Riv. Mat. Univ. Parma (5) **6** (1997), 135-142

SANDRO RAJOLA (*)

Disegni in sistemi di Steiner ed iperovali non regolari di $PG(2, q)$ (**)

1 - Introduzione

Partendo da sistemi di Steiner con gruppo degli automorfismi transitivo sulle coppie di punti, si costruiscono disegni e si studiano gli insiemi a due caratteri in tali disegni. Inoltre vengono analizzate le iperovali non regolari di $PG(2, q)$. Una *iperovale* di $PG(2, q)$, con q pari, è un insieme di $q+2$ punti a tre a tre non allineati ed essa si dice *regolare* se è unione di una conica non degenere e del suo nucleo.

B. Segre ha provato che in $PG(2, q)$, con q pari e $q > 8$, esistono iperovali non regolari se q è diverso da alcuni particolari valori. Il problema della determinazione del numero b_{NR} delle iperovali non regolari di $PG(2, q)$, con q pari e $q > 8$, è ancora aperto.

In questo lavoro, utilizzando esclusivamente tecniche aritmetiche e combinatoriche, si determinano *condizioni necessarie* per b_{NR}. Si prova ad esempio che, per $q = 16$, $b_{NR} \equiv 0 \bmod. 58240$ e che, per $q = 32$, $b_{NR} \equiv 0 \bmod. 16776704$.

2 - Alcuni disegni in un sistema di Steiner

Siano $S = S(2, k, v)$ un *sistema di Steiner*, $\mathcal{S}$ l'insieme dei punti di S ed $\mathcal{R}$ l'insieme delle rette di S.

Sia $\mathcal{G}$ il gruppo degli automorfismi di S. Supponiamo che $\mathcal{G}$ sia transitivo sulle coppie di punti.

(*) Dip. di Mat. Univ. La Sapienza, P.le A. Moro 2, 00185 Roma, Italia.

(**) Ricevuto il 20 ottobre 1997. Classificazione AMS 51 E 21.

Infine, sia $\mathcal{P}$ la famiglia di tutti i sottoinsiemi di S che godono di una fissata proprietà invariante per automorfismi di S.

Fissato un intero $c \geqslant 2$, sia $\mathcal{F} = \{A_j\}_{j=1,\dots,b}$ la famiglia dei sottoinsiemi di S di cardinalità c ed appartenenti a $\mathcal{P}$. Supponiamo $\mathcal{F} \neq \emptyset$. Dall'ipotesi fatta su $\mathcal{G}$ e dalla definizione di $\mathcal{F}$ segue che *la coppia* $(S, \mathcal{F})$ *è un* $2-(v, c, \lambda_2)$ *disegno*, dove λ_2 è il numero dei blocchi passanti per due punti distinti.

Indicato poi con λ_1 il numero dei blocchi passanti per un fissato punto, è noto che:

$$\lambda_1 v = cb \tag{2.1}$$

$$b = \frac{v(v-1)}{c(c-1)} \lambda_2 \tag{2.2}$$

$$\lambda_1(c-1) = \lambda_2(v-1). \tag{2.3}$$

Fissati due interi m ed n tali che $0 \leqslant m < n$, diremo che un insieme T è di *classe* $[m, n]$ rispetto alla famiglia $\mathcal{F}$, se $|T \cap A_j| \in \{m, n\}$ per ogni $j = 1, \dots, b$ ([3], [4]).

