Konačne geometrije i primjene

Novosel, Iva

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Iva Novosel

KONAČNE GEOMETRIJE I PRIMJENE

Diplomski rad

Voditelj rada:
doc. dr. sc. Matija Bašić

Zagreb, rujan, 2019

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Kombinatorika je grana matematike koja se bavi prebrojavanjem elemenata konačnih skupova i načina da se ti elementi rasporede. Jedno od područja kombinatorike je teorija dizajna. Teorija dizajna proučava postojanje, konstrukciju i svojstva sustava konačnih skupova ([1]). Blok dizajn (u daljnjem tekstu *dizajn*) je struktura u kojoj su elementi konačnih skupova (točke i pravci) raspoređeni po zadanim pravilima. S obzirom na to razlikujemo balansirani nepotpuni blok dizajn - BIBD, Hadamardove matrice, latinske kvadrate itd. Teorija dizajna posebno se razvija toko 18. i 19. stoljeća. Jedan od najutjecajnijih matematičara u tom području bio je Ronald Fisher koji je dizajne koristio u svojim istraživanjima na području biologije. Općenito, dizajni se koriste za dizajniranje eksperimenata, u raznim algoritmima i računalnim kodovima, ali i pri određivanju rasporeda dvoboja na turnirima i mnogim drugim primjenama.

U ovome radu vidjet ćemo koja je veza dizajna s konačnim projektivnim i afinim ravninama reda n. Konačne ravnine su ravnine koje imaju konačan broj točaka i pravaca. Najmanja konačna projektivna ravnina naziva se Fanova ravnina i ima sedam točaka i sedam pravaca. Konstrukcija Fanove ravnine, ali i svih drugih konačnih projektivnih i afinih ravnina može se provesti pomoću konačnih polja. Konkretno, ako u vektorskom trodimenzionalnom prostoru nad poljem $\mathbb{Z}_2$ definiramo skup svih jednodimenzionalnih potprostora ($\mathcal{T}$) i skup svih dvodimenzinalnih potprostora ($\mathcal{B}$) danog vektorskog prostora, uz relaciju inkluzije I struktura $(\mathcal{T}, \mathcal{B}, I)$ je projektivna ravnina reda 2, odnosno Fanova ravnina. Uvjeti postojanja projektivne ravnine reda n dani su Bruck-Ryserovim teoremom.

U radu se pojavljuju razni primjeri vezani za konačna polja, projektivne i afine ravnine i dizajne. Krajnji cilj rada je prikazati na koji način se dane strukure iz prva tri poglavlja mogu prilagoditi učenicima u školi. Nastava matematike, ako je dobro provedena, potiče kognitivnu aktivnost kod učenika. Prikazat ćemo kako možemo izvesti nekoliko nastavnih sati u kojima učenik razmišlja, analizira i interpretira dobivena rješenja, te na taj način razvija kreativno, apstraktno i kombinatorno razmišljanje koji ga dovode do željenog rezultata. Osim toga, kroz zadatke upoznaje matematičke strukture s kojima se još nije susreo. Bitno je da sav materijal koji koristimo prilikom izvođenja nastave prilagodimo

učenicima i njihovoj dobi, a naglasak je na očekivanim odgojno-obrazovnim ishodima nakon provođenja nastavnog sata. Također, u dodacima su predloženi nastavni listići sa zadacima primijenjeni učenicima.

Rad je podijeljen u četiri poglavlja. U prvom poglavlju izneseni su osnovni rezultati o konačnim poljima i dane su ilustracije polja $\mathbb{Z}$ modulo n, te polja s osam elemenata pomoću polinoma. U drugom i trećem poglavlju promatramo projektivne i afine ravnine te dizajne kao njihovu generalizaciju. Uz osnovne definicije i teoreme o uvjetima postojanja konačnih afinih i projektivnih ravnina reda n, na dva načina prikazana je veza među spomenutim ravninama. Prikazana su i dokazana svojstva konačnih projektivnih i afinih ravnina. Navedeni su neki poznati problemi, npr. Kirkmanov problem 15 učenica. Uz to, riješeni su razni primjeri te su prikazane strukure kao npr. Fanova ravnina i Hesseova konfiguracija. U četvrtom poglavlju bavimo se prilagodbom sadržaja iz prva tri poglavlja za učenike u školama. Pri tome su dani očekivani odgojno-obrazovni ishodi koje želimo postići provedbom nastavnih sati.

Poglavlje 1

Konačna polja

U prvom poglavlju promatrat ćemo konačna polja $\mathbb{Z}$ modulo n i vidjeti kako konstrurati konačna polja pomoću polinoma. Također ćemo iznijeti osnovne rezultate o konačnim poljima koji će nam koristiti u drugom djelu rada.
Podsjetimo se na početku što je to *polje*. Ako imamo skup $\mathbb{F}$ koji sadrži barem dva elementa, 0 kao neutralni element za zbrajanje i 1 kao neutralni element za množenje, i binarne operacije, zbrajanje i množenje, polje $(\mathbb{F}, +, \cdot)$ je algebarska struktura u kojoj je $(\mathbb{F}, +)$ Abelova grupa, a $(\mathbb{F}^\times, \cdot)$, pri čemu je $\mathbb{F}^\times = \mathbb{F}\backslash\{0\}$, isto Abelova grupa. Uz to, vrijedi distributivnost množenja prema zbrajanju. Najpoznatiji primjeri polja su $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ i njima se najčesće koristimo. Konačna polja su ona polja koja imaju konačan broj elemenata. Svi rezultati o konačnim poljima i dokazi teorema su prezeti i mogu se naći u [8].

1.1 Polja $\mathbb{Z}$ modulo n

Promotrimo na početku skup $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$. Taj skup ima konačno mnogo elemenata koje dobijemo kao cjelobrojne ostatke djeljenja cijelih brojeva sa n. Pri tome s $\overline{0}$ označavamo klasu ekvivalencije elemenata višekratnika broja n, s $\overline{1}$ klasu ekvivalencije elemenata čiji je ostatak pri dijeljenju s n jednak 1, i tako dalje. Na taj način skup $\mathbb{Z}$ podijelili smo na n klasa. Radi jednostavnosti umjesto oznake $\mathbb{Z}/n\mathbb{Z}$ koristit ćemo oznaku $\mathbb{Z}_n$. Zbrajanje i množenje na skupu $\mathbb{Z}_n$ definirat ćemo na sljedeći način. Neka su $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Uzmimo neke $x, y \in \mathbb{Z}$ različite od a i b takve da vrijedi

$$n|x - a$$

$$n|y - b.$$

x i a su tada reprezentanti iste klase ekvivalencije modulo n u oznaci $\overline{a}$. Isto tako y i b pripadaju istoj klasi ekvivalencije modulo n u oznaci $\overline{b}$.

Pokažimo prvo da je zbrajanje $+_n : \mathbb{Z}_n \to \mathbb{Z}_n$, $\overline{a} +_n \overline{b} = \overline{(a+b)}$ dobro definirano.

$$x + y = q_1 n + a + q_2 n + b = ()a + b) + n(q_1 + q_2) \implies x + y \equiv a + b \pmod{n}$$

pa je $\overline{x+y} = \overline{a+b}$.
Slično se pokaže da je množenje $\cdot_n : \mathbb{Z}_n \to \mathbb{Z}_n$, $\overline{a} \cdot_n \overline{b} = \overline{a \cdot b}$ dobro definirano. Uzmemo li $x, y \in \mathbb{Z}$ kao i kod zbrajanja dobivamo:

$$\begin{aligned} x \cdot y = (q_1 n + a) \cdot (q_2 n + b) &= q_1 q_2 n^2 + q_1 b n + q_2 n a + ab \\ &= (q_1 q_2 n + q_1 b + q_2 a) n + ab \implies n | xy - ab \end{aligned} \quad (1.1)$$

pa zaključujemo:

$$\overline{x \cdot y} = \overline{a \cdot b}.$$

Lako se pokaže da je sa tako definiranim zbrajanjem i množenjem struktura $(\mathbb{Z}_n, +_n)$ Abelova grupa, a $(\mathbb{Z}_n^\times, \cdot_n)$ monoid, odnosno vrijedi asocijativnost i postoji neutralni element. Uz to vrijedi i distributivnost množenja prema zbrajanju pa je $(\mathbb{Z}_n, +_n, \cdot_n)$ *prsten s jedinicom*. Međutim u nekim slučajevima je struktura $(\mathbb{Z}_n, +_n, \cdot_n)$ polje. Jedan od primjera je $\mathbb{Z}_3$ sa operacijama množenja modulo 3 i zbrajanja modulo 3. Elementi polja su $\overline{0}$, $\overline{1}$ i $\overline{2}$, odnosno klase ekvivalencije cjelobrojnih ostataka pri dijeljenju sa brojem 3.

$+_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Tablica 1.1: Tablica zbrajanja modulo 3

$\cdot_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Tablica 1.2: Tablica množenja modulo 3

Možemo se zapitati, za koje prirodne brojeve n je struktura $(\mathbb{Z}_n, +_n, \cdot_n)$ polje? Na to nam odgovor daje sljedeći teorem.

Teorem 1.1.1. *$(\mathbb{Z}_n, +_n, \cdot_n)$ je polje ako i samo ako je n prosti broj.*

Dokaz. Prethodno smo komentirali da $(\mathbb{Z}_n, +_n, \cdot_n)$ ima strukturu prstena s jedinicom. Stoga, trebamo provjeriti za koje prirodne brojeve n svaki element skupa $\mathbb{Z}_n^\times$ ima inverzni element. Pretpostavimo da je n prirodni broj veći od 1 i da nije prost. Tada postoje $1 < a < n$ i $1 < b < n$ takvi da vrijedi

$$a \cdot b = n.$$

Iz toga slijedi:

$$\overline{a} \cdot_n \overline{b} = \overline{0}.$$

Odnosno ili $n|a$ ili $n|b$ što je u kontradikciji sa pretpostavkom da vrijedi $1 < a < n$ i $1 < b < n$, pa za n složeni brojevi $\overline{a}$ i $\overline{b}$ ne mogu biti invertibilni. Dakle, struktura $(\mathbb{Z}_n, +_n, \cdot_n)$ nije polje.
Pretpostavimo sada da je $n = p$ prirodni, prosti broj. Postojanje inverznog elementa pokazujemo na skupu $\mathbb{Z}_p^\times = \{\overline{1}, \overline{2}, ..., \overline{p-1}\}$. Želimo pokazati da za svaki $\overline{x} \in \mathbb{Z}_p^\times$ postoji $\overline{y} \in \mathbb{Z}_p^\times$ takav da $p|xy - 1$.
Neka su $\overline{x}, \overline{z}, \overline{z'} \in \mathbb{Z}_p^\times$. Pretpostavimo da vrijedi

$$\begin{aligned} & xz \equiv xz' \pmod{p} \\ \iff & x(z - z') \equiv 0 \pmod{p} \\ \implies & p \mid x \text{ ili } p \mid z - z' \end{aligned}$$

Kako su $\overline{x}, \overline{z}, \overline{z'} \in \mathbb{Z}_p^\times$, onda $p \nmid x$.
Dakle,

$$p \mid z - z' \implies z = z' \tag{1.2}$$

Time dobivamo da skup $\{\overline{x}, \overline{x} \cdot_p \overline{2}, \overline{x} \cdot_p \overline{3}, ..., \overline{x} \cdot_p \overline{p-1}\}$ generiran elementom $\overline{x} \in \mathbb{Z}_p^\times$ sadrži $p - 1$ različitih elemenata. Stoga jedan od njih mora biti jedan 1, odnosno zaključujemo da za svaki $\overline{x} \in \mathbb{Z}_p^\times$ postoji $\overline{y} \in \mathbb{Z}_p^\times$ takav da vrijedi $\overline{x} \cdot_p \overline{y} = 1$. □

1.2 Osnovni rezultati o konačnim poljima

Još jedan pojam koji će nam biti potreban je karatkeristika konačnog polja. Neka je $\mathbb{F}$ konačno polje. Za broj n kažemo da je *karakteristika* konačnog polja $\mathbb{F}$ ako za svaki $a \in \mathbb{F}$ vrijedi $n \cdot a = 0$ i ako je n najmanji takav broj.

Propozicija 1.2.1. *Karakteristika konačnog polja je prost broj.*

Dokaz. Pretpostavimo da je n karakteristika polja i nije prosti broj. Neka su k i m prirodni brojevi takvi da su $1 < k < n$ i $1 < m < n$, te vrijedi $n = km$. Tada je

$$(\sum_{i=1}^{k} 1) \cdot (\sum_{i=1}^{m} 1) = \sum_{i=1}^{km} 1 = 0,$$

pa vrijedi

$$(\sum_{i=1}^{k} 1) = 0 \text{ ili } (\sum_{i=1}^{m} 1) = 0.$$

Ali to je u kontradikciji s tvrdnjom teorema da je n najmanji takav broj. Dakle, $n = p$ je prosti broj. □

Teorem 1.2.2. *Ako je $\mathbb{F}$ konačno polje onda je $|\mathbb{F}| = p^m$.*

Dokaz. Ako je $\mathbb{F}$ konačno polje, prema propoziciji 1.2.1, karakteristika polja $\mathbb{F}$ je p pri čemu je p prosti broj. S druge strane, skup $\{1, 1+1, 1+1+1, ..., \underbrace{1+1+1+...+1}_{p-1}, 0\}$, koji je podskup od $\mathbb{F}$, također tvori polje s operacijama u polju $\mathbb{F}$ i to polje $\mathbb{Z}_p$. Iz ovoga zaključujemo da je $\mathbb{F}$ vektorski prostor nad poljem $\mathbb{Z}_p$ sa definiranim zbrajanjem kao u polju $\mathbb{F}$ i množenjem $\overline{x} \cdot a$ za dane $\overline{x} \in \mathbb{Z}_p, a \in \mathbb{F}$. Primijetimo da je množenje isto tako definirano kao i u polju $\mathbb{F}$ jer je $\{1, 1+1, 1+1+1, ..., \underbrace{1+1+1+...+1}_{p-1}, 0\}$ podskup od $\mathbb{F}$.

Tvrdnju možemo pokazati provjerom aksioma. Kako je $\mathbb{F}$ vektorski prostor nad $\mathbb{Z}_p$ znači da postoji m takav da $\mathbb{F} = (\mathbb{Z}_p)^m$ pa je time $| \mathbb{F} | = p^m$ i tvrdnja teorema je dokazana. □

Obrat ovog teorema također vrijedi, odnosno ako imamo skup $\mathbb{F}$ sa p^m elemenata, sa dobro definiranim zbrajanjem i množenjem, struktura $(\mathbb{F}, +, \cdot)$ je polje. Konstrukciju takve strukture promatrat ćemo u potpoglavlju 1.3.

Prethodno smo vidjeli primjer konačnog polja kada je broj elemenata prosti broj, a sada ćemo ilustrirati konstrukciju polja sa p^m elemenata.

1.3 Konstrukcija konačnih polja pomoću polinoma

Promotrimo polinome oblika $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_m x^m$ pri čemu su koeficijenti $f_1, ..., f_m \in \mathbb{Z}_p$. Skup svih polinoma nad poljem $\mathbb{Z}_p$ označimo sa $\mathbb{Z}_p[x]$. Polinomi se zbrajaju tako da zbrojimo koeficijente uz jednake potencije, a množe primjenom distributivnosti. Pri tome, koeficijente zbrajamo odnosno množimo modulo p.

Definicija 1.3.1. *1. Za $f(x), g(x) \in \mathbb{Z}_p[x]$ kažemo da $f(x)$* dijeli *$g(x)$ ako postoji polinom $q(x) \in \mathbb{Z}_p[x]$ takav da vrijedi*

$$g(x) = q(x) f(x).$$

2. *Za $f(x) \in \mathbb{Z}_p[x]$ definiramo* stupanj *od f, u oznaci $deg(f)$, kao najveći eksponent i od x pri čemu je $f_i \neq 0$.*

3. *Neka su $f(x), g(x), h(x) \in \mathbb{Z}_p[x]$ i $deg(f) = n \geq 1$. Definiramo*

$$[g(x)] = [h(x)]$$

ako vrijedi

$$f(x) \mid g(x) - h(x).$$

4. *Kažemo da je $f(x)$* ireducibilan *polinom ako ne postoje $g(x)$ i $q(x)$ stupnja većeg od 1 takvi da vrijedi $f(x) = g(x)q(x)$*

Propozicija 1.3.2. *Neka je p prosti broj i $\mathbb{Z}_p[x]$ skup polinoma nad poljem $\mathbb{Z}_p$. Tada je $(\mathbb{Z}_p[x], +, \cdot)$ prsten.*

Zbrajanje i množenje na skupu $\mathbb{Z}_p[x]$ definirani su na sljedeći način:
Neka su $f(x), r(x), s(x) \in \mathbb{Z}_p[x]$ i neka je $r(x) = g(x) \pmod{f}(x)$ i $s(x) = h(x) \pmod{f}(x)$.Radi jednostavnosti $f(x)$ ćemo označiti sa f. Tada je $r = g - qf$, a $s = h - tf$ za neke polinome g i h. Za zbrajanje vrijedi:

$$g + h = r + s - (q + t)f$$

pa je $g + h \equiv r + s \pmod{f}$. Dakle, možemo definirati operaciju zbrajanja modulo f kao

$$[r(x)] + [s(x)] = [r(x) + s(x)]. \tag{1.3}$$

Slično dobivamo množenjem:

$$gh = rs - (qs + tr)f + qtf^2$$

iz čega vidimo da vrijedi $gh \equiv rs \pmod{f}$ pa množenje modulo f definiramo kao

$$[r(x)] \cdot [s(x)] = [r(x)s(x)]. \tag{1.4}$$

Ostali aksiomi koji daju da je $(\mathbb{Z}_p[x], +, \cdot)$ prsten lako se provjere.

