# LA MATEMATICA DISCRETA ATTRAVERSO I PROBLEMI

Franco Eugeni
*Dipartimento di Informatica, Terza Università di Roma*

*Questo lavoro è dedicato al ricordo del caro amico Bruno Rizzi, mio impareggiabile compagno di tante ricerche*

## 1. Introduzione

Lo scopo principale di questo articolo è presentare alcune problematiche della Matematica Discreta ad un pubblico vario e specialmente allo studioso che, avendo con questa disciplina scarsa familiarità, desideri compiere un primo approccio.

Il settore della Matematica Discreta è esploso negli ultimi trenta anni sia per i suoi aspetti teorici, sia per gli aspetti applicativi. La Matematica classica fondata sul sistema infinito dei numeri reali, densa di circa trecento anni di ragguardevoli risultati, non sembra offrire aiuto per tutta una serie di vaste problematiche sia di antica data sia nate, in tempi recenti, nella società contemporanea. Così appena ci accostiamo a problematiche di gestione aziendale si ha a che fare sempre e soltanto con insiemi finiti (finiti sono il numero dei lavoratori, delle macchine, dei reparti, dei prodotti e delle scorte ed anche dei mutui rapporti tra questi "oggetti").

Domina oggi la teoria dell'Informazione, nata dal lavoro di Shannon del 1948, e sviluppatasi maggiormente negli aspetti discreti. La moneta oggi è e viene trattata come una informazione. Le transazioni finanziarie vengono eseguite, sempre più in tempo reale, per vie informatiche. Ci si può proteggere dal pericolo degli interventi dall'esterno, da parte di personaggi non autorizzati, mediante l'uso di sofisticate tecniche crittografiche. Tali tecniche entrate prepotentemente nel settore civile, dopo secoli di servizio nel solo mondo militare, permettono di inviare messaggi riservati con alto grado di protezione, nei canali pubblici, di autenticare gli stessi anzi di creare per essi una sorta di firma elettronica. Non solo si è in grado di fare tutto questo e di farlo in tempo reale ma si è anche in grado di fornire assieme al prodotto crittografico anche una "misura", in termini di probabilità, della "bontà" del prodotto. Le soluzioni più agibili per protocolli di autenticazione fanno ricorso ai campi di Galois e alle geometrie costruite su di essi (geometrie finite). Nella firma elettronica con il metodo R.S.A. il segreto del codice consiste in una "difficoltà computazionale", precisamente la difficoltà di trovare i fattori di un prodotto di due primi di circa 150 cifre decimali.

Ancora una osservazione. Spesso nell'ambito della matematica applicata, esiste una tendenza a forzare alcuni fenomeni, che per loro natura sarebbero discreti, con una rappresentazione che utilizza la matematica del continuo (per esempio equazioni differenziali). Costruito il modello accade sovente che esso debba essere discretizzato per ottenere soluzioni sia anche approssimate. Questo doppio passaggio, spessissimo unica possibilità che abbiamo, può condurre anche a situazioni discordi con la realtà. La Matematica Discreta in qualche caso ha operato invece uno studio diretto e i suoi recenti successi, dovuti all'avvento di calcolatori sempre più potenti, sono una grande speranza per il domani e per la matematica del secondo millennio.

È molto difficile dare una definizione generale di Matematica Discreta. Molti tentano di darne definizioni indirette dicendo di cosa si occupano i cultori della disciplina. Gli interessi degli stessi sono molteplici e a volte anche piuttosto sghembi tra le varie sottobranche. Taluno suole dire in prima approssimazione che gli insiemi della Matematica Discreta si accumulano all'infinito. Ma anche questo chiarisce un obiettivo ma non definisce il campo di ricerche.

Altri la indicano come una sorta di matematica parallela mettendo tra loro a confronto i due seguenti quadri:

| **Matematica del Continuo** | **Matematica Discreta** |
|---|---|
| Analisi infinitesimale<br>Numeri reali e complessi, analisi reale e complessa, equazioni differenziali. | Analisi algebrica.<br>Campi di Galois, teoria delle funzioni generatrici, algebre di incidenza (Rota), analisi algebrica, teoria dei numeri. |
| Geometria<br>Geometrie euclidea, non euclidee, spazi vettoriali reali e complessi. | Geometrie finite e teoria dei grafi. |
| Generalizzazioni di strutture classiche | |
| Iperspazi<br>Spazi funzionali, etc | Disegni e spazi di blocchi<br>Sistemi di Steiner e grafi.<br>Iperstrutture. |
| Applicazioni in: | |
| Fisica, meccanica, teoria dei sistemi, scienze delle costruzioni, idraulica, economia matematica - etc. | Informatica, crittografia, teoria della autenticazione, teoria dei giochi e dei codici correttori, ricerca operativa. |

Concludiamo l'introduzione con due messaggi di due dei grandi padri fondatori di queste teorie. Il primo è di Gian Carlo Rota. Citiamo letteralmente:

«Vorremmo mettere in guardia il lettore contro l'impressione erronea che la teoria combinatoria si limiti allo studio degli insiemi finiti. Una collezione infinita di insiemi finiti non è affatto un insieme finito, e l'infinito riesce ad intrufolarsi anche nei ragionamenti più "finiti". Proprio nel perenne intrecciarsi di finito ed infinito sta il fascino del pensiero combinatorio». (G.C. Rota, 1973).

Il secondo pensiero che riporto è del mio Maestro Giuseppe Tallini, recentemente scomparso, pensiero che si può così riassumere.

Si tratta in sostanza di capire come la Combinatoria, apparentemente finita, in realtà operi su numeri così grandi da presentare le stesse difficoltà dell'infinito. Inoltre mancando una continuità e spesso anche una sorta di regolarità, si va a cadere nella sporadicità dei fenomeni. I problemi sono allora di enorme difficoltà, ma di estrema ed elegante bellezza.

La parte più teorica della Matematica Discreta, detta anche Geometria Combinatoria è rivolta allo studio dei Campi di Galois e delle Geometrie di Galois che si costruiscono su di essi. La nozione di spazio geometrico si generalizza nell'idea più generale dei disegni di blocchi. Particolari disegni sono i sistemi di Steiner, i piani e spazi affini e proiettivi, ma anche i grafi siano essi semplici o multipli. In tale ambiente spesso le vecchie idee della geometria classica concorrono assieme a risolvere i principali problemi che la teoria stessa ci pone.

Il primo lavoro di Combinatoria della Storia può essere considerato quello di Leibnitz del 1666: *Dissertatio de Arte Combinatoria*. Usualmente la data di nascita di questa disciplina, con il nome di Analisi Algebrica, si colloca nel 1840 con i lavori di Woodhouse (1844) e Kirkman (1847). Il problema principale della Teoria è quello di combinare assieme degli elementi di un dato insieme, chiamati punti, in famiglie di sottoinsiemi, chiamati blocchi, in modo che certe regole prefissate siano rispettate. Nascono in questo modo i *Block Designs* (disegni di blocchi), strutture più generali degli spazi proiettivi ed affini ed anche dei grafi. Recentemente molti risultati si sono avuti nell'ambito della Matematica Discreta. Grandi e meno grandi problemi sono stati affrontati, è stato risolto il problema dei quattro colori, creando problemi filosofici circa la validità delle prove al computer, replicabili, ma in temi lunghi. Analagomente problemi minori si sono posti per i disegni e si è provata la non esistenza del piano d'ordine dieci. I Disegni sono usati in Crittografia per la costruzione dei *threshold schemes* e per costruire tanti nuovi sistemi crittografici ancora allo studio.

Per concludere questa introduzione rispondiamo ad una domanda che spesso viene fatta. Perché le strutture geometriche finite si prestano alle applicazioni? È un miracolo o vi sono delle ragioni per questo? La risposta è molto semplice. Intanto la maggior parte delle applicazioni moderne trattano con universi discreti e non con universi continui (i computers, la protezione dell'informazione, le scienze sociali, la teoria dei Giochi cooperativi etc.). Inoltre i modelli derivanti da Geometrie Finite sono i più regolari in Combinatorica e i più "trattabili", potendosi descrivere con l'aiuto di strutture algebriche quali aritmetiche modulari e campi di Galois. A volte le ragioni della fortuna di una teoria sono banali, ed è questo il caso!

## 2. Dagli assiomi di Hilbert ai piani finiti

Una introduzione razionale della geometria tridimensionale euclidea classica, a parte quello che può essere il visivo modello empirico intuitivo, poggia su una assiomatica, prime tra tutte quella dovuta a David Hilbert. In particolare abolendo tutti gli assiomi in cui interviene la parola "piano", otteniamo gli assiomi che definiscono il solo *piano–euclideo.*

Sia S un insieme astratto di oggetti che chiamiamo *punti* e che indichiamo con lettere latine maiuscole:

$$S = \{ A, B, C, ... \}.$$

Consideriamo assieme ad S una famiglia R di sottoinsiemi di S:

$$R = \{ \{A,B,C, \}, \{H,K,L, \}, \{X,Y,Z, \} \ ... \}$$

Ogni elemento di R si dice un *blocco* una *retta* e la coppia (S, R) si chiama uno *spazio geometrico.*

La coppia (S, R) si chiama *piano euclideo* se per essa richiediamo siano verificati i cinque gruppi di assiomi seguenti, detti assiomi di Hilbert.

I. Assiomi di appartenenza
II. Assiomi di ordinamento
III. Assiomi di congruenza
IV. Assioma di continuità
V. Assioma delle parallele

Se aboliamo dall'elenco il gruppo V, costituito dal solo *assioma delle parallele*, otteniamo, i cosiddetti *piani non euclidei.* Se modifichiamo in un qualsiasi modo, o consideriamo solo una parte, o una variante, di tali assiomi otteniamo *"geometrie diverse dalla euclidea"*.

