Дискретне структуре 1

предавање 1 (4.11.2025.)

Тема: УВОД У ТЕОРИЈУ СКУПОВА

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Скоро све што радимо у математици темељи се, посредно или непосредно, на појму скупа.

Појам скупа је интуитивно јасан: замишљамо га као колекцију неких објеката. Термин колекција често користимо као синоним за појам скупа.

Међутим, уколико на тај начин посматрамо скупове, брзо наилазимо на проблеме.

Берберинов парадокс: У неком селу берберин брије све становнике тог села који не бријy сами себе. Поставља се питање да ли берберин брије сам себе?

- ако је одговор не, дакле берберин не брије сам себе, тада је и он један од становника села који се не бријy сами, па мора бријати сам себе, што је противуречност
- ако је одговор да, опет долазимо до противуречности јер берберин брије искључиво људе из села који се не бријy сами

Парадокс лажљивца: Филозоф Епименид (6 век п.н.е.) са Крита рекао је "Крићани увек лажу". Да ли је говорио истину?

Друга верзија парадокса лажливца: Инспирисана је причом о Пинокију. Поставља се питање шта ће се десити ако Пинокио каже: "Мој нос ће сада порасти."?

Грелинг-Нелсонов парадокс: Постоје неки придеви који описују себе, нпр. петнаестословни, вишесложан... Речи које не описују саме себе се зову хетерологичке. Да ли је придев "хетерологички" хетерологичка реч?

Претходни примери су у вези са чувеним **Раселовим парадоксом:**

Посматрајмо колекцију S дефинисану са

$$x \in S \text{ акко } x \notin x.$$

Да ли $S \in S$?

- ако $S \in S$, на основу дефиниције колекције онда $S \notin S$
- ако $S \notin S$, опет на основу дефиниције колекције S закључујемо да $S \in S$

Закључак: Овако дефинисану колекцију S **не можемо** сматрати скупом у математичком смислу.

Основна релација међу скуповима је релација припадности.
Скуп A припада скупу B записујемо са $A \in B$. Кажемо да је A елемент од B.

Зермело-Френкелова теорија скупова

Скупови се заснивају (дефинишу) аксиоматски. (Зермело-Френкелова (ЗФ) теорија скупова)

Аксиома екстензије

Два скупа су једнака ако имају исте елменте.

нпр. скупови $A = \{2, 3\}$ и $B = \{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\}$ су једнаки.

Аксиома празног скупа

Постоји скуп који нема ниједан елемент.

Овај скуп називамо празан скуп и означавамо га са $\emptyset$. Према аксиоми екстензије овај скуп је јединствен.

Аксиома пара

За све скупове x и y постоји скуп z чији су једини елементи x и y.

Скуп z означавамо са $z = \{x, y\}$. Важи следеће:

$$u \in \{x, y\} \text{ акко } u = x \text{ или } u = y.$$

Можемо формирати скуп са једним елементом ако узмено да је $x = y$. Према аксиоми екстензије важи $\{x, x\} = \{x\}$.

Зермело-Френкелова теорија скупова

Аксиома уније

За сваки скуп x постоји скуп z тако да $u \in z$ ако и само ако $u \in y$ за неки $y \in x$. Скуп z представља унију чланова скупа x и означавамо га са $\bigcup x$.

Скуп $z = \bigcup x$ састоји се од елемената елемената скупа x. На пример, ако је $x = \{a, b\}$ тада је $z = \bigcup\{a, b\} = a \cup b$.

дефиниција: Скуп a је *подскуп* скупа b, у ознаци $a \subseteq b$, ако за све $x \in a$ важи да $x \in b$.

Нпр. скуп $\emptyset$ је подскуп сваког скупа.

Важи да је $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Аксиома партитивног скупа

За сваки скуп x постоји скуп $\mathcal{P}(x)$, који се састоји од свих подскупова од x.

Ако је $x = \{a, b\}$, тада је $\mathcal{P}(x) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Ако је $x = \emptyset$, тада је $\mathcal{P}(x) = \mathcal{P}(\emptyset) = \{\emptyset\}$.

Зермело-Френкелова теорија скупова

Аксиома издвајања скупа (Аксиома сепарација)

За сваки скуп a и сваку формулу $\phi(x)$ важи да је $\{x \in a \mid \phi(x)\}$ скуп.

Примене аксиоме издвајања поскупа:

$A \cap B = \{x \in A \mid x \in B\}$ – пресек скупова A и B

$A \setminus B = \{x \in A \mid x \notin B\}$ – разлика скупова A и B

нека $A \subseteq U$, $A^c = \{x \in U \mid x \notin A\}$ – комплемент скупа A у скупу U

Основни скуповни идентитети:

1. $(A \cap B) \cap C = A \cap (B \cap C)$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. $A \cap B = B \cap A$
7. $A \cup B = B \cup A$
8. $A \triangle B = B \triangle A$
9. $A \cap A = A$
10. $A \cup A = A$
11. $A \cap (A \cup B) = A$
12. $A \cup (A \cap B) = A$
13. $(A \cap B)^c = A^c \cup B^c$
14. $(A \cup B)^c = A^c \cap B^c$
15. $(A^c)^c = A$
16. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
17. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Уређени парови

тврђење: За скупове a, b, c, d важи:

$$\{a, b\} = \{c, d\} \text{ ако и само ако } (a = c \text{ и } b = d) \text{ или } (a = d \text{ и } b = c).$$

доказ: Ако важи неки од два услова са десне стране, јасно је да је $\{a, b\} = \{c, d\}$. С друге стране, претпоставимо да је $\{a, b\} = \{c, d\}$. Како је $a \in \{a, b\}$, то је $a \in \{c, d\}$, па је $a = c$ или $a = d$. Нека је прво $a = c$. Важи $d \in \{c, d\}$, па $d \in \{a, b\}$, а тиме и $d = a$ или $d = b$. Ако је $b = d$ важи десна страна. Ако је $a = d$, имамо да је $a = c = d$. Из $b \in \{a, b\} = \{c, d\}$ следи $b = c = d$, па важи десна страна. Слично се доказује и други случај, када је $a = d$.

дефиниција: *Уређени пар* (a, b) скупова a и b је скуп $\{\{a\}, \{a, b\}\}$.

тврђење: За уређене парове (a, b) и (c, d) важи: $(a, b) = (c, d)$ акко $a = c$ и $b = d$.

доказ: Ако важи $a = c$ и $b = d$, онда је $(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d)$. Нака је сад $(a, b) = (c, d)$. Онда је $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Према претходном тврђењу, важи да је ($\{a\} = \{c\}$ и $\{a, b\} = \{c, d\}$) или ($\{a\} = \{c, d\}$ и $\{a, b\} = \{c\}$.) Ако важи први део, мора бити $a = c$. Такође, важи ($a = c$ и $b = d$) или ($a = d$ и $b = c$). У првој случају имамо $a = c$ и$b = d$. У другом случају $d = a = c = b$, па је специјално и $a = c$ и $b = d$. Ако важи други део, онда је $a = b = c = d$, па опет важе тражене једнакости.

Декартов производ два скупа

дефиниција: Декартов производ скупова A и B је скуп

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

нпр. Декартов производ скупова $A = \{1, 2, 3\}$ и $B = \{x, y\}$ је

$$A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}.$$

Како је $B \times A = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$, видимо да не мора важити једнакост између скупова $A \times B$ и $B \times A$.

напомена: $A \times B = \emptyset$ акко $A = \emptyset$ или $B = \emptyset$

Особине Декартовог призвода:

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$
$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

Декартов производ више скупова

дефиниција: Уређена n-торка елемената a_1, a_2, ..., a_n је објекат $(a_1, a_2, \ldots, a_n)$ такав да важи

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \text{ акко } a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n.$$

уређена n-торка може се дефинисати преко појма уређеног пара:

$$(a_1, a_2, \ldots, a_n) := (a_1, (a_2, (\ldots, (a_{n-1}, a_n) \cdots)))$$

нпр. $(a_1, a_2, a_3) := (a_1, (a_2, a_3))$
$(a_1, a_2, a_3, a_4) := (a_1, (a_2, (a_3, a_4)))$

дефиниција: Декартов производ скупова $A_1, A_2, \ldots, A_n$ је скуп

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n\}.$$

Дискретне структуре 1

предавање 2 (14.11.2025.)

Тема: РЕЛАЦИЈЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Дефиниција и примери

Неформално речено, појам релације бави се остваривањем веза између неких елемената скупова које посматрамо.

дефиниција: Нека су A и B скупови. **Релација** ρ са скупа A у скуп B је сваки подскуп од $A \times B$. Дакле, $\rho \subseteq A \times B$. Ако је $A = B$ онда кажемо да је ρ бинарна релација на скупу A.

Чињеницу да $(a, b) \in \rho$ пишемо и $a\rho b$.

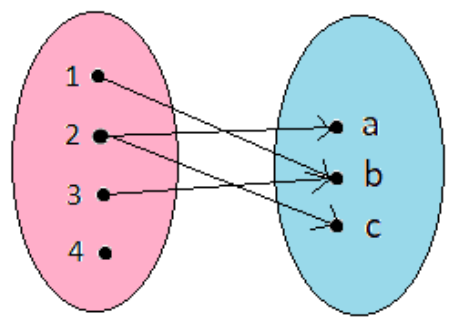
Пример: $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$
$\rho = \{(1, b), (2, a), (2, c), (3, b)\}$ је једна релација са скупа A на скуп B.
$\sigma = \{(1, 3), (2, 1), (4, 2)\}$ је једна бинарна релација на скупу A

Различити начини представљања релација:

$$\rho = \{(1, b), (2, a), (2, c), (3, b)\} \subseteq A \times B$$

	a	b	c
1	0	1	0
2	1	0	1
3	0	1	0
4	0	0	0

табелари приказ



приказ помоћу дијаграма

Домен релације $\rho \subseteq A \times B$:

$$\mathrm{Dom}(\rho) = \{a \in A \mid \text{постоји } b \in B \text{ тако да је } (a,b) \in \rho\}.$$

Слика релације $\rho \subseteq A \times B$:

$$\mathrm{Im}(\rho) = \{b \in B \mid \text{постоји } a \in A \text{ тако да је } (a,b) \in \rho\}.$$

Инверзна релација релације $\rho \subseteq A \times B$:

$$\rho^{-1} = \{(b,a) \in B \times A \mid (a,b) \in \rho\} \subseteq B \times A.$$

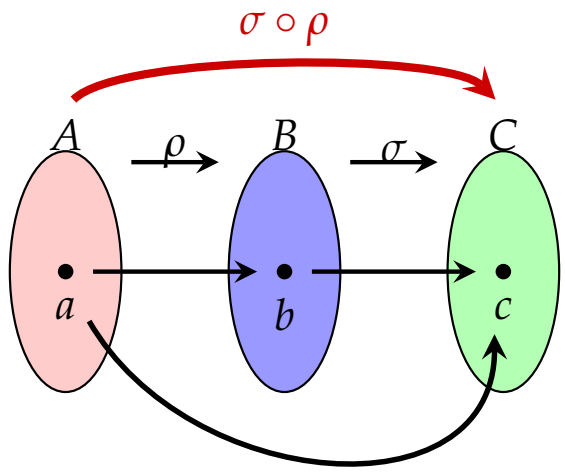
Композиција релација $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$:

$$\sigma \circ \rho = \{(a,c) \in A \times C \mid \text{постоји } b \in B \text{ тако да } (a,b) \in \rho \text{ и } (b,c) \in \sigma\} \subseteq A \times C.$$

Пример:
$A = \{1,2,3,4\}$, $B = \{x,y,z\}$, $C = \{\alpha,\beta,\gamma\}$ $\rho = \{(1,y),(2,z),(2,x),(3,y)\} \subseteq A \times B$,
$\sigma = \{(x,\beta),(y,\beta)\} \subseteq B \times C$