Sia T un sottoinsieme di S di classe $[m, n]$ rispetto ad $\mathcal{F}$, con $|T| \geqslant 2$. Sia t_i, con $i \in \{m, n\}$, il numero degli insiemi della famiglia $\mathcal{F}$ che sono i-secanti T. Contando in due modi diversi le coppie costituite da un punto X di T e da un elemento di $\mathcal{F}$ contenente X, si ha

$$mt_m + nt_n = \lambda_1 |T| . \tag{2.4}$$

Contando in due modi diversi le coppie costituite da una coppia di punti distinti X, Y di T e da un elemento di $\mathcal{F}$ contenente X ed Y, si ha

$$m(m-1)\, t_m + n(n-1)\, t_n = \lambda_2 |T|(|T|-1). \tag{2.5}$$

Dalle (2.2) e (2.4) segue:

$$t_m = \frac{\lambda_2 v(v-1)\, n - \lambda_1 |T| c(c-1)}{c(c-1)(n-m)} \tag{2.6}$$

$$t_n = \frac{\lambda_1 |T| c(c-1) - \lambda_2 v(v-1)\, m}{c(c-1)(n-m)} . \tag{2.7}$$

Dalle (2.5), (2.6) e (2.7) deriva l'uguaglianza

$$\begin{aligned}\lambda_2 c(c-1)\,|T|^2 + [\lambda_1 c(c-1)(1-m-n) - \lambda_2 c(c-1)]\,|T| \\ + mn\lambda_2 v(v-1) = 0\,.\end{aligned} \tag{2.8}$$

Infine dalle (2.3), (2.8) segue la relazione

$$c(c-1)\,|T|^2 + [c(v-1)(1-m-n) - c(c-1)]\,|T| + mnv(v-1) = 0\,. \tag{2.9}$$

In particolare, se $m = 0$, dalla (2.9) segue la

$$|T| = \frac{(v-1)(n-1)}{c-1} + 1\,. \tag{2.10}$$

Le osservazioni precedenti conducono al

Teorema 1. *Sia $S = S(2, k, v)$ un sistema di Steiner con il gruppo degli automorfismi transitivo sulle coppie di punti e sia $\mathcal{S}$ l'insieme dei punti di S. Allora, se $\mathcal{F} \neq \emptyset$ e T è un sottoinsieme di $\mathcal{S}$ di classe $[m, n]$ rispetto ad $\mathcal{F}$, con $|T| \geq 2$, sussiste l'uguaglianza* (2.9). *In particolare, se $m = 0$, sussiste la* (2.10).

Sia ancora $\mathcal{F} \neq \emptyset$ e sia T un sottoinsieme di $\mathcal{S}$ tale che

$$|T| \geq 2 \qquad |T \cap A_j| = t \qquad \forall j = 1, \ldots, b\,. \tag{2.11}$$

Osserviamo che $t \geq 2$. Infatti da $\mathcal{F} \neq \emptyset$ segue che esiste un $A_j \in \mathcal{F}$. Siano X_1, Y_1 due punti distinti di A_j (tali punti esistono perché $|A_j| = c \geq 2$) e siano X_2, Y_2 due punti distinti di T (tali punti esistono perché $|T| \geq 2$).

Dall'ipotesi fatta su $\mathcal{G}$ segue che vi è un $g \in \mathcal{G}$ tale che $g(\{X_1, Y_1\}) = \{X_2, Y_2\}$. Dunque $g(A_j)$, che è un elemento di $\mathcal{F}$ e che contiene $g(\{X_1, Y_1\})$, ha in comune con T almeno i punti X_2, Y_2. Ne segue $t \geq 2$.

L'insieme T può essere interpretato come insieme di classe $[0, t]$, ovvero di classe $[t, t+n_1]$, o ancora di classe $[t, t+n_2]$ rispetto ad $\mathcal{F}$ con $n_1 > 0$, $n_2 > 0$, $n_1 \neq n_2$. Per ciascuna di tali interpretazioni vale la (2.9) (Teorema 1).

