# Diskretne strukture

## Šesti sklop izročkov

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

13. november 2020

Vsebovanost elementa $x$ v množici $A$ podamo z **relacijo pripadnosti** $\ldots x \in A$. Pravimo, da $x$ *pripada* $A$.

Množice lahko podamo na naslednja načina:

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

**Primer**

*Zgledi množic so:*

$$\begin{aligned} A &= \{x\ ;\ x \neq x\} = \emptyset \qquad \textit{prazna množica}, \\ B &= \{x\ ;\ x = 0 \vee x = 1 \vee x = 2\} = \{0, 1, 2\}, \\ C &= \{x\ ;\ x^2 + 1 \geq 5\}. \end{aligned}$$

**Pozor - Russellov paradoks:** Vsaka izjavna formula ni dobra!

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

Ali velja $R \in R$? $\quad R \in R$ natanko tedaj, ko $R \notin R$.

## Enakost in vsebovanost

- Množici $A$ in $B$ sta **enaki**,

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

Pravimo, da je $A$ v relacije **enakosti** z $B$.

- Množica $A$ je **podmnožica** množice $B$,

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

Pravimo, da je $A$ v relacije **inkluzije** z $B$.

- Množica $A$ je **prava podmnožica** množice $B$,

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

Pravimo, da je $A$ v relacije **stroge inkluzije** z $B$.

**Trditev**

*Za poljubne množice $A$, $B$ in $C$ velja*

- $\emptyset \subseteq A$ *in* $A \subseteq A$.
- $A \subseteq A$.
- $A = B$ *natanko tedaj, ko je* $A \subseteq B$ *in* $B \subseteq A$.
- *Če* $A \subseteq B$ *in* $B \subseteq C$, *potem* $A \subseteq C$.

Osnovne operacije z množicami so:

- **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** $A \setminus B = \{x\,;\, x \in A \wedge x \notin B\}$
- **simetrična razlika** $A + B = \{x\,;\, x \in A \veebar x \in B\}$

Lastnosti osnovnih operacij pa so:

- $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
- $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$
- $A \cap B \subseteq A \subseteq A \cup B$

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

**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

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

Komplementiranje ima naslednje lastnosti:

- $(A^c)^c = A$
- $(A \cup B)^c = A^c \cap B^c$

  Dokaz. Veljajo naslednje ekvivalence:

  - $x \in (A \cup B)^c$ natanko tedaj, ko $x \in S \setminus (A \cup B)$.. . . (definicija $^c$).
  - $x \in S \setminus (A \cup B)$ ntk $x \in S$ in $x \notin A \cup B$. . . . (def $\setminus$)
  - $x \in S$ in $x \notin A \cup B$ ntk $x \in S$ in $x \notin A$ in $x \notin B$. . . . (def $\cup$)
  - $x \in S$ in $x \notin A$ in $x \notin B$ ntk $x \in S \setminus A = A^c$ in $x \in S \setminus B = B^c$. . . . (def $^c$)
  - $x \in A^c$ in $x \in B^c$ ntk $x \in A^c \cap B^c$. . . . (def $\cap$)
- $(A \cap B)^c = A^c \cup B^c$
- $A \setminus B = A \cap B^c$

  Dokaz. Veljajo naslednje ekvivalence:

  $$(x \in A \setminus B) \text{ ntk } (x \in A \text{ in } x \notin B) \text{ ntk } (x \in A \text{ in } x \in B^c) \text{ ntk } x \in A \cap B^c.$$

- $A \subseteq B \Rightarrow B^c \subseteq A^c$
- $A \cap B = \emptyset \iff A \subseteq B^c \iff B \subseteq A^c$

Po prednosti je komplement $^c$ močnejši od preseka $\cap$ in razlike $\setminus$, ti dve pa močnejši od unije $\cup$ in simetrične razlike $+$:

| | | |
|---|---|---|
| $^c$ | $\cap$ $\setminus$ | $\cup$ $+$ |

Operacije z množicami *"podedujejo"* ustrezne lastnosti izjavnih veznikov.

**Zakon dvojnega komplementa** $(A^c)^c = A$

**Idempotenca**
$$A \cap A = A$$
$$A \cup A = A$$

**Komutativnost**
$$A \cap B = B \cap A$$
$$A \cup B = B \cup A$$
$$A + B = B + A$$

**Asociativnost**
$$(A \cap B) \cap C = A \cap (B \cap C)$$
$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A + B) + C = A + (B + C)$$

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

Dokaz drugega dela absorpcije. Vzemimo poljuben element $x$ iz $A \cap (A \cup B)$. Od tod sledi $x \in A$ in $x \in (A \cup B)$. Posebej torej $x \in A$, iz česar sledi vsebovanost $A \cap (A \cup B) \subseteq A$.

Vzemimo poljuben element $x$ iz $A$. Sledi $x \in A \cup B$ in zato $x \in A \cap (A \cup B)$. Torej imamo tudi vsebovanost $A \subseteq A \cap (A \cup B)$.

Iz obeh vsebovanosti sledi enakost $A \cap (A \cup B) = A$.

