

Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

30. oktober 2025

Zakoni predikatnega računa

So nekateri pomembni pari enakovrednih izjavnih formul:

$$\neg \forall x W \sim \exists x \neg W$$

$$\neg \exists x W \sim \forall x \neg W$$

de Morganova zakona

$$\forall x \forall y W \sim \forall y \forall x W$$

$$\exists x \exists y W \sim \exists y \exists x W$$

zamenjava istostnih
kvantifikatorjev

$$\forall x (W \wedge V) \sim \forall x W \wedge \forall x V$$

$$\exists x (W \vee V) \sim \exists x W \vee \exists x V$$

distributivnost

Zakoni predikatnega računa z omejitvami

Če se x ne pojavi (prosto) v formuli C , potem veljajo naslednje enakovredosti:

$$\forall x (C \vee W) \sim C \vee \forall x W$$

$$\exists x (C \vee W) \sim C \vee \exists x W$$

$$\forall x (C \wedge W) \sim C \wedge \forall x W$$

$$\exists x (C \wedge W) \sim C \wedge \exists x W$$

Preneksna normalna oblika

Trditev

Vsako formulo lahko enakovredno zapišemo tako, da se kvantifikatorji nahajajo samo na začetku.

Kako?

1. Preimenujemo spremenljivke.
2. Znebimo se $\Rightarrow$ in $\Leftrightarrow$, raje imamo $\neg$, $\wedge$ in $\vee$.
3. Izvlečemo kvantifikatorje na začetek z uporabo zakonov predikatnega računa.

Zgled

prosta spremenljivka

$$\forall x A(x) \vee \exists x B(x) \Rightarrow D(x) \wedge \exists x D(x)$$

$$\begin{aligned} & \forall w A(w) \vee \exists z B(z) \Rightarrow D(x) \wedge \exists y D(y) \sim \\ & \neg (\forall w A(w) \vee \exists z B(z)) \vee (D(x) \wedge \exists y D(y)) \sim \\ & (\neg \forall w A(w) \wedge \neg \exists z B(z)) \vee \exists y (D(x) \wedge D(y)) \sim \\ & (\exists w \neg A(w) \wedge \forall z \neg B(z)) \vee \exists y (D(x) \wedge D(y)) \sim \end{aligned}$$

$$\exists y (\exists w (\neg A(w) \wedge \forall z \neg B(z)) \vee (D(x) \wedge D(y))) \sim$$

$$\exists y \exists w (\forall z (\neg A(w) \wedge \neg B(z)) \vee (D(x) \wedge D(y))) \sim$$

prevedeno normalna oblika

$$\exists y \exists w \forall z ((\neg A(w) \wedge \neg B(z)) \vee (D(x) \wedge D(y)))$$

Zgled

Zamenjava raznovrstnih kvantifikatorjev v splošnem ni možna.

$P(x, y)$... x pozna y -ona.

Včasih vseeno lahko:

$$\forall x \exists y (P(x) \wedge Q(y)) \sim \exists y \forall x (P(x) \wedge Q(y))$$

$$\forall x \exists y (P(x) \wedge Q(y)) \sim$$

$$\forall x (P(x) \wedge \exists y Q(y)) \sim$$

$$(\forall x P(x) \wedge \exists y Q(y)) \sim$$

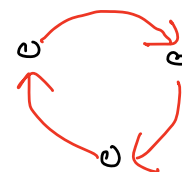
$$\exists y (\forall x P(x) \wedge Q(y)) \sim$$

$$\exists y \forall x (P(x) \wedge Q(y))$$

$$\forall x \exists y P(x, y)$$

$$\exists y \forall x P(x, y)$$

nista enakovredni



Operacije z množicami

relacija pripadnosti ... $x \in A$

x pripada A .

x je element množice A

podajanje množic

- ▶ z naštevanjem elementov $A = \{0, 1, 2\}$
- ▶ z neko izjavno formulo $A = \{x ; \varphi(x)\}$
Velja: $x \in A \iff \varphi(x)$

x ne pripada A

x ni element A

$x \notin A$

$0 \in A$ in $1 \in A$ in $2 \in A$

$A = \{0, 2, 2, 1, 0\}$

$0 \in A$ in $2 \in A$ in $2 \in A$ in
 $1 \in A$ in $0 \in A$

x je naravno število in

$A = \{x ; \underbrace{\quad}_\perp x \text{ je popoln kvadrat}\} = \{0, 1, 4, 9, 16, \dots\}$

Zgledi množic

$$A = \{x ; x \neq x\} = \emptyset \quad \text{prazna množica}$$

$$B = \{x ; x = 0 \vee x = 1 \vee x = 2\} = \{0, 1, 2\}$$

$$C = \{x ; x^2 + 1 \geq 5\} = \{x, \begin{array}{l} |x| \geq 2 \\ x \in \mathbb{R} \end{array} \}$$

↑
od kod so x'i
iz $\mathbb{R}$

$$3 \in C \quad \Leftrightarrow \quad \begin{array}{l} 3^2 + 1 \geq 5 \\ 10 \geq 5 \end{array}$$

Russellov paradoks

Ni vsaka izjavna formula dobra!

$$R = \{x; x \notin x\}$$

Ali velja $R \in R$?