Pensando T come insieme di classe $[0, t]$, dalla (2.9), essendo $m = 0$, $n = t$, segue

$$(c-1)\,|T| + v - vt + t - c = 0\,. \tag{2.12}$$

Pensando T come insieme di classe $[t, t+n_1]$, dalla (2.9), essendo $m = t$,

$n = t + n_1$, si ha

$$(2.13)\qquad \begin{aligned} &c(c-1)\,|T|^2 + [c(v-1)(1-2t-n_1) - c(c-1)]\,|T| \\ &\qquad + t(t+n_1)\,v(v-1) = 0\,. \end{aligned}$$

Pensando T come insieme di classe $[t,\, t+n_2]$, dalla (2.9) si ha (essendo $m = t$, $n = t + n_2$)

$$(2.14)\qquad \begin{aligned} &c(c-1)\,|T|^2 + [c(v-1)(1-2t-n_2) - c(c-1)]\,|T| \\ &\qquad + t(t+n_2)\,v(v-1) = 0\,. \end{aligned}$$

Le (2.13), (2.14) implicano

$$(2.15)\qquad |T|\,c = tv$$

da cui, tenuto conto della (2.12), segue

$$(2.16)\qquad |T| = v\,,\quad c = t \qquad \text{ovvero} \qquad |T| = t\,,\quad c = v\,.$$

Si può dunque concludere con il

Corollario 1. *Sia $S = S(2, k, v)$ un sistema di Steiner con il gruppo degli automorfismi transitivo sulle coppie di punti e sia $\mathcal{S}$ l'insieme dei punti di S. Sia $\mathcal{F} \neq \emptyset$, e sia T un sottoinsieme di $\mathcal{S}$ soddisfacente le condizioni* (2.11). *Allora sussiste la* (2.16).

Dal Teorema 1, scegliendo $S(2, k, v) = PG(r, q)$, deriva poi il

Corollario 2. *In $PG(r, q)$, sia $\mathcal{S}_p$ l'insieme dei punti. Sia $\mathcal{F} \neq \emptyset$ e sia T un sottoinsieme di $\mathcal{S}_p$ di classe $[m, n]$ rispetto ad $\mathcal{F}$, con $|T| \geqslant 2$. Allora si ha*

$$(2.17)\qquad c(c-1)\,|T|^2 + [c(\theta_r - 1)(1-m-n) - c(c-1)]\,|T| + mn\theta_r(\theta_r - 1) = 0$$

dove $\theta_r = q^r + q^{r-1} + \ldots + q + 1$.

In particolare, se $m = 0$, si ha

$$(2.18)\qquad |T| = \frac{(\theta_r - 1)(n-1)}{c-1} + 1\,.$$

Sempre dal Teorema 1, scegliendo $S(2, k, v) = AG(r, q)$, discende il

Corollario 3. *In $AG(r, q)$ sia S_a l'insieme dei punti. Sia $\mathcal{F} \neq \emptyset$ e sia T un sottoinsieme di S_a di classe $[m, n]$ rispetto ad $\mathcal{F}$ con $|T| \geq 2$. Allora risulta*

$$c(c-1)|T|^2 + [c(q^r - 1)(1 - m - n) - c(c-1)]|T| + mnq^r(q^r - 1) = 0 . \tag{2.19}$$

In particolare, se $m = 0$, si ha

$$|T| = \frac{(q^r - 1)(n-1)}{c-1} + 1 . \tag{2.20}$$

Esempio 1. In $AG(2, 4)$ sia $\mathcal{F} = \{A_j\}_{j=1, \ldots, b}$ la famiglia di tutti gli insiemi A_j che sono unione di due rette parallele e distinte. Evidentemente si ha $|A_j| = c = 8$ per ogni $j = 1, \ldots, b$. Sia T un insieme di $AG(2, 4)$ tale che $|T \cap A_j| = 2, 4$ per ogni $j = 1, \ldots, b$. In questo caso dalla (2.19) segue

$$7|T|^2 - 82|T| + 240 = 0 \tag{2.21}$$

che ammette $|T| = 6$ come unica soluzione intera.

