Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odjel

Maja Andrić

Blokade konačnih projektivnih ravnina

Magistarski rad

Voditelj rada:
prof.dr.sc. Juraj Šiftar

Zagreb, 2009.

Sadržaj

Uvod

Blokada $\mathcal{B}$ je skup točaka projektivne ili afine ravnine gdje svaki pravac ravnine sadrži barem jednu točku iz $\mathcal{B}$. Najzanimljivija pitanja vezana za blokadu su "koja je veličina najmanje blokade?" te "koje su moguće veličine minimalnih blokada?". Za blokadu kažemo da je *minimalna* ako se uklanjanjem neke njene točke ne može dobiti blokada. U projektivnoj ravnini blokada je minimalna ako je pravac ili ako ne sadržava neki pravac, tj. sve njegove točke. Ako blokada projektivne ravnine sadrži sve točke nekog pravca, onda je nazivamo *trivijalnom* blokadom, no od stvarnog interesa su samo *netrivijalne* blokade. Za afine ravnine ovakvih uvjeta na nesadržavanje točaka nekog pravca nema. U ovom radu proučavaju se i blokade u Desarguesovim ravninama $PG(2,q)$ i $AG(2,q)$, gdje su ocjene veličine blokade još bolje.

Početak proučavanja blokada vezuje se za Jane di Paola koja je 1969. u [20] odredila minimalne veličine netrivijalnih blokada za projektivne ravnine reda 4,5,7,8 i 9, te je opisala strukture najmanjih netrivijalnih blokada u projektivnim ravninama reda 3, 4, 5 i 9. Problem blokade datira iz još ranijeg doba. Blokada se kao pojam prvi put javlja 1956. u teoriji igara. Tada Richardson u [28] definira konačnu projektivnu ravninu igre tako što za igrače uzima točke ravnine i označava pravce ravnine kao minimalne dobitne koalicije. Tada je *blokirajuća koalicija* skup točaka koja ne sadrži pravac, ali siječe svaki pravac. Tu je riješen i problem određivanja najmanje moguće netrivijalne blokade za ravninu reda 3. Još ranije, 1944. von Neumann i Morgenstern u [30] pokazali su da u ravnini reda 2 ne postoji netrivijalna blokada.

U prvom od sedam poglavlja dan je kratak pregled osnovnih svojstava konačnih polja, te projektivnih i afinih ravnina, s naglaskom na kratnosti polinoma, obzirom da su polinomi nad konačnim poljima od posebne važnosti za određivanje veličine blokade.

Veliki napredak u proučavanju blokada je Bruenov rezultat: za blokadu $\mathcal{B}$ projektivne ravnine reda q vrijedi $card\ \mathcal{B} \geq q + \sqrt{q} + 1$ ([12], [13]). Ovo je pokazano u drugom poglavlju, kao i to da za minimalnu blokadu vrijedi $card\ \mathcal{B} \leq q\sqrt{q} + 1$. U istom poglavlju dovodi se u vezu blokada i k-luk ravnine (skup točaka kod kojeg su najviše dvije njegove točke kolinearne).

Pregled blokada projektivnih ravnina reda $q \leq 11$ dan je u trećem poglavlju. Navode se primjeri projektivnih trovrha, projektivnih trijada, Baerovih podravnina i Hermiteovih lukova.

Polinom je *lakunaran* ako su mu jedan ili više uzastopnih koeficijenata nakon vodećeg člana jednaki nuli. Teoriju potpuno reducibilnih lakunarnih polinoma razvio je Rédei te ju primijenio, među ostalim, na ocjenu broja smjerova određenim grafom

funkcije nad konačnim poljem ([27]). Njegovi rezultati korišteni su u određivanju veličina blokada u Desarguesovim projektivnim ravninama, što je sadržaj četvrtog poglavlja.

Za blokadu od $q+m$ točaka u $PG(2,q)$ kažemo da je *Rédeijeva blokada* ako postoji pravac ravnine koji siječe blokadu u m točaka. Ove blokade su razmatrane u petom poglavlju te se navode primjeri Rédeijevih blokada konstruiranih iz funkcija nad konačnim poljem. Njihova veličina je također ocijenjena pomoću lakunarnih polinoma.

U šestom poglavlju proučavaju se *višestruke blokade* projektivne ravnine. Ako ih svaki pravac ravnine siječe u barem t točaka, onda ih nazivamo t-strukim blokadama, a osnovni rezultat njihove veličine u ravnini reda q je $card\ \mathcal{B} \geq tq + \sqrt{tq} + 1$. Ova ocjena je poboljšana za višestruke blokade u Desarguesovim projektivnim ravninama. Posebno su pokazani rezultati za dvostruke blokade. Analogno drugom poglavlju, ovdje se prikazuje veza višestrukih blokada i lukova višeg reda.

Blokade afine ravnine $AG(2,q)$ razmatrane su u sedmom poglavlju. Za njihovu veličinu vrijedi ocjena $card\ \mathcal{B} \geq 2q-1$ i ona je znatno veća od one za blokadu projektivne ravnine, no najbolja je moguća. Ako promatramo t-struku blokadu $\mathcal{B}$ u projektivnoj ravnini $PG(2,q)$ i ako ona sadrži sve točke nekog pravca l, onda je $\mathcal{B} \setminus l$ $(t-1)$-struka blokada u $AG(2,q) = PG(2,q) \setminus l$. Za veličinu t-struke blokade afine ravnine vrijedi $card\ \mathcal{B} \geq (t+1)(q-1)+1$.

Iskreno se zahvaljujem svom mentoru, prof. dr. sc. Juraju Šiftaru na ukazanom strpljenju i razumijevanju te motivaciji i pomoći pri nastajanju ovog rada.

Poglavlje 1

Projektivne ravnine

1.1 Konačna polja

1. Uređena trojka $(K, +, \cdot)$, koja se sastoji od nepraznog skupa K te dviju binarnih operacija $+$ i $\cdot$ definiranih na tom skupu, naziva se *polje*, ako vrijedi:

   (i) $(K, +)$ je Abelova grupa s neutralnim elementom 0;

   (ii) $(K^*, \cdot)$ je Abelova grupa s neutralnim elementom 1, gdje je $K^* = K \setminus \{0\}$;

   (iii) $x(y+z) = xy + xz, \quad (x+y)z = xz + yz, \quad \forall\, x, y, z \in K.$

2. *Konačno polje* je polje koje ima konačan broj elemenata. Taj broj naziva se *red* konačnog polja.

3. Najmanji $p \in \mathbb{N}$ sa svojstvom

$$px = \underbrace{x + x + \cdots + x}_{p} = 0, \quad \forall x \in K,$$

   naziva se *karakteristika* polja K. Ako takav p ne postoji, onda kažemo da je K polje karakteristike 0. Karakteristika p je prim broj. Karakteristika konačnog polja ne može biti 0.

4. $(\mathbb{Z}_p, +_p, \cdot_p)$ je konačno polje reda p uz operacije zbrajanje i množenje *mod* p, gdje je p prim broj, tj. $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ se sastoji od ostataka dijeljenja s p u skupu $\mathbb{Z}$. Polje $\mathbb{Z}_p$ je karakteristike p.

5. Neka je L polje i $K \subseteq L$ također polje obzirom na operacije u L. Tada se L naziva *proširenje* od K, a K *potpolje* od L. Najmanje potpolje od L je presjek svih njegovih potpolja. Svako polje L ima najmanje potpolje koje zovemo *prosto potpolje* i ono je izomorfno ili polju racionalnih brojeva $\mathbb{Q}$ ili polju $\mathbb{Z}_p$. U prvom slučaju je polje L karakteristike 0, a u drugom je L karakteristike p.

6. *Polinom n-tog stupnja* nad poljem K je izraz $f(x)$ oblika

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in K.$$

Za polinom $f(x)$ kažemo da je *normiran* ukoliko je $a_n = 1$.
S $K[x]$ označavamo prsten polinoma nad poljem K u varijabli x.

Ako za neki $b \in K$ vrijedi $f(b) = 0$, onda kažemo da je b *korijen* ili *nul-točka polinoma* $f(x)$. Tada je polinom $f(x)$ djeljiv polinomom $x - b$, tj. postoji polinom $g(x)$ nad K takav da je $f(x) = (x - b)g(x)$.
Ako je $f(x)$ djeljiv polinomom $(x - b)^m$, a nije djeljiv s $(x - b)^{m+1}$, onda za b kažemo da je *m-struki korijen polinoma* $f(x)$.
Ireducibilni polinom u $K[x]$ je polinom koji se ne može prikazati kao produkt dva nekonstantna polinoma iz $K[x]$. Nijedan korijen ireducibilnog polinoma nije sadržan u polju K.
Neka je $f(x)$ ireducibilni polinom u $K[x]$. Ako je L najmanje proširenje od K koje sadrži sve korijene polinoma $f(x)$, onda L nazivamo *poljem razlaganja* polinoma $f(x)$ nad poljem K.

7. Neka je $f(x)$ ireducibilni polinom u $K[x]$. Tada postoji polje razlaganja polinoma $f(x)$ nad K i svaka dva takva polja su izomorfna.

OSNOVNA SVOJSTVA KONAČNIH POLJA

1. Svako konačno polje karakteristike p ima p^h elemenata za neki $h \in \mathbb{N}$.

2. Za svaki prim broj p i prirodan broj h postoji jedinstveno polje (do na izomorfizam) od p^h elemenata.

Podsjetimo se da je $\mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\}$ grupa klasa ostataka modulo p, gdje je p prim broj, pri čemu se elementi ove grupe klase, dakle podskupovi od $\mathbb{Z}$ oblika $[k] = k + p\mathbb{Z}$.

DEFINICIJA 1.1 *Neka je $\mathbf{F}_p = \{0, 1, \ldots, p-1\}$, gdje je p prim broj. Definiramo li preslikavanje $\psi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbf{F}_p$ s $\psi([a]) = a$, za svaki $a \in \mathbf{F}_p$, tada se polje $(\mathbf{F}_p, +, \cdot)$ inducirano preslikavanjem ψ naziva **Galoisovo polje** reda p.*

Za Galoisovo polje $\mathbf{F}_p$ koristimo još i oznaku $GF(p)$.

Navedimo neka svojstva Galoisovog polja $GF(q)$, gdje je $q = p^h$.

(*i*) $GF(q)$ je reda q i karakteristike p.

(*ii*) $GF(q)$ je polje razlaganja polinoma $f(x) = x^q - x$ nad $GF(p)$ i vrijedi

$$x^q - x = \prod_{a \in GF(q)} (x - a).$$

(*iii*) Neka je $f(x)$ bilo koji ireducibilni polinom stupnja h nad $GF(p)$. Tada je

$$GF(q) \cong GF(p)[x]/(f(x)) = \{a_0 + a_1 t + \cdots + a_{h-1}t^{h-1} \mid a_i \in GF(p),\ f(t) = 0\}.$$

(*iv*) Multiplikativna grupa $GF(q)^*$ je ciklička grupa.
Generator grupe $GF(q)^*$ naziva se *primitivni korijen* ili *primitivni element* od $GF(q)$. Ako je s primitivni korijen, tada vrijedi

$$GF(q) = \{0, 1, \ldots, s^{q-2} \mid s^{q-1} = 1\}.$$

(*v*) Ako je $p = 2$, onda su svi elementi iz $GF(q)$ kvadrati (tj. oblika a^2).
Ako je $p \neq 2$, onda točno pola elemenata iz $GF(q)^*$ čine kvadrati.
Također vrijedi

$$q \equiv 1 (mod\ 4) \iff -1 \text{ je kvadrat u } GF(q),$$

$$q \equiv -1 (mod\ 4) \iff -1 \text{ nije kvadrat u } GF(q).$$

Npr, -1 je kvadrat u polju $GF(5)$, ali nije u polju $GF(7)$.

(*vi*) Svaki element iz $GF(q)$ se može napisati kao zbroj dva kvadrata tog polja.

(*vii*) $GF(p^n)$ ima potpolje izomorfno polju $GF(p^m)$ ako i samo ako $m \mid n$.

Elemente konačnog polja $GF(2)$ zapisujemo $GF(2) = \{0, 1\}$. Konačno polje $GF(p)$, za prim broj $p \neq 2$, pisat ćemo na sljedeći način:

$$GF(p) = \{0, 1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\}\ ,$$

tj. umjesto elementa $p - a$ pišemo $-a$, za $a \in \{0, 1, \ldots, \frac{p-1}{2}\}$. Dakle,
$GF(3) = \{0, 1, -1\}$,
$GF(5) = \{0, 1, -1, 2, -2\}$,
$GF(7) = \{0, 1, -1, 2, -2, 3, -3\}$, itd.

Izgradnju konačnog polja $GF(q)$, za $q = p^h$, tj.

$$GF(q) \cong GF(p)[x]/(f(x)),$$

gdje je $f(x)$ ireducibilni polinom stupnja h nad $GF(p)$, pokazat ćemo na primjeru polja $GF(9) = GF(3^2)$.
Prosto potpolje od $GF(9)$ je $GF(3) = \{0, 1, -1\}$ uz operacije zbrajanja i množenja *mod* 3. Kako tražimo proširenje stupnja 2 nad prostim potpoljem $GF(3)$, prvo trebamo naći normirani ireducibilni polinom stupnja 2 u $GF(3)[x]$. Svi normirani polinomi drugog stupnja su:

- $x^2, \quad x^2 + 1, \quad x^2 - 1$
- $x^2 + x, \quad x^2 + x + 1, \quad x^2 + x - 1$
- $x^2 - x, \quad x^2 - x + 1, \quad x^2 - x - 1.$

Odredimo ireducibilne polinome između ovih devet.
Svaki polinom bez slobodnog člana se može faktorizirati, pa polinomi x^2, x^2+x, x^2-x nisu ireducibilni.
Polinomi x^2-1, x^2+x+1 za korijen imaju element 1, a korijen polinoma x^2-x+1 je -1 te ni oni nisu ireducibilni.
Dakle, polinomi x^2+1, x^2+x-1 i x^2-x-1 su ireducibilni normirani polinomi u $GF(3)[x]$.
Kako je multiplikativna grupa $GF(9)^*$ ciklička, možemo odrediti njen generator, tj. primitivni korijen polja $GF(9)$.
Npr. neka je ε korijen od x^2+1. Iz $\varepsilon^2+1=0$ proizlazi da je $\varepsilon^2=-1$, tj.

$$\begin{aligned}\varepsilon^1 &= \varepsilon\\ \varepsilon^2 &= -1\\ \varepsilon^3 &= \varepsilon^2\cdot\varepsilon=-\varepsilon\\ \varepsilon^4 &= \varepsilon^2\cdot\varepsilon^2=1\end{aligned}$$

tako da ε ima red 4 i ne generira cikličku grupu reda 8 tj. ε nije primitivni element.
Promotrimo polinom x^2+x-1 i označimo s μ korijen tog polinoma. Iz $\mu^2+\mu-1=0$ slijedi da je $\mu^2=-\mu+1$. Odredimo $\mu^i, i\in\{1,2,\dots,8\}$.

$$\begin{aligned}\mu^1 &= \mu\\ \mu^2 &= -\mu+1\\ \mu^3 &= \mu^2\cdot\mu=(-\mu+1)\cdot\mu=-\mu^2+\mu=\mu-1+\mu=-\mu-1\\ \mu^4 &= \mu^3\cdot\mu=(-\mu-1)\cdot\mu=-\mu^2-\mu=\mu-1-\mu=-1\\ \mu^5 &= \mu^4\cdot\mu=-1\cdot\mu=-\mu\\ \mu^6 &= \mu^5\cdot\mu=-\mu\cdot\mu=-\mu^2=\mu-1\\ \mu^7 &= \mu^6\cdot\mu=(\mu-1)\cdot\mu=\mu^2-\mu=-\mu+1-\mu=\mu+1\\ \mu^8 &= \mu^7\cdot\mu=(\mu+1)\cdot\mu=\mu^2+\mu=-\mu+1+\mu=1\end{aligned}$$

Dakle, μ je primitivni korijen od $GF(9)$ pa su elementi ovog polja oblika

$$GF(9)=\{0,1,\mu,\dots,\mu^7 \mid \mu^2+\mu-1=0\}.$$

Ako je polinom $f(x)\in GF(q)[x]$ ireducibilan polinom stupnja s i ako je α njegov korijen u $GF(q^s)$, tada je $\{\alpha,\alpha^q,\dots,\alpha^{q^{s-1}}\}$ skup korijena tog polinoma u $GF(q^s)$.
Kad primijenimo ovo na gornji polinom x^2+x-1 i njegov korijen μ, dobijemo da je $\{\mu,\mu^3\}=\{\mu,-\mu-1\}$ skup korijena polinoma x^2+x-1 u $GF(9)$.

AUTOMORFIZMI

Permutacije skupa $\mathcal{X}$ su bijekcije sa $\mathcal{X}$ u $\mathcal{X}$. Skup svih permutacija označavamo s $\Sigma_{\mathcal{X}}$, a djelovanje permutacije $\sigma\in\Sigma_{\mathcal{X}}$ na element $x\in\mathcal{X}$ zapisujemo x^σ.
$\Sigma_{\mathcal{X}}$ je grupa obzirom na množenje permutacija koje definiramo kao kompoziciju preslikavanja, tj.

$$x^{\sigma_1\sigma_2}=(x^{\sigma_1})^{\sigma_2},\ \forall\ x\in\mathcal{X}.$$

Grupu $\Sigma_{\mathcal{X}}$ nazivamo *simetrična grupa* skupa $\mathcal{X}$, a svaku njenu podgrupu nazivamo *permutacijska grupa* skupa $\mathcal{X}$.

Permutacija σ polja K naziva se *automorfizam* ako za svaki $x, y \in K$ vrijedi

(i) $(x+y)^\sigma = x^\sigma + y^\sigma$,

(ii) $(xy)^\sigma = x^\sigma y^\sigma$.

Grupa automorfizama polja $GF(q)$, $q = p^h$, u oznaci $Aut(GF(q))$, izomorfna je grupi $\mathbb{Z}_h$, a generirana *Frobeniusovim automorfizmom* $\phi\colon GF(q) \to GF(q)$,

$$x^\phi = x^p$$

i pritom je $x^{\phi^i} = x^{p^i}$.
Također, ako je $\sigma \in Aut(GF(q))$, onda je $\sigma = \phi^i$, za neki i. Dakle,

$$Aut(GF(q)) = \{1, \phi, \phi^2, \ldots, \phi^{h-1}\}.$$

Kako je ϕ automorfizam, onda vrijedi

$$(x+y)^p = x^p + y^p, \quad \forall\ x, y \in GF(q).$$

Neka je $L = GF(\rho^m)$, $K = GF(\rho)$ i $G = G_{L/K}$ grupa automorfizama od L koji fiksiraju svaki element iz K.
Preslikavanje $Tr_{L/K}\colon L \to L$ definirano s

$$Tr_{L/K}(t) = \sum_{\sigma \in G} t^\sigma = t + t^\rho + t^{\rho^2} + \ \cdots\ + t^{\rho^{m-1}}$$

naziva se *trag*.
Preslikavanje $Norm_{L/K}\colon L \to L$ definirano s

$$Norm_{L/K}(t) = \prod_{\sigma \in G} t^\sigma = t^{1+\rho+\rho^2+\ \cdots\ +\rho^{m-1}}$$

naziva se *norma*.

Slika traga i norme je polje K. Kad se polja L i K podrazumijevaju umjesto $Tr_{L/K}$ i $Norm_{L/K}$ pišemo Tr_ρ te $Norm_\rho$.

Svojstva traga su

(i) $Tr_\rho(\alpha+\beta) = Tr_\rho(\alpha) + Tr_\rho(\beta),\ \forall \alpha, \beta \in L$;

(ii) $Tr_\rho(x\alpha) = xTr_\rho(\alpha),\ \forall \alpha \in L, x \in K$;

(iii) $Tr_\rho(x) = mx,\ \forall x \in K$;

(iv) $Tr_\rho(\alpha)^\rho = Tr_\rho(\alpha),\ \forall \alpha \in L$.

Svojstva norme su

(*i*) $Norm_\rho(\alpha\beta) = Norm_\rho(\alpha)Norm_\rho(\beta),\ \forall\alpha,\beta \in L$;

(*ii*) $Norm_\rho(\alpha) = 0 \Longleftrightarrow \alpha = 0$;

(*iii*) $Norm_\rho(x) = x^m,\ \forall x \in K$;

(*iv*) $Norm_\rho(\alpha)^\rho = Norm_\rho(\alpha),\ \forall\alpha \in L$.

Posebno, za $L = GF(q)$ i $K = GF(p)$, gdje je $q = p^h$, koristimo oznake Tr_p i $Norm_p$. Vrijedi

$$Tr_p(t) = \sum_{\sigma\in Aut(GF(q))} t^\sigma = t + t^p + t^{p^2} + \ \cdots\ + t^{p^{h-1}},$$

$$Norm_p(t) = \prod_{\sigma\in Aut(GF(q))} t^\sigma = t^{1+p+p^2+\ \cdots\ +p^{h-1}}.$$

PRIMJER 1.2 *Trag definiran na polju karakteristike 2.*

Neka je $L = GF(2^h)$ i $K = GF(2)$. Tada je

$$Tr_2(t) = t + t^2 + t^4 + \ \cdots\ + t^{2^{h-1}}.$$

Očito vrijedi $Tr_2(t)^2 + Tr_2(t) = 0,\ \forall t$, pa je ili $Tr_2(t) = 0$ ili $Tr_2(t) = 1$. Primijetimo da mora postojati neki $t \in L$ za koji je $Tr_2(t) = 1$ jer u protivnom bi svaki element polja L bio korijen polinoma $Tr_2(t)$ (koji je stupnja 2^{h-1}) što je nemoguće. Dakle,

$$L = \mathcal{T}_0 \cup \mathcal{T}_1$$

gdje je $\mathcal{T}_0 = \{t \in L \mid Tr_2(t) = 0\}$ i $\mathcal{T}_1 = \{t \in L \mid Tr_2(t) = 1\}$. Također, vrijedi

(*i*) $0 \in \mathcal{T}_0$;

(*ii*) $q = 2^{2m} \Rightarrow 1 \in \mathcal{T}_0$;

(*iii*) $q = 2^{2m+1} \Rightarrow 1 \in \mathcal{T}_1$;

(*iv*) $t \in \mathcal{T}_i \Rightarrow t^\sigma \in \mathcal{T}_i$ za svaki automorfizam $\sigma \in Aut(L)$;

(*v*) $s \in \mathcal{T}_i,\ t \in \mathcal{T}_j \Rightarrow \begin{cases} s + t \in \mathcal{T}_0 & \text{ako je } i = j \\ s + t \in \mathcal{T}_1 & \text{ako je } i \neq j \end{cases}$

(*vi*) $card\ \mathcal{T}_0 = card\ \mathcal{T}_1 = 2^{h-1}$.

KORIJENI JEDINICE

Riješimo jednadžbu oblika $x^n = 1$ u polju $GF(q)$, $q = p^h$. Neka je $d = (n, q-1)$, $e = (q-1)/d$ i s primitivni korijen od $GF(q)$. Tada vrijedi

(*i*) jednadžba ima d rješenja, i to su $x = 1, s^e, s^{2e}, \ldots, s^{(d-1)e}$;

(*ii*) jednadžba ima jedinstveno rješenje $x = 1$ ako je $d = 1$;

(*iii*) jednadžba ima n rješenja ako $n \mid (q-1)$, i to su $x = 1, s^{(q-1)/n}, \ldots, s^{(n-1)(q-1)/n}$.

Naime, neka su $u, v \in \mathbb{Z}$ takvi da je $d = u \cdot n + v \cdot (q-1)$. Tada za svako rješenje x jednadžbe $x^n = 1$ vrijedi $x^d = (x^n)^u \cdot (x^{q-1})^v = 1 \cdot 1 = 1$.

U slučaju $d = 1$ jedino je rješenje $x = 1 \Rightarrow (ii)$.

Neka je $d > 1$ i $x \neq 1$ rješenje od $x^n = 1$. Tada je $x = s^k$ za neki $k \in \mathbb{N}$, $1 \leq k < q - 1 = de$. Imamo: $x^d = s^{kd} = 1$.
Obzirom da je $kd > 1$, a s primitivni korijen, tada kd mora biti djeljiv s $q - 1 = de$, tj. $de \mid kd$, odnosno $e \mid k$. Zbog $k < de$, k može biti samo: $e, 2e, \ldots, (d-1)e \Rightarrow (i)$.

Neka $n \mid (q-1)$. Tada je $d = n$ i $e = (q-1)/n$. Uvrstimo ovo u $(i) \Rightarrow (iii)$.

1.2 Projektivne ravnine

Neka su $\mathcal{P}$ i $\mathcal{L}$ disjunktni skupovi, a $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ relacija incidencije. Elemente skupa $\mathcal{P} = \{A, B, C, \ldots\}$ nazivat ćemo **točkama**, a elemente skupa $\mathcal{L} = \{a, b, c, \ldots\}$ **pravcima**. Ako je $(P, l) \in \mathcal{I}$ tada kažemo da je točka P incidentna s pravcem l ili pravac l je incidentan s točkom P.

Uređena trojka $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ naziva se **incidencijska struktura**.

DEFINICIJA 1.3 *Incidencijska struktura $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ naziva se **projektivna ravnina** ako vrijede sljedeći aksiomi*

(P1) Postoji točno jedan pravac incidentan s dvije različite točke.

(P2) Postoji točno jedna točka incidentna s dva različita pravca.

(P3) Postoje četiri različite točke od kojih nikoje tri nisu kolinearne.

DEFINICIJA 1.4 *Podskup elemenata Π_0 projektivne ravnine Π naziva se **podravnina** od Π, ako je Π_0 projektivna ravnina obzirom na istu relaciju incidencije koja je definirana u Π.*

DEFINICIJA 1.5 *Podravnina Π_0 projektivne ravnine Π naziva se **Baerova podravnina** od Π, ako vrijedi*

(i) Svaka točka $P \in \Pi \setminus \Pi_0$ je incidentna s točno jednim pravcem iz Π_0.

(ii) Svaki pravac $p \in \Pi \setminus \Pi_0$ je incidentan s točno jednom točkom iz Π_0.

PRINCIP DUALNOSTI PROJEKTIVNE RAVNINE

Zamijenimo li u nekoj valjanoj izreci (teoremu) projektivne geometrije ravnine pojam točka dualnim pojmom pravac, i obrnuto, a pojam incidencije ostavimo nepromijenjenim, opet dobijemo neku valjanu izreku (teorem) projektivne geometrije ravnine. Za takve dvije izreke kažemo da su **dualne** jedna drugoj.
Relaciju incidencije često izričemo na način: točka P *leži na* pravcu l ili pravac l *prolazi kroz* točku P, te pišemo $P \in l$. Ako je neka točka incidentna s dva različita pravca, onda kažemo da je ta točka *sjecište* pravaca, a ako je neki pravac incidentan s dvije različite točke, onda kažemo da je taj pravac *spojnica* točaka. Dualizacija izreka u projektivnoj ravnini provodi se na sljedeći način:

točka	$\longleftrightarrow$	pravac
leži na	$\longleftrightarrow$	prolazi kroz
sjecište	$\longleftrightarrow$	spojnica

Dual projektivne ravnine je opet projektivna ravnina, pri čemu je dualan zahtjev aksiomu *(P3)* postojanje četiri različita pravca od kojih nikoja tri nisu konkurentna.

Promotrimo sada neke figure koje imaju istaknutu ulogu u projektivnim ravninama.

DEFINICIJA 1.6 *Bilo koji podskup točaka i pravaca projektivne ravnine naziva se* ***ravninska figura****.*

DEFINICIJA 1.7 *Ravninska figura koja se sastoji od n točaka u cikličkom redoslijedu, od kojih po tri susjedne nisu kolinearne, te od n spojnica parova susjednih točaka naziva se* ***(obični) n-terovrh*** *projektivne ravnine. Dane točke zovemo* ***vrhovima****, a njihove spojnice* ***stranicama*** *tog n-terovrha.*

DEFINICIJA 1.8 *Ravninska figura koja se sastoji od n točaka od kojih po tri nisu kolinearne i od $\frac{1}{2}n(n-1)$ spojnica parova točaka naziva se* ***potpuni n-terovrh*** *projektivne ravnine.*

Dualizacijom dobijemo sljedeće figure dualne običnom i potpunom n-terovrhu.

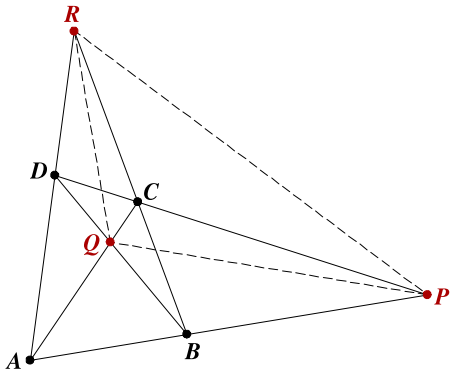
DEFINICIJA 1.9 *Ravninska figura koja se sastoji od n pravaca u cikličkom redoslijedu, od kojih po tri susjedna nisu konkurentna, te od n sjecišta parova susjednih pravaca naziva se* ***(obični) n-terostran*** *projektivne ravnine. Dane pravce zovemo* ***stranicama****, a njihova sjecišta* ***vrhovima*** *tog n-terostrana.*

DEFINICIJA 1.10 *Ravninska figura koja se sastoji od n pravaca od kojih po tri nisu konkurentna i od $\frac{1}{2}n(n-1)$ sjecišta parova pravaca naziva se* ***potpuni n-terostran*** *projektivne ravnine.*

Za $n = 3$ figure nazivamo trovrh i trostran. Trovrh je ujedno i obični i potpuni trovrh, a isto to vrijedi i za trostran.

PRIMJER 1.11 *Potpuni četverovrh projektivne ravnine.*

Potpuni četverovrh projektivne ravnine se sastoji od 4 točke A, B, C i D, od kojih po tri nisu kolinearne, te od 6 spojnica AB, AC, AD, BC, BD i CD (Slika 1.1).



Slika 1.1 *Potpuni četverovrh*

Dvije stranice koje ne prolaze istim vrhom nazivamo *parom suprotnih stranica*. To su parovi AB i CD, AC i BD, te AD i BC. Sjecišta P, Q i R parova suprotnih stranica nazivamo *dijagonalnim točkama*, a njihove spojnice PQ, QR i PR *dijagonalama* potpunog četverovrha.
Dijagonalne točke i dijagonale čine dijagonalni trovrh potpunog četverovrha.

KONAČNE PROJEKTIVNE RAVNINE

DEFINICIJA 1.12 *Projektivna ravnina koja ima konačan broj točaka i pravaca naziva se* ***konačna projektivna ravnina****.*

TEOREM 1.13 *Za konačnu projektivnu ravninu postoji* $q \in \mathbb{N}$, $q \geq 2$, *takav da vrijedi*

(*i*) *svaka točka je incidentna s* $q+1$ *pravcem;*

(*ii*) *svaki pravac je incidentan s* $q+1$ *točkom;*

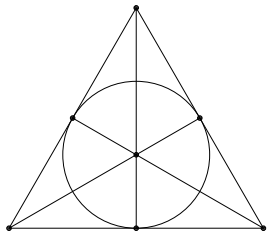
(*iii*) *postoji* q^2+q+1 *točaka;*

(*iv*) *postoji* q^2+q+1 *pravaca.*

Broj q se naziva **red** projektivne ravnine.

PRIMJER 1.14 *Projektivna ravnina reda* 2*.*

Najmanja projektivna ravnina ima red 2, a poznata je još pod nazivom i Fano-ova ravnina (Slika 1.2). Sastoji se od 7 točaka i isto toliko pravaca, svaki pravac je incidentan s 3 točke, i svaka točka je incidentna s 3 pravca.



Slika 1.2 *Fano-ova ravnina*

Za konačne projektivne ravnine moguće vrijednosti redova podravnina ograničene su sljedećim teoremom.

TEOREM 1.15 *Neka je* Π_0 *podravnina reda* p *projektivne ravnine* Π *reda* q*. Tada vrijedi jedna od tvrdnji*

(*i*) $q = p^2$,

(*ii*) $q \geq p^2 + p$.

TEOREM 1.16 *Neka je* Π_0 *podravnina reda* p *projektivne ravnine* Π *reda* q*.* Π_0 *je Baerova podravnina ako i samo ako je* $q = p^2$*.*

Baerova podravnina Π_0 ima svojstvo da svaki pravac ravnine Π sadrži ili točno jednu ili $p+1$ točku iz Π_0.

EGZISTENCIJA KONAČNIH PROJEKTIVNIH RAVNINA

Definicija projektivne ravnine je kombinatorička, ali sve poznate konstrukcije konačne projektivne ravnine se baziraju na algebri. Najjednostavnija i najvažnija konstrukcija projektivne ravnine je ona nad konačnim poljem $GF(q)$.

Neka je $\mathcal{V}$ 3-dimenzionalni vektorski prostor nad $GF(q)$, $\mathcal{P}$ skup 1-dimenzionalnih potprostora od $\mathcal{V}$, a $\mathcal{L}$ skup 2-dimenzionalnih potprostora od $\mathcal{V}$. Relaciju incidencije između $P \in \mathcal{P}$ i $l \in \mathcal{L}$ definiramo pravilom: P je incidentno s l ako i samo ako je $P \subseteq l$. Tada vrijede aksiomi projektivne ravnine:

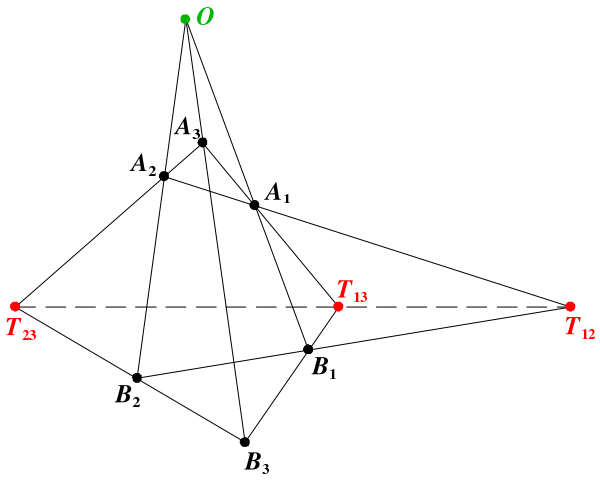
($P1$) Dva 1-dimenzionalna potprostora razapinju 2-dimenzionalni potprostor.

($P2$) Dva 2-dimenzionalna potprostora presijecaju se u 1-dimenzionalnom potprostoru.

($P3$) Postoje četiri 1-dimenzionalna potprostora od kojih nikoja tri ne razapinju 2-dimenzionalan potprostor: $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,1)$.

Ovako dobivena konačna projektivna ravnina se označava s $PG(2,q)$. Ravnine $PG(2,q)$ mogu se prepoznati među konačnim projektivnim ravninama po Desarguesovom teoremu.

