# Kriptomorfizmi matroida

Ivančić, Marija

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Marija Ivančić

# Kriptomorfizmi matroida

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Vedran Krčadinac

Zagreb, rujan 2015.

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

# 1 Uvod

Teorija matroida aktivno je područje matematike koja koristi ideje iz apstraktne i linearne algebre, konačne geometrije, kombinatorike i teorije grafova. Časopis i online bibliografska baza podataka Mathematical Reviews popisala je oko 2000 objava u kojima se nalazi riječ “matroid” u naslovu. Od toga više od trećina tih objava pojavila se u posljednjem desetljeću. Gian-Carlo Rota je rekao da je teorija matroida sažetak svih trendova suvremene matematike u jednu konačnu strukturu [2, str. 60.]. U ovom diplomskom radu matroide ćemo promatrati ponajviše iz geometrijskog stajališta fokusirajući se na nezavisnost. Promatrat ćemo končne podskupove u vektorskom prostoru, točke u Euklidskom prostoru te bridove u grafovima, što povezuje matroide s linearnom algebrom, diskretnom geometrijom i teorijom grafova. Apstraktno poimanje nezavisnosti povezuje različite klase matroida. Na tu ideju prvi je došao Hassler Witney, koji je definirao matroide u svom radu 1935. godine i koji je imao bitnu ulogu u ranom razvoju teorije matroida [9]. Teorija matroida polako se razvijala između 1940. i 1950. godine. U tom razdoblju Garrett Birkhoff [1] proučavao je ravnine matroida iz gledišta teorije rešetka, Saunders MacLane [3] povezao je matroide s projektivnom geometrijom, a Richard Rado [5] povezao je bipartitne grafove s matroidima. Vrlo važan, suvremeniji pristup teoriji matroida dao je William Tutte 1958. godine [6]. On je opisao binarne i regularne matroide preko pojmova isključenih minora. Pronalazak isključenih minora za klase matroida jedno je od najdubljih i najživljih područja suvremene matematike u teoriji matroida. Time se nećemo baviti u ovom diplomskom radu. Koncentrirat ćemo se na geometrijski pristup koji je popularizirao Gian-Carlo Rota. On je matroide još nazivao “kombinatrornom pregeometrijom”, no taj se termin nije zadržao [2, str. 3.].

Postoje desetine ekvivalentnih definicija matroida, tj. matroidi se mogu definirati na razne kriptomorfne načine. To je prilično korisno za rješavanje različitih problema. Mi ćemo spomenuti samo najvažnije. Za matroid $M$ definirat ćemo sedam ključnih pojmova: nezavisni skupovi, baze, ciklusi, funkcija ranga, ravnine, hiperravnine i operator zatvarača. Pojmovi nezavisni skupovi, baze, ciklusi i funkcija ranga povezani su s linearnom algebrom ili teorijom grafova, a pojmovi ravnine, hiperravnine i operator zatvarača povezani su s geometrijom ili topologijom. U ovom diplomskom radu bavit ćemo se kriptomorfizmima između ovih sedam ključnih pojmova. U poglavlju ravnine i hiperravnine uvest ćemo i pojam geometrijske rešetke, koja nam daje dobar način prikaza ravnina matroida i još jedan drukčiji način definiranja matroida. Prvo ćemo definirati matroid preko nezavisnih skupova pomoću svojstava $(I1)$, $(I2)$ i $(I3)$ (vidi def 2.1) i reći nešto o matroidima nastalim iz matrica i iz grafova. Zatim ćemo uspostaviti kriptomorfizam između nezavisnih skupova i baza i na taj način pokazati da matroid možemo definirati i preko baza. Navest ćemo i kriptomorfizme između nezavisnih skupova i ciklusa, između nezavisnih skupova i funkcije ranga, funkcije ranga i operatora zatvarača, ravnina i operatora zatvarača, ravnina i hiperravnina (vidi sliku 1).

$$\mathcal{I} \overset{tm4.4}{\longleftrightarrow} \mathcal{B} \qquad \mathcal{I} \overset{tm5.2}{\longleftrightarrow} \mathcal{C}$$

$$\mathcal{I} \overset{tm6.4}{\longleftrightarrow} rang \overset{tm8.7}{\longleftrightarrow} zatvarač$$

$$\mathcal{F} \overset{tm8.4}{\longleftrightarrow} zatvarač \qquad \mathcal{F} \overset{tm8.13}{\longleftrightarrow} \mathcal{H}$$

Slika 1: Kriptomorfizam između određenih pojmova matroida.

Funkciju ranga koristit ćemo kao most između pojmova "linearne algebre": nezavisnih skupova, baza i ciklusa te "geometrijskih" pojmova ravnina, hiperravnina i zatvarača. Uspostavljanjem kriptomorfizma između tih pojmova pokazat ćemo da svaki od tih pojmova možemo koristiti kao početnu točku u definiranju matroida. U posljednjem poglavlju nezavisne skupove matroida definirat ćemo preko greedy algoritma. Ta veza daje nam dodatan uvid u važnost i posebnost matroida.

# 2 Matroidi iz matrica

Prvi koji je definirao matroide preko nezavisnih skupova bio je Hassler Whitney [9]. On je želio razumjeti koliko posebna obilježja vektora zavise o polju koeficijenata (točnije, koliko je linearne algebre nezavisno od koordinata) te je uočio da svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$ koja su niže navedena, izlaze iz linearne nezavisnosti podskupova u vektorskom prostoru. Uvedimo najprije osnovne pojmove, a zatim navedimo nekoliko primjera matroida.

**Definicija 2.1.** N*eka je $E$ konačan skup i $\mathcal{I}$ familija podskupova skupa $E$. Kažemo da je uređeni par $M = (E, \mathcal{I})$ matroid ako familija $\mathcal{I}$ zadovoljava:*

*(I1)* $\mathcal{I} \neq \emptyset$.

*(I2) Ako je $J \in \mathcal{I}$ i $I \subseteq J$, onda je $I \in \mathcal{I}$.*

*(I3) Ako su $I, J \in \mathcal{I}$ takvi da je $|I| < |J|$, onda postoji $x \in J \setminus I$ takav da je $I \cup \{x\} \in \mathcal{I}$.*

*Skup $E$ zovemo temeljni skup matroida, a podskupove iz $\mathcal{I}$ zovemo nezavisnim skupovima.*

Rang matroida je veličina najvećeg nezavisnog skupa. Označava se s $r(M)$. Slijedi teorem koji povezuje matroide i matrice.

**Definicija 2.2.** *Neka je $V$ vektorski prostor nad poljem $\mathbb{F}$ i $S$ neprazni podskup od $V$. Tada je linearna ljuska ili linearni omotač podskupa $S$ u oznaci $[S]$, najmanji potprostor prostora $V$ koji sadrži skup $S$.*

**Lema 2.3.** *Linearna ljuska podskupa $S$ je skup svih linearnih kombinacija vektora iz $S$, to jest:*

$$[S] = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \,|\alpha_1, ...\alpha_n \in \mathbb{F}, v_1, ..., v_n \in S, n \in \mathbb{N}\}.$$

*Posebno* $[\emptyset] = \{0_v\}$.

*Dokaz.* Neka je $L = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \,|\alpha_1, ...\alpha_n \in \mathbb{F}, v_1, ..., v_n \in S, n \in \mathbb{N}\}$. Treba dokazati da je $[S] = L$, tj. da je $[S] \subseteq L$ i $[S] \supseteq L$. Neka su $\alpha_1, \alpha_2 \in \mathbb{F}$ i $v_1, v_2 \in L$ proizvoljni. Vrijedi $\alpha_1 v_1 + \alpha_2 v_2 \in L$ pa je $L$ potprostor od $V$. Također vrijedi $S \subseteq L$ jer je $L$ skup svih linearnih kombinacija vektora iz $S$. Dakle, $L$ je potprostor od $V$ koji sadrži $S$, a $[S]$ je najmanji potprostor prostora $V$ koji sadrži skup $S$ pa je $[S] \subseteq L$. Sada pokažimo da je $[S] \supseteq L$. Linearna ljuska $[S]$ je potprostor prostora $V$ i sadrži $S$, pa sadrži i sve linearne kombinacije vektora iz S. Vrijedi $[S] \supseteq L$. Dakle, $[S] = L$. $\square$

**Teorem 2.4.** *Neka je $E$ skup svih stupaca matrice $A$ nad poljem $\mathbb{F}$ i neka je $\mathcal{I}$ skup svih podskupova od $E$ koji su linearno nezavisni. Tada je $M = (E, \mathcal{I})$ matroid i njegov rang jednak je rangu matrice $A$.*

*Dokaz.* Trebamo dokazati da familija $\mathcal{I}$ zadovoljava svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$. Prazan skup je sigurno element od $\mathcal{I}$ pa je $\mathcal{I} \neq \emptyset$ i svojstvo $(I1)$ je zadovoljeno. Svaki podskup linearno nezavisnog skupa je linearno nezavisan pa vrijedi i svojstvo $(I2)$. Preostaje nam pokazati svojstvo $(I3)$. Neka su $I$ i $J$ dva linearno nezavisna skupa takva da je $|I| < |J|$ i neka je $x \in J \setminus [I]$. Takav $x$ sigurno postoji jer je $[I]$ potprostor dimenzije manje od $|J|$, a $J$ je linearno nezavisan pa $J$ ne može biti podskup od $[I]$.

Sada treba još dokazati da je $I \cup \{x\}$ linearno nezavisan skup. Neka je $I = \{v_1, v_2, ..., v_n\}$ i neka je $[I]$ linearna ljuska podskupa $I$. Znamo da $x \notin [I]$ jer je $x \in J \setminus [I]$. Pretpostavimo suprotno, da je $I \cup \{x\}$ linearno zavisan skup. Tada postoje $\alpha_1, \alpha_2 ... \alpha_n, \beta \in \mathbb{F}$ koji nisu svi 0, takvi da je

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n + \beta x = 0.$$

Znamo da je $\beta \neq 0$ jer je $\{v_1, ..., v_n\}$ linearno nezavisan skup. Sada imamo:

$$\begin{aligned} \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n + \beta x = 0 / \cdot \frac{1}{\beta} \\ \frac{\alpha_1}{\beta} v_1 + \frac{\alpha_2}{\beta} v_2 + ... + \frac{\alpha_n}{\beta} v_n + x = 0 \\ x = \frac{-1}{\beta}(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n) \end{aligned}$$

Iz prethodne leme slijedi da je $x \in [I]$, što je u kontradikciji s $x \notin [I]$. Dakle, $I \cup \{x\}$ je linearno nezavisan skup.

Familija $\mathcal{I}$ zadovoljava svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$ pa je $M = (E, \mathcal{I})$ matroid. Još trebamo dokazati da je rang matroida jednak rangu matrice $A$. Rang matrice definira se kao najveći broj linearno nezavisnih stupaca matrice, a rang matroida je veličina najvećeg nezavisnog skupa. Očito je rang matroida jednak rangu matrice $A$. □

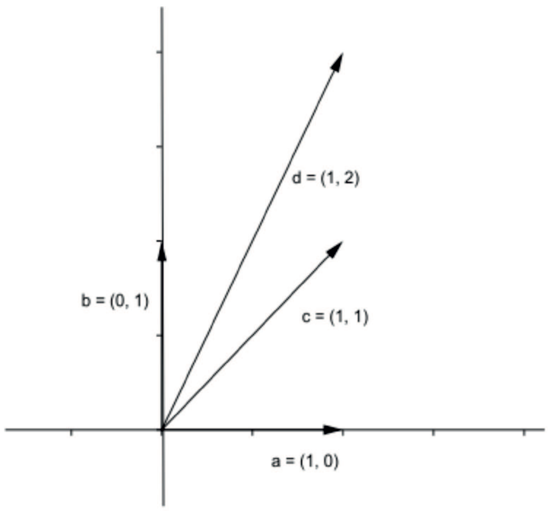
Primjeri matroida koji dolaze iz matrica su sljedeći.

**Primjer 2.5.** *Neka je matrica* $A = \begin{array}{c} \begin{matrix} a & b & c & d \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix} \end{array}.$

*Uočimo četiri stupca* $a = (1,0)$ , $b = (0,1)$, $c = (1,1)$, $d = (1,2)$. *Sada promotrimo podskupove stupaca koji su linearno nezavisni i one koji su linearno zavisni. U matrici* $A$, *svaki par vektora je linearno nezavisan podskup od* $\mathbb{R}^2$, *a svaki podskup od tri vektora je linearno zavisan jer je prostor dvodimenzionalan. Skup od četiri vektora je linearno zavisan iz istog razloga. Prema tome, u ovom primjeru je familija* $\mathcal{I} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}\}$.

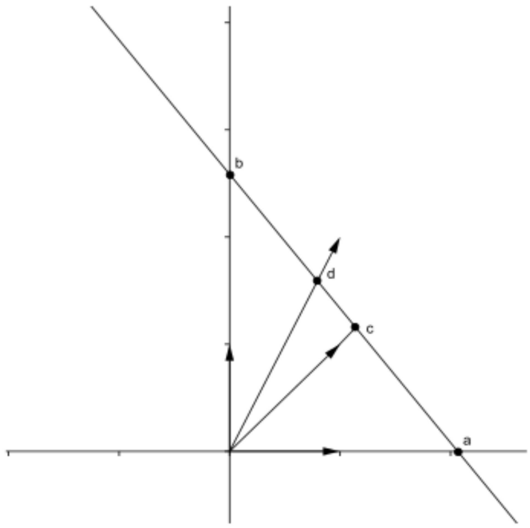
Pitamo se kako možemo opisati linearnu zavisnost podskupova skupa $\{a, b, c, d\}$. Jedan od načina je da se ispišu svi skupovi vektora koji su linearno zavisni, u ovom slučaju $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$, $\{b, c, d\}$, $\{a, b, c, d\}$. To nije najbolji pristup tom problemu. Postoji još puno načina kojima možemo opisati ove skupove, no mi ćemo se bazirati na geometrijskom načinu. Nacrtat ćemo sliku koja predstavlja linearnu zavisnost i nezavisnost podskupova $\{a, b, c, d\}$. Postupak se provodi u tri koraka:

Korak 1. Nacrtaju se vektori u ravnini (vidi sliku 2).




Slika 2: Četiri vektora iz primjera 2.5.

Korak 2. Nacrta se pravac koji nije paralelan ni s jednim od zadanih vektora. Produže se ili smanje svi vektori tako da pravac siječe svaki vektor ili njegovo produženje odnosno smanjenje. Gledaju se presjecišta pravca i vektora, odnosno presjecišta pravca i produženih ili smanjenih vektora (vidi sliku 3).




Slika 3: Četiri vektora iz primjera 2.5 i pravac.

Korak 3. Slika koja predstavlja linearnu zavisnost podskupova $\{a, b, c, d\}$ dobiva se tako da se zadrži pravac koji siječe vektore ili njihova produženja i smanjenja, njihova sjecišta označe se s točkama, a vektori se odbace (vidi sliku 4). Slika 4 prikazuje matroid koji se sastoji od četiri kolinearne točke. Uočimo da je dimenzija slike matroida 1, a rang matroida 2. Dakle, rang matroida jednak je dimenziji slike matroida uvećanoj za jedan.

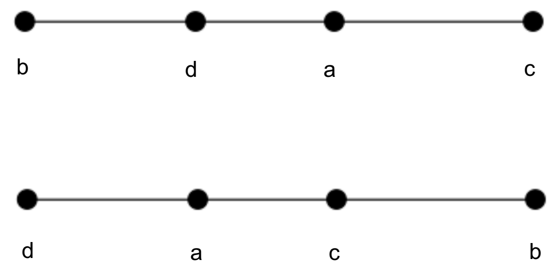

Slika 4: Slika matroida iz primjera 2.5.

Postupak koji smo gore opisali je postupak crtanja matroida iz matrice s dva retka. Duljina vektora nije bitna. Na primjer, slika 4 bit će ista ako zamijenimo (1,1) s (2,2). Također, mogli smo zamijeniti vektor s njemu suprotnim vektorom bez da promijenimo sliku 4.

Ako želimo preskočiti crtanje vektora i doći izravno iz matrice $A$ do slike matroida koristimo ova pravila:

- svaki vektor koji se nalazi u stupcu matrice predstavlja se točkom
- ako su tri vektora linearno zavisna, onda će tri odgovarajuće točke biti kolinearne.

Koristeći ta dva pravila možemo prikazati linearnu zavisnost stupaca matrice $A$. Slika 5 prikazuje dva načina obilježavanja linearne zavisnosti stupaca matrice $A$. Naravno, postoji još mnogo drugih obilježavanja.




Slika 5: Dva različita obilježavanja linearne zavisnosti stupaca matrice $A$.

Ovaj postupak je ispravan jer znamo da su tri vektora linearno zavisni ako i samo ako su komplanarni. A ta tri vektora su komplanarni ako i samo ako su tri odgovarajuće točke na slici matroida kolinearne. To je lako uočiti za vektore u $\mathbb{R}^2$: dva vektora u ravnini su linearno nezavisna ako imaju različit smjer. U tom slučaju oni sijeku pravac (iz koraka 2.) u različitim točkama pa su linearno nezavisni u matroidu. Ako su dva vektora u ravnini linearno zavisna, onda će oni siječi pravac iz koraka 2. u istoj točki što će rezultirati pojavom "višestrukih točaka" u slici matroida, tj. pojavom zavisnog skupa od dva elementa. Moguće je da matroid ima zavisne jednočlane skupove. Takve pojave objasnit ćemo kasnije na primjeru.

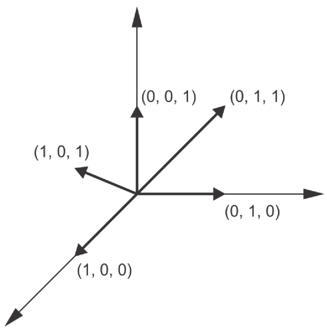
**Primjer 2.6.** *Neka je matrica* $B = \begin{array}{c} \begin{matrix} a & b & c & d & e \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$.

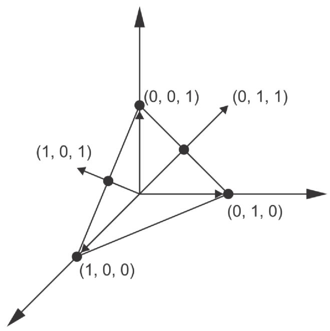
*Kao u primjeru 2.5 želimo nacrtati sliku koja prikazuje zavisnost stupaca u matrici.*

Zamislimo projiciranje vektora u proizvoljnu ravninu, tako da možemo koristiti analogan postupak crtanja kao u primjeru 2.5. Postupak crtanja matroida iz matrice s tri retka:

Korak 1. Nacrtaju se vektori stupaca u prostoru (vidi sliku 6).

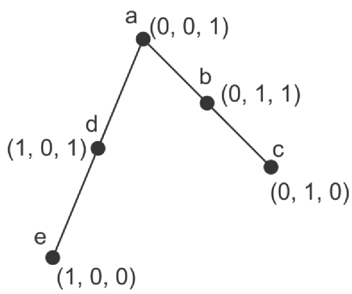
Korak 2. Nacrta se ravnina koja nije paralelna ni s jednim od zadanih vektora. Produže se ili smanje svi vektori tako da ravnina siječe svaki vektor ili njegovo produženje odnosno smanjenje. Gledaju se presjecišta ravnine i vektora, odnosno presjecišta ravnine i produženih ili smanjenih vektora (vidi sliku 6).



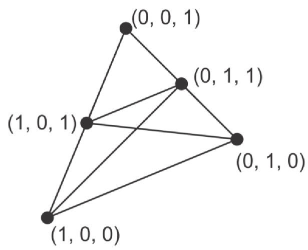

Slika 6: Projekcija vektora u ravninu $x + y + z = 1$.

Korak 3. Točke presjecišta ravnine i vektora, odnosno presjecišta ravnine i produženih ili smanjenih vektora u ravnini bit će slike zavisnosti vektora u stupcima matrice $B$ (vidi sliku 7). Uočimo da je dimenzija slike matroida 2, a rang matroida 3.




Slika 7: Slika matroida iz primjera 2.6.

Na slici 7 po konvenciji ne crtamo dužine koje povezuju dvije točke ako su one jedine dvije točke na toj dužini. Glavni razlog je da bi dodavanjem takvih dužina slika postala nepregledna (vidi sliku 8). U matroidu koji prikazuje slika 8 postoje četiri takve dužine: $\{b, d\}$, $\{b, e\}$, $\{c, d\}$, $\{c, e\}$.

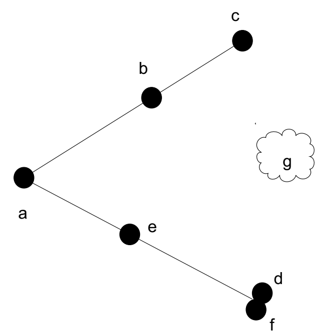



Slika 8: Slika matroida iz primjera 2.6 sa svim ucrtanim dužinama.

Kod primjera 2.6 najprije se crtaju vektori stupaca matrice i uz pomoć crteža se dolazi do slike matroida. No što možemo reći o linearnoj zavisnosti i nezavisnosti vektora ako imamo sliku matroida matrice s tri retka? Pomoću sljedećeg primjera pokazat ćemo što nam slika matroida govori o linearnoj zavisnosti i nezavisnosti vektora stupaca matrice.

**Primjer 2.7.** *Neka je matrica* $C = \begin{array}{c} \begin{array}{ccccccc} a & b & c & d & e & f & g \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & -1 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 & -4 & 0 \end{bmatrix} \end{array}.$

*Slika matroida koja prikazuje zavisnost stupaca matrice $C$ je sljedeća.*




Slika 9: Slika matroida iz primjera 2.7.

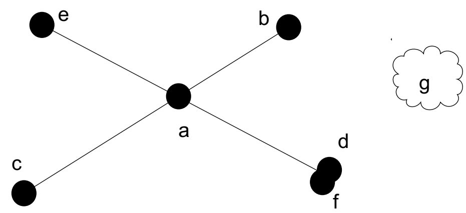
Najprije uočimo da matrica $C$ ima rang 3 i da je prema očekivanom dimenzija slike matroida 2. U ovoj matrici pojavljuju se dvije nove pojave:

- zavisan skup koji se sastoji od jednog elementa $\{g\}$, koji je jednak nulvektoru,
- zavisan skup koji se sastoji od dva elementa $\{d, f\}$.

Ostali zavisni skupovi su prikazani preko kolinearnosti točaka. Primjerice, vektori $a$, $b$ i $c$ su linearno zavisni jer je $(1, 1, 0) + (0, -1, 1) = (1, 0, 1)$.
Iz slike 9 dobivamo podatke o zavisnosti za matroid:

- $\{g\}$ je zavisan skup,
- $\{d, f\}$ je zavisan skup, a svi ostali dvočlani podskupovi od $\{a, b, c, d, e, f\}$ su nezavisni,
- $\{a, b, c\}$, $\{a, d, e\}$, $\{a, e, f\}$ su zavisni, a sve ostale trojke točaka uzete iz skupa $\{a, b, c, d, e, f\}$ koje ne sadrže istovremeno $d$ i $f$ su linearno nezavisne
- svaki skup koji ima četiri ili više točaka je zavisan.