2	3	7	9	1	11	8
---	---	---	---	---	----	---

tabelica naravnih
števil ni naravno število.

Ali $R \in R$?

$$R \in R \iff R \notin R$$

Če $R \in R$, potem mora zanj veljati $R \notin R$,
Če $R \notin R$, potem $R \in R$.



B. Russell 1905 opisi tečeno 2 "mavico" R .

Enakost in vsebovanost

Množici A in B sta *enaki*,

$$A = B \iff \forall x (x \in A \iff x \in B)$$

Ekvivalenca v naravnem jeziku

Množica A je *podmnožica* množice B ,

$$A \subseteq B \iff \forall x (x \in A \Rightarrow x \in B)$$

$\subseteq$

$\subset$

$\leq$

$<$

relacija *inkluzije*

Množica A je *prava podmnožica* množice B ,

$$A \subset B \iff A \subseteq B \wedge A \neq B$$

relacija *stroge inkluzije*

Enakost in vsebovanost

Trditev

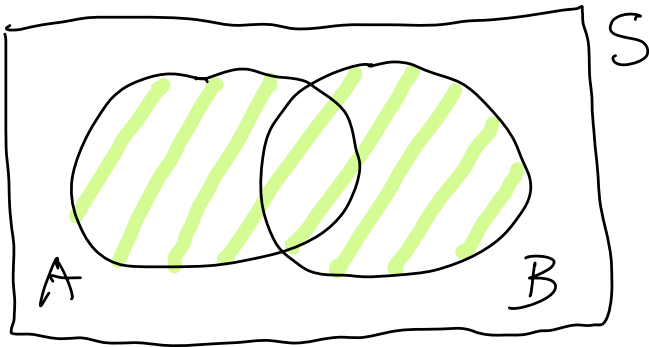
Za poljubne množice A , B in C velja

- ▶ $\emptyset \subseteq A$
- ▶ $A \subseteq A$
- ▶ Če $A \subseteq B$ in $B \subseteq C$, potem $A \subseteq C$.

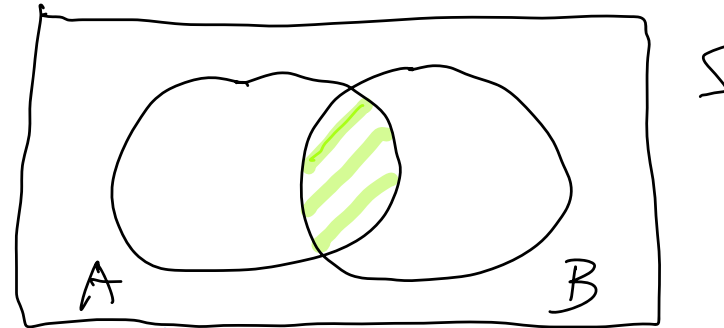
$$\begin{array}{ll} \emptyset \subseteq A & \dots \quad \forall x (x \in \emptyset \Rightarrow x \in A) \\ A \subseteq A & \dots \quad \forall x (x \in A \Rightarrow x \in A) \end{array}$$

Operacije z množicami

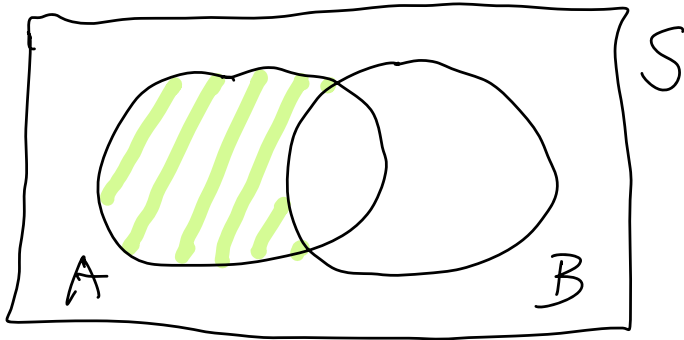
- ▶ *unija* $A \cup B = \{x; x \in A \vee x \in B\}$
- ▶ *presek* $A \cap B = \{x; x \in A \wedge x \in B\}$
- ▶ *razlika* $A \setminus B = \{x; x \in A \wedge x \notin B\}$... *A brez B*
- ▶ *simetrična razlika* $A + B = \{x; x \in A \vee x \in B\}$