TEOREM 1.17 (Desargues) *Neka su $A_1A_2A_3$ i $B_1B_2B_3$ dva trovrha projektivne ravnine. Pravci A_1B_1, A_2B_2 i A_3B_3 su konkurentni ako i samo ako su točke $T_{12} = A_1A_2 \cap B_1B_2$, $T_{13} = A_1A_3 \cap B_1B_3$ i $T_{23} = A_2A_3 \cap B_2B_3$ kolinearne.*



Slika 1.3 *Desarguesov teorem*

TEOREM 1.18 *Konačna projektivna ravnina je izomorfna ravnini $PG(2,q)$ ako i samo ako u njoj vrijedi Desarguesov teorem.*

DEFINICIJA 1.19 *Ravnina u kojoj vrijedi Desarguesov teorem nazivamo* ***Desarguesova ravnina****.*

Za $q = 2, 3, 4, 5, 7, 8$ poznato je da postoje samo Desarguesove projektivne ravnine. Također je poznato da za $q = 9$ uz Desarguesovu projektivnu ravninu postoje do izomorfizma još samo tri projektivne ravnine.

Postoje mnoge poznate projektivne ravnine koje nisu izomorfne s $PG(2, q)$, no svi poznati primjeri za red imaju broj $q = p^h$, gdje je p prim broj i $h \in \mathbb{N}$. Ovo nas dovodi do vjerojatno najpoznatijeg od mnogo neriješenih problema konačne geometrije:

PRETPOSTAVKA *Red projektivne ravnine je potencija prim broja.*

Premda za $q \neq p^h$ projektivne ravnine nisu poznate, znamo da vrijedi sljedeći teorem.

TEOREM 1.20 (Bruck-Ryser) *Ako je $q \equiv 1$ (mod 4) ili $q \equiv 2$ (mod 4), pri čemu q nije zbroj dva kvadrata, tada ne postoji projektivna ravnina reda q.*

Dakle, ne postoje ravnine reda $q = 6, 14, 21, 22, \ldots$
Za $q = 10, 12, 15, 18, \ldots$ teorem ne daje informacije. Lam, Thiel and Swiercz su pokazali, uz pomoć računala, da ne postoji projektivna ravnina reda 10 pa je najmanji mogući protuprimjer navedenoj pretpostavci ravnina reda 12.

ANALITIČKI MODEL KONAČNE PROJEKTIVNE RAVNINE $PG(2, q)$

1. Točke u $PG(2, q)$ su klase uređenih trojki

   $$\lambda(x_0, x_1, x_2) = (\lambda x_0, \lambda x_1, \lambda x_2),$$

   gdje je $x_i \in GF(q)$, $\lambda \in GF(q)^*$, uz uvjet da je isključena trojka $(0, 0, 0)$. Uređenu trojku nazivamo *homogenim koordinatama točke*. Dvije trojke (x_0, x_1, x_2) i (y_0, y_1, y_2) predstavljaju istu točku ako pripadaju istoj klasi, tj. ako postoji $\lambda \neq 0$ takav da je $(x_0, x_1, x_2) = (\lambda y_0, \lambda y_1, \lambda y_2)$. Posebnu oznaku koristimo za sljedeće točke: $\mathbf{U_0} = (1, 0, 0)$, $\mathbf{U_1} = (0, 1, 0)$, $\mathbf{U_2} = (0, 0, 1)$ i $\mathbf{U} = (1, 1, 1)$.

2. Pravci u $PG(2, q)$ su klase uređenih trojki

   $$\mu[u_0, u_1, u_2] = [\mu u_0, \mu u_1, \mu u_2],$$

   koje nazivamo *homogenim koordinatama pravca*, gdje je $u_i \in GF(q)$, $\mu \in GF(q)^*$ i isključena je trojka $[0, 0, 0]$. Dvije trojke $[u_0, u_1, u_2]$ i $[v_0, v_1, v_2]$ predstavljaju isti pravac ako postoji $\mu \neq 0$ takav da je $[u_0, u_1, u_2] = [\mu v_0, \mu v_1, \mu v_2]$. Posebnu oznaku koristimo za sljedeće pravce: $\mathbf{u_0} = [1, 0, 0]$, $\mathbf{u_1} = [0, 1, 0]$, $\mathbf{u_2} = [0, 0, 1]$ i $\mathbf{u} = [1, 1, 1]$.

3. Relacija incidencije definirana je sa:
   Točka (x_0, x_1, x_2) i pravac $[u_0, u_1, u_2]$ su incidentni ako i samo ako vrijedi

   $$u_0x_0 + u_1x_1 + u_2x_2 = 0.$$

Ako konačno polje $GF(q)$ zamijenimo poljem realnih brojeva $\mathbb{R}$, dobijemo analitički model realne projektivne ravnine, koja naravno nije konačna, ali jest Desarguesova.

1.3 Afine ravnine

DEFINICIJA 1.21 *Uređena trojka $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ naziva se* ***afina ravnina*** *ako vrijede sljedeći aksiomi*

(A1) Postoji točno jedan pravac incidentan s dvije različite točke.

(A2) Za svaku točku P koja nije incidentna s pravcem m postoji točno jedan pravac n incidentan s P takav da m i n nemaju zajedničkih točaka.

(A3) Postoje tri različite točke koje nisu kolinearne.

Za pravce afine ravnine m i n kažemo da su *paralelni* i pišemo $m \| n$, ako nemaju ni jednu zajedničku točku ($m \cap n = \emptyset$) ili su im sve točke zajedničke. Refleksivnost i simetričnost ove relacije su očite. Ako je $m \| n$ i $n \| p$, onda je $m \| p$, jer u suprotnom postoji točka $P \in m \cap p$ takva da je $P \notin n$ što je kontradikcija s $(A2)$. Dakle vrijedi i tranzitivnost pa je paralelizam relacija ekvivalencije.

Afina ravnina se može dobiti iz projektivne ravnine i obrnuto. Naime, neka je l pravac projektivne ravnine Π reda q i neka je Π^l incidencijska struktura dobivena uklanjanjem pravca l sa svim njegovim točkama iz Π. Tada za Π^l vrijede aksiomi $(A1)$ - $(A3)$, tj. Π^l je afina ravnina.
Uklonjeni pravac l se naziva *beskonačno daleki pravac* i označava l_∞. Uklanjanjem različitih pravaca iz projektivne ravnine mogu se dobiti neizomorfne afine ravnine.

Neka je $\mathcal{P}$ skup točaka afine ravnine i $\mathcal{L}$ skup pravaca, a $\mathcal{E}$ skup klasa ekvivalencije paralelnih pravaca. Svaki pravac l pripada nekoj klasi $E \in \mathcal{E}$. Definirajmo novi pravac $l^+ = l \cup \{E\}$. Incidencijska struktura čije su točke $\mathcal{P} \cup \mathcal{E}$, a pravci $\{l^+ \mid l \in \mathcal{L}\}$ i beskonačno daleki pravac $l_\infty = \{E \mid E \in \mathcal{E}\}$ je projektivna ravnina.

KONAČNE AFINE RAVNINE

TEOREM 1.22 *Za konačnu afinu ravninu postoji $q \in \mathbb{N}$, $q \geq 2$, takav da vrijedi*

(i) svaka točka je incidentna s $q+1$ pravcem;

(ii) svaki pravac je incidentan s q točaka;

(iii) postoji q^2 točaka;

(iv) postoji $q^2 + q$ pravaca.

Afina ravnina nad konačnim poljem $GF(q)$ se označava s $AG(2, q)$ i naziva se Desarguesova afina ravnina. Sve afine ravnine dobivene iz Desarguesove projektivne ravnine su međusobno izomorfne.
U ravnini $AG(2, q)$ postoji $q+1$ paralelna klasa od kojih svaka sadrži točno q pravaca. Klase ekvivalencije nazivamo *smjerovima* u ravnini. Ako promatramo projektivnu ravninu kao proširenje afine ravnine beskonačno dalekim pravcem, onda točke tog pravca odgovaraju smjerovima pravaca afine ravnine.

ANALITIČKI MODEL KONAČNE AFINE RAVNINE $AG(2,q)$

1. Točke u $AG(2,q)$ su uređeni parovi (a,b), koje nazivamo *afinim koordinatama* točke, gdje su $a,b \in GF(q)$.

2. Pravci u $AG(2,q)$ su oblika

$$\begin{aligned} y = kx + l, &\quad \text{kosi pravac} \\ y = l, &\quad \text{horizontalni pravac} \\ x = c, &\quad \text{vertikalni pravac} \end{aligned}$$

   gdje su $k,l,c \in GF(q)$.

3. Relacija incidencije definirana je sa:

   (i) Točka (a,b) i pravac $y = kx+l$ su incidentni ako i samo ako je $b = ka+l$.

   (ii) Točka (a,b) i pravac $y = l$ su incidentni ako i samo ako je $b = l$.

   (iii) Točka (a,b) i pravac $x = c$ su incidentni ako i samo ako je $a = c$.

Pogledajmo vezu između homogenih koordinata u $PG(2,q)$ i afinih u $AG(2,q)$.

1. $PG(2,q) \to AG(2,q)$

Točka projektivne ravnine je oblika (x_0,x_1,x_2). Neka je $x_2 \neq 0$. Tada je pripadna točka afine ravnine $\left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right)$.
Neka je $[u_0,u_1,u_2]$ pravac projektivne ravnine. Tada vrijedi

$$u_0x_0 + u_1x_1 + u_2x_2 = 0 \ / \ : x_2 \neq 0$$

$$u_0\frac{x_0}{x_2} + u_1\frac{x_1}{x_2} + u_2 = 0 \quad \Rightarrow \quad u_0x + u_1y + u_2 = 0.$$

Pripadni pravci afine ravnine su oblika:

$$u_0, u_1 \neq 0 \quad \to \quad y = -\frac{u_0}{u_1}x - \frac{u_2}{u_1}, \quad \text{kosi pravac}$$

$$u_0 = 0, u_1 \neq 0 \quad \to \quad y = -\frac{u_2}{u_1}, \quad \text{horizontalni pravac}$$

$$u_1 = 0 \quad \to \quad x = -\frac{u_2}{u_0}, \quad \text{vertikalni pravac}$$

2. $AG(2,q) \to PG(2,q)$

Za točku (a,b) afine ravnine, pripadna točka projektivne ravnine je oblika $(a,b,1)$. Za pravce vrijedi

$$\begin{aligned} y = kx + l &\quad \to \quad [k,-1,l], \quad \text{kosi pravac} \\ y = l &\quad \to \quad [0,-1,l], \quad \text{horizontalni pravac} \\ x = c &\quad \to \quad [-1,0,c], \quad \text{vertikalni pravac} \end{aligned}$$

BESKONAČNO DALEKI ELEMENTI

Beskonačno daleke točke T^∞ su oblika $(x_0, x_1, 0)$ i pripadaju beskonačno dalekom pravcu

$$l_\infty = \{(x_0, x_1, x_2) \mid x_2 = 0\} = [0, 0, 1] = \mathbf{u_2}.$$

Za kosi pravac je pripadana $T^\infty = (1, k, 0)$. Naime, ako je točka $(a, b, 0)$ incidentna s pravcem $[k, -1, l]$, onda vrijedi

$$k \cdot a - 1 \cdot b + l \cdot 0 = 0 \;\Rightarrow\; b = ka,$$

$$T^\infty = (a, b, 0) = (a, ka, 0) = (1, k, 0).$$

Beskonačno daleka točka horizontalnog pravac $[0, -1, l]$ je

$$0 \cdot a - 1 \cdot b + l \cdot 0 = 0 \;\Rightarrow\; b = 0,$$

$$T^\infty = (a, b, 0) = (a, 0, 0) = (1, 0, 0) = \mathbf{U_0}.$$

Za vertikalni pravac $[-1, 0, c]$ vrijedi

$$-1 \cdot a + 0 \cdot b + c \cdot 0 = 0 \;\Rightarrow\; a = 0,$$

$$T^\infty = (a, b, 0) = (0, b, 0) = (0, 1, 0) = \mathbf{U_1}.$$

1.4 Kratnosti polinoma nad konačnim poljima

Neka je $R = GF(q)[x, y]$ prsten polinoma nad poljem $GF(q)$ u varijablama x i y. Ako je f polinom u R, onda se on može prikazati kao suma članova

$$f = \sum \alpha_{ij} x^i y^j.$$

Neka je $P = (a, b) \in GF^2(q)$ točka afine ravnine $AG(2, q)$, te neka je $x_0 = x - a$, $y_0 = y - b$. Polinom f se tada može "proširiti do P" sljedećom formulom

$$f = \sum \beta_{ij} x_0^i y_0^j.$$

Neka je $t \geq 0$ najveći cijeli broj takav da za svaki $\beta_{ij} \neq 0$ vrijedi $i + j \geq t$. Tada kažemo da polinom f ima **kratnost** t **u točki** P i pišemo $\text{mult}_P f = t$. Ako je f nula polinom, onda je $\text{mult}_P f \geq t$ za svaki pozitivan cijeli broj t i pišemo $\text{mult}_P f = \infty$. Vrijede sljedeće leme.

LEMA 1.23 *Ako je* $\text{mult}_P f \geq t$ *i* $\text{mult}_P g \geq t$*, gdje su* f *i* g *polinomi iz* R*, onda vrijedi* $\text{mult}_P(f \pm g) \geq t$.

LEMA 1.24 *Neka su* f*,* g *i* h *polinomi iz* R *takvi da je* $f = gh$*. Ako je* $\text{mult}_P f \geq t$ *i* $\text{mult}_P g = s \leq t$*, onda vrijedi* $\text{mult}_P h \geq t - s$.

Neka je $t \geq 0$ cijeli broj i $J_t(x, y)$ ideal u prstenu polinoma R generiran s $(x^q - x)^i (y^q - y)^j$, gdje su $i, j \geq 0$ te $i + j = t$.

Za svaku točku $P \in AG(2, q)$ i svaki polinom $f \in J_t(x, y)$ vrijedi $\text{mult}_P f \geq t$. Pokazat ćemo da vrijedi i obrat. No prvo pogledajmo slučaj polinoma jedne varijable.

TEOREM 1.25 *Neka je* f *polinom iz* $GF(q)[x]$ *takav da je* $\text{mult}_a f \geq t$ *za svaki* $a \in GF(q)$*, gdje je* $t \geq 0$ *cijeli broj. Tada je* $f \in J_t(x)$.

Dokaz Neka je $J_t(x)$ ideal generiran s $(x^q - x)^t$. Ako je $\text{mult}_a f \geq t$ za svaki $a \in GF(q)$, onda je polinom f djeljiv s $(x - a)^t$ za svaki $a \in GF(q)$. To znači da je djeljiv i s

$$\prod_{a \in GF(q)} (x - a)^t = \Big[\prod_{a \in GF(q)} (x - a) \Big]^t = (x^q - x)^t.$$

Dakle, polinom f pripada idealu $J_t(x)$. ∎

TEOREM 1.26 *Neka je* f *polinom iz* $R = GF(q)[x, y]$ *takav da je* $\text{mult}_P f \geq t$ *za svaku točku* P *ravnine* $AG(2, q)$*, gdje je* $t \geq 0$ *cijeli broj. Tada je* $f \in J_t(x, y)$.

Dokaz Teorem ćemo dokazati indukcijom po kratnosti t. Neka je $J_t(x, y)$ ideal generiran s $(x^q - x)^{t-i} (y^q - y)^i$ za $i = 0, \ldots, t$.
Ako je $t = 0$ onda tvrdnja vrijedi trivijalno.

Neka je $\alpha_1 \in GF(q)$ i zapišimo

$$f(x,y) = (x-\alpha_1)A_1 + B_1,$$

gdje je $B_1(y) = f(\alpha_1, y)$. Po pretpostavci je $\text{mult}_P f \geq t$ za svaku točku P, pa posebno i za sve točke oblika (α_1, β). Slijedi da B_1 ima kratnost barem t za svaki $\beta \in GF(q)$ te po Teoremu 1.25 B_1 pripada idealu $J_t(y)$. No onda pripada i idealu $J_t(x,y)$. Neka je

$$f(x,y) = g(x,y) + B_1,$$

gdje je

$$g(x,y) = (x-\alpha_1)A_1.$$

Tada po Lemi 1.23 slijedi da je $\text{mult}_P g \geq t$ za svaku točku $P \in AG(2,q)$.

Neka je $\alpha_2 \in GF(q)$, $\alpha_2 \neq \alpha_1$ i zapišimo

$$A_1 = (x-\alpha_2)A_2 + B_2,$$

gdje je $B_2(y) = A_1(\alpha_2, y)$. Tada polinom

$$g(x,y) = (x-\alpha_1)(x-\alpha_2)A_2 + (x-\alpha_1)B_2$$

ima kratnost barem t, posebno u svim točkama (α_2, β). Slijedi da $(\alpha_2 - \alpha_1)B_2$ ima kratnost barem t za svaki $\beta \in GF(q)$ te po Teoremu 1.25 $(\alpha_2 - \alpha_1)B_2$, pa i B_2 pripada idealu $J_t(y)$, tj. $J_t(x,y)$. Tada je i $(x-\alpha_1)B_2 \in J_t(x,y)$ obzirom da je $J_t(x,y)$ ideal. Sada po Lemi 1.23 slijedi da polinom

$$h(x,y) = (x-\alpha_1)(x-\alpha_2)A_2$$

ima kratnost barem t za svaku točku $P \in AG(2,q)$.

Neka je $\alpha_3 \in GF(q)$, $\alpha_3 \neq \alpha_1, \alpha_2$ i zapišimo

$$A_2 = (x-\alpha_3)A_3 + B_3.$$

Nastavljajući ovako za svaki $\alpha_j \in GF(q)$, slijedi da postoje polinomi U i V takvi da vrijedi

$$f = \Big[\prod_{\alpha \in GF(q)} (x-\alpha)\Big]U + V = (x^q - x)U + V$$

gdje je V iz ideala $J_t(x,y)$. Ponovo zaključujemo da polinom $(x^q - x)U$ po Lemi 1.23 ima kratnost barem t za svaku točku $P \in AG(2,q)$. Po Lemi 1.24 slijedi da polinom U ima kratnost barem $t-1$ za svaku točku $P \in AG(2,q)$. Po indukciji slijedi da U pripada idealu $J_{t-1}(x,y)$ pa polinom $(x^q - x)U$ pripada idealu $J_t(x,y)$. Kako je $J_t(x,y)$ ideal kojem pripada i V onda slijedi da i polinom

$$f = (x^q - x)U + V$$

pripada idealu $J_t(x,y)$. ■

Poglavlje 2

Blokade projektivne ravnine

Neka je Π konačna projektivna ravnina reda q.

DEFINICIJA 2.1 *Skup $\mathcal{B}$ točaka u Π naziva se* ***blokada*** *ravnine Π ako svaki pravac ravnine Π sadrži barem jednu točku iz $\mathcal{B}$.*

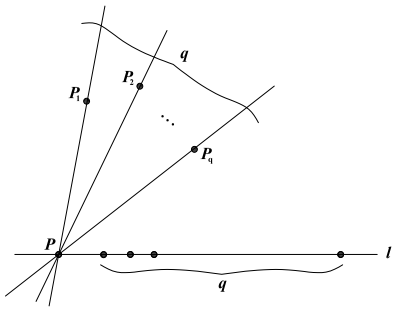
DEFINICIJA 2.2 *Blokada koja sadrži sve točke nekog pravca naziva se* ***trivijalna blokada****, inače se naziva* ***netrivijalna blokada****.*

Obzirom da su točke i pravci međusobno dualni elementi, spomenut ćemo i dualan pojam blokade. U dualnom se slučaju skup $\mathcal{B}$ pravaca u Π naziva blokada ravnine Π, ako kroz svaku točku ravnine Π prolazi barem jedan pravac iz $\mathcal{B}$. Blokada je tada trivijalna ako sadrži sve pravce kroz neku točku.

Trivijalne blokade nisu od stvarnog interesa, stoga ćemo nadalje proučavati samo netrivijalne blokade. Iz same definicije netrivijalne blokade slijedi da je njen komplement također netrivijalna blokada. Naime, budući netrivijalna blokada siječe svaki pravac ravnine i pritom ne postoji pravac ravnine čije su sve točke sadržane u blokadi, onda i skup $\Pi \setminus \mathcal{B}$ ima ista svojstva.

PRIMJER 2.3 *Netrivijalna blokada od $2q$ točaka u ravnini reda $q > 2$.*

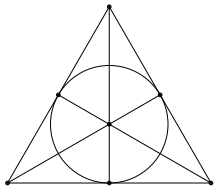
U svakoj ravnini reda $q > 2$ postoji netrivijalna blokada, a primjer za to je skup od $2q$ točaka definiran na sljedeći način. Neka je P bilo koja točka proizvoljnog pravca l u ravnini (Slika 2.1). Kroz točku P prolazi još q pravaca ravnine. Sa svakog pravca uzmimo po jednu točku, uz uvjet da su odabrane točke $\{P_1, P_2, \ldots, P_q\}$ nekolinearne. Tada one i još q točaka pravaca $l \setminus \{P\}$ čine netrivijalnu blokadu od $2q$ točaka.



Slika 2.1

PRIMJER 2.4 *Blokade projektivne ravnine* $PG(2,2)$.

Još 1944. godine von Neumann i Morgenstern pokazali su da u Fano-ovoj ravnini $PG(2,2)$ (Slika 2.2) ne postoji blokada koja ne sadrži pravac ([30]). Lako se vidi da bilo koji skup nekolinearnih točaka Fano-ove ravnine ne siječe sve pravce ravnine. Ovo je jedina projektivna ravnina koja ne sadrži netrivijalnu blokadu.



Slika 2.2 *Fano-ova ravnina*

Pod pojmom blokada podrazumijevat ćemo odsad netrivijalnu blokadu. Njen kardinalni broj, tj. broj njenih točaka, označavamo s *card* $\mathcal{B}$.

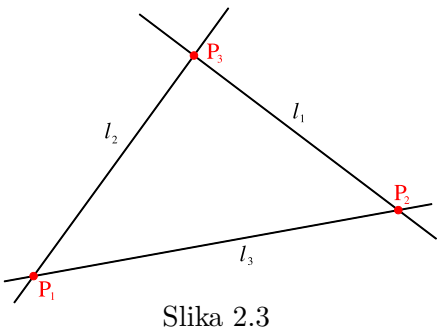
DEFINICIJA 2.5 *Blokada* $\mathcal{B}$ *je* ***minimalna*** *ili* ***ireducibilna blokada*** *ako za svaku točku* P *iz* $\mathcal{B}$ *vrijedi da skup* $\mathcal{B} \setminus \{P\}$ *nije blokada.*

LEMA 2.6 *Blokada* $\mathcal{B}$ *je minimalna ako i samo ako za svaku točku* P *iz* $\mathcal{B}$ *postoji u ravnini* Π *pravac* l *tako da je* $\mathcal{B} \cap l = \{P\}$.

Dokaz Neka je blokada $\mathcal{B}$ minimalna i neka postoji točka $P \in \mathcal{B}$ tako da svaki pravac l kroz P sadrži još jednu točku iz $\mathcal{B}$. Tada je skup $\mathcal{B} \setminus \{P\}$ blokada, odnosno $\mathcal{B}$ nije minimalna blokada.
Obrat. Pretpostavimo da $\mathcal{B}$ zadovoljava uvjet. Tada skup $\mathcal{B} \setminus \{P\}$ ne siječe pravac l, dakle nije blokada, a to znači da je $\mathcal{B}$ minimalna blokada. ■

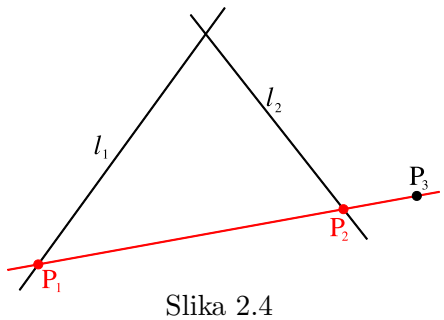
PRIMJER 2.7 *Minimalne blokade u* $PG(2,q)$.

1. Neka su l_1, l_2 i l_3 nekonkurentni pravci i neka je $\mathcal{B} = (l_1 \cup l_2 \cup l_3) \setminus \{P_1, P_2, P_3\}$ (Slika 2.3). Tada je $\mathcal{B}$ minimalna blokada od $3q - 3$ točaka.



Slika 2.3

2. Neka su P_1 i P_2 proizvoljne točke na pravcima l_1 i l_2, $P_1, P_2 \neq l_1 \cap l_2$, te neka je $P_3 \neq P_1, P_2$ točka na njihovoj spojnici (Slika 2.4). Tada je $\mathcal{B} = (l_1 \cup l_2 \cup \{P_3\}) \setminus \{P_1, P_2\}$ minimalna blokada od $2q$ točaka.



Slika 2.4

PROPOZICIJA 2.8 *Za blokadu $\mathcal{B}$ ravnine Π vrijedi card $\mathcal{B} > q + 1$.*

Dokaz Svakom točkom iz $\Pi \setminus \mathcal{B}$ prolazi $q+1$ pravac koji siječe blokadu u barem jednoj točki pa vrijedi *card* $\mathcal{B} \geq q+1$. U slučaju jednakosti blokada je trivijalna, tj. sadržava pravac. Naime, pretpostavimo da je *card* $\mathcal{B} = q+1$ i neka je l pravac koji spaja dvije točke iz $\mathcal{B}$. Ukoliko postoji točka $P \in l \setminus \mathcal{B}$, onda kroz P prolazi još q pravaca ravnine koji sijeku blokadu u barem jednoj točki pa je *card* $\mathcal{B} \geq 2 + q$, a to je kontradikcija. ■

PROPOZICIJA 2.9 *Neka je $\mathcal{B}$ blokada ravnine Π. Ako je card $\mathcal{B} = q + m$, onda svaki pravac ravnine Π sadrži najviše m točaka iz $\mathcal{B}$.*

Dokaz Neka je *card* $\mathcal{B} = q + m$. Pretpostavimo da postoji pravac l ravnine Π koji sadrži $m+1$ točku iz $\mathcal{B}$. Neka je $P \in l \setminus \mathcal{B}$. Kroz točku P prolazi još q pravaca ravnine koji sijeku blokadu u barem jednoj točki pa je *card* $\mathcal{B} \geq m + 1 + q$, a to je kontradikcija. ■

PROPOZICIJA 2.10 *Ako neki pravac ravnine Π sadrži m točaka blokade $\mathcal{B}$, onda je card $\mathcal{B} \geq q + m$.*

Dokaz Neka pravac l ravnine Π sadrži m točaka iz $\mathcal{B}$ i neka je $P \in l \setminus \mathcal{B}$. Kroz točku P prolazi još q pravaca ravnine koji sijeku blokadu u barem jednoj točki, što znači *card* $\mathcal{B} \geq m + q$. ■

PRIMJER 2.11 *Blokada projektivne ravnine $PG(2,3)$.*

Neka je $\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ cikličke reprezentacija projektivne ravnine $PG(2,3)$. Na svakom pravcu nalaze se četiri točke i svakom točkom prolaze četiri pravca. Pravce ravnine, dobivene cikličkim pomakom točaka, prikazujemo u stupcima tablice:

0	1	**2**	3	**4**	**5**	6	7	**8**	9	10	**11**	12
1	**2**	3	**4**	**5**	6	7	**8**	9	10	**11**	12	**0**
3	**4**	**5**	6	7	**8**	9	10	**11**	12	**0**	1	**2**
9	10	**11**	12	**0**	1	**2**	3	**4**	**5**	6	7	**8**

Tablica 2.1

Promotrimo skup $\mathcal{B} = \{0, 2, 4, 5, 8, 11\}$. $\mathcal{B}$ je blokada jer svaki pravac ravnine siječe skup $\mathcal{B}$ u barem jednoj točki. Za svaku točku P iz $\mathcal{B}$ postoji pravac l tako da je $\mathcal{B} \cap l = \{P\}$, pa je po Lemi 2.6 blokada $\mathcal{B} = \{0, 2, 4, 5, 8, 11\}$ minimalna u $PG(2, 3)$.

Ako gledamo analitički model ravnine $PG(2, 3)$ i njene točke $\{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (0, 1, 1), (1, 1, 1), (1, -1, 1), (-1, 1, 1), (1, 0, 1), (1, -1, 0), (0, 1, -1), (1, 1, -1), (1, 0, -1)\}$, onda je blokada $\mathcal{B} = \{(1, 0, 0), (0, 0, 1), (0, 1, 1), (1, 1, 1), (1, 0, 1), (1, 1, -1)\}$.

Neke primjere blokade možemo konstruirati pomoću pojmova projektivnog trovrha i projektivne trijade.

DEFINICIJA 2.12 ***Projektivni trovrh*** *stranice n u projektivnoj ravnini $P(2, q)$ je skup $\mathcal{B}$ od $3(n-1)$ točaka za koji postoji trovrh $P_0P_1P_2$ takav da vrijedi:*

(i) svaka stranica trovrha $P_0P_1P_2$ sadrži n točaka iz $\mathcal{B}$;

(ii) vrhovi P_0, P_1, P_2 pripadaju $\mathcal{B}$;

(iii) ako su $Q_0 \in P_1P_2$ i $Q_1 \in P_2P_0$ u $\mathcal{B}$, onda je i $Q_2 = Q_0Q_1 \cap P_0P_1$ u $\mathcal{B}$.

DEFINICIJA 2.13 ***Projektivna trijada*** *stranice n u projektivnoj ravnini $P(2, q)$ je skup $\mathcal{B}$ od $3n - 2$ točaka za koju postoje tri konkurentna pravca l_0, l_1, l_2 takva da vrijedi:*

(i) svaki od tri konkurentna pravca l_0, l_1, l_2 sadrži n točaka iz $\mathcal{B}$;

(ii) vrh $P = l_0 \cap l_1 \cap l_2$ pripada $\mathcal{B}$;

(iii) ako su $Q_0 \in l_0$ i $Q_1 \in l_1$ u $\mathcal{B}$, onda je i $Q_2 = Q_0Q_1 \cap l_2$ u $\mathcal{B}$.

LEMA 2.14 *(i) U projektivnoj ravnini $PG(2, q)$ neparnog reda q, postoji projektivni trovrh stranice $\frac{1}{2}(q+3)$ koji je minimalna blokada od $\frac{3}{2}(q+1)$ točaka.*

(ii) U projektivnoj ravnini $PG(2, q)$ parnog reda q, postoji projektivna trijada stranice $\frac{1}{2}(q+2)$ koja je minimalna blokada od $\frac{1}{2}(3q+2)$ točaka.

Dokaz

(i) Točke $Q_0(a_0) = (0, 1, a_0)$, $Q_1(a_1) = (1, 0, a_1)$ i $Q_2(a_2) = (-a_2, 1, 0)$, različite od vrhova P_0, P_1, P_2, kolinearne su ako i samo ako vrijedi

$$\begin{vmatrix} 0 & 1 & a_0 \\ 1 & 0 & a_1 \\ -a_2 & 1 & 0 \end{vmatrix} = 0.$$

Izračunavanjem se dobije da su točke $Q_0(a_0)$, $Q_1(a_1)$ i $Q_2(a_2)$ kolinearne ako i samo ako je $a_0 = a_1 a_2$.

Neka se $\mathcal{B}$ sastoji od vrhova i svih točaka $Q_i(a_i)$ za koje su a_i kvadrati različiti od nule. Svaki pravac l koji ne prolazi vrhom, siječe stranice trovrha $\mathbf{u_0}$, $\mathbf{u_1}$, $\mathbf{u_2}$ u točkama $Q_0(a_0)$, $Q_1(a_1)$, $Q_2(a_2)$. Pritom je ili jedna ili tri vrijednosti od a_0, a_1, a_2 kvadrat, tako da je $card\ (l \cap \mathcal{B}) = 1$ ili 3. Svaka stranica siječe $\mathcal{B}$ u $\frac{1}{2}(q+3)$ točaka, jer kvadrata u polju ima $\frac{1}{2}(q-1)$ pa na stranicama ima $\frac{1}{2}(q-1)$ točaka te još 2 vrha. Svaki drugi pravac kroz vrh siječe $\mathcal{B}$ u jednoj ili dvije točke. Dakle, $\mathcal{B}$ je blokada. Ako je $a_0' = a_1' a_2'$ i ako dvije vrijednosti od a_0', a_1', a_2' nisu kvadrati, onda pravac $Q_0(a_0')Q_1(a_1')Q_2(a_2')$ siječe $\mathcal{B}$ u samo jednoj točki, te se ta točka ne može izbaciti. Također, vrhovi se ne smiju izbacit, a to znači da je $\mathcal{B}$ minimalna blokada od $3 \cdot \frac{q-1}{2} + 3 = \frac{3}{2}(q+1)$ točaka.

(ii) Točke $Q_0(a_0) = (0, 1, a_0)$, $Q_1(a_1) = (1, 0, a_1)$, $Q(c) = (1, 1, c)$ na pripadnim pravcima $\mathbf{u_0}$, $\mathbf{u_1}$ i $X_0 + X_1 = 0$ kolinearne su ako i samo ako vrijedi

$$\begin{vmatrix} 0 & 1 & a_0 \\ 1 & 0 & a_1 \\ 1 & 1 & c \end{vmatrix} = 0.$$

Izračunavanjem se dobije da su točke $Q_0(a_0)$, $Q_1(a_1)$ i $Q(c)$ kolinearne ako i samo ako $c = a_0 + a_1$.

Neka se $\mathcal{B}$ sastoji od vrha $\mathbf{U_2} = (0, 0, 1)$ i svih točaka $Q_0(a_0)$, $Q_1(a_1)$, $Q(c)$ pri čemu a_0, a_1 i c imaju trag nula. Tada svaki pravac l koji prolazi kroz $\mathbf{U_2}$ siječe $\mathcal{B}$ u jednoj ili $\frac{1}{2}(q+2)$ točaka (obzirom da u polju trag nula ima $q/2$ elemenata, pa na zadanim pravcima ima $q/2$ točaka te još vrh), a svaki pravac koji ne prolazi kroz $\mathbf{U_2}$ siječe $\mathcal{B}$ u jednoj ili tri točke. Dakle, $\mathcal{B}$ je blokada. Ako je $c' = a_0' + a_1'$ i ako dvije vrijednosti od c', a_0', a_1' imaju trag jedan, onda pravac $Q_0(a_0')Q_1(a_1')Q(c')$ siječe $\mathcal{B}$ u samo jednoj točki, te se ta točka ne može izbaciti. Također, vrh $\mathbf{U_2}$ se ne smije izbaciti, a to znači da je $\mathcal{B}$ minimalna blokada od $3 \cdot \frac{q}{2} + 1 = \frac{1}{2}(3q+2)$ točaka. ■

2.1 Veličina blokade u projektivnoj ravnini

DEFINICIJA 2.15 *Neka je $\mathcal{S}$ skup točaka u Π. Za pravac l ravnine Π kažemo da je **i-sekanta** skupa $\mathcal{S}$ ako vrijedi $card\ (\mathcal{S} \cap l) = i$.*

Posebno, za 0-sekantu, 1-sekantu i 2-sekantu skupa $\mathcal{S}$ koristimo još i nazive *vanjski pravac*, *unisekanta* (ili *tangenta*) i *bisekanta* skupa $\mathcal{S}$. Broj i-sekanti skupa $\mathcal{S}$ označavamo s τ_i.

