

Capitolo 9

Blocking set

9.1 Generalit 

Siano X un insieme finito non vuoto ed \mathcal{F} una famiglia di sottoinsiemi di X .

DEFINIZIONE 9.1.1. Un insieme B di elementi di X prende il nome di *blocking set* rispetto ad \mathcal{F} , o *\mathcal{F} -blocking set*, se B non contiene elementi di \mathcal{F} e ogni elemento di \mathcal{F} ha intersezione non vuota con B .

Un \mathcal{F} -blocking set B si dice *minimale* se $B \setminus \{b\}$ non   un blocking set, per ogni elemento $b \in B$. In altre parole, B   minimale se, e soltanto se, ogni elemento $b \in B$ appartiene ad almeno un elemento di \mathcal{F} che interseca B nel solo punto b . Si dice invece che B   di *ordine minimo* se X non contiene \mathcal{F} -blocking set con un numero di punti minore di quello di B . \square

ESERCIZIO 9.1.2. *Provare che ogni \mathcal{F} -blocking set di ordine minimo   anche minimale.*

DEFINIZIONE 9.1.3. Se X   l'insieme dei punti di un piano affine o proiettivo finito π , un blocking set rispetto alla famiglia di tutte le rette di π si chiama *blocking set di π* . \square

Nei paragrafi che seguono esporremo alcuni tra i principali risultati relativi ai blocking set dei piani affini e proiettivi su un campo di Galois.

Fissati X e la famiglia \mathcal{F} , uno dei problemi fondamentali della teoria dei blocking set   quello di *calcolare il minimo ordine di un \mathcal{F} -blocking set e descrivere la struttura degli \mathcal{F} -blocking set di minima cardinalit *. Tale problema, e la stessa nozione di blocking set, trovano le loro motivazioni iniziali in una serie di conferenze tenute a Princeton agli inizi degli anni '50 da *L.S. Shapley* allo scopo di generalizzare le teorie di *J. von Neumann* e *O. Morgenstern* contenute nel loro famoso libro del 1947 dal titolo *Theory of games and economic behavior* [63]. Le idee sviluppate da Shapley si rivelarono particolarmente utili ed interessanti nel caso in cui la famiglia \mathcal{F} era l'insieme di tutti i sottospazi di fissata dimensione in uno spazio affine o proiettivo su un campo di Galois. Nacque cos  l'esigenza di studiare i blocking set negli spazi affini e proiettivi e il primo articolo sull' argomento, che si deve a *M. Richardson* [71], risale al 1956. In questo lavoro

viene per la prima volta posto esplicitamente il problema di calcolare la minima cardinalità di un blocking set rispetto alla famiglia dei sottospazi di una fissata dimensione in $PG(n, q)$ e, per quanto riguarda i piani, viene provato che 6 è il minimo numero di punti di un blocking set di $PG(2, 3)$. Più di dieci anni dopo queste tematiche vennero riprese da *J. di Paola*, che in [66],[67] determinò gli ordini minimi dei blocking set nei piani proiettivi d'ordine 4, 5, 7, 8, 9 e, nei casi 3, 4, 5, 9 descrisse anche la struttura dei blocking set corrispondenti. Lo studio dei blocking set ha poi assunto l'aspetto di una vera e propria teoria con i primi lavori e risultati di *A.A. Bruen* [21],[22].

Per il Lettore interessato a maggiori informazioni sui legami tra la teoria dei giochi e quella dei blocking set si consiglia l'articolo [5].

ESERCIZIO 9.1.4. Sia α_n un piano affine finito d'ordine n . Provare che l'unione X di due rette distinte e incidenti di α_n ha ordine $2n - 1$ ed è ad intersezione non vuota con ogni retta.

ESERCIZIO 9.1.5. Sia α_n un piano affine finito d'ordine n . Siano ℓ, m due rette distinte e incidenti di α_n , a un punto non appartenente ad $\ell \cup m$. Siano a_m la proiezione di a su ℓ nella direzione di m e a_ℓ la proiezione di a su m nella direzione di ℓ . Detto b un punto della retta $a_m a_\ell$ diverso da a_m e a_ℓ , provare che

$$B = (\ell \setminus \{a_m\}) \cup (m \setminus \{a_\ell\}) \cup \{a, b\}$$

è un blocking set minimale di α_n con $2n - 1$ punti.

ESEMPIO 9.1.6. Sia π_n un piano proiettivo finito d'ordine n . Se n è un quadrato, i sottopiani di Baer di π_n sono blocking set minimali d'ordine $n + \sqrt{n} + 1$ (cfr.7.2.7). In particolare, $PG(2, q)$ è un blocking set minimale di $PG(2, q^2)$ d'ordine $q^2 + q + 1$ (cfr.7.2.5). \square

ESEMPIO 9.1.7. Sia π_n un piano proiettivo finito d'ordine n . Se n è un quadrato, gli archi hermitiani di π_n sono blocking set minimali d'ordine $n\sqrt{n} + 1$ (cfr.7.2.8). In particolare una curva hermitiana $H(2, q)$ di $PG(2, q)$ è un blocking set minimale d'ordine $q\sqrt{q} + 1$ (cfr.7.2.10). \square

ESERCIZIO 9.1.8. Provare che $PG(2, 2)$ non contiene blocking set.