Sada možemo krenuti u konstukciju polja. Na sličan način kako smo od $\mathbb{Z}$ dobili polje $\mathbb{Z}_p$ možemo konstruirati polje $\mathbb{Z}_p[x]/(f(x))$.

Teorem 1.3.3. *Neka je p prosti broj i $f(x) \in \mathbb{Z}_p[x]$. Tada je $\mathbb{Z}_p[x]/(f(x))$ konačno polje ako i samo ako je $f(x)$ ireducibilan polinom.*

Ovaj teorem nećemo dokazivati. Dokaz se provodi na sličan način kao i dokaz teorema 1.1.1. Umjesto toga ilustirat ćemo konstrukciju polja sa $2^3 = 8$ elemenata. Obrat teorema 1.2.2 daje nam egzistenciju konačnog polja sa 8 elemenata. Za njegovu konstrukciju trebamo pronaći ireducibilan polinom stupnja 3 nad poljem $\mathbb{Z}_2$. Za početak ćemo ispisati skup polinoma $\mathbb{Z}_2[x]$ do polinoma trećeg stupnja. $\mathbb{Z}_2[x] = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3.x^3+1, x^3+x, x^3+x^2, x^3+x+1, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1, ..\}$. Jedan od načina da nađemo iredcibilan polinom je množenje polinoma iz skupa $\mathbb{Z}_2[x]$ tako da dobijemo neki polinom trećeg stupnja, odnosno korištenjem Eratostenovog sita. Množenje i zbrajanje polinoma definirano je kao u propoziciji 1.3.2. Na primjer, pomnožimo $x \cdot (x+1) \cdot (x+1)$.

$$x \cdot (x+1) \cdot (x+1) = (x^2 + x) \cdot (x+1) = x^3 + 2x^2 + x.$$

Budući da se nalazimo nad poljem $\mathbb{Z}_2$ u kojem brojevi 0 i 2 pripadaju istoj klasi ekvivalencije $\overline{0}$ dobivamo da je $2x^2 = 0$ pa je umnožak polinoma jednak

$$x \cdot (x+1) \cdot (x+1) = x^3 + x.$$

Na isti način množimo ostale polinome pa imamo

$$\begin{aligned}
x \cdot x \cdot x &= x^3 \\
x \cdot x \cdot (x+1) &= x^3 + x^2 \\
(x+1) \cdot (x+1) \cdot (x+1) &= x^3 + x^2 + x + 1 \\
x \cdot (x^2+1) &= x^3 + x \\
x \cdot (x^2+x) &= x^3 + x^2 \\
x \cdot (x^2+x+1) &= x^3 + x^2 + x \\
(x+1) \cdot (x^2+1) &= x^3 + x^2 + x + 1 \\
(x+1) \cdot (x^2+x) &= x^3 + x \\
(x+1) \cdot (x^2+x+1) &= x^3 + 1
\end{aligned}$$

Na ovaj način dobili smo sve reducibilne polinome trećeg stupnja. Primijetimo da među dobivenim polinomima nema dva polinoma, $f_1(x) = x^3+x+1$ i $f_2(x) = x^3+x^2+1$. Dakle, oni su ireducibilni. Za konstrukciju polja možemo koristiti bilokoji od ta dva polinoma. Neka je $f(x) = x^3 + x + 1$.[1] Dakle, elemente polja $\mathbb{F}_{2^3} = \mathbb{Z}_2[x]/(f(x))$ dobit ćemo kao ostatke polinoma u $\mathbb{Z}_2[x]$ pri dijeljenju s $f(x)$. Budući da je ireducibilni polinom stupnja 3, ostaci će biti stupnja najviše 2. Pogledamo li ponovno skup polinoma $\mathbb{Z}_2[x]$ lako ćemo ispisati one koji su stupnja manjeg ili jednakog 2, a to su $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

[1] Kasnije ćemo pokazati da se isto polje dobije konstruiranjem polja $\mathbb{Z}_2/(x^3 + x^2 + 1)$.

Jedinica za množenje je polinom 1, a nula za zbrajanje je polinom 0. Da bismo pokazali da svaki element ima svoj inverz i suprotni element napisat ćemo tablicu množenja modulo $f(x)$, odnosno zbrajanja modulo $f(x)$. Pokažmo najprije jedan primjer kako se množe dva polinoma. Jasno je da je $x \cdot (x+1) = x^2 + x$. Međutim, na koji način smo dobili $(x^2+1) \cdot (x^2+x) = x+1$? Pomnožimo polinome s lijeve strane jednakosti.

$$(x^2+1) \cdot (x^2+x) = x^4 + x^3 + x^2 + x$$

Budući da se nalazimo u polju $\mathbb{Z}_p[x]/(x^3+x+1)$ znači da smo polinome koji se nalaze u prstenu $\mathbb{Z}_2[x]$ podijelili u klase. Polinom $f(x) = x^3 + x + 1$ nalazi se u istoj klasi kao i $g(x) = 0$. Prema tome, pišemo $f(x) = 0$, pa je

$$x^3 + x + 1 = 0 \implies x^3 = -x - 1. \tag{1.5}$$

Uvrštavanjem dobivamo da je

$$\begin{aligned}(x^2+1) \cdot (x^2+x) &= x^4 + x^3 + x^2 + x \\ &= x(-x-1) - x - 1 + x^2 + x = -x^2 - x - 1 + x^2 = -x - 1 = x + 1.\end{aligned}$$

Primijetimo da $(x^3 + x + 1)$ dijeli $(-x - 1 - (x + 1))$, pa polinomi $-x - 1$ i $x + 1$ pripadaju istoj klasi ekvivalencije. Ostatak tablice popunjen je analogno.

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Tablica 1.3: Tablica zbrajanja modulo $f(x) = x^3 + x + 1$.

$\cdot$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x	$x+1$	$x+1$

Tablica 1.4: Tablica množenja modulo $f(x) = x^3 + x + 1$.

Iz tablica vidimo da je struktura $(\mathbb{Z}_2[x]/(f(x)), +, \cdot)$ polje.

Lako smo konstruirali polje sa 8 elemenata, međutim već je konstrukcija polja sa npr. 2^5 elemenata problem jer trebamo naći ireducibilni polinom stupnja 5. Sljedeći teorem pomoći će nam da dođemo do tog polinoma.

Teorem 1.3.4. *Neka je $f \in \mathbb{F}_q[x]$ ireducibilan polinom stupnja m. Tada f dijeli $x^{p^n} - x$ ako i samo ako m dijeli n.*

Drugim riječima, polinom $x^{p^n} - x$ može se faktorizirati na ireducibilne polinome stupnjeva m takvih da m dijeli n. Tvrdnju teorema prikazat ćemo na našem primjeru. Promatrali smo polje reda $8 = 2^3$. Prema teoremu 1.3.4 polinom $x^{2^3} - x$ djeljiv je sa ireducibilnim polinomima stupnjeva 1 i 3, odnosno, možemo ga faktorizirati na ireducibilne polinome. Faktorizacijom dobivamo

$$x^{2^3} - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Na sličan način možemo dobiti ireducibilan polinom stupnja 5 faktorizacijom polinoma $x^{2^5} - x$ kojom dobivamo

$$\begin{aligned} x^{2^5} - x = x \cdot (x-1) \cdot (x^5 + x^2 + 1) \cdot (x^5 + x^3 + x^2 + x + 1) \cdot \\ (x^5 + x^4 + x^2 + x + 1) \cdot (x^5 + x^3 + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1) \cdot (x^5 + x^4 + x^3 + x + 1) \end{aligned}$$

Dakle, postoje tri ireducibilna polinoma stupnja 5. Teorem 1.3.4 navodi nas na sljedeći zaključak.

Teorem 1.3.5. *Za svako konačno polje $\mathbb{F}$ i prirodni broj n postoji ireducibilan polinom stupnja n nad poljem $\mathbb{F}$.*

Iz svega prikazanog slijedi teorem.

Teorem 1.3.6. *Konačno polje reda n postoji ako i samo ako je n potencija prostog broja.*

Nama je još preostalo pokazati da izborom različitih ireducibilnih polinoma istog stupnja dobivamo izomorfna polja.

Teorem 1.3.7. *Svako konačno polje $\mathbb{F}_q$ karakteristike p i reda q je izomorfno polju ostataka polinoma $\mathbb{F}_p[x]/(g(x))$ gdje je $g(x)$ ireducibilan polinom u $\mathbb{F}_p[x]$ stupnja m. Uz to, vrijedi da je $q = p^m$ za m prirodni broj.*

Ilustrirajmo izomorfizam na našem primjeru. Uzmimo α takav da vrijedi $\alpha^3+\alpha^2+1 = 0$ i β takav da $\beta^3 + \beta + 1 = 0$. Iz toga slijedi da je:

$$\beta^3 + \beta + 1 = 0 \iff \beta^3 \cdot (1 + \beta^{-2} + \beta^{-3}) = 0$$

Primijetimo da je β^{-1} nultočka polinoma $x^3 + x^2 + 1$ stoga možemo napraviti preslikavanje $\alpha \mapsto \beta^{-1}$. Podijelimo li $\beta^3 + \beta + 1 = 0$ sa β^{-1} dobivamo $\beta^{-1} = \beta^2 + 1$ pa imamo $\alpha \mapsto \beta^2 + 1$. Ispišimo dalje sva preslikavanja.

$$\begin{aligned}
\alpha &\mapsto \beta^2 + 1 \\
\alpha^2 &\mapsto \beta^2 + \beta + 1 \\
\alpha^2 + 1 &\mapsto \beta^2 + \beta \\
\alpha^2 + \alpha + 1 &\mapsto \beta + 1 \\
\alpha + 1 &\mapsto \beta^2 \\
\alpha^2 + \alpha &\mapsto \beta \\
1 &\mapsto 1
\end{aligned}$$

Prikazano preslikavanje je izomorfizam.

Poglavlje 2

Projektivne i afine ravnine

U drugom poglavlju napravit ćemo uvod u projektivne i afine ravnine. Afine i projektivne ravnine primjeri su incidencijskih struktura kao i dizajni koje ćemo proučavati u trećem poglavlju. Prikazat ćemo osnovne definicije i teoreme te ćemo pokazati nekoliko primjera gdje se takve strukture pojavljuju. Posebno ćemo obratiti pažnju na konačne ravnine koje ćemo konstruirati pomoću konačnih polja.

2.1 Afina ravnina

Upoznajmo se najprije s terminologijom.

Definicija 2.1.1. Incidencijska struktura *je uređena trojka* $(\mathcal{T}, \mathcal{B}, I)$ *pri čemu je* $\mathcal{T}$ *skup čije elemente zovemo* točkama*,* $\mathcal{B}$ *je skup čije elemente zovemo* blokovima *ili* pravcima*, a* $I \subseteq \mathcal{T} \times \mathcal{B}$ *je* relacija incidencije*.*

Ako vrijedi $(A, p) \in I$ kažemo da točka A leži na pravcu p ili da pravac p prolazi kroz točku A. Nama najpoznatija afina ravnina je ona euklidska. Općenito, afina ravnina je incidencijska struktura koja zadovoljava neka ista svojstva kao i ona euklidska. Pogledajmo koja su to svojstva.

Definicija 2.1.2. *Incidencijsku strukturu* $\mathcal{A} = (\mathcal{T}, \mathcal{B}, I)$ *nazivamo* afina ravnina*, ako su zadovoljeni aksiomi:*

(A1) za svake dvije točke A, B *postoji točno jedan pravac* p *takav da vrijedi*

$$(A, p) \in I \text{ i } (B, p) \in I;$$

(A2) za svaki pravac q *i svaku točku* C *koja ne leži na* q *postoji točno jedan pravac* p *takav da je* $(C, p) \in I$ *i* p *nema zajedničkih točaka sa* q*;*

(A3) postoje tri različite nekolinearne točke.

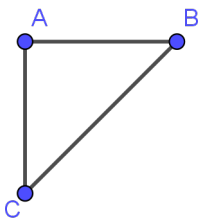
Pravce koji zadovoljavaju aksiom $(A2)$ nazivamo *paralelni pravci*. Preciznije, *relaciju paralelnosti* $\parallel$ definiramo na skupu $\mathcal{B}$ tako da za dva pravca $p, q \in \mathcal{B}$ kažemo da su paralelni ako je $p = q$ ili $p \cap q = \emptyset$ i pišemo $p \parallel q$. Lako se pokaže da je relacija paralelnosti relacija ekvivalencije. Klase ekvivalencije su klase paralelnih pravaca i svaku klasu nazivamo *smjerom*.

Neka je $\mathbb{F}$ polje. Afinu ravninu nad poljem $\mathbb{F}$ možemo konstruirati tako da nam točke predstavljaju uređeni parovi $(x, y) \in \mathbb{F}^2$, a pravci su prikazani jednadžbama $y = kx + l$ ili $y = a$ za neke $a, k, l \in \mathbb{F}$. Na taj način dobivamo da su točke oblika

$$\{(x, kx + l) : x \in \mathbb{F}\}, \text{ za } k, l \in \mathbb{F},$$
$$\{(a, y) : y \in \mathbb{F}\} \text{ za sve } a \in \mathbb{F}.$$

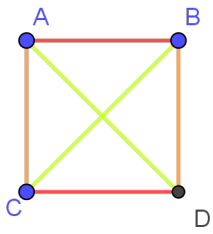
Pri tome kažemo da točka A leži na pravcu p ako zadovoljava linearnu jednadžbu. Afinu ravninu nad poljem $\mathbb{F}$ označavamo sa $AG(\mathbb{F})$. Euklidsku ravninu dobijemo konstrukcijom afine ravnine nad poljem $\mathbb{R}$. Afinu ravninu koja ima konačan broj točaka nazivamo konačna afina ravnina.

Pokažimo koliko najmanje točaka treba imati afina ravnina. Zbog aksioma $(A3)$ postoje barem tri točke, a prema $(A1)$ svake dvije točke spojene su jednim pravcem.



Slika 2.1: Tri nekolinearne točke i pravci

Osim točke C koja je nekolinearna s A i B, prema aksiomu $(A2)$ postoji pravac paralelan s AB kroz točku C. Također, kroz točku A postoji pravac paralelan s BC, a kroz točku B pravac paralelan s AC. Pravci kroz A, B i C nisu paralelni. To se lako pokaže korištenjem tranzitivnosti relacije paralelnosti. Neka se ta tri pravca sijeku u jednoj točki D. Tada dobivamo najmanju afinu ravninu sa 4 točke i 6 pravaca i prikazujemo ju kao na slici 2.2. Pri tome istobojni pravci predstavljaju par paralelnih pravaca.

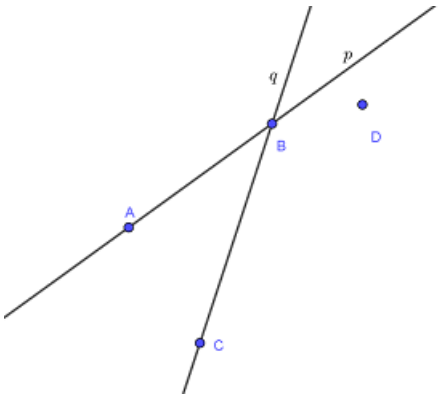


Slika 2.2: Afina ravnina reda 2

Lako se pokaže da se na svakom pravcu nalaze barem dvije točke. Treba li na svakom pravcu biti jednak broj točaka? Odgovor nam daje iduća propozicija.

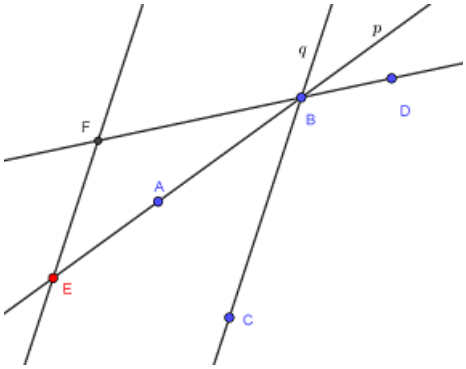
Propozicija 2.1.3. *U konačnoj afinoj ravnini, na svakom pravcu leži jednak broj točaka.*

Dokaz. Uzmimo prvo dva pravca, p i q, koji nisu paralelni. Sjecište označimo sa B. Na svakom pravcu nalaze se barem dvije točke. Neka se na pravcu p nalazi točka A i na pravcu q točka C takve da su A i C različite od B. Prethodno smo vidjeli da afina ravnina sadrži barem 4 točke. Neka je točka D takva da ne leži niti na p niti na q.