TEOREM 2.16 (Bruen) *Za blokadu $\mathcal{B}$ ravnine Π vrijedi $card\ \mathcal{B} \geq q + \sqrt{q} + 1$.*

Dokaz Neka je $card\ \mathcal{B} = q + n$ i neka je τ_i broj i-sekanti od $\mathcal{B}$. Naravno, $i \in \{1, 2, \ldots, q\}$, tj. $i \neq 0$ jer je $\mathcal{B}$ blokada, a kako ne sadrži sve točke nekog pravca onda je $i \neq q + 1$. Također, $\tau_i = 0$ za $i > n$ jer bi u protivnom blokada sadržavala više od $q + n$ točaka. Pravaca ukupno ima

$$\sum_{i=1}^{n} \tau_i = q^2 + q + 1.$$

Prebrojimo sve parove (P, l), gdje je P točka blokade $\mathcal{B}$ koja pripada pravcu l

$$\sum_{i=1}^{n} i\tau_i = card\ \mathcal{B} \cdot (q + 1) = (q + n)(q + 1).$$

Prebrojimo sve trojke (P, Q, l), gdje su P i Q dvije različite točke iz $\mathcal{B}$, a l njihova spojnica. Samih parova (P, Q) ima

$$\binom{card\ \mathcal{B}}{2} = \frac{(q + n)(q + n - 1)}{2}$$

i oni jednoznačno određuju pravac l. Svaki pravac na i-sekanti sadrži $\binom{i}{2}$ parova (P, Q), dakle

$$\sum_{i=2}^{n} \binom{i}{2} \tau_i = \binom{card\ \mathcal{B}}{2}$$

$$\Rightarrow \quad \sum_{i=2}^{n} i(i-1)\tau_i = (q + n)(q + n - 1).$$

Sada imamo jednadžbe

$$\sum_{i=1}^{n} \tau_i = q^2 + q + 1, \tag{2.1}$$

$$\sum_{i=1}^{n} i\tau_i = (q + n)(q + 1), \tag{2.2}$$

$$\sum_{i=2}^{n} i(i-1)\tau_i = (q + n)(q + n - 1). \tag{2.3}$$

Oduzimanjem jednadžbi (2.2) i (2.1) dobije se

$$\sum_{i=2}^{n}(i-1)\tau_i = qn + n - 1.$$

Očito je $i \leq n$. Ako uvrstimo ovo u jednadžbu (2.3) dobijemo

$$\sum_{i=2}^{n} i(i-1)\tau_i \leq \sum_{i=2}^{n} n(i-1)\tau_i = n\sum_{i=2}^{n}(i-1)\tau_i$$

tj.

$$\begin{aligned}(q+n)(q+n-1) &\leq n(qn+n-1)\\ q^2+2qn-q+n^2-n &\leq qn^2+n^2-n\\ q^2 \leq q(n-1)^2 \quad &\Rightarrow \quad n \geq \sqrt{q}+1.\end{aligned}$$

Kako je $card\ \mathcal{B} = q+n$, slijedi $card\ \mathcal{B} \geq q+\sqrt{q}+1$. ■

Za blokade konačne projektivne ravnine Π kvadratnog reda q vrijedi ocjena $card\ \mathcal{B} = q+\sqrt{q}+1$ i ona je najbolja moguća, jer sve te ravnine sadrže podravninu (Baerovu) reda $\sqrt{q}$. Pokažimo da je Baerova podravnina blokada.

TEOREM 2.17 *Baerova podravnina je blokada projektivne ravnine kvadratnog reda.*

Dokaz Projektivna ravnina Π kvadratnog reda q svakako sadrži podravninu reda $\sqrt{q}$. Kako svaki pravac ravnine Π sadrži najviše $\sqrt{q}+1$ točaka iz $\mathcal{B}$, tada slijedi da svaki pravac ravnine Π sadrži barem jednu točku koja nije u $\mathcal{B}$. Neka je l pravac ravnine Π i točka $P \in l \setminus \mathcal{B}$. Tada postoji najviše jedan pravac u $\mathcal{B}$ kroz P, jer je $\mathcal{B}$ podravnina (u protivnom bi se dva pravca podravnine sjekli u točki izvan nje). Također, kako svake dvije točke ravnine Π pripadaju jedinstvenom pravcu, slijedi da se $q+\sqrt{q}+1$ točka iz $\mathcal{B}$ nalazi na $q+1$ pravcu iz Π kroz P. Ako pravac l ne sadrži nijednu točku iz $\mathcal{B}$, onda bi pravci ravnine Π kroz P sadržavali najviše $(\sqrt{q}+1)+(q-1)\cdot 1 = q+\sqrt{q}$ točaka iz $\mathcal{B}$. Dakle, l mora sadržavati barem jednu točku iz $\mathcal{B}$, tj. $\mathcal{B}$ je blokada ravnine. ■

TEOREM 2.18 *Blokada $\mathcal{B}$ ravnine Π je Baerova podravnina ako i samo ako je $card\ \mathcal{B} = q+\sqrt{q}+1$.*

Dokaz Ako je $card\ \mathcal{B} = q+\sqrt{q}+1$, onda po Propoziciji 2.9 slijedi da svaki pravac ravnine sadrži najviše $\sqrt{q}+1$ točku blokade $\mathcal{B}$. Jednakost $n = \sqrt{q}+1$ vrijedi u slučaju jednakosti suma

$$\sum_{i=2}^{n} i(i-1)\tau_i = \sum_{i=2}^{n} n(i-1)\tau_i.$$

Ovo vrijedi samo ako je $\tau_2 = \tau_3 = \cdots = \tau_{n-1} = 0$, odnosno $\tau_1 \neq 0$ i $\tau_n \neq 0$. To znači da svaki pravac siječe blokadu $\mathcal{B}$ ili u jednoj ili u točno n točaka. Tada je $\mathcal{B}$ podravnina reda $n-1 = \sqrt{q}+1-1 = \sqrt{q}$, tj. $\mathcal{B}$ je Baerova podravnina.
Obrat. Trivijalno. ■

KOROLAR 2.19 *Za blokadu $\mathcal{B}$ ravnine Π vrijedi*

$$q + \sqrt{q} + 1 \leq card\ \mathcal{B} \leq q^2 - \sqrt{q}.$$

Dokaz Kako je komplement blokade također blokada, a ukupan broj točaka ravnine $q^2 + q + 1$, vrijedi $card\ \mathcal{B} \leq q^2 + q + 1 - q - \sqrt{q} - 1 = q^2 - \sqrt{q}$. ■

TEOREM 2.20 *Za minimalnu blokadu $\mathcal{B}$ ravnine Π vrijedi $card\ \mathcal{B} \leq q\sqrt{q} + 1$.*

Dokaz Neka je $card\ \mathcal{B} = q + n$ i τ_i broj i-sekanti od $\mathcal{B}$. Kako je $\mathcal{B}$ minimalna blokada, onda za svaku točku $P \in \mathcal{B}$ postoji pravac ravnine koji siječe blokadu u samo toj točki P, tj. vrijedi $\tau_1 \geq q+n$. Pravaca koji ne sijeku $\mathcal{B}$ u samo jednoj točki ima $N = q^2+q+1-\tau_1$. Označimo ih sa $\{l_1, l_2, \ldots, l_N\}$ i definirajmo $n_j = card\ (\mathcal{B} \cap l_j)$. Prebrojimo sve parove (P, l_j), gdje je $P \in \mathcal{B} \cap l_j$

$$\sum_{j=1}^{N} n_j = card\ \mathcal{B} \cdot (q+1) - \tau_1,$$

$$\sum_{j=1}^{N} n_j = (q+n)(q+1) - \tau_1. \tag{2.4}$$

Prebrojimo sve trojke (P, Q, l_j), gdje su P i Q dvije različite točke iz $\mathcal{B} \cap l_j$. Samih parova (P, Q) ima

$$\binom{card\ \mathcal{B}}{2} = \frac{(q+n)(q+n-1)}{2}$$

i oni jednoznačno određuju pravac l_j. Dakle,

$$\sum_{j=1}^{N} \binom{n_j}{2} = \binom{card\ \mathcal{B}}{2},$$

$$\sum_{j=1}^{N} n_j(n_j - 1) = (q+n)(q+n-1). \tag{2.5}$$

Zbrajanjem jednadžbi (2.4) i (2.5) dobije se

$$\sum_{j=1}^{N} n_j^2 = (q+n)(2q+n) - \tau_1.$$

Također, vrijedi

$$N \sum_{j=1}^{N} n_j^2 - \Big(\sum_{j=1}^{N} n_j \Big)^2 = \sum_{i<j} (n_i - n_j)^2 \geq 0$$

odnosno

$$\Big(\sum_{j=1}^{N} n_j \Big)^2 \leq N \sum_{j=1}^{N} n_j^2\ .$$

Uvrštavanjem prethodno dobivenih jednadžbi i $N = q^2 + q + 1 - \tau_1$ u gornju nejednakost dobijemo

$$\Big[(q+n)(q+1) - \tau_1\Big]^2 \leq (q^2+q+1-\tau_1)\Big[(q+n)(2q+n) - \tau_1\Big].$$

Kako je $\tau_1 \geq q+n$, slijedi $-\tau_1 \leq -(q+n)$, tj.

$$\Big[(q+n)(q+1) - (q+n)\Big]^2 \leq \Big[q^2+q+1-(q+n)\Big]\Big[(q+n)(2q+n) - (q+n)\Big]$$

$$q^2(q+n)^2 \leq (q^2-n+1)(q+n)(2q+n-1)$$
$$q^2(q+n) \leq (q^2-n+1)(2q+n-1)$$
$$q^3 + q^2n \leq 2q^3 + q^2n - q^2 - 2qn - n^2 + 2n + 2q - 1$$
$$-q^3 + q^2 + 2qn + n^2 - 2q - 2n + 1 \leq 0$$
$$(q+n)^2 - 2(q+n) + 1 - q^3 \leq 0$$
$$\big[(q+n) - 1\big]^2 - \big[q\sqrt{q}\big]^2 \leq 0$$
$$(q+n-1-q\sqrt{q})(q+n-1+q\sqrt{q}) \leq 0.$$

Od ova dva izraza samo prvi može biti negativan, tj.

$$q+n-1-q\sqrt{q} \leq 0 \quad \Rightarrow \quad q+n \leq q\sqrt{q}+1.$$

Kako je $card\ \mathcal{B} = q+n$, slijedi $card\ \mathcal{B} \leq q\sqrt{q}+1$. ■

Primjere blokada i minimalnih blokada za pojedine vrijednosti q navest ćemo u Poglavlju 3.

2.2 Blokade i potpuni *k*-lukovi

Promotrit ćemu vezu blokada i lukova projektivne ravnine.

DEFINICIJA 2.21 *Skup $\mathcal{K}$ koji se sastoji od k točaka ravnine Π tako da su najviše dvije njegove točke kolinearne, naziva se* ***k-luk*** *ili* ***luk stupnja dva*** *ravnine Π.*

Svaki pravac ravnine siječe k-luk u 0, 1 ili 2 točke, tj. pravac ravnine je vanjski pravac, unisekanta ili bisekanta k-luka. Pritom je τ_0 oznaka za broj vanjskih pravaca, τ_1 za broj unisekanti i τ_2 za broj bisekanti k-luka.
Neka je P točka k-luka. Broj unisekanti kroz P označavamo s t_P.

LEMA 2.22 *Za k-luk ravnine Π vrijedi*

(i) $t_P = q + 2 - k$,

(ii) $\tau_0 = \frac{1}{2}q(q-1) + \frac{1}{2}t_P(t_P - 1), \quad \tau_1 = k \cdot t_P, \quad \tau_2 = \frac{1}{2}k(k-1)$.

Dokaz

(i) Pravaca kroz točku P koji sijeku k-luk u P i još jednoj točki ima $k-1$, a ukupno kroz P prolazi $q+1$ pravaca ravnine. Dakle, broj pravaca kroz P koji sijeku k-luk samo u točki P ima $t_P = q + 1 - (k-1) = q + 2 - k$.

(ii) Očito je da unisekanti k-luka ima $\tau_1 = k \cdot t_P$, a bisekanti $\tau_2 = \binom{k}{2} = \frac{1}{2}k(k-1)$. Ukupno ih ima

$$\tau_1 + \tau_2 = k \cdot t_P + \frac{k(k-1)}{2} = \frac{k(2t_P + k - 1)}{2}.$$

Kako je $k = q + 2 - t_P$, imamo

$$\tau_1 + \tau_2 = \frac{(q + 2 - t_P)(t_P + q + 1)}{2} = \frac{q^2 + 3q + t_P + 2 - t_P^2}{2}.$$

Broj vanjskih pravaca k-luka je

$$\tau_0 = q^2 + q + 1 - \tau_1 - \tau_2$$

$$\tau_0 = q^2 + q + 1 - \frac{q^2 + 3q + t_P + 2 - t_P^2}{2} = \frac{q^2 - q + t_P^2 - t_P}{2},$$

odnosno,

$$\tau_0 = \frac{q(q-1)}{2} + \frac{t_P(t_P - 1)}{2}$$

■

DEFINICIJA 2.23 *k-luk koji se dodavanjem još jedne točke ravnine ne može proširiti do $(k+1)$-luka naziva se* ***potpuni k-luk*** *ravnine Π.*

Očito je k-luk potpun ako svaka točka ravnine leži na nekoj njegovoj bisekanti.

LEMA 2.24 *Za k-luk ravnine Π vrijedi $k \leq q+2$.*

Dokaz Kroz svaku točku k-luka prolazi $q+1$ pravac, a na svakom od njih može ležati najviše još jedna točka k-luka, pa je $k \leq q+2$. ■

DEFINICIJA 2.25 *$(q+2)$-luk ravnine Π naziva se **maksimalan luk** ravnine Π.*

LEMA 2.26 *k-luk ravnine Π je maksimalan ako i samo ako je svaki pravac ravnine njegov vanjski pravac ili bisekanta.*

Dokaz Neka je $k = q+2$. Pretpostavimo da postoji pravac ravnine koji siječe k-luk u jednoj točki, npr. u točki P. Kroz nju prolazi još q pravaca s najviše još jednom točkom k-luka, pa vrijedi $k \leq q+1$ što je kontradikcija.
Obrat. Neka su svi pravci ravnine vanjski pravci k-luka ili njegove bisekante. Tada je $\tau_1 = k \cdot t_P = 0$, odnosno $t_P = q+2-k = 0$. Iz ovog slijedi $k = q+2$, tj. k-luk je maksimalan. ■

LEMA 2.27 *Maksimalan luk ne postoji u projektivnoj ravnini neparnog reda.*

Dokaz Pretpostavimo da u projektivnoj ravnini neparnog reda q postoji maksimalan luk od $q+2$ točke. Neka je b broj bisekanti kroz neku točku ravnine koja ne pripada maksimalnom luku. Tada vrijedi $2b = q+2$, a ova jednakost je nemoguća zbog neparnosti broja q. ■

PRIMJER 2.28 *Oval i hiperoval.*

1. ***Oval*** je skup od $q+1$ točaka od kojih nikoje tri nisu kolinearne. Za oval vrijedi

$$t_P = 1,$$

$$\tau_0 = \frac{q(q-1)}{2}, \quad \tau_1 = q+1, \quad \tau_2 = \frac{q(q+1)}{2}.$$

   Oval je $(q+1)$-luk ravnine Π i za projektivnu ravninu neparnog reda je najveći mogući luk.

2. ***Hiperoval*** je skup od $q+2$ točaka od kojih nikoje tri nisu kolinearne. Za hiperoval vrijedi

$$t_P = 0,$$

$$\tau_0 = \frac{q(q-1)}{2}, \quad \tau_1 = 0, \quad \tau_2 = \frac{(q+1)(q+2)}{2}.$$

   Hiperoval je $(q+2)$-luk ravnine Π i on je maksimalan luk za projektivnu ravninu parnog reda.

Blokade su povezane s k-lukovima, što pokazuje sljedeća lema.

LEMA 2.29 *Neka je $\mathcal{K}$ potpun k-luk ravnine Π i neka je Π' ravnina dualna ravnini Π. Ako je $k < q+2$, onda je dualna figura skupa svih bisekanti k-luka $\mathcal{K}$ blokada veličine $\frac{1}{2}k(k-1)$ u ravnini Π'.*

Dokaz Neka je $\mathcal{B}$ dualna figura skupa svih bisekanti k-luka $\mathcal{K}$. Zbog potpunosti k-luka $\mathcal{K}$, svaka točka ravnine Π leži na bisekanti od $\mathcal{K}$, dakle svaki pravac u Π' sadrži bar jednu točku iz $\mathcal{B}$, pa je $\mathcal{B}$ blokada. Provjerimo da ne postoji pravac ravnine čije su sve točke sadržane u $\mathcal{B}$. Kako svaka točka ravnine Π leži na najviše $k-1$ bisekanti od $\mathcal{K}$ (maksimum se postiže za točke k-luka), onda zbog uvjeta $k < q+2$ slijedi $k-1 \leq q$, tj. q je najveći mogući broj bisekanti od $\mathcal{K}$ kroz bilo koju točku u Π. Dualno, q je najveći mogući broj točaka iz $\mathcal{B}$ na nekom pravcu ravnine Π' pa ne postoji pravac ravnine čije su sve točke sadržane u $\mathcal{B}$. Nadalje, broj bisekanti k-luka je $\binom{k}{2}$, tj. $card\ \mathcal{B} = \frac{1}{2}k(k-1)$. ∎

TEOREM 2.30 *Za potpuni k-luk ravnine Π vrijedi $q \leq \frac{1}{2}(k-1)(k-2)$.*

Dokaz Neka je $\mathcal{B}$ dualna figura skupa svih bisekanti k-luka $\mathcal{K}$. Svakoj točki M k-luka $\mathcal{K}$ odgovara pravac m blokade $\mathcal{B}$ koji sadrži $k-1$ točaka iz $\mathcal{B}$. Po prethodnom teoremu je $card\ \mathcal{B} = \frac{1}{2}k(k-1)$. Odaberimo proizvoljnu točku $P \in m \setminus \mathcal{B}$. Kako je $\mathcal{B}$ blokada, na preostalih q pravaca kroz P leži po barem jedna točka iz $\mathcal{B}$. Tada je $card\ \mathcal{B} \geq k-1+q$, odnosno $q \leq \frac{1}{2}(k-1)(k-2)$. ∎

TEOREM 2.31 *Blokada $\mathcal{B}$ dobivena je iz potpunog k-luka ako i samo ako vrijede sljedeće tvrdnje:*

(i) $card\ \mathcal{B} \leq \binom{k}{2}$;

(ii) broj $(k-1)$-sekanti iz $\mathcal{B}$ je barem k;

(iii) nikoje tri $(k-1)$-sekante iz $\mathcal{B}$ nisu konkurentne.

Dokaz Pretpostavimo da za blokadu $\mathcal{B}$ vrijede sve tri tvrdnje. Neka je L_{k-1} skup od $(k-1)$-sekanti iz $\mathcal{B}$ i neka je $\mathcal{I}$ skup incidencija točaka iz $\mathcal{B}$ s pravcima iz L_{k-1}. Zbog (ii) je $card\ \mathcal{I} \geq k(k-1)$. Točke sjecišta parova pravaca iz L_{k-1} različite su zbog (iii). Neka je n od tih sjecišta iz $\mathcal{B}$. To daje $card\ \mathcal{B} - n \leq \binom{k}{2} - n$ točaka iz $\mathcal{B}$ leže ili na jednom ili na nijednom pravcu iz L_{k-1}. Odavde slijedi

$$card\ \mathcal{I} \leq n \cdot 2 + \binom{k}{2} - n,$$

$$k(k-1) \leq n + \binom{k}{2} \quad \Rightarrow \quad n \geq \frac{k(k-1)}{2}.$$

Međutim, po definiciji je $n \leq card\ \mathcal{B} \leq \frac{1}{2}k(k-1)$. To znači da je

$$n = \frac{k(k-1)}{2}, \quad card\ \mathcal{I} = k(k-1), \quad card\ L_{k-1} = k, \quad card\ \mathcal{B} = \frac{k(k-1)}{2}.$$

Pritom su točke iz $\mathcal{B}$ upravo sjecišta parova pravaca iz L_{k-1}. Neka je $\mathcal{K}$ dual od L_{k-1}, tj. skup točaka iz dualne ravnine Π' koje odgovaraju pravcima iz L_{k-1}. Dakle, $\mathcal{K}$ je k-luk, a dual od $\mathcal{B}$ je skup bisekanti od $\mathcal{K}$. Budući je $\mathcal{B}$ blokada, $\mathcal{K}$ mora biti potpuni k-luk, pa je blokada $\mathcal{B}$ dobivena iz potpunog k-luka.
Obrat. Trivijalno. ∎

Za ocjenu veličine minimalnih blokada bit će nam potrebno jedno poopćenje pojma k-luka, a to je Hermiteov luk.

DEFINICIJA 2.32 ***Hermiteov luk*** *je skup od* $q\sqrt{q}+1$ *točaka ravnine* Π *tako da svaki pravac ravnine sadrži ili jednu ili* $\sqrt{q}+1$ *točku luka.*

TEOREM 2.33 *Neka je* $\mathcal{B}$ *minimalna blokada ravnine* Π. $\mathcal{B}$ *je Hermiteov luk ako i samo ako je* $card\ \mathcal{B} = q\sqrt{q}+1$.

Dokaz Neka je $card\ \mathcal{B} = q\sqrt{q}+1$ i τ_i broj i-sekanti od $\mathcal{B}$. Kako je $\mathcal{B}$ minimalna blokada, onda za svaku točku $P \in \mathcal{B}$ postoji pravac ravnine koji siječe blokadu u samo toj točki P, tj. vrijedi

$$\tau_1 \geq q\sqrt{q}+1. \tag{2.6}$$

Pravaca koji ne sijeku $\mathcal{B}$ u samo jednoj točki ima $N = q^2+q+1-\tau_1$. Označimo ih sa $\{l_1, l_2, \ldots, l_N\}$ i definirajmo $n_j = card\ (\mathcal{B} \cap l_j)$.
Prebrojimo sve parove (P, l_j), gdje je $P \in \mathcal{B} \cap l_j$

$$\sum_{j=1}^{N} n_j = card\ \mathcal{B} \cdot (q+1) - \tau_1,$$

$$\sum_{j=1}^{N} n_j = (q\sqrt{q}+1)(q+1) - \tau_1. \tag{2.7}$$

Prebrojimo sve trojke (P, Q, l_j), gdje su P i Q dvije različite točke iz $\mathcal{B} \cap l_j$. Samih parova (P, Q) ima

$$\binom{card\ \mathcal{B}}{2} = \frac{q\sqrt{q}(q\sqrt{q}+1)}{2}$$

i oni jednoznačno određuju pravac l_j. Dakle,

$$\sum_{j=1}^{N} \binom{n_j}{2} = \binom{card\ \mathcal{B}}{2},$$

$$\sum_{j=1}^{N} n_j(n_j-1) = q\sqrt{q}(q\sqrt{q}+1). \tag{2.8}$$

Zbrajanjem jednadžbi (2.7) i (2.8) dobije se

$$\sum_{j=1}^{N} n_j^2 = (q\sqrt{q}+1)(q+q\sqrt{q}+1) - \tau_1.$$

Također, vrijedi

$$N\sum_{j=1}^{N} n_j^2 - \Big(\sum_{j=1}^{N} n_j\Big)^2 = \sum_{i<j}(n_i - n_j)^2 \geq 0$$

odnosno

$$\Big(\sum_{j=1}^{N} n_j\Big)^2 \le N \sum_{j=1}^{N} n_j^2 \ . \tag{2.9}$$

Uvrštavanjem prethodno dobivenih jednadžbi i $N = q^2+q+1-\tau_1$ u (2.9) dobijemo

$$\Big[(q\sqrt{q}+1)(q+1)-\tau_1\Big]^2 \le (q^2+q+1-\tau_1)\Big[(q\sqrt{q}+1)(q+q\sqrt{q}+1)-\tau_1\Big].$$

Odavde slijedi

$$\begin{aligned}&(q\sqrt{q}+1)^2(q+1)^2 - 2\tau_1(q\sqrt{q}+1)(q+1) \le \\ &\le (q^2+q+1)(q\sqrt{q}+1)(q+q\sqrt{q}+1) - \tau_1\Big[q^2+q+1+(q\sqrt{q}+1)(q+q\sqrt{q}+1)\Big],\end{aligned}$$

$$\begin{aligned}&(q\sqrt{q}+1)\Big[(q\sqrt{q}+1)(q^2+2q+1) - (q^2+q+1)(q+q\sqrt{q}+1)\Big] \le \\ &\le \tau_1\Big[2(q\sqrt{q}+1)(q+1) + (q\sqrt{q}+1)(q+q\sqrt{q}+1) - q^2-q-1\Big],\end{aligned}$$

$$\begin{aligned}&(q\sqrt{q}+1)\Big[q^3\sqrt{q}+2q^2\sqrt{q}+q\sqrt{q}+q^2+2q+1-q^3-q^3\sqrt{q}-2q^2-q^2\sqrt{q}-2q-q\sqrt{q}-1\Big] \le \\ &\le \tau_1\Big[(q\sqrt{q}+1)(q-q\sqrt{q}+1) - q^2-q-1\Big],\end{aligned}$$

odnosno

$$\begin{aligned}(q\sqrt{q}+1)(-q^3-q^2+q^2\sqrt{q}) &\le \tau_1(-q^3-q^2+q^2\sqrt{q}),\\ -q^2(q\sqrt{q}+1)(q+1-\sqrt{q}) &\le -q^2\tau_1(q+1-\sqrt{q}),\\ (q\sqrt{q}+1) &\ge \tau_1. \end{aligned}\tag{2.10}$$

Iz (2.6) i (2.10) slijedi $\tau_1 = q\sqrt{q}+1$, što povlači jednakost u (2.9). Tada je n_j konstanta, pa iz (2.7) slijedi

$$N \cdot n_j = q(q\sqrt{q}+1),$$

$$(q^2+q-q\sqrt{q})n_j = q(q\sqrt{q}+1),$$

$$\begin{aligned} n_j &= \frac{q(q\sqrt{q}+1)}{q^2+q-q\sqrt{q}} = \frac{q\sqrt{q}+1}{q+1-\sqrt{q}} \cdot \frac{q+1+\sqrt{q}}{q+1+\sqrt{q}} = \frac{(\sqrt{q}+1)(q^2+q+1)}{q^2+q+1} \\ &= \sqrt{q}+1. \end{aligned}$$

Dakle, svaki pravac ravnine Π siječe minimalnu blokadu $\mathcal{B}$ u jednoj ili $\sqrt{q}+1$ točki, odnosno $\mathcal{B}$ je Hermiteov luk. ∎

U Poglavlju 6. razmatrat ćemo općenito tzv. lukove višeg reda, koji uključuju i Hermiteov luk.

Poglavlje 3

Blokade u projektivnim ravninama malog reda

U ovom poglavlju proučavat ćemo blokade u projektivnim ravninama $\Pi = PG(2, q)$ malog reda, tj. reda $q \leq 11$. Poznato je da ne postoje projektivne ravnine reda $q = 6$ i $q = 10$, a u Primjeru 2.4 pokazali smo da za projektivnu ravninu reda $q = 2$ postoje samo trivijalne blokade, tj. one koje sadržavaju sve točke nekog pravca.

U prethodnom poglavlju pokazali smo da za blokadu $\mathcal{B}$ projektivne ravnine reda q vrijedi

$$q + \sqrt{q} + 1 \leq card\ \mathcal{B} \leq q^2 - \sqrt{q},$$

pri čemu je blokada $\mathcal{B}$ Baerova podravnina ako i samo ako je $card\ \mathcal{B} = q + \sqrt{q} + 1$, dok za minimalnu blokadu vrijedi

$$card\ \mathcal{B} \leq q\sqrt{q} + 1,$$

pri čemu je minimalna blokada $\mathcal{B}$ Hermiteov luk ako i samo ako je $card\ \mathcal{B} = q\sqrt{q}+1$.

Po Lemi 2.14 u projektivnoj ravnini $PG(2, q)$ neparnog reda q postoji projektivni trovrh stranice $\frac{1}{2}(q+3)$ koji je minimalna blokada od $\frac{3}{2}(q+1)$ točaka, a u projektivnoj ravnini $PG(2, q)$ parnog reda q postoji projektivna trijada stranice $\frac{1}{2}(q + 2)$ koja je minimalna blokada od $\frac{1}{2}(3q + 2)$ točaka.

$q = 3$

- $6 \leq card\ \mathcal{B} \leq 7$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 6$, $\mathcal{B}$ minimalna blokada

U $PG(2, 3)$ postoji projektivni trovrh stranice $\frac{1}{2}(q+3) = 3$ koji je minimalna blokada od $\frac{3}{2}(q + 1) = 6$ točaka.

Jedina druga blokada je komplement projektivnog trovrha koji sadrži 7 točaka.

$q = 4$

- $7 \leq card\ \mathcal{B} \leq 14$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 9$, $\mathcal{B}$ minimalna blokada

U $PG(2,4)$ postoji projektivna trijada stranice $\frac{1}{2}(q+2) = 3$ koja je minimalna blokada od $\frac{1}{2}(3q+2) = 7$ točaka. To je ujedno i Baerova podravnina $PG(2,2)$ ravnine $PG(2,4)$.

Minimalna blokada od 9 točaka je Hermiteov luk, tj. skup točaka kojeg svaki pravac ove ravnine siječe u jednoj ili tri točke.

Opišimo minimalnu blokadu od 8 točaka. Neka je $\mathcal{B}$ blokada od 8 točaka. Tada jednadžbe (2.1) - (2.3) imaju oblik

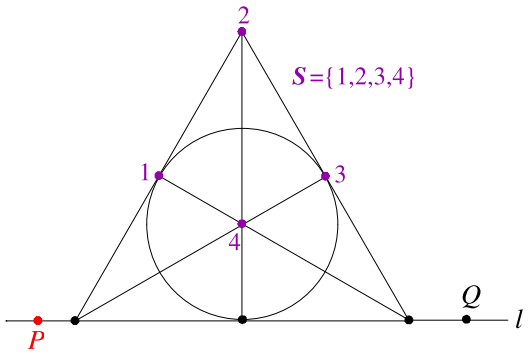
$$\tau_1 + \tau_2 + \tau_3 + \tau_4 = 21, \quad \tau_1 + 2\tau_2 + 3\tau_3 + 4\tau_4 = 40, \quad \tau_2 + 3\tau_3 + 6\tau_4 = 28.$$

Oduzimanjem prvih dviju jednadžbi dobije se $\tau_2 + 2\tau_3 + 3\tau_4 = 19$, što uz treću jednadžbu daje $\tau_3 + 3\tau_4 = 9$. Tada je $\tau_4 \leq 3$ pa su mogući sljedeći slučajevi

τ_1	τ_2	τ_3	τ_4
11	1	9	0
10	4	6	1
9	7	3	2
8	10	0	3

Pretpostavimo da je $\tau_4 = 0$. Tada je $\tau_1 = 11$, $\tau_2 = 1$ i $\tau_3 = 9$. Sa ρ_i označimo broj i-sekanti od $\mathcal{B}$ kroz neku točku $P \in \mathcal{B}$. Tada je $\rho_1 + \rho_2 + \rho_3 = q + 1 = 5$. Također, ako spojimo točku P sa preostalih $card\ \mathcal{B} - 1 = 7$ točaka, onda vrijedi $\rho_2 + 2\rho_3 = 7$. Iz ove dvije jednadžbe je $\rho_2 \neq 0$ za svaku točku iz $\mathcal{B}$, pa je $\tau_2 > 1$ što je kontradikcija.

Pretpostavimo da je $\tau_4 = 1$. Tada je $\tau_1 = 10$, $\tau_2 = 4$ i $\tau_3 = 6$. Neka je pravac l 4-sekanta od $\mathcal{B}$ i točka $P \in l \setminus \mathcal{B}$, te neka je $\mathcal{S} = \mathcal{B} \setminus l$ kao na Slici 3.1.

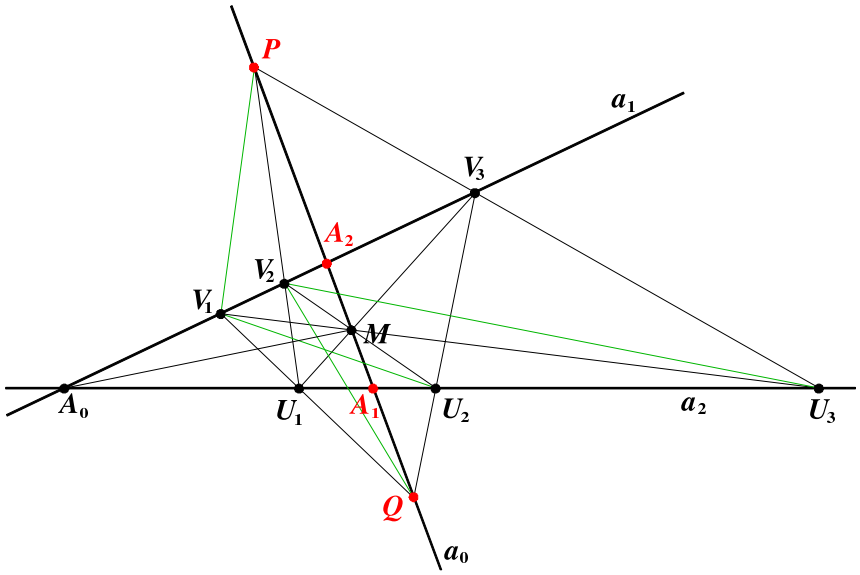


Slika 3.1

Preostala četiri pravca kroz P sijeku $\mathcal{B}$ u jednoj točki, a pravci kroz točku iz $l \cap \mathcal{B}$ sijeku $\mathcal{S}$ u najviše dvije točke, pa je $\mathcal{S} \cup \{P\}$ 5-luk. Točke od $\mathcal{S}$ su vrhovi četverovrha

čije stranice sijeku l u točkama iz $\mathcal{B}$. Dakle, dvije dijagonalne točke četverovrha leže na pravcu l, a kako je q paran onda i treća dijagonalna točka pripada pravcu l. Ove tri dijagonalne točke zajedno s $\mathcal{S}$ formiraju PG(2,2), a četvrtu točku iz $l \cap \mathcal{B}$ koja nije dijagonalna označimo s Q. Tada je blokada $\mathcal{B} = PG(2,2) \cup \{Q\}$, a ona očito nije minimalna.