9.2 Blocking set e nuclei in $AG(2, q)$

Sia $AG(2, q)$ il piano affine ottenuto da $PG(2, q)$ eliminando i punti di una sua fissata retta ℓ_∞ e denotiamo con (x, y) le coordinate affini di un generico punto di $AG(2, q)$ in un riferimento proiettivo $\{E_0, E_1, E_2, E\}$ di $PG(2, q)$ nel quale la retta ℓ_∞ abbia equazione $x_2 = 0$.

Sia $GF(q^2) = GF(q)[j]$ il campo di Galois ottenuto aggiungendo a $GF(q)$ una radice j di un polinomio di secondo grado $f(x) \in GF(q)[x]$ irriducibile su $GF(q)$ e ricordiamo che, in queste ipotesi, risulta

$$GF(q^2) = \{a + jb \ : \ a, b \in GF(q) \text{ e } f(j) = 0\}.$$

Nel seguito spesso, con abuso di notazione e di linguaggio, identificheremo i punti di $AG(2, q)$ con gli elementi di $GF(q^2)$ mediante la seguente funzione biunivoca

$$P = (x, y) \in AG(2, q) \rightarrow x + jy \in GF(q^2).$$

PROPOSIZIONE 9.2.1. Tre punti di $a, b, c \in AG(2, q)$ sono allineati se, e soltanto se, in $GF(q^2)$ risulta

$$(b - a)^{q-1} = (c - a)^{q-1}.$$

DIMOSTRAZIONE. Se consideriamo $GF(q^2)$ come spazio vettoriale di dimensione 2 su $GF(q)$, abbiamo la seguente catena di equivalenze

$$\begin{aligned} a, b, c \text{ allineati} &\Leftrightarrow (b - a) = \lambda(c - a) \text{ con } \lambda \in GF(q) \Leftrightarrow \\ \frac{b - a}{c - a} = \lambda \in GF(q) &\Leftrightarrow \left(\frac{b - a}{c - a}\right)^{q-1} = \frac{(b - a)^{q-1}}{(c - a)^{q-1}} = 1, \end{aligned}$$

da cui segue l'asserto. □

DEFINIZIONE 9.2.2. Sia X un insieme non vuoto di punti di $AG(2, q)$. Un punto $a \notin X$ prende il nome di *nucleo* di X se ogni retta passante per a é ad intersezione non vuota con X . L'insieme dei nuclei di X si denota con $N(X)$.

ESERCIZIO 9.2.3. Sia X un insieme non vuoto di punti di $AG(2, q)$. Provare che risulta $N(X) = AG(2, q) \setminus X$ se, e soltanto se, X é un blocking set di $AG(2, q)$.

ESERCIZIO 9.2.4. Sia a un nucleo di un insieme X di punti di $AG(2, q)$. Provare che ogni retta per a interseca X in esattamente un punto se, e soltanto se, $|X| = q + 1$.

Allo scopo di valutare il massimo numero di nuclei che puó avere un insieme di punti X premettiamo due lemma.

LEMMA 9.2.5. (lemma di A. Blokhuis) Sia $\mathbf{x} = (x_1, x_2, \dots, x_{q+n})$, $0 < n \leq q$, una successione di $q + n$ elementi di $GF(q^2)$ contenente tutte le $q + 1$ radici $(q + 1)$ -esime dell'unitá di $GF(q^2)$. Allora risulta

$$\sigma_n(\mathbf{x}) = \sum_{0 < j_1 < j_2 < \dots < j_n} x_{j_1} x_{j_2} \dots x_{j_n} = 0.$$

DIMOSTRAZIONE. Non é restrittivo supporre che x_1, x_2, \dots, x_{q+1} siano radici $(q + 1)$ -esime dell'unitá fra loro distinte e, in queste ipotesi, abbiamo

$$t^{q+1} - 1 = \prod_{j=1}^{q+1} (t - x_j).$$

Ora, consideriamo il polinomio $F(t) \in GF(q^2)[t]$ definito da

$$F(t) = \prod_{j=1}^{q+n} (t - x_j) = \sum_{j=0}^{q+n} (-1)^j \sigma_j(\mathbf{x}) t^{q+n-j}$$

e osserviamo che, a meno del segno, $\sigma_n(\mathbf{x})$ é il coefficiente di t^q in $F(t)$. D'altra parte possiamo scrivere

$$\begin{aligned} F(t) &= [(t - x_1)(t - x_2) \dots (t - x_{q+1})](t - x_{q+2}) \dots (t - x_{q+n}) = \\ &= (t^{q+1} - 1)(t^{n-1} + G(t)), \end{aligned}$$

ove $G(t)$ é un polinomio di grado minore di $n - 1$, e da ciò segue che é nullo il coefficiente di t^q in $F(t)$, cioè l'asserto. □

LEMMA 9.2.6. *Siano $q = p^r$ una potenza di un primo p ed n un intero positivo minore o uguale a q . Allora il coefficiente binomiale*

$$\binom{q+n}{n}$$

non é divisibile per p .

