Unitali

V. Krčadinac, ljetni semestar 2009./2010., 30 sati.

Unitali su blokovni dizajni s parametrima 2-$(q^3+1, q+1, 1)$. Primjeri unitala dobivaju se kao skupovi apsolutnih točaka i neapsolutnih pravaca unitarnog polariteta projektivne ravnine reda q^2. Postoje unitali koji se ne mogu uložiti u projektivnu ravninu, kao i unitali koji se mogu uložiti, ali ne dobivaju se od unitarnog polariteta.

Na početku kolegija kratko ćemo se osvrnuti na opće unitale i pitanja o njihovoj egzistenciji i klasifikaciji za male parametre. Veći dio kolegija bit će posvećen unitalima u projektivnim ravninama, prema knjizi [1]. Ponovit ćemo osnovne činjenice o konačnim projektivnim ravninama i njihovim polaritetima [3], posebno o ravninama nad poljima i hermitskim unitalima [2]. Spomenut ćemo neke strukture povezane s unitalima kao što su ovali, lukovi i blokade.

Posebna pažnja bit će posvećena konstrukcijama unitala u projektivnim ravninama i otvorenim pitanjima o unitalima. Studenti će se aktivno uključivati u nastavu kroz domaće zadaće i projektne zadatke. Polaganje ispita predviđa se kroz individualne projektne zadatke koji se mogu izložiti usmeno na znanstvenom seminaru ili u obliku pisanog rada.

Literatura

1. S. Barwick, G. Ebert, *Unitals in Projective Planes*, Springer, 2008.
2. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, 1998.
3. D.R. Hughes, F.C. Piper, *Projective Planes*, Springer, 1973.
4. C.M. O'Keefe, *Unitals*, Intensive Course on Galois Geometry and Generalized Polygons (lecture notes), University of Ghent, 1998. `http://cage.rug.ac.be/~fdc/intensivecourse/unitals.ps`

B. From now on whenever I read a math book, I'm going to try to figure out by myself how everything was done, before looking at the solution. Even if I don't figure it out, I think I'll be able to see the beauty of a proof then.

A. And I think we should also try to guess what theorems are coming up; or at least, to figure out how and why anybody would try to prove such theorems in the first place. We should imagine ourselves in the discoverer's place. The creative part is really more interesting than the deductive part. Instead of concentrating just on finding good answers to questions, it's more important to learn how to find good questions!

B. You've got something there. I wish our teachers would give us problems like, "Find something interesting about x," instead of "Proove x."

A. Exactly. But teachers are so conservative, they'd be afraid of scaring off the "grind" type of students who obediently and mechanically do all the homework. Besides, they wouldn't like the extra work of grading the answers to nondirected questions. The traditional way is to put off all creative aspects until the last part of graduate school. **For seventeen or more years, students are thaught examsmanship; then suddenly after passing enough exams in graduate school they're told to do something original.**

B. Right. I doubt if many of the really original students have stuck around that long.

A. Oh, I don't know, maybe they're original enough to find a way to enjoy the system. Like putting themselves into the subject, as we were saying. That would make the traditional college courses tolerable, maybe even fun.

B. You always were an optimist. I'm afraid you're painting too rosy a picture. But look, the rain has stopped. Let's lug this rock back to the camp and see what it says.

D.E.Knuth, *Surreal numbers*

Sadržaj

1 Unitali i projektivne ravnine

Što je unital? Što je konačna projektivna ravnina?

Definicija 1.1 Steinerov 2-dizajn *s parametrima* 2-$(v, k, 1)$*, odnosno* $S(2, k, v)$*, je konačna incidencijska struktura s* v *točaka i* b *pravaca, takva da na svakom pravcu leži* k *točaka i kroz svake dvije točke prolazi jedan pravac.*

Generalizacije:

- blokovni dizajni 2-(v, k, λ)
- Steinerovi sustavi $S(t, k, v)$
- t-(v, k, λ) dizajni

Propozicija 1.2 *Kroz svaku točku Steinerovog* 2*-dizajna* $S(2, k, v)$ *prolazi* $r = \frac{v-1}{k-1}$ *pravaca. Ukupan broj pravaca je* $b = \frac{v(v-1)}{k(k-1)}$.

Dokaz. Dvostrukim prebrojavanjem. □

Teorem 1.3 (Fisherova nejednakost) *Broj pravaca nije manji od broja točaka:* $v \leq b$.

Dokaz. Obično se dokazuje "linearnoalgebarskom metodom", npr. u [41]. Originalni Fisherov dokaz koristi dvostruko prebrojavanje i minimizaciju kvadratne funkcije. □

Nužni uvjeti za postojanje $S(2, k, v)$ dizajna:

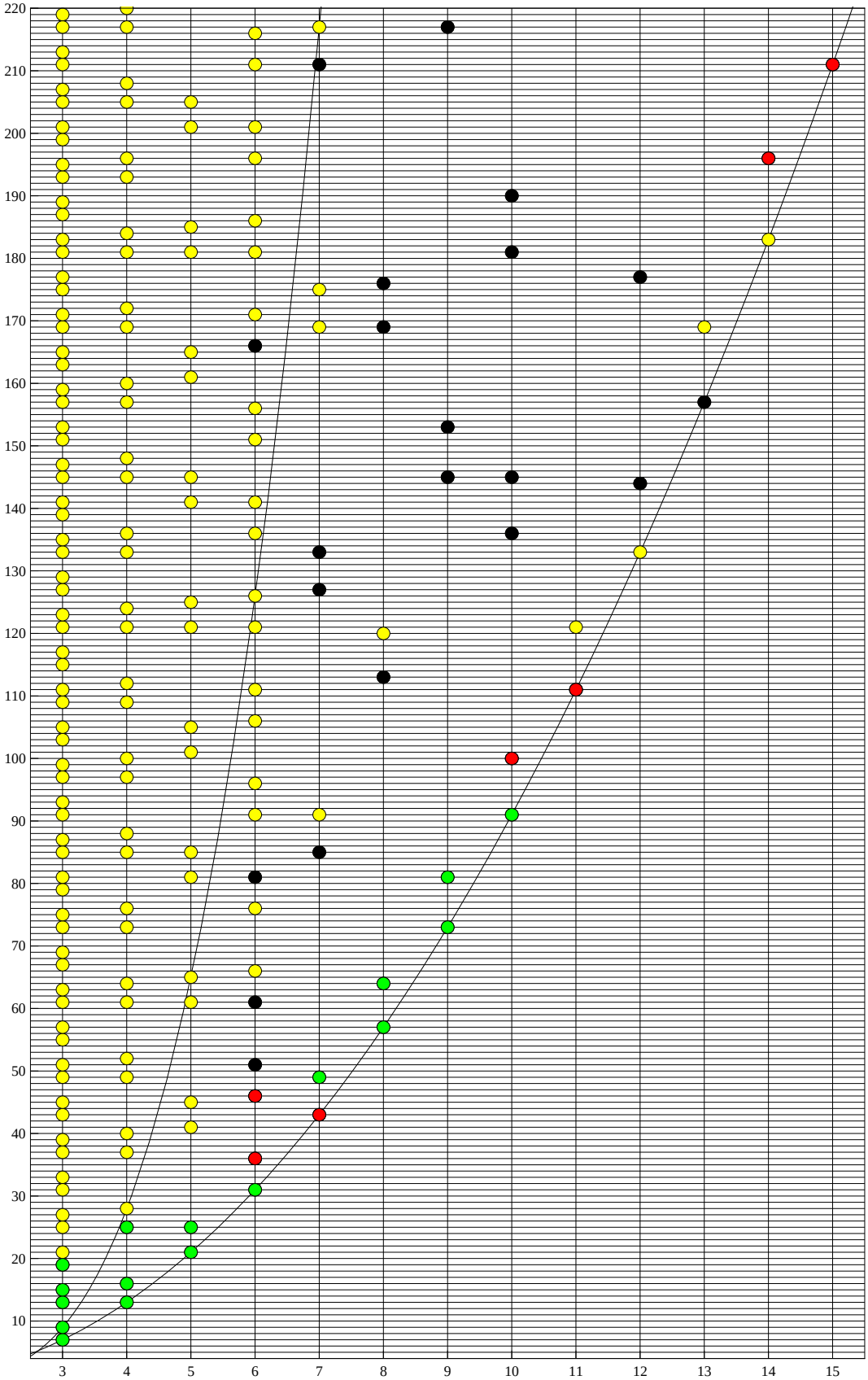
1. $k - 1 \mid v - 1$,
2. $k(k-1) \mid v(v-1)$,
3. $v \geq k^2 - k + 1$.

Parametre koji zadovoljavaju nužne uvjete nazivamo *dopustivima*.

Koji su dovoljni uvjeti za postojanje $S(2, k, v)$ dizajna?

- $k = 3$

Dizajni $S(2, 3, v)$ su Steinerovi sustavi trojki $STS(v)$. Znamo da su za njih nužni uvjeti $v \equiv 1$ ili 3 (mod 6), $v \geq 7$ ujedno i dovoljni.


220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
3
4
5
6
7
8
9
10
11
12
13
14
15

- $k = 4$

Za $S(2, 4, v)$ dizajne nužni uvjeti $v \equiv 1$ ili 4 (mod 12), $v \geq 13$ također su dovoljni. Nedavno je objavljen pregledni članak o takvim dizajnima [39]. Oni se *ne* zovu Steinerovi sustavi četvorki – to ime rezervirano je za $S(3, 4, v)$ dizajne!

- $k = 5$

I za $S(2, 5, v)$ dizajne nužni uvjeti su dovoljni: $v \equiv 1$ ili 5 (mod 20), $v \geq 21$. Taj i prethodni rezultat dokazao je Haim Hanani [26].

- $k = 6$

Za $S(2, 6, v)$ dizajne nužni uvjeti *nisu* dovoljni. Ne postoji $S(2, 6, 36)$ dizajn (afina ravnina reda 6) i $S(2, 6, 46)$ dizajn iako su parametri dopustivi. Drugi rezultat dokazan je s pomoću računala [28]. Za neke od parametara $S(2, 6, v)$ ne zna se da li postoje dizajni, kao i za sve ostale $k \geq 6$.

Teorem 1.4 (Wilson) *Za svaki $k \geq 3$ postoji v_0 takav da za sve dopustive parametre $S(2, k, v)$, $v \geq v_0$, postoje dizajni.*

Umjesto parametara s fiksnim k, promotrimo familije parametrizirane s k.

Definicija 1.5 Konačne projektivne ravnine *su $S(2, k, k^2 - k + 1)$ dizajni.* Konačne afine ravnine *su $S(2, k, k^2)$ dizajni.*

Alternativno, konačne projektivne ravnine su simetrični $S(2, k, v)$ dizajni, tj. takvi da je $v = b$. Obično se kao parametar uzima *red* $n = k - 1$ i parametri se zapisuju kao $S(2, n + 1, n^2 + n + 1)$ ili 2-$(n^2 + n + 1, n + 1, 1)$. Veza između projektivnih i afinih ravnina $S(2, n, n^2)$ je poznata konstrukcija brisanja / dodavanja "pravca u beskonačnosti". Za projektivne ravnine poznat je netrivijalan nužan uvjet za egzistenciju.

Teorem 1.6 (Bruck-Ryser) *Ako postoji projektivna ravnina reda $n \equiv 1$ ili 2 (mod 4), onda se n može prikazati kao suma dvaju kvadrata cijelih brojeva, tj. u nekvadratnom dijelu od n nema prostih faktora $p \equiv 3$ (mod 4).*

Iz teorema slijedi nepostojanje projektivne ravnine reda 6 i reda 14. Nepostojanje ravnine reda 10 dokazano je s pomoću računala [32].

Definicija 1.7 Unitali *su Steinerovi 2-dizajni s parametrima oblika $S(2, n + 1, n^3 + 1)$.*

Primjer 1.8 *Neka je dana projektivna ravnina reda n^2 s unitarnim polaritetom. Tada skup apsolutnih točaka i neapsolutnih pravaca čini unital $S(2, n + 1, n^3 + 1)$.*

O čemu je tu riječ?

Što se zna o "malim" unitalima?

- $n = 2$

Unital $S(2, 3, 9)$ je afina ravnina reda 3, odnosno $STS(9)$. Postoji točno jedan takav dizajn (do na izomorfizam). Definicija unitala iz knjige [7] ima ograničenje $n \geq 3$, pa se taj dizajn ne smatra unitalom. Ja bih ga priznao, jer nastaje od unitarnog polariteta projektivne ravnine reda 4.

- $n = 3$

Unitale $S(2, 4, 28)$ i njihovo ulaganje u projektivne ravnine reda 9 proučavao je Brouwer [11]. Našao je 11 primjera koje je moguće uložiti i preko 100 primjera koje nije moguće uložiti. Kasnije su Penttila i Royle [38] potpuno klasificirali unitale uložene u ravnine reda 9 i pronašli 17 neizomorfnih primjera. Sve četiri projektivne ravne reda 9 sadrže unitale: klasična 2, Hallova (translacijska) i njoj dualna po 4, a Hughesova 8. Jedan od unitala ulaže se u dvije ravnine (Hallovu i njoj dualnu), a svi ostali točno u jednu ravninu.

U [31] klasificirani su svi $S(2, 4, 28)$ s netrivijalnom grupom automorfizama. Ima ih točno 4466. U sljedećoj tablici dana je distribucija prema redu pune grupe automorfizama.

|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#
12096	1	48	12	18	1	6	60
1512	1	42	1	16	10	4	374
216	1	32	2	12	12	3	1849
192	2	27	1	9	18	2	2028
72	1	24	12	8	71		
64	1	21	6	7	2		

Dizajn s grupom reda 12096 je klasični unital (dobiven od unitarnog polariteta klasične projektivne ravnine), a dizajn s grupom reda 1512 je Reeov unital. Unitali uloženi u projektivne ravnine imaju grupe reda 12096, 216, 192, 48 ($\times 4$), 24 ($\times 2$), 8 ($\times 4$), 6 ($\times 2$), 4 i 3.

A.Betten, D.Betten i V.D.Tonchev [9] konstruirali su 909 unitala s pomoću taktičkih dekompozicija definiranih od priduženih dualnih binarnih kodova. Među njima je 187 primjera s trivijalnom grupom automorfizama. Brouwer [11] je također našao 26 primjera s trivijalnom grupom.

Kaski i Östergard [30] potpuno su klasificirali rastavljive $S(2, 4, 28)$ (eng. *resolvable*; također sam koristio termin *razlučivi*). To znači da im pravce možemo particionirati na paralelne klase. Dokazali su da ih ima točno 6 (bili su poznati od prije). Klasični i Reeov $S(2, 4, 28)$ su oba rastavljivi, a Reeov se može rastaviti na dva neizomorfna načina (svi ostali samo na jedan). Broj neizomorfnih rastava (razlučenja, eng. resolutions) $S(2, 4, 28)$ dizajna

je stoga 7.

- $n = 4$

Stoichev i Tonchev [42] proučavali su unitale $S(2, 5, 65)$ u projektivnim ravninama reda 16. Poznate su 22 ravnine (4 samodualne i 9 parova dualnih) i u svima postoje unitali. Potraga nije bila iscrpna (tražili su unitale invarijantne obzirom na grupu automorfizama ravnine reda barem 4), a pronađeno je 38 unitala. Uzevši u obzir i dualne unitale (vidi teorem 1.9), postoji barem 73 neizomorfna $S(2, 5, 65)$ uložena u projektivne ravnine. Od ranije su poznata dva ciklička unitala koja nije moguće uložiti, što čini ukupno 75 neizomorfna primjera. Nije teško konstruirati još primjera s netrivijalnim grupama automorfizama. Trenutačno na hard disku imam 705 neizomorfna $S(2, 5, 65)$ s grupama reda 249600, 1200, 780, 768, 600, 384, 300, 260, 256, 200, 192, 150, 128, 100, 96, 80, 78, 64, 50, 48, 39, 32, 24, 20, 16, 13, 12, 8 i 4 (prvi je klasični, a ciklički imaju pune grupe reda 780 i 260). Primjeri u ravninama reda 16 koje su pronašli Stoichev i Tonchev imaju pune grupe automorfizama reda 4, 8, 12, 16, 20, 24, 32, 48, 64, 80, 100, 128, 192, 768, 1200 i 249600. Među njima je 15 rastavljivih.

- $n = 5$

U Handbooku [20] piše da su poznata dva unitala $S(2, 6, 126)$ od kojih je jedan rastavljiv. S druge strane, tamo to isto piše za $S(2, 5, 65)$. Vjerojatno je poznato više unitala s tim parametrima u projektivnim ravninama reda 25 i može ih se konstruirati još.

- $n = 6$

Unital $S(2, 7, 217)$ je do sada jedini poznati primjer kod kojeg n nije prim potencija. Našli su ga neovisno Mathon [33] te S. Bagchi i B. Bagchi [2]. Ima cikličku grupu automorfizama. Nije poznato može li se uložiti u projektivnu ravninu reda 36 (za koju se ne zna da li postoji).

Teorem 1.9 *Neka je unital $\mathcal{U}$ s parametrima $S(2, n+1, n^3+1)$ uložen u projektivnu ravninu $\mathcal{P}$ reda n^2. Tada tangente na $\mathcal{U}$ i točke koje ne pripadaju $\mathcal{U}$ tvore drugi unital $\mathcal{U}^*$ s istim parametrima, koji zovemo* dualnim unitalom.

Dokaz. Uloženi unital shvaćamo kao $(n^3 + 1)$-člani podskup skupa točaka projektivne ravnine sa svojstvom da ga $b = \frac{(n^3+1)n^2}{(n+1)n} = n^4 - n^3 + n^2$ pravaca od $\mathcal{P}$ siječe u $(n+1)$-članim podskupovima. Te pravce nazivamo *sekantama*, a njihove presjeke s $\mathcal{U}$ *tetivama* (tetive su pravci unitala). Kroz svaku točku od $\mathcal{U}$ prolazi $r = \frac{n^3}{n} = n^2$ sekanti i još jedan pravac projektivne ravnine koji nije sekanta. Takve pravce, koje $\mathcal{U}$ sijeku točno u jednoj točki, nazivamo *tangentama*, a sjecišta *diralištima*. Tangenti ima isto koliko i točaka unitala,

n^3+1. Ukupan broj pravaca od $\mathcal{P}$ jednak je zbroju broja tangenti i sekanti, pa je svaki pravac tangenta ili sekanta.

Definiramo novu incidencijsku strukturu $\mathcal{U}^*$ kojoj su TOČKE tangente na $\mathcal{U}$, a PRAVCI točke iz $\mathcal{P} \setminus \mathcal{U}$. Elemente nove strukture pišemo velikim slovima (ideja P. Camerona). Nova struktura ima n^3+1 TOČAKA i $n^4+n^2+1-n^3-1 = b$ PRAVACA, isto kao $\mathcal{U}$. Nadalje, kroz svake dvije TOČKE prolazi jedinstveni PRAVAC jer se svaka dva pravca projektivne ravnine sijeku, a tangente se ne mogu sijeći u točkama od $\mathcal{U}$. Isto tako jasno je da kroz svaku TOČKU prolazi n^2 PRAVACA.

Nije odmah jasno da na svakom PRAVCU leži $n+1$ točaka. Incidencijska struktura koja je balansirana i u kojoj su sve točke istog stupnja ne mora biti dizajn, ali u ovom slučaju znamo da parametri v, b i r odgovaraju dopustivim parametrima dizajna. Pretpostavimo da su stupnjevi PRAVACA redom $k_1, \ldots, k_b$. Prebrojavanjem incidencija vidimo da je $\sum k_i = vr$. Nadalje, prebrojavanjem parova TOČAKA dobivamo $\binom{v}{2} = \sum \binom{k_i}{2}$, što sređivanjem daje $\sum k_i^2 = v(v-1)+vr = bk^2$. Suma na lijevoj strani poprima minimalnu vrijednost uz uvjet $\sum k_i = vr$ kada su varijable k_i jednake. Taj minimum je upravo bk^2, pa zaključujemo da je $k_1 = \ldots = k_b = k$. Time smo dokazali da je $\mathcal{U}^*$ unital s istim parametrima kao $\mathcal{U}$. □

Projektni zadaci

1. Konstruirajte nove primjeri unitala za $n = 3$ (s trivijalnim grupama – taktičke dekompozicije, heuristike) i $n = 4, 5$ (s netrivijalnim grupama – KMAD).

2. Konstrukcija unitala za $n = 6$ (Mathon, Bagchi i Bagchi).

3. Reeovi unitali.

4. Ulaganje unitala u projektivne ravnine (kompjutorski program). Provjeriti poznate rezultate za $n = 3, 4$. Primijeniti na nove primjere unitala $S(2, 5, 65)$.

Domaća zadaća

1. Nađite još unitala za $n = 6$.

2. Konstruirajte unitale za neki $n > 6$ koji nije prim potencija, npr. $n = 10$ (tj. $S(2, 11, 1001)$ dizajne).

3. Postoji li projektivna ravnina reda n^2 koja ne sadrži niti jedan unital reda n?

4. Konstruirajte dizajne s parametrima koji odgovaraju bilo kojem od crnih kružića na str. 5.

2 Klasični unitali

U ovom poglavlju dokazat ćemo sljedeći teorem.

Teorem 2.1 *Ako je q potencija prostog broja, onda postoji unital $S(2, q+1, q^3+1)$.*

Primijenit ćemo konstrukciju iz primjera 1.8 na klasičnu projektivnu ravninu reda q^2.