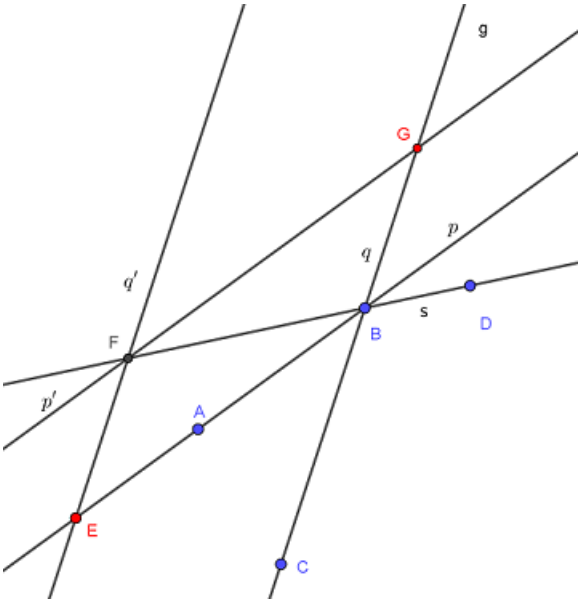
Slika 2.3: Pravci p i q sijeku se u B

Povucimo pravac koji prolazi kroz B i D i označimo ga sa s. Neka je točka E točka na pravcu p. Povucimo kroz točku E pravac paralelan sa pravcem q i označimo ga sa q'. Takav pravac postoji prema aksiomu $(A2)$. Sjecište pravaca q' i s označimo sa točkom F. Zbog tranzitivnosti relacije paralelnosti pravci q' i s nisu paralelni pa postoji njihovo sjecište.



Slika 2.4: Sjecište pravaca q' i s je točka F

Kroz točku F povucimo paralelan pravac sa pravcem p i označimo ga sa p'. Sjecište q i p' označimo sa G. Na ovaj način dodali smo jednu točku na pravac p i jednu na pravac q.



Slika 2.5: Sjecište pravaca p' i q je točka G

Ovaj postupak možemo ponavljati. U svakom trenutku broj točaka na pravcu p veći je ili jednak broju točaka na pravcu q. Zamijenimo li uloge pravaca p i q dobit ćemo da je broj točaka na q veći ili jednak broju točaka na p, pa zbog konačnosti možemo zaključiti da je

broj točaka na p i q jednak.
Drugi slučaj je kada su pravci paralelni. Nazovimo ih m i l. Neka je na pravcu m točka A i na pravcu l točka B. Pravac koji prolazi kroz točke A i B označimo sa p. Primijetimo da p nije paralelan niti sa m niti sa l. Neka je točka C točka na pravcu m (ako postoji). Kroz točku C povucimo pravac paralelan sa p i označimo ga sa p'. Pravac p' siječe pravac l. Označimo sjecište sa K'. Iste argumente koje smo koristili u prethodnom slučaju možemo iskoristiti i u ovome. Dakle, na svakom pravcu nalazi se jednak broj točaka. □

Afinu ravninu u kojoj na svakom pravcu leži n točaka nazivamo afina ravnina reda n i označavamo je sa $AG(2, n)$.

Teorem 2.1.4. *Za konačnu ravninu reda n vrijedi:*

(1) svaka točka leži na $n + 1$ *pravaca.*

(2) ukupno ima $n + 1$ *smjerova.*

(3) ukupno ima n^2 *točaka.*

(4) ukupno ima $n^2 + n$ *pravaca.*

Dokaz. (1) Neka su A i B točke u afinoj ravnini reda n. Ako na pravcu AB leže sve točke afine ravnine tada nije zadovoljen aksiom $(A3)$. Dakle, postoji točka C koja nije na pravcu AB. Neka je c pravac paralelan sa AB koji prolazi točkom C. Budući da je afina ravnina reda n tada na pravcu c leži n točaka. Označimo te točke sa $A_1, A_2, .., A_n$. Bez smanjenja općenitosti, neka je $C = A_1$. Povucimo pravce $AA_1, AA_2, .., AA_n$. Primijetimo da se niti jedan od pravaca AA_j ne podudara s pravcem AB jer su AB i c paralelni. Dakle, kroz točku A prolazi $n + 1$ pravaca. Kada bi kroz točku A prolazio još jedan pravac, označimo ga sa p, tada bi pravac p sijekao i pravac c u točki koja je različita od A_j. Tada na pravcu c imamo $n + 1$ točaka. To je nemoguće jer se pravac nalazi u afinoj ravnini reda n.

(2) Svaki pravac koji prolazi kroz jednu točku afine ravnine određuje jedan smjer pa je zbog (1) ukupni broj smjerova $n + 1$.

(3) U (1) smo pokazali da kroz svaku točku A prolazi $n + 1$ pravac. Također, kako na svakom pravcu leži n točaka, tada na svakom pravcu kroz točku A leži $n - 1$ točaka različitih od točke A pa je ukupni broj točaka

$$(n - 1)(n + 1) + 1 = 1 + n^2 - 1 = n^2.$$

(4) Ukupno imamo n^2 točaka i kroz svaku točku prolazi $n + 1$ pravaca. Međutim, svaki smo pravac brojali n puta pa je ukupni broj pravaca

$$\frac{n^2(n+1)}{n} = n^2 + n.$$

□

2.2 Igra SET

Prvi primjer koji ćemo promatrati je društvena igra SET. Igra se sastoji od 81 karte. Na svakoj karti nalaze se objekti koji se razlikuju u četiri svojstva prikazana u tablici 2.1. Svojstva su oblici (romb, ovalni i nepavilni), boje (crvena, zelena i ljubičasta), ispunjenosti (puna boja, istrtkano i prazni) i broj (jedan, dva ili tri lika).

BOJA	CRVENA	ZELENA	LJUBIČASTA
BROJ	JEDAN	DVA	TRI
OBLIK	OVALNI	ROMB	NEPRAVILNI
ISPUNJENJE	ISCRTKANO	PRAZNO	PUNO

Tablica 2.1: Vrste karata u igri SET

Cilj igre je naći SET među 12 otvorenih karata. SET se sastoji od tri karte na kojima su svojstva ili sva ista ili sva različita. Na primjer, tri karte na kojima su po dva romba, na svakoj karti drukčije boje i svaki drukčije ispunjenosti čine SET.
Osim što je zabavna, igru SET možemo modelirati pomoću afinog prostora. Neka je V 4-dimenzionalni vektorski prostor nad poljem $\mathbb{Z}_3$. Svaku kartu prikazat ćemo kao vektor u V tako da će prva koordinata označavati boju, druga broj, treća oblik i četvrta ispunjenje na karti. Budući da se nalazimo nad poljem $\mathbb{Z}_3$ koordinate poprimaju vrijednosti $\overline{0}, \overline{1}$ ili $\overline{2}$. Radi jednostavnosti, gledajmo klase ekvivalencije kao brojeve 0, 1 i 2. Sa 0 označimo svojstva iz drugog stupca tablice 2.1, sa 1 svojstva iz trećeg stupca, a sa 2 svojstva iz četvtog stupca. Tada npr. vektor $(0, 1, 1, 2)$ predstavlja kartu na kojoj se nalaze dva crvena puna romba, vektor $(1, 2, 2, 1)$ predstavlja tri zelena prazna nepravilna oblika, itd. U tom slučaju, SET predstavljaju tri vektora kojima je zbroj jednak $\vec{0}$. Pokažimo da je to ustinu tako. Promatrat ćemo samo prvu koordinatu. Da bismo dobili SET boja na sve tri karte mora biti ili različita ili ista. Ako je boja na sve tri karte različita tada je zbroj prvih koordinata triju vektora jednak $0+1+2 = 3$ (do na poredak) što je kongruentno $0 \pmod 3$ pa umjesto 3 možemo napisati 0. Ako su boje na kartama jednake tada je dobiveni zbroj višekratnik broja 3 (jer zbrajamo tri ista broja) što je opet kongruentno $0 \pmod 3$ pa kao i

u prethodnom slučaju možemo pisati 0. Iste argumente koristimo za zbrajanje ostalih triju koordinata. Budući da ne postoji drugi način za dobivanje SET-a zaključujemo da zbroj triju vektora koji daju SET jednak 0. Prikažimo sada vezu sa afinim prostorom. Model je preuzet iz članka *Geometric models of the card game SET* Cherith Tuckera [11]. Neka je $AG(4,3)$ 4-dimenzionalni afini prostor reda 3. Pravci prostora dani su kao $\{v+kw : k \in \mathbb{Z}_3\}$, za neke $\vec{v}, \vec{w} \in \mathbb{Z}_3^4$. Tada vrijedi sljedeći teorem.

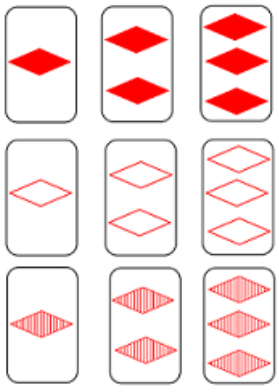
Teorem 2.2.1. *Tri karte tvore SET ako i samo ako su njihove točke u* $AG(4,3)$ *kolinearne.*

Dokaz. Neka su v_1, v_2, v_3 vektori u $AG(4,3)$. Vektori v_1, v_2, v_3 tvore SET ako i samo ako vrijedi

$$\begin{aligned} & v_1 + v_2 + v_3 = 0 \\ \iff & v_1 + (v_1 + (v_2 - v_1)) + (v_1 - (v_2 - v_1)) = 0 \end{aligned}$$

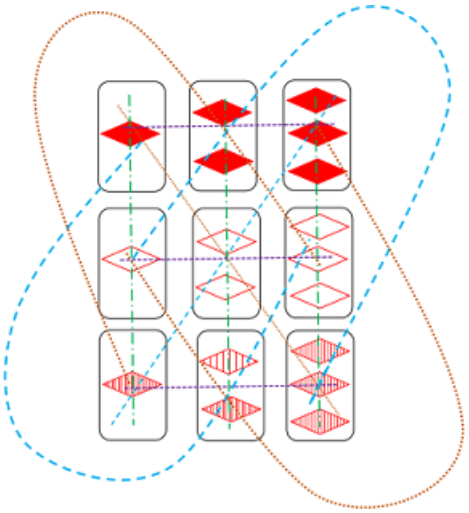
Pritom smo koristili da nad $\mathbb{Z}_3$ vrijedi $v_3 = -v_1 - v_2 = 2v_1 - v_2$. Sada primijetimo da su vektori v_1, v_2, v_3 oblika $\{v_1 + k(v_2 - v_1) : k \in \mathbb{Z}_3\}$ pa se nalaze na istom pravcu, tj. kolinearni su. □

Da bismo lakše vidjeli poveznicu s afinom ravninom promotrimo sljedeći slučaj. Uzmimo od 81 karte one sa istom bojom, npr. crvenom, i istim oblikom npr. romb. Tada imamo ukupno 9 karata. Ako koristimo prikaz kao uređene četvorke one su oblika $(0, x, 1, y)$ za $x, y \in \mathbb{Z}_3$. Budući da su prva i treća koordinata jednake za svaku kartu umjesto uređene četvorke možemo gledati uređene parove (x, y). Sa x je označen broj objekata na karti, a sa y ispunjenost. Vrijednosti za x i y određuju se na isti način kao i u uređenim četvorkama. Na slici 2.6 prikazano je koje karte imamo.



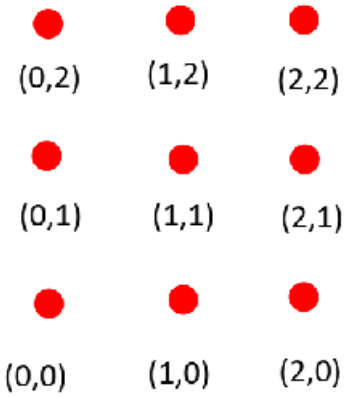
Slika 2.6: Crvene karte-romb

Koje od tih 9 karata čine SET? Na slici 2.7 karte koje čine SET spojene su istom bojom.



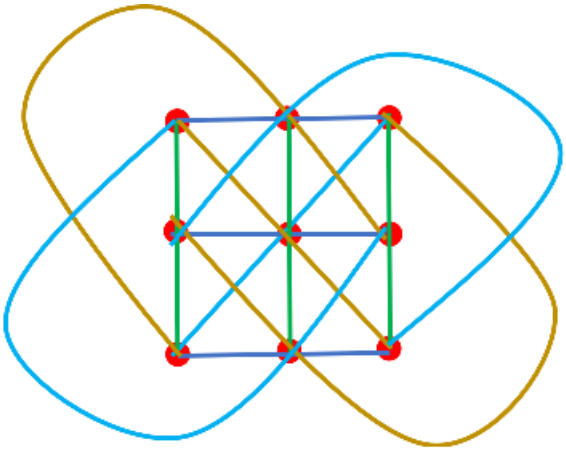
Slika 2.7: SET-ovi

SETovi su obojeni u četiri različite boje. Zamijenimo sada karte sa točkama s koordinatama (x, y) u koordinatnom sustavu $\mathbb{Z}_3 \times \mathbb{Z}_3$.



Slika 2.8: Koordinatni prikaz

Spojimo točke koje tvore SET.



Slika 2.9: Afina ravnina reda 3

Lako je vidljivo da se točke nalaze na pravcima $y = 0$, (točke $(0,0),(1,0),(2,0)$), $y = 1$ (točke $(0,1),(1,1),(2,1)$), $y = 2$ (točke $(0,2),(1,2),(2,2)$). Također, lako odredimo koje točke leže na pravcima $x = 0$, $x = 1$ i $x = 2$. Dalje imamo pravac $y = x$ sa točkama $(0,0),(1,1),(2,2)$. Međutim i točke $(0,1),(1,2),(2,0)$ leže na istom pravcu, $y = x + 1$. Slično možemo dobiti svaki pravac na kojem se nalaze po tri točke. Pravci su oblika $y = kx + l$ za $k, l \in \mathbb{Z}_3$. Istobojni pravci predstavljaju smjerove odnosno klase ekvivalencije relacije paralelnosti. Dobivena struktura je afina ravnina reda 3 u oznaci $AG(2,3)$ odnosno Hesseova konfiguracija.

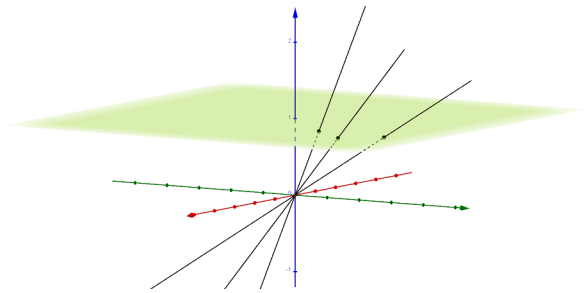
2.3 Veza projektivne i afine ravnine

Na slici 2.10 tračnice koje se protežu u daljinu izgledaju kao da su sve uže i da se lijeva i desna tračnica sijeku u jednoj točki. Iz iskustva znamo da to nije tako. Takav privid događa se zbog perspektive.

Slika 2.10: Točka nedogleda

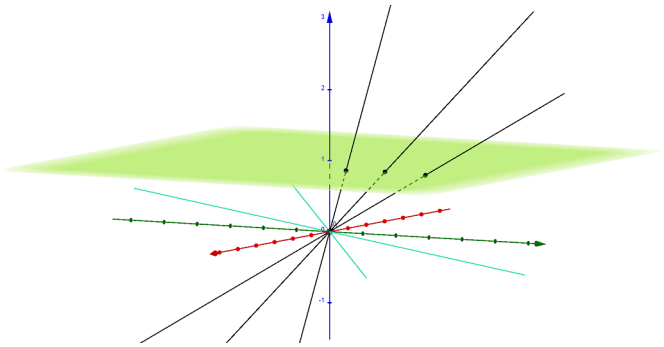
Perspektiva je način prikazivanja onoga što vidimo u tri dimenzije na ravninu projekcije. Stvaranje perspektivne slike zasniva se na linearnom smanjenju predmeta s obzirom na udaljenost predmeta od gledaoca. Isto tako, postoji jedna točka u kojoj se sijeku sve linije okomite na ravninu projekcije. Ta točka naziva se točka nedogleda, a mi ju doživljavamo kao točku u beskonačnosti u kojoj se sijeku paralelne linije. Ta teza nije u skladu s onime što znamo iz euklidske geometrije. Međutim postoji matematički sustav u kojem je to dozvoljeno i nazivamo ga projektivna geometrija. Projektivna geometrija postupno se razvijala, a najznačajniji koraci dogodili su se u 17. i 19. stoljeću. U projektivnoj geometriji promatramo projektivne prostore. Posebno, ako je prostor dimenzije 2 onda govorimo o projektivnoj ravnini. Projektivnu ravninu možemo dobiti iz afine ravnine dodavanjem točaka u beskonačnosti, u kojima se sijeku paralelni pravci i dodavanjem pravca u beskonačnosti na kojem se nalaze sve točke u beskonačnosti.

Promotrimo sliku 2.11. Na slici je prikazana afina ravnina $z = 1$. Primijetimo da za svaku točku ravnine $z = 1$ postoji jedan pravac kroz ishodište koji probada ravninu u toj točki. Projektivnu ravninu dobijemo tako da nam pravci kroz ishodište predstavljaju točke u projektivnoj ravnini, odnosno, sve točke na pravcu identificiramo sa točkom u kojoj pravac kroz ishodište siječe ravninu $z = 1$.



