Mreže

Filip Koprivec, Samo Kralj

April 2016

Kazalo

1 Uvod

Mreža je množica z dodatno strukturo (delno urejenostjo), ki zadošča poguju, da ima poljuben par elementov infimum in supremum. Najprej si bomo pogledali mreže s stališča matematične logike in urejenosti, kasneje pa si jih bomo ogledali še s stališča algebraičnih operacij nad njimi, ter pokazali, zakaj sta ta dva pogleda ekvivalentna.

1.1 Osnovne definicije

Definicija 1: Naj bo $\mathcal{L}$ množica, relacija $\leq$ je **(šibka) delna urejenost**, če je

- refleksivna ($a \leq a$)
- antisimetrična ($a \leq b \wedge b \leq a \implies a = b$)
- tranzitivna ($a \leq b \wedge b \leq c \implies a \leq c$)

Pišemo a je manjši ali enak b, občasno tudi a je pod b.

Opomba: Zgolj iz preprostosti definiramo še drugo relacijo $a \geq b \iff b \leq a$, ki je očitno tudi delna urejenost.

Opomba: Poznamo tudi **strogo delno urejenost**, ki jo definiramo kot $a < b \iff a \leq b \wedge a \neq b$

Primer:
Tipičen primer delne urejenosti je kar sama motivacija za vpeljavo relacije. Vzemimo množico realnih števil $\mathbb{R}$ in na njej relacijo $\leq$, za katero preprosto preverimo da je delna urejenost.

Trditev 1: Relacija deljivosti ($|$) na množici $\mathbb{N}$ je delna urejenost.

Dokaz. Preverili bomo da ta relacija zadošča vsem zahtevam. Spomnimo se, da a deli b natanko tedaj, kadar obstaja tako celo število k, da zadosti enakosti $b = ka$, oziroma $a \mid b \iff \exists k \in \mathbb{Z}.\ b = ka$.

- Refleksivnost: $a = 1 * a$, torej $a \mid a$
- Antisimetričnost: $a \mid b \implies b = k_1 a$, $b \mid a \implies a = k_2 b$, vstavimo a v prvo enakost in dobimo $b = k_1 k_2 b$, torej $k_1 = k_2^{-1}$, torej $k_1 = k_2 = 1$ in dobimo $b = a$
- Tranzitivnost: $a \mid b \wedge b \mid c \implies a \mid c$, vemo torej $b = k_1 a$ in $c = k_2 b$, vstavimo prvo enakost v drugo in dobimo $c = \underbrace{k_2 k_1}_{\in \mathbb{Z}} a$ torej $a \mid c$.

□

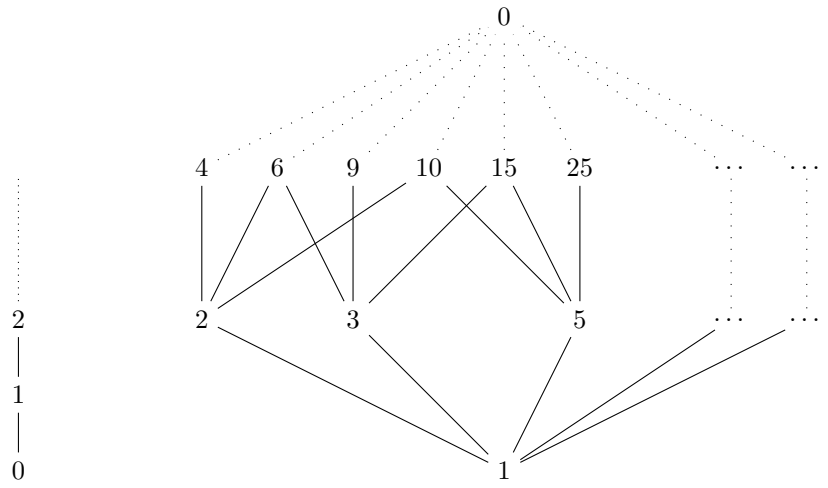
Opomba: Preprosto preverimo, da je za poljubno množico $\mathcal{A}$, relacija $\subseteq$ delna urejenost na potenčni množici množice $\mathcal{A}$ ($P(\mathcal{A})$).

Definicija 2: Množica $\mathcal{L}$ je **linearno urejena**, če za poljubna x, y velja $x \leq y$ ali $y \leq x$

Primer:
Množica $\mathbb{N}$ z urejenostjo $\leq$ je linearno urejena, saj za poljubna x in y velja $x \leq y \vee y \leq x$, če pa velja $x = y$, potem pa sta pravilna celo oba dela izjave. Množica $\mathbb{N}$ urejena glede na relacijo deljivosti pa **ni** linearno urejena, saj za recimo dve poljubni praštevilo velja $p_1 \nmid p_2 \wedge p_2 \nmid p_1$.
Opomba: Pridstavitem linearno urejenih množic s Hassejevim diagramom nas spominja na premico, od torej tudi izraz. To je lepo vidno na sliki (1a).
Za lepšo predstavo splošnih linearnih urejenih diagramov si pomagamo s Hassejevim diagramom, ki s pomočjo povezav med točkami prikaže relacije med njimi.

Definicija 3: Naj bo $\mathcal{L}$ delno urejena množica glede na neko relacijo, ki o označimo z $\leq$. Hassejev diagram je graf, katerega točke so elementi $\mathcal{L}$, med točkama x in y pa je povazava natnko tedaj, kadar velja:

$$x \leq y \wedge \nexists z \in \mathcal{L}.\ x \leq z \leq y$$



(a) $\mathbb{N}, \leq$ (b) Hassejev diagram za $(\mathbb{N}, |)$

Slika 1: Primer Hassejevih diagramov

1.2 Supremum in infimum

Definicija 4: S je **supremum** x in y, če velja:

- $S \geq x \wedge S \geq y$ (Zgornja meja)
- $\forall S' \in \mathcal{L} \implies (S' \geq x \wedge S' \geq y \implies S \leq S')$ (Je najmanjša zgornja meja)

Torej je S natačna zgornja meja x in y, če je njuna zgornja meja, hkrati pa je vsaka od S različna zgornja meja večja ali enaka S. Označimo: $S = x \vee y$.

