Appunti di geometria combinatoria

Giorgio Ragusa
gragusa@dmi.unict.it

1 Calcolo combinatorio

Dato un insieme A di n elementi, si chiamano *disposizioni di classe k* i suoi sottoinsiemi ordinati di k elementi. Se si ammette che gli elementi possano anche ripetersi si parla di disposizioni con ripetizione, altrimenti di disposizioni semplici. Le disposizioni semplici aventi $n = k$ si chiamano *permutazioni* semplici. Si chiama permutazione con ripetizione una permutazione di n elementi non tutti distinti. Si chiamano invece *combinazioni di classe k* i sottoinsiemi di A non ordinati di k elementi. Se si ammette che gli elementi possono anche ripetersi si parla di combinazioni con ripetizione, altrimenti di combinazioni semplici.

Teorema 1.1. *Dato un insieme di n elementi e detti rispettivamente $D_{n,k}$, $D^r_{n,k}$, $C_{n,k}$, $C^r_{n,k}$, P_n, $P^r_{n_1,n_2,\dots,n_k}$, le disposizioni semplici e con ripetizione, le combinazioni semplici e con ripetizione, le permutazioni semplici e con ripetizione, supponendo in quest'ultimo caso che l'insieme abbia n_i elementi indistinguibili per ogni $i \in \{1, 2, \dots, k\}$, si ha:*

1. $D_{n,k} = n(n-1)(n-2)\dots(n-k+1)$,
2. $D^r_{n,k} = n^k$,
3. $P_n = n!$,
4. $P^r_{n_1,n_2,\dots,n_k} = \frac{n!}{n_1!n_2!\dots n_k!}$,
5. $C_{n,k} = \frac{D_{n,k}}{P_k}$,
6. $C^r_{n,k} = C_{n+k-1,k}$.

Dimostrazione La prima si ottiene osservando che per formare una disposizione semplice di classe k occorre scegliere uno degli n elementi come primo elemento, poi uno dei rimanenti $n-1$ elementi come secondo e così via fino a scegliere dei $n-(k-1)$ elementi rimasti il k-esimo elemento. Analogamente si dimostra la seconda relazione ricordando che stavolta ciascuna delle k scelte si può fare in n modi. La terza è un caso particolare della prima. La quarta si ottiene dalla terza osservando che, considerata una disposizione di n elementi di cui n_1 indistingubili, se si permutano questi n_1 elementi si ottiene la stessa disposizione ed analogamente per $n_2, \dots, n_k$. La quinta si ottiene considerando che le disposizioni di classe k che contengono gli stessi elementi ma in un ordine diverso sono equivalenti come combinazioni ed il loro numero è proprio P_k. Per dimostrare l'ultima

uguaglianza possiamo supporre senza ledere la generalità che il nostro insieme sia l'insieme dei primi n numeri interi positivi e sempre senza ledere la generalità possiamo dire che le sue combinazioni con ripetizione di classe k sono tutte e sole le sue successioni non decrescenti di lunghezza k. Associando alla successione non decrescente $a_1, a_2, \ldots, a_k$ la successione crescente $a_1, a_2 + 1, a_3 + 2, \ldots, a_k + (k-1)$ si ottiene una corrispondenza biunivoca fra l'insieme delle combinazioni con ripetizione di n elementi di classe k e le combinazioni semplici di $n+k-1$ elementi di classe k e da ciò segue la loro equipotenza. □

Esempio 1.1. *In quanti modi si possono distribuire 4 caramelle identiche a due bambini distinguibili, contando anche i casi in cui un bambino resta senza caramelle?* Indicati con 1,2 i due bambini, il problema equivale a quello di contare le possibili successioni non decrescenti di lunghezza 4 ed elementi 1,2: 1111, 1112, 1122, 1222, 2222. A queste successioni l'applicazione definita nella dimostrazione del teorema precedente associa rispettivamente 1234, 1235, 1245, 1345, 2345, che sono tutte e sole le combinazioni semplici di classe 4 degli elementi $1, 2, 3, 4, 5$. Pertanto $C^r_{2,4} = C_{5,4} = \frac{D_{5,4}}{P_4} = \frac{5 \cdot 4}{4} = 5$.

2 Preliminari algebrici: campi finiti e quasigruppi

Un gruppo abeliano è una coppia $(G, +)$ formata da un insieme G ed una operazione binaria ad esso interna $+$ tale che:

1. $\forall a, b \in G, (a + b) + c = a + (b + c)$ (proprietà associativa);
2. $\forall a, b \in G, a + b = b + a$ (proprietà commutativa);
3. $\forall a \in G, \exists e \in G : a + e = a$ (esistenza dell'elemento neutro).
4. $\forall a \in G, \exists b \in G : a + b = e$ (esistenza dell'opposto).

Esempio 2.1. Per ogni $n > 0$ l'insieme delle classi di resto modulo n $\mathbb{Z}_n$ con la somma usuale è un gruppo abeliano finito.

Un campo è un terna $(C, +, \cdot)$ formata da un insieme C con due operazioni binarie ad esso interne $+$ e $\cdot$ tali che $(C, +)$ e $(C \backslash \{0\}, \cdot)$, con 0 elemento neutro dell'operazione $+$, sono gruppi abeliani e le due operazioni sono legate dalla proprietà distributiva: $\forall a, b, c, (a + b) \cdot c = a \cdot c + b \cdot c$.

Teorema 2.1. *Per ogni $q = p^h$, con p primo, esiste un campo GF(q) di ordine q.*

Dimostrazione Per $h = 1$ basta porre $GF(q) = \mathbb{Z}_p$, poiché per $(\mathbb{Z}_p, +, \cdot)$ sono valide tutte le proprietà dei campi. Se $h > 1$, sia $f(x) \in \mathbb{Z}_p[x]$ irriducibile di grado h e sia $GF(q) = \{g(x) \in \mathbb{Z}_p[x] : deg(g) < h\}$. E' ovvio che $|GF(q)| = p^h$ e che $GF(q)$ con la usuale somma di polinomi e il prodotto modulo $f(x)$ è un campo, poiché il fatto che $f(x)$ abbia grado h garantisce che l'operazione di prodotto sia interna e l'irriducibilità di $f(x)$ garantisce che quello ottenuto sia un dominio (anello senza divisori dello zero) e quindi essendo finito un campo. Infatti l'unica proprietà che resterebbe da provare è l'esistenza dell'inverso di ogni elemento non nullo rispetto al prodotto, visto che le altre sono ovvie. Sia allora $0 \neq a \in GF(q)$ e consideriamo gli elementi di $GF(q)$ $\{ag_1, ag_2, \ldots, ag_q\}$, essendo $GF(q) = \{g_1, g_2, \ldots, g_q\}$. Dal fatto che $GF(q)$ è un dominio si deduce che $ag_i = ag_j \Rightarrow$

$a(g_i - g_j) = 0 \Rightarrow g_i = g_j$ e quindi $GF(q) = \{ag_1, ag_2, \ldots, ag_q\}$. Allora esiste un indice i tale che $1 = ag_i$ e quindi g_i è l'inverso dell'elemento non nullo $a \in GF(q)$. □

Dall'algebra è noto che un campo finito ammette un elemento primitivo, cioè un elemento θ tale che $GF(q) = \{0, \theta, \theta^2, \ldots, \theta^{q-1} = 1\}$ e che, per $h > 1$, scegliendo opportunamente $f(x)$ è possibile fare in modo che esso sia il polinomio x. Quando ciò accade il polinomio $f(x)$ si dice primitivo, mentre per $h = 1$ un elemento primitivo si dice anche radice primitiva. La seguente tabella fornisce radici e polinomi primitivi per tutti i valori di $q < 10$.

q	radici e polinomi primitivi
3	2
4	$x^2 + x + 1$
5	2
7	3
8	$x^3 + x + 1$
9	$x^2 + 2x + 2$

Esempio 2.2. Sia $q = 4$, allora $GF(4) = \{0, x, x+1 = x^2, 1 = x^3\}$, scegliendo $f(x) = x^2 + x+1$, $\theta = x$. Si ottiene facilmente la seguente tabella moltiplicativa

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Teorema 2.2. *Se q è dispari, detto θ un elemento primitivo e Q l'insieme dei quadrati non nulli di $GF(q)$, allora:*

1. *Q èformato dalle potenze pari di θ;*
2. *$\theta^{\frac{q-1}{2}} = -1$;*
3. *$-1 \in Q$ se e solo se $q \equiv 1 \pmod 4$;*
4. *$Q = -Q$ se e solo se $q \equiv 1 \pmod 4$.*

Dimostrazione La prima proprietà è ovvia. La seconda segue dal fatto che $\theta^{q-1} - 1 = 0 \rightarrow (\theta^{\frac{q-1}{2}} - 1)(\theta^{\frac{q-1}{2}} + 1) = 0 \rightarrow \theta^{\frac{q-1}{2}} = -1$, poiché θ ha ordine $q - 1$. Da ciò segue che se $q = 4m + 1$ allora $\theta^{2m} = -1$, mentre se $q = 4m + 3$ allora $\theta^{2m+1} = -1$ e quindi la terza proprietà che implica la quarta, poiché $-x = (-1)x$. □

Esempio 2.3. In $\mathbb{Z}_5$, $Q = -Q = \{1, 4 = -1\}$, mentre in $\mathbb{Z}_7$ si ha $Q = \{1, 4, 2\}$, $-Q = \{6 = -1, 3, 5\}$.