Supponiamo ora che il nostro obiettivo sia costruire una geometria nella quale ci siano rette con un numero finito di punti, salvando il resto degli assiomi. Allora restano fermi gli assiomi di appartenenza che sono due, occorre cancellare gli assiomi dell'ordine, della congruenza e di continuità che presuppongono le rette dotate di infiniti punti e si lascia l'assioma delle parallele. Si deduce così una assiomatica nella quale è possibile ammettere che esista qualche retta avente un numero finito di punti, assiomatica che conduce alla seguente definizione.

Uno spazio geometrico (S, R) si dice un piano affine se esso verifica i seguenti assiomi:

1) Per due punti passa una ed una sola retta.
2) Esistono tre punti non appartenenti ad una stessa retta e ogni retta ha almeno due punti.
3) Dati un punto A ed una retta r -- con A non appartenente ad r-- esiste una ed una sola retta per A (detta *la parallela*) non avente punti in comune con r. (l'unicità implica banalmente che il parallelismo è simmetrico e transitivo).

Riguardo l'ipotesi di esistenza di almeno una retta finita si dimostra che:

**Teorema:** Sia (S, R) un piano affine. Supponiamo che esista una retta r contenente un numero finito n ($\geq 2$) di punti, allora:
(a) Ogni retta ha n punti.
(b) Per un punto passano n + 1 rette.

(c) Esistono n rette parallele o coincidenti con una retta data.
(d) Esistono esattamente $n^2$ punti.
(e) Esistono esattamente $n^2 + n$ rette.

**Dimostrazione.** Dimostriamo il teorema per passi successivi.

**Passo 1.-** *Ogni retta* s *diversa da* r *ha n punti e da ogni punto del piano escono* n+1 *rette.*
Si prenda una retta t per un punto P di r e per un punto Q di s (si suppone che P sia diverso da Q nel caso che le due rette siano incidenti). Una retta t' per un punto P' di r e parallela a t incontra necessariamente s, altrimenti t' sarebbe parallela sia a t (per costruzione) sia ad s (ciò è assurdo perché per Q passerebbero s e t entrambe parallele a t'). Segue che per ciascuno degli n-1 punti di r diversi da P escono n-1 rette tra loro parallele intersecanti s in n-1 punti oltre Q.

**Passo 2.-** Per un qualunque punto P del piano passano n+1 punti.
Sia r una retta qualsiasi avente n punti, per quanto provato al passo 1, e sia P un punto fuori di r (certamente esistente perché esistono almeno tre punti non allineati). Per P allora passano le n rette che congiungono P con i punti di r (ovviamente tutte distinte) più la parallela per P ad r.

**Passo 3.-** *Il numero delle rette parallele o coincidenti con una retta data è n.*
Ovvia in quanto fissata una retta s ed una retta t incidente s per gli n-1 punti di t diversi dal punto comune escono esattamente n-1 rette parallele alla prefissata s. (Si osservi che due diverse parallele ad s sono anche parallele tra loro, altrimenti detto Q il loro punto comune, per Q passerebbero due parallele ad s).

**Passo 4.-** Il piano affine contiene esattamente $n^2$ punti.
Segue dal fatto che un fascio di rette parallele è una partizione del piano in n parti disgiunte ciascuna avente n elementi.

**Passo 5.-** Il piano affine contiene esattamente $n^2 + n$ rette.
Utilizziamo un ragionamento tipicamente combinatorio. Indichiamo con b il numero delle rette del piano e con v il numero dei punti del piano.
Contiamo il numero N delle coppie ordinate (P, r) dove P è un punto di r.
Fissato P nel piano (in v modi) per P passano n + 1 rette e quindi ogni fissato P determina n + 1 coppie. Segue che $N = v(n + 1)$.
Fissata nel piano una retta r (in b modi) essa, contenendo n punti, determina n coppie. Dunque $N = b\,n$. Dal confronto e per quanto provato nel passo 4 segue che è: $v(n+1) = bn$. Segue $b = n(n+1)$ cioè l'asserto.

**Definizione.** Un piano affine nel quale esista una retta avente un numero finito n di punti si denota con $\grave{A}(n)$ e si chiama *piano affine finito di ordine n.*

***Problema.*** Per quali interi n esistono piani affini d'ordine n?

**I Classe.** ***Piani desarguesiani***
Sia dato un campo finito (o campo di Galois); esso ha per ordine (numero di elementi) una potenza di un primo $q = p^h$ (p primo, $h \geq 1$). Se $\mathbf{Z}_p = \{ 0, 1, ...., p-1\}$ denota il campo delle "classi resto modulo p", ogni campo di Galois si può ottenere dall'anello **Z** degli interi relativi con una opportuna costruzione (analoga a quella con cui dal campo reale si passa al campo complesso) (cfr. Appendice). Un campo di Galois con $q = p^h$ elementi si denota con GF(q) (Galois Field of order q) e quando h=1 risulta $GF(p) = \mathbf{Z}_p$.
Possiamo associare ad ogni campo di Galois GF(q) un particolare piano affine (S,R) che denoteremo con il simbolo AG(2, q) (Affine Geometry of dimension 2 on GF(q) ), che prende il nome di piano affine desarguesiano su GF(q) e che si definisce nel seguente modo:

(a) L'insieme S dei punti è l'insieme delle coppie ordinate (x, y) con $x, y \in GF(q)$
(b) Ogni retta di R è il luogo dei punti (x, y) che sono soluzioni di una equazione del tipo:
$ax + by + c = 0$ con $a,b,c \in GF(q)$ e $(a, b) \neq (0, 0)$.

I tre assiomi caratteristici di un piano affine sono di immediata verifica sul modello AG(2, q).
(Infatti la retta per i due punti (h,k) e (m,n) è quella di equazione: (n-k)(x-h) = (m-h)(y-k); esistono tre punti: (0,0),(1,0),(0,1) mai allineati; la parallela per (h,k) di una generica retta è la a(x-h)+b(y-k) = 0).

Vale la pena di ricordare che:
1) Un campo finito o di Galois ha, come si prova, necessariamente ordine (numero degli elementi) una potenza di un primo,
2) Due campi di Galois di egual ordine sono necessariamente isomorfi e quindi sono isomorfi al modello costruibile come ampliamento delle classi resto riportato in appendice.
3) Due piani affini (o proiettivi) desarguesiani di egual ordine sono necessariamente isomorfi e quindi sono isomorfi al "modello tipo cartesiano" costruito sopra.

Pertanto ad ogni potenza di un primo q rimane associato un unico piano affine desarguesiano AG(2,q) avente q punti su una generica retta.

Esempio. Il piano desarguesiano AG(2, 3) d'ordine 3.

Considero il campo GF(3). L'insieme degli elementi del campo è l'insieme delle classi resto modulo 3, cioè l'insieme Z(3) = {0, 1, 2}. Le operazioni in Z(3) sono definite dalle ben note tabelle delle addizioni e moltiplicazioni modulo 3. Il piano affine AG(2,3) cioè il piano costruito su GF(3) ha 9 punti, ogni sua retta ha 3 punti, per un punto passano 4 rette e ci sono 3(3 + 1) = 12 rette. Il piano può essere schematizzato con entrambi i quadrati seguenti:

| | |
|---|---|
| (0,2) (1,2) (2,2) | 7 8 9 |
| (0,1) (1,1) (2,1) | 4 5 6 |
| (0,0) (1,0) (2,0) | 1 2 3 |

dove si è posto: 1 = (0,0), 2= (1,0), 3 = (2,0), 9 = (2,2).
Vogliamo costruire le rette del piano sia con le rispettive equazioni, sia dando le terne di punti di ciascuna retta sia le classi di parallelismo, sia una loro visualizzazione nei due quadrati.

I. - CLASSE DI PARALLELISMO

| | | |
|---|---|---|
| X = 0 | costituita dai punti | 1, 4, 7. |
| X = 1 | | 2, 5, 8 |
| X = 2 | | 3, 6, 9 |

Da notare sia che le coordinate di 1, 4, 7 verificano la corrispondente equazione X=0 (analogamente per le altre equazioni) sia che le rette di questa prima classe di parallelismo sono le colonne dei quadrati considerati.

II. - CLASSE DI PARALLELISMO

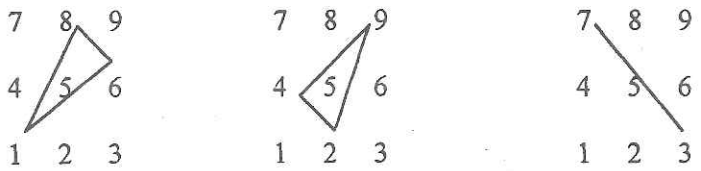
| | | |
|---|---|---|
| Y = 0 | costituita dai punti | 1, 2, 3 |
| Y = 1 | | 4, 5, 6 |
| Y = 2 | | 7, 8, 9. |

Le coordinate di 1, 2, 3 verificano la corrispondente equazione Y=0 (analogamente per le altre equazioni); le rette di questa classe di parallelismo sono le righe dei quadrati considerati.

III. - CLASSE DI PARALLELISMO

| | | | | |
|---|---|---|---|---|
| Y = 2X | ovvero | X + Y = 0 | costituita dai punti | 1 , 6 , 8 |
| Y = 2X+ 1 | ovvero | X + Y = 1 | | 2 , 4 , 9 |
| Y = 2X+ 2 | ovvero | X + Y = 2 | | 3 , 5 , 7. |

Le rette verificano la condizione di avere lo stesso "coefficiente angolare", inoltre si possono descrivere dicendo che sono formate dalla diagonale principale del secondo quadrato e dai due triangoli di Sarrus associati.