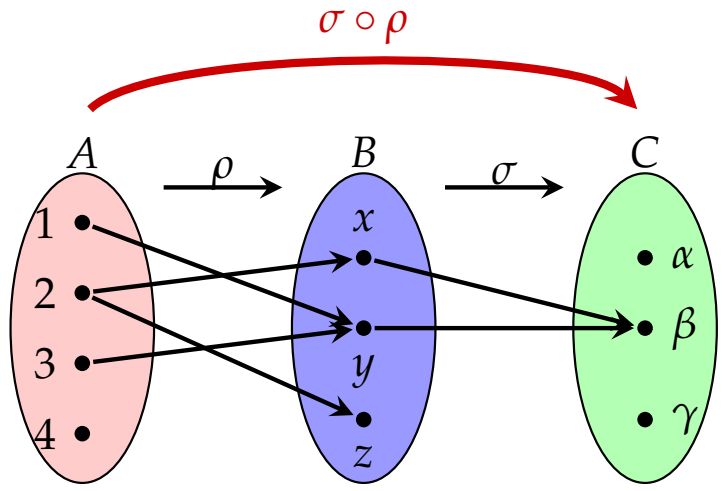
$$\mathrm{Dom}(\rho) = \{1,2,3\} \qquad \rho^{-1} = \{(y,1),(z,2),(x,2),(y,3)\}$$
$$\mathrm{Im}(\rho) = \{x,y,z\}$$

Композиција релација



$a\ (\sigma \circ \rho)\ c$ акко $a\,\rho\,b$ и $b\,\sigma\,c$ за неко $b \in B$

Пример:
$A = \{1, 2, 3, 4\},\ B = \{x, y, z\}$
$C = \{\alpha, \beta, \gamma\}$
$\rho = \{(1, y), (2, z), (2, x), (3, y)\} \subseteq A \times B,$
$\sigma = \{(x, \beta), (y, \beta)\} \subseteq B \times C$
$\sigma \circ \rho = \{(1, \beta), (2, \beta), (3, \beta)\}$



Особине инверзне релације:

Нека су дате релације $\rho, \sigma \subseteq A \times B$ тада важи:

- Ако је $\rho \subseteq \sigma$, онда је $\rho^{-1} \subseteq \sigma^{-1}$.
- $(\rho^{-1})^{-1} = \rho$.
- $(\sigma \cup \rho)^{-1} = \sigma^{-1} \cup \rho^{-1}$
- $(\sigma \cap \rho)^{-1} = \sigma^{-1} \cap \rho^{-1}$.

  Докази: на часу

Особине композиције:

Нека је $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$ и $\tau \subseteq C \times D$, тада важи:

- $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$
- $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$

  Докази: на часу

Особине релација

дефиниција: Нека је ρ бинарна релација на скупу A. Кажемо да је ρ

- рефлексивна, ако је $(a,a) \in \rho$ за свако $a \in A$;
- антирефлексивна, ако је $(a,a) \notin \rho$ за свако $a \in A$;
- симетрична, ако за све $a,b \in A$ из $(a,b) \in \rho$ следи $(b,a) \in \rho$;
- антисиметрична, ако за све $a,b \in A$ из $(a,b) \in \rho$ и $(b,a) \in \rho$ следи да је $a = b$;
- транзитивна, ако за све $a,b,c \in A$ из $(a,b) \in \rho$ и $(b,c) \in \rho$ следи да $(a,c) \in \rho$.

Нека је $\triangle_A = \{(a,a) \mid a \in A\}$, релација ρ је

- рефлексивна, ако је $\triangle_A \subseteq \rho$;
- антирефлексивна, ако је $\triangle_A \cap \rho = \emptyset$;
- симетрична, ако је $\rho \subseteq \rho^{-1}$;
- антисиметрична, ако је $\rho \cap \rho^{-1} \subseteq \triangle_A$;
- транзитивна, ако је $\rho \circ \rho \subseteq \rho$.

Примери

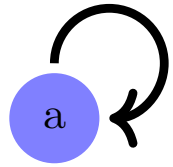
	$\leq$ на $\mathbb{R}$	паралелност правих на скупу правих у простору	нормалност правих на скупу правих у простору
рефлексивност	да	да	не
антирефлексивност	не	не	да
симетричност	не	да	да
антисиметричност	да	не	не
транзитивност	да	да	не

$A = \{a, b, c\}$
$\rho = \{(a, a), (b, b), (a, b), (b, a)\} \subseteq A^2$
$\sigma = \{(a, c), (b, a)\} \subseteq A^2$

	ρ	σ
рефлексивност	не	не
антирефлексивност	не	да
симетричност	да	не
антисиметричност	не	да
транзитивност	да	не

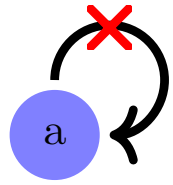
Матрични приказ особина релације

Рефлексивност:



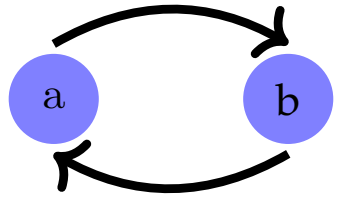
$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

Антирефлексивност:



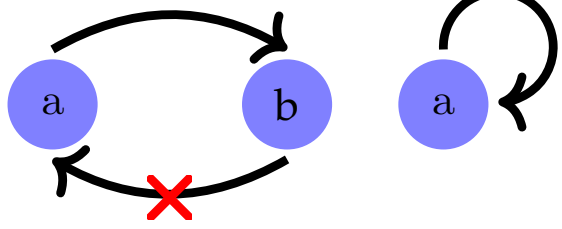
$$\begin{pmatrix} 0 & & \\ & 0 & \\ & & 0 \end{pmatrix}$$

Симетричност:



$$\begin{pmatrix} & 1 & \\ 1 & & 0 \\ & 0 & \end{pmatrix}$$

Антисиметричност:



$$\begin{pmatrix} & 0 & & \\ 1 & & 1 & \\ & 0 & & 0 \\ & & 0 & \end{pmatrix}$$

Матрица композиције релација

Нека $R, S \in M_n(\{0,1\})$. **Булов производ матрица** $R = [r_{ij}]_{i,j=\overline{1,n}}$ и $S = [s_{ij}]_{i,j=\overline{1,n}}$, у ознаци $R \otimes S$, је матрица $T = [t_{ij}]_{i,j=\overline{1,n}}$ таква да је

$$t_{ij} = (r_{i,1} \wedge s_{1,j}) \vee (r_{i,2} \wedge s_{2,j}) \vee \cdots \vee (r_{i,n} \wedge s_{n,j}),$$

при чему су бинарна операције $\wedge, \vee : \{0,1\} \times \{0,1\} \to \{0,1\}$ дефинисане на следећи начин:

$\wedge$	0	1
0	0	0
1	0	1

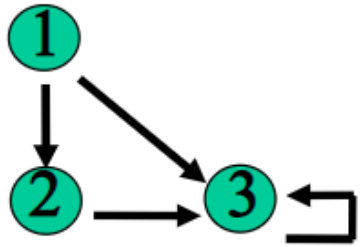
$\vee$	0	1
0	0	1
1	1	1

Матрицу релације ρ означаваћемо са M_ρ.

теорема: Нека је ρ бинарна релација на произвољном скупу A, тада је $M_{\sigma\circ\rho} = M_\rho \otimes M_\sigma$.

Доказ. На часу.

Транзитивност и матрица релације



ТРАНЗИТИВНА РЕЛАЦИЈА

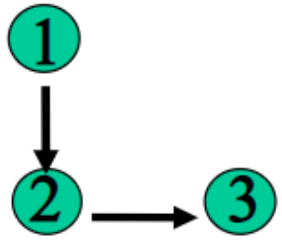
$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \end{array} \quad \mathbf{R}$$

$$\otimes$$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \end{array} \quad \mathbf{R}$$

$$=$$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \end{array} \quad \mathbf{R^2 \subseteq R}$$



РЕЛАЦИЈА НИЈЕ ТРАНЗИТИВНА

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \end{array} \quad \mathbf{R}$$

$$\otimes$$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \end{array} \quad \mathbf{R}$$

$$=$$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{array} \quad \mathbf{R^2 \not\subseteq R}$$

Дискретне структуре 1

предавање 3 (21.11.2025.)

Тема: РЕЛАЦИЈЕ ЕКВИВАЛЕНЦИЈЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Дефиниција и примери

дефиниција: Нека је ρ бинарна релација на скупу A. Кажемо да је ρ **релација еквиваленције**, ако је рефлексивна, симетрична и транзитивна.

Релација ρ је релација еквиваленције на скупу A акко важи

$$\triangle_A \subseteq \rho, \qquad \rho = \rho^{-1}, \qquad \rho \circ \rho = \rho.$$

Примери релација еквиваленције:

- Релација једнакости реалних бројева.
- Релација сличности у скупу троуглова еуклидске равни.
- Нека је $m \geq 2$. Релација $\equiv_m$ дефинисана на скупу $\mathbb{Z}$ са:

$$x \equiv_m y \quad \text{акко} \quad m \mid x - y$$

је релација еквиваленције.

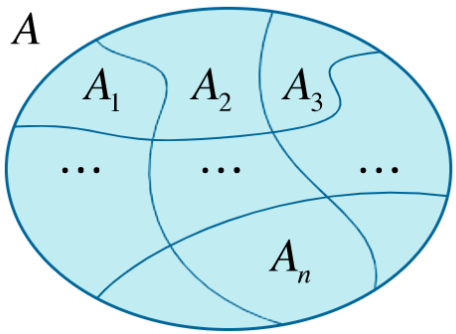
Класе еквиваленције

A – скуп људи који живе у једној држави X

$A_1, A_2, \ldots, A_n$ – скуп градова државе X

На скупу A дефинисана је релација $\sim \subseteq A^2$ на следећи начин:

$$P_1 \sim P_2 \quad \text{акко} \quad \text{особа } P_1 \text{ живи у истом граду као и особа } P_2.$$



дефиниција: Нека је $\sim$ релација еквиваленције на скупу A. **Класа еквиваленције елемента** $a \in A$ је скуп

$$C_a = \{x \in A \mid a \sim x\} \subseteq A.$$

Означавамо је и са $[a]$ и кажамо да је елемент a **представник класе** C_a.

Класе еквиваленције и количнички скуп

Особине класа:

1. Све класе еквиваленције су непразни скупови.
2. Нека је $a, b \in A$. Ако је $C_a \cap C_b \neq \emptyset$, онда је $C_a = C_b$.
3. Унија свих класа еквиваленције је једнака скупу A.

Доказ. На часу.

Свака релација еквиваленције дели скуп на коме је дефинисана на непразне, дисјунктне скупове чија унија је једнака целом скупу. Таква подела се назива **партиција скупа**.

дефиниција: **Количнички скуп** скупа A за релацију еквиваленције $\sim$ је

$$A/_\sim = \{C_x \mid x \in A\}.$$

Приметимо да је $A/_\sim \subseteq \mathcal{P}(A)$, јер важи да је $C_a \subseteq A$, за све $a \in A$.

Особине количничког скупа:

1. Ако $X, Y \in A/_\sim$ и $X \neq Y$, тада је $X \cap Y = \emptyset$.
2. Важи да је $\bigcup A/_\sim = \bigcup_{X \in A/_\sim} X = A$.

Дискретне структуре 1

предавање 4 (25.11.2025.)

Тема: РЕЛАЦИЈЕ ПОРЕТКА

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Дефиниција и примери

дефиниција: Нека је ρ бинарна релација на скупу A. Кажемо да је ρ **релација парцијалног уређења** или **поретка**, ако је рефлексивна, антисиметрична и транзитивна.

Скуп A на коме је дефинисана релација парцијалног уређења ρ називамо **парцијално уређен скуп** или **посет**.

Релација ρ је релација поретка на скупу A ако и само ако важи:

$$\triangle_A \subseteq \rho \qquad \rho \cap \rho^{-1} = \triangle_A \qquad \rho \circ \rho = \rho.$$

Примери релација парцијалног уређења:

1. Релација мање или једнако на скупу реалних бројева: $\leq$.
2. Релација дељивости на скупу природних бројева: $|$.
3. Релација инклузије на партитивном скупу неког скупа: $\subseteq$.

Нека је $\rho \subseteq A^2$ поредак. Елементи a и b су **упоредиви** ако важи $a \rho b$ или $b \rho a$. У супротном, a и b су **неупоредиви**.

$a \rho b$ читамо: a је ρ-мање од b, односно, b је ρ-веће од a.