Slika 2.11: Projektivna i afina ravnina

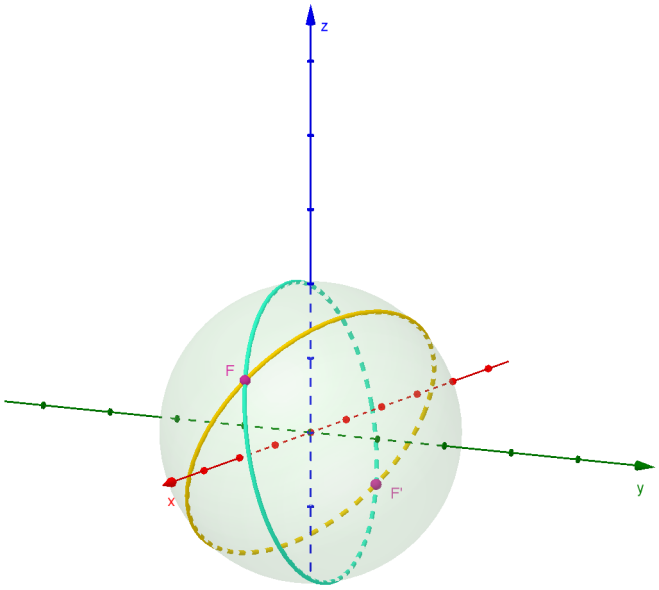
Promotrimo sada pravce kroz ishodište koji leže u ravnini $z = 0$. Nacrtani su plavom bojom na slici 2.12.



Slika 2.12: Projektivna i afina ravnina

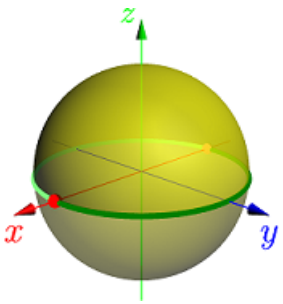
Pravci u xy ravnini ne probadaju ravninu $z = 1$. Za te pravce u projektivnoj ravnini definiramo točke u beskonačnosti u kojima se sijeku sa paralelnim pravcima ravnine $z = 1$. Iz ovog prikaza vidimo da iz afine ravnine možemo dobiti projektivnu ravninu. Štoviše, iz projektivne ravnine može se konstruirati afina ravnina.

Drugi način za prikaz projektivne ravnine je pomoću sfere. Neka nam pravce predstavljaju kružnice koje dobijemo presjekom ravnine kroz središte i površine sfere, a točke neka su nam parovi antipodalnih točaka na sferi. Na slici 2.13 prikazano je sjecište dviju kružnica, odnosno pravaca ako govorimo u terminima projektivne ravnine. Takvom konstrukcijom dobivamo da se svake dvije kružnice (pravci) sijeku u paru antipodalnih točaka. Slično kako smo pravce kroz ishodište identificirali sa jednom točkom u ravnini $z = 1$ u prethodnoj ilustraciji, tako točke koje se nalaze na donjoj polusferi identificiramo njihovim antipodalnim točkama iz gornje polusfere.



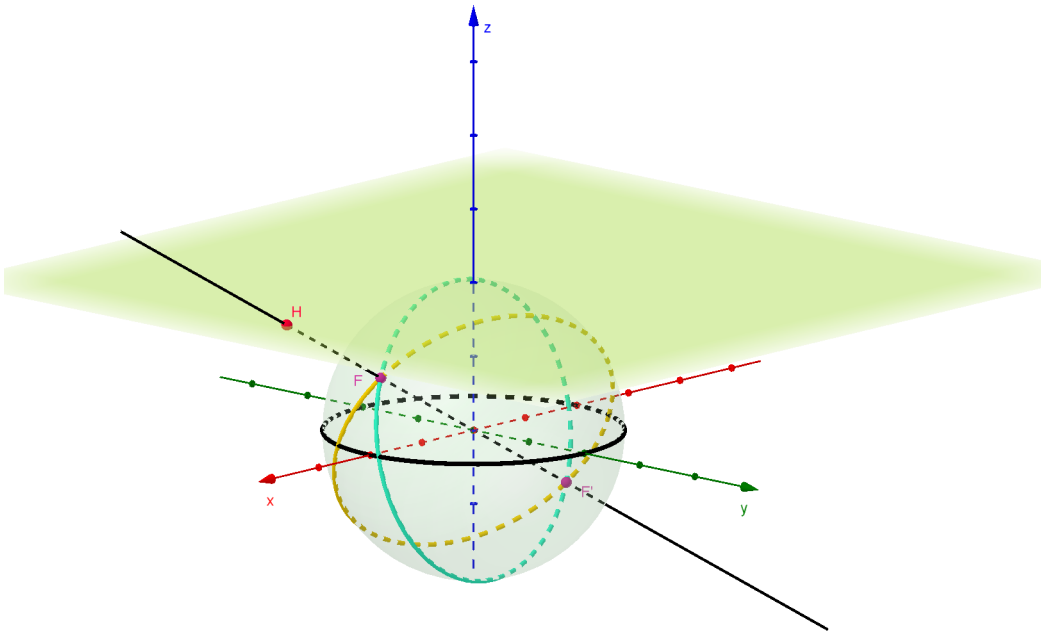
Slika 2.13: Dvije kružnice (pravci) sijeku se u paru antipodalnih točaka F i F'

Projektivnu ravninu u tome slučaju dobivamo particijom sfere na klase ekvivalencije pri relaciji $\sim$ gdje je $x \sim y$ ako vrijedi $y = -x$. Drugačije rečeno, točke su u istoj klasi ako i samo ako su antipodalne. Na slici 2.13 točke F i F' pripadaju istoj klasi jer su antipodalne. Prikaz projektivne ravnine tada je dan slikom 2.14.



Slika 2.14: Projektivnu ravninu predstavlja žuto obojena hemisfera, tamno zeleno obojana polukružnica i crvena točka na osi x; Preuzeto iz [2].

Veza prikaza projektivne ravnine pomoću sfere i afine ravnine slična je kao u prvom slučaju. Na slici 2.15 vidimo da pravac kroz ishodište probada gornju polusferu i ravninu $z = 1$ u jednoj točki.



Slika 2.15: Pravac kroz središte sfere siječe gornju polusferu i ravninu $z = 1$ u jednoj točki.

Svaku točku polusfere možemo identificirati sa točkom iz afine ravnine $z = 1$. Konkretno, na slici 2.15 točku F identificiramo s točkom H. Promotrimo li pravce u xy ravnini vidimo da oni ne sijeku ravninu $z = 1$. Za njih dodajemo točke u beskonačnosti u kojima se sijeku sa paralelnim pravcima iz zadane ravnine.

2.4 Projektivna ravnina

Prethodno smo vidjeli na koji način se projektivna ravnina može dobiti iz afine ravnine. Definirajmo je sada aksiomima.

Definicija 2.4.1. *Incidencijska struktura* $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ *naziva se* projektivna ravnina *ako su zadovoljeni aksiomi:*

(P1) svake dvije točke leže na točno jednom pravcu;

(P2) za svaka dva različita pravca p i q postoji točka A tako da vrijedi

$$(A, p) \in I \text{ i } (A, q) \in I;$$

(P3) postoje četiri različite točke takve da nikoje tri od njih nisu kolinearne, to jest da nisu sve tri incidentne s nekim pravcem.

Iz aksioma $(P2)$ vidimo da u projektivnoj ravnini ne postoje paralelni pravci. U prethodnom smo potpoglavlju vidjeli na koji način se može dobiti projektivna ravnina iz afine. Pokažimo sada kako se konstruira pomoću vektorskog prostora. Teorem je preuzet iz [9].

Teorem 2.4.2. *Neka je V vektorski prostor dimenzije 3 nad poljem* $\mathbb{F}$*. Definiramo incidencijsku strukturu* $\mathcal{P} = (\mathcal{T}, \mathcal{B}, I)$ *tako da je* $\mathcal{T}$ *skup svih 1-dimenzionalnih potprostora,* $\mathcal{B}$ *skup svih 2-dimenzinalnih potrostora prostora V, a I relacija inkluzije među skupovima. Tada je* $\mathcal{P}$ *projektivna ravnina koju označavamo sa* $PG(2, \mathbb{F})$*. Posebno, ako je* $\mathbb{F}$ *konačno polje reda n, onda je* $PG(2, \mathbb{F}) = PG(2, n)$ *projektivna ravnina reda n.*

Dokaz. Iz linearne algebre znamo da je presjek dvaju vektorskih potprostora također vektorski potprostor. Isto tako, svaka dva potprostora nalaze su u svojoj sumi tj. ako su A i B potprostori tada su oni sadržani u $A + B$ i taj prostor je jedinstven. Pokažimo da vrijede aksiomi $(P1) - (P3)$. Svaka dva 1-dimenzionalna potprostora, označimo ih sa P i Q, su dio potprostora $P + Q$ i taj prostor je jedinstven za svaki P i Q. S druge strane, budući da svi 2-dimenzionalni potprostori moraju sadržavati nul-vektor onda se sigurno sjeku. Dimenziju presjeka možemo izračunati pomoću formule $\dim(U+W) = \dim(U)+\dim(W)-\dim(U\cap W)$. Pri tome je $\dim(U + W) = \dim(V) = 3$. Ove rezultate možemo vizualizirati pomoću euklidske ravnine. 1-dimenzionalni potprostori su pravci kroz ishodište, a 2-dimenzinalni potprostori ravnine koje sadržavaju ishodište. U tom slučaju, svaka dva pravca leže u točno jednoj ravnini koja prolazi kroz ishodište, a svake dvije ravnine sijeku se po točno jednom pravcu. Aksiom $(P3)$ također je zadovoljen jer u vektorskom prostoru nad bilo kojim poljem postoje vektori $(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)$ od kojih nikoja tri nisu linearno zavisna, tj. ne leže u istoj ravnini.

Pogledajmo sada vektorski prostor nad konačnim poljem. Uzmimo konačno polje reda n. Najprije ćemo pokazati da u projektivnoj ravnini reda n na svakom pravcu leži $n + 1$ točaka. U prethodnom smo potpoglavlju dokazali da se na svakom pravcu afine ravnine nalazi n točaka. Projektivnu ravninu dobijemo dodavanjem jedne točke u svakom smjeru i pravca na kojem leže te točke. Budući da postoji $n + 1$ smjerova slijedi da se svakom pravcu projektivne ravnine reda n nalazi $n + 1$ točaka. Dakle, da bi konstrukcijom dobili projektivnu ravninu trebamo prebrojati koliko točaka se nalazi na bilo kojem pravcu. U našim terminima, tražimo koliko 1-dimenzinalnih potrostora sadrži svaki 2-dimenzionalni potprostor. U svakom dvodimenzinalnom potprostoru postoji n^2 vektora od kojih je $n^2 - 1$ različit od nulvektora. S druge strane, svaki 1-dimenzinalni potprostor sadrži $n - 1$ ne-nulvektor. Iz toga slijedi da u svakom 2-dimenzionalnom potprostoru postoji $\frac{n^2-1}{n-1} = n+1$ 1-dimenzionalni potprostor. Time dobivamo da je red projektivne ravnine jednak $n+1-1 = n$ što smo htjeli i pokazati. □

Od posebnog interesa su nam konačne projektivne ravnine. Konačna projektivna ravnina je ravnina koja ima konačan broj pravaca i točaka.

Teorem 2.4.3. *Za konačnu projektivnu ravninu red n vrijedi:*

(1) ukupan broj točaka je $n^2 + n + 1$

(2) svaka točka nalazi se na $n + 1$ *pravaca*

Dokaz. (1) Slično kako je u prethodnom teoremu pokazano da na svakom pravcu leži $n + 1$ točaka, možemo pokazati koliki je ukupan broj točaka. Uzmimo konačno polje reda n i vektorski prostor V nad tim konačnim poljem. Ukupan broj vektora različitih od nulvektora je $n^3 - 1$. S druge strane, u svakom 1-dimenzionalnom potprostoru nalazi se $n - 1$ vektora. Iz toga zaključujemo da je ukupan broj 1-dimenzionalnih prostora

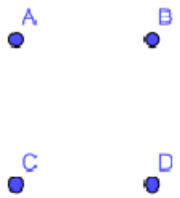
$$\frac{n^3 - 1}{n - 1} = n^2 + n + 1.$$

(2) Neka je P točka, a l pravac u projektivnoj ravnini. Ako vrijedi $P \notin l$ tada za svaku točku $Q \in l$ postoji pravac koji spaja točke P i Q. Neka su l i m dva različita pravca. Prema aksiomu $(P3)$ postoji točka P koja ne leži niti na l niti na m. Prema aksiomu $(P1)$ postoje pravci koji spajaju točku P sa svakom od točaka na pravcima l i m. Tada je, s jedne strane, broj pravaca kroz točku P jednak broju točaka na pravcu l, a s druge strane broj pravaca kroz točku P jednak je broju točaka koje leže na pravcu m. Možemo zaključiti da je broj točaka na pravcima l i m jednak. Kako na jednom pravcu leži $n + 1$ točaka, broj pravaca kroz P jednak je $n + 1$.

□

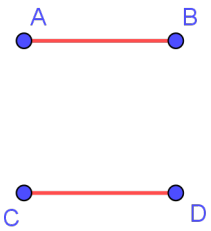
Primijetimo da su svojstva točaka i pravaca simetrična. Na primjer, aksiom ($P2$) možemo izreći i na sljedeći način: svaka dva pravca imaju jedinstveno sjecište. To je istina jer kad bi dva pravca imala dva sjecišta, odnosno dvije zajedničke točke tada bi dvije točke ležale na dva različita pravca što ne može biti zbog aksioma ($P1$). Ukratko, iz svake istinite tvrdnje dobiva se istinita tvrdnja tako da umjesto „točaka" pišemo „pravci", umjesto „leže na" pišemo „prolaze kroz" itd. Ovaj princip naziva se princip dualnosti.

Pogledajmo sada koji je najmanji broj točaka koji treba sadržavati projektivna ravnina. Iz aksioma vidimo da postoje barem 4 točke. Iz aksioma ($P2$) i ($P3$) možemo zaključiti da na svakom pravcu leže tri točke. Pogledajmo zašto. Neka su četiri točke koje zadovoljavaju aksiom ($P3$) točke A, B, C i D kao na slici 2.16.



Slika 2.16: Točke od kojih nikoje tri nisu kolinearne

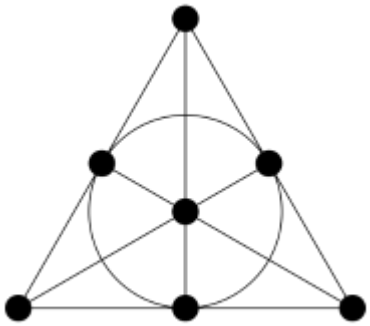
Aksiom ($P1$) kaže da svake dvije točke leže na jednom pravcu. Povucimo pravac kroz točke A i B (u oznaci AB) te kroz točke C i D (u oznaci CD). Pravce prikazujemo kao spojnice točaka.



Slika 2.17: Pravci kroz A i B te C i D

S ovakvim rasporedom točaka dobili smo par paralelnih pravaca (paralelni u euklidskoj geometriji). Aksiom ($P2$) zahtijeva da za svaka dva različita pravca postoji točka koja leži

na oba pravca. Prema tome, pravci AB i CD moraju imati zajedničku točku. U tu svrhu uvodimo točku u beskonačnosti u kojoj će se sijeći svi pravci paralelni sa pravcima AB i CD. Isti postupak možemo ponoviti ako gledamo pravce CA i DB. Sada smo dodali već dvije točke pa ih imamo ukupno šest. Međutim trebamo još dodati i sjecište pravaca AD i BC. Na taj način dobili smo ukupno 7 točaka i 7 pravaca. Dobivenu projektivnu ravninu nazivamo *Fanova ravnina* i možemo ju prikazati kao na slici 2.18.