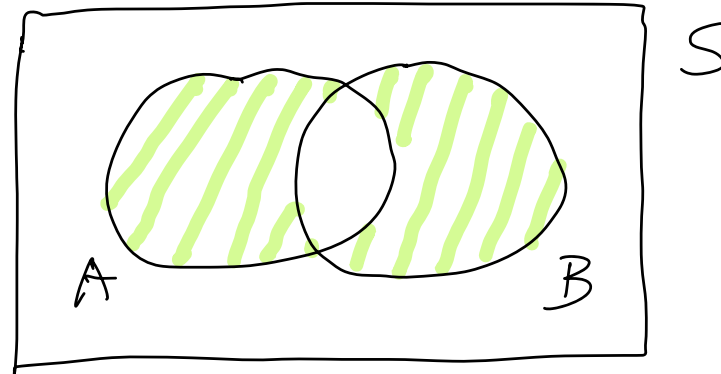
$A \cup B$



$A \cap B$



$A \setminus B$



$A + B$

Lastnosti operacij

► $A = B \iff A \subseteq B \wedge B \subseteq A$

► $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$

► $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$

► $A \cap B \subseteq A \subseteq A \cup B$

} usklajenost $\subseteq$ z $\cup, \cap$

$$3 \leq 5$$

$$3+2 \leq 5+2$$

$$3 \cdot 2 \leq 5 \cdot 2$$

Pravimo, da sta množici A in B **disjunktni**, če je $A \cap B = \emptyset$.

Dokaz. $A = B \dots \dots \forall x (x \in A \iff x \in B) \dots \dots$
 $\forall x ((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \dots$
 $\forall x (x \in A \Rightarrow x \in B) \wedge \forall x (x \in B \Rightarrow x \in A) \dots$
 $A \subseteq B \quad \wedge \quad B \subseteq A$ □

Dokaz. izberimo poljuben x

$$x \in A \cap B$$

$$x \in A \wedge x \in B$$

$$x \in A$$

$$x \in A \cap B \Rightarrow x \in A$$

$$\forall x (x \in A \cap B \Rightarrow x \in A)$$

$$A \cap B \subseteq A$$
 □

pred PS

def $\cap$

P₀

PS

Univerzalna množica in komplement

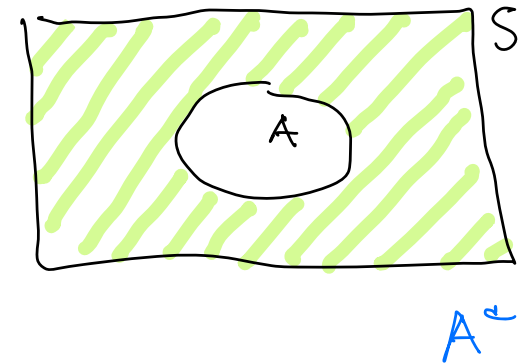
Univerzalna množica, označimo jo z S , ustreza področju pogovora v predikatnem računu.

Vse obravnavane množice so vsebovane v univerzalni množici S .

Komplement množice A , označimo ga z A^c , definiramo kot

$$A^c = S \setminus A$$

$$x \in A^c \quad \dots \quad x \notin A \wedge x \in S$$



$$S = \mathbb{N}$$

$$A = \{0, 1, 2\}$$

$$A^c = \{3, 4, 5, \dots\}$$

Lastnosti komplementa

- ▶ $(A^c)^c = A$
- ▶ $(A \cup B)^c = A^c \cap B^c$
- ▶ $(A \cap B)^c = A^c \cup B^c$
- ▶ $A \setminus B = A \cap B^c$
- ▶ $A \subseteq B \Rightarrow B^c \subseteq A^c$
- ▶ $A \cap B = \emptyset \iff A \subseteq B^c \iff B \subseteq A^c$

Enakosti z množicami

absorbirajo



Pokažimo, da velja

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

Dokaz.

izberimo poljuben x

$$x \in A \cup (A \cap B) \dots$$

$$x \in A \vee x \in A \cap B \dots$$

$$x \in A \vee (x \in A \wedge x \in B) \dots$$

$$a \vee (a \wedge b) \dots \text{absorbirajo}$$

$$a \dots$$

$$x \in A$$

$$x \in A \dots a$$

$$x \in B \dots b$$

$$A \cup (A \cap B) = A.$$

Kako pokažemo,
da sta množici L in D enaki?

• pokažemo $L \subseteq D$ in $D \subseteq L$

• $x \in L$ vlečemo
enakovrednosti

$$x \in D$$

Kako pokažemo, da L in D
nista enaki.

izberemo konkretni množici

$$A = \{1, 2, 3\}, B = \{3, 4\}$$

in pokažemo, da, ki
pripada L in ne pripada D ,
(oz. obratno).