Definicija 5: s je **infimum** x in y, če velja:

- $s \leq x \wedge s \leq y$ (Spodnja meja)
- $\forall s' \in \mathcal{L} \implies (s' \leq x \wedge s' \leq y \implies s' \leq s)$ (Je največja spodnja meja)

Torej je s natačna spodnja meja x in y, če je njuna spodnja meja, hkrati pa je vsaka od s različna zgornja meja manjša ali enaka s. Označimo: $s = x \wedge y$.

Opomba: V literaturi se za supremum občasno uporablja tudi oznaka $\cup$, za infimum pa $\cap$.
Primer:
1. Za množico $\mathbb{R}$, ki je urejena glede na $\leq$ in poljubni števili x, y velja: $x \vee y = max\{x, y\}$ in $x \wedge y = min\{x, y\}$.
2. Za množico $\mathbb{N}$, ki je urejena glede na relacijo deljivosti in poljubni števili x, y velja: $x \vee y = lcm\{x, y\}$ (najmanjši skupni večkratnik) in $x \wedge y = gcd\{x, y\}$ (največji skupni delitelj).

1.3 Definicija mreže

Definicija 6: Množica $\mathcal{L}$ je **mreža**, če za poljuben par x, y v $\mathcal{L}$ obstajata infimum in supremum.

Primer:
Naravna števila so mreža tako za urejenost glede na relacijo $\leq$, kot tudi za urejenost glede na relacijo deljivosti. To lahko lepo vidimo na sliki (1).

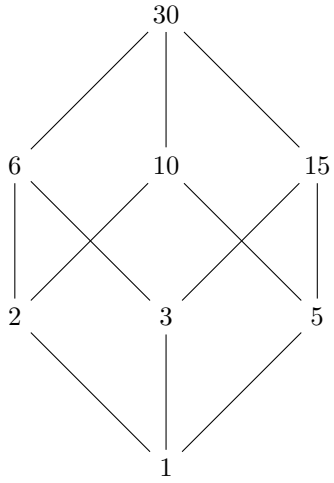
Definicija 7: Mreža $\mathcal{L}$ je polna, če za poljubno $\mathcal{A} \subseteq \mathcal{L}$ obstajata infimum in supremum za $\mathcal{A}$.

Primer:
Poljubna končna mreža je tudi polna mreža. Preprosto za infumum in supremum vzamemo infimum in supremum elementov po parih. Na podoben način pa dobimo mreže, ki niso polne. $\mathbb{R}, \leq$ ni polna, saj množica $\mathbb{N}$ nima niti infimuma niti supremuma.

2 Osnovni primeri mrež

Od prej se spomnimo, je poljubna podmnožica $\mathbb{R}$, urejena glede na relacijo $\leq$ mreža. Za poljubni števili x, y velja: $x \vee y = max\{x, y\}$ in $x \wedge y = min\{x, y\}$, seveda pa sta tako infimum kot supremum v mreži. Opazimo, da so te množice vedno liearno urejene.

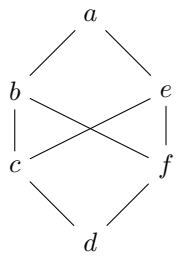
Množica naravnih števil pa nam poleg urejenosti z $\leq$ omogoča tudi ureditev



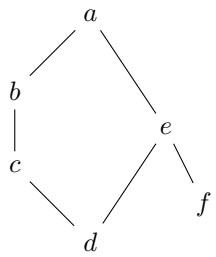
Slika 2: Mreža deliteljev števila 30 urejena glede na relacijo deljivosti

z |. V tem primeru dobimo Hassejev diagram iz slike (1b). Ta množica nima linearne ureditve, opazimo, pa da elementa 0 in 1 na nek način zaključujeta mrežo, saj so vsa naravna števila pod 0 (delijo 0), hkrati pa 1 deli vsa ostala naravna števila. S slike tudi lepo opazimo, da s v prvem nivoju urejenosti samo praštevila, v drugem nivoju urejenosti števila z natančno dvema deliteljema in v n-tem, nivoju ptevila z n delitelji.

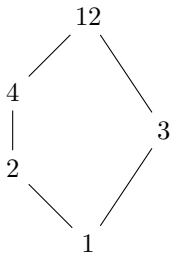
Opomba: Če v naravna števila vključimo tudi 0, potem formula za supremum in infimum glede na najmanjše skupne večkratnike in največje skupne delitelje ne deluje več kadar je eden izmed argumentov 0.
Pomembne mreže pa predstavljajo tudi mreže deliteljev posameznega naravnega števila. To lepo vidmo na sliki (2).
Delno urejene množice lahko predstavimo zgolj s Hassejevim diagramom. Poglejmo si nekaj množic, ki niso mreže in razložimo zakaj ne.