Con riferimento a tale soluzione, alcune possibilità per T sono le seguenti (chiamando *iperovale di $AG(2, q) \subset PG(2, q)$* una iperovale di $PG(2, q)$ contenuta in $AG(2, q)$):

a. $T_1 = \mathcal{C}$ *dove $\mathcal{C}$ è una iperovale*

b. $T_2 = AG(2, 4) - \mathcal{C} \cup t$, *dove $\mathcal{C}$ è una iperovale e t è una retta esterna a $\mathcal{C}$*

c. $T_3 = s_1 \cup s_2 - \{P\}$, *dove s_1 ed s_2 sono due rette incidenti nel punto P.*

Le coppie $(\mathcal{F}, T_1)$, $(\mathcal{F}, T_2)$, $(\mathcal{F}, T_3)$ costituiscono tre diversi esempi per il Corollario 3 con $r = 2$, $m = 2$, $n = 4$, $c = 8$, $q = 4$.

Gli esempi che seguono generalizzano l'Esempio 1.

Esempio 2. Sia N un intero tale che $2 \leq N \leq q-1$, con $q = 2^h \geq 4$. In $AG(2, q)$ sia $\mathcal{F}' = \{A_j'\}_{j=1, \ldots, b'}$ la famiglia di tutti gli insiemi A_j' che sono unione di N parallele e distinte. Evidentemente si ha $|A_j'| = c = Nq$ per ogni $j = 1, \ldots, b'$.

Sia T' un insieme di $AG(2, q)$ tale che $|T' \cap A_j'| = \frac{1}{2}(N-1)q, \frac{1}{2}Nq$ per ogni $j = 1, \ldots, b'$. In questo caso dalla (2.19), tenendo presente che $r = 2$, $m = \frac{1}{2}(N-1)q$, $n = \frac{1}{2}Nq$, $c = Nq$, $T = T'$, segue

$$(Nq-1)|T'|^2 + \frac{1}{2}(2q^2 - 2Nq^3 + q^3 - q)|T'| + \frac{1}{4}q^3(N-1)(q^2-1) = 0 . \tag{2.22}$$

Le soluzioni della (2.22) sono:

$$\frac{1}{2}(q^2-q) \quad \text{e} \quad \frac{1}{2}\frac{(N-1)(q+1)\,q^2}{Nq-1}\,. \tag{2.23}$$

Con riferimento alla soluzione $|T'| = \frac{1}{2}(q^2-q)$, una possibilità è che T' sia un insieme di tipo $(0, \frac{1}{2}q)$. Dunque la coppia $(\mathcal{F}', T')$, con T' insieme di tipo $(0, \frac{1}{2}q)$, costituisce una classe di esempi al variare di N.

Esempio 3. In $AG(2, q)$, con q pari e $q \geq 4$, sia $\mathcal{F}'' = \{A_j''\}_{j=1,\dots b''}$ la famiglia di tutti gli insiemi A_j'' che sono unione di $\frac{1}{2}q$ rette parallele e distinte. Evidentemente si ha $|A_j''| = c = \frac{1}{2}q^2$ per ogni $j = 1, \dots, b''$. Sia T'' un insieme di $AG(2, q)$ tale che $|T'' \cap A_j''| = \frac{1}{4}q^2 - \frac{1}{2}q, \ \frac{1}{4}q^2$ per ogni $j = 1, \dots, b''$. In questo caso dalla (2.19) segue (tenendo presente che $r = 2$, $m = \frac{1}{4}q^2 - \frac{1}{2}q$, $n = \frac{1}{4}q^2$, $c = \frac{1}{2}q^2$, $T = T''$)

$$\left(\frac{q^2}{2} - 1\right)|T''|^2 + \left(q^2 - \frac{q^4}{2} + \frac{q^3}{2} - \frac{q}{2}\right)|T''| + \frac{q^2}{2}\left(\frac{q^2}{4} - \frac{q}{2}\right)(q^2-1) = 0\,. \tag{2.24}$$

Le soluzioni della (2.24) sono:

$$\frac{1}{2}q(q-1) \quad \text{e} \quad \frac{1}{2}\frac{q(q^2-2q)(q+1)}{q^2-2}\,. \tag{2.25}$$

Con riferimento alla soluzione $|T''| = \frac{1}{2}(q^2-q)$, una possibilità per T'' è la seguente

$$T'' = AG(2, q) - S - l \tag{2.26}$$

dove S è un insieme di tipo $(0, \frac{1}{2}q)$ ed l è una retta esterna ad S. Dunque la coppia $(\mathcal{F}'', T'')$, con T'' dato dalla (2.26), costituisce un esempio.