DIMOSTRAZIONE. Per ogni $j = 1, 2, \dots, n$, poniamo $j = t_j p^{s_j}$, con $s_j \geq 0$ e t_j non divisibile per p . Allora risulta

$$\begin{aligned} \binom{q+n}{n} &= \frac{(q+1)(q+2)\cdots(q+n)}{n!} = \prod_{j=1}^n \frac{p^r + j}{j} = \\ &= \prod_{j=1}^n \frac{p^r + t_j p^{s_j}}{t_j p^{s_j}} = \prod_{j=1}^n \frac{p^{r-s_j} + t_j}{t_j}. \end{aligned}$$

A questo punto osserviamo che l'ultimo prodotto non può essere divisibile per p , altrimenti esisterebbe un indice k per cui p divide $p^{r-s_k} + t_k$ e ciò é assurdo. Ne segue l'asserto. \square

PROPOSIZIONE 9.2.7. *(teorema di A.Blokhuis) Sia X un insieme di $q+n$ punti di $AG(2, q)$ con $n > 0$. Allora risulta*

$$|N(X)| \leq n(q-1).$$

DIMOSTRAZIONE. Sia $X = \{x_1, x_2, \dots, x_{q+n}\}$ e assumiamo $n \leq q$, altrimenti l'asserto é banale. Consideriamo il polinomio $F_X(t) \in GF(q^2)[t]$ definito da

$$F_X(t) = \sigma_n((t-x_1)^{q-1}, (t-x_2)^{q-1}, \dots, (t-x_{q+n})^{q-1})$$

e osserviamo che il coefficiente di $t^{n(q-1)}$ in $F_X(t)$ é

$$\binom{q+n}{n},$$

che per la 9.2.6 non é un multiplo di p . Pertanto $F_X(t)$ ha grado $n(q-1)$.

Sia ora a un nucleo di X e osserviamo che $(x-a)^{q-1}$ é una radice $(q+1)$ -esima dell'unitá in $GF(q^2)$ (cfr. 4.1). Allora, poiché ogni retta per a ha almeno un punto su X , in forza della 9.2.1 abbiamo che la successione

$$((a-x_1)^{q-1}, (a-x_2)^{q-1}, \dots, (a-x_{q+n})^{q-1})$$

contiene tutte le radici $(q+1)$ -esime dell'unitá di $GF(q^2)$ e la 9.2.5 assicura che é $F_X(a) = 0$. Resta cosí provato che ogni nucleo di X é una radice del polinomio $F_X(t)$ e quindi il numero di tali punti non può superare il grado di $F_X(t)$, cioè $n(q-1)$. \square

Come corollari della 9.2.7 si hanno subito i due seguenti teoremi.

COROLLARIO 9.2.8. *(teorema di Blokhuis-Wilbrink) Se X é un insieme di $q+1$ punti di $AG(2, q)$ risulta*

$$|N(X)| \leq q-1.$$

COROLLARIO 9.2.9. (teorema di R.Jamison) Se B é un blocking set di $AG(2, q)$ risulta

$$|B| \geq 2q - 1.$$

DIMOSTRAZIONE. Posto $|B| = q + n$, la 9.2.7 assicura che

$$|N(B)| = q^2 - q - n \leq n(q - 1),$$

da cui si ricava subito la disuguaglianza cercata. \square

OSSERVAZIONE 9.2.10. Il corollario 9.2.8 stabilisce che il massimo numero di nuclei di un insieme X di $q + 1$ punti di $AG(2, q)$ é $q - 1$. Un esempio di insieme X tale che $|N(X)| = q - 1$ si ottiene prendendo $X = \ell \cup \{a\}$, ove ℓ é una retta e a un punto non appartenente ad ℓ . Tale insieme, infatti, ha per nuclei tutti e soli i $q - 1$ punti della retta per a parallela ad ℓ e diversi da a . A parte quelli appena descritti, si conosce soltanto un altro esempio in $AG(2, 5)$ di insieme con $q + 1$ punti dotato di $q - 1$ nuclei e una congettura tuttora aperta vuole che questi siano gli unici possibili ([11],[12],[13],[62]). \square

OSSERVAZIONE 9.2.11. Il corollario 9.2.9 dice che un blocking set di ordine minimo in $AG(2, q)$ deve avere $2q - 1$ punti e la 9.1.5 prova che tali blocking set esistono. Il problema di descrivere tutti i blocking set di ordine minimo in $AG(2, q)$ é tuttora aperto. \square

OSSERVAZIONE 9.2.12. La limitazione di cui al corollario 9.2.9 per il numero di punti di un blocking set di $AG(2, q)$ non vale in generale in un piano non desarguesiano. Per esempio, A.A. Bruen e M.J. de Resmini hanno costruito in [24] un blocking set d'ordine 16 per un piano affine non desarguesiano d'ordine 9. Al momento, per quanto riguarda i piani affini non desarguesiani, non é nota alcuna limitazione significativa per il minimo numero di punti di un blocking set. \square

ESERCIZIO 9.2.13. In $PG(2, q)$ siano X un insieme di punti d'ordine maggiore di $q - 1$ ed L un insieme di punti disgiunto da X . Provare che L é una retta esterna ad X se, e solo se, ogni retta incidente X interseca L in esattamente un punto.

9.3 Blocking set nei piani proiettivi

Sia π_n un piano proiettivo finito d'ordine n .