Pretpostavimo da je $\tau_4 = 2$. Tada je $\tau_1 = 9$, $\tau_2 = 7$ i $\tau_3 = 3$. Neka je $\mathcal{T}$ projektivni trovrh $A_0A_1A_2$ sa stranicama $a_0 = (A_1, A_2)$, $a_1 = (A_0, A_2)$, $a_2 = (A_0, A_1)$, te neka je $\mathcal{T}^* = (a_1 \cup a_2) \setminus (A_1 \cup A_2) \cup \{M\}$, gdje je $M \in a_0$ točka različita od vrhova.



Slika 3.2

Neka je $\mathcal{B} = \{A_0, U_1, U_2, U_3, V_1, V_2, V_3, M\}$, gdje su $U_i \in a_2$, $V_i \in a_1$ kao na Slici 3.2. Dvije 4-sekante od $\mathcal{B}$, a_1 i a_2, sijeku se u A_0. Tri 3-sekante su pravci (M, U_i) koji sadrže odgovarajuće V_j. Sedam 2-sekanti su pravci kroz dvije preostale točke P i Q s pravca a_0 i točke U_i koji sadrže odgovarajuće V_j, te pravac (A_0, M). Devet 1-sekanti su pravci (A_2, U_i), (A_1, V_i), zatim dva pravca kroz A_0 i točke P, Q s pravca a_0, te pravac (A_1, A_2) koji siječe $\mathcal{B}$ u točki M. $\mathcal{B} = \mathcal{T}^*$ je minimalna blokada od 8 točaka.

Pretpostavimo da je $\tau_4 = 3$. Tada je $\tau_1 = 8$, $\tau_2 = 10$ i $\tau_3 = 0$. Dvije 4-sekante od $\mathcal{B}$ nužno se sijeku u točki iz $\mathcal{B}$. Treća 4-sekanta implicira da $\mathcal{B}$ ima barem 9 točaka što je kontradikcija.

$q = 5$

- $9 \leq card\ \mathcal{B} \leq 22$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 12$, $\mathcal{B}$ minimalna blokada

U $PG(2,5)$ postoji projektivni trovrh stranice $\frac{1}{2}(q+3) = 4$ koji je minimalna blokada od $\frac{3}{2}(q+1) = 9$ točaka.

$q = 7$

- $11 \leq card\ \mathcal{B} \leq 46$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 19$, $\mathcal{B}$ minimalna blokada

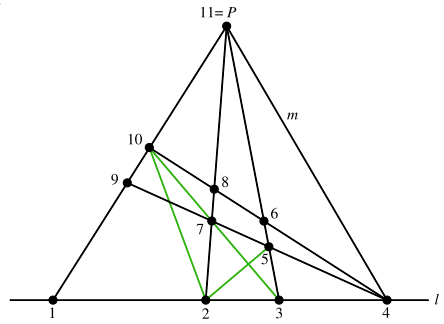
U $PG(2,7)$ postoji projektivni trovrh stranice $\frac{1}{2}(q+3) = 5$ koji je minimalna blokada od $\frac{3}{2}(q+1) = 12$ točaka.

Pokažimo da ne postoji blokada od 11 točaka. Pretpostavimo da je $card\ \mathcal{B} = 11$. Kako je $11 = q + 4$, onda neki pravac $l \in \Pi$ sadrži točno 4 točke iz $\mathcal{B}$ i niti jedan pravac ravnine ne sadrži više od 4 točke iz $\mathcal{B}$. Također, nikoje dvije točke iz $\mathcal{B} \setminus l$ nisu kolinearne s točkom iz $l \setminus \mathcal{B}$. Obzirom na raspodjelu točaka iz $\mathcal{B}$ na pravce kroz neku točku $P \in \mathcal{B} \setminus l$, imamo dva slučaja:

(A) Postoji pravac m koji sadrži točno 2 točke iz $\mathcal{B}$.

(B) Postoje točno dvije 3-sekante kroz P.

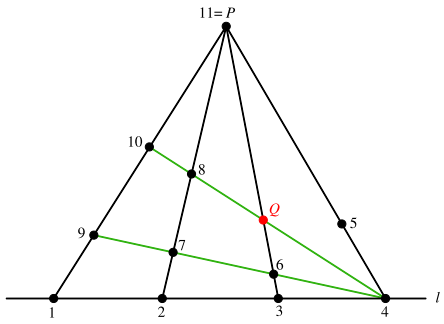
Slučaj (A): Neka je $m = (P, 4)$ 2-sekanta, a $(P, 1)$, $(P, 2)$ i $(P, 3)$ 4-sekante od $\mathcal{B}$.



Slika 3.3 *Slučaj* (A)

Spojimo točku 4 s bilo kojom točkom iz $\mathcal{B} \setminus l$ na pravcu $(P, 3)$, npr. 5. Kako je $card\ \mathcal{B} = 11$, pravac $(4, 5)$ siječe $(P, 1)$ i $(P, 2)$ u točkama iz $\mathcal{B}$, pa imamo pravac $(4, 5, 7, 9)$. Slično dobijemo pravac $(4, 6, 8, 10)$. Odaberimo točku sa $l \cap \mathcal{B}$, npr. 2 i spojimo je s točkom iz $\mathcal{B} \setminus l$, npr. 10. Pravac $(2, 10)$ siječe $(3, P)$ u točki 5, pa je $(2, 10)$ 3-sekanta. Pravac $(10, 7)$ siječe $(3, P)$ u točki 3, pa je $(7, 10)$ također 3-sekanta. Dakle, postoje točno dvije 3-sekante kroz točku 10 pa se slučaj (A) svodi na (B).

Slučaj (B): Neka su $(P, 3)$ i $(P, 4)$ 3-sekante, a $(P, 1)$ i $(P, 2)$ 4-sekante od $\mathcal{B}$.



Slika 3.4 *Slučaj* (B)

Spojimo točku 4 s točkama iz $\mathcal{B} \setminus l$ na pravcu $(P, 2)$, tj. sa 7 i 8. Ta dva pravca sijeku $(P, 1)$ u točkama iz $\mathcal{B}$ i tako sadrže po barem tri točke iz $\mathcal{B}$. Jedan od njih mora sjeći $(P, 3)$ u točki Q koja nije u $\mathcal{B}$. Dakle, na pravcu $(4, Q)$ su 3 točke iz $\mathcal{B}$ i na pravcu (P, Q) su 3 točke iz $\mathcal{B}$. Kroz Q prolazi još $q - 1 = 6$ pravaca ravnine i svi oni sijeku $\mathcal{B}$ u barem jednoj točki jer je $\mathcal{B}$ blokada ravnine. To povlači da je $card\ \mathcal{B} \geq 3 + 3 + 6 = 12$, što je kontradikcija.

Dakle za blokadu $\mathcal{B}$ ravnine $PG(2, 7)$ vrijedi da je najmanja blokada ravnine prethodno spomenuti projektivni trovrh od 12 točaka.

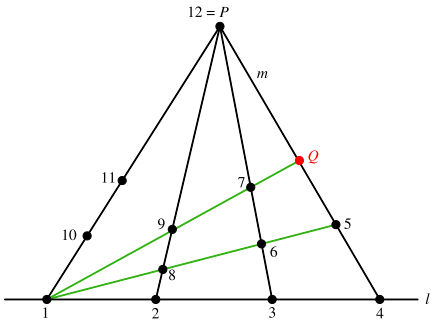
$q = 8$

- $12 \leq card\ \mathcal{B} \leq 61$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 23$, $\mathcal{B}$ minimalna blokada

U $PG(2, 8)$ postoji projektivna trijada stranice $\frac{1}{2}(q + 2) = 5$ koja je minimalna blokada od $\frac{1}{2}(3q + 2) = 13$ točaka.

Pokažimo da ne postoji blokada od 12 točaka. Pretpostavimo da je $card\ \mathcal{B} = 12$. Kako je $12 = q + 4$, onda neki pravac $l \in \Pi$ sadrži točno 4 točke iz $\mathcal{B}$ i niti jedan pravac ravnine ne sadrži više od 4 točke iz $\mathcal{B}$. Također, nikoje dvije točke iz $\mathcal{B} \setminus l$ nisu kolinearne s točkom iz $l \setminus \mathcal{B}$. Obzirom na raspodjelu točaka iz $\mathcal{B}$ na pravce kroz neku točku $P \in \mathcal{B} \setminus l$, vrijedi samo slučaj:

(A) Postoji pravac m koji sadrži točno 3 točke iz $\mathcal{B}$.



Slika 3.5 *Slučaj* (A)

Neka je $m = (P, 4)$ 3-sekanta, a $(P, 1)$, $(P, 2)$ i $(P, 3)$ 4-sekante od $\mathcal{B}$. Spojimo točku 1 s točkama iz $\mathcal{B} \setminus l$ na pravcu $(P, 2)$, tj. sa 8 i 9. Ta dva pravca sijeku $(P, 3)$ u točkama iz $\mathcal{B}$ i tako sadrže po barem tri točke iz $\mathcal{B}$. Jedan od njih mora sjeći $(P, 4)$ u točki Q koja nije u $\mathcal{B}$. Dakle, na pravcu $(1, Q)$ su 3 točke iz $\mathcal{B}$ i na pravcu (P, Q) su 3 točke iz $\mathcal{B}$. Kroz Q prolazi još $q-1 = 7$ pravaca ravnine i svi oni sijeku $\mathcal{B}$ u barem jednoj točki jer je $\mathcal{B}$ blokada ravnine. To povlači da je $card\ \mathcal{B} \geq 3+3+7 = 13$, što je kontradikcija.

Dakle za blokadu $\mathcal{B}$ ravnine $PG(2, 8)$ vrijedi da je najmanja blokada ravnine prethodno spomenuta projektivna trijada od 13 točaka.

$q = 9$

- $13 \leq card\ \mathcal{B} \leq 78$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 28$, $\mathcal{B}$ minimalna blokada

Baerova podravnina $PG(2,3)$ ravnine $PG(2,9)$ je minimalna blokada od 13 točaka.

U $PG(2,9)$ postoji projektivni trovrh stranice $\frac{1}{2}(q+3) = 6$ koji je minimalna blokada od $\frac{3}{2}(q+1) = 15$ točaka.

Minimalna blokada od 28 točaka je Hermiteov luk, tj. skup točaka kojeg svaki pravac ove ravnine siječe u jednoj ili četiri točke.

$q = 11$

- $16 \leq card\ \mathcal{B} \leq 117$, $\mathcal{B}$ blokada
- $card\ \mathcal{B} \leq 37$, $\mathcal{B}$ minimalna blokada

U $PG(2,11)$ postoji projektivni trovrh stranice $\frac{1}{2}(q+3) = 7$ koji je minimalna blokada od $\frac{3}{2}(q+1) = 18$ točaka.

Pokažimo da ne postoji blokada od 16 točaka. Pretpostavimo da je $card\ \mathcal{B} = 16$. Kako je $16 = q + 5$, onda neki pravac $l \in \Pi$ sadrži točno 5 točaka iz $\mathcal{B}$ i niti jedan pravac ravnine ne sadrži više od 5 točaka iz $\mathcal{B}$. Također, nikoje dvije točke iz $\mathcal{B} \setminus l$ nisu kolinearne s točkom iz $l \setminus \mathcal{B}$. Obzirom na raspodjelu točaka iz $\mathcal{B}$ na pravce kroz neku točku $P \in \mathcal{B} \setminus l$, imamo tri glavna slučaja:

(A) Postoji pravac m koji sadrži točno 2 točke iz $\mathcal{B}$.

(B) Svaki pravac iz $\mathcal{B}$ koji prolazi točkom P sadrži barem 3 točke iz $\mathcal{B}$ i postoji pravac m koji sadrži točno 3 točke iz $\mathcal{B}$.

(C) Svaki pravac iz $\mathcal{B}$ sadrži barem 4 točke iz $\mathcal{B}$.

Vrijede sljedeći podslučajevi od (A):

(A_1) Postoji točno jedna 3-sekanta kroz P.

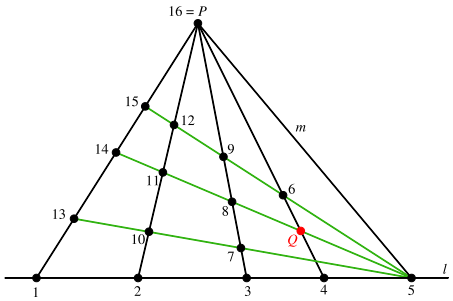
(A_2) Svaki pravac iz $\mathcal{B}$ kroz P osim m sadrži barem 4 točke iz $\mathcal{B}$.

i podslučajevi od (B):

(B_1) Postoje točno dvije 3-sekante kroz P.

(B_2) Svaki pravac iz $\mathcal{B}$ kroz P osim m sadrži barem 4 točke iz $\mathcal{B}$.

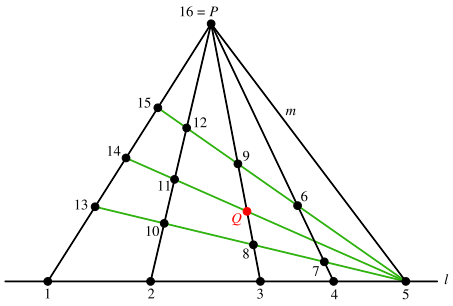
Slučaj (A_1): Neka je $m = (P, 5)$ 2-sekanta, $(P, 4)$ 3-sekanta i $(P, 1)$, $(P, 2)$, $(P, 3)$ 5-sekante od $\mathcal{B}$ kao na Slici 3.6.



Slika 3.6 *Slučaj* (A_1)

Spojimo točku 5 s točkama iz $\mathcal{B} \setminus l$ na pravcu $(P, 3)$, tj. sa 7, 8 i 9. Ta tri pravca sijeku $(P, 1)$ i $(P, 2)$ u točkama iz $\mathcal{B}$, pa sadrže po barem 4 točke iz $\mathcal{B}$. Barem jedan od njih mora sjeći $(P, 4)$ u točki Q koja nije u $\mathcal{B}$. Dakle, na pravcu $(5, Q)$ su 4 točke iz $\mathcal{B}$, a na pravcu (P, Q) su 3 točke iz $\mathcal{B}$. Kroz Q prolazi još $q - 1 = 10$ pravaca ravnine i svi oni sijeku $\mathcal{B}$ u barem jednoj točki jer je $\mathcal{B}$ blokada ravnine. To povlači da je $card\ \mathcal{B} \geq 4 + 3 + 10 = 17$, što je kontradikcija.

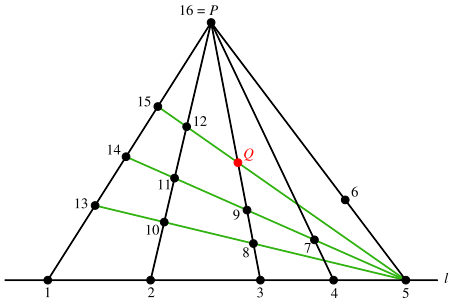
Slučaj (A_2): Neka je $m = (P, 5)$ 2-sekanta, $(P, 3)$ i $(P, 4)$ 4-sekante, te $(P, 1)$ i $(P, 2)$ 5-sekante od $\mathcal{B}$ kao na Slici 3.7.



Slika 3.7 *Slučaj* (A_2)

Spojimo točku 5 s točkama iz $\mathcal{B} \setminus l$ na pravcu $(P, 2)$, tj. sa 10, 11 i 12. Ta tri pravca sijeku $(P, 1)$ u točkama iz $\mathcal{B}$ i tako sadrže po barem 3 točke iz $\mathcal{B}$. Jedan od njih mora sjeći $(P, 3)$ u točki Q koja nije u $\mathcal{B}$. Dakle, na $(5, Q)$ su 3 točke iz $\mathcal{B}$, na (P, Q) su 4 točke iz $\mathcal{B}$, a na preostalih 10 pravaca ravnine kroz Q je barem jedna točka iz $\mathcal{B}$. Ovo povlači da je $card\ \mathcal{B} \geq 3 + 4 + 10 = 17$, što je kontradikcija.

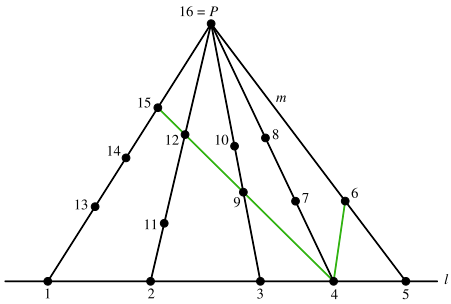
Slučaj (B_1): Neka su $(P,4)$ i $(P,5)$ 3-sekante, $(P,3)$ 4-sekanta, te $(P,1)$ i $(P,2)$ 5-sekante od $\mathcal{B}$ kao na Slici 3.8.



Slika 3.8 *Slučaj* (B_1)

Spojimo točku 5 s točkama iz $\mathcal{B} \setminus l$ na pravcu $(P,2)$, tj. sa 10, 11 i 12. Ta tri pravca sijeku $(P,1)$ u točkama iz $\mathcal{B}$ i tako sadrže barem tri točke iz $\mathcal{B}$. Jedan od njih mora sjeći $(P,3)$ u točki Q koja nije u $\mathcal{B}$. Proučavajući pravce ravnine kroz Q vrijedi da je $card\ \mathcal{B} \geq 3+4+10 = 17$, što je kontradikcija.

Slučaj (B_2): Neka je $m = (P,5)$ 3-sekanta, $(P,2)$, $(P,3)$ i $(P,4)$ 4-sekante, te $(P,1)$ 5-sekanta od $\mathcal{B}$ kao na Slici 3.9.



Slika 3.9 *Slučaj* (B_2)

Neka je točka 6 na pravcu $(P,5)$. Pravac $(4,6)$ mora sjeći pravac $(P,1)$ u točki iz $\mathcal{B}$, npr. 15. Također, pravac $(4,6)$ siječe $(P,2)$ i $(P,3)$ u točkama iz $\mathcal{B}$, pa je $(4,6)$ 5-sekanta. Dakle, postoje barem dvije 5-sekante kroz točku 15 pa se slučaj (B_2) svodi na jedan od prethodnih slučajeva.

Slučaj (C): Kako je $card\ \mathcal{B} = 16$, onda nikoja dva pravaca ne mogu se sjeći u točki koja nije iz $\mathcal{B}$. To znači da točke i pravci od $\mathcal{B}$ tvore podravninu od Π. Kako 16 nije oblika q^2+q+1 za niti jedan q, slučaj (C) nije moguć.

Dakle za blokadu $\mathcal{B}$ ravnine $PG(2,11)$ vrijedi da je $card\ \mathcal{B} \geq 17$. U teoremima koji slijede ova ocjena će se još poboljšati, odnosno vidjet ćemo da je najmanja blokada ove ravnine prethodno spomenuti projektivni trovrh od 18 točaka.

Poglavlje 4

Lakunarni polinomi i blokade

Promatramo potpuno reducibilni polinom oblika

$$f(X) = X^n + g(X)$$

takav da je stupanj polinoma g najviše $n-2$, tj. f je polinom kojem je jedan ili više uzastopnih koeficijenata nakon vodećeg člana jednak nuli. Ovakav polinom naziva se **lakunaran polinom**. Teoriju potpuno reducibilnih lakunarnih polinoma razvio je Rédei te ju primijenio, među ostalim, na ocjenu broja smjerova određenim grafom funkcije nad konačnim poljem ([27]).
Za stupanj polinoma f koristit ćemo oznaku f°. Drugi stupanj polinoma f, u oznaci $f^{\circ\circ}$, stupanj je polinoma g. Dakle, polinom je lakunaran ako vrijedi $f^\circ - f^{\circ\circ} \geq 2$.

Neka je p prim broj i $h \in \mathbb{N}$. Lakunarne polinome promatrat ćemo nad konačnim poljima u oznakama

- $K = GF(p)$, konačno polje reda p,
- $L = GF(q)$, konačno polje reda $q = p^h$ i karakteristike p.

Prsten polinoma nad K i L označavamo s $K[X]$ i $L[X]$.

PRIMJER 4.1 *Potpuno reducibilni lakunarni polinomi.*

1. $f(X) = X^{q-1} - 1,\ q > 2,\ f(X) \in L[X]$

Lakunarnost: $f^\circ - f^{\circ\circ} = q - 1 \geq 2$.
Za svaki element a cikličke grupe $(L^*, \cdot)$ koja je reda $q-1$, vrijedi $a^{q-1} = 1$.
Dakle, f je potpuno reducibilan lakunaran polinom, $f(X) = \prod_{a \in L^*}(X - a)$.

2. $Xf(X) = X^q - X = \prod_{a \in L}(X - a),\ q > 2,\ Xf(X) \in L[X]$

3. $g(X) = X^d - a^d,\ d \in \mathbb{N},\ d \mid (q-1),\ a \in L,\ g(X) \in L[X]$

Lakunarnost: $g^\circ - g^{\circ\circ} = d \geq 2$.
Neka je ω generator od L^*, tj. primitivni korijen od L za kojeg vrijedi $\omega^{q-1} = 1$, te neka je $q - 1 = m \cdot d$. Tada je $\omega^{q-1} = \omega^{md} = (\omega^m)^d = 1$, odnosno $\omega^m \in L$ je d-ti primitivni korijen jedinice, a $\{\omega^m, \omega^{2m}, \ldots, \omega^{(d-1)m}, 1\}$ je ciklička podgrupa reda d od L^*. Lakunaran polinom g je potpuno reducibilan jer vrijedi

$$\begin{aligned} g(X) &= X^d - a^d = a^d\Big[\Big(\frac{X}{a}\Big)^d - 1\Big] \\ &= a^d \prod_{i=1}^{d} \Big(\frac{X}{a} - \varepsilon_i\Big),\ \varepsilon_i = \omega^{im} \in L \\ &= \prod_{i=1}^{d} (X - a\varepsilon_i),\ a\varepsilon_i \in L. \end{aligned}$$

4. $h(X) = X^p - X^{\frac{p+1}{2}},\ p > 2,\ h(X) \in K[X]$

Lakunarnost: $h^\circ - h^{\circ\circ} = \frac{1}{2}(p-1) \geq 2$.
Polinom je potpuno reducibilan po prethodnom jer $\frac{p-1}{2} \mid (p-1)$ i vrijedi $h(X) = X\big(X^{p-1} - X^{\frac{p-1}{2}}\big) = X^{\frac{p+1}{2}}\big(X^{\frac{p-1}{2}} - 1\big)$. Osim za prim broj p, ovaj lakunaran polinom je potpuno reducibilan i za neparan q.

5. $l(X) = X^q \pm 2X^{\frac{q+1}{2}} + X,\ l(X) \in L[X]$

Lakunarnost: $l^\circ - l^{\circ\circ} = \frac{1}{2}(q-1) \geq 2$.
Vrijedi $l(X) = X(X^{q-1} \pm 2X^{\frac{q-1}{2}} + 1) = X(X^{\frac{q-1}{2}} \pm 1)^2$. Polinom $X(X^{\frac{q-1}{2}} - 1)^2$ očito je potpuno reducibilan. Neka je $l(X) = X(X^{\frac{q-1}{2}} + 1)^2$. Ako je $\omega^{q-1} = 1$, onda je $\omega^{\frac{q-1}{2}} = -1$ te vrijedi $X^{\frac{q-1}{2}} + 1 = X^{\frac{q-1}{2}} - (-1) = X^{\frac{q-1}{2}} - \omega^{\frac{q-1}{2}}$, pa je i u ovom slučaju lakunaran polinom potpuno reducibilan.

Promotrimo sada svojstva derivacije polinoma. Neka je $f(X) \in L[X]$ polinom oblika

$$f(X) = a_0 + a_1X + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i.$$

Derivaciju polinoma definiramo kao polinom

$$f'(X) = \sum_{i=1}^{n} ia_iX^{i-1}.$$

Ako je $a \in L$ m-struki korijen od f, tj. $(X-a)^m \mid f(X)$, $f(X) = (X-a)^m g(X)$, $g(a) \neq 0$, onda je a $(m-1)$-struki korijen od f'. Naime,

$$f'(X) = m(X-a)^{m-1}g(X) + (X-a)^m g'(X) = (X-a)^{m-1}\big[mg(X) + (X-a)g'(X)\big].$$

Ako $p \mid m$, onda je a i m-struki korijen od f', jer je $m = 0$ u $L[X]$, pa vrijedi

$$f'(X) = (X - a)^m g'(X).$$

Ako je $f = c$, onda je $f' = 0$. Ako je $f' = 0$, onda je $ia_i = 0$, $i \in \{1, 2, \ldots, n\}$. U slučaju da $p \mid i$, onda je $ia_i = 0$ i za $a_i \neq 0$, odnosno,

$$f' = 0 \quad \Leftrightarrow \quad f(X) \in L[X^p].$$

TEOREM 4.2 *Neka je $f(X) \in K[X]$ polinom oblika $f(X) = X^p + g(X)$, pri čemu je $f^{\circ\circ} = g^\circ < p$. Ako je $f(X)$ potpuno reducibilan nad K, onda vrijedi jedna od tvrdnji*

(i) $g(X)$ *je konstanta* ;

(ii) $g(X) = -X$;

(iii) $g^\circ \geq \frac{p+1}{2}$.

Dokaz Neka je $f(X) = l(X)r(X)$, gdje polinom $l(X)$ sadrži sve linearne faktore od $f(X)$ točno jedan put. Tada je polinom $r(X)$ sastavljen od onih faktora koji su višestruki u $f(X)$. Polinom $l(X)$ dijeli polinome $(X^p - X)$ i $f(X)$, pa je $l(X)$ njihova najveća zajednička mjera, tj. vrijedi

$$l(X) \mid \big[f(X) - (X^p - X)\big] = \big[g(X) + X\big].$$

Nadalje,

$$f'(X) = p\ X^{p-1} + g'(X) = g'(X),$$
$$f'(X) = l'(X)r(X) + l(X)r'(X).$$

Polinom $r(X)$ dijeli $f'(X) = g'(X)$, pa vrijedi

$$f(X) = l(X)r(X) \mid \big[g(X) + X\big]g'(X).$$

Pretpostavimo da vrijedi $\big[g(X) + X\big]g'(X) = 0$. Ako je $g'(X) = 0$, onda zbog $g^\circ < p$ vrijedi tvrdnja (i) $g(X)$ je konstanta. Ako je $\big[g(X) + X\big] = 0$, onda vrijedi tvrdnja (ii) $g(X) = -X$.
Pretpostavimo da vrijedi $\big[g(X) + X\big]g'(X) \neq 0$. Tada je $f^\circ \leq (g(X) + X)^\circ + g'(X)^\circ$, odnosno $p \leq g^\circ + g^\circ - 1$, pa vrijedi tvrdnja (iii) $g^\circ \geq \frac{p+1}{2}$. ■

Za slučaj $g^\circ = \frac{p+1}{2}$ možemo preciznije odrediti strukturu polinoma f. Iz dokaza vidimo da je tada $l^\circ = g^\circ$ i $r^\circ = (g')^\circ$ pa postoje $c_1, c_2 \in K^*$ takvi da je $l(X) = c_1\big[g(X) + X\big]$, $r(X) = c_2 g'(X)$. Dakle

$$f(X) = X^p + g(X) = c \cdot g'(x)\big[g(X) + X\big].$$

Neka je

$$g(X) = \gamma_{\frac{p+1}{2}} X^{\frac{p+1}{2}} + \gamma_{\frac{p-1}{2}} X^{\frac{p-1}{2}} + g_1(X),\ g_1^\circ < \frac{p-1}{2}.$$

Odredimo supstituciju $X \to X + a$, $a \in K$, tako da koeficijent uz član $X^{\frac{p-1}{2}}$ bude jednak nuli.

$$\begin{aligned} f(X+a) &= (X+a)^p + \gamma_{\frac{p+1}{2}}(X+a)^{\frac{p+1}{2}} + \gamma_{\frac{p-1}{2}}(X+a)^{\frac{p-1}{2}} + g_1(X+a) \\ &= X^p + a + \gamma_{\frac{p+1}{2}}(X^{\frac{p+1}{2}} + \frac{p+1}{2}X^{\frac{p-1}{2}}a + \cdots) + \\ &\quad + \gamma_{\frac{p-1}{2}}(X^{\frac{p-1}{2}} + \frac{p-1}{2}X^{\frac{p-3}{2}}a + \cdots) + g_1(X+a) \\ &= X^p + \gamma_{\frac{p+1}{2}}X^{\frac{p+1}{2}} + \big[\frac{p+1}{2}a\gamma_{\frac{p+1}{2}} + \gamma_{\frac{p-1}{2}}\big]X^{\frac{p-1}{2}} + \cdots \end{aligned}$$

Dakle,

$$\frac{p+1}{2}a\gamma_{\frac{p+1}{2}} + \gamma_{\frac{p-1}{2}} = 0 \;\Rightarrow\; a = -2\gamma_{\frac{p-1}{2}}/\gamma_{\frac{p+1}{2}},$$

te polinom g ima oblik

$$g(X) = \gamma_{\frac{p+1}{2}}X^{\frac{p+1}{2}} + \gamma_k X^k + g_2(X),\ \gamma_k \neq 0,\ k = g_1^\circ.$$

Uvedimo jednostavnije oznake, neka je $\alpha = \gamma_{\frac{p+1}{2}}$ i $\beta = \gamma_k$, tj.

$$g(X) = \alpha X^{\frac{p+1}{2}} + \beta X^k + g_2(X).$$

Pretpostavimo da je $k > 1$. Vrijedi

$$c \cdot g'(x)\big[g(X) + X\big] = c\big[\alpha\frac{p+1}{2}X^{\frac{p-1}{2}} + k\beta X^{k-1} + \cdots\big]\big[\alpha X^{\frac{p+1}{2}} + \beta X^k + \cdots\big].$$

Kako je $X^p + g(X) = c \cdot g'(x)\big[g(X) + X\big]$, onda izjednačimo koeficijente uz $X^{\frac{p-1}{2}+k}$ pa vrijedi

$$c(\alpha\frac{p+1}{2}\beta + k\beta\alpha) = 0 \quad \Rightarrow \quad c(\alpha\beta)(\frac{p+1}{2} + k) = 0$$

što je nemoguće. Dakle, $k = 1$, tj.

$$g(X) = \alpha X^{\frac{p+1}{2}} + \beta X + \gamma,\ \beta \neq 0.$$

Ponovimo postupak,

$$X^p + g(X) = c \cdot g'(x)\big[g(X) + X\big],$$

$$X^p + \alpha X^{\frac{p+1}{2}} + \beta X + \gamma = c\big[\alpha\frac{p+1}{2}X^{\frac{p-1}{2}} + \beta\big]\big[\alpha X^{\frac{p+1}{2}} + (\beta+1)X + \gamma\big],$$

i izjednačimo koeficijente uz $X^{\frac{p-1}{2}}$. Vrijedi

$$c(\alpha\frac{p+1}{2}\gamma) = 0 \quad \Rightarrow \quad \gamma = 0.$$

Dakle, ako je $g^\circ = \frac{p+1}{2}$, onda polinom f ima oblik (do na linearnu transformaciju)

$$f(X) = X^p + \alpha X^{\frac{p+1}{2}} + \beta X.$$

TEOREM 4.3 *Neka je $f(X) \in L[X]$ polinom oblika $f(X) = X^q + g(X)$, pri čemu je $f^{\circ\circ} = g^\circ < q$. Ako je $f(X)$ potpuno reducibilan nad L, onda vrijedi jedna od tvrdnji*

(i) $g(X) \in L[X^p]$;

(ii) $g(X) = -X$;

(iii) $g^\circ \geq \frac{q+1}{2}$.

Dokaz Dokaz ovog teorema je analogan dokazu prethodnog teorema, osim u slučaju $g'(X) = 0$, kada polinom $g(X)$ mora biti u varijabli X^p. Inače bi postojao član oblika X^m, gdje $p \nmid m$, pa bi $g'(X)$ imao član $mX^{m-1} \neq 0$. Dakle, u slučaju $g'(X) = 0$ vrijedi tvrdnja (i) $g(X) \in L[X^p]$. ■

TEOREM 4.4 *Neka je $f(X) \in L[X]$ potpuno reducibilan polinom nad L oblika $f(X) = X^q v(X) + w(X)$, gdje v i w nemaju zajedničkih faktora, $m = max(v^\circ, w^\circ)$, $m < q$ i neka je e najveći cijeli broj takav da je f p^e-ta potencija. Tada vrijedi jedna od tvrdnji*

(i) $e = h$, $m = 0$ *i* $f(X) = c_1 X^q + c_2$;

(ii) $\dfrac{h}{2} \leq e < h$ *i* $m \geq p^e$;

(iii) $0 < e < \dfrac{h}{2}$ *i* $m \geq p^e \left\lceil \dfrac{p^{h-e}+1}{p^e+1} \right\rceil$;

(iv) $e = 0$, $m = 1$ *i* $f(X) = c(X^q - X)$.

Također, ako je q prim broj i $m > 1$, onda je $m \geq \frac{1}{2}(q+1)$.

Dokaz Kako je $m < q$, onda svaki član od f ima eksponent koji je višekratnik od p^e, tj. polinomi v i w su također p^e-te potencije.
Ako je $e = h$, onda je $m = 0$ (u protivnom $m \geq q$), pa vrijedi tvrdnja (i).
Za $e \geq \frac{h}{2}$ je ili $m = 0$ (tj. $e = h$) ili $m \geq p^e$ što povlači tvrdnju (ii).

