UNIVERSITÀ DEGLI STUDI ROMA TRE

FACOLTÀ DI SCIENZE M.F.N.

Sintesi della tesi di Laurea in Matematica

di

Alessia Compagnucci

Piani proiettivi finiti e quadrati latini

Relatore

Prof. Andrea Bruno

Il Candidato

Il Relatore

ANNO ACCADEMICO 2003 - 2004

Luglio 2004

Classificazione AMS : O5B15, 050651Exx, O5B25

Parole Chiave : Piani proiettivi finiti, quadrati latini, codici.

L'oggetto principale di questa tesi è quello dei quadrati latini. Un quadrato latino è una matrice $n \times n$ i cui elementi sono n simboli tali che ognuno di essi compare esattamente una volta su ogni riga e su ogni colonna. Si usano di solito come simboli gli interi da $1, \ldots, n$. Tali entità matematiche, introdotte da Eulero nel XVIII secolo, sono legati in modo diretto a vari problemi inerenti a campi molto lontani da quello della geometria combinatoria, cui i quadrati latini appartengono.

La problematica principale è l'esistenza e la classificazione di quadrati latini ortogonali tra loro e nasce con il cosiddetto 'problema dei 36 ufficiali', formulato da Eulero stesso e che si enuncia come segue: sistemare 36 ufficiali, 6 da ognuno dei 6 reggimenti, di 6 gradi differenti in un quadrato 6×6, in modo tale che ogni riga e ogni colonna contenga un ufficiale di ogni rango ed uno di ogni reggimento. Come spiegheremo in seguito, tale problema si può generalizzare a quadrati latini di ogni ordine e solo all'inizio del XX secolo ha trovato completa soluzione. Si conoscono, cioè tutti e soli n per cui vale l'asserto.

Un primo contesto fertile alle applicazioni della teoria dei quadrati latini è quello algebrico. Essi sono, infatti, legati a strutture algebriche più devoli di quelle classiche, come semigruppi e loop; un quadrato latino risulta essere la tavola delle moltiplicazioni di un semigruppo ed in tale contesto che si riformula la congettura di Eulero.

Un secondo ambito di applicazioni è quello geometrico, in cui per geometria si intende lo studio delle proprietà di piani proiettivi finiti. In particolare, l'esistenza di siffatti piani di ordine n è intimamente legata all'esistenza di quadrati latini ortogonali e dunque la congettura di Eulero ha ricadute immediate in questo campo.

Un ulteriore e più recente applicazione dei quadrati latini è la teoria dei codici: essi intervengono, infatti, nello sviluppo di codici di correzione nella trasmissione attraverso un canale rumoroso.

Più in dettaglio la tesi è così organizzata.

Nel primo capitolo introduciamo un concetto più generale di quello usuale di piano proiettivo. Per noi

Definizione 1 *Un* piano proiettivo Π *è una terna ($\mathcal{P}$, L, **I**) dove $\mathcal{P}$ è un insieme i cui elementi sono chiamati* punti*, L è un insieme i cui elementi sono detti* rette *ed* ***I*** *è una relazione tra punti e rette chiamata* incidenza *che definiamo come segue: se $A \in \mathcal{P}$ e $m \in L$ diremo che A è incidente ad m, e scriveremo* A **I** m*; in pratica il punto A è sulla retta m e la retta m passa per il punto A. La terna così definita è tale che:*

P_1) *Ogni coppia di punti distinti è incidente in un'unica retta.*

P_2) *Ogni coppia di rette distinte è incidente in un unico punto.*

P_3) *Esistono 4 punti a 3 a 3 non incidenti con la stessa retta.*

Nel XIX secolo i matematici si interessarono largamente ai problemi riguardanti i fondamenti della matematica. Si occuparono di molte discipline per esaminare e rafforzare le basi assiomatiche. Una di queste discipline fu la geometria, che raggiunse il suo culmine nella prima parte del secolo. L'esistenza di geometrie non euclidee aveva scosso la credenza che il sistema assiomatico della geometria fosse irreprensibile. Nel riesaminare gli argomenti di base, G. Fano si interrogò su quale degli assiomi implicasse l'esistenza di un numero infinito di punti su una retta. Con sua grande sorpresa, si accorse che non potesse essere dedotto da nessuno degli assiomi esistenti e che se ne sarebbe dovuto creare uno ulteriore. Fu in grado di mostrarlo fornendo esempi di sistemi soddisfacenti tutti gli assiomi ma che non avevano un numero finito di punti su una retta. Fu così che nacquero le Geometrie Finite.