Teorem 2.2 *Ako je q potencija prostog broja, onda postoji projektivna ravnina reda q, tj. dizajn $S(2, q+1, q^2+q+1)$.*

Dokaz. Neka je F polje s q elemenata. Označimo retke i stupce matrice $A = [a_{ij}]$ vektorima $(0,0,1)$, $(0,1,z)$ i $(1,y,z)$, za $y, z \in F$. Definiramo $a_{ij} = 1$ ako je "skalarni produkt" odgovarajućih vektora jednak 0, a $a_{ij} = 0$ inače. Pokazuje se da je A incidencijska matrica projektivne ravnine reda q. □

Projektivnu ravninu dobivenu od polja nazivamo *klasičnom* ili *Desarguesovom* i označavamo $PG(2, F)$, odnosno $PG(2, q)$ u slučaju konačnog polja s q elemenata. Dokaz teorema 2.2 možemo direktno implementirati u programskom sustavu GAP. Ovako dobivamo incidencijsku matricu projektivne ravnine reda q^2:

```
q:=3;
el:=Elements(GF(q^2));
v1:=[[el[1],el[1],el[2]]];
v2:=Cartesian([el[1]],[el[2]],el);
v3:=Cartesian([el[2]],el,el);
v:=Concatenation(v1,v2,v3);
jedan:=function(x) if x then return 1; else return 0; fi; end;
A:=List(v,y->List(v,x->jedan(x*y=el[1])));
```

Pogledamo li dokaz teorema 2.1 u knjizi [7], vidjet ćemo da klasičnom unitalu pripadaju točke označene vektorima (x, y, z) koji zadovoljavaju jednadžbu $x^{q+1} + y^{q+1} + z^{q+1} = 0$. Sekante su pravci označeni vektorima koji ne zadovoljavaju tu jednadžbu. Ovako dobivamo incidencijsku matricu unitala:

```
u:=Filtered(v,x->x[1]^(q+1)+x[2]^(q+1)+x[3]^(q+1)=el[1]);
s:=Difference(v,u);
A:=List(u,y->List(s,x->jedan(x*y=el[1])));
```

2.1 Konačna polja

Teorem 2.3 *Konačno polje s n elemenata postoji ako i samo ako je n potencija prostog broja. Svaka dva konačna polja istog reda su izomorfna.*

Konačno polje s q elemenata označavamo $GF(q)$ ili $\mathbb{F}_q$. Najjednostavnija su konačna polja prostog reda p. Možemo uzeti cijele brojeve modulo p, tj. $(\mathbb{Z}_p, +_p, \cdot_p)$. Konačno polje reda $q = p^e$ konstruiramo kao polinome stupnja manjeg od e s koeficijentima iz $\mathbb{Z}_p$. Zbrajamo ih na uobičajen način, a množimo modulo nekog ireducibilnog polinoma stupnja e nad $\mathbb{Z}_p$. Iz ove konstrukcije slijedi:

Propozicija 2.4 *Aditivna grupa polja $GF(p^e)$ je elementarno Abelova, tj. izomorfna s direktnom sumom $\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ (e sumanada).*

Važan je i sljedeći teorem.

Teorem 2.5 *Multiplikativna grupa $GF(q)^* = GF(q) \setminus \{0\}$ je ciklička.*

Dokaz. Hungerford, teorem V.5.3 na str. 279. □

Generator multiplikativne grupe konačnog polja zovemo *primitivnim elementom* polja i obično ga označavamo s ω. Iz "fundamentalnog teorema Galoisove teorije" slijede teoremi o automorfizmima i potpoljima konačnog polja.

Teorem 2.6 *Grupa automorfizama polja $GF(p^e)$ je ciklička reda e. Generirana je* Frobeniusovim automorfizmom $x \mapsto x^p$.

Teorem 2.7 *Za svaki d koji je djelitelj od e polje $GF(p^e)$ ima jedinstveno potpolje reda p^d. To su jedina potpolja od $GF(p^e)$.*

Označimo s $QR(q) = \{x^2 \mid x \in GF(q)^*\}$ nenul kvadrate u konačnom polju $GF(q)$ (eng. *quadratic residues*). Ako je q paran (tj. potencija od 2), $QR(q)$ je cijeli $GF(q)^*$. Ako je q neparan, $QR(q)$ je podgrupa multiplikativne grupe $GF(q)^*$ indeksa 2. Posebno, pola elemenata iz $GF(q)^*$ su kvadrati, a pola nisu kvadrati.

Lema 2.8 *Neka je q neparna prim potencija. Tada je $-1 \in QR(q)$ ako i samo ako je $q \equiv 1 \pmod 4$.*

Dokaz. Neka je ω primitivni element polja $GF(q)$. Nenul kvadrati su potencije od ω s parnim eksponentom, a nekvadrati s neparnim eksponentom. Element $x = \omega^{(q-1)/2}$ nije 1 i zadovoljava $x^2 = 1$, pa je $x = -1$. Vidimo da je -1 kvadrat točno kada je $\frac{q-1}{2}$ paran, tj. $q \equiv 1 \pmod 4$. □

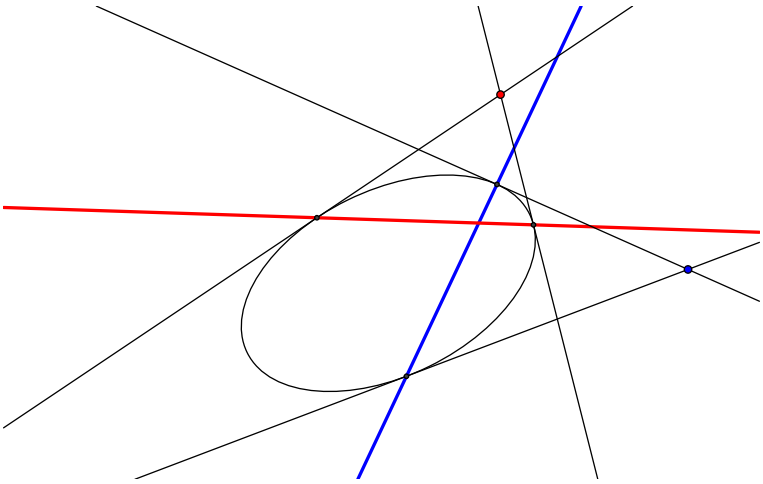
2.2 Polariteti

Sjetimo se definicije pola i polare iz analitičke geometrije:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

$$T_0 = (x_0, y_0) \quad \mapsto \quad p_0 \ldots \frac{x_0\, x}{a^2} + \frac{y_0\, y}{b^2} = 1$$

Geometrijska interpretacija:



Važna svojstva:

1. Točka T leži na pravcu p ako i samo ako pol od p leži na polari od T.
2. Involutornost: točka T je pol od p ako i samo ako je p polara od T.
3. Polara točke na elipsi je tangenta u toj točki.

Koja je geometrijska interpretacija polare za točke unutar elipse?

Automorfizmi projektivnih ravnina obično se nazivaju *kolineacijama*. To su bijekcije koje točkama pridružuju točke, pravcima pridružuju pravce i koje čuvaju incidenciju. Bijekcije koje "okreću" incidenciju nazivaju se *korelacijama*.

Definicija 2.9 *Neka je $(\mathcal{T}, \mathcal{P}, I)$ projektivna ravnina.* Korelacija *je bijekcija $\rho : \mathcal{T} \cup \mathcal{P} \to \mathcal{T} \cup \mathcal{P}$ takva da je $\mathcal{T}^\rho = \mathcal{P}$, $\mathcal{P}^\rho = \mathcal{T}$ i da vrijedi $TIp \iff p^\rho I T^\rho$, za sve točke $T \in \mathcal{T}$ i pravce $p \in \mathcal{P}$.* Polaritet *je involutorna korelacija, tj. takva da je $\rho^2 = id$.*

Spomenuli smo da je polara točke na elipsi tangenta, pa su u tom slučaju pol i polara incidentni. Vrijedi i više: točka pripada elipsi ako i samo ako leži na svojoj polari. Takve točke nazivamo *apsolutnim*.

Definicija 2.10 *Neka je ρ polaritet projektivne ravnine. Točke i pravce zovemo* apsolutnim *ako su incidentni sa svojom slikom po ρ. U suprotnom zovemo ih* neapsolutnim *točkama, odnosno pravcima.*

Propozicija 2.11 *Svaka apsolutna točka leži na jedinstvenom apsolutnom pravcu. Dualno, svaki apsolutni pravac prolazi kroz jedinstvenu apsolutnu točku.*

Dokaz. Neka je A apsolutna točka. Po definiciji, A leži na A^ρ. Pretpostavimo da na A^ρ leži i neka druga apsolutna točka B. Budući da je B na A^ρ, slijedi da je A na B^ρ. Vidimo da se A i B podudaraju jer su obje na presjeku pravaca A^ρ i B^ρ. □

Korolar 2.12 *U projektivnoj ravnini s polaritetom ρ ne može svaka točka biti apsolutna.*

Dokaz. Ako je A apsolutna točka, ostale točke na pravcu A^ρ nisu apsolutne. □

Krivulja drugog reda (konika) može se definirati kao skup apsolutnih točaka određene vrste polariteta (tzv. ortogonalnog polariteta). Nad kompleksnim brojevima postoje druge vrste polariteta, tzv. unitarni polariteti. Njihovi skupovi apsolutnih točaka su *hermitske krivulje*. Unitali su konačni analogoni hermitskih krivulja, a za krivulje drugog reda konačni analogoni su *ovali*.

Zna li netko geometrijska svojstva hermitskih krivulja?

Primjer 2.13 *U projektivnoj ravnini konstruiranoj od polja kao u dokazu teorema 2.2 incidencijska matrica je simetrična, pa imamo "očiti polaritet" (transponiranje incidencijske matrice).*

Za incidencijsku strukturu kažemo da je *samodualna* ako je izomorfna dualnoj incidencijskoj strukuturi, tj. ako posjeduje korelaciju. U tom slučaju broj točaka jednak je broju pravaca. Može li se postići da incidencijska matrica samodualne strukture bude simetrična?

Propozicija 2.14 *Incidencijska matrica konačne incidencijske strukture može se zapisati tako da bude simetrična ako i samo ako struktura posjeduje polaritet, tj. ako je* samopolarna.

Dokaz. Ako je incidencijska matrica simetrična, transponiranje je polaritet (isto kao kod klasične projektivne ravnine). Obrnuto, neka imamo polaritet ρ i neka reci incidencijske matrice A redom odgovaraju točkama $T_1, \ldots, T_v$, a stupci pravcima $p_1, \ldots, p_v$. Retke (ili stupce) možemo permutirati tako da vrijedi $T_i^\rho = p_i$, $i = 1, \ldots, v$. Tada je $a_{ij} = 1 \iff T_i I p_j \iff p_j^\rho I T_i^\rho \iff T_j I p_i \iff a_{ji} = 1$. Vidimo da je A simetrična matrica. □

Najmanji primjer samodualne strukture koja nije samopolarna sastoji se od 7 točaka i 7 pravaca [12].

Domaća zadaća: postoji li projektivna ravnina koja je samodualna, a nije samopolarna? Prema [7] i [29], to je otvoren problem.

Postoji li simetrični dizajn s tim svojstvom?

2.3 Polariteti konačnih projektivnih ravnina

Želimo ocijeniti koliko najviše, a koliko najmanje apsolutnih točaka može imati polaritet konačne projektivne ravnine reda n. Broj apsolutnih točaka polariteta ρ označavat ćemo $a(\rho)$. Dokazi tvrdnji iz ove cjeline nalaze se u XII. poglavlju knjige [29].

Vidjeli smo da ne može svaka točka biti apsolutna, tj. $a(\rho) < n^2 + n + 1$. Može li se dogoditi da niti jedna točka nije apsolutna? Za beskonačne ravnine to je moguće, npr. u ravnini $PG(2, \mathbb{R})$ konstruiranoj kao u dokazu teorema 2.2 točka (x, y, z) je apsolutna za "očiti polaritet" ako i samo ako je $x^2+y^2+z^2 = 0$. Jedino realno rješenje te jednadžbe je $(0, 0, 0)$. Međutim, u konačnim projektivnim ravninama svaki polaritet ima apsolutnih točaka. Za dokaz nam treba ova lema.

Lema 2.15 *Neka je I jedinična $v \times v$ matrica, J $v \times v$ matrica popunjena jedinicama i $C = nI + J$, za neki $n \in \mathbb{N}$. Onda je $n+v$ svojstvena vrijednost od C kratnosti 1, a n svojstvena vrijednost od C kratnosti $v - 1$.*

Zbog simetričnosti algebarska kratnost jednaka je geometrijskoj kratnosti. Ako je A incidencijska matrica projektivne ravnine reda n, poznato je da je $A \cdot A^\tau = nI + J$.

Propozicija 2.16 *Polaritet ρ projektivne ravnine reda n ima bar jednu apsolutnu točku. Ako red n nije kvadrat, onda ρ ima točno $n + 1$ apsolutnih točaka.*

Bez obzira je li n kvadrat, apsolutnih točaka ima barem $n + 1$, ali je dokaz kompliciraniji. Treba nam sljedeća lema.

Lema 2.17 *Neka je ρ polaritet projektivne ravnine reda n i p bilo koji neapsolutni pravac. Tada je broj apsolutnih točaka na p suprotne parnosti od n, tj. kongruentan je s $n + 1 \pmod 2$.*

Korolar 2.18 *U ravnini parnog reda s polaritetom, svaki pravac sadrži bar jednu apsolutnu točku.*

Teorem 2.19 *Polaritet projektivne ravnine reda n ima bar $n+1$ apsolutnih točaka.*

Dobili smo ocjenu $a(\rho) \geq n + 1$. Idući cilj je dobiti gornju ocjenu za ravnine kvadratnog reda.

Teorem 2.20 *Neka je ρ polaritet projektivne ravnine reda $n = m^2$. Onda je $a(\rho) \leq m^3 + 1$.*

Sada znamo da je $n + 1 \leq a(\rho) \leq n^{3/2} + 1$. Ako n nije kvadrat, vrijedi jednakost $a(\rho) = n+1$. Takve polaritete zovemo *ortogonalnim*. U ravninama parnog reda, skup apsolutnih točaka ortogonalnog polariteta je skup točaka nekog pravca. U ravninama neparnog reda, apsolutne točke ortogonalnog polariteta čine oval.

Definicija 2.21 Luk *je skup točaka projektivne ravnine u kojem nikoje tri točne nisu kolinearne.*

Propozicija 2.22 *Ako u ravnini reda n postoji luk od m točaka, onda je $m \leq n + 2$.*

Dokaz. Spajanjem čvrste točke luka s ostalim točkama dobivamo različite pravce. Prema tome, $m-1$ ne može biti veći od broja pravaca kroz čvrstu točku, $n+1$. □

Definicija 2.23 *Luk od $n+1$ točaka u ravnini reda n zovemo* oval, *a luk od $n+2$ točaka* hiperoval.

Pokazuje se da hiperovali mogu postojati samo u ravninama parnog reda. Dakle, u ravninama neparnog reda ovali su maksimalni lukovi. Rekli smo da su u ravninama neparnog reda skupovi apsolutnih točaka ortogonalnih polariteta ovali, ali u klasičnoj ravnini vrijedi i obrat!

Teorem 2.24 (Segre) *U projektivnoj ravnini $PG(2,q)$ neparnog reda q, svaki oval je skup apsolutnih točaka nekog ortogonalnog polariteta.*

Projektni zadatak: dokaz Segreovog teorema.

U ravninama reda $n=m^2$ mogu postojati polariteti koji nisu ortogonalni. Njihov broj apsolutnih točaka je veći od m^2+1, ali ne može biti veći od m^3+1. Najzanimljiviji nam je upravo slučaj kad je broj apsolutnih točaka maksimalan. Takve polaritete nazivamo *unitarnim*.

Teorem 2.25 *Neka je ρ unitarni polaritet projektivne ravnine reda m^2. Skup apsolutnih točaka i neapsolutnih pravaca od ρ čini unital s parametrima $S(2,m+1,m^3+1)$.*

Pokazat ćemo da klasična projektivna ravnina $PG(2,q^2)$ ima unitarni polaritet i time će teorem 2.1 biti dokazan. Tako konstruirane unitale zovemo *klasičnim* ili *hermitskim*.

U klasičnim projektivnim ravninama mogući su samo ortogonalni i unitarni polariteti. Takvi polariteti su *regularni*, što znači da postoji t takav da je broj apsolutnih točaka na neapsolutnom pravcu 0, 1 ili $t+1$. Za ortogonalne polaritete je $t=1$, a za unitarne je $t=m$. Postoje neklasične projektivne ravnine reda m^2 s polaritetom ρ za koji je $m^2+1 < a(\rho) < m^3+1$.

Domaća zadaća: postoji li regularni polaritet koji nije ortogonalan niti unitaran? Prema [29], pitanje je otvoreno.

Projektni zadatak: pronađite sve polaritete ρ u samodualnim projektivnim ravninama reda 9 i 16 za koje je $m^2+1 < a(\rho) < m^3+1$. Usput ćete provjeriti

da su sve te projektivne ravnine samopolarne. Ispitajte koje su mogućnosti za $a(\rho)$ i za broj apsolutnih točaka na neapsolutnom pravcu. Ako uzmemo apsolutne točke i pravce koje ih sijeku u konstantnom broju točaka, dobivamo li konfiguracije?

2.4 Polariteti klasičnih projektivnih ravnina

Koliko apsolutnih točaka ima "očiti polaritet" ravnine $PG(2, q)$?

Očiti polaritet preslikava točku kojoj odgovara vektor (x, y, z) u pravac kojem odgovara isti vektor. Točka je apsolutna, tj. incidentna sa svojom polarom, ako vrijedi $x^2+y^2+z^2 = 0$. Prebrojimo koliko vektora oblika $(0, 0, 1)$, $(0, 1, z)$ i $(1, y, z)$ zadovoljava tu jednadžbu.

Vektor $(0, 0, 1)$ ne zadovoljava jednadžbu. Vektor $(0, 1, z)$ je zadovoljava akko vrijedi $z^2 = -1$. Ako je q paran postoji jedan takav z, ako je $q \equiv 1 \pmod 4$ postoje dva, a u slučaju $q \equiv 3 \pmod 4$ ne postoji takav z. Konačno, vektor $(1, y, z)$ zadovoljava jednadžbu akko je $y^2+z^2 = -1$. U slučaju parnog q za svaki $z \in GF(q)$ postoji jedinstveni y takav da relacija vrijedi, pa jednadžbu zadovoljava q vektora oblika $(1, y, z)$. Pokazuje se da u slučaju $q \equiv 1 \pmod 4$ jednadžbu zadovoljava $q - 1$, a u slučaju $q \equiv 3 \pmod 4$ zadovoljava je $q + 1$ takvih vektora. U svakom slučaju, ukupan broj vektora koji zadovoljavaju jednadžbu je $q + 1$.

Zadatak: dokažite da se u konačnom polju svaki element može prikazati kao zbroj dvaju kvadrata. Za prirodne brojeve uvjet prikazivosti kao zbroja dvaju kvadrata je netrivijalan (Fermatov teorem, vidi iskaz teorema 1.6).

Vidjeli smo da očiti polaritet ima $q + 1$ apsolutnih točaka, pa je ortogonalan. Ako je q paran apsolutne točke su točke jednog pravca, a za neparan q dobivamo oval (za dokaz vidi [29, teoremi 12.6 i 12.7]). Očiti polaritet ćemo ubuduće zvati *očiti ortogonalni polaritet*.

Postoji li u ravnini $PG(2, q^2)$ "očiti unitarni polaritet"?

Iskoristit ćemo involutorni automorfizam konačnog polja $GF(q^2)$. Sjetimo se: ako je $q^2 = p^{2e}$, grupa automorfizama polja $GF(q^2)$ je ciklička reda $2e$ i generirana je Frobeniusovim automorfizmom $x \mapsto x^p$. To znači da su

automorfizmi preslikavanja $x \mapsto x^{p^k}$, za $k = 0, \ldots, 2e-1$.

Zadatak: zašto je preslikavanje $x \mapsto x^p$ uopće automorfizam?

Involutorni automorfizam dobiva se za $k = e$; to je preslikavanje $x \mapsto x^{p^e} = x^q$. On fiksira potpolje $GF(q)$ i analogan je kompleksnom konjugiranju. Zvat ćemo ga *konjugiranje*.

Zadatak: za $q \equiv 3 \pmod 4$, polje $GF(q^2)$ možemo dobiti od $GF(q)$ na isti način kao što $\mathbb{C}$ nastaje od $\mathbb{R}$ – kao uređene parove $(x, y) \in GF(q)^2$ uz zbrajanje po koordinatama i množenje $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. Konjugiranje je tada promjena predznaka "imaginarnom dijelu": $(x, y)^q = (x, -y)$. Kako modificirati ovu konstrukciju da bi funkcionirala za paran q i za $q \equiv 1 \pmod 4$?

S pomoću konjugiranja definiramo preslikavanje točaka projektivne ravnine $PG(2, q^2)$ na pravce: $(x, y, z) \mapsto (x^q, y^q, z^q)$. Definicija je dobra, tj. ne ovisi o izboru vektora predstavnika jednodimenzionalnih potprostora: $(tx, ty, tz)^q = t^q(x^q, y^q, z^q)$. Preslikavanje je involutorno i čuva incidenciju, tj. "okreće je": $(x, y, z)\, I\, (a, b, c) \iff (a, b, c)^q\, I\, (x, y, z)^q$. Prema tome, to je polaritet. Prebrojimo njegove apsolutne točke!

Uvjet je $(x, y, z)\, I\, (x, y, z)^q \iff x^{q+1} + y^{q+1} + z^{q+1} = 0$. Sad je jasno od kuda jednadžba za točke klasičnog unitala s početka ovog poglavlja! Treba vidjeti koliko vektora oblika $(0, 0, 1)$, $(0, 1, z)$ i $(1, y, z)$ zadovoljava tu jednadžbu. Prvi vektor je ne zadovoljava, a za drugi je uvjet $z^{q+1} = -1$.

Proučimo svojstva preslikavanja $x \mapsto x^{q+1}$. To preslikavanje zove se *norma*, po analogiji s kompleksnim brojevima ($x^{q+1} = x \cdot x^q \rightsquigarrow |z|^2 = z \cdot \overline{z}$).

