Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Nikola Badrov

Optimizacija na matroidu

Diplomski rad

Voditelj rada:
prof.dr.sc. Vedran Krčadinac

Zagreb, 2017.

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

U ovom nam je radu cilj predstaviti teoriju matroida s naglaskom na primjenu u optimizaciji. Matroide je prvi uveo američki matematičar Hassler Whitney 1935. u seminalnom radu *On the abstract properties of linear dependence* pokušavajući apstrahirati pojam linearne (ne)zavisnosti. U tom je radu definirao aksiome *nezavisnosti* i matroidima nazvao bilo koju strukturu koja zadovoljava te aksiome. Teorija je matroida dakle mlado i aktivno područje matematike koje koristi ideje linearne algebre, teorije grafova, kombinatorike, geometrije itd. pa se i mnogo terminologije preuzima iz tih grana.

Matroid je moguće definirati na mnoge, međusobno ekvivalentne, načine. Oni se u teoriji matroida nazivaju *kriptomorfizmima*. U drugom poglavlju definirat ćemo matroide preko nezavisnih skupa, ali kako će nam biti korisno imate i druge karakterizacije, dokazat ćemo kriptomorfizme s definicijama preko ciklusa i baza. Također, pokazat ćemo vezu s matricama i grafovima, te će nam to biti glavna inspiracija za primjenu matroida u optimizaciji.

U trećem ćemo poglavlju dokazati da *pohlepni algoritam* rješava problem nalaska baze maksimalne težine u matroidu, što je svojevrstan glavni rezultat rada. Pohlepni je algoritam zapravo klasa algoritama koji počivaju na heuristici koja u svakom koraku uzima trenutno optimalno rješenje da bi na kraju dobila globalno optimalno rješenje. Taj će nam rezultat omogućiti karakterizaciju i rješavanje cijelih klasa stvarnih problema, od kojih ćemo u radu ilustrirati dva.

U četvrtom ćemo poglavlju uvesti pojam dualnosti u matroidu, svojevrsni analogon dualnosti u teoriji grafova, te prikazati neke operacije na matroidima. Koristeći dualnost, u petom ćemo poglavlju definirati algoritam *plavog pravila i crvenog pravila* koji poopćava skoro pa sve pohlepne algoritme, pa tako Primov i Kruskalov, pohlepne algoritme koje ćemo koristiti na grafovima u trećem poglavlju.

Nadalje, u šestom ćemo poglavlju definirati presjek matroida te pokazati da je maksimalno sparivanje u bipartitnom grafu presjek posebne klase matroida, tzv. *particijskih* matroida. Pomoću dualnosti, dokazat ćemo općenitiji oblik teorema vezanog uz maksimalno sparivanje, poznatijeg kao Kőnigov teorem u teoriji grafova.

2 Matroidi

2.1 Osnovne definicije

Definiranje matroida možemo izvesti na brojne načine (ekvivalentne definicije matroida zovemo *kriptomorfizmima*). Ovdje ćemo navesti njih nekoliko koje su nam bitni za daljnju raspravu, no kao osnovnu definiciju uzet ćemo sljedeću:

Definicija 2.1. Matroid *M je par $(E, \mathscr{I})$ gdje je E konačni skup elemenata, a $\mathscr{I}$ familija podskupova od E (takve podskupove zovemo* ***nezavisnim****) takva da vrijedi:*

(I1) $\emptyset \in \mathscr{I}$, tj. $\emptyset$ je nezavisan skup.

(I2) Za svaki $A' \subset A \subset E$ takav da je $A \in \mathscr{I}$, slijedi $A' \in \mathscr{I}$. Riječima, svaki podskup nezavisnog skupa jest nezavisni skup.

(I3) Za svaki $I, J \in \mathscr{I}$, $|I| < |J|$ vrijedi da postoji element $e \in J - I$ takav da je $I \cup \{e\} \in \mathscr{I}$.

Baza matroida jest maksimalni nezavisni skup matroida, tj. nezavisni skup koji nije pravi podskup niti jednog drugog nezavisnog skupa. Ta nam je definicija bitna jer ćemo sada definirati matroid u terminima baza te potom dokazati kriptomorfizam između definicije preko baza te preko nezavisnih skupova. Sljedeće tvrdnje uvijek vrijede za familiju baza $\mathscr{B}$ matroida M:

(B1) $\mathscr{B} \neq \emptyset$

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

(B3) Ako su B_1, $B_2 \in \mathscr{B}$ i postoji element $x \in B_1 - B_2$, tada postoji element $y \in B_2 - B_1$ takav da je $(B_1 - \{x\}) \cup \{y\} \in \mathscr{B}$.

Primijetimo da (B2) možemo zapisati i kao

(B2') Ako su B_1, $B_2 \in \mathscr{B}$, tada je $|B_1| = |B_2|$.

Ekvivalentnost (B2) i (B2') zapravo proizlazi iz sljedeće tvrdnje - maksimalni (najveći) nezavisni skup možemo definirati kao onaj koji je po kardinalnosti najveći, ali i kao onaj kojeg ne sadrži niti jedan drugi skup. Općenito, te dvije definicije nisu podudarne, ali u slučaju matroida jesu i to zbog trećeg aksioma (I3): kada bi B_1 bio manje kardinalnosti od B_2, tada bi postojao element e takav da je $B_3 := B_1 \cup \{e\}$ također nezavisan skup pa B_1 ne bi bio maksimalan jer bi bio sadržan u B_3.
Dakle, sve baze matroida imaju istu kardinalnost.

Sada smo spremni za dokaz kriptomorfizma. Dokaz se dijeli u tri dijela: prvo moramo dokazati da $\mathscr{B}$ zadovoljava $(B1)-(B3)$ kada pretpostavimo $(I1)-(I3)$, a u drugom dijelu moramo pokazati obrat. Treći se dio sastoji u tome da dokažemo da kompozicije kriptomorfizama daju identitetu. Neka je f funkcija koja familiji nezavisnih skupova pridružuje familiju baza, a g funkcija koja bazama pridružuje nezavisne skupove. Moramo pokazati da je $g(f(\mathscr{I})) = \mathscr{I}$ i $f(g(\mathscr{B})) = \mathscr{B}$. Također, možemo zamijeniti uvjet $(B2)$ sa $(B2')$ zbog gore objašnjene ekvivalencije.

Teorem 2.2. *Neka je E konačan skup i neka je $\mathscr{B}$ familija podskupova od E koja zadovoljava $(B1)$, $(B2')$ i $(B3)$. Tada je par $(E, \mathscr{B})$ kriptomorfan matroidu $M = (E, \mathscr{I})$ i $\mathscr{B}$ je familija baza matroida M.*

Dokaz. Prvi dio: dan je matroid $M = (E, \mathscr{I})$, tj. vrijede $(I1)-(I3)$. Definirajmo $\mathscr{B}$ kao familiju maksimalnih podskupova od $\mathscr{I}$, tj. $\mathscr{B} := \{B \in \mathscr{I} : B \subseteq B' \in \mathscr{I} \text{ povlači } B = B'\}$. Sada moramo dokazati da $\mathscr{B}$ zadovoljava svojstva $(B1)-(B3)$.

$(B1)$: Budući da je $\emptyset \in \mathscr{I}$ i E je konačan, možemo pronaći $B \in \mathscr{I}$ koji nije sadržan niti u jednom drugom nezavisnom skupu. Dakle, $B \in \mathscr{B}$ pa $\mathscr{B} \neq \emptyset$.

$(B2')$: Pretpostavimo suprotno. Ako imamo dva skupa B_1 i $B_2 \in \mathscr{B}$ takva da je $|B_1| < |B_2|$, tada, budući da su B_1, $B_2 \in \mathscr{I}$ postoji element $x \in B_2 - B_1$ takav da je $B_1 \cup \{x\} = J$. Ali, iz toga slijedi da je B_1 pravi podskup od $B_1 \cup \{x\}$ što je kontradikcija s definicijom od $\mathscr{B}$. Dakle, vrijedi $(B2')$.

$(B3)$: Neka su B_1, $B_2 \in \mathscr{B}$ i $x \in B_1 - B_2$. Kako su B_1, $B_2 \in \mathscr{I}$, možemo koristiti $(I2)$ pa vidimo da je $B_1 - x \in \mathscr{I}$. Sada primijenimo $(I3)$ na skupove $B_1 - x$ i B_2. Kako je $|B_1 - x| < |B_2|$ (to vrijedi jer $B_1 - x$ nije maksimalni skup), postoji element $y \in B_2 - (B_1 - x)$ i $(B_1 - x) \cup \{y\} \in \mathscr{I}$.
Preostaje nam dokazati da je $(B_1 - x) \cup \{y\} \in \mathscr{B}$ pa pretpostavimo da to ne vrijedi. Kako je $|(B_1 - x) \cup \{y\}| = |B_1| = |B_2|$, pa ako ne vrijedi da je $(B_1 - x) \cup \{y\}$ u $\mathscr{B}$, onda postoji $B_3 \in \mathscr{B}$ za koji vrijedi $(B_1 - x) \cup \{y\} \subset B_3$ i $|B_1| < |B_3|$, što je onda kontradikcija s $(B2')$.

Drugi dio: neka je $\mathscr{B}$ familija podskupova od E koja zadovoljava $(B1)-(B3)$ i neka je $\mathscr{I} = \{I : I \subseteq B \text{ za neki } B \in \mathscr{B}\}$. Moramo pokazati da $\mathscr{I}$ zaodovoljava $(I1)-(I3)$, to jest da je $(E, \mathscr{I})$ matroid.

Kako je $\mathscr{B} \neq \emptyset$ (po $(B1)$) i $\mathscr{B} \subseteq \mathscr{I}$, slijedi da je $\emptyset \in \mathscr{I}$ pa $(I1)$ vrijedi. Kako bismo dokazali $(I2)$, moramo pokazati da ako $I' \subseteq I$ za neki $I \in \mathscr{I}$, tada slijedi $I' \in \mathscr{I}$. Sada s obzirom na način kako je $\mathscr{I}$ konstruiran, znamo da je $I \subseteq B$ za neki $B \in \mathscr{B}$. No tada $I' \subseteq I \subseteq B$, te je i I' element od $\mathscr{I}$ pa $(I2)$ vrijedi.

Dokazivanje $(I3)$ provest ćemo u nekoliko dijelova. Neka su I_1, $I_2 \in \mathscr{I}$, $|I_1| < |I_2|$ i pretpostavimo da $(I3)$ ne vrijedi. Pokazat ćemo da tada slijedi $|I_1| \geq |I_2|$, što je očito kontradikcija.

Budući da su I_1, $I_2 \in \mathscr{I}$, postoje B_1, $B_2 \in \mathscr{B}$ takvi da vrijede $I_1 \subseteq B_1$ i $I_2 \subseteq B_2$. Pretpostavimo da vrijedi $I_1 \cap I_2 = B_1 \cap I_2$. Također, odabiremo B_2 tako da je $|B_2 - (I_2 \cup B_1)|$ najmanje moguće vrijednosti.