Поредак је **линеаран** (**тоталан**) ако су свака два елемента упоредива. Уколико нису свака два елемента упоредива, поредак је **парцијалан**. Линеарно уређен подскуп неког парцијално уређен скуп назива се **ланац**. Подскупове парцијално уређеног скупа у којима су свака два елемента неупоредива називамо **антиланци**.

Примери:

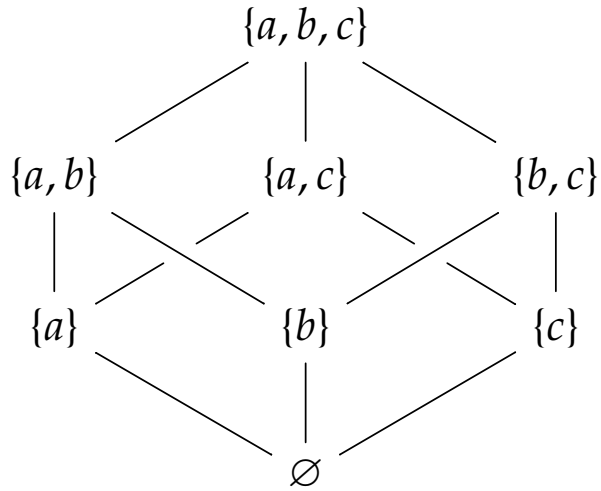
1. $\leq$ је линеаран поредак на $\mathbb{R}$,
2. $\mid$ није линеаран поредак на $\mathbb{N}$,
   скуп $\{2^n \mid n \in \mathbb{N}\}$ је један ланац на $\mathbb{N}$
3. $\subseteq$ није линеаран поредак на $\mathcal{P}(X)$, за произвољан скуп X,
   скуп свих једночланих подскупова од X је један антиланац у $\mathcal{P}(X)$

Хасеов дијаграм

Парцијално уређени скупови могу се представити графички помоћу **Хасеовог дијаграма**. Ако је A скуп на коме је дато парцијално уређење ρ, Хасеов дијаграм посета A формира се на следећи начин:

- сваком елементу скупа A одговара једна тачка у равни;
- тачке које одговарају елементима $x, y \in A$ су спојене линијом ако и само ако је $x \rho y$, при чему се x налази ниже на цртежу од y.

Пример: Нека је $X = \{a, b, c\}$. Скуп $\mathcal{P}(X)$ уређен је релацијом $\subseteq$ и у односу на ову релацију представља се помоћу Хасеовог дијаграма на следећи начин:



дефиниција: Нека је ρ релација парцијалног поретка на скупу A и нека је $B \subseteq A$. Кажемо да је $a \in A$:

- **минималан елемент** скупа B ако $a \in B$ и важи: ако је $x \,\rho\, a$, онда је $x = a$, за све $x \in B$;
- **максималан елемент** скупа B ако $a \in B$ и важи: ако је $a \,\rho\, x$, онда је $x = a$, за све $x \in B$;
- **најмањи елемент (минимум)** скупа B ако $a \in B$ и за све $x \in B$ важи $a \,\rho\, x$;
- **највећи елемент (максимум)** скупа B ако $a \in B$ и за све $x \in B$ важи $x \,\rho\, a$;

Примери:

	$\mathcal{P}(\{1,2,3\}),\ \subseteq$	$\mathcal{P}(\{1,2,3\}) \setminus \{\emptyset\},\ \subseteq$	$\mathbb{N},\ \mid$	$\mathbb{N} \setminus \{1\},\ \mid$
минимум	$\emptyset$	нема	1	нема
максимум	$\{1,2,3\}$	$\{1,2,3\}$	0	0
минимални елемент(и)	$\emptyset$	$\{1\},\{2\},\{3\}$	1	прости бројеви
максимални елемент(и)	$\{1,2,3\}$	$\{1,2,3\}$	0	0

Важи следеће:

1. Ако постоји најмањи елемент скупа B, онда је он јединствен.
2. Ако постоји најмањи елемент скупа B, тада и једини минималан елемент.
3. Уколико постоји минималан елемент, не мора нужно постојати најмањи елемент.
4. Ако постоји највећи елемент скупа B, онда је он јединствен.
5. Ако постоји највећи елемент скупа B, тада и једини максималан елемент.
6. Уколико постоји максималан елемент, не мора нужно постојати највећи елемент.

Доказ: на часу

дефиниција: Нека је ρ релација парцијалног уређење на скупу A, $B \subseteq A$ и $a \in A$. Кажемо да је елемент a

- **доње ограничење** скупа B ако $a \rho b$ за све $b \in B$;
- **горње ограничење** скупа B ако $b \rho a$ за све $b \in B$.

Ако постоји највеће доње ограничење, називамо га **инфимум** скупа B. Ако постоји најмање горње ограничење називамо га **супремум** скупа B. Инфимум и супремум скупа B редом означавамо са $\inf(B)$ и $\sup(B)$.

Важи следеће:

1. Ако постоји минимум у скупу B, онда је он једнак инфинуму скупа B.
2. Ако постоји максимум у скупу B, онда је он једнак супремуму скупа B.

Доказ: на часу.

Дискретне структуре 1

предавање 5 (2.12.2025.)

Тема: ФУНКЦИЈЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

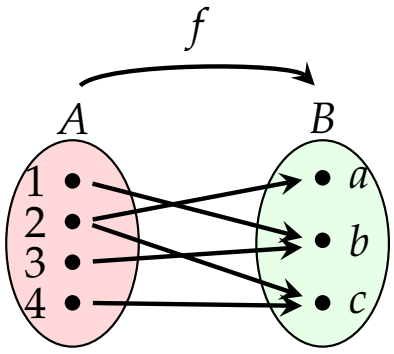
Математички факултет, Београд

дефиниција: Нека је $f \subseteq A \times B$ релација. Кажемо да је f **функција** ако за свако $a \in \mathrm{Dom}(f)$ постоји тачно једно $b \in B$ тако да $(a,b) \in f$.

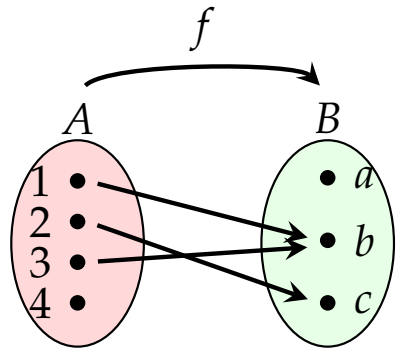
Ако је $f \subseteq A \times B$ функција уместо $(a,b) \in f$ пишемо $b = f(a)$ и елемент b називамо слика елемента a при функцији f.

Ако је $\mathrm{Dom}(f) = A$, пишемо $f : A \to B$ и кажемо да је f функција из A у B. Скуп A је **домен** а B **кодомен** функције. Слика функције f је скуп $\mathrm{Im}(f) = \{f(a) \mid a \in A\} \subseteq B$.

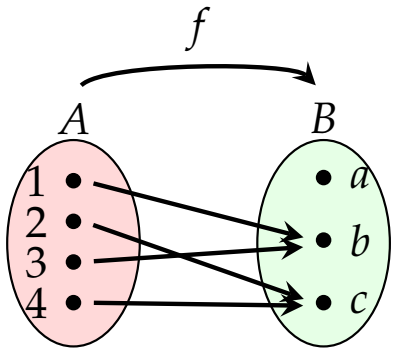
Пример: $A = \{1,2,3,4\}$, $B = \{a,b,c\}$, $f \subseteq A \times B$



f није функција из A у B



f није функција из A у B



f је функција из A у B

Инверзна функција

Ако је $f \subseteq A \times B$ функција, f^{-1} је инверзна релација. Али f^{-1} не мора бити и функција.

Пример: Релација $f \subseteq \mathbb{R} \times \mathbb{R}$ дефинисана са $f = \{(x, x^2) \mid x \in \mathbb{R}\}$ је функција. Међутим, релација $f^{-1} = \{(x^2, x) \mid x \in \mathbb{R}\}$ није функција.

дефиниција: Функција $f : A \to B$ је **сурјекција**, или "на" функција, ако важи

$$\text{за свако } b \in B \text{ постоји } a \in A \text{ тако да је } f(a) = b.$$

Функција $f : A \to B$ је **injекција**, или "1-1" функција, ако важи

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2, \text{ за све } a_1, a_2 \in A.$$

За функцију $f : A \to B$ кажемо да је **бијекција** ако је инјекција и сурјекција.

Инверзна функција

теорема: Релација $f^{-1} \subseteq B \times A$ је функција која слика скуп B у скуп A ако и само ако је $f : A \to B$ је бијекција.

Доказ: на часу.

теорема: Ако су релације $f \subseteq A \times B$ и $g \subseteq B \times C$ функције, онда је и релација $g \circ f$ функција и важи $(g \circ f)(a) = g(f(a))$, за свако $a \in \mathrm{Dom}(g \circ f)$.

Доказ: на часу.

дефиниција: Нека су $f : A \to B$ и $g : B \to C$ функције. **Композиција** функције f и g је функција $g \circ f : A \to C$ таква да је $(g \circ f)(x) = g(f(x))$ за све $x \in A$.

теорема: Нека је $f : A \to B$. Тада важи: f је бијекција ако и само ако постоји функција $g : B \to A$ тдј. $g \circ f = id_A$ и $f \circ g = id_B$. (у том случају је $g = f^{-1}$)

Доказ: на часу.

Директна и инверзна слика

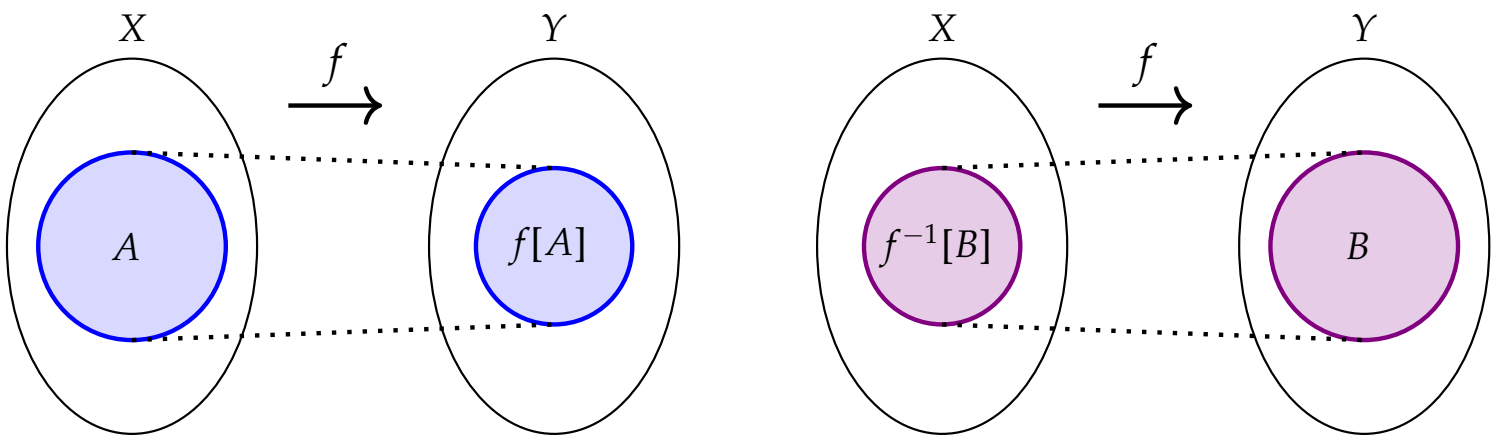
дефиниција: Нека је $f : X \to Y$ и $A \subseteq X$. **Директна слика** скупа A је скуп

$$f[A] = \{f(x) \mid x \in A\}.$$

Нека је $f : X \to Y$ и $B \subseteq Y$. **Инверзна слика** скупа B је скуп

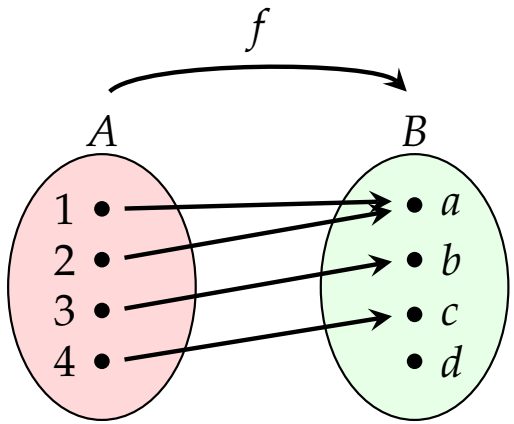
$$f^{-1}[B] = \{x \in X \mid f(x) \in B\}.$$

Инверзна слика скупа $f^{-1}[B]$ је појам који је дефинисан без обзира на то да ли постоји инверзна функција f^{-1}.