Pretpostavimo da je $e < \frac{h}{2}$. Neka je $E = p^e$, $f(X) = f_1(X)^E$, $v(X) = v_1(X)^E$, $w(X) = w_1(X)^E$. Tada je

$$f_1(X) = X^{q/E} v_1(X) + w_1(X).$$

Primijenimo rastav na f_1, tj. neka je $f_1(X) = l(X)r(X)$, gdje polinom $l(X)$ sadrži sve linearne faktore od $f_1(X)$ točno jedan put, a polinom $r(X)$ ostalo, tj. one faktore koji su višestruki u $f_1(X)$. Polinom $l(X)$ dijeli polinome $(X^q - X)$ i $f(X)$, pa dijeli i polinom $f(X) - v(X)(X^q - X)$, tj.

$$l(X) \mid Xv(X) + w(X).$$

Vrijedi $(X^{q/E})' = 0$. Polinom $r(X)$ dijeli $f_1'(X) = X^{q/E}v_1'(X) + w_1'(X)$ i $f_1(X)$, pa dijeli i polinom $f_1'(X)v_1(X) - v_1'(X)f_1(X)$, odnosno

$$r(X) \mid \big[X^{q/E}v_1'(X) + w_1'(X)\big]v_1(X) - v_1'(X)\big[X^{q/E}v_1(X) + w_1(X)\big],$$
$$r(X) \mid w_1'(X)v_1(X) - v_1'(X)w_1(X).$$

Kako je $(v, w) = 1$, a v_1 i w_1 nisu oba p-te potencije, onda je $w_1'(X)v_1(X) - v_1'(X)w_1(X) \neq 0$. Dakle,

$$f_1(X) = l(X)r(X) \mid \big[Xv(X) + w(X)\big]\big[w_1'(X)v_1(X) - v_1'(X)w_1(X)\big].$$

Ako je $Xv(X) + w(X) = 0$, onda zbog $(v, w) = 1$ je $m = 1$ pa vrijedi tvrdnja (iv). Pretpostavimo da vrijedi $Xv(X) + w(X) \neq 0$. Za stupanj polinoma f_1 vrijedi

$$f_1^\circ = \big[X^{q/E}v_1(X) + w_1(X)\big]^\circ,$$
$$f_1^\circ \leq \big[Xv(X) + w(X)\big]^\circ + \big[w_1'(X)v_1(X) - v_1'(X)w_1(X)\big]^\circ.$$

Pretpostavimo da je $v^\circ = w^\circ = m$, tada je $v_1^\circ = w_1^\circ = m_1$, gdje je $m = Em_1$. U ovom slučaju ponište se članovi najvišeg reda u $w_1'(X)v_1(X) - v_1'(X)w_1(X)$, pa vrijedi

$$\frac{q}{E} + m_1 \leq 1 + m + 2m_1 - 2,$$
$$\frac{q}{E} + 1 \leq m + m_1 = m(1 + \frac{1}{E}),$$
$$p^{h-e} + 1 \leq m(1 + p^{-e}),$$

a zbog cjelobrojnosti vrijedi

$$m \geq p^e \left\lceil \frac{p^{h-e} + 1}{p^e + 1} \right\rceil, \tag{4.1}$$

odnosno vrijedi tvrdnja (iii).
Pretpostavimo sada da je $v^\circ < w^\circ$, tj. $w^\circ = m^\circ$, $w_1^\circ = m_1$ i $m = Em_1$. Tada je

$$\frac{q}{E} + v_1^\circ \leq m + m_1 - 1 + v_1^\circ, \quad \Rightarrow \quad \frac{q}{E} + 1 \leq m(1 + \frac{1}{E}),$$

što opet daje nejednakost (4.1) i tvrdnju (iii).
Ako je $v^\circ > w^\circ$, odnosno $v^\circ = m^\circ$, $v_1^\circ = m_1$ i $m = Em_1$, onda je

$$\frac{q}{E} + m_1 \leq m + 1 + 2(m_1 - 1), \quad \Rightarrow \quad \frac{q}{E} + 1 \leq m(1 + \frac{1}{E}),$$

tj. vrijedi nejednakost (4.1) i tvrdnja (iii).

Ako je q prim broj i $m > 1$, onda je $e = 0$, $E = 1$ i $m = m_1$ pa za stupanj polinoma f_1 vrijedi

$$q + m \leq 1 + m + 2m - 2,$$
$$q + 1 \leq 2m,$$
$$m \geq \frac{1}{2}(q + 1),$$

čime je dokazana i posljednja tvrdnja ovog teorema. ∎

4.1 Smjerovi i Rédeijevi polinomi

Neka je funkcija $f\colon GF(q) \to GF(q)$. Zanima nas koliko je smjerova određeno funkcijom f, odnosno kolika je veličina skupa

$$\mathcal{D} = \left\{ \frac{f(x)-f(y)}{x-y} \;\middle|\; x,y \in GF(q), x \neq y \right\}.$$

PRIMJER 4.5

1. $f(x) = x^{\sqrt{q}}$, q kvadrat

$$\frac{f(x)-f(y)}{x-y} = \frac{x^{\sqrt{q}}-y^{\sqrt{q}}}{x-y} = \frac{(x-y)^{\sqrt{q}}}{x-y} = (x-y)^{\sqrt{q}-1},$$

tj. $\mathcal{D} = \{z^{\sqrt{q}-1} \mid z \in GF(q)^*\}$. Kako je $(z^{\sqrt{q}-1})^{\sqrt{q}+1} = z^{q-1} = 1$, onda su elementi skupa $\mathcal{D}$ rješenja jednadžbe $x^{\sqrt{q}+1} = 1$, pa zaključujemo da je $card\ \mathcal{D} = \sqrt{q}+1$.

2. $f(x) = x^{\frac{q+1}{2}}$, q neparan

Kako je $t^q = t$, onda slijedi

$$t^{\frac{q+1}{2}} = \begin{cases} t, & \text{ako je } t \text{ kvadrat,} \\ -t, & \text{ako } t \text{ nije kvadrat.} \end{cases}$$

Dakle,

$$\frac{f(x)-f(y)}{x-y} = \begin{cases} \frac{x-y}{x-y} = 1, & \text{ako su } x \text{ i } y \text{ kvadrati,} \\ \frac{-(x-y)}{x-y} = -1, & \text{ako } x \text{ i } y \text{ nisu kvadrati,} \\ \frac{x+y}{x-y} = \frac{1+z}{1-z}, & \text{ako je ili } x \text{ ili } y \text{ kvadrat,} \end{cases}$$

gdje je $x \neq y$ i z nije kvadrat. Za z postoji $\frac{q-1}{2}$ mogućnosti, pa je $card\ \mathcal{D} = 2 + \frac{q-1}{2} = \frac{1}{2}(q+3)$.

3. $f(x) = x^{q_1}$, $q = p^h$, $q_1 = p^r$, $r \mid h$

$$\frac{f(x)-f(y)}{x-y} = \frac{x^{q_1}-y^{q_1}}{x-y} = (x-y)^{q_1-1}.$$

Obzirom da $(q_1-1) \mid (q-1)$, vrijedi $card\ \mathcal{D} = \frac{q-1}{q_1-1}$.

4. $f(x) = Tr_{q_1}(x) = x + x^{q_1} + x^{q_1^2} + \cdots + x^{q/q_1}$

$$\frac{Tr_{q_1}(x)-Tr_{q_1}(y)}{x-y} = \frac{Tr_{q_1}(z)}{z},$$

gdje je $z = x-y$. Ako je $Tr_{q_1}(z) = 0$, onda je $Tr_{q_1}(z)/z = 0$ za q/q_1 vrijednosti od z. Ako je $Tr_{q_1}(z) \neq 0$ i $\alpha \in GF(q_1)^*$, onda je $Tr_{q_1}(\alpha z)/(\alpha z) = Tr_{q_1}(z)/z$, za $(q-q/q_1)/(q_1-1) = q/q_1$ različitih vrijednosti, pa je $card\ \mathcal{D} = q/q_1 + 1$.

Neka je $\mathcal{S}$ skup od q točaka afine ravnine $AG(2,q)$. Zanima nas koliko ima smjerova pravaca određeni parovima točaka iz $\mathcal{S}$.
Ako su $(a_1,b_1),(a_2,b_2)\in\mathcal{S}$, onda je

$$k=\begin{cases}\dfrac{b_2-b_1}{a_2-a_1}, & a_1\neq a_2,\\ \infty, & a_1=a_2.\end{cases}$$

Smjerova ukupno ima $q+1$, a po Dirichletu vrijedi da skup s više od q točaka određuje sve smjerove. Kako bi odredili ocjenu za broj smjerova skupa od q točaka koristimo Rédeijeve polinome.

DEFINICIJA 4.6 *Polinom pridružen skupu $\mathcal{S}\subseteq AG(2,q)$ zadan s*

$$r_{\mathcal{S}}(U,V,W)=\prod_{(a,b)\in\mathcal{S}}(aU+bV+W)$$

naziva se ***Rédeijev polinom****.*

Rédeijev polinom je homogeni, potpuno reducibilni polinom, totalnog stupnja q.
Ako je $(a,b)\in\mathcal{S}$ incidentna s pravcem $[u,v,w]$, onda je $r_{\mathcal{S}}(u,v,w)=0$, odnosno, svaki pravac kroz (a,b) poništava Rédeijev polinom.

Za projektivnu ravninu i skup $\mathcal{S}\subseteq PG(2,q)$ Rédeijev polinom ima oblik

$$r_{\mathcal{S}}(U,V,W)=\prod_{(a,b,c)\in\mathcal{S}}(aU+bV+cW).$$

Neka je $\mathcal{S}$ skup od q točaka afine ravnine $AG(2,q)$. Promotrimo pravac zadanog smjera k. Ako nas zanima da li ovaj pravac siječe skup $\mathcal{S}$, tj. da li sadrži neku njegovu točku, onda promatramo trojke $[k,-1,l]$. Koristimo oznake

$$\begin{aligned}H(U,W) &= r_{\mathcal{S}}(U,-1,W)=\prod_{(a,b)\in\mathcal{S}}(aU-b+W)\\ &= \sum_{j=0}^{q}h_j(U)W^j,\ h_j^{\circ}\leq q-j.\end{aligned}$$

$$H_k(W)=H(k,W)=\prod_{(a,b)\in\mathcal{S}}(ak-b+W)=\sum_{j=0}^{q}h_j(k)W^j.$$

Ako k nije određen skupom $\mathcal{S}$, onda će svi linearni faktori $ak-b+W$ biti različiti, pa vrijedi

$$H_k(W)=\prod_{(a,b)\in\mathcal{S}}(ak-b+W)=\prod_{c\in GF(q)}(W-c)=W^q-W.$$

Dakle, $h_j(k)=0$, za $j\in\{0\}\cup\{2,\ldots,q-1\}$, pa je k korijen od h_j.

Ako je k zastupljen u skupu $\mathcal{S}$, onda postoje barem dvije točke $(a_1, b_1), (a_2, b_2) \in \mathcal{S}$ takve da vrijedi $l = b_1 - ka_1 = b_2 - ka_2$. To znači da će doći do ponavljanja linearnih faktora $ak - b + W$.

Neka je d ukupan broj smjerova u $\mathcal{S}$, $(d-1)$ koeficijenata smjera iz $GF(q)$ i smjer ∞ (broj smjerova ne ovisi o koordinatnom sustavu pa ga odaberemo tako da pravac $x = 0$ sadrži barem dvije točke iz $\mathcal{S}$). Tada skalara iz $GF(q)$ koji nisu koeficijenti smjera određeni skupom $\mathcal{S}$ ima $q - (d-1) = q - d + 1$. Kako je $h_j^\circ \leq q - j$, onda h_j ima korijena barem onoliko koliko ima k koji nisu određeni skupom $\mathcal{S}$, tj. imat ćemo $h_j \equiv 0$ za h_j čiji je broj korijena veći od $q - j$. Kandidati za korijene su smjerovi koji nisu određeni skupom $\mathcal{S}$, a njih ima $q - d + 1 > q - j$, tj. $j \geq d$, pa je $h_j \equiv 0$ za $q > j \geq d$. Dakle, za k određen točkama iz $\mathcal{S}$, dobije se polinom

$$\begin{aligned} H_k(W) &= \sum_{j=0}^{q} h_j(k) W^j \\ &= W^q + h_{q-1}(k)W^{q-1} + \cdots + h_d(k)W^d + h_{d-1}(k)W^{d-1} + \cdots + h_0(k), \end{aligned}$$

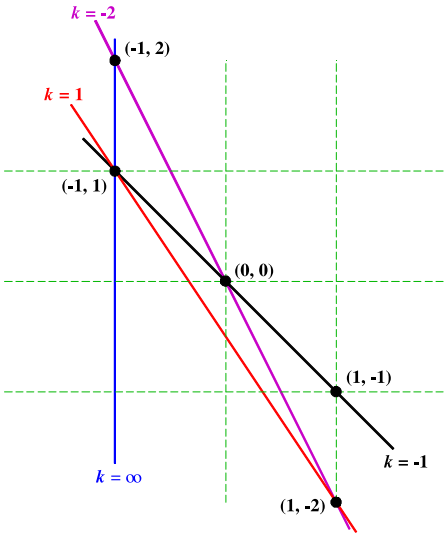
pri čemu je sigurno $h_{q-1}(k)W^{q-1} + \cdots + h_d(k)W^d = 0$, pa vrijedi

$$H_k^{\circ\circ} \leq d - 1 \quad \Rightarrow \quad d \geq H_k^{\circ\circ} + 1.$$

Što je više smjerova, to je manje uzastopnih koeficijenata nakon vodećeg člana jednako nuli.

PRIMJER 4.7 *Rédeijevi polinomi skupa* $\mathcal{S} \subset AG(2, 5)$.

Neka je $L = GF(5) = \{0, \pm 1, \pm 2\}$ i $\mathcal{S} = \{(0,0), (1,-1), (1,-2), (-1,1), (-1,2)\}$.



Slika 4.1

Smjerovi određeni točkama iz $\mathcal{S}$ su

$$k = \frac{b_2 - b_1}{a_2 - a_1} = \{1, -1, -2, \infty\},$$

pa je $d = 4$, a $H_k^{\circ\circ} \leq 3$. Ostali smjerovi koji nisu određeni točkama iz $\mathcal{S}$ su $k = \{0, 2\}$.

Odredimo Rédeijeve polinome

$$H_k(W) = \prod_{(a,b)\in\mathcal{S}} (ak - b + W).$$

Rédeijevi polinomi za smjerove $k = \{1, -1, -2\}$ određene točkama iz $\mathcal{S}$:

$$\begin{aligned} H_1(W) &= \prod_{(a,b)\in\mathcal{S}} (a - b + W) \\ &= W(2+W)(-2+W)(-2+W)(2+W) \\ &= W(W^2+1)^2 = W(W^4+2W^2+1) \\ &= W^5 + 2W^3 + W \end{aligned}$$

$$\begin{aligned} H_{-1}(W) &= \prod_{(a,b)\in\mathcal{S}} (-a - b + W) \\ &= W(0+W)(1+W)(0+W)(-1+W) = W^3(W^2-1) \\ &= W^5 - W^3 \end{aligned}$$

$$\begin{aligned} H_{-2}(W) &= \prod_{(a,b)\in\mathcal{S}} (-2a - b + W) \\ &= W(-1+W)(0+W)(1+W)(0+W) = W^3(W^2-1) \\ &= W^5 - W^3 \end{aligned}$$

Rédeijevi polinomi za smjerove $k = \{0, 2\}$ koji nisu određeni točkama iz $\mathcal{S}$:

$$\begin{aligned} H_0(W) &= \prod_{b\in L} (W - b) \\ &= W(W-1)(W+1)(W-2)(W+2) = W(W^4-1) \\ &= W^5 - W \end{aligned}$$

$$\begin{aligned} H_2(W) &= \prod_{(a,b)\in\mathcal{S}} (2a - b + W) \\ &= W(-2+W)(-1+W)(2+W)(1+W) = W(W^4-1) \\ &= W^5 - W \end{aligned}$$

4.2 Veličina blokade određena lakunarnim polinomima

Rezultate Rédeijeve teorije potpuno reducibilnih lakunarnih polinoma upotrijebit ćemo za ocjenu veličine blokade u Desarguesovoj projektivnoj ravnini nad konačnim poljem $GF(q)$, reda $q = p^h$ i karakteristike p.

TEOREM 4.8 *Neka je $\mathcal{B}$ blokada ravnine $PG(2,q)$, te neka je card $\mathcal{B} = k$. Tada vrijede tvrdnje*

(i) ako je q prim broj, onda je $k \geq \frac{3}{2}(q+1)$;

(ii) ako je q kvadrat, onda je $k \geq q + \sqrt{q} + 1$;

(iii) ako je h neparan, onda je $k \geq q + \sqrt{pq} + 1$.

Dokaz Tvrdnja (ii) je sadržana u Teoremu 2.16, a znamo i da se donja granica postiže, obzirom da konačna projektivna ravnina kvadratnog reda q sadrži Baerovu podravninu od $q + \sqrt{q} + 1$ točaka koja je po Teoremu 2.18 blokada. Ovdje ćemo (ii) ponovo dokazati, ovaj put koristeći Rédeijeve polinome.

Neka je $\mathcal{B} = \mathcal{S} \cup \{\mathbf{U_0}\}$ blokada ravnine $PG(2,q)$ i neka je *card* $\mathcal{B} = q + m + 1$. Pretpostavimo da postoji pravac koji siječe blokadu u samo jednoj točki, jer u suprotnom možemo ukloniti jednu ili više točaka, a da $\mathcal{B}$ i dalje bude blokada. Neka je $l_\infty = \mathbf{u_2}$ unisekanta od $\mathcal{B}$ tako da je $\mathcal{S} \subset AG(2,q) = PG(2,q) \setminus l_\infty$.

Neka je $\mathcal{S} = \{(a_i, b_i) \mid i = 1, \ldots, q+m\} \subset AG(2,q)$. Horizontalni pravac $[0,-1,c]$ ima jednadžbu $y = c$ i njegova beskonačno daleka točka je $\mathbf{U_0} \in l_\infty$. Skup $\mathcal{S}$ ima po barem jednu točku na svakom pravcu koji nije horizontalan (oni su oblika $[1,u,t]$). Dakle, za svaki par $u, t \in GF(q)$ jednadžba $x + uy + t = 0$ ima rješenje u $\mathcal{S}$, tj. $a_i + ub_i + t = 0$ za neki i. Odavde slijedi da je Rédeijev polinom

$$r_{\mathcal{S}}(1,U,T) = \prod_{(a_i,b_i)\in\mathcal{S}} (a_i + b_i U + T)$$

jednak nuli za svaki $u, t \in GF(q)$, tj. $r_{\mathcal{S}}(1,u,t) = 0$, pa se po Teoremu 1.26 $r_{\mathcal{S}}$ nalazi u idealu generiranom s $U^q - U$ i $T^q - T$. Zapišimo polinom u obliku

$$r_{\mathcal{S}}(1,U,T) = F(U,T) = (U^q - U)H(U,T) + (T^q - T)G(U,T), \tag{4.2}$$

gdje su G i H totalnog stupnja m u varijablama U i T. Neka je F_0 homogeni dio u F stupnja $q+m$, i neka su G_0 i H_0 homogeni dijelovi u G i H stupnja m. Tada je

$$F_0 = U^q H_0 + T^q G_0$$

gdje je

$$F_0(U,T) = \prod_{i=1}^{q+m} (T + b_i U). \tag{4.3}$$

Varijabla U više nema ulogu, obzirom da je jednadžba (4.3) homogena, pa uvrstimo $U = 1$ i definirajmo $F_1(T) = F_0(1,T)$, $G_1(T) = G_0(1,T)$, $H_1(T) = H_0(1,T)$. Tada je

$$F_1(T) = \prod(T + b_i)$$

odnosno, F_1 je potpuno reducibilan,

$$F_1 = T^q G_1 + H_1,$$

gdje je $G_1^\circ = m$, $H_1^\circ \leq m$.

Ako je F_1 djeljiv s $T^q + b_j$, za neki $b_j \in GF(q)$, onda obzirom da je $T^q + b_j = (T + b_j)^q$, slijedi da je svih q točaka horizontalnog pravca $y = b_j$ sadržano u $\mathcal{S}$. No tada $\mathcal{B}$ sadržava pravac, što je kontradikcija s činjenicom da je $\mathcal{B}$ blokada.

Pretpostavimo da F_1 nije djeljiv s $T^q + b_j$, za svaki $b_j \in GF(q)$. Nakon dijeljenja, po potrebi, s najvećim zajedničkim djeliteljem od G_1 i H_1, granica na m pa onda i na $k = card\ \mathcal{B}$ slijedi po Teoremu 4.4.

(i) Neka je q prim broj. Tada je po posljednjoj tvrdnji Teorema 4.4 $m \geq \frac{1}{2}(q+1)$, pa je $k = q + m + 1 \geq q + \frac{1}{2}(q+1) + 1 = \frac{3}{2}(q+1)$.

(ii) Neka je q kvadrat. Po tvrdnji (ii) Teorema 4.4 za $e = \frac{h}{2}$ je $q = p^{2e}$ i $m \geq p^e = \sqrt{q}$, pa je $k = q + m + 1 \geq q + \sqrt{q} + 1$.

(iii) Neka je h neparan. Pokažimo prvo da vrijedi $\dfrac{p^{e+1}+1}{p^e+1} > p - 1$.
Pretpostavimo suprotno

$$\frac{p^{e+1}+1}{p^e+1} \leq p-1 \quad \Rightarrow \quad p^{e+1}+1 \leq p^{e+1} + p - p^e - 1 \quad \Rightarrow \quad p \geq p^e + 2,$$

a ovo je kontradikcija. Dakle

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

pa po tvrdnji (iii) Teorema 4.4 za $e = \frac{h-1}{2}$ i $q = p^{2e+1}$ vrijedi

$$m \geq p^e \left\lceil \frac{p^{e+1}+1}{p^e+1} \right\rceil \geq p^{e+1} = \sqrt{pq},$$

tj. $k = q + m + 1 \geq q + \sqrt{pq} + 1$. ∎

PRIMJER 4.9 *Donja granica veličine blokada u $PG(2,q)$, $q \leq 11$.*

U Poglavlju 3 proučavali smo veličine blokada u ravninama $PG(2,q)$ reda $q \leq 11$. Po Teoremu 2.16 za blokadu $\mathcal{B}$ vrijedi $card\ \mathcal{B} \geq q+\sqrt{q}+1$. Ako primijenimo Teorem 4.8, onda se donja granica veličine blokade za $q = 7$ poboljšava sa $card\ \mathcal{B} \geq 11$ na $card\ \mathcal{B} \geq 12$, za $q = 8$ sa $card\ \mathcal{B} \geq 12$ na $card\ \mathcal{B} \geq 13$, a za $q = 11$ sa $card\ \mathcal{B} \geq 16$ na $card\ \mathcal{B} \geq 18$.

PRIMJER 4.10 *Lakunaran polinom blokade u $PG(2,7)$.*

Skup točaka $\mathcal{B}$ je blokada u $PG(2,7)$:

$$\mathcal{B} = \{(1,0,0),(0,1,0),(0,0,1),(1,1,1),(1,-3,2),(1,2,-3),(2,1,1),(1,2,1),(1,1,2),$$
$$(-3,1,1),(1,-3,1),(1,1,-3)\}.$$

Pritom je $card\ \mathcal{B} = \frac{3}{2}(q+1) = 12$ te ova blokada postiže donju granicu tvrdnje (i) Teorema 4.8. Afine točke ove blokade su:

$$\mathcal{S} = \{(0,0),(1,1),(-3,2),(2,-3),(2,1),(1,2),(-3,-3),(-3,1),(1,-3),(2,2)\}.$$

Oznake polinoma F_1, G_1 i H_1 odgovaraju terminologiji Teorema 4.8, pa je lakunaran polinom koji odgovara ovoj blokadi oblika

$$\begin{aligned} F_1(T) &= \prod(T+b_i) \\ &= T(T+1)^3(T+2)^3(T-3)^3 \ = \ T\big[(T+1)(T+2)(T-3)\big]^3 \\ &= T(T^3+1)^3 \ = \ T^{10}+3T^7+3T^4+T \\ &= T^7(T^3+3)+3T^4+T \\ &= T^7G_1(T)+H_1(T), \end{aligned}$$

$G_1(T) = T^3+3, \quad H_1(T) = 3T^4+T.$

PRIMJER 4.11 *Lakunaran polinom blokade u $PG(2,13)$.*

Skup točaka

$$\mathcal{B} = \{(1,0,0),(0,1,0),(0,0,1),(1,a,0),(0,1,a),(a,0,1),(b,c,1) \mid a^3 = -1, b^3 = c^3 = 1\}$$

blokada je u $PG(2,13)$, tj. $a \in \{-1,-3,4\}$, $b,c \in \{1,3,-4\}$ i

$$\mathcal{B} = \{(1,0,0),(0,1,0),(0,0,1),(1,-1,0),(1,-3,0),(1,4,0),(0,1,-1),(0,1,-3),$$
$$(0,1,4),(-1,0,1),(-3,0,1),(4,0,1),(1,1,1),(1,3,1),(1,-4,1),(3,1,1),$$
$$(3,3,1),(3,-4,1),(-4,1,1),(-4,3,1),(-4,-4,1)\}.$$

Pritom je $card\ \mathcal{B} = \frac{3}{2}(q+1) = 21$ te ova blokada postiže donju granicu tvrdnje (i) Teorema 4.8. Afine točke ove blokade su:

$$\mathcal{S} = \{(0,0),(0,-1),(0,4),(0,-3),(-1,0),(-3,0),(4,0),(1,1),(1,3),(1,-4),(3,1),$$
$$(3,3),(3,-4),(-4,1),(-4,3),(-4,-4)\}.$$

Oznake polinoma F_1, G_1 i H_1 odgovaraju terminologiji Teorema 4.8, pa je lakunaran polinom koji odgovara ovoj blokadi oblika

$$\begin{aligned} F_1(T) &= \prod(T+b_i) \\ &= T^4(T-1)(T+4)(T-3)(T+1)^3(T+3)^3(T-4)^3 \\ &= T\big[(T-1)(T^2+T+1)\big]\big[(T+1)(T^2-T+1)\big]^3 \\ &= T^4(T^3-1)(T^3+1)^3 \;=\; T^4(T^6-1)(T^6+2T^3+1) \\ &= T^4(T^{12}+2T^9-2T^3-1) \;=\; T^{16}+2T^{13}-2T^7-T^4 \\ &= T^{13}G_1(T)+H_1(T), \end{aligned}$$

$G_1(T) = T^3+2, \quad H_1(T) = -2T^7-T^4.$

Poglavlje 5

Blokade Rédeijevog tipa

Neka je $\Pi = PG(2,q)$ konačna projektivna ravnina reda q i $L = GF(q)$ konačno polje reda $q = p^h$ i karakteristike p.

DEFINICIJA 5.1 *Blokada $\mathcal{B}$ od $q+m$ točaka u Π naziva se **Rédeijeva blokada** ravnine Π ako postoji pravac ravnine koji siječe $\mathcal{B}$ u točno m točaka.*

Neka je dana funkcija $f\colon L \to L$. Broj smjerova određenih funkcijom f je veličina skupa

$$\mathcal{D} = \left\{ \frac{f(x)-f(y)}{x-y} \;\middle|\; x,y \in L, x \neq y \right\}.$$

LEMA 5.2 *Rédeijeva blokada se može konstruirati u Π iz bilo koje funkcije $f\colon L \to L$ koja nije linearna ili koja ne određuje sve smjerove.*

Dokaz Neka je $\mathcal{B} = \{(t, f(t), 1) \mid t \in L\} \cup \{(1, d, 0) \mid d \in \mathcal{D}\}$ skup od k točaka. Promotrimo pravce kroz neku točku $P \in l_\infty = \mathbf{u_2}$. Tada je ili $P = (1, d_1, 0)$ za neki $d_1 \in \mathcal{D}$ ili svi pravci kroz P sijeku skup $\{(t, f(t), 1) \mid t \in L\}$ u točno jednoj točki. Dakle, svaki pravac sadrži neku točku iz $\mathcal{B}$. Ostaje pitanje da li $\mathcal{B}$ sadržava neki cijeli pravac. Ako f određuje sve smjerove, tada $\mathcal{B}$ sadržava cijeli l_∞. Ako je f linearna funkcija, npr. $f(t) = at + b$, onda je $\mathcal{D} = \{a\}$ i $\mathcal{B}$ sadržava pravac $X_1 - f(X_0) = 0$ na kojem leže sve točke $(t, f(t), 1), t \in L$. Ovo znači da ako f nije linearna funkcija i ako ne određuje sve smjerove, onda je $\mathcal{B}$ blokada (netrivijalna). Također, pravac l_∞ je $(k-q)$-sekanta skupa $\mathcal{B}$ pa je blokada $\mathcal{B}$ Rédeijevog tipa, odnosno minimalna blokada. ■

PRIMJER 5.3 *Rédeijeve blokade i funkcije nad L.*

U Primjeru 4.5 izračunali smo ukupan broj smjerova za nekoliko funkcija. Za pripadne Rédeijeve blokade konstruirane iz tih funkcija vrijedi $card\ \mathcal{B} = q + card\ \mathcal{D}$, odnosno:

1. $f(x) = x^{\sqrt{q}}$, q kvadrat
$\Rightarrow \quad card\ \mathcal{D} = \sqrt{q} + 1 \quad \Rightarrow \quad card\ \mathcal{B} = q + \sqrt{q} + 1$

2. $f(x) = x^{\frac{q+1}{2}}$, q neparan
$\Rightarrow \quad card\ \mathcal{D} = \frac{1}{2}(q+3) \quad \Rightarrow \quad card\ \mathcal{B} = \frac{3}{2}(q+1)$

3. $f(x) = x^{q_1}$, $q = p^h$, $q_1 = p^r$, $r \mid h$
$\Rightarrow \quad card\ \mathcal{D} = \frac{q-1}{q_1-1} \quad \Rightarrow \quad card\ \mathcal{B} = q + \frac{q-1}{q_1-1}$

4. $f(x) = Tr_{q_1}(x) = x + x^{q_1} + x^{q_1^2} + \cdots + x^{q/q_1}$
$\Rightarrow \quad card\ \mathcal{D} = q/q_1 + 1 \quad \Rightarrow \quad card\ \mathcal{B} = q + q/q_1 + 1$

Izborom koordinata u $PG(2,q)$ za beskonačno daleki pravac l_∞ možemo uzeti m-sekantu Rédeijeve blokade $\mathcal{B}$. Tada je $\mathcal{S} = \mathcal{B} \setminus l_\infty$ skup od q točaka u $AG(2,q)$ i možemo ga shvatiti kao graf neke funkcije na polju L, pri čemu je $\mathcal{D}$ skup svih smjerova određenih točkama iz $\mathcal{S}$, odnosno

$$\mathcal{D} = \left\{ \frac{u_2 - v_2}{u_1 - v_1} \;\middle|\; u \neq v, u = (u_1, u_2), v = (v_1, v_2) \in \mathcal{S} \right\} \subset L \cup \{\infty\}.$$

TEOREM 5.4 *Neka je $\mathcal{S} \subset AG(2,q)$ skup od $q = p^h$ točaka i neka je $\mathcal{D}$ skup svih smjerova određenih točkama iz $\mathcal{S}$, pri čemu je $card\ \mathcal{D} = m$. Neka je e, $0 \leq e \leq h$, najveći cijeli broj takav da svaki pravac čiji je smjer sadržan u $\mathcal{D}$ sadrži višekratnik od p^e točaka iz $\mathcal{S}$. Tada vrijedi jedna od tvrdnji:*

(i) $e = 0$ *i* $\dfrac{q+3}{2} \leq m \leq q+1$;

(ii) $e = 1$, $p = 2$ *i* $\dfrac{q+5}{3} \leq m \leq q-1$;

(iii) $p^e > 2$, *e dijeli h* *i* $\dfrac{q}{p^e} + 1 \leq m \leq \dfrac{q-1}{p^e - 1}$;

(iv) $e = h$ *i* $m = 1$.

Dokaz Za skup $\mathcal{S}$ definiramo pripadni Rédeijev polinom

$$R(X,Y,Z) = \prod_{(u_1,u_2)\in\mathcal{S}} (X + u_1 Y - u_2 Z) = \sum_{j=0}^{q} r_j(Y,Z) X^j.$$

Neka je $R_y(X) = R(X, y, 1)$ za $y \in L$ tj.

$$R_y(X) = \prod_{(u_1,u_2)\in\mathcal{S}} (X + u_1 Y - u_2) = \sum_{j=0}^{q} r_j(y) X^j$$

i neka je $R_\infty(X) = R(X, 1, 0)$. Tada je R_y normirani polinom stupnja q u varijabli X. Ovaj polinom bilježi veličine presjeka pravaca smjera y sa skupom $\mathcal{S}$, tj. ove veličine presjeka su u biti kratnosti korijena od R_y. Ako y nije određen skupom $\mathcal{S}$, tada svi mogući korijeni imaju kratnost jedan:

$$R_y(X) = X^q - X \quad \Leftrightarrow \quad y \notin \mathcal{D}.$$

Skalara y koji nisu koeficijenti smjera određeni skupom $\mathcal{S}$ ima $q-(m-1) = q-m+1$ (smjer ∞ je određen skupom $\mathcal{S}$). Obzirom da je $R_y^\circ = q$, tada je $r_j^\circ \leq q-j$. Polinom r_y čiji je broj korijena veći od stupnja jednak je nuli, a r_j ima korijena barem onoliko koliko ima y koji nisu određeni skupom $\mathcal{S}$, tj. imat ćemo $r_j \equiv 0$ za r_j čiji je broj korijena veći od $q-j$. Kandidati za korijene su smjerovi koji nisu određeni skupom $\mathcal{S}$, pa vrijedi

$$q-m+1 > q-j \quad \Rightarrow \quad q-m \geq q-j \quad \Rightarrow m \leq j,$$

odnosno $r_j \equiv 0$ za $1 < j < q$ i $j \geq m$. Dakle, za y određen točkama iz $\mathcal{S}$, dobije se polinom

$$\begin{aligned} R_y(X) &= \sum_{j=0}^{q} r_j(y)X^q \\ &= X^q + r_{q-1}(y)X^{q-1} + \cdots + r_m(y)X^m + r_{m-1}(y)X^{m-1} + \cdots + r_0(y), \end{aligned}$$

pri čemu je sigurno $r_1(y)X^{q-1} + \cdots + r_m(y)X^m = 0$, pa vrijedi

$$\begin{aligned} R_y^{\circ\circ} &\leq m-1, \\ m &\geq 1 + R_y^{\circ\circ}. \end{aligned} \tag{5.1}$$

Drugi stupanj polinoma R_y, kada je definiran, mnogo je manji nego sam stupanj polinoma pa je R_y lakunaran polinom. Također je potpuno reducibilan nad L pa možemo primijeniti Teorem 4.4.

Neka je E_y djelitelj od q takav da je $R_y \in L[X^{E_y}] \setminus L[X^{pE_y}]$ i neka je $E = min_{y\in\mathcal{D}} E_y$. Tada svaki pravac smjera y siječe skup $\mathcal{S}$ u višekratnik od E_y točaka, a svaka sekanta siječe $\mathcal{S}$ u višekratnik od E točaka. Po terminologiji Teorema 4.4 vrijedi $E = p^e$.

Prebrojimo točke skupa $\mathcal{S}$ kojeg pravci iz fiksne točke $u \in \mathcal{S}$ sijeku u svim mogućim smjerovima. Sekanti kroz u ima ukupno m i svaka ta sekanta sadržava barem $E-1$ točaka iz $\mathcal{S} \setminus \{u\}$. Kako je $card\ \mathcal{S} \setminus \{u\} = q-1$ vrijedi

$$m(E-1) \leq q-1,$$

odnosno za $E > 1$ dobijemo gornju granicu

$$m \leq \frac{q-1}{E-1}. \tag{5.2}$$

Za donju granicu primijenimo rezultat Teorema 4.4 na R_y, odnosno

$$R_y^{\circ\circ} \geq p^e \left\lceil \frac{p^{h-e}+1}{p^e+1} \right\rceil,$$

$$R_y^{\circ\circ} \geq \frac{q+E}{E+1}.$$

Ako uvrstimo ovo u (5.1), slijedi donja granica

$$m \geq 1 + \frac{q+E}{E+1}. \tag{5.3}$$

Dokažimo tvrdnje teorema.