Tale sistema di assiomi, che ovviamente riprende quello classico degli spazi proiettvi come insiemi di rette di uno spazio affine banale, è quello in cui i lavori di Fano trovano naturale collocazione.

Mentre la geometria euclidea è caratterizzata dalla relazione di parallelismo tra rette, in quella proiettiva tale nozione decade lasciando il posto a quella di incidenza. Abbiamo quindi il seguente teorema che caratterizza i piani proiettivi finiti

Teorema 1 *Se una retta di un piano proiettivo finito è incidente solo in un numero finito di punti, ad esempio* $n + 1$*, allora:*

a) ogni retta è incidente in $n + 1$ *punti*

b) ogni punto è incidente in $n + 1$ *rette*

c) ci sono $n^2 + n + 1$ *punti in* $\mathcal{P}$

d) ci sono $n^2 + n + 1$ *rette in* L*.*

Due teoremi fondamentali sono quelli di Pappo-Pascal e Desargues, di cui risulta particolarmente utile alla trattazione una loro caratterizzazione in termini più algebrici. Diremo infatti che un piano proiettivo è *desarguesiano* se per esso vale il teorema di Desargues e che un piano proiettivo è *pappiano* se per esso vale il teorema di Pappo. Si ha

Proposizione 1

1. *Un piano proiettivo è pappiano se e soltanto se è coordinabile a destra su un campo.*

2. *Un piano proiettivo è desarguesiano se e soltanto se è coordinabile a destra su un corpo.*

Nel caso $\mathbb{K}$ sia un corpo finito, un teorema di Wedderburn assicura che $\mathbb{K}$ è un campo e, di conseguenza, otteniamo che un piano proiettivo finito è desarguesiano se, e solo se, è pappiano.

Nel secondo capitolo studieremo le caratteristiche dei quadrati latini. Ne vedremo proprietà e principali teoremi, soffermandoci in particolare sul concetto di quadrati latini ortogonali, importantissimi per l'applicazione alla geometria finita. Abbiamo visto che un quadrato latino è una matrice $n \times n$ i cui elementi sono n simboli tali che ognuno di essi compare esattamente una volta su ogni riga e su ogni colonna. Si usano di solito come simboli gli interi da $1, \ldots, n$.

Esempio:

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}$$

I primi tre esempi seguono lo stesso schema; ogni riga è determinata permutando ciclicamente la colonna precedente a destra. Due quadrati latini si dicono **isotopici** se possono essere ottenuti uno dall'altro mediante una delle seguenti operazioni:

1. Permutazione delle righe
2. Permutazione delle colonne

L'isotopia è una relazione di equivalenza.

Introducendo, ora, particolari strutture algebriche, vogliamo applicare il concetto di qudarto latino appena introdotto.

Definizione 2 *Un* **semigruppo** (S,$\otimes$) *è un insieme S con una operazione binaria ($\otimes$) tale che:*

1. *L'operazione è chiusa, cioè: $a \otimes b \in S$, $\forall$ a,$b \in S$.*
2. *Dati a,$b \in S$, le equazioni*
   - $a \otimes x = b$
   - $y \otimes a = b$

   hanno un'unica soluzione per ogni x e y.

Esempio Un esempio semplice di semigruppo finito è l'insieme $\{0, 1, 2\}$ con l'operazione $\otimes$ definita da:

$$a \otimes b = 2a + b + 1$$

dove le addizioni e le moltiplicazioni sono le usuali operazioni modulo 3. La tavola delle moltiplicazioni è quindi:

$(\otimes)$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

Definizione 3 *Un* **loop** *è un semigruppo* (S,$\otimes$) *che ha un elemento neutro, cioè tale che esiste un elemento $e \in S$ tale che:*

$$e \otimes x = x \otimes e = x \qquad con\ x \in S.$$

Un loop è un gruppo non associativo. In un gruppo, l'equazione ax = b può essere risolta utilizzando gli assiomi di definizione del gruppo e si può dimostrare che la soluzione è unica ed è data da: $x = a^{-1}b$. In un loop sappiamo sempre che questa equazione ha una soluzione, ma non quale sia e come trovarla in generale. Per cui vediamo il seguente risultato:

Teorema 2 *La tavola delle moltiplicazioni di un semigruppo è un quadrato latino.*

L'associazione tra il semigruppo e il quadrato latino non è unica. Gli elementi presenti sui bordi della tavola delle moltiplicazioni del semigruppo possono essere disposti in ogni ordine. Quindi lo stesso semigruppo può dar luogo a quadrati latini diversi, che però saranno isotopici.