Un quasigruppo $(A, \circ)$ è una coppia formata da un insieme A e da una operazione ad essa interna $\circ$ tale che le equazioni $a \circ x = b$ e $y \circ a = b$ abbiano una ed una sola soluzione per ogni coppia a, b di elementi di A. Un quasigruppo si dice commutativo se $a \circ b = b \circ a$ per ogni coppia a, b di elementi di A, si dice idempotente se $a \circ a = a$ per ogni a in A, si dice semi-idempotente se $A = \{a_1, a_2, \ldots, a_{2n}\}$ e se $a_i \circ a_i = a_i$ se $1 \leq i \leq n$, $a_j \circ a_j = a_{j-n}$ se $n + 1 \leq j \leq 2n$.

Teorema 2.3. *Per ogni n dispari esiste un quasigruppo commutativo idempotente di ordine n e per ogni n pari esiste un quasigruppo commutativo semi-idempotente di ordine n.*

Dimostrazione E' sufficiente rinominare opportunamente la tabella additiva di $(\mathbb{Z}_n, +)$, visto che un gruppo abeliano è ovviamente un quasigruppo commutativo. □

Esempio 2.4. *Dai gruppi $(\mathbb{Z}_2, +), (\mathbb{Z}_3, +)$ si ottengono i seguenti quasigruppi commutativi il primo dei quali è semi-idempotente ed il secondo idempotente:* $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$.

3 t-disegni e BIBD

Un $t-(v,k,\lambda)$ disegno con $t \leq k \leq v$ è una coppia $(V, \mathcal{B})$ in cui V è un insieme di cardinalità $v > 0$ di elementi detti vertici o punti e $\mathcal{B}$ è una famiglia di parti di V ciascuna di cardinalità k dette blocchi e non necessariamente distinte con la proprietà che ciascuna t-upla di vertici è contenuta in esattamente λ blocchi. Ad un $t-(v,k,\lambda)$ disegno si può associare una matrice detta di incidenza $A = (a_{ij})$ dove $a_{ij} = 1$ se il blocco j incide nel vertice i e $a_{ij} = 0$ altrimenti.

Teorema 3.1. *Il numero dei blocchi di un $t-(v,k,\lambda)$ disegno è $\frac{\lambda\binom{v}{t}}{\binom{k}{t}}$.*

Dimostrazione Segue dal fatto che il numeratore della frazione è il numero di t-uple contenute nell'insieme dei vertici ripetendole λ volte, mentre il denominatore è il numero di t-uple contenute in un blocco. □

Un $t-(v,k,\lambda)$ con $t = 2$ e $k < v$ si chiama (v,k,λ) BIBD o (v,k,λ) disegno. Un disegno con blocchi di cardinalità $k_1, k_2, \ldots, k_n$ si chiama $(v; k_1, k_2, \ldots, k_n; \lambda)$ PBD.

Teorema 3.2. *Se esiste un (v,k,λ) BIBD, allora $\lambda(v-1) = r(k-1)$, $bk = vr$, $b \geq v$ (diseguaglianza di Fisher), dove b è il numero totale di blocchi ed r è il numero di blocchi incidenti in un vertice.*

Dimostrazione La prima uguaglianza segue dal fatto che ciascuno dei due membri indica il numero di coppie contenenti un vertice fissato, mentre la seconda segue dalla prima e dal teorema precedente con $t = 2$. Per dimostrare la diseguaglianza, detta A la matrice di incidenza del disegno, non è difficile calcolare che $|A^tA| = rk(r-\lambda)^{v-1} > 0$ poiché $k < v \to r > \lambda$ e quindi il rango di A^tA è v. Ma questo rango non può superare quello di A che d'altra parte deve essere minore o uguale a b, quindi $b \geq v$. □

Un (v,k,λ) BIBD tale che il numero di blocchi coincide con il numero di vertici si dice simmetrico. Tale aggettivo è giustificato dal seguente

Teorema 3.3. *In un (v,k,λ) BIBD simmetrico ogni coppia di vertici appartiene a λ blocchi ed ogni coppia di blocchi ha λ vertici a comune.*

Dimostrazione La prima affermazione segue dalla definizione. Proviamo la seconda. Essendo il disegno simmetrico $v = b, k = r$. Detta x_i la cardinalità dell'intersezione di un blocco B con il blocco B_i, con $1 \leq i \leq v-1$, ciascuno dei $k = r$ vertici di B appartiene ad altri $r-1$ blocchi, quindi è $\sum x_i = r(r-1) = \lambda(v-1)$. Ciascuna delle $k(k-1)/2 = r(r-1)/2 = \lambda(v-1)/2$ coppie di vertici di B appartiene ad altri $\lambda - 1$ blocchi, quindi è $\frac{\sum x_i(x_i-1)}{2} = \lambda(\lambda-1)(v-1)/2$. Per la precedente relazione il secondo membro è uguale a $\frac{\sum x_i^2 - \sum x_i}{2} = \frac{\sum x_i^2 - \lambda(v-1)}{2}$ e quindi $\sum x_i^2 - \lambda(v-1) = \lambda(v-1)(\lambda-1)$, da cui $\sum x_i^2 = \lambda^2(v-1)$, quindi $\sum(x_i - \lambda)^2 = 0$, cioè $x_i = \lambda$. □

Corollario 3.4. *Il residuo di un (v, k, λ) BIBD eliminando un blocco e tutti i vertici in esso contenuti anche dagli altri blocchi è un $(v-k, k-\lambda, \lambda)$ BIBD.*

Teorema 3.5. *Se esiste un (v, k, λ) BIBD simmetrico e v è pari, allora $n = k - \lambda$ è un quadrato perfetto.*

Dimostrazione Sia A la matrice di incidenza di un disegno simmetrico allora non è difficile calcolare che $|A|^2 = k^2(k-\lambda)^{v-1} \Rightarrow |A| = k(k-\lambda)^{\frac{v-1}{2}}$. Essendo $|A|$ e k interi, $(k-\lambda)^{\frac{v-1}{2}}$ deve essere razionale e quindi, essendo $v-1$ dispari, $n = k - \lambda$ è un quadrato perfetto. □

Teorema 3.6. *[Bruck-Chowla-Ryser, 1949-50] Se esiste un (v, k, λ) BIBD simmetrico e v è dispari, allora l'equazione $z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ ha soluzioni non tutte nulle.*

Si noti che il teorema precedente fornisce una condizione necessaria ma non sufficiente per l'esistenza di un (v, k, λ) BIBD. Infatti è stato recentemente dimostrato che non esiste un $(111, 11, 1)$ BIBD, nonostante $x = z = 1$, $y = 3$ sia una soluzione non nulla dell'equazione $z^2 = 10x^2 - y^2$.

Dato un (v, k, λ) BIBD, D, considerando i complementari di ciascun blocco rispetto all'insieme dei vertici si ottiene un nuovo BIBD, $\overline{D}$, detto disegno complementare, come illustra il seguente

Teorema 3.7. *Se $b - 2r + \lambda > 0$ allora il complementare di un (v, k, λ) BIBD è un $(v, v-k, b-2r+\lambda)$ BIBD.*

Dimostrazione I blocchi di $\overline{D}$ che contengono una coppia di vertici x,y sono i complementari di quelli di D che non contengono né x né y. Quindi con ovvio significato dei simboli $\overline{b} = b - \{\text{blocchi che contengono almeno uno fra x ed y}\} = b - (r + r - \lambda) = b - 2r + \lambda$. □

Un $t - (v, k, \lambda)$ disegno si dice risolubile se l'insieme dei suoi blocchi può essere partizionato in classi (dette classi di risoluzione) tali che in ciascuna di esse ogni elemento di V appartiene ad uno ed un solo blocco. Due blocchi disgiunti si dicono anche paralleli. Un $(n^2, n, 1)$ BIBD si dice piano affine di ordine n, mentre un $(n^2+n+1, n+1, 1)$ BIBD con $n > 1$, si dice piano proiettivo di ordine n.

Teorema 3.8. *Un piano proiettivo è un disegno simmetrico ed ha una geometria ellittica, cioè non ha blocchi paralleli.*

Dimostrazione La prima proprietà deriva dal fatto che per il teorema 3.2 si ha $v = b = n^2 + n + 1$ e la seconda è conseguenza della prima e del teorema 3.3. □

Teorema 3.9. *Un piano affine ha una geometria euclidea, cioè, dato un blocco B ed un punto $x \notin B$, esiste un unico blocco che incide in x ed è parallelo a B. Blocchi paralleli a B ne esistono invece $n-1$.*

Dimostrazione I blocchi che incidono in x sono $r = n+1$; diciamoli $B_1, B_2, \ldots, B_{n+1}$. Per ogni $b \in B$, x e b appartengono ad un solo blocco B_i. Vi è quindi una corrispondenza iniettiva dai punti di B all'insieme dei B_i, ma essendo $|B| = n$, esiste un unico B_i che incide in x ed è parallelo a B. Per provare la seconda parte del teorema basta osservare che ciascuno degli n punti di B appartiene ad altri n blocchi, fornendo così n^2 blocchi che intersecano B, tutti distinti poiché $\lambda = 1$. Essendo $b = n^2+n$, ci sono $n^2+n-n^2-1 = n-1$ blocchi paralleli a B. □

Teorema 3.10. *Un piano affine di ordine n è risolubile in $n+1$ classi di risoluzione.*