Višestruku točku *df* i, općenito, višestruke točke matroida geometrijski prikazujemo tako da stavimo točku pokraj točke. Zavisan skup koji ima jedan element nije moguće prikazati kao točku. Njega prikazujemo tako da oko njega nacrtamo oblak (u našem slučaju oko $g$ smo nacrtali oblak). Takav zavisan jednočlan skup zove se petlja. Linearnu zavisnost vektora stupaca matrice $C$ možemo prikazati i slikom 10. Ova slika ekvivalentana je slici 9. Možemo uočiti da je redoslijed točaka nevažan. Važan je samo vjeran prikaz zavisnosti.




Slika 10: Slika matroida iz primjera 2.7.

U dosadašnjim primjerima temeljni skup matroida $E$ je bio skup vektora, no to ne mora uvijek biti tako. Na primjer, $E$ može biti skup bridova grafa. Primjeri takvih matroida bit će navedeni u idućoj cjelini.

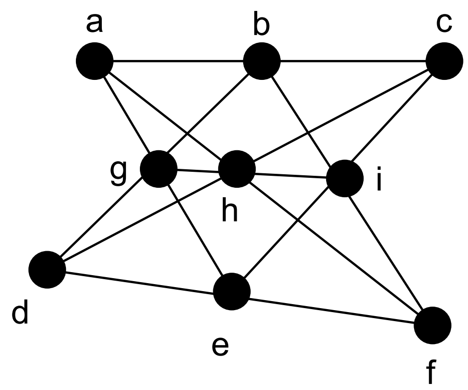
**Definicija 2.8.** M*atroid je reprezentabilan (prikazivi) nad poljem* $\mathbb{F}$ *ako postoji matrica* $A$ *nad poljem* $\mathbb{F}$ *takva da se zavisnost stupaca te matrice poklapa sa zavisnošću u matroidu.*

Stupci matrice $A$ čine temeljni skup reprezentabilnog matroida, a linearno nezavisan skup (nad poljem $\mathbb{F}$) stupaca matrice $A$ je linearno nezavisan skup $\mathcal{I}$ matroida.

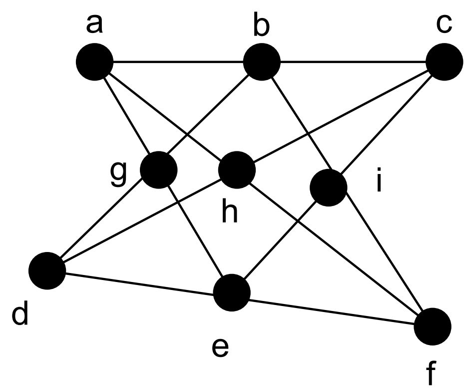
**Primjer 2.9.** *Neka je* $E = \{e_1, e_2, ..., e_n\}$. *Neka je* $k \leq n$ *i neka je* $\mathcal{I}$ *skup svih podskupova od* $E$ *s* $k$ *ili manje elemenata . Tada* $\mathcal{I}$ *zadovoljava aksiome* $(I1)$, $(I2)$ *i* $(I3)$. *Takav matroid naziva se uniformni matroid i označava se s* $U_{k,n}$. *Matroid* $U_{n,n}$ *zove se Booleova algebra i označava se s* $B_n$. *Matroid iz primjera 2.5 je uniformni matroid* $U_{2,4}$.

Postavlja se pitanje je li svaki matroid reprezentabilan? Svaki matroid sa sedam ili manje elemenata je reprezentabilan nad nekim poljem [2, str. 224.], no općenito svaki matroid nije reprezentabilan. U sljedećem primjeru navesti ćemo dva matroida čija konstrukcija je slična. Jedan matroid je reprezentabilan, a drugi nije.

**Primjer 2.10.**




Slika 11: Slika Papusovog matroida.




Slika 12: Slika ne-Papusovog matroida.

Matroid na slici 11 zovemo Papusov matroid po Papusu Aleksandrijskom. On je otkrio teorem koji se danas naziva Papusov teorem i njega koristimo u dobivanju slike Papusovog matroida. Slika Papusovog matroida dobiva se na sljedeći način:

- Nacrtaju se dvije dužine, dužina $\overline{abc}$ i dužina $\overline{def}$ tako da se na svakoj od njih nalaze tri odgovarajuće točke
- Točka $g$ se dobije kao sjecište dužina $\overline{ae}$ i $\overline{bd}$,
- Točka $h$ se dobije kao sjecište dužina $\overline{af}$ i $\overline{cd}$,

- Točka $i$ se dobije kao sjecište dužina $\overline{bf}$ i $\overline{ce}$,
- Prema Papusovom teoremu tri dobivene točke $g$, $h$, i $i$ trebaju biti kolinearne.

Matroid kod kojeg tri dobivene točke $g$, $h$, i $i$ nisu kolinearne zove se ne-Papusov matroid. Slika 12 prikazuje ne-Papusov matroid. Ne-Papusov matroid nije reprezentabilan ni nad jednim poljem. Ideja dokaza je sljedeća. Pokušava se pronaći matrica koja predstavlja ne-Papusov matroid. Dobiva se da takva matrica postoji samo ako su vektori $g$, $h$ i $i$ linearno zavisni, odnosno točke $g$, $h$ i $i$ kolinearne. Dakle, za ne-Papusov matroid ne postoji matrica takva da se zavisnost stupaca te matrice poklapa sa zavisnošću u matroidu pa ne-Papusov matroid nije reprezentabilan.

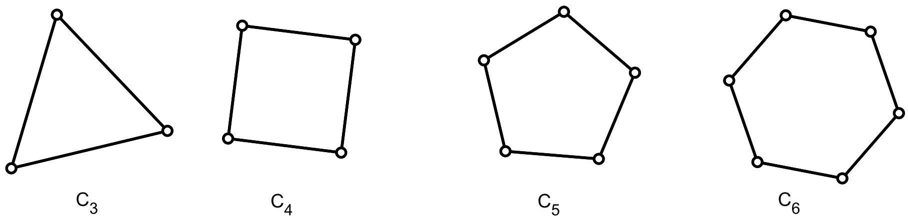
# 3 Matroidi iz grafova

Teorija matroida i teorija grafova su vrlo povezane. Mnogi izrazi vezani uz matroide dolaze upravo iz teorije grafova. Prije uspostave veze između matroida i grafova uvest ćemo osnovne pojmove vezane uz same grafove.

**Definicija 3.1.** *Graf $G$ je uređena trojka $G = (V(G), E(G), \psi(G))$ koja se sastoji od nepraznog skupa $V = V(G)$, čiji su elementi vrhovi od $G$, skupa $E = E(G)$ disjunktnog s $V(G)$, čiji su elementi bridovi od $G$ i funkcije incidencije $\psi(G)$ koja svakom bridu od $G$ pridružuje neuređeni par (ne nužno različitih) vrhova od $G$.*

Brid čiji se krajevi podudaraju zove se petlja. Dva brida ili više njih s istim parom krajeva zovu se višestruki bridovi. Bridove s bar jednim zajedničkim krajem zovemo incidentnim. Dva vrha su susjedna ako imaju zajednički brid.

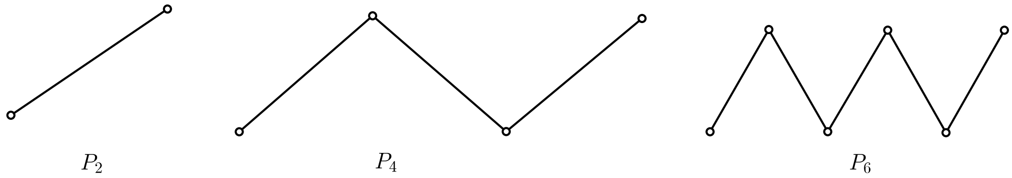
Ciklus $C_n$ na $n$ vrhova možemo definirati skupom vrhova $V = \{1, 2, ..., n\}$ i skupom bridova $E = \{\{i, i+1\} \,|i < n\} \cup \{\{1, n\}\}$:




Slika 13: Ciklusi.

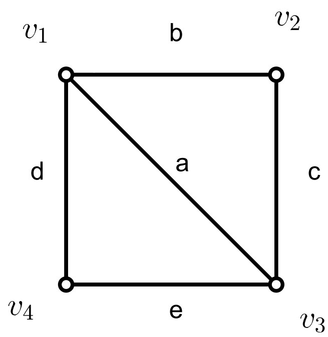
Podskup bridova je acikličan ako ne sadrži niti jedan ciklus.

Put $P_n$ na $n$ vrhova možemo definirati skupom vrhova $V = \{1, 2, ..., n\}$ i skupom bridova $E = \{\{i, i+1\} \,|i < n\}$:




Slika 14: Putovi.

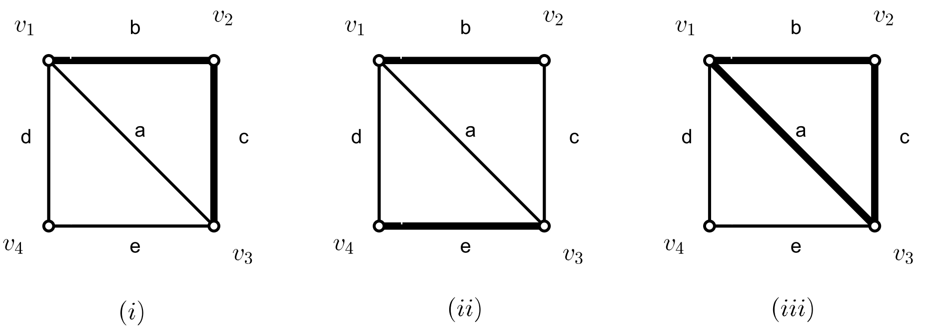
**Primjer 3.2.** *Analizirajmo graf $G$ na slici* 15.




Slika 15: Graf $G$.

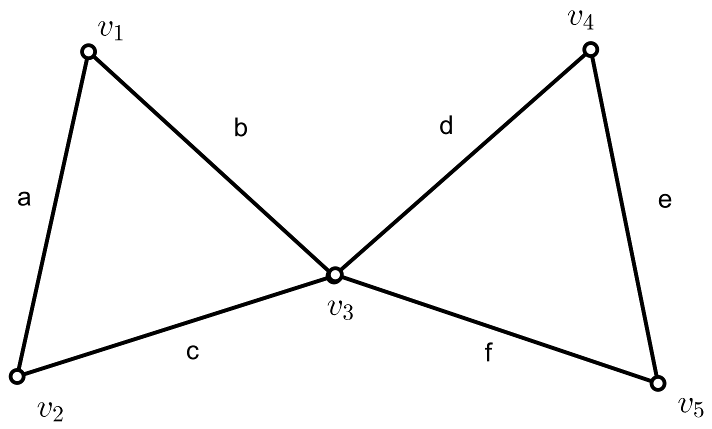
Graf $G$ na slici 15 ima skup vrhova $V = \{v_1, v_2, v_3, v_4\}$ i skup bridova $E = \{a, b, c, d, e\}$. Uočimo da su točke na slici 15 vrhovi grafa, a ne točke matroida. Također bridove grafa možemo crtati ravno ili zakrivljeno, oni nisu dužine kao kod matroida. Vrhove grafa možemo zamišljati kao gradove, a bridove kao ceste. Konkretno u ovom primjeru možemo ići iz grada $v_1$ cestom $b$ do grada $v_2$, zatim cestom $c$ do grada $v_3$. Takvo putovanje naziva se put u grafu $G$ i skraćeno zapisuje $(v_1, b, v_2, c, v_3)$ ili još kraće $(b, c)$ (vidi sliku 16 $(i)$).

Dva brida $(b, e)$ ne tvore put jer nisu incidentni (vidi sliku 16 $(ii)$). Nizovi u kojima se bridovi ponavljaju, također nisu putovi. Na primjer niz $(b, c, e, c)$ nije put jer se ponavlja brid $c$. Putovima ne zovemo ni nizove gdje se vrhovi ponavljaju (osim ciklusa) pa ni $(b, c, a, d)$ nije put. Ako putu $(b, c)$ dodamo brid $a$ dobivamo ciklus, odnosno put koji počinje i završava u istom vrhu (vidi sliku 16 $(iii)$).




Slika 16: Tri kopije grafa $G$: (i) put $bc$, (ii) skup bridova $be$, (iii) ciklus $abc$.

**Primjer 3.3.** *Promotrimo graf na slici* 17.



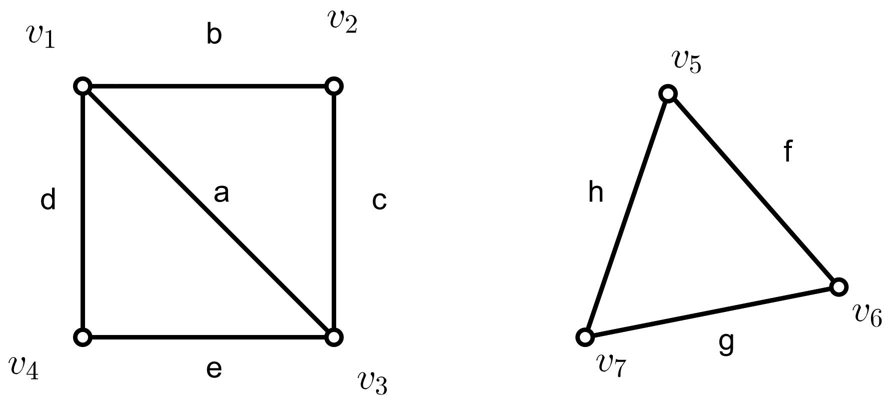

Slika 17: Graf $F$.

*Niz bridova* $(a, b, d, e, f, c)$ *grafa* $F$ *ne čini jedan ciklus nego dva ciklusa.*

Graf je povezan ako se svaka dva vrha mogu povezati putom u grafu, a inače je nepovezan. Svaki se nepovezani graf može prikazati kao unija povezanih grafova. Svaki član te unije zovemo komponentom povezanosti. Broj komponenti povezanosti grafa $G$ označavamo s $\omega(G)$.

**Definicija 3.4.** *Neka su* $G$ *i* $H$ *grafovi. Ako je* $V(H) \subseteq V(G)$ *i* $E(H) \subseteq E(G)$*, a svaki brid iz* $H$ *ima iste krajeve u* $H$ *kao što ih ima u* $G$*, onda kažemo da je* $H$ *podgraf od* $G$ *i pišemo* $H \subseteq G$*, a* $G$ *zovemo nadgraf od* $H$*.*

**Primjer 3.5.** *Promotrimo dva grafa, graf na slici* 15 *iz primjera 3.2 i graf na slici* 18.



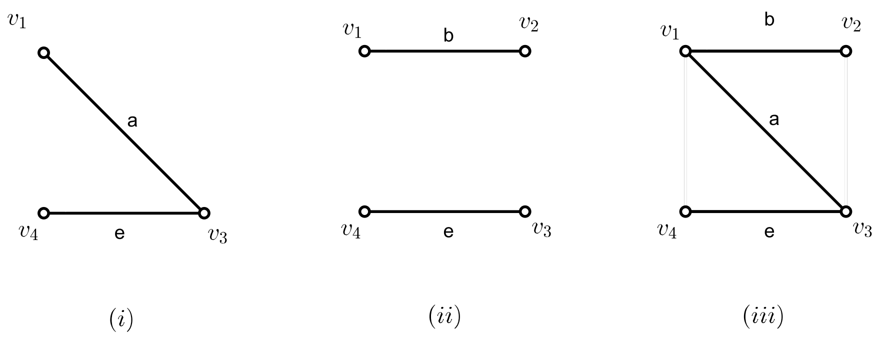

Slika 18: Graf $H$.

Graf $G$ na slici 16 je povezan, a graf $H$ na slici 18 je nepovezan jer na primjer ne postoji put u $H$ iz $v_2$ do $v_6$. $H$ je nepovezan graf sastavljen od dvije komponente povezanosti. Svaka komponenta je podgraf od $H$. Svi ciklusi i putovi iz primjera 3.2 su podgrafovi od grafa $G$.

Povezan graf koji ne sadrži cikluse zove se stablo, a graf koji nema ciklusa zove se šuma. Razapinjuće stablo povezanog grafa $G$ je stablo koje sadži sve vrhove grafa $G$. U povezanom grafu razapinjuća stabla su maksimalni aciklički podskupovi bridova. Minimalni ciklički podskupovi bridova su ciklusi.

**Primjer 3.6.** *Promotrimo ponovo graf $G$ iz primjera 3.2.*

Graf $G$ sadrži mnogo podgrafova koji su stabla ili šume.




Slika 19: Podgrafovi grafa $G$: (i) stablo, (ii) nepovezana šuma, (iii) razapinjuće stablo.

Slika 19 $(i)$ pokazuje jedno od stabala grafa $G$, 19 $(ii)$ pokazuje jednu šumu grafa $G$, a slika 19 $(iii)$ pokazuje jedno razapinjuće stablo grafa $G$. Podgraf grafa $G$ koji se sastoji od brida $e$ je također primjer šume. Šuma je i podgraf koji se sastoji od brida $e$ i vrha $v_1$.

**Teorem 3.7.** *Svaki povezani graf ima razapinjujuće stablo. Svako stablo s $n$ vrhova ima $n-1$ bridova.*

*Dokaz.* Neka je graf $G$ povezan. Promotrimo skup svih povezanih razapinjućih podgrafa od $G$. Taj je skup neprazan jer npr. sadrži $G$. Neka je $T$ minimalni element tog skupa. Prema definiciji je $\omega(T) = 1$ i $\omega(T \setminus e) > 1$ za svaki $e \in E(T)$. Iz toga slijedi da je svaki brid $e$ od $T$ takav da je $\omega(T \setminus e) > \omega(T)$, odnosno izbacivanjem svakog brida $e$ od $T$, graf $T$ se raspada na više komponenti povezanosti. $T$ je povezan, pa iz korolara 5 [8, str. 263.] slijedi da je $T$ stablo. Time smo dokazali da svaki povezani graf ima razapinjuće stablo.

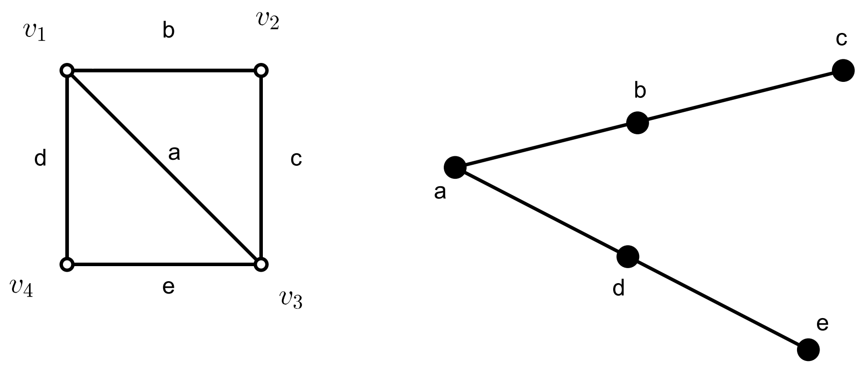
Dokažimo još da svako stablo s $n$ vrhova ima $n-1$ bridova. Tvrdnju ćemo dokazati matematičkom indukcijom po broju vrhova stabla. Graf $G$ je stablo pa ne sadrži ciklus. Ako uklonimo jedan brid iz $G$ dobivamo dva stabla s manje vrhova. Baza indukcije je očita. Pretpostavimo da tvrdnja vrijedi za sve grafove s manje od $n$ vrhova. Po pretpostavci indukcije dva stabla dobivena uklanjanjem jednog brida imaju $n_1 - 1$, odnosno $n_2 - 1$ bridova. Ovo znači da smo u početnom stablu, prije uklanjanja brida, imali $(n_1-1)+(n_2-1)+1$ bridova, a kako je $n_1+n_2 = n$, dobili smo da je početno stablo imalo $n-1$ bridova. Po aksiomu matematičke indukcije zaključujemo da svako stablo s $n$ vrhova ima $n-1$ bridova. $\square$

Povežimo sada matroide i grafove.

**Teorem 3.8.** *Neka je $E$ skup svih bridova grafa $G$ i $\mathcal{I}$ skup svih acikličnih podskupova bridova. Tada je uređeni par $(E, \mathcal{I})$ matroid $M(G)$.*

*Dokaz.* Trebamo dokazati da familija $\mathcal{I}$ zadovoljava svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$. Prazan skup je acikličan pa je sigurno element od $\mathcal{I}$. Dakle, $\mathcal{I} \neq \emptyset$ i svojstvo $(I1)$ je zadovoljeno. Ako je $B$ podskup acikličnih bridova i $A \subseteq B$, onda je $A$ također acikličan podskup bridova pa vrijedi i svojstvo $(I2)$. Preostaje nam pokazati svojstvo $(I3)$. Neka su $A$ i $B$ aciklični podskupovi bridova takvi da je $|A| < |B|$. Trebamo naći brid $b \in B \setminus A$ takav da $A \cup \{b\}$ ne sadrži ciklus. Razlikujemao dva slučaja. Pretpostavimo da je $A$ stablo. Tada je bridovima od $A$ pridruženo $|A| + 1$ vrhova grafa $G$. Skup $B$ je šuma pa se sastoji od $|B| + k$ vrhova, gdje je $k$ broj komponenti od $B$ i $k \geq 1$. Kako je $|B| > |A|$, vrijedi $|B| + k > |A| + 1$. Iz toga zaključujemo da su bridovima od $B$ pridruženi vrhovi od $G$ koji nisu pridruženi ni jednom bridu iz $A$. Nazovimo jedan takav vrh $v$ i neka je $b \in B$ bilo koji brid kojemu je pridružen vrh $v$. Tada je $A \cup \{b\}$ acikličan skup jer brid $b$ sadrži vrh koji nije pridružen ni jednom bridu iz $A$ pa $(I3)$ vrijedi. Sada promotrimo slučaj kada $A$ nije stablo. Pretpostavimo da se $A$ sastoji od $c$ disjunktnih stabala, nazovimo ih $T_1, T_2, ..., T_c$. Ako je bridovima iz $B$ pridružen bar jedan novi vrh (vrh koji nije pridružen ni jednom bridu iz $A$) , onda možemo postupiti kao u prethodnom slučaju. Pretpostavimo suprotno, da $B$ nije pridružen ni jedan novi vrh od $G$. S $e_i$ označimo broj bridova u stablu $T_i$, tako da je $e_1 + e_2 + ... + e_c = |A|$. Postoji brid u $B$ koji spaja dva stabla $T_i$ i $T_j$ iz $A$. U suprotnom, $B$ bi imao najviše $e_1$ bridova od $T_1$, $e_2$ bridova od $T_2$, itd..., jer bridovi iz $B$ nisu incidentni niti s jednim novim vrhom. Iz toga bi slijedilo da $|B| \leq e_1 + e_2 + ... + e_c = |A|$, što je u kontradikciji s $|A| < |B|$. Iz tog razloga $B$ mora imati brid koji spaja vrhove nekog stabla $T_i$ s vrhovima nekog stabla $T_j$. Taj brid možemo dodati u $A$ bez da stvorimo ciklus, pa $(I3)$ vrijedi. $\square$

**Primjer 3.9.** *Usporedimo graf $G$ iz primjera 3.2 i matroid sa slike* 20 *koji je povezan s njime. Matroid koji je povezan s grafom $G$ označavamo s $M(G)$.*

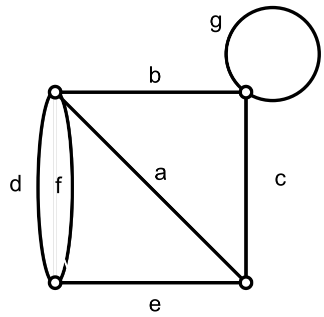


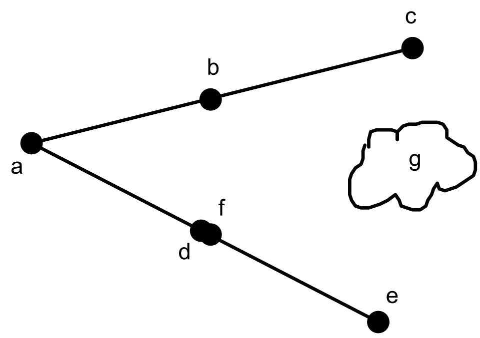

Slika 20: Lijevo: Graf $G$, desno: matroid $M(G)$.