Lema 2.26 *Norme svih elemenata iz $GF(q^2)$ su elementi potpolja $GF(q)$.*

Dokaz. Nenul elemente možemo prikazati kao ω^i, gdje je ω primitivni element od $GF(q^2)$. Multiplikativna grupa potpolja $GF(q)^*$ generirana je s ω^{q+1} (zbog $q^2 - 1 = (q-1)(q+1)$). Prema tome, elementi $(\omega^i)^{q+1} = (\omega^{q+1})^i$ pripadaju potpolju. □

Lema 2.27 *Jednadžba $z^{q+1} = a$ ima jedinstveno rješenje $z = 0$ za $a = 0$, ima točno $q + 1$ rješenja za $a \in GF(q)^*$ i nema rješenja za $a \in GF(q^2) \setminus GF(q)$.*

Dokaz. Nula je jedini element norme nula jer u polju nema djelitelja nule. Prema tome, $GF(q)^*$ je "pogođen" normama elemenata iz $GF(q^2)^*$ ukupno

$q^2-1=(q-1)(q+1)$ puta. Polinomijalna jednadžba $z^{q+1}=a$ može imati najviše $q+1$ različitih rješenja. Zaključujemo da za svaki $a \in GF(q)^*$ jednadžba ima točno $q+1$ različitih rješenja u $GF(q^2)$, a po prethodnoj lemi nema rješenja za $a \in GF(q^2) \setminus GF(q)$. □

Iz leme slijedi da naš polaritet ima točno $q+1$ apsolutnih točaka oblika $(0,1,z)$. Isto vrijedi i za apsolutne točke oblika $(1,y,0)$.

Preostaje prebrojati apsolutne točke oblika $(1,y,z)$, za $z \neq 0$. Uvjet je $y^{q+1}+z^{q+1}=-1$. Zbog $z \neq 0$ mora biti $y^{q+1} \neq -1$, a znamo da takvih $y \in GF(q^2)$ ima točno $q^2-(q+1)=q^2-q-1$. Za svaki takav y jednadžba $z^{q+1}=-1-y^{q+1}$ ima točno $q+1$ rješenja z, jer je izraz s desne strane iz $GF(q)^*$. Dakle, u ovom slučaju broj apsolutnih točaka je $(q^2-q-1)(q+1)$.

Ukupan broj apsolutnih točaka je $2(q+1)+(q^2-q-1)(q+1)=(q^2-q+1)(q+1)=q^3+1$ i naš polaritet je unitaran. Zvat ćemo ga *očiti unitarni polaritet*. Njegove apsolutne točke i neapsolutni pravci čine klasični unital s parametrima $S(2,q+1,q^2+1)$. Time je teorem 2.1 konačno dokazan.

Kao i za svaki unital $S(2,q+1,q^2+1)$ uložen u projektivni ravninu reda q^2, za klasični unital točno $q^4-q^3+q^2$ pravaca ravnine su sekante (sijeku unital u $q+1$ točaka), a preostalih q^3+1 pravavca su tangente (sijeku unital u jednoj točki). Kroz točke unitala prolazi q^2 sekanti i jedna tangenta, a kroz točke izvan unitala prolazi q^2-q sekanti i $q+1$ tangenti. Zadnja tvrdnja dokazuje se prebrojavanjem. Ako broj sekanti i tangenti kroz točku T izvan unitala označimo redom s a i b, vrijedi $a+b=q^2+1$ i $(q+1)a+b=q^3+1$ (spajamo T s točkama unitala). Iz toga slijedi $a=q^2-q$, $b=q+1$.

Dirališta tangenata kroz zadanu točku T izvan unitala zovemo *nožištima*. Za unitale dobivene od unitarnog polariteta možemo preciznije opisati nožišta nego u općem slučaju.

Propozicija 2.28 *Neka je $\mathcal{U}$ unital u projektivnoj ravnini reda q^2 dobiven kao skup apsolutnih točaka i neapsolutnih pravaca unitarnog polariteta ρ. Za svaku točku T izvan $\mathcal{U}$, nožišta od T su kolinearna i leže na polari T^ρ.*

Dokaz. Neka je p tangenta kroz T koja dira unital u nožištu P. Pravac p ne pripada unitalu, pa je apsolutan i vrijedi $p=P^\rho$. Iz $T \in P^\rho$ slijedi $P \in T^\rho$. Vidimo da sva nožišta leže na T^ρ. □

Jesu li unitali dobiveni od unitarnih polariteta karakterizirani kolinearnim skupovima nožiša?

U ovom trenutku ne znam status ovog pitanja. Možda ćemo znati odgovor kad naučimo druge konstrukcije unitala u projektivnim ravninama ili kad

netko riješi ovaj projektni zadatak.

Projektni zadatak: ispitajte nožišta na unitale uložene u projektivne ravnine reda 9 i 16.

Vidjeli smo da klasična projektivna ravnina $PG(2, q^2)$ ima očiti ortogonalni polaritet i očiti unitarni polaritet. Idući cilj je dokazati da su svi polariteti klasične ravnine ortogonalni ili unitarni, tj. da ne postoje polariteti ρ s $q^2 + 1 < a(\rho) < q^3 + 1$.

Što se zna o kolineacijama (automorfizmima) klasične projektivne ravnine?

Točke i pravce ravnine $PG(2, q)$ shvaćamo kao jednodimenzionalne, odnosno dvodimenzionalne potprostore vektorskog prostora $V = GF(q)^3$. Regularni linearni operatori s V na V čuvaju potprostore, dimenziju i inkluziju, pa na prirodan način induciraju kolinearcije od $PG(2, q)$. Proporcionalni operatori na potprostore djeluju identično i induciraju istu kolineaciju. Zato grupa kolineacija koju dobivamo od regularnih linearnih operatora nije $GL(3, q)$, nego $PGL(3, q) = GL(3, q)/S^*$, gdje je S^* grupa skalarnih nenul matrica (to je centar grupe $GL(3, q)$). Kolineacije dobivene na taj način zovemo *homografijama* ili *projektivitetima*.

Zadatak: odredite red grupa $GL(3, q)$ i $PGL(3, q)$.

Rješenje. $|GL(3, q)| = (q^3-1)(q^3-q)(q^3-q^2) = q^3(q-1)^3(q+1)(q^2+q+1)$, $|PGL(3, q)| = |GL(2, q)|/(q - 1) = q^3(q - 1)^2(q + 1)(q^2 + q + 1)$. □

Projektiviteti nisu jedine kolineacije od $PG(2, q)$. Daljnje primjere dobivamo od automorfizama polja $GF(q)$. Kombiniranjem te dvije vrste kolineacija dolazimo do polulinearnih operatora na vektorskom prostoru V.

Definicija 2.29 *Za funkciju $A : V \to V$ kažemo da je* polulinearni operator *ako je aditivna i ako postoji automorfizam polja $\varphi \in \operatorname{Aut} GF(q)$ takav da je $A(\alpha x) = \alpha^{\varphi} A(x)$, za sve $x \in V$ i $\alpha \in GF(q)$. Ako je A bijekcija, kažemo da je* regularan.

Grupu regularnih polulinearnih operatora (s obzirom na kompoziciju) označavamo $\Gamma L(3, q)$. Kao i ranije, ona inducira grupu kolineacija izomorfnu s kvocijentom $\Gamma L(3, q)/S^* =: P\Gamma L(3, q)$.

Zadatak: kako dobivamo $\Gamma L(3,q)$ od $GL(3,q)$ i $\operatorname{Aut} GF(q)$ (i analogno za projektivne grupe)?

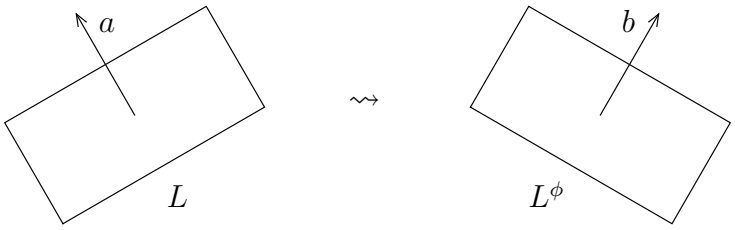
Rješenje. Kao semidirektni produkt: vrijedi $A(x^\varphi) = (A^{\varphi^{-1}}x)^\varphi$, za $x \in V$, $A \in GL(3,q)$ i $\varphi \in \operatorname{Aut} GF(q)$. Posebno, red tih grupa je $|\Gamma L(3,p^e)| = e \cdot |GL(3,p^e)|$ i $|P\Gamma L(3,p^e)| = e \cdot |PGL(3,p^e)|$. □

Teorem 2.30 (fundamentalni teorem projektivne geometrije) *$P\Gamma L(3,q)$ je puna grupa kolineacija projektivne ravnine $PG(2,q)$, tj. sve kolineacije klasične projektivne ravnine inducirane su regularnim polulinearnim operatorima.*

Dokaz ovog teorema može se naći u knjizi [10].

Kako možemo reprezentirati korelacije i polaritete klasične projektivne ravnine?

Kompozicija dviju korelacija je kolineacija. Prema tome, proizvoljnu korelaciju ρ dobivamo uzastopnim djelovanjem automorfizma polja $\varphi \in \operatorname{Aut} GF(q)$, regularne matrice $A \in GL(3,q)$ i očitog ortogonalnog polariteta. Točki od $PG(2,q)$ reprezentiranoj vektorom $x \in V$ (tj. jednodimenzionalnom potprostoru od V razapetom s x) pridružujemo pravac reprezentiran vektorom $A(x^\varphi)$, tj. dvodimenzionalni potprostor kojem je to "vektor normale". Da bismo vidjeli kako ρ djeluje na pravce, moramo proučiti kako djelovanje od A i φ utječe na vektore normala. Neka je ϕ kolineacija inducirana s A i φ.



Neka je $L < V$ dvodimenzionalni potprostor s vektorom normale a, tj. $a \cdot x = 0$, $\forall x \in L$. Neka je b vektor normale slike $L^\phi = \{A(x^\varphi) \mid x \in L\}$. Tada je $0 = b \cdot A(x^\varphi) = A^\tau b \cdot x^\varphi = (A^\tau b)^{\varphi^{-1}} \cdot x$, $\forall x \in L$, pa je vektor $(A^\tau b)^{\varphi^{-1}}$ proporcionalan s a. Slijedi da je b proporcionalan s $(A^\tau)^{-1}a^\varphi$. Dakle, korelacija ρ preslikava pravac reprezentiran vektorom a u točku reprezentiranu vektorom $(A^\tau)^{-1}a^\varphi$.

Korelacija je polaritet ako je involutorna, tj. $\rho^2 = id$. Da bi to vrijedilo, kompozicija $(A^\tau)^{-1} \circ \varphi \circ A \circ \varphi = (A^\tau)^{-1} \cdot A^\varphi \circ \varphi^2$ treba predstavljati identičnu

kolineaciju. To je ekvivalentno s činjenicom da je φ^2 identiteta na $GF(q)$, a $(A^\tau)^{-1} \cdot A^\varphi$ skalarna matrica. Imamo dvije mogućnosti: ili je φ identiteta na $GF(q)$, ili je φ involutorni automorfizam (konjugiranje).

U prvom slučaju A mora biti simetrična matrica. Polaritet ρ preslikava točku reprezentiranu s $x \in V$ u pravac reprezentiran s Ax, pa uvjet da bi točka bila apsolutna glasi $x \cdot Ax = 0$. Slično kao za očiti ortogonalni polaritet, pokazuje se da ρ ima $q+1$ apsolutnih točaka (dijagonalizacijom matrice A).

Drugi slučaj je moguć samo za polja kvadratnog reda (inače ne postoji involutorni automorfizam). Matrica A mora biti "hermitska", točnije mora vrijediti $(A^\tau)^\varphi = \alpha A$ za neki skalar α sa svojstvom $\alpha \cdot \alpha^\varphi = 1$. Množenjem A skalarom (što ne mijenja korelaciju koju predstavlja) može se postići da bude $\alpha = 1$, tj. da matrica A zaista bude hermitska. Dijagonalizacijom te matrice dobivamo uvjet za apsolutne točke sličan uvjetu za očiti unitarni polaritet. Pokazuje se da ga zadovoljava točno $q^{3/2}+1$ normaliziranih vektora, pa je ρ u ovom slučaju unitarni polaritet. Time je dokazan sljedeći teorem.

Teorem 2.31 *Ako q nije kvadrat, svi polariteti od $PG(2,q)$ su ortogonalni i mogu se reprezentirati simetričnim matricama $A \in GL(3,q)$. Ako je q kvadrat, osim takvih polariteta $PG(2,q)$ ima još samo unitarne polaritete reprezentirane hermitskim matricama $A \in GL(3,q)$ i konjugiranjem.*

Što možemo reći o automorfizmima klasičnog unitala?

BSOMP da je unital dobiven od očitog unitarnog polariteta ravnine $PG(2,q^2)$. Točke unitala, tj. apsolutne točke ravnine reprezentirane su vektorima $x \in V$ koji zadovoljavaju $x \cdot x^q = 0$, tzv. *izotropnim vektorima*. Promotrimo koje kolineacije ravnine $PG(2,q^2)$ čuvaju apsolutne točke. Neka je kolineacija ϕ reprezentirana automorfizmom polja φ i "unitarnom matricom" $A \in GL(3,q^2)$, koja zadovoljava $(A^q)^\tau \cdot A = \alpha I$ za neki $\alpha \in GF(q^2)^*$ (nije teško pokazati da je nužno $\alpha^q = \alpha$, tj. $\alpha \in GF(q)^*$). Ako je $x \in V$ izotropni vektor, tvrdimo da je tada i Ax^φ izotropan:

$$Ax^\varphi \cdot (Ax^\varphi)^q = Ax^\varphi \cdot A^q (x^\varphi)^q = (A^q)^\tau Ax^\varphi \cdot (x^\varphi)^q = \alpha x^\varphi \cdot (x^q)^\varphi = \alpha (x \cdot x^q)^\varphi = 0.$$

Kao i ranije, množenjem A nenul skalarom možemo postići da bude $\alpha = 1$, tj. da A zaista bude unitarna matrica, koja zadovoljava $(A^q)^\tau \cdot A = I$. Time ne gubimo općenitost jer proporcionalne matrice reprezentiraju istu kolineaciju.

Skup svih unitarnih matrica označavamo $GU(3,q^2)$ i zovemo *općom unitarnom grupom*. Odgovarajuće kolineacije dobivamo uzimanjem kvocijenta s njezinim centrom, koji je reda $q+1$ (kvocijentnu grupu označavamo $PGU(3,q^2)$).

Zadatak: $|GU(3,q^2)| = (q^3+1)q^3(q^2-1)(q+1)$, $|PGU(3,q^2)| = (q^3+1)q^3(q^2-1)$.

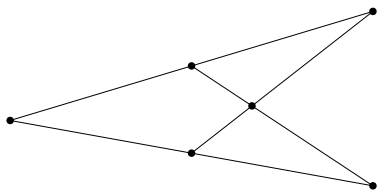
U [29, teorem 2.50] dokazano je da $PGU(3,q^2)$ djeluje dvostruko tranzitivno na apsolutne točke i da su stabilizatori parova apsolutnih točaka reda q^2-1. Iz toga direktno slijedi red te grupe.

Vidjeli smo da i kolineacije inducirane automorfizmima polja čuvaju apsolutne točke (budući da automorfizmi polja komutiraju s konjugiranjem). Odgovarajuće semidirektne produkte od $GU(3,q^2)$ i $PGU(3,q^2)$ s $\mathrm{Aut}\, GF(q^2)$ označavamo $\Gamma U(3,q^2)$ i $P\Gamma U(3,q^2)$.

Zadatak: $|\Gamma U(3,p^{2e})| = 2e(p^{3e}+1)p^{3e}(p^{2e}-1)(p^e+1)$, $|P\Gamma U(3,q^2)| = 2e(p^{3e}+1)p^{3e}(p^{2e}-1)$.

Propozicija 2.32 *Grupa $P\Gamma U(3,q^2)$ djeluje kao grupa automorfizama na klasičnom unitalu u projektivnoj ravnini $PG(2,q^2)$.*

To je podgrupa grupe kolineacija projektivne ravnine $PG(2,q^2)$ koje čuvaju apsolutne točke. Postavlja se pitanje jesu li to jedini automorfizmi klasičnog unitala, tj. je li $P\Gamma U(3,q^2)$ njegova puna grupa automorfizama? Michael O'Nan je u članku [36] dokazao da jest (članak je dio njegove doktorske disertacije). U istom članku O'Nan je dokazao da u klasičnom unitalu ne postoje konfiguracije od četiri pravca koji se sijeku u šest točaka:



Takve konfiguracije nazivamo *O'Nanovim* ili *Paschovim* konfiguracijama. Poznato je otvoreno pitanje jesu li klasični unitali jedini bez tih konfiguracija. Primjeri neklasičnih unitala $S(2,4,28)$ koje imam sadrže od 276 do 735 O'Nanovih konfiguracija, a neklasični unitali $S(2,5,65)$ od 4442 do 21760.

Domaća zadaća: dokažite ili opovrgnite: ako u unitalu nema O'Nanovih konfiguracija, onda je to klasični unital.

Projektni zadatak: dokaz da je $P\Gamma U(3,q^2)$ puna grupa automorfizama klasičnog unitala i da on ne sadrži O'Nanove konfiguracije (prikaz članka [36]).

Naučili smo dosta o polaritetima konačnih projektivnih ravnina. Netko bi mogao održati seminar o polaritetima konačnih struktura koje su generalizacije projektivnih ravnina i odgovarajućim generalizacijama unitala.

Projektni zadatak: polariteti i unitali simetričnih dizajna [34].

Projektni zadatak: polariteti eliptičkih poluravnina [3, 43].

3 Projektivni prostori i kvadrike

3.1 Projektivni prostori - analitički pristup

Neka je F polje, a V neka je $(d+1)$-dimenzionalni vektorski prostor nad F (npr. $V = F^{d+1}$). *Projektivni prostor* $PG(d, F)$ možemo definirati na sljedeći način:

- točke su jednodimenzionalni potprostori od V,
- k-dimenzionalni projektivni potprostori (k-ravnine) su $(k+1)$-dimenzionalni vektorski potprostori od V,
- incidencija je inkluzija $\subseteq$.

Jednodimenzionalne ravnine zovemo *pravcima*, a $(d-1)$-ravnine *hiperravninama*. Ako je F konačno polje $GF(q)$, projektivni prostor označavamo $PG(d, q)$. Tada točke i k-ravnine čine dizajn s parametrima 2-$(\frac{q^{d+1}-1}{q-1}, \frac{q^{k+1}-1}{q-1}, \lambda)$ za $\lambda = \frac{(q^{d-1}-1)(q^{d-2}-1)\cdots(q^{d-k+1}-1)}{(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)}$. Taj dizajn je Steinerov za $k = 1$ (kroz svake dvije točke prolazi jedinstveni pravac), a simetričan za $k = d-1$ (hiperravnina ima jednako mnogo kao točaka).

3.2 Projektivni prostori - sintetički pristup

Projektivnu ravninu možemo definirati kao incidencijsku strukturu (točke, pravci, incidencija) koja zadovoljava sljedeće aksiome:

(P_1) kroz svake dvije točke prolazi jedinstveni pravac,

(P_2) svaka dva pravca sijeku se u jedinstvenoj točki,

(P_3) aksiom nedegeneriranosti, npr. postojanje četiri točke od kojih nikoje tri nisu kolinearne, ili zahtjev da na svakom pravcu leže bar tri točke i da postoje bar dva pravca.

U konačnom slučaju može se dokazati da postoji prirodan broj $n \geq 2$ (*red* ravnine) takav da na svakom pravcu leži $n+1$ točaka i kroz svaku točku prolazi $n+1$ pravaca, a ukupan broj točaka i pravaca je n^2+n+1. To znači da su konačne projektivne ravnine 2-$(n^2+n+1, n+1, 1)$ dizajni (tako smo ih definirali u prvom poglavlju). Sve poznate projektivne ravnine imaju red koji je prim potencija, ali *nisu* sve izomorfne klasičnoj projektivnoj ravnini $PG(2,q)$!
Aksiomi projektivnog prostora dobivaju se oslabljivanjem zahtjeva (P_2), tj. zamjenom s Veblen-Youngovim aksiomom:

(P_2') za svake tri točke A, B, C, ako neki pravac siječe pravce AB i AC (tako da nisu oba sjecišta A), onda on siječe i pravac BC.

U projektivnoj ravnini to je ispunjeno jer se svaka dva pravca sijeku. Općenito mogu postojati pravci koji se ne sijeku – zovemo ih *mimoilaznim* ili *mimosmjernim* pravcima (u projektivnoj geometriji nema paralelnih pravaca!).

Vrijedi li Veblen-Youngov aksiom u analitičkom modelu $PG(d,F)$?

Definicija 3.1 Ravnina *ili* linearni skup *je svaki skup točaka $\mathcal{R}$ sa svojstvom da za svake dvije točke $A, B \in \mathcal{R}$ sadrži i sve točke pravca AB.*

Trivijalni primjeri ravnina su jednočlani skupovi (0-ravnine) i cijeli prostor. Za bilo koji skup točaka $\mathcal{S}$ definiramo *ravninu razapetu sa $\mathcal{S}$* (oznaka: $\langle \mathcal{S} \rangle$) kao presjek svih ravnina koje sadrže $\mathcal{S}$. Da bismo dobili konačnodimenzionalne projektivne prostore treba nam sljedeći aksiom:

(P_4) postoji konačan skup točaka koji razapinje cijeli prostor.

Dokazi teorema u nastavku nalaze se u knjizi [10].

Teorem 3.2 *Neka je $\mathcal{R}$ ravnina i T točka koja joj ne pripada. Tada je $\langle \mathcal{R}, T \rangle = \bigcup_{R \in \mathcal{R}} (TR)$, pri čemu (TR) označava skup svih točaka na pravcu TR.*

Teorem 3.3 (svojstvo zamjene) *Neka je $\mathcal{R}$ ravnina i T točka koja joj ne pripada. Ako je $S \in \langle \mathcal{R}, T \rangle \setminus \mathcal{R}$, onda je $T \in \langle \mathcal{R}, S \rangle \setminus \mathcal{R}$. Tada vrijedi $\langle \mathcal{R}, T \rangle = \langle \mathcal{R}, S \rangle$.*

Definicija 3.4 *Za skup točaka $\mathcal{S}$ kažemo da je* nezavisan *ako za svaku točku $T \in \mathcal{S}$ vrijedi $T \notin \langle \mathcal{S} \setminus \{T\} \rangle$. Nezavisan skup točaka koji razapinje cijeli prostor zovemo* bazom.