Директна и инверзна слика

Пример:



$f[\{1\}] = \{f(1)\} = \{a\}$

$f[\{1,2\}] = \{f(1), f(2)\} = \{a\}$

$f[\{1,3\}] = \{f(1), f(3)\} = \{a,b\}$

$f^{-1}[\{a\}] = \{1,2\}$

$f^{-1}[\{a,b\}] = \{1,2,3\}$

$f^{-1}[\{a,b,d\}] = \{1,2,3\}$

$f^{-1}[\{d\}] = \emptyset$

Особине директне и инверзне слике:

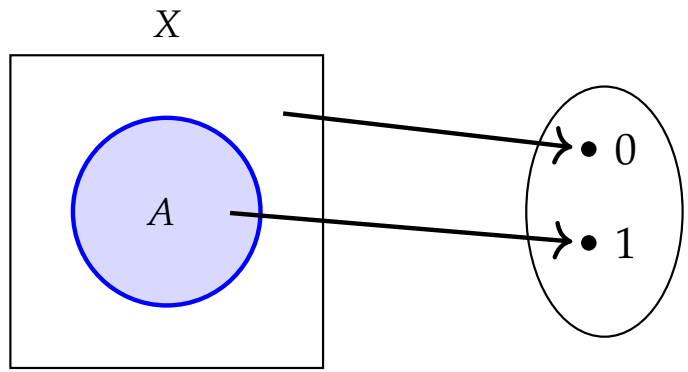
Нека је $f : X \to Y$ и $A, A_1, A_2 \subseteq X, B, B_1, B_2 \subseteq Y$. Тада важи:

1. Ако је $A_1 \subseteq A_2$, онда је $f[A_1] \subseteq f[A_2]$.
2. Ако је $B_1 \subseteq B_2$, онда је $f^{-1}[B_1] \subseteq f^{-1}[B_2]$.
3. Важи да је $f^{-1}[f[A]] \supseteq A$. Ако је f инјективна, тада је $f^{-1}[f[A]] = A$.
4. Важи да је $f[f^{-1}[B]] \subseteq B$. Ако је f сурјективна, тада је $f[f^{-1}[B]] = B$.

Карактеристична функција скупа

дефиниција: Нека је X било који скуп и $A \subseteq X$. **Карактеристична функција скупа** A је $\chi_A : X \to \{0,1\}$ таква да је

$$\chi_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A. \end{cases}.$$



Пример: $X = \{a,b,c,d,e,f\}$, $A = \{c,d,f\} \subseteq X$. Карактеристична функција скупа A:

$$\chi_A : X \to \{0,1\} \qquad \begin{array}{lcllcl} \chi_A(a) & = & 0 & \chi_A(d) & = & 1 \\ \chi_A(b) & = & 0 & \chi_A(e) & = & 0 \\ \chi_A(c) & = & 1 & \chi_A(f) & = & 1. \end{array}$$

теорема: За скупове A и B важи: $A = B$ ако и само ако $\chi_A = \chi_B$.
Доказ: на часу.

$Y^X = \{f \mid f : X \to Y\}$ - скуп функција које сликају скуп X у скуп Y

теорема: Функција $\Phi : \mathcal{P}(X) \to \{0,1\}^X$ дефинисана са $\Phi(A) = \chi_A$ је бијекција.
Доказ: на часу.

Нека су операције сабирања и множења на скупу $\{0,1\}$ дефинисане на следећи начин:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Збир $f+g$ и производ $f \cdot g$ функција $f, g \in \{0,1\}^X$ дефинисан је са:

$$(f+g)(x) \overset{\text{def}}{=} f(x) + g(x)$$
$$(f \cdot g)(x) \overset{\text{def}}{=} f(x) \cdot g(x).$$

Нека $f, g, h \in \{0,1\}^X$. Тада важи:

$$f + g = g + f \qquad f + (g + h) = (f + g) + h \qquad f \cdot (g + h) = f \cdot g + f \cdot h$$
$$f \cdot g = g \cdot f \qquad f \cdot (g \cdot h) = (f \cdot g) \cdot h \qquad (g + h) \cdot f = g \cdot f + h \cdot f$$

Применом претходних једнакости на карактеристичне функције добијамо следеће важне једнакости:

- $\chi_\emptyset = \mathbf{0}$, $\chi_X = \mathbf{1}$,
- $\chi_{A\cap B} = \chi_A\chi_B$,
- $\chi_{A\cup B} = \chi_A + \chi_B + \chi_A\chi_B$,
- $\chi_{A^c} = 1 + \chi_A$,
- $\chi_{A\setminus B} = \chi_A + \chi_A\chi_B$,
- $\chi_{A\triangle B} = \chi_A + \chi_B$,
- $\chi_A + \chi_A = \mathbf{0}$,
- $\chi_A\chi_A = \chi_A$.

Докази: на часу.

теорема: (**Канторова теорема**) Нека је X произвољан скуп. Постоји инјекција из X у $\mathcal{P}(X)$, али не постоји бијекција између тих скупова.

Доказ: на часу.

Дискретне структуре 1

предавање 6 (9.12.2025.)

Тема: ПРИРОДНИ БРОЈЕВИ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Аксиома доброг заснивања (регуларности)

Аксиома доброг заснивања или регуларности

Сваки непразни скуп A садржи елемент a такав да је $A \cap a = \emptyset$.

тврђење: (Последице аксиоме регуларности)

1. Не постоји скуп x такав да је $x \in x$.
2. Не постоје скупови x и y такви да $x \in y$ и $y \in x$.
3. Не постоји низ скупова $x_0, x_1, x_2, \ldots$ таквих да је $x_0 \ni x_1 \ni x_2 \ni \ldots$.

Доказ: на часу.

тврђење: Ако је $x \cup \{x\} = y \cup \{y\}$, онда је $x = y$.

Доказ: на часу.

Пеанове аксиоме

П1 0 је природан број.

П2 Ако је x природан број, онда је и x' природан број.

П3 Ако су x и y природни бројеви и $x' = y'$, онда је $x = y$.

П4 За сваки природан број x важи $x' \neq 0$.

П5 Нека је Φ својство природних бројева за које важи:

1) 0 има својство Φ;
2) Ако природан број x има својство Φ, тада и x' има својство Φ.

Тада сваки природни број има својство Φ.

0 - симбол константе
$'$ - унарни функцијски симбол

Пеанове аксиоме описују природне бројеве али не говоре на коју структуру се тачно мисли!

Фон Нојманов модел природних бројева заснован на теорији скупова:

$$0 := \emptyset,\ 1 := \{0\},\ 2 := \{0,1\},\ 3 := \{0,1,2\},\ldots$$

Прецизније, $0 := \emptyset,\ n' = n \cup \{n\}$ и $\mathbb{N} := \{0,1,2,\ldots\}$.

тврђење: Фон Нојманов модел природних бројева задовољава Пеанове аксиоме.

Доказ: на часу.

Принцип математичке индукције

Нека је Φ својство природних бројева за које важи:

1) тачно је $\Phi(0)$;
2) ако за природни број n тачно $\Phi(n)$, онда и тачно и $\Phi(n+1)$.

Тада је за сваки природни број n тачно $\Phi(n)$.

Услов 1. се назива база индукције, а услов 2. индуктивни корак. Формула $\Phi(n)$ у индуктивном кораку се назива индуктивна претпоставка. Има аритметичких тврђења која нису тачна за неколико најмањих природних бројева, али су тачна за све остале. У тим случајевима можемо користити мало измењени принцип матаматичке индукције, који гласи овако:

Нека је Φ својство природних бројева за које важи:

1) тачно је $\Phi(k)$;
2) ако за природни број $n \geq k$ тачно $\Phi(n)$, онда и тачно и $\Phi(n+1)$.

Тада је за сваки природни број $n \geq k$ тачно $\Phi(n)$.

Принцип потпуне индукције

Нека је Φ својство природних бројева и нека важи: ако је $\Phi(0), \Phi(1), \ldots, \Phi(n)$ тачно, тачно је и $\Phi(n')$, за све $n \in \mathbb{N}$. Тада важи $\Phi(n)$ за све природне бројеве n.

За природне бројеве x и y операција сабирања дефинише се са:

$$\begin{aligned} m+0 &:= m \\ m+n' &:= (m+n)'. \end{aligned}$$

тврђење: (Особине сабирања) За све природне бројеве m, n и k важи:

1. $(m+n)+k = m+(n+k)$
2. $m+0 = 0+m = m$
3. $m+1 = 1+m$
4. $m+n = n+m$
5. $m+n = 0 \Rightarrow m = 0$ и $n = 0$
6. $m+k = n+k \Rightarrow m = n$

Докази: на часу.

За бројеве $x, y \in \mathbb{N}$ за које је $x = y+z$, за неко $z \in \mathbb{N}$, дефинишемо разлику броја x и броја y као

$$x - y \stackrel{\text{def}}{=} z.$$

За природне бројеве x и y операција множења дефинише се са:

$$m \cdot 0 \stackrel{\text{def}}{=} 0$$

$$m \cdot n' \stackrel{\text{def}}{=} m \cdot n + m.$$

тврђење: (Особине множења) За све природне бројеве m, m и k важи:

1. $m \cdot (n + k) = m \cdot n + m \cdot k$
2. $(m \cdot n) \cdot k = m \cdot (n \cdot k)$
3. $0 \cdot m = 0$
4. $1 \cdot m = m$
5. $(m + n) \cdot k = m \cdot k + n \cdot k$
6. $m \cdot n = n \cdot m$
7. $m \cdot n = 0 \Rightarrow m = 0 \vee n = 0$

Доказ: на часу.

Дискретне структуре 1

предавање 7 (16.12.2025.)

Тема: ДЕЉИВОСТ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Еуклидско дељење

дефиниција: Нека су $a, b \in \mathbb{N}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{N}$ тако да је $b = a \cdot c$.

теорема: (**О Еуклидском дељењу**) Нека су $a, b \in \mathbb{N}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{N}$ који су јединствено одређени тако да је

$$a = b \cdot q + r, \ \ 0 \leq r < b.$$

Доказ: на часу.

дефиниција: Нека су $a, b \in \mathbb{Z}$. Кажемо да a дели b или да је b дељив са a и пишемо $a \mid b$ ако постоји број $c \in \mathbb{Z}$ тако да је $b = a \cdot c$.

теорема: Нека су $a, b \in \mathbb{Z}$ и $b \neq 0$. Тада постоје бројеви $q, r \in \mathbb{Z}$ који су јединствено одређени тако да је

$$a = q \cdot b + r, \ \ 0 \leq r < |b|.$$

Доказ: на часу.

НЗС и НЗД

дефиниција: Број $d \in \mathbb{N}$ је заједнички делилац природних бројева a и b ако $d \mid a$ и $d \mid b$. За такав број d кажемо да је **највећи заједнички делилац** бројева a и b ако $d' \mid d$ за сваки заједнички делилац d' тих бројева. У том случају пишемо $d = \text{нзд}(a, b)$.

дефиниција: Број $s \in \mathbb{N}$ је заједнички садржалац природних бројева a и b ако $a \mid s$ и $b \mid s$. За такав број s кажемо да је **најмањи заједнички садржалац** бројева a и b ако $s \mid s'$ за сваки заједнички садржалац s' тих бројева. У том случају пишемо $s = \text{нзс}(a, b)$.

тврђење: Ако је $a = bq + r$ онда је $\text{нзд}(a, b) = \text{нзд}(b, r)$.

Доказ: на часу.