(*i*) Neka je $e = 0$. Tada je $E = p^e = 1$, a po (5.3) vrijedi

$$m \geq 1 + \frac{q+E}{E+1} \quad \Rightarrow \quad m \geq \frac{q+3}{2}.$$

Gornja granica ove tvrdnje je trivijalna, ona uvijek vrijedi, tj.

$$m \leq q + 1.$$

(*ii*) Neka je $e = 1$ i $p = 2$. Tada je $E = p^e = 2$, pa za donju granicu (5.3) vrijedi

$$m \geq 1 + \frac{q+E}{E+1} \quad \Rightarrow \quad m \geq \frac{q+5}{3}.$$

Kako je $E > 1$, iz (5.2) dobijemo i gornju granicu

$$m \leq \frac{q-1}{E-1} \quad \Rightarrow \quad m \leq q - 1.$$

(*iv*) Neka je $e = h$. Tada je $E = p^e = q$ odnosno svaka sekanta siječe $\mathcal{S}$ u q točaka pa one pripadaju jednom pravcu. Dakle $m = 1$, a smjer je ∞.

(*iii*) Neka je $p^e > 2$ i neka e dijeli h. Tada je $E = p^e > 2$ te iz (5.2) slijedi gornja granica

$$m \leq \frac{q-1}{E-1} \quad \Rightarrow \quad m \leq \frac{q-1}{p^e-1}.$$

Za donju granicu (5.3) vrijedi

$$m \geq 1 + \frac{q+E}{E+1} = 1 + \frac{q+p^e}{p^e+1} = 2 + \frac{q-1}{p^e+1}.$$

Želimo pokazati $m \geq \frac{q}{p^e} + 1$.

Kako je $R_y^{\circ\circ} \leq m - 1$, onda gornja granica (5.2) za m povlači

$$R_y^{\circ\circ} \leq m - 1 \leq \frac{q-1}{E-1} - 1 = \frac{q-E}{E-1}.$$

Potrebna nam je sljedeća lema.

LEMA 5.5 *Neka je $f(X) = X^{q/E} + g(X)$, $f \in L[X] \setminus L[X^p]$ potpuno reducibilan polinom nad L, gdje je $E = p^e$, $0 \leq e < h$, tako da je $g^\circ \leq \frac{q-E}{E(E-1)}$ ako je $E \geq 4$ ili $g^\circ \leq q/E^2$ ako je $E = 3$. Tada vrijedi*

$$X^{q/E} + g = (g^E + X)g'.$$

Dokaz Neka je $f(X) = l(X)r(X)$, gdje polinom $l(X)$ sadrži sve linearne faktore od $f(X)$ točno jedan put, a polinom $r(X)$ ostalo, tj. one faktore koji su višestruki u $f(X)$. Polinom $l(X)$ dijeli polinome $(X^q - X)$, $f(X)$, ali i $[f(X)]^E = X^q + [g(X)]^E$, pa dijeli i polinom $[f(X)]^E - (X^q - X)$, tj.

$$l(X) \mid [g(X)]^E + X.$$

Polinom $r(X)$ dijeli $f'(X)$, a kako vrijedi $(X^{q/E})' = 0$, onda polinom $r(X)$ dijeli $f'(X) = g'(X)$. Dakle,

$$f(X) = l(X)r(X) \mid \big([g(X)]^E + X\big)g'(X),$$

te možemo pisati

$$w(X^{q/E} + g) = (g^E + X)g' \tag{5.4}$$

za neki polinom w stupnja

$$w^\circ = Eg^\circ + g'^\circ - q/E. \tag{5.5}$$

Odredimo derivaciju (5.4).

$$(X^{q/E} + g)' = \Big(\frac{(g^E + X)g'}{w}\Big)',$$

$$g' = \frac{[(g^E + X)'g' + (g^E + X)g'']w - [(g^E + X)g']w'}{w^2}, \quad / \cdot w^2$$

$$w^2 g' = [g' + (g^E + X)g'']w - (g^E + X)g'w',$$

$$(w^2 - w)g' = (g^E + X)(g''w - g'w'). \tag{5.6}$$

Ako je $g''w - g'w' = 0$, onda je $w = 1$ pa tvrdnja leme vrijedi.
Pretpostavimo da je $g''w - g'w' \neq 0$ i usporedimo stupnjeve polinoma:

$$((w^2 - w)g')^\circ \geq (g^E + X)^\circ,$$

$$2w^\circ + g'^\circ \geq Eg^\circ,$$

$$2(Eg^\circ + g'^\circ - q/E) + g'^\circ \geq Eg^\circ,$$

$$Eg^\circ + 3g'^\circ \geq 2q/E.$$

Neka je $E = 3$. Tada je po uvjetima leme $g^\circ \leq q/E^2$, što je nemoguće jer je tada

$$2q/E \leq Eg^\circ + 3g'^\circ,$$

$$2q/3 \leq 3g^\circ + 3g'^\circ = 3(2g^\circ - 1) \leq 3(2q/9 - 1),$$

$$2q/9 \leq 2q/9 - 1,$$

a ovo je kontradikcija.

Neka je $E \geq 4$. Tada koristimo uvjet leme $g^\circ \leq \frac{q-E}{E(E-1)}$ i svojstvo da je $g'^\circ < g^\circ$:

$$2q/E \leq Eg^\circ + 3g'^\circ < Eg^\circ + 3g^\circ,$$
$$\frac{2q}{E} < (E+3)g^\circ \leq (E+3)\frac{q-E}{E(E-1)},$$
$$2q(E-1) \leq (E+3)(q-E),$$
$$q(E-5) \leq -E(E+3).$$

Dakle, $E < 5$, odnosno $E = 4$ i $p = 2$. Neka je $k = g''w - g'w'$ te ga uvrstimo u (5.4) i (5.6) (pritom koristimo svojstva $f^E - (X^q - X) = g^E + X$ i $f' = g'$). Dobijemo sljedeće jednadžbe

$$wf = (f^E - (X^q - X))f', \tag{5.7}$$
$$w(w-1)f' = (f^E - (X^q - X))k. \tag{5.8}$$

Pokažimo kroz četiri koraka da je tada $w = 1$.

1. *Ako je $f(a) = 0$, onda je $w(a) = \mu_a$, gdje je μ_a kratnost od a kao korijena polinoma f.*

   Neka je μ_a kratnost korijena a i zapišimo f u obliku $f(X) = (X-a)^{\mu_a}h(X)$. Promotrimo sljedeće

   $$\begin{aligned}(X-a)\frac{f'(X)}{f(X)} &= (X-a)\frac{\mu_a(X-a)^{\mu_a-1}h(X) + (X-a)^{\mu_a}h'(X)}{(X-a)^{\mu_a}h(X)} \\ &= \frac{\mu_a(X-a)^{\mu_a-1}h(X) + (X-a)^{\mu_a}h'(X)}{(X-a)^{\mu_a-1}h(X)} \\ &= \mu_a + (X-a)\frac{h'(X)}{h(X)}.\end{aligned}$$

   Vrijedi $(X-a)\frac{f'(X)}{f(X)}\big|_{X-a} = \mu_a$. Nadalje,

   $$\begin{aligned}\frac{f^E - (X^q - X)}{X-a} &= \frac{f^E}{X-a} - \frac{X^q - X + a - a}{X-a} \\ &= \frac{f^E}{X-a} - \frac{X^q - a}{X-a} - \frac{-X+a}{X-a} \\ &= \frac{f^E}{X-a} - \frac{X^q - a^q}{X-a} + 1,\end{aligned}$$

   pa je $\frac{f^E - (X^q - X)}{X-a}\big|_{X-a} = 1$, odnosno

   $$w(a) = \frac{(f^E - (X^q - X))f'}{f}\big|_{X-a} = \frac{(f^E - (X^q - X))}{(X-a)}\frac{(X-a)f'}{f}\big|_{X-a} = 1\cdot\mu_a = \mu_a.$$

2. *Broj korijena polinoma f s neparnom kratnošću je najviše w°.*

   Neka je a korijen od f s neparnom kratnošću, tj. $f(X) = (X-a)^{2n+1}h(X)$. Tada je a korijen polinoma f' s parnom kratnošću $2n$ obzirom da je

   $$f'(X) = (X-a)^{2n}[h(X) + (X-a)h'(X)].$$

   Nadalje, iz jednadžbe (5.7) vidimo da je svaki korijen od f korijen i od $(f^E - (X^q - X))$ kratnosti jedan. Pogledajmo kratnost korijena a za polinom $k = g''w - g'w' = f''w - f'w'$. Vrijedi

   $$\begin{aligned} f''(X) &= (X-a)^{2n}[h(X) + (X-a)h'(X)]' \\ &= (X-a)^{2n}[(X-a)h''(X)] \;=\; (X-a)^{2n+1}h''(X), \end{aligned}$$

   $$\begin{aligned} k(X) &= (X-a)^{2n+1}h''(X)w(X) - (X-a)^{2n}[h(X) + (X-a)h'(X)]w'(X) \\ &= (X-a)^{2n}\big[(X-a)h''(X)w(X) - h(X)w'(x) - (X-a)h'(X)w'(x)\big], \end{aligned}$$

   pa je a korijen parne kratnosti od k. Sada usporedimo kratnosti korijena a u jednadžbi (5.8). Kako znamo da a nije korijen od w, a da je s desne strane njegova kratnost ukupno neparna, onda a mora biti korijen od $w-1$. Dakle, korijeni koji imaju neparnu kratnost su korijeni od $w-1$, a njih je najviše w°.

3. *Stupanj od k je barem $q/4 - w^\circ$.*

   Po prethodnom je broj korijena parne kratnosti barem $q/4 - w^\circ$, pa f možemo zapisati u obliku

   $$f(X) = [(X-a_1)^{2\alpha_1}(X-a_2)^{2\alpha_2} \;\cdots\; (X-a_n)^{2\alpha_n}]h(x),$$

   gdje su a_i parne kratnosti, $n \geq q/4 - w^\circ$, odnosno, ako uzmemo baš $\eta = q/4 - w^\circ$ takvih korijena imamo

   $$\begin{aligned} f(X) &= [(X-a_1)^{2\alpha_1}(X-a_2)^{2\alpha_2} \;\cdots\; (X-a_\eta)^{2\alpha_\eta}]h_1(x), \\ &= [(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2} \;\cdots\; (X-a_\eta)^{\alpha_\eta}]^2 h_1(x), \end{aligned}$$

   pa f ima kvadratni faktor stupnja $q/4 - w^\circ$. Ovaj faktor dijeli f' obzirom je

   $$f'(X) = [(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2} \;\cdots\; (X-a_\eta)^{\alpha_\eta}]^2 h_1'(x),$$

   te se svaki korijen također javlja i u $w(w-1)$ jer je za korijen parne kratnosti $w(a_i) = \mu_{a_i} = 2\alpha_i = 0$. S desne strane jednadžbe (5.8) znamo da korijeni od $(f^E - (X^q - X))$ imaju kratnost jedan, pa slijedi da kvadratni faktor dijeli k, odnosno $k^\circ \geq q/4 - w^\circ$.

4. $k = 0$ *i* $w = 1$.

   Po pretpostavci je $g^\circ \leq \frac{q-E}{E(E-1)} = \frac{q-4}{12} < q/12$, a uspoređujući stupnjeve polinoma u (5.6) vrijedi $2w^\circ + g^\circ - 1 = 4g^\circ + k^\circ$, odnosno $2w^\circ + g^\circ > 4g^\circ + k^\circ$. Dakle,

   $$2w^\circ > 3g^\circ + q/4 - w^\circ \quad \Rightarrow \quad 3w^\circ - 3g^\circ > q/4.$$

   Kako je po (5.5) $w^\circ = 4g^\circ + g'^\circ - q/4 < 5g^\circ - q/4$,

   $$3(5g^\circ - q/4) - 3g^\circ > q/4 \quad \Rightarrow \quad 12g^\circ > q,$$

   što je kontradikcija.

Ovim je pokazano da je $w = 1$ i da vrijedi tvrdnja leme: $X^{q/E} + g = (g^E + X)g'$. ■

Promotrimo diferencijalnu jednadžbu $X^{q/E} + g = (g^E + X)g'$. Neka je $z = g'$. Želimo pokazati da je g uglavnom oblika $g(X) = X + X^E + \cdots + X^{q/E^2}$, odnosno da je z konstanta i da e dijeli h (iz $q/E = Eg^\circ + z^\circ$ za konstantan z slijedi $g^\circ = q/E^2$). U slučaju kada z nije konstanta možemo vrlo precizno odrediti granice njegovog stupnja i naći informacije o samom obliku polinoma. Vrijedi sljedeća lema.

LEMA 5.6 *Neka je* $X^{q/E} + g = (g^E + X)z$, *gdje je* $z = g'$. *Tada je ili* z *konstanta ili za neki* $i > 0$ *vrijedi* $z \in L[X^{E^i}] \setminus L[X^{E^{i+1}}]$,

$$\frac{q(E-1)}{E^{i+2}} \leq z^\circ < \frac{q(E-1)}{E^{i+2} - E}$$

i $z = \eta\zeta^{E-1}$, $\eta \in L[X^{E^{i+1}}]$, $\zeta \in L[X^{E^i}]$. *Pritom, svaki korijen od* z *ima kratnost barem* $(E-1)E^i$.

Dokaz Ako $z = g'$ nije konstanta, onda je $q > E^2$ te iz $q/E = Eg^\circ + z^\circ$ slijedi $q/E > Eg^\circ$, odnosno $z^\circ + 1 \leq g^\circ < q/E^2$. Ako u identiteti

$$X^{q/E} + (g - Xz) = g^E z \tag{5.9}$$

usporedimo članove s obje strane kojima stupanj nije djeljiv s E, onda s lijeve strane takvi imaju stupanj najviše q/E^2, a s desne imamo faktor g^E stupnja Eg°. Međutim, iz $X^{q/E} + g = (g^E + X)z$ dobijemo

$$q/E = Eg^\circ + z^\circ \leq Eg^\circ + g^\circ - 1 \quad \Rightarrow \quad q/E + 1 \leq g^\circ(E+1)$$

$$Eg^\circ \geq (q+E)/(E+1).$$

Vrijedi $(q+E)/(E+1) > q/E^2$ jer tada imamo

$$\frac{q+E}{E+1} > \frac{q}{E^2} \quad \Rightarrow \quad qE^2 + E^3 > qE + q \quad \Rightarrow \quad q(E^2 - E - 1) > -E^3,$$

a ova nejednakost vrijedi za svaki $E > 2$. Dakle, $Eg^\circ > q/E^2$ pa z nema nijedan član čiji stupanj nije djeljiv s E, tj. $z \in L[X^E]$.

Neka je $z \in L[X^{E^i}] \setminus L[X^{E^{i+1}}]$. Tada je $i \geq 1$ i

$$q/E = Eg^\circ + z^\circ \geq E(z^\circ + 1) + z^\circ = (E+1)z^\circ + E \geq (E+1)E^i + E > E^{i+1},$$

odnosno $q > E^{i+2}$. Za $j \geq 0$ označimo sa g_j sljedeće funkcije

$$g_j = g - Xz - X^E z^{E+1} - X^{E^2} z^{E^2+E+1} - \ \cdots \ - X^{E^{j-1}} z^{E^{j-1}+ \cdots +E+1},$$

odnosno

$$\begin{aligned}
g_0 &= g, \\
g_1 &= g - Xz, \\
g_2 &= g - Xz - X^E z^{E+1}, \\
g_3 &= g - Xz - X^E z^{E+1} - X^{E^2} z^{E^2+E+1}, \\
g_4 &= g - Xz - X^E z^{E+1} - X^{E^2} z^{E^2+E+1} - X^{E^3} z^{E^3+E^2+E+1}, \\
&\dots
\end{aligned}$$

Pokažimo induktivno da za $1 \leq j \leq i$ iz identitete (5.9) slijedi

$$X^{q/E} + g_j = g_{j-1}^E z,$$

što povlači $g_j(X) \in L[X^{E^j}]$.
Neka je $j = 1$. Tada vrijedi $X^{q/E} + g_1 = X^{q/E} + (g - Xz) = g^E z = g_0^E z$. Pretpostavimo da vrijedi $X^{q/E} + g_j = g_{j-1}^E z$ i pogledajmo jednakost za $j+1$.

$$\begin{aligned}
X^{q/E} + g_{j+1} &= X^{q/E} + g_j - X^{E^j} z^{E^j+ \cdots +E+1} \\
&= g_{j-1}^E z - X^{E^j} z^{E^j+ \cdots +E} z \\
&= [g_{j-1}^E - X^{E^j} z^{E^j+ \cdots +E}] z \\
&= [g_{j-1} - X^{E^{j-1}} z^{E^{j-1}+ \cdots +1}]^E z \\
&= g_j^E z.
\end{aligned}$$

Za $0 \leq j \leq i-1$ svi članovi od g_{j+1} se pojavljuju u g_j (obzirom da nijedan član $g_{j+1} - g_j = -X^{E^j} z^{E^j+ \cdots +1}$ ne leži u $L[X^{E^{j+1}}]$) tako da je $g_i^\circ \leq g^\circ$, odnosno

$$g_i = g - Xz - X^E z^{E+1} - X^{E^2} z^{E^2+E+1} - \ \cdots \ - X^{E^{i-1}} z^{E^{i-1}+ \cdots +E+1},$$

$$g_i + Xz + X^E z^{E+1} + X^{E^2} z^{E^2+E+1} + \ \cdots \ + X^{E^{i-1}} z^{E^{i-1}+ \cdots +E+1} = g,$$

$$\left[g_i + Xz + X^E z^{E+1} + X^{E^2} z^{E^2+E+1} + \ \cdots \ + X^{E^{i-1}} z^{E^{i-1}+ \cdots +E+1} \right]^\circ = g^\circ,$$

$$E^{i-1} + z^\circ (E^{i-1} + E^{i-2} + \ \cdots \ + E + 1) \ \leq \ g^\circ,$$

$$E^{i-1} + z^\circ \frac{E^i - 1}{E - 1} \leq g^\circ. \tag{5.10}$$

Neka je $\tilde{g} = g_i$. Tada $\tilde{g}$ zadovoljava

$$X^{q/E} + \tilde{g} - X^{E^i} z^{E^i + \cdots + E+1} = \tilde{g}^E z. \tag{5.11}$$

Ako je nejednakost (5.10) stroga, onda je $\tilde{g}^\circ = g^\circ$.

Pretpostavimo prvo da imamo jednakost u (5.10). Tada možemo odrediti g° i z° iz jednakosti $Eg^\circ + z^\circ = q/E$, i dobijemo

$$E^{i-1} + z^\circ \frac{E^i - 1}{E - 1} = \frac{q}{E^2} - \frac{z^\circ}{E} \quad / \cdot E^2(E-1)$$

$$z^\circ E^2(E^i - 1) + z^\circ E(E-1) = q(E-1) - E^{i+1}(E-1)$$

$$z^\circ = \frac{(E-1)(q - E^{i+1})}{E^{i+2} - E},$$

pa je

$$\begin{aligned} g^\circ &= E^{i-1} + z^\circ \frac{E^i - 1}{E-1} = E^{i-1} + \frac{(E-1)(q-E^{i+1})}{E^{i+2}-E} \frac{E^i - 1}{E-1} \\ &= \frac{E^{2i+1} - E^i + qE^i - q - E^{2i+1} + E^{i+1}}{E^{i+2} - E}, \end{aligned}$$

tj.

$$g^\circ = \frac{q(E^i - 1) + E^i(E-1)}{E^{i+2} - E}.$$

Zapišimo z° u obliku

$$z^\circ = \frac{(p^e - 1)(p^h - p^{(i+1)e})}{p^{(i+2)e} - p^e} = \frac{(p^e - 1)(p^h - p^{(i+1)e})}{p^e(p^{(i+1)e} - 1)}.$$

Kako je stupanj pozitivan cijeli broj, onda $(i+1)e$ dijeli h, tj. $h = k \cdot (i+1)e$ za neki $k \geq 2$, pa je $p^h \geq p^{2(i+1)e}$ odnosno $q \geq E^{2i+2}$. Da je tada z° cijeli broj vidimo iz

$$z^\circ = \frac{(p^e - 1)(p^{k(i+1)e} - p^{(i+1)e})}{p^e(p^{(i+1)e} - 1)} = \frac{(p^e - 1)p^{ie}(p^{(k-1)(i+1)e} - 1)}{p^{(i+1)e} - 1}.$$

Pokažimo da z° zadovoljava nejednakosti leme:

$$\frac{q(E-1)}{E^{i+2}} \leq z^\circ < \frac{q(E-1)}{E^{i+2} - E}.$$

Desna nejednakost se dobije jednostavno

$$z^\circ = \frac{(E-1)(q - E^{i+1})}{E^{i+2} - E} < \frac{(E-1)q}{E^{i+2} - E}.$$

Dokažimo lijevu nejednakost. Pretpostavimo suprotno

$$\frac{q(E-1)}{E^{i+2}} > z^\circ \quad \Rightarrow \quad q(E^{i+2} - E) > E^{i+2}(q - E^{i+1})$$

$$qE^{i+2} - qE > qE^{i+2} - E^{2i+3} \quad \Rightarrow \quad -qE > -E^{2i+3} \quad \Rightarrow \quad q < E^{2i+2}$$

što je kontradikcija.

Pokažimo da z ima traženi oblik.

Neka je $\tilde{g} = 0$. Tada iz (5.11) slijedi da je z monom. Imamo jednakost u (5.10) i $z = \alpha X^{z^\circ}$, gdje je $z^\circ = (E-1)(q - E^{i+1})/(E^{i+2} - E)$ i $\alpha^{E^i + \cdots + 1} = 1$. Dakle, z je $(E-1)$-va potencija.

Neka je $\tilde{g} \neq 0$. Zapišimo

$$z = \sum_{j=0}^{E-1} \eta_j X^{jE^i}, \quad \tilde{g} = \sum_{j=0}^{E-1} \gamma_j X^{jE^i},$$

gdje su η_j,$\gamma_j \in L[X^{E^{i+1}}]$, $0 \leq j \leq E-1$, te uvrstimo u (5.11) :

$$X^{q/E} + \tilde{g} - X^{E^i} z^{E^i + \cdots + E + 1} = \tilde{g}^E z$$

$$X^{q/E} + \sum_{j=0}^{E-1} \gamma_j X^{jE^i} - X^{E^i} z \cdot z^{E^i + \cdots + E} = \tilde{g}^E z$$

$$X^{q/E} + \sum_{j=0}^{E-1} \gamma_j X^{jE^i} - \Big[X^{E^i} \sum_{j=0}^{E-1} \eta_j X^{jE^i}\Big] z^{E^i + \cdots + E} = \tilde{g}^E \sum_{j=0}^{E-1} \eta_j X^{jE^i}$$

$$X^{q/E} + \sum_{j=0}^{E-1} \gamma_j X^{jE^i} - \Big[\sum_{j=0}^{E-1} \eta_j X^{(j+1)E^i}\Big] z^{E^i + \cdots + E} = \tilde{g}^E \sum_{j=0}^{E-1} \eta_j X^{jE^i}$$

$$X^{q/E} + \sum_{j=0}^{E-1} \gamma_j X^{jE^i} - \Big[\sum_{j=1}^{E} \eta_{j-1} X^{jE^i}\Big] z^{E^i + \cdots + E} = \tilde{g}^E \sum_{j=0}^{E-1} \eta_j X^{jE^i}$$

$$X^{q/E} + \gamma_0 + \sum_{j=1}^{E-1} \gamma_j X^{jE^i} - \Big[\sum_{j=1}^{E-1} \eta_{j-1} X^{jE^i} + \eta_{E-1} X^{E^{i+1}}\Big] z^{E^i + \cdots + E} = \tilde{g}^E \sum_{j=0}^{E-1} \eta_j X^{jE^i}.$$

Tada je za $1 \leq j \leq E-1$

$$\gamma_j - \eta_{j-1} z^{E^i + \cdots + E} = \tilde{g}^E \eta_j, \tag{E_j}$$

i

$$X^{q/E} + \gamma_0 - \eta_{E-1} X^{E^{i+1}} z^{E^i + \cdots + E} = \tilde{g}^E \eta_0. \tag{E_0}$$

Kako $\tilde{q}^E$ ima veći stupanj od γ_j, onda se vidi iz (E_j) da ako je $\eta_j \neq 0$, onda je i $\eta_{j-1} \neq 0$. Posebno, $\eta_0 \neq 0$. Štoviše, $\eta_1 \neq 0$ jer $z \notin L[X^{E^{i+1}}]$.
Izračunavanjem $\eta_j \cdot (E_j) - \eta_{j-1} \cdot (E_{j+1})$ za $1 \leq j \leq E-2$ dobijemo

$$\eta_j(\gamma_j - \eta_{j-1} z^{E^i + \cdots + E}) - \eta_{j-1}(\gamma_{j+1} - \eta_j z^{E^i + \cdots + E}) = \eta_j \tilde{g}^E \eta_j - \eta_{j-1} \tilde{g}^E \eta_{j+1},$$

odnosno

$$\eta_j \gamma_j - \eta_{j-1} \gamma_{j+1} = \tilde{g}^E (\eta_j^2 - \eta_{j-1} \eta_{j+1}).$$

Lijeva strana ima stupanj najviše $g^\circ + z^\circ$, dok je desna strana ili nula ili ima stupanj barem $E\tilde{g}^\circ$. Želimo pokazati da je $E\tilde{g}^\circ > g^\circ + z^\circ$.

Zaista, ili je $E\tilde{g}^\circ = Eg^\circ > g^\circ + z^\circ$, ili imamo jednakost u (5.10) tj.

$$E^{i-1} + z^\circ \frac{E^i - 1}{E - 1} = g^\circ$$

pa iz jednadžbe (E_1) možemo odrediti (za $E \geq 3$):

$$\gamma_1 - \eta_0 z^{E^i + \,\cdots\, + E} = \tilde{g}^E \eta_1 \quad \Rightarrow \quad \eta_0^\circ + (E^i + \,\cdots\, + E) z^\circ = E\tilde{g}^\circ + \eta_1^\circ,$$

$$\begin{aligned} E\tilde{g}^\circ &= (E^i + \,\cdots\, + E) z^\circ + \eta_0^\circ - \eta_1^\circ \;\geq\; (E^i + \,\cdots\, + E) z^\circ - z^\circ \\ &= z^\circ \frac{E(E^i - 1)}{E - 1} - z^\circ \;=\; E(g^\circ - E^{i-1}) - z^\circ \;=\; Eg^\circ - E^i - z^\circ \\ &= g^\circ + (E - 1) g^\circ - E^i - z^\circ. \end{aligned}$$

Pokažimo da je $(E-1)g^\circ - E^i - z^\circ > z^\circ$. Pretpostavimo suprotno, tj.

$$(E-1)g^\circ - E^i - z^\circ \leq z^\circ \quad \Rightarrow \quad (E-1)(E^{i-1} + z^\circ \frac{E^i - 1}{E - 1}) \leq E^i + 2z^\circ$$

$$E^{i-1}(E-1) + z^\circ (E^i - 3) \leq E^i \quad \Rightarrow \quad z^\circ \leq \frac{E^{i-1}}{E^i - 3} < 1$$

što je kontradikcija.

Dakle, $E\tilde{g}^\circ > g^\circ + z^\circ$, odnosno $\eta_j \gamma_j - \eta_{j-1}\gamma_{j+1} = \eta_j^2 - \eta_{j-1}\eta_{j+1} = 0$ za $1 \leq j \leq E-2$ pa je

$$\begin{array}{lll} \eta_1^2 = \eta_0 \eta_2 & \Rightarrow & \eta_2 = \eta_1^2/\eta_0 \\ \eta_2^2 = \eta_1 \eta_3 & \Rightarrow & \eta_3 = \eta_2^2/\eta_1 = \frac{1}{\eta_1}(\eta_2)^2 = \frac{1}{\eta_1}\frac{\eta_1^4}{\eta_0^2} = \eta_1^3/\eta_0^2 \\ \eta_3^2 = \eta_2 \eta_4 & \Rightarrow & \eta_4 = \eta_3^2/\eta_2 = \frac{1}{\eta_2}(\eta_3)^2 = \frac{\eta_0}{\eta_1^2}\frac{\eta_1^6}{\eta_0^4} = \eta_1^4/\eta_0^3 \\ \cdots & & \end{array}$$

odnosno $\eta_j = \eta_0(\eta_1/\eta_0)^j$ za $0 \leq j \leq E-1$, te vrijedi

$$\begin{aligned} z &= \eta_0 \sum_j \Big(\frac{\eta_1}{\eta_0} X^{E^i}\Big)^j \;=\; \eta_0 \Big(1 + \frac{\eta_1}{\eta_0} X^{E^i} + \frac{\eta_1^2}{\eta_0^2} X^{2E^i} + \,\cdots\, + \frac{\eta_1^{E-1}}{\eta_0^{E-1}} X^{(E-1)E^i}\Big) \\ &= \eta_0 \frac{(\frac{\eta_1}{\eta_0} X^{E^i})^E - 1}{\frac{\eta_1}{\eta_0} X^{E^i} - 1} \;=\; \eta_0 \Big(\frac{\eta_1}{\eta_0} X^{E^i} - 1\Big)^{E-1}. \end{aligned}$$

Neka je $\eta_0 = u_0 u$ i $\eta_1 = u_1 u$ gdje je u najveća zajednička mjera od η_0 i η_1 tako da su u_0 i u_1 relativno prosti. Tada je $u, u_0, u_1 \in L[X^{E^{i+1}}]$ i

$$z = u_0 u \Big(\frac{u_1 u}{u_0 u} X^{E^i} - 1\Big)^{E-1} = \frac{u}{u_0^{E-2}} (u_1 X^{E^i} - u_0)^{E-1}.$$

Sada slijedi da u_0^{E-2} dijeli u (naime, ako $X \mid u_0$ onda je kratnost faktora X u u_0 i u višekratnik od E^{i+1}, dok je u $(u_1 X^{E^i} - u_0)^{E-1}$ manja od E^{i+1}). Neka je $u/u_0^{E-2} = \eta$, $\eta \in L[X^{E^{i+1}}]$. Tada z ima traženi oblik $z = \eta \zeta^{E-1}$ uz $\zeta = u_1 X^{E^i} - u_0$.

Preostaje pokazati procjenu stupnja za z u slučaju $\tilde{g}^\circ = g^\circ$.

U ovom slučaju je $z^\circ = q/E - Eg^\circ$ višekratnik od E^{i+1}, pa je $\eta_0^\circ = z^\circ$. Nadalje, iz $\eta_0 = u_0 u = u_0 \eta u_0^{E-2} = \eta u_0^{E-1}$ i $\eta_1 = u_1 u = u_1 \eta u_0^{E-2}$ slijedi

$$\eta_0 = z^\circ = \eta^\circ + (E-1)u_0^\circ \quad \Rightarrow \quad u_0^\circ = \frac{z^\circ - \eta^\circ}{E-1}$$

$$\eta_1^\circ = u_1^\circ + \eta^\circ + (E-2)u_0^\circ = u_1^\circ + \eta^\circ + \frac{E-2}{E-1}(z^\circ - \eta^\circ),$$

$$\eta_1^\circ = \frac{E-2}{E-1}z^\circ + u_1^\circ + \frac{1}{E-1}\eta^\circ \quad \Rightarrow \quad \eta_1^\circ \geq \frac{E-2}{E-1}z^\circ$$

Promotrimo sada $\eta_1 \cdot (E_0) - \eta_0 \cdot (E_1)$

$$\eta_1 X^{q/E} + \eta_1\gamma_0 - \eta_0\gamma_1 + (\eta_0^2 - \eta_1\eta_{E-1}X^{E^{i+1}})z^{E^i + \cdots + E} = 0,$$

$$\eta_1[X^{q/E} + \gamma_0 - \eta_{E-1}X^{E^{i+1}} z^{E^i + \cdots + E}] = \eta_0[\gamma_1 - \eta_0 z^{E^i + \cdots + E}],$$

te usporedimo stupnjeve

$$\eta_1^\circ + q/E = 2\eta_0^\circ + E\frac{E^i - 1}{E-1}z^\circ.$$

Kako je $\eta_0^\circ = z^\circ$, vrijedi

$$\eta_1^\circ + \frac{q}{E} = \frac{E^{i+1} + E - 2}{E-1}z^\circ.$$

Uvrstimo $\eta_1^\circ \geq z^\circ(E-2)/(E-1)$.

$$\frac{E^{i+1} + E - 2}{E-1}z^\circ = \eta_1^\circ + \frac{q}{E} \geq \frac{E-2}{E-1}z^\circ + \frac{q}{E} \quad / \cdot E(E-1)$$

$$E^{i+2}z^\circ \geq q(E-1) \quad \Rightarrow \quad z^\circ \geq \frac{q(E-1)}{E^{i+2}}.$$

Također vrijedi

$$\frac{E^{i+1} + E - 2}{E-1}z^\circ = \eta_1^\circ + \frac{q}{E} < \frac{q}{E} \quad / \cdot E(E-1)$$

$$E(E^{i+1} + E - 2)z^\circ < q(E-1)$$

$$z^\circ < \frac{q(E-1)}{E^{i+2} + E^2 - 2E} = \frac{q(E-1)}{E^{i+2} - E + (E^2 - E)} < \frac{q(E-1)}{E^{i+2} - E}.$$

Dakle, stupanj od z zadovoljava nejednakosti leme i u slučaju $\tilde{g}^\circ = g^\circ$ te je lema u potpunosti dokazana. ■

S E_y označavali smo djelitelja od q takvog da je $R_y \in L[X^{E_y}] \setminus L[X^{pE_y}]$, pri čemu je $E = min_{y\in\mathcal{D}} E_y$. Neka je $\mathcal{D}_w$ skup svih $y \in \mathcal{D}$, gdje je $w = E_y$, te neka je $card\ \mathcal{D}_w = m_w$. Tada je $m = \sum_w m_w$. Kako svaki pravac smjera y siječe skup $\mathcal{S}$ u višekratnik od E_y točaka, a svaka sekanta siječe $\mathcal{S}$ u višekratnik od E točaka, onda je ukupan broj točaka skupa $\mathcal{S}$ kojeg pravci iz fiksne točke $u \in \mathcal{S}$ sijeku u svim mogućim smjerovima $\sum m_w(w-1)$. Obzirom da je $card\ \mathcal{S} \setminus \{u\} = q-1$ vrijedi

$$\sum m_w(w-1) \le q-1.$$

Ako je $m_{\bar{w}} = 0$ za $E < \bar{w} < t$, a iz (5.3) slijedi $m > q/(E+1)$, onda je

$$\begin{aligned}
(t-E)\sum_{w>E} m_w &= (t-1)\sum_{w>E} m_w + (1-E)\sum_{w>E} m_w \\
&= \sum_{w>E} m_w(t-1) - (E-1)\sum_{w>E} m_w \\
&= \Big[\sum_{w>E} m_w(t-1) + (E-1)m_E\Big] - \Big[(E-1)m_E + (E-1)\sum_{w>E} m_w\Big] \\
&< \sum_{w} m_w(w-1) - (E-1)m \\
&\le q-1-(E-1)\frac{q}{E+1} \;=\; \frac{qE+q-qE+q}{E+1} - 1 \;<\; \frac{2q}{E+1}
\end{aligned}$$

tj.

$$\sum_{w>E} m_w < \frac{2q}{(t-E)(E+1)},$$

$$m_E = m - \sum_{w>E} m_w > \frac{q}{E+1} - \frac{2q}{(t-E)(E+1)}.$$

Posebno, ove nejednakosti vrijede i za $t = pE$.