Prednost operacij z množicami:

$$\cap, \cup, +$$

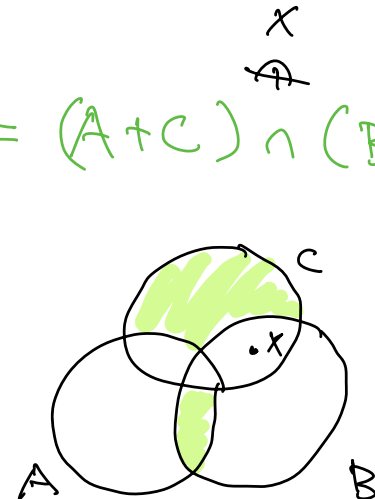
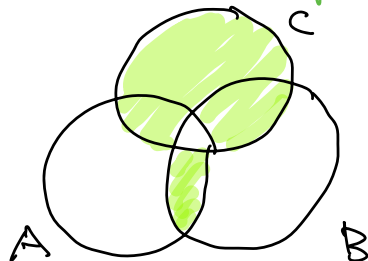
Zbiranje 2
leve poti desni.

Enakosti z množicami

1. Zakon dvojnega komplementa: $(A^c)^c = A$
2. Idempotenca: $A \cap A = A$ $A \cup A = A$
3. Komutativnost: $A \cap B = B \cap A$ $A \cup B = B \cup A$
 $A + B = B + A$
4. Asociativnost: $(A \cap B) \cap C = A \cap (B \cap C)$
 $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A + B) + C = A + (B + C)$
5. Absorpcija: $A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$
6. Distributivnost: $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
 $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
 $(A + B) \cap C = (A \cap C) + (B \cap C)$
7. de Morganova zakona: $(A \cup B)^c = A^c \cap B^c$
 $(A \cap B)^c = A^c \cup B^c$

→ "Druška distributivnost" $(A \cap B) + C = (A + C) \cap (B + C)$
v splošnem ne velja.

$$\begin{aligned} A &= \emptyset \\ B &= \{x\} \\ C &= \{x\} \end{aligned}$$



Enakosti z množicami

8. Kontrapozicija: $A \subseteq B \sim B^c \subseteq A^c$

9. Lastnosti prazne množice $\emptyset$ in univerzalne množice S :

$$A \cup A^c = S \quad A \cap A^c = \emptyset$$

$$A + A = \emptyset \quad A + A^c = S$$

10. Še lastnosti $\emptyset$ in S : $A \cap \emptyset = \emptyset \quad A \cup \emptyset = A$

$$A \cap S = A \quad A \cup S = S$$

11. Lastnosti vsebovanosti:

$$A \subseteq B \sim A \cup B = B \sim A \cap B = A \sim A \setminus B = \emptyset$$

$$\text{če } A \subseteq B, \text{ potem } A \cup C \subseteq B \cup C$$

$$\text{če } A \subseteq B, \text{ potem } A \cap C \subseteq B \cap C$$

$$A \cap B \subseteq A, B \subseteq A \cup B$$

12. Lastnosti razlike množic: $A \setminus B = A \cap B^c$

13. Lastnosti simetrične razlike: $A + B = (A \setminus B) \cup (B \setminus A)$

$$A + B = (A \cup B) \setminus (A \cap B)$$

Potenčna množica

Potenčna množica množice A , $\mathcal{P}A$, je množica vseh podmnožic množice A .

P_1, P_2, P_3

$P_i \sim 1 \dots i \in \text{podmnožici}$

$$\mathcal{P}A = \{B ; B \subseteq A\}$$

Tako $\emptyset$ kot A pripadata potenčni množici $\mathcal{P}A$.

$$\mathcal{P}\{1, 2, 3\} = \{\underbrace{\emptyset}_{000}, \underbrace{\{1\}}_{100}, \underbrace{\{2\}}_{010}, \underbrace{\{3\}}_{001}, \underbrace{\{1, 2\}}_{110}, \underbrace{\{1, 3\}}_{101}, \underbrace{\{2, 3\}}_{011}, \underbrace{\{1, 2, 3\}}_{111}\}$$

$$\mathcal{P}\emptyset = \{\emptyset\} \quad \mathcal{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$$

če izberem A , potem $\emptyset \subseteq A$ in $A \subseteq A$,
 $\emptyset \in \mathcal{P}A$ in $A \in \mathcal{P}A$

Potenčna množica

Trditev

Če množica A vsebuje natanko n elementov in je n naravno število, potem $\mathcal{P}A$ vsebuje natanko 2^n elementov.

Trditev

Če $A \subseteq B$, potem $\mathcal{P}A \subseteq \mathcal{P}B$.

Doka. Vsaka množica C , za katero velja
 $C \subseteq A$ ($C \in \mathcal{P}A$),
je tudi $C \subseteq B$
($C \in \mathcal{P}B$). □