Teorem 3.5 *Neka je $\mathcal{S}$ konačan skup točaka koji razapinje cijeli prostor. Onda postoji podskup $\mathcal{B} \subseteq \mathcal{S}$ koji je baza. Posebno, projektivni prostor ima konačnu bazu.*

Lema 3.6 *Neka je $\mathcal{S}$ konačan nezavisan skup točaka i neka su $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{S}$ njegovi podskupovi. Onda vrijedi $\langle \mathcal{S}_1 \cap \mathcal{S}_2 \rangle = \langle \mathcal{S}_1 \rangle \cap \langle \mathcal{S}_2 \rangle$.*

Lema 3.7 *Neka je $\mathcal{B}$ konačna baza i T bilo koja točka projektivnog prostora. Onda postoji točka $B \in \mathcal{B}$ takva da je $(\mathcal{B} \setminus \{B\}) \cup \{T\}$ također baza.*

Teorem 3.8 (Steinitzov teorem zamjene) *Neka je $\mathcal{B}$ konačna baza projektivnog prostora koja sadrži r točaka. Ako je $\mathcal{S}$ nezavisan skup koji sadrži s točaka, onda je $s \leq r$ i postoji $(r-s)$-člani podskup $\mathcal{B}' \subseteq \mathcal{B}$ takav da je $\mathcal{S} \cup \mathcal{B}'$ baza.*

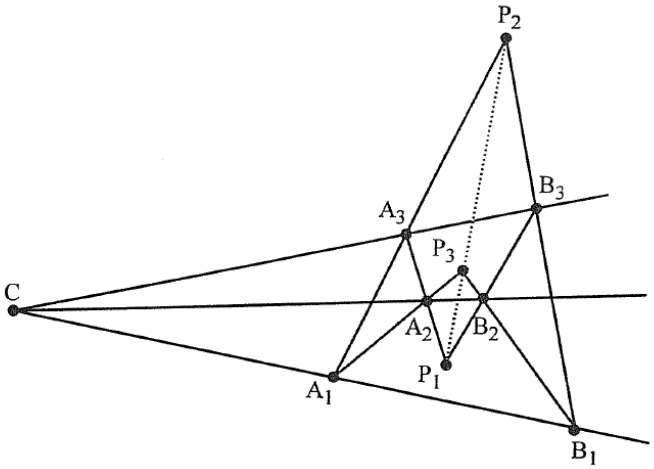
Korolar 3.9 *Svake dvije baze projektivnog prostora imaju jednako mnogo elemenata. Svaki nezavisni skup može se nadopuniti do baze.*

Definicija 3.10 *Ako je $d+1$ broj elemenata bilo koje baze, kažemo da je d* dimenzija *projektivnog prostora $\mathcal{P}$ i pišemo $d = \dim \mathcal{P}$.*

Lema 3.11 *Neka je $\mathcal{R}$ ravnina projektivnog prostora $\mathcal{P}$. Onda je $\dim \mathcal{R} \leq \dim \mathcal{P}$, a jednakost vrijedi ako i samo ako je $\mathcal{R} = \mathcal{P}$.*

Lema 3.12 *Za svake dvije ravnine $\mathcal{R}_1$, $\mathcal{R}_2$ vrijedi formula $\dim\langle \mathcal{R}_1, \mathcal{R}_2 \rangle = \dim \mathcal{R}_1 + \dim \mathcal{R}_2 - \dim(\mathcal{R}_1 \cap \mathcal{R}_2)$.*

Teorem 3.13 *U svakom projektivnom prostoru dimenzije $d \geq 3$ vrijedi Desarguesov teorem: za bilo koje točke A_1, A_2, A_3 i B_1, B_2, B_3 takve da pravci A_1B_1, A_2B_2, A_3B_3 prolaze kroz neku točku C (i pritom je $C \neq A_i \neq B_i \neq C$, $i = 1,2,3$ te nikoje tri od točaka C, A_1, A_2, A_3 ili C, B_1, B_2, B_3 nisu kolinearne), točke $P_1 = A_2A_3 \cap B_2B_3$, $P_2 = A_1A_3 \cap B_1B_3$ i $P_3 = A_1A_2 \cap B_1B_2$ leže na jednom pravcu.*

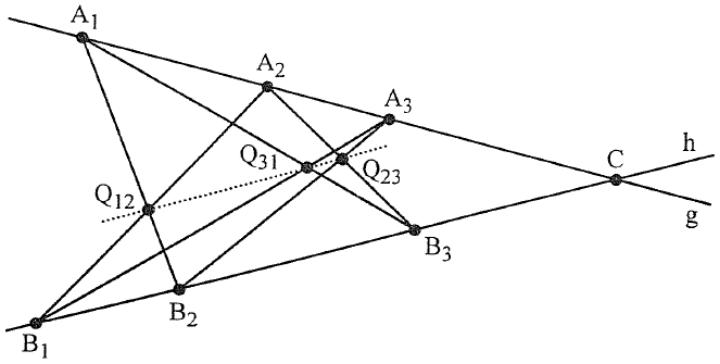


Postoje projektivne ravnine (tj. projektivni prostori dimenzije $d = 2$) u kojima ne vrijedi Desarguesov teorem!

Teorem 3.14 *Neka je $\mathcal{P}$ projektivni prostor dimenzije $d \geq 2$ u kojem vrijedi Desarguesov teorem. Onda postoji tijelo F takvo da je $\mathcal{P}$ izomorfan s $PG(d, F)$.*

Korolar 3.15 *Svaki projektivni prostor dimenzije $d \geq 3$ izomorfan je s $PG(d, F)$ za neko tijelo F.*

Prvenstveno nas zanimaju konačni projektivni prostori, a poznato je da su sva konačna tijela zapravo polja (Wedderburnov teorem). Zato smo se ograničili na taj slučaj. Općenito, projektivni prostori nad poljima karakterizirani su Paposovim teoremom. Desarguesov teorem govori o univerzalnom zatvaranju određene (10_3) konfiguracije, a Paposov teorem o zatvaranju (9_3) konfiguracije:



(slike za Desarguesov i Paposov teorem preuzete su iz knjige [10]). Budući da je polje specijalni slučaj tijela u kojem je množenje komutativno, očito Paposov teorem implicira Desarguesov, ali to nije baš jednostavno dokazati direktno (Hessenbergov teorem).

Afini d-dimenzionalni prostor $\mathcal{A} = AG(d, F)$ dobiva se od projektivnog prostora $\mathcal{P} = PG(d, F)$ brisanjem "hiperravnine u beskonačnosti" H_∞. Točke od $\mathcal{A}$ su točke od $\mathcal{P}$ koje ne pripadaju H_∞. Pravci od $\mathcal{A}$ su pravci od $\mathcal{P}$ koji ne leže u H_∞. Općenito, k-ravnine od $\mathcal{A}$ su k-ravnine od $\mathcal{P}$ koji ne leže u H_∞. Incidencija u $\mathcal{A}$ je naslijeđena iz $\mathcal{P}$. Tako dobiveni prostor $AG(d, F)$ izomorfan je afinom prostoru definiranom na način na koji smo naviknuti, u kojem su točke elementi vektorskog prostora $V = F^d$, a k-ravnine translati k-dimenzionalnih potprostora od V ("linearne mnogostrukosti").

Za $d = 2$, konstrukcija brisanja pravca u beskonačnosti funkcionira i u nedesarguesovim projektivnim ravninama, ali tada nije svejedno koji pravac izaberemo. Brisanjem različitih pravaca možemo dobiti neizomorfne afine ravnine.

3.3 Kvadrike - analitički pristup

Definicija 3.16 Kvadrika *u* $PG(d, F)$ *je skup točaka čije homogene koordinate zadovoljavaju danu homogenu jednadžbu stupnja* 2*. Ako se ta jednadžba promjenom baze može svesti na manje od* $d + 1$ *varijabli, kažemo da je kvadrika* singularna *ili* degenerirana*. U suprotnom kažemo da je* nesingularna*,* nedegenerirana *ili* ireducibilna*.*

Ako je F polje realnih brojeva, kvadrika može biti prazna. Zanimaju nas prvenstveno kvadrike nad konačnim poljima, koje su uvijek neprazne.

Za $d = 2$ kvadrike zovemo *konikama* (*krivljama drugog reda*). Ireducibilna konika u $PG(2, q)$ je jedinstvena do na promjenu baze. Jednadžba se može svesti na kanonski oblik $x_1^2 - x_0x_2 = 0$. To je zgodnije od oblika $x_0^2 + x_1^2 + x_2^2 = 0$ koji smo susreli u poglavlju 2.4, jer možemo eksplicitno napisati normalizirane vektore koji zadovoljavaju kanonsku jednadžbu: $\{(0, 0, 1)\} \cup \{(1, t, t^2) \mid t \in GF(q)\}$. Znamo da je to oval, tj. skup od $q + 1$ točaka od kojih nikoje tri nisu kolinearne. Kroz svaku točku konike prolazi jedinstvena tangenta. Za neparan q kroz točke izvan konike prolazi 0 ili 2 tangente; u prvom slučaju točku nazivamo *unutrašnjom*, a u drugom *vanjskom*. Prema tome, ireducibilna konika u $PG(2, q)$ je za neparan q slična elipsi u euklidskoj ravnini $\mathbb{R}^2$. Međutim, za paran q sve tangente prolaze kroz točku $N = (0, 1, 0)$, koju zovemo *jezgrom* (eng. *nucleus*).

Kako svodimo jednadžbe na kanonski oblik?

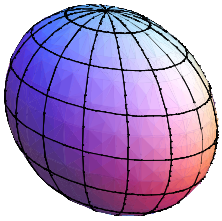
Postoje tri vrste degeneriranih konika u projektivnoj ravnini $PG(2, q)$: par pravaca (kanonska jednadžba $x_0x_1 = 0$), pravac (kanonska jednadžba $x_0^2 = 0$) i točka. Kanonska jednadžba točke je $x_0^2 + bx_0x_1 + cx_1^2 = 0$, pri čemu je na lijevoj strani *ireducibilna kvadratna forma* u dvije varijable. To znači da je $x^2 + bx + c$ ireducibilni kvadratni polinom (tj. da nema nultočaka u $GF(q)$).

U trodimenzionalnom projektivnom prostoru $PG(3, q)$ postoje dvije vrste nedegeneriranih kvadrika: *eliptička kvadrika* s kanonskom jednadžbom $f(x_0, x_1) + x_2x_3 = 0$ (f je ireducibilna kvadratna forma) i *hiperbolička kvadrika* s kanonskom jednadžbom $x_0x_1 + x_2x_3 = 0$.

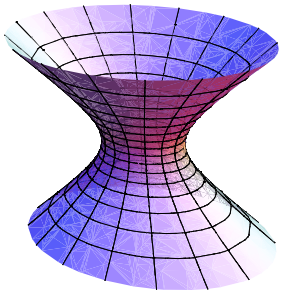
Eliptička kvadrika sastoji se od $q^2 + 1$ točaka i donekle podsjeća na euklidski elipsoid. Kroz svaku njezinu točku prolazi jedinstvena *tangencijalna ravnina*, koja siječe eliptičku kvadriku samo u toj točki. Sve ostale ravnine (tj. dvodimenzionalni projektivni potprostori od $PG(3, q)$) sijeku eliptičku kvadriku u ireducibilnoj konici. Zovemo ih *sekantnim ravninama*. Za razliku od euklidskog elipsoida, ne postoje ravnine koje uopće ne sijeku eliptičku kvadriku.

Hiperbolička kvadrika sastoji se od $(q+1)^2$ točaka, a ravnine je sijeku u ireducibilnoj konici ili u paru pravaca. U prvom slučaju ravninu zovemo *sekantnom*, a u drugom slučaju *tangentnom*. Hiperbolička kvadrika je *pravčasta ploha* - kroz svaku njezinu točku prolaze dva pravca koja su cijela sadržana u kvadrici. To svojstvo kasnije ćemo detaljnije proučiti.

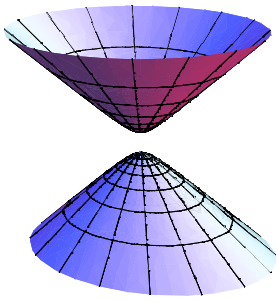
Sjetimo se da u realnom afinom trodimenzionalnom prostoru postoji pet vrsta nedegeneriranih kvadrika:



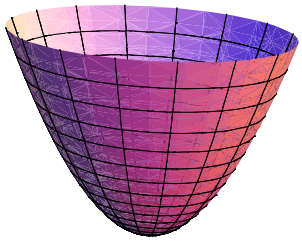
Elipsoid



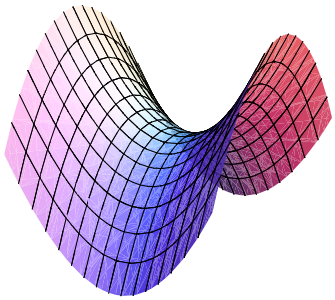
Jednoplohni hiperboloid



Dvoplohni hiperboloid



Eliptički paraboloid



Hiperbolički paraboloid

Zadatak: koje afine kvadrike dobivamo od eliptičke kvadrike, a koje od hiperboličke kvadrike "brisanjem" ravnina u različitim položajima prema kvadrici?

Zadatak: zadana su tri pravca u prostoru od kojih su svaka dva mimoilazna. Promotrimo familiju pravaca koji sijeku sva tri zadana pravca. Koju plohu tvore točke na toj familiji pravaca?

U projektivnom prostoru $PG(3,q)$ postoji četiri tipa degeneriranih kvadrika: pravac (kanonska jednadžba $f(x_0,x_1) = 0$, gdje je f ireducibilna

kvadratna forma), ravnina (kanonska jednadžba $x_0^2 = 0$), dvije ravnine koje se sijeku u pravcu (kanonska jednadžba $x_0x_1 = 0$) i *kvadratni konus* s kanonskom jednadžbom $x_1^2 - x_0x_2 = 0$. Riječ je skupu točaka na pravcima koji spajaju točku $(0, 0, 0, 1)$ (*vrh* konusa) s točkama na ireducibilnoj konici (*bazom* konusa) u ravnini $x_3 = 0$.

Kvadratne konuse možemo definirati općenitije, u bilo kojem projektivnom prostoru $PG(d, F)$. Neka su Π_1 i Π_2 disjunktne ravnine (projektivni potprostori) i neka je $\mathcal{Q}$ nedegenerirana kvadrika u Π_2. *Kvadratni konus* s vrhom Π_1 i bazom $\mathcal{Q}$ je skup točaka na pravcima koji spajaju točke iz Π_1 s točkama iz $\mathcal{Q}$.

Više informacija o kvadrikama u konačnim projektivnim prostorima, uključujući izvode kanonskih jednadžbi u svim slučajevima, može se pronaći u knjizi [27]. U uvodu knjige [7] obrađene su još i kvadrike u četverodimenzionalnom projektivnom prostoru $PG(4, q)$, posebno *eliptički konus*. Njemu je baza eliptička kvadrika u trodimenzionalnom projektivnom potprostoru, a vrh točka izvan tog potprostora. Vratit ćemo mu se kad nam bude potreban.

Projektni zadatak: izvodi kanonskih jednadžbi i svojstva kvadrika u $PG(4, q)$.

3.4 Kvadrike - sintetički pristup

Kvadrike su sintetički proučavane tek u 70-tim godinama prošlog stoljeća. Francis Buekenhout uveo je pojam *kvadratnog skupa* u projektivnom prostoru. Definicije i teoremi iz ove cjeline preuzeti su iz knjige [10] i tamo se mogu naći dokazi. U nastavku, neka je $\mathcal{Q}$ skup točak d-dimenzionalnog projektivnog prostora $\mathcal{P}$.

Definicija 3.17 *Za pravac kažemo da je* tangenta *na $\mathcal{Q}$ ako ga siječe samo u jednoj točki T, ili ako je cijeli sadržan u $\mathcal{Q}$. U prvom slučaju kažemo da je taj pravac tangenta na $\mathcal{Q}$* u točki *T.*

Pravce sadržane u $\mathcal{Q}$ zovemo još i $\mathcal{Q}$-pravcima. Općenitije, projektivni potprostor $\mathcal{R}$ od $\mathcal{P}$ zovemo *$\mathcal{Q}$-potprostorom* ako su sve točke iz $\mathcal{R}$ sadržane u $\mathcal{Q}$.

Definicija 3.18 *Za točku $T \in \mathcal{Q}$ definiramo* tangencijalni prostor *$\mathcal{Q}_T$ kao skup koji se sastoji od točke T i svih točaka X takvih da je XT tangenta na $\mathcal{Q}$.*

Tangencijalni prostor općenito ne mora biti potprostor od $\mathcal{P}$. Naprimjer, ako je $\mathcal{Q} = \{T_1, T_2\}$ dvočlan skup, $\mathcal{Q}_{T_1}$ i $\mathcal{Q}_{T_2}$ se sastoje od svih točaka od $\mathcal{P}$ osim točaka na spojnici T_1T_2, a to nije potprostor. No nas zanimaju samo specijalni skupovi $\mathcal{Q}$, za koje je $\mathcal{Q}_T$ uvijek potprostor.

Definicija 3.19 *Za $\mathcal{Q}$ kažemo da je* kvadratni skup *u $\mathcal{P}$ ako zadovoljava sljedeće aksiome:*

1. *za svaki $T \in \mathcal{Q}$, tangencijalni prostor $\mathcal{Q}_T$ je hiperravnina ili cijeli $\mathcal{P}$,*
2. *ako pravac ima tri zajedničke točke s $\mathcal{Q}$, onda je cijeli sadržan u $\mathcal{Q}$.*

Dakle, osim aksioma o tangencijalnim prostorima, za kvadratne skupove zahtijevamo da ih svi pravci koji nisu u njima sadržani sijeku u 0, 1 ili 2 točke.

Primjeri kvadratnih skupova su potprostori od $\mathcal{P}$. Oni po definiciji 3.1 sadrže sve pravce koji s njima imaju dvije zajedničke točke. Nadalje, ako je $\mathcal{Q}$ potprostor, onda je $\mathcal{Q}_T$ uvijek cijeli prostor $\mathcal{P}$: pravci kroz T su ili sadržani u $\mathcal{Q}$, ili ga sijeku samo u T, pa su svi tangente.

Manje trivijalan primjer kvadratnog skupa je unija dviju hiperravnina, $\mathcal{Q} = H_1 \cup H_2$. Za točke $T \in H_1 \cap H_2$ je $\mathcal{Q}_T$ cijeli $\mathcal{P}$. Ako je pak $T \in H_1 \setminus (H_1 \cap H_2)$ (ili $T \in H_2 \setminus (H_1 \cap H_2)$), onda je $\mathcal{Q}_T = H_1$ (ili $\mathcal{Q}_T = H_2$).

Oba spomenuta primjera su degenerirane kvadrike. Ovali u projektivnim ravninama (posebno, ireducibilna konika u $PG(2, q)$) također očito zadovoljavaju aksiome kvadratnog skupa. Za nedegenerirane kvadrike i kvadratni konus u $PG(3, q)$ nije baš očito. U poglavlju 4.7 knjige [10] dokazano je da svaka kvadrika zadovoljava aksiome kvadratnog skupa.

Definicija 3.20 Radikal *kvadratnog skupa $\mathcal{Q}$ je skup* $\operatorname{rad}\mathcal{Q}$ *svih točaka $T \in \mathcal{Q}$ takvih da je $\mathcal{Q}_T$ cijeli prostor. Ako je* $\operatorname{rad}\mathcal{Q} = \emptyset$*, kažemo da je $\mathcal{Q}$* nedegeneriran.

Nije teško provjeriti da degenerirane kvadrike u smislu definicije 3.16 imaju neprazan radikal, tj. da su degenerirane i u smislu prethodne definicije. Pretpostavimo da je kvadrika $\mathcal{Q}$ zadana jednadžbom u kojoj nedostaje prva varijabla x_0. Onda točka s homogenim koordinatama $(1, 0, \ldots, 0)$ očito zadovoljava jednadžbu i pripada kvadrici $\mathcal{Q}$. Tvrdimo da je svaki pravac kroz tu točku tangenta na $\mathcal{Q}$. Neka takav pravac siječe $\mathcal{Q}$ u još jednoj točki $(x_0, x_1, \ldots, x_d)$. Projektivni pravac kroz te dvije točke je dvodimenzionalni potprostor razapet s odgovarajućim vektorima; sastoji se od vektora oblika $(\alpha x_0 + \beta, \alpha x_1, \ldots, \alpha x_d)$. Oni svi zadovoljavaju jednadžbu kvadrike jer je homogena i ne ovisi o prvoj varijabli. Dakle, promatrani pravac leži u $\mathcal{Q}$, pa je tangenta.

Za obrat bismo trebali pokazati da se svaka kvadrika s nepraznim radikalom može zadati homogenom kvadratnom jednadžbom s manje od $d+1$ varijabli. Pomoći će nam sljedeći teorem.

Lema 3.21 *Neka je $\mathcal{Q}$ kvadratni skup, a $\mathcal{R}$ potprostor projektivnog prostora $\mathcal{P}$. Onda je $\mathcal{Q}' = \mathcal{Q} \cap \mathcal{R}$ kvadratni skup u $\mathcal{R}$ i za svaku točku $T \in \mathcal{Q}'$ vrijedi $\mathcal{Q}'_T = \mathcal{Q}_T \cap \mathcal{R}$.*

Teorem 3.22 *Neka je $\mathcal{Q}$ kvadratni skup u projektivnom prostoru $\mathcal{P}$.*

(a) *Radikal od $\mathcal{Q}$ je potprostor od $\mathcal{P}$.*

(b) *Neka je $\mathcal{R}$ direktni komplement od* $\operatorname{rad}\mathcal{Q}$*, tj. potprostor od $\mathcal{P}$ takav da je $\mathcal{R}\cap\operatorname{rad}\mathcal{Q}=\emptyset$ i $\langle\mathcal{R},\operatorname{rad}\mathcal{Q}\rangle=\mathcal{P}$. Onda je $\mathcal{Q}'=\mathcal{Q}\cap\mathcal{R}$ nedegenerirani kvadratni skup u $\mathcal{R}$.*

(c) *$\mathcal{Q}$ je konus s vrhom* $\operatorname{rad}\mathcal{Q}$ *i bazom $\mathcal{Q}'$, tj. sastoji se od točaka koje leže na spojnicama VT, za $V\in\operatorname{rad}\mathcal{Q}$ i $T\in\mathcal{Q}'$.*

Ako imamo kvadriku s nepraznim radikalom, možemo uzeti bazu od $\operatorname{rad}\mathcal{Q}$ i nadopuniti je do baze cijelog prostora. U toj bazi jednadžba kvadrike neće ovisiti o varijablama koje odgovaraju elementima baze iz radikala.

