-k$, $j=n+h-k$.

REMARK 2- If $P \in r$ and $P \neq P$, then $r = P\ P\alpha P\alpha^2$ is equivalent to $r \in \mathcal{L}_0$.

Assume that an orbit θP contains three collinear points. From Lemma 1.2 it follows that this is equivalent to assuming that there exists a line $r \in \mathcal{L}$ such that $r = P\ P\alpha^i P\alpha^j$ where $1 \leq i < j < h$.

LEMMA 1.3- If a) $j=2i$ or $j+i=h$ or

b) $i=h-2s$ and $j=h-s$ for some s , then r is a line of $\mathcal{L}_0$.

Proof:

The length of the orbit θr is less than h if and only if there exists s , $1 \leq s < h$ such that $r\alpha^s = P\alpha^s\ P\alpha^{i+s}\ P\alpha^{j+s} = r = P\ P\alpha^i\ P\alpha^j$.

If $j=2i$, then $r\alpha^i = P\alpha^i\ P\alpha^{2i}\ P\alpha^{j+i}$ and

$$r \cap r\alpha^i \supset \left\{ P^i, P^{2i} = P^j \right\} ;$$

if $j+i=h$, then $r\alpha^i = P\alpha^i\ P\alpha^{2i}\ P\alpha^{j+i}$ and $r \cap r\alpha^i \supset \left\{ P\alpha^i, P\alpha^{j+i} = P\alpha^h = P \right\}$; in both cases , $r = r\alpha^i$.

If $i=h-2s$ and $j=h-s$, then $r\alpha^s = P\alpha^s\ P\alpha^{i+s}\ P\alpha^{j+s} = P\alpha^s\ P\alpha^{h-s}\ P\alpha^h = P\alpha^s\ P\alpha^{h-s}\ P$ and since $r = P\ P\alpha^i\ P\alpha^j = P\ P\alpha^{h-2s}\ P\alpha^{h-s}$, we have $r \cap r\alpha^s \supset \left\{ P, P\alpha^{h-s} \right\}$; hence $r = r\alpha^s$.

LEMMA 1.3'- The dual of Lemma 1.3.

PROPOSITION 1.1- If $h=5$, then the point-orbits θP are of the following three types: 1)trivial; 2) incident a line ; 3) a 5-arc;

the line-orbits θr are of the following three types: 1') trivial; 2') confluent in a point; 3') a 5-gon.

Proof:

Let P be a point of Π ; if $P \in \mathscr{P}_o$ then θP is trivial ; if $P \in r$ where $r \in \mathscr{L}_o$ and $P \notin \mathscr{P}_o$, then $\theta P \subset r$.

Let P be a point of $\mathscr{P} - \mathscr{P}_o$ such that $P \notin r \ \forall r \in \mathscr{L}_o$; such a point does exist since Π_o is not a Baer subplane. The orbit θP contains three collinear points if and only if there exist i,j $1 \leq i < j < 5$ such that P, $P\alpha^i$, $P\alpha^j$ are collinear (see Lemma 1.2).

Let $r = P\ P\alpha^i\ P\alpha^j$; by Lemma 1.3,a), we obtain $r = r\alpha^i \ \forall (i,j) \in \{(1,2), (2,4), (1,4), (2,3)\}$, and by b), $r = r\alpha^s$, $s=1,2$ $\forall (i,j) \in \{(3,4),(1,3)\}$.

This means that for all the possibilities of the choices i,j $1 \leq i < j < 5$ the line r is a line of $\mathscr{L}_o$, $\theta P \subset r$, a contradiction. Hence there exist no exponents i,j such that P , $P\alpha^i$, $P\alpha^j \in \theta P$ are collinear. Equivalently, the orbit θP is a 5-arc. The dual arguments hold for the line orbits.

Let θP be a point-orbit such that $P \notin \mathscr{P}_o$ and $\theta P \not\subset r \ \forall r \in \mathscr{L}$. Assume that θP contains three collinear points, that is, there exists a line $r = P\ P\alpha^i\ P\alpha^j$ $1 \leq i < j < h$ and $|\theta r| \neq 1$.

Let $\mathscr{S} = (\theta P, \theta r, I_{/\theta P \times \theta r})$ be the incidence structure consisting of the points of the orbits of P and the lines of the orbit of r .