PROPOSIZIONE 9.3.1. Se B é un blocking set in π_n e ℓ una retta, risulta

$$|B \cap \ell| \leq |B| - n.$$

In particolare, se é $|B| = n + k$, allora ogni retta di π_n interseca B in al piú k punti.

DIMOSTRAZIONE. Sia P un punto di ℓ non appartenente a B . Poiché ogni retta per P contiene almeno un punto di B , abbiamo $n + |B \cap \ell| \leq |B|$, da cui segue l'asserto. \square

DEFINIZIONE 9.3.2. Sia B un blocking set di π_n d'ordine $n + k$. Una retta ℓ che intersechi B in k punti si chiama *retta di Rédei*. Un blocking set per il quale esista almeno una retta di Rédei prende il nome di *blocking set di Rédei*. \square

ESERCIZIO 9.3.3. *Provare che un sottopiano di Baer di π_n è un blocking set di Rédei e calcolare il numero delle sue rette di Rédei.*

ESERCIZIO 9.3.4. *Provare che un arco hermitiano di π_n non ammette rette di Rédei.*

ESERCIZIO 9.3.5. *Sia K un k -arco massimale di π_n con $k < n + 1$. Provare che l'insieme delle rette secanti K è un blocking set minimale nel piano duale di π_n .*

ESERCIZIO 9.3.6. *Siano ℓ una retta di π_n , $\alpha = \pi_n \setminus \{\ell\}$ e X un insieme di n punti non allineati di α . Si denoti con $D(X)$ l'insieme dei punti di ℓ appartenenti ad almeno una retta secante X e si supponga $D(X) \neq \ell$.*

Provare che l'insieme

$$B(X) = X \cup D(X)$$

è un blocking set minimale di π_n e che ℓ è una sua retta di Rédei. Il blocking set $B(X)$ si chiama blocking set di Rédei associato ad X .

Provare inoltre che ogni blocking set di Rédei minimale di π_n è del tipo precedentemente descritto.

PROPOSIZIONE 9.3.7. *(teorema di A.A.Bruen) Se B è un blocking set di π_n , risulta*

$$|B| \geq n + \sqrt{n} + 1,$$

l'uguaglianza avendosi se, e soltanto se, n è un quadrato e B un sottopiano di Baer.

DIMOSTRAZIONE. Posto $|B| = n + k$ e detto s il massimo numero di punti comuni a B e ad una retta, risulta $s \leq k$ (cfr.9.3.1). Dunque, le equazioni dei caratteri (cfr.7.1) di B sono

$$\sum_{j=0}^s t_j = n^2 + n + 1,$$

$$\sum_{j=1}^s j t_j = (n + k)(n + 1),$$

$$\sum_{j=2}^s j(j-1)t_j = (n + k)(n + k - 1).$$

Moltiplicando la prima equazione per $-k$, la seconda per k , la terza per -1 e sommando, abbiamo

$$\sum_{j=2}^s (j-1)(k-j)t_j = n(k^2 - 2k - n + 1) \quad (9.1)$$

e, essendo il primo membro della 9.1 non negativo, deve essere

$$k^2 - 2k - n + 1 \geq 0.$$

Poiché l'equazione in k

$$k^2 - 2k - n + 1 = 0$$

ha una radice negativa ed una positiva, data da $k = \sqrt{n} + 1$, ne segue che $k \geq \sqrt{n} + 1$, cioè la prima parte dell'asserto.

Supponiamo ora che n sia un quadrato e $|B| = n + \sqrt{n} + 1$. In queste ipotesi, la 9.1 diventa

$$\sum_{j=2}^s (j-1)(\sqrt{n}+1-j)t_j = 0$$

e, essendo $t_s > 0$ e

$$(j-1)(\sqrt{n}+1-j)t_j \geq 0$$

per ogni $j = 2, 3, \dots, s-1$, deve per forza essere

$$s = \sqrt{n} + 1 \text{ e } t_2 = t_3 = \dots = t_{\sqrt{n}} = 0.$$

Ne segue che ogni retta di π_n interseca B in 1 o $\sqrt{n} + 1$ punti e da ciò si ha facilmente che B è un sottopiano di Baer (cfr.7.2.6). \square

Notiamo che esiste anche una limitazione superiore per il numero di punti di un blocking set minimale. Essa è fornita dal seguente teorema [25], di cui omettiamo la dimostrazione.

PROPOSIZIONE 9.3.8. (teorema di A.A.Bruen-J.A.Thas) *Se B è un blocking set minimale di π_n , risulta*

$$|B| \leq n\sqrt{n} + 1,$$

l'uguaglianza avendosi se, e soltanto se, n è un quadrato e B un arco hermitiano.

9.4 Blocking set in $PG(2, q)$

Il teorema di Bruen 9.3.7 fornisce la migliore limitazione inferiore per il numero dei punti di un blocking set in un piano proiettivo finito d'ordine quadrato. Se il piano è coordinabile su un campo finito e il suo ordine non è un quadrato, la disuguaglianza di Bruen può essere migliorata ed è appunto di questo problema che ci occuperemo nel presente paragrafo.

Ricordiamo che un polinomio $f \in GF(q)[x]$ si dice *completamente riducibile* se può scomporsi nel prodotto di fattori lineari su $GF(q)$.