Zbog prethodnog teorema dovoljno je proučavati nedegenerirane kvadratne skupove. Svi njihovi tangencijalni prostori su hiperravnine, a pridruživanje $T\mapsto\mathcal{Q}_T$ je injektivno:

Lema 3.23 *Neka je $\mathcal{Q}$ nedegenerirani kvadratni skup. Ako su $T_1,T_2\in\mathcal{Q}$ različite točke, onda je $\mathcal{Q}_{T_1}\neq\mathcal{Q}_{T_2}$.*

Iz toga slijedi da se radikal kvadratnog skupa dobivenog kao presjek od $\mathcal{Q}$ s tangencijalnim prostorom $\mathcal{Q}_T$ sastoji samo od točke T. Kvadratni skupovi dobiveni kao presjek s ostalim hiperravninama su nedegenerirani.

Lema 3.24 *Neka je $\mathcal{Q}$ nedegenerirani kvadratni skup.*

(a) *Ako je $\mathcal{R}$ hiperravnina koja nije tangencijalna na $\mathcal{Q}$, onda je $\mathcal{Q}'=\mathcal{Q}\cap\mathcal{R}$ nedegenerirani kvadratni skup u $\mathcal{R}$.*

(b) *Ako je $T\in\mathcal{Q}$ i $\mathcal{R}$ direktni komplement od T u $\mathcal{Q}_T$, onda je $\mathcal{Q}'=\mathcal{Q}\cap\mathcal{R}$ nedegenerirani kvadratni skup u $\mathcal{R}$.*

Definicija 3.25 *Neka $\mathcal{Q}$ kvadratni skup i $t-1$ maksimalna dimenzija $\mathcal{Q}$-potprostora. Onda broj t zovemo* indeksom *od $\mathcal{Q}$, a $\mathcal{Q}$-potprostore dimenzije $t-1$* maksimalnim $\mathcal{Q}$-potprostorima.

Naprimjer, eliptička kvadrika u $PG(3,q)$ je indeksa 1 jer ne sadrži pravce, a hiperboločka kvadrika indeksa 2 jer sadrži pravce i ne sadrži ravnine.

Lema 3.26 *Neka je $\mathcal{Q}$ kvadratni skup indeksa t u $\mathcal{P}$. Kroz svaku točku od $\mathcal{Q}$ prolazi maksimalni $\mathcal{Q}$-potprostor. Točnije, neka je $T\in\mathcal{Q}$ točka i $\mathcal{M}$ maksimalni $\mathcal{Q}$-potprostor (dimenzije $t-1$) koji nisu incidentni. Onda postoji maksimalni $\mathcal{Q}$-potprostor $\mathcal{M}'$ kroz T koji siječe $\mathcal{M}$ u $(t-2)$-dimenzionalnom $\mathcal{Q}$-potprostoru.*

Posebno, na hiperboličkoj kvadrici $\mathcal{H}$ u $PG(3,q)$ kroz svaku točku T i $\mathcal{H}$-pravac p koji nisu incidentni, postoji $\mathcal{H}$-pravac p' kroz T koji siječe p.

Lema 3.27 *Neka je $\mathcal{Q}$ kvadratni skup i $\mathcal{S}$ njegov podskup sa svojstvom da je spojnica bilo koje dvije točke iz $\mathcal{S}$ $\mathcal{Q}$-pravac. Tada je $\langle\mathcal{S}\rangle$ $\mathcal{Q}$-potprostor.*

Teorem 3.28 *Neka je $\mathcal{Q}$ nedegenerirani kvadratni skup u projektivnom prostoru $\mathcal{P}$. Za svaki maksimalni $\mathcal{Q}$-potprostor $\mathcal{M}$ postoji maksimalni $\mathcal{Q}$-potprostor $\mathcal{M}'$ koji je mimoilazan s $\mathcal{M}$.*

Teorem 3.29 *Neka je $\mathcal{Q}$ nedegenerirani kvadratni skup indeksa t u d-dimenzionalnom projektivnom prostoru $\mathcal{P}$. Ako je d paran, onda je $t \leq d/2$; ako je d neparan, onda je $t \leq (d+1)/2$.*

U dosadašnjem razmatranju $\mathcal{P}$ je bio projektivni prostor nad bilo kojim poljem F. Sada se ograničavamo na konačni slučaj $F = GF(q)$ (odnosno $\mathcal{P} = PG(d,q)$). Tada imamo samo tri mogućnosti za indeks kvadratnog skupa $\mathcal{Q}$.

Lema 3.30 *Za točku $T \in \mathcal{Q} \setminus \operatorname{rad}\mathcal{Q}$, označimo s a broj $\mathcal{Q}$-pravaca kroz T.*

(a) Tangencijalna hiperravnina $\mathcal{Q}_T$ sadrži točno $aq+1$ točaka iz $\mathcal{Q}$.

(b) Vrijedi $|\mathcal{Q}| = 1 + q^{d-1} + aq$; posebno, a ne ovisi o izboru točke $T \in \mathcal{Q} \setminus \operatorname{rad}\mathcal{Q}$.

Teorem 3.31 *Neka je $\mathcal{Q}$ nedegeneriran kvadratni skup indeksa t u projektivnom prostoru $\mathcal{P} = PG(d,q)$. Ako je d paran, onda je $t = d/2$; ako je d neparan, onda je $t = (d-1)/2$ ili $t = (d+1)/2$.*

Kvadratni skupovi tih triju indeksa igraju važnu ulogu i u beskonačnim projektivnim prostorima, a ne samo u konačnim (gdje su to jedini mogući indeksi nedegeneriranog skupa).

Definicija 3.32 *Neka je $\mathcal{Q}$ nedegeneriran kvadratni skup u projektivnom prostoru $\mathcal{P} = PG(d,F)$. Ako je d paran i $\mathcal{Q}$ indeksa $d/2$, kažemo da je $\mathcal{Q}$* parabolički *kvadratni skup. Ako je d neparan, a $\mathcal{Q}$ indeksa $(d-1)/2$, odnosno $(d+1)/2$, kažemo da je $\mathcal{Q}$* eliptički*, odnosno* hiperbolički *kvadratni skup.*

Ireducibilna konika i, općenitije, ovali u projektivnoj ravnini $PG(2,q)$ su parabolički kvadratni skupovi. Sada znamo da i u četverodimenzionalnom prostoru $PG(4,q)$ postoji samo jedan tip nedegeneriranog kvadratnog skupa.

U trodimenzionalnom prostoru $PG(3,q)$ eliptičke i hiperboličke kvadrike su primjeri nedegeneriranih kvadratnih skupova, ali u eliptičkom slučaju ipak nisu jedini primjeri.

Definicija 3.33 *Za skup točaka $\mathcal{O}$ projektivnog prostora $\mathcal{P} = PG(d, F)$ kažemo da je* ovoid *ako nikoje tri točke iz $\mathcal{O}$ nisu kolinearne te za svaku točku $T \in \mathcal{O}$ tangente kroz T čine hiperravninu u $\mathcal{P}$.*

Ovali su ovoidi u ravnini $PG(2, q)$. Po definiciji 2.23 sadrže $q + 1$ točaka, pa kroz svaku točku ovala prolazi jedna tangenta, a to je hiperravnina u $PG(2, q)$. Vrijedi i obrat, tj. ovoidi u ravnini su ovali prema definiciji 2.23. Prema Segreovom teoremu za $d = 2$ i za neparan q ireducibilne konike su jedini ovali. Za paran q postoje ovali koji nisu konike, a za $d = 3$ postoje ovoidi koji nisu kvadrike.

Primjeri takvih ovala i ovoida?

Prema fundamentalnom teoremu Buekenhouta [18], svaki nedegenerirani kvadratni skup je kvadrika ili ovoid.

Projektni zadatak: kvadratni skupovi u $PG(d, q)$ (dokazi teorema iz ove cjeline).

4 Buekenhoutovi unitali

4.1 Regulusi i spreadovi u $PG(3, q)$

Kako prevesti 'regulus' i 'spread' na hrvatski?

Potprostori projektivnog prostora $\mathcal{P}$ koji se ne sijeku nazivaju se *mimoilaznim*. Ako imamo skup međusobno mimoilaznih potprostora, pravac nazivamo *transverzalom* tog skupa ako svaki od potprostra siječe točno u jednoj točki.

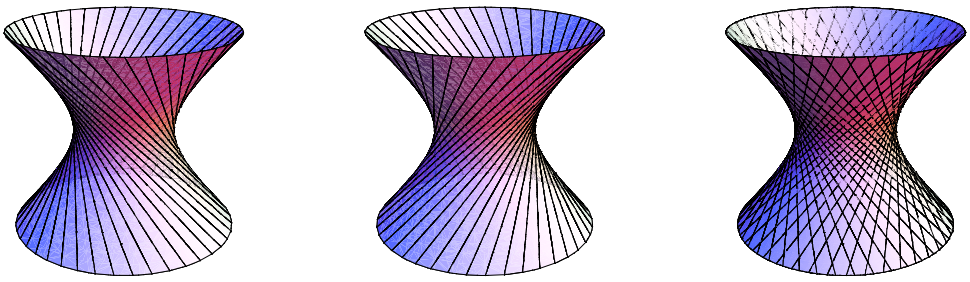
Lema 4.1 *Neka su p_1 i p_2 mimoilazni pravci i T točka koja im ne pripada. Tada postoji najviše jedna transverzala tih dvaju pravaca koja prolazi kroz T. Ako je $\mathcal{P}$ trodimenzionalan, onda postoji točno jedna takva transverzala.*

Teorem 4.2 (teorem 16 točaka, Dandelinov teorem) *Neka je $\mathcal{P} = PG(3, F)$ trodimenzionalni projektivni prostor nad tijelom F. Neka su $\{p_1, p_2, p_3\}$ i $\{q_1, q_2, q_3\}$ skupovi mimoilaznih pravaca takvi da se svaki od pravaca p_i siječe sa svakim od pravaca q_j. Tijelo F je komutativno (tj. polje) ako i samo ako se svaka transverzala p od $\{q_1, q_2, q_3\}$ siječe sa svakom transverzalom q od $\{p_1, p_2, p_3\}$.*

Definicija 4.3 *Neka je $\mathcal{P}$ trodimenzionalni projektivni prostor. Skup mimoilaznih pravaca $\mathcal{R}$ zovemo* regulus *ako vrijedi:*

- *kroz svaku točku na svakom pravcu iz $\mathcal{R}$ prolazi transverzala od $\mathcal{R}$,*
- *kroz svaku točku na svakoj transverzali od $\mathcal{R}$ prolazi pravac iz $\mathcal{R}$.*

Ako je $\mathcal{R}$ regulus, skup $\mathcal{R}'$ svih transverzala od $\mathcal{R}$ je također regulus, koji nazivamo *suprotnim regulusom* od $\mathcal{R}$. U konačnom slučaju, kad je $\mathcal{P} = PG(3, q)$, transverzala od $\mathcal{R}$ sadrži $q + 1$ točaka. Kroz svaku od tih točaka prolazi pravac od $\mathcal{R}$ i to su svi pravci iz $\mathcal{R}$, pa se regulus sastoji od $q + 1$ pravaca.



Teorem 4.4 *Neka je $\mathcal{P} = PG(3, F)$ trodimenzionalni projektivni prostor nad tijelom F i p_1, p_2, p_3 tri mimoilazna pravca iz $\mathcal{P}$.*

(a) Postoji najviše jedan regulus koji sadrži p_1, p_2 i p_3.

(b) Ako F nije polje, onda ne postoji regulus u $\mathcal{P}$.

(c) Ako je F polje, onda postoji točno jedan regulus koji sadrži p_1, p_2 i p_3.

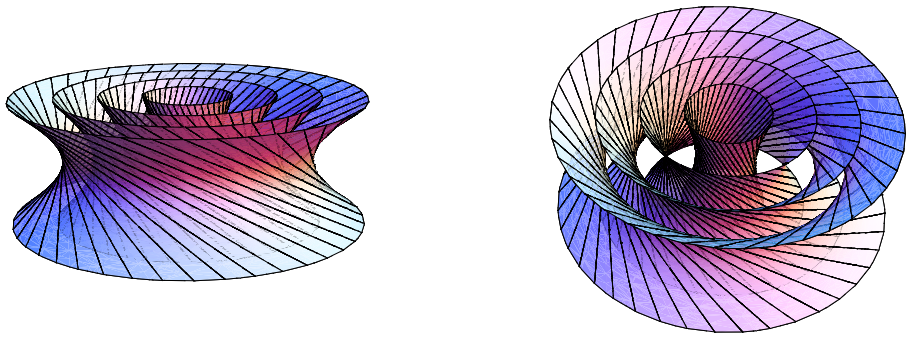
Teorem 4.5 *Neka je $\mathcal{P} = PG(3, F)$ trodimenzionalni projektivni prostor nad poljem F i p_1, p_2, p_3 tri mimoilazna pravca iz $\mathcal{P}$. U odgovarajućem četverodimenzionalnom vektorskom prostoru V možemo izabrati bazu tako da ti pravci (tj. odgovarajući dvodimenzionalni potprostori od V) budu zadani s*

$$p_1 = \langle (1,0,0,0), (0,1,0,0) \rangle,$$
$$p_2 = \langle (0,0,1,0), (0,0,0,1) \rangle,$$
$$p_3 = \langle (1,0,1,0), (0,1,0,1) \rangle.$$

Tada je skup točaka na pravcima regulusa određenog s p_1, p_2, p_3 jednak skupu točaka s homogenim koordinatama (x_0, x_1, x_2, x_3) koje zadovoljavaju jednadžbu $x_0x_3 - x_1x_2 = 0$.

To je jednadžba hiperboličke kvadrike u $PG(3, F)$ (skoro kanonska!). Dokazi prethodnih teorema u ovoj cjelini nalaze se u knjizi [10], a teorema u nastavku u knjizi [7].

Definicija 4.6 Spread *projektivnog prostora* $\mathcal{P} = PG(3, F)$ *je skup mimoilaznih pravaca* $\mathcal{S}$ *koji čine particiju skupa točaka od* $\mathcal{P}$. *Kažemo da je spread* $\mathcal{S}$ regularan *ako za svaka tri pravca iz* $\mathcal{S}$ *sadrži i sve ostale pravce jedinstvenog regulusa određenog s ta tri pravca.*



```
h = Table[ RevolutionPlot3D[{t,a,t/a}, {t,-a,a}, Boxed->False,
Axes->False, Mesh->{0,40}, ViewPoint->{1.3,-2.4,1}], {a,0.5,2,0.5}];
Show[h, PlotRange->All]
```

U konačnom slučaju $F = GF(q)$ spread je jednostavno skup od $q^2 + 1$ mimoilaznih pravaca. Regularni spread možemo konstruirati tako da uložimo $PG(3, q)$ u $PG(3, q^2)$. Pravci iz $PG(3, q^2)$ sijeku $PG(3, q)$ u 0, 1 ili $q + 1$ točaka; zovemo ih redom *vanjskim pravcima*, *tangentama* i *sekantama*.

Lema 4.7 *Neka je* T *točka iz* $PG(3, q^2) \setminus PG(3, q)$. *Onda kroz* T *prolazi* $q^4 - q^3$ *vanjskih pravaca, jedna sekanta i* $q^3 + q^2$ *tangenata na* $PG(3, q)$.

Teorem 4.8 *Neka je* $\ell = \{T_1, \ldots, T_{q^2+1}\}$ *vanjski pravac od* $PG(3, q^2)$ *obzirom na* $PG(3, q)$. *Neka je* p_i *jedinstvena sekanta na* $PG(3, q)$ *kroz točku* T_i. *Tada odgovarajuće tetive (sjecišta sekanata* p_i *s* $PG(3, q)$*) čine spread od* $PG(3, q)$.

Isti taj spread može se dobiti s pomoću konjugiranja $x \mapsto x^q$ u konačnom polju $GF(q^2)$. Konjugiranje inducira automorfnu kolineaciju $(x_0, x_1, x_2, x_3) \mapsto (x_0^q, x_1^q, x_2^q, x_3^q)$ projektivnog prostora $PG(3, q^2)$ koja fiksira točke i sekante na $PG(3, q)$.

Teorem 4.9 *Neka je $\ell = \{T_1, \ldots, T_{q^2+1}\}$ vanjski pravac od $PG(3, q^2)$ obzirom na $PG(3, q)$. Tada su $p_i = T_i T_i^q$ sekante na $PG(3, q)$, a odgovarajuće tetive čine spread od $PG(3, q)$.*

Teorem 4.10 *Spread konstruiran u prethodna dva teorema je regularan.*

Obrnuto, svaki regularni spread može se dobiti na taj način [14, Teorem 5.3]. Prema tome, regularnom spreadu $\mathcal{S}$ pridružena su dva pravca ℓ i ℓ^q iz $PG(3, q^2) \setminus PG(3, q)$, koje zovemo *transverzalama spreada*. Svaka od transverzala jedinstveno određuje $\mathcal{S}$. Obrnuto, $\mathcal{S}$ jedinstveno određuje svoje dvije transverzale (ℓ i ℓ^q su jedina dva vanjska pravca koji sijeku svaki "produženi" pravac iz $\mathcal{S}$).

Teorem 4.11 *Neka je $\mathcal{S}$ regularni spread od $PG(3, q)$ i p pravac koji nije iz $\mathcal{S}$. Onda $q + 1$ pravaca iz $\mathcal{S}$ koji sijeku p tvore regulus.*

Zadatak: može li se skup svih $(q^2 + 1)(q^2 + q + 1)$ pravaca od $PG(3, q)$ rastaviti na $q^2 + q + 1$ disjunktnih spreadova? Drugim riječima, je li dizajn točaka i pravaca od $PG(3, q)$ rastavljiv?

Zadatak: zadana su tri mimoilazna pravca p_1, p_2 i p_3 u $PG(3, q)$. Koliko ima regularnih spreadova koji sadrže ta tri pravca?

Rješenje. Pravci p_1, p_2, p_3 razapinju jedinstveni regulus $\mathcal{R}$. Bilo koji pravac r mimoilazan sa svim pravcima iz $\mathcal{R}$ određuje jedinstveni regularni spread koji sadrži r i $\mathcal{R}$. Stoga takvih spreadova ima $(q^2 - q)/2$; svaka dva se sijeku u $\mathcal{R}$. □

Postoje li spreadovi koji nisu regularni?

Neka je $\mathcal{S}$ regularni spread koji sadrži regulus $\mathcal{R}$. Zamijenimo li $\mathcal{R}$ sa suprotnim regulusom $\mathcal{R}'$, dobit ćemo spread $\mathcal{S}'$ koji nije regularan. Postupak možemo ponavljati i na taj način dobiti puno neregularnih spreadova.

Domaća zadaća: može li se svaki spread u $PG(3, q)$ dobiti na taj način od regularnog spreada? Može li se svaki regularni spread dobiti od bilo kojeg drugog? Hipoteza je postavljena u [15]; tamo piše da vrijedi za $q = 3$.

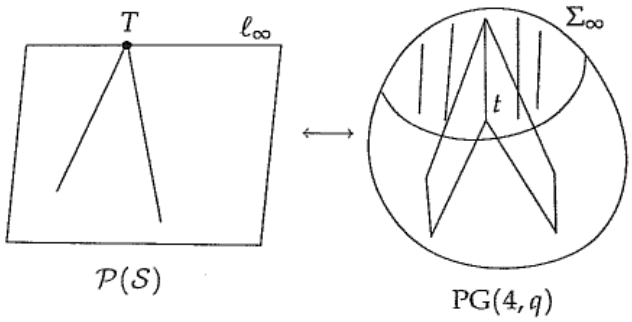
4.2 Bruck-Boseova reprezentacija

Što će nam projektivni prostori dimenzije $d > 2$ ako nas zanimaju samo unitali u projektivnim ravninama?

Ideja: $PG(2, q^2) \leftrightsquigarrow PG(2 \cdot 2, q)$

Projektivna ravnina reda q^2 ima $q^4 + q^2 + 1$ točaka, a projektivni prostor $PG(4, q)$ ima $q^4+q^3+q^2+q+1$ točaka. Ako izbacimo točke neke hiperravnine Σ_∞, ostat će nam q^4 točaka (kao u afinoj ravnini reda q^2). Do projektivne ravnine nedostaje $q^2 + 1$ točaka, a toliko ima pravaca u spreadu izbačene hiperravnine $\Sigma_\infty \cong PG(3, q)$.