Neka se skalar $y \in \mathcal{D}$ naziva *regularnom točkom* ako je $E_y = E$. Broj regularnih točaka je m_E. Obzirom da je $R_y^{\circ\circ} \le \frac{q-E}{E-1}$, prethodne leme možemo primijeniti na regularne točke, tj. $R_y^{1/E} = X^{q/E} + g_y = (g_y^E + X)z_y$, gdje je $z_y = g_y'$, pritom osiguravajući da je $E \ge 4$ ili $E = 3$ i $m \le q/3+1$. Za regularnu točku $y \in \mathcal{D}$ reći ćemo da je *tipa* i ako je $z_y \in L[X^{E^i}] \setminus L[X^{E^{i+1}}]$, odnosno *regularna točka tipa* ∞ ako je z_y konstanta.

LEMA 5.7 *Neka je $E \ge 4$ ili $E = 3$ i $m \le q/3+1$. Tada postoji regularna točka y takva da je z_y konstanta.*

Dokaz Prebrojimo trojke $(a,b,y) \in \mathcal{S}\times\mathcal{S}\times\mathcal{D}$ gdje pravac koji spaja a i b ima smjer y. Kako svaki par određuje jedan smjer, trojki ima točno $q(q-1)$. Neka je m_y broj trojki za fiksni y. Ako je y regularna točka tipa $i < \infty$, onda svaka J-sekanta skupa $\mathcal{S}$ smjera y doprinosi sa $J(J-1)$ u m_y, tako da je

$$m_y = \sum_J J(J-1) = \sum_J J(J-E+E-1) = \sum_J J(J-E) + (E-1)\sum_J J,$$

$$m_y = \sum_J J(J-E) + q(E-1).$$

No pravci koji sijeku $\mathcal{S}$ u više od E točaka tada sijeku $\mathcal{S}$ u $E(1+a_\alpha E^i)$ točaka pa doprinose faktor kratnosti $(1+a_\alpha E^i)$ u g_y i faktor kratnosti $(a_\alpha E^i)$ u z_y. Kako je $\sum_\alpha a_\alpha E^i = z_y^\circ$ i $a_\alpha \geq E-1$ po prethodnoj lemi, onda slijedi

$$\begin{aligned}\sum_J J(J-E) &\geq \sum_\alpha E(1+a_\alpha E^i)[E(1+a_\alpha E^i)-E] = \sum_\alpha E(1+a_\alpha E^i)E(a_\alpha E^i)\\ &\geq E^{i+2}\sum_\alpha a_\alpha(1+a_\alpha E^i) > E^{i+2}(E-1)z_y^\circ \geq (E-1)^2 q.\end{aligned}$$

Slijedi da je

$$m_y = \sum_J J(J-E) + q(E-1) \geq (E-1)^2 q + q(E-1) = q(E^2-E).$$

Nadalje,

$$q(q-1) = \sum_y m_y \geq \sum_{y \text{ reg.tipa } i<\infty} q(E^2-E),$$

tj. broj regularnih točaka koje nisu tipa ∞ je najviše

$$\frac{q(q-1)}{q(E^2-E)} = \frac{q-1}{E^2-E}.$$

Kako je broj regularnih točaka

$$m_E > \frac{q}{E+1} - \frac{2q}{E(E+1)(p-1)},$$

a ovo je veće od $(q-1)/(E^2-E)$, onda postoji regularna točka y s konstantom z_y za $E \geq 3$. ■

Nastavak dokaza Teorema 5.4 Sada možemo dokazati i donju granicu za m u tvrdnji (iii) Teorema 5.4, tj. za $p^e > 2$ kada e dijeli h vrijedi $m \geq q/p^e+1 = q/E+1$. Dakle, za diferencijalnu jednadžbu $R_y^{1/E} = X^{q/E} + g_y = (g_y^E + X)z_y$, gdje je $z_y = g_y'$, proizlazi da je pod uvjetima tvrdnje (iii) z_y konstanta, odnosno da je g_y oblika $g_y(X) = X + X^E + \cdots + X^{q/E^2}$. Tada je $(R_y^{1/E})^{\circ\circ} = g_y^\circ = q/E^2$, odnosno $R_y^{\circ\circ} = q/E$. Uvrstimo ovo u (5.1):

$$m \geq 1 + R_y^{\circ\circ} = 1 + q/E.$$

Ovim su dokazane sve tvrdnje Teorema 5.4. ■

NAPOMENA 5.8

U Primjeru 5.3.2 postiže se donja granica tvrdnje (i) ovog teorema. Za tvrdnju (iii) gornja granica postiže se u Primjeru 5.3.3, dok se njena donja granica postiže u Primjeru 5.3.4.

PRIMJER 5.9 *Lakunarni polinomi Rédeijevih blokada u* $PG(2, 11)$.

1. Pokažimo prvo primjer konstrukcije Rédeijeve blokade. Neka je $\mathcal{B}_0$ skup sljedećih točaka u $AG(2, q)$:

$$\mathcal{B}_0 = \{(1,2,0),(1,3,0),(1,4,0),(1,5,0),(1,-5,0),(1,-4,0),(1,-3,0),$$
$$(1,-2,0),(1,-1,0)\}.$$

Dovoljno je pronaći skup točaka afine ravnine kojeg presijecaju pravci $x = b$, $y = b$ i $y = x + b$, gdje je $b \in GF(11)$.

Prvi skup čine presječne točke pravaca $y = -x - 2$ i $y = x - (2i - 1)$, za $i = 1, 2, 3, 4$, tj. točke $(\frac{2i-3}{2}, \frac{-2i-1}{2})$:

$$\mathcal{B}_1 = \{(5,4),(-5,3),(-4,2),(-3,1)\}.$$

Ove točke također blokiraju pravce $y = i$ te $x = i - \frac{3}{2}$, $i = 1, 2, 3, 4$.

Drugi skup čine presječne točke pravaca $y = -x$ i $y = x-(4i-4)$, za $i = 1, 2, 3$, tj. točke $(2i - 2, -2i + 2)$:

$$\mathcal{B}_2 = \{(0,0),(2,-2),(4,-4)\}.$$

Treći skup čine presječne točke pravaca $y = -x - 4$ i $y = x - (4i - 2)$, $i = 1, 2$, tj. točke $(2i - 3, -2i - 1)$:

$$\mathcal{B}_3 = \{(-1,-3),(1,-5)\}.$$

Na kraju dodajmo točke $(3, 5)$ i $(-2, -1)$. One se nalaze na preostalih 7 pravaca: $y = -x - 3$, $y = x + 1$, $y = x + 2$, $y = 5$, $x = 3$ i $x = -2$.

Sada je $\mathcal{B}$ Rédeijeva blokada u $PG(2, 11)$:

$$\mathcal{B} = \{(1,2,0),(1,3,0),(1,4,0),(1,5,0),(1,-5,0),(1,-4,0),(1,-3,0),(1,-2,0),$$
$$(1,-1,0),(5,4,1),(-5,3,1),(-4,2,1),(-3,1,1),(0,0,1),(2,-2,1),$$
$$(4,-4,1),(-1,-3,1),(1,-5,1),(3,5,1),(-2,-1,1)\}.$$

Pritom je $card\ \mathcal{B} = 20 = q + 9$, a pravac koji siječe Rédeijevu blokadu u 9 točaka je $\mathbf{u_2}$.

Afine točke ove blokade su:

$$\mathcal{S} = \{(5,4),(-5,3),(-4,2),(-3,1),(0,0),(2,-2),$$
$$(4,-4),(-1,-3),(1,-5),(3,5),(-2,-1)\}.$$

Oznake polinoma F_1, G_1 i H_1 odgovaraju terminologiji Teorema 4.8, pa je lakunaran polinom koji odgovara ovoj Rédeijevoj blokadi oblika

$$\begin{aligned} F_1(T) &= \prod(T+b_i) \\ &= T(T^2-1)(T^2-4)(T^2+2)(T^2-5)(T^2-3) \\ &= T(T^4-5T^2+4)(T^4-3T^2+1)(T^2-3) \\ &= T(T^8+3T^6-2T^4+5T^2+4)(T^2-3) \\ &= T(T^{10}-1) \;=\; T^{11}-T \\ &= T^{11}G_1(T)+H_1(T), \end{aligned}$$

$G_1(T)=1, \quad H_1(T)=-T.$

2. Skup točaka $\mathcal{B}$ je Rédeijeva blokada u $PG(2,11)$:

$$\begin{aligned} \mathcal{B} = \{&(1,0,0),(0,1,0),(0,0,1),(1,-1,0),(0,1,-1),(-1,0,1),(1,2,0),(0,1,2),\\ &(2,0,1),(1,-3,0),(0,1,-3),(-3,0,1),(1,-4,0),(0,1,-4),(-4,0,1),\\ &(1,-5,0),(0,1,-5),(-5,0,1)\}. \end{aligned}$$

Pritom je $card\ \mathcal{B} = \frac{3}{2}(q+1) = 18 = q+7$, te ova blokada postiže donju granicu tvrdnje (i) Teorema 5.4, tj. $m = \frac{q+3}{2} = 7$. Pravac koji siječe Rédeijevu blokadu u 7 točaka je $\mathbf{u_2}$.

Afine točke ove blokade su:

$$\begin{aligned} \mathcal{S} = \{&(0,0),(0,-1),(-1,0),(0,-5),(2,0),(0,-4),\\ &(-3,0),(0,-3),(-4,0),(0,2),(-5,0)\}. \end{aligned}$$

Oznake polinoma F_1, G_1 i H_1 odgovaraju terminologiji Teorema 4.8, pa je lakunaran polinom koji odgovara ovoj Rédeijevoj blokadi oblika

$$\begin{aligned} F_1(T) &= \prod(T+b_i) \\ &= T^6(T-1)(T-5)(T-4)(T-3)(T+2) \\ &= T^6(T-1)(T^2+2T-2)(T^2-T+5) \\ &= T^6(T-1)(T^4+T^3+T^2+T+1) \\ &= T^6(T^5-1) = T^{11}-T^6 \\ &= T^{11}G_1(T)+H_1(T), \end{aligned}$$

$G_1(T)=1, \quad H_1(T)=-T^6.$

Poglavlje 6

Višestruke blokade projektivne ravnine

Neka je Π konačna projektivna ravnina reda q.

DEFINICIJA 6.1 *Skup $\mathcal{B}$ točaka u Π naziva se **t-struka blokada** ravnine Π ako svaki pravac ravnine Π sadrži barem t točaka iz $\mathcal{B}$ i pritom neki pravac sadrži točno t točaka iz $\mathcal{B}$.*

Za $t > 1$ se ne zahtjeva da višestruka blokada ne smije sadržavati sve točke nekog pravca; ionako ovaj uvjet nema nikakvog utjecaja na granicu veličine t-struke blokade.
Posebno, 1-blokadu projektivne ravnine nazivamo samo blokadom, a za 2-blokadu i 3-blokadu koristimo nazive ***dvostruka blokada***, odnosno ***trostruka blokada***.

LEMA 6.2 *Za t-struku blokadu $\mathcal{B}$ ravnine Π vrijedi $card\ \mathcal{B} \geq t(q+1)$.*

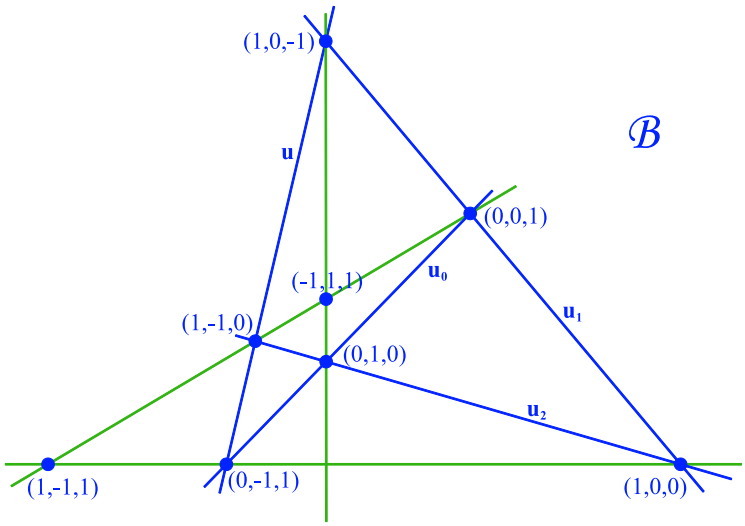
Dokaz Svakom točkom iz $\Pi \setminus \mathcal{B}$ prolazi $q+1$ pravac koji siječe blokadu u barem t točaka pa vrijedi $card\ \mathcal{B} \geq t(q+1)$. ∎

Očita ideja konstrukcije višestrukih blokada je unija više 1-blokada. Navest ćemo nekoliko primjera.

PRIMJER 6.3 *Višestruke blokade*

1. Stranice trovrha formiraju dvostruku blokadu projektivne ravnine od $3q$ točaka. Naime, na svakoj stranici trovrha nalazi se osim vrhova još $q-1$ točaka, što ukupno čini $3q$ točaka blokade. Svaki pravac ravnine koji ne prolazi vrhom siječe trovrh u 3 točke, dok ga pravci ravnine kroz vrh sijeku u 2 točke.

2. Neka $\mathcal{B}$ sadrži sve točke pravaca $\mathbf{u_0}$, $\mathbf{u_1}$, $\mathbf{u_2}$, $\mathbf{u}$ i točke $(-1,1,1)$, $(1,-1,1)$. Tada je $\mathcal{B}$ trostruka blokada od $4q-1$ točaka ako je q paran, odnosno $4q$ točaka ako je q neparan.



Slika 6.1

Neka je $\mathcal{S} = \{\mathbf{u_0}, \mathbf{u_1}, \mathbf{u_2}, \mathbf{u}\}$ i $\mathcal{T} = \{\mathbf{u_0} \cap \mathbf{u_1}, \mathbf{u_0} \cap \mathbf{u_2}, \mathbf{u_0} \cap \mathbf{u}, \mathbf{u_1} \cap \mathbf{u_2}, \mathbf{u_1} \cap \mathbf{u}, \mathbf{u_2} \cap \mathbf{u}\}$. Svaki pravac ravnine koji ne prolazi presječnim točkama iz $\mathcal{T}$ siječe $\mathcal{S}$ u 4 točke i eventualno prolazi kroz $(-1,1,1)$ ili $(1,-1,1)$. Pravci ravnine koji prolaze jednom točkom iz $\mathcal{T}$ sijeku $\mathcal{S}$ u još 2 točke i eventualno prolaze kroz $(-1,1,1)$ ili $(1,-1,1)$, što čini barem 3 točke u presjeku. Pravci kroz dvije točke iz $\mathcal{T}$ sijeku $\mathcal{B}$ u barem još jednoj točki, npr. pravac kroz $(0,-1,1)$ i $(1,0,0)$ siječe $\mathcal{B}$ još u točki $(1,-1,1)$, dok pravac kroz $(1,-1,0)$ i $(0,0,1)$ siječe $\mathcal{B}$ još u točkama $(1,-1,1)$ i $(-1,1,1)$. Dakle, $\mathcal{B}$ je trostruka blokada.
Nadalje, $card\ \mathcal{B} = 4(q-2) + card\ \mathcal{T} + 2 = 4q - 8 + 6 + 2 = 4q$. Ako je q paran, onda je $1 = -1$, pa je $(-1,1,1) = (1,-1,1)$, tj. $card\ \mathcal{B} = 4q - 1$.

3. Neka je q kvadrat i $t \leq q - \sqrt{q} + 1$. Tada je unija t disjunktnih podgeometrija $PG(2, \sqrt{q})$ (Baerovih podravnina) u $PG(2,q)$ t-struka blokada veličine $t(q + \sqrt{q} + 1)$. Obzirom da postoji particija ravnine $PG(2,q)$ na $q - \sqrt{q} + 1$ Baerovu podravninu, onda je ova konstrukcija moguća za svaki odgovarajući t. Ova t-struka blokada ima svojstvo da je svaki pravac ravnine siječe u t ili u $t + \sqrt{q}$ točaka.

Za veći t lako se konstruira manja blokada u projektivnoj ravnini kvadratnog reda. Npr. komplement Hermiteovog luka je $(q - \sqrt{q})$-struka blokada (Primjer 6.10) i ona je mnogo manja od unije $q - \sqrt{q}$ Baerovih podravnina. Naime, neka je blokada $\mathcal{B}_H$ komplement Hermiteovog luka i $\mathcal{B}_B$ unija Baerovih podravnina. Tada je $card\ \mathcal{B}_H \leq card\ \mathcal{B}_B$ jer vrijedi

$$q^2 + q - q\sqrt{q} \leq t(q + \sqrt{q} + 1) \leq (q - \sqrt{q} + 1)(q + \sqrt{q} + 1),$$

$$q^2 + q - q\sqrt{q} \leq q^2 + q + 1,$$

a ovo očito vrijedi.

4. *Konika u projektivnoj ravnini neparnog reda.*

Neka je q neparan. Konika u $PG(2,q)$ sadrži $q+1$ točaka. Vanjskih točaka konike (onih koje su incidentne s točno dvije različite tangente konike) ukupno ima $(q^2+q)/2$, dok unutrašnjih točaka konike (one točke kroz koje ne prolazi niti jedna tangenta) ukupno ima $(q^2-q)/2$.

Vanjske točke konike zajedno sa svim točkama konike osim jedne čine $\frac{q+1}{2}$-struku blokadu projektivne ravnine (koja je komplement $(\frac{q^2-q}{2}+1; \frac{q+1}{2})$-luka, Primjer 6.11.2), te ukupno ima $q(q+3)/2$ točaka.

Ova blokada sadržava jedan cijeli pravac. Kada se isključi $q+1$ točaka tog pravca preostaje $(q^2+q)/2-1$ točaka afine ravnine koje čine $\frac{q-1}{2}$-struku blokadu afine ravnine. Blokade afine ravnine razmatrat ćemo u Poglavlju 7.

6.1 Veličina *t*-struke blokade u projektivnoj ravnini

Pokažimo prvo osnovnu granicu za veličinu t-struke blokade.

TEOREM 6.4 *Za t-struku blokadu $\mathcal{B}$ ravnine Π koja ne sadrži sve točke nekog pravca vrijedi*

$$card\ \mathcal{B} \geq tq + \sqrt{tq} + 1.$$

Dokaz Neka je $\mathcal{B}$ t-struka blokada koja ne sadrži sve točke nekog pravca i neka je $card\ \mathcal{B} = k$. Pretpostavimo prvo da postoji pravac l ravnine Π koji siječe blokadu $\mathcal{B}$ u barem $\lceil \sqrt{tq}\ \rceil + 1$ točaka, a manje od $q+1$. Tada kroz točku $P \in l \setminus \mathcal{B}$ prolazi još q pravaca ravnine koji sijeku blokadu u barem po t točaka pa vrijedi $card\ \mathcal{B} \geq tq + \lceil \sqrt{tq}\ \rceil + 1 \geq tq + \sqrt{tq} + 1$.

Pretpostavimo sada da svaki pravac ravnine sadrži manje od $\lceil \sqrt{tq}\ \rceil + 1$ točaka blokade $\mathcal{B}$. Neka je τ_i broj i-sekanti od $\mathcal{B}$, $i \in \{t, t+1, \ldots, q\}$. Pravaca ukupno ima

$$\sum_{i=t}^{q} \tau_i = q^2 + q + 1.$$

Prebrojimo sve parove (P, l), gdje je P točka blokade $\mathcal{B}$ koja pripada pravcu l

$$\sum_{i=t}^{q} i\tau_i = card\ \mathcal{B} \cdot (q+1) = k(q+1).$$

Prebrojimo sve trojke (P, Q, l), gdje su P i Q dvije različite točke iz $\mathcal{B}$, a l njihova spojnica. Samih parova (P, Q) ima

$$\binom{card\ \mathcal{B}}{2} = \frac{k(k-1)}{2}$$

i oni jednoznačno određuju pravac l. Svaki pravac na i-sekanti sadrži $\binom{i}{2}$ parova (P, Q), dakle

$$\sum_{i=t}^{q} \binom{i}{2} \tau_i = \binom{card\ \mathcal{B}}{2}$$

$$\Rightarrow \quad \sum_{i=t}^{q} i(i-1)\tau_i = k(k-1).$$

Sada imamo jednadžbe

$$\sum_{i=t}^{q} \tau_i = q^2 + q + 1, \tag{6.1}$$

$$\sum_{i=t}^{q} i\tau_i = k(q+1), \tag{6.2}$$

$$\sum_{i=t}^{q} i(i-1)\tau_i = k(k-1). \tag{6.3}$$

Kako je $t \leq card\ (l \cap \mathcal{B}) \leq \lceil \sqrt{tq}\ \rceil$, onda za svaki pravac l vrijedi

$$\sum_{i=t}^{\lceil \sqrt{tq}\ \rceil} (i-t)(i-\sqrt{tq}-1)\tau_i < 0.$$

Obzirom je $\tau_i = 0$ za $i > \lceil \sqrt{tq}\ \rceil$, sumu možemo proširiti i do q, te vrijedi

$$\sum_{i=t}^{q} i(i-\sqrt{tq}-1)\tau_i - t\sum_{i=t}^{q}(i-\sqrt{tq}-1)\tau_i < 0,$$

$$\sum_{i=t}^{q} i(i-1)\tau_i - (\sqrt{tq}+t)\sum_{i=t}^{q} i\tau_i + t(\sqrt{tq}+1)\sum_{i=t}^{q}\tau_i < 0,$$

odnosno

$$k(k-1) - (\sqrt{tq}+t)(q+1)k + t(\sqrt{tq}+1)(q^2+q+1) < 0.$$

Sada imamo

$$k^2 - k - kq\sqrt{tq} - ktq - k\sqrt{tq} - kt + tq^2\sqrt{tq} + tq\sqrt{tq} + t\sqrt{tq} +$$
$$+tq^2 + tq + t \pm t^2q \pm q\sqrt{tq} < 0,$$

$$k^2 - k(tq+\sqrt{tq}+1) - k(t+q\sqrt{tq}) + t(tq+\sqrt{tq}+1) + q\sqrt{tq}(tq+\sqrt{tq}+1) +$$
$$+q\sqrt{tq}(t-1) - tq(t-1) < 0,$$

$$k(k-t-q\sqrt{tq}) + (tq+\sqrt{tq}+1)(-k+t+q\sqrt{tq}) + (t-1)q(\sqrt{tq}-t) < 0,$$

$$[k-(tq+\sqrt{tq}+1)][k-(t+q\sqrt{tq})] + (t-1)q(\sqrt{tq}-t) < 0. \tag{6.4}$$

Kako je $\sqrt{tq} - t \geq 0$, onda je $(t-1)q(\sqrt{tq}-t) \geq 0$. Pretpostavimo sada da je $k-(tq+\sqrt{tq}+1) < 0$. Tada je

$$\begin{aligned} k-(t+q\sqrt{tq}) &< tq+\sqrt{tq}+1-t-q\sqrt{tq} \\ &= t(q-1)+\sqrt{tq}(1-q)+1 \\ &= (q-1)(t-\sqrt{tq})+1 \ \leq\ 0. \end{aligned}$$

No tada je lijeva strana izraza (6.4) pozitivna, što je kontradikcija, pa za $1 \leq t \leq q$ slijedi $card\ \mathcal{B} = k \geq tq+\sqrt{tq}+1$. ■

Navedeni teorem ima uvjet da t-struka blokada ne sadrži sve točke nekog pravca. Ako promatramo t-struku blokadu $\mathcal{B}$ u Desarguesovoj projektivnoj ravnini $\Pi = PG(2,q)$ i ako ona sadrži pravac l, onda je $\mathcal{B} \setminus l$ $(t-1)$-struka blokada u $AG(2,q) = PG(2,q) \setminus l$. Blokade afine ravnine razmatrat ćemo u Poglavlju 7.

U slučaju kada je q prim broj i $\Pi = PG(2,q)$, ocjena veličine t-struke blokade može se znatno poboljšati.

TEOREM 6.5 *Neka je $\mathcal{B}$ t-struka blokada ravnine $PG(2,q)$, gdje je $q > 3$ prim broj.*

(i) Ako je $t < q/2$, onda je $card\ \mathcal{B} \geq (t+\frac{1}{2})(q+1)$.

(ii) Ako je $t > q/2$, onda je $card\ \mathcal{B} \geq (t+1)q$.

Dokaz Neka je $l = \mathbf{u_2}$ t-sekanta od $\mathcal{B}$. Pretpostavimo da je $\mathbf{U_0} \in \mathcal{B}$ i $card\ \mathcal{B} = tq + m + t$. Neka je $\mathcal{S} = \mathcal{B} \setminus l$, tako da je $card\ \mathcal{S} = tq + m$. Pretpostavimo također da je $t + m < q$, jer bi u suprotnom odmah bilo $card\ \mathcal{B} \geq (t+1)q$. Neka je

$$\mathcal{S} = \{(a_i, b_i) \mid i = 1, \ldots, tq+m\} \subset AG(2,q) = PG(2,q) \setminus l.$$

Neka $d_1, \ldots, d_{t-1}$ označavaju smjerove određene točkama iz $\mathcal{B} \cap (l \setminus \{\mathbf{U_0}\})$. Za svaku točku $P_j \in \mathcal{B} \cap l$ neka je $-d_j^{-1}$ nagib pravaca koji sijeku l u P_j. Svaki pravac $x + uy + s = 0$ ima t rješenja u $\mathcal{S}$ za $u \notin \{d_j \mid j = 1, \ldots, t-1\}$. Slijedi da polinom

$$F(S,U) = \prod_{j=1}^{t-1}(U - d_j) \prod_{i=1}^{tq+m}(S + a_i + b_i U)$$

ima nule stupnja t za svaki S i U. Po Teoremu 1.26 ovo znači da polinom $F(S,U)$ leži u idealu generiranim s $(S^q - S)^r (U^q - U)^{t-r}$ za $r = 0, \ldots, t$. Dakle, postoje polinomi $G_r(S,U)$ takvi da je

$$F(S,U) = \sum_{r=0}^{t}(S^q - S)^r (U^q - U)^{t-r} G_r(S,U).$$

Neka su $F^*(S,U)$ i $G_r^*(S,U)$ homogeni dijelovi u $F(S,U)$ i $G_r(S,U)$ totalnog stupnja $tq + m + t - 1$ i $m + t - 1$ respektivno. Tada je

$$F^*(S,U) = \sum_{r=0}^{t} S^{rq} U^{(t-r)q} G_r^*(S,U) = U^{t-1} \prod_{i=1}^{tq+m}(S + b_i U).$$

Kako je jednadžba homogena, varijabla U se može fiksirati. Definirajmo $f(S) = F^*(S,1)$, $g_r(S) = G_r^*(S,1)$. Tada je

$$f(S) = \sum_{r=0}^{t} S^{rq} g_r(S) = \prod_{i=1}^{tq+m}(S + b_i). \tag{6.5}$$

Ovo znači da je stupanj od g_t jednak m, a stupnjevi preostalih g_r su najviše $m+t-1$.

Skalar b_i poprima vrijednost u $GF(q)$ barem $t-1$ put, obzirom da svaki horizontalni pravac $y = b_i$ sadrži barem $t-1$ točaka iz $\mathcal{S}$. Dakle, $(S^q - S)^{t-1}$ dijeli $f(S)$. Ovaj uvjet djeljivosti povlači da S^{t-1} dijeli g_0 jer je $(S^q - S)^{t-1} = S^{t-1}(S^{q-1} - 1)^{t-1}$ i

$$f(S) = g_0(S) + S^q g_1(S) + S^{2q} g_2(S) + \cdots + S^{tq} g_t(S).$$

Definirajmo $g^*(S)$

$$g_0(S) = (-1)^{t-1} S^{t-1} g^*(S).$$

Kako $(S^q - S)^{t-1}$ dijeli $f(S)$, definirajmo $\hat{f}(S)$

$$f(S) = (S^q - S)^{t-1}[S^q g_t(S) + \hat{f}(S) + g^*(S)],$$

odnosno

$$f(S) = S^{t-1}(S^{q-1} - 1)^{t-1}[S^q g_t(S) + \hat{f}(S) + g^*(S)].$$

Stupanj od $\hat{f}$ je najviše $m+t-1 < q-1$. Kako S^q dijeli $f(S) - g_0(S)$, onda S^q dijeli $S^{t-1}\hat{f}(S)$, tj. S^{q-t+1} dijeli $\hat{f}(S)$. Obzirom da $f(S)$ nema članova sa eksponentom jednakim $-1 (\mathrm{mod}\ q)$, slijedi da takvih nema ni funkcija $(S^q - S)^{t-1}\hat{f}(S)$. Zapišimo

$$(S^q - S)^{t-1}\hat{f}(S) = \sum_{r=0}^{t-1} \binom{t-1}{r} (-1)^r S^{(t-1-r)q+r} \hat{f}(S).$$

Binomni koeficijenti $\binom{t-1}{r}$ različiti su od nule za $r = 0, \ldots, t-1$, pa $\hat{f}(S)$ ne sadrži članove reda većeg od $q - t$. Naime, ako bi red nekog člana bio $q - t + 1$, onda uz $r = t-1$ vrijedi $S^{t-1}S^{q-t+1} = S^q$, a znamo da je stupanj od $\hat{f}$ najviše $q-1$. Nadalje, kako S^{q-t+1} dijeli $\hat{f}(S)$ onda je $\hat{f} = 0$ i

$$f(S) = (S^q - S)^{t-1}[S^q g_t(S) + g^*(S)].$$

Podijelimo $S^q g_t(S) + g^*(S)$ s najvećim zajedničkim djeliteljem od $g_t(S)$ i $g^*(S)$, i tako po mogućnosti smanjimo m. Sada primijenimo Teorem 4.4.

Ako je $m = 0$ onda primijenimo tvrdnju (i) Teorema 4.4. Tada je

$$f(S) = (S^q - S)^{t-1}(c_1 S^q + c_2),$$

pa $S^q g_t(S) + g^*(S)$ sadrži faktor oblika $S^q - c = (S - c)^q$. Uz dodatak faktoru $(S - c)^{t-1}$ prisutnom u $(S^q - S)^{t-1}$, ovo daje previše faktora $S - c$ u $f(S)$.

Ako je $m = 1$ onda primijenimo tvrdnju (iv) Teorema 4.4 te vrijedi

$$f(S) = (S^q - S)^{t-1}(cS^q - cS).$$

No tada je g_t konstanta, a stupanj od g_t nije manji od stupnja g^* pa se ovaj slučaj ne može pojaviti.

Dakle $m > 1$, a kako je q prim broj, onda po posljednjoj tvrdnji Teorema 4.4 $m \geq \dfrac{q+1}{2}$ i vrijedi

$$card\ \mathcal{B} = tq + m + t \geq tq + \frac{1}{2}(q+1) + t = (t + \frac{1}{2})(q+1).$$

Dokažimo sada tvrdnje teorema.

(i) Neka je $t < q/2$. Tada je

$$card\ \mathcal{B} \geq (t + \frac{1}{2})(q + 1).$$

(ii) Neka je $t > q/2$. Tada je

$$card\ \mathcal{B} \geq (t + \frac{1}{2})(q + 1) = tq + \frac{q}{2} + t + \frac{1}{2} > tq + q + \frac{1}{2} \geq (t + 1)q.$$

■

PRIMJER 6.6 *Konika u $PG(2, q)$, gdje je q neparan.*

1. Vanjskih točaka konike ima $(q^2 + q)/2$ i one čine t-struku blokadu, gdje je $t = (q - 1)/2$. Ovaj primjer postiže donju granicu tvrdnje (i) u prethodnom teoremu.

2. Vanjske točke konike zajedno sa svim točkama konike osim jedne čine t-struku blokadu od $q(q+3)/2$ točaka, gdje je $t = (q+1)/2$. Ovaj primjer postiže donju granicu tvrdnje (ii) prethodnog teorema.

6.2 t-struke blokade i potpuni $(k;n)$-lukovi

Blokade su povezane s lukovima, odnosno $(k;n)$-luk projektivne ravnine je komplement t-struke blokade kada je $n+t=q+1$. Općenito, $(k;n)$-lukove promatramo kad je n malen, a t-struke blokade kad je t malen.

DEFINICIJA 6.7 *Skup K koji se sastoji od k točaka ravnine Π tako da je najviše n njegovih točaka kolinearno, naziva se* ***$(k;n)$-luk*** *ili* ***luk stupnja n*** *ravnine Π.*

Svaki pravac ravnine siječe $(k;n)$-luk u i točaka, $0 \leq i \leq n$, tj. pravci su i-sekante $(k;n)$-luka, a za njihov broj koristimo i ovdje oznaku τ_i.

DEFINICIJA 6.8 *$(k;n)$-luk koji se dodavanjem još jedne točke ravnine ne može proširiti do $(k+1;n)$-luka naziva se* ***potpuni $(k;n)$-luk*** *ravnine Π.*

Očito je $(k;n)$-luk potpun ako svaka točka ravnine leži na nekoj njegovoj n-sekanti.

LEMA 6.9 *Za $(k;n)$-luk ravnine Π vrijedi $k \leq qn-q+n$.*

Dokaz Kroz svaku točku $(k;n)$-luka prolazi $q+1$ pravac, a na svakom od tih pravaca može ležati najviše još $n-1$ točaka $(k;n)$-luka pa je $k \leq (n-1)(q+1)+1 = qn-q+n$. ∎

PRIMJER 6.10 *Hermiteov luk.*

Hermiteov luk je skup od $q\sqrt{q}+1$ točaka ravnine Π tako da svaki pravac ravnine sadrži ili jednu ili $\sqrt{q}+1$ točaka luka. On je dakle $(q\sqrt{q}+1;\sqrt{q}+1)$-luk.
Komplement Hermiteovog luka je t-struka blokada gdje je $t=q+1-n=q-\sqrt{q}$ i ona sadrži $q^2+q+1-q\sqrt{q}-1=q^2+q-q\sqrt{q}$ točaka ravnine Π.

PRIMJER 6.11 *Konika u $PG(2,q)$, gdje je q neparan.*

1. Unutrašnje točke zajedno sa svim točkama konike, kojih ima $q+1$, čine potpun $((n-1)q+1;n)$-luk, gdje je $n=(q+3)/2$.
   Njegov komplement je t-struka blokada iz Primjera 6.6.1.

2. Unutrašnjih točaka konike ima $(q^2-q)/2$. One čine zajedno s jednom točkom konike potpun $((n-1)q+1;n)$-luk, gdje je $n=(q+1)/2$.
   Njegov komplement je t-struka blokada iz Primjera 6.6.2.