Dimostrazione Considerato un blocco B_1 ed un punto $x \notin B_1$, per la prima parte del teorema 3.9 esiste un unico B_2 contenente x e parallelo a B_1. Sia $y \notin B_1 \cup B_2$. Esiste un unico blocco B_3 contenente y e parallelo a B_1. Esso è parallelo anche a B_2 poiché altrimenti esisterebbero due blocchi passanti per B_2 e paralleli a B_1. Continuando a procedere così si giunge ad ottenere $n-1$ blocchi paralleli a B_1 che esauriscono gli n^2 punti del piano. Partendo ora da un blocco C_1 non ancora utilizzato si può costruire una seconda classe di risoluzione che non contiene nessun blocco già utilizzato per la seconda parte del teorema 3.9. Procedendo così fino ad esaurire i blocchi del piano si ottengono $\frac{n(n+1)}{n} = n+1$ classi di risoluzione. □

Teorema 3.11. *Esiste un piano affine di ordine n se e solo se esiste un piano proiettivo di ordine n.*

Dimostrazione Il residuo di un piano proiettivo di ordine n è chiaramente un piano affine di ordine n. Viceversa sia A un piano affine di ordine n. Esso è risolubile per il teorema precedente. Aggiungendo un nuovo vertice ∞_i a tutti i blocchi della i-esima classe di risoluzione e aggiungendo anche il blocco $\{\infty_1, \infty_2, \ldots, \infty_{n+1}\}$ si ottiene un piano proiettivo di ordine n. □

Teorema 3.12. *Se $n = p^h$ con p primo, allora esiste un piano affine di ordine n.*

Dimostrazione Sia $V = GF(n) \times GF(n)$ e diciamo blocco un insieme di tutti i punti di V che soddisfano una equazione del tipo $x = c$ o del tipo $y = mx+q$ con $c, m, q \in GF(n)$. E' chiaro che ciascun blocco ha n punti e che, fissati due punti di V, esiste uno ed un solo blocco incidente in essi, poiché le coordinate dei due punti consentono di determinare in maniera unica i parametri m, q (o il solo parametro c), essendo essi elementi di un campo. □

Esempio 3.1. Per $n = 2$ si ha $V = \mathbb{Z}_2 = \{0, 1\}$. I blocchi sono $B_1 = \{(0,0),(0,1)\}$ di equazione $x = 0$, $B_2 = \{(1,0),(1,1)\}$ di equazione $x = 1$, $B_3 = \{(0,0),(1,1)\}$ di equazione $y = x$, $B_4 = \{(0,1),(1,0)\}$ di equazione $y = x+1$, $B_5 = \{(0,0),(1,0)\}$ di equazione $y = 0$, $B_6 = \{(0,1),(1,1)\}$ di equazione $y = 1$. Le classi di risoluzione sono $\{B_1, B_2\}$, $\{B_3, B_4\}$, $\{B_5, B_6\}$. Aggiungendo un nuovo vertice ∞_i a tutti i blocchi della i-esima classe di risoluzione ed il blocco $\{\infty_1, \infty_2, \infty_3\}$ si ottiene il piano proiettivo di ordine 2 che si chiama piano di Fano.

Un $(4n-1, 2n-1, n-1)$ BIBD si chiama disegno di Hadamard di dimensione n. Il piano di Fano è l'unico disegno che è sia un piano proiettivo che un disegno di Hadamard, visto che $n = 2$ è l'unico valore per cui si ha $4n - 1 = n^2 + n + 1$ e $n - 1 > 0$ (affinché sia un disegno di Hadamard). I piani proiettivi e i disegni di Hadamard sono i due casi estremi di disegni simmetrici, poiché si può provare che in un disegno simmetrico (v, k, λ), posto $n = k - \lambda$, si ha $4n - 1 \leq v \leq n^2 + n + 1$.

Fino ad oggi non sono stati trovati piani affini (proiettivi) aventi ordine diverso da una potenza di un unico primo ed è stato quindi congetturato che non ne esistano.

4 Quadrati latini e quadrati magici

Un quadrato latino di ordine n è una matrice quadrata di ordine n con n simboli tale che ciscuna riga e ciascuna colonna contiene tutti i simboli. Se esso è simmetrico rispetto alla diagonale principale si dice simmetrico. E' chiaro quindi che un quadrato latino è la tabella moltiplicativa di un quasigruppo e che quindi, visto che $(\mathbb{Z}_n, +)$ è un gruppo commutativo per ogni $n > 0$, esiste un quadrato latino simmetrico per ogni $n > 0$.

Date due matrici quadrate di ordine n, $A = (a_{ij})$ e $B = (b_{ij})$, si chiama $Join(A, B)$ la matrice quadrata di ordine n $C = (c_{ij})$ con $c_{ij} = (a_{ij}, b_{ij})$. Due quadrati latini si dicono ortogonali se tutte le entrate del loro Join, che Eulero chiamava quadrato greco-latino perché utilizzava le lettere greche per uno e quelle latine per l'altro, sono distinte cioè coprono una ed una sola volta tutte le n^2 coppie di elementi. Equivalentemente $A = (a_{ij})$ e $B = (b_{ij})$ sono ortogonali se $a_{ij} = a_{IJ}$ e $b_{ij} = b_{IJ}$ implicano $i = I$ e $j = J$, cioè i quadrati possono avere entrate coincidenti con un fissato valore solo in una posizione.

Teorema 4.1. *Se $A_1, A_2, \ldots, A_r$ sono quadrati latini di ordine n a due a due ortogonali (MOLS) si ha $r \leq n - 1$.*

Dimostrazione Supponiamo per assurdo che esistano n MOLS. Rinominando gli elementi dei quadrati latini in modo che le prime righe coincidano tutte con $\{1, 2, \ldots, n\}$, ci si rende subito conto che ci sarebbero due quadrati in cui le entrate a_{21}, ad esempio, dovrebbero coincidere con un valore i e quindi si ripeterebbe una seconda volta nel loro Join la coppia (i, i). □

Teorema 4.2. *Esistono $n - 1$ MOLS se e solo se esiste un piano affine di ordine n.*

Dimostrazione Siano $A_1, A_2, \ldots, A_{n-1}$ MOLS(n) con elementi $\{1, 2, \ldots, n\}$ e $A_r = (a_{ij}^{(r)})$. Definiamo la seguente matrice quadrata di ordine n $S = (s_{ij})$, con $s_{ij} = (i-1)n + j$ e siano R_i, C_j le righe e le colonne di S. Definiamo inoltre i seguenti blocchi: $B_{r,m} = \{x : x = s_{ij}, a_{ij}^{(r)} = m\}$, $1 \leq r \leq n-1$, $1 \leq m \leq n$, e sia $\mathcal{B} = (\bigcup R_i) \cup (\bigcup C_j) \cup (\bigcup B_{r,m})$. Dalla ortogonalità di $A_1, A_2, \ldots, A_{n-1}$ segue che due punti appartengono ad uno ed un solo blocco, poiché se x, y stessero sia in B_{r_1,m_1} che in B_{r_2,m_2}, allora la coppia (m_1, m_2) comparirebbe due volte nel Join(A_{r_1}, A_{r_2}). Quindi $(\{1, 2, \ldots, n^2\}, \mathcal{B})$ è un piano affine di ordine n. Viceversa, dato un piano affine di ordine n, essendo esso risolubile per il teorema 3.10, rinominando opportunamente i suoi punti si può far in modo che una prima classe di risoluzione sia formata dagli R_i ed una seconda dai C_j. Numerate da 1 ad $n - 1$ le

altre classi di risoluzione, definiamo $A_h = (a_{ij}^{(h)})$, $1 \leq h \leq n-1$, ponendo $a_{ij}^{(h)} = l$ dove $(i-1)n+j$ appartiene al blocco l-esimo della classe h-esima. Dal fatto che ogni coppia di punti sta in un ed un solo blocco del piano affine segue che gli A_h sono $n-1$ quadrati latini, poiché se $a_{ij}^{(h)} = a_{iJ}^{(h)} = l$ allora il blocco l-esimo della classe h-esima conterrebbe sia $(i-1)n+j$ che $(i-1)n+J$, che sono entrambi contenuti nel blocco R_i. Due quadrati A_h e A_k $(h \neq k)$ sono ortogonali poiché se $a_{ij}^{(h)} = a_{IJ}^{(h)} = l$ e $a_{ij}^{(k)} = a_{IJ}^{(k)} = m$ allora i due punti $(i-1)n+j$, $(I-1)n+J$ starebbero entrambi sia nel blocco l-esimo della classe h-esima che nel blocco m-esimo della classe k-esima che appartenendo a classi distinte sono sicuramente distinti. Ne segue che $i = I$ e $j = J$, cioè i due quadrati sono ortogonali. □

Esempio 4.1. Sia $n = 2$ e siano $A_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Con la costruzione illustrata nel teorema si ottiene il piano affine di ordine 2, isomorfo a quello costruito nell'esempio 3.1 $(V, \mathcal{B})$ con $V = \{1,2,3,4\}$, $\mathcal{B} = \{R_1, R_2, C_1, C_2, B_{1,1}, B_{1,2}\}$ dove $R_1 = \{1,2\}$, $R_2 = \{3,4\}$, $C_1 = \{1,3\}$, $C_2 = \{2,4\}$, $B_{1,1} = \{1,4\}$, $B_{1,2} = \{2,3\}$.

Un quadrato latino di ordine n ortogonale al suo trasposto si dice self-orthogonal, SOLS(n).