LEMMA 1.4- $\mathscr{S}$ is an incidence structure with parameters $b=v=h$, $r,k \geq 3$.

Proof:

Any line $m \in \theta r$ contains at least three distinct points , namely $P\alpha^s$, $P\alpha^{i+s}$, $P\alpha^{j+s}$ as $m = r\alpha^s$ for some s . For any point $Q \in \theta P$, $Q = P\alpha^t$ for some t ; hence Q is incident with the following three distinct lines: $r\alpha^t$, $r\alpha^s$ where $s=t-i$, $r\alpha^{s'}$ where $s'=t-j$ as image of P under α^t; of $P\alpha^i$ under α^s ; of $P\alpha^j$ under $\alpha^{s'}$, respectively.

PROPOSITION 1.2- If $h=7$ then the point-orbits θP are of the following three

types : 1) trivial ; 2) incident a line ; 3) a 7-arc ;

the line-orbits θr are of the following three types : 1')trivial ;

2') confluent in a point ; 3') a 7-gon.

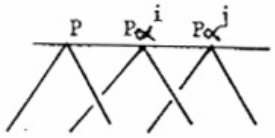
Proof:

Let $P \in \mathcal{P}$; if $P \in \mathcal{P}_o$ then θP is trivial ; if $P \notin \mathcal{P}_o$ and $P \in r$, where $r \in \mathcal{L}_o$, then $\theta P \subset r$.

Let P be a point of $\mathcal{P} - \mathcal{P}_o$ such that $P \notin r \ \forall r \in \mathcal{L}_o$. Such a point does exist since Π_o is not a Baer subplane.

Assume that r contains three collinear points, that is, assume that there exists $r = P\, P\alpha^i\, P\alpha^j$, $1 \leq i < j < 7$.

From Lemma 1.4 it follows that each of the points P, $P\alpha^i$, $P\alpha^j$ is incident with two distinct lines of θr other than r ; that is, the lines through P $P\alpha^i$, $P\alpha^j$ are all the lines of θr since h=7. Hence $r \cap r\alpha^s \in \{P,\ P\alpha^i,\ P\alpha^j\}$ $\forall$ s=1,...,6. We prove that, $\forall$ t,t'=1,...,6,



$r\alpha^t \cap r\alpha^{t'} \in \theta P$:

$R = r\alpha^t \cap r\alpha^{t'}$ is equivalent to $R\alpha^{-t} = r \cap r\alpha^{t'-t}$.

From the above we obtain $R\alpha^{-t} \in \{P\ ,\ P\alpha^i\ ,\ P\alpha^j\}$ or $R \in \{P\alpha^t\ ,\ P\alpha^{i+t}\ ,\ P\alpha^{j+t}\}$. Thus any two lines of θr are incident with a point of θP.

Given P and $P\alpha^t \in \theta P$ set $\bar{r} = P\, P\alpha^t$. Since P is incident with three lines $r_1, r_2, r_3 \in \theta r$ and each line of θr contains three points of θP, on these three lines through P lie all points of θP . Hence $\bar{r} = r_i$ for some i=1,2,3 . As $r' = P\alpha^s\, P\alpha^{s'}$ is equivalent to $r'\alpha^{-s} = P\, P\alpha^{s'-s}$, we conclude that any two of the points of θP are incident with a line of θr and $\mathcal{S} = (\theta P, \theta r, I_{/\theta P \times \theta r})$ is the projective plane PG(2,2) and $2/q = p^r$, a contradiction.

Hence the orbit θP cannot have three collinear points.

2. FURTHER PROPERTIES OF THE COLLINEATION α

As in Sec. 1 , let $\Pi = PG(2,q^h)$, $\Pi_o = PG(2,q)$ $\Pi_o < \Pi$.
Represent $\Pi = (\mathcal{P}, \mathcal{L}, I)$. Let α be the collineation of Π induced by the automorphism of F fixing elementwise K . Thus α fixes elementwise the points and the lines of Π_o . We can partition the sets $\mathcal{P}$ and $\mathcal{L}$ as follows :

$$\mathcal{P}_1 = \{ P \in \mathcal{P} \ / \ P\alpha = P \} \quad ; \quad \mathcal{L}_1 = \{ r \in \mathcal{L} \ / \ r\alpha = r \}$$

$$\mathcal{P}_2 = \{ P \in \mathcal{P} \ / \ \exists r \in \mathcal{L}_1 \text{ s.t. } P \ I \ r \} \ ; \ \mathcal{L}_2 = \{ r \in \mathcal{L} \ / \ \exists P \in \mathcal{P}_1 \text{ s.t. } r \ I \ P \}$$

$$\mathcal{P}_3 = \mathcal{P} - (\mathcal{P}_1 \cup \mathcal{P}_2) \quad ; \quad \mathcal{L}_3 = \mathcal{L} - (\mathcal{L}_1 \cup \mathcal{L}_2) \ .$$