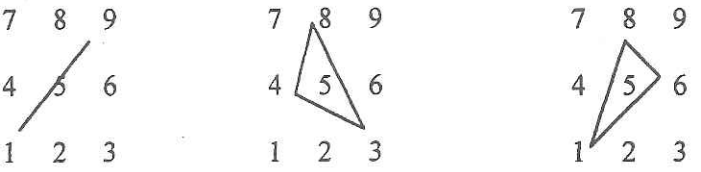



Notiamo che a differenza di quanto accade nel piano reale la retta di equazione X + Y = 0 si può scrivere come Y = 2X essendo nel campo GF(3) " 3 = 0." e quindi -1 = 2.

## IV. - CLASSE DI PARALLELISMO

| | | | |
|---|---|---|---|
| Y = X | ovvero 2X + Y = 0 | costituita dai punti | 1 , 5 , 9 |
| Y = X+ 1 | ovvero 2X + Y = 1 | | 3 , 4 , 8 |
| Y = X+ 2 | ovvero 2X + Y = 2 | | 2 , 6 , 7. |

Le rette verificano la condizione di avere lo stesso "coefficiente angolare" (il termine è usato con abuso di linguaggio non esistendo la nozione di angolo), inoltre si possono descrivere con la diagonale secondaria del quadrato e con i due triangoli di Sarrus ad essa associati.




L'introduzione di queste strutture è a volte essenziale ai fini della risoluzione di problemi di combinatorica, di fatto piuttosto complessi, allora che si desiderino affrontare per altra via.

Un tipico problema che si risolve con l'uso di queste strutture è il seguente:

PROBLEMA DEI FRATELLI

Un padre decide di mandare i suoi 9 figli al cinema per un certo numero di serate tre per tre in uno stesso cinema rispettando la condizione che due qualsiasi dei fratelli vadano al cinema insieme una ed una sola volta. Si chiede se ciò sia possibile e in quante serate.

La soluzione del problema è costituita dalla distribuzione delle classi di parallelismo di AG(2,3). Utilizzando le classi di parallelismo (di Sarrus) si ha la seguente distribuzione:

| 1 sera | 2 sera | 3 sera | 4 sera |
|---|---|---|---|
| 1 2 3 | 1 4 7 | 1 5 9 | 3 5 7 |
| 4 5 6 | 2 5 8 | 2 6 7 | 1 6 8 |
| 7 8 9 | 3 6 9 | 4 8 3 | 2 4 9 |

Poiché tutte le rette intervengono e poiché due qualsiasi figli, che sono due punti, individuano una sola terna (cioè una sola retta) il problema è risolto nel modo richiesto.

Questo problema è una versione semplificata del problema delle quindici studentesse posto dal Reverendo Kirkman (1847) – uno dei più noti rompicapo della matematica combinatorica, del quale ci occuperemo nel seguito del lavoro.

**II Classe.** ***Piani non desarguesiani.***

Sono i piani che non possono essere ottenuti con la costruzione precedente o come si suol dire

"non coordinatizzabili in un campo".

Sono noti esempi di piani affini non desarguesiani per ogni ordine "q *potenza di un primo ad esponente almeno due con* q *diverso da 4 ed* 8 " a cominciare dal caso q = 9 che è l'ordine più piccolo per il quale esistono piani non desarguesiani. Anzi q = 9 è un caso veramente critico. È il primo ordine per il quale oltre al caso desarguesiano si presentano altri esempi non desarguesiani e in questo caso esistono esattamente quattro piani tra loro non isomorfi dei quali cui uno ovviamente desarguesiano e tre non desarguesiani.

Rimarchiamo che non sono noti esempi di piani non desarguesiani di ordine primo, mentre a partire dai campi delle classi resto modulo un primo sono costruibili i corrispettivi esempi di piani affini desarguesiani tutti tra loro isomorfi. Non sono noti esempi, ovviamente non desarguesiani, di piani affini di ordine n non potenza di un primo.

Riguardo l'esistenza di piani affini l'unico teorema diretto è l'oramai più che celebre teorema di non esistenza provato nel 1949 dai matematici Bruck e Ryser

TEOREMA DI BRUCK È RYSER

Se n = 4k + 1 oppure n = 4k + 2 e se n non è la somma di quadrati di due interi qualsiasi allora non esiste alcun piano affine d'ordine n.

*Esempio 1.* 6 = 4*1 + 2, inoltre 6 non è somma di quadrati essendo 6 = 1+5 = 2+4 = 3+3, dunque non esiste il piano affine d'ordine 6.
*Esempio 2.* 14 = 3*4 + 2 inoltre 14 non è somma di quadrati essendo 14 = 1+13 = 4+10 = 9+5, dunque non esiste il piano affine d'ordine 14.
*Esempio 3.* Si ha 21 = 5*4 + 1, inoltre 21 non è somma di quadrati essendo 21 = 1+20 = 4+17 = 9+12 = 16 + 5, dunque non esiste il piano affine d'ordine 21.

Compariamo le seguenti tabelle:

| k | n = 4k+1 | $n = a^2 + b^2$ | k | n = 4k+2 | $n = a^2 + b^2$ |
|---|---|---|---|---|---|
| 1 | 5 | 5=1+4 | 1 | 6 | NO |
| 2 | 9 | 9=0+9 | 2 | 10 | 10=1+9 |
| 3 | 13 | 13=4+9 | 3 | 14 | NO |
| 4 | 17 | 17=1+16 | 4 | 18 | 18=9+9 |
| 5 | 21 | NO | 5 | 22 | NO |
| 6 | 25 | 25=16+9 | 6 | 26 | 26=1+25 |

Rimarchiamo che in alcuni casi come n = 10, 18, 26 il Teorema di Bruck- Ryser "non dice di no", tuttavia l'esistenza dei piani è dubbia essendo l'ordine non potenza di un primo, e in alcuni casi come n=10 la non esistenza è provata per altra via..

Generalmente si suole sempre indicare cosa succede per i cosiddetti "piccoli ordini" cioè per q entro il dieci. Riportiamo una casistica leggermente più ampia. Per i primi casi si sa che:

| n | esistenza di A(n) | numero di A(n) non isomorfi |
|---|---|---|
| 2 | SI | solo caso desarguesiano |
| 3 | SI | solo caso desarguesiano |
| 4 | SI | solo caso desarguesiano |
| 5 | SI | solo caso desarguesiano |
| 6 | NO | ZERO (Bruck & Ryser) |
| 7 | SI | solo caso desarguesiano |
| 8 | SI | solo caso desarguesiano |
| 9 | SI | 4 piani,uno desarguesiano |
| 10 | NO | ZERO (Tecnorema) |
| 11 | SI | numero ??, esempio desarguesiano |
| 12 | ? | ??? |
| 13 | SI | numero ??, esempio desarguesiano |
| 14 | NO | ZERO (Bruck & Ryser) |
| 15 | ? | ??? |
| 16 | SI | numero ??, esempio desarguesiano |

| n | esistenza di A(n) | numero di A(n) non isomorfi |
|---|---|---|
| 17 | SI | numero ??, esempio desarguesiano |
| 18 | ? | ??? |
| 19 | SI | numero ??, esempio desarguesiano |
| 20 | ? | ??? |
| 21 | NO | ZERO (Bruck & Ryser) |

Il caso più celebrato è il caso del piano di ordine 10 sul quale esiste un fiume di letteratura. Molti autori hanno scritto interi lavori che iniziano con "se esiste il piano d'ordine 10 allora.....", lavori che sono diventati vuoti dopo la prova della non esistenza di tale piano.

Tale dimostrazione è di quelle che possono chiamarsi un TECNOREMA, cioè una prova mediante Computer, eseguita in tempi molto lunghi (sembra più di un anno) ma in maniera da avere una esperienza ripetibile. L'eventuale esistenza di tale piano è stata ricondotta, facendo ricorso alla Teoria dei Codici, alla esistenza di un certo numero di configurazioni o combinazioni di punti in modo del tutto analogo a quanto fatto per il problema dei 4 colori. La non esistenza delle configurazioni è stata stabilita in modo esaustivo dal Computer. L'esame esaustivo diretto non era possibile poiché sarebbero occorsi secoli e secoli. Dunque sappiamo che il piano d'ordine 10 non esiste, indipendentemente dalla filosofia dell'accettare o meno una prova al computer. È vero che un tecnorema è un esperimento e quindi, almeno in teoria, si può, se si vuole, ripeterlo. È ben difficile stabilire dei confini filosofici in questi casi. Vi sono esempi di teoremi manuali che costituiscono di fatto una sorta di esperienza non ripetibile. Un esempio è il teorema di classificazione dei gruppi finiti sporadici, detto delle 15.000 pagine. Ciò dipende dal fatto che il corpo di tutti i lavori che hanno condotto negli anni al risultato consta di circa 15.000 pagine.

### 3. Quadrati latini, quadrati greco-latini e piani affini

Una matrice quadrata, nella quale ogni riga e ogni colonna siano una permutazione dei numeri 0, 1, 2,...., n - 1 si chiama un *quadrato latino–d'ordine n.*

Consideriamo, per esempio:

```
                0 1 2 3 4
                1 2 3 4 0
0 1 2           2 3 4 0 1
1 2 0           3 4 0 1 2
2 0 1           4 0 1 2 3
```

Il nome di quadrato latino fu dato da Eulero per il fatto che egli era solito indicare la prima riga con lettere latine che poi permutava. Da un certo punto di vista i quadrati latini si possono riguardare come una *generalizzazione del concetto di gruppo finito*. Ricordiamo che un *quasi gruppo* è una struttura algebrica (S, *) nella quale le equazioni di primo grado con coefficiente sia a destra che a sinistra hanno unica soluzione. Un quasigruppo dotato di elemento neutro si dice *cappio*. Infine un cappio associativo è un gruppo.