Teorema 4.3. *[Mendelsohn, 1971] Se $n = p^m$, $n \neq 2, 3$, esiste un SOLS(n).*

Dimostrazione Sia GF(n) $= \{c_1 = 0, c_2, \ldots, c_n\}$ e si scega $\lambda \in GF(n)$ tale che $\lambda \neq 0, 1$ e $2\lambda \neq 1$. Definendo una matrice quadrata $A = (a_{ij})$ di ordine n ponendo $a_{ij} = \lambda c_i + (1-\lambda)c_j$, si ottiene un quadrato latino, poiché se $a_{ij} = a_{ik}$ allora $\lambda c_i + (1-\lambda)c_j = \lambda c_i + (1-\lambda)c_k$ $\Rightarrow c_j = c_k \Rightarrow j = k$, essendo $\lambda \neq 1$; se $a_{ij} = a_{kj}$ allora $\lambda c_i + (1-\lambda)c_j = \lambda c_k + (1-\lambda)c_j$ $\Rightarrow c_i = c_k \Rightarrow i = k$, essendo $\lambda \neq 0$. A è self-orthogonal, poiché, detto $A^t = (a'_{ij})$, $a_{ij} = a_{kl}$ e $a'_{ij} = a'_{kl}$ implicano $\lambda c_i + (1-\lambda)c_j = \lambda c_k + (1-\lambda)c_l$ e $\lambda c_j + (1-\lambda)c_i = \lambda c_l + (1-\lambda)c_k$. Sommando e semplificando le due ultime uguaglianze si otterrebbe $(1-2\lambda)c_j = (1-2\lambda)c_l$, da cui, visto che $2\lambda \neq 1$, si ha $c_j = c_l$ e quindi $j = l$ e $i = k$. □

Esempio 4.2. *:* Se $n = 4$, considerando il $GF(4)$ costruito nell'esempio 2.2 e scegliendo $\lambda = x$ (unica scelta possibile in questo caso) si ottiene il seguente $SOLS(4)$:

$$A = \begin{pmatrix} 0 & 1 & x & x+1 \\ x+1 & x & 1 & 0 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \end{pmatrix}$$

che, come si verifica facilmente, è ortogonale al suo trasposto

$$A^t = \begin{pmatrix} 0 & 1+x & 1 & x \\ 1 & x & 0 & x+1 \\ x & 1 & x+1 & 0 \\ x+1 & 0 & x & 1 \end{pmatrix}.$$

Si ottiene poi un esempio di 3 MOLS(4) (e quindi un piano affine di ordine 4 per il teorema 4.2), considerando i 3 quadrati latini A, A^t, B, con

$$B = \begin{pmatrix} 0 & 1 & x & x+1 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \end{pmatrix}.$$

Teorema 4.4. *[Brayton, 1973] Esiste un SOLS(n) per ogni $n \neq 2, 3, 6$.*

E' immediato verificare che non esistono MOLS(2) ed Eulero aveva dimostrato che non esistono MOLS(6) nel suo celebre problema dei 36 ufficiali (si possono disporre 36 ufficiali di 6 gradi diversi e appartenenti a 6 diversi reggimenti in un quadrato greco-latino di lato 6?), congetturando che non esistessero MOLS(n) per infiniti n, ma dal teorema di Brayton e, per $n = 3$, dai teoremi 3.12, 4.2 segue che

Corollario 4.5. *Per ogni $n \neq 2, 6$ esistono due quadrati latini ortogonali di ordine n.*

In un quadrato latino di ordine n, un trasversale è un insieme di n entrate che sono tutte distinte e che si trovano tutte in righe e colonne diverse.

Lemma 4.1. *Se A è un SOLS(n), la sua diagonale principale è un trasversale.*

Dimostrazione Il trasposto di A ha la stessa diagonale principale di A. Quindi se $a_{ii} = a_{jj} = k$ con $i \neq j$, la coppia (k, k) comparirebbe due volte nel Join(A, A^t), contro l'ortogonalità. □

Un SAMDRR(n) è un torneo fra n coppie di coniugi in cui due qualsiasi giocatori dello stesso sesso sono avversari esattamente una volta, mentre ciascun giocatore gioca con ciascuno di quelli di sesso opposto tranne il coniuge una sola volta come partner ed una sola volta come avversario.

Teorema 4.6. *Esiste un SOLS(n) se e solo se esiste un SAMDRR(n).*

Dimostrazione Dette (M_i, F_i) le n coppie di coniugi, definiamo una matrice $A = (a_{ij})$ ponendo $a_{ii} = i$ e $a_{ij} = l$, dove F_l è il partner di M_i quando M_i gioca contro M_j. Dalla definizione di SAMDRR(n) si deduce che A è un SOLS(n), poiché, posto $A^t = (a'_{ij})$, se fosse $a_{ij} = a_{IJ} = l$ e $a_{ji} = a_{JI} = m$ si dovrebbero avere le partite $(M_i, F_l) - (M_j, F_m)$, $(M_I, F_l) - (M_J, F_m)$ da cui $i = I$ e $j = J$. Viceversa, sia $A = (a_{ij})$ un SOLS(n). Esso per il lemma precedente può essere rinominato in maniera tale che $a_{ii} = i$ per ogni i. Allora se $a_{ij} = l$ e $a_{ji} = m$, le partite $(M_i, F_l) - (M_j, F_m)$ formano un SAMDRR(n). □

Esempio 4.3. Rinominando il SOLS(4) A costruito nell'esempio 4.2 in modo tale che $a_{ii} = i$ e che $0 \to 1, 1 \to 2, x \to 3, x + 1 \to 4$, si ottiene $\begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. Esso fornisce il seguente SAMDRR(4): $(M_1, F_4) - (M_2, F_3)$, $(M_1, F_2) - (M_3, F_4)$, $(M_1, F_3) - (M_4, F_2)$, $(M_2, F_4) - (M_3, F_1)$, $(M_2, F_1) - (M_4, F_3)$, $(M_3, F_2) - (M_4, F_1)$.

Un quadrato semimagico di ordine n è una matrice quadrata di ordine n con entrate tutte distinte e tale che la somma di ciascuna riga e di ciascuna colonna è uguale ad una costante detta costante magica. Se inoltre anche la somma di ciascuna delle due diagonali è uguale alla costante magica, il quadrato si dice magico.

Teorema 4.7. *Dati due quadrati latini di ordine n ortogonali, $A = (a_{ij})$ e $B = (b_{ij})$, il quadrato $C = (c_{ij})$ con $c_{ij} = n(a_{ij} - 1) + b_{ij}$ è semimagico.*

Teorema 4.8. *Un quadrato magico di ordine n esiste per ogni $n > 0$.*

Se gli elementi di un quadrato magico di ordine n sono $\{1, 2, \ldots, n^2\}$, allora il quadrato magico si dice perfetto.

Teorema 4.9. *La costante magica di un quadrato magico perfetto è* $\frac{n(n^2+1)}{2}$.

Dimostrazione La somma di tutti gli elementi della matrice è la somma dei numeri $1, 2, \ldots, n^2$ che, per una nota formula aritmetica, è $\frac{n^2(n^2+1)}{2}$. Poiché ciascuna riga ha somma uguale alla costante magica, quest'ultima è uguale a $\frac{n^2(n^2+1)}{2n} = \frac{n(n^2+1)}{2}$. □

Per ottenere un quadrato magico perfetto di ordine dispari n basta porre $1 = a_{1,\frac{n+1}{2}}$ ed utilizzare la formula ricorsiva $k+1 = a_{i-1,j+1}$ essendo $k = a_{i,j}$ ed eseguendo tutte le operazioni in $\mathbb{Z}_n$ fin quando la cella $a_{i-1,j+1}$ è libera; se essa è occupata si pone $k+1 = a_{i+1,j}$ e si ripete il procedimento ricorsivo.

Esempio 4.4. Con il procedimento indicato si ottiene il seguente quadrato magico perfetto di ordine 3 e quindi costante magica 15: $\begin{pmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{pmatrix}$.

5 Sistemi di Steiner

Un $t-(v,k,\lambda)$ disegno con $\lambda = 1$ si chiama sistema di Steiner $S(t,k,v)$. Gli $S(2,3,v)$ e gli $S(3,4,v)$ si chiamano rispettivamente sistemi di terne e di quaterne di Steiner, STS(v) e SQS(v).

Teorema 5.1. *Un* $S(1,k,v)$ *esiste se e solo se* k *divide* v.

Dimostrazione Dalla definizione segue che un $S(1,k,v)$ è una partizione di V in classi di cardinalità k e quindi la condizione caratteristica è ovvia. □

Teorema 5.2. *Un* $STS(v)$ *esiste se e solo se* $v \equiv 1, 3 \pmod 6$.