Slika 2.18: Fanova ravnina; Preuzeto iz [3]

Fanova ravnina je projektivna ravnina reda 2. Ako u konstrukciji nemamo paralelne pravce jednostavno dodajemo sjecišta svih pravaca. Na slici vidimo da je jedan pravac u Fanovoj ravnini prikazan kao kružnica. Je li moguće točke rasporediti tako da pravci Fanove ravnine budu ravne linije, odnosno možemo li Fanovu ravninu prikazati u euklidskoj ravnini? Na to nam odgovor daje sljedeći teorem.[1]

Teorem 2.4.4 (Sylvester-Gallai teorem)**.** *Ako se n točaka ne nalazi na jednom pravcu, onda postoji pravac koji prolazi kroz točno dvije od njih.*

Kellyjev dokaz. Ovaj dokaz izveo je američki matematičar Leroy Milton Kelly. Pretpostavimo da u skupu od n točaka nisu sve kolinearne. Definiramo spojnicu kao pravac koji spaja barem dvije od točaka iz skupa. Neka su točka A i spojnica l takvi da je udaljenost među njima najmanja od svih udaljenosti među parovima točka-spojnica. Dokazat ćemo da je spojnica l pravac koji prolazi kroz točno dvije od n točaka u skupu.
Pretpostavimo da l prolazi kroz barem tri točke. Neka je A' ortogonalna projekcija točke A na spojnicu l. Tada postoje barem dvije točke koje leže na spojnici l s iste strane točke

[1] Teorem i dokaz preuzeti su iz [4]

A'. Neka su to točke B i C i neka je točka B bliže točki A'. Povucimo spojnicu kroz A i C i označimo je sa m. Neka je B' ortogonalna projekcija točke B na spojnicu m. Trokuti $BB'C$ i $AA''C$ su slični pa kako je duljina dužine $\overline{BC}$ manja od duljine dužine $\overline{AC}$ slijedi da je duljina dužine $\overline{BB'}$ manja od duljine dužine $\overline{AA'}$. Međutim, to je u kontradikciji s tim da je udaljenost između točke A i spojnice l najmanja od svih udaljenosti između parova točka-spojnica. Dakle, l prolazi kroz točno dvije točke. □

U našem slučaju imamo 7 točaka od kojih nisu sve kolinearne, a na svakom pravcu imamo tri točke. Stoga Fanovu ravninu ne možemo prikazati u euklidskoj ravnini koristeći samo pravce.

Konstrukciju Fanove ravnine možemo provesti i primjenom teorema 2.4.2. Neka je $V = (\mathbb{Z}_2)^3$ vektorski prostor nad poljem $\mathbb{Z}_2$. Vektore ćemo pisati u obliku (x_1, x_2, x_3) gdje su $x_i \in \mathbb{Z}_2, i = 1, 2, 3$. Ispišimo sve 1-dimenzionalne potprostore.

$$\{(0,0,0),(0,0,1)\}$$
$$\{(0,0,0),(0,1,0)\}$$
$$\{(0,0,0),(1,0,0)\}$$
$$\{(0,0,0),(0,1,1)\}$$
$$\{(0,0,0),(1,0,1)\}$$
$$\{(0,0,0),(1,1,0)\}$$
$$\{(0,0,0),(1,1,1)\}.$$

Primijetimo da postoji točno sedam 1-dimenzinalnih potprostora, što smo i očekivali. Ispišimo sada sve 2-dimenzionalne potprostore.

$$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}$$
$$\{(0,0,0),(0,0,1),(1,0,0),(1,1,0)\}$$
$$\{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}$$
$$\{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\}$$
$$\{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}$$
$$\{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\}$$
$$\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$$

Možemo primijetiti da se svaka dva 2-dimenzionalna potprostora sijeku u točno jednom 1-dimenzionalnom potprostoru, te da se svaka dva 1-dimenzionalna prostora nalaze u točno jednom 2-dimenzionalnom prostoru što odgovara aksiomima projektivne ravnine.

Za koje sve prirodne brojeve n možemo konstruirati projektivnu ravninu reda n? Još uvijek postoje otvoreni problemi vezani za postojanje projektivnih ravinina određenih redova. Pogledajmo što je poznato o tom problemu.

Teorem 2.4.5. *Ako je $n = p^k$ za p prosti broj, a k ne-negativni cijeli broj tada postoji projektivna ravnina reda n.*

Dokaz. Prema teoremu 1.3.6 postoji konačno polje reda p^k za p prosti, a k prirodni broj. Tada možemo konstruirati afinu ravninu kako je opisano u potpoglavlju 2.1.. Kako projektivnu ravninu možemo konstruirati iz afine ravnine slijedi tvrdnja teoerma. □

Dakle, iz teorema možemo zaključiti da postoje projektivne ravnine reda 2, 3, 4, 5, 7, 8, 9 itd.. Nadalje, matematičari Richard Hubert Bruck i Herbert John Ryser sredinom 20. stoljeća došli su do još jednog zaključka.

Teorem 2.4.6 (Bruck-Ryserov teorem)**.** *Ako postoji projektivna ravnina reda n i vrijedi $n \equiv 1, 2 \pmod 4$ tada je n zbroj dva kvadrata.*

Dokaz ovog teorema nećemo provoditi, možete ga naći u članku [7].

Prema Bruck-Ryserovom teoremu, za $n = 6$ ne postoji projektivna ravnina. Dugogodišnji problem bio je postojanje projektivne ravnine reda 10. Primijetimo,

$$10 \equiv 2 \pmod 4 \text{ i } 10 = 1^2 + 3^2$$

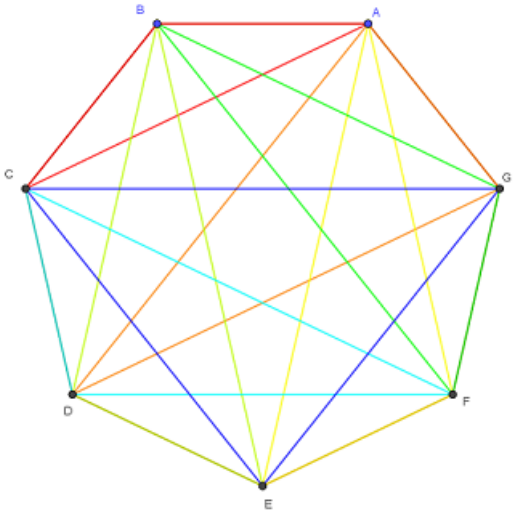
što zadovoljava uvjete Bruck-Ryserovog teorema. Međutim, uz pomoć računala je dokazano da projektivnu ravninu reda 10 nije moguće konstruirati. Postojanje projektivne ravnine reda 12 još se istražuje. Za sada se još uvijek ne zna postoji li ili ne budući da 12 nije niti potencija prostog broja, niti zadovoljava kriterije Bruck-Ryserovog teorema.

2.5 Primjer s natjecanja

Sljedeći zadatak preuzet je s *Hrvatske juniorske matematičke olimpijade 2019*.

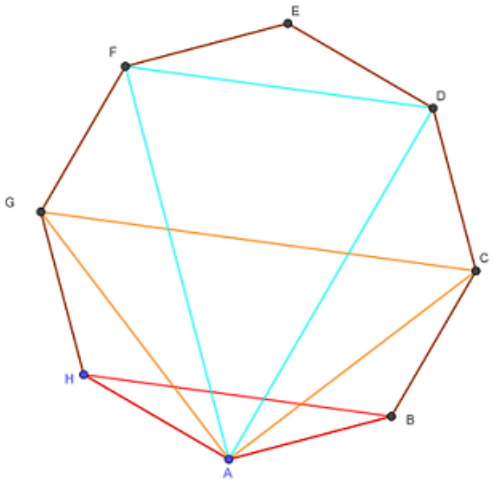
Zadatak 2.5.1. *Prirodni broj n je dobar ako svaku stranicu i dijagonalu pravilnog n-terokuta možemo obojiti u neku boju tako da za svaka dva vrha A i B postoji točno jedan vrh C, različit od A i B takav da su dužine $\overline{AB}$, $\overline{BC}$ i $\overline{AC}$ obojene istom bojom. Odredi koji su od brojeva 7, 8, 9, 10, 11 i 12 dobri.*

Najintuitivniji početak rješavanja ovog zadatka je crtanje mnogokuta i pronalaženje zaključaka koji nam mogu olakšati da bi lakše došli do rješenja zadatka. Za $n = 7$ lako nacrtamo sve dužine.



Slika 2.19: $n = 7$

Budući da smo uspjeli obojiti dužine na traženi način zaključujemo da je 7 dobar. Na isti način možemo pokušati nacrtati za $n = 8$.



Slika 2.20: $n = 8$

Vidimo da nam je ostala jedna točka koju ne možemo spojiti s niti jednom drugom. Promatrajmo jedan vrh mnogokuta, npr. vrh A. Želimo li nacrtati sve trokute kojima pripada vrh A, preostali vrhovi moraju biti u paru. Isto objašnjenje proizlazi za bilo koji vrh koji promatramo pa možemo zaključiti da je konstrukcija moguća ako je broj vrhova n-terokuta neparan. Stoga 8, 10 i 12 nisu dobri brojevi.

Možemo li nešto zaključiti za brojeve 9 i 11? Ako bismo išli crtati sve bi izgledalo kaotično. Pristupimo zadatku na drugačiji način.

Prisjetimo se, u potpoglavlju 2.1. govorili smo o konačnim afinim ravninama. Konačnu afinu ravninu reda 3 prikazali smo u primjeru igre SET. Zamislimo da su trokuti u zadatku pravci, a vrhovi mnogokuta točke. Svaki trokut određuju tri vrha, a svaka dva vrha nalaze se u jednom trokutu. Drugačije, na svakom pravcu leže tri točke i svake dvije točke leže na točno jednom pravcu. Ako zadatak interpretiramo na ovaj način možemo primijetiti da Hesseova konfiguracija, prikazana na slici 2.9, zadovoljava uvjete zadatka. Konstruirajmo taj primjer. Neka su vrhovi deveterokuta označeni slovima $A, B, C, .., H, I$. Trokut na kojem leže točke A, B i C označit ćemo sa ABC i analogno za ostale trokute. Ispišimo sve trokute.

$$\begin{array}{cccc} ABC & ADG & AEI & AFH \\ DEF & BEH & BFG & BDI \\ GHI & CFI & CDH & CEG \end{array}$$

Sada možemo zaključiti da je 9 dobar broj. Primijetimo da je ovakvom interpretacijom zadatka sedmerokut prikazan Fanovom ravninom.

Ostaje nam pokazati što je s brojem 11. Označimo sa $\mathcal{T}$ skup svih istobojnih trokuta. Prebrojimo na dva načina elemente skupa

$$K = \{(T, D) : T \in \mathcal{T}, D \text{ je dužina koja pripada trokutu } T.\}$$

Neka je broj elemenata u $\mathcal{T}$ jednak t. Za svaki trokut imamo tri dužine koje mu pripadaju pa vrijedi

$$|K| = t \cdot 3.$$

S druge strane, dužinu u n-terokutu možemo odabrati na $\binom{n}{2} = \frac{n(n-1)}{2}$ načina, a svaka dužina pripada točno jednom trokutu pa vrijedi:

$$|K| = \frac{n(n-1)}{2} \cdot 1.$$

Dakle, vrijedi

$$t \cdot 3 = \frac{n(n-1)}{2} \cdot 1.$$

Iz posljednje jednakosti možemo zaključiti da je ili n djeljiv s 3 ili $n - 1$ djeljiv s 3. Iz toga slijedi da 11 nije dobar broj.

Proširenje ovog zadatka može biti pitanje jesu li brojevi 13, 15, 17, 19,.. dobri i kako se taj rezultat može prikazati. Odnosno, postoji li neka matematička struktura pomoću koje možemo doći do zaključaka. Primijetimo da kod svakog broja koji je dobar i čija je konstrukcija prikazana pomoću pravaca i točaka kako je prethodno opisano, svake dvije točke leže na jednom pravcu i na svakom pravcu leže tri točke. Takvu strukturu nazivamo Steinerova trojka i njome ćemo se baviti u trećem poglavlju.

Poglavlje 3

Dizajni

Kao generalizacija konačnih afinih i projektivnih ravnina javljaju se konačne strukture koje nazivamo blok dizajni. Primjena blok dizajna je široka. Početak korištenja vezan je za izradu eksperimenata za ispitivanje karakteristika nekih procesa s obzirom na faktore koji mogu utjecati na njihov ishod. Jedan od utjecajnijih matematičara u tome području bio je Ronald Fisher koji došao do značajnih rezultata u statistici i biologiji. Osim u eksperimentima, dizajni se koriste kao kodovi za uklanjanje pogrešaka pri komunikaciji elektroničkim uređajima i mnogim drugim područjima.

U ovom poglavlju definirat ćemo što su dizajni i navesti glavne rezultate vezane za njihovu strukturu. Rezultati su preuzeti iz Stinsonove knjige *Combinatorial Designs: Construction and Analysis* [10].

3.1 Balansirani nepotpuni blok dizajni-BIBD

Definicija 3.1.1. Blok dizajn *je uređeni par* $(\mathcal{X}, \mathcal{B})$ *takav da vrijede sljedeća svojstva:*

1. $\mathcal{X}$ *je skup elemenata koje zovemo* točke*,*
2. $\mathcal{B}$ *je multiskup nepraznih podskupova skupa* $\mathcal{X}$ *koje zovemo* blokovi*.*

Skup $\mathcal{B}$ je definiran kao multiskup jer je dopušteno postojanje više identičnih blokova. Mi ćemo se posebno baviti balansiranim nepotpunom blok dizajnima.

Definicija 3.1.2. *Neka su* $v > k \geq t \geq 0$ *i* $\lambda > 0$ *cijeli brojevi.* Dizajn *s parametrima* $t-(v,k,\lambda)$ *je konačna struktura sa svojstvima:*

1. *ukupan broj točaka je v,*

2. *na svakom bloku leži točno k točaka,*

3. *svaki t-člani skup točaka sadržan je u točno λ blokova.*

Ako je $t = 2$ strukturu nazivamo *balansirani nepotpuni blok dizajn*. Skraćeno ćemo pisati BIBD (balanced incomplete block design).

Primjer 3.1.3. *Neka je $(\mathcal{X}, \mathcal{B})$ $(7, 3, 1)$-BIBD. Tada imamo:*

$$\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7\},$$
$$\mathcal{B} = \{123, 145, 167, 246, 257, 347, 356\}.$$

Pri tome oznaka 123 označava pravac na kojem leže točke 1, 2 i 3. Primijetimo da ukupno imamo sedam točaka, na svakom pravcu leže tri točke i kroz svake dvije točke prolazi jedan pravac. Prikažemo li $(7, 3, 1)$-BIBD dijagramom vidjet ćemo da je to upravo Fanova ravnina, odnosno projektiva ravnina reda 2. Kanije ćemo vidjeti da se sve konačne projektivne i afine ravnine mogu prikazati kao blok dizajni.

Osim parametara v, k i λ u BIBD-u su određena još dva parametra: r - broj blokova na kojem leži svaka točka i b - ukupni broj blokova.

Teorem 3.1.4. *U (v, k, λ)-BIBD-u, svaka točka leži na točno*

$$r = \frac{\lambda(v-1)}{k-1}$$

blokova.

Dokaz. Dokaz ćemo provesti tako da ćemo definirati skup I koji ćemo prebrojati na dva različita načina.

Neka je $(\mathcal{X}, \mathcal{B})$ (v, k, λ)-BIBD. Za neki $x \in \mathcal{X}$ označimo sa r_x broj blokova na kojima se nalazi x. Skup I definirat ćemo na sljedeći način:

$$I = \{(y, B) : y \in \mathcal{X}, y \neq x, B \in \mathcal{B}, \{x, y\} \in \mathcal{B}\}$$

Riječima, elementi skupa I su svi uređeni parovi (y, B) takvi da je y točka različita od x, a B blok na kojem leže i y i x. Prebrojimo elemente skupa na dva načina. Postoji $v-1$ načina za odabrati točku $y \in \mathcal{X}$ različitu od x. Svake dvije točke nalaze se na λ blokova pa je

$$|I| = \lambda(v-1).$$

S druge strane, blok B na kojem leži točka x možemo odabrati na r_x načina. Pri tome, na $k-1$ način možemo odabrati točku $y \in \mathcal{X}$ koja leži na bloku B i da je različita od x.

Tada je

$$|I| = r_x(k-1).$$

Izjednačavanjem dviju jednakosti dobivamo:

$$\lambda(v-1) = r_x(k-1) \implies r_x = \frac{\lambda(v-1)}{k-1}. \tag{3.1}$$

Budući da smo x uzeli proizvoljno, tvrdnja vrijedi za svaki x iz $\mathcal{X}$. □

Teorem 3.1.5. *(v, k, λ)-BIBD sadrži točno*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

blokova.

Dokaz. Kao i u prethodnom dokazu, definirat ćemo skup čije ćemo elemente prebrojiti na dva načina. Neka je $(\mathcal{X}, \mathcal{B})$ (v, k, λ)-BIBD i $b = |\mathcal{B}|$. Definiramo skup

$$I = \{(x, B) : x \in \mathcal{X}, B \in \mathcal{B}, x \in \mathcal{B}\}.$$

Točku x možemo odabrati na v načina. Za svaki takav x postoji r blokova na kojima leži x pa vrijedi

$$|I| = vr.$$

S druge strane, ukupni broj blokova je b. Na svakom bloku $B \in \mathcal{B}$ leži k točaka pa je

$$|I| = bk.$$

Konačno dobivamo

$$bk = vr \implies b = \frac{vr}{k}. \tag{3.2}$$

□

Želimo li naglasiti sve parametre BIBD-a strukturu zapisujemo kao (v, b, r, k, λ)-BIBD. Kako ukupni broj blokova i broj blokova kroz svaku točku moraju biti cijeli brojevi iz teorema 3.1.2. i 3.1.3. slijedi sljedeći korolar.

Korolar 3.1.6. *Ako (v, k, λ)-BIBD postoji, tada vrijedi*

$$\lambda(v-1) \equiv 0 \pmod{k-1} \; i \; \lambda v(v-1) \equiv 0 \pmod{k(k-1)}.$$

Za svaki dizajn možemo definirati matricu incidencije.