Se consideriamo la struttura algebrica definita sull'insieme 0, 1,..., n-1 la cui tavola di composizione è un quadrato latino si ottiene un quasigruppo finito, essendo la risolubilità delle equazioni di primo grado manifestamente equivalente ad essere le righe e le colonne permutazioni della permutazione fondamentale. Giova rimarcare che i due quadrati latini dell'esempio riportato sopra sono le tavole di composizione dei due gruppi additivi [Z(3),+] e [Z(5),+]. Invece i due quadrati latini dati da:

```
                0 1 2 3 4
0 2 1           1 2 0 4 3
1 0 2           2 3 4 0 1
2 1 0           3 4 1 2 0
                4 0 3 1 2
```

sono, il primo la tabella di composizione di un quasigruppo non cappio (non esiste l'elemento neutro "bilatero"); il secondo definisce un cappio essendo 0 l'elemento neutro, ma non valendo l'associativa (è per esempio 2(34) = 20 = 2 con (23)4 = 04 = 4).

Si chiama prodotto di due quadrati latini A e B dello stesso ordine n, di elementi generici a(i,j) e b(i,j) la matrice quadrata M di ordine n avente come elemento generico c(i,j) la coppia definita ponendo:

$$c(i,j) = (a(i,j), b(i,j)) = a(i,j) * b(i,j)$$

Scriveremo formalmente:

$$A * B = M.$$

Esempio.

```
2 0 1     1 2 0 3     2*1  0*2  1*0
1 2 0  *  2 0 1 3  =  1*2  2*0  0*1
0 1 2     0 1 2 3     0*0  1*1  2*2
```

Due quadrati latini si dicono *ortogonali* se il prodotto (cfr. esempio) ha tutte le coppie tra loro diverse. In questo caso il prodotto M = A*B si chiama un quadrato *greco-latino* di *ordine–n.* Il nome di quadrato greco-latino è riportato nel libro di Mc Mahon che, per indicarlo, usava mescolare lettere greche con lettere latine.

In un volume di Leonard Eulero (Rend. della Soc. delle Sc. di Flessinga, vol. IX, 1782) appare il seguente PROBLEMA DEI 36 Ufficiali. Si trova traducendo letteralmente: «Certe questioni riguardano un insieme di 36 ufficiali di sei gradi diversi e provenienti da sei reggimenti diversi che desideriamo disporre in un quadrato in modo che su ogni riga o colonna dello stesso si trovino 6 ufficiali sia di grado che di reggimento diverso. Ora considerate tutte le probabilità che possono aversi, per risolvere tale problema, ci si può convincere che una tale disposizione è assolutamente improbabile, anche se occorrerebbe dare una dimostrazione».

Disporre 36 ufficiali in un quadrato 6 X 6 in modo che in ogni riga o colonna compaia ogni grado e ogni arma una ed una sola volta.

Ovvero:

Costruire un quadrato greco latino d'ordine 6 (o due Q.L. d'ordine 6 ortogonali).

Eulero, a tale riguardo, enunciò la seguente congettura:

CONGETTURA DEI QUADRATI GRECO-LATINI (di Eulero -- 1782--). Se n = 2 (2k+1) cioè se n è il doppio di un numero dispari allora non esistono Q. G. L. di ordine n.

Nel 1900 Gaston Tarry prova il

TEOREMA DI TARRY: La congettura di Eulero è vera per n = 6.
Cioè il problema dei 36 ufficiali non ha soluzione!

Un passo avanti in una direzione piuttosto costruttiva è costituita da un teorema provato nel 1943 da Henry B.Mann, un eminente statistico, il quale prova il:

TEOREMA DI MANN: Se n non è il doppio di un numero dispari, se n = a * b*.....* z essendo a,b,...., z potenze di primi tra loro distinte e se poniamo m = min.(a,b, .....,z) allora esistono esattamente m - 1 quadrati latini d'ordine n a due a due ortogonali.

La congettura di Eulero, dopo il teorema di Mann sembrava resistere più che salda. Gli anni passavano, la congettura era ritenuta da tutti più che vera ma la sua prova non veniva, la congettura resisteva ad ogni assalto. Siamo nel 1959, sono trascorsi 179 anni dalla formulazione della congettura di Eulero, quando contro ogni aspettativa il grande matematico indiano Bose con i suoi altrettanto geniali collaboratori provano il

TEOREMA (di Bose-Shirkande-Parker): La congettura di Eulero è vera solo per n = 6.

Ciò significa che se n = 2(2k + 1) con k = 2, 3, ...., cioè se n = 10, 14, 18, ...., allora esistono coppie di Q. L. ortogonali. L'unico caso di non esistenza è quello originale dei 36 ufficiali che Eulero aveva, con straordinaria sensibilità, preso a modello.

179 anni per risolvere la questione !

A titolo di curiosità dunque non esistono 9 quadrarti latini d'odine 10 mutuamente ortogonali, non esistendo il piano affine d'ordine 10. Ci si può porre allora la questione di quale sia il massimo numero di quadrati latini mutuamente ortogonali esistenti. Il problema è aperto e noi non conosciamo tre Q.L. d'ordine 10 mutuamente ortogonali. Siamo in grado per n = 10 di mostrare la seguente coppia di Q.L. ortogonali

| | |
|---|---|
| 0 1 2 3 4 5 6 7 8 9 | 0 1 2 3 4 5 6 7 8 9 |
| 1 0 7 8 9 3 2 4 6 5 | 5 8 6 9 0 4 7 2 3 1 |
| 2 3 9 4 5 6 1 0 7 8 | 1 2 3 0 7 8 9 4 5 6 |
| 3 2 1 0 7 8 9 5 4 6 | 7 5 8 6 9 0 4 3 1 2 |
| 4 5 6 9 8 7 0 3 2 1 | 8 9 4 5 1 2 3 6 0 7 |
| 5 6 8 7 0 1 4 9 3 2 | 6 0 7 1 2 3 5 8 9 4 |
| 6 7 0 1 2 4 5 8 9 3 | 9 4 1 2 3 7 8 5 6 0 |
| 7 4 5 6 3 9 8 2 1 0 | 3 6 0 7 8 1 2 9 4 5 |
| 8 9 3 2 1 0 7 6 5 4 | 4 7 5 8 6 9 0 1 2 3 |
| 9 8 4 5 6 2 3 1 0 7 | 2 3 9 4 5 6 1 0 7 8 |

Cosa si può dire in generale.
Si prova che detto M(n) il massimo numero di Q. L. mutuamente ortogonali risulta:

$$M(n) \leq n - 1$$

Un insieme di n-1 quadrati latini, mutuamente ortogonali, si chiama un sistema completo di Q.L. mutuamente ortogonali. Il problema che si pone è sapere quando nella limitazione vale il segno di eguaglianza. È ancora Bose che nel 1938 assieme a Stevens enuncia un teorema esprimente il profondo legame tra quadrati latini e piani affini.

TEOREMA DI BOSE E STEVENS (1938). Esiste un piano affine di ordine n se e solo se M(n) = n - 1, cioè se e solo se esiste un sistema completo di Q. L. mutuamente ortogonali.

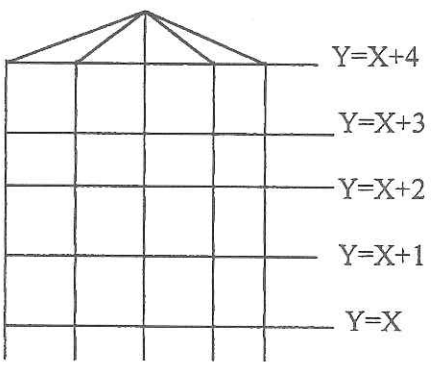
È abbastanza interessante, per comprendere questo risultato costruire il sistema completo dei 4 quadrati latini mutuamente ortogonali di ordine 5 come semplice esercizio
Consideriamo AG(2, 5) cioè il piano affine d'ordine 5 a coordinate in GF(5). Prendiamo in esame la retta Y = X in coppia con la retta Y = mX dando una alla volta i valori m = 2, 3, 4.
La prima accoppiata è Y = X con Y = 2X. I due fasci di rette parallele:

$$Y = X + h, \qquad Y = 2X + k$$

rappresentati simbolicamente come orizzontali e verticali, come si prova con facili calcoli, danno luogo al reticolato di coordinate seguente:

*verticali:* fascio di rette di direzione 2..... Y=2X+k.....

| | | | | |
|---|---|---|---|---|
| (4,3) | (0,4) | (1,0) | (2,1) | (3,2) |
| (3,1) | (4,2) | (0,3) | (1,4) | (2,0) |
| (2,4) | (3,0) | (4,1) | (0,2) | (1,3) |
| (1,2) | (2,3) | (3,4) | (4,0) | (0,1) |
| (0,0) | (1,1) | (2,2) | (3,3) | (4,4) |




Le coordinate dei punti del reticolato di intersezione dei due fasci di rette formano un quadrato greco-latino, divisibile nei due quadrati latini ortogonali seguenti:

| | |
|---|---|
| 40123 | 34012 |
| 34012 | 12340 |
| 23401 | 40123 |
| 12340 | 23401 |
| 01234 | 01234 |

costruito il primo con le ascisse dei punti del reticolato, il secondo con le ordinate.k

Se ripeto il procedimento con Y=X fissa e con la nuova retta Y=3X trovo un nuovo quadrato greco latino che si spezza in due quadrati latini dei quali il primo è il primo dei due trovati sopra mentre il secondo è nuovo. Ripetendo ancora il procedimento con la seconda retta di equazione Y = 4X si trova un quarto quadrato latino mutuamente ortogonale con i precedenti.