Ma molti dei problemi inerenti quadrati latini si basano sul concetto di *ortogonalità*, di cui vediamo ora più in dettaglio la definizione e le proprietà.

Definizione 4 *Due quadrati latini $L_1 = |a_{ij}|$ e $L_2 = |b_{ij}|$ si dicono* ortogonali *se ogni coppia ordinata di simboli compare esattamente una volta tra le n^2 coppie (a_{ij}, b_{ij}), dove $i = 1, 2, \ldots, n$ e $j = 1, 2, \ldots, n$.*

Esempio: Consideriamo due quadrati latini di ordine 3. 'Sovrapponendo' i due quadrati ne otteniamo un terzo i cui elementi sono tutti distinti. I due quadrati si dicono quindi ortogonali.

$$\begin{array}{ccc} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{array} \qquad \begin{array}{ccc} 2,2 & 3,1 & 1,3 \\ 1,1 & 2,3 & 3,2 \\ 3,3 & 1,2 & 2,1 \end{array}$$

I quadrati ortogonali si dicono a volte *complementi ortogonali* l'uno dell'altro. Dalla teoria dei quadrati latini unitamente alla teoria dei gruppi otteniamo la seguente

Proposizione 2 *Esiste una coppia di quadrati latini ortogonali per ogni ordine dispari.*

La questione riguardante l'esistenza di coppie di quadrati latini di ordine pari è molto più difficile da sistemare ed ha una storia famosa. Questo problema è stato inizialmente affrontato da Eulero ed è noto come il 'Problema dei 36 ufficiali. Eulero lo formulò come segue nel 1779: sistemare 36 ufficiali, 6 da ognuno dei 6 reggimenti, di 6 gradi differenti in un quadrato 6×6, in modo tale che ogni riga e ogni colonna contenga un ufficiale di ogni rango ed uno di ogni reggimento. E' ovvio che la soluzione si otterrebbe trovando una coppia di quadrati latini ortogonali. Già Eulero tentò di risolvere il problema in questa maniera, ma fu incapace sia di trovare tale coppia sia di dimostrarne la non esistenza. Fece quindi la seguente congettura:

CONGETTURA DI EULERO

Non esistono quadrati latini ortogonali di ordine $n = 4k+2$, con $k \in \mathbb{Z}_+$.
Solo 120 anni dopo Eulero, Tarry nel 1900 dimostrò l'irrisolubilità del problema dei 36 ufficiali. Egli utilizzò il metodo empirico: scrisse cioè gli 812 851 200 quadrati latini 6×6 e esaminandoli a due a due si accorse che non vi erano complementi ortogonali. Osserviamo che ora, lavorando con i quadrati ridotti basterebbe esaminarne 'solo' 9408 coppie.

Teorema 3 *Per ogni $n \neq 2$ e $n \neq 6$ esiste una coppia di quadrati latini ortogonali di ordine n.*

Un insieme di quadrati latini dello stesso ordine ciascuno dei quali è complemento ortogonale degli altri si dice insieme di *quadrati latini mutuamente ortogonali (MOLS)*. Sia $N(n)$ il massimo numero di MOLS di ordine n.