Dimostrazione La necessità segue dal fatto che sia il numero di blocchi $\frac{v(v-1)}{6}$ sia il numero di blocchi incidenti in un fissato vertice $\frac{v-1}{2}$ debbono essere interi. Per la sufficienza, siano $v = 6n+3$, $(Q, \circ)$ un quasigruppo commutativo idempotente con $Q = \{1, 2, \ldots, 2n+1\}$, $V = Q \times \{1,2,3\}$, $\mathcal{B}_1 = \{\{(x,1),(x,2),(x,3)\} : x \in Q\}$, $\mathcal{B}_2 = \{\{(x,i),(y,i),(x \circ y, i+1)\} : 1 \leq x < y \leq 2n+1, i \in \{1,2,3\}\}$, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Si ha $|\mathcal{B}| = (2n+1) + 3C_{2n+1,2} = \frac{v(v-1)}{6}$ e comunque si fissano due vertici di V esiste almeno un blocco che li contiene. Infatti, se i due punti (a,b) e (c,d) hanno $a = c$ allora appartengono ad un blocco di $\mathcal{B}_1$, mentre se $a \neq c$ possono presentarsi due casi: se $b = d$ i due punti appartengono al blocco $\{(a,b),(c,b),(a \circ c, b+1)\}$, mentre se $b \neq d$, ad esempio $1 = b \neq d = 2$, allora esiste $x \in Q$ tale che $x \circ a = a \circ x = c$ poiché Q è un quasigruppo commutativo e si ha $x \neq a$ poiché Q è idempotente; allora $\{(a,1),(x,1),(a \circ x, 2)\}$ contiene i due punti dati e questo è sufficiente affinché $(V, \mathcal{B})$ sia un $STS(6n+3)$. Siano ora $v = 6n+1$ con $n > 0$, $(Q, \circ)$ un quasigruppo commutativo semi-idempotente con $Q = \{1, 2, \ldots, 2n\}$, $V = (Q \times \{1,2,3\}) \cup \{\infty\}$, $\mathcal{B}_1 = \{\{(x,1),(x,2),(x,3)\} : 1 \leq x \leq n\}$, $\mathcal{B}_2 = \{\{\infty, (n+x,i),(x,i+1)\} : i \in \{1,2,3\}, 1 \leq x \leq n\}$, $\mathcal{B}_3 = \{\{(x,i),(y,i),(x \circ y, i+1)\} : 1 \leq x < y \leq 2n, i \in \{1,2,3\}\}$, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$. Si ha $|\mathcal{B}| = n + 3n + 3C_{2n,2} = \frac{v(v-1)}{6}$ e comunque si fissano due vertici di V esiste almeno un blocco che li contiene. Infatti,

se due punti (a,b) e (c,d) hanno $a = c \leq n$ allora appartengono ad un blocco di $\mathcal{B}_1$, se uno dei due punti è ∞ appartengono ad un blocco di $\mathcal{B}_2$ e negli altri casi analogamente a prima si dimostra che appartengono ad un blocco di $\mathcal{B}_3$. Questo è sufficiente affinché $(V, \mathcal{B})$ sia un $STS(6n+1)$. □

Esempio 5.1. Utilizzando il quasigruppo commutativo semi-idempotente di ordine 2 dell'esempio 2.4 si ottengono i seguenti blocchi di un $STS(7)$ isomorfo al piano di Fano:
$\mathcal{B}_1 = \{\{(1,1),(1,2),(1,3)\}\}$, $\mathcal{B}_2 = \{\{\infty,(2,1),(1,2)\},, \{\infty,(2,2),(1,3)\}, \{\infty,(2,3),(1,1)\}\}$,
$\mathcal{B}_3 = \{\{(1,1),(2,1),(2,2)\}, \{(1,2),(2,2),(2,3)\}, \{(1,3),(2,3),(2,1)\}\}$.

Gli STS(v) risolubili si chiamano sistemi di terne di Kirkman, KTS(v), poiché risolvono il celebre problema delle v studentesse posto da Kirkman nel 1844: date v studentesse è possibile disporle in fila per tre per $\frac{v-1}{2}$ giorni in modo tale che ciascuna di esse sia nella stessa fila di ciascun altra una ed una sola volta?

Teorema 5.3. *Se esiste un KTS(v) allora* $v \equiv 3 \pmod 6$.

Dimostrazione Segue dal teorema precedente e dal fatto che il numero di blocchi di ogni classe di risoluzione deve essere multiplo di 3. □

Teorema 5.4. *[Ray-Chaudhuri-Wilson, 1971] Per* $v \equiv 3 \pmod 6$ *esiste un KTS(v).*

Esempio 5.2. Una soluzione al problema delle 15 studentesse $\{1,2,3,4,5,\ 6,7,8,9,0,\ A,B,C,D,E\}$ è la seguente, in cui G_i è la disposizione dell'i-esimo giorno:
$G_1 = \{123, 456, 789, 0AB, CDE\}$, $G_2 = \{14B, 270, 38D, 59C, 6AE\}$,
$G_3 = \{19E, 26C, 340, 58B, 7AD\}$, $G_4 = \{167, 25A, 3BE, 48C, 90D\}$,
$G_5 = \{15D, 29B, 3AC, 47E, 680\}$, $G_6 = \{18A, 24D, 369, 50E, 7BC\}$,
$G_7 = \{10C, 28E, 357, 49A, 6BD\}$.

Teorema 5.5. *Se esiste un* $S(t,4,v)$ $(V,\mathcal{B})$ *con* $t = 2,3$ *allora si ha rispettivamente* $v \equiv 1,4 \pmod{12}$, $v \equiv 2,4 \pmod 6$.

Dimostrazione Per $t = 2$ il risultato segue dal fatto che sia il numero di blocchi $\frac{v(v-1)}{12}$ sia il numero di blocchi incidenti in un fissato vertice $\frac{v-1}{3}$ debbono essere interi. Per $t = 3$, fissato un vertice x, sia $V_x = V \setminus \{x\}$ e sia $\mathcal{B}_x = \{\{y,z,w\} : \{x,y,z,w\} \in \mathcal{B}\}$ allora $(V_x, \mathcal{B}_x)$ è un $STS(v-1)$ e quindi per il teorema 5.2 deve essere $v - 1 \equiv 1,3 \pmod 6$, da cui la tesi. □

Teorema 5.6. *Se* $v = 2^h$, $h \geq 3$, *allora esiste un* $SQS(v)$.

Dimostrazione Sia $V = \mathbb{Z}_2^h$ e sia $\mathcal{B} = \{\{a,b,c,d\} : a,b,c,d \in V, a+b+c+d = 00\ldots0, |\{a,b,c,d\}| = 4\}$. E' chiaro che per ogni terna di elementi distinti di V $\{a,b,c\}$ esiste una ed una sola quaterna che la contiene, cioè $\{a,b,c,a+b+c\}$ e quindi si ha la tesi. □

Teorema 5.7. *[Hanani, 1960-62] Se* $v \equiv 1,4 \pmod{12}$, $v \equiv 2,4 \pmod 6$ *allora esiste un* $S(t,4,v)$ *con* $t = 2,3$ *rispettivamente.*

6 Metodi delle differenze

Un (v, k, λ) difference set è un insieme $D = \{d_1, d_2, \ldots, d_k\}$ di elementi distinti di un gruppo abeliano additivo G di ordine v tale che ciascun elemento non nullo di G può essere espresso come differenza di elementi di D in λ modi o, come si può dire più brevemente, ammette λ D-rappresentazioni. In questo caso $\{D+g = \{d_1+g, d_2+g, \ldots, d_k+g\} : g \in G\}$ è l'insieme dei v traslati di D che costituiscono i blocchi di un disegno simmetrico detto ciclico, nel caso in cui G sia un gruppo ciclico.

Teorema 6.1. *Se esiste un (v, k, λ) difference set allora $\lambda(v-1) = k(k-1)$, ciascuno dei suoi traslati è anch'esso un (v, k, λ) difference set e i suoi traslati costituiscono i blocchi di un (v, k, λ) BIBD simmetrico.*

Dimostrazione L'uguaglianza deriva dal fatto che entrambi i membri indicano il numero di differenze. Un traslato è un difference set poiché, per ogni $a \in G$, $(d_i + a) - (d_j + a) = m \leftrightarrow d_i - d_j = m$. Fissati $a, b \in G$, si osservi che $a = d_i + (a - d_i)$ per ogni i, quindi a compare nei traslati $D + (a - d_i)$ e b compare nei traslati $D + (b - d_i)$. Allora a, b compaiono in un traslato $D + d$ se e solo se $d = a - d_i = b - d_j$ per qualche i, j. Ma $a - d_i = b - d_j \leftrightarrow a - b = d_i - d_j$ e ciò accade per λ coppie i, j, quindi a, b appartengono a λ traslati e da ciò la tesi. □

Teorema 6.2. *Il complementare di un (v, k, λ)-difference set è un $(v, v-k, v-2k+\lambda)$-difference set.*

Dimostrazione Sia fissato un $d \in G \setminus \{0\}$. Per ogni $e \in D$, c'è una unica rappresentazione di d come $d = e - x$ (basta considerare $x = e - d$). Per λ scelte di e si ha che $x \in D$ poiché d si può esprimere come differenza di elementi entrambi in D in λ modi. Allora per $k - \lambda$ scelte di e si ha che x sta nel complementare di D. Ciò dimostra che $d = e - f$ con $e \in D$ e $f \notin D$ in $k - \lambda$ modi. Analogamente $d = e - f$ con $e \notin D$ e $f \in D$ in $k - \lambda$ modi. Ma essendo $d = e - f$ con $e \in G$ e $f \in G$ in v modi, si ha che $d = e - f$ con $e \notin D$ e $f \notin D$ in $v - \lambda - 2(k - \lambda) = v - 2k + \lambda$ modi. □

Teorema 6.3. *[Paley, 1933] Se $q = p^h = 4n - 1$, allora esiste un disegno di Hadamard di dimensione n.*

Dimostrazione E' sufficiente verificare che l'insieme Q dei quadrati non nulli di GF(q) è un $(4n - 1, 2n - 1, n - 1)$ difference set e quindi la tesi seguirà dal teorema 6.1. Dal teorema 2.2 segue che Q è l'insieme delle potenze pari e $-Q$ è l'insieme delle potenze dispari di θ. Se 1 ha λ Q-rappresentazioni anche θ^{2s} ha λ Q-rappresentazioni e viceversa, poiché basta moltiplicare o dividere per θ^{2s} ciascuna Q-rappresentazione. Quindi ogni elemento di Q ha lo stesso numero λ di rappresentazioni come differenza di elementi di Q. Ma anche ogni elemento di $-Q$ ha lo stesso numero λ di Q-rappresentazioni, come si ottiene moltiplicando o dividendo per -1 ciascuna Q-rappresentazione. Chiaramente $k = |Q| = 2n - 1$ e dalla relazione $\lambda(v - 1) = k(k - 1)$ si ottiene $\lambda = n - 1$. □

Teorema 6.4. *Se $q = p^h = 4n - 1$, allora esiste un $(4n - 1, 2n, n)$ BIBD.*

Dimostrazione L'insieme $R \cup \{0\}$, dove $R = -Q$, è un $(4n - 1, 2n, n)$ difference set per il teorema di Paley e per il teorema 6.2 e quindi la tesi segue dal teorema 6.1. □

Un difference system è una famiglia di insiemi $\{D_1, D_2, \ldots, D_t\}$ con elementi in un gruppo abeliano additivo G tali che ciascun elemento non nullo di G si possa esprimere

come differenza di elementi di $\bigcup D_i$ in λ modi. Se tutti i D_i hanno cardinalità k si dice che è un (v, k, λ)-difference system. Per i difference system si definiscono in maniera analoga ai difference set i traslati e si prova che i traslati di un difference system formano i blocchi di un BIBD se tutti i D_i hanno la stessa cardinalità e di un PBD in caso contrario e che vale l'uguaglianza $\lambda(v-1) = tk(k-1)$.