Teorem 4.12 *Neka je Σ_∞ hiperravnina u projektivnom prostoru $PG(4, q)$, a $\mathcal{S}$ spread u Σ_∞. Definiramo novu incidencijsku strukturu $\mathcal{P}(\mathcal{S})$ kojoj su TOČKE točke iz $PG(4, q) \setminus \Sigma_\infty$ i pravci iz $\mathcal{S}$, a PRAVCI dvodimenzionalne ravnine iz $PG(4, q)$ koji sijeku Σ_∞ u pravcu iz $\mathcal{S}$ (proširene tim pravcem) te još jedan PRAVAC ℓ_∞ koji sadrži sve TOČKE iz $\mathcal{S}$. Tada je $\mathcal{P}(\mathcal{S})$ projektivna ravnina reda q^2. (Slika je preuzeta iz [7].)*



Dokaz. Već smo primijetili da je ukupan broj TOČAKA $q^4 + q^2 + 1$. Broj TOČAKA na PRAVCU ℓ_∞ je $|\mathcal{S}| = q^2+1$, a na bilo kojem drugom PRAVCU također $q^2 + q + 1 - (q + 1) + 1 = q^2 + 1$. Još treba provjeriti da kroz svake dvije TOČKE prolazi jedinstveni PRAVAC. Ako izaberemo dvije TOČKE iz $\mathcal{S}$, jedinstveni PRAVAC na kojem leže je ℓ_∞. TOČKA iz $\mathcal{S}$ i TOČKA iz $PG(4, q) \setminus \Sigma_\infty$ također leže na jedinstvenom PRAVCU, jer pravac iz $\mathcal{S}$ i točka iz $PG(4, q) \setminus \Sigma_\infty$ razapinju jedinstvenu dvodimenzionalnu ravninu u $PG(4, q)$. Konačno, ako izaberemo dvije TOČKE (točke) $T_1, T_2 \in PG(4, q) \setminus \Sigma_\infty$, one razapinju jedinstveni pravac u $PG(4, q)$ koji siječe Σ_∞ u jednoj točki. Ta točka leži na jedinstvenom pravcu $t \in \mathcal{S}$ (TOČKI $T \in \mathcal{S}$), pa opet imamo jedinstveni PRAVAC $\langle T_1, T_2, t\rangle$ kroz T_1 i T_2. □

Točke iz $PG(4, q) \setminus \Sigma_\infty$ su ujedno TOČKE i označavat ćemo ih velikim slovima. Sve te TOČKE čine afinu ravninu $\mathcal{P}(\mathcal{S}) \setminus \ell_\infty$, koju ćemo označavati $\mathcal{A}(\mathcal{S})$. TOČKE $T \in \ell_\infty$ su zapravo pravci $t \in \mathcal{S}$ i označavat ćemo ih odgovarajućim velikim i malim slovom.

Je li ravnina $\mathcal{P}(\mathcal{S})$ Desarguesova, tj. izomorfna klasičnoj ravnini $PG(2, q^2)$?

Bruck i Bose [15] su dokazali da je $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$ ako i samo ako je spread $\mathcal{S}$ regularan (bavit ćemo se prvenstveno tim slučajem). Općenito, $\mathcal{P}(\mathcal{S})$ je translacijska ravnina dimenzije najviše 2 nad svojom jezgrom. Vrijedi i obrat: svaka takva projektivna ravnina može se prikazati kao $\mathcal{P}(\mathcal{S})$ za neki spread $\mathcal{S}$ u $PG(4, q)$.

Projektni zadatak: prikaz Bruckovog i Boseovog rada [15]. Opis opće konstrukcije $PG(2, q^n) \rightsquigarrow PG(2n, q)$ i dokaz da regularnim spreadovima odgovaraju klasične ravnine. Vidjeti također [16] i [6].

Neka je $\mathcal{S}$ regularni spread u $PG(3, q)$. Tada možemo uspostaviti vezu između koordinata u $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$ i koordinata u $PG(4, q)$. Veza se zasniva na prikazu elemenata x iz polja $GF(q^2)$ u obliku $x = x_0 + x_1 i$, $x_0, x_1 \in GF(q)$, analognom prikazu kompleksnih brojeva. Možemo uzeti ireducibilni polinom $x^2 - t_1 x - t_0$ nad $GF(q)$ i konstruirati $GF(q^2)$ kao odgovarajuće kvadratno proširenje polja. Tada je $i \in GF(q^2)$ nultočka tog polinoma. Konjugiranje $x \mapsto x^q$ u $GF(q^2)$ fiksira elemente potpolja $GF(q)$ i zamjenjuje i s drugom nultočkom polinoma.

U slučaju $q \equiv 3 \pmod 4$ element -1 nije kvadrat u $GF(q)$, pa je polinom $x^2 + 1$ ireducibilan. Uzmemo li taj polinom, dobit ćemo istu formulu za množenje parova $x_0 + x_1 i$ kao za kompleksne brojeve (vidi treći zadatak u cjelini 2.4). Za paran q i za $q \equiv 1 \pmod 4$ moramo uzeti drugi polinom, jer $x^2 + 1$ nije ireducibilan.

U projektivnoj ravnini $PG(2, q^2)$ koristimo homogene koordinate (x, y, z) s komponentama iz $GF(q^2)$. Pretpostavimo da pravac ℓ_∞ ima jednadžbu $z = 0$. Tada točke afine ravnine $AG(2, q^2) = PG(2, q^2) \setminus \ell_\infty$ imaju koordinate (x, y, z) sa $z \neq 0$. Desnim normaliziranjem dobivamo afine koordinate tih točaka $(x, y, 1)$, koje identificiramo s (x, y).

U projektivnom prostoru $PG(4, q)$ koristimo homogene koordinate (x_0, x_1, y_0, y_1, z) s komponentama iz $GF(q)$. Pretpostavimo da hiperravnina Σ_∞ ima jednadžbu $z = 0$. Točkama afinog prostora $AG(4, q) = PG(4, q) \setminus \Sigma_\infty$ odgovaraju koordinate sa $z \neq 0$, koje također možemo desno normalizirati $(x_0, x_1, y_0, y_1, 1)$ i identificirati s afinim koordinatama (x_0, x_1, y_0, y_1).

Definiramo *Bruck-Boseovo preslikavanje* $\varphi : PG(2, q^2) \setminus \ell_\infty \to PG(4, q) \setminus \Sigma_\infty$ tako uzmemo afine koordinate (x, y) točke iz ravnine, raspišemo komponente kao $x = x_0 + x_1 i$ i $y = y_0 + y_1 i$ za $x_0, x_1, y_0, y_1 \in GF(q)$ i pridružimo joj točku iz prostora s afinim koordinatama (x_0, x_1, y_0, y_1). Jasno je da je φ bijekcija. Točkama na pravcu ℓ_∞ odgovaraju elementi regularnog spreada $\mathcal{S}$, tj. određeni pravci sadržani u Σ_∞. Cilj nam je odrediti jednadžbe tih

pravaca.

Točki $T \in \ell_\infty$ odgovara paralelna klasa pravaca u $AG(2, q^2)$. S pomoću Bruck-Boseovog preslikavanja možemo transformirati jednadžbe pravaca iz paralelne klase u jednadžbe odgovarajućih 2-ravnina iz afinog prostora $AG(4, q)$. Sve te 2-ravnine sijeku Σ_∞ u jednom pravcu $t \in \mathcal{S}$, koji odgovara točki T. Preko njihovih jednadžbi možemo doći do jednadžbe pravca t.

Koordinate točaka na ℓ_∞ su oblika $(x, y, 0)$; lijevim normaliziranjem dobivamo $(0, 1, 0)$ i $(1, \alpha, 0)$ za $\alpha \in GF(q^2)$. Pretpostavimo najprije da je T točka s koordinatama $(0, 1, 0)$. Tada pravci kroz T imaju jednadžbe $x = \beta z$, odnosno $x = \beta$ u afinim koordinatama, za $\beta = \beta_0 + \beta_1 i \in GF(q^2)$. Bruck-Boseovim preslikavanjem dobivamo jednadžbu $x_0 + x_1 i = \beta_0 + \beta_1 i$, odnosno dvije jednadžbe $x_0 = \beta_0$ i $x_1 = \beta_1$ dviju hiperravnina iz afinog prostora koje se sijeku u 2-ravnini. Odgovarajuće projektivne jednadžbe su $x_0 = \beta_0 z$, $x_1 = \beta_1 z$. Za bilo koje $\beta_0, \beta_1 \in GF(q)$ točke $(0, 0, 1, 0, 0), (0, 0, 0, 1, 0) \in \Sigma_\infty$ leže na tim hiperravninama, pa zaključujemo da sve te 2-ravnine sadrže pravac $p_\infty = \langle (0, 0, 1, 0, 0), (0, 0, 0, 1, 0) \rangle$ iz Σ_∞. Dakle, točka $T = (0, 1, 0) \in \ell_\infty$ odgovara pravcu $p_\infty \in \mathcal{S}$.

Neka je sada $T \in \ell_\infty$ točka s koordinatama $(1, \alpha, 0)$, $\alpha = \alpha_0 + \alpha_1 i \in GF(q^2)$. Pravci kroz T imaju jednadžbe $\alpha x - y + \beta z = 0$, odnosno afine jednadžbe $y = \alpha x + \beta$, za $\beta = \beta_0 + \beta_1 i \in GF(q^2)$. Svakom od tih pravaca Bruck-Boseovo preslikavanje φ pridružuje 2-ravninu u $AG(4, q)$ zadanu kao presjek hiperravnina s afinim jednadžbama

$$\begin{aligned} y_0 &= \alpha_0 x_0 + t_0 \alpha_1 x_1 + \beta_0 \\ y_1 &= \alpha_1 x_0 + (\alpha_0 + t_1 \alpha_1) x_1 + \beta_1, \end{aligned}$$

odnosno odgovarajućim projektivnim jednadžbama

$$\begin{aligned} \alpha_0 x_0 + t_0 \alpha_1 x_1 - y_0 + \beta_0 z &= 0 \\ \alpha_1 x_0 + (\alpha_0 + t_1 \alpha_1) x_1 - y_1 + \beta_1 z &= 0. \end{aligned}$$

Ovdje su $t_0, t_1 \in GF(q)$ koeficijenti primitivnog polinoma $x^2 - t_1 x + t_0$ elementa i. Točke $(1, 0, \alpha_0, \alpha_1, 0), (0, 1, t_0 \alpha_1, \alpha_0 + t_1 \alpha_1, 0) \in \Sigma_\infty$ leže na svim tim 2-ravninama (variramo $\beta_0, \beta_1 \in GF(q)$). Dakle, u ovom slučaju pravac $p_\alpha = \langle (1, 0, \alpha_0, \alpha_1, 0), (0, 1, t_0 \alpha_1, \alpha_0 + t_1 \alpha_1, 0) \rangle$ odgovara točki $T = (1, \alpha, 0)$. Tako smo preko Bruck-Boseovog preslikavanja dobili spread $\mathcal{S} = \{p_\infty\} \cup \{p_\alpha \mid \alpha \in GF(q^2)\}$ u hiperravnini Σ_∞. Budući da je $\mathcal{P}(\mathcal{S}) = PG(2, q^2)$ Desarguesova, taj spread mora biti regularan.

Analogna veza između koordinata može se dobiti za translacijske ravnine reda q^2 koordinatizirane kvazipoljem kojemu je jezgra polje $GF(q)$. Također, može se generalizirati na Bruck-Boseovu reprezentaciju ravnine $PG(2, q^n)$ u prostoru $PG(2n, q)$ (vidi [6]).

Zadatak: u slučaju $q \equiv 3 \pmod 4$, konstrukcija $GF(q^2)$ od $GF(q)$ analogna je konstrukciji $\mathbb{C}$ od $\mathbb{R}$. Može li se preko te analogije dobiti parametrizacija regularnog spreada u $\mathbb{R}^3$?

4.3 Buekenhoutove konstrukcije

Buekenhout [19] je proučavao unitale s pomoću Bruck-Boseove reprezentacije. Neka je U unital u projektivnoj ravnini $PG(2, q^2)$. Odgovarajući skup točaka u prostoru $PG(4, q)$ označavat ćemo s $\mathcal{U}$. Svojstva tog skupa ovise o položaju unitala U prema pravcu u beskonačnosti ℓ_∞ koji se u Bruck-Boseovoj reprezentaciji preslika u hiperravninu Σ_∞.

Teorem 4.13 *Neka je U klasični unital u $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$ kojemu je ℓ_∞ tangenta s diralištem u točki D. Onda je $\mathcal{U}$ eliptički konus kojemu vrh leži na odgovarajućem pravcu $d \in \mathcal{S}$.*

Točnije, postoji točka $V \in d$ i eliptička kvadrika $\mathcal{E}$ u hiperravnini $\mathcal{H} \cong PG(3, q)$ koja ne sadrži V, takva da se $\mathcal{U}$ sastoji od točaka na spojnicama $\langle T, V\rangle$, za $T \in \mathcal{E}$. Dokaz teorema u [7] sadrži jednu malu pogrešku (vrh konusa V ima koordinate $(0, 0, t_1, -2, 0)$, a ne $(0, 0, 1, 0, 0)$). Točan dokaz nalazi se u [19].

Teorem 4.14 *Neka je U klasični unital u $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$ kojemu je ℓ_∞ sekanta. Onda je $\mathcal{U}$ nedegenerirana kvadrika u $PG(4, q)$, a točke presjeka $U \cap \ell_\infty$ odgovaraju regulusu u $\mathcal{S}$.*

Dokazi prethodnog teorema i teorema u nastavku također se nalaze u [7]. Obrati prethona dva teorema predstavljaju prvu opću konstrukciju unitala koja nije zasnovana na polaritetima.

Teorem 4.15 *Neka je $\mathcal{S}$ spread (ne nužno regularan) u hiperravnini Σ_∞ prostora $PG(4, q)$. Ako je $\mathcal{U}$ ovoidalni konus koji siječe Σ_∞ u pravcu iz spreada $\mathcal{S}$, onda je odgovarajući skup točaka U ravnine $\mathcal{P}(\mathcal{S})$ unital kojemu je ℓ_∞ tangenta.*

Što su i kako izgledaju ovoidalni konusi u $PG(4, q)$?

Sjetimo se definicije 3.33: ovoid je nedegenerirani kvadratni skup indeksa 1. Prema teoremu 3.31, ovoidi mogu postojati samo u $PG(2, q)$ i u $PG(3, q)$. Ovoid u ravnini $PG(2, q)$ je oval i sadrži $q + 1$ točaka.

Lema 4.16 *Ovoid u $PG(3, q)$ sadrži $q^2 + 1$ točaka.*

U $PG(3,q)$, kroz svaku točku ovoida prolazi jedinstvena tangencijalna ravnina, a sve ostale ravnine sijeku ovoid u $q+1$ točaka od kojih nikoje tri nisu kolinearne, tj. u ovalu. Za neparan q vrijedi analogon Segreovog teorema: jedini primjeri ovoida u $PG(3,q)$ su eliptičke kvadrike (vidi [4] i [37]). Za paran q, poznata je jedna klasa ovoida koji nisu kvadrike. Otkrio ih je Tits [44], a budući da na njima djeluju Suzukijeve grupe, zovemo ih *Suzuki-Titsovim ovoidima*. Oni postoje za $q = 2^e$, pri čemu je $e \geq 3$ neparan.

Projektni zadatak za nekoga tko zna francuski: Suzuki-Titsovi ovoidi (prikaz članka [44]).

Domaća zadaća: postoje li u $PG(3,q)$ (za parni q) ovoidi koji nisu kvadrike niti Suzuki-Titsovi ovoidi?

Ovoidalni konus u $PG(4,q)$ je konus kojemu je baza ovoid u nekoj hiperravnini, a vrh točka izvan te hiperravnine.

Lema 4.17 *Ovoidalni konus u $PG(4,q)$ sadrži q^3+q+1 točaka.*

U $PG(4,q)$, trodimenzionalne ravnine su hiperravnine, a 2-ravnine zvat ćemo samo *ravninama*. Hiperravnina siječe ovoidalni konus u pravcu, u trodimenzionalnom konusu nad ovalom, ili u ovoidu. Ravnina siječe ovoidalni konus u točki, u pravcu, u paru pravaca kroz vrh konusa, ili u ovalu.

Pravci koji spajaju vrh konusa s točkama baznog ovoida nazivaju se *izvodnicama*. Izvodnice su jedini pravci sadržani u ovoidalnom konusu. Hiperravninu koja siječe ovoidalni konus u izvodnici g nazivamo *tangencijalnom hiperravninom* kroz g, a ravninu koja ga siječe u g *tangencijalnom ravninom* kroz g.

Lema 4.18 *Neka je g izvodnica ovoidalnog konusa u $PG(4,q)$. Onda postoji jedinstvena tangencijalna hiperravnina na taj konus kroz g. Svaka tangencijalna ravnina kroz g sadržana je u tangencijalnoj hiperravnini kroz g.*

Teorem 4.19 *Neka je $\mathcal{S}$ spread (ne nužno regularan) u hiperravnini Σ_∞ prostora $PG(4,q)$. Ako je $\mathcal{U}$ nedegenerirana kvadrika u $PG(4,q)$ koja siječe Σ_∞ u regulusu spreada $\mathcal{S}$, onda je odgovarajući skup točaka U ravnine $\mathcal{P}(\mathcal{S})$ unital kojemu je ℓ_∞ sekanta.*

Buekenhoutu je u [19] osnovni cilj bio dokazati egzistenciju unitala u translacijskim ravninama. Zaista, u teoremima 4.15 i 4.19 spread $\mathcal{S}$ ne mora biti regularan, iz čega slijedi postojanje unitala u svim translacijskim ravninama

reda q^2 kojima jezgra sadrži $GF(q)$ (npr. Hallovim i Andréovim ravninama).

Projektni zadatak: translacijske ravnine i unitali u translacijskim ravninama (prema [7] i [29]).

Ovdje nas prvenstveno zanimaju neklasični unitali u klasičnoj projektivnoj ravnini $PG(2, q^2)$. Buekenhout [19] je primijetio da se neklasični unitali dobivaju konstrukcijom iz teorema 4.15 ako za bazu konusa uzmemo ovoid koji nije eliptička kvadrika. Ako je $q \geq 8$ potencija od 2 s neparnim eksponentom, možemo uzeti Suzuki-Titsove ovoide, a odgovarajući unitali nazivaju se *Buekenhout-Titsovim unitalima*. Kasnije je Metz [35] koristeći konstrukciju iz teorema 4.15 dokazao postojanje neklasičnih unitala u $PG(2, q^2)$ za sve $q > 2$.

Lema 4.20 *Neka je $\mathcal{C}$ ireducibilna konika u ravnini π prostora $PG(3, q)$ i neka je ℓ pravac u ravnini π koji ne siječe $\mathcal{C}$. Neka je π' neka druga ravnina kroz pravac ℓ. Za svaku točku $T \in \pi' \setminus \ell$ postoji ovoid $\mathcal{O}$ u $PG(3, q)$ koji sadrži $\mathcal{C}$, sadrži T i π' mu je tangencijalna ravnina.*

Teorem 4.21 *Ako ovoid iz prethodne leme na odgovarajući način uložimo u projektivni prostor $PG(4, q)$ s regularnim spreadom u Σ_∞, primjenom teorema 4.15 dobivamo unital u $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$ koji nije klasični.*

Korolar 4.22 *Za svaku prim potenciju $q > 2$ postoje neklasični unitali u $PG(2, q^2)$.*

Brown [13] je dokazao da je, za paran q, ovoid koji sadrži koniku nužno eliptička kvadrika. Za neparan q, svi ovoidi su kvadrike (prema [4] i [37]), pa su Metzovi ovoidi svakako kvadrike. Neklasične unitale iz teorema 4.21 zovemo *Buekenhout-Metzovim unitalima*. Oni odgovaraju konusima u $PG(4, q)$ nad eliptičkim kvadrikama. Dokaz da nisu klasični zasniva se na postojanju sekante koja ih siječe u skupu koji nije tzv. *Baerov pravac* u $PG(2, q^2)$. Naime, poznato je da su sve tetive klasičnog unitala Baerovi pravci.

S druge strane, konstrukcija iz teorema 4.19 uvijek daje klasične unitale u $PG(2, q^2)$.

Teorem 4.23 *Unital dobiven od regularnog spreada $\mathcal{S}$ i nedegenerirane kvadrike u $PG(4, q)$ kao u teoremu 4.19 je klasični unital u ravnini $\mathcal{P}(\mathcal{S}) \cong PG(2, q^2)$.*

Ovaj rezultat dokazala je S. Barwick [5]. Svi danas poznati unitali u $PG(2, q^2)$ (klasični, Buekenhout-Titsovi, Buekenhout-Metzovi) dobivaju se s pomoću

konstrukcije iz teorema 4.15.

Domaća zadaća: postoje li unitali u klasičnoj ravnini $PG(2, q^2)$ koji nisu Buekenhoutovi, tj. ne mogu se dobiti iz teorema 4.15?

Zadatak: neka je $\mathcal{S}$ spread u hiperravnini Σ_∞ prostora $PG(4, q)$ i $\mathcal{H}$ neka druga hiperravnina tog prostora. Kako izgleda odgovarajući skup točaka H u ravnini $\mathcal{P}(\mathcal{S})$?

Rješenje. Skup H se sastoji od jedne točke T na pravcu ℓ_∞ i točaka na q pravaca kroz T (različitih od ℓ_∞). Ukupno sadrži $q^3 + 1$ točaka, isto kao i unital u $\mathcal{P}(\mathcal{S})$. □

Projektni zadatak: neka je $\mathcal{S}$ spread u hiperravnini Σ_∞ prostora $PG(4, q)$. Neka je $\mathcal{H}$ neka druga hiperravnina tog prostora u kojoj je zadana hiperbolička kvadrika, te $\mathcal{C}$ konus kojemu je baza ta kvadrika, a vrh neka točka iz $\Sigma_\infty \setminus \mathcal{H}$. Istražite kako izgleda odgovarajući skup točaka C u ravnini $\mathcal{P}(\mathcal{S})$.

To prvenstveno ovisi o položaju ravnine $\mathcal{R} = \mathcal{H} \cap \Sigma_\infty$ prema hiperboličkoj kvadrici u $\mathcal{H}$. Ravnina može biti sekantna (presjek s kvadrikom je nedegenerirana konika u $\mathcal{R}$) ili tangentna (presjek je par pravaca u $\mathcal{R}$). Nadalje, ovisi o tome koliko pravaca iz spreada $\mathcal{S}$ sadrži presjek $\mathcal{C} \cap \Sigma_\infty$. U nekim slučajevima skup C sadrži $q^3 + 1$ točaka, isto kao i unital u $\mathcal{P}(\mathcal{S})$.

4.4 Neka svojstva Buekenhoutovih unitala u $PG(2, q^2)$

U poglavlju 4.2 knjige [7] detaljno se razmatraju Buekenhoutovi unitali u klasičnim ravninama $PG(2, q^2)$. Budući da se konstrukcijom iz teorema 4.19 dobivaju samo klasični unitali, od interesa je prvenstveno konstrukcija iz teorema 4.15. Unitale dobivene na taj način zvat ćemo *ovoidalnim Buekenhoutovim unitalima*. Oni uključuju klasične unitale, Buekenhout-Titsove unitale i Buekenhout-Metzove unitale.