Skup $\{a, b, e\}$ i svi njegovi podskupovi ne sadrže cikluse pa su nezavisni u matroidu $M(G)$. Skup $\{a, b, c\}$ je ciklus i on je zavisan u matroidu $M(G)$. Uočavamo da su minimalni zavisni skupovi matroida $M(G)$ tri ciklusa u grafu $G$: $C_1 = abc, C_2 = ade, C_3 = bced$. Zaključujemo da vrijedi općenito: Minimalni zavisni skupovi matroida su ciklusi grafa. Sada lako možemo odrediti koji su nezavisni skupovi matroida $M(G)$ gledajući samo graf $G$. To su svi podskupovi skupa $E = \{a, b, c, d, e\}$ koji ne sadrže ni jedan od tri ciklusa $C_1, C_2, C_3$. Dakle, svaki podskup koji sadrži 0,1 ili 2 elementa je nezavisan. Također svaki podskup od 3 elementa osim podskupova $abc$ i $ade$ je nezavisan. Ni jedan skup od 4 ili 5 elementa ne može biti nezavisan jer sadrži skup $abc$ ili skup $ade$. Uočimo da je najveći nezavisan skup matroida $M(G)$ razapinjuće stablo grafa $G$. Svako razapinjuće stablo ima tri brida pa je rang matroida $M(G)$ jednak 3. Ovaj zaključak vrijedi i općenito.

**Teorem 3.10.** *Neka je $G$ povezan graf s $n$ vrhova. Rang matroida $M(G)$ je jednak broju bridova u razapinjućem stablu grafa $G$, odnosno rang matroida je $n - 1$.*

**Primjer 3.11.** *Usporedimo graf $G$ sa slike* 21 *i matroid sa slike* 21 *koji je povezan s njime.*






Slika 21: Lijevo: Graf $G$, desno: matroid $M(G)$.

*Petlje u grafu $G$ odgovaraju petljama matroida $M(G)$. Mjesto petlje u grafu je nevažno za sliku matroida. Ako bi imali samo sliku matroida bilo bi nemoguće odrediti na kojem vrhu u grafu $G$ se nalazi petlja. Dvostruki brid df na slici matroida se pojavljuje kao višestruka točka df. Uočimo još da je matroid sa slike* 21 *matroid iz primjera 2.7.*

Kao što smo se prije pitali dobiva li se svaki matroid iz matrice sada se pitamo dobiva li se svaki matroid iz grafa? Odgovor na ovo pitanje također je negativan.

**Definicija 3.12.** *Matroid $M$ je grafovski ako postoji graf $G$ takav da se aciklički skupovi bridova grafa $G$ poklapaju s nezavisnim skupovima matroida $M$.*

U sljedećem primjeru navest ćemo matroid koji nije nastao od grafa. Prije toga istaknut ćemo propoziciju koju ćemo koristiti da pokažemo da postoji matroid koji nije nastao od grafa.

**Propozicija 3.13.** *Neka je $G$ graf i $M(G)$ grafovski matroid. Tada postoji povezan graf $G'$ takav da je $M(G) = M(G')$.*

**Primjer 3.14.** *Promotrimo uniformni matroid $U_{2,4}$ iz primjera 2.5. Pokazati ćemo da uniformni matroid $U_{2,4}$ nije grafovski.*

Pokušajmo konstruirati graf $G$ tako da je $M(G) = U_{2,4}$. Možemo pretpostaviti da ako takav graf postoji, onda je on povezan (vidi propoziciju 3.13).

Temeljni skup matroida $M$ je $\{a, b, c, d\}$. Iz toga slijedi da graf $G$ treba imati četiri brida. Razapinjuća stabla grafa $G$ imaju dva brida, pa prema teoremu 3.7, $G$ mora imati tri vrha. Nadalje, svi podskupovi s 0, 1 ili 2 elementa su nezavisni, a svi podskupovi s 3 ili 4 elementa su zavisni. Iz toga slijedi da ako $G$ postoji, onda on ima tri vrha, četiri brida i nema petlji ni višestrukih bridova. Kako graf s tri vrha i bez petlji te višestrukih bridova ima najviše tri brida, zaključujemo da graf $G$ ne postoji. Dakle, uniformni matroid $U_{2,4}$ nije grafovski.

Svi grafovski matroidi su reprezentabilni matroidi, odnosno postoji matrica čiji stupci odgovaraju bridovima grafa. Podskup vektora u stupcima matrice bit će linearno nezavisan ako i samo ako su odgovarajući bridovi u grafu aciklični (teorem 8.13 i 8.28 [2, str. 303., 313.]).

Postoji bliska veza između matroida i sparivanja u bipartitnim grafovima.

**Definicija 3.15.** *Bipartitan graf je graf čiji se skup vrhova može particionirati u dva međusobno disjunktna skupa $X$ i $Y$ tako da svaki brid ima jedan kraj u $X$, a drugi u $Y$. Paricija $(X, Y)$ zove se biparticija grafa.*

**Definicija 3.16.** *Sparivanje u grafu $G = (V, E)$ je podskup $M \subseteq E$ bridova čiji se krajevi ne podudaraju i nikoja dva brida iz $M$ nisu susjedna (tj. nikoja dva brida nisu incidentna s istim vrhom). Kažemo da su dva kraja brida u $M$ sparena u $M$.*

Za sparivanje $M$ grafa s biparticijom $(X, Y)$ neka je $M_X$ skup svih vrhova iz $X$ incidentnih s bridom iz $M$, a $M_Y$ skup svih vrhova iz $Y$ incidentnih s bridom iz $M$.

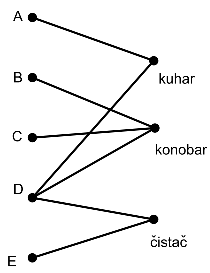
Navesti ćemo nekoliko primjera u kojima ćemo pobliže upoznati bipartitne grafove i njihovu vezu s matroidima.

**Primjer 3.17.** *Marko otvara restoran. Želi zaposliti kuhara, konobara i čistača. Pet osoba se prijavilo na natječaj. Tablica* 1 *pokazuje tko je zainteresiran za koji posao.*

| OSOBE | POSLOVI |
|---|---|
| Ana, Darija | kuhar |
| Boris, Cecilija, Darija | konobar |
| Darija, Edin | čistač |

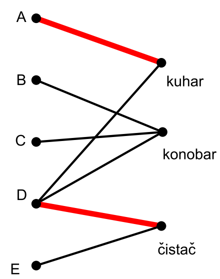
Tablica 1: Osobe i njihova stručna sprema.

Nacrtajmo bipartitni graf za ovaj problem (vidi sliku 22).




Slika 22: Bipartitni graf.

Skup $X = \{A, B, C, D, E\}$ predstavlja pet ljudi koji su se prijavili na natječaj, a skup $Y = \{kuhar, konobar, čistač\}$ prestavlja tri posla. Pogledajmo moguća sparivanja ovog grafa. Ona odgovaraju raspodjeli poslova ljudima. Na primjer, ako zaposlimo Anu na mjesto kuhara, a Dariju na mjesto čistača dobijemo sparivanje kao na slici 23.



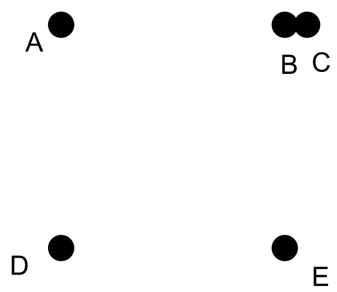

Slika 23: Sparivanje Ana - kuhar, Darija - čistač.

Podskupovi zaposlenih osoba mogu biti sljedeći: $\emptyset$, svi jednočlani podskupovi, svi dvočlani podskupovi osim $BC$, svi tročlani podskupovi osim $ABC, BCD, BCE$. Podskup od četiri osobe ne može biti podskup zaposlenih osoba jer Marko traži samo tri osobe koje će zaposliti. Ako Marko želi popuniti sva tri mjesta, on to može učiniti na razne načine. Naravno, istodobno ne može zaposliti Borisa i Ceciliju jer traži samo jednog konobara. Skup svih mogućih sparivanja daje nam vezu s matroidima.

**Teorem 3.18.** *Neka je $G$ bipartitni graf s biparticijom $(X, Y)$. Neka je $\mathcal{I}$ skup svih podskupova $I \subseteq X$ takvih da je postoji sparivanje $M$ u grafu $G$ za koje je $I = M_X$. Tada $\mathcal{I}$ zadovoljava svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$.*

Matroid $T(G)$ koji je povezan s bipartitnim grafom $G$ zovemo transverzalni matroid. Prema prethodnom teoremu iz bipartitnog grafa iz primjera

3.17 možemo dobiti matroid. Temeljni skup tog matroida je $\{A, B, C, D, E\}$, a nezavisni skupovi su svi oni podskupovi koji sudjeluju u sparivanju. Prema tome, nezavisni podskupovi su sljedeći: $\emptyset$, svi jednočlani skupovi, svi dvočlani skupovi osim $BC$, svi tročlani skupovi osim $ABC, BCD, BCE$. Ni jedan četveročlani skup nije nezavisan. Slika 24 je slika transverzalnog matroida grafa iz primjera 3.17.




Slika 24: Slika matroida iz primjera 3.17.

# 4 Nezavisni skupovi i baze

Gian-Carlo Rota je tvrdio da su matroidi jedna od najbogatijih i najkorisnijih ideja suvremene matematike [2, str. 40.]. Postoji mnogo ekvivalentnih definicija matroida i korisno je prevesti jedan aksiomatski sustav u drugi. Metoda kojom jedan aksiomatski sustav prevodimo u drugi zove se kriptomorfizam. Snaga matroida krije se u njihovom broju kriptomorfnih definicija. U drugom poglavlju definirali smo matroide preko nezavisnih skupova. Naveli smo tri svojstva $(I1)$, $(I2)$ i $(I3)$ koja nezavisni skupovi matroida trebaju zadovoljavati. No ta svojstva nisu jedina svojstva nezavisnih skupova matroida. Nezavisne skupove matroida možemo definirati i na drukčiji način. Sljedeća propozicija daje nam alternativnu definiciju matroida preko svojstva nezavisnosti.

**Propozicija 4.1.** *Neka je $E$ konačan skup. Familija $\mathcal{I}$ tvori nezavisne skupove matroida ako i samo ako:*

$(I1')$ $\emptyset \in \mathcal{I}$.

$(I2)$ *Ako je $J \in \mathcal{I}$ i $I \subseteq J$, onda je $I \in \mathcal{I}$.*

$(I3')$ *Ako su $I, J \in \mathcal{I}$ takvi da je $|J| = |I| + 1$, onda postoji $x \in J \setminus I$ takav da je $I \cup \{x\} \in \mathcal{I}$.*

*Dokaz.* Trebamo dokazati da $\mathcal{I}$ zadovoljava $(I1)$, $(I2)$ i $(I3)$ ako i samo ako zadovoljava $(I1')$, $(I2)$ i $(I3')$. Neka je $M = (E, \mathcal{I})$ matroid koji zadovoljava $(I1)$, $(I2)$ i $(I3)$. Pokažimo da matroid zadovoljava i $(I1')$ i $(I3')$. Uočimo da je svojstvo $(I3')$ poseban slučaj od $(I3)$. Preostaje nam pokazati da je zadovoljeno svojstvo $(I1')$. Prema $(I1)$ je $\mathcal{I} \neq \emptyset$, pa postoji skup $X \in \mathcal{I}$. Svaki podskup od $X$ je nezavisan, pa je $\emptyset \in \mathcal{I}$. Dakle, matroid zadovoljava i svojstvo $(I1')$.

Neka je sada $E$ konačan skup i $\mathcal{I}$ familija podskupova od $E$ koja zadovoljava $(I1')$, $(I2)$ i $(I3')$. Pokazat ćemo da $\mathcal{I}$ zadovoljava i svojstva $(I1)$, $(I2)$ i $(I3)$ pa stoga $\mathcal{I}$ tvori matroid. Vrijedi $\emptyset \in \mathcal{I}$, pa je $\mathcal{I} \neq \emptyset$. Preostaje nam još dokazati $(I3)$. Neka su $I, J \in \mathcal{I}$ takvi da $|I| < |J|$. Moramo naći $x \in J \setminus I$ takav da je $I \cup \{x\} \in \mathcal{I}$. Neka je $I'$ bilo koji podskup od $J$ takav da $|I'| = |I| + 1$. Kako je $I' \in \mathcal{I}$ (prema $(I2)$), prema $(I3')$ postoji $x \in I' \setminus I$ takav da je $I \cup \{x\} \in \mathcal{I}$. Iz $I' \subseteq J$ slijedi da je $x \in J \setminus I$ i time je dokaz gotov. $\square$

Maksimalni podskupovi familije $\mathcal{I}$ su svi oni podskupovi koji nisu sadržani ni u jednom drugom skupu te familije. Oni su maksimalni u odnosu na relaciju inkluzije $\subseteq$. Najveći podskupovi su podskupovi s najviše elemenata u familiji (imaju najveći kardinalni broj od svih podskupova). Najveći podskupovi moraju biti maksimalni, no obrat ne vrijedi. Na primjer, familija podskupova $\{\emptyset, \{a\}, \{c\}, \{a, b\}\}$ ima dva maksimalna podskupa $\{a, b\}$ i $\{c\}$, ali samo jedan najveći podskup $\{a, b\}$. Za familiju nezavisnih skupova matroida maksimalni i najveći podskupovi se podudaraju (slijedi iz svojstva $(I3)$). Možemo reći da su svi maksimalni nezavisni skupovi iste veličine. Te maksimalne nezavisne skupove u matroidu zovemo baze matroida.

**Definicija 4.2.** *Neka je $M$ matroid s familijom nezavisnih skupova $\mathcal{I}$. Maksimalne elemente familije $\mathcal{I}$ zovemo bazama matroida $M$.*

Matroid možemo definirati i preko baza. Za familiju svih baza $\mathcal{B}$ matroida vrijede ova svojstva:

(B1) $\mathcal{B} \neq \emptyset$.

(B2) Ako su $B_1$, $B_2 \in \mathcal{B}$ i $B_1 \subseteq B_2$, onda je $B_1 = B_2$.

(B3) Ako su $B_1$, $B_2 \in \mathcal{B}$ i $x \in B_1 \setminus B_2$, onda postoji $y \in B_2 \setminus B_1$ takav da je $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Ta svojstva koristit ćemo za definiranje matroida preko baza. Ona se mogu uzeti kao ekvivalentan aksiomatski sustav za matroide.

Svojstvo $(B2)$ možemo izreći i na sljedeći način:

(B2') Ako je $B_1$, $B_2 \in \mathcal{B}$, onda je $|B_1| = |B_2|$.

Prije nego uspostavimo kriptomorfizam između nezavisnih skupova i baza navesti ćemo još jednu propoziciju koju ćemo koristiti u dokazu teorema koji slijedi.

**Propozicija 4.3.** *Neka je $E$ konačan skup i $\mathcal{B}$ familija podskupova od $E$. Familija $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2)$ i $(B3)$ ako i samo ako $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$.*

*Dokaz.* Neka familija $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2)$ i $(B3)$. Pokažimo da tada ona zadovoljava i svojstva $(B1)$, $(B2')$ i $(B3)$. Zapravo trebamo dokazati da ona zadovoljava svojstvo $(B2')$. Neka su $B_1, B_2 \in \mathcal{B}$. Pretpostavimo da svojstvo $(B2')$ ne vrijedi, odnosno da je $|B_1| \neq |B_2|$. Tada je $|B_1| < |B_2|$ ili $|B_1| > |B_2|$. Promotrimo slučaj kada je $|B_1| < |B_2|$. Znamo da $B_1 \not\subseteq B_2$ jer bi inače $B_1 = B_2$ (prema svojstvu $(B2)$) pa bi $|B_1| = |B_2|$. Iz tog razloga postoji $x \in B_1 \setminus B_2$, pa prema svojstvu $(B3)$ postoji $y \in B_2 \setminus B_1$ takav da je $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$. Neka je $B_3 = (B_1 \setminus \{x\}) \cup \{y\}$. Vrijedi $B_3 \in \mathcal{B}$. Znamo da je $|B_3| = |B_1| < |B_2|$. Ako je $B_3 \subseteq B_2$, onda je prema $(B2)$, $B_3 = B_2$

pa je i $|B_3| = |B_2|$, što je u kontradikciji s $|B_3| < |B_2|$. Ako $B_3 \nsubseteq B_2$ onda postoji još neki $x_1 \in B_3 \setminus B_2$ i $y_1 \in B_2 \setminus B_3$ takav da je $(B_3 \setminus \{x_1\}) \cup \{y_1\} \in \mathcal{B}$. Uzmemo sada $B_4 = (B_3 \setminus \{x_1\}) \cup \{y_1\}$. Postupak ponavljamo sve dok ne dođemo do nekog $B_k$ takvog da je $B_k \subseteq B_2$. Jer je $B_k \subseteq B_2$, onda je prema $(B2)$, $B_k = B_2$ pa je i $|B_k| = |B_2|$, što je u kontradikciji s $|B_k| < |B_2|$. Dakle, svojstvo $(B2')$ vrijedi. Slučaj kada je $|B_2| < |B_1|$ analogan je slučaju kada je $|B_1| < |B_2|$, samo zamijenimo ulogu $B_1$ i $B_2$.

Neka sada familija $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$. Pokažimo da tada ona zadovoljava i svojstva $(B1)$, $(B2)$ i $(B3)$. Zapravo trebamo dokazati da ona zadovoljava svojstvo $(B2)$. Neka su $B_1, B_2 \in \mathcal{B}$ takvi da je $B_1 \subseteq B_2$. Prema svojstvu $(B2')$ vrijedi da je $|B_1| = |B_2|$. Sada iz $B_1 \subseteq B_2$ i $|B_1| = |B_2|$ slijedi da je $B_1 = B_2$ pa svojstvo $(B2)$ vrijedi. $\square$

Objasnimo još što znači pojam biti "kriptomorfan" na primjeru nezavisnih skupova i baza. Kako bi pokazali da su nezavisni skupovi i baze kriptomorfni trebamo slijediti ove korake:

(1) Pretpostavimo da nam je dana familija $\mathcal{I}$ nezavisnih skupova matroida. Definiramo familiju podskupova $\mathcal{B}$ kao skup maksimalnih nezavisnih skupova:
$$\mathcal{B} = \{B \in \mathcal{I} | B \subseteq A \in \mathcal{I} \Rightarrow B = A\}.$$

(2) Dokažemo da ako familija $\mathcal{I}$ zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$, onda familija $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$.

(3) Okrenemo postupak: pretpostavimo da nam je dana familija $\mathcal{B}$. Definiramo familiju podskupova $\mathcal{I}$ kao skup svih elemenata baza u $\mathcal{B}$:
$$\mathcal{I} = \{I \in E | \exists B \in \mathcal{B} \text{ takav da je } I \subseteq B\}.$$

(4) Dokažemo da ako familija $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$, onda familija $\mathcal{I}$ zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$.

(5) Dokažemo da su ova dva pridruživanja jedno drugom inverzna. Ako nam je zadana familija $\mathcal{I}$ i ako na nju primjenimo prvo transformaciju (1), a zatim transformaciju (3), onda se trebamo uvjeriti da opet dobijemo početnu familiju $\mathcal{I}$. Također trebamo provjeriti da je i obrnuta kompozicija indentiteta. Ako nam je zadana familija $\mathcal{B}$ i ako na nju djelujemo prvo transformacijom (3), a zatim transormacijom (1), onda se trebamo uvjeriti da opet dobijemo početnu familiju $\mathcal{B}$ (vidi sliku 25).

Sada možemo izreći teorem.

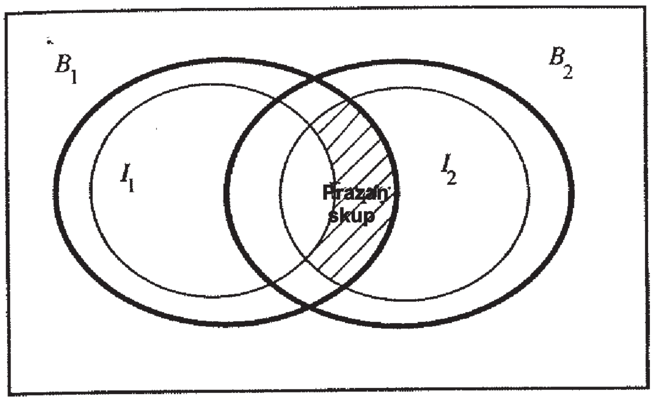
**Teorem 4.4.** *Neka je $E$ konačan skup i $\mathcal{B}$ familija podskupova od $E$ koja zadovoljava svojstva $(B1)$, $(B2)$ i $(B3)$. Tada je $(E, \mathcal{B})$ kriptomorfan s matroidom $M = (E, \mathcal{I})$ i $\mathcal{B}$ je skup baza tog matroida.*


Slika 25: Kriptomorfizam između nezavisnih skupova i baza.