LEMMA 9.4.1. *Sia $f(x)$ un polinomio completamente riducibile a coefficienti in $GF(q)$, $q = p^h$, e del tipo*

$$f(x) = x^q g(x) + h(x),$$

ove $g(x), h(x) \in GF(q)[x]$. Sia inoltre k il massimo fra i gradi di $g(x)$ e $h(x)$ e si supponga $k < q$. Allora esiste un intero positivo s tale che $f(x)$ appartiene a $GF(q)[x^{p^s}]$ se, e solo se, $g(x)$ e $h(x)$ appartengono a $GF(q)[x^{p^s}]$.

DIMOSTRAZIONE. E' chiaro che, se $g(x), h(x) \in GF(q)[x^{p^s}]$, cioé

$$g(x) = (g_1(x))^{p^s} \text{ e } h(x) = (h_1(x))^{p^s},$$

risulta

$$f(x) = \left(x^{p^{h-s}} g_1(x) + h_1(x) \right)^{p^s} \in GF(q)[x^{p^s}].$$

Mettiamoci dunque nell'ipotesi che $f(x) \in GF(q)[x^{p^s}]$ e osserviamo che la derivata

$$f^{(p^s)}(x) = x^q g^{(p^s)}(x) + h^{(p^s)}(x)$$

d'ordine p^s di $f(x)$ é il polinomio nullo, onde

$$x^q g^{(p^s)}(x) = -h^{(p^s)}(x).$$

Dal confronto dei gradi dei polinomi che compaiono nella precedente uguaglianza ricaviamo che i polinomi $g^{(p^s)}(x)$ e $h^{(p^s)}(x)$ sono nulli e, di conseguenza, appartengono a $GF(q)[x^{p^s}]$. \square

PROPOSIZIONE 9.4.2. (teorema di A.Blokhuis) Sia $f(x)$ un polinomio completamente riducibile a coefficienti in $GF(q)$, $q = p^h$, e del tipo

$$f(x) = x^q g(x) + h(x),$$

ove $g(x), h(x)$ sono coprimi. Sia inoltre k il massimo fra i gradi di $g(x)$ e $h(x)$. Allora si ha una delle seguenti possibilitá:

- (i) $k = 0$,
- (ii) $k = 1$ e $f(x) = a(x^q - x)$, con $a \in GF(q)^*$,
- (iii) $q = p$ é primo e $k \geq \frac{p+1}{2}$,
- (iv) q é un quadrato, cioé $h = 2e$ e $k \geq p^e$,
- (v) q non é un quadrato, cioé $h = 2e + 1$ e $k \geq p^{e+1}$.

DIMOSTRAZIONE. Se l'intero k é maggiore di $q - 1$, l'asserto é banalmente verificato; supponiamo quindi $k < q$. In questa ipotesi, il piú grande intero t per cui $f(x) \in GF(q)[x^{p^t}]$ é anche il piú grande intero tale che $g(x), h(x) \in GF(q)[x^{p^t}]$ (cfr.9.4.1) e abbiamo

$$f(x) = (f_1(x))^{p^t} = \left(x^{p^{h-t}} g_1(x) + h_1(x) \right)^{p^t},$$

con

$$g(x) = (g_1(x))^{p^t}, \quad h(x) = (h_1(x))^{p^t}$$

e i polinomi derivati $f'_1(x), g'_1(x), h'_1(x)$ sono non nulli.

Nel caso $t = h$, i gradi di $g(x)$ e $h(x)$ devono essere multipli di $p^h = q$ e, avendo supposto $k < q$, non può che essere $k = 0$, cioé la (i).

Supponiamo dunque

$$\frac{h}{2} \leq t < h$$

e osserviamo che non può essere $k < p^t$. In tale ipotesi, infatti, i polinomi $g(x)$ e $h(x)$ risulterebbero costanti e avremmo

$$f(x) = x^q a + b = (xa + b)^q,$$

con $a, b \in GF(q)$ e $t = h$, il che è escluso. Allora abbiamo $k \geq p^t$, da cui segue $k \geq p^e$, nel caso $q = p^{2e}$ sia potenza pari di p , e $k \geq p^{e+1}$, nel caso $q = p^{2e+1}$ sia potenza dispari di p ; cioè le (iv) e (v).

Supponiamo ora

$$0 \leq t < \frac{h}{2}$$

e poniamo

$$F_1(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_c),$$

ove $\alpha_1, \alpha_2, \dots, \alpha_c$ sono le radici distinte di $f_1(x)$ in $GF(q)$. Il polinomio $F_1(x)$, dividendo $x^q - x$ e $f_1(x)$, divide

$$(f_1(x))^{p^t} - (x^q - x)g(x) = f(x) - (x^q - x)g(x) = xg(x) + h(x),$$

mentre $f_1(x)/F_1(x)$, dividendo $f_1'(x)$ e $f_1(x)$, divide

$$f_1'(x)g_1(x) - f_1(x)g_1'(x) = h_1'(x)g_1(x) - h_1(x)g_1'(x).$$

Da queste due relazioni di divisibilità segue che

$$f_1(x) \text{ divide } (xg(x) + h(x))(h_1'(x)g_1(x) - h_1(x)g_1'(x)). \quad (9.2)$$

Nel caso $xg(x) + h(x)$ è il polinomio nullo, essendo $g(x)$ e $h(x)$ coprimi, si ottiene che $g(x) = a$ è una costante non nulla, $h(x) = -ax$ e

$$f(x) = a(x^q - x),$$

da cui $t = 0$, $k = 1$, cioè la (ii).