It is clear that $\Pi_o = (\mathcal{P}_1, \mathcal{L}_1, I)$.
Let A_o be the group of the automorphisms of Π which map Π_o onto itself.

LEMMA 2.1- For any $\sigma \in A_o$ it is :

i) $\sigma' = \alpha \sigma \alpha^{-1} \in A_o$ and σ' works as σ on Π_o ;

ii) $\sigma'(\mathcal{P}_i) = \mathcal{P}_i$ and $\sigma'(\mathcal{L}_i) = \mathcal{L}_i$ $\forall$ i=1,2,3.

Proof:

i) : for any $P \in \mathcal{P}_1$ set $P' = P\sigma$; it is $P' \in \mathcal{P}_1$ and $P\sigma' = P\,\alpha\sigma\alpha^{-1} = P\,\sigma\alpha^{-1} = P'\,\alpha^{-1} = P' = P\sigma$ .The dual arguments hold for the lines of $\mathcal{L}_1$.

ii) : by i), it follows $\sigma'(\mathcal{P}_1) = \mathcal{P}_1$ and $\sigma'(\mathcal{L}_1) = \mathcal{L}_1$.
For any point $P \in \mathcal{P}_2$ there exists exactly one line $r \in \mathcal{L}_1$ such that $P \ I \ r$ and $P\sigma'$ is a point of $r\sigma' = r'$ where $r' \in \mathcal{L}_1$, by i) , that is $P\sigma'$ is a point of $\mathcal{P}_2$. The dual arguments holds for the lines of $\mathcal{L}_2$. Thus $\sigma'(\mathcal{P}_2) = \mathcal{P}_2$ and $\sigma'(\mathcal{L}_2) = \mathcal{L}_2$. Therefore it must be also $\sigma'(\mathcal{P}_3) = \mathcal{P}_3$ and $\sigma'(\mathcal{L}_3) = \mathcal{L}_3$.

Let $C_o \subset A_o$ be the subset of the central collineations of Π having the center and the axis in Π_o . It is known that $\langle C_o \rangle = A_o$ (see [3]).

LEMMA 2.2- For any $\sigma \in C_o$ it is $\alpha\sigma = \sigma\alpha$.

Proof:

Let $\sigma \in C_o$; let $C \in \mathcal{P}_1$ and $a \in \mathcal{L}_1$ be the center and

the axis of σ, respectively, and let $P\sigma = Q$ where $P, Q \in \mathfrak{P}_1$. Take $\sigma' = \alpha\sigma\alpha^{-1}$. By Lemma 2.1 we have that $\sigma' \in A_o$, $C\sigma' = C$, $\forall A \in \mathfrak{P}_1$ s.t. $A \mathrm{I} a$ then $A\sigma' = A$ and $\forall r \in \mathfrak{L}_1$ s.t. $C \mathrm{I} r$ then $r\sigma' = r$; moreover $P\sigma' = Q$. For any line r such that $C \mathrm{I} r$, if $r \notin \mathfrak{L}_1$, then $r \in \mathfrak{L}_2$, $r\alpha \in \mathfrak{L}_2$ and $C \mathrm{I} r\alpha$; thus $r\sigma' = r\alpha\sigma\alpha^{-1} = r\alpha\alpha^{-1} = r$.

For any point $R \in \mathfrak{P}_1$ such that $R \mathrm{I} a$, if $R \notin \mathfrak{P}_1$ then $R \in \mathfrak{P}_2$ and $R\alpha \in \mathfrak{P}_2$, $R\alpha \mathrm{I} a$; thus $R\sigma' = R\alpha\sigma\alpha^{-1} = R\alpha\alpha^{-1} = R$.