Si trova in tale modo un sistema completo di quattro quadrati latini mutuamente ortogonali di ordine 5. D'altro canto la ricostruzione delle rette non parallele agli assi di un piano d'ordine n a partire da un sistema completo d'ordine n-1 è abbastanza evidente.

## 4. Il problema di Kirkman

Il 15 dicembre 1846, ad una riunione della Litterary and Philosophical Society di Manchester, veniva letto un lavoro del Reverendo Thomas Kirkman (1806 - 1895) dal titolo "On a problem in combination". In questo articolo si pone il seguente problema:

..... "Dati v oggetti stabilire quante parti di k oggetti si possono costruire in modo che t elementi arbitrari siano contenuti in una sola di tali parti".

Ciò equivale a costruire uno spazio geometrico (S,B) dove S è un v-insieme e B è una famiglia di parti di S con la proprietà che per t punti di S passi uno ed un solo blocco di B.

Un sistema siffatto si chiama oggi *Sistema di Steiner* di tipo S(t, k, v). (Steiner in realtà ritrovò i risultati di Kirkman essendo rimasto il lavoro di Kirkman sconosciuto per anni).

Nei casi particolari si noti che per t = 2 i blocchi si chiamano rette mentre gli S(2, k, v) si chiamano anche "Balanced Incomplete Block Design"in sigla (BIBD) in accordo con il fatto che per t = k il sistema contiene come blocchi tutte le possibili combinazioni di classe k e pertanto un sistema S(k,k,v) si può chiamare un disegno di blocchi completo.

Da notare, e questo è di grande interesse, che i piani affini sono dei particolari sistemi di Steiner precisamente quelli di tipo $S(2, n, n^2)$ ma anche gli spazi affini e proiettivi sono particolari sistemi di Steiner con t = 2 e con i valori k e v speciali. Dunque gli S(2,k,v) appaiono una ampia generalizzazione delle più classiche strutture geometriche finite e gli S(t,k,v) sono ancora più generali. Al crescere di t le difficoltà sono veramente notevoli. Si pensi che:

NON SONO NOTI ESEMPI DI SISTEMI DI STEINER PER t > 5!

Nel suddetto lavoro Kirkman risolve completamente il problema nel caso di t = 2 e k = 3 provando che le condizioni:

$$v = 6n + 1 \quad \text{oppure} \quad v = 6n + 3$$

sono necessarie e sufficienti per l'esistenza dei sistemi suddetti. Si sa per gli S(2, 3, v) che al crescere di v il numero di sistemi di terne cresce con estrema rapidità

| n | v = 6n + 1 | v = 6n + 3 | esistenza | numero di sistemi |
|---|---|---|---|---|
| 1 | v = 7 | | SI | 1 |
| 1 | | v = 9 | SI | 1 |
| 2 | v = 13 | | SI | 2 |
| 2 | | v = 15 | SI | 80 |
| 3 | v = 19 | | SI | ? > 284407 |
| 3 | | v = 21 | SI | ? > 2160980 |
| 4 | v = 25 | | SI | enorme |
| 4 | | v = 27 | SI | enorme |

Nel 1850 Kirkman stesso pose in "THE LADY'S AND GENTLEMAN'S DIARY" il problema tuttora noto come PROBLEMA DELLE 15 STUDENTESSE, che possiamo enunciare nel seguente modo:

"La direttrice di un collegio vuole suddividere le sue 15 alunne in gruppi di tre ciascuno, in modo tale che durante i sette giorni della settimana esse possono uscire per la passeggiata e che due qualunque di esse siano state in una terna una ed una sola volta".

Dal punto di vista dei sistemi di Steiner si tratta di costruire un sistema di Steiner di tipo S(2,3,15) dotato di un parallelismo (problema analogo a quello dei fratelli dove abbiamo costruito un sistema S(2,3,9) dato dal piano affine d'ordine tre).

Gli S(2, k, v) dotati di parallelismo sono anche chiamati "Resolvable BIBD". Dire che esiste un parallelismo significa dire che la relazione di parallelismo individua delle classi di equivalenza ognuna delle quali sia un ricoprimento dell'insieme dei punti. Esempi di S(2, k, v) con parallelismo si ottengono prendendo ad esempio i piani affini (questi sono sempre "resolvable") e più in generale gli spazi affini, ma questi sono solo una piccola parte. Si prova facilmente che se esiste un parallelismo allora esistono esattamente:

$$r = (v - 1)/(k - 1)$$

diverse classi di rette parallele.

Dunque se in un sistema di Steiner S(2,3,15) esiste un parallelismo allora ci sono esattamente $(15 - 1)/(3 - 1) = 14/2 = 7$ classi di parallelismo. Un esempio di sistema di Steiner S(2, 3, 15) si può costruire considerando uno spazio proiettivo PG(3,2) di dimensione tre ed ordine due. Tale spazio si può dare assegnando l'elenco dei blocchi che daremo ora ripartiti per classi di equivalenza ciascuna denotata con un nome di un giorno della settimana.

| | | | |
|---|---|---|---|
| Lunedì | 1 2 3<br>4 10 14<br>5 8 13<br>6 9 15<br>7 11 12 | Martedì | 1 4 5<br>2 8 10<br>3 12 15<br>6 11 13<br>14 7 3 |
| Mercoledì | 1 6 7<br>2 9 11<br>3 13 14<br>4 12<br>5 10 15 | Giovedì | 1 8 9<br>2 13 15<br>3 4 7<br>5 11 14<br>6 10 12 |
| Venerdì | 1 14 15<br>2 4 6<br>3 8 11<br>5 9 12<br>7 10 13 | Sabato | 1 10 11<br>2 12 14<br>7 8 15<br>3 5 6<br>4 9 13 |
| Domenica | 1 12 13<br>2 5 7<br>3 9 10<br>4 11 15<br>6 8 14 | | |

I matematici Cole, Cummings e Porter hanno provato che esistono esattamente 80 sistemi S(2,3,15) non isomorfi e per ciascuno di essi si ha un differente problema delle 15 studentesse. Solo per sette di essi il problema delle 15 studentesse è risolubile.

## 5. Verso le applicazioni. I sistemi di autenticazione

In questo paragrafo supporremo che due personaggi abbiano bisogno di comunicarsi importanti messaggi ma il loro desiderio è di sapere se un terzo individuo sia o no intervenuto dall'esterno a

modificare il messaggio. Per proteggersi da tali rischi e per garantire l'integrità del messaggio trasmesso si utilizzano gli schemi di autenticazione. Tra questi sistemi alcuni che si dicono perfetti, sono ottimali nel senso che sarà precisato. Tali schemi perfetti sono stati costruiti mediante le geometrie finite.

Supponiamo che Mr Primo mandi un messaggio M a Mr Secondo. È importante che un utente esterno che chiamiamo Mr X desideri alterare il messaggio. Per prevenire questo tipo di attacco Mr P e Mr S concordano una chiave segreta K ed un algoritmo f. Quando Mr P manda il messaggio M, invia assieme ad M un autenticatore costituito da A = f(M,K). In altre parole Mr P invia una coppia (M,A). Quando Mr S riceve una coppia diciamo (M', A), tale coppia può avere il messaggio eventualmente alterato, diciamo da M in M', assieme ad un autenticatore A eventualmente modificato anche lui. Mr S conosce il modo per effettuare un controllo: egli, conoscendo la chiave K e l'algoritmo f, computa A*= f(M',K) e, solo se A* calcolato coincide con A* ricevuto, allora egli accetta il messaggio M' come autentico.

1) Mr P forma A = F(M,K) invia (M,A).
2) Mr X modifica (M,A) in (M', A')
3) Mr S riceve (M', A') forma A*= f(M', K)
   solo se ..... A* = A'.....accetta M' !

Cosa può fare l'intruso Mr X perché il suo M' venga accettato? Egli non conosce l'algoritmo f e non conosce la chiave K. Allora Mr X può solo fare dei tentativi per forzare il sistema cioè per indovinare l'autenticatore A' compatibile con il nuovo messaggio M' da lui formato. Le sue reali possibilità di "indovinare" una coppia (M', A') coerente è espressa dal seguente teorema, provato nel 1974:

TEOREMA – (Gilbert-Mc Williams-Sloane) Supponiamo che tutti i messaggi e tutte le chiavi si presentino con la stessa probabilità. Allora in ogni schema di autenticazione la possibilità di vittoria di un intruso è almeno pari al reciproco della radice quadrata del numero totale delle chiavi.

Uno schema di autenticazione nel quale la probabilità di successo dell'intruso è minima si dice *perfetto,* nel caso che la probabilità di successo sia dello stesso ordine di grandezza della probabilità minima allora si parlerà di schemi di autenticazione *essenzialmente perfetti.* Un modello di schema di autenticazione perfetto è stato costruito dai tre solutori del problema dell'autenticazione Gilbert, Mc Williams e Sloane facendo ricorso a piani proiettivi. Questo modello ha un elevato numero di chiavi rispetto ai messaggi, così esso sembra essere molto buono. Vediamo ora lo schema perfetto di autenticazione di Gilbert, Mc Williams e Sloane.

Fissiamo un piano affine finito AG(2,q) di ordine q. Se Y = m X + h è una qualunque retta al variare di m definiamo come *messaggi* i q+1 punti impropri di coordinate omogenee:

$$(m) = (0,1,m) \text{ e } (00) = (1,0,0).$$

Chiamiamo le *chiavi* i $q^2$ punti propri del piano affine.