Definicija 3.1.7. Matrica incidencije *dizajna* $(\mathcal{X}, \mathcal{B})$ *je matrica* $M = (m_{i,j})$ *dimenzije* $v \times b$ *takva da je*

$$m_{i,j} = \begin{cases} 1, & ako\ x_i \in B_j. \\ 0, & ako\ x_i \notin B_j. \end{cases}$$

Lako se vidi da u svakom stupcu postoji k jedinica, svaki redak sadrži r jedinica, a svaka dva retka imaju jedinicu u točno λ stupaca. Osim uvjeta iz prethodnog korolara do još jednhog uvjeta za postojanje BIBD-a došao je već spomenuti statističar Ronald Fisher.

Teorem 3.1.8 (Fisherova nejednakost)**.** *U svakom* (v, b, r, k, λ)*-BIBD-u vrijedi* $b \geq v$.

Dokaz. Neka je $(\mathcal{X}, \mathcal{B})$ dizajn takav da su $\mathcal{X} = \{x_1, ..., x_v\}$ i $\mathcal{B} = \{B_1, ..., B_b\}$. Neka je M matrica incidencije tog dizajna i $\mathbf{s}_j$ j-ti redak matrice M^T. Vektori $\mathbf{s}_1, ..., \mathbf{s}_v$ su v-dimenzionalni vektori u vektorskom prostoru $\mathbb{R}^v$. Definirajmo skup $S = \{\mathbf{s}_j | 1 \leq j \leq b\}$ i sa $\mathbf{S}$ označimo skup $\{\sum_{j=1}^{b} \alpha_j \mathrm{s}_j | \alpha_1, ..., \alpha_b \in \mathbb{R}\}$. Pokažimo da je $\mathbf{S} = \mathbb{R}^v$, odnosno da vektori iz S razapinju vektorski prostor $\mathbb{R}^v$.
Za $1 \leq i \leq v$ definirajmo $\mathbf{e}_i \in \mathbb{R}^v$ tako da vektor $\mathbf{e}_i$ ima jedinicu na i-tom mjestu, a ostale koordinate su mu nule. Vektori $\mathbf{e}_1, ..., \mathbf{e}_v$ razapinju prostor $\mathbb{R}^v$ pa se svaki vektor iz $\mathbb{R}^v$ može zapisati kao linearna kombinacija vektora $\mathbf{e}_1, ..., \mathbf{e}_v$. Da bismo pokazali da je $\mathbf{S} = \mathbb{R}^v$ trebamo pokazati da svaki vektor $\mathbf{e}_i$ možemo prikazati kao linearna kombinacija vektora iz S. Na početku primijetimo da je

$$\sum_{j=1}^{b} \mathbf{s}_j = (r, ..., r). \tag{3.3}$$

Taj zaključak slijedi iz činjenice da kroz svaku točku prolazi r blokova, a blokove predstavljaju upravo retci transponirane matrice incidencije odnosno vektori $\mathbf{s}_j$. Nadalje, za neki i takav da je $1 \leq i \leq v$ imamo:

$$\sum_{\{j | x_i \in B_j\}} \mathbf{s}_j = (r - \lambda)\mathbf{e}_i + (\lambda, ..., \lambda) \tag{3.4}$$

Iz jednadžbe (3.1) znamo da je $\lambda(v - 1) = r(k - 1)$ pa uz uvjete iz definicije dizajna $v > k$ imamo $r - \lambda \neq 0$. Stoga, kombiniranjem jednadžbi 3.3 i 3.4 dobivamo

$$\mathbf{e}_i = \sum_{\{j | x_i \in B_j\}} \frac{1}{r - \lambda} \mathbf{s}_j - \sum_{j=1}^{b} \frac{\lambda}{r(r - \lambda)} \mathbf{s}_j \tag{3.5}$$

□

Primjer 3.1.9. *U kušanju deset vrsta vina sudjeluje n sommeliera pri čemu su zadovoljena ova tri uvjeta:*

(a) Svaki sommelier kuša točno pet vina.

(b) Svaku vrstu vina kuša jednak broj sommeliera.

(c) Za sve parove sommeliera broj vina koja su oba sommeliera probala je jednak.

Odredi sve n za koje je to moguće provesti.

Rješenje: Prikažimo sommeliere kao točke, a vina kao blokove. Ukupno imamo 10 blokova. Zbog (a) kroz svaku točku prolazi točno 5 blokova, zbog (b) na svakom bloku leži jednak broj točaka (označimo taj broj sa k) i zbog (c) svake dvije točke nalaze se na λ blokova. Dakle imamo sljedeće podatke:
$v = n$, $b = 10$, $r = 5$
Koristeći izraz (3.2) dobivamo:

$$10 = \frac{5n}{k} \implies k = \frac{n}{2}. \tag{3.6}$$

Iz ovog rezultata možemo zaključiti da n treba biti paran broj. Nadalje iz jednadžbe (3.1.) imamo:

$$5 = \frac{\lambda(n-1)}{\frac{1}{2}n - 1}, \tag{3.7}$$

pa nakon sređivanja dobivamo

$$\lambda = 5 - \frac{5n}{2(n-1)}. \tag{3.8}$$

Kako su n i $n-1$ te 2 i 5 relativno prosti slijedi da

$$n - 1|5 \text{ i } 2|n.$$

Iz ovoga lako primijetimo da su mogućnosti za n 2 i 6. Međutim, imamo li dva sommeliera dobivamo da svaka dva sommeliera neće kušati niti jednu istu vrstu vina, odnosno ne postoji blok na kojem leže obje točke što nije u skladu sa definicijom dizajna pa takav dizajn ne postoji. Dakle, da bi bili zadovoljeni uvjeti $(a) - (c)$ treba biti šest sommeliera. Uvrštavanjem u (3.6) dobivamo da svaku vrstu vina kušaju tri sommeliera, a iz (3.8) imamo da svaka dva sommeliera kušaju dvije vrste vina. Dizajn kojim možemo konstruirati degustaciju vina je $(6, 3, 2)$-BIBD. Konstruirajmo taj dizajn. Neka su sommelieri označeni s $A, B, ..., F$.

1. vino kušaju sommelieri A, B i C
2. vino kušaju sommelieri A, B i D
3. vino kušaju sommelieri A, C i E
4. vino kušaju sommelieri A, D i F
5. vino kušaju sommelieri A, E i F
6. vino kušaju sommelieri B, C i F
7. vino kušaju sommelieri B, D i E
8. vino kušaju sommelieri B, E i F
9. vino kušaju sommelieri C, D i E
10. vino kušaju sommelieri C, D i F

3.2 Simetrični BIBD

Posebna vrsta BIBD-a su *simetrični* balansirani nepotpuni blok dizajni.

Definicija 3.2.1. *BIBD u kojem je $v = b$ naziva se simetrični BIBD.*

Ekvivalentni uvjeti kao u definiciji su $r = k$ i $\lambda(v-1) = k(k-1)$ što se lako provjeri uvrštavanjem u jednadžbe 3.1 i 3.2.

Promotrimo primjer 3.1.3. $(7, 3, 1)$-BIBD ima 7 točaka. Uvrstimo li parametre u jednadžbe 3.1. i 3.2. dobivamo da je ukupan broj blokova jednak 7, a broj blokova kroz jednu točku jednak je 3. Tada zaključujemo da je $(7, 3, 1)$ simetrični BIBD. Sjetimo se, $(7, 3, 1)$-BIBD predstavlja projektivnu ravninu reda 2. Vrijedi li to općenito za projektivne ravnine reda n?

Primjer 3.2.2. *$(n^2 + n + 1, n + 1, 1)$-BIBD za $n \geq 2$ je projektivna ravnina reda n.*

Uvrštavanjem parametara u izraz $\lambda(v-1) = k(k-1)$ dobivamo $1 \cdot (n^2 + n + 1 - 1) = (n+1)(n+1-1)$ što je istina za svaki $n \geq 2$. U prethodnom poglavlju pokazali smo da postoji projektivna ravnina reda q ako je q potencija prostog broja. To nas dovodi do sljedećeg teorema.

Teorem 3.2.3. *Za svaki $n \geq 2$ takav da je n potencija prostog broja, postoji simetrični $(n^2 + n + 1, n + 1, 1)$-BIBD.*

Konstrukciju Fanove ravnine pomoću vektorskog prostora napravili smo u potpoglavlju 2.1. Pogledajmo ponovno sve 1-dimenzionalne i 2-dimenzionalne potprostore vektorskog prostora $(\mathbb{Z}_2)^3$. Skup svih 1-dimenzionalnih potprostora označimo sa V_1, a 2-dimenzionalnih sa V_2.

1-dimenzionalni potprostori	2-dimenzionalni potprostori
$C_1 = \{(0,0,0),(0,0,1)\}$	$B_1 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}$
$C_2 = \{(0,0,0),(0,1,0)\}$	$B_2 = \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\}$
$C_3 = \{(0,0,0),(1,0,0)\}$	$B_3 = \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}$
$C_4 = \{(0,0,0),(0,1,1)\}$	$B_4 = \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\}$
$C_5 = \{(0,0,0),(1,0,1)\}$	$B_5 = \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}$
$C_6 = \{(0,0,0),(1,1,0)\}$	$B_6 = \{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\}$
$C_7 = \{(0,0,0),(1,1,1)\}$	$B_7 = \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$

Definirajmo blok kao

$$A_B = \{C \in V_1 : C \subseteq B\},$$

a skup svih blokova

$$\mathcal{B} = \{A_B : B \in V_2\}.$$

Ispišimo sve blokove A_B.

$$\begin{aligned}
A_{B_1} &= \{C_1, C_2, C_4\} \\
A_{B_2} &= \{C_1, C_3, C_5\} \\
A_{B_3} &= \{C_1, C_6, C_7\} \\
A_{B_4} &= \{C_2, C_3, C_6\} \\
A_{B_5} &= \{C_2, C_5, C_7\} \\
A_{B_6} &= \{C_3, C_4, C_7\} \\
A_{B_7} &= \{C_4, C_5, C_6\}
\end{aligned}$$

S ovako definiranim skupovima struktura $(V_1, \mathcal{B})$ je simetrični $(7,3,1)$-BIBD odnosno projektivna ravnina reda 2.

Primjer 3.2.4. *Neka je $n \geq 2$. $(n^2, , n, 1)$-BIBD je afina ravnina reda n.*

Na primjer, uzmemo li afinu ravninu reda 3 dobivamo 9 točaka, 12 blokova, kroz svaku točku prolazi 4 bloka, na svakom bloku leže 3 točke i kroz svake dvije točke prolazi jedan blok. Prikažemo li $(9,3,1)$-BIBD dijagramom dobit ćemo upravo prezentaciju kao na slici 2.9.

U drugom poglavlju komentirali smo uvjete za postojanje projektivne i afine ravnine reda n. Generalizacija Bruck-Ryserova teorema, Bruck-Ryser-Chowla teorem, daje nam nužan uvjet za egzistenciju simetričnih dizajna. Razlikujemo dva slučaja, jedan za v neparni broj, a drugi za v parni broj.

Teorem 3.2.5 (Bruck-Ryeser-Chowla teorem za v paran broj)**.** *Pretpostavimo da postoji simetrični (v, k, λ)-BIBD tako da je v paran broj. Tada se $k - \lambda$ može zapisati kao kvadrat nekog prirodnog broja.*

Dokaz. Neka je M matrica incidencije simetričnog (v, k, λ)-BIBD-a i neka je v paran broj. Neka je M^T transponirana matrica matrice M. Neka je I_n jedinična matrica $n \times n$ i J_n $n \times n$ matrica u kojoj na svakom mjestu stoji jedinica. Može se pokazati da vrijedi $MM^T = \lambda J_v + (r - \lambda)I_v$. Dokaz tvrdnje možete pogledati u [10] na stranicama 6 i 7.

Kako je u simetričnom dizajnu $r = k$ i $v = b$ imamo $MM^T = \lambda J_v + (k - \lambda)I_v$ pri čemu su M i M^T $v \times v$ matrice. Budući da matrice M i M^T imaju jednake determinante tada vrijedi:

$$\det(\lambda J_v + (k - \lambda)I_v) = \det(MM^T) = (\det M)(\det M^T) = (\det M)^2$$

Promotrimo matricu

$$\lambda J_v + (k - \lambda)I_v = \begin{bmatrix} k & \lambda & \lambda & \cdots & \lambda \\ \lambda & k & \lambda & \cdots & \lambda \\ \lambda & \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & k \end{bmatrix}.$$

Oduzmimo od svakog retka prvi redak matrice, pa dobivamo

$$\begin{bmatrix} k & \lambda & \lambda & \cdots & \lambda \\ \lambda - k & k - \lambda & & \cdots & 0 \\ \lambda - k & 0 & k - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda - k & 0 & 0 & \cdots & k - \lambda \end{bmatrix}.$$

Sada, dodajmo prvom stupcu stupce 2 do v:

$$\begin{bmatrix} k + (v-1)\lambda & \lambda & \lambda & \cdots & \lambda \\ 0 & k - \lambda & & \cdots & 0 \\ 0 & 0 & k - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & k - \lambda \end{bmatrix}.$$

Primijetimo da smo dobili gornjetrokutastu matricu. Determinanta je onda jednaka umnošku elemenata na glavnoj dijagonali.

$$(\det M)^2 = (k + (v-1)\lambda)(k - \lambda)^{v-1} = k^2(k - \lambda)^{v-1}$$

uz $(v - 1)\lambda = k(k - 1)$. Budući da su elementi matrice M prirodni brojevi, determinanta $\det M$ je također prirodni broj. Uz to, kako je v paran slijedi da $k - \lambda$ mora biti kvadrat nekog prirodnog broja. □

Drugi slučaj nećemo dokazivati. Dokaz možete pogledati u [10].

Teorem 3.2.6 (Bruck-Ryser-Chowla teorem za v neparan broj)**.** *Pretpostavimo da postoji simetrični (v, k, λ)-BIBD takav da je v neparan broj. Tada postoji cijeli brojevi x, y i z od kojih je barem jedan različit od nule, takvi da vrijedi*

$$x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2.$$

Uz dokaz da projektivna ravnina reda 10 ne postoji, Bruck-Ryser-Chowla teoremi su jedini dokazani teoremi koji daju uvjete za postojanje simetričnih BIBD-ova.

3.3 Steinerova trojka

Na kraju potpoglavlja 2.5. spomenuli smo Steinerove trojke. *teinerova trojka*, u oznaci STS(v) je $(v, 3, 1)$-BIBD. Projektivna ravnina reda 2 i afina ravnina reda 3 su Steinerove trojke. Pogledajmo koji je nužan uvjet za postojanje dizajna.

Teorem 3.3.1. *Ako postoji STS(v), onda vrijedi $v \equiv 1, 3 \pmod 6, v \geq 7$.*

Dokaz. Neka je STS(v) $(v, 3, 1)$-BIBD. Tada vrijedi

$$b = \frac{\lambda(v^2 - v)}{k^2 - k} \implies 6b = v(v - 1),$$

pa iz toga slijedi da je $v \equiv 0, 1, 3, 4 \pmod 6$ jer je b cijeli nenegativan broj. Nadalje, vrijedi

$$r = \frac{\lambda(v - 1)}{k - 1} = \frac{v - 1}{2},$$

što daje $v \equiv 1, 3, 5 \pmod 6$. Uz ta dva uvjeta imamo $v \equiv 1, 3 \pmod 6$. □

Može se pokazati da vrijedi i obrnuti smjer, odnosno ako je $v \equiv 1, 3 \pmod 6$ onda postoji STS(v). Dokaz tvrdnje možete pogledati u [10].

Kirkmanov problem 15 učenica

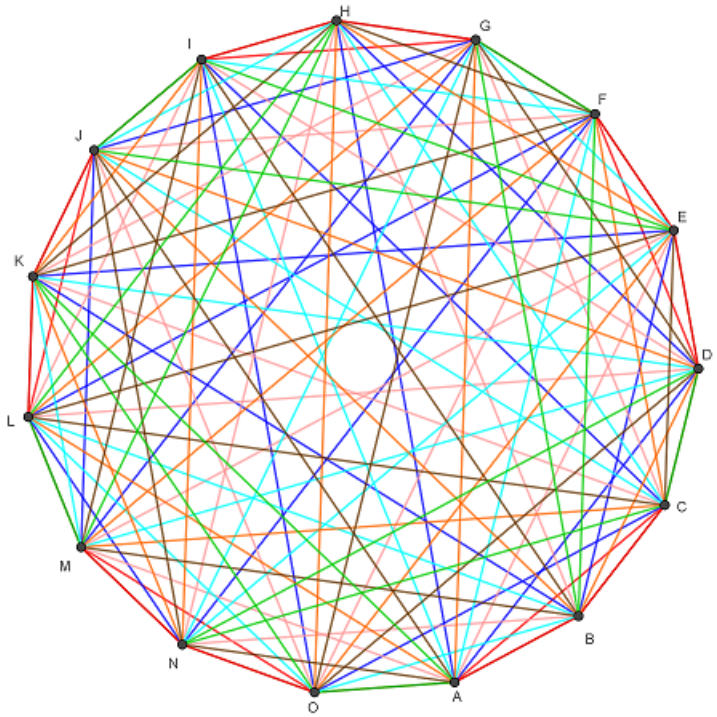
Problem 15 učenica objavljen je 1850. godine u časopisu *Lady's and Gentleman's Diary*, a glasi ovako: Petnaest učenica šeta do škole svaki dan u pet redova po tri učenice. Mogu li se učenice rasporediti tako da se svake dvije učenice nađu u istom redu točno jednom u sedam dana?