Therefore σ' is a central collineation of Π having center C, axis a and $P\sigma' = Q$; this means that $\sigma' = \sigma$; equivalently $\alpha\sigma = \sigma\alpha$

Set $\theta s = \{s, s\alpha, \ldots, s\alpha^{h-1}\}$ $\forall s \in \mathfrak{P} \cup \mathfrak{L}$.

PROPOSITION 2.1- For any $\sigma \in A_o$ it is $\alpha\sigma = \sigma\alpha$ and $(\theta s)\sigma = \theta(s\sigma)$.

Proof:

As $\langle C_o \rangle = A_o$, for any $\sigma \in A_o$, $\sigma = \sigma_1\sigma_2 \ldots\sigma_r$ where $\sigma_i \in C_o$; it is

$$\alpha\sigma\alpha^{-1} = \alpha\sigma_1 \ldots \sigma_r\alpha^{-1} = \alpha\sigma_1\alpha^{-1}\alpha\sigma_2\alpha^{-1} \ldots \alpha\sigma_r\alpha^{-1} = \sigma_1\sigma_2 \ldots\sigma_r = \sigma,$$

$$(\theta s)\sigma = \{s, s\alpha, \ldots, s\alpha^{h-1}\}\sigma = \{s, s\alpha\sigma, \ldots, s\alpha^{h-1}\sigma\} =$$
$$\{s, (s\sigma)\alpha, \ldots, (s\sigma)\alpha^{h-1}\} = \theta(s\sigma).$$

PROPOSITION 2.2- For any point $P \in \mathfrak{P}_1$ there are $q^3 - q^2 - 1$ non-identical collineations of C_o of center P: $q^2 - 1$ of them are elations, $q^3 - 2q^2$ of them are homologies.

Proof:

The non-identical elations of C_o of center P are as many are the lines of Π_o incident P, that is, $q+1$, times $q-1$, where $q-1$ is the number of the points of $\ell \cap \mathfrak{P}_1$, any $\ell \in \mathfrak{L}_1$ $\ell \ni P$, which are different from P and from a chosen and fixed point of $\ell \cap \mathfrak{P}_1$.

The non identical homologies of C_o of center P are as many are the lines r of $\mathcal{L}_1$ incident P, that is, q^2, times $q-2$ which is the number of the points $\mathcal{P}_1$ of any line ℓ of π_o through P, different from P, from $\ell \cap r$ and from a fixed point of $\ell \cap \mathcal{P}_1$.

Choose and fix any point $P \in \mathcal{P}_3$; set

$$P A_o = \{ P\sigma \ / \ \forall \sigma \in A_o \} \quad , \quad r A_o = \{ r\sigma \ / \ \forall \sigma \in A_o \}.$$

THEOREM 2.1- $P A_o = \mathcal{P}_3$, $r A_o = \mathcal{L}_3$ precisely when $h=3$.

Proof:

Let $\mathcal{P}' = \{ P' = P\sigma \ / \ \forall \sigma \in A_o \}$; it is $\mathcal{P}' \subseteq \mathcal{P}_3$. For any $\sigma \in A_o$ it is $\sigma = \sigma_1 \sigma_2$ where $\sigma_1, \sigma_2 \in C_o$.

Consider the subgroup $\Sigma_1 < C_o$ of the collineations of π_o of center $P_1 \in \mathcal{P}_1$. It is $P\Sigma_1 \subseteq P P_1 \cap \mathcal{P}_3$ where $P P_1 \in \mathcal{L}_2$ and $|P \Sigma_1| = q^3 - q^2$.

For any $P_2 \in \mathcal{P}_1$, $P_2 \neq P_1$ and $\Sigma_2 < C_o$, consider the point $P\sigma_1\sigma_2 \quad \forall \sigma_i \in \Sigma_i$, $i=1,2$.

It is $P\sigma_1\sigma_2 \in P_2 P\sigma_1$; if $P\sigma_1\sigma_2 \in P_1 P P\sigma_1$, then the lines $P_2 P\sigma_1$ and $P_1 P P\sigma_1$ would have two different points $P\sigma_1$ and $P\sigma_1\sigma_2$ in common, thus $P_1 = P_2$, a contradiction. If there would be points Q in the set $P P_1 \cap \mathcal{P}_3 - P\Sigma_1$, there would exists no $\sigma \in A_o$ such that $P\sigma = Q$. Hence, $P\Sigma_1 = P P_1 \cap \mathcal{P}_3$ and $h=3$ follows.