Sada tvrdimo da je $B_2 - (I_2 \cup B_1) = \emptyset$. Ako je $x \in B_2 - (I_2 \cup B_1)$, tada iz $(B3)$ za redom B_2 i B_1 slijedi da postoji $y \in B_1 - B_2$ takav da je $B_3 = B_2 - x \cup \{y\} \in \mathscr{B}$. Ali vrijedi $I_2 \subseteq B_3$ i $|B_3 - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$, što je kontradikcija s izborom B_2. Dakle, $B_2 - (I_2 \cup B_1) = \emptyset$.

Analognim argumentiranjem možemo izabrati B_1 tako da je $B_1 - (I_1 \cup B_2) = \emptyset$. Pogledajmo sada skupove $B_2 - B_1$ i $B_1 - B_2$:

$$B_2 - B_1 = I_2 - B_1 = I_2 - I_1$$

i

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

Sada iz $(B2')$ slijedi $|B_1| = |B_2|$, pa i $|B_2 - B_1| = |B_1 - B_2|$. No iz toga slijedi $|I_2 - I_1| \leq |I_1 - I_2|$ što povlači $|I_2| \leq |I_1|$. Kontradikcija.

Treći dio: na kraju još moramo dokazati da kriptomorfizmi dobro komponiraju, tj. $g(f(\mathscr{I})) = \mathscr{I}$ i $f(g(\mathscr{B})) = \mathscr{B}$.

$g \circ f$: Imamo matroid $M = (E, \mathscr{I})$ i neka su $f(\mathscr{I}) = \mathscr{B}$ svi maksimalni elementi od $\mathscr{I}$ i $g(\mathscr{B}) = \mathscr{I}'$. Moramo dokazati $\mathscr{I} = \mathscr{I}'$. Ako je $I \in \mathscr{I}$, tada je I u nekom maksimalnom B, koji sadrži I. Dakle, $I \in \mathscr{I}' = (g \circ f)(\mathscr{I})$. Obratno, ako je $I' \in \mathscr{I}'$, tada je $I' \subseteq B$, za neki maksimalni $B \in \mathscr{I}$. Po $(I2)$ slijedi da je $I' \in \mathscr{I}$ pa je $\mathscr{I} = \mathscr{I}'$.

$f \circ g$: Dan nam je matroid $(E, \mathscr{B})$, gdje $\mathscr{B}$ zadovoljava $(B1)-(B3)$. Neka su u $\mathscr{B}' = (f \circ g)(\mathscr{B})$ maksimalni elementi od $\mathscr{I} = g(\mathscr{B})$. Moramo dokazati $\mathscr{B} = \mathscr{B}'$. Pretpostavimo prvo da je $B \in \mathscr{B}$. Kad bi vrijedilo $B \notin \mathscr{B}'$, to bi značilo da B nije maksimalni element od $\mathscr{I} = g(\mathscr{B})$, pa bi postojao B' takav da $B \subset B'$ što je kontradikcija s $(B2')$. Dakle, $B \in \mathscr{B}'$.

Neka je sada $B' \in \mathscr{B}'$. To znači da je $B' \in \mathscr{I}$ pa postoji neki $B \in \mathscr{B}$ takav da vrijedi $B' \subseteq B$. Kako je B' maksimalni element od $\mathscr{I}$, a B je u $\mathscr{I}$ također, slijedi $B = B'$, pa je i $B' \in \mathscr{B}$.

$\square$

U prethodnom smo dijelu prikazali i dokazali jedan kriptomorfizam. No, zapravo ima mnogo međusobno ekvivalentnih definicija matroida. U nastavku ćemo definirati pojmove pomoću kojih je moguće uspostaviti kriptomorfizme, ali detalje i dokaze nećemo navoditi, a mogu se pronaći u [2].

Definicija 2.3. *Neka je M matroid. Ako je C zavisan skup, a svaki njegov pravi podskup jest nezavisan, tada C zovemo ciklus matroida.*

Iz definicije vidimo kako familiju $\mathscr{C} = \{C : C \text{ je ciklus matroida}\}$ možemo dobiti iz $\mathscr{I}$. Obratno, nezavisni skupovi su svi podskupi od E koji ne sadrže ciklus $C \in \mathscr{C}$. Već uviđamo ekvivalenciju s nezavisnim skupovima, ali za njeno formaliziranje, kao i s bazama, trebamo identificirati ključna svojstva familije $\mathscr{C}$ pomoću kojih možemo definirati matroid:

Teorem 2.4. *Neka je E konačan skup i $\mathscr{C}$ familija podskupova od E koja zadovoljava sljedeća svojstva:*

(C1) $\emptyset \notin \mathscr{C}$

(C2) ako su C_1 i $C_2 \in \mathscr{C}$ te vrijedi $C_1 \subseteq C_2$, tada je $C_1 = C_2$.

(C3) ako su C_1 i $C_2 \in \mathscr{C}$ takvi da $C_1 \neq C_2$ i $x \in C_1 \cap C_2$, tada je $C_3 \subseteq C_1 \cup C_2 - x$ za neki $C_3 \in \mathscr{C}$

Tada je $(E, \mathscr{C})$ kriptomorfno matroidu $M = (E, \mathscr{I})$ i $\mathscr{C}$ je familija ciklusa matroida M.

Dokaz ima istu strukturu kao i za baze: pretpostavimo da imamo matroid definiran preko nezavisnih skupova, definiramo cikluse kao minimalne zavisne skupove te dokažemo svojstva $(C1) - (C3)$. Onda definiramo nezavisne skupove preko ciklusa i dokažemo da zadovoljavaju $(I1) - (I3)$. Konačno, pokažemo da se kriptomorfizmi dobro komponiraju.

Definicija 2.5. *Neka je $M = (E, \mathscr{I})$ matroid i $A \subseteq E$.* ***Rang od A****, oznakom $r(A)$, definiramo kao veličinu najvećeg nezavisnog podskupa od A:*

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

Rang matroida $r(M)$ je jednostavno $r(E)$.

Teorem 2.6. *Neka je $M = (E, \mathscr{I})$ matroid. Tada za svaki $A \subseteq E$, ako su I i I' maksimalni nezavisni podskupovi od A, vrijedi $|I| = |I'|$.*

Obratno, ako je M konačna struktura koja zadovoljava gornju tvrdnju te $(I1)$, $(I2)$, onda je M i matroid.

Dokaz. Pretpostavimo suprotno, da postoje maksimalni nezavisni podskupovi od A za koje vrijedi $|I| < |I'|$. No, tada po $(I3)$ postoji $e \in I' - I$ takav da je $I \cup \{e\}$ nezavisan, što je kontradikcija s tvrdnjom da je I maksimalan u A.

Obratno, neka vrijede ($I1$) i ($I2$) te neka za sve maksimalne nezavisne skupove $I, I' \subseteq A$ vrijedi $|I| = |I'|$, gdje je A proizvoljan podskup od E. Uzmimo sada dva proizvoljna nezavisna skupa J i J' takva da vrijedi $|J| < |J'|$. Definirajmo $A = J \cup J'$. Zbog pretpostavke sada slijedi da J sigurno nije maksimalan s obzirom na definirani A pa sigurno postoji element $e \in J'$ takav da je $J \cup \{e\}$ nezavisan. Dakle, vrijedi i aksiom ($I3$).

□

Ovim smo teoremom pokazali da smo rang $r(A)$ mogli definirati kao kardinalni broj maksimalnog nezavisnog skupa u A.

Može se pokazati da funkcija ranga zadovoljava sljedeća svojstva za A, $B \subseteq E$:

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

(R2) ako je $A \subseteq B$, tada je $r(A) \leq r(B)$

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

Naglasimo samo da se svojstvo ($R3$) zove semimodularnost. U sljedećem ćemo poglavlju iskazati vezu funkcije ranga matroida i ranga matrice, po kojem je i dobila ime. Postoji, naravno, kriptomorfizam između funkcije ranga i nezavisnih skupova i to prema prethodno definiranoj vezi, a postupa se analogno kao i u prošlim primjerima.

Sljedeća definicija usko se veže uz pojam funkcije ranga. *Zatvoreni skup* u matroidu je onaj skup koji je *maksimalan s obzirom na rang*: ako dodamo bilo koji novi element u zatvoreni skup, njegov se rang poveća.

Definicija 2.7. *Neka je $M = (E, \mathscr{I})$ matroid. Podskup $F \subseteq E$ jest* ***zatvoreni skup*** *ako vrijedi $r(F \cup \{x\}) > r(F)$ za svaki $x \notin F$.*

Direktna veza između zatvorenih i nezavisnih skupova možda nije očita, ali može se uspostaviti kriptomorfizam između zatvorenih skupova i funkcije ranga.

Sada ćemo definirati *operator zatvaranja.* Ideja je da od proizvoljnog skupa $A \subseteq E$ dobijemo zatvoreni $\bar{A}$. Dakle, $\bar{A}$ je jednostavno najmanji zatvoreni skup koji sadrži A. Kao i u topologiji (odakle i dolazi terminologija), zatvarač ćemo formalno definirati kao presjek svih zatvorenih skupova koji sadrže A:

Definicija 2.8. *Neka je M matroid i $\mathscr{F}$ familija zatvorenih skupova i $A \subseteq R$. Tada* ***zatvarač od*** *A, u oznaci $\bar{A}$, definiramo kao*

$$\bar{A} = \bigcap \{F : A \subseteq F, F \in \mathscr{F}\}.$$

2.2 Primjeri matroida

Sama nas terminologija, posebice *nezavisnih skupova* navodi da teorija matroida ima dosta veze s linearnom algebrom i teorijom grafova. U ovom ćemo dijelu uspostaviti veze matroida s matricama i grafovima.

2.2.1 Matrični matroidi

Prvo pitanje koje nam se nameće jest kako od matrice napraviti matroid. Ono što definira matroide jesu nezavisni skupovi koji zadovoljavaju aksiome $(I1)$–$(I3)$. Dakle, ideja je da pojam nezavisnosti u terminima teorije matroida shvatimo kao *linearnu nezavisnost* u linearnoj algebri. Podsjetimo se, skup vektora je **linearno zavisan** ako se barem jedan od vektora može prikazati kao linearna kombinacija ostalih vektora; ako skup nije linearno zavisan, kažemo da je **linearno nezavisan**.

No, da bismo to opravdali, moramo odgovoriti na pitanje zadovoljavaju li podskupovi linearno nezavisnih stupaca matrice aksiome $(I1) - (I3)$:

Teorem 2.9. *Neka je E skup stupaca matrice A, neka je $\mathscr{I}$ familija podskupova od E koji su linearno nezavisni. Tada je $\mathscr{I}$ familija nezavisnih skupova matroida.*

Dokaz. Svojstva $(I1)$, $(I2)$ slijede trivijalno - $(I1)$ zbog činjenice da je $\emptyset$ (trivijalno) linearno nezavisan, a $(I2)$ slijedi direktno iz definicije linearne nezavisnosti.