Quando Mr P vuole inviare un messaggio (m) si accorda con Mr S per la scelta segreta di una chiave precisamente accordano come chiave il punto-chiave K= (a,b).

Allora Mr P costruisce un *autenticatore* del dato messaggio (m) nel modo seguente: considera la retta per K di direzione m, cioe:

$$Y = mX + A = m\,(X-a) + b = mX + (b-ma)$$

il termine noto A = b-ma è l'autenticatore. Dunque Mr P invia la coppia:

$$(m,\ b-ma)$$

Mr S riceve la coppia modificata (m', A') e conoscendo la chiave K forma b-m'a ed accetta il messaggio solo se b-m'a = A'.

Quale speranza ha Mr X di costruire A' giusto? È chiaro che deve indovinare K = (a,b) vedendo

la retta Y = mX + A, cioè deve indovinare un punto della retta. Avendo la retta q punti la sua probabilità di indovinare è 1/q cioè l'inverso della radice del numero delle chiavi che sono $q^2$.

Nella pratica si prende $q = 2^n$. Infatti in tale caso sia m che b-ma sono due sequenze di zeri ed uno ciascuna lunga n. Anche la coppia (m, b-ma) sarà una sequenza lunga 2n senza soluzione di continuità e seguiranno nel messaggio altre sequenze lunghe n attaccate alle altre. Basterà sapere che ogni sequenza di n bit è una porzione di messaggio e che la seconda sequenza, ad esempio, è l'autenticatore.

Naturalmente una sequenza lunga n è in realtà un polinomio di grado n-1 a coefficienti 0 ed 1 e i polinomi si addizionano normalmente e si moltiplicano normalmente con la sola riduzione per le potenze data da:

$$X^n = X + 1$$

È questa l'algebra dei campi di Galois di ordine $q = 2^n$ che per il nostro caso da luogo a schemi di autenticazione con probabilità di rottura $1/2^n$ ed n arbitrario. Sono dunque schemi il cui grado di sicurezza può essere valutato e scelto a piacere, secondo quanto è importante l'autentica che si deve fare.

## 6. Ancora una applicazione: block designs è schemi di soglia

Lo scopo di questo ultimo paragrafo è quello di mostrare un utilizzo dei disegni di blocchi (block designs). I disegni di blocchi sono una generalizzazione molto ampia dei Sistemi di Steiner introdotti nel paragrafo 4 e quindi delle Geometrie di Galois. Per la loro comprensione sono richiesti pochissimi prerequisiti. È immediato impadronirsi della pochissima teoria che è alla base di queste stutture, peraltro estremamente generali, inoltre tali disegni si prestano per un immediato utilizzo anche da parte di coloro non molto esperti in Combinatorica. Questo apparente "paradosso" si spiega con facilità: *è molto facile usare disegni di blocchi noti, è invece molto difficile inventare o scoprire disegni nuovi.*

Denotiamo con S un insieme di v elementi che diremo *punti* (o anche trattamenti, players, shadows secondo l'aspetto applicato che desideriamo evidenziare). Sia B una famiglia di b parti di S. Ogni elemento di B si chiama *blocco* (o anche retta, coalizione, blocco d'informazione, gruppo etnico etc.). Una coppia (S,B) di questo tipo si dice solitamente uno *spazio geometrico finito* o un ipergrafo.

Si può rappresentare, come spesso si fa, una coppia (S,B) in modo tabellare. Questo significa numerare gli elementi di S da 1 fino a w ed assegnare l'elenco dei gruppi di numeri che concorrono a formare i singoli blocchi.

*Esempio.* Sia S = {1,2,....,7 }è un 7-insieme una famiglia B di blocchi su S è la seguente:

1 2 3 2 5 7 3 4 5 1 4 7 2 4 6 1 6 7 3 6 7

Tale (S,B) non è altri che il piano proiettivo d'ordine due, altrimenti detto Piano di Fano.

Diamo ora la seguente:

DEFINIZIONE. Siano t, k, w, $\lambda$ (interi assegnati con $1< t < k < v.$ e $\lambda \geq 1$. Con il termine disegno di blocchi o anche t-(v,k,$\lambda$) *disegno*, si indica una coppia (S,B) soddisfacente le seguenti condizioni:

a.- Ogni blocco contiene esattamente k punti

b.- Ogni t-insieme è contenuto in esattamente $\lambda$ blocchi.

Da notare che ogni t-(v,k,$\lambda$) disegno con $\lambda = 1$ è un sistema di Steiner di tipo S(t,k,v), dunque i t-disegni generalizzano i sistemi di Steiner e quindi generalizzano gli spazi affini e proiettivi.

Un esempio banale è il seguente t-disegno, detto *disegno completo*: È dato un v-insieme S, e viene data come famiglia B tutte le possibili parti di fissata cardinalità $k < v$. Fissato allora in modo arbitrario un intero t con $1 < t<k<v$ si osservi che per ogni arbitrario t-insieme assegnato in S vi sono esattamente

$$\lambda = \begin{pmatrix} v - t \\ k - t \end{pmatrix}$$

modi aggiungere k-t punti al t-insieme dato. Si ottiene in tale modo un disegno e precisamente un t-(v,k,$\lambda$) disegno dove $\lambda$ è dato dall'espressione scritta sopra. È interessante osservare che questo

disegno completo è l'unico che si conosce con t qualsiasi. Non si conoscono esempi di disegni di blocchi incompleti (cioè non coinvolgenti tutti i k-sottoinsiemi) che abbiano $t > 6$.

Casi particolari esclusi a priori dalla definizione sono il caso t=k nel quale la famiglia dei blocchi sarebbe quella dei k-sottoinsiemi. Si esclude anche il caso k=v che darebbe luogo ad un disegno con un solo blocco.

Vogliamo ora scrivere alcune relazioni aritmetiche valide in generale per i t-disegni e quindi anche per i sistemi di Steiner e per gli spazi affini e proiettivi.

Supponiamo di avere un t-$(v,k,\lambda)$ disegno; diciamo (S,B). Indichiamo con $r_i$ il numero dei blocchi che contengono un fissato i-insieme, con $i = 0,1, ..., t$.Si dimostra allora che: valgono le seguenti formule:

$$r_i = \binom{v-i}{t-i} \lambda / \binom{k-i}{t-i} \qquad i = 0,1, ....., t$$

Se un disegno di dati parametri esiste allora i secondi membri delle $r_i$ sono degli interi esprimenti il numero dei blocchi per i punti. Da notare che per $i = 0$ si ottiene il numero dei blocchi non sottoposti ad alcuna condizione cioè il numero totale b dei blocchi. Ancora per i=t si ritrova il numero $\lambda$ dei blocchi per t punti. Tuttavia le relazioni scritte hanno anche un ulteriore utilizzo.

Supponiamo di non sapere se un disegno di dati parametri esista o meno. È chiaro allora che se nel calcolo delle eventuali $r_i$ qualche rapporto di coefficienti binomiali del secondo membro non è un intero allora il disegno con quei parametri non può esistere.

Dunque i secondi membri delle $r_i$, per $i = 0,1,...,t-1$, esprimono delle condizioni di divisibilità che sono condizioni necessarie per l'esistenza dei disegni. Le condizioni sono tuttavia non sufficienti in quanto esistono sistemi di parametri per i quali le condizioni necessarie sono verificate, tuttavia per altra via si è stabilita la non esistenza del disegno. Esempi a riguardo sono i disegni dei piani affini A(6) = S(2,6,36) e A(10) = S(2,10,100) la cui non esistenza equivale alla impossibilità del problema dei 36 ufficiali e al tecnorema del piano d'ordine 10. Ma questa è solo la "cima di un iceberg" e vi sono tanti altri casi.

Ad esempio non è noto se esista o meno il sistema di Steiner di tipo S(4,5,17). Un tale disegno se esiste ha parametri $r_i$ dati da:

$$r_4 = 1,\ r_3 = 7,\ r_2 = 35,\ r_1 = 140,\ r_0 = 476.$$

Sembrerebbe molto facile ragionare su questi piccoli numeri, invece si tratta di un difficile ed annoso problema aperto della Geometria Combinatoria.

Per passare ora ad introdurre i cosiddetti *schemi di soglia* (threshold schemes) occorre fare mente locale al fatto che molte transazioni finanziarie oggi e, forse ancor più domani, saranno trattate elettronicamente. L'accesso ai segreti delle modalità e possibilità di trasmissione deve essere protetto da un sistema di sicurezza, chiamato appunto schema di ingresso o di soglia. L'accesso deve essere permesso solo se un certo numero di utenti autorizzati danno un assenso.

Per analogia possiamo pensare ad una cassaforte di Banca con due o più chiavi distribuite tra più controllori. Possiamo ancora pensare a gruppi che gestiscono operazioni nelle quali occorre prendere decisioni di grande responsabilità, come un eventuale lancio di un missile, decisione che usualmente richiede l'accordo di un certo numero di persone autorizzate. Ancora possiamo pensare al caso di decisioni prese da un consiglio di Amministrazione del futuro magari operante con un servizio di Videotel, possiamo pensare all'accesso a documenti e banche dati con contenuto impegnativo. Per questi sistemi ed altri non vi è dubbio che vi sia una chiara domanda di schemi di soglia.

L'idea degli schemi di soglia risale al 1979 su proposte dei crittologi Blakley e Shamir. La filosofia è semplice: alcuni "pezzi" o "tracce" (shadows) di informazioni vengono ripartiti tra diversi personaggi "fidati" in maniera che un gruppo di essi, in pieno e legittimo accordo tra loro, quando raggiungono un "quorum" o numero soglia di "pezzi d'informazione", siano in grado di ricostruire l'intera informazione.