Sia allora $xg(x) + h(x)$ non nullo. Poiché $h_1'(x)g_1(x) - h_1(x)g_1'(x)$ è non nullo, essendo $g_1(x)$ e $h_1(x)$ coprimi e $g_1'(x)$ e $h_1'(x)$ diversi da zero, dalla 9.2 otteniamo

$$\deg(f_1) \leq \deg(xg + h) + \deg(h_1'g_1 - h_1g_1') \quad (9.3)$$

e possiamo distinguere i seguenti tre casi:

$$(1) \quad k = \deg(h) > \deg(g),$$

$$(2) \quad k = \deg(g) > \deg(h),$$

$$(3) \quad k = \deg(g) = \deg(h).$$

Nel primo caso, dalla 9.3 abbiamo

$$\frac{q}{p^t} + \deg(g_1) \leq \deg(f_1) \leq k + \frac{k}{p^t} - 1 + \deg(g_1),$$

da cui segue

$$\frac{k}{p^t} \geq \left\lceil \frac{p^{h-t} + 1}{p^t + 1} \right\rceil. \quad (9.4)$$

Nel secondo caso, dalla 9.3 abbiamo

$$\deg(f_1) = \frac{q}{p^t} + \frac{k}{p^t} \leq k + 1 + 2 \left(\frac{k}{p^t} - 1 \right),$$

da cui segue ancora la 9.4.

Nel terzo caso, osserviamo che i polinomi $h'_1(x)g_1(x)$ e $h_1(x)g'_1(x)$ hanno lo stesso coefficiente di grado $2\frac{k}{p^t} - 1$ e, di conseguenza, il polinomio $h'_1(x)g_1(x) - h_1(x)g'_1(x)$ ha grado non superiore a $2(\frac{k}{p^t} - 1)$. Allora, ragionando come nei casi precedenti, si ottiene di nuovo la 9.4.

Ciò premesso, se $q = p$ è primo, risulta $t = 0$ e dalla 9.4 si ottiene subito

$$k \geq \frac{p+1}{2},$$

cioè la (iii).

Se poi $q = p^{2e}$ è un quadrato, la 9.4 assicura che

$$k \geq \frac{p^{2e} + p^t}{p^t + 1} > \frac{p^{2e} + p^t}{p^e} > p^e + \frac{p^t}{p^e} > p^e,$$

cioè la (iv).

Se, infine, $q = p^{2e+1}$ è potenza dispari di p , essendo $t < \frac{h}{2} = e + \frac{1}{2}$, risulta $t \leq e$. Allora, se è $t = e$, dalla 9.4 ricaviamo

$$\frac{k}{p^e} \geq \left\lceil \frac{p^{e+1} + 1}{p^e + 1} \right\rceil = \left\lceil p - \frac{p-1}{p^e + 1} \right\rceil \geq p,$$

da cui segue $k \geq p^{e+1}$, cioè la (v). Se invece è $t < e$, abbiamo

$$\begin{aligned} \frac{p^{2e+1} + p^t}{p^t + 1} - p^{e+1} &\geq 0 \Leftrightarrow \\ p^t &\leq \frac{p^{2e+1} - p^{e+1}}{p^{e+1} - 1} = p^e - 1 + \frac{p^e - 1}{p^{e+1} - 1} \Leftrightarrow \\ p^t &\leq p^e - 1 \Leftrightarrow t < e. \end{aligned}$$

Allora, dalla 9.4 ricaviamo

$$k \geq p^t \left\lceil \frac{p^{h-t} + 1}{p^t + 1} \right\rceil \geq \frac{p^{2e+1} + p^t}{p^t + 1} \geq p^{e+1},$$

cioè ancora la (v). L'asserto è così completamente provato. \square

PROPOSIZIONE 9.4.3. (teorema di A.Blokhuis) Siano $q > 2$ e B un blocking set di $PG(2, q)$. Allora risulta

$$|B| \geq \begin{cases} p + \frac{p+3}{2} & \text{se } q = p \\ p^{2e} + p^e + 1 & \text{se } q = p^{2e}, e > 0 \\ p^{2e+1} + p^{e+1} + 1 & \text{se } q = p^{2e+1}, e > 0 \end{cases} .$$

DIMOSTRAZIONE. Senza ledere le generalit  del problema, supponiamo che B sia minimale, che contenga $q + n + 1$ punti e assumiamo $n < q$, altrimenti l'asserto   banale. Allora esiste almeno un punto $P \in B$ per cui passa una retta tangente ℓ_∞ a B ; supponiamo che sia $P = (1, 0, 0)$ e ℓ_∞ la retta di equazione $x_2 = 0$. In queste ipotesi, l'insieme $X = B \setminus \{(1, 0, 0)\}$ pu  essere considerato come un insieme di $q + n$ punti del piano affine $AG(2, q) = PG(2, q) \setminus \{\ell_\infty\}$. Poniamo dunque

$$X = \{P_i = (a_i, b_i) : i = 1, 2, \dots, q + n\},$$

ove (a_i, b_i) sono le coordinate affini di P_i in $AG(2, q)$.