Za dokazivanje svojstva $(I3)$, uzmimo X i Y, dva linearno nezavisna podskupa stupaca matrice A takvi da je $|X| < |Y|$. Mi sada želimo pronaći element $e \in Y - X$ takav da je $X \cup \{e\}$ linearno nezavisan. Problem je zapravo naći baš onaj e koji dodan skupu X, neće stvoriti linearno zavisan skup. Tome možemo doskočiti tako da gledamo **linearnu ljusku** $\langle X \rangle$, tj. skup svih linearnih kombinacija elemenata iz skupa X. Budući da smo dodali samo linearno zavisne elemente, dimenzija je ljuske jednaka $|X|$, pa postoji element e iz $Y - \langle X \rangle$ zato što je Y linearno nezavisan skup s više elemenata od $\dim\langle X \rangle$. Nadalje, kako su u $\langle X \rangle$ sve linearne kombinacije elemenata iz X, vidimo da dodavanje elementa e neće narušiti nezavisnost, tj. $X \cup \{e\}$ će ostati linearno nezavisan.

Dakle, pokazali smo da postoji element e koji dodan u X zadržava svojstvo linearne nezavisnosti pa vrijedi aksiom $(I3)$ te je time dokaz gotov. $\square$

Ovime smo zapravo pokazali da bilo koji podskup vektora može inducirati matroid; u tom slučaju, matroid induciran matricom A označavamo sa $M(A)$. Obratno pitanje, je li svaki matroid induciran nekom matricom, izlazi iz okvira ovog rada, ali odgovor je negativan i kontraprimjer se može pronaći u [2].

Sada kada smo dokazali da je $M(A)$ matroid, možemo usporediti neke pojmove iz teorije matroida s analogonima u linearnoj algebri. Neki su i terminološki ekvivalentni: baza, rang, nezavisan skup. Ciklus matroida je jednostavno minimalni *linearno* zavisan skup.

Primjer 2.10. *Definirajmo matricu A*

$$\begin{bmatrix} 1 & 0 & 2 & 4 & 3 \\ 0 & 3 & 4 & 8 & 1 \end{bmatrix}$$

i označimo stupce redom a, b, c, d i e. Iz linearne algebre znamo da je maksimalni mogući rang ove matrice 2 jer ima 2 retka. Odmah uočavamo da su prvi i drugi stupac linearno nezavisni pa je rang uistinu 2.

Kako bismo inducirali matroid $M = (E, \mathscr{I})$, trebamo definirati skupove E i $\mathscr{I}$. Skup E je jednostavno skup svih stupaca matrice $E := \{a, b, c, d, e\}$. Zbog prethodnog teorema znamo da $\mathscr{I}$ odgovara svim podskupovima od skupa stupaca koji su linearno nezavisni. To je naravno prazan skup i svi jednočlani skupovi $\{a\}, \{b\}, \{c\}, \{d\}, \{e\}$. Kako je rang 2, znamo da ne postoje tročlani skupovi stupaca koji su linearno nezavisni, pa nam preostaje samo provjeriti koji su dvočlani skupovi stupaca linearno nezavisni. Uočavamo da je samo skup $\{c, d\}$ linearno zavisan jer $(2, 4) = 2 \cdot (4, 8)$. Dakle, sve ostali dvočlani skupovi stupaca ulaze u $\mathscr{I}$ pa dobivamo

$$\mathscr{I} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{a, b\}, \{a, c\}, \\ \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, e\}, \{d, e\}\}.$$

Time smo definirali matroid $M(A)$. Možemo primijetiti da je najveći skup u familiji kardinaliteta 2, pa je uistinu rang matroida isti kao i rang matrice.

2.2.2 Grafni matroidi

Prvo ćemo definirati neke pojmove iz teorije grafova koji su nam bitni za nastavak. **Graf** G definiramo kao uređeni par $G = (V, E)$ gdje je V konačan skup čije elemente zovemo vrhovima i E konačan skup čije elemente zovemo bridovima. Brid spaja dva vrha, a ako spaja dva ista vrha, onda se zove **petlja**. Kažemo da je vrh **incidentan** s bridom ako brid spaja taj vrh. Za dva vrha kažemo da su **susjedni** ako imaju zajednički brid.

Šetnja u grafu je niz $(v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$ gdje je e_i brid između vrhova v_{i-1} i v_i. Kažemo da je šetnja zatvorena ako je $v_0 = v_n$. **Put** je šetnja u kojoj su svi vrhovi različiti (osim eventualno prvog i zadnjeg). Ako je put zatvoren, onda govorimo o **ciklusu**. Graf je povezan ako postoji šetnja između svaka dva vrha. Povezani graf koji nema ciklusa zovemo **stablo**. Graf bez ciklusa zovemo **šumom**. Ako je G povezani graf, tada stablo koje sadrži sve vrhove od G i njegov je podgraf (svaki brid pripada i grafu G) zovemo **razapinjućim stablom** od G. U povezanom grafu, razapinjuće stablo je maksimalni aciklični podskup bridova.

Graf $G = (V, E)$ zovemo **bipartitnim** ako se V može particionirati u skupove A i B tako da svaki brid povezuje A i B. Može se dokazati ekvivalencija da je graf bipartitan ako i samo ako mu je svaki ciklus parne duljine. **Sparivanje** je skup bridova grafa G koji međusobno ne dijele niti jedan vrh. **Pokrivanje** je takav skup vrhova grafa G da je svaki brid od G incidentan s barem jednim vrhom iz tog skupa.

Iz teorije grafova znamo da svaki povezani graf G ima razapinjuće stablo te ako G ima n vrhova, tada je broj bridova u razapinjućem stablu $n - 1$. Posljedica ove tvrdnje jest da ako je G šuma satavljena od v vrhova, e bridova i c disjunktnih stabala, tada je $e = v - c$. Broj disjunktnih stabala c još zovemo i broj komponenti od G.

Sada smo spremni povezati grafove i matroide.

Teorem 2.11. *Neka je $G = (V, E)$ graf i neka je $\mathscr{I}$ familija podskupova od E koji ne sadrže ciklus. Tada $\mathscr{I}$ čini nezavisne skupove matroida na skupu E, to jest $M(G) = (E, \mathscr{I})$ je matroid.*

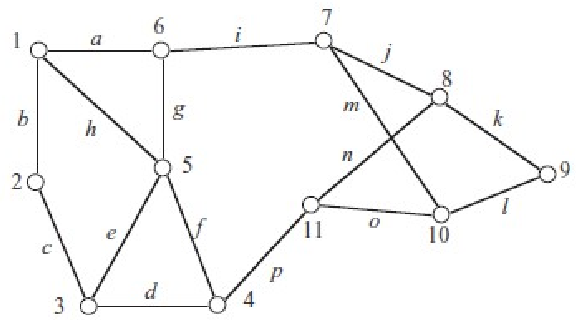
Dokaz. Moramo dokazati da aciklički podskupovi bridova grafa zadovoljavaju svojstva $(I1) - (I3)$. $(I1)$ je trivijalan - prazan skup sigurno je acikličan. $(I2)$ isto lagano slijedi - ako je B podskup bridova koji ne sadrže ciklus, tada sigurno ni njegov podskup $A \subseteq B$ ne sadrži ciklus.

Sada moramo pokazati da vrijedi $(I3)$. Neka su A i B aciklični podskupovi takvi da je $|A| < |B|$. Zapravo moramo pronaći brid u B koji nije u A i može se dodati u A bez da čini ciklus.

Prvo pretpostavimo da je A stablo. Tada su bridovi od A incidentni sa samo $|A| + 1$ vrhova grafa G. Kako je B šuma, ona je incidentna s $|B| + k$ vrhova gdje je $k \geq 1$ broj komponenti od B. Kako je $|B| > |A|$ slijedi $|B| + k > |A| + 1$. To znači da su bridovi od B incidentni s nekim vrhom koji nije incidentan niti s jednim bridom od A. Neka je taj vrh v i neka je $b \in B$ bilo koji brid koji je incidentan s v (može ih biti više, naravno). Tada je $A \cup \{b\}$ acikličan i $(I3)$ vrijedi.

Ali ako A nije stablo, tada ne možemo tvrditi kao prije da će postojati vrh v. No, možemo koristiti istu tu argumentaciju ako gledamo svako pojedinačno stablo iz šume A. Pretpostavimo da je A sastavljeno od c disjunktnih stabala $T_1, T_2, \ldots, T_c$. Ako postoji v kao prije, gotovi smo. Ako ne postoji, tada tvrdimo da postoji brid u B koji povezuje dva disjunktna stabla T_i, T_j u A.

Pretpostavimo suprotno. Prebrojimo koliko bridova onda ima B: može imati najviše $e_1+\cdots+e_c$ bridova gdje je e_i broj bridova u stablu T_i. No, tada imamo $|A| = |B|$ što je kontradikcija sa $|A| < |B|$. Dakle, B mora sadržati neki brid koji povezuje neka dva disjunktna stabla u A te taj brid možemo dodati u A bez da čini ciklus. Time je dokaz završen. $\square$



Slika 1: preuzeto iz [1]

Primjer 2.12. *Neka je G graf kao na slici 1. Sada ćemo interpretirati termine teorije matroida u smislu teorije grafova.*

- *Nezavisni skup $\leftrightarrow$ šuma. Na primjer, $I = \{a, b, c, d, e, j, o, l\}$ je šuma sastavljena od tri stabla: $T_1 = \{a, b, c, d, e\}, T_2 = \{j\}, T_3 = \{l, o\}$. Ta tri stabla induciraju particiju vrhova od G:*

$$\{1, 2, 3, 4, 5, 6\}, \{7, 8\}, \{9, 10, 11\}.$$

  Ovakve particije igraju važnu ulogu u opisivanju zatvorenih skupova.

- *Baze $\leftrightarrow$ razapinjuća stabla. Kako je G povezan, maksimalni aciklični podskupovi bridova su stabla koja sadrže svaki vrh, to jest razapinjuća stabla. Na primjer, $B = \{b, c, e, f, g, k, l, m, o, p\}$ je razapinjuće stablo. Primijetimo da svako razapinjuće stablo ima 10 bridova.*

- *Ciklusi matroida $\leftrightarrow$ ciklusi grafa. Na primjer, ciklus u grafu $\{a, b, c, e, g\}$ je i ciklus odgovarajućeg matroida.*

- *Rang* $\leftrightarrow$ *veličina najvećeg acikličnog skupa bridova u* A. *Na primjer, za* $A = \{a, c, d, e, f, g, h, j, k, l, m\}$, *dobivamo šumu od dva stabla* $\{c, d, f, g, h\}$ *i* $\{j, k, l\}$. *Ova šuma ima osam bridova, dakle* $r(A) = 8$.