(a) Delno urejena množica, ki ni mreža



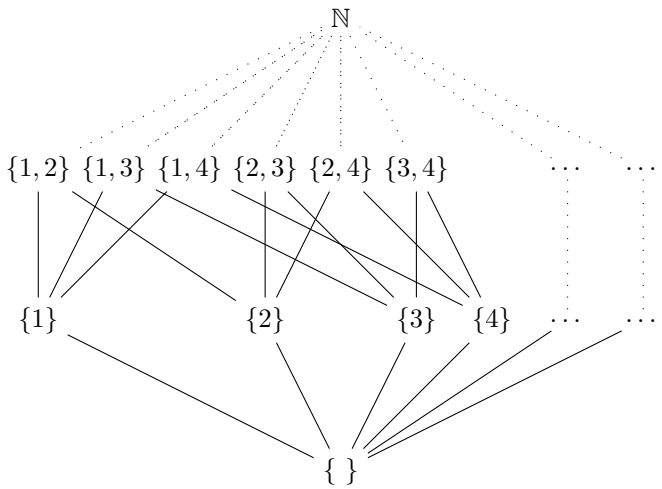
(b) $\{a, b, c, d, e, f\}$, ni mreža



(c) $(\{1, 2, 3, 4, 12\}, |)$, je mreža

Slika 3: Primer delno urejenih množic, ki niso mreže

Če si pogledamo sliko (3) lahko hitro vidimo, zakaj te množici nista mreži. Množica na sliki (3a) ni mreža, saj elementa c in f nimata natančno določenega supremuma. Vidimo, da bi to lahko bila tako element e kot tudi element b,



Slika 4: Hassejev diagram za $\mathcal{P}(\mathbb{N}), \subseteq$

vendar pa ju med samo ne moremo primerjati. Množica na sliki (3a) zato ni mreža. Bi pa postala mreža, če bi odstranili povezamo med c in e.

Če pa pogledamo sliko (3b) vidimo, da je problematičen element f. Tako recimo elementa $c \vee f = a$, medtem, ko je $c \wedge f$ nedoločen in zato množica ni mreža, bi pa to postala, če bi iz nje odstranili element f in tako dobili mrežo vseh deliteljev števila 12.

Pomemben primer mreže je tudi potenčna množica poljubne množice urejena glede na relacijo inkluzije ($\subseteq$), to lepo vidimo na sliki (4). Da se prepričamo, da je ta množica mreža, preprosto preverimo supremume in infimume.
Vidimo, da velja $x \vee y = x \cup y$ in $x \wedge y = x \cap y$, kar nam pojasni, zakaj se občasno za označevanje supremuma in infimuma uporablja oznaki $\cap, \cup$, saj naravno sledita iz potenčne množice kot mreže.
Takoj opazimo, da je tako kot mreža $(\mathbb{N}, |)$ tudi ta mreža omejena, saj je $\{\}$ pod vsemi ostalimi, $\mathbb{N}$ pa nad vsemi. Prav tako pa vidimo da v n tem nivoju nastopajo vse možne n-elementne podmnožice začetne množice.

Opomba: Če bi za mrežo vzeli potenčno množico kakšne končne množice bi lahko s pomočjo kombinatorike lepo prešteli število množic v posameznem nivoju. Tako je za množico moči n v k-tem nivoju $\binom{n}{k}$ elementov. Seštevek množic po vseh nivojih pa ravno 2^n, torej ravno moč potenčne množice.

3 Zakoni v mrežah

Mreže smo si do sedaj pogledali s stališča linearne urejenosti, kmalu pa bomo videli tudi, da lahko zgolj iz nekaterih zakonov, ki veljajo za infimume in supremume na poljubni množici za to množico dobimo delno urejenost in tako iz množice skupaj s temi zakoni tudi mrežo.

Izrek 1:
Za poljubno mrežo $\mathcal{L}$ in poljubne $x, y, z \in \mathcal{L}$ veljajo naslednji zakoni:

- $x \vee x = x$, $x \wedge x = x$ *(Idempotentnost)*
- $x \vee y = y \vee x$, $x \wedge y = y \wedge x$ *(Komutativnost)*
- $(x \vee y) \vee z = x \vee (y \vee z)$
  $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *(Asociativnost)*
- $x \vee (x \wedge y) = x$
  $x \wedge (x \vee y) = x$ *(Absorbcija)*

Dokaz.

- Idempotentnost: Zaradi relfeksivnosti velja $x \leq x$ in je torej tako zgornja kot spodnja meja x, x, prav tako pa so vse ostale spodnje ali zgornje meje manjše ali večje od x.
- Komutativnost: Preprosto sledi iz definicije, saj je meja neodvisna od vrstnega reda elementov
- Asociativnost: Preverimo za $\vee$:
  Naj bo $a = (x \vee y) \vee z$ in $b = x \vee (y \vee z)$
  Iz definicje ali sledi $a \geq z$ in $a \geq (x \vee y)$ in torej $a \geq x, a \geq y$
  Potem velja tudi $a \geq (y \vee z)$ in $a \geq x \vee (y \vee z)$ torej $a \geq b$
  Podobno postopamo za nasprotno stran in tako dobimo $b \geq a$, ker pa je zaradi antisimetričnosti relacije mogoče zgolj, kadar velja $a = b$
  Na analogen način preverimo tudi za $\wedge$, samo da a in b omejimo navzgor.
- Absorbcija: Preverimo za $x \wedge (x \vee y) = x$:
  Iz definicije $\vee$ vemo $x \leq (x \vee y)$ in $x \leq x$ torej $x \leq x \wedge (x \vee y)$
  Iz definicije $\wedge$ pa sledi $x \geq x \wedge (x \vee y)$
  Torej $x \leq x \wedge (x \vee y)$ in $x \geq x \wedge (x \vee y)$, dobimo $x = x \wedge (x \vee y)$
  Drugo enakost preverimo analogno.

□

Pomembno ugotovitev pa nam prinaša naslednji izrek, ki nam pove, da sta si ta dva pogoja za mrežo ekvivalentna.

Izrek 2:
Če imamo množico $\mathcal{L}$, za katero sta definirani operaciji $\vee, \wedge$ in če za te dve operacji veljajo zgornji zakoni(idempotentnost, komutativost, asociativnost, absorbcija), potem je ta množica mreža.