U slučaju kada je baza ovoidalnog konusa eliptička kvadrika, moguće je parametrizirati odgovarajući Buekenhoutov unital. Takve unitale zvat ćemo *ortogonalnim Buekenhoutovim unitalima* (uključuju klasične i Buekenhout-Metzove unitale). Parametrizacija glasi:

$$U_{\alpha,\beta} = \{(x, \alpha x^2 + \beta x^{q+1} + r, 1) \mid x \in GF(q^2), r \in GF(q)\} \cup \{(0, 1, 0)\},$$

pri čemu su $\alpha, \beta \in GF(q^2)$ zadani.

Teorem 4.24 *Ako je q neparan i $d = (\beta^q - \beta)^2 + 4\alpha^{q+1}$ je nekvadrat u $GF(q)$, onda je $U_{\alpha,\beta}$ ortogonalni Buekenhoutov unital u $PG(2, q^2)$. Obrnuto, svaki ortogonalni Buekenhoutov unital u $PG(2, q^2)$ s neparnim q ekvivalentan je unitalu parametriziranom na taj način.*

Za $q = 2^e$ vrijedi ista parametrizacija, ali su uvjeti na α i β drugačiji. Definiramo $T : GF(2^e) \to GF(2)$ s $T(x) = x+x^2+x^4+\ldots+x^{2^{e-1}}$ (to je tzv. *funkcija apsolutnog traga*). Pokazuje se da kvadratna jednadžba $ax^2+bx+c = 0$ nema rješenje u $GF(2^e)$ ako i samo ako je $b \neq 0$ i $T(ac/b^2) = 1$.

Teorem 4.25 *Ako je q paran, $\beta \in GF(q^2) \setminus GF(q)$ i za $d = \alpha^{q+1}/(\beta^q + \beta)^2$ vrijedi $T(d) = 0$, onda je $U_{\alpha,\beta}$ ortogonalni Buekenhoutov unital u $PG(2, q^2)$. Obrnuto, svaki ortogonalni Buekenhoutov unital u $PG(2, q^2)$ s parnim q ekvivalentan je unitalu parametriziranom na taj način.*

Pod ekvivalentnošću unitala u projektivnoj ravnini podrazumijevamo postojanje kolineacije ravnine koja preslikava jedan unital u drugi. Ekvivalentni unitali su izomorfni kao dizajni, ali obrat ne mora vrijediti. Moguće je izračunati točan broj ortogonalnih Buekenhoutovih unitala u $PG(2, q^2)$ do na ekvivalenciju.

Teorem 4.26 *Neka je $q = p^e$ neparna prim potencija i $e = 2^t e_0$, pri čemu je e_0 neparan. Broj neekvivalentnih ortogonalnih Buekenhoutovih unitala u $PG(2, q^2)$ dan je s*

$$\frac{1}{e}\left[e_0 + \sum_{m|e} \varphi\left(\frac{2e}{m}\right) p^m\right],$$

gdje je φ Eulerova funkcija.

Teorem 4.27 *Neka je $q = 2^e$ za neki $e \geq 2$. Broj neekvivalentnih ortogonalnih Buekenhoutovih unitala u $PG(2, q^2)$ dan je s*

$$\frac{1}{2e} \sum_{m|e} \varphi\left(\frac{2e}{m}\right) 2^m,$$

gdje je φ Eulerova funkcija.

Ova dva teorema dokazuju se primjenom Möbiusove inverzije.

Domaća zadaća: koliko ima ortogonalnih Buekenhoutovih unitala u $PG(2, q^2)$ do na izomorfizam (promatranih kao dizajni)?

Poznato je da su svaka dva klasična unitala ekvivalentni. Moguće je točno odrediti uvjet pod kojim je $U_{\alpha,\beta}$ klasični unital.

Teorem 4.28 *Unital u $PG(2,q^2)$ parametriziran kao $U_{\alpha,\beta}$ je klasični unital ako i samo ako je $\alpha = 0$ (za parni i za neparni q).*

Nožišta tangenti spuštenih iz bilo koje točke na klasični unital su kolinearna. Za neklasične ortogonalne Buekenhoutove unitale zna se točan uvijet pod kojim su nožišta kolinearna.

Teorem 4.29 *Neka je $U_{\alpha,\beta}$ neklasični ortogonalni Buekenhoutov unital u $PG(2,q^2)$ i $T \in PG(2,q^2) \setminus U_{\alpha,\beta}$ točka izvan unitala. Nožišta tangenti spuštenih iz T na unital su kolinearna ako i samo ako je $T \in \ell_\infty$ (za paran i za neparan q).*

Moguće je odrediti podgrupu grupe kolineacija $P\Gamma L(3,q^2)$ ravnine $PG(2,q^2)$ koja fiksira unital $U_{\alpha,\beta}$ (vidi teoreme 4.12 i 4.23 u [7]). Ta podgrupa je grupa automorfizama od $U_{\alpha,\beta}$ promatranog kao dizajna, ali ne mora biti njegova puna grupa automorfizama.

Domaća zadaća: odredite pune grupe automorfizama ortogonalnih Buekenhoutovih unitala u $PG(2,q^2)$ (promatranih kao dizajna).

S pomoću parametrizacije $U_{\alpha,\beta}$ može se riješiti pitanje samodualnosti ortogonalnih Buekenhoutovih unitala i još neka geometrijska pitanja o tim unitalima.

Teorem 4.30 *Ortogonalni Buekenhoutov unital u $PG(2,q^2)$ parametriziran kao $U_{\alpha,\beta}$ je samodualan (za paran i za neparan q).*

Teorem 4.31 *Neka je $U_{\alpha,\beta}$ ortogonalni Buekenhoutov unital u $PG(2,q^2)$ za neparan q. Onda $U_{\alpha,\beta}$ ne sadrži ireducibilnu koniku koja ne prolazi kroz točku $(0,1,0)$ (diralište unitala s ℓ_∞). Nadalje, $U_{\alpha,\beta}$ sadrži ireducibilnu koniku koja prolazi kroz $(0,1,0)$ ako i samo ako je $\beta \in GF(q)$. U tom slučaju $U_{\alpha,\beta}$ je unija q ireducibilnih konika koje se u parovima sijeku u točki $(0,1,0)$.*

Teorem 4.32 *Neka je $U_{\alpha,\beta}$ ortogonalni Buekenhoutov unital u $PG(2,q^2)$ za paran $q \geq 4$. Onda $U_{\alpha,\beta}$ ne sadrži niti jedan oval u $PG(2,q^2)$ (posebno, ne sadrži ireducibilnu koniku).*

Za paran q, osim ortogonalnih Buekenhoutovih unitala poznata je još jedna klasa ovoidalnih Buekenhoutovih unitala u $PG(2,q^2)$. To su Buekenhout-Titsovi unitali konstruirani od konusa nad Suzuki-Titsovim ovoidima. U poglavlju 4.2 knjige [7] dana je parametrizacija Buekenhout-Titsovih unitala, izračunata je podgrupa od $P\Gamma L(3,q^2)$ koja ih stabilizira i riješena su druga pitanja o tim unitalima.

Teorem 4.33 *Neka je U Buekenhout-Titsov unital u $PG(2,q^2)$, pri čemu je $q=2^e$ potencija od 2 s neparnim eksponentom $e\geq 3$. Ako je $T\in PG(2,q^2)\setminus U$, nožišta tangenti iz T na U su kolinearna ako i samo ako je $P\in\ell_\infty$.*

Teorem 4.34 *Buekenhout-Titsovi unitali su samodualni.*

Teorem 4.35 *Buekenhout-Titsovi unitali ne sadrže ovale.*

Projektni zadatak: Buekenhout-Titsovi unitali u $PG(2,q^2)$ (prema [7], str. 83–87).

Na kraju poglavlja 2.4 spomenuli smo da klasični unitali ne sadrže O'Nanove konfiguracije. Vjeruje se da ih to svojstvo karakterizira. Za ovoidalne Buekenhoutove unitale može se dokazati da ne sadrže O'Nanove konfiguracije kroz diralište P_∞ s pravcem ℓ_∞. Poznato je da mali primjeri neklasičnih ovoidalnih Buekenhoutovih unitala sadrže O'Nanove konfiguracije disjunktne s P_∞, ali nije poznata opća konstrukcija.

Domaća zadaća: nađite opću konstrukciju O'Nanovih konfiguracija u neklasičnim ovoidalnim Buekenhoutovim unitalima.

4.5 Rastavljivost Buekenhoutovih unitala

U ovoj cjelini pokazat ćemo da su ovoidalni Buekenhoutovi unitali rastavljivi (kao dizajni). Sjetimo se da je *paralelna klasa* dizajna skup blokova koji čine particiju skupa svih točaka. U dizajnu točaka i pravaca projektivnog prostora $PG(3,q)$ koristili smo termin *spread* za taj pojam, a u knjizi [7] *spread* se koristi i za unitale. *Rastav* (eng. *resolution*) dizajna je particija skupa svih blokova na paralelne klase (u knjizi [7] koristi se termin *pakiranje*).

Paralelna klasa unitala $S(2,q+1,q^3+1)$ sastoji se od $(q^3+1)/(q+1)=q^2-q+1$ pravaca. Ukupan broj pravaca je $q^2(q^2-q+1)$, pa se rastav unitala sastoji od q^2 paralelnih klasa. Za unitale uložene u projektivnu ravninu reda q^2 postojanje paralelnih klasa je povezano s pitanjem kolinearnosti nožišta. Ako je T točka ravnine koja ne pripada unitalu, sjetimo se da kroz T prolazi q^2-q sekanti (pravaca koji sijeku unital u $q+1$ točaka) i $q+1$ tangenti (pravaca koji sijeku unital u jednoj točki, *nožištu*). Za unitale dobivene kao skup apsolutnih točaka polariteta projektivne ravnine, pokazali smo da $q+1$ nožišta spuštenih iz točke T nužno leže na polari od T (propozicija 2.28).

Kada god imamo točku T sa svojstvom da su odgovarajuća nožišta kolinearna, dobivamo paralelnu klasu unitala. Naime, pravac na kojem leže nožišta zajedno sa sekantama kroz T čini skup od q^2-q+1 međusobno

disjunktnih pravaca. Da bismo dobili rastav unitala, treba nam q^2 takvih točaka i moramo biti sigurni da su odgovarajuće paralelne klase disjunktne.

Lema 4.36 *Neka je $\mathcal{U}$ unital reda q uložen u projektivnu ravninu $\mathcal{P}$ reda q^2. Neka postoji tangenta t na $\mathcal{U}$ takva da za svaku točku $T \in t$ (osim dirališta D) vrijedi da su nožišta iz T kolinearna. Tada je unital $\mathcal{U}$ rastavljiv.*

Dokaz. Skup od $q+1$ nožišta iz T sadrži diralište D, dakle riječ je o skupu točaka na nekom pravcu kroz D. Za dvije točke $T_1, T_2 \in t \setminus \{D\}$ odgovarajući pravci na kojima su nožišta su različiti, jer kroz točku unitala prolazi samo jedna tangenta. Jasno je da su i sekante kroz T_1 i T_2 različite. Prema tome, q^2 paralelnih klasa dobivenih od točaka iz $t \setminus \{D\}$ su disjunktne i čine rastav unitala. □

U teoremima 4.29 i 4.33 saznali smo da za ortogonalne Buekenhoutove unitale i Buekenhout-Titsove unitale u klasičnoj projektivnoj ravnini $PG(2, q^2)$ tangenta ℓ_∞ ima svojstvo iz prethodne leme. To vrijedi za svaki ovoidalni Buekenhoutov unital u bilo kojoj ravnini $\mathcal{P}(\mathcal{S})$.

Teorem 4.37 *Neka je $\mathcal{U}$ ovoidalni Buekenhoutov unital u ravnini $\mathcal{P}(\mathcal{S})$ koja ne mora biti klasična (tj. spread $\mathcal{S}$ ne mora biti regularan). Za svaku točku $T \in \ell_\infty$ (različitu od dirališta) nožišta iz T na $\mathcal{U}$ su kolinearna.*

Teorem je dokazao Dover [23], a dokaz se može naći i u [7]. Za dokaz je potrebna sljedeća lema.

Lema 4.38 *Neka je g izvodnica ovoidalnog konusa u $PG(4, q)$ s vrhom V. Svaka ravnina u $PG(4, q)$ koja siječe taj konus u jednoj točki, koja leži na pravcu g i nije V, sadržana je u tangencijalnoj hiperravnini kroz g.*

Korolar 4.39 *Svaki ovoidalni Buekenhoutov unital je rastavljiv.*

Korolar 4.40 *Dual svakog ovoidalnog Buekenhoutovog unitala je rastavljiv.*

Ako je $\mathcal{U}$ klasični unital, nožišta bilo koje točke iz $PG(2, q^2) \setminus \mathcal{U}$ su kolinearna. Prema tome, za svaku tangentu dobivamo rastav od $\mathcal{U}$, pa rastava ima bar $q^3 + 1$. No budući da je podgrupa od $P\Gamma L(3, q^2)$ koja čuva $\mathcal{U}$ tranzitivna na točkama od $\mathcal{U}$, svi ti rastavi su ekvivalentni. Za $q = 3$ to su jedini rastavi klasičnog unitala, no za $q = 4$ klasični unital dozvoljava četiri neekvivalentna rastava [25].

Domaća zadaća: koliko neekvivalentnih rastava dozvoljava klasični unital u $PG(2, q^2)$ za $q > 4$?

Ako je $q = 3^e$ potencija od 3 s neparnim eksponentom e, poznat je i Reeov unital reda q. Vjeruje se da ga se ne može uložiti u projektivnu ravninu reda q^2, pa ne možemo dobiti rastav kao u lemi 4.36. Dover [24] je tehnikama iz teorije grupa dokazao da za $q > 3$ Reeovi unitali dozvoljavaju bar $q^3 + 1$ rastava. Ti rastavi su ekvivalentni i svaka dva imaju zajedničku točno jednu paralelnu klasu. Za $q = 3$ Reeov unital dozvoljava točno 10 rastava i među njima su dva neekvivalentna.

5 Neke strukture povezane s unitalima

5.1 Blokade projektivnih ravnina

Definicija 5.1 Blokada *projektivne ravnine je skup točaka koji siječe svaki pravac ravnine, ali ne sadrži niti jedan cijeli pravac.*

Primjeri:

1. Unital reda n u projektivnoj ravnini reda n^2 je blokada.
2. Podravnina reda n projektivne ravnine reda n^2 (Baerova podravnina) je blokada.
3. U bilo kojoj projektivnoj ravnini reda n možemo uzeti točke nekog pravca p osim jedne točke T i po jednu točku na svakom pravcu kroz T različitom od p. Tako dobivamo blokadu od $2n$ točaka.

Teorem 5.2 *Svaka blokada $\mathcal{B}$ projektivne ravnine $\mathcal{P}$ reda n sadrži barem $n + \sqrt{n} + 1$ točaka. Ako je $|\mathcal{B}| = n + \sqrt{n} + 1$, onda je n kvadrat, a $\mathcal{B}$ Baerova podravnina od $\mathcal{P}$.*

Ovaj rezultat dokazao je Bruen 1970. Dokaz se može naći u magistarskom radu [1]. Komplement blokade je također blokada, pa za proizvoljnu blokadu $\mathcal{B}$ vrijedi gornja ocjena $|\mathcal{B}| \leq n^2 - \sqrt{n}$. Od interesa je gornja ocjena za tzv. minimalne blokade.

Definicija 5.3 *Za blokadu $\mathcal{B}$ kažemo da je* minimalna *ako za svaku točku $T \in \mathcal{B}$ skup $\mathcal{B} \setminus \{T\}$ nije blokada.*

Teorem 5.4 *Minimalna blokada $\mathcal{B}$ projektivne ravnine $\mathcal{P}$ reda n sadrži najviše $n\sqrt{n}+1$ točaka. Ako je $|\mathcal{B}| = n\sqrt{n}+1$, onda je n kvadrat, a $\mathcal{B}$ je unital u $\mathcal{P}$.*

Ovaj teorem dokazali su Bruen i Thas [17], a dokaz se također može naći u [1].

5.2 Inverzijske ravnine

Sjetimo se definicije t-(v,k,λ) dizajna: to je konačna incidencijska struktura $(\mathcal{P},\mathcal{B})$ od $v = |\mathcal{P}|$ točaka, s $k = |B|$ točaka na svakom bloku $B \in \mathcal{B}$, takva da je svaki t-člani skup točaka sadržan točno u λ blokova.

Propozicija 5.5 *Svaki t-(v,k,λ) dizajn je ujedno s-(v,k,λ_s) dizajn, za $s \leq t$ i $\lambda_s = \lambda \cdot \binom{v-s}{t-s} / \binom{k-s}{t-s}$.*

Propozicija 5.6 *Neka je $\mathcal{D} = (\mathcal{P},\mathcal{B})$ dizajn s parametrima t-(v,k,λ) i $x \in \mathcal{P}$ točka tog dizajna. Onda je incidencijska struktura*

$$\mathrm{der}_x\mathcal{D} = (\mathcal{P} \setminus \{x\},\ \{B \setminus \{x\} \mid B \in \mathcal{B},\ x \in B\})$$

dizajn s parametrima $(t-1)$-$(v-1,k-1,\lambda)$, koji zovemo deriviranim dizajnom *od $\mathcal{D}$ u točki x.*

Propozicija 5.7 *Neka je $\mathcal{D} = (\mathcal{P},\mathcal{B})$ dizajn s parametrima t-(v,k,λ) i $x \in \mathcal{P}$ točka tog dizajna. Onda je incidencijska struktura*

$$\mathrm{res}_x\mathcal{D} = (\mathcal{P} \setminus \{x\},\ \{B \mid B \in \mathcal{B},\ x \notin B\})$$

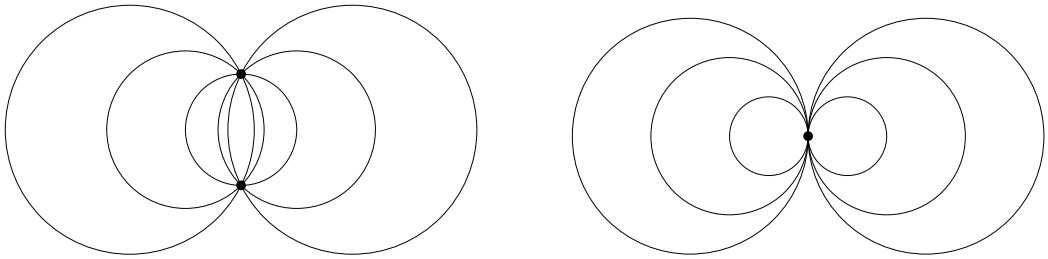
dizajn s parametrima $(t-1)$-$(v-1,k,\lambda_{t-1}-\lambda)$, koji zovemo rezidualnim dizajnom *od $\mathcal{D}$ u točki x.*

Definicija 5.8 Inverzijska ravnina *reda $n \geq 2$ je dizajn s parametrima* 3-$(n^2+1,n+1,1)$. *Koriste se i nazivi* Möbiusova ravnina *ili* geometrija kružnica*, a blokovi se u ovom slučaju nazivaju* kružnicama.

Ukupan broj kružnica je $b = \lambda_0 = n(n^2+1)$, broj kružnica kroz bilo koju točku je $r = \lambda_1 = n(n+1)$, a broj kružnica kroz bilo koje dvije točke je $\lambda_2 = n+1$. Derivirani dizajn inverzijske ravnine je afina ravnina s parametrima 2-$(n^2,n,1)$, a rezidualni dizajn ima parametre 2-$(n^2,n+1,n)$.

Presjek dviju kružnica sastoji se od 0, 1 ili 2 točke (ako imaju bar 3 zajedničke točke, podudaraju se). Zovemo ih redom *disjunktnim* kružnicama, *tangentnim* kružnicama ili *sijekućim* kružnicama. Skup svih kružnica kroz

zadane dvije točke M, N zovemo *snopom kružnica* (eng. *bundle*). Snop sadrži $\lambda_2 = n + 1$ kružnica i jednoznačno je određen točkama M i N, koje zovemo *nosačima snopa*. *Pramen kružnica* (eng. *pencil*) je maksimalni skup kružnica koje su tangentne u nekoj točki N. Pramen je jednoznačno određen točkom N (*nosačem* pramena) i nekom kružnicom kroz N, ili s bilo koje dvije tangentne kružnice. Pramen sadrži $r - (k-1)(\lambda_2 - 1) = n$ kružnica.



Propozicija 5.9 *Neka je k kružnica konačne inverzijske ravnine te $A \in k$ i $B \notin k$ dvije točke. Onda postoji jedinstvena kružnica iz pramena određenog s A i k kroz točku B (tj. postoji jedinstvena kružnica kroz A i B koja je tangentna kružnici k).*

Dokaz. Snop kružnica kroz A i B sadrži $n + 1$ kružnica. Za svaku od n točaka $T \in k \setminus \{A\}$ imamo jedinstvenu kružnicu iz tog snopa koja se siječe s k. Prema tome, točno jedna kružnica iz snopa je tangentna na k. □

Svojstvo iz prethodne propozicije uzima se kao aksiom inverzijske ravnine u beskonačnom slučaju, uz aksiom da kroz svake tri točke prolazi jedinstvena kružnica i aksiom nedegeneriranosti (vidi [21]). U konačnom slučaju iz tih aksioma slijedi postojanje prirodnog broja $n \geq 2$ takvog da na svakoj kružnici leži $k = n + 1$ točaka i da je ukupan broj točaka $v = n^2 + 1$.

Klasična (realna) inverzijska ravnina dobiva se nadopunjavanjem euklidske ravnine jednom točkom u beskonačnosti, tako da inverzije na kružnici budu bijekcije koje čuvaju incidenciju. KRUŽNICE inverzijske ravnine su kružnice i pravci euklidske ravnine, s time da su svi pravci prošireni točkom u beskonačnosti. Alternativno, klasičnu inverzijsku ravninu možemo definirati s pomoću projektivnog pravca nad poljem $\mathbb{C}$. Ta konstrukcija funkcionira i u konačnom slučaju.