- *Zatvoreni skupovi* $\leftrightarrow$ *skup bridova koji odgovara particiji vrhova. Iako nas najčešće vrhovi ne zanimaju za strukturu matroida, ovdje igraju ulogu. Prvo, uzmimo neku particiju vrhova:*

  $$\Pi = \{1, 3, 4, 5\}, \{2\}, \{6\}, \{7, 8, 10, 11\}, \{9\}$$

  Sada nađimo sve bridove koji spajaju vrhove unutar svakog bloka od Π. *Za jednočlane blokove, naravno, ne postoje takvi bridovi. Za blok* $\{1, 3, 4, 5\}$ *imamo bridove* d, e, f *i* h. *Za blok* $\{7, 8, 10, 11\}$ *imamo bridove* j, m, n *i* o. *Dakle, zatvoreni skup* F_Π *s obzirom na particiju* Π *je* $\{d, e, f, h, j, m, n, o\}$.

  Zašto je ovo zatvoreni skup? Dodavanje bilo kojeg novog brida u F_Π *povećava rang tako da bilo pogodi novi vrh (recimo brid* c *bi pogodio vrh* 2*), bilo da spoji dvije komponente od* F_Π *(recimo, brid* p *spoji* $\{d, e, f, h\}$ *i* $\{j, m, n, o\}$*).*

- *Zatvarač* $\leftrightarrow$ *sadrži sve bridove koji ne povećavaju rang od* A. *Uzmimo* $A = \{c, d, e, h, j, k, l\}$, *tada je* $\bar{A} = A \cup \{b, f, m\}$. *Primijetimo da* $\bar{A}$ *možemo konstruirati iz particije* $\Pi = \{1, 2, 3, 4, 5\}, \{6\}, \{7, 8, 9, 10\}, \{11\}$.

2.2.3 Particijski matroidi

Definicija 2.13. *Uzmimo neku particiju skupa E u skupove $E_1, \dots, E_l$ i neka je*

$$\mathscr{I} = \{X \subseteq E : |X \cap E_i| \leq k_i \text{ za svaki } i = 1, \dots, l\}$$

gdje su k_i neki parametri koji zadovoljavaju $0 \leq k_i \leq |E_i|$. Tada $M = (E, \mathscr{I})$ zovemo ***particijskim matroidom****.*

Sada ćemo opravdati definiciju, tj. da je opisani objekt matroid za bilo koju particiju skupa E i bilo koje parametre k_i:

Propozicija 2.14. *Gore definirana struktura $M = (E, \mathscr{I})$ jest matroid.*

Dokaz. Kao i do sada, trebamo dokazati da M zadovoljava aksiome $(I1) - (I3)$. $(I1)$ trivijalno slijedi budući da je $|\emptyset \cap E_i| = 0$ za bilo koji E_i. Uzmimo neki $I \subset \mathscr{I}$; vidimo da će i svaki podskup $A \subset I$ biti u $\mathscr{I}$ zato što vrijedi $|A \cap E_i| \leq |I \cap E_i| \leq k_i$, za svaki i, pa je time zadovoljen i $(I2)$.

Sada uzmimo $I, J \in \mathscr{I}$ takve da je $|I| < |J|$. Iz te nejednakosti slijedi da postoji i takav da je $|I \cap E_i| < |J \cap E_i|$. Ako uzmemo bilo koji element e iz skupa $E_i \cap (J - I)$, vidimo da će i dalje skup $I \cup \{e\}$ biti u $\mathscr{I}$ jer njegova kardinalnost može biti najviše $|J \cap E_i|$, a znamo da vrijedi $|J \cap E_i| \leq k$ budući da je $J \in \mathscr{I}$. Ovime smo pokazali da vrijedi i $(I3)$. □

Primijetimo da je ključna činjenica da su E_i međusobno disjunktni (jer čine particiju). U suprotnom, ne bi vrijedila prethodna propozocija.

Primjer 2.15. *Neka je $E = \{1, 2, 3\}$. Definirajmo $E_1 = \{1, 2\}$ i $E_2 = \{2, 3\}$ i neka je $k_1 = k_2 = 1$. Vidimo da su skupovi $Y = \{1, 3\}$ i $X = \{2\}$ elementi od $\mathscr{I}$ jer vrijedi $|X \cap E_1| = |X \cap E_2| = |Y \cap E_1| = |Y \cap E_2| = 1$. No, ne vrijedi $(I3)$ jer ne možemo naći niti jedan element u $Y - X$ koji bi dodan u X i dalje bio elementom od $\mathscr{I}$: $|(X \cup \{1\}) \cap E_1| = 2 = |(X \cup \{3\}) \cap E_2|$.*

3 Matroidi i pohlepni algoritam

Sada ćemo se usredotočiti na primjenu teorije matroida. Promatrat ćemo matroid $M = (E, \mathscr{I})$ čijim su elementima e_i pridružene određene težine $w(e_i)$. Cilj nam je pronaći nezavisni skup za koji je suma težina najveća moguća. Svako pridruživanje težina elementima inducira leksikografski uređaj na nezavisnim skupovima. Dakle, pretpostavimo da su $I_1 = \{a_1, ..., a_m\}$ i $I_2 = \{b_1, ..., b_n\}$ dva nezavisna skupa, čiji su elementi sortirani silazno po težini. Tada kažemo da je I_1 **leksikografski veći** od I_2 ako postoji neki k takav da je $w(a_i) = w(b_i)$, za $1 \leq i \leq k-1$ i $w(a_k) > w(b_k)$ ili ako je $w(a_i) = w(b_i)$, za $1 \leq i \leq n$ i $m > n$. Za skup koji nije leksikografski manji ni od kojeg drugog, kažemo da je **leksikografski maksimum**. Naravno, takav leksikografski maksimalni nezavisni skup mora biti baza, a ako su sve težine različite, takva je baza jedinstvena.

Teorem 3.1. *Neka je $\mathscr{I}$ familija nezavisnih skupova matroida. Tada:*

(1) Za bilo koje nenegativne težine $w = (w_i)$ elemenata iz E, skup leksikografskog maksimuma iz $\mathscr{I}$ ima i najveću težinu.

Obratno, ako $M = (E, \mathscr{I})$ ima konačnu strukturu koja zadovoljava prva dva aksioma matroida i (1), tada je M matroid.

Dokaz. Neka je $\mathscr{I}$ familija nezavisnih skupova matroida s težinama. Neka je $B = \{b_1, ..., b_n\}$ leksikografski maksimalna baza i neka je $I = \{a_1, a_2, ..., a_m\}$ bilo koji nezavisni skup takvi da su silazno sortirani, tj. $w(b_{i+1}) \geq w(b_i)$ i $w(a_{i+1}) \geq w(a_i)$. Ono što mi sada tvrdimo sada jest da je B i element po element veći od skupa I, tj. $w(b_i) \geq w(a_i)$. Pretpostavimo suprotno, da postoji k takav da je $w(b_k) < w(a_k)$. Bez smanjenja općenitosti, neka je k najmanji takav. Tada promotrimo skupove:

$$B_{k-1} = \{b_1, ..., b_{k-1}\}$$
$$I_k = \{a_1, ..., a_k\}$$

Po trećem aksiomu matroida, $\{b_1, b_2, ..., b_{k-1}, a_i\}$, za neki i, $1 \leq i \leq k$, jest nezavisan skup i leksikografski je veći od B. Ali to je kontradikcija s činjenicom da je B leksikografski maksimum. Dakle, vrijedi da je $w(b_p) \geq w(a_p)$ za sve p, pa zbog toga i nenegativnosti težina slijedi:

$$\sum_{1 \leq p \leq n} w(b_p) \geq \sum_{1 \leq p \leq m} w(a_p).$$

Obratno, pretpostavimo da M nije matroid. Ako M nije matroid, tada zbog teorema 2.6. mora postojati podskup $A \subseteq E$ i dva maksimalna podskupa I i I' od A iz $\mathscr{I}$, takvi da $|I| < |I'|$. Neka svaki element iz I ima težinu $1+\varepsilon$, gdje je $\varepsilon > 0$ proizvoljno mali broj, svaki element iz $I' - I$ ima težinu 1, a svi preostali elementi iz E imaju težinu 0. Tada je I sadržan u leksikografskom maksimumu od E čije su težine manje od težina skupa I'. Dakle, *(1)* ne vrijedi, što je kontradikcija. $\square$

Iz dokaza ovog teorema vidimo da leksikografski maksimalna baza ima još jače svojstvo od prvotno definiranog. Naime, takva je baza član po član teža od bilo kojeg drugog nezavisnog skupa.

Primijetimo da nam ovaj rezultat daje praktični način za računanje maksimalnog nezavisnog skupa - ako znamo da je maksimalna baza teža član po član od bilo koje druge, to znači da pri konstruiranju takve maksimalne baze, samo moramo paziti da u svakom koraku uzimamo element najveće težine koji ne narušava njenu nezavisnost.

Ono što smo upravo opisali jest tzv. **pohlepni algoritam**. Pohlepni je algoritam zapravo bilo koji algoritam koji u svakom koraku traži lokalno optimalno rješenje kako bi došao do globalno optimalnog. Takav algoritam ne preisputuje donesene odluke, nego samo na temelju prethodnih donosi nove. Zato se i zove *pohlepnim*, jer u svakom trenutku uzima najbolju trenutnu opciju. Konkretno na našem primjeru, mi u svakom koraku biramo trenutni maksimalan element (koji ne narušava nezavisnost), a na kraju dobivamo skup koji je u globalnom smislu maksimalan, baš zbog prethodnog teorema. Pohlepni algoritam leži matroidima zato što to i jest struktura u pozadini tog algoritma - moglo bi se zaključiti, da su matroidi baš i zato tako definirani!

Zapišimo formalno korake pohlepnog algoritma na matroidu $M = (E, \mathscr{I})$ koji daje maksimalnu bazu B:

uzmi najteži element $e_1 \in E$ i definiraj $B := \{e_1\}$
$i = 1$
dok je $i > 0$
  ako postoji bar jedan element koji dodan u B ne narušava nezavisnost
    uzmi najteži takav
    dodaj ga u B
  inače
    $i = 0$

Cilj nastavka rada bit će predstaviti razne optimizacijske probleme, pokazati njihovu vezu s matroidima kako bismo ih riješili pomoću razvijene teorije. Sada ćemo zapravo vidjeti korisnost matroida i visoko apstraktnog pristupa - bilo koji problem maksimizacije ili minimizacije koji možemo svesti na inherentnu strukturu matroida, znamo kako riješiti!