Teorema 4 *Esistono al più n-1 MOLS di ordine n.*

Tutto il lavoro dei ricercatori è stato rivolto alla ricerca di altri valori per la funzione $N(n)$, ma la questione è immensa e non completamente risolubile con i metodi tutt'ora noti. Ci limitiamo quindi a darne un estremo inferiore, essendo quello superiore $n - 1$. Una buona approssimazione è stata data da MacNeish nel 1920, e si basava sulla costruzione che vedremo nel seguente

Teorema 5 (MacNeish – 1922) *Supponiamo esistano r MOLS di ordine n e r MOLS di ordine m, allora esistono r MOLS di ordine mn.*

Nel terzo capitolo affronteremo la relazione che intercorre tra quadrati latini ortogonali e piani proiettivi finiti. Attorno al problema di determinare per quali valori di n esistano insiemi di $n-1$ quadrati latini mutuamente ortogonali gravitano alcuni importanti fatti noti. Il problema di Veblen ha messo in luce come un piano proiettivo finito di ordine n è equivalente ad un insieme di $n-1$ MOLS. Inoltre, è noto che se n è un numero primo o potenza di un numero primo, allora si può costruire un piano proiettivo di ordine n. Possiamo, quindi, definire il *piano di Galois* e dimostrarne l'esistenza. Tutto ciò ci permette di dimostrare il teorema di Bruck–Ryser sull'esistenza di piani proiettivi di ordine n, che non sia necessariamente potenza di un numero primo p.

Teorema 6 (Bruck-Ryser) *Se $n \equiv 1 \ (mod 4)$ oppure $n \equiv 2 \ (mod 4)$ allora un piano proiettivo di ordine n non esiste a meno che n non sia tale che: $n = a^2 + b^2$.*

Tale teorema implica la non esistenza di piani proiettivi di ordine 6, risultato ottenuto anche nel secondo capitolo utilizzando il MOLS. Ora, un piano di Galois è desarguesiano, poiché in esso vale la configurazione del teorema di Desargues. Un esempio semplice di piano desarguesiano è il piano di traslazione. Notiamo che ogni campo di Galois è un corpo destro. Se un corpo destro è anche un campo di Galois, possiamo introdurre coordinate omogenee in modo elementare; risulta quindi che il piano associato è isomorfo ad un piano di Galois dello stesso ordine. Possiamo quindi dedurre che l'esistenza di piani di traslazione finiti che siano geometricamente distinti dai piani di Galois, dipende dall'esistenza di quasi–campi destri che non siano dei campi. Possiamo quindi definire il *sistema di Veblen-Wedderburn* come segue

Definizione 5 *Sia F un campo commutativo dato e sia $f(x) = x^2 - rx - s,\ r, s \in F$ un polinomio irriducibile su F. Allora l'insieme degli elementi*

$a = a_1 + ua_2,\ a_1, a_2 \in F$ *è un sistema di Veblen-Wedderburn J con le seguenti condizioni per addizione e moltiplicazione:*

1) $(a_1 + ua_2) + (b_1 + ub_2) = (a_1 + b_1) + u(a_2 + b_2)$

2) $(a_1 + ua_2)b_1 = a_1b_1 + ua_2b_1$

3) $(a_1 + ua_2)(b_1 + ub_2) = sA_2 + b(A_1 + rA_2)$
dove $A_1 = a_1 - a_2b_1b_2^{-1},\ A_2 = a_2b_2^{-1}$ *avendo posto* $b_2 \neq 0,\ b = b_1 + ub_2,$
$a = a_1 + ua_2 = A_1 + bA_2.$
Si ha:
$(a_1+ua_2)(b_1+ub_2)sa_2b_2^{-1}+a_1b_1-a_2b_1^2b_2^{-1}+ra_2b_1b_2^{-1}+u(a_1b_2-a_2b_1+ra_2).$

Il più piccolo ordine per cui la costruzione precedente dà luogo ad un corpo destro che non è un campo è 9.

Una *struttura di incidenza* è una terna $\Delta\,(A, B, I)$, dove A e B sono due insiemi di punti e rette rispettivamente. I è un sottoinsieme di $A \times B$ detto *relazione incidenza.* In altre parole, la relazione significa che presa una retta ℓ, un punto $p \in \ell$, cioè:

$$I = \{p \in A : (p, \ell) \in I, \text{con } \ell \in B\} \ \subseteq A \times B.$$

Tale definizione ci permette di legare intimamente gli insiemi completi di MOLS con i piani proiettivi con il seguente

Teorema 7 *Condizione necessaria e sufficiente affinché, in un insieme completo di MOLS in forma standard, le righe del quadrato* L_k *siano le stesse del quadrato* L_h *a meno dell'ordine è che il quadrato rappresenti la struttura di incidenza di un piano proiettivo in cui valga il primo teorema minore di Desargues.*

Mostrando la connessione tra reti e geometriche e quadrati latini, si osserva che le 'rette' nella definizione che segue possono essere curve del piano reale nelle applicazioni alla geometria proiettiva.