Dokaz. Najprej si s pomočjo supremuma in infimuma definirajo relacijo delne urejenosti.
Definiramo: $x \leq y \iff x \wedge y = x$ in preverimo, da to ustreza zahtevam delne urejenosti:

- Refleksivnost: $x \wedge x = x \implies x \leq x$
- Antisimetričnost: $x \leq y$ in $y \leq x$, torej $x \wedge y = x$ in $y \wedge x = y$, uporabimo komutativnost in dobimo $x = y$
- Tranzitivnost: $x \leq y$ in $y \leq z$ torej velja $x = x \wedge y$ in $y = y \wedge z$
  Namesto y uporabimo $y \wedge z$ in dobimo $x = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$ torej $x \leq z$
  Da ustreza relaciji na mreži moramo preveriti še da velja: $x \wedge y = x \iff x \vee y = y$:
  Uporabimo zadnji zakon in dobimo $x \vee y = (x \vee y) \wedge y = y$, v drugo smer pa postopamo identično.

Da pa bo množica skupaj s to operacijo mreža, moramo še preveriti obstoj supremuma in infimuma za poljubna dva elementa.
Za supremum se ponuja $x \vee y$. Vemo, da je $x \vee y \geq x$, $x \vee y \geq y$ po definicji relacije $\leq$. Preverimo, še da je to natančna zgornja meja. Naj bo z neka druga zgornja meja, velja torej $z \vee x = z \vee y = z$. Potem velja $(x \vee y) \vee z = x \vee (y \vee z) = z$, kar pomeni da $x \vee y \leq z$ in je torej natančna zgornja meja.
Analogno dokažemo, da je infimum $x \wedge y$.

□

4 Podmreže, enote in komplementarne mreže

4.1 Podmreže

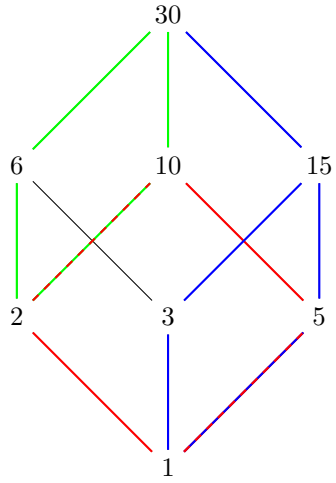
Prej smo že podali primer, da je množica $\mathbb{N}$ z relacijo $|$ mreža, prav tako pa je mreža tudi množica vseh deliteljev števila 30 urejena glede na enako relacijo. Naravno nas zanima, ali lahko podobno kot pri drugih algebraičnih strukturah tudi pri mrežah najdemo podstrukture, ki bi ustrezale našim pričakovanjem.

Definicija 8: Neprazna množica $\mathcal{M} \subseteq \mathcal{L}$ je **podmreža**, če je tudi sama mreža za isti operaciji in se na njih ujema. Povedano drugače $\forall x, y \in \mathcal{M}.\ x \vee y \in \mathcal{M}$ in $x \wedge y \in \mathcal{M}$.

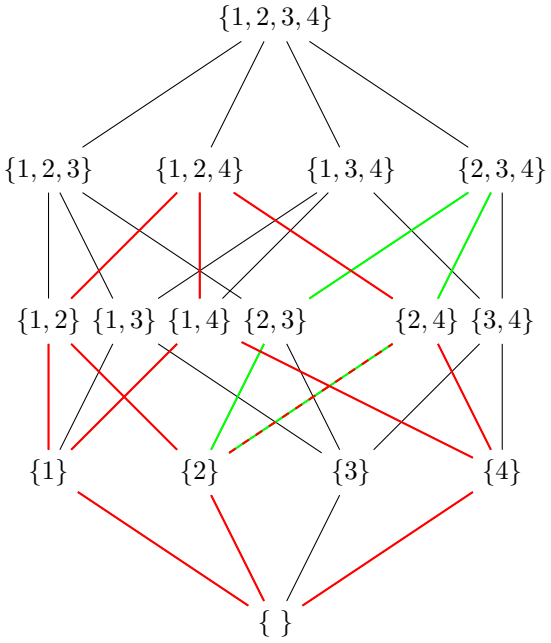
Primer:
1. Če vzamemo $\mathbb{R}$ z relacijo $\leq$, potem je poljubna podmnožica tudi podmreža.
2. Slik (8a in 8b) prikazujeti dva primera podmrež na že znanih mrežah. Tako sta na primer množica deliteljev števila 10, kot tudi množica$\{2, 6, 10, 30\}$ podmreža mreže deliteljev števila 30 (slika 8a). Prav tako pa je $P(\{1, 2, 4\})$ podmreža mreže $P(\{1, 2, 3, 4\})$ (slika 8b).

Naravno nas zanima, ali lahko iz že obstoječih mrež na preprost način dobimo podmreže, če si pogledamo prejšnje primere lahko iz vseh razen modrega na sliki (8a) ugotovimo da so to podmreže sestavljene iz elementoc, ki so med dvema elementoma v mreži. Zanima nas, ali lahko to posplošimo.

Trditev 2: Če v mreži $\mathcal{L}$ vzamemo poljubna $x \leq y$, potem je množica $\mathcal{L}(x, y) := \{z \in \mathcal{L} |\ x \leq z \leq y\}$ podmreža mreže $\mathcal{L}$.



Slika 5: Mreža deljiteljev števila 30 s tremi podmrežami



Slika 6: Mreža $(\{1,2,3,4\}, \subseteq)$ z dvema podmrežama

Dokaz. Preprosto preverimo obstoj imfimuma in supremuma
Vzemimo poljubna $x', y' \in \mathcal{L}(x,y)$ in preverimo zaprtost: $x \geq x' \vee y' \geq x' \wedge y' \geq y$ □

4.2 Enote in komplementi

Ob preučevanju do sedaj predstavljenih mrež smo opazili, da so nekateri njihovi elementi posebni, tako smo recimo za prazno množico pri urejenosti glede na

inkluzijo, da je vedno pod vsem ostalimi podmnožicami, seveda bi sedaj radi to ugotovitev posplošili še na ostale mreže, kadar to lahko storimo.