3.1 Dizajn eksperimenata

Poljoprivrednik zna da je za dobar urod određene sadnice važno n minerala. Pretpostavlja da postoji linearna veza između količine dodanih minerala i poboljšanja sjetve. Preciznije, poboljšanje Y dano je formulom

$$Y = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

gdje je x_i količina dodanog i-tog minerala u formi gnojiva. Problem s kojim se suočava jest određivanje koeficijenata $a_1, a_2, \ldots, a_n$.
Pretpostavimo da poljoprivrednik može napravit određen broj odvojenih eksperimenata, svaki put s različitim gnojivom. Gnojivo j sadrži a_{ij} jedinica minearala i i njegova uporaba košta c_j novčanih jedinica. Koje je najjeftiniji izbor gnojiva koji će mu omogućiti da odredi koeficijente a_i?
Gnojiva dakle odgovaraju stupcima matrice $A = (a_{ij})$. Poljoprivrednik mora izabrati podskup stupaca koji ima rang n i koji je linearno zavisan, jer inače čini više nego što je potrebno da odredi potrebne informacije: rezultat barem jednog gnojiva može se u tom slučaju predvidjeti iz rezultata ostalih gnojiva. Dakle, ono što poljoprivrednik traži je linearno nezavisan podskup od n stupaca, za koji je suma c_j-ova što manja. Kako je matrica matroid, i problem se svodi na pronalaženje minimalnog linearnog nezavisnog podskupa, znamo da će pohlepni algoritam dati rješenje. Opišimo dakle kako bi izgledala realizacija pohlepnog algoritma na matrici:

Pohlepni algoritam za matrične matroide

Kao što smo utvrdili već ranije, nezavisni skupovi matričnog matroida linearno su nezavisni skupovi stupaca matrice. Imajući to u vidu, trebamo samo paziti da zadržimo linearnu nezavisnost skupa, a to kod matrica možemo provesti pomoću Gaussovih transformacija:

1. Uredimo stupce matrice tako da su najveći najljeviji, tj. $w_1 \geq w_2 \geq \cdots \geq w_n$. Neka je $k = 1$.

2. (a) Ako je stupac k nula, idi na (b). Inače, izaberi bilo koji element različit od nule u stupcu, npr. a_{ik}, i s njim eliminiraj sve nenul elemente desno od njega, tj. od j-tog stupca oduzmi k-ti stupac pomnožen s $\frac{a_{ij}}{a_{ik}}$, $j \geq k$

   (b) Ako je $k < n$, stavi $k = k + 1$ i vrati se na (a). Inače, stop.
   Nenul stupci su elementi optimalne baze, i kardinalitet baze je, naravno, rang matrice.

Vratimo se na naš primjer. Neka stupac j ima težinu $w_j = W - c_j$ gdje je W dovoljno velik broj.

Primjer 3.2. *Neka ja poljoprivredniku na raspolaganju pet gnojiva od kojih svaki može sadržavati četiri različita minerala. Troškovi i sastav gnojiva su:*

1. $c_1 = 12$, *sastav* $= (2, 1, 8, 5)$
2. $c_2 = 19$, *sastav* $= (1, 1, 4, 2)$
3. $c_3 = 11$, *sastav* $= (0, 1, 2, 1)$
4. $c_4 = 16$, *sastav* $= (0, 1, 1, 0)$
5. $c_5 = 20$, *sastav* $= (1, 0, 3, 2)$

Koristimo pohlepni algoritam za matrične matroide:

(1) *Definiramo* $w_i := N - c_i$, *gdje je* $N = 20$. *Sada matricu* A *sortiramo silazno po stupcima s obzirom na težine* $w = (8, 1, 9, 4, 10)$.

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 2 & 8 & 1 & 4 \\ 2 & 1 & 5 & 0 & 2 \end{pmatrix}$$

(2) *S elementom* a_{11} *eliminiramo ostatak reda:*

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 2 & 2 & 1 & 1 \\ 2 & 1 & 1 & 0 & 0 \end{pmatrix}$$

S elementom a_{22} *nastavljamo eliminaciju:*

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & -1 & -1 \\ 2 & 1 & 0 & -1 & -1 \end{pmatrix}$$

Kako je treći stupac cijeli 0, idemo na četvrti stupac i koristimo element a_{34} *i dobivamo:*

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & -1 & 0 \\ 2 & 1 & 0 & -1 & 0 \end{pmatrix}$$

Došli smo do petog koraka u algoritmu, što je jednako n, *gotovi smo s algoritmom.*

Dakle, poljoprivredniku je najjeftinija opcija upotrijebiti gnojiva 1, 2 *i* 3 *kako bi odredio koeficijente* a_i *i to će platiti* $10 + 11 + 16 = 37$ *novčanih jedinica.*

3.2 Problem maksimalnog razapinjućeg stabla

Sada ćemo dati primjere problema koje u teoriji grafova svodimo da na problem maksimalnog razapinjućeg stabla. Pretpostavimo da imamo neusmjeren, povezan i težinski graf te želimo naći razapinjuće stablo koje ima maksimalnu težinu. Kao što smo već ranije zaključili, razapinjuća stabla grafa odgovaraju bazama pripadnog matroida; ako k tome imamo još i težine definirane na svakom bridu, pronalazak maksimalnog razapinjućeg stabla upravo je problem pronalaska maksimalnog nezavisnog skupa grafnog matroida koji rješavamo pohlepnim algoritmom.

U literaturi, češće se spominje problem *minimalnog razapinjućeg stabla*, u smislu da tražimo razapinjuće stablo najmanje težine. Taj je problem trivijalno ekvivalentan, kao što ćemo i pokazati u narednom primjeru.

Kruskalov algoritam

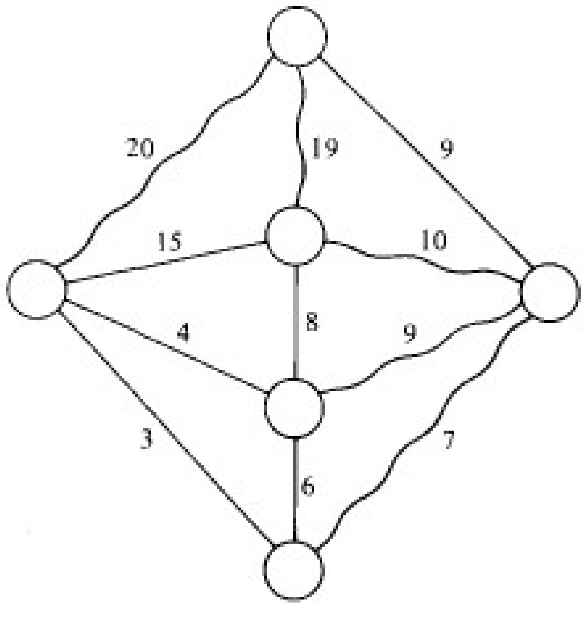
Algoritam bismo mogli za dani problem ovako definirati: nađi brid najveće težine, dodaj ga u skup rješenja te zatim nađi drugi najteži brid koji dodan u skup ne čini ciklus. Taj proces ponavljamo sve dok ne dobijemo razapinjuće stablo. Vidimo da je to pohlepni algoritam, u literaturi poznat kao Kruskalov algoritam, i da je u potpunosti analogan generalnom matroidnom pohlepnom algoritmu.

Ono što bismo mogli primijetiti kao svojevrsni nedostatak ovog algoritma jest da pri stvaranju maksimalnog razapinjućeg stabla nemamo povezani podgraf. To jest, algoritam u koracima generira graf koji ne mora nužno biti povezan (na kraju će, naravno, graf biti povezan). Na primjer, to može biti nekonstruktivno u raznim stvarnim problemima poput gradnje vodovodne mreže između mreže kućanstava - kućanstva predstavljaju vrhove, a cijevi bridove čija je težina obrnuto proporcionalna trošku gradnje. Naravno, želimo povezati sva kućanstva u vodovodnu mrežu te minimizirati troškove gradnje. Kada bismo slijedili Kruskalov algoritam, u fazama bismo gradnje mogli dobiti dva kućanstva koja nisu međusobno povezana, što u ovom kontekstu ne bi baš imalo smisla. Zato ćemo u nastavku na analognom primjeru dati alternativni algoritmam koji u svakom koraku nalazi brid koji će biti incidentan sa skupom prethodno odabranih bridova.

Problem televizijske mreže

Televizijska mreža planira povezati svoje postaje tako da čine povezanu mrežu. Svaka veza (i, j) između dvije postaje ima svoj trošak a_{ij}. Kako konstruirati mrežu s minimalnim ukupnim troškom?
Kada bismo postaje shvatili kao vrhove, a veze kao bridove, problem bismo mogli reformulirati kao problem pronalaženja razapinjućeg stabla minimalnog troška. Kako bismo ovaj problem pretvorili u maksimizacijski, troškove a_{ij} zamijenit ćemo sa težinama $w_{ij} = N - a_{ij}$, gdje je N neki veliki broj.
Kao što smo već i ranije zaključili, razapinjuća stabla grafa odgovaraju bazama pripadnog matroida. Dakle, problem koji smo opisali točno je pronalazak maksimalnog nezavisnog skupa matroida koji rješavamo pohlepnim algoritmom.

Primjer 3.3. *Uzmimo ovaj graf kao vizualizaciju danog problema, gdje vrhovi predstavljaju TV postaje, a bridovi veze među njima.*



Slika 2: preuzeto iz [1]

Prvo odabiremo brid težine 20, pa 19; kad bismo izabrali 15, dobili bismo ciklus, pa ga odbacujemo. Nastavljamo sa bridom težine 10 i 9, 8 odbacujemo i, konačno, razapinjuće stablo dobivamo sa bridom težine 7. Odabrani bridovi označeni su valovitom crtom.

Gornji smo primjer riješili na prste - ubacivali smo bridove sortirane po težini dok nismo dobili razapinjuće stablo tako da u svakom koraku imamo povezani graf. No, ipak opišimo malo sistematičnije algoritam.

Robert Prim je predložio pristup u kojem se konstruira sve veći i veći skup optimalno povezanih vrhova. Taj skup vrhova označujemo sa slovom P. Komplement skupa P označujemo sa T.
Počinjemo s proizvoljnim vrhom iz P, pronađemo najteži brid između njega i bilo kojeg vrha iz skupa T. Taj je vrh dodan u rješenje, a vrh k s drugog kraja brida stavlja se u P. Tada usporedimo, za svaki vrh i u T, težinu brida (i, k) sa težinom najtežeg brida od i do bilo kojeg vrha u P, te tada nađemo brid s najvećom težinom od svih lukova između T i P koji onda stavimo u rješenje. Vrh iz skupa T koji je incidentan s tim bridom postaje vrh k; dodaje se u skup P i proces se nastavlja. Dakle, ovako glasi Primov algoritam:

Algoritam za maksimalno razapinjuće stablo (Prim)

Dan je povezan graf $G = (N, A)$, sa danim težinama w_{ij} za svaki brid $(i, j) \in A$.

1. korak
   - Postavi $i(j) = 1$ i $u_j = w_{1j}$, za $j = 2, 3, \ldots, n$.
   - Postavi $P = \{1\}$, $T = \{2, 3, \ldots, n\}$.
   - $S = \emptyset$

2. korak Nađi $k \in T$, gdje je $u_k = \max(u_j : j \in T)$
   - Postavi $T = T - k$, $P = P + k$
   - Postavi $S = S + (i(k), k)$
   - Ako je $T = \emptyset$, stop. Bridovi u S tvore maksimalno razapinjuće stablo.

3. korak Za svaki $j \in T$, ako je $w_{kj} > u_j$, postavi $u_j = w_{kj}$ i $i(j) = k$. Idi na korak 1.

Vidimo da Primov algoritam, za razliku od Kruskalova algoritma, u svakom koraku ima povezan graf, što je intuitivniji i korisniji pristup s obzirom na prirodu problema.