*Dokaz.* Neka je $M = (E, \mathcal{I})$ matroid. Tada familija $\mathcal{I}$ podskupova od $E$ zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$. Neka je $\mathcal{B}$ skup svih maksimalnih podskupova od $\mathcal{I}$, odnosno $\mathcal{B} = \{B \in \mathcal{I} \,|\, B \subseteq B' \Rightarrow B = B'\}$. Trebamo dokazati da $\mathcal{B}$ zadovoljava $(B1)$, $(B2')$ i $(B3)$ (prema prethodnoj propoziciji možemo zamijeniti $(B2)$ s $(B2')$. Prvo dokažimo da $\mathcal{B}$ zadovoljava $(B1)$. Kako je $\emptyset \in \mathcal{I}$, a $E$ je konačan skup, možemo naći $B \in \mathcal{I}$ koji nije sadržan ni u jednom drugom nezavisnom skupu. Stoga $B \in \mathcal{B}$, pa $\mathcal{B} \neq \emptyset$ i $(B1)$ vrijedi. Dokažimo sada da $\mathcal{B}$ zadovoljava $(B2')$. Ako postoje skupovi $B_1$, $B_2 \in \mathcal{B}$ takvi da je $|B_1| < |B_2|$, tada postoji $x \in B_2 \setminus B_1$ takav da je $B_1 \cup \{x\} \in \mathcal{I}$ ($B_1, B_2 \in \mathcal{I}$ pa koristimo $(I3)$). $B_1$ je podskup od $B_1 \cup \{x\}$ pa dolazimo do kontradikcije s definicijom baze $\mathcal{B}$. Dakle, $|B_1| = |B_2|$, pa vrijedi i $(B2')$. Preostaje nam dokazati da $\mathcal{B}$ zadovoljava $(B3)$. Neka su $B_1$, $B_2 \in \mathcal{B}$ takvi da je $x \in B_1 \setminus B_2$. Ako je $B_1 \neq B_2$, onda takav $x$ sigurno postoji zbog načina na koji smo definirali $\mathcal{B}$. Kako su $B_1, B_2 \in \mathcal{I}$ na njih možemo primijeniti svojstva nezavisnosti $(I1)$, $(I2)$ i $(I3)$. Iz $(I2)$ slijedi da je $B_1 \setminus \{x\} \in \mathcal{I}$. Sada primijenimo $(I3)$ na skupove $B_1 \setminus \{x\}$ i $B_2$. Vrijedi $|B_1 \setminus \{x\}| < |B_2|$, pa postoji $y \in B_2 \setminus (B_1 \setminus \{x\})$ takav da je $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{I}$. Ako pokažemo da $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ dokazali smo da $\mathcal{B}$ zadovoljava $(B3)$. Vrijedi $|(B_1 \setminus \{x\}) \cup \{y\}| = |B_1| = |B_2|$, pa ako bi $(B_1 \setminus \{x\}) \cup \{y\}$ bio iz $\mathcal{I}$, ali ne bi bio iz $\mathcal{B}$, onda postojao $B_3 \in \mathcal{B}$ takav da $(B_1 \setminus \{x\}) \cup \{y\} \subset B_3$ i $|B_1| = |(B_1 \setminus \{x\}) \cup \{y\}| < |B_3|$. Ta činjenica je u kontradikciji s $(B2')$ pa za sve $B_1$, $B_2 \in \mathcal{B}$ takve da je $x \in B_1 \setminus B_2$ postoji $y \in B_2 \setminus B_1$ takav da je

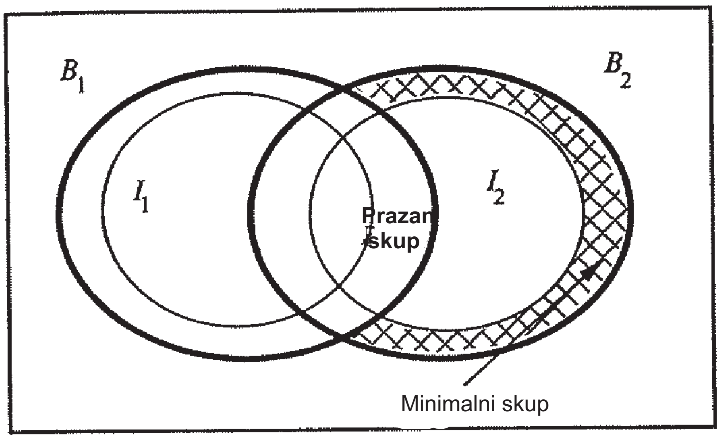
$(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ i $(B3)$ vrijedi. Dakle, svojstva $(B1)$, $(B2')$ i $(B3)$ slijede iz svojstava $(I1)$, $(I2)$ i $(I3)$.

Neka je $\mathcal{B}$ familija podskupova od $E$ takva da zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$ i neka je $\mathcal{I} = \{I \,|\, I \subseteq B, B \in \mathcal{B}\}$. Mi trebamo dokazati da $\mathcal{I}$ zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$ i time je $(E, \mathcal{I})$ matroid. Iz $(B1)$ slijedi da je $\mathcal{B} \neq \emptyset$ i $\mathcal{B} \subseteq \mathcal{I}$, pa je $\mathcal{I} \neq \emptyset$ i $(I1)$ vrijedi. Da bi dokazali da vrijedi svojstvo $(I2)$ trebamo pokazati da ako je $I' \subseteq I$ za neki $I \in \mathcal{I}$, onda je $I' \in \mathcal{I}$. Na način na koji smo definirali $\mathcal{I}$, znamo da je $I \subseteq B$ za neki $B \in \mathcal{B}$. No tada $I' \subseteq I \subseteq B$, pa $I' \in \mathcal{I}$ i $(I2)$ vrijedi. Za svojstvo $(I3)$ koristit ćemo dokaz kontradikcijom. Neka su $I_1, I_2 \in \mathcal{I}$ takvi da je $|I_1| < |I_2|$. Pretpostavimo da $(I3)$ ne vrijedi. Pokazat ćemo da to povlači $|I_1| \geq |I_2|$ što je u kontradikciji s $|I_1| < |I_2|$. Kako su $I_1, I_2 \in \mathcal{I}$, postoje $B_1, B_2 \in \mathcal{B}$ takvi da je $I_1 \subseteq B_1$ i $I_2 \subseteq B_2$. Vrijedi $I_1 \cap I_2 = B_1 \cap I_2$ (ili $I_2 \setminus B_1 = I_2 \setminus I_2$) jer u suprotnome postoji $x \in (I_2 \cap B_1) \setminus I_1$, pa bi $I_1 \cup \{x\} \subseteq B_1$ i aksiom $(I3)$ bi vrijedio, a pretpostavili smo da ne vrijedi (vidi sliku 26).



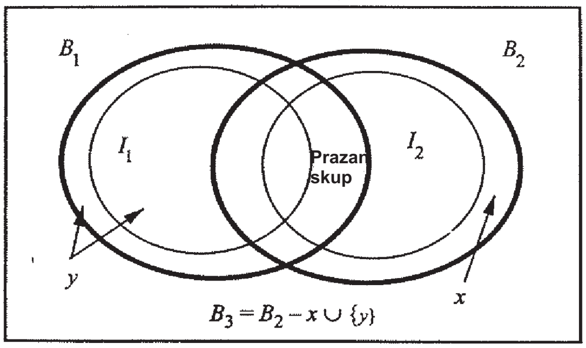

Slika 26: $I_1 \cap I_2 = B_1 \cap I_2$.

Skup $B_2$ možemo izabrati na više načina jer postoji više baza čiji je podskup $I_2$. Mi sada uzmemo $B_2 \in \mathcal{B}$ takav da je $I_2 \subseteq B_2$ i $|B_2 \setminus (I_2 \cup B_1)|$ je minimalalan (vidi sliku 27).




Slika 27: Odaberemo $B_2$ tako da je $|B_2 \setminus (I_2 \cup B_1)|$ minimalan.

Uz takav izbor $B_2$ vrijedi $B_2 \setminus (I_2 \cup B_1) = \emptyset$ jer ako bi postojao $x \in B_2 \setminus (I_2 \cup B_1)$, onda uz zamjenu uloga $B_1$ i $B_2$ u $(B3)$, postoji i neki $y \in B_1 \setminus B_2$ takav da je $B_3 = (B_2 \setminus \{x\}) \cup y \in \mathcal{B}$ (vidi sliku 28). No, $I_2 \subseteq B_3$ i $|B_3 \setminus (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_1)|$, što je u kontradikciji s minimalnišću $|B_2 \setminus (I_2 \cup B_1)|$, pa je stoga $B_2 \setminus (I_2 \cup B_1) = \emptyset$.



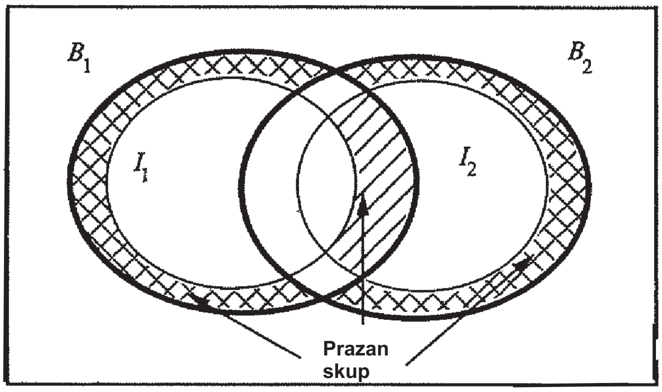

Slika 28: Zbog minimalnosti kod izbora $B_2$ vrijedi $B_2 \setminus (I_2 \cup B_1) = \emptyset$.

Slično, možemo izabrati $B_1$ takav da je $B_1 \setminus (I_1 \cup B_2) = \emptyset$. Sada promotrimo skupove $B_2 \setminus B_1$ i $B_1 \setminus B_2$ (vidi sliku 29):

$$B_2 \setminus B_1 = I_2 \setminus B_1 = I_2 \setminus I_1$$

i

$$B_1 \setminus B_2 = I_1 \setminus B_2 \subseteq I_1 \setminus I_2.$$




Slika 29: $B_2 \setminus B_1 = I_2 \setminus I_1$ i $B_1 \setminus B_2 \subseteq I_1 \setminus I_2$.

Sada iz $(B2')$ slijedi $|B_1| = |B_2|$, pa je i $|B_2 \setminus B_1| = |B_1 \setminus B_2|$. No iz toga slijedi $|I_2 \setminus I_1| \leq |I_1 \setminus I_2|$, pa stoga $|I_2| \leq |I_1|$. To je u kontradikciji s $|I_1| < |I_2|$ pa vrijedi svojstvo $(I3)$.

Način na koji definiramo $\mathcal{I}$ preko $\mathcal{B}$ ili $\mathcal{B}$ preko $\mathcal{I}$ određuje dvije funkcije na skupu svih familija podskupova od $E$:

$$f(\mathcal{I}) = \{B \in \mathcal{I} | B \subseteq B' \Rightarrow B = B'\},$$

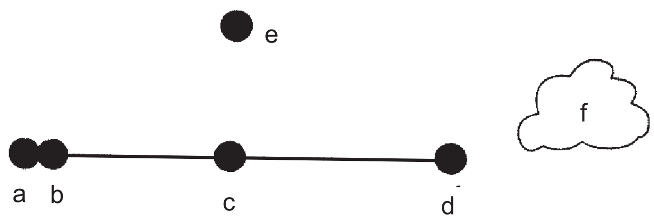
$$g(\mathcal{B}) = \{I | I \subseteq B; B \in \mathcal{B}\}.$$

Neka su $f$ i $g$ te dvije "kriptomorfne funkcije". Trebamo pokazati da se one pravilno komponiraju, odnosno da je $g(f(\mathcal{I})) = \mathcal{I}$ i $f(g(\mathcal{B})) = \mathcal{B}$ (vidi sliku 25). Neka je $M = (E, \mathcal{I})$ matroid, i neka su $f(\mathcal{I}) = \mathcal{B}$ svi maksimalni elementi od $\mathcal{I}$ i $g(\mathcal{B}) = \mathcal{I}'$ svi podskupovi elemenata iz $\mathcal{B}$. Znamo da je $\mathcal{I}' = \{I | I \subseteq B, B \in \mathcal{B}\}$. Trebamo pokazati $\mathcal{I} = \mathcal{I}'$. Za dokazivanje inkluzije $\mathcal{I}' \subseteq \mathcal{I}$ bitno je da familija $\mathcal{I}$ zadovoljava svojstvo $(I2)$, odnosno da je familija $\mathcal{I}$ zatvorena na uzimanje podskupova, pa su elementi kompozicije $\mathcal{I} \to f(\mathcal{I}) \to g(f(\mathcal{I}))$ uvijek u $\mathcal{I}$. Prvo pokažimo da je $\mathcal{I} \subseteq \mathcal{I}'$. Ako je $I \in \mathcal{I}$, onda postoji neki maksimalni $B$ koji sadrži $I$. Zbog toga $I \in \mathcal{I}' = (g \circ f)(\mathcal{I})$. Sada pokažimo da $\mathcal{I}' \subseteq \mathcal{I}$. Neka je $I' \in \mathcal{I}'$. Tada $I' \subseteq B$ za neki maksimalni $B \in \mathcal{I}$. Prema $(I2)$ vrijedi $I' \in \mathcal{I}$, pa je $\mathcal{I} = \mathcal{I}'$ i $(g \circ f)(\mathcal{I}) = \mathcal{I}$.

Neka je sada dan matroid $(E, \mathcal{B})$ takav da $\mathcal{B}$ zadovoljava svojstva $(B1)$, $(B2')$ i $(B3)$ i neka je $\mathcal{B}' = (f \circ g)(\mathcal{B})$ skup svih maksimalnih podskupova u $\mathcal{I} = g(\mathcal{B})$, tj. $\mathcal{B}' = \{B \in \mathcal{I} | B \subseteq B' \in \mathcal{I} \Rightarrow B = B'\}$. Moramo pokazati $\mathcal{B} = \mathcal{B}'$. Za dokazivanje inkluzije $\mathcal{B}' \subseteq \mathcal{B}$ bitno je da familija $\mathcal{B}$ zadovoljava svojstvo $(B2)$, pa ćemo postupkom $\mathcal{B} \to g(\mathcal{B}) \to f(g(\mathcal{B}))$ uvijek dobiti $\mathcal{B}$. Prvo dokažimo da je $\mathcal{B} \subseteq \mathcal{B}'$. Pretpostavimo $B \in \mathcal{B}$. Trebamo pokazati da

$B \in \mathcal{B}'$, odnosno da je $B$ maksimalni podskup od $g(\mathcal{B}) = \mathcal{I}$. U suprotnome, $B$ ne bi bio maksimalni podskup od $\mathcal{I}$, pa bi vrijedilo $B \subseteq B'$ za neki $B' \neq B$, što je u kontradikciji s $(B2')$. Dakle, $\mathcal{B} \subseteq \mathcal{B}'$. Pokažimo sada da je $\mathcal{B}' \subseteq \mathcal{B}$. Ako je $B' \in \mathcal{B}'$, onda je $B' \in \mathcal{I}$, pa $B' \subseteq B$ za neki $B \in \mathcal{B}$. Kako je $B'$ maksimalni podskup od $\mathcal{I}$ i $B \in \mathcal{I}$ zaključujemo da je $B = B'$, pa je $B' \in \mathcal{B}$. Dakle, $\mathcal{B} = \mathcal{B}'$. □

**Primjer 4.5.** *Neka je $M$ matroid s temeljnim skupom $E = \{a, b, c, d, e, f\}$ i bazama $\mathcal{B} = \{ace, ade, bce, bde, cde\}$. Sliku tog matroida prikazuje slika* 30.




Slika 30: Slika matroida iz primjera 4.5.

Zanimljivi su nam elementi $e$ i $f$ matroida. Element $e$ je element svake baze matroida. Može se dodati u svaki nezavisan skup matroida bez da promijeni nezavisnost skupa. Takav element zove se rezni element ili kopetlja matroida. S druge strane, element $f$ nije ni u jednoj bazi matroida, štoviše nije ni u jednom nezavisnom skupu matroida. Kako smo prije naveli taj element zovemo petlja.

**Definicija 4.6.** *Neka je $M$ matroid s temeljnim skupom $E$. Kopetlja je element $x \in E$ koji je u svakoj bazi. Petlja je element $x \in E$ koji nije ni u jednoj bazi.*

# 5 Ciklusi i nezavisni skupovi

Mininalne zavisne skupove u matroidu zovemo ciklusi.

**Definicija 5.1.** *Neka je $M = (E, \mathcal{I})$ matroid. Skup $C \subseteq E$ zovemo ciklus matroida ako je $C$ zavisan skup, a svaki njegov podskup je nezavaisan.*

U matroidu iz primjera 4.5 postoje četiri ciklusa:

$$\mathcal{C} = \{f, ab, acd, bcd\}\,.$$

Navođenje ciklusa najčešće je vrlo učinkovit način opisivanja matroida. Vrlo je lako rekonstruirati nezavisne skupove iz ciklusa. Pojmovi minimalni i najmanji su različiti pojmovi za zavisne skupove. Za razliku od baza, ciklusi mogu imati različiti broj elemenata. Matroid iz primjera 4.5 ima petlju $f$ koja je ciklus sama po sebi i kopetlju $e$ koja nije sadržana ni u jednom ciklusu matroida $M$. Navedimo sada tri svojstva koja zadovoljava familija ciklusa matroida i pomoću ta tri svojstva definirajmo matroid.

Familija $\mathcal{C}$ svih ciklusa matroida zadovoljava ova svojstva:

(C1) $\emptyset \notin \mathcal{C}$.

(C2) Ako su $C_1$, $C_2 \in \mathcal{C}$ i $C_1 \subseteq C_2$, onda je $C_1 = C_2$.

(C3) Ako su $C_1$, $C_2 \in \mathcal{C}$ takvi da je $C_1 \neq C_2$ i $x \in C_1 \cap C_2$, onda postoji neki $C_3 \in \mathcal{C}$ takav da je $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$.

Veza između skupa $\mathcal{C}$ i $\mathcal{I}$ je sljedeća. Neka je $M = (E, \mathcal{I})$ matroid. Ciklusi $\mathcal{C}$ su minimalni podskupovi od $E$ koji nisu nezavisni. Odnosno

$$\mathcal{C} = \{C \subseteq E \,|C \notin \mathcal{I}; I \subset C \Rightarrow I \in \mathcal{I}\}\,.$$

Nezavisni skupovi $\mathcal{I}$ su svi podskupovi od $E$ koji ne sadrže ciklus, odnosno

$$\mathcal{I} = \{I \subseteq E \,|\forall C \in \mathcal{C}, C \nsubseteq I\}\,.$$

Sada možemo uspostaviti kriptomorfizam između ciklusa i nezavisnih skupova (vidi sliku 31).

**Teorem 5.2.** *Neka je $E$ konačan skup i $\mathcal{C}$ familija podskupova od $E$ koja zadovoljava svojstva $(C_1)$, $(C_2)$ i $(C_3)$. Tada je $(E, \mathcal{C})$ kriptomorfan s matroidom $M = (E, \mathcal{I})$ i $\mathcal{C}$ je skup ciklusa matroida $M$.*


Slika 31: Kriptomorfizam između nezavisnih skupova i ciklusa.

Skica dokaza je sljedeća.

(1) Pretpostavimo da imamo matroid definiran preko nezavisnih skupova $\mathcal{I}$. Definiramo cikluse kao minimalne zavisne skupove:

$$\mathcal{C} = \{C \subseteq E \,|C \notin \mathcal{I}; I \subset C \Rightarrow I \in \mathcal{I}\}\,.$$

(2) Dokažemo da ako familija $\mathcal{I}$ matroida zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$, onda familija $\mathcal{C}$ zadovoljava svojstva $(C_1)$, $(C_2)$ i $(C_3)$.

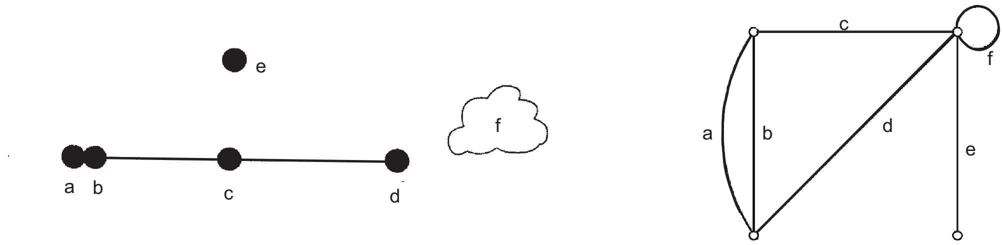
(3) Sada pretpostavimo da imamo familiju ciklusa $\mathcal{C}$. Definiramo familiju nezavisnih skupova na sljedeći način:

$$\mathcal{I} = \{I \subseteq E \,|\forall C \in \mathcal{C}, C \nsubseteq I\}\,.$$

(4) Dokažemo da ako familija $\mathcal{C}$ zadovoljava svojstva $(C_1)$, $(C_2)$ i $(C_3)$, onda familija $\mathcal{I}$ zadovoljava svojstva $(I1)$, $(I2)$ i $(I3)$.

(5) Dokažemo da su pridruživanja (1) i (3) jedna drugom inverzna.

**Primjer 5.3.** *Neka je $M$ matroid s temeljnim skupom $E = \{a, b, c, d, e, f\}$ i bazama $\mathcal{B} = \{ace, ade, bce, bde, cde\}$. To je isti matroid iz primjera 4.5. Slika* 32 *prikazuje taj matroid i graf $G$ koji mu je pridružen.*




Slika 32: Lijevo: slika matroida $M$ iz primjera 4.5, desno: graf $G$ povezan s matroidom $M$.

*Analizirajmo sliku* 32 *i objasnimo na slici što nam točno govori svojstvo* $(C3)$*.*

Skup $B$ je baza matroida $M$ ako se $B$ sastoji od tri nekolinearne točke. Primijetimo da je kopetlja $e$ u svakom takvom skupu. Baze matroida $M$ odgovaraju razapinjućim stablima grafa $G$, a brid grafa, čije uklanjanje bi izdvojilo jedan vrh grafa $G$ od ostatka grafa, odgovara kopetlji $e$. Objasnimo sada svojstvo $(C3)$. Neka su $C_1 = \{a, b\}$ i $C_2 = \{b, c, d\}$. Tada je $b \in C_1 \cap C_2$. Prema svojstvu $(C_3)$ postoji ciklus $C_3$ takav da je $C_3 \subseteq (C_1 \cup C_2) \setminus \{b\} = \{a, c, d\}$. Iz slike 32 vidimo da je $\{a, c, d\}$ ciklus, pa $C_3 = \{a, c, d\}$ zadovoljava svojstvo $(C_3)$. Promotrimo što to znači u grafu $G$. Dvobrid $ab$ i trokut $bcd$ su dva ciklusa u grafu $G$. Ta dva ciklusa se presjecaju u bridu $b$ i jasno je da je $(C_1 \cup C_2) \setminus \{b\}$ također ciklus. Štoviše, za grafove, $(C_1 \cup C_2) \setminus (C_1 \cap C_2)$ bit će disjunktna unija ciklusa. Primijetimo da se za matroid iz primjera 4.5 graf može konstruirati i drukčije. Na primjer, petlju smo mogli smjestiti na bilo koji vrh grafa, a to smo mogli učiniti i s kopetljom dok god ona ne bi tvorila ciklus s nekim drugim bridom.

# 6 Rang

Neka je $A$ podskup temeljnog skupa $E$ matroida. Pogledajmo veličinu svih nezavisnih skupova koji su sadržani u $A$. Najveći nezavisan podskup od $A$ je rang tog skupa.