Poich  ogni retta non orizzontale di $AG(2, q)$ (i.e. non parallela all'asse coordinato $y = 0$) ha almeno un punto in comune con X , ogni equazione

$$x + uy + t = 0,$$

con $u, t \in GF(q)$, ha qualche soluzione in X , cio  $a_i + ub_i + t = 0$ per un opportuno indice i . Ne segue che il polinomio $F(t, u)$ definito da

$$F(t, u) = \prod_{i=1}^{q+n} (a_i + ub_i + t) \quad (9.5)$$

  identicamente nullo su $GF(q)$.

Osserviamo esplicitamente che il coefficiente in $F(t, u)$ di t^{q+n}   1, mentre quello di u^{q+n}  

$$\prod_{i=1}^{q+n} b_i,$$

che   zero se tale   almeno un b_i . Ne segue che $F(t, u)$ ha grado $q + n$, che il grado di $F(t, u)$ nella variabile t   ancora $q + n$, mentre quello nella variabile u   al pi  $q + n$.

Osserviamo ancora che, in forza della 5.1.4, $F(t, u)$   del tipo

$$F(t, u) = (t^q - t)G(t, u) + (u^q - u)H(t, u),$$

ove $G(t, u)$ e $H(t, u)$ sono polinomi di grado al pi  n . Il polinomio $G(t, u)$, per quanto osservato precedentemente, deve avere grado n rispetto alla variabile t .

Consideriamo ora la parte $F_0(t, u)$ di $F(t, u)$ che   omogenea di grado $q + n$, cio 

$$F_0(t, u) = \prod_{i=1}^{q+n} (t + ub_i),$$

e notiamo che risulta

$$F_0(t, u) = t^q G_0(t, u) + u^q H_0(t, u),$$

ove $G_0(t, u)$ e $H_0(t, u)$ sono le parti omogenee di grado n rispettivamente di $G(t, u)$ e $H(t, u)$. Per quanto detto prima, il grado di $H_0(t, u)$ rispetto alla variabile t non può superare quello di $G_0(t, u)$ rispetto alla stessa variabile.

A questo punto, posto

$$f(t) = F_0(t, 1), \quad g(t) = G_0(t, 1), \quad h(t) = H_0(t, 1),$$

abbiamo

$$f(t) = t^q g(t) + h(t) = \prod_{i=1}^{q+n} (t + b_i)$$

e

$$f^*(t) = t^q g^*(t) + h^*(t),$$

ove si é posto

$$f^* = \frac{f}{MCD(g, h)}, \quad g^* = \frac{g}{MCD(g, h)}, \quad h^* = \frac{h}{MCD(g, h)}.$$

Osserviamo esplicitamente che il grado di $h^*(t)$ non supera quello di $g^*(t)$. Se denotiamo con $q+k$ il grado di $f^*(t)$, cioè diciamo k il grado di $g^*(t)$, ricordando la forma di $f(t)$, abbiamo che esistono $q+k$ punti in X , per esempio $(a_1, b_1), (a_2, b_2), \dots, (a_{q+k}, b_{q+k})$, tali che

$$f^*(t) = t^q g^*(t) + h^*(t) = \prod_{j=1}^{q+k} (t + b_j).$$

Il polinomio $f^*(t)$, il cui grado non supera quello di $f(t)$, verifica evidentemente le ipotesi della 9.4.2 e di conseguenza, poiché k é il massimo dei gradi fra $g^*(t)$ e $h^*(t)$, abbiamo una delle seguenti possibilità:

- (1) $k = 0$,
- (2) $k = 1$ e $f^*(t) = a(t^q - t)$,
- (3) $q = p$ e $k \geq \frac{p+1}{2}$,
- (4) $q = p^{2e}$, $e > 0$ e $k \geq p^e$,
- (5) $q = p^{2e+1}$, $e > 0$ e $k \geq p^{e+1}$.

Il primo caso non può verificarsi, altrimenti g^* e h^* sarebbero due costanti a, b e avremmo

$$f^*(t) = t^q a + b = (at + b)^q$$

e, avendo f^* coefficiente direttore uguale ad 1, dovrebbe essere $a = 1$ e quindi

$$f^*(t) = (t + b)^q.$$

L'ultima uguaglianza significa che nel secondo membro della 9.5 esistono q fattori distinti del tipo $(a_i + ub + t)$ e cioè che ogni punto della retta affine $y = b$ appartiene ad X , così la retta di $PG(2, q)$ di equazione $x_2 = bx_3$ dovrebbe essere tutta contenuta in B , il che non é possibile.

Neanche il secondo caso può essere verificato, altrimenti avremmo $g(t) = a$ e $h(t) = -at$, contro il fatto che il grado di $h(t)$ non supera quello di $g(t)$.

Dai rimanenti tre possibili casi, tenendo presente che é

$$q + n = |B| - 1 = \deg(F) \geq \deg(f) \geq \deg(f^*) = q + k,$$

segue subito l'asserto. □

Descriviamo ora alcuni metodi per costruire blocking set minimali.