Teorema 6.5. *Se $q = p^h = 6m+1$, allora esiste un $STS(q)$.*

Dimostrazione E' sufficiente verificare che, detto θ un elemento primitivo di GF(q), gli insiemi $D_i = \{0, \theta^i, \theta^{m+i}\}$, $0 \leq i \leq m-1$ formano un $(6m+1, 3, 1)$ difference system e da ciò seguirà la tesi. Si ha $\theta^{6m} = 1$ e $\theta^{3m} = -1$ (teorema 2.2) quindi $0 = \theta^{3m} + 1 = (\theta^m + 1)(\theta^{2m} - \theta^m + 1)$ con $\theta^m + 1 \neq 0$, poiché θ ha ordine $6m$; quindi $\theta^{2m} = \theta^m - 1$. Utilizzando questa relazione si trova che le differenze in D_i sono $\{\theta^i, \theta^{m+i}, \theta^{2m+i}, \theta^{3m+i}, \theta^{4m+i}, \theta^{5m+i}\}$ e poiché i prende tutti i valori da 0 ad $m-1$ si ha che le differenze coprono tutti gli elementi non nulli di $GF(6m+1)$. □

Teorema 6.6. *Se $q = p^h = 6m+1$, allora esiste un $(6m+1, 4, 2)$ BIBD.*

Dimostrazione E' sufficiente verificare che, detto θ un elemento primitivo di GF(q), gli insiemi $D_i = \{0, \theta^i, \theta^{2m+i}, \theta^{4m+i}\}$, $0 \leq i \leq m-1$ formano un $(6m+1, 4, 2)$ difference system e da ciò seguirà la tesi. Analogamente al teorema precedente si ottiene che le differenze in D_i sono $(A_i = \{\theta^i, \theta^{m+i}, \theta^{2m+i}, \theta^{3m+i}, \theta^{4m+i}, \theta^{5m+i}\}) \cup (\theta^m + 1)A_i$ e poiché i prende tutti i valori da 0 ad $m-1$ si ha che le differenze coprono due volte tutti gli elementi non nulli di $GF(6m+1)$. □

Da questo teorema per $m = 1$ si ha $D_0 = \{0, 1, 3\}$ e l'STS(7) da esso generato è il piano di Fano costruito anche nell'esempio 3.1, mentre per $m = 2$ si ottiene $D_0 = \{0, 1, 4\}$, $D_1 = \{0, 2, 8\}$ e calcolando i loro traslati si ottengono, fra gli altri, i blocchi $D_0 + 3 = \{3, 4, 7\}$, $D_1 + 3 = \{3, 5, 11\}$, entrambi incidenti nel vertice 3 e paralleli al blocco $D_1 = \{0, 2, 8\}$. Quindi si ottiene un STS(13) che ha una geometria iperbolica, mentre l'STS(7) (che si dimostra essere unico a meno di isomorfismi) essendo un piano proiettivo ha una geometria ellittica e l'STS(9) (anch' esso unico a meno di isomorfismi) essendo un piano affine ha una geometria euclidea.

Teorema 6.7. *Se $q = p^h = 4n+1$, allora esiste un $(4n+1, 2n, 2n-1)$BIBD.*

Dimostrazione E' sufficiente verificare che l'insieme dei quadrati non nulli di GF(q) ed il suo complementare R rispetto a $GF(q) \setminus \{0\}$ costituiscono un $(4n+1, 2n, 2n-1)$ difference system e da ciò seguirà la tesi. Dal teorema 2.2 segue che $Q = -Q$ è l'insieme delle potenze pari e $R = -R$ è l'insieme delle potenze dispari di θ. Analogamente alla dimostrazione del teorema di Paley si prova che ogni elemento di Q ha lo stesso numero λ_1 di Q-rappresentazioni e che ogni elemento di R ha λ_2 Q-rappresentazioni. Ma, essendo $R = \theta Q$, ad ogni Q-rappresentazione di $r \in R$ corrisponde una R-rappresentazione di $q \in Q$ e viceversa; quindi ogni elemento di Q ha lo stesso numero λ_2 di R-rappresentazioni e ogni elemento di R ha λ_1 R-rappresentazioni. In conclusione ogni elemento non nullo di $GF(q)$ ha lo stesso numero $\lambda_1 + \lambda_2$ di $(Q \cup R)$-rappresentazioni. Chiaramente $k = |Q| = 2n$ e dalla relazione $\lambda(v-1) = tk(k-1)$ si ottiene $\lambda = 2n-1$. □

Teorema 6.8. *Se $q = p^h = 4n-1$, allora esiste un $(4n-1; 2n-1, 2n; 2n-1)$ PBD ed un $(4n, 2n, 2n-1)$ BIBD.*

Dimostrazione E' sufficiente verificare che l'insieme $R = -Q$ dei non quadrati di $GF(q)$ ed il suo complementare $Q \cup \{0\}$ costituiscono un difference system e da ciò seguirà la prima parte della tesi. Infatti, come nella dimostrazione del teorema di Paley si prova che ogni elemento non nullo di $GF(q)$ ha $n-1$ Q-rappresentazioni e quindi, aggiungendo la rappresentazione $q-0$ o $0-q$, ha n $(Q \cup \{0\})$-rappresentazioni. Essendo $R = -Q$ ogni elemento non nullo di $GF(q)$ ha $n-1$ R-rappresentazioni e quindi ogni elemento non nullo di $GF(q)$ ha $n+n-1 = 2n-1$ $(Q \cup \{0\}, R)$-rappresentazioni come si voleva. Aggiungendo poi un nuovo vertice ai traslati di R si ottiene un $(4n, 2n, 2n-1)$ BIBD. □

In un torneo di Whist con $4n+1$ giocatori si gioca coppia contro coppia in modo tale che le partite siano suddivise in $4n+1$ round con n partite in cui ogni giocatore sia partner di ciascuno altro una volta e suo avversario due volte.

Teorema 6.9. *Se $q = p^h = 4n+1$, allora esiste un $Wh(4n+1)$.*

Dimostrazione Sia $V = GF(q)$, quindi per il teorema 2.2 si ha $\theta^{4n} = 1$ e $\theta^{2n} = -1$. Fissando il seguente primo round $\{(\theta^i, \theta^{2n+i}) - (\theta^{n+i}, \theta^{3n+i}) : 0 \leq i \leq n-1\}$ in esso le differenze fra i partners sono $A_i = \{2\theta^i, 2\theta^{n+i}, 2\theta^{2n+i}, 2\theta^{3n+i}\}$ e quindi, essendo $0 \leq i \leq n-1$, coprono esattamente tutti gli elementi di $GF(q) \setminus \{0\}$, mentre le differenze fra avversari coprono due volte l'insieme $(\theta^n - 1)A_i$ cioè due volte tutti gli elementi di $GF(q) \setminus \{0\}$. Aggiungendo agli elementi di questo primo round tutti gli elementi di $V = GF(q)$ si ottengono i $4n+1$ round del $Wh(4n+1)$. □

Teorema 6.10. *[Baker] Per ogni $n > 0$, esiste un $Wh(4n+1)$.*

Esempio 6.1. *:* Per $n = 1$, il $Wh(5)$ che si ottiene con il teorema 6.9 è: $\{(1,4) - (2,3)\}$, $\{(2,0) - (3,4)\}$, $\{(3,1) - (4,0)\}$, $\{(4,2) - (0,1)\}$, $\{(0,3) - (1,2)\}$.

7 Matrici e codici di Hadamard

Una matrice di Hadamard di ordine n è una matrice quadrata di ordine n ad elementi in $\{+1, -1\}$ tale che $HH^t = nI_n$, essendo I_n la matrice identità di ordine n.

Lemma 7.1. *Una matrice è di Hadamard se e solo se il prodotto interno di due righe distinte è nullo e di due righe coincidenti è uguale all'ordine della matrice. Inoltre se H è di Hadamrd, anche H^t lo è.*

Dimostrazione Dalla definizione segue che il prodotto di R_i e C'_j (j-esima colonna di H^t) è nullo se $i \neq j$, mentre vale n se $i = j$. Visto che la j-esima colonna di H^t coincide con la j-esima riga di H, si ha la prima parte della tesi. La seconda parte è un semplice calcolo: $HH^t = nI_n \Rightarrow H^t = nH^{-1} \Rightarrow H^tH = nI_n$. □

Una matrice di Hadamard si dice normalizzata se la prima riga e la prima colonna sono tutte positive. Si osservi che qualsiasi matrice di Hadamard si può facilmente normalizzare.