Problem je objavio Thomas Penyngton Kirkman pa ga nazivamo Kirkamnov problem 15 učenica. Postoji nekoliko načina kako se može prikazati rješenje Kirkmanovog problema. U tablici 3.1 dan je raspored šetnji za tjedan dana. Učenice smo označili slovima A, B, C....

Ponedjeljak	ABC	DEF	GHI	JKL	MNO
Utorak	ADH	BEK	CIO	FLN	GJM
Srijeda	AEM	BHN	CGK	DIL	FJO
Četvrtak	AFI	BLO	CHJ	DKM	EGN
Petak	AGL	BDJ	CFM	EHO	IKN
Subota	AJN	BIM	CEL	DOG	FHK
Nedjelja	AKO	BFG	CDN	EIJ	HLM

Tablica 3.1: Raspored šetnji 15 učenica

Ispisivanje šetnji na ovakav način je komplicirano. Prisjetimo se zadatka 2.5.1 u potpoglavlju 2.5. Uvjet je bio da se svaka dva vrha mnogokuta nađu točno jednom u trokutu. Konstrukcija zadatka za petnaesteorkut prikazana je na slici 3.1.



Slika 3.1: Konstrukcija zadatka 2.5.1 za $n = 15$.

Primijetimo da rješenje zadatka upravo odgovara rješenju Kirkmanovog problema 15 učenica. Dakle, ako učenice predstavljaju vrhove, a redovi blokove, rješenje za Kirkmanov problem je $(15, 3, 1)$-BIBD odnosno Steinerova trojka za $v = 15$.

Vidimo da postoji više prikaza rješenja Kirkmanovog problema. Još jedan prikaz je pomoću trodimenzinalnog projektivnog prostora nad poljem $\mathbb{Z}_2$. Opis prikaza dan je u [5].

Primijetimo još nešto kod rješenja problema. Za svaki dan vrijedi da jedna učenica ne šeta u dva reda istovremeno i sve učenice šetaju svaki dan. Ovo opažanje dovodi nas do još jednog tipa BIBD-a, rješivi BIBD.

3.4 Rješivi BIBD

Definicija 3.4.1. *Neka je* $(\mathcal{X}, \mathcal{B})$ (v, k, λ)*-BIBD. Podskup disjuntnih blokova iz* $\mathcal{B}$ *takvih da je njihova unija jednaka* $\mathcal{X}$ *nazivamo* klasa paralelizma*. Particija skupa* $\mathcal{B}$ *na disjunktne klase paralelizma naziva se* rezolucija *i kažemo da je* $(\mathcal{X}, \mathcal{B})$ rješiv *BIBD ako postoji barem jedna rezolucija.*

U Kirkmanovom problemu imamo jednu rezoluciju, sedam klasa paralelizma koje sadrže po 5 disjunktnih blokova. Primijetimo da će u klasi paralelizma biti $\frac{v}{k}$ blokova pa možemo zaključiti da BIBD može imati klase paralelizma ako vrijedi $v \equiv 0 \pmod{k}$.

Nama dobro poznata afina ravnina je rješiv BIBD. U potpoglavlju 3.2. rekli smo da je afina ravnina reda n $(n^2, n + 1, 1)$-BIBD. Prisjetimo se kako smo definirali relaciju paralelnosti. Definirali smo je na skupu pravaca, u terminima dizajna to bi bili blokovi. Označimo skup blokova sa $\mathcal{B}$. Tada za $L, B \in \mathcal{B}$ vrijedi:

$$L \parallel B \implies L = B \text{ ili } L \cap B = \emptyset.$$

Pokažimo da je svaka klasa relacije paralelnosti klasa paralelizma afine ravnine tj. $(\mathcal{X}, \mathcal{B})$ $(n^2, n + 1, 1)$-BIBD-a.

Lema 3.4.2. *Neka je* $(\mathcal{X}, \mathcal{B})$ *afina ravnina reda n. Tada je svaka klasa relacije paralelnosti* $\parallel$ *klasa paralelizma u* $(\mathcal{X}, \mathcal{B})$*.*

Dokaz. Neka je Π klasa relacije paralelnosti i neka je $B \in \mathcal{B}$. Tada vrijedi:

$$\Pi = \{M \in \mathcal{B} : B \parallel M\}.$$

Budući da zbog aksioma $(A1)$ nema ponavljajućih blokova, blokovi u Π su disjunktni. Nadalje, prema $(A2)$ za svaku točku $x \in \mathcal{X}$ postoji blok $M \in \Pi$ takav da je $x \in M$. Iz toga slijedi da je unija svih blokova iz Π jednaka $\mathcal{X}$ odnosno svaka klasa relacije paralelnosti je particija od $\mathcal{X}$. □

Teorem 3.4.3. *Svaka afina ravnina je rješiva.*

Dokaz. Prema prethodnoj lemi svaka klasa relacije parelelnosti je klasa paralelizma BIBD-a. Također, svaki blok BIBD-a nalazi se u točno jednoj klasi relacije paralelnosti. Dakle, klase relacije paralelnosti tvore rezoluciju afine ravnine, pa je afina ravnina rješivi BIBD. □

Prisjetimo se opet kako izgleda afina ravnina reda 3 (slika 2.9). Označimo točke sa brojevima 1-9 tako da u prvom donjem redu imamo točke 1-3 s lijeva na desno, u drugom 4-6 i u trećem 7-9. Klase paralelizma su skupovi paralelnih pravaca/blokova ravnine. Ispišimo sve klase:

$$\Pi_1 = \{123, 456, 789\}$$
$$\Pi_2 = \{159, 267, 348\}$$
$$\Pi_3 = \{147, 258, 369\}$$
$$\Pi_4 = \{168, 249, 357\}$$

Primijetimo, svaka klasa sadrži $\frac{v}{k}$ blokova. Isto tako, vidimo da skup svih klasa paralelizma sadrži sve blokove afine ravnine, pa je to rezolucija.

Iznijeli smo osnovne rezultate za BIBD-ove, a sada ćemo pokazati na koji način se prva tri poglavlja rada mogu prilagoditi za učenike u školi.

Poglavlje 4

Konačna polja i dizajni u nastavi matematike

Sve češće čujemo da se u obrazovanju mora nešto promijeniti, kao i u svakom predmetu tako i u nastavi matematike. Očekivanja roditelja, ali i obrazovnih institucija je da učenici nakon završetka školovanja budu sposobni za rad ili daljnje obrazovanje. Međutim, zadnjih se godina događa da su rezultati državne mature i PISA testova na istoj, ako ne i na nižoj razini nego prijašnjih godina što dovodi do zaključka da se učeničke kompetencije za iduću etapu u životu ne poboljšavaju. Mi kao nastavnici možemo i moramo pridonijeti tome da učenik nauči razmišljati i bude sposoban obaviti posao nakon završetka školovanja.

Cilj zadataka danih u radu je, prije svega, razvoj apstraktnog mišljenja, kombinatornog, proporcionalnog i logičkog zaključivanja. Od petog razreda osnovne škole učenici bi kognitivno, prema Piagetu, trebali biti u razdoblju formalnih operacija. Osim poznavanja pojmova i rješavanja jednostavnih zadataka, u razdoblju formalnih operacija učenici mogu rješavati zadatke sa složenim postupkom, logički zaključivati, apstraktno, kombinatorno i probabilistički razmišljati. Međutim, sve češće se događa da dolaskom u srednju školu učenici nisu u mogućnosti doći do željenog zaključka ukoliko im nije dano „sve na pladnju".

Promotrimo klasičan primjer iz fizike u kojem treba koristiti proporcionalno zaključivanje. Takav zadatak javlja se u trećem razredu srednje škole.

Zadatak 4.0.1. *Coulombova sila između dva naboja iznosi* $F = k\frac{q_1 q_2}{r^2}$ *pri čemu su sa* q *označeni iznosi naboja,* r *označava udaljenost među nabojima, a* k *je konstanta. Kako će se promijeniti Coulombova sila među nabojima ako iznos jednog naboja povećamo dva puta i udaljenost povećamo tri puta?*

Ovakvih tipova zadataka u fizici, ali i u matematici ima jako puno. Problemi pri njihovom rješavanju često leže u krivom interpretiranju zadatka. Drugi problem je što nije zadan niti jedan broj i učenici jednostavno ne znaju što bi sa svim tim „slovima" u jednadžbi. Još jedan od problema je nemogućnost zamišljanja danog objekta. U slučaju naboja, neki učenici ne mogu zamisliti što bi bio naboj i kako naboji međudjeluju ako se ne dodiruju. Matematički, učenik treba primijetiti koje su veličine proporcionalne, a koje obrnuto proporcionalne. Kada shvati što znači proporcionalno, a što obrnuto proporcionalno može zaključiti kako će se sila promijeniti sa promjenom veličina. U ovome slučaju, budući da su naboj i sila proporcionalni, a kvadrat udaljenosti i sila obrnuto proporcionalni, sila koju dobivamo povećanjem naboja i udaljenosti iznosi $\frac{2}{9}$ početne sile.

Očekivanje nas kao nastavnika je da učenici nemaju problema kod rješavanja ovakvih zadataka. Pitanje je kako razviti takvo razmišljanje?

Postoji puno zadataka koji mogu služiti kao alat za poticanje mišljenja kod učenika. Zbog njihove raznolikosti učenicima se mogu zadavati razni zadaci u kojima će svaki put morati razmisliti kako pristupiti zadatku, a da ne postoji šablona koju bi naučili na pamet. U ovom poglavlju želimo prikazati kako se dio matematike pokazan u prva tri poglavlja rada može prilagoditi učenicima različite dobi i kako ga možemo iskoristiti za razvijanje apstraktnog, kreativnog i kombinatornog razmišljanja. Koncepti s kojima bi učenici trebali baratati su asocijativnost, komutativnost, suprotni/inverzni element, distributivnost, pravac, točka, itd. Svi se ti koncepti uvode još u osnovnoj školi. Zadaci u radu nisu prezahtjevni da ih učenici ne bi mogli shvatiti, ali nije unaprijed jasno kako doći do rješenja i kojim se poznatim alatima treba koristiti. Zadaci vezani za konačna polja omogućili bi učeniku da sam vidi razliku između raznih struktura. Provjeravanjem bi lako uočili da u skupu $\mathbb{Z}$ ne postoji inverzni element za množenje. Osim poznatih skupova cijelih, realnih i racionalnih brojeva promatrali bi i konačne skupove ostataka pri dijeljenju sa prirodnim brojem n. Zadavanjem skupova za neki mali broj n, npr. od 2 do 15, učenici mogu provjeriti svojstva zadanih računskih operacija. S obzirom da stavljamo naglasak na razliku među strukturama dovoljna je provjera postojanja inverznog elementa za množenje za svaki element skupa. U tom trenutku možemo, ali i ne moramo, ovisno o dobi učenika, uvesti pojmove polje i prsten. Učenici ne moraju znati te pojmove, ali naučili bi koja je razlika među njima. Taj dio algebre jako je zanimljiv, a učenicima služi da razvijaju apstraktno mišljenje.

Osvrnimo se na zadatke koje smo riješili u prethodna tri poglavlja. U potpoglavlju 2.5. nalazi se zadatak 2.5.1 koji uz malo crtanja i razmišljanja učenici mogu djelomično, ako ne i potpuno sami riješiti. Nadamo se da bi svaki učenik crtanjem mnogokuta i trokuta došao do zaključka da se za parni n ne može obojati trokut na željeni način. Naravno da ne očekujemo da će učenici sami doći do zaključka da se trokuti mogu gledati kao

pravci, a vrhovi trokuta kao točke koje pripadaju pravcima. Te pretpostavke i pogled na zadatak je nešto što bi mi kao nastavnici trebali približiti učeniku, a onda mu ostaviti da pokuša konstruirati takve strukture za određene prirodne brojeve. Moramo biti svjesni da je učeniku potpuno apstraktno zašto trokut možemo zamijeniti pravcem pa je bitno razviti način razmišljanja koji omogućava prelazak na drugačiji grafički model u kojem je situaciju lakše prikazati. Uvođenjem drugačijeg grafičkog prikaza možemo napraviti uvod u pojam konačne projektivne i afine ravnine kao ravnine sa konačnim brojem točaka i pravaca. U spomenutom zadatku koristili smo metodu dvostrukog prebrojavanja kako bismo došli do nekih uvjeta da n bude dobar broj. To je poznata metoda pomoću koje neke teže zadatke učenici mogu riješiti bez da znaju komplicirane matematičke pojmove ili strukture. Na sličan način do određenih uvjeta dolazimo i u zadatku s degustacijom vina. Teži dio u rješavanju zadataka metodom dvostrukog prebrojavanja je određivanje skupa koji će se prebrojavati i u tome moramo učenicima biti od pomoći. Kada dobijemo rješenje bitno ga je konstruirati odnosno pokazati da je takva situacija zbilja moguća.

Opisane aktivnosti mogu se provoditi na redovnoj ili dodatnoj nastavi ili kao projektna nastava, zavisno o predznanju učenika. U školi se algebra polja i prstenova pojavljuje u kratkim crtama, a kombinatorika se javlja uglavnom u matematičkim gimnazijama. Ukoliko se nađe vremena bilo bi dobro provesti bar dio opisanih ili sličnih aktivnosti. Učenici bi malo odmorili od „onoga što moraju znati za ocjenu“, a u raznim zadacima mogli bi proširiti znanje o matematici i kroz zabavu naučiti nešto više što bi im se moglo svidjeti. Uz to, potiče se njihova aktivnost, a samim time se razvija i kreativnost.

4.1 Polja i prsteni

U dodatku A prikazan je nastavni listić kojim bismo učenicima približili svojstva algebarskih strukuta. Prvom stranicom listića želimo pokazati razliku među strukturama $(\mathbb{Z}, +, \cdot)$ i $(\mathbb{Q}, +, \cdot)$. Sat počinjemo ponavljanjem koncepata asocijativnosti, komutativnosti i distributivnosti. Uz to, prisjećamo se što su skupovi cijelih, racionalnih i realnih brojeva. U prva dva zadatka učenici sami konstruiraju primjere koji se traže u zadatku. Na taj način samo mogu evaluirati shvaćaju li uistinu što su već spomenuti koncepti. Poteškoću koju očekujemo u drugom zadatku je interpretacija teksta zadatka pa kroz razgovor pomažemo učenicima što se u zadatku traži. Kroz diskusiju i nekoliko primjera dolazimo do zaključka da u svakom skupu postoji element koji zadovoljava svojstva iz drugog zadatka i uvodimo pojam neutralni element za množenje. Rješavanjem zadanih linearnih jednadžbi učenici uočavaju da u skupu $\mathbb{Z}$ ne postoji rješenje, osima za $b = 1$ i $b = -1$ u jednadžbi $bx = 1$. Broj x koji zadovoljava danu jednadžbu nazovemo inverz broja b. U tom trenutku, kroz razgovor, učenicima predstavimo da postoje razne algebarske strukure u kojima su zado-

voljena određena svostva zbrajanja i množenja. S obzirom na to možemo zaključiti da $(\mathbb{Z}, +, \cdot)$ i $(\mathbb{Q}, +, \cdot)$ nisu iste strukture.

U ostatku listića bavimo se konačnim skupovima. Nakon petog zadatka bitna je diskusija kako možemo podijeliti cijele brojeve u klase ekvivalencije s obzirom na ostatke pri dijeljenju brojem n. U našem slučaju gledamo klase ekvivalencije modulo 3 i 6. Pojam klase ne moramo uvoditi. Umjesto toga možemo reći *skup svih brojeva čiji je ostatak pri dijeljenju s 3 jednak 0*. Tada se može definirati skup

$$\{\overline{0}, \overline{1}, \overline{2}\}$$

čiji su elementi klase ekvivalencije odnosno skupovi opisani u prethodnoj rečenici. Nakon kratke vježbe sa razvrstavanjem cijelih brojeva u klase ekvivalencije slijedi diskusija o zbrajanju i množenju elemenata skupa. Nakon nekoliko primjera, kao vježba, može se odigrati igra *Memory*. Učenici mogu igrati u grupi ili paru, ovisno o broju učenika. Da bi došli do rješenja rješavaju zadatke s kartica i pri tome vježbaju računanje s klasama. Primjer zadataka na karticama prikazan je u dodatku A. Igra je napravljena za skup ostataka pri dijeljenju brojem 7. Kao i kod beskonačnih skupova, želimo da učenici uoče razliku među strukutrama $(\mathbb{Z}_3, +, \cdot)$, $(\mathbb{Z}_4, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$ i $(\mathbb{Z}_6, +, \cdot)$ sa dobro definiranim zbrajanjem i množenjem.