DEFINICIJA 6.12 *$(qn-q+n;n)$-luk ravnine Π naziva se* ***maksimalan luk*** *ravnine Π.*

LEMA 6.13 *$(k;n)$-luk ravnine Π je maksimalan ako i samo ako je svaki pravac ravnine njegov vanjski pravac ili n-sekanta.*

Dokaz Neka je $k = qn - q + n$. Pretpostavimo da postoji pravac ravnine koji siječe $(k;n)$-luk u $t < n$ točaka i neka je P jedna od njih. Kroz P prolazi još q pravaca sa najviše još $n-1$ točaka $(k;n)$-luka, pa vrijedi $k \leq q(n-1) + t < qn - q + n$ što je kontradikcija.
Obrat. Neka su svi pravci ravnine vanjski pravci $(k;n)$-luka ili njegove n-sekante. Neka je Q točka izvan $(k;n)$-luka. Kroz nju prolazi k/n pravca koji su n-sekante $(k;n)$-luka. Ovaj broj mora biti cijeli, dakle n dijeli k. Kako kroz Q prolazi $q+1$ pravac, onda vanjskih pravaca kroz Q ima $q+1-k/n$. Ovo znači da je $\tau_n = (q+1)k/n$, a $\tau_0 = (q+1-n)(q+1-k/n)$. Iz $\tau_n + \tau_0 = q^2 + q + 1$ slijedi

$$(q+1)\frac{k}{n} + (q+1-n)(q+1-\frac{k}{n}) = q^2 + q + 1,$$

$$(q+1)\frac{k}{n} + (q+1)^2 - n(q+1) - (q+1)\frac{k}{n} + k = q^2 + q + 1,$$

$$q^2 + 2q + 1 - nq - n + k = q^2 + q + 1.$$

Dakle, $k = qn - q + n$, tj. $(k;n)$-luk je maksimalan. ∎

Rezultati vezani za t-struke blokade relevantni su za $(k;n)$-lukove. Npr. Teoremu 6.5 za blokade odgovara sljedeći teorem za lukove.

TEOREM 6.14 *Neka je $\mathcal{K}$ $(k;n)$-luk ravnine $PG(2,q)$, gdje je $q > 3$ prim broj.*

(i) Ako je $n > q/2 + 1$, onda je $card\ \mathcal{K} \leq (n-1)q + n - (q+1)/2$.

(ii) Ako je $n < q/2 + 1$, onda je $card\ \mathcal{K} \leq (n-1)q + 1$.

Dokaz Komplement od $\mathcal{K}$ je $(q+1-n)$-struka blokada ravnine Π, gdje je $q > 3$ prim broj. Primijenimo Teorem 6.5.

(i) Neka je $t < q/2$ i $card\ \mathcal{B} \geq (t + \frac{1}{2})(q+1)$. Tada je $n = q + 1 - t > q/2 + 1$. Nadalje,

$$\begin{aligned} card\ \mathcal{K} &= q^2 + q + 1 - card\ \mathcal{B} \\ &\leq q^2 + q + 1 - t(q+1) - (q+1)/2 \\ &= q^2 + q + 1 - (q+1-n)(q+1) - (q+1)/2 \\ &= qn - q + n - (q+1)/2. \end{aligned}$$

(ii) Neka je $t > q/2$ i $card\ \mathcal{B} \geq (t+1)q$. Tada je $n = q + 1 - t < q/2 + 1$. Nadalje,

$$\begin{aligned} card\ \mathcal{K} &= q^2 + q + 1 - card\ \mathcal{B} \\ &\leq q^2 + q + 1 - (t+1)q \\ &= q^2 + q + 1 - (q+1-n+1)q \\ &= qn - q + 1. \end{aligned}$$

∎

6.3 Dvostruke blokade

Dvostruka blokada $\mathcal{B}$ je skup točaka u Π takvih da svaki pravac ravnine Π sadrži barem dvije točke iz $\mathcal{B}$. Pritom neki pravac sadrži točno dvije točke iz $\mathcal{B}$.

Lema koja slijedi kao i razmatranje Baerovog potpravca potrebni su nam za glavni rezultat o dvostrukim blokadama u projektivnim ravninama $PG(2,q)$ kvadratnog reda.

LEMA 6.15 *Neka je $f(X) \in GF(q)[X]$ polinom oblika $X^{\sqrt{q}}(X+b)+(cX+d)$, gdje je $d \neq bc$. Tada je f potpuno reducibilan ako i samo ako je $c = b^{\sqrt{q}}$ i $d \in GF(\sqrt{q})$.*

Dokaz Pretpostavimo prvo da je $f(X) = X^{\sqrt{q}}(X+b)+cX+d$, $d \neq bc$, potpuno reducibilan polinom. Pokažimo da f ne sadrži višestruke faktore.
Kako je $f'(X) = X^{\sqrt{q}} + c$, onda je $f(X) - (X+b)f'(x) = d - bc \neq 0$. Slijedi da f dijeli

$$f^{\sqrt{q}} = X(X^{\sqrt{q}} + b^{\sqrt{q}}) + c^{\sqrt{q}}X^{\sqrt{q}} + d^{\sqrt{q}} (mod\ X^q - X),$$

$$\text{tj.} \quad f^{\sqrt{q}} = X^{\sqrt{q}}(X + c^{\sqrt{q}}) + b^{\sqrt{q}}X + d^{\sqrt{q}} (mod\ X^q - X).$$

Kako su stupnjevi od f i$f^{\sqrt{q}} (mod\ X^q - X)$ jednaki , slijedi $c = b^{\sqrt{q}}$ i $d \in GF(\sqrt{q})$.
Obrat. Pretpostavimo da je $c = b^{\sqrt{q}}$ i $d \in GF(\sqrt{q})$, te

$$f = X^{\sqrt{q}}(X+b) + b^{\sqrt{q}}X + d = M(X+b) - M(b) + d,$$

gdje je M funkcija norme s $GF(q)$ na $GF(\sqrt{q})$, tj. $M(x) = Norm_{\sqrt{q}}(x) = x^{1+\sqrt{q}}$. Kako f ima stupanj $\sqrt{q}+1$, a x je nul-točka od f kad je $M(x+b) = M(b) - d \neq 0$, slijedi da je f potpuno reducibilan polinom. ■

DEFINICIJA 6.16 *Neka je Π_0 Baerova podravnina od $PG(2,q)$, gdje je q kvadrat. Ako za neki pravac l vrijedi card $(l \cap \Pi_0) = \sqrt{q}+1$, onda $l \cap \Pi_0$ nazivamo* ***Baerovim potpravcem*** *od l.*

Polje $GF(q) \cup \{\infty\}$ može se identificirati s projektivnim pravcem $PG(1,q)$, a on sadržava Baerov potpravac $GF(\sqrt{q}) \cup \{\infty\}$. Nul-točke funkcije f oblika kao u Lemi 6.15 formiraju Baerov potpravac koji ne prolazi točkom ∞, i obrnuto, svakom Baerovom potpravcu l koji ne sadrži ∞ odgovaraju $b \in GF(q)$ i $a \in GF(\sqrt{q})^*$, takvi da vrijedi

$$l = \{X \in GF(q) \mid M(X+b) = a\}.$$

Koristit ćemo sljedeća svojstva Baerovog potpravca.

1. Presjek duala Baerovog potpravca s pravcem je Baerov potpravac.

2. Dva Baerova potpravca sijeku se u najviše dvije točke.

3. Neka su dane dvije točke P i Q, te dva duala Baerovih potpravca kroz ove dvije točke. Ako pravac koji spaja P i Q leži u oba duala Baerovih potpravaca, onda presjek pravaca dualnih Baerovih potpravaca sadrži Baerovu podravninu.

TEOREM 6.17 *Neka je $\mathcal{B}$ dvostruka blokada ravnine $PG(2,q)$.*

(i) Ako je $q > 16$ i q kvadrat, onda je $card\ \mathcal{B} \geq 2q + 2\sqrt{q} + 2$.

(ii) Ako je $3 < q = p^{2\epsilon+1}$, onda je $card\ \mathcal{B} \geq 2q + p^{\epsilon}\left\lceil \frac{p^{\epsilon+1}+1}{p^{\epsilon}+1} \right\rceil + 2$.

Dokaz U dokazu Teorema 6.5 stavimo da je $t = 2$. Tada je

$$card\ \mathcal{B} = 2q + m + 2$$

i

$$f(S) = (S^q - S)(S^q g_2(S) + g^*(S)), \quad (g^*)^\circ < g_2^\circ.$$

Pretpostavimo da je uklonjen svaki zajednički faktor iz g_2 i g^*. Polinom $S^q g_2(S) + g^*(S)$ zadovoljava uvjete Teorema 4.4.

(1) Slučaj (i) Teorema 4.4 : $e = h$, $m = 0$ i

$$f(S) = (S^q - S)(c_1 S^q + c_2).$$

Slijedi da f sadrži faktor oblika $S^q - c = (S - c)^q$, uz faktor $S - c$ koji je već prisutan u $S^q - S$. Ovo daje previše faktora $S - c$ u f.

(2) Slučaj (ii) Teorema 4.4 : $\frac{h}{2} \leq e < h$ i $m \geq p^e$.

Ako q nije kvadrat, tj. $q = p^{2\epsilon+1}$, onda je $e \geq \frac{h}{2} = \epsilon + \frac{1}{2}$, a zbog cjelobrojnosti je $e \geq \epsilon + 1$. Tada je $m \geq p^e \geq p^{\epsilon+1}$, što je bolje od tražene granice $m \geq p^{\epsilon}\left\lceil \frac{p^{\epsilon+1}+1}{p^{\epsilon}+1} \right\rceil$.

Neka je q kvadrat, tj. $q = p^{2\epsilon}$. Tada je $e \geq \frac{h}{2} = \epsilon$.
Ako je $e > \epsilon$, onda je $e \geq \epsilon + 1$ i $m \geq p^e \geq p^{\epsilon+1} = p\sqrt{q} \geq 2\sqrt{q}$ te vrijedi

$$card\ \mathcal{B} \geq 2q + 2\sqrt{q} + 2.$$

Neka je sada $e = \epsilon$. Tada je ili $m \geq 2p^{\epsilon} = 2\sqrt{q}$ pa slijedi tražena granica, ili je $m = p^{\epsilon}$. Pokažimo da slučaj $m = p^{\epsilon} = \sqrt{q}$ nije moguć.

Neka je $e = \epsilon$, $m = p^e$ i $card\ \mathcal{B} = 2q + \sqrt{q} + 2$. Nakon izvlačenja p^e-tog korijena iz $S^q g_2 + g^*$ dobije se potpuno reducibilna funkcija oblika $S^{\sqrt{q}}(S + b) + (cS + d)$. Iz Leme 6.15 slijedi da je ova funkcija oblika $M(S + b) - M(b) + d$, te su njene nul-točke upravo točke podgeometrije $PG(1, \sqrt{q})$ (tj. Baerovog potpravca) od $GF(q) \cup \{\infty\}$ koja ne sadrži ∞. Ovo znači da među pravcima kroz $\mathbf{U_0}$ koji sadrže više od dvije točke iz $\mathcal{B}$, postoji njih $\sqrt{q} + 1$ koji sadrže barem $\sqrt{q} + 2$ točaka, formirajući dual Baerovog potpravca. Točka $\mathbf{U_0}$ nije ništa posebno, tj. ovaj se slučaj javlja u svakoj točki.

Neka se pravci koji sijeku $\mathcal{B}$ u barem $\sqrt{q} + 2$ točaka nazivaju *dugi pravci*. Dva duga pravca moraju se sjeći u točki iz $\mathcal{B}$, jer u suprotnom ako prebrojimo točke u $\mathcal{B}$ na pravcima kroz presječnu točku dobijemo da je $card\ \mathcal{B} \geq 2(q-1) + 2(\sqrt{q} + 2) = 2q + 2\sqrt{q} + 2$.

Nadalje, presjek $\mathcal{B}$ s dugim pravcem d sadrži Baerov potpravac. Naime, neka je P proizvoljna točka iz $\mathcal{B}$ koja nije na pravcu d. Dugi pravci kroz P sadrže dual Baerovog potpravca, i svi oni sijeku d u točki iz $\mathcal{B}$. Štoviše, mnogo jače svojstvo vrijedi: ako je Q proizvoljna točka iz $\mathcal{B}$ koja pripada pravcu d, onda d sadrži Baerov potpravac u $\mathcal{B}$ koji ne sadrži Q. Da bi ovo vidjeli dovoljno je uzeti bilo koju točku P takvu da je PQ bisekanta.

Sada, dva Baerova potpravca se sijeku u najviše dvije točke. Dakle, za $q \geq 9$, slijedi da svi dugi pravci imaju barem $2\sqrt{q}$ točaka, što znači

$$card\ \mathcal{B} \geq 1 + (\sqrt{q}+1)(2\sqrt{q}-1) + (q-\sqrt{q}) = 3q$$

što je svakako veće od $2q + 2\sqrt{q} + 2$.

(3) Slučaj (iii) Teorema 4.4 : $0 < e < \frac{h}{2}$ i

$$m \geq p^e \left\lceil \frac{p^{h-e}+1}{p^e+1} \right\rceil.$$

Ako q nije kvadrat, tj. $q = p^{2\epsilon+1}$, tada je $e < \frac{h}{2} = \epsilon + \frac{1}{2} \leq \epsilon$ i vrijedi

$$\begin{aligned} m &\geq p^e \left\lceil \frac{p^{h-e}+1}{p^e+1} \right\rceil = \left\lceil \frac{p^h+p^e}{p^e+1} \right\rceil = \left\lceil \frac{p^h-1}{p^e+1} + 1 \right\rceil \\ &\geq \left\lceil \frac{p^h-1}{p^\epsilon+1} + 1 \right\rceil = p^\epsilon \left\lceil \frac{p^{\epsilon+1}+1}{p^\epsilon+1} \right\rceil. \end{aligned}$$

Tražena ocjena je postignuta, odnosno za $3 < q = p^{2\epsilon+1}$ je

$$card\ \mathcal{B} \geq 2q + p^\epsilon \left\lceil \frac{p^{\epsilon+1}+1}{p^\epsilon+1} \right\rceil + 2.$$

Ako je q kvadrat, tj. $q = p^{2\epsilon}$, tada je $e < \frac{h}{2} = \epsilon \leq \epsilon - 1$ i vrijedi

$$m \geq p^e \left\lceil \frac{p^{h-e}+1}{p^e+1} \right\rceil \geq \left\lceil \frac{p^h-1}{p^{\epsilon-1}+1} + 1 \right\rceil = p^{\epsilon-1} \left\lceil \frac{p^{\epsilon+1}+1}{p^{\epsilon-1}+1} \right\rceil.$$

Ako je $q \neq 4, 9, 16$, onda je $\dfrac{p^{\epsilon+1}+1}{p^{\epsilon-1}+1} \geq 2p - 1$, tj. $m \geq 2p^\epsilon = 2\sqrt{q}$. Dakle, za $q > 16$ i q kvadrat vrijedi

$$card\ \mathcal{B} \geq 2q + 2\sqrt{q} + 2.$$

(4) Slučaj (iv) Teorema 4.4 : $e = 0$, $m = 1$ i

$$f(S) = (S^q - S)(cS^q - cS).$$

Ovdje je stupanj od g_2 manji od stupnja od g^*, pa se ovaj slučaj ne može pojaviti.

■

NAPOMENA 6.18

U tvrdnji (i) Teorema 6.17 imamo uvjet $q > 16$. Razlog tomu je što za $q = 4, 9, 16$ donja granica na m u tvrdnji (iii) Teorema 4.4 nije dovoljno velika da bi se dobilo $m \geq 2\sqrt{q}$. Naime, neka je $\mathcal{B}$ dvostruka blokada od $2q + m + 2$ točaka, gdje je $m \geq p^e\lceil(p^{h-e}+1)/(p^e+1)\rceil$, $e = \epsilon$ ako je $h = 2\epsilon+1$, odnosno $e = \epsilon-1$ ako je $h = 2\epsilon$.

Ako je $q = 4 = 2^2$, onda je $e = 0$ i $m = 3$. Iz dokaza Teorema 6.17 slijedi da je $card\ \mathcal{B} \geq 13$, dok bi iz tvrdnje (i) Teorema 6.17 slijedilo $card\ \mathcal{B} \geq 14$. Sljedeći primjer daje dvostruku blokadu ravnine $PG(2, 4)$ od 12 točaka, i ona je najmanja moguća.

Ako je $q = 9 = 3^2$, onda je $e = 0$ i $m = 5$. Iz dokaza Teorema 6.17 slijedi da je $card\ \mathcal{B} \geq 25$, dok bi iz tvrdnje (i) Teorema 6.17 slijedilo $card\ \mathcal{B} \geq 26$.

Ako je $q = 16 = 2^4$, onda je $e = 1$ i $m = 6$. Iz dokaza Teorema 6.17 slijedi da je $card\ \mathcal{B} \geq 40$, dok bi iz tvrdnje (i) Teorema 6.17 slijedilo $card\ \mathcal{B} \geq 42$.

PRIMJER 6.19 *Lakunaran polinom dvostruke blokade u* $PG(2, 4)$.

Neka je $\mathcal{H}$ Hermiteov luk ravnine $PG(2, 4)$. $\mathcal{H}$ je skup od $q\sqrt{q}+1 = 9$ točaka ravnine $PG(2, 4)$ tako da svaki pravac ravnine sadrži ili jednu ili $\sqrt{q} + 1 = 3$ točke iz $\mathcal{H}$, tj. Hermiteov luk je $(9; 3)$-luk.

Neka je $l = \mathbf{u_2}$ i

$$\mathcal{H} = \{(X_0, X_1, X_2) \in PG(2, 4) \mid X_0^3 + X_1^3 + X_2^3 = 0\}.$$

Kako je $GF(4) = \{0, 1, \omega, \omega^2 \mid \omega^2 + \omega + 1 = \omega^3 + 1 = 0\}$, tada je

$$\mathcal{H} = \{(0,1,1), (1,0,1), (1,1,0), (0,1,\omega), (0,\omega,1), (1,0,\omega), (1,\omega,0), (\omega,0,1), (\omega,1,0)\}.$$

Neka je $\mathcal{B}$ komplement od $\mathcal{H}$. Tada je $\mathcal{B}$ dvostruka blokada $(n + t = q + 1)$ od 12 točaka u $PG(2, 4)$.

$$\mathcal{B} = \{(1,0,0), (0,1,0), (0,0,1), (1,1,1), (1,1,\omega), (1,\omega,1), (\omega,1,1),$$

$$(1,1,\omega^2), (1,\omega^2,1), (\omega^2,1,1), (1,\omega,\omega^2), (1,\omega^2,\omega)\}.$$

Afine točke ove blokade su:

$$\mathcal{S} = \{(0,0), (1,1), (\omega^2,\omega^2), (1,\omega), (\omega,1), (\omega,\omega), (1,\omega^2), (\omega^2,1), (\omega,\omega^2), (\omega^2,\omega)\}.$$

Oznake polinoma f, g i g^* odgovaraju terminologiji Teorema 6.17 te vrijedi

$$\begin{aligned}
f(S) &= \prod(S+b_i) \\
&= S(S+1)^3(S+\omega)^3(S+\omega^2)^3 \;=\; S\big[(S+1)(S+\omega)(S+\omega^2)\big]^3 \\
&= S\big[(S+1)(S^2+S\omega+S\omega^2+\omega^3)\big]^3 \;=\; S\big[(S+1)(S^2+S\omega+S+S\omega+1)\big]^3 \\
&= S\big[(S+1)(S^2+S+1]^3 \;= S(S^3+1)^3 \\
&= S^{10}+S^7+S^4+S \;=\; (S^4+S)(S^6+1) \\
&= (S^4+S)(S^4g(S)+g^*(S)),
\end{aligned}$$

Lakunaran polinom koji odgovara ovoj dvostrukoj blokadi je oblika $S^4g(S)+g^*(S)$, gdje je $g(S)=S^2$ i $g^*(S)=1$.

Poglavlje 7

Blokade afine ravnine

Kod blokada projektivnih ravnina razlikujemo trivijalne (one blokade koje sadrže sve točke nekog pravca) od netrivijalnih blokada. U afinoj ravnini ovakvih razlika nema, tj. blokadu $\mathcal{B}$ definiramo kao skup točaka za koji vrijedi da svaki pravac afine ravnine sadrži barem jednu točku iz $\mathcal{B}$.

Za ocjenu veličine višestruke blokade afine ravnine vrijedi sljedeći teorem.

TEOREM 7.1 *Za t-struku blokadu $\mathcal{B}$ ravnine $AG(2,q)$ vrijedi*

$$card\ \mathcal{B} \geq (t+1)(q-1)+1.$$

Dokaz Neka je $\mathcal{B}$ t-struka blokada u $AG(2,q)$ koja sadrži ishodište $(0,0)$, te neka je $card\ \mathcal{B} = k$. Definirajmo

$$F(U,V) = \prod_{(a_i,b_i)\in\mathcal{B}\setminus\{(0,0)\}} (a_iU + b_iV + 1),$$

tako da je $F^\circ = k-1$. Kako svaki pravac koji ne prolazi ishodištem sadrži t točaka iz $\mathcal{B}$, onda polinom F ima nul-točku kratnosti t u svim točkama iz $AG(2,q)$, osim u ishodištu gdje je različit od nule. Pokazat ćemo indukcijom da F ima stupanj barem $(t+1)(q-1)$.

Neka je $J_t(U,V)$ ideal generiran s $(U^q-U)^{t-i}(V^q-V)^i$ za $i=0,\ldots,t$. Neka je $\alpha_1 \in GF(q)\setminus\{0\}$ i zapišimo

$$F(U,V) = (U-\alpha_1)A_1 + B_1,$$

gdje je $B_1(V) = F(\alpha_1, V)$. Stupanj od B_1 je najviše F° pa je $1 + A_1^\circ \leq F^\circ$. Kako je $\alpha_1 \neq 0$, onda je $B_1(v)$ nula t puta za svaki $v \in GF(q)$, tj. $\mathrm{mult}_v B_1 \geq t$ za svaki v, te po Teoremu 1.25 B_1 pripada idealu $J_t(V)$, a onda pripada i idealu $J_t(U,V)$. Polinom A_1 jednak je nuli t puta u svim točkama osim u ishodištu.

Neka je $\alpha_2 \in GF(q)\setminus\{0\}$ i zapišimo

$$F(U,V) = (U-\alpha_1)(U-\alpha_2)A_2 + B_2,$$

gdje je $B_2(V) = B_1(V) + (U-\alpha_1)A_1(\alpha_2, V)$. Stupanj od B_2 je najviše F° pa je $2 + A_2^\circ \leq F^\circ$. Nadalje, B_2 je nula t puta u svim točkama kao i $A_1(\alpha_2, V)$, pa po Teoremu 1.25 slijedi da B_2 pripada J_t.

Nastavljajući ovako za svaki $\alpha_j \in GF(q) \setminus \{0\}$, slijedi da postoje polinomi A i B takvi da je

$$F(U,V) = (U^{q-1} - 1)A + B,$$

gdje je B iz ideala J_t i ima stupanj najviše F°. Kako je $F \neq 0$ u ishodištu , onda je i $A \neq 0$ u ishodištu. Po Lemi 1.23 i Lemi 1.24 slijedi da polinom B ima nul-točku kratnosti t u svakoj točki, a polinom A ima nul-točku kratnosti $t-1$ u svim točkama iz $AG(2,q)$ osim u ishodištu. Po indukciji, stupanj od A je barem $t(q-1)$, pa je stupanj od F barem $(t+1)(q-1)$.

Neka je $t = 1$. Kako F nula u svim točkama osim u ishodištu, slijedi da $(V^{q-1}-1)$ dijeli A, pa F ima stupanj barem $2(q-1)$. ■

KOROLAR 7.2 *Ako je $\mathcal{B}$ blokada ravnine $AG(2,q)$, onda je card $\mathcal{B} \geq 2q-1$.*

Ova ocjena je znatno veća od one za blokadu projektivne ravnine, no najbolja je moguća za Desarguesove afine ravnine.

PRIMJER 7.3 *Blokada od $2q-1$ točaka u $AG(2,q)$.*

Jednostavan način kako konstruirati blokadu afine ravnine od $2q-1$ točaka je uzeti jedan pravac i nadodati po jednu točku sa svakog od $q-1$ paralelnog pravca.

Neka je $\mathcal{K}$ $(k;n)$-luk, tj. skup od k točaka tako da je najviše n njegovih točaka kolinearno. U projektivnoj ravnini komplement luka $\mathcal{K}$ je $(q+1-n)$-struka blokada od $q^2+q+1-k$ točaka, dok je u afinoj ravnini komplement luka $(q-n)$-struka blokada od q^2-k točaka. Navest ćemo primjer maksimalnog luka afine ravnine.

PRIMJER 7.4 *Dennistonov luk.*

Neka je $q = 2^h$ i $e \leq h$. Dennistonov luk je skup od $2^e q - q + 2^e$ točaka ravnine $AG(2,q)$ tako da je najviše 2^e njegovih točaka kolinearno, i ovakav luk postoji za svaki $e \leq h$ ([19]). On je dakle $(2^e q - q + 2^e; 2^e)$-luk i to maksimalan pa je svaki pravac ravnine njegov vanjski pravac ili 2^e-sekanta.
Komplement Dennistonovog luka je t-struka blokada afine ravnine gdje je $t = q - 2^e$ i ona sadrži $q^2 - 2^e q + q - 2^e$ točaka ravnine $AG(2,q)$.

U prethodnom poglavlju smo vidjeli da ako t-struka blokada $\mathcal{B}$ u $PG(2,q)$ sadrži sve točke nekog pravca l, onda je $\mathcal{B}\setminus l$ $(t-1)$-struka blokada u $AG(2,q) = PG(2,q)\setminus l$. Ako $\mathcal{B}$ sadrži k točaka projektivne ravnine, onda $\mathcal{B} \setminus l$ sadrži $k-q-1$ točaka afine ravnine. Vrijedi sljedeći teorem.

TEOREM 7.5 *Za t-struku blokadu $\mathcal{B}$ ravnine $PG(2,q)$ koja sadrži sve točke nekog pravca vrijedi card $\mathcal{B} \geq tq + q - t + 2$.*

Dokaz Neka je $\mathcal{B}$ t-struka blokada u $PG(2,q)$ koja sadrži sve točke pravca l i neka je $card\ \mathcal{B} = k$, $\mathcal{S} = \mathcal{B} \setminus l$.
$\mathcal{S}$ je $(t-1)$-struka blokada u $AG(2,q)$ i $card\ \mathcal{S} = k-q-1$, a po Teoremu 7.1 vrijedi

$$card\ \mathcal{S} \geq ((t-1)+1)(q-1)+1 = t(q-1)+1,$$

tj.

$$k-q-1 \geq t(q-1)+1 \quad \Rightarrow \quad k \geq tq+q-t+2.$$

■

PRIMJER 7.6 *Konika.*

U Primjeru 6.3 smo vidjeli da vanjske točke konike zajedno sa svim točkama konike osim jedne čine $\frac{q+1}{2}$-struku blokadu projektivne ravnine neparnog reda q. Ona sadrži sve točke jednog cijelog pravca i kada se isključi $q+1$ točaka tog pravca preostaje $(q^2+q)/2-1$ točaka afine ravnine koje čine $\frac{q-1}{2}$-struku blokadu afine ravnine.

Neka je npr. $q = 5$. Tada konika u $PG(2,5)$ sadrži 6 točaka. Vanjskih točaka konike ima 15, a unutrašnjih 10. Dakle, vanjske točke i 5 točaka konike čine trostruku blokadu projektivne ravnine $PG(2,5)$. Afinih točaka tada ima 14 i one čine dvostruku blokadu afine ravnine $AG(2,5)$.

Literatura

[1] S. Ball, *Multiple blocking sets and arcs in finite planes*, J. London Math. Soc., 54:581-593, 1996.

[2] S. Ball, A. Blokhuis, *On the size of the double blocking sets in* $PG(2, q)$, Finite Fields Appl., 2:125-137, 1996.

[3] S. Ball, A. Blokhuis, A. E. Brouwer, *On the number of slopes of the graph of a function defined on a finite field*, J. Combin. Theory Ser. A, 86:187-196, 1999.

[4] A. Blokhuis, *Extremal problems in finite geometries*, In Extremal problems for finite sets, Bolyai Soc. Math. Studies, 3:111-135, 1991.

[5] A. Blokhuis, *On the size of the blocking set in* $PG(2, p)$, Combinatorica, 14:111-114, 1994.

[6] A. Blokhuis, *Blocking sets in Desarguesian planes*, In Combinatorics, Paul Erdős is Eighty, Bolyai Soc. Math. Studies, 2:133-155, 1996.

[7] A. Blokhuis, *Blocking sets in projective and affine planes*, Intesive course, Ghent, 1998.

[8] A. Blokhuis, *Combinatorial problems in finite geometry and lacunary polynomials*, ICM, 3:537-545, 2002.

[9] A. Blokhuis, A. E. Brouwer, T. Szőnyi, *The number of directions determined by a function f on a finite field*, J. Combin. Theory Ser. A, 70:349-353, 1995.

[10] A. Blokhuis, A. E. Brouwer, H. A. Wilbrink, *Blocking sets in* $PG(2, p)$ *for small p, and partial spreads in* $PG(3, 7)$, Advances in Geometry, Special Issue, 2003.

[11] A. Blokhuis, L. Strome, T. Szőnyi, *Lacunary polynomials, multiple blocking sets and Baer subplanes*, J. London Math. Soc., 60:321-332, 1999.

[12] A. A. Bruen, *Baer subplanes and blocking sets*, Bull. Amer. Math. Soc., 76:342-344, 1970.

[13] A. A. Bruen, *Blocking sets in finite projective planes*, SIAM J. Appl. Math., 21:380-392, 1971.

[14] A. A. Bruen, *Polynomial multiplicities over finite fields and intersection sets*, J. Combin. Theory Ser. A, 60:19-33, 1992.

[15] A. A. Bruen, J. C. Fisher, *Blocking sets and complete k-arcs*, Pacific J. Math., 53:73-84, 1974.

[16] A. A. Bruen, B. L. Rothschild, *Lower bounds on blocking sets*, Pacific J. Math., 118:303-311, 1985.

[17] A. A. Bruen, J. A. Thas, *Blocking sets*, Geom. Dedicata, 6:193-203, 1977.

[18] J. Danielsson, *Minimal blocking sets of size* $2p-2$ *and* $3p-3$ *in* $PG(2,p)$*,* p *prime and* $p > 5$, J. Geom., 88:15-18, 2008.

[19] R. H. F. Denniston, *Some maximal arcs in finite projective planes*, J. Combin. Theory, 6:317-319, 1969.

[20] J. W. Di Paola, *On minimum blocking coalitions in small projective plane games*, SIAM J. Appl. Math., 17:378-392, 1969.

[21] A. Gács, T. Szőnyi, Z. Weiner *On the spectrum of minimal blocking sets in* $PG(2,q)$, J. Geom., 76:256-281, 2003.

[22] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Clarendon Press Oxford, 1998.

[23] K. Horvatić, *Linearna algebra*, Golden marketing-Tehnička knjiga, Zagreb, 2004.

[24] D. R. Hughes, F. C. Piper, *Projective Planes*, Springer-Verlag New Yok Heidelberg Berlin, 1973.

[25] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, 2008.

[26] D. Palman, *Projektivna geometrija*, Školska knjiga, Zagreb, 1984.

[27] L. Rédei, *Lacunary Polynomials over Finite Fields*, Akadémiai Kiadó, Budapest, 1973.

[28] M. Richardson, *On finite projective games*, Proc. Amer. Math. Soc., 7:458-465, 1956.

[29] T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, Finite Fields Appl., 3:187-202, 1997.

[30] J. von Neumann, O. Morgenstern, *Theory of games and economic behavior*, Bull. Amer. Math. Soc., 51:498-504, 1945.

[31] D. Žubrinić, *Diskretna matematika*, Element, Zagreb, 2002.

Sažetak

U ovom radu prikazana su osnovna svojstva blokada u konačnim projektivnim ravninama. Blokada $\mathcal{B}$ je skup točaka gdje svaki pravac ravnine sadrži barem jednu točku iz $\mathcal{B}$. Ako svaki pravac ravnine siječe $\mathcal{B}$ u barem t točaka, onda $\mathcal{B}$ nazivamo t-strukom blokadom. Radnjom im je opisana struktura, egzistencija te ocjena njihove veličine. Također, obuhvaćeni su i lakunarni polinomi (polinomi kojima je jedan ili više uzastopnih koeficijenata nakon vodećeg člana jednaki nuli) nad konačnim poljima, a rezultati teorije potpuno reducibilnih lakunarnih polinoma korišteni su u određivanju veličina blokada u Desarguesovim projektivnim ravninama. Posebno su prikazane Redéijeve blokade, te veza blokada i lukova projektivnih ravnina.
Metode u radu se temelje na povezivanju geometrijskih, kombinatoričkih i algebarskih razmatranja, kako je uobičajeno u području konačnih geometrija.

Summary

Basic properties of blocking sets in projective planes over finite fields are presented. A blocking set $\mathcal{B}$ is a set of points which meets every line of a plane. If each line of a plane contains at least t points of $\mathcal{B}$ then $\mathcal{B}$ is called a t-fold blocking set. This thesis describes their structure, existence and examines possible bounds on the size of blocking sets. The lacunary polynomials over finite field are also included (fully reducible polynomials with a gap between its degree and second degree). Results of the theory of fully reducible lacunary polynomials are fundamental in determining further lower bounds on the size of blocking sets in Desarguesian projective planes. Blocking sets of Redéi type are examined also. Furthermore, blocking sets are related to arcs, so this connection is pointed out. Since we are dealing with the field of finite geometries, the methods are based on integration of geometrical, combinatorial and algebraic observations.

Životopis

Rođena sam 29. prosinca 1973. godine u Splitu, gdje sam završila osnovnu školu (1988.), maturirala u Matematičko-informatičkom obrazovnom centru (1992.), te diplomirala na Fakultetu prirodoslovno-matematičkih znanosti i odgojnih područja Sveučilišta u Splitu na programu studija Matematika i informatika (1999.). Diplomski rad pod naslovom *Diferencijalne nejednakosti u teoriji običnih diferencijalnih jednadžbi* izradila sam pod vodstvom dr.sc. Tanje Vučičić.
2002. godine upisala sam Poslijediplomski znanstveni studij matematike na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.
Kao profesor informatike radila sam u III. gimnaziji u Splitu (1997.-2001.), zatim kao vanjski suradnik pri Zavodu za informatiku na Fakultetu prirodoslovno-matematičkih znanosti i odgojnih područja u Splitu (1997.-2000.), te kao profesor informatike u Privatnoj jezičnoj gimnaziji "Pitagora" u Splitu (2000.-2002.).
Od 2002. godine zaposlena sam kao asistent na Katedri za geometriju Građevinsko-arhitektonskog fakulteta u Splitu.
Član sam Hrvatskog matematičkog društva (HMD), Hrvatskog društva za geometriju i grafiku (HDGG) te Seminara za geometriju.