Lemma 7.2. *Se H è una matrice normalizzata di Hadamard di ordine $n > 2$, si ha $n = 4m$, ha ogni riga (colonna) tranne la prima con $2m$ elementi positivi e $2m$ negativi. Inoltre ogni coppia di righe (colonne) distinte fra loro ed entrambe dalla prima sono entrambe positive in m posti, entrambe negative in m posti e quindi differiscono in $2m$ posti.*

Dimostrazione Per il lemma precedente è sufficiente provare i risultati solo per le righe. Poiché la prima riga è formata solo da elementi 1 e poiché il prodotto di due righe è nullo, ogni altra riga è formata da $n/2$ positivi ed $n/2$ negativi. Quindi n è pari ed invertendo le colonne senza mutare gli elementi che si vogliono dimostrare, si può supporre che la seconda riga sia positiva fino all'elemento $a_{2,\frac{n}{2}}$ e negativa in tutti gli elementi successivi. La riga R_i con $i > 2$ ha u entrate positive nella prima metà, v entrate positive nella seconda metà, quindi $\frac{n}{2} - u$ entrate negative nella prima metà, $\frac{n}{2} - v$ entrate negative nella seconda metà. Si ha $0 = R_1 R_i = u + v$ e $0 = R_2 R_i = u - (\frac{n}{2} - u) - v + (\frac{n}{2} - v)$, da cui $n = 4u = 4v$. Questo ragionamento prova anche la seconda parte del teorema se si confrontano le righe R_2 ed R_i ed è chiaro che analogamente si può ragionare su due qualsiasi righe R_i ed R_j distinte fra loro e dalla prima. □

Teorema 7.1. *Una matrice di Hadamard di ordine $4m \geq 8$ esiste se e solo se esiste un disegno di Hadamard $(4m-1, 2m-1, m-1)$ di dimensione m.*

Dimostrazione Sia H la matrice che possiamo supporre normalizzata. Cancelliamo la prima riga e la prima colonna e sostituiamo -1 con 0 ottenendo una matrice A di ordine $4m-1$. Per il lemma precedente ogni riga (colonna) ha $2m-1$ elementi positivi e due righe sono entrambe positive in $m-1$ posti. A è quindi la matrice di incidenza di un disegno di Hadamard $(4m-1, 2m-1, m-1)$. Il procedimento inverso consente di ottenere una matrice di Hadamard da un disegno di Hadamard. □

Teorema 7.2. *Esistono disegni di Hadamard di dimensione m per ogni $m = 2^k$.*

Dimostrazione La seguente è una matrice di Hadamard normalizzata di ordine 2: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Se H è una matrice di Hadamard di ordine m, $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ è una matrice di Hadamard di ordine $2m$ poiché soddisfa le condizioni sufficienti del lemma 7.1. Quindi esiste una matrice di Hadamard per ogni $m = 2^k$ e dal teorema precedente segue la tesi. □

Un (n, d)-codice binario è un sottoinsieme di $\mathbb{Z}_2^n$ i cui elementi sono dette parole e sono tali che due qualsiasi di esse differiscono almeno in d posizioni. Se da una matrice di Hadamard di ordine $4m$ si elimina la prima colonna e si sostituiscono i simboli -1 con 0, le $4m$ righe di lunghezza $4m-1$ sono tali che due qualsiasi di esse differiscono per $2m$ elementi (per il lemma 7.2) e quindi costituiscono un $(4m-1, 2m)$-codice binario detto codice di Hadamard di tipo $4m-1$. Dal teorema precedente segue che si possono ottenere (n, d)-codici aventi minima distanza d arbitrariamente grande. L'importanza di questo risultato dipende dal fatto che un (n, d)-codice può intercettare ovviamente $d-1$ errori e correggerne $\lceil \frac{d}{2} - 1 \rceil$ e quindi è sempre possibile realizzare un codice che sia in grado di correggere un qualsiasi numero di errori. Ciò tuttavia sarebbe possibile anche con un codice costituito da due sole parole: la prima costituita da n zeri e la seconda da d uni e da $n-d$ zeri. Ma questo codice è ovviamente troppo povero di parole ed allora è importante considerare anche la cardinalità del codice per ottenerne uno più "ricco" possibile di parole. Diciamo allora $A(n, d)$ e $B(n, d)$ la massima cardinalità di un (n, d)-codice binario avente parole di distanza almeno d o esattamente d rispettivamente. Ovviamente $B(n, d) \leq A(n, d)$.

Teorema 7.3. *[Plotkin, 1960] Se $d > \frac{n}{2}$ allora $A(n, d) \leq \frac{2d}{2d-n}$.*

Teorema 7.4. *Per tutti gli m per cui esiste un disegno di Hadamard di dimensione m si ha $B(4m-1,2m) = A(4m-1,2m) = 4m$.*

Dimostrazione Infatti per questi m è possibile costruire una matrice di Hadamard di ordine $4m$ per il teorema 7.1 e da essa ricavare il codice di Hadamard di tipo $4m-1$ in cui due qualsiasi delle $4m$ parole hanno distanza fra loro $2m$ e quindi si ha $B(4m-1,2m) \geq 4m$. Dal teorema di Plotkin si ricava che $A(4m-1,2m) \leq \frac{4m}{4m-4m+1} = 4m$, da cui la tesi. □

Questo teorema impedisce di costruire codici con parole di lunghezza $4m-1$ più ricchi di quello di Hadamard, ma è possibile costruire un codice con parole di lunghezza $4m$ che ha il doppio delle parole e sempre distanza minima $2m$, semplicemente considerando una matrice di Hadamard H di ordine $4m$ e sostituendo -1 con 0 nella matrice $\binom{H}{-H}$. Le $8m$ righe di questa matrice non possono avere distanza maggiore di $2m$ in virtù del lemma 7.2 e quindi costituiscono un $(4m,2m)$-codice detto codice di Hadamard di tipo $4m$ o anche codice di Reed-Muller, che è stato usato nel 1972 dalla sonda Mariner 9 per inviare foto da Marte, che vengono usati anche nei compact disc e che è stato congetturato essere usati dalla natura nella codifica del DNA. Esso è infatti anche in questo caso il più ricco possibile con questi parametri, come si evince dal seguente

Teorema 7.5. *Per tutti gli m per cui esiste un disegno di Hadamard di dimensione m si ha $A(4m,2m) = 8m$.*

Dimostrazione $A(4m,2m) \geq 8m$ segue dalla esistenza dei codici di Hadamard di tipo $4m$. Per provare la disuguaglianza inversa, si consideri un (n,d)-codice C avente $A(n,d)$ parole con $0 < d < n$ e sia C' il codice da esso ottenuto considerando solo le parole di C che iniziano con 1 e cancellando questo 1. C' è un $(n-1,d')$-codice con $d' \geq d$ e quindi $|C'| \leq A(n-1,d') \leq A(n-1,d)$, visto che ovviamente un (n,d)-codice è anche un (n,d')-codice se $d' \geq d$. Analogamente, sia C'' il codice ottenuto da C considerando solo le parole di C che iniziano con 0 e cancellando questo 0. C'' è un $(n-1,d'')$-codice con $d'' \geq d$ e quindi $|C''| \leq A(n-1,d'') \leq A(n-1,d)$. Ne segue che $A(n,d) = |C| = |C'| + |C''| \leq 2A(n-1,d)$. In particolare allora $A(4m,2m) \leq 2A(4m-1,2m) = 8m$, per il teorema precedente. □

8 Ipergrafi, Γ-decomposizioni, Γ-fattorizzazioni

Si dice ipergrafo una coppia ordinata $H = (V,\mathcal{S})$ in cui V è un insieme finito non vuoto di elementi detti vertici o punti e $\mathcal{S}$ è una famiglia di parti di V detti spigoli eventualmente ripetute e tali che la loro unione sia V. Se lo spigolo s contiene il vertice v si dice che s è incidente in v. Se tutti gli spigoli sono distinti l'ipergrafo si dice semplice e se tutti gli spigoli hanno la stessa cardinalità t l'ipergrafo si dice uniforme di rango t o grafo di dimensione $t-1$. Un ipergrafo i cui spigoli sono quelli di H ripetuti $\lambda > 0$ volte e con lo stesso insieme di vertici si indica con il simbolo λH. Un ipergrafo uniforme $(V,\mathcal{S})$ si dice completo se $\mathcal{S}$ è l'insieme di tutte le t-uple senza ripetizioni di elementi di V.

Dato un ipergrafo $H = (V,\mathcal{S})$ si dice sottoipergrafo un ipergrafo $(W,\mathcal{S}')$ tale che $W \subseteq V$ e $\mathcal{S}' \subseteq \mathcal{S}$. Se $W = V$ il sottoipergrafo H si dice fattore di H. Due ipergrafi $(V,\mathcal{S})$ e $(V',\mathcal{S}')$ si dicono isomorfi se esiste una corrispondenza biunivoca fra V e V' che preserva l'appartenenza agli spigoli, cioè tale da indurre una corrispondenza biunivoca fra gli spigoli in cui il corrispondente di uno spigolo contiene i vertici corrispondenti.