Еуклидов алгоритам

Еуклидов алгоритам представља поступак за одређивање највећег заједничког делиоца датих целих бројева a и $b \neq 0$. Састоји се од узастопног примењивања теореме о еуклидском дељењу за целе бројеве. Прво, број a при дељењу са b даје неки количник q_1 и остатак r_1. Ако је $r_1 \neq 0$, можемо поделити b са r_1. У том случају добијамо количник q_2 и остатак r_2. Ако је $r_2 \neq 0$ настављамо поступак са бројевима r_1 и r_2. Поступак се завршава када добијемо остатак који је једнак нули. Алгоритам можемо представити шемом

$$
\begin{array}{rcll}
a & = & bq_1 + r_1, & 0 \leq r_1 < |b| \\
b & = & r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 & = & r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\
\vdots & & & \\
r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} & = & r_nq_{n+1} + r_{n+1}, & 0 \leq r_{n+1} < r_n
\end{array}
$$

тврђење: (**Безуова релација**) Ако је нзд$(a, b) = d$, онда постоје бројеви x и y тако да $ax + by = d$.

Доказ: на часу.

Еуклидов алгоритам

$a, b \in \mathbb{Z}$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Матрицу M_{n+1} добијамо од матрице M_n једном од следећих трансформација:

T1: множење врсте целим бројем и додавање другој врсти;

T2: множење врсте са -1;

T3: замена места врстама.

тврђење: Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $x = ap + bq$ и $y = as + bt$.

Доказ: на часу.

тврђење: Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $\text{нзд}(a, b) = \text{нзд}(x, y)$.

Доказ: на часу.

дефиниција: Бројеви $a, b \in \mathbb{Z}$ су **узајамно прости** ако је нзд$(a, b) = 1$.

тврђење: Ако $a \mid bc$ и нзд$(a, b) = 1$ онда $a \mid c$.
Доказ: на часу.

тврђење: Нека је $d =$ нзд(a, b), $a = da'$, $b = db'$, тада је нзд$(a', b') = 1$.
Доказ: на часу.

тврђење: Нека је $d =$ нзд(a, b), тада је нзс$(a, b) = \dfrac{|ab|}{d}$.
Доказ: на часу.

Дискретне структуре 1

предавање 7 (23.12.2025.)

Тема: ДИОФАНТОВЕ ЈЕДНАЧИНЕ.
ПРОСТИ БРОЈЕВИ. КОНГРУЕНЦИЈЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Диофантове једначине

дефиниција: Диофантова једначина је једначина са целобројним коефицијентима код које тражимо решења у скупу $\mathbb{Z}$.

Пример: Једначина $ax = b$, где су $a, b \in \mathbb{Z}$ и $a \neq 0$ је Диофантова једначина. Има решење у $\mathbb{Z}$ ако и само ако $a \mid b$.

У наставку ћемо посматрати Диофантову једначину облика

$$ax + by = c.$$

теорема: Једначина $ax + by = c$, где је $a, b \neq 0$ има целобројна решења ако и само ако $\text{нзд}(a, b) \mid c$. У том случају опште решење ове једначине је

$$\begin{aligned} x &= p\frac{c}{\text{нзд}(a,b)} + \frac{b}{\text{нзд}(a,b)} \cdot t \\ y &= q\frac{c}{\text{нзд}(a,b)} - \frac{a}{\text{нзд}(a,b)} \cdot t, \qquad t \in \mathbb{Z}, \end{aligned}$$

где су p и q добијени помоћу (обрнутог) Еуклидовог алгоритма такви да важи $ap + bq = \text{нзд}(a, b)$.

Доказ: на часу.

Прости бројеви

дефиниција: Цео број $p > 1$ је **прост** ако су једини делиоци тог броја 1 и p.
Цео број $n > 1$ који није прост је **сложен**.

тврђење: Постоји бесконачно много простих бројева.
Доказ: на часу.

тврђење: Ако је p прост број и $p \mid ab$, онда је $p \mid a$ или $p \mid b$.
Доказ: на часу.

тврђење: Сваки природан број већи од 1 је прост или се може представити као производ простих бројева.
Доказ: на часу.

теорема: (Основна теорема аритметике) Сваки природни број већи од 1 може се представити у облику производа простих бројева на јединствен начин (до на редослед простих фактора).
Доказ: на часу.

Конгруенције

дефиниција: Нека је m природни број већи од 1. Кажемо да су бројеви $a, b \in \mathbb{Z}$ конгруентни по модулу m и пишемо $a \equiv b \pmod{m}$ или $a \equiv_m b$ ако $m \mid (a-b)$.

Релација $\equiv_m$ је релација еквиваленције.

тврђење: Ако је $a \equiv a_1 \pmod{m}$ и $b \equiv b_1 \pmod{m}$ онда је

$$\begin{aligned} a+b &\equiv a_1+b_1 \pmod{m} \\ a \cdot b &\equiv a_1 \cdot b_1 \pmod{m} \\ a^n &\equiv a_1^n \pmod{m}, \text{ за све } n \geq 1. \end{aligned}$$

Доказ: на часу.

тврђење: Нека $d \mid a, b, m$ и нека је $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Тада је $a \equiv_m b$ акко $a' \equiv_{m'} b'$.

Доказ: на часу.

Када има решења и шта су решења једначине $ax \equiv b \pmod{m}$, где су $a, b \in \mathbb{Z}$?

теорема: (Вилсонова теорема) Ако је p прост број тада је

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказ: на часу.

Дискретне структуре 1

предавање 9 (27.12.2025.)

Тема: КОНГРУЕНЦИЈЕ. КИНЕСКА ТЕОРЕМА О ОСТАЦИМА. ОЈЛЕРОВА ТЕОРЕМА

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

теорема: (Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_n \geq 2$ узајамно прости у паровима и нека $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Систем конгруенција

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

има решење. Решење је јединствено у интервалу $[0, m_1 m_2 \cdots m_n)$ а опште решење је облика $x = x_0 + m_1 m_2 \cdots m_n \cdot t$, где је $t \in \mathbb{Z}$ и x_0 је решење из интервала $[0, m_1 m_2 \cdots m_n)$.

Доказ: на часу.

теорема: (Кинеска теорема о остацима (опште тврђење)) Систем конгруенција

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

има решење ако нзд$(m_i, m_j) \mid (a_i - a_j)$ за све $i \neq j$. Ако је $\overline{x}$ неко решење тог система, онда је опште решење облика $x = \overline{x} + \text{нзс}(m_1, \ldots m_k) \cdot t$, где је $t \in \mathbb{Z}$.

Доказ: на часу.

Ојлерова функција

дефиниција: Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

тврђење: Нека су $m, n > 1$ природни бројеви такви да је нзд$(m, n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ: на часу.

Последица: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда је $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

теорема: (Ојлерова теорема) Нека су a и n позитивни природни бројеви, такви да нзд$(a, n) = 1$. Тада важи $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказ: на часу.

теорема: (Мала Фермаова теорема) Ако је p прост број, тада је $a^p \equiv a$.

Доказ: на часу.

Дискретне структуре 1

предавање 10 (3.1.2026.)

Тема: КАРДИНАЛНОСТ. ПРЕБРОЈИВИ И НЕПРЕБРОЈИВИ СКУПОВИ.

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Кардиналност скупова

дефиниција: Нека су A и B скупови.

- Кажемо да је скуп A кардиналности мање или једнаке од B, и пишемо $|A| \leq |B|$, ако постоји функција $A \overset{''1-1''}{\longrightarrow} B$.
- Кажемо да је кардиналност скуп A једнака кардиналности скупа B, и пишемо $|A| = |B|$, ако постоји функција $A \overset{''\text{на}''}{''1-1''} \longrightarrow B$.
- Кажемо да је скуп A кардиналности строго мање од B, и пишемо $|A| < |B|$, ако је $|A| \leq |B|$ и $|A| \neq |B|$.

Особине кардиналности:

Нека су A, B, C скупови. Тада важи:

1. $|A| = |A|$.
2. Ако је $|A| = |B|$, онда је $|B| = |A|$.
3. Ако је $|A| = |B|$ и $|B| = |C|$, тада је $|A| = |C|$.
4. Ако је $|A| = |B|$, онда је $|A| \leq |B|$ и $|B| \leq |A|$.
5. Ако је $|A| \leq |B|$ и $|B| \leq |C|$, онда је $|A| \leq |C|$.
6. (Кантор-Бернштајнова теорема) Ако је $|A| \leq |B|$ и $|B| \leq |A|$, онда је $|A| = |B|$.
7. (Берштајнова теорема) За свака два скупа A и B важи $|A| \leq |B|$ или $|B| \leq |A|$.

Докази: на часу.

Пребројиви скупови

дефиниција: Скуп A је **пребројив** ако је исте кардиналности као и скуп природних бројева (тј. $|A| = |\mathbb{N}|$). Ознака за $|\mathbb{N}| = \aleph_0$ (алеф-нула).

дефиниција: Скуп A је **коначан** ако постоји природан број n такав да постоји бијекција $f : A \to \{1, 2, \cdots, n\}$. Ако A није коначан, кажемо да је **бесконачан**.

Скуп A је бесконачан ако и само ако постоји прави подскуп $A' \subset A$ такав да су A и A' у бијекцији.

тврђење: Скуп природних бројева је бесконачан.
Доказ: на часу.

дефиниција: Ако је скуп A коначан или пребројив, кажемо да је **највише пребројив**. Ако скуп није највише пребројив, онда је **непребројив**.

(Не)пребројивост

Примери пребројивих скупова:

1. $\mathbb{Z}$ је пребројив.
2. Ако је $A \subseteq \mathbb{N}$, онда је A пребројив.
3. $\mathbb{N} \times \mathbb{N}$ је пребројив.
4. Ако је $\mathcal{P}_{fin}(X) = \{A \subseteq X \mid A \text{ је коначан}\}$, тада је $\mathcal{P}_{fin}(\mathbb{N})$ пребројив.
5. $\mathbb{Q}$ је пребројив.

Докази: на часу.

Примери скупова који нису пребројиви:

1. $\mathbb{R}$ није пребројив.
2. $\mathcal{P}(\mathbb{Q})$ није пребројив.
3. $\mathcal{P}(\mathbb{N})$ није пребројив.
4. $\mathbf{2}^{\mathbb{N}}$ није пребројив.

Докази: на часу.

дефиниција: Скуп A је **моћи континуума** ако је $|A| = |\mathbb{R}|$. Ознака за $|\mathbb{R}| = \boldsymbol{c}$.

Дискретне структуре 1

предавање 11 (20.01.2026.)

Тема: БУЛОВЕ АЛГЕБРЕ

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Увео их је Џорџ Бул средином 19. века.

дефиниција: Алгебарска структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\curlyvee$ и $\curlywedge$ су бинарне а $'$ је унарна операција на скупу B, је **Булова алгебра** уколико су задовољене следеће аксиоме:

A1: $x \curlyvee y = y \curlyvee x$,

A2: $x \curlywedge y = y \curlywedge x$,

A3: $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$,

A4: $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$,

A5: $x \curlyvee 0 = x$,

A6: $x \curlywedge 1 = x$,

A7: $x \curlyvee x' = 1$,

A8: $x \curlywedge x' = 0$,

A9: $0 \neq 1$.

за свако $x, y, z \in B$.

Операције $\curlyvee$, $\curlywedge$ и $'$ редом називамо буловска дисјункција, буловска конјункција и буловски комплемент. Када је у неком контексту јасно да се ради о буловским операцијама тада их краће називамо конјункција, дисјункција и комплемент. Скуп B називамо домен. Уколико је скуп B коначан, тада је кажемо да је Булова алгебра $\mathbb{B}$ коначна, иначе кажемо да је бесконачна.

Пример 1: (Прекидачка алгебра) Алгебарска структура
$\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$, где су операције $\vee$, $\wedge$ и $\neg$ дефинисане на следећи начин:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$\neg$	
0	1
1	0

је Булова алгебра. Овако дефинисане операције су, у ставри, логичка дисјункција ($\vee$), логичка конјункција ($\wedge$) и негација ($\neg$).

Пример 2: (Алгебра партитивног скупа) Нека је X произвољан непразан скуп и $\mathcal{P}(X)$ партитивни скуп скупа X. Скуп $\mathcal{P}(X)$ заједно са операцијама уније, пресека и скуповног комплементирања (у односу на скуп X) и истакнутим елементима $\emptyset$ и X чини Булову алгебру $\boldsymbol{\mathcal{P}(X)} = (\mathcal{P}(X), \cup, \cap, ^c, \emptyset, X)$. Ако $A, B, C \in \mathcal{P}(X)$, једнакости Булове алгебре

A1: $A \cup B = B \cup A$,

A2: $A \cap B = B \cap A$,

A3: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

A4: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

A5: $A \cup \emptyset = A$,

A6: $A \cap X = A$,

A7: $A \cup A^c = X$,

A8: $A \cap A^c = \emptyset$,

A9: $X \neq \emptyset$.