**Definicija 6.1.** *Neka je $M = (E, \mathcal{I})$ matroid i $A \subseteq E$. Rang skupa $A$ je veličina najvećeg nezavisnog podskupa od $A$:*

$$r(A) := \max \{|I| | I \in \mathcal{I}, I \subseteq A\}.$$

Rang matroida $r(M)$ jednak je rangu temeljnog skupa $r(E)$. Rang je zapravo funkcija $r$ iz skupa svih podskupova temeljnog skupa $E$ matroida u skup nenegativnih cijelih brojeva:

$$r : 2^E \to \mathbb{N} \cup 0.$$

**Primjer 6.2.** *Nađimo rang različitih podskupova matroida iz primjera 4.5.*

- $r(A) = 0$: $r(\emptyset) = 0$, svaki podskup koji sadrži samo petlje također ima rang 0: $r(\{f\}) = 0$.
- $r(A) = 1$: Svi jednočlani skupovi osim petlje $f$ imaju rang 1, također svi dvočlani skupovi koji sadrže petlju $f$ imaju rang 1 pa skupovi $af, bf, cf, df, ef$ imaju rang 1. Rang 1 imaju i skupovi $ab$ i $abf$.
- $r(A) = 2$: Ako zanemarimo petlju, skup ima rang 2 ako razapinje dužinu. Ako izaberemo bilo koje dvije ili više točaka $a, b, c, d$, osim para $ab$, one će razapinjati dužinu. Postoji 10 takvih podskupova skupa $\{a, b, c, d\}$. Podskupovi koji sadrže točku $e$ i imaju rang 2 su: $r(abe) = r(ae) = r(be) = r(ce) = r(de) = 2$. Ti podskupovi odgovaraju dužinama koje sadrže samo dvije točke i po konvenciji ih ne crtamo na slici matroida. Ako bilo kojem od navedenih podskupova koji imaju rang 2 dodamo petlju $f$, rang tih podskupova neće se promijeniti, pa dobivamo još 15 podskupova ranga 2.
- $r(A) = 3$: Rang od $A$ bit će 3 onda kada $A$ sadrži bazu. Dakle, rang 3 imaju svi oni podskupovi $A$ koji sadrže točku $e$ i razapinju dužinu koja sadrži točke $a, b, c, d$.

| Rang | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| Broj podskupova | 2 | 12 | 30 | 20 |

Tablica 2: Broj podskupova matroida iz primjera 4.5 prema rangu.

Tablica 2 pokazuje broj podskupova određenog ranga. Primijetimo da je $2 + 12 + 30 + 20 = 64$ i $2^6 = 64$ što znači da smo naveli sve podskupove od $E$. Primijetimo još da su maksimalni podskupovi ranga 2 skupovi: $\{abef, cef, def, abcdf\}$. Svi oni razapinju dužinu i rang bi im povećalo dodavanje bilo koje točke. Vidimo još da dodavanje petlje $f$ bilo kojem skupu ne povećava njegov rang. Međutim, dodavanje kopetlje $e$ uvijek povećava rang skupa $A$ (ako $e$ već nije bio u tom skupu). Iz tih opažanja slijedi sljedeća propozicija.

**Propozicija 6.3.** *Neka je $M$ matroid s temeljnim skupom $E$ i funkcijom ranga $r$.*

*(1) Element $x \in E$ je petlja ako i samo ako za sve $A \subseteq E$ vrijedi $r(A \cup \{x\}) = r(A)$.*

*(2) Element $x \in E$ je kopetlja ako i samo ako za sve $A \subseteq E$ takve da $x \notin A$ vrijedi $r(A \cup \{x\}) = r(A) + 1$.*

*Dokaz.* Prvo dokažimo (1). Neka je $x \in E$ petlja, $A \subseteq E$ i $x \notin A$. Element $x$ je petlja pa po definiciji on nije ni u jednoj bazi. Neka je $B = A \cup \{x\}$. Očito $r(B) \geq r(A)$. Pretpostavimo da je $r(B) > r(A)$. Tada je $x$ u bazi jer se rang povećao što je u kontradikciji s time da $x$ nije ni u jednoj bazi. Dakle, $r(B) = r(A \cup \{x\}) = r(A)$. Pretpostavimo sada da je $A \subseteq E$, $x \notin A$ i $r(A \cup \{x\}) = r(A)$. Iz toga slijedi da $x$ nije ni u jednoj bazi jer ne povećava rang ni jednom podskupu skupa $E$ pa je po definiciji, element $x$ petlja.

Sada dokažimo (2). Neka je $x \in E$ kopetlja, $A \subseteq E$ i $x \notin A$. Element $x$ je kopetlja pa je po definiciji u svakoj bazi. Ako imamo skup $A$ i njemu dodamo element $x$ koji nije u $A$ njegov rang će ostati isti ili će se povisiti najviše za 1. Pošto je $x$ u svakoj bazi vrijedi $r(A \cup \{x\}) = r(A) + 1$. Pretpostavimo sada da je $A \subseteq E$, $x \notin A$ i $r(A \cup \{x\}) = r(A) + 1$. Vidimo da element $x$ povećava rang svakog podskupa skupa $E$ pa je element $x$ u svakoj bazi te je po definciji element $x$ kopetlja. □

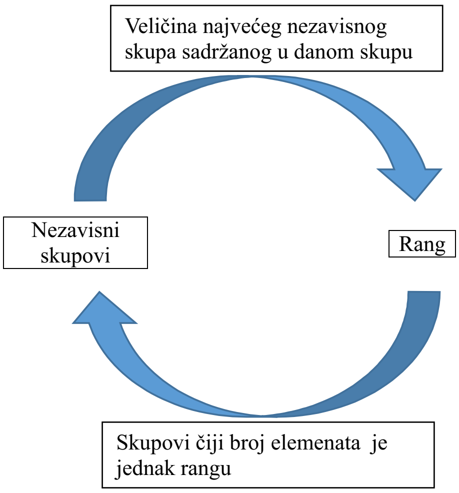
Definicija matroida preko funkcije ranga iskazana je sljedećim teoremom.

**Teorem 6.4.** *Neka je $E$ konačan skup s cjelobrojnom funkcijom $r$ definiranom na podskupovima od $E$. Funkcija $r$ je funkcija ranga matroida ako i samo ako za sve $A, B \subseteq E$ vrijedi:*

$(R1)$ $0 \leq r(A) \leq |A|$.

$(R2)$ *Ako je $A \subseteq B$, onda je $r(A) \leq r(B)$.*

$(R3)$ $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.




Slika 33: Kriptomorfizam između nezavisnih skupova i ranga.

Prije nego dokažemo teorem navest ćemo ekvivalentna svojstva svojstvima $(R1)$, $(R2)$ i $(R3)$:

$(R1')$ $r(\emptyset) = 0$.

$(R2')$ Ako je $A \subseteq E$ i $x \in E$, onda je $r(A) \leq r(A \cup \{x\}) \leq r(A) + 1$.

$(R3')$ Ako je $r(A) = r(A \cup \{x\}) = r(A \cup \{y\})$, za $x, y \notin A$, tada je $r(A) = r(A \cup \{x, y\})$.

Sljedeća lema pomoći će nam u dokazivanju ekvivalentnosti ovih svojstava.

**Lema 6.5.** *Ako je $A \subseteq B$, onda je $r(A \cup \{x\}) - r(A) \geq r(B \cup \{x\}) - r(B)$ za svaki $x \in E$.*

*Dokaz.* Pretpostavimo da funkcija $r$ ima svojstva $(R1)$, $(R2)$ i $(R3)$. Dokazujemo da iz $A \subseteq B$ i $x \in E$ slijedi nejednakost $r(A \cup \{x\}) - r(A) \geq r(B \cup \{x\}) - r(B)$. Ako je $x \in B$, onda je $B = B \cup \{x\}$ pa je desna strana jednaka 0. Tada je nejednakost ekvivalentna s $r(A) \leq r(A \cup \{x\})$, a to očito slijedi iz monotonosti $(R2)$. Pretpostavimo sada da $x \notin B$. Primijenimo svojstvo $(R3)$ na skupove $A \cup \{x\}$ i $B$:

$$r((A \cup \{x\}) \cup B) + r((A \cup \{x\}) \cap B) \leq r(A \cup \{x\}) + r(B).$$

Očito je $(A \cup \{x\}) \cup B = B \cup \{x\}$ i $(A \cup \{x\}) \cap B = A$, pa imamo:

$$r(B \cup \{x\} + r(A) \leq r(A \cup \{x\}) + r(B).$$

To je ekvivalentno s nejednakosti:

$$r(A \cup \{x\} - r(A) \geq r(B \cup \{x\} - r(B).$$

$\square$

**Propozicija 6.6.** *Svojstva funkcije ranga* $(R1)$*,* $(R2)$ *i* $(R3)$ *ekvivalentna su svojstvima* $(R1')$*,* $(R2')$ *i* $(R3')$*.*

*Dokaz.* Pretpostavimo da za rang vrijede svojstva $(R1)$, $(R2)$ i $(R3)$. Dokažimo da tada vrijede svojstva $(R1')$, $(R2')$ i $(R3')$. Kako je $0 \leq r(\emptyset) \leq 0$, odmah dobivamo da je $r(\emptyset) = 0$, pa svojstvo $(R1')$ vrijedi. Neka je $A \subseteq E$ i $x \in E$. Pokažimo da vrijedi $r(A) \leq r(A \cup \{x\}) \leq r(A) + 1$. Prema svojstvu $(R2)$ vrijedi $r(A) \leq r(A \cup \{x\})$, pa nam preostaje još pokazati $r(A \cup \{x\}) \leq r(A) + 1$. Neka je $B = \{x\}$. Tada prema svojstvu $(R3)$ vrijedi $r(A \cup \{x\}) + r(A \cap \{x\}) \leq r(A) + r(\{x\})$. Vrijedi $0 \leq r(A \cap \{x\}) \leq 1$ i $0 \leq r(\{x\}) \leq 1$ pa imamo $r(A \cup \{x\}) \leq r(A \cup \{x\}) + r(A \cap \{x\}) \leq r(A) + r(\{x\}) \leq r(A) + 1$, odnosno $r(A \cup \{x\}) \leq r(A) + 1$, što je i trebalo pokazati. Pokažimo još da vrijedi i svojstvo $(R3')$, odnosno pokažimo da ako je $r(A) = r(A \cup \{x\}) = r(A \cup \{y\})$, onda je $r(A) = r(A \cup \{x, y\})$. Zbog monotonosti $(R2)$ očito je $r(A) \leq r(A \cup \{x, y\})$. Suprotna nejednakost slijedi iz leme 6.5, primijenjene na $A$ i $B = A \cup \{y\}$:

$$r(A \cup \{x\}) - r(A) \geq r(B \cup \{x\}) - r(B).$$

Po pretpostavci je $r(B) = r(A)$ i lijeva strana je 0. Dakle, $r(A) = r(B) \geq r(B \cup \{x\}) = r(A \cup \{x, y\})$. Time smo dokazali jednakost $r(A) = r(A \cup \{x, y\})$.

Pretpostavimo sada da funkcija $r$ zadovoljava svojstva $(R1')$, $(R2')$ i $(R3')$. Dokažimo da tada zadovoljava i svojstva $(R1)$, $(R2)$ i $(R3)$. Svojstvo $(R2)$ slijedi iz svojstva $(R2')$: ako je $A \subseteq B$, onda postoje $x_1, x_2, ..., x_k \in E$ takvi da je $B = A \cup \{x_1, ..., x_k\}$. Uzastopnom primijenom lijeve nejednakosti iz $(R2')$ dobivamo $r(A) \leq r(A \cup \{x_1\}) \leq r(A \cup \{x_1\} \cup \{x_2\}) \leq ... \leq r(A \cup \{x_1\} \cup ... \cup \{x_k\}) = r(B)$. Dakle, svojstvo $(R2)$ vrijedi. Dokažimo sada da vrijedi svojstvo $(R1)$. Lijeva strana nejednakosti $(R1)$, $0 \leq r(A)$, slijedi iz $(R1')$ i upravo dokazane monotonosti $(R2)$. Naime, $\emptyset \subseteq A$, pa vrijedi $0 \leq r(\emptyset) \leq r(A)$. Desnu stranu nejednakosti $(R1)$, $r(A) \leq |A|$, dobijemo uzastopnom primijenom desne nejednakosti iz $(R2')$: ako je $A = \{x_1, ..., x_k\}$, onda redom dobivamo $r(\{x_1\}) \leq r(\emptyset) + 1 = 1$, $r(\{x_1, x_2\}) \leq r(\{x_1\}) + 1 \leq 2$, $r(\{x_1, x_2, x_3\}) \leq r(\{x_1, x_2\}) + 1 \leq 3$,..., $r(A) = r(\{x_1, ..., x_k\}) \leq k = |A|$. Preostaje još dokazati da svojstvo $(R3)$ slijedi iz svojstava $(R1')$, $(R2')$ i $(R3')$. Da tvrdnja $(R3)$ vrijedi dokazati ćemo pomoću leme 6.5 indukcijom po $|A \setminus B|$. Ako je $|A \setminus B| = 0$, onda je $A \subseteq B$, pa je $A \cup B = B$ i $A \cap B = A$. U tom slučaju očito vrijedi tvrdnja ($R3$). Ako je $|A\backslash B| = 1$, recimo $A\backslash B = \{x\}$, označimo s $A' = A \setminus \{x\}$. Tada je $A' \subseteq B$ pa možemo primijeniti lemu 6.5: $r(A' \cup \{x\}) - r(A') \geq r(B \cup \{x\}) - r(B)$. Očito je $A' \cup \{x\} = A$, $A' = A \cap B$ i $B \cup \{x\} = A \cup B$, pa imamo $r(A) - r(A \cap B) \geq r(A \cup B) - r(B)$ što je ekvivalentno s tvrdnjom ($R3$). Pretpostavimo sada da tvrdnja ($R3$) vrijedi uvijek kad je $|A \setminus B| = n$ i uzmimo skupove za koje je $|A \setminus B| = n + 1$. Izaberemo neki $x \in A \setminus B$ i definiramo $A' = A \setminus \{x\}$. Po pretpostavci indukcije tvrdnja ($R3$) vrijedi za skupove $A'$ i $B$, tj. vrijedi

$$r(A' \cup B) + r(A' \cap B) \leq r(A') + r(B) \Leftrightarrow$$

$$r(A' \cup B) - r(A') \leq r(B) - r(A' \cap B) = r(B) - r(A \cap B) \qquad (1)$$

(očito je $A \cap B = A' \cap B$). Sada primijenimo lemu 6.5 na skupove $A' = A' \cup B$ i element $\{x\}$:

$$r(A' \cup \{x\}) - r(A') \geq r(A' \cup B \cup \{x\}) - r(A' \cup B) \Leftrightarrow$$

$$\Leftrightarrow r(A) - r(A') \geq r(A \cup B) - r(A' \cup B) \Leftrightarrow$$

$$\Leftrightarrow r(A \cup B) - r(A) \leq r(A' \cup B) - r(A'). \qquad (2)$$

Iz nejednakosti (1) i (2) slijedi $r(A \cup B) - r(A) \leq r(B) - r(A \cap B)$, a to je ekvivalentno s tvrdnjom ($R3$) primijenjenom na skupove $A$ i $B$. Dakle, tvrdnja ($R3$) vrijedi za sve prirodne brojeve $|A\backslash B| \in \mathbb{N}$, tj. za sve podskupove $A, B \subseteq E$.

U dokazu smo koristili tvrdnju leme 6.5, koju smo dokazali iz aksioma ($R1$), ($R2$) i ($R3$). Preostaje još dokazati lemu 6.5 iz slabijih aksioma ($R1'$), ($R2'$) i ($R3'$). Pretpostavimo da je $A \subseteq B$ i $x \notin B$. Zbog aksioma ($R2'$) je $0 \leq r(A \cup \{x\}) - r(A) \leq 1$ i $0 \leq r(B \cup \{x\}) - r(B) \leq 1$, pa je nejednakost iz leme 6.5 ekvivalentna s implikacijom $r(B \cup \{x\}) = r(B) + 1 \Rightarrow r(A \cup \{x\}) = r(A) + 1$. Prvo dokazujemo tu implikaciju u slučaju kad je $B = A \cup \{y\}$, tj. $|B \setminus A| = 1$. Pretpostavimo suprotno, da je $r(B \cup \{x\}) = r(B) + 1$ i $r(A \cup \{x\}) = r(A)$. Ako je $r(B) = r(A \cup \{y\}) = r(A)$, dobivamo kontradikciju s aksiomom ($R3'$) (tada bi vrijedilo $r(B \cup \{x\}) = r(A \cup \{x, y\}) = r(A) = r(B)$). Ako je $r(B) = r(A \cup \{y\}) = r(A) + 1$, slijedi da je $r(A \cup \{x, y\}) = r(B \cup \{x\}) = r(B) + 1 = r(A) + 2$. S druge strane, iz aksioma ($R2'$) slijedi $r(A \cup \{x, y\}) \leq r(A \cup \{x\}) + 1 = r(A) + 1$. Opet smo dobili kontradikciju pa implikacija vrijedi kad je $|B \setminus A| = 1$. Opći slučaj $|B \setminus A| = n \in \mathbb{N}$ dokazuje se indukcijom po $n$. Ako uzmemo proizvoljni $y \in B \setminus A$ i definiramo $B' = B \setminus \{y\}$, onda iz $r(B \cup \{x\}) = r(B) + 1$ po upravo dokazanom slijedi $r(B' \cup \{x\}) = r(B') + 1$. Iz toga i iz pretpostavke indukcije tada slijedi $r(A \cup \{x\}) = r(A) + 1$. $\square$

Iskažimo još jednu propoziciju koja će nam pomoći u dokazivanju teorema 6.4.

**Propozicija 6.7.** *Neka je $r$ funkcija ranga matroida. Za svaki $A \subseteq E$ i $x_1, x_2, ..., x_n \in E$ vrijedi:*

($R3''$) *Ako je $r(A) = r(A \cup \{x_1\}) = r(A \cup \{x_2\}) = ... = r(A \cup \{x_n\})$, onda je $r(A \cup \{x_1, x_2, ..., x_n\}) = r(A)$.*

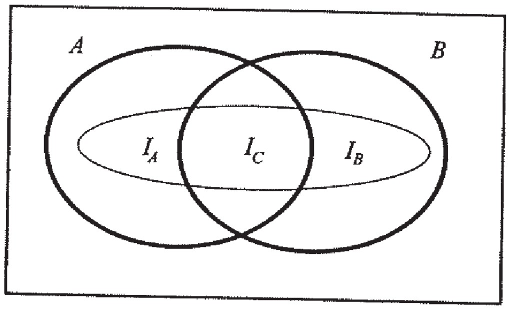
*Dokaz.* Tvrdnja slijedi iz svojstva ($R3'$) indukcijom po $n$. Za $n = 2$ očit se tvrdnje ($R3'$) i ($R3''$) podudaraju. Pretpostavimo da ($R3''$) vrijedi za neki $n \geq 2$ i pokažimo da tada vrijedi i za $n + 1$. Neka je $A' = A \cup \{x_{n+1}\}$. Prema ($R3'$) primijenjenom na skup $A$ i elemente $x_i$, $x_{n+1}$ zaključujemo da je $r(A) = r(A') = r(A \cup \{x_i, x_{n+1}\}) = r(A' \cup \{x_i\})$, za $i = 1, ..., n$. Po pretpostavci indukcije tada je $r(A) = r(A') = r(A' \cup \{x_1, ..., x_n\}) = r(A \cup \{x_1, ..., x_n, x_{n+1}\})$. □

Dokažimo sada teorem 6.4.

*Dokaz.* Neka je $M = (E, \mathcal{I})$ matroid. Definiramo $r(A)$ kao veličinu najvećeg nezavisnog skupa koji je sadržan u $A$. Pokažimo da $r$ zadovoljava svojstva ($R1$), ($R2$) i ($R3$). Iz definije funkcije $r$ slijedi da je $0 \leq r(A) \leq |A|$, pa ($R1$) vrijedi. Ako je $A \subseteq B \subseteq E$, tada će svaki nezavisan podskup od $A$ biti nezavisan podskup od $B$, pa imamo

$$r(A) = max\{|I| : I \subseteq A; I \in \mathcal{I}\} \leq max\{|J| : J \subseteq B; J \in \mathcal{I}\} = r(B).$$

Dakle, i svojstvo ($R2$) vrijedi. Pokažimo da vrijedi i svojstvo ($R3$). Neka su $A$ i $B$ podskupovi od $E$ i neka je $I_C$ baza od $A \cap B$, odnosno neka je $I_C$ maksimalni nezavisni podskup od $A \cap B$. Koristimo svojstvo ($I3$) i proširimo $I_C$ do baze $I$ za $A \cup B$. Neka je $I_A = I \cap (A \setminus B)$ i $I_B = I \cap (B \setminus A)$. Po konstrukciji, $r(A \cap B) = |I_C|$, $r(A \cup B) = |I| = |I_A| + |I_B| + |I_C|$. Skup $I_A \cup I_C$ je nezavisan skup sadržan u $A$ (jer je $I_A \cup I_C \subseteq I$). Zbog toga, $r(A) \geq |I_A| + |I_C|$ (prema ($R2$)). Slično, $r(B) \geq |I_B| + |I_C|$. Kombiniranjem ovih činjenica dobivamo: $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$ (vidi sliku 34).




Slika 34: Dokaz svojstva $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Neka je sada dana funkcija $r$ definirana na podskupovima konačnog skupa $E$ koja zadovoljava svojstva $(R1)$, $(R2)$ i $(R3)$. Definiramo familiju $\mathcal{I}$ kao skup svih podskupova $I$ od $E$ takvih da je $r(I) = |I|$. Pokazat ćemo da je $\mathcal{I}$ familija nezavisnih skupova matroida tako da ćemo dokazat da $\mathcal{I}$ zadovoljava svojstva $(I1')$, $(I2)$ i $(I3)$. Prema $(R1)$, $r(\emptyset) = 0$, pa $r(\emptyset) = |\emptyset|$, što znači da $\emptyset \in \mathcal{I}$. Dakle, svojstvo $(I1')$ je zadovoljeno. Dokažimo sada da vrijedi svojstvo $(I2)$. Neka je $J \in \mathcal{I}$ i $I \subseteq J$. Koristimo sad svojstvo $(R3)$. Neka je $A = J \setminus I$ i $B = I$. Pokažimo da $r(I) = |I|$. Kako je $J \in \mathcal{I}$, znamo da je $r(J) = |J|$, pa:

$$r(A \cup B) + r(A \cap B) = r(J) + r(\emptyset) = |J|.$$

Sada prema $(R1)$, znamo da $r(S) \leq |S|$ za sve $S \subseteq E$, pa

$$r(A) + r(B) = r(J \setminus I) + r(I) \leq |J \setminus I| + |I| = |J|.$$

Sada imamo:

$$|J| = r(J) + r(\emptyset) \leq r(J \setminus I) + r(I) \leq |J \setminus I| + |I| = |J|.$$

Iz toga zaključujemo da je $r(J \setminus I) = |J \setminus I|$ i $r(I) = |I|$. Dakle, $I \in \mathcal{I}$ i svojstvo $(I2)$ vrijedi. Još trebamo dokazati da familija $\mathcal{I}$ zadovoljava svojstvo $(I3)$. To ćemo dokazat kontradikcijom. Neka su $I, J \in \mathcal{I}$ takvi da je $|I| < |J|$ i neka je $J \setminus I = \{x_1, x_2, ..., x_k\}$ za neki $k \geq 1$. Po pretpostavci, znamo da $r(I) = |I|$ i $r(J) = |J|$. Sada pretpostavimo da za sve $x_i \in J \setminus I$, svojstvo $(I3)$ ne vrijedi: $I \cup \{x_i\} \notin \mathcal{I}$. Tada, po definiciji od $\mathcal{I}$ mora vrijediti:

$$|I| = r(I) = r(I \cup \{x_1\}) = r(I \cup \{x_2\}) = ... = r(I \cup \{x_k\}).$$

Prema $(R3'')$, $r(I \cup \{x_1, x_2, ..., x_k\}) = |I|$. No, $|I \cup \{x_1, x_2, ..., x_k\}| = |J|$, pa je $|J| = r(J) \leq |I| < |J|$, što je kontradikcija. Dakle, svojstvo $(I3)$ vrijedi.