ESEMPIO 9.4.4. In $GF(q)$, con q dispari, denotiamo con Q l'insieme dei suoi quadrati non nulli. Consideriamo in $PG(2, q)$ l'insieme

$$B = \{(0, 1, -s), (-s, 0, 1), (1, -s, 0) : s \in Q\} \cup \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

e osserviamo che, se una retta interseca i lati del triangolo fondamentale nei punti $(0, 1, -a)$, $(-b, 0, 1)$, $(1, -c, 0)$, allora $abc = 1 \in Q$. Ne segue che almeno uno fra a, b, c é un quadrato in $GF(q)$ (cfr.4.3.4) e quindi B é un blocking set. Dalla 4.3.3 si ha subito che

$$|B| = q + \frac{q+3}{2}. \tag{9.6}$$

Il blocking set appena costruito risulta di Rédei e prende il nome di *triangolo proiettivo*. □

ESEMPIO 9.4.5. Siano x_0, x_1, x_2 coordinate proiettive di $PG(2, q)$, ℓ_∞ la retta di equazione $x_2 = 0$ e $AG(2, q) = PG(2, q) \setminus \ell_\infty$. Per ogni funzione

$$f : GF(q) \rightarrow GF(q),$$

si consideri il grafico X_f di f in $AG(2, q)$, si ponga cioè

$$X_f = \{(a, f(a)) : a \in GF(q)\}.$$

Poiché $D(X_f)$ é in corrispondenza biunivoca con l'insieme dei coefficienti angolari delle rette di $AG(2, q)$ secanti X_f , il suo ordine é pari al numero di elementi dell'insieme

$$\left\{ \frac{f(a) - f(b)}{a - b} : a, b \in GF(q), a \neq b \right\}.$$

Ora, nell'ipotesi $D(X_f) \neq \ell_\infty$, poiché $|X_f| = q$, si può considerare il blocking set di Rédei $B(X_f)$ associato a X_f e risulta

$$|B(X_f)| = q + |D(X_f)|. \tag{9.7}$$

Ne segue che i blocking set di Rédei minimali di $PG(2, q)$ aventi ℓ_∞ come retta di Rédei e non contenenti il punto $(0, 1, 0)$ sono tutti del tipo $B(X_f)$. □

PROPOSIZIONE 9.4.6. Sia $q = q_1^m$ e denotiamo con $T = T_{q_1}$ la traccia di $GF(q)$ su $GF(q_1)$, cioè

$$T : a \in GF(q) \rightarrow a + a^{q_1} + a^{q_1^2} + \dots + a^{q_1^{m-1}} \in GF(q_1) (\subset GF(q)).$$

In $AG(2, q)$ sia X il grafico della funzione $y = T(x)$ e sia $B(X)$ il blocking set di Rédei di $PG(2, q)$ associato a X . Allora risulta

$$|B(X)| = q + \frac{q}{q_1} + 1. \quad (9.8)$$

DIMOSTRAZIONE. Ricordiamo che la funzione traccia é lineare su $GF(q_1)$ e osserviamo che, in forza dell'esercizio 9.4.5 e della 9.7, dobbiamo calcolare l'ordine $t(q_1)$ dell'insieme

$$\left\{ \frac{T(a) - T(b)}{a - b} = \frac{T(a - b)}{a - b} : a, b \in GF(q), a \neq b \right\} = \left\{ \frac{T(a)}{a} : a \in GF(q)^* \right\}.$$

Osserviamo ancora che, se $a, b \notin Ker(T)$, si ha

$$\frac{T(a)}{a} = \frac{T(b)}{b} \Rightarrow \frac{T(a)}{T(b)} = \frac{a}{b} \in GF(q_1)$$

e

$$\frac{a}{b} \in GF(q_1) \Rightarrow bT(a) = b \frac{a}{b} T(a) = b \frac{a}{b} T\left(\frac{b}{a}a\right) = aT(b) \Rightarrow \frac{T(a)}{a} = \frac{T(b)}{b};$$

cióé

$$\frac{T(a)}{a} = \frac{T(b)}{b} \Leftrightarrow \frac{a}{b} \in GF(q_1)^*.$$

Dalla relazione trovata, ricordando che

$$Ker(T) = \{c^{q_1} - c : c \in GF(q)\}$$

(cfr. dimostrazione della 4.4.3) contiene esattamente q_1^{m-1} elementi e che la funzione traccia é suriettiva, segue che

$$t(q_1) = 1 + \frac{(q-1) - (q_1^{m-1} - 1)}{q_1 - 1} = 1 + \frac{q - q_1^{m-1}}{q_1 - 1} = 1 + q_1^{m-1},$$

cióé l'asserto. □

Le 9.4.4 e 9.4.6 provano che le limitazioni per il numero di punti di un blocking set trovate con la 9.4.3 sono le migliori possibili nei casi $q = p$ e $q = p^3$, p primo. Nel caso $q = p^{2e+1}$, con $e > 1$, non é noto se esistano o meno in $PG(2, q)$ blocking set con $p^{2e+1} + p^{e+1} + 1$ punti. Il Lettore interessato ad altri risultati sull'argomento può consultare [10].