I grafi di dimensione 1 si dicono semplicemente grafi. Un grafo completo con v vertici si indica con il simbolo K_v, mentre un grafo i cui vertici sono partizionati in $V_1, V_2, \ldots, V_n$ e tale che tutte le coppie di vertici non appartenenti alla stessa classe sono suoi spigoli si dice multipartito completo e si indica con il simbolo $K_{v_1,v_2,\ldots,v_n}$, con $|V_i| = v_i$. Si indicano invece con i simboli P_k e C_k due grafi aventi entrambi $V = \{v_1, v_2, \ldots, v_k\}$, ma aventi come spigoli $\mathcal{S} = \{\{v_i, v_{i+1}\} : 1 \leq i \leq k-1\}$ e $\mathcal{S} \cup \{\{v_k, v_1\}\}$ rispettivamente.

Dato un ipergrafo $H = (V, \mathcal{S})$ uniforme e una famiglia Γ di sottoipergrafi di H si dice Γ-decomposizione di H una coppia $(V, \mathcal{B})$ dove $\mathcal{B}$ è un insieme di sottoipergrafi detti blocchi ciascuno dei quali è isomorfo ad un elemento della famiglia Γ e tale che gli insiemi dei loro spigoli costituiscono una partizione di $\mathcal{S}$; una Γ-decomposizione di H che può essere partizionata in fattori si dice risolubile o Γ-fattorizzazione.

Se H è un ipergrafo completo uniforme di rango t con v vertici e Γ è costituito solo da un sottoipergrafo completo con k vertici ($t \leq k \leq v$), una Γ-decomposizione di λH è un $t-(v, k, \lambda)$ disegno.

Una Γ-decomposizione di K_v tale che $\mathcal{B}$ abbia il massimo numero possibile di triangoli si chiama maximum packing di K_v con triangoli, $MPT(v)$. L'insieme dei blocchi di $\mathcal{B}$ che non sono triangoli si chiama leave.

Lemma 8.1. *Se $v \equiv 5 \pmod 6$, allora esiste una Γ-decomposizione di K_v i cui blocchi sono tutti K_3 ad eccezione di un K_5.*

Teorema 8.1. *Il leave di un $MPT(v)$ è:*

1. *vuoto se e solo se $v \equiv 1, 3 \pmod 6$;*
2. *un 1-fattore (cioé una P_2-fattorizzazione di K_v) se e solo se $v \equiv 0, 2 \pmod 6$;*
3. *un C_4 se e solo se $v \equiv 5 \pmod 6$;*
4. *un tripolo (cioé un S_3 ed un 1-fattore degli altri vertici) se e solo se $v \equiv 4 \pmod 6$.*

Dimostrazione Il primo caso segue direttamente dal teorema 5.2. Il secondo caso si riconduce ad esso eliminando un vertice da un $MPT(v+1)$. Il terzo caso deriva dal lemma 8.1, poiché dal K_5 $\{a, b, c, d, e\}$ si possono ottenere i due K_3 $\{a, b, c\}$, $\{a, d, e\}$ ed il C_4 (b, d, c, e) che costituisce il leave. Anche il quarto caso deriva dal lemma 8.1, eliminando dalla Γ-decomposizione di K_{v+1} uno dei vertici del K_5. □

Un torneo singolo è una P_2-fattorizzazione di K_v, poiché ciascun giocatore deve incontrare ciascun altro una ed una sola volta.

Teorema 8.2. *Un torneo singolo con v giocatori esiste se e solo se v è pari.*

Dimostrazione La necessità segue dal fatto che ogni fattore ha $v/2$ blocchi. Per la sufficienza si verifica che, detto $V = \mathbb{Z}_{2n-1} \cup \{\infty\}$, $\{\{2, 0\}, \{3, 2n-2\}, \ldots, \{n, n+1\}\}$ è un difference system in $\mathbb{Z}_{2n-1}$ e quindi unendo ad esso la coppia $\{1, \infty\}$ e calcolando i traslati dell'insieme ottenuto si ha una soluzione. □

Esempio 8.1. Un torneo singolo con 6 giocatori è il seguente: $G_1 = \{1-\infty, 2-0, 3-4\}$, $G_2 = \{2-\infty, 3-1, 4-0\}$, $G_3 = \{3-\infty, 4-2, 0-1\}$, $G_4 = \{4-\infty, 0-3, 1-2\}$, $G_5 = \{0-\infty, 1-4, 2-3\}$.

Si chiama problema dei v prigionieri il problema di disporre v prigionieri ammanettati in fila per tre per $\frac{3(v-1)}{4}$ giorni in modo tale che ciascuno di essi sia ammanettato a ciascun altro una ed una sola volta.

Teorema 8.3. *Il problema dei v prigionieri ha soluzione solo se* $v \equiv 9 \pmod{12}$.

Dimostrazione Evidentemente il problema equivale a quello dell'esistenza di una P_3-fattorizzazione di K_v. La tesi è una conseguenza del fatto che sia il numero $\frac{v}{3}$ di blocchi di ciascun fattore, sia il numero $\frac{3(v-1)}{4}$ di fattori debbono essere interi. □

Teorema 8.4. *[Wilson] Se* $v \equiv 9 \pmod{12}$ *allora esiste una soluzione del problema dei v prigionieri.*

Esempio 8.2. Una soluzione al problema dei 9 prigionieri è la seguente, dove G_i è la disposizione dell'i-esimo giorno: $G_1 = \{413, 276, 598\}$, $G_2 = \{746, 519, 832\}$, $G_3 = \{179, 843, 265\}$, $G_4 = \{124, 739, 586\}$, $G_5 = \{457, 163, 829\}$, $G_6 = \{781, 496, 253\}$.

Teorema 8.5. *Una* P_v*-fattorizzazione di* K_v *esiste se e solo se v è pari.*

Dimostrazione La necessità segue dal fatto che il numero $\frac{v}{2}$ di blocchi deve essere intero. Per la sufficienza si verifica che $V = \mathbb{Z}_v$, $\mathcal{B} = \{0+i, (v-1)+i, 1+i, (v-2)+i, 2+i, \ldots, (\frac{v}{2})-1+i, \frac{v}{2}+i : i \in \mathbb{Z}_{v/2}\}$ è una soluzione. □

Esempio 8.3. Per $v = 6$ si ha la seguente P_6-fattorizzazione di K_6: $\mathcal{B} = \{[0, 5, 1, 4, 2, 3], [1, 0, 2, 5, 3, 4], [2, 1, 3, 0, 4, 5]\}$.

Il problema dei v cavalieri consiste nel disporre v cavalieri attorno ad un'unica tavola rotonda con v posti per $\frac{v-1}{2}$ giorni in modo tale che ciascuno di essi sia seduto accanto a ciascun altro una ed una sola volta.

Teorema 8.6. *Il problema dei v cavalieri ha soluzione se e solo se v è dispari.*

Dimostrazione Evidentemente il problema equivale a quello dell'esistenza di una C_v-fattorizzazione di K_v, dove C_v è il ciclo (cammino elementare chiuso) di lunghezza v. La necessità segue dal fatto che il numero $\frac{v-1}{2}$ di blocchi deve essere intero. Per la sufficienza si verifica che $V = \mathbb{Z}_{v-1} \cup \{\infty\}$, $\mathcal{B} = \{(\infty, 0+i, (v-2)+i, 1+i, (v-3)+i, 2+i, \ldots, \frac{v-1}{2}+i) : i \in \mathbb{Z}_{\frac{v-1}{2}}\}$ è una soluzione. □

Esempio 8.4. Per $v = 7$ si ha la seguente soluzione del problema dei 7 cavalieri: $\mathcal{B} = \{(\infty, 0, 5, 1, 4, 2, 3), (\infty, 1, 0, 2, 5, 3, 4), (\infty, 2, 1, 3, 0, 4, 5)\}$.

Problema di Oberwolfach: Per quali valori $n, s_1, s_2, \ldots, s_n$**, esiste una** $\{C_{s_1}, C_{s_2}, \ldots, C_{s_n}\}$**-fattorizzazione di** $K_{s_1+s_2+\ldots+s_n}$**?** Questo è un problema ancora aperto, anche se sono note molte soluzioni particolari. Ad esempio, per $s_1 = s_2 = \ldots = s_n = 3$ esso coincide con il problema delle v studentesse e quindi ammette soluzione se e solo se n è dispari, mentre per $n = 1$ il problema coincide con quello dei v cavalieri e quindi ha soluzione se e solo se s_1 è dispari.

Se $H = \lambda K_v$ e Γ è costituito solo da un grafo G, una Γ-decomposizione di H si chiama $G-$disegno di ordine v e indice λ.

Se $H = \lambda K_v$ e $\Gamma = \{K_{k_1}, K_{k_2}, \ldots, K_{k_n}\}$, una Γ-decomposizione di H è un $(v; k_1, k_2, \ldots, k_n; \lambda)$ PBD. Come già notato, per $n = 1$ un PBD diventa un BIBD.

Se $H = K_{v_1,v_2,\ldots,v_n}$ e $\Gamma = \{K_{k_1}, K_{k_2}, \ldots, K_{k_h}\}$, una Γ-decomposizione di H è un $\{k_1, k_2, \ldots, k_h\}-$GDD di tipo $v_1 v_2 \ldots v_n$. Le classi che partizionano l'insieme dei vertici si chiamano gruppi e dalla definizione segue che ogni coppia di vertici appartenenti ad uno stesso gruppo non appartiene a nessun blocco, mentre ogni coppia di vertici appartenenti a gruppi diversi appartiene ad un blocco. Se $h = 1, k_1 = n, v_1 = v_2 = \ldots = v_n = m$ allora si ha un trasversal design $TD(n, m)$. Ovviamente per $n = 1$ si ha un $(v_1; k_1, k_2, \ldots, k_h; 1)$ PBD.