Ako projektivni pravac promatramo kao samostalnu incidencijsku strukturu, svaka permutacija točaka bila bi automorfizam. Zato se pravac promatra uložen u klasičnu projektivnu ravninu i automorfizmima se smatraju

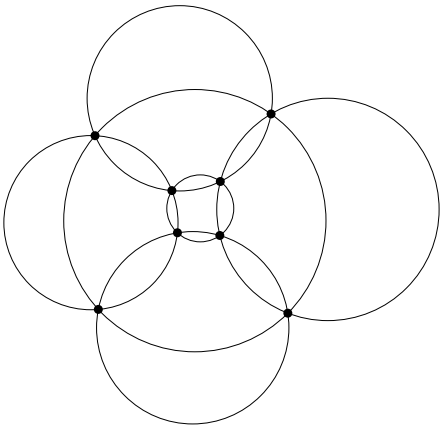
permutacije inducirane grupom kolineacija ravnine. Alternativno, projektivni pravac $PG(1, F)$ možemo definirati kao skup svih jednodimenzionalnih potprostora dvodimenzionalnog vektorskog prostora nad poljem F uz grupu automorfizama $P\Gamma L(2, F)$. Ako je $F = GF(q^2)$, pravac $PG(1, q^2)$ sadrži $q^2 + 1$ točaka. Tada postoji jedinstveno potpolje reda q koje određuje "potpravac" $PG(1, q)$ od $q+1$ točaka (jednodimenzionalnih potprostora vektorskog prostora razapetih vektorima kojima su sve komponente iz $GF(q)$). *Baerovi pravci* u $PG(1, q^2)$ su slike potpravca $PG(1, q)$ pod djelovanjem grupe kolineacija $P\Gamma L(2, q^2)$. Budući da automorfizmi polja $GF(q^2)$ fiksiraju potpolje $GF(q)$, možemo gledati samo slike pod djelovanjem grupe projektiviteta $PGL(2, q^2)$ (dobivamo iste $(q + 1)$-člane podskupove kao Baerove pravce).

Teorem 5.10 *Skup svih točaka projektivnog pravca $PG(1, q^2)$ i svih Baerovih pravaca kao kružnica čini inverzijsku ravninu reda q.*

Dokaz. Ukupan broj točaka je $|PG(1, q^2)| = q^2 + 1$, a broj točaka na svakoj kružnici $|PG(1, q)| = q + 1$. Treba provjeriti da za svake tri točke $A, B, C \in PG(1, q^2)$ postoji jedinstveni Baerov pravac koji ih sadrži. Neka je $A = \langle a \rangle$, $B = \langle b \rangle$ i $C = \langle c \rangle$. Vektori a i b razapinju različite jednodimenzionalne potprostore, pa čine bazu dvodimenzionalnog vektorskog prostora $V = GF(q^2)^2$. Zato vektor c možemo prikazati kao $c = \alpha a + \beta b$. Očito su $\alpha, \beta \neq 0$, jer bismo u suprotnom imali $B = C$ ili $A = C$. Zato možemo zamijeniti a s αa i b s βb, pa ćemo imati $C = \langle a + b \rangle$. Tvrdimo da je $\{\langle b \rangle\} \cup \{\langle a + tb \rangle \mid t \in GF(q)\}$ Baerov pravac kroz A, B i C. Zaista, on je slika potpravca $PG(1, q) = \{\langle (0, 1) \rangle\} \cup \{\langle (1, t) \rangle \mid t \in GF(q)\}$ pod linearnim operatorom koji prebacuje vektore kanonske baze $e_1 = (1, 0)$ i $e_2 = (0, 1)$ redom u a i b. Jedinstvenost slijedi zbog toga što $GF(q^2)$ ima samo jedno potpolje reda q. □

Inverzijsku ravninu iz prethodnog teorema nazivamo *Miquelovom* ravninom i označavamo je $M(q)$. U njoj vrijedi Miquelov teorem.

Teorem 5.11 (Miquel) *Neka su k_1, k_2, k_3, k_4 četiri kružnice koje se u parovima sijeku, ali nikoje tri nemaju zajedničku točku. Ako označimo sjecišta $k_i \cap k_{i+1} = \{A_i, B_i\}$, točke A_1, A_2, A_3, A_4 leže na kružnici ako i samo ako točke B_1, B_2, B_3, B_4 leže na kružnici.*



Može se pokazati da je svaka inverzijska ravnina u kojoj vrijedi Miquelov teorem izomorfna ravnini konstruiranoj kao u teoremu 5.10. Točke projektivnog pravca $PG(1, q^2)$ s homogenim koordinatama $(1, x)$ možemo idetificirati s elementima polja $x \in GF(q^2)$, a točku $(0, 1)$ s ∞. Uz tu identifikaciju djelovanje grupe $PGL(2, q^2)$ odgovara razlomljenim linearnim funkcijama $x \mapsto \frac{ax+b}{bx+c}$ s koeficijentima $a, b, c, d \in GF(q^2)$, $ad - bc \neq 0$. Punu grupu automorfizama Miquelove ravnine $M(q)$ dobivamo ako dodamo automorfizme polja $GF(q^2)$ koji fiksiraju potpolje $GF(q)$.

Baerove pravce definirali smo samo u klasičnom projektivnom pravcu $PG(1, q^2)$, tj. u ravnini $PG(2, q^2)$ u kojoj je uložen. U proizvoljnoj projektivnoj ravnini reda n^2 Baerov pravac možemo definirati kao pravac neke Baerove podravnine. U klasičnom slučaju definicije se slažu – za svaki Baerov pravac postoji Baerova podravnina u kojoj je to pravac, i svaki pravac Baerove podravnine od $PG(2, q^2)$ je Baerov pravac. Zanimljivo je da su tetive klasičnog unitala u $PG(2, q^2)$ također Baerovi pravci.

Propozicija 5.12 *Pravci klasičnog unitala u klasičnoj ravnini $PG(2, q^2)$ su Baerovi pravci te ravnine.*

Dokaz. Jednadžbu klasičnog unitala možemo dovesti u oblik $xy^q - x^q y + z^{q+1} = 0$. Zbog tranzitivnosti dovoljno je pokazati da je jedna tetiva Baerov pravac ravnine. Promotrimo sekantu unitala s jednadžbom $z = 0$, tj. pravac $\{(0, 1, 0)\} \cup \{(1, t, 0) \mid t \in GF(q^2)\}$. Odgovarajuću tetivu čini točka $(0, 1, 0)$ i točke $(1, t, 0)$ koje zadovoljavaju $t^q = t$. Rješenja te jednadžbe su točno elementi potpolja $GF(q)$, pa je tetiva Baerov pravac $\{(0, 1, 0)\} \cup \{(1, t, 0) \mid t \in GF(q)\}$. □

U Metzovim unitalima postoje pravci koji nisu Baerovi. Tako se dokazuje da Metzovi unitali nisu izomorfni klasičnim unitalima.

Alternativni model klasične inverzijske ravnine dobivamo kao točke na sferi u trodimenzionalnom euklidskom prostoru i kružnice koje nastaju presjecima sfere s ravninama. Konstrukcija se također može provesti u konačnom slučaju.

Propozicija 5.13 *Neka je $\mathcal{O}$ ovoid u $PG(3,q)$. Točke od $\mathcal{O}$ i presjeci sa sekantnim ravninama iz $PG(2,q)$ kao kružnice čine inverzijsku ravninu reda q.*

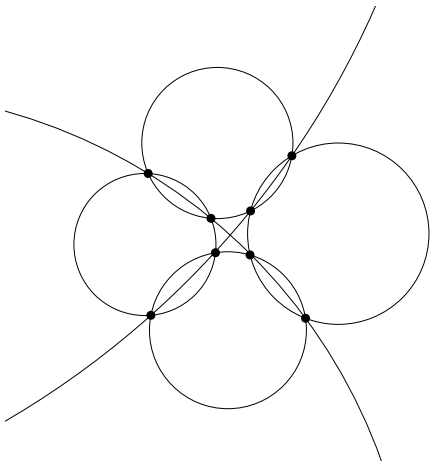
Dokaz. Iz leme 4.16 znamo da $\mathcal{O}$ sadrži q^2+1 točaka. Presjeci sa sekantnim ravninama su ovali koji sadrže $q+1$ točaka. Bilo koje tri točke na $\mathcal{O}$ nisu kolinearne po definiciji ovoida, pa razapinju jedinstvenu ravninu u $PG(3,q)$ koja je sekantna na $\mathcal{O}$. Dakle, kroz svake tri točke prolazi jedinstvena kružnica. □

Inverzijske ravnine konstruirane na ovaj način od ovoida u $PG(3,q)$ nazivamo *jajolikim inverzijskim ravninama.* Ako za ovoid uzmeno eliptičku kvadriku, dobivamo Miquelovu inverzijsku ravninu $M(q)$. Inverzijsku ravninu dobivenu od Suzuki-Titsovog ovoida označavamo $S(q)$.

Postoje li inverzijske ravnine koje nisu izomorfne s $M(q)$ ili $S(q)$? Postoje li inverzijske ravnine koje nisu jajolike?

Pokazuje se da u jajolikim inverzijskim ravninama vrijedi tzv. teorem o snopovima (eng. *bundle theorem*).

Teorem 5.14 (o snopovima) *Neka su k_1, k_2, k_3, k_4 četiri kružnice koje se u parovima sijeku ili su tangentne. Snop ili pramen određen s k_1, k_2 ima zajedničku kružnicu sa snopom ili pramenom određenim s k_3, k_4, ako i samo ako isto vrijedi za snopove ili pramenove određene s k_1, k_3 i s k_2, k_4.*



Prema [21], nije poznato povlači li teorem o snopovima jajolikost inverzijske ravnine. Miquelov teorem očito implicira teorem o snopovima, jer vrijedi samo u inverzijskim ravninama $M(q)$ koje su jajolike. Obrat ne vrijedi: u ravninama $S(q)$ ispunjen je teorem o snopovima, ali nije ispunjen Miquelov teorem.

Zadatak: neka su M i N dvije točke inverzijske ravnine. *Jatom* kružnica (eng. *flock*) s nosačem $\{M, N\}$ zovemo skup međusobno disjunktnih kružnica koje particioniraju skup svih točaka bez M i N. Ako postoji, jato sadrži $n-1$ kružnica. Dokažite da u jajolikoj inverzijskoj ravnini svake dvije točke M, N određuju jedinstveno jato kružnica.

Propozicija 5.15 *Derivirani dizajn jajolike inverzijske ravnine reda q u bilo kojoj točki izomorfan je klasičnoj afinoj ravnini $AG(2, q)$.*

Dokaz. Promatramo derivirani dizajn u točki D jajolike inverzijske ravnine. Neka je π_D tangencijalna ravnina ovoida $\mathcal{O}$ u točki D, a π neka druga tangencijalna ravnina od $\mathcal{O}$. Neka je $\ell_\infty = \pi \cap \pi_D$. Tangencijalne ravnine su uložene u $PG(3, q)$ i izomorfne su s $PG(2, q)$, pa je afina ravnina $\pi \setminus \ell_\infty$ izomorfna s $AG(2, q)$. Izomorfizam deriviranog dizajna s $\pi \setminus \ell_\infty$ dobivamo "stereografskom projekcijom": točki $T \in \mathcal{O} \setminus \{D\}$ pridružimo sjecište pravca DT s ravninom π. □

Ako je derivirani dizajn jajolike inverzijske ravnine reda q u svakoj točki izomorfan s $AG(2, q)$, je li ta inverzijska ravnina nužno jajolika?

Sljedeći teorem povezuje ovoidalni Buekenhotov unital s jajolikom inverzijskom ravninom dobivenom od ovoida koji je baza konusa. Dokazali su ga nezavisno Dover [23] i Barwick i O'Keefe [8]. Dokaz se može naći u [7].

Teorem 5.16 *Neka je U ovoidalni Buekenhoutov unital u projektivnoj ravnini $\mathcal{P}(\mathcal{S})$ s tangentom ℓ_∞ u točki D. Neka je $\mathcal{U}$ odgovarajući ovoidalni konus u $PG(4, q)$. Definiramo incidencijsku strukturu $\mathcal{D}$ kojoj su TOČKE pravci od U kroz D. BLOKOVI su skupovi TOČAKA koje dobijemo spajajući D s točkama nekog pravca od U koji ne prolazi kroz D. Struktura $\mathcal{D}$ je 2-$(q^2, q+1, q)$ dizajn izomorfan s rezidualnim dizajnom jajolike inverzijske ravnine dobivene od bilo kojeg ovoida koji je presjek konusa $\mathcal{U}$ s hiperravninom.*

Mogu li se karakterizirati 2-$(n^2, n+1, n)$ dizajni koji su rezidualni dizajni inverzijskih ravnina / jajolikih inverzijskih ravnina / inverzijskih ravnina $M(q)$ i $S(q)$?

Rezultati u nastavnku su iz knjige [21]. Dembowski je karakterizirao jajolikost inverzijskih ravnina s pomoću pojma *ortogonalnosti*. To je simetrična binarna relacija $\perp$ na skupu kružnica inverzijske ravnine koja zadovoljava sljedeće aksiome:

1. za svaku kružnicu k i svake dvije točke $A \in k$, $B \notin k$ postoji jedinstvena kružnica m takva da vrijedi $A, B \in m \perp k$,

2. ako je k kružnica ortogonalna na dvije kružnice iz snopa određenog točkama A i B, onda je k ortogonalna na sve kružnice iz tog snopa.

U beskonačnoj inverzijskoj ravnini konstruiranoj od sfere u euklidskom prostoru, ortogonalnost dobivamo preko okomitosti ravnina koje definiraju kružnice. Za konačne jajolike inverzijske ravnine također možemo definirati ortogonalnost. Naime, pokazuje se da je svaki ovoid skup apsolutnih točaka polariteta od $PG(3, q)$.

Teorem 5.17 *Neka je $\mathcal{O}$ ovoid u $PG(3, q)$, $q > 2$. Onda postoji polaritet ρ od $PG(3, q)$ koji preslikava svaku točku iz $\mathcal{O}$ u njezinu tangencijalnu ravninu. Za neparan q taj polaritet je ortogonalan, a za paran q simplektički.*

Za neparan q to slijedi iz rezultata da je svaki ovoid eliptička kvadrika [4], [37], a za paran q iz Segreovog rada [40]. Ortogonalnost dobivamo s pomoću polariteta ρ tako da definiramo $k \perp m \iff k^\rho \in m$. Dembowski i Hughes [22] dokazali su da vrijedi obrat, tj. da je svaka inverzijska ravnina u kojoj postoji ortogonalnost nužno jajolika.

Teorem 5.18 *Inverzijska ravnina je jajolika ako i samo ako dopušta ortogonalnost.*

Za sve inverzijske ravnine parnog reda pokazuje se da postoji jedinstvena ortogonalnost definirana na sljedeći način: $k \perp m \iff k = m$ ili su k i m tangentne kružnice. Neposredna posljedica je sljedeći rezultat.

Teorem 5.19 *Svaka inverzijska ravnina parnog reda n je jajolika. Prema tome, ravnina zadovoljava teorem o snopovima i n je potencija od 2.*

Za neparne redove također se može dokazati jedinstvenost ortogonalnosti, a egzistencija je ekvivalentna s činjenicom da je ravnina izomorfna s $M(q)$.

Teorem 5.20 *Inverzijska ravnina neparnog reda dozvoljava ortogonalnost ako i samo ako je Miquelova.*

Korolar 5.21 *Inverzijska ravnina neparnog reda je jajolika ako i samo ako je Miquelova, tj. izomorfna s $M(q)$.*

Domaća zadaća: konstruirajte inverzijsku ravninu neparnog reda koja nije jajolika, ili dokažite da ne postoji.

Domaća zadaća: konstruirajte jajoliku inverzijsku ravninu parnog reda koja nije izomorfna s $M(q)$ i $S(q)$, ili dokažite da ne postoji. Ekvivalentno: egzistencija ovoida u $PG(3, 2^e)$ koji nisu eliptičke kvadrike niti Suzuki-Titsovi ovoidi.

Literatura

[1] M. Andrić, *Blokade konačnih projektivnih ravnina*, magistarski rad, Sveučilište u Zagrebu, 2009.

[2] S. Bagchi, B. Bagchi, *Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner 2-designs*, Journal of Combinatorial Theory A **52** (1989), 51–61.

[3] R.D. Baker, *Polarities of elliptic semiplanes*. Proceedings of the Ninth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1978), pp. 85–96, Congress. Numer., XXI, Utilitas Math., Winnipeg, Man., 1978.

[4] A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. Unione Mat. Ital. **10** (1955), 498–506.

[5] S. Barwick, *A characterization of the classical unital*, Geom. Dedicata **52** (1994), 175–180.

[6] S. Barwick, L.R.A. Casse, C.T. Quinn, *The André/Bruck and Bose representation in $PG(2h, q)$: unitals and Baer subplanes*, Bull. Belg. Math. Soc. Simon Stevin **7** (2000), 173–197.

[7] S. Barwick, G. Ebert, *Unitals in Projective Planes*, Springer, 2008.

[8] S.G. Barwick, C.M. O'Keefe, *Unitals and inversive planes*, J. Geometry **58** (1997), 43–52.

[9] A. Betten, D. Betten, V.D. Tonchev, *Unitals and Codes*, Disrete Math. **267** (2003), 23–33.

[10] A. Beutelspacher, U. Rosenbaum, *Projective geometry: from foundations to applications*, Cambridge University Press, 1998.

[11] A.E. Brouwer, *Some unitals on* 28 *points and their embeddings in projective planes of order* 9, Geometries and Groups, Proc. Colloq. Berlin 1981, Lecture Notes in Math. **893** (1981), 183–188.

[12] A.E. Brouwer et al., *Self-dual, not self-polar*, preprint, 2003.

[13] M.R. Brown, *Ovoids of* $PG(3, q)$*,* q *even, with a conic section*, J. London Math. Soc. **62** (2000), 569–582.

[14] R.H. Bruck, *Construction problems of finite projective planes*, Conference on Combinatorial Mathematics and its Applications, University of North Carolina Press (1969), 426–514.

[15] R.H. Bruck, R.C. Bose, *The construction of translation planes from projective spaces*, Journal of Algebra **1** (1964), 85–102.

[16] R.H. Bruck, R.C. Bose, *Linear representations of projective planes in projective spaces*, Journal of Algebra **4** (1966), 117–172.

[17] A.A. Bruen, J.A. Thas, *Blocking sets*, Geom. Dedicata **6** (1977), 193–203.

[18] F. Buekenhout, *Ensembles quadratiques des espaces projectifs*, Math. Z. **110** (1969), 306–318.

[19] F. Buekenhout, *Existence of unitals in finite translation planes of order* q^2 *with a kernel of order* q, Geom. Dedicata **5** (1976), 189–194.

[20] C.J. Colbourn, J.H. Dinitz (eds.), *The handbook of combinatorial designs, Second edition*, CRC Press, 2007.

[21] P. Dembowski, *Finite Geometries*, Springer, 1968.

[22] P. Dembowski, D.R. Hughes, *On finite inversive planes*, J. London Math. Soc. **40** (1965), 171–182.

[23] J.M. Dover, *Some design-theoretic properties of Buekenhout unitals*, J. Combin. Des. **4** (1996), 449–456.

[24] J.M. Dover, *Spreads and resolutions of Ree unitals*, Ars Combin. **54** (2000), 301–309.

[25] J.M. Dover, *Subregular spreads of Hermitian unitals*, Des. Codes Cryptogr. **39** (2006), 5–15.

[26] H. Hanani, *The existence and construction of balanced incomplete block designs*, Ann. Math. Statist. **32** (1961), 361–386.

[27] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, 1998.

[28] S.K. Houghten, L.H. Thiel, J. Janssen, C.W.H. Lam, *There is no* $(46, 6, 1)$ *block design*, J. Combin. Des. **9** (2001), 60–71.

[29] D.R. Hughes, F.C. Piper, *Projective Planes*, Springer, 1973.

[30] P. Kaski, P.R.J. Östergard, *Classification of resolvable balanced incomplete block designsThe unitals on 28 points*, Mathematica Slovaca **59** (2009), 121–136.

[31] V. Krčadinac, *Steiner* 2*-designs* $S(2, 4, 28)$ *with nontrivial automorphisms*, Glas. Mat. Ser. III **37(57)** (2002), 259–268.

[32] C.W.H. Lam, L. Thiel, S. Swiercz, *The nonexistence of finite projective planes of order 10*, Canadian Journal of Mathematics **41** (1989), 1117–1123.

[33] R. Mathon, *Constructions for cyclic Steiner* 2*-designs*, Ann. Discrete Math. **34** (1987), 353–362.

[34] R. Mathon, T. van Trung, *Unitals and unitary polarities of symmetric designs*, Designs, Codes and Cryptography **10** (1997), 237–250.

[35] R. Metz, *On a class of unitals*, Geom. Dedicata **8** (1979), 125–126.

[36] M. O'Nan, *Automorphisms of unitary block designs*, Journal of Algebra **20** (1972), 495–511.

[37] G. Panella, *Caratterizzazione delle quadriche di un spazio (tridimenzionale) lineare sopra un corpo finito*, Boll. Unione Mat. Ital. **10** (1955), 507-513.

[38] T. Penttila, G.F. Royle, *Sets of type* (m, n) *in the affine and projective planes of order* 9, Des. Codes Cryptography **6** (1995), 229–245.

[39] C. Reid, A. Rosa, *Steiner systems* $S(2, 4, v)$ *- a survey*, The Electronic Journal of Combinatorics (2010), #DS18.

[40] B. Segre, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta Artihm. **5** (1959), 315–332.

[41] D.R. Stinson, *Combinatorial designs. Construction and analysis*, Springer, 2004.

[42] S.D. Stoichev, V.D. Tonchev, *Unital designs in planes of order* 16, Discrete Applied Mathematics **102** (2000), 151–158.

[43] J.A. Thas, *On polarities of symmetric partial geometries*, Arch. Math. (Basel) **25** (1974), 394–399.

[44] J. Tits, *Ovoides et groupes du Suzuki*, Arch. Math. **13** (1962), 187–198.