су познати скуповни идентитети.

Принцип дуалности

Идентитети F_1 и F_2 су **дуални** ако се идентитет F_2 може добити од идентитета F_1 тако што се свако појављивање операције $\curlyvee$ замени са $\curlywedge$, свако појављивање операције $\curlywedge$ замени са $\curlyvee$, свако појављивање 0 замени са 1 и свако појављивање 1 замени са 0.

Пример: Идентитети $(x \curlyvee y) \curlywedge y' = x$ и $(x \curlywedge y) \curlyvee y' = x$ су дуални идентитети, као и идентитети $(x \curlywedge 0) \curlywedge (1 \curlyvee x) = x' \curlyvee 0$ и $(x \curlyvee 1) \curlyvee (0 \curlywedge x) = x' \curlywedge 1$.

Нека је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ произвољан Булов исказ. Тада је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ теорема акко је $\phi(\curlywedge, \curlyvee, ', 1, 0)$ теорема. Аксиоме су дуалне и принцип дуалности је директна последица тога.

У произвољној Буловој алгебри $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ за све $x, y, z \in B$ важе следећи идентитети:

1. $0' = 1$, $1' = 0$;
2. $x \curlyvee x = x$, $x \curlywedge x = x$ (*закон идемпотеције*);
3. $x \curlyvee (x \curlywedge y) = x$, $x \curlywedge (x \curlyvee y) = x$ (*закон апсорпције*);
4. Ако је $x \curlyvee y = 1$ и $x \curlywedge y = 0$, тада је $x = y'$. (*јединственост комплемента*)
5. $(x')' = x$ (*закон инволуције*);
6. $x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z$, $x \curlywedge (y \curlywedge z) = (x \curlywedge y) \curlywedge z$ (*закон асоцијативности*);
7. $(x \curlywedge y)' = x' \curlyvee y'$, $(x \curlyvee y)' = x' \curlywedge y'$ (*Де Морганови закони*).

Булово уређење

Нека је структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ Булова алгебра. На скупу B можемо дефинисати релацију парцијалног уређења на следећи начин:

$$x \preccurlyeq y \quad \text{акко} \quad x \curlywedge y = x.$$

Пар $(B, \preccurlyeq)$ је парцијално уређени скуп. Уколико је домен B коначан, Булову алгебру $\mathbf{B}$ можемо представити графички помоћу Хасеовог дијаграма.

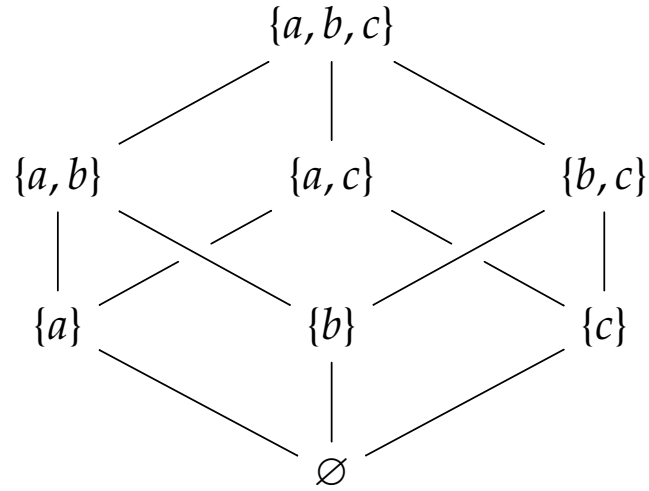
Пример: Посматрајмо Булову алгебру

$$\boldsymbol{\mathcal{P}(\{a,b,c\})} = (\mathcal{P}(\{a,b,c\}), \cup, \cap, ^c, \emptyset, \{a,b,c\}).$$

На скупу $\mathcal{P}(\{a,b,c\})$ дефинисано је Булово уређење $\preccurlyeq$ са:

$$A \preccurlyeq B \quad \text{акко} \quad A \cap B = A \quad \text{акко} \quad A \subseteq B.$$

Булова алгебра $\boldsymbol{\mathcal{P}(\{a,b,c\})}$ представљена помоћу Хасеовог дијаграма:



Пример: На скупу $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ делилаца броја 30, дефинисане су бинарне операције нзс(x, y) и нзд(x, y) и унарна операција $30/x$, за све $x, y \in B$. Структура $\mathbf{D_{30}} = (D_{30}, \text{нзс}, \text{нзд}, 30/, 1, 30)$ је Булова алгебра. За све $x, y \in D_{30}$, испуњени су следећу услови:

A1: $\text{нзс}(x, y) = \text{нзс}(y, x)$,

A2: $\text{нзд}(x, y) = \text{нзд}(y, x)$,

A3: $\text{нзс}(x, \text{нзд}(y, z)) = \text{нзд}(\text{нзс}(x, y), \text{нзс}(x, z))$,

A4: $\text{нзд}(x, \text{нзс}(y, z)) = \text{нзс}(\text{нзд}(x, y), \text{нзд}(x, z))$,

A5: $\text{нзс}(x, 1) = x$,

A6: $\text{нзд}(x, 30) = x$,

A7: $\text{нзс}(x, 30/x) = 30$,

A8: $\text{нзд}(x, 30/x) = 1$,

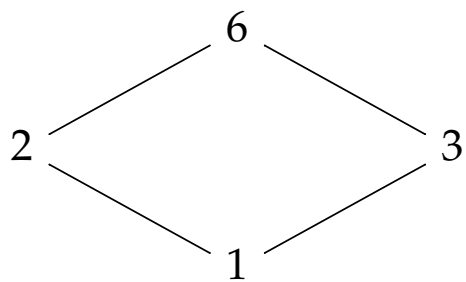
A9: $1 \neq 30$.

Генерално, уколико је природан број n производ различитих простих бројева и D_n скуп свих делилаца броја n, тада је структура $\mathbf{D_n} = (D_n, \text{нзс}, \text{нзд}, n/, 1, n)$ Булова алгебра. Булово уређење $\preccurlyeq$ на скупу D_n дефинисано је са:

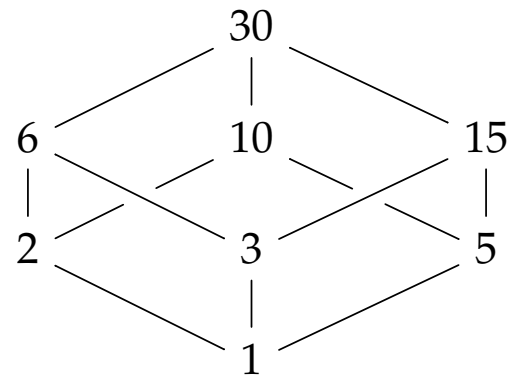
$$x \preccurlyeq y \quad \text{акко} \quad \text{нзд}(x, y) = x \quad \text{акко} \quad x \mid y.$$

Хасеови дијаграми парцијално уређених скупова $(D_6, |)$ и $(D_{30}, |)$. ($D_6 = \{1, 2, 3, 6\}$ и $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$)

D_6 :



D_{30} :



Атоми

дефиниција: Нека је $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ произвољна Булова алгебра. Елемент $a \in B$ је **атом** уколико важи следеће:

1) $0 \prec a$;
2) ако постоји $y \in B$ такво да је $0 \preccurlyeq y \preccurlyeq a$, тада је $y = 0$ или је $y = a$.

У генералном случају, Булова алгебра не мора да садржи атоме. Уколико Булова алгебра не садржи ниједан атом, кажемо да је **безатомична**. Коначне Булове алгебре увек имају атоме. Шта више, сваки елемент произвољне коначне Булове алгебре може се представити као буловска дисјункција атома.

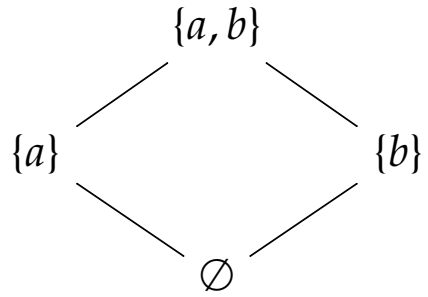
тврђење: Нека је $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ коначна Булова алгебра, тада важи следеће:

1. Ако је $x \neq 0$ и $x \in B$, тада постоји атом $a \in B$ такав да је $a \preccurlyeq x$.
2. Ако је $x \neq 0$ и $x \in B$, тада је $x = \curlyvee\{a \mid a \in B \text{ је атом и } a \preccurlyeq x\}$.

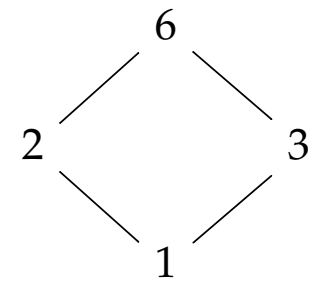
Доказ: на часу.

Хасеови дијаграми Булових алгебри

$$\boldsymbol{\mathcal{P}(\{a,b\})} = \left(\mathcal{P}(\{a,b\}), \cup, \cap, ^C, \emptyset, \{a,b\}\right) \quad \text{и} \quad \mathbf{D_6} = (\{1,2,3,6\}, \text{нзс}, \text{нзд}, 6/, 1, 6)$$



и



Претходна два дијаграма су идентична (до на ознаку елемената). Табеле операција ових Булових алгебри разликују се до на ознаку елемената и ознаку операција.

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

$\longleftrightarrow$

нзс	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

$\longleftrightarrow$

нзд	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

A	A^C
$\emptyset$	$\{a,b\}$
$\{a\}$	$\{b\}$
$\{b\}$	$\{a\}$
$\{a,b\}$	$\emptyset$

$\longleftrightarrow$

x	$6/x$
1	6
2	3
3	2
6	1

Изоморфизам Булових алгебри

дефиниција: Булове алгебре $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ и $\mathbf{B^*} = (B^*, \curlyvee^*, \curlywedge^*, '^*, 0^*, 1^*)$ су *изоморфне* уколико постоји бијекција $f : B \to B^*$ за коју важи:

1) $f(x \curlyvee y) = f(x) \curlyvee^* f(y)$,
2) $f(x \curlywedge y) = f(x) \curlywedge^* f(y)$,
3) $f(x') = f(x)'^*$,

за све $x, y \in B$. Изоморфизам Булових алгебри $\mathbf{B}$ и $\mathbf{B^*}$ означавамо са: $\mathbf{B} \cong \mathbf{B^*}$.

теорема: (Стонова теорема) Ако је $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ коначна Булова алгебра тада постоји коначан скуп S такав да је $\mathbf{B} \cong \boldsymbol{\mathcal{P}(S)}$.

Доказ: на часу.

Коначну Булова алгебру могуће је конструисати само на скуповима који имају 2^m елеменатам, где је $m \geq 1$.

Дискретне структуре 1

предавање 12 (27.01.2026.)

Тема: ИСКАЗНА ЛОГИКА

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Исказна алгебра

исказна алгебра: $\mathbf{2} = \{0, 1\}$

унарна операциј:

p	$\neg p$
0	1
1	0

бинарне операције:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

p	q	$p \veebar q$
0	0	0
0	1	1
1	0	1
1	1	0

Језик исказне алгебре $\mathcal{L}$:

- логичке константе $\{\top, \bot\}$
- пребројиви скуп исказних слова $\mathcal{P}$
- логички везници
- заграде $(,)$

Формуле језика $\mathcal{L}$:

1° исказна слова и логичке константе су исказне формуле

2° ако су A и B исказне формуле, тада су исказне формуле и

$$\neg A, \quad (A \wedge B), \quad (A \vee B), \quad (A \Rightarrow B), \quad (A \Leftrightarrow B), \quad (A \veebar B)$$

- исказне формуле се добијају једино коначном применом правила 1° и 2°

For $\mathcal{L}$ – скуп формула над језиком $\mathcal{L}$

Да бисмо избегли гомилање заграда уводимо правило брисања спољасњих заграда и приоритет операција. Највећи приоритет има операција $\neg$, средњег приоритета су операције $\wedge$ и $\vee$, а најмањег операције $\Rightarrow, \Leftrightarrow, \veebar$.

$$\begin{array}{cc} (\neg p) \wedge q & \neg p \wedge q \\ (p \vee q) \Leftrightarrow r & p \vee q \Leftrightarrow r \\ ((p \veebar q) \wedge (\neg r)) \Rightarrow (p \vee (q \wedge r)) & (p \veebar q) \wedge \neg r \Rightarrow p \vee (q \wedge r) \end{array}$$

дефиниција: *Валуација* је било која функција $v : \mathcal{P} \to \{0,1\}$.