Sempre con riferimento alla prima delle (2.25), un'altra possibilità per T'' è data da

$$T'' = s_1 \cup s_2 \cup \dots \cup s_{\frac{1}{2}q} - \{P\} \tag{2.27}$$

dove $s_1, s_2, \dots, s_{\frac{1}{2}q}$ sono rette di $AG(2, q)$ passanti per il punto P. Dunque la coppia $(\mathcal{F}'', T'')$, con T'' dato dalla (2.27), costituisce un esempio.

3 – Sulle iperovali non regolari di $PG(2, q)$

In $PG(2, q)$ con q pari sia $\mathcal{S}$ l'insieme dei punti, sia $\mathcal{F}$ la famiglia delle *iperovali non regolari* (cfr. [1] e [2]) e sia $\mathcal{F} \neq \emptyset$, $|\mathcal{F}| = b_{NR}$. Il numero μ_2 degli elementi di $\mathcal{F}$ per due punti distinti X, Y di $\mathcal{S}$, non dipende da X, Y. Allora la coppia $(\mathcal{S}, \mathcal{F})$ è un $2-(q^2+q+1,\, q+2,\, \mu_2)$ disegno. In modo analogo il numero μ_3 (μ_4) delle iperovali non regolari passanti per tre punti distinti e non allineati (quattro punti distinti a tre a tre non allineati) non dipende dai tre punti (quattro punti) fissati.

Denotato con μ_1 il numero delle iperovali non regolari per un fissato punto, contando in due modi diversi le coppie costituite da un punto X e da una iperovale non regolare per X, risulta

$$\mu_1(q^2+q+1) = (q+2)\, b_{NR}\,. \tag{3.1}$$

Contando in due modi diversi le coppie costituite da una coppia ordinata (X, Y) di punti distinti e da una iperovale non regolare per X ed Y, si trova

$$(q+2)\, b_{NR} = q(q^2+q+1)\,\mu_2\,. \tag{3.2}$$

Contando in due modi diversi le coppie costituite da una terna ordinata di punti distinti e non allineati (X, Y, Z) e da una iperovale non regolare per X, Y, Z si ha

$$\mu_2 = \mu_3 q\,. \tag{3.3}$$

Contando in due modi diversi le coppie costituite da una quaterna ordinata di punti distinti a tre a tre non allineati (X, Y, Z, V) e da una iperovale non regolare per X, Y, Z, V, si ottiene

$$\mu_3 = (q-1)\,\mu_4. \tag{3.4}$$

Infine, dalle (3.2), (3.3), (3.4) segue l'uguaglianza

$$b_{NR} = q^2(q-1)(q^2+q+1)\,\frac{\lambda_4}{q+2}\,. \tag{3.5}$$

Dalla (3.5) derivano, ad esempio, i risultati citati nel n. 1.

Bibliografia

[1] B. SEGRE, *Sui k-archi nei piani finiti di caratteristica due,* Rev. Math. Pures Appl. 2 (1957), 289-300.

[2] B. SEGRE, *Ovali e curve σ nei piani di Galois di caratteristica due,* Atti Accad. Naz. Lincei, Rend. 32 (1962), 785-790.

[3] G. TALLINI, *Some new results on sets of type (m, n) in projective planes,* J. Geom. 29 (1987), 191-199.

[4] M. TALLINI SCAFATI, *Sui $\{k, n\}$-archi di un piano grafico finito con particolare riguardo a quelli con due caratteri,* Atti Accad. Naz. Lincei, Rend. 40 (1966), 812-818, 1020-1025.

Summary

Starting from a Steiner system $S(2, k, v)$, we construct some designs and study the two characters sets in such designs. Moreover, we get an expression for the number of non-regular hyperovals of $PG(2, q)$.

***