4 Dualnost matroida

Ideja dualnosti važan je koncept i u linearnoj algebri i u teoriji grafova, pa tako i u teoriji matroida.

Definicija 4.1. *Neka je M matroid definiran na skupu E. Tada je* ***dualni matroid*** *M^* matroid s istim skupom E takav da vrijedi*

$$\mathscr{B}(M^*) = \{E - B : B \in \mathscr{B}(M)\}.$$

Vidimo da smo dualni matroid definirali na istom skupu, ali smo za njegove baze uzeli komplemente baza početnog matroida. No, moramo pokazati da je dualni matroid uistinu matroid - to jest, moramo pokazati da komplementi baza također zadovoljavaju aksiome $(B1) - (B3)$.
Kako bismo to dokazali, koristit ćemo tzv. jaku varijantu aksioma $(B3)$:

Lema 4.2. *Pretpostavimo da familija $\mathscr{B}$ zadovoljava:*

(B1) $\emptyset \neq \mathscr{B}$

(B2') *Ako su B_1, $B_2 \in \mathscr{B}$, tada je $|B_1| = |B_2|$.*

(B3') *Ako su B_1, $B_2 \subseteq \mathscr{B}$ i postoji element $x \in B_1 - B_2$, tada postoji element $y \in B_2 - B_1$ takav da je $(B_1 - x) \cup \{y\} \in \mathscr{B}$ i $(B_2 - y) \cup \{x\} \in \mathscr{B}$.*

Tada je $\mathscr{B}$ familija baza matroida.

Teorem 4.3. *Neka je M matroid s bazama $\mathscr{B}$. Tada su $\{E - B : B \in \mathscr{B}\}$ također baze nekog matroida.*

Dokaz. Označimo $\mathscr{B}^* := \{E - B : B \in \mathscr{B}\}$. Dokazat ćemo da $\mathscr{B}$ zadovoljava aksiome $(B1)$, $(B2')$ i $(B3')$ pa će po prethodnoj lemi dokaz biti gotov.

Provjera da dual zadovoljava aksiom $(B1)$ prilično je očita - budući da je M matroid, postoji baza $B \in \mathscr{B}$ pa postoji i komplement $E - B \in \mathscr{B}^*$. Aksiom $(B2')$ isto lagano slijedi: svaka baza ima $r(M)$ elemenata, pa svaki komplement baze ima $|E| - r(M)$ elemenata, dakle, $\mathscr{B}^*$ zadovoljava $(B2')$ zato što ga $\mathscr{B}$ zadovoljava.

Preostaje nam provjera trećeg aksioma $(B3)$. Neka su $B_1^c = E - B_1$ i $B_2^c = E - B_2$ dva bazna komplementa, gdje su $B_1, B_2 \in \mathscr{B}$. Neka je $x \in B_1^c - B_2^c$; mi sada moramo pronaći $y \in B_2^c$ tako da su oba skupa $(B_1^c - x) \cup y$ i $(B_2^c - y) \cup x$ u $\mathscr{B}^*$.

Ideja kako to pokazati jest uzeti komplement kako bismo mogli iskoristiti aksiom $(B3')$ na matroidu M, na kojem znamo da vrijedi, pa ponovno uzeti komplement. Neka je $x \in B_1^c$. Vratimo li se u termine originalnih baza, imamo tvrdnje da $x \notin B_1$ i $x \in B_2$. Sada upotrebljavajući $(B3')$ na matroidu M, imamo element $y \in B_1$ tako da su i $(B_1 \cup x) - y$ i $(B_2 \cup y) - x$ baze od M. No, u terminima komplemenata sada imamo da su i $((B_1 \cup x) - y)^c$ i $((B_2 \cup y) - x)^c$ u $\mathscr{B}^*$. No, $((B_1 \cup x) - y)^c = (B_1^c \cup y) - x$ i $((B_2 \cup y) - x)^c = (B_2^c \cup x) - y$ čime je dokaz gotov.

□

Sada ćemo navesti nekoliko jednostavnih rezultata koji slijede iz prethodnog teorema.

Propozicija 4.4. $r(M) + r(M^*) = |E|$.

Dokaz. Budući da je $r(M)$ veličina baze od M, imamo $r(M) + r(M^*) = r(M) + |E| - r(M) = |E|$. □

Propozicija 4.5. $(M^*)^* = M$.

Dokaz. Slijedi iz činjenice da za bilo koji skup S vrijedi $(S^c)^c = S$. □

Teorem 4.6. $r^*(A) = r(E - A) + |A| - r(M)$.

Dokaz. Rang od A u M^* određen je bazom od M s minimalnim brojem elemenata u A. Maksimalni kardinalitet nezavisnog skupa od M, disjunktnog sa A, jest $r(E - A)$. Takav je skup sadržan u bazi sa $r(M)$ elemenata, od kojih je njih $r(M) - r(E - A)$ sadržano u A. Dakle, broj elemenata od A koji nisu sadržani u ovoj bazi jest $r(E - A) + |A| - r(M)$. □

Kako smo se najviše i bavili matričnim i grafnim matroidima, možemo se zapitati što bi bio njihov dual - to jest, je li npr. dual matričnog matroida opet matrični matroid? Odgovor na to pitanje je da; može se pokazati da je matrica dualnog matroida od $M(A)$ zapravo matrica sastavljena od baze nulprostora matrice A.

Priča s grafnim matroidima malo je drukčija. S obzirom na to da se u teoriji grafova dualni grafovi definiraju samo za planarne grafove, moglo se i naslutiti da će dual grafnog matroida biti grafni matroid ako je polazni graf planaran.

Obe tvrdnje nadilaze obuhvat rada te se dokazi mogu pronaći u [2].

4.1 Operacije nad matroidima

Na različite smo načine definirali matroide i oprimjerili ih. Sada se pitamo kako možemo od postojećih matroida napraviti nove. Prikazat ćemo dvije operacije na matroidima i njihov dualni odnos.

Definicija 4.7. *Neka je $M = (E, \mathscr{I})$ matroid.*

- ***Brisanje.*** *Za svaki $e \in E$ koji se ne nalazi u svim bazama, matroid* ***M-{e}*** *definiran je sa skupom $E - \{e\}$ i pripadnim nezavisnim skupovima od $\mathscr{I}$ koji ne sadrže e.*

- ***Kontrakcija.*** *Za svaki $e \in E$ koji se nalazi barem u jednoj bazi, matroid* ***M/e*** *definiran je sa skupom $E - \{e\}$ i pripadnim nezavisnim skupovima koji su formirani na način da od svih elemenata od $\mathscr{I}$ koji sadrže e, izbacimo e iz svakog takvog skupa.*

U duhu ove dvije definicije, korisno je particionirati nezavisne skupove matroida M u dvije familije: one nezavisne skupove koji sadrže e i one koji ne sadrže. One redom postaju nezavisni skupovi od $M - e$ te nezavisni skupovi od M/e (nakon što izbacimo e iz takvih skupova).

Također, svaku od ovih operacija možemo primijeniti više puta. Matroid dobiven brisanjem elemenata iz skupa $Z = E - Y$ ima smisla onda označiti sa $M - Z$, ali i sa $M|Y$, što interpretiramo kao matroid M restringiran na skup Y. Analogno za kontrakciju, sa M/Z označujemo kontrakciju matroida M sa skupom Z, i uvodimo oznaku $M \cdot Y := M/Z$.

Sada je potrebno dokazati da brisanje i kontrakcija matroida uistinu za rezultat daju matroid:

Teorem 4.8. *$M - e$ i M/e su matroidi.*

Dokaz. Prvo dokažimo tvrdnju za $M - e$. Neka se e ne nalazi u svim bazama. Neka je $\mathscr{I}_1$ familija svih nezavisnih skupova koji ne sadrže e. Trebamo dokazati da je $(E - \{e\}, \mathscr{I}_1)$ matroid. $(I1)$ je zadovoljen jer je $\emptyset \in \mathscr{I}$, a kako ne sadrži e, nalazi se u $\mathscr{I}_1$. Kako je $\mathscr{I}_1 \subset \mathscr{I}$, $(I2)$ i $(I3)$ trivijalno slijede.

Sada dokažimo da je $(E - \{e\}, \mathscr{I}_2)$ matroid. Neka je e element koji se nalazi u barem jednoj bazi te neka je $\mathscr{I}_2$ familija svih nezavisnih skupova koji sadrže e, iz kojih smo izbacili element e. $(I1)$ je zadovoljen jer ako je e sadržan u barem jednoj bazi matroida M, zbog $(I2)$ na matroidu M, skup $\{e\}$ jest sadržan u $\mathscr{I}$. Tada ćemo u familiji $\mathscr{I}_2$ biti sadržan $\{e\} - \{e\} = \emptyset$. Kako su u $\mathscr{I}_2$ svi skupovi koji su $\mathscr{I}$ imali element e, izbacivanje tog elementa neće utjecati na svojstva $(I2)$ i $(I3)$ naslijeđena od matroida M.

□

Sada opravdajmo restrikciju elemenata s kojima radimo operacije. Što bi se dogodilo kada bi izbrisali element e koji se nalazi u svakoj bazi? U dokazu nismo nigdje koristili tu pretpostavku, ali kada sa nezavisnih skupova prijeđemo na baze, dolazi do problema: primijetimo da su baze od $M - e$ upravo one baze od M koje ne sadrže e. Kada bismo dakle izbrisali element e, matroid $M - e$ po toj tvrdnji ne bi imao niti jednu bazu, što je kontradikcija sa $(B1)$. Također možemo primijetiti da vrijedi $r(M) = r(M - e)$, a kada bismo izbrisali element e koji se nalazi u svakoj bazi, jednakost ne bi vrijedila jer bi se rang novonastalog matroida strogo smanjio.

A kada bismo kontrahirali elementom e koji se ne nalazi niti u jednoj bazi, tada bi $\emptyset$ bio zavisan skup što je kontradikcija sa $(I1)$, a to je vidljivo i u dokazu prethodnog teorema. Analogno primijetimo da su baze od M/e one dobivene na način da smo od svih baza od M koje sadrže e skupovno oduzeli e.

Primjer 4.9. *Neka je M matroid na skupu $E = \{a, b, c, d\}$ i neka je $\mathscr{I} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}\}$. Vidimo da su baze matroida $\mathscr{B} = \{\{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}\}$. Pronađimo nezavisne skupove i baze ako izbrišemo i kontrahiramo $e = a$. Primijetimo da a nije sadržan u svim bazama, ali je sadržan u barem jednoj pa su obje operacije dobro definirane.*

- *Za $M - a$ nezavisni su skupovi oni nezavisni skupovi od M koji ne sadrže a. To su: $\{\emptyset, \{b\}, \{c\}, \{d\}, \{b, c\}, \{b, d\}\}$. Nadalje, baze su $\{b, c\}$ i $\{b, d\}$.*

- *Za M/a, nezavisni su skupovi $\{\emptyset, \{b\}, \{d\}\}$. Njih smo dobili tako da smo od nezavisnih skupova koji sadrže a (skupovno) oduzeli a. Baze su, naravno, $\{b\}$ i $\{d\}$.*

Primijetimo da vrijedi tvrdnja da ove operacije dijele $\mathscr{B}$ u dvije familije, točno na isti način kako dijele i familiju $\mathscr{I}$

Pokažimo sada dualnost ovih dviju operacija.