Пример: $\mathcal{P} = \{p, q, r\}$.

Са $v(p) = 0$, $v(q) = 1$ и $v(r) = 0$ је задата једна валуација.

$$v : \begin{pmatrix} p & q & r \\ 0 & 1 & 0 \end{pmatrix}.$$

Сваку валуацију $v : \mathcal{P} \to \{0,1\}$ можемо продужити до функције $v : For \to \{0,1\}$ на следећи начин:

$$\begin{aligned} v(\neg A) &= \neg v(A) \\ v(A \wedge B) &= v(A) \wedge v(B) \\ v(A \vee B) &= v(A) \vee v(B) \\ v(A \Rightarrow B) &= v(A) \Rightarrow v(B) \\ v(A \Leftrightarrow B) &= v(A) \Leftrightarrow v(B) \\ v(A \veebar B) &= v(A) \veebar v(B), \end{aligned}$$

за све $A, B \in For$.

Пример: $\mathcal{P} = \{p, q, r\}$

$v : \mathcal{P} \to \{0, 1\}$ дата са $v(p) = 0$, $v(q) = 1$ и $v(r) = 0$.

$v' : \mathcal{P} \to \{0, 1\}$ дата са $v'(p) = 0$, $v'(q) = 0$ и $v'(r) = 1$

$$\begin{aligned} v\big((p \vee q) \Rightarrow (p \vee r)\big) &= v(p \vee q) \Rightarrow v(p \vee r) \\ &= (v(p) \vee v(q)) \Rightarrow (v(p) \vee v(r)) \\ &= (0 \vee 1) \Rightarrow (0 \vee 0) \\ &= 1 \Rightarrow 0 \\ &= 0, \end{aligned}$$

$$\begin{aligned} v'\big((p \vee q) \Rightarrow (p \vee r)\big) &= v'(p \vee q) \Rightarrow v'(p \vee r) \\ &= (v'(p) \vee v'(q)) \Rightarrow (v'(p) \vee v'(r)) \\ &= (0 \vee 0) \Rightarrow (0 \vee 1) \\ &= 0 \Rightarrow 1 \\ &= 1, \end{aligned}$$

дефиниција: Формула A је *таутологија* ако је $v(A) = 1$ за све валуације v. Ако за сваку валуацију v важи $v(A) = 0$, онда кажемо да је A *контрадикција*.

дефиниција: Формула A је *задовољива* ако постоји валуација v тако да је $v(A) = 1$. Скуп формула Φ је задовољив ако постоји валуација v тако да је $v(A) = 1$ за све формуле $A \in \Phi$.

дефиниција: Формула A је *порецива* ако постоји валуација v тако да је $v(A) = 0$.

дефиниција: Формуле A и B су *логички (елементарно, семантички) еквивалентне* ако за сваку валуацију v важи $v(A) = v(B)$. Пишемо $A \equiv B$.

$\equiv$ је релација еквиваленције

$(\mathrm{For}\,\mathcal{L}/\equiv, \vee, \wedge, ', 0, 1)$ – Линденбаум-Тарски алгебра

дефиниција: Формула A је *логичка (семантичка) последица* формуле B ако за сваку валуацију v за коју је $v(B) = 1$ важи да је $v(A) = 1$.
ознака: $B \models A$

формула A је логичка последица формуле B ако и само ако је $B \Rightarrow A$ таутологија

Следеће формуле су таутологије:

$p \wedge p \Leftrightarrow p$	закон идемпотентности за конјункцију
$p \vee p \Leftrightarrow p$	закон идемпотентности за дисјункцију
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	закон асоцијативности за дисјункцију
$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	закон асоцијативности за конјункцију
$p \wedge q \Leftrightarrow q \wedge p$	закон комутативности за конјункцију
$p \vee q \Leftrightarrow q \vee p$	закон комутативности за дисјункцију
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	закон дистрибуције конјункције према дисјункцији
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	закон дистрибуције дисјункције према конјункцији
$\neg\neg p \Leftrightarrow p$	закон двоструке негације
$p \vee \neg p$	закон искључења трећег
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	Де Морганов закон
$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	Де Морганов закон
$p \wedge q \Rightarrow p$	слабљење конјункције
$p \Rightarrow p \vee q$	увођење дисјункције
$p \Rightarrow p$	закон рефлексивности за импликацију
$p \Leftrightarrow p$	закон рефлексивности за еквиваленцију
$p \wedge (p \vee q) \Leftrightarrow p$	закон апсорпције конјункције према дисјункцији
$p \vee (p \wedge q) \Leftrightarrow p$	закон апсорпције дисјункције према конјункцији
$(p \wedge (p \Rightarrow q)) \Rightarrow q$	модус поненс
$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$	правило уклањања импликације
$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$	правило уклањања еквиваленције
$(p \veebar q) \Leftrightarrow \neg(p \Leftrightarrow q)$	правило уклањања ексклузивне дисјункције
$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$	закон транзитивности за импликацију
$((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Rightarrow (p \Leftrightarrow r)$	закон транзитивности за еквиваленцију
$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	закон контрапозиције

Нормалне форме

Литерал – логичко слово или негација логичког слова

дефиниција: Логичка формула је у *дисјунктивној нормалној форми*, краће ДНФ, ако је облика

$$F_1 \vee F_2 \vee \cdots \vee F_k,$$

где је за свако $i \in \{1, 2, \ldots, k\}$, формула F_i конјункција литерала.

дефиниција: Логичка формула је у *конјунктивној нормалној форми*, краће КНФ, ако је облика

$$F_1 \wedge F_2 \wedge \cdots \wedge F_k,$$

где је за свако $i \in \{1, 2, \ldots, k\}$, формула F_i дисјункција литерала.

Пример:

формула $\neg p \vee (\neg q \wedge r) \vee (p \wedge q \wedge r)$ је у дисјунктивној нормалној форми

формула $(p \vee \neg q) \wedge (p \vee r) \wedge (\neg p \vee q \vee \neg r)$ у конјунктивној нормалној форми.

КНФ-ДНФ алгоритам

свака логичка формула еквивалентна је некој формули која је у дисјунктивној/конјунктивној нормалној форму

КНФ-ДНФ алгоритам:

1° елиминишемо везнике који се примењују на логичке константе $\top$ и $\bot$

2° елиминишемо $\veebar$ користећи $p \veebar q \equiv \neg(p \Leftrightarrow q)$

3° елиминишемо $\Leftrightarrow$ користећи $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

4° елиминишемо $\Rightarrow$ користећи $p \Rightarrow q \equiv \neg p \vee q$

5° примењујемо Де Морганове законе $\neg(p \wedge q) \equiv \neg p \vee \neg q$ и $\neg(p \vee q) \equiv \neg p \wedge \neg q$ докле год је могуће

6° елиминишемо дупле негације користећи $\neg\neg p \equiv p$

7° у зависности од тога да ли желимо да добијемо КНФ или ДНФ примењујемо законе дистрибуције:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r),$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Пример: $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$.

$$\begin{aligned}
(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r) &\equiv \neg(\neg p \vee q) \vee (\neg(\neg q \vee r) \vee (\neg p \vee r)) \\
&\equiv (p \wedge \neg q) \vee ((q \wedge \neg r) \vee (\neg p \vee r)) \\
&\equiv (p \wedge \neg q) \vee ((q \vee \neg p \vee r) \wedge (\neg r \vee \neg p \vee r)) \\
&\equiv (p \wedge \neg q) \vee ((q \vee \neg p \vee r) \wedge (\neg p \vee \top)) \\
&\equiv (p \wedge \neg q) \vee ((q \vee \neg p \vee r) \wedge \top) \\
&\equiv (p \wedge \neg q) \vee q \vee \neg p \vee r \\
&\equiv (p \vee q \vee \neg p \vee r) \wedge (\neg q \vee q \vee \neg p \vee r)
\end{aligned}$$

ДНФ: $(p \wedge \neg q) \vee q \vee \neg p \vee r$,
КНФ: $(p \vee q \vee \neg p \vee r) \wedge (\neg q \vee q \vee \neg p \vee r)$.

конјунктивна и дисјунктивна нормална форма нису јединствене у синтаксном смислу:

$(p \wedge r) \vee (q \wedge \neg r)$ и $(p \wedge q) \vee (p \wedge r) \vee (q \wedge \neg r)$ су логички еквивалентне
$(p \vee r) \wedge (q \vee \neg r)$ и $(p \vee q) \wedge (p \vee r) \wedge (q \vee \neg r)$ су логички еквивалентне

Савршене нормалне форме

исказна формула A у којој се појављују искључиво исказна слова $p_1, p_2, \ldots, p_k$ може се представити у следеће две форме:

1° $SDNF(A) = \bigvee_{u \in \{v \mid v(A)=1\}} \left(p_1^{u(p_1)} \wedge p_2^{u(p_2)} \wedge \cdots \wedge p_k^{u(p_k)} \right)$ – савршена (или канонска или потпуна) дисјунктивна нормална форма формуле A (краће СДНФ),

2° $SKNF(A) \equiv \bigwedge_{u \in \{v \mid v(A)=0\}} \left(p_1^{u(\neg p_1)} \vee p_2^{u(\neg p_2)} \vee \cdots \vee p_k^{u(\neg p_k)} \right)$ – савршена (или канонска или потпуна) конјунктивна нормална форма формуле A (краће СКНФ),

где је $p_i^0 := \neg p_i$, а $p_i^1 := p_i$.

Пример: $A = p \Leftrightarrow (q \Leftrightarrow r)$.

	p	q	r	$q \Leftrightarrow r$	$A = p \Leftrightarrow (q \Leftrightarrow r)$
v_1	0	0	0	1	0
v_2	0	0	1	0	1
v_3	0	1	0	0	1
v_4	0	1	1	1	0
v_5	1	0	0	1	1
v_6	1	0	1	0	0
v_7	1	1	0	0	0
v_8	1	1	1	1	1

$\{v \mid v(A) = 1\} = \{v_2, v_3, v_5, v_8\}$ па је СДНФ формуле A:

$$(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$$

$\{v \mid v(A) = 0\} = \{v_1, v_4, v_6, v_7\}$ па је СКНФ формуле A:

$$(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$$

Дискретне структуре 1

предавање 13 (03.02.2026.)

Тема: ПРЕДИКАТСКА ЛОГИКА

Александра Костић Матијевић

Катедра за алгебру и математичку логику

Математички факултет, Београд

Језик предикатске логике

Језик предикатске логике чине:

- скуп променљивих *Var* (променљиве обично означавамо са $x, y, z, \ldots$);
- логички везници: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
- квантификатори $\forall$ и $\exists$;
- интерпункцијски знаци (зарез, лева и десна заграда): , ( ) ;
- знак једнакости =;
- скуп функцијских (или операцијских) симбола *Fun* (обично ћемо их означавати са $f, g, h, \ldots$);
- скуп релацијских (или предикатских) симбола *Rel* (обично ћемо их означавати са $p, q, r, \ldots$);
- скуп константи *Const* (обично ћемо их означавати са $a, b, c, \ldots$).

Релацијски и функцијски симболи имају своју *дужину* која је природан број $n > 0$ и која се назива и *арност* релације или функције. Означавамо је са *ar*.

Избором скупова *Fun*, *Rel*, *Const* бирамо конкретан језик предикатске логике.

$$\mathcal{L} = Fun \sqcup Rel \sqcup Const$$

Синтакса предикатске логике

Терми језика $\mathcal{L}$:

1° Променљиве и константе су терми.

2° Ако су $t_1, \ldots, t_n$ терми и f функцијски симбол дужине n онда је $f(t_1, \ldots, t_n)$ терм.