Definizione 6 *Una* rete geometrica *è un insieme di oggetti chiamati* punti *e di sottoinsiemi chiamati* rette*. Le rette si raccolgono in* classi di parallelismo *in modo tale che:*

(a) ogni punto corrisponde esattamente una retta di ciascuna classe di parallelismo;

(b) se ℓ_1 e ℓ_2 sono rette di differenti classi di parallelismo, allora ℓ_1 e ℓ_2 hanno esattamente un punto in comune;

(c) esistono al meno 3 classi di parallelismo e almeno due punti su una retta.

Un insieme che ha k classi di parallelismo si chiama k-rete.

Si ha quindi il seguente risultato

Teorema 8 *Un piano affine è una rete geometrica in cui ogni coppia di punti è incidente in una retta.*

Equivalentemente, diremo che un piano affine di ordine n è una rete di ordine n con n+1 classi di parallelismo.

Nel quarto e ultimo capitolo di questo lavoro abbiamo voluto vedere quali siano le applicazioni pratiche di quanto studiato. Si è dunque visto che esistono strette connessioni tra quadrati latini, piani proiettivi e teoria dei grafi, ma che tutto ciò sfocia in maniera naturale nella teoria dei codici. Ora

Definizione 7 *Una matrice si dice* matrice canonica di incidenza *per un piano proiettivo* π *se soddisfa le seguenti proprietà:*

i) *le matrici* C_{1j} *e* C_{i1} $(i, j = 1, 2, \ldots, n)$ *sono matrici identità* $n \times n$

ii) C_{ij} *con* $i, j > 1$ *non contengono elementi 1 sulla diagonale principale*

iii) *le k–esime righe di* C_{is} *e* C_{cr}*, per* $s \neq r$ *e* $i > 1$*, sono distinte*

iv) *le k–esime righe di* C_{is} *e* C_{cr}*, per* $s \neq r$ *e* $i > 1$*, non possono essere simultaneamente uguali alle p–esime righe di* C_{ms} *e* C_{mr} *per ogni* p *e per* $m \neq i > 1$

La matrice C_{ij} prende il nome di *nucleo* della matrice di incidenza. Da una matrice canonica possiamo costruire una matrice D_{i-1} con $i = 1, 2, \ldots, n$, definendo

$$D_{(i-1),j} = C_{ij}(1\ 2\ \ldots\ n)^T \qquad \text{per } j = 1, 2, \ldots, n.$$

D_{i-1} è un quadrato latino di ordine $n - 1$. In generale, tali quadrati non saranno ortogonali, ma godranno sempre della seguente proprietà:

v) *per ogni coppia di colonne data, ad esempio* r *e* s *con* $r \neq s$*, le* $n(n-1)$ *coppie di numeri* (h, k)*, ottenute prendendo gli elementi che compaiono in tali colonne per ciascuna riga degli* $n - 1$ *quadrati latini, sono tutte distinte e la coppia* (h, h) *non compare tra di essi.*

Le coppie di numeri definite nella proprietà v) prendono il nome di *grafi orientati*. Dato un insieme di $n-1$ quadrati latini che posseggano la proprietà v), possiamo riordinare le colonne di ciascuno separatamente in modo che su ogni prima colonna vi siano $1, 2, \ldots, n$ nell'ordine naturale. Un siffatto insieme prende il nome di *insieme completo di grafi orientati.* Si ha quindi il seguente risultato

Teorema 9 *Condizione necessaria e sufficiente per l'esistenza di un piano proiettivo con n^2+n+1 punti e rette è che esista un grafo orientato completo di quadrati latini.*