Teorem 4.10. *Neka je M matroid na skupu E te $e \in E$.*

(1) Ako e nije sadržan ni u jednoj bazi, tada je $(M - e)^* = M^*/e$.

(2) Ako je e sadržan u barem jednoj bazi, tada je $(M/e)^* = M^* - e$.

Dokaz. Dokažimo prvu tvrdnju. Pretpostavimo da je B baza za $(M - e)^*$. Tada vrijedi $B \subseteq (E - \{e\})$ i $(E - \{e\}) - B$ je baza za $M - e$. To znači da je $(E - \{e\}) - B$ također baza i za M, pa je njezin komplement baza za M^*:

$E - ((E - \{e\}) - B)$ je baza za M^*. Ali, $E - ((E - \{e\}) - B) = B \cup \{e\}$. Dakle, $B \cup \{e\}$ je baza za M^*, pa je B baza za M^*/e.

Sada smo pokazali da ako je B baza za $(M - e)^*$, tada je B također baza za M^*/e. Obratna tvrdnja slijedi iz iste argumentacije počevši od kraja prema početku, budući da za sve gornje implikacije vrijedi ekvivalencija. Time je dokazana prva tvrdnja.

Drugu ćemo tvrdnju dokazati pomoću prve tvrdnje. Kako bismo dokazali da je $M^* - e = (M/e)^*$, neka je $N = M^*$, te primijenimo *(1)* na N: $(N - e)^* = N^*/e$. Sada uzmemo dual te jednakosti:

$$((N - e)^*)^* = (N^*/e)^*.$$

Sada zamijenimo N sa M^* i primijenimo propoziciju 4.5. dvaput:

$$M^* - e = (M/e)^*.$$

$\square$

5 Algoritam plavog pravila i crvenog pravila

U trećem smo poglavlju uveli problem minimalnog (tj. maksimalnog) razapinjućeg stabla u težinskom grafu te dali dvije varijante pohlepnog algoritma za njegovo rješavanje. Sada ćemo prezentirati algoritam *plavog pravila i crvenog pravila*, koji je poopćenje skoro svih algoritama za rješavanje danog problema.

Neka je $G = (V, E)$ neusmjereni povezani težinski graf. Promotrimo ova dva pravila za bojanje bridova grafa G:

- **Plavo pravilo:** Pronađi *rez* (particija skupa V u dva skupa X i $V - X$) takav da niti jedan plavi brid ne spaja X i $V - X$. Izaberi neobojani brid minimalne težine između X i $V - X$ te ga oboji u plavo.
- **Crveno pravilo:** Pronađi ciklus koji ne sadrži niti jedan crveni brid. Izaberi neobojani brid maksimalne težine u tom ciklusu i oboji ga crveno.

Cilj nam je dokazati sljedeću tvrdnju:

Teorem 5.1. *Uzmemo li (neobojani) graf te zatim primjenjujemo crveno ili plavo pravilo u proizvoljnom redoslijedu, dokle god ih možemo primijeniti, konačan skup plavih bridova daje minimalno razapinjuće stablo.*

Naravno, ideja kako da ovo dokažemo jest da preformuliramo problem u matroidnim terminima te iskoristimo razvijenu teoriju. Pojam ciklusa u matroidima već smo definirali i to je upravo ciklus u grafnom matroidu. Definirajmo **rez u matroidu** kao zatvorene skupove ranga $r(M) - 1$. To jest, to su maksimalni zatvoreni skupovi koji nisu cijeli matroid. Primijetimo da rezove matroida možemo protumačiti kao minimalni (u smislu skupovne inkluzije) skup čiji presjek s bilo kojom bazom nije prazan skup. No, rez u matroidu i rez u grafu nisu potpuno ekvivalentni pojmovi: rez u grafnom matroidu predstavlja sve minimalne rezove u grafu koje svako razapinjuće stablo mora preći. No, ta je razlika zanemariva u kontekstu plavog pravila.

Sada možemo preformulirati pravila u terminima matroida:

- **Plavo pravilo:** Pronađi rez u matroidu bez ijednog plavog elementa. Izaberi neobojani element minimalne težine tog reza i oboji ga plavo.
- **Crveno pravilo:** Pronađi ciklus koji ne sadrži niti jedan crveni brid. Izaberi neobojani element maksimalne težine u tom ciklusu i oboji ga crveno.

Sada ćemo pomoću dualne teorije matroida dokazati dualnu prirodu između plavog i crvenog pravila:

Teorem 5.2. *Rezovi u matroidu M su ciklusi u M^*. Ekvivalentno, ciklusi u M su rezovi u M^*.*

Dokaz. Pretpostavimo da je C ciklus u M, to znači da je on minimalni zavisni skup u M što je ekvivalentnto s tvrdnjom da je C minimalan skup koji nije sadržan ni u jednoj bazi od M. Sada vidimo da je $E - C$ maksimalan skup koji ne sadrži niti jedan komplement baze. No, takav je skup nužno i rez jer je očito zatvoren i ranga $r(M^*) - 1$ (jer u suprotnom ne bi bio maksimalan). Dakle, $E - C$ je rez u M^*.

□

Korolar 5.3. *Plavo pravilo u matroidu M s težinama w jest crveno pravilo u matroidu M^* s težinama $-w$.*

Sada ćemo se usmjeriti na dokazivanje ispravnosti plavog i crvenog pravila na proizvoljnim matroidima.

Definicija 5.4. *Neka je $M = (E, \mathscr{I})$ matroid s pripadajućim dualom $M^* = (E, \mathscr{I}^*)$.* ***Prihvatljivo bojanje*** *je par disjunktnih skupova $B \in \mathscr{I}$ (plavi elementi) i $R \in \mathscr{I}^*$ (crveni elementi). Prihvatljivo bojanje B, R je* ***totalno*** *ako vrijedi $B \cup R = E$, tj. ako je B baza za M i R baza za M^*. Prihvatljivo bojanje B', R' je* ***proširenje*** *prihvatljivog bojanja B, R ako vrijedi $B \subseteq B'$ i $R \subseteq R'$.*

Lema 5.5. *Svako prihvatljivo bojanje ima totalno prihvatljivo proširenje.*

Dokaz. Neka su B, R prihvatljiva bojanja. Neka je U^* maksimalni element od $\mathscr{I}^*$ koji je proširenje od R, i neka je $U = E - U^*$. Tada je U maksimalni element od $\mathscr{I}$ disjunktan s R. Dokle god vrijedi $|B| < |U|$, uzmi elemente iz U i dodaj ih u B tako da se zadrži nezavisnost. Neka je $\hat{B}$ konačan takav skup. Budući da svi maksimalni nezavisni skupovi imaju istu kardinalnost, $\hat{B}$ je maksimalni element od $\mathscr{I}$ koji je disjunktan sa R i sadrži B. Traženo je proširenje $\hat{B}, E - \hat{B}$. □

Lema 5.6. *Presjek ciklusa i reza ne može biti jedan element.*

Dokaz. Neka je C rez, a D ciklus i pretpostavimo da je $C \cap D = \{x\}$. Tada je $D - \{x\}$ nezavisan i $C - \{x\}$ je nezavisan u dualu. Obojimo $D - \{x\}$ plavom, a $C - \{x\}$ crvenom bojom. Po prethodnoj lemi, ovo bojanje ima proširenje koje je totalno prihvatljivo bojanje. No, ovisno o boji elementa x, ili je C cijeli crveni ili je D cijeli plavi. No, to je nemoguće u prihvatljivom bojanju, budući da je D zavisan i C je zavisan u dualu. □

Pretpostavimo da je B nezavisan, a $B \cup \{x\}$ zavisan. Tada je $B \cup \{x\}$ najmanji zavisni skup, to jest ciklus, koji zovemo **fundamentalni ciklus** od x i B. To uistinu jest ciklus jer je B nezavisan skup.

Lema 5.7. *Neka je B, R totalno prihvatljivo bojanje. Tada vrijede sljedeće tvrdnje:*

(i) Neka je $x \in R$ i neka y leži na fundamentalnom ciklusu od x i B. Ako se zamijene boje od x i y, novodobiveno bojanje je također prihvatljivo.

(ii) Neka je $y \in B$ i neka x leži na fundamentalnom rezu od x i R (tj. na fundamentalnom ciklusu dualnog matroida). Ako se zamijene boje od x i y, novodobiveno bojanje je također prihvatljivo.

Dokaz. Zbog dualnosti, potrebno je dokazati samo tvrdnju (i). Neka je C fundamentalni ciklus od x i B i neka $y \in C$. Ako je $x = y$, nemamo što dokazivati. U suprotnom, neka je $y \in B$. Tada je $C - \{y\}$ nezavisan budući da je C minimalan. Sada proširujemo skup $C - \{y\}$ elementima iz B kao u lemi 5.5. sve dok ne dobijemo bazu B'. Tada je $B' = (B - \{y\}) \cup \{x\}$ i totalno prihvatljivo bojanje $B', S - B'$ je dobiveno od B, R zamjenom boja od x i y. □

Totalno prihvatljivo bojanje B, R zovemo **optimalnim** ako je B minimalne težine među bazama; ekvivalentno, ono je optimalno ako je R maksimalne težine među dualnim bazama.

Lema 5.8. *Ako prihvatljivo bojanje ima optimalno totalno proširenje prije izvršenja plavog ili crvenog pravila, tada ima i nakon izvršenja nekog od pravila.*

Dokaz. Dokazat ćemo lemu ako primjenjujemo plavo pravilo. Tvrdnja za crveno pravilo slijedi iz dualnosti. Neka je B, R prihvatljivo bojanje s optimalnim totalnim proširenjem $\hat{B}, \hat{R}$. Neka je A rez koji ne sadrži plave element, i neka je x neobojani element od A najmanje težine. Ako je $x \in \hat{B}$, tada smo gotovi pa pretpostavimo da je $x \in \hat{R}$. Neka je C fundamentalni ciklus od x i $\hat{B}$. Po lemi 5.6. $A \cap C$ mora sadržavati barem još jedan element uz x, recimo y. Tada je $y \in \hat{B}$ i $y \notin B$ jer nema plavih elemenata u A. Po lemi 5.7., boje od x i y u $\hat{B}, \hat{R}$ mogu se zamijeniti kako bi se postiglo totalno prihvatljivo bojanje $\hat{B}', \hat{R}'$ koje je proširenje od $B \cup \{x\}, R$. Također, $\hat{B}'$ je i minimalne težine jer težina od x sigurno nije veća od težine od y. □

Lema 5.9. *Ako prihvatljivo bojanje nije totalno, tada je plavo ili crveno pravilo primjenjivo*

Dokaz. Neka su B, R prihvatljiva bojanja s neobojenim elementom x. Po lemi 5.6., bojanje B, R ima totalno proširenje $\hat{B}, \hat{R}$. Zbog dualnosti, bez smanjenja općenitosti možemo pretpostaviti da je $x \in \hat{B}$. Neka je C fundamentalni rez od x i $\hat{R}$. Budući da su svi elementi iz C osim x u $\hat{R}$, nijedan od njih nije plav u B. Dakle, plavo je pravilo primjenjivo. □

Kada iskombiniramo zadnje dvije leme dobijemo dokaz tražene tvrdnje:

Teorem 5.10. *Ako počnemo s neobojenim težinskim matroidom i primijenimo plavo ili crveno pravilo u bilo kojem rasporedu sve dok su primjenjivi, tada je konačno bojanje optimalno totalno prihvatljivo bojanje.*

Ono što je zapravo u pozadini ovog teorema jest da podskupovi baza minimalnih težina tvore podmatroid, a plavo pravilo predstavlja pohlepni algoritam koji nam na kraju daje bazu minimalne težine.