3° Терми се могу добити једино коначном применом правила 1° и 2°. Скуп терма означавамо са *Term*.

Атомичке формуле језика $\mathcal{L}$:

1° Ако су t_1 и t_2 терми, онда је $t_1 = t_2$ атомичка формула.

2° Ако су $t_1, \ldots, t_n$ терми и p релацијски симбол дужине n, онда је $p(t_1, \ldots, t_n)$ атомичка формула.

Формуле језика $\mathcal{L}$:

1° Атомичка формула је формула.

2° Ако су A и B формуле, онда су формуле и

$$\neg A, \quad (A \wedge B), \quad (A \vee B), \quad (A \Rightarrow B), \quad (A \Leftrightarrow B), \quad \forall x A \quad \text{и} \quad \exists x A.$$

3° Формуле се добијају једино коначном применом правила 1° и 2°. Скуп формула означавамо са *For*.

Синтакса предикатске логике

приоритет операција:

$$\neg \qquad \forall \qquad \exists$$

$$\wedge \qquad \vee$$

$$\Rightarrow \qquad \Leftrightarrow \qquad \veebar$$

Пример:

$Fun = \{f, g\}$, $Rel = \{p, q\}$ и $Const = \{a\}$

$ar(f) = ar(q) = 1$ и $ar(g) = ar(p) = 2$

$\forall x \forall y p(x, y)$	формула
$g(f(x), a)$	терм
$\forall x f(x)$	ни терм ни формула
$g(x, y) = a$	формула (атомичка)
$p(x, q(x))$	ни терм ни формула
$\forall x(p(x, y) \Rightarrow g(x, y))$	ни терм ни формула

Семантика предикатске логике

дефиниција: Нека је $\mathcal{L}$ језик предикатске логике. *Структура језика* $\mathcal{L}$ (или $\mathcal{L}$-*структура*) у ознаци $\mathbb{M}$ се састоји од:

- непразног скупа M;
- функције $f^{\mathbb{M}} : M^n \to M$ дужине n за сваки функцијски симбол $f \in Fun$;
- релације $p^{\mathbb{M}}$ дужине n на скупу M за сваки релацијски симбол $p \in Rel$;
- елемента $a^{\mathbb{M}} \in M$ за сваки симбол константе $a \in Const$.

$$\mathbb{M} = \left(M, \ldots, f^{\mathbb{M}}, \ldots, p^{\mathbb{M}}, \ldots, a^{\mathbb{M}}\right)$$

Пример:

$Fun = \{f, g\}$, $Rel = \{p, q\}$ и $Const = \{a\}$

$ar(f) = ar(q) = 1$ и $ar(g) = ar(p) = 2$

$\mathcal{L}$-структура $\left(\mathbb{N}, f^{\mathbb{N}}, g^{\mathbb{N}}, p^{\mathbb{N}}, q^{\mathbb{N}}, a^{\mathbb{N}}\right)$ можемо дефинисати са:

$$f^{\mathbb{N}}(x) = x + 1, \qquad p^{\mathbb{N}}(x, y) = 1 \text{ ако је } x \leqslant y,$$
$$g^{\mathbb{N}}(x, y) = x + y, \qquad q^{\mathbb{N}}(x) = 1 \text{ ако је } x \text{ прост број.}$$
$$a^{\mathbb{N}} = 0$$

Семантика предикатске логике

дефиниција: *Валуација* v за скуп променљивих Var у односу на домен M је свако пресликавање $v : Var \to M$. Ако је $v(x) = a \in M$, онда кажемо да је a вредност променљиве x у валуацији v. Нека су v и w две валуације за исти скуп променљивих и у односу на исти домен. Кажемо да су v и w x-близу, ако је $v(y) = w(y)$ за сваку променљиву y која је различита од x и пишемо $v \sim_x w$.

Валуације v можемо продужити са скупа Var на скуп $Term$:

- ако је t променљива x, онда је $v(t) = v(x)$;
- ако је t симбол константе a, онда је $v(t) = a^{\mathbb{M}}$;
- ако је t једнак $f(t_1, \ldots, t_n)$ за $f \in Fun$, онда је $v(t) = f^{\mathbb{M}}(v(t_1), \ldots, v(t_n))$.

Пример: $v = \begin{pmatrix} x & y & \cdots \\ 2 & 7 & \cdots \end{pmatrix}$

$$
\begin{aligned}
v(g(x,a)) &= g^{\mathbb{N}}(v(x), v(a)) = g^{\mathbb{N}}(2, a^{\mathbb{N}}) = g^{\mathbb{N}}(2,0) = 2+0 = 2 \\
v(f(g(x,y))) &= f^{\mathbb{N}}(v(g(x,y))) = f^{\mathbb{N}}(g^{\mathbb{N}}(v(x), v(y))) = f^{\mathbb{N}}(g^{\mathbb{N}}(2,7)) = f^{\mathbb{N}}(2+7) \\
&= f^{\mathbb{N}}(9) = 9+1 = 10 \\
v(g(f(x), f(a))) &= g^{\mathbb{N}}(v(f(x)), v(f(a))) = g^{\mathbb{N}}(f^{\mathbb{N}}(v(x)), f^{\mathbb{N}}(v(a))) = g^{\mathbb{N}}(f^{\mathbb{N}}(2), f^{\mathbb{N}}(a^{\mathbb{N}})) \\
&= g^{\mathbb{N}}(2+1, f^{\mathbb{N}}(0)) = g^{\mathbb{N}}(3, 0+1) = g^{\mathbb{N}}(3,1) = 3+1 = 4.
\end{aligned}
$$

Семантика предикатске логике

Истинитосна вредност формуле у валуацији v и $\mathcal{L}$-структури $\mathbb{M}$:

1° ако је A атомичка формула тако да:

- A је $t_1 = t_2$ за терме t_1 и t_2, онда је $v(A) = 1$ ако је $v(t_1) = v(t_2)$;
- A је $p(t_1, \ldots, t_n)$ за релацијски симбол p, онда је $v(A) = 1$ ако $(v(t_1), \ldots, v(t_n)) \in p^{\mathbb{M}}$;

2° ако је F формула тако да је:

- $F = \neg A$ за формулу A, онда је $v(F) = 1$ ако је $v(A) = 0$;
- $F = A \wedge B$ за формуле A и B, онда је $v(F) = 1$ једино ако је $v(A) = 1$ и $v(B) = 1$;
- $F = A \vee B$ за формуле A и B, онда је $v(F) = 0$ једино ако је $v(A) = 0$ и $v(B) = 0$;
- $F = A \Rightarrow B$ за формуле A и B, онда је $v(F) = 0$ једино ако је $v(A) = 1$ и $v(B) = 0$;
- $F = A \Leftrightarrow B$ за формуле A и B, онда је $v(F) = 1$ ако је $v(A) = v(B)$;
- $F = \forall x A$ за формулу A, онда је $v(F) = 1$ ако за сваку валуацију w тако да $w \sim_x v$ важи $w(A) = 1$;
- $F = \exists x A$ за формулу A, онда је $v(F) = 1$ ако постоји валуација w тако да $w \sim_x v$ и $w(A) = 1$.

Семантика предикатске логике

У случају да за неку предикатску формулу F важи $v(F) = 1$ за неку валуацију v и $\mathcal{L}$-структуру $\mathbb{M}$, онда кажемо да је формула F тачна у тој валуацији $\mathcal{L}$-структуре $\mathbb{M}$. Ако је $v(F) = 0$, кажемо да је F нетачна у валуацији v $\mathcal{L}$-структуре $\mathbb{M}$.

Пример: $v = \begin{pmatrix} x & y & \dots \\ 2 & 3 & \dots \end{pmatrix}$

$g(x, a) = f(f(a))$ – тачна у валуацији v

$p(g(x, y), f(a))$ – нетачна у валуацији v

$q(f(x)) \Rightarrow p(x, x)$ – тачна у валуацији v

Слободне и везане промењљиве

Ако се појављивање промењљиве x у формули F налази под утицајем квантификатора, онда кажемо да је то појављивање промењљиве *везано појављивање*. У супротном је *слободно појављивање*.

Промењљива је *слободна* у формули F ако има бар једно слободно појављивање.

Fr – скуп свих слободних промењљивих у формули F

дефиниција: Скуп свих слободних промењљивих у формулама:

- $\mathrm{Fr}(t_1 = t_2) = \mathrm{Fr}(t_1) \cup \mathrm{Fr}(t_2)$, где $t_1, t_2 \in \mathit{Term}$, а $\mathrm{Fr}(t)$ означава скуп свих промењљивих које се појављују у терму t,
- $\mathrm{Fr}(p(t_1, \ldots, t_n)) = \mathrm{Fr}(t_1) \cup \ldots \cup \mathrm{Fr}(t_n)$, где $t_1, \ldots, t_n \in \mathit{Term}$, $p \in \mathit{Rel}$ и $ar(p) = n$,
- $\mathrm{Fr}(\neg A) = \mathrm{Fr}(A)$, где $A \in \mathit{For}$,
- $\mathrm{Fr}(A \star B) = \mathrm{Fr}(A) \cup \mathrm{Fr}(B)$, где $A, B \in \mathit{For}$ и $\star \in \{\vee, \wedge, \veebar, \Rightarrow, \Leftrightarrow\}$,
- $\mathrm{Fr}(\exists x A) = \mathrm{Fr}(\forall x A) = \mathrm{Fr}(A) \setminus \{x\}$, где $A \in \mathit{For}$ и $x \in \mathit{Var}$.

Ако је $\mathrm{Fr}(F) = \{x_1, x_2, \ldots, x_n\}$, онда формулу F записујемо и као $F(x_1, x_2, ..., x_n)$ ако желимо да нагласимо да су промењљиве $x_1, x_2, \ldots, x_n$ слободне у F

Слободне и везане промењљиве

Пример:

$p(x,y)$	појављивање промењљивих x, y је слободно
$\forall x\, p(x,y)$	прво појављивање промењљиве x је везано, као и друго, док је појављивање промењљиве y слободно
$\exists x\, p(x,y) \Rightarrow q(x)$	промењљива x: прво појављивање везано, друго везано, треће слободно; промењљива y: појављивање је слободно
$\exists y(p(x,y) \Rightarrow \forall x\, p(x,y))$	промењљива x: прво појављивање слободно, друго везано, треће везано; промењљива y: прво појављивање везано, друго везано, треће везано

Вредност формуле зависи само од слободних промењљивих које се у њој појављују.

дефиниција: Формула у којој нема слободних промењљивих назива се *реченица*.

Пример:

$\forall x\, p(x, f(x))$
$\forall x \forall y(f(x) = f(y))$
$\forall x \forall y \forall z(p(x,y) \Leftrightarrow p(g(x,z), g(y,z))$

Модел и контрамодел

дефиниција: Ако за неку $\mathcal{L}$-структуру $\mathbb{M}$ и формулу F важи да је $v(F) = 1$ за сваку валуацију $v : Var \to \mathbb{M}$, онда кажемо да је $\mathcal{L}$-структура $\mathbb{M}$ *модел* за формулу F. Ако не важи $v(F) = 1$ за сваку валуацију $v : Var \to \mathbb{M}$, онда кажемо да је $\mathcal{L}$-структура $\mathbb{M}$ *контрамодел* за формулу F.

дефиниција: Ако је свака $\mathcal{L}$-структура модел за формулу F, онда кажемо да је F *ваљана*. Уколико формула F није ваљана онда је *порецива*.

дефиниција: Ако за неку $\mathcal{L}$-структуру $\mathbb{M}$ и формулу F важи да је $v(F) = 1$ при некој валуацији $v : Var \to \mathbb{M}$, онда кажемо да валуација v *задовољава* формулу F у структури $\mathbb{M}$, односно да је формула F *задовољива у структури* $\mathbb{M}$. Формула F је *задовољива* ако постоји $\mathcal{L}$-структуру $\mathbb{M}$ у којој је задовољива. Ако формула није задовољива онда кажемо да је *контрадикторна*.

Пример:

$\forall x\, p(x, f(x))$ – $\mathbb{N}$ је модел
$\forall x \forall y (f(x) = f(y))$ – $\mathbb{N}$ је контрамодел
$\forall x \forall y \forall z (p(x, y) \Leftrightarrow p(g(x, z), g(y, z))$ – $\mathbb{N}$ је модел