Definicija 9: Če v mreži $\mathcal{L}$ obstaja tak x, da za poljuben $y \in \mathcal{L}$ velja $x \geq y$, potem takemu elementu rečemo **največji element** in ga označimo z 1 ($\forall x \in \mathcal{L}.\ x \leq 1$).

Definicija 10: Če v mreži $\mathcal{L}$ obstaja tak x, da za poljuben $y \in \mathcal{L}$ velja $x \leq y$, potem takemu elementu rečemo **najmanjši element** in ga označimo z 0. ($\forall x \in \mathcal{L}.\ x \geq 0$).

Posledica: Če v mreži $\mathcal{L}$ obstajata 0 in 1, potem za poljuben $x \in \mathcal{L}$ veljajo naslednje trditve:

- $x \vee 1 = 1$
- $x \vee 0 = x$
- $x \wedge 0 = 0$
- $x \wedge 1 = x$

Dokaz. Te trditve so zgolj prevod relacije $\leq$ v njihovo formulacijo glede na operaciji $\vee$ in $\wedge$. □

Opomba: Vidimo, da je 1 enota za operacijo $\wedge$ in 0 enota za operacijo $\vee$.

Primer:
1. Za interval $[0, 1]$ oznake za mrežo kar sovpadajo z števili. Tako je element 0 kar število 0, element 1 pa število 1.
2. Za potenčno množico neke množice $\mathcal{A}$ urejeno glede na relacijo inkluzije je element 0 prazna množica ($\{\}$), element 1 pa kar celotna množica $\mathcal{A}$.
3. Za mrežo $(\mathbb{N}, |)$ je 0 število 1, saj deli vsa druga naravna števila, element 1 pa število 0, saj jo delijo vsa naravna števila.

Sedaj ko imamo enoto za operacije se nam zdi naravno, da bi definirali tudi neke vrste inverz

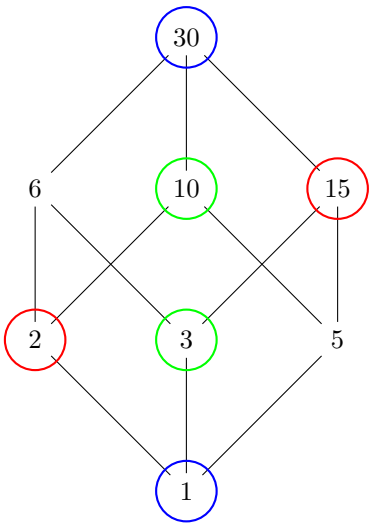
Definicija 11: Naj bo $\mathcal{L}$ mreža z elemetoma 0 in 1 in $x \in x' \in \mathcal{L}$. Elementa x in x' imenujemo **komplementarna elementa**, če veljata naslednji enakosti:

- $x \vee x' = 1$
- $x \wedge x' = 0$

Definicija 12: Mrežo, v kateri poljubnemu x pripada **vsaj** en komplementarni element imenujemo **komplementarna mreža**.

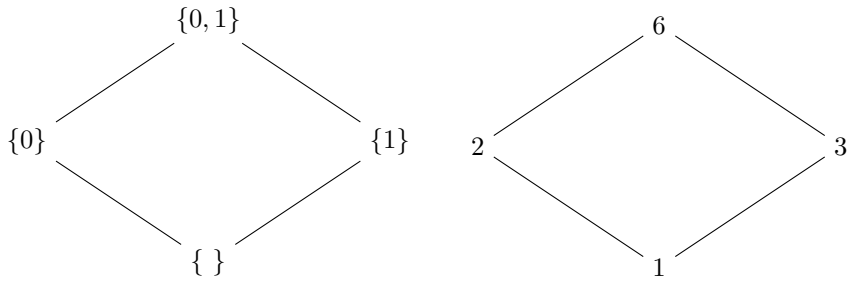
Opomba: Obstoj komplementarnega elementa v mreži z 0 in 1 ni zagotovljen, prav tako pa ima lahko poljuben element več komplementov.

Primer:
1. Lep primer komplementarnih prostorov so vektorski podprostori vektorskega prostora V, ki je opremljen s skalarnim produktom. Tu je infimum dveh podprostorov kar njun presek, medtem ko je supremum njuna direktna vsota. 1 je kar celoten prostor V, medtem ko je 0 njegov ničelni podprostor. Tako je komplement poljubnega podprostora kar njegov ortogonalni komplement, presek dveh komplementarnih elementov pa ničelni prostor, direktna vsota pa kar celoten prostor V.
2. Drug primer komplementarne mreže je mreža sestavljena iz ravnine ter na njej ležečih premic in točk. Tako je komplement premice poljubna točka, ki na njej ne leži, komplement točke pa je poljubna premica, ki ne vsebuje te točke. Vidimo, da ima lahko element več komplementov (celo neskončno).
3. V mreži $(\{1,2,3,4\},\subseteq)$ so komplementi posameznih elementov kar njihovi komplementi v smislu teorije množic, prav tako vidimo, da ima vsak element natančno en komplement
4. V mreži deliteljev števila 30 urejeni glede na deljivost velja, da je komplement elementa x kar $\frac{30}{x}$, kar je lepo prikazano na sliki (7). Ta lastnost pa nam nakazuje neko zelo pomembno značilnost takih mrež, ki jo bomo spoznali v nadaljevanju.