Sada možemo reformulirati Primov algoritam u terminima plavog i crvenog pravila: uzmimo bilo koji vrh v te ga stavimo u skup B. Sve dok možemo, primjenjujemo plavo pravilo na rez induciran skupom B.

Za tumačenje Kruskalova algoritma, uzmimo brid e. Ako su oba incidentna vrha od brida e u istom plavom stablu, oboji e crvenom bojom primjenjujući crveno pravilo na taj ciklus. Ako nisu, oboji brid e plavom bojom primjenjujući plavo pravilo na rez koji se sastoji od vrhova plavog stabla jednog od incidentnih vrhova.

6 Presjek matroida

Vidjeli smo da pohlepni algoritam rješava problem maksimalnog nezavisnog skupa danog matroida, što ima brojne primjene u optimizaciji. No s druge strane, pohlepni algoritam ne nalazi optimalno rješenje za mnoge druge optimizacijske probleme, što implicira ograničenje koristi matroida.

No, u ovom ćemo poglavlju pokazati da nije nužno tako - uvodeći pojam *presjeka* matroida, proširit ćemo i spektar primjenjivih problema, za koje ćemo pokazati da su specijalni slučajevi razvijene teorije.

Definicija 6.1. *Neka su $M_1 = (E, \mathscr{I}_2)$ i $M_2 = (E, \mathscr{I}_2)$ dva matroida definirana na istom skupu E.* ***Presjek matroida*** *M_1 i M_2 definiramo kao*

$$M_1 \cap M_2 = (E, \mathscr{I}_1 \cap \mathscr{I}_2).$$

Cilj ovog poglavlja jest dati algoritam za pronalaženje skupa $I \in \mathscr{I}_1 \cap \mathscr{I}_2$ koji je nezavisan u oba matroida, a $|I|$ maksimalan. Ovom problemu trebamo pristupiti drukčije nego ranije, zbog ključnog razloga što presjek matroida nije nužno matroid:

Primjer 6.2. *Neka su $M_1 = (E, \{\{\emptyset\}, \{a,b,c\}, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}\})$ i $M_2 = (E, \{\{\emptyset\}, \{a,b,c\}, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}\})$ dva matroida gdje je $E = \{a,b,c\}$. Njihov je presjek tada $M_1 \cap M_2 = (E, \{\{a,b,c\}, \{\{a\}, \{b\}, \{c\}, \{a,b\}\})$. Pokažimo da presjek ne zadovoljava $(I3)$.*

Uzmimo $I = \{c\}$ i $J = \{a,b\}$. Tada je $J - I = \{a,b\}$. Sada bi po $(I3)$ trebao postojati element e iz $J - I$ takav da je $\{c\} \cup \{e\}$ nezavisan skup. No, niti $\{a,c\}$ niti $\{b,c\}$ nisu u nezavisnom skupu presjeka pa presjek nije matroid.

Teorem 6.3. *Neka su $M_1 = (E, \mathscr{I}_1)$ i $M_2 = (E, \mathscr{I}_2)$ dva matroida, sa rangovima redom r_1 i r_2. Tada vrijedi:*

$$\max_{I \in \mathscr{I}_1 \cap \mathscr{I}_2}(|I|) = \min_{U \subseteq E}(r_1(U) + r_2(E - U))$$

Dokaz. Neka je $k = \min_{U \subseteq E}(r_1(U) + r_2(E - U))$. Vidimo da maksimalni element presjeka ne može biti veći od k, budući da za bilo koji zajednički nezavisni skup I i i bilo koji $U \subseteq E$ vrijedi:

$$|I| = |I \cap U| + |I - U| \leq r_1(U) + r_2(E - U).$$

Jednakost ćemo sada dokazati indukcijom po kardinalnosti skupa E. Kako je za $|E| = 1$ slučaj trivijalan, pretpostavimo da je $|E| > 1$.

Ako se minimum postiže za $U = E$ ili $U = \emptyset$, uzmimo $e \in E$. Tada je $r_1(U) + r_2(E - (U \cup \{e\})) \geq k$ za svaki $U \subseteq E - \{e\}$, jer bi u suprotnom i U i $U \cup \{e\}$ postigli minimum implicirajući $\{U, U \cup \{e\}\} = \{\emptyset, E\}$, što je kontradikcija sa $|E| > 1$. Dakle, indukcijom, $M_1 - e$ i $M_2 - e$ imaju zajednički nezavisni skup veličine k, što dokazuje teorem.

Sada možemo pretpostaviti da se minimum postiže za neki U, $\emptyset \neq U \neq E$. Tada $M_1|U$ i $M_2 \cdot U$ imaju zajednički nezavisni skup I veličine $r_1(U)$. To vrijedi jer bi u suprotnom, po indukciji, postojao podskup $T \subseteq U$ za koji bi vrijedilo

$$r_1(U) > r_{M_1|U}(T) + r_{M_2 \cdot U}(U - T) = r_1(T) + r_2(E - T) - r_2(E - U)$$

što je kontradikcija sa tvrdnjom da U postiže minimum. Analogno vrijedi da $M_1 \cdot (E - U)$ i $M_2|(E - U)$ imaju nezavisni zajednički skup J veličine $r_2(E - U)$.

Sada imamo skup $I \cup J$ koji je nezavisni zajednički skup i od M_1 i od M_2: $I \cup J$ je nezavisan u M_1 jer je I nezavisan u $M_1|U$, a J je nezavisan budući da vrijedi $M_1 \cdot (E - U) = M_1/U$. Analogno se dokaže nezavisnost i u M_2. Kako je $|I \cup J| = r_1(U) + r_2(E - U)$, time smo dokazali teorem.

$\square$

6.1 Kőnigov teorem

Neka je $G = (V, E)$ bipartitni graf s particijom A i B. Particionirajmo skup bridova $E = \cup\{\delta(v) : v \in A\}$, gdje $\delta(v)$ označava bridove incidentne s vrhom v. To stvarno jest particija budući da svi bridovi imaju točno jedan incidentan vrh u skupu A. Sada definirajmo skup bridova nezavisnim ako ima najviše jedan brid incidentan sa svakim vrhom iz A. Primijetimo da familiju takvih skupova možemo zapisati ovako:

$$\mathscr{I}_A = \{F : |F \cap \delta(v)| \leq 1, \forall v \in A\}.$$

Primijetimo da smo upravo definirali particijski matroid $M_A = (E, \mathscr{I}_A)$ za $k_i = 1$. Sada analogno definiramo particijski matroid $M_B = (E, \mathscr{I}_B)$ gdje je

$$\mathscr{I}_B = \{F : |F \cap \delta(v)| \leq 1, \forall v \in B\}.$$

Pogledajmo koja bi bila interpretacija skupa $F \in (\mathscr{I}_A \cap \mathscr{I}_B)$. Ako uzmemo skup bridova F za koji vrijedi da ne postoje dva brida koja su incidentna s istom vrhom ni u A ni u B, dobit ćemo skup bridova koji međusobno nemaju niti jedan zajednički vrh (jer A i B čine particiju vrhova), što smo ranije definirali kao sparivanje u bipartitnom grafu.

U teoriji grafova dobro je poznat problem pronalaska maksimalnog sparivanja (u bipartitnom grafu), a mi ga sada možemo protumačiti kao problem pronalaska maksimalnog nezavisnog skupa presjeka dvaju particijskih matroida. Konačno, možemo upotrijebiti teorem 6.3. i protumačiti ga u terminima teorije grafova:

Teorem 6.4. *U bilo kojem bipartitnom grafu, broj bridova u maksimalnom sparivanju jednak je broju vrhova u minimalnom pokrivanju.*

Treba još samo argumentirati zašto je desna strana teorema 6.3. sparivanje; no, to je očito jer su vrhovi iz A pokriveni sa U, a vrhovi iz B sa $E - U$.

Literatura

[1] E. L. Lawler, *Combinatorial optimization: Networks and Matroids*, Saunders College Publishing, SAD, 1976.

[2] G. Gordon, J. McNulty, *Matroids: A Geometric Introduction*, Cambridge University Press, Cambridge, 2012.

[3] A.Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, Springer, 2004.

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

Sažetak

U ovom smo radu izložili osnove teorije matroida s naglaskom na primjene u optimizaciji. Pokazali smo da je matroid, struktura utemeljena na apstrahiranom pojmu nezavisnosti, prirodna struktura u pozadini pohlepnog algoritma. Dokazavši da je svaka matrica i graf matroid, definirali smo neke optimizacijske probleme u terminima teorije matroida te ih riješili koristeći odgovarajuće varijante pohlepnog algoritma. Nadalje, koristivši dualnu teoriju matroida, definirali smo algoritam plavog pravila i crvenog pravila, apstrahiranu varijantu mnogih pohlepnih algoritama, naročito koristan u teoriji grafova. Na kraju smo uveli pojam presjeka matroida te ga protumačili u terminima teorije grafova te dokazali Kőnigov teorem.

Summary

In this thesis we introduced the basics of theory of matroids with emphasis on its application in optimization. We showed that a matroid, a structure based on an abstract notion of independence, is the natural structure behind the greedy algorithm. By showing that every matrix and graph is a matroid, we were able to define some optimization problems in terms of matroid theory and solve them by using appropriate variants of the greedy algorithm. Furthermore, by using duality theory in matroids, we defined the blue rule - red rule algorithm, an abstract variant of many greedy algorithms, especially useful in graph theory. To conclude, we introduced matroid intersection and described it in terms of graph theory and proved Kőnig's theorem.

Životopis

Nikola Badrov rođen je 27. veljače 1993. godine u Splitu. Nakon završene Osnovne škole Ostrog u Kaštelima, upisuje V. gimnaziju Vladimir Nazor, u kojoj sve razrede završava s izvrsnim uspjehom. Godine 2011. upisuje Prirodoslovno - matematički fakultet u Zagrebu, smjer Matematika, na kojem 2014. stječe akademsku titulu sveučilišnog prvostupnika matematike. Te godine na istom fakultetu upisuje diplomski studij smjer Financijska i poslovna matematika. Tijekom studija, također je bio aktivan u veslačkoj sekciji fakulteta.