Preostaje nam još dokazati da se kriptomorfizam pravilno komponira, odnosno da $\mathcal{I} \to r \to \mathcal{I}'$ daje $\mathcal{I} = \mathcal{I}'$ i $r \to \mathcal{I} \to s$ zadovoljava $r = s$. Prvo dokažimo da $r \to \mathcal{I} \to s$ zadovoljava $r = s$. Neka je $r$ funkcija ranga koja zadovoljava svojstva $(R1)$, $(R2)$ i $(R3)$. Definiramo familiju $\mathcal{I}$: $I \in \mathcal{I}$ ako $r(I) = |I|$. Koristimo familiju $\mathcal{I}$ za definiranje nove funkcije ranga $s$: $s(A) = max\,\{|I| : I \in \mathcal{I}, I \subseteq A\}$. Naš cilj je pokazati da je funkcija ranga $r$ jednaka funkciji ranga $s$: $r(A) = s(A)$ za sve $A \subseteq E$. Neka je $A \subseteq E$. Dokazat ćemo da je $r(A) = s(A)$ tako da ćemo pokazat da vrijedi $s(A) \leq r(A)$ i $r(A) \leq s(A)$. Primijetimo da $s(A) = |I| = r(I)$ za neki $I \subseteq A$. Prema $(R2)$ imamo $r(I) \leq r(A)$, odnosno ako to izrazimo preko funkcije $s$, imamo:

$$s(A) = |I| = r(I) \leq r(A).$$

Preostaje još pokazati da $s(A) \geq r(A)$. Pretpostavimo da to ne vrijedi, tj. da $s(A) < r(A)$ za neki $A \subseteq E$. Tada za sve $I \in \mathcal{I}$ takve da $I \subseteq A$, mora vrijediti $r(A) > |I|$. Neka $I$ bude takav maksimalan skup. Tada za sve $x \in A \setminus I$, imamo $I \cup \{x\} \notin \mathcal{I}$. Zato, $r(I \cup \{x\}) = r(I)$ za sve $x \in A \setminus I$. Prema $(R3'')$, dobivamo $r(A) = r(I) = |I|$, što je u kontradikciji s $r(A) > |I|$, pa vrijedi $s(A) \geq r(A)$.

Sada dokažimo da iz $\mathcal{I} \to r \to \mathcal{I}'$ slijedi $\mathcal{I} = \mathcal{I}'$. Neka je $\mathcal{I}$ familija nezavisnih skupova. Definiramo funkciju ranga: $r(A) = max\,\{|I| : I \in \mathcal{I}, I \subseteq A\}$. Dakle, $r(A)$ je veličina najvećeg nezavisnog podskupa od $A$. Neka je familija $\mathcal{I}'$ skup svih podskupova takvih da je $r(I) = |I|$. Pokažimo da je $\mathcal{I} = \mathcal{I}'$. Ako je $I \in \mathcal{I}$, onda je $r(I) = |I|$ po definiciji funkcije $r$, pa je $I \in \mathcal{I}'$. Ako je $I \in \mathcal{I}'$, onda je $r(I) = |I|$, pa je $I$ najveći nezavisni podskup od $\mathcal{I}$ (po definiciji funkcije ranga $r$). Stoga $I \in \mathcal{I}'$. Dakle, $\mathcal{I} = \mathcal{I}'$. □

Pomoću sljedećeg primjera objasnit ćemo nužnost dokazivanja pravilnog komponiranja kriptomorfizma.

**Primjer 6.8.** *Kada dokazujemo u teoremu 6.4 da se kriptomorfizam dobro komponira, pokazujemo između ostalog i da su dvije funkcije ranga $r(A)$ i $s(A)$ ekvivalentne kada prelazimo iz $r$, u $\mathcal{I}$, pa u $s$. Koristimo aksiom $(R2)$ kada dokazujemo da je $s(A) \leq r(A)$ za sve podskupove od $A$. Je li to stvarno potrebno? Kako bi odgovorili na ovo pitanje, definiramo funkciju ranga na skupu $E = \{a, b\}$: $r(\emptyset) = r(ab) = 0, r(a) = r(b) = 1$. Tu je svojstvo $(R2)$ narušeno, pa tako definirana funkcije nije funkcija ranga matroida. Formiramo $\mathcal{I}$ kao u kriptomorfizmu i dobivamo $\mathcal{I} = \{\emptyset, a, b\}$. Korištenjem familije $\mathcal{I}$ u definiranju funkcije $s$, dobivamo: $s(\emptyset) = 0, s(a) = s(b) = s(ab) = 1$. Vidimo da je $r(ab) < s(ab)$. Dakle, dokazivanje pravilnog komponiranja kriptomorfizma je nužno.*

**Primjer 6.9.** *Pokažimo da je svojstvo* $(R3)$ *zadovoljeno promatrajući sliku matroida iz 4.5. Neka je* $A = \{a, b, c, e\}$ *i* $B = \{a, b, d\}$. *Tada* $r(A) = 3$, $r(B) = 2$, $r(A \cup B) = 3$ *i* $r(A \cap B) = 1$. *Vidimo da je* $r(A) + r(B) = 5$, *a* $r(A \cup B) + r(A \cap B) = 4$, *pa je svojstvo* $(R3)$ *zadovoljeno. Štoviše,* $r(A \cup B) + r(A \cap B) < r(A) + r(B)$, *odnosno vrijedi stroga nejednakost.*

Ako imamo familiju nezavisnih skupova, relativno je lako pronaći rang svakog podskupa od skupa $E$.

**Primjer 6.10.** *Neka je zadan temeljni skup* $E = \{a, b, c\}$ *matroida* $M$ *i rang svakog podskupa od* $E$*:*

$$r(\emptyset) = 0; r(a) = r(b) = r(c) = r(ab) = 1; r(ac) = r(bc) = r(abc) = 2.$$

*Nađimo nezavisne skupove matroida* $M$.

Rang nezavisnog skupa jednak je broju elemenata tog skupa (nezavisni skupovi jednini su skupovi s ovim svojstvom). Iz tog razloga nezavisni skupovi su svi oni skupovi $I$ takvi da je $r(I) = |I|$ (vidi sliku 33). U ovom primjeru svi nezavisni skupovi su: $\{\emptyset, a, b, c, ac, bc\}$.

# 7 Ravnine i hiperravnine

Ravnina u matroidu je podskup maksimalnog ranga: ako se ravnini doda bilo koji novi element, rang se poveća.

**Definicija 7.1.** *Neka je $E$ temeljni skup matroida $M$. Podskup $F \subseteq E$ je ravnina ako je $r(F \cup \{x\}) > r(F)$ za bilo koji $x \notin F$.*

Ravnine se još zovu zatvoreni skupovi.

**Primjer 7.2.** *Promotromo matroid iz primjera 4.5 i nabrojimo sve ravnine.*

- ravnine ranga 0: Postoji smo jedna ravnina ranga 0 i to je petlja $f$. Općenito vrijedi da uvijek postoji točno jedna ravnina ranga 0. Ako matroid $M$ nema petlje, onda je ravnina ranga 0 prazan skup $\emptyset$. Ako matroid $M$ ima jednu ili više petlji, onda je ravnina ranga 0 skup svih petlji.
- ravnine ranga 1: $abf, cf, df, ef$.
- ravnine ranga 2: Maksimalni skupovi ranga 2 su: $abef, cef, def, abcdf$. Ti skupovi su ravnine ranga 2.
- ravnine ranga 3: Temeljni skup $E$ matroida čini ravninu ranga 3: $abcdef$.

Važne stvari vezane uz ravnine su sljedeće.

(1) Petlja $f$ je u svakoj ravnini.

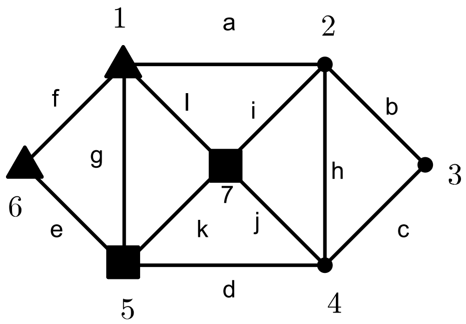
(2) Ako uklonimo kopetlju $e$ iz ravnine $F$ koja ju sadrži, nastaje nova ravnina. Također, ako dodamo kopetlju $e$ bilo kojoj ravnini nastaje nova ravnina. Preciznije, ako je $e$ kopetlja i $F$ ravnina, onda $e \notin F \Rightarrow F \cup \{e\}$ je ravnina, a $e \in F \Rightarrow F \setminus \{e\}$ je također ravnina.

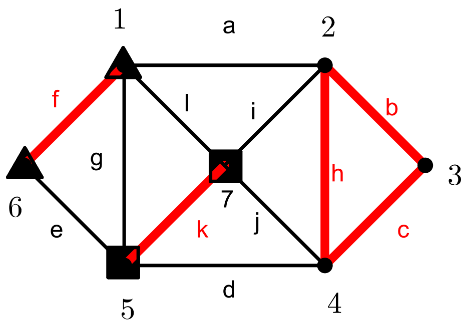
(3) Prazan skup $\emptyset$ je ravnina samo onda kada $M$ nema petlji.

(4) Skup $E$ je ravnina u bilo kojem matroidu. To je jedinstvena ravnina ranga $r(M)$.

Uočimo da je relativno lako odrediti ravnine iz slike matroida. U slučaju da nam je zadan samo graf grafovskog matroida, ravnine je nešto teže odrediti. Neka je $G = (V, E)$ graf iz kojeg se može dobiti grafovski matroid i neka je $F$ podskup skupa bridova $E$. Podskup bridova $F \subseteq E$ čini podgraf od $G$ i taj podgraf se može sastojati od nekoliko komponenti povezanosti. Neformalnim jezikom možemo reći da je $F$ ravnina u grafovskom matroidu ako se dodavanjem bridova podskupu $F$ smanjuje broj komponenti povezanosti. Točnije, ako je $\Pi$ particija vrhova grafa $G$, a $F_\Pi$ skup bridova grafa $G$ čiji su krajevi sadržani u istom bloku particije, onda je $F_\Pi$ ravnina matroida $M(G)$.

**Primjer 7.3.** *Promotrimo graf na slici 35. Particija vrhova* $\Pi = \{16, 234, 57\}$ *odgovara ravnini* $F_\Pi = \{b, c, f, h, k\}$. *Dodavanjem bilo kojeg brida koji nije u* $F_\Pi$ *u ravninu* $F_\Pi$, *povisit će rang (smanjit će se broj komponenti povezanosti).*




Slika 35: Gore: graf $G$ s particijom vrhova $\Pi = \{16, 234, 57\}$; dolje: ravnina $F_\Pi = \{b, c, f, h, k\}$.

Važno svojstvo koje zadavoljavaju ravnine je sljedeće.

**Propozicija 7.4.** *Ako su* $F_1$ *i* $F_2$ *ravnine u matroidu, onda je i* $F_1 \cap F_2$ *ravnina u matroidu.*

Gore smo naveli da su ravnine maksimalnog ranga, odnosno da dodavanje bilo kojeg elementa koji nije u toj ravnini dovodi do povećanja ranga za jedan. Izrecimo tu tvrdnju propozicijom.

**Propozicija 7.5.** *Neka je $F$ ravnina matroida $M$ i $x \notin F$. Tada je $r(F \cup \{x\}) = r(F) + 1$.*

*Dokaz.* Prema definiciji ravnine znamo da je $r(F \cup \{x\}) > r(F)$. Ako je $r(F \cup \{x\}) = k$, tada postoji nezavisan skup $I$ veličine $k$ koji je sadržan u $F \cup \{x\}$. Ako $x \notin I$, onda $I \subseteq F$ i $r(F) \geq k = r(F \cup \{x\})$, što je kontradikcija s činjenicom $r(F \cup \{x\}) > r(F)$. Iz tog razloga, $x \in I$. Prema $(I2)$ skup $I \setminus x$ je nezavisan skup sadržan u $F$ veličine $k - 1$. Dakle, $r(F) \geq k - 1 = r(F \cup \{x\}) - 1$, odnosno $r(F \cup \{x\}) \leq r(F) + 1$. Kako je $r(F) < r(F \cup \{x\}) \in \mathbb{Z}$ slijedi da je $r(F \cup \{x\}) = r(F) + 1$. $\square$

Ravnine smo definirali preko funkcije ranga. Sljedećim primjerom pokazat ćemo kako dobijemo funkciju ranga preko ravnina matroida.

**Primjer 7.6.** *Neka je $E = \{a, b, c\}$ temeljni skup matroida i $\mathcal{F} = \{\emptyset, ab, c, abc\}$ skup ravnina matroida. Nađimo rang nekog podskupa od skupa $E$.*

Da bi odredili rang podskupa $A \subseteq E$ trebamo sljediti ove korake:

(1) Nađemo najmanju ravninu koja sadrži $A$. Nazovemo tu ravninu s $F_A$.

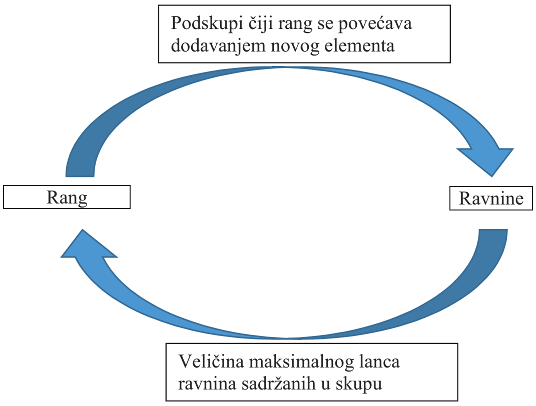
(2) Nađemo maksimalan lanac ravnina (vidi definiciju 7.13) $F_0 \subsetneq F_1 \subsetneq .... \subsetneq F_r = F_A$; $r(F_0) = 0$, $r(F_1) = 1$, itd...

(3) $r(A)$ je veličina maksimalnog lanca ravnina, tj. broj ravnina koje se javljaju u maksimalnom lancu umanjen za jedan.

Kako je $\emptyset$ ravnina, matroid nema petlji. Iz toga slijedi da je $r(a) = r(b) = r(c) = 1$. Sada jer $a$ i $b$ nisu ravnine, znamo da nema ravnina između $\emptyset$ i $ab$, pa je $r(ab) = 1$ ($ab$ je višestruka točka). Maksimalan lanac ravnina

$$\emptyset \subsetneq ab \subsetneq abc$$

nam govori da je $r(M) = 2$. Možemo provjeriti da je $r(ac) = r(bc) = 2$. Slika 36 nam daje vezu između ravnina i funkcije ranga.




Slika 36: Kriptomorfizam između ravnina i ranga.

Ravnine matroida, s relacijom inkluzije $\subseteq$, tvore strukturu zvanu geometrijska rešetka. Prije nego definiramo rešetku, definirat ćemo parcijalno uređen skup.

**Definicija 7.7.** *Binarna relacija $R$ na skupu $E$ je podskup od $E \times E$, gdje je $E \times E = \{(a,b)\,|a,b \in E\}$ skup svih uređenih parova elemenata iz $E$. Pišemo $(a,b) \in R$ i kažemo $a$ je u relaciji s $b$.*

Binarna relacija $R$ na skupu $E$ može imati sljedeća svojstva:

- Refleksivnost: za svaki $a \in E$, $(a,a) \in R$.
- Simetričnost: ako je $(a,b) \in R$, onda je $(b,a) \in R$, za sve $a,b \in E$.
- Antisimetričnost: ako je $(a,b) \in R$ i $(b,a) \in R$ , onda je $a = b$, za sve $a,b \in E$.
- Tranzitivnost: ako je $(a,b) \in R$ i $(b,c) \in R$, onda je $(a,c) \in R$, za sve $a,b,c \in E$ .

**Primjer 7.8.** *Neka je $E = \{a,b,c,d\}$ i $R = \{(a,a),(b,b),(c,c),(d,d),(a,b),(a,c),(a,d)\}$. Relacija $R$ zadovoljava svojstva refleksivnosti, antisimetričnosti i tranzitivnosti, no ne zadovoljava svojstvo simetričnosti.*

**Definicija 7.9.** *Binarna relacija $R$ na skupu $E$ je relacija ekvivalencije ako je $R$ refleksivna, simetrična i tranzitivna.*

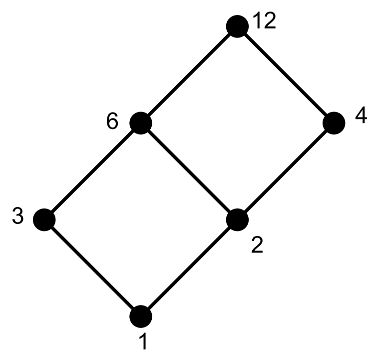
**Definicija 7.10.** *Parcijalni uređaj je binarna relacija koja je refleksivna, antisimetrična i tranzitivna. Parcijalno uređen skup $(E,\preceq)$ je skup na kojem je zadan parcijalni uređaj $\preceq$.*

Primijetimo da je relacija iz primjera 7.8 parcijalni uređaj. Slijedi primjer važne klase parcijalno uređenog skupa.

**Primjer 7.11.** *Neka je $D_n$ skup svih pozitivnih djelitelja broja $n$, gdje je $n$ pozitivan cijeli broj. Na primjer $D_{12} = \{1, 2, 3, 4, 6, 12\}$. Definiramo parcijalni uređaj na $D_n$ po djeljivosti, označimo ga s "$|$". Na primjer, 2 je u relaciji s 4 jer $2|4$, ali 4 nije u relaciji s 6 jer $4 \nmid 6$. $(D_n, |)$ je parcijalno uređen skup.*

**Definicija 7.12.** *Neka je $(E, \preceq)$ parcijalno uređen skup i $x, y \in E$, $x \neq y$. Kažemo da $y$ pokriva $x$ ako vrijedi $x \preceq y$ i ako za sve $z \in E$, takve da je $x \preceq z \preceq y$, vrijedi $z = x$ ili $z = y$. Ako $y$ pokriva $x$ još kažemo da je $x$ pokriven s $y$ i označavamo $x \lessdot y$.*

Slike koje opisuju parcijalni uređaj zovu se Hasseovi dijagrami i dobivaju se na sljedeći način. Svaki element od $E$ predstavlja se točkom na dijagramu. Ako je $x$ prekriven s $y$, onda se crta dužina s orjentacijom prema gore od $x$ do $y$. Koristeći tranzitivnost, možemo rekonstruirati cijeli parcijalni uređaj iz relacije pokrivenosti. Točnije, ako $x \preceq y$, tada u Hasseovom dijagramu postoji put prema gore iz $x$ prema $y$. Slika 37 pokazuje Hasseov dijagram za $D_{12}$.




Slika 37: Hasseov dijagram za parcijalno uređen skup $(D_{12}, |)$.

Element $x$ je maksimalan ako u Hasseovom dijagramu ne postoji element iznad, odnosno ako $x \preceq y$ povlači da je $x = y$. Element $x$ je minimalan ako u Hasseovom dijagramu ne postoji element ispod, odnosno ako $y \preceq x$ povlači da je $x = y$. Konačan parcijalno uređen skup mora imati najmanje jedan minimalni i maksimalni element. Ako skup $P$ ima točno jedan maksimalni element $x$, tada je $y \prec x$ za sve $y \neq x$. Takav element $x$ obično se označava s $\hat{1}$ i zove se najveći element parcijalno uređenog skupa. Ako skup $P$ ima točno jedan minimalni element $x$, tada je $x \succ y$ za sve $y \neq x$. Takav element $x$ obično se označava s $\hat{0}$ i zove se najmanji element parcijalno uređenog skupa.

**Definicija 7.13.** *Lanac u parcijalno uređenom skupu je skup $\{x_1, x_2, ..., x_k\}$ elementa iz $P$ takvih da vrijedi $x_1 \preceq x_2 \preceq ... \preceq x_k$. Lanac je maksimalan ako nije sadržan ni u jednom duljem lancu. Lanac $x_1 \preceq x_2 \preceq ... \preceq x_k$ je zasićen ako $x_{i+1}$ pokriva $x_i$ za sve $i = 1, 2, ..., k-1$. Dužina zasićenog lanca $x_1 \preceq x_2 \preceq ... \preceq x_k$ je $k$. Parcijalno uređen skup je graduiran ako za svaki par elemenata $x$ i $y$, svi zasićeni lanci koji počinju pri $x$ i završavaju pri $y$ imaju istu dužinu.*

Ako je parcijalno uređen skup graduiran, možemo definirati funkciju ranga $\rho$ na skupu elemenata parcijalno uređenog skupa. To će biti ključna veza između parcijalno uređenog skupa i matroida. Pomoću sljedećeg primjera lakše ćemo uočiti tu ideju.

**Primjer 7.14.** *Neka je $S = [n] = \{1, 2, ..., n\}$ i definiramo parcijalno uređen skup $B_n$ na podskupovima skupa $S$ tako da je $A \preceq B$ ako i samo ako $A \subseteq B$. $B_n$ se zove Booleova algebra ili Boleoova rešetka. Vrijede činjenice:*

- $\hat{0} = \emptyset$ *i* $\hat{1} = S$.
- *$B_n$ je graduiran s funkcijom ranga $\rho(A) = |A|$ (uočimo da je $\rho(\emptyset) = 0$).*
- *$B$ pokriva $A$ ako i samo ako $B = A \cup \{x\}$ za neki $x \notin A$.*
- *Broj maksimalnih lanaca u $B_n$ je $n!$.*
- *Ako je $|A| = k$, tada $A$ pokriva $k$ elemenata od $B_n$ i $A$ je pokriven s $n-k$ elemenata.*

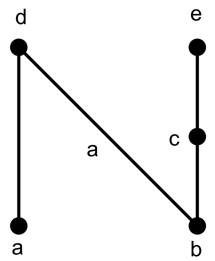
Jedna od posljedica tih činjenica o lancima u $B_n$ je sljedeća. Neka je $\{A_1, ..., A_m\}$ skup svih podskupova od $S$ s $k$ elemenata. Tada je broj maksimalnih lanaca koji prolaze kroz podskup $A_i$, $k!(n-k)!$ jer postoji $k!$ lanaca od $\emptyset$ do $A_i$ i $(n-k)!$ lanaca od $A_i$ do $S$. Kako svaki od $n!$ maksimalnih lanaca u parcijalno uređenom skupu prolazi kroz točno jedan skup $A_i$, imamo $mk!(n-k)! = n!$, odnosno:

$$m = \frac{n!}{k!(n-k)!}.$$

To daje dokaz da je broj $k$-članih podskupova od $S$ jednak binomnom koeficijentu $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

**Definicija 7.15.** *Neka je $(E, \preceq)$ parcijalno uređen skup i $x, y \in E$. Najmanja gornja granica ili supremum od $x$ i $y$, u oznaci $x \vee y$, je najmanji element iz skupa $\{z : x \preceq z; y \preceq z\}$ (ako postoji). Najveća donja granica ili infimum od $x$ i $y$, u oznaci $x \wedge y$, je najveći element iz skupa $\{w : w \preceq x; w \preceq y\}$ (ako postoji).*

**Primjer 7.16.** *(1) Neka je $P$ parcijalno uređen skup i slika 38 Hasseov dijagram tog skupa. Tada je $a \vee b = d$ i $d \wedge e = b$, a $a \vee c$ i $a \wedge c$ nije definirano. Taj parcijalno uređen skup nije graduiran (dva maksimalna lanca $a$ i $b \lessdot c \lessdot e$ imaju različitu dužinu).*




Slika 38: Parcijalno uređen skup $P$ iz primjera 7.16.