Slika 7: Mreža deliteljev števila 30 z označenimi nekaterimi komplementi

5 Homomorfizmi mrež



(a) Mreža $(\{0,1\}, \subseteq)$ (b) Mreža deliteljev števila 6

Slika 8: Izomorfni mreži

Če si pogledamo zgornji mreži na sliki (8) opazimo, da se zdita zelo podobni. Tako kot pri vseh algebrskih strukturah tudi tukaj definiramo pojem homomorfizma, s pomočjo katerega bomo lahko podobne objekte med seboj "enačili".

Definicija 13: Naj bosta L_1 in L_2 mreži. Funkcija $f : L_1 \to L_2$ je homomorfizem, če velja:

$$f(a \wedge b) = f(a) \wedge f(b)$$
$$f(a \vee b) = f(a) \vee f(b)$$

za vsaka $a, b \in L_1$.

Ena izmed stvari, ki jih pri homorfizmu opazimo je, da homomorfizem ohranja smer urejenosti elementov. Torej, da velja $a \leq b \Rightarrow f(a) \leq f(b)$. To vidimo takole:

$$a \leq b \iff a = a \wedge b$$

Torej imamo

$$f(a) = f(a \wedge b) = f(a) \wedge f(b),$$

kar pa ravno pomeni, da je $f(a) \leq f(b)$.

Izrek 3:
Bijektivna preslikava iz L_1 v L_2 je izomorfizem, če ohranja urejenost iz L_1 v L_2 in nazaj.

Dokaz. Naj bosta $a, b \in L_1$. Ker je $a \wedge b \leq a$ in je tudi $a \wedge b \leq b$, potem zaradi ohranjanja smeri velja:

$$f(a \wedge b) \leq f(a), f(a \wedge b) \leq f(b)$$

Ker je $f(a \wedge b)$ manjši od obeh $f(a)$ in $f(b)$ je manjši tudi od njunega infinuma.

$$f(a \wedge b) \leq f(a) \wedge f(b)$$

S tem smo pokazali, da je $f(a \wedge b)$ spodnja meja elementov $f(a)$ in $f(b)$. Pokažimo, da je to še natačna spodnja meja.
Denimo, da $f(c) \leq f(a) \wedge f(b)$. To pomeni, da je

$$f(c) \leq f(a)$$

$$f(c) \leq f(b)$$

Ker preslikava ohranja red v obe smeri velja:

$$c \leq a$$

$$c \leq b$$

zato pa je c tudi manjši od infinuma teh dveh elementov. $c \leq a \wedge b$.
Uporabimo sedaj preslikavo in ohranjanje smeri, ter dobimo:

$$f(c) \leq f(a \wedge b)$$

Pokazali smo, da je vsaka druga spodnja meja elementov $f(a)$ in $f(b)$ manjša od $f(a \wedge b)$. Po definiciji supremuma sedaj sledi

$$f(a \wedge b) = f(a) \wedge f(b)$$

Enakost

$$f(a \vee b) = f(a) \vee f(b)$$

dokažemo na analogen način. Pokazali smo, da je bijektivna preslikava, ki ohranja smer v obe smeri, homomorfizem mrež. Ker pa je naša preslikava bijektivna sledi, da je to izomorfizem mrež. □

6 Distributivne mreže

Za mrežo pravimo, da je **distributivna**, če zanjo veljata naslednja zakona:

$$(f(a) \wedge f(b)) \vee f(c) = (f(a) \vee f(c)) \wedge (f(b) \vee f(c))$$

$$(f(a) \vee f(b)) \wedge f(c) = (f(a) \wedge f(c)) \vee (f(b) \wedge f(c))$$

in to za vse a, b in c iz mreže.

Primer:
1. Za mrežo vzemimo potenčno množico $\mathbb{N}$ urejeno glede na $\subseteq$. V tem primeru se operacija supremum dveh elementov ujema z unijo dveh množic. Prav tako se infinum dveh elementov ujema s presekom dveh množic. Iz teorije množic pa vemo, da za unijo in presek veljajo distributivni zakoni. Torej je $(\mathcal{P}(\mathbb{N}), \subseteq)$ distributivna mreža.
2. Linearno urejeno množico L lahko hitro prevedemo na prejšnji primer. To storimo tako, da poljuben element $a \in L$ slikamo v množico, ki vsebujejo vse elementa, ki so a manjši.

$$a \to \{x \in L | x \leq a\}$$

Od tukaj naprej pa iz prejšnega primera vemo, da veljajo distributivni zakoni.

Ena izmed lepih lastnosti distributivnih mrež je ta, da če ima nek $a \in L$ komplement, potem je ta komplement gotovo en sam. Recimo, da ima $a \in L$ dva komplementa a_1 in a_2. Sledi:

$$a_2 = 1 \wedge a_2 = (a_1 \vee a) \wedge a_2 = (a_1 \wedge a_2) \vee (a \wedge a_2)$$

Ker velja $a \wedge a_2 = 0$ in $(a_1 \wedge a_2) \vee 0 = a_1 \wedge a_2$, dobimo:

$$a_2 = a_2 \wedge a_1$$

To pa je ekvivalentno pogoju $a_2 \leq a_1$. Z analognim razmislekom dobimo še $a_1 \leq a_2$ in od tod zaradi antisimetričnosti sledi: $a_1 = a_2$ Torej je v distributivnih mrežah komplement elementa, v primeru da obstaja, le en sam. Seveda pa nam nič ne zagotavlja, da bi element distributivne mreže komplement sploh imel.

7 Modulske mreže

Pogoj distributivnosti je zahteven pogoj in marsikatere mreže, ki so uporabne, pogoju distributivnosti ne zadoščajo. Zadoščajo pa nekoliko lažjemu pogoju, ki ga imenujemo modularni zakon.