Uno schema di soglia è un certo numero s di pezzi di informazioni con la condizione che:

1 - Un certo blocco o pacchetto di informazioni può essere completamente ricostruito dalla conoscenza di t pezzi di informazioni comunque presi tra gli s distribuiti.

2 - È impossibile ricostruire il blocco dalla conoscenza di meno di t pezzi di informazioni.

Usando un linguaggio di tipo combinatorio, uno schema di soglia di indice t (t-threshold scheme) è uno spazio geometrico (S,B) nel quale è fissato almeno un blocco speciale, sia X, detto blocco delle informazioni principali, ed almeno n punti in esso, detti utenti autorizzati, in modo tale che:

(1) fissati comunque t tra gli n punti di X, esiste un solo blocco di B che contiene i t punti;

(2) fissati arbitrariamente al più t-1 tra gli n punti di X vi sono "molti" blocchi di W contenenti quei punti.

Può essere opportuno anche scegliere un insieme C che interseca il blocco X delle informazioni principali in un insieme Y di punti. Quale è il ruolo dell'insieme Y nello schema? Supponiamo di immettere nel sistema un certo numero di pezzi di informazione, o "punti". Il sistema tenta di costruire il blocco principale X delle informazioni per essi. Se il blocco per tali punti non è unico, l'assenso all'accesso non viene dato. Se al contrario esiste un solo blocco L per quei punti, allora il sistema forma l'insieme Y* dei punti comuni ad L e l'insieme fissato C. Solo se Y* = Y, l'assenso all'operazione viene dato. È opportuno che l'insieme C scelto per "bloccare" X non contenga X stesso, anzi è opportuno che C contenga pochi punti di B. Il motivo è ovvio: qualcuno potrebbe tentare di cercare X dentro C, scoperto per "qualche via".

Noi siamo interessati, per ovvie ragioni di praticità e di economia, ad avere schemi multipli, cioè schemi nei quali ci sia una famiglia B, anche vasta, di blocchi di informazioni principali. In questo contesto è bene avere un insieme C che abbia la proprietà di essere intersecato da ogni blocco di B in almeno un punto ma che non contenga alcun blocco principale. Siffatti insiemi C prendono in letteratura il nome di blocking sets e a loro riguardo sono state fatte ampie e profonde ricerche.

Dunque un disegno di blocchi pensati tutti come blocchi delle informazioni principali e un blocking set in esso ed ecco uno schema di soglia realizzato. Ma è sufficiente chiaramente anche un disegno parziale, cioè la considerazione di solo una parte dei blocchi del disegno e un blocking set rispetto a quella parte.

In questo ambito vi è ancora molto lavoro da fare e molti aspetti sono da approfondire.

Spero solo con questa panoramica di essere riuscito a dare una idea sia pure parziale di una Matematica Discreta presentata per problemi antichi e moderni, salottieri e concreti, astratti e reali. Se questi aspetti vi hanno interessati io ho raggiunto il mio scopo.

## Appendice. I campi di Galois

Questa breve appendice ha lo scopo di introdurre "brutalmente" il lettore non esperto ai primi elementi relativi alla teoria dei campi, in particolare quelli finiti o di Galois.

Indichiamo con F un insieme contenente almeno due distinti elementi, diciamo 0 (zero) ed 1 (uno). In F si suppongono definite due operazioni binarie ed interne, (+) e () che chiameremo formalmente addizione e moltiplicazione. La struttura algebrica (F,+,.) si dice che è un *campo* se valgono le seguenti proprietà:

a) La prima struttura (F,+) è un gruppo commutativo.

(Cioè l'operazione (+) gode delle proprietà associativa e commutativa, esiste un elemento neutro che si denota con 0, e per ogni elemento x di F esiste un unico elemento y di F tale che x+y = y+x = 0; un tale y è detto l'opposto di x ed è denotato con -x).

b) Sia F*=F\0. La seconda struttura (F*,.) è anche un gruppo commutativo.

(Cioè anche la moltiplicazione è associativa e commutativa, l'elemento neutro è indicato a con 1 e per ogni elemento non nullo x esiste un unico elemento y tale che xy = yx =1. Un tale y si dice l'inverso di x e si denota con x'.

c) Il legame tra le due strutture consiste nel richiedere che l'operazione di moltiplicazione sia distributiva rispetto a quella di addizione. Cioè che sia, quale che siano gli elementi considerati in F:

a (b+c) = ab + ac.

Esempi di campi con infiniti elementi sono il campo dei numeri razionali, reali, complessi e delle funzioni razionali.

Un qualsiasi campo che contenga un numero finito q di elementi si chiama un campo di Galois d'ordine q e si indica con GF(q).

Si dimostra, e questo è fondamentale per il seguito, che l'ordine q di un campo, cioè il numero q

dei suoi elementi, è necessariamente una potenza di un numero primo p. Dunque $q = p^h$. Inoltre si dimostra che un campo è univocamente determinato dal suo ordine q, nel senso che se K e K' sono due campi di un medesimo ordine q allora essi sono isomorfi, esiste cioè una corrispondenza biunivoca di K su K' che, conservando le operazioni, muta l'uno di essi esattamente nell'altro "conservando la struttura algebrica", come accade ad esempio tra numeri naturali ed interi positivi. In tal caso le strutture vengono riguardate come identiche. Vogliamo ora costruire i campi GF(p) aventi come ordine un numero primo. Introduciamo, per questo, l'aritmetica modulare. Fissiamo un qualsiasi intero m che sia almeno 2 e formiamo le seguenti colonne:

| | | | | | | |
|---|---|---|---|---|---|---|
| ..... | ..... | ..... | ..... | ..... | ..... | |
| -m | -m+1 | -m+2 | ..... | -m+r | ..... | -1 |
| 0 | 1 | 2 | ..... | r | ..... | m-1 |
| m | m+1 | m+2 | ..... | m+r | ..... | 2m-1 |
| ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| hm | hm+1 | hm+2 | ..... | hm+r | ..... | hm-1 |
| ..... | ..... | ..... | ..... | ..... | ..... | ..... |

Ogni colonna prende il nome di classe resto modulo m. Quando ciò non dà luogo ad equivoci, una classe resto si indica con il più piccolo intero non negativo che la rappresenta. Questo simbolismo, pur essendo molto scorrevole, può, se non si presta attenzione, generare qualche confusione tra classi resto ed interi. Quindi le colonne sono identificate con i numeri

0, 1, ..., m-1. Il nome classe-resto modulo m, sta a significare che nella colonna indicata con r vi sono tutti e soli i numeri che divisi per il modulo m danno per resto proprio r. Così si ha:

3 = 4.5+2 = h.5+2 (mod 5), 2 = 8 = 2h = 0 (mod 2).

È del tutto naturale definire la somma e il prodotto di due colonne nel modo seguente:

col a + col b = col (a+b), col a. col b = col (a.b)

così per ogni modulo m fissato si hanno diverse tabelle di operazioni facilmente costruibili. Inoltre, per abuso di linguaggio, scriveremo semplicemente a+b ed a.b in luogo di col a + col b ovvero di col a.col b.

La struttura algebrica delle classi-resto modulo m è dunque una struttura con due operazioni, che si indica con Z(m). Si dimostra in Algebra che Z(m) è un campo se e solo se l'intero m è un numero primo. Nel caso che m = h.k (h,k diversi da 1) si ha in termini di Z(m) che h.k = col m = col 0 = 0, cioè sono presenti i famigerati divisori dello zero, a differenza di quanto accade nei campi. Segue allora che un qualsiasi campo finito GF(p) d'ordine primo p coincide con Z(p). Un concreto esempio di campo è ad esempio GF(5), nel quale si ha ad esempio

3+2 = 0 (mod 5) cioè -5=-2 (mod 5),
3*2 = .5+1 = 1 (mod 5) cioè 3=1/2 (mod 5).

Sappiamo dunque costruire e lavorare con tutti i campi aventi per ordine un numero primo. Non è semplice illustrare la costruzione generale di un modello di campo avente per ordine una potenza di un primo. Presentiamo per prima cosa tre esempi.

Vogliamo costruire GF(9). Prendiamo Z(3) = GF(3) formato dalle colonne 0,1,2 e dalle tabelle di operazione:

1+0=2+2=1, 1+1=2+0=2, 0+0=2+2=0, 1.2=2, 2.2=1.1=1.

In Z(3) l'equazione $x^2+1 = 0$ (in analogia a quanto accade nel passaggio dal campo reale a quello complesso) è priva di soluzioni, essendo non nulli ciascuno dei tre numeri 0*0+1, 1*1+1, 2*2+1. Consideriamo ora i binomi formali del tipo a+ib dove a,b variano in Z(3) ed i è una "soluzione inventata" dell'equazione fissata. Sappiamo sommare due binomi e li sappiamo moltiplicare purché al posto del quadrato di i si metta -1 cioè 2 nel nostro caso (Da 3=0 segue 2 = -1). Ad esempio si ha:(2+i)+(2+2i)=(1+i).(1+2i)=1+4=2, i(1+i)=2+i.

L'insieme dei binomi con le due operazioni è una descrizione di GF(9). Volendo posso cambiare l'equazione irriducibile (ad esempio posso prendere $2x^2+x+1$) e se cambio l'equazione cambia la

rappresentazione del campo, ma i campi ottenuti sono isomorfi e ho sempre GF(9), a meno di isomorfismi.

Costruiamo ora GF(4). In GF(2) consideriamo l'equazione irriducibile $x^2+x+1 = 0$ (in questo caso l'equazione $x^2+1 = 0$ non si può usare perché è riducibile) Gli elementi di GF(4) sono allora 0, 1, i, i+1 e, ad esempio, si ha: i(i+1)=1.