*(2) Za parcijalno uređen skup $B_n$ na svim podskupovima od $[n]$ iz primjera 7.14 vrijedi $A \vee B = A \cup B$ i $A \wedge B = A \cap B$.*

*(3) Za parcijalno uređen skup $D_n$ iz primjera 7.11 vrijedi da je $a \vee b$ najmanji zajednički višekratnik od $a$ i $b$, a $a \wedge b$ je najveći zajednički djelitelj od $a$ i $b$.*

Operacije $\vee$ i $\wedge$ su asocijativne pa možemo pisati $a \vee b \vee c$ ili $a \wedge b \wedge c$. Te operacije često nisu definirane na svim parovima elemenata. Nama će biti zanimljive one situacije kada su te operacije definirane na svim parovima.

Sada ćemo definirati rešetku i objasniti što znači da je rešetka geometrijska.

**Definicija 7.17.** *Ako je $L = (E, \preceq)$ konačan parcijalno uređen skup takav da svaki par elemenata ima supremum i infimum, onda je $L$ rešetka.*

**Propozicija 7.18.** *Konačna, neprazna rešetka $L$ ima najmanji element $\hat{0}$ i najveći element $\hat{1}$.*

Kako rešetke imaju najmanji i najveći element, možemo govoriti o onim elementima koji pokrivaju $\hat{0}$ i onim koji su pokriveni s $\hat{1}$.

**Definicija 7.19.** *Elemente rešetke $L$ koji pokrivaju $\hat{0}$ zovemo atomi rešetke $L$, a elemente koji su pokriveni s $\hat{1}$ zovemo koatomi rešetke $L$.*

U primjeru 7.11, atomi su prosti brojevi koji dijele $n$. Za rešetku $B_n$ iz primjera 7.14, atomi su podskupovi od $[n]$ veličine 1.

**Definicija 7.20.** *Rešetku $L$ u kojoj se svaki element može napisati kao supremum atoma zovemo atomska.*

U Booleovoj rešetki, svaki podskup $A$ je supremum svih jednočlanih skupova koje $A$ sadrži, pa je $B_n$ atomska. S druge strane rešetka $(D_{12}, |)$, nije atomska jer na primjer 4 nije supremum atoma. Kako bi uspostavili vezu između rešetke i matroida trebamo definirati funkciju ranga za rešetku.

**Definicija 7.21.** *(1) Neka je $(E, \preceq)$ graduiran parcijalno uređen skup s najmanjim elementom $\hat{0}$. Definiramo rang $\rho(x)$ elemeta $x$ kao dužinu zasićenog lanca iz $\hat{0}$ do $x$.*

*(2) Neka je $L$ rešetka s funkcijom ranga $\rho$. Tada je funkcija $\rho$ polumodularna ako za sve $x, y \in L$ vrijedi:*

$$\rho(v \vee y) + \rho(x \wedge y) \leq \rho(x) + \rho(y).$$

*(3) Neka je $L$ rešetka s funkcijom ranga $\rho$ Tada je $\rho$ modularna ako za sve $x, y \in L$ vrijedi:*

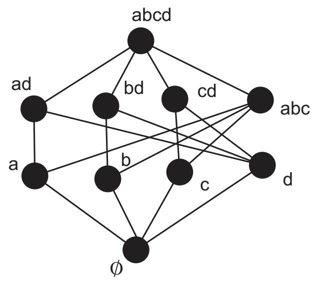
$$\rho(x \vee y) + \rho(x \wedge y) = \rho(x) + \rho(y).$$

Rešetka je polumodularna ili modularna ako je funkcija ranga $\rho$ polumodularna ili modularna. Modularne rešetke su polumodularne ali obrat nužno ne vrijedi. Booleove rešetke su modularne: $|A \cup B| + |A \cap B| = |A| + |B|$. Definirajmo sada geometrijsku rešetku.

**Definicija 7.22.** *Geometrijska rešetka je rešetka koja je polumodularna i atomska.*

**Primjer 7.23.** *Neke je $L = (\mathcal{F}, \subseteq)$ rešetka, gdje je*

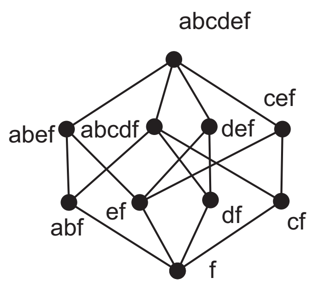
$$\mathcal{F} = \{\emptyset, a, b, c, d, ad, bd, cd, abc, abcd\}.$$




Slika 39: Hasseov dijagram za rešetku $L$ iz primjera 7.23.

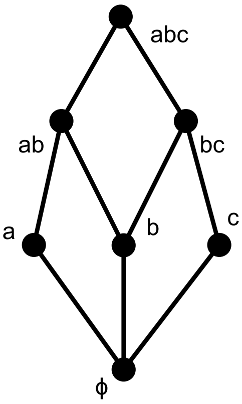
*Slika 39 prikazuje Hasseov dijagram za rešetku $L$. Da bi pokazali da je $L$ geometrijska rešetka, trebamo provjeriti da je svaki skup koji se pojavljuje u $\mathcal{F}$ supremum atoma i da je funkcija ranga polumodularna. Lako se provjeri da je svaki skup iz $\mathcal{F}$ supremum atoma. Primjerice, skup $abcd = (a \vee d) \vee (b \vee d)$. Također, možemo provijeriti da za sve $x, y \in L$ vrijedi: $\rho(x \vee y) + \rho(x \wedge y) \leq \rho(x) + \rho(y)$. Primjerice, za $x = a$ i $y = b$ vrijedi: $2 = \rho(a \vee b) + \rho(a \wedge b) \leq \rho(a) + \rho(b) = 2$. Dakle, funkcija ranga je i polumodularna pa je $L$ geometrijska rešetka.*

**Primjer 7.24.** *Prikažimo rešetku za matroid na slici 30.*




Slika 40: Rešetka ravnina $L$ matroida sa slike 30.

**Primjer 7.25.** *Promotrimo rešetku $L = (\mathcal{F}, \subseteq)$, gdje je $\mathcal{F} = \{\emptyset, a, b, c, ab, bc, abc\}$. Hasseov dijagram za L dan je na slici 41.*




Slika 41: Primjer rešetke koja nije geometrijska.

*Rešetka L nije geometrijska rešetka. Vrijedi* $a \vee c = abc$. *Za* $x = a$ *i* $y = c$ *pa ne vrijedi svojstvo polumodularnosti:*

$$3 = \rho(a \vee c) + \rho(a \wedge c) > \rho(a) + \rho(c) = 2.$$

**Teorem 7.26.** *Neka je* $M$ *matroid, a* $\mathcal{F}$ *familija svih ravnina u* $M$. *Tada je* $(\mathcal{F}, \subseteq)$ *geometrijska rešetka.*

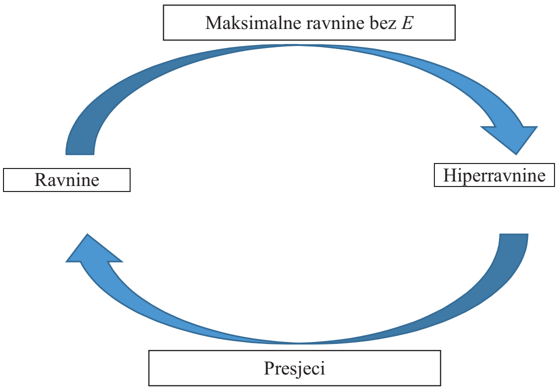
Skup $\mathcal{F}$ iz primjera 7.23 je skup ravnina matroida na skupu $E = \{a, b, c, d\}$.

Hiperravnine su posebne vrste ravnina. To su maksimalne ravnine koje nisu čitav matroid.

**Definicija 7.27.** *Neka je* $E$ *temeljni skup matroida* $M$. *Podskup* $H \subseteq E$ *je hiperravnina ako je* $H$ *ravnina od* $M$ *i* $r(H) = r(M) - 1$.

**Primjer 7.28.** *Hiperravnine je, također kao ravnine, relativno lako odrediti iz slike matroida. Matroid na slici 32 ima rang 3, pa su hiperravnine ravnine ranga 2: dužine (s uključenim petljama)* $abcdf, abef, cef$, *i* $def$.

Hiperravnine su ravnine ranga $r(M) - 1$. Različite hiperravnine mogu biti različite veličine. Iz tog razloga svojsto koje vrijedi za baze, da su maksimalni skupovi jednaki najvećim skupovima, ne vrijedi za hiperravnine. Očito je da možemo odrediti sve hiperravnine matroida iz skupa svih njegovih ravnina. Hiperravnine su one ravnine $H$ takve da ni jedna ravnina $H'$ ne zadovoljava $H \subset H' \subset E$. Drugim riječima to su maksimalne ravnine iz skupa $\mathcal{F} \setminus E$. Također, ako nam je zadan temeljni skup $E$ matroida i skup svih hiperravnina matroida, možemo odrediti ravnine tog matroida. Svaka ravnina je presjek nekih skupova hiperravnina matroida (vidi propoziciju 8.11). Dakle, ako pogledamo sve moguće presjeke skupova hiperravnina, možemo dobiti sve ravnine matroida (vidi sliku 42).




Slika 42: Kriptomorfizam između ravnina i hiperravnina.

**Primjer 7.29.** *Provjerimo da ravnine iz primjera 7.28 možemo dobiti kao presjek hiperravnina. Presjek hiperravnine sa samom sobom daje tu hiperravninu pa na taj način dobivamo sve hiperravnine. Presjek svih hiperravnina je ravnina $f$, a $E$ je "prazan presjek". Sada preostaje još naći ravnine ranga 1. Dobivamo ih kao presjeke sljedećih hiperravnina:*

$$abf = abcdf \cap abef$$

$$cf = abcdf \cap cef$$
$$df = abcdf \cap def$$
$$ef = cef \cap def.$$

*Uočavamo da ti presjeci odgovaraju presjecima dviju dužina na slici 32.*

Definiranje matroida pomoću hiperravnina je još jedan kiriptomorfizam.

# 8 Zatvarač

Neka je $A \subseteq E$. Zatvarač skupa $A$, u oznaci $\overline{A}$ je također podskup od $E$. Funkcija $A \mapsto \overline{A}$ je funkcija iz skupa $2^E$ u samog sebe. Zatvarač $\overline{A}$ se može definirati kao presjek svih zatvorenih skupova koji su sadržani u $A$ ili kao najmanji zatvoreni skup koji sadrži $A$. Za matroide, zatvarač skupa $A \subseteq E$ je jedinstvena najmanja ravnina koja sadrži $A$. Također se označava s $\overline{A}$. Sljedeća lema nam govori o postojanju takve ravnine.

**Lema 8.1.** *Neka je $M$ matroid s temeljnim skupom $E$ i skupom ravnina $\mathcal{F}$. Neka je $A \subseteq E$. Tada:*

*(1) Postoji jedninstvena ravnina $F \in \mathcal{F}$ takva da je*

*a) $A \subseteq F$, i*

*b) Ako je $A \subseteq F'$ za neku ravinu $F'$, onda je $F \subseteq F'$.*

*(2) Ravnina $F$ iz dijela* (1) *zadovoljava: $F = \bigcap \{F' \in \mathcal{F} | A \subseteq F'\}$.*

Definirajmo sada zatvarač matroida.

**Definicija 8.2.** *Neka je $M$ matroid sa skupom ravnina $\mathcal{F}$ i neka je $A \subseteq E$. Tada je zatvarač od skupa $A$, u oznaci $\overline{A}$, definiran kao:*

$$\overline{A} = \bigcap \{F \in \mathcal{F} | A \subseteq F\} .$$

**Primjer 8.3.** *Promotrimo primjer 4.5. Provjerimo da je $\overline{ad} = abcdf$, koristeći definiciju zatvarača. Jedine ravnine $F$ koje sadrže $ad$ su ravnine $abcdf$ i $E$ pa je $\overline{ad} = abcdf$. Odredimo čemu je jednak $\overline{a}$. Ravnine koje sadrže $a$ su dužine $abef$ i $abcdf$ (i $E$), pa je $\overline{a} = abef$.*

Iz definicije zatvarača jasno je da su ravnine u matroidu skupovi $F$ takvi da je $\overline{F} = F$. Veza između zatvarača i ravnina je prikazana na slici 43.


Slika 43: Kriptomorfizam između ravnina i zatvarača.

Ako je $A \subseteq E$, onda je $A \subseteq \overline{A}$ i $\overline{\overline{A}} = \overline{A}$. Ta dva svojstva zatvarača su važna u definiranju matroida preko zatvarača. Definirajmo sada matroid preko operatora zatvarača.

**Teorem 8.4.** *Neka je $E$ konačan skup s operatorom zatvarača $A \mapsto \overline{A}$ koji je definiran na podskupovima od $E$. Tada je operator zatvarača dobiven od matroida ako i samo ako za sve $A, B \subseteq E$ vrijedi:*

$(Z1)$ $A \subseteq \overline{A}$.

$(Z2)$ *Ako je $A \subseteq B$, onda je $\overline{A} \subseteq \overline{B}$.*

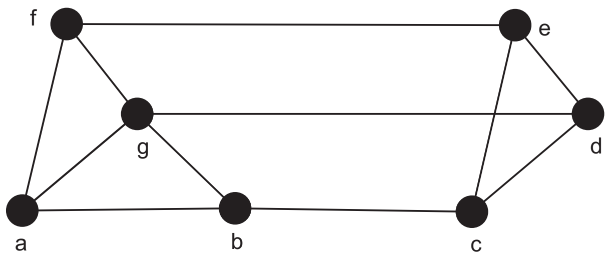
$(Z3)$ $\overline{\overline{A}} = \overline{A}$.

$(Z4)$ *Ako je $x \in \overline{A \cup \{y\}} \setminus \overline{A}$, onda je $y \in \overline{A \cup \{x\}}$.*

Svojstvo $(Z4)$ zove se Maclane-Steinitzov aksiom razmjene. To svojstvo razlikuje klasu matroida od općenitih matematičkih struktura.

**Primjer 8.5.** *Provjerimo vrijedi li svojstvo $(Z4)$. Pogledajmo ponovo matroid na slici 32. Izaberemo $A = ab$, $x = c$ i $y = d$. Vrijedi $\overline{A} = abf$, $\overline{A \cup \{c\}} = abcdf$ i $\overline{A \cup \{d\}} = abcdf$, pa je $c \in \overline{A \cup \{d\}} \setminus \overline{A}$. Aksiom razmjene $(Z4)$ zahtijeva da je $d \in \overline{A \cup \{c\}}$, što je istinito.*

**Primjer 8.6.** *Promotrimo matroid ranga 4 na slici 44.*




Slika 44: Matroid ranga 4.

*Odaberemo* $A = bc$, *y neka bude bilo koja točka* $y \notin \overline{A}$, *recimo* $y = f$. *Znamo da je* $\overline{A} = abc$ *i* $\overline{A \cup \{f\}} = abcef$, *pa je e jedina točka (osim f) u* $\overline{A \cup \{f\}} \setminus \overline{A}$. *Aksiom (Z4) je zadovoljen jer je* $f \in \overline{A \cup \{e\}} = \overline{A \cup \{f\}} = abcef$.

Napravimo sada skicu dokaza teorema 8.4. Taj dokaz uspostavlja kriptomorfizam između funkcije ranga i operatora zatvarača (vidi sliku 45).

(1) Pretpostavimo da imamo matroid definiran preko funkcije ranga. Definiramo zatvarač $\overline{A}$ skupa $A$ kao skup elemenata koje možemo dodati skupu $A$ bez da se povisi njegov rang:

$$\overline{A} = \{x \in E \,|r(A \cup \{x\}) = r(A)\}\,.$$

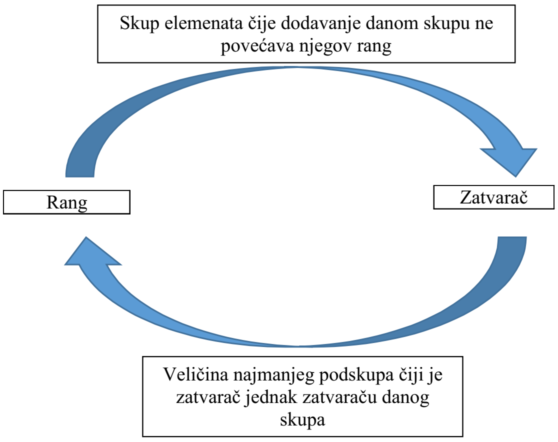
(2) Dokažemo da ako funkcija $r$ zadovoljava svojstva $(R1)$, $(R2)$ i $(R3)$, onda operator zatvarača zadovoljava svojstva $(Z1)$, $(Z2)$, $(Z3)$ i $(Z4)$.

(3) Sada pretpostavimo da imamo matroid definiran preko operatora zatvarača. Definiramo $r(A)$ kao veličinu najmanjeg podskupa $I$ od skupa $A$ za koji vrijedi $\overline{I} = \overline{A}$:

$$r(A) = min\left\{|I||\overline{I} = \overline{A}, I \subseteq A\right\}.$$

(4) Dokažemo da ako operator zatvarača zadovoljava svojstva $(Z1)$, $(Z2)$, $(Z3)$ i $(Z4)$, onda funkcija $r$ zadovoljava svojstva $(R1)$, $(R2)$ i $(R3)$.

(5) Dokažemo da su pridruživanja iz koraka (1) i (3) jedna drugom inverzna.




Slika 45: Kriptomorfizam između ranga i zatvarača.

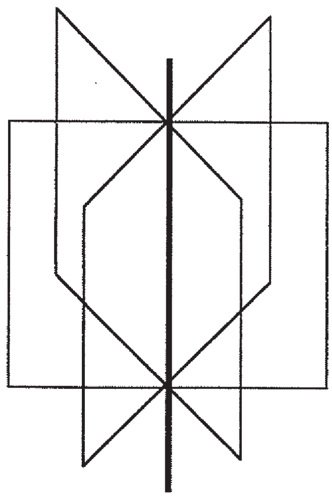
Uspostavimo sada kriptomorfizam između operatora zatvarača i ravnina.

**Teorem 8.7.** *Neka je $E$ konačan skup i $\mathcal{F}$ familija podskupova od $E$. Tada familija $\mathcal{F}$ čini ravnine matroida ako i samo ako:*

$(F1)$ $E \in \mathcal{F}$.

$(F2)$ *Ako su $F_1, F_2 \in \mathcal{F}$, onda je $F_1 \cap F_2 \in \mathcal{F}$.*

$(F3)$ *Ako je $F \in \mathcal{F}$ i $\{F_1, F_2, ..., F_k\}$ skup svih ravnina koje pokrivju $F$, tada je $\{F_1 \setminus F, F_2 \setminus F, ..., F_k \setminus F\}$ particija skupa $E \setminus F$.*



Slika 46: Geometrijska motivacija za aksiom ($F3$).

Geometrijska motivacija za aksiom ($F3$) dolazi iz sljedeće ideje. Neka je dan pravac u $\mathbb{R}^3$. Ravnine koje sadrže taj pravac particioniraju ostatak od $\mathbb{R}^3$. Slika 46 prikazuje tu interpretaciju aksioma ($F3$) u $\mathbb{R}^3$ (na slici su prikazane samo tri od beskonačnog broja ravnina koje sadrže zadani pravac). Pogledajmo svojstvo ($F3$) na nekoliko primjera.

**Primjer 8.8.** *Promotrimo matroid ranga 4 na slici 44. Ravnine matroida uključuju točke, dužine i ravnine koje se nalaze na toj slici. Kako bi pokazali da* ($F3$) *vrijedi uzet ćemo* $F = ae$ *i promotrit ćemo one ravnine koje pokrivaju* $F$ *u geometrijskoj rešetki.* $F$ *je dužina pa su ravnine koje pokrivaju skup* $F$ *sve ravnine koje ga sadrže. Postoje tri takve ravnine:* $F_1 = ade$, $F_2 = abcef$ *i* $F_3 = aeg$ *(ravnine* $ade$ *i* $aeg$ *nisu nacrtane na slici, ali one su ravnine ranga 3). Možemo uočiti da je skup* $\{F_1 \setminus F, F_2 \setminus F, F_3 \setminus F\}$ *particija od* $E \setminus F$. *Geometrijski, to znači da se svaka točka* $p$ *koja nije na dužini* $F$ *nalazi na jedinstvenoj ravnini koja sadrži točku* $p$ *i dužinu* $F$. *Vidi tablicu 3 za tu particiju.*

| Točka | $b$ | $c$ | $d$ | $f$ | $g$ |
|---|---|---|---|---|---|
| Ravnina | $abcef$ | $abcef$ | $ade$ | $abcdf$ | $aeg$ |

Tablica 3: Točke koje nisu na dužini $ae$ i jedinstvene ravnine koje ih sadrže.

**Primjer 8.9.** *Promotrimo rešetku* $L = (\mathcal{F}, \subseteq)$ *na slici 40. To nije geome-*

*trijska rešetka, pa elementi rešetke nisu ravnine matroida. Možemo uočiti da je ovdje narušen aksiom* $(F3)$*. Ako je* $F = a$*, onda je* $F_1 = ab$ *jedni element rešetke koji pokriva* $F$*. Stoga* $\{F_1 \setminus F\}$ *nije particija od* $E \setminus F$*.*

Skica dokaza teorema 8.7 je sljedeća (vidi sliku 43).

(1) Pretpostavimo da imamo matroid definiran preko operatora zatvarača. Definiramo familiju ravnina:

$$\mathcal{F} = \left\{ F \subseteq E \,\middle|\, F = \overline{F} \right\}.$$

(2) Dokažemo da ako operator zatvarača zadovoljava svojstva $(Z1)$, $(Z2)$, $(Z3)$ i $(Z4)$, onda familija $\mathcal{F}$ zadovoljava svojstva $(F1)$, $(F2)$ i $(F3)$.