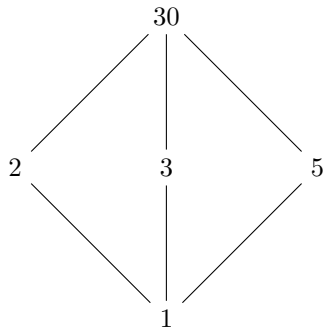
Definicija 14: Mreža $\mathcal{L}$ je modulska, če za vsak $a, b, c \in \mathcal{L}$, pri pogoju, da je burek $a \leq c$, velja:

$$(a \vee b) \wedge c = a \vee (b \wedge c)$$

Da ugotovimo, da je to res šibkejši pogoj od distributivnosti si poglejmo, da so distributivne mreže hkrati tudi modulske, obratno pa ni res. Če je mreža distributivna namreč velja:

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$$

To pa je ravno pogoj modularnosti. Tu smo uporabili distributivnost in nato predpostavko $a \leq c$. Da pa pokažemo da obratno ni res, pa si poglejmo mrežo na sliki (9)



Slika 9: Modulska mreža, ki ni distributivna

Preden se lotimo naslednjega primera, si poglejmo še formulo, ki velja za prav vsako mrežo. Naj bodo $a, b, c \in L$ in naj velja $a \leq c$. Ker je $a \leq c$ in $a \leq (a \vee b)$ sledi, da je

$$a \leq (a \vee b) \wedge c$$

Vemo tudi, da velja, da je $b \wedge c \leq b \leq a \vee b$. in $b \wedge c \leq c$. Torej je tudi

$$b \wedge c \leq (a \vee b) \wedge c$$

Iz te in zgornje ugotovitve pa vidimo, da velja še

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c$$

Za lep primer modulskih mrež pa bomo pokazali, da je množica podgrup edink grupe G, urejena glede na vsebovanost, modulska mreža. Naprej preverimo, da je to sploh mreža. Množica gotovo ni prazna, saj vemo, da sta $\{1\}$ in G podgrupi edinki. Naj bosta H in K poljubni podgrupi G. Za infinum dveh podrup edink vemo, da je $H \cap K$ najmanjša podgrupa, ki ju vsebuje. Za supremum dveh podgrup pa $H \cup K$ seveda ni nujno podgrupa. Vemo pa, da je najmanjša podgrupa, ki H in K vsebuje, podgrupa:

$$HK = \{hk | h \in H, k \in K\}$$

Za dano podgrupo pa se hitro prepičamo, da je tudi edinka. Naj bo $c \in G$ in

$$chkc^{-1} = chc^{-1}ckc^{-1}$$

Ker sta H in K edinki velja $chc^{-1} \in H$ in $ckc^{-1} \in K$. Od tod pa, da je $chkc^{-1} \in HK$. Sledi, da je HK podgrupa edinka.
Izrek 4:
Mreža podgrup edink grupe G je modulska.

Dokaz. Naj bo G grupa in naj bodo $H_1, H_2, H_3 \triangleleft G$. Od zgoraj že vemo, da velja

$$H_1(H_2 \cap H_3) \leq (H_1H_2) \cap H_3$$

Pokazati moramo še, da velja obratno. Torej:

$$(H_1H_2) \cap H_3 \leq H_1(H_2 \cap H_3)$$

V množici $(H_1H_2) \cap H_3$ so vsi elementi, za katere velja enakost $ab = c$, kjer je $a \in H_1$, $b \in H_2$ in $c \in H_3$.. Zapišimo drugače: $b = a^{-1}c$. Ker je $H_1 \subseteq H_3$ je $a^{-1} \in H_3$ in sledi, da je $a^{-1}c = b \in H_3$. Od tod sledi, da je $b \in H_2H_3$ in zaključimo, da je $ab \in H_1(H_2 \cap H_3)$. S tem smo pokazali:

$$(H_1H_2) \cap H_3 \leq H_1(H_2 \cap H_3)$$

in zaradi antisimetričnosti sledi enakost.

$$(H_1H_2) \cap H_3 = H_1(H_2 \cap H_3)$$

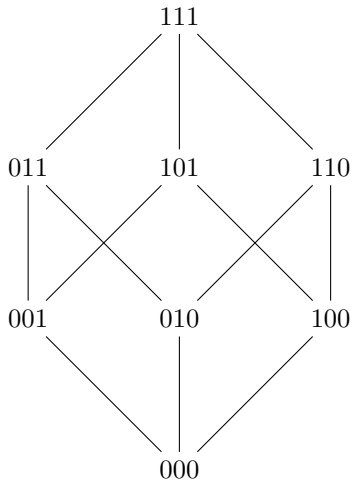
□

8 Booleovi kolobarji

Definicija 15: Booleov kolobar K je kolobar, v katerem je vsak element idempotenten. Torej

$$\forall a \in K.\ a^2 = a$$

Primer:
Najbolj enostaven Booleovega kolobarja je kar kolobar $\mathbb{Z}_2$ z operacijo navadnega seštevanja in množenja. Še kakšen drug primer Booleovega kolobarja pa najlaže dobimo tako, da skupaj vzamemo več kopij $\mathbb{Z}_2$. Še več, da se pokazati, da so prav vsi Booleovi kolobarji izomorfni nekemu številu kopij $\mathbb{Z}_2$. Booleov kolobar moči 2^3 je prikazan na sliki (10).