Očekivani odgojno-obrazovni ishodi

Učenici će:

- osmisliti primjere asocijativnosti, komutativnosti i distributivnosti operacija zbrajanja i množenja na skupovima $\mathbb{Z}$ u $\mathbb{Q}$.
- upotrijebiti znanja iz prethodnih razreda i donijeti zaključak o postojanju neutralnog elementa za množenje u skupovima $\mathbb{Z}$ i $\mathbb{Q}$.
- riješiti linearne jednadžbe i diskutirati o prirodi njihova rješenja.
- opisati razliku među strukturama $(\mathbb{Z}, +, \cdot)$ i $(\mathbb{Q}, +, \cdot)$.
- definirati konačan skup.
- grupirati pozitivne cijele brojeve s obzirom na ostatak pri dijeljenju s tri, odnosno sa šest.
- objasniti što su klase ekvivalncije brojeva s obzirom djeljivost s n.

- grupirati pozitivne cijele brojeve s obzirom na ostatak pri dijeljenju s brojem tri, odnosno sa šest.
- računati s klasama ekvivalencije.
- primijeniti svojstva asocijativnosti, komutativnosti i distributivnosti pri rješavanju zadataka s klasama ekvivalencije.
- provjeriti postoji li inverz za svaki element skupova $\mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$ i $\mathbb{Z}_6$ i interpretirati dobiveno rješenje.
- opisati razliku među strukturama $(\mathbb{Z}_3, +_3, \cdot_3)$, $(\mathbb{Z}_4, +_4, \cdot_4)$, $(\mathbb{Z}_5, +_5, \cdot_5)$ i $(\mathbb{Z}_6, +_6, \cdot_6)$.

4.2 Prebrojavanja i dizajni

Pravila igre SET opisali smo u potpoglavlju 2.2. Primjena igre u nastavi može biti raznolika. Mi ćemo pokazati nekoliko zadataka koji mogu pridonijeti razvijanju kombinatornog zaključivanja. Također, pomoću igre približit ćemo učenicima koncept konačne afine ravnine.

U dodatku B prikazan je nastavni listić koji se može koristiti na nastavnom satu. Najidealnije bi bilo kada bi učenici bili podijeljeni u grupe i kada bi svaka grupa imala sve kartice SET-a. Većina zadataka svodi se na prebrojavanje mogućnosti za dobivanje SET-a uz određene uvjete. Vođenje razreda u ovakvim zadacima je bitno jer su kombinatorni zadaci slabo zastupljeni u nastavi, a većina učenika nema razvijno kombinatorno razmišljanje i ne znaju kako pristupiti zadatku. S druge strane, ne smijemo mi riješiti sve zadatke nego moramo biti strpljivi i pustiti učenike da sami prebrojavaju. Ukoliko vidimo da se učenici ne mogu izboriti s time, igra se može pojednostaviti tako da uzmemo npr. samo crvene rombove pa ukupno imamo 9 karata. U tom slučaju, pitanja moramo malo prilagoditi. Popunjavanje 3×3 rešetke zanimljivo je jer se spajanjem SET-ova dobije prikaz afine ravnine reda 3. Učenicima tada možemo predstaviti konačnu ravninu koja zadovoljava određena svojstva kao i njima poznata euklidska ravnina, a njen prikaz sami su otkrili rješavanjem zadatka koji nije eksplicitno vezan za geometriju. Osim rješavanja predloženih zadataka nije loše učenike pustiti da igru odigraju. Na taj način primijenjuju razne strategije za pronalazak SET-a što se kasnije može komentirati i diskutirati koja je strategija najefikasnija.

Zadatak s degustacijom vina klasičan je zadatak u kojem učenici primijenjuju dvostruko prebrojavanje. Problem u ovom zadatku javlja se kod određivanja skupa koji će prebrojati na dva načina. Uz to, dvostruko prebrojavnje mora se provesti dva puta. Učenike treba uputiti na pravilnosti zadane u zadatku i na taj način potaknuti razmišljanje o tome koje veličine žele dovesti u vezu. Tako će odrediti traženi skup. Dobivanjem rješenja i njegovim prikazom učenicima približavamo koncept dizajna. Također, s učenicima možemo

diskutirati o sličnosti zahtjeva za konačnu afinu ravninu i dizajna. Na sličan način aktivnost se može provesti rješavanjem zadatka 2.5.1.

Kirkmanov problem je zadatak koji ne očekujemo da će učenici sami riješiti. Očekujemo da bi većina učenika probala ispisati sve šetnje tako da zadovolje zadane uvjete. Naš zadatak je usmjeriti učenike na drukčiji prikaz i pristup zadatku. Možemo ga prikazati kao na slici 3.1 i diskutirati s učenicima što bi prikazivalo šetnje, a što učenice u 15-erokutu. Učenici bi tada sami mogli konstuirati trokute i probali doći do rješenja zadatka. Međutim, takav 15-erokut teško je konstruirati. Postoji mnogo načina za dobivanje rješenja, a mi moramo odabrati koji će pristup biti najjasniji učenicima s kojima radimo. Zanimljivi prikaz rješenja dan je u [6]. U takvom prikazu bitno je opaziti na koji način su spojene točke. Zbog lakše vizualizacije učenici mogu nacrtati svih sedam dijagrama odnosno rotacija danog prikaza. Tada rješenje mogu pokazati i tablično.

Očekivani odgojno-obrazovni ishodi

Učenici će:

- opisati princip uzastopnog prebojavanja.
- riješiti zadatke koristeći kombinacije i varijacije.
- opisati metodu dvostrukog prebojavanja skupova.
- koristiti metodu dvostrukog prebrojavanja pri rješavanju zadatka s degustacijom vina.
- argumentirati smislenost mogućih rješenja u zadatku s degustacijom vina.
- prikazati rješenje zadatka s degustacijom vina na različite načine.
- prikazati rješenje Kirkmanovog problema na više načina.

Dodatak A

Polja i prsteni

Strutkure

1. Što su asocijativnost i komutativnost množenja i zbrajanja, a što je distributivnost? Napiši primjere za skupove $\mathbb{Q}$ i $\mathbb{Z}$.

2. Postoji li broj k u skupu cijelih brojeva za koji vrijedi $a \cdot k = k \cdot a = a$ za svaki a cijeli broj? Postoji li takav broj u skupovima racionalnih i realnih brojeva?

3. Riješite jednadžbe

   $$2x = 1 \qquad\qquad 3x = 4$$

   Kojem skupu pripadaju rješenja?

4. Riješite jednadžbe:

   $$bx = 1 \qquad\qquad ax = b$$

   za a i b cijele brojeve, $a, b \neq 0$ i $a \neq b$. Kojem skupu pripadaju rješenja?

Zaključak:

4. Što je za tebe konačan skup? Napiši primjer.

5. Koji su mogući ostaci pri dijeljenju pozitivnih cijelih brojeva s brojem 3, a koji s brojem 6?

6. Razvrstaj zadane brojeve s obzirom na ostatak pri dijeljenju s brojem 3.
   0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 17, 25, 35, 39, 55, 68, 84

7. Brojeve iz prethodnog zadatka razvrstaj s obzirom na ostatak pri dijeljenju s brojm 6.

8. Provjeri postoji li inverzni element za svaki element skupa ostataka pri dijeljenju sa 3, 4, 5 i 6.

Zaključak:

Kartice za igru *Memory*

$\overline{1}+\overline{2}$	$\overline{3}\cdot\overline{5}+\overline{3}\cdot\overline{4}$
$(\overline{1}+\overline{2})+\overline{4}$	$\overline{5}\cdot\overline{4}+\overline{3}\cdot(\overline{2}+\overline{1})$
$(\overline{5}+\overline{6})\cdot\overline{3}$	$\overline{4}\cdot\overline{2}+\overline{3}\cdot\overline{5}$
$\overline{5}\cdot\overline{6}+\overline{2}$	$\overline{4}\cdot\overline{6}+\overline{3}\cdot\overline{6}$
$\overline{5}+\overline{6}$	$\overline{5}+\overline{1}\cdot\overline{3}$
$(\overline{3}+\overline{5})\cdot\overline{3}$	$\overline{6}\cdot\overline{6}+\overline{4}$
$(\overline{4}+\overline{5})+(\overline{6}+\overline{1})$	$(\overline{2}+\overline{3}+\overline{4})\cdot\overline{3}$

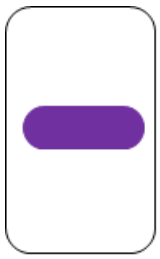
Slika A.1: Zadaci za igru *Memory*

Dodatak B

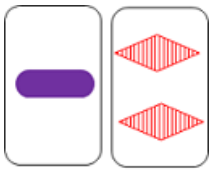
Prebrojavanja i dizajni

Kombinatorika

1. Nađi tri SET-a, ako je na jednoj karti jedan ljubičasti puni ovalni oblik. Koliko ukupno ima takvih SET-ova?



2. Na slici su zadane dvije karte. Koje karte možete dodati da dobijete SET? Koliko ukupno ima takvih SET-ova?

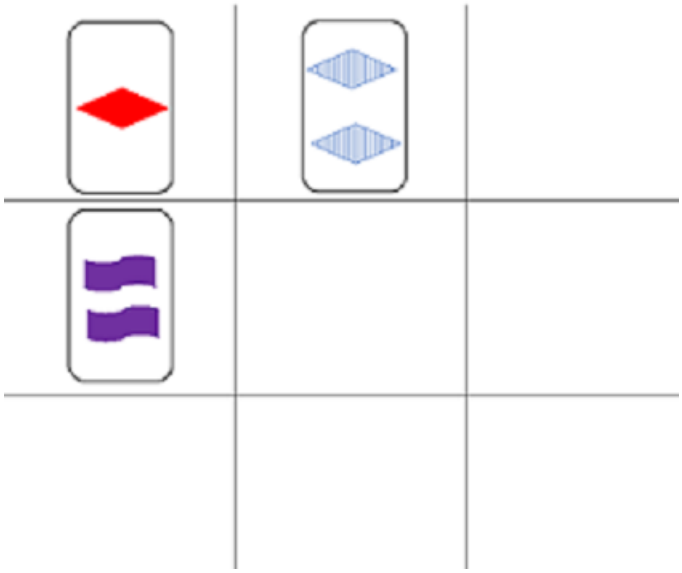


3. Koliki je ukupni broj SET-ova u igri?

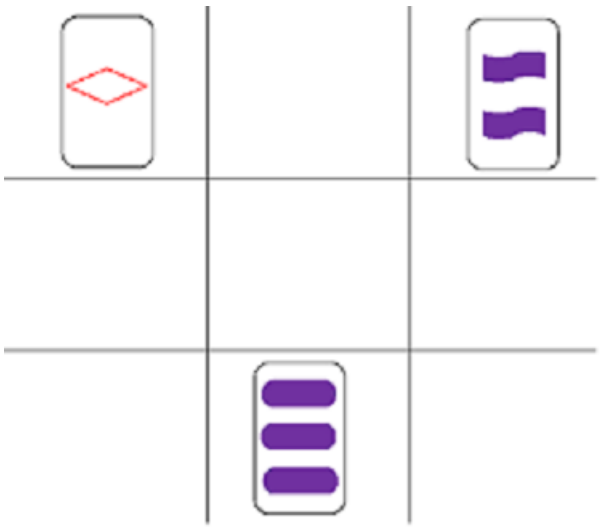
4. Na koliko je načina u igri moguće otvoriti prvih 12 karata?

5. U 3×3 rešetki dane su tri karte. Popunite rešetke tako da svaka dijagonala, svaki stupac i svaki red tvore SET.

   a)

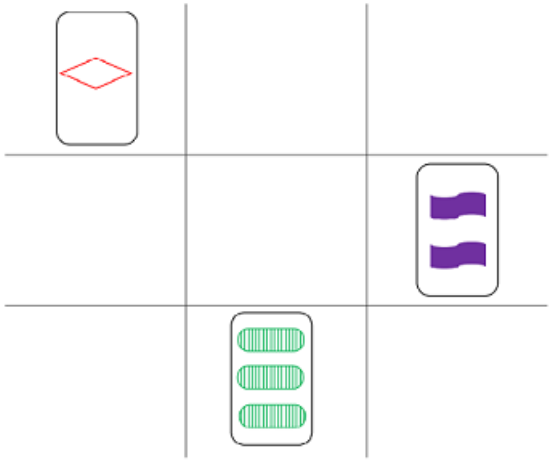


b)



Koliko ukupno SET-ova postoji u svakoj od rešetki? SET-ove spojite linijama.

6. Na koliko različitih načina možete popuniti 3×3 rešetku tako da svaki red, stupac i dijagonala čine SET?



7. U kušanju deset vrsta vina sudjeluje n sommeliera pri čemu su zadovoljena ova tri uvjeta:

   (a) Svaki sommelier kuša točno pet vina.

   (b) Svaku vrstu vina kuša jednak broj sommeliera.

   (c) Za sve parove sommeliera broj vina koja su oba sommeliera probala je jednak.

   Odredi sve n za koje je to moguće provesti.

8. **Kirkmanov problem 15 učenica.** Petnaest učenica šeta do škole svaki dan u pet redova po tri učenice. Mogu li se učenice rasporediti tako da se svake dvije učenice nađu u istom redu točno jednom u sedam dana?

Bibliografija

[1] https://en.wikipedia.org/wiki/Combinatorial_design, pristupljeno u kolovozu 2019.

[2] http://quibb.blogspot.com/2016/02/the-projective-plane-visual-introduction.html, pristupljeno u kolovozu 2019.

[3] https://en.wikipedia.org/wiki/Fano_plane, pristupljeno u kolovozu 2019.

[4] https://en.wikipedia.org/wiki/Sylvester%E2%80%93Gallai_theorem, pristupljeno u kolovozu 2019.

[5] https://en.wikipedia.org/wiki/Kirkman%27s_schoolgirl_problem, pristupljeno u kolovozu 2019.

[6] http://www.algorithm.uni-bayreuth.de/en/research/discreta/EXAMPLES/kirkman.html, pristupljeno u kolovozu 2019.

[7] R. H. Bruck i H. J. Ryser, *The Nonexistence of Certain Finite Projective Planes*, Canadian Journal of Mathematics **1** (1949), br. 1, 88–93.

[8] T. W. Hungerford, *Algebra*, Springer, 2003.

[9] J. Šiftar i V. Krčadinac, *Konačne geometrije*, skripta, akademska godina 2012./2013.

[10] Douglas Stinson, *Combinatorial designs: constructions and analysis*, Springer Science & Business Media, 2007.

[11] Cherith Tucker, *Geometric models of the card game SET*, Rose-Hulman Undergraduate Mathematics Journal **8** (2007), br. 1, 10.

Sažetak

Blok dizajni su konačne strukture u kojima su elementi konačnih skupova raspoređeni po zadanim pravilima. Specijalni slučajevi blok dizajna su konačne afine i projektivne ravnine. U radu su prikazane konstrukcije konačnih afinih i projektivnih ravnina pomoću konačnih polja, npr. Fanove ravnine kao najmanje projektivne ravnine. Na nekoliko načina prikazana je veza između afine i projektivne ravnine. Posebni naglasak stavljen je na prilagođavanje koncepata konačnih polja, afinih i projektivnih ravnina te dizajna učenicima u školi. Uz to, dane su aktivnosti kojima konačna polja, afine i projektivne ravnine te dizajne možemo približiti učenicima u školi.

Rad je podijeljen u četiri dijela. Prva tri poglavlja donose osnovne teorijske rezultate o konačnim poljima, projektivnim i afinim ravninama i blok dizajnima. Svako poglavlje sadrži konstrukcije raznih struktura i rješenja nekih poznatih problema, npr. Kirkmanov problem 15 učenica. U četvrtom poglavlju promatramo na koji način učenicima možemo približiti teme iz prva tri poglavlja u svrhu razvijanja mišljenja i poticanja kognitivne aktivnosti. U tome je najbitnija prilagodba materijala i izražavanje prilikom izvođenja nastave. U dodacima se nalaze nastavni listići za provođenje aktivnosti na nastavnom satu.

Summary

Block designs are finite structures in which the elements of finite sets satisfy some properties. Special cases of block designs are affine and projective planes. In this thesis we present the construction of affine and projective plane using the finite fields, for example Fano plane as the smallest finte projective plane. In several ways conection between affine and projective plane is shown. Particular emphasis is given on the adaptation concepts of finite fields, affine and projective planes and designs to students in school. Also, activities are given which can be used to bring finite fields, affine and projective planes and designs closer to students.

The thesis consists of four parts. First three chapters bring basic theoretical results of finite fields, affine and projective planes and block designs. Every chapter contains constructions of different structures and solutions of some familiar problems, such as Kirkman's schoolgirl problem. In chapter four we discuss how to bring topics from first three chapters closer to students in order to encourage cognitive activities. In order to do so, most important is good adjustment of materials and expression during class. Appendices contain sheets for teaching in the class.

Životopis

Zovem se Iva Novosel i rođena sam 31.10.1994. u Zagrebu. Od 2001. godine pohađala sam Osnovnu školu dr. Ante Starčevića u zagrebačkoj Dubravi. Nakon završetka osnovne škole upisujem prirodoslovno-matematički smjer u III. gimnaziji u Zagrebu. Nakon položene državne mature upisujem Integrirani preddiplomski i diplomski sveučilišni studij Matematike i fizike nastavničkog smjera na Prirodoslovno-matematičkom fakultetu u Zagrebu.