(3) Sada pretpostavimo da imamo matroid definiran preko familije $\mathcal{F}$. Za neki $A \subseteq E$ definiramo operator zatvarača:

$$\overline{A} = \bigcap \{F \in \mathcal{F} | A \subseteq F\}.$$

(4) Dokažemo da ako familija $F$ zadovoljava svojstva $(F1)$, $(F2)$ i $(F3)$, onda operator zatvarača zadovoljava svojstva $(Z1)$, $(Z2)$, $(Z3)$ i $(Z4)$.

(5) Dokažemo da su pridruživanja (1) i (3) međusobno inverzna.

Vratimo se na hiperravnine. Hiperravnine su maksimalne prave ravnine (ravnina je prava ako nije temeljni skup $E$). Zbog toga, $H$ je hiperravnina ako i samo ako $E$ pokriva $H$ u rešetki ravnina matroida $M$. Matroid možemo opisati pomoću nezavisnih skupava ili pomoću maksimalnih nezavisnih skupava, odnosno baza. Teorem 4.4 pokazuje da su ove dvije familije skupova ekvivalentne u definiranju matroida. Analogno, definicija matroida pomoću ravnina ekvivalentna je definiciji matroida pomoću maksimalnih pravih ravnina, tj. hiperravnina. Veza između nezavisnih skupova i baza analogna je vezi između ravnina i hiperravnina. Sljedeća propozicija govori nam o povezanosti hiperravnina s drugim pojmovima vezanim za matroid.

**Propozicija 8.10.** *Neka je* $M$ *matroid i* $E$ *temeljni skup tog matroida. Za podskup* $H \subseteq E$ *sljedeće tvrdnje su ekvivalntne:*

*(1)* $H$ *je hiperravnina.*

*(2)* $H$ *je maksimalna prava ravnina.*

*(3)* $r(H) = r(E) - 1$ *i* $r(H \cup \{x\}) = r(E)$ *za sve* $x \notin H$*.*

*(4) $H$ je maksimalna s poštivanjem da ne sadrži bazu.*

*(5) $\overline{H} = H$ i $\overline{H \cup x} = E$ za sve $x \notin H$.*

*(6) $H$ je pokrivena s $E$ u rešetki ravnina.*

*(7) $H$ ima jedinstveni pokrivač u rešetki ravnina.*

Ranije smo spomenuli da je rešetka ravnina atomska, tj. da je svaka ravnina supremum atoma. Obrnuta izjava također vrijedi.

**Propozicija 8.11.** *Neka je $M$ matroid i $E$ temeljni skup matroida. Tada je rešetka ravnina koatomska, tj. svaka ravnina je presjek nekog skupa hiperravnina.*

*Dokaz.* U dokazu nam je bitno svojstvo $(F3)$, odnosno činjenica da ravnine koje pokrivaju danu ravninu čine particiju komplementa te ravnine. Također, koristit ćemo indukciju po korangu ravnine, tj. $r(M) - r(F)$. Neka je $F$ ravnina. Ako je $r(M) - r(F) = 0$, onda je $F = E$, pa smo gotovi s dokazom jer je $E$ presjek hiperravnina (prazan presjek). Propozicija je istinita i za sve ravnine koranga 1 jer su to hiperravnine. Pretpostavimo sada da je propozicija istinita za sve ravnine koranga $k$ za neki $k \geq 1$. Moramo pokazati da je tada svaka ravnina koranga $k+1$ također presjek hiperravnina. Neka je $F$ ravnina takva da vrijedi $r(F) = r(M) - (k+1)$. Neka je $H_1, H_2, ..., H_p$ skup hiperravnina koje sadrže $F$, tj. $F \subseteq H_i$ za hiperravnine $H_i$, gdje je $1 \leq i \leq p$. Tada je očito $F \subseteq \bigcap_{i=1}^{p} \{H_i\}$. Trebamo pokazati da $F \supseteq \bigcap_{i=1}^{p} \{H_i\}$ kako bi dobili $F$ kao presjek hiperravnina i dovršili dokaz. Pretpostavimo da to ne vrijedi. Tada postoji neki $x \notin F$ takav da je $x \in H_i$ za sve $i$, $1 \leq i \leq p$. Znamo da $F$ nije hiperravnina pa prema propoziciji 8.10 (7), $F$ je pokrivena s minimalno dvije različite ravnine $F_1$ i $F_2$. Tada:

- Kako je $x \in E \setminus F$, prema $(F3)$, postoji jedinstveni pokrivač od $F$ koji sadrži $x$. Zbog toga $x$ nije istodobno u $F_1$ i u $F_2$. Pretpostavimo $x \notin F_1$.

- Kako je $F \subseteq F_1$, svaka hiperravnina koja sadrži $F_1$, također sadrži $F$. Pretpostavimo da je $F_1$ sadržana u hiperravninama $H_1, H_2, ..., H_s$ za neki $s < p$.

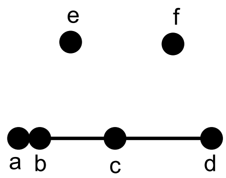
- $F_1$ ima korang $k$ pa prema koraku indukcije, $F_1$ je presjek hiperravnina, tj. $F_1 = \bigcap_{i=1}^{s} \{H_i\}$. Zbog toga $x \notin H_j$ za neki $j$, $1 \leq j \leq s$.

- $x \in H_i$ za sve $1 \leq i \leq p$.

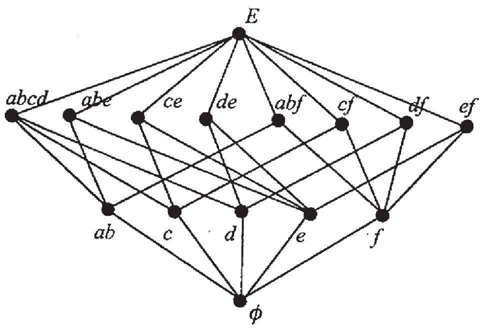
$\square$

Posljedica prethodne propozicije je sljedeća. Točka $x$ je u svakoj hiperravnini ako i samo ako je $x$ petlja, tj. $x \in \overline{\emptyset}$. Kako su geometrijske rešetke koatomske, možemo probati "obrnuti" geometrijsku rešetku. Rešetku koju ćemo dobiti bit će atomska (orginalna je bila koatomska). Pogledajmo o čemu je točno riječ na sljedećem primjeru i provjerimo također svojstvo polumodularnosti.

**Primjer 8.12.** *Neka je $M$ matroid na slici 47.*




Slika 47: Matroid $M$ iz primjera 8.12.




Slika 48: Rešetka ravnina matroida $M$.

*Slika 48 prikazuje rešetku ravnina matroida $M$. Neka su sada $H_1 = ef$ i $H_2 = abcd$ dvije hiperravnine matroida $M$. Tada u obrnutoj rešetki, funkcija ranga $r'$ zadovoljava $r'(H_1) = r'(H_2) = 1$, a $r'(H_1 \cap H_2) = r'(\emptyset) = 3$ (funkcija ranga $r'$ je funkcija koranga u početnom matroidu $M$). Iz tog razloga obrnuta rešetka nije rešetka ravnina matroida, tj. nije geometrijska.*

**Teorem 8.13.** *Neka je $E$ konačan skup i neka je $\mathcal{H}$ familija podskupova od $E$. Tada je familija $\mathcal{H}$ skup hiperravnina matroida ako i samo ako:*

$(H1)$ $E \notin \mathcal{H}$.

$(H2)$ *Ako su* $H_1, H_2 \in \mathcal{H}$ *i* $H_1 \subseteq H_2$*, onda je* $H_1 = H_2$.

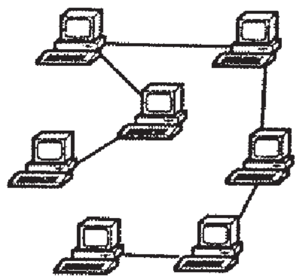
$(H3)$ *Za sve različite* $H_1, H_2 \in \mathcal{H}$ *i za sve* $x \in E$*, postoji* $H \in \mathcal{H}$ *takva da je* $(H_1 \cap H_2) \cup \{x\} \subseteq H$.

Dokaz prethodnog teorema sličan je dokazu teorema 5.2. Provjerimo svojstvo $(H3)$ na matroidu iz primjera 8.12.

**Primjer 8.14.** *Promotrimo hiperravnine* $H_1 = abcd$*,* $H_2 = abe$ *i* $x = f$ *matroida na slici 47. Svojstvo* $(H3)$ *zahtijeva postojanje hiperravnine* $H$ *koja sadrži* $abf$*. Za matroid sa slike 47* $H = abf$ *je hiperravnina pa je svojstvo* $(H3)$ *zadovoljeno (i tražena hiperravnina je jedinstvena). Nađimo još jedan primjer. Promotrimo hiperravnine* $H_1 = ce$*,* $H_2 = df$ *i* $x = a$*. Tada imamo* $H_1 \cap H_2 = \emptyset$*, pa trebamo samo naći ravninu koja sadrži točku* $a$*. Ovaj put imamo mnogo izbora, tj. postoji puno hiperravnina koje zadovoljavaju* $(H3)$*:* $abcd$*,* $abe$ *i* $abf$*.*

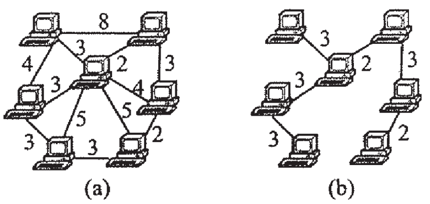
# 9 Program za optimizaciju: greedy algoritam

Postoje brojni slučajevi u kojima želimo povezati skup objekata (računala, kuće, gradove) na optimalan način. Na primjer, pretpostavimo da želimo povezati grupu računala vodovima. Zamislimo da su računala vrhovi, a vodovi između njih bridovi. Mi tražimo optimalno povezani graf. Ako dodamo uvjet da želimo koristiti najmanji broj vodova kako bismo povezali računala, onda sigurno nećemo imati ni jedan ciklus. Zbog toga mi zapravo tražimo razapinjuće stablo grafa (vidi sliku 49).



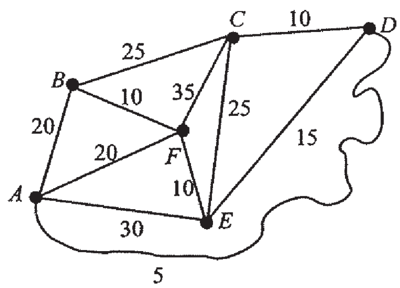
Slika 49: Povezivanje računala.

Također, možemo tražiti da računala budu povezana na način za koji je ukupna duljina vodova minimalna. To zahtijeva da znamo kolika je udaljenost između računala. Tu udaljenost u grafu bilježimo na način da dodamo oznaku svakom bridu i tu oznaku zovemo težina brida. Takav graf zovemo težinski graf. Dakle, optimalno povezan graf je razapinjuće stablo s minimalnom ukupnom težinom (vidi sliku 50).




Slika 50: (a) Mreža računala s težinama bridova; (b) Minimalno težinsko razapinjuće stablo mreže računala.

**Primjer 9.1.** *Planeri grada Skoroutopije žele napraviti biciklističke putove duž svih cesta unutar grada. Nažalost, za razliku od susjednog grada Utopije, oni nemaju dovoljno novca da bi napravili biciklističke staze duž svih cesta. Članovi gradske skupštine moraju odlučiti gdje napraviti biciklističke staze. Oni su odlučili da žele da biciklisti budu u mogućnosti proputovati sva važna raskrižja grada (označena slovima $A, B, C, D, E, F$ na slici 51). Dodatno, oni žele dodati biciklističke staze najprometnijim cestama.*




Slika 51: Plan grada Skoroutopije s podacima o prometu biciklima.

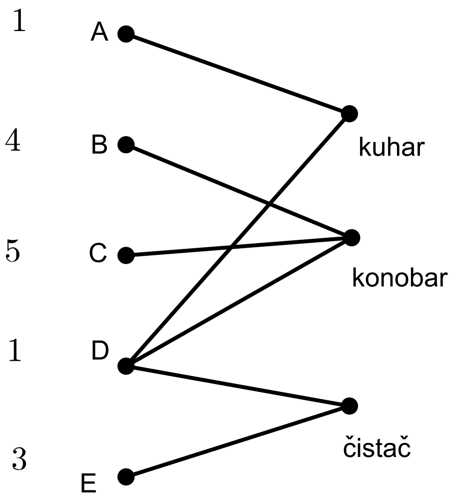
*Nakon pomnog promatranja dobiveni su podaci o dnevnom prometu biciklima po cesti. Na slici 51, težina bridova pretstavlja prosječni broj biciklista po satu koji su proputovali danom cestom. Pomozimo planerima grada tako da nađemo maksimalno težinsko razapinjuće stablo Skoroutopije.*

Prethodni primjer je poseban slučaj općenitijeg problema optimizacije matroida. U problemu s računalima, tražili smo da težina bude minimalna, a u prethodnom primjeru tražili smo da težina bude maksimalna. Sada ćemo riješiti problem maksimiziranja pomoću greedy algoritma. Pomoću tog algoritma možemo riješiti i problem minimiziranja. Problem iz primjera 9.1 često zovemo problem minimalnog razapinjućeg stabla (MRS). Problem MRS ima dugu i bogatu prošlost. Problem je prvi put zabilježen 1926., kada ga je Otakar Boruvka spomenuo u kontekstu konstruiranja optimalne energetske mreže u Južnoj Moraviji. Inačica s matroidima je sljedeća. Neka je $M = (E, \mathcal{I})$ matroid s težinskom funkcijom $\omega : E \to \mathbb{R}$. Definiramo težinu podskupa: $\omega(A) = \sum_{x \in A} \omega(x)$. Tada prethodni problem mreže motivira sljedeći općenitiji problem optimiziranja matroida. Neka je dan matroid $M = (E, \mathcal{I})$ s težinskom funkcijom $\omega : E \to \mathbb{R}$. Nađimo bazu $B \in \mathcal{B}$ maksimalne težine. Taj problem može se rješiti prilično lako. Navesti ćemo algoritam, takozvani greedy algoritam, koji rješava problem optimiziranja matroida. Greedy algoritam glasi:

| |
|---|
| Ulaz: Konačan skup $E$, težinska funkcija $\omega : E \to \mathbb{R}$ i familija $\mathcal{I}$ podskupova od $E$.<br>Poredaj elemente od $E$: $e_1, e_2, ..., e_n$ tako da $\omega(e_i) \geq \omega(e_j)$ za $i \leq j$.<br>Skup $B := \emptyset$.<br>Za $i = 1$ do $n$,<br>Ako je $B \cup \{e_i\} \in \mathcal{I}$, onda dodaj $B := B \cup \{e_i\}$.<br>Izlaz: $B$, maksimalni član od $\mathcal{I}$ najveće moguće težine. |

Neformalno o greedy algoritmu možemo razmišljati kao ponavljanje pravila: "izaberi element najveće težine koji ne stvara cikluse s elementima koje si već izabrao". Da greedy algoritam rješava problem optimizacije znači da baza $B_G$ koja je nastala algoritmom, zadovoljava $\omega(B_G) \geq \omega(B)$ za sve baze $B$. Možemo reći da greedy algoritam karakterizira matroide. To ćemo vidjeti iz teorema koji ćemo malo kasnije navesti.

**Primjer 9.2.** *Prije zapošljavanja osoblja novog restorana, Marko je odlučio razgovarati s kandidatima. Marko treba ocijeniti kandidate na skali od 1 do 5 (5 je najveća ocjena). On je zainteresiran za zapošljavanje tri najbolje ocijenjenih osoba na pozicijama kuhara, konobara i čistača. Kvalifikacije i ocjene za pet kandidata Ane, Borisa, Cecilije, Darije i Edina, dane su na slici 52.*




Slika 52: Bipartitni graf.

Troje najbolje ocijenjenih zaposlenika su Boris, Cecilija i Edin. Nažalost, zaposlenje ovih troje ljudi popunit će samo dvije pozicije od tri. Izrečeno u duhu matroida, skup $\{a, c, e\}$ nije nezavisan skup u transverzalnom matroidu. Iz tog razloga problem je jednak problemu s traženjem biciklističkih putova gdje smo tražili bazu maksimalne težine transverzalnog matroida. Marko može zaposliti najbolje ocijenjene kandidate na tri pozicije koristeći greedy algoritam:

- Prvo zaposli Ceciliju jer ona ima najveću ocjenu. Kako se ona prijavila samo za posao konobara, Marko je mora zaposliti na to mjesto.
- To znači da sljedeći najbolje ocijenjen kandidat, Boris, ne može biti zaposlen ($\{b, c\}$ je ciklus u matroidu). Sljedeći najbolje ocijenjen kandidat je Edin i njega Marko može zaposliti na mjesto čistača.
- Naposljetku, preostale su Ana i Darija, koje su ocijenjene istom ocjenom. Marko može slučajnim odabirom izabrati bilo koju od njih dvije na mjesto kuhara.

Sada možemo izreći teorem koji povezuje greedy algoritam i nezavisne skupove matroida.

**Teorem 9.3.** *Neka je dan par $(E, \mathcal{I})$ i neka $\mathcal{I}$ zadovoljva svojstva $(I1)$ i $(I2)$. Za sve težinske funkcije $\omega : E \to \mathbb{R}$ greedy algoritam daje maksimalni član od $\mathcal{I}$ najveće moguće težine ako i samo ako familija $\mathcal{I}$ zadovoljava i svojstvo $(I3)$, tj. $\mathcal{I}$ je familija nezavisnih skupova matroida.*

**Primjer 9.4.** *Neka je $E = \{a, b, c, d\}$ i $\mathcal{I} = \{\emptyset, a, b, c, d, ab, ac, ad, acd\}$ familija koja zadovoljava svojstva $(I1)$ i $(I2)$ s težinskom funkcijom: $\omega(a) = 2, \omega(b) = 1, \omega(c) = \omega(d) = \frac{3}{4}$. Provjerimo da u ovom slučaju greedy algoritam ne radi. Izlaz greedy algoritma je maksimalan skup ab težine 3. Možemo provjeriti da maksimalni skup acd ima težinu $3\frac{1}{2}$ i greedy algoritam nije dao maksimalni skup najveće moguće težine. Kako greedy algoritam ne radi, po teoremu 9.3, familija $\mathcal{I}$ nije nezavisan skup matroida. To možemo vidjeti i provjeravajući svojstvo $(I3)$ na skupovima acd i ab. Vidimo da svojstvo $(I3)$ na tim skupovima ne vrijedi.*

Greedy algoritam je brz i jednostavan za primjenu. Nažalost, ne vrijedi na mnogim problemima optimizacije. Navesti ćemo jedan takav primjer.

**Primjer 9.5.** *Problem trgovačkog putnika: dana je mreža težinskih bridova. Možemo li naći ciklus koji sadrži sve vrhove mreže ukupne minimalne težine? Ciklus koji sadrži sve vrhove grafa zove se Hamiltonov ciklus. Trgovački putnik koji mora posjetiti određen broj gradova (i mora se vratiti kući) putuje Hamiltonovim ciklusom mreže koja je određena tim gradovima.*

Taj primjer sličan je problemu MRS. Samo, umjesto da trebamo naći razapinjuće stablo, ovdje trebamo naći Hamiltonov ciklus. Nažalost nije poznat ni jedan učinkovit algoritam za riješiti taj problem.

# Literatura


[1] G. Birkhoff, *Abstract linear dependence in latices*, Amer. J. Math. 57 (1935), 800–804.

[2] G. Gordon, J. McNulty, *Matroids: a geometric introduction*, Cambridge University Press, New York, 2012.

[3] S. MacLane, *Some interpretations of abstract linear dependence in term of projective geometry*, Amer. J. Math. 58 (1936), 236–240.

[4] M. Primc, *Linearna algebra*, skripta, PMF-Matematički odjel, Zagreb, 2010. Dostupno na:
`http://web.math.pmf.unizg.hr/nastava/laf/data/knjiga11.pdf` (srpanj, 2015.).

[5] R. Rado, *A theorem on independence relatic*, Quart. J. Math. 13 (1942), 83–89.

[6] W. Tutte, *A homotopy theorem for matroids relatic*, Trans. Amer. J. Math. Soc. 88 (1958), 144–174.

[7] D. Veljan *Kombinatorika s teorijom grafova*, Školska knjiga, Zagreb, 1989.

[8] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb, 2001.

[9] H. Whitney, *On the abstract properties of linear dependence*, Amer. J. Math. 57 (1935), 509–533.

# Sažetak

U ovom diplomskom radu proučavamo razne definicije pojma matroida. Za definicije koje su međusobno ekvivalentne, ali ta ekvivalencija nije očita, kažemo da su kriptomorfne. Za matroid $M$ definiramo sedam ključnih pojmova: nezavisni skupovi, baze, ciklusi, funkcija ranga, ravnine, hiperravnine i operator zatvarača. Najprije definiramo matroid preko nezavisnih skupova i upoznajemo matroide nastale iz matrica i iz grafova. Zatim uspostavljamo kriptomorfizam između nezavisnih skupova i baza i na taj način pokazujemo da matroid možemo definirati i preko baza. Navodimo i kriptomorfizme između nezavisnih skupova i ciklusa, između nezavisnih skupova i funkcije ranga, funkcije ranga i operatora zatvarača, ravnina i operatora zatvarača, ravnina i hiperravnina. Uspostavljanjem kriptomorfizma između tih pojmova pokazujemo da se svaki od tih pojmova može koristiti kao polazište u definiranju matroida. U posljednjem poglavlju, nezavisne skupove matroida definiramo preko greedy algoritma. Ta veza daje nam dodatan uvid u važnost i posebnost matroida.

# Summary

This thesis is a study of various definitions of matroids. Definitions that are equivalent, but the equivalence is not obvious, are called cryptomorphic. For the matroid $M$ the following seven key concepts are defined: independent sets, bases, cycles, rank function, planes, hyperplanes and closure operator. First we define matroids in terms of independent sets and elaborate matroids coming from matrices and graphs. Then, we explain cryptomorphism between independent sets and bases, thus showing that a matroid can be defined in terms of bases. Next, cryptomorphisms between independent sets and cycles, between independent sets and rank function, rank function and closure operator, planes and closure operator, planes and hyperplanes are established. By establishing cryptomorphisms between these concepts it is shown that each of them can be used as a starting point in defining matroids. In the last chapter, independent sets of matroids are defined through the greedy algorithm. This connection gives us further insight into the importance and uniqueness of matroids.

# Životopis

Rođena sam 1. veljače 1991. godine u Mariboru. Osnovnu školu sam pohađala u Cestici, malom mjestu pokraj Varaždina. U Varaždinu sam 2009. godine završila Opću gimnaziju u Prvoj gimnaziji Varaždin. Te godine upisala sam matematiku na Prirodoslovno-matematičkom fakultetu u Zagrebu (nastavnički smjer). Prediplomski studij završila sam 2012. godine i upisala diplomski studij na istom fakultetu. Tijekom svog visokoškolskog obrazovanja volontirala sam u župi Marije Pomoćnice u Zagrebu te tako stekla dodatno iskustvo u poučavanju djece matematici.