3. THE GEOMETRIC INTERPRETATION

Let $F=GF(q^3)$ be a Galois field, $q=p^r$, p prime $p>2$, and let $K=GF(q)$ be the subfield of F of order q.

Let $\overline{\Pi}=PG(2,q^3)$ be the Galois plane of order q^3 and $\overline{\Pi}_o=PG(2,q)$, $\overline{\Pi}_o < \overline{\Pi}$.

Let α be the collineation of $\overline{\Pi}$ induced by the automorphism of F fixing pointwise the subfield K. The order of α is 3 and α fixes precisely the points and the lines of $\overline{\Pi}_o$ (see Sec. 1).

We can represent $\overline{\Pi}$ as an incidence structure $\overline{\Pi}=(\mathcal{P},\mathcal{L},I)$ and we can partition the sets $\mathcal{P}$ and $\mathcal{L}$ into three classes $\mathcal{P}_i$ and $\mathcal{L}_i$ $i=1,2,3$ according to the three possible orbits of points, lines respectively, under the action of α (see [2]).

It is $\overline{\Pi}_o=(\mathcal{P}_1,\mathcal{L}_1,I)$.

The incidence relation I can be partitionned into nine sets

$$I_{ij}= I\cap(\mathcal{P}_i \times \mathcal{L}_j) \qquad \forall\, i,j=1,2,3 \;;$$

note that $I_{13}=\emptyset=I_{31}$ and $I_{33}\neq\emptyset$ (compare [2]).

Define a map $\mu:\mathcal{P}_3\to\mathcal{L}_3$

$$P\mu = P\,\alpha\, P\,\alpha^2 \tag{3.1}$$

and a map $\mu':\mathcal{L}_3\to\mathcal{P}_3$

$$r\mu' = r\,\alpha\cap r\alpha^2 \tag{3.2}$$

Take

$$I^* = (I-I_{33})\cup I'_{33} \qquad \text{where}$$

$(P,r)\in I'_{33}$ if and only if $(r\mu',P\mu)\in I_{33}$

The incidence structure $\overline{\Pi}^*=(\mathcal{P},\mathcal{L},I^*)$ is a Figueroa plane (compare [2]).

The projective plane $\overline{\Pi}^*$ can be obtained by $\overline{\Pi}$ "redefining" the incidence relation between the points of $\mathcal{P}_3$ and the lines of $\mathcal{L}_3$ as follows:

$$P\ I^*\ r \text{ if and only if } P\mu\ I\ r\mu' \tag{3.3}$$

LEMMA 3.1- If $P \in \mathfrak{P}_3$ and $r \in \mathfrak{L}_3$, then

$P\ I^*\ r$ is equivalent to $P\ P\alpha\ I\ r \cap r\alpha$.

Proof:

The relation (3.3) is equivalent to

(3.4) $P\alpha \cdot P\alpha^2 \quad I \quad r\alpha \cap r\alpha^2$

Applying α^3 to (3.4), we obtain $P\ P\alpha\ I\ r \cap r\alpha$.

LEMMA 3.2- a) $r \in \mathfrak{L}_3$ is equivalent to $r \cap r\alpha \in \mathfrak{P}_3$;

b) $|r \cap \mathfrak{P}_2| = q^2+q+1$, $|r \cap \mathfrak{P}_3| = q^h - q^2 - q$.

Proof:

a): let $Q = r \cap r\alpha$; it must be $Q \in \mathfrak{P}_2 \cup \mathfrak{P}_3$ (otherwise, $r \in \mathfrak{P}_1$); $Q \in \mathfrak{P}_2$ is equivalent to "$\exists\, a \in \mathfrak{L}_1$ s.t. $Q = a \cap r$", or $Q\alpha = a \cap r\alpha$ and $Q = Q\alpha$, a contradiction.

b): let P_o be a point of $r \cap \mathfrak{P}_1$, then $P_o = r \cap r\alpha$ contradicts a); thus $r \cap \mathfrak{P}_1 = \emptyset$. For any $r_1 \in \mathfrak{L}_1$, $Q_1 = r_1 \cap r$ is a point of $r \cap \mathfrak{P}_2$. Let $r_2 \in \mathfrak{L}_1$, $r_2 \neq r_1$, $Q_2 = r_2 \cap r$; if $Q_1 = Q_2$ then $Q_1 = r_1 \cap r_2$ is a point of $r \cap \mathfrak{P}_1$, a contradiction to a). Therefore $|r \cap \mathfrak{P}_2| = |\mathfrak{L}_1|$. The remaining points of r are in $\mathfrak{P}_3$.