Slika 10: Mreža na kolobarju $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Izrek 5:
Booleov kolobar ima karakteristiko 2 *in je komutativen.*

Dokaz. Vemo, da velja

$$(a+a)^2 = (a+a)$$

Razpišimo:

$$a^2 + 2aa + a^2 = 2a$$

$$4a = 2a$$

Dobimo $2a = 0$. Ker je bil a poljuben ima kolobar karakteristiko 2. Še komutativnost:

$$(a+b)^2 = (a+b)$$

$$a^2 + ab + ba + b^2 = a + b$$

Nato pa sledi $ab = -ba$. Zaradi karakteristike 2 pa sledi $ab = ba$. □

Pokažimo sedaj, da lahko iz Booleovega kolobarja pridemo do mreže. V ta namen definirajmo operaciji supremum in infinum in pokažimo, da zadoščata aksimom mreže.

$$a \vee b = a + b + ab$$

$$a \wedge b = ab$$

1. (Idempotentnost)
$$a \vee a = a + a + a^2 = a$$
$$a \wedge a = aa = a$$

2. (Komutativnost) smo že pokazali.

3. (Asociativnost)
$$(a \vee b) \vee c = (a + b + ab) \vee c = a + b + c + ab + ac + bc + abc$$
$$a \vee (b \vee c) = a \vee (b + c + bc) = a + b + c + ab + ac + bc + abc$$
$$(a \wedge b) \wedge c = (ab)c = a(bc) = a \wedge (b \wedge c)$$

4. (Absorbcija)
$$a \wedge (a \vee b) = a \wedge (a + b + ab) = a^2 + ab + ab = a$$
$$a \vee (a \wedge b) = a \vee ab = a + ab + a^2 b = a$$

S tem smo pokazali, da je Booleov kolobar z operacijama supremum in infinum kot smo ju definirali, zgoraj mreža.
Za Booleove kolobarje pa velja še celo več. Velja namreč, da je ta mreža distributivna. To najlaže pokažemo kar z direktnim računom.

$$a \wedge (b \vee c) = a \wedge (b + c + bc) = ab + ac + abc$$

$$(a \wedge b) \vee (a \wedge c) = ab \vee ac = ab + ac + abc$$

V Booleovem kolobarju ničelni element sovpada z minimalnim elementom mreže. Prav tako tudi element 1.

$$a \wedge 0 = a0 = 0$$

$$a \vee 0 = a + 0 + a0 = a$$

$$a \wedge 1 = 1a = a$$

$$a \vee 1 = a + 1 + a = 1$$

8.1 Lastnosti in primeri Booleovih kolobarjev

Ugotovili smo že da je poljubno kopij $\mathbb{Z}_2$ Booleov kolobar, če pa si pobližje pogledamo sliko (10) in sliko (2) vidimo da sta si izomorfni. Zanima nas, ali bi lahko to kako posplošili.

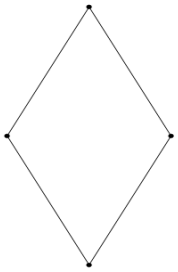
Trditev 3: Booleov kolobar moči 2^n je izomorfen mreži vseh deliteljev naravnega števila m, ki ima n različnih praštevilskih deliteljev, ne deli pa ga kvadrat kakega praštevila.

Dokaz. (Zgolj skica) naj bo $m = p_1 p_2 \dots p_n$, potem je vsak delitelj števila m oblike $k = p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}$, kjer $i \in \{0, 1\}$. Pripdajoč izomorfizem bo potem kar $\varphi(p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}) = (i_1, i_2, \dots, i_n)$, ki je očitno bijektiven, to da pa ohranja red v obeh smereh pa preprosto preverimo z računom. □

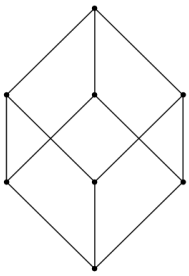
Opomba: Da se pokazati tudi, da sta dva Booleova kolobarja izomorfna natanko tedaj, ko imata enako število elementov ter da imajo Booleovi kolobarji 2^n elementov za neko naravno število n.

Če bi Hassejev diagram Booleovega kolobarja iz n kopij narisali kot graf v prostoru $\mathbb{R}^n$, kjer bi se koordinate vozlišč diagrama skladale bi dobili ravno n-dimenzionalni graf hiperkocke. To preprosto vidimo tako, da je vsak element v diagramu povezan zgolj z tistimi elementi, ki imajo različno natanko eno koordinato, to lepo vidimo na sliki (10) in sliki (11).

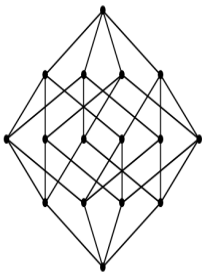
(a) Booleov kolobar $\mathbb{Z}_2$



(b) Booleov kolobar $\mathbb{Z}_2 \oplus \mathbb{Z}_2$



(c) Booleov kolobar $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$



(d) Booleov kolobar $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Slika 11: Primeri Booleovih kolboarjev

9 Literatura

- P. M. Cohn *Basic Algebra*, cop. 2012.
- Ivan Vidav *Algebra*, cop. 2010.
- Predavanja iz algebraične kombinatorike dostopna na `http://www.math.cornell.edu/~levine/18.312/`
- `https://en.wikipedia.org/wiki/Partially_ordered_set`
- `https://en.wikipedia.org/wiki/Lattice_%28order%29`
- `https://en.wikipedia.org/wiki/Modular_lattice`
- `https://en.wikipedia.org/wiki/Distributive_lattice`
- `http://www-rohan.sdsu.edu/~gawron/mathling/course_core/lectures/posets_slides.pdf`
- `http://www.math.hawaii.edu/~jb/math618/os9uh.pdf`

Opomba o avtorstvu

Kot je bilo dogovorjeno je bil seminar sestavljen iz dveh delov.
Filip Koprivec je spisal poglavja: Uvod (1), Osnovni primeri mrež (2), Podmreže, enote in komplementarne mreže (4) in Booleovi kolobarji (8).
Samo Kralj se spisal poglavja: Zakoni v mrežah (3), Homomorfizmi mrež (5), Distributivne mreže (6) in Modulske mreže (7).