Supponiamo ora di voler trasmettere una sequenza, $a_1, a_2, \ldots$, attraverso un canale disturbato: ad esempio un canale telegrafico. Il rumore sul canale potrebbe causare la trasmissione errata del dato a_i, con risultato che il messaggio risulterebbe differente da quello trasmesso. Non è possibile prevenire tali errori, ma si possono inserire degli elementi di controllo al fine di ridurre gli effetti indesiderati della trasmissione del codice. Diremo *alfabeto* con q lettere un qualsiasi insieme finito, $\mathbb{A}_q$, costituito da q elementi, detti *lettere.* Se, ad esempio, $\mathbb{A}_2 = \{0, 1\} = \mathbb{Z}_2$ si avrà un *alfabeto binario.* Risulta

$$\left|\mathbb{A}_q^n\right| = q^n$$

Ogni elemento $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ si dirà *parola con n lettere.* Un codice costruito con q elementi, $0, 1, 2, \ldots, q-1$, si dice *codice q–ario.* Nella rappresentazione del codice nello spazio vettoriale, il campo $\mathbb{K}$ risulta essere un campo di Galois con q elementi.

Per poter capire meglio la ricerca dell'errore, dobbiamo introdurre il concetto di *distanza di Hamming* tra due parole. Definiamo quindi tale distanza $d(\mathbf{a}, \mathbf{b})$ come il numero di 'posti' per cui i due elementi differiscono, cioè il numero degli indici per cui risulti $a_i \neq b_i$. Essa gode delle proprietà che caratterizzano le funzioni distanza:

- $d(\mathbf{a}, \mathbf{a}) = 0$

- $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{b}, \mathbf{a})$

- $d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) \geq d(\mathbf{a}, \mathbf{c})$

Interrogandosi su quale fosse il massimo numero di parole in un codice le cui parole hanno n elementi e distanza minima uguale a d, D.D. Joshi ha mostrato che il massimo è minore o uguale a q^{n-d+1} (dove q è il numero delle lettere dell'alfabeto usato). Tale massimo prende il nome di *limite di Joshi*. Si ha

Teorema 10 *Se $n \leq q + 1$ e $d = n - 1$ oppure se $n \leq q$ e $d = n$, il limite di Joshi può sempre essere ottenuto se q è l'ordine di un piano proiettivo finito.*

Bibliografia

[1] R.C. Bose, S.S. Shrikhande, E.T. Parker *Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler's Conjecture*, Canadian Journal of Mathematics, 12(1960), 189-203.

[2] R.C. Bose, S.S. Shrikhande *On the Construction of Sets of Mutually Orthogonal Latin Squares and Falsity of a Conjecture of Euler*, Transactions of the American Mathematical Society, 95(1960), 191-209.

[3] R.C. Bose, S.S. Shrikhande *On the Falsity of Euler's Conjecture About the Non-existence of Two Orthogonal Latin Squares of Order 4t + 2*, Proceedings of the National Academy of Science, 45(1959), pp. 734-737.

[4] B. Cherowitzo *Lecture notes of the graduate course I*, University of Colorado at Denver, 2003.

[5] J. Denes e A.D. Keedwell *Latin Squares and Their Applications*, Academic Press, New York, 1974.

[6] R. Hartshorne, *Foundations of Projective Geometry*, Benjamin Press, 1967.

[7] Hughes, Piper, *Projective Planes*, Springer-Verlag, New York, 1973.

[8] Hughes, *A class of non desarguesian projective planes*, Canadian Journal of Mathematics, 9(1957), 378–388.

[9] Z. Lie, *A Short Disproof of Euler's Conjecture Concerning Orthogonal Latin Squares*, Ars Combinatoria, 14(1982), pp. 47–55.

[10] F. Mazzocca *Appunti del corso di Geometria superiore*, Seconda Università degli studi di Napoli, 2003.

[11] Maria Scafati, Giuseppe Tallini *Geometria di Galois e teoria dei codici*, C.I.S.U., Roma, 1995.

[12] E. Sernesi, *Geometria 1*, Bollati Boringhieri, 1989.

[13] I. Stewart *Galois Theory*, Chapman and Hall, 1989.

[14] I.N. Stewart e D.O. Tall *Algebric Number Theory*, Chapman and Hall, 1987, pp. 154-156.

[15] D.R. Stinson, *A short proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six*, Journal of Combinatorial Theory, Series A, 36(1984), pp. 373-376.

[16] G. Tarry, *Le problème des 36 officiers*, C.R. Assoc. France Av. Sci., 29 (1900) part 2,pp 170-203.