Let $r \in \mathfrak{L}_3$; take $Q = r \cap r\alpha$.

LEMMA 3.3- It is :

$$\{P \in \mathfrak{P} \,/\, P\ I\ r\} \cap \{P \in \mathfrak{P} \,/\, P\ I^*\ r\} = \{P \in \mathfrak{P}_2 \,/\, P\ I\ r\} \cup \{Q,\ Q\alpha^{h-1}\}.$$

Proof:

By Lemma 3.2, we can write $r = r_2 \cup r_3$ where

$r_2 = \{P \in \mathfrak{P}_2 \,/\, P\ I\ r\}$, $r_3 = \{P \in \mathfrak{P}_3 \,/\, P\ I\ r\}$.

For any point $P \in r_2$ it is equivalent " $P\ I\ r$ " and " $P\ I^*\ r$ ".

For any point $P \in r_3$, $P\ I^*\ r$ if and only if $P\ P\alpha\ I\ Q$; if $P \neq Q$ and $P\alpha \neq Q$ then $P\ P\alpha\ \not I\ Q$. Thus there are only two possibility : $P = Q$ or $P\alpha = Q$.

Let us introduce a coordinate system in $\overline{\Pi}$ so that a point P of $\overline{\Pi} - r_\infty$, r_∞ a distinguished line, has non-homogeneaous coordinates (x,y), $x,y \in F$, $(x,y) \equiv (x,y,1)$, and for any point P' of r_∞ it is $P' = (x,y,0)$. Moreover, $P\alpha = (x^q, y^q)$ and $P'\alpha = (x^q, y^q, 0)$.

Any line r is represented by an equation $x=c$ or $y=xm+b$ and $r\alpha$ by $x=c^q$ or $y=xm^q+b^q$, respectively.

Set $\mathcal{C}' = \{ P \in \mathcal{P}_3 / P\ I^*\ r \}$; by Lemma 1.1 it follows that
$\mathcal{C}' = \{ P \in \mathcal{P}_3 / P\ P\alpha\ I\ Q \}$.

PROPOSITION 3.1- $\mathcal{C}'$ is a subset of an algebraic curve $\mathcal{C}$ of Π of order $q+1$.

Proof:

Let $P=(x',y')$ be a point of $\mathcal{C}'$; since $P \in \mathcal{P}_3$, then $P\alpha=(x'^q,y'^q)$ where $x'^q \neq x'$ and $y'^q \neq y'$.

Let $y=xm+b$ be the equation of r ; $y=xm^q+b^q$ is the equation of $r\alpha$ and $m^q \neq m$, $b^q \neq b$, as $r \in \mathcal{L}_3$ (see Sec. 1).

The equation of the line $P\ P\alpha$ is $y=xn+c$ where :

$$n=(y'-y'^q)(x'-x'^q)^{-1} \quad , \quad c=(x'y'^q-x'^q y')(x'-x'^q)^{-1} .$$

The line $P\ P\alpha$ is incident to the point Q if and only if $P\ P\alpha$ belongs to the bundle (Q) of the lines of Π with center Q , equivalently if and only if there exists $\lambda,\mu \in F$ such that

$$(3.5)\quad \lambda+\mu = 1,\ \lambda m+\mu m^q = n\ ,\ \lambda b+\mu b^q = c\ .$$

The relations (3.5) are equivalent to

$$(m - m^q)(b - b^q)^{-1} = (n - m^q)(c - b^q)^{-1}$$

or ,

$$(3.6)\quad (m-m^q)(x'y'^q-x'^q y')-(b-b^q)(y'-y'^q)+(bm^q-b^q m)(x'-x'^q)= 0\ .$$

The equation (3.6) in x',y' represents an algebraic curve $\mathcal{C}$ of Π of order $q+1$.