Analogamente possiamo costruire GF(27) dall'equazione cubica $x^3+2x+1=0$, priva di soluzioni essendo 0.0.0+2.0+1=1.1.1+2.1+1=2.2.2+2.2+1 = 0. Gli elementi di GF(27) sono i trinomi del tipo $ai^2+bi+c$ ove a,b,c variano in Z(3), l'addizione di trinomi è quella usuale e al posto di i-cubo si sostituisce -2i-1 ovvero i+2.

Ancora è utile esercizio costruire GF(16) ricorrendo all'equazione $x^4=x+1$ e prendendo come "elementi" i polinomi di terzo grado.

L'idea generale è ora chiara. A partire da GF(p) si può prendere una equazione irriducibile di grado n mediante la quale si calcolano le potenze n-me di una indeteminata. Gli elementi dell'ampliamento sono allora i polinomi di grado n-1 nella indeterminata; essi si calcolano mod p e per le potenze si usa la riduzione mediante il polinomio prefissato. La struttura che si ottiene è un campo di ordine "p *alla* n" isomorfo ad ogni campo dello stesso ordine.

Nei campi finiti si possono introdurre idee classiche in modo a volte non atteso. Una di queste idee è l'idea del *logaritmo discreto* così interessante ad esempio a fini applicativi. Per introdurre il concetto occorre sapere che, come si dimostra, in un qualsiasi campo finito esistono degli elementi, detti *generatori,* che hanno la proprieta seguente:

se a è un generatore di GF(q) allora le potenze di a prima, seconda, terza,..., fino alla (q-2)-ma sono tutte distinte e riproducono l'intero insieme degli elementi non nulli, la potenza (q-1)-ma è ancora 1 e così via.

Se allora l'elemento a è un fissato generatore di GF(q) ed n è un intero positivo incognito segue, da quanto detto sopra, che l'equazione

$$a^n = b$$

essendo b fissato in modo arbitrario (non nullo) in GF(q), ha esattamente una soluzione. Tale intero n prende il nome di logaritmo discreto in base a dell'elemento b. La nozione si presenta di importanza notevole nel problema della trasmissione pubblica di chiavi segrete e che tali devono restare. Presentiamo un esempio. In GF(7) l'elemento 3 è generatore in quanto:

$$3^1= 3, \quad 3^2= 2, \quad 3^3= 6, \quad 3^4= 4, \quad 3^5= 5, \qquad 3^6= 1 \ .....$$

Segue che l'equazione $3^x = b$, con b elemento non nullo di GF(7),ha esattamente una soluzione (ad esempio dall'esame delle potenze segue che b=5 implica x = 5 mentre b=6 implica x=3), e quindi si ha: $\log_3 5= 5$ ed anche $\log_3 6 = 3$. Naturalmente se q è "piccolo", a tentativi si elencano tutte le potenze di tutti i generatori ed il logaritmo si trova sempre. Se q è molto, molto grande, si è di fronte ad una funzione unidirezionale, cioè di semplice calcolo in un verso (calcolo delle potenze) ed impraticabile inversione (calcolo del logaritmo discreto).

A partire da questi campi costruiamo ora le geometrie finite.

Anche ora conviene procedere per gradi. Abbiamo introdotto un modello di piano affine desarguesiano su GF(q) nel quale si opera come nella ordinaria geometria analitica, ad esempio è possibile trovare il punto comune di due rette risolvendo i corrispondenti sistemi, anche con il metodo di Cramer. Di fatto tutta la teoria delle matrici e dei sistemi lineari, come è ben noto, sussiste del tutto inalterata sopra in un qualsiasi campo. Possiamo introdurre la nozione di piano proiettivo di Galois. Un piano proiettivo su un campo di Galois d'ordine q, in simboli PG(2,q), ha come insieme dei punti tutte le possibili terne ordinate (x,y,t), con x,y,t elementi di GF(q), tali che:

a) le terne sono composte da elementi non tutti nulli;

b) terne proporzionali si riguardano come identiche.

Se t non è nullo il punto si dice proprio ed ad esso si attribuiscono coordinate "cartesiane-affini" X=x/t, Y=y/t, in accordo con il fatto che terne proporzionali sono lo "stesso punto". Se t=0, il punto (a,b,0) si dice un punto improprio ed ad esso si associano tutte le rette affini del tipo bX-aY+c=0.

Definiamo le "rette" nel piano proiettivo come gli insiemi di punti le cui coordinate omogenee sono soluzione di una equazione a coefficienti in GF(q), del tipo:

$$ax+by+ct = 0, \quad \text{con a,b,c non tutti nulli.}$$

Se a,b sono nulli si ha la retta impropria t=0, che è il luogo dei punti impropri ovvero delle q+1 direzioni del piano affine. Se a,b non sono entrambi nulli, si ha sulla retta il punto (b,-a,0) e tutti i q

punti della retta affine aX+bY+c=0. In totale dunque una retta proiettiva ha q+1 punti: precisamente i q punti della retta affine sottogiacente ed in più il punto improprio. Ci sono q+1 rette per un punto ci sono $q^2+q+1$ punti nel piano ed altrettante rette. Inoltre è possibile, come nel caso reale, ampliare un piano affine in un piano proiettivo utilizzando le direzioni e viceversa costruire all'interno di un piano proiettivo una struttura di piano affine fissando in esso "la retta impropria" e chiamando "parallele" due rette che si incontrino sulla speciale retta scelta. "Mutatis mutandis" tutto torna. Si possono definire ovviamente strutture più dimensionali, ma questo esula dai nostri scopi.

## BIBLIOGRAFIA


[1] L. BERARDI-M. DI FONSO-F. EUGENI, *Threshold schemes based on criss-cross block design*, J. of Information & Opti. Sci., 1 (1990), pp.153-160.

[2] L. BERARDI-F. EUGENI-S. INNAMORATI, *Generalized Designs, hypergroupoids and algebraic cryptography*, Proçeedings of the Fourth International Conference AHA, Kanthi, Grece, 1990, pp. 55-66.

[3] L. BERARDI-B. RIZZI, *Generalizziamo il codice RSA e la funzione di Eulero,* Atti I Simposio internazionale *"Stato e prospettive della ricerca crittografica in Italia"*, Roma, Fondazion Bordoni,1987.

[4] L. BERARDI-A. BEUTELSPACHER, *I buoni angeli custodi,ovvero i protettori di un messaggio,* Archimede, 2/3 (1989), pp. 129-140.

[5] A. BEUTELSPACHER, *Enciphered Geometry-.Some applications of Geometry to Crypto-graphy,* Annals of Discrete Math., 37 (1988), pp. 59-68.

[6] A. BEUTELSPACHER, *Perfect and essentially perfect authentication systems,* Eurocrypto '87, pp. 167-170.

[7] A. BICHARA, *Elementary proof of non-existence of the plane of order six,* Mitteilungen Sem. Math. Uni. Giessen, (1987), pp. 1-6.

[8] G.R. BLAKLEY, *Safeguarding criptographic keys,* Proc., NCC, AFIPS Press Montvale, N.J, 48 (1979), pp. 313-317.

[9] P. H. BRUCK- H. J. RYSER, *The non existence of certain finite projective planes*, Canad. J. Math., 1 (1949) pp. 88-93.

[10] M. CERASOLI-F. EUGENI-M. PROTASI, *Elementi di Matematica Discreta*, Zanichelli, Bologna, 1988.

[11] F. N. COLE-L. D. CUMMUNGS and H. S. WHITE, *The complete enumeration of triad systems in 15 elements*, PROC. NAT. ACAD. SCI. U.S.A., 3 (1917), pp. 197-199.

[12] B.K. DASS-F. EUGENI, *How to share secrets: the idea of geometric threshold games*, J. of Information & Opti. Sci., 3 (1991), pp. 451-458.

[13] P. DEMBOWSKI, *Finite geometries*, Springer Verlag, 1968.

[14] F. EUGENI-A. MATURO, *A new authentication code based on generalized affine planes*, J. of Information & Opti. Sci., 1 (1992), pp. 53-60.

[15] F. EUGENI, *Combinatorics and cryptography*, Annals of Discrete Math., 52 (1992), pp. 159-174 - Proceedigs of International Conference "Combinatorics '90".

[16] E.N. GILBERT-F.J. MC WILLIAMS-N.J. SLOANE, *Codes which detect deception*, Bell Syst.Tech.J., 53 (1974), pp. 405-424.

[17] M. GIONFRIDDO-F. EUGENI, *On the minimum number of blocks of a maximal partial spread in STS(v) and SQS(v)*, J.Geometry, 2 (1990), pp. 12-20.

[18] H. B. MANN, *On the construction of sets orthogonal latin sequences*, Ann. Math. Stat., 14 (1943), pp. 401-414.

[19] G.C. ROTA, *Analisi combinatoria*, in *Le scienze matematiche*, Zanichelli ed., Bologna, 1973, pp. 226-238.

[20] B. SEGRE, *Lectures on modern geometry*, Cremonese; 1961.

[21] A. SGARRO, *Crittografia,* Muzzio, Padova, 1986.

[22] A. SHAMIR, *How to share a secret*, Communications ACM, 11 (1979), pp. 612-613.

[23] G. TALLINI, *Strutture grafiche proiettive*, Liguori Napoli, 1973.

[24] G. TARRY, *Le probleme des 36 officiers*, C.R. Ass. France Av.Sci., 1 (1900), pp. 122-123 e 2 (1901), pp. 170-203...

[25] M. TALLINI SCAFATI, *Strutture di incidenza e piani affini*, Liguori Napoli, 1971.