As Π^* is a projective plane and a point $P=(x,y)$ belongs to $\mathcal{P}_1$ if and only if $P\alpha=(x^q,y^q)=(x,y)=P$ (see Sec. 1) then we can easily prove the following:

PROPOSITION 3.2- For any line r of $\mathcal{L}_3$, the curve $\mathcal{C}$ contains all the points of Π_o and $\mathcal{C}'=\mathcal{C}-(\mathcal{C} \cap \mathcal{P}_1)$ consists of q^3-q^2-q points of $\mathcal{P}_3$.

For any line $r \in \mathcal{L}_3$ of equation $y=xm+b$ set :

$r_2 = \{(x,y) \in \mathcal{P}_2 \ / \ y=xm+b\}$, $r_3 = \{(x,y) \in \mathcal{P}_3 \ / \ y=xm+b\}$ and

$r_3^* = \{ \mathcal{P} \in \mathcal{P}_3 \ / \ P \ I^* \ r \} = \{P=(x,y) \in \mathcal{P}_3 \ / \ (x,y) \text{ satisfy } (3.6)\}$

It is $r = r_2 \cup r_3$.

Take

(3.7) $r^* = r_2 \cup r_3^*$; $\mathcal{L}_3^* = \{r^* / \forall r \in \mathcal{L}_3\}$; $\mathcal{L}^* = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3^*$

As an easy consequence of Lemmas 3.1, 3.3 and of the Propositions 3.1, 3.2 we can state the following

THEOREM 3.1- The Figueroa plane $\Pi^* = (\mathcal{P}, \mathcal{L}, I^*)$ of order q^3 is represented by $(\mathcal{P}, \mathcal{L}^*, I)$.

REMARK 1 - The representation of Π^* by $(\mathcal{P}, \mathcal{L}^*, I)$ starts again from Π ; the subset $\mathcal{L}_3$ of the lines is replaced by $\mathcal{L}_3^*$, any new line $r^* \in \mathcal{L}_3^*$ consisting of two subsets : the subset r_2 of the "old" line r and the subset $\mathcal{C}'$ of the curve $\mathcal{C}$ defined by r , which replaces the points of $r \cap \mathcal{P}_3$.

REMARK 2 - Let α be the collineation of Π described by the diagonal matrix A 3x3 over F , $A=\text{diag}(1, r^i, r^{i+1})$ where $2i+1=h$, r is an element of F of order h . It is $A^h = I$.
Define a map $\mu : \mathcal{P}' \longrightarrow \mathcal{L}$ where $\mathcal{P}' \subset \mathcal{P}$ is the set of the point of Π not fixed by α , $P\mu = P\alpha^i \, P\alpha^{i+1}$ and a map $\mu' : \mathcal{L}' \longrightarrow \mathcal{P}$ where $\mathcal{L}' \subset \mathcal{L}$ is the set of the lines of Π not fixed by α , $s\mu' = s\alpha^i \cap s\alpha^{i+1}$ (compare [2] , for i=1).
We can easily prove that the mappings μ and μ' are involutorial birational reciprocities as $(x,y,z)\mu = [\theta yz, xz, xy]$ in homogeneous coordinates of points, resp., lines in Π ,where $\theta = -r^{i^2}(1+r^i)$; the analogous holds for μ'.

REFERENCES

[1] R.FIGUEROA : "A Family of not (V,1)-transitive Projective Planes of order q^3, $q \neq 1$ (3) and $q > 2$ ", Math.Z. 181 (1981) 471-479.

[2] T.GRUNDHÖFER : "A Synthetic construction of the Figueroa Planes", J.of Geometry, 26 (1986) 191-201.

[3] K.W.GRUENBERG, A.J.WEIR : "Linear Geometry", Springer-Verlag , N.Y - Heidelberg, Berlin (1967).

[4] C.HERING, H.J.SHAFFER : "On the nex Projective Planes of R.Figueroa", Comb. Theory, Proc.Schloss Ruischholzhausen 1982, ed. D.Jugnickel and K.Vedder, Berlin , Heidelberg, N.Y. (1982) 187-190.

[5] I.R.SHAFAREVICH : "Basic Algebraic Geometry", Berlin , Heidelberg, N.Y. 1974.

Rita Vincenti
Dipartimento di Matematica
Università degli Studi
Via Vanvitelli 1
06100 PERUGIA (I)