**Distributivnost**
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B + C) = (A \cap B) + (A \cap C)$$

Dokaz prvega dela distributivnosti. Vzemimo poljuben element $x$ iz $A \cap (B \cup C)$. Od tod sledi $x \in A$ in $x \in (B \cup C)$. Sledi $x \in B$ ali $x \in C$. V prvem primeru imamo $x \in A \cap B$, v drugem pa $x \in A \cap C$. Sklepamo, da $x \in (A \cap B) \cup (A \cap C)$, iz česar sledi vsebovanost $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Vzemimo poljuben element $x$ iz $(A \cap B) \cup (A \cap C)$. Sledi $x \in A \cap B$ ali $x \in A \cap C$. V prvem primeru sledi $x \in A$ in $x \in B$, v drugem pa $x \in A$ in $x \in C$. V obeh primerih torej $x \in A$ in $x \in B \cup C$. Sklepamo, da $x \in A \cap (B \cup C)$, iz česar sledi vsebovanost $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Iz obeh vsebovanosti sledi enakost $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

| | |
|---|---|
| **de Morganova zakona** | $(A \cap B)^c = A^c \cup B^c$<br>$(A \cup B)^c = A^c \cap B^c$ |
| **Kontrapozicija** | $A \subseteq B \Leftrightarrow B^c \subseteq A^c$ |
| $\emptyset$ **in** $S$ | $A \cap \emptyset = \emptyset$<br>$A \cap S = A$<br>$A \cup \emptyset = A$<br>$A \cup S = S$ |
| **Lastnosti simetrične razlike** | $A + B = (A \setminus B) \cup (B \setminus A)$<br>$A + B = (A \cup B) \cup (A \cap B)$ |

# Potenčna množica

**Potenčna množica** množice $A$, $\mathcal{P}A$, je množica vseh podmnožic množice $A$. S simboli:

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

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

## Primer

- $\mathcal{P}\{1,2,3\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.
- $\mathcal{P}\emptyset = \{\emptyset\} \qquad \mathcal{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$

## Trditev

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

Premislek: Vsak element iz $A$ bodisi je element podmnožice bodisi ni element podmnožice. Torej imamo za vsak element 2 možnosti. Skupaj imamo tako $2^n$ različnih možnosti. Vsaka od možnosti ustreza neki podmnožici množice $A$.

## Trditev

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

Premislek: Vsaka podmnožice množice $A$ je posebej tudi podmnožica množice $B$.

Naj bo
$$\mathcal{A} = \{A_1, A_2, A_3, \ldots\} = \{A_i \,;\, i \in \mathcal{I}\}$$
**družina množic**. Z $\mathcal{I}$ označimo indeksno množico.

- **Unija družine** $\mathcal{A}$ je množica
$$\bigcup \mathcal{A} = \bigcup_{i \in \mathcal{I}} A_i = \{x \,;\, \exists i\, (i \in \mathcal{I} \wedge x \in A_i)\}$$
- **Presek družine** $\mathcal{A}$ je množica
$$\bigcap \mathcal{A} = \bigcap_{i \in \mathcal{I}} A_i = \{x \,;\, \forall i\, (i \in \mathcal{I} \Rightarrow x \in A_i)\}$$
- Družina množic $\mathcal{A} = \{A_i \,;\, i \in \mathcal{I}\}$ je **pokritje** množice $B$, če je
$$B = \bigcup_{i \in \mathcal{I}} A_i.$$
- Družina množic $\mathcal{A} = \{A_i \,;\, i \in \mathcal{I}\}$ je **razbitje** množice $B$, če je
  - $\mathcal{A}$ pokritje množice $B$ ($B = \bigcup_{i \in \mathcal{I}} A_i$)
  - elementi $\mathcal{A}$ so neprazni ($\forall i \in \mathcal{I} :\ A_i \neq \emptyset$) in
  - elementi $\mathcal{A}$ so paroma disjunktni ($\forall i, j \in \mathcal{I}, i \neq j : A_i \cap A_j \neq \emptyset$).

Primer. $\mathcal{C} = \{[i, i+1] \colon i \in \mathbb{Z}\}$ je pokritje za $\mathbb{R}$, $\mathcal{D} = \{[i, i+1) \colon i \in \mathbb{Z}\}$ pa je razbitje za $\mathbb{R}$.

**Urejeni par** s prvo komponento (koordinato) $a$ in drugo komponento (koordinato) $b$ označimo z $(a, b)$ in definiramo kot

$$(a, b) = \{\{a\}, \{a, b\}\}$$

**Trditev (osnovna lastnost urejenih parov)**

$$(a, b) = (c, d) \iff a = c \text{ in } b = d$$

**Kartezični produkt** množic $A$ in $B$ je množica vseh urejenih parov. S simboli:

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

Definicijo kartezičnega produkta lahko razširimo na več faktorjev.

$A \times B \times C$ je množica vseh urejenih trojic s prvo koordinato v $A$, drugo v $B$ in tretjo koordinato v množici $C$.

$(a_1, a_2, \ldots, a_n)$ je **urejena $n$-terica**. $A_1 \times A_2 \times \cdots \times A_n$ je množica vseh urejenih $n$-teric s prvo koordinato v $A_1$, drugo v $A_2$, ... in zadnjo v $A_n$.

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

  Dokaz. Naj bo $(x, y)$ poljuben element iz $A \times (B \cup C)$. Torej je $x \in A$ in $y \in B \cup C$. Sledi $y \in B$ ali $y \in C$. V prvem primeru je $(x, y) \in A \times B$, v drugem pa $(x, y) \in A \times C$. V obeh primerih pa je $(x, y) \in (A \times B) \cup (A \times C)$. Sklepamo na vsebovanost $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

  Naj bo $(x, y)$ poljuben element iz $(A \times B) \cup (A \times C)$. Torej je $(x, y) \in A \times B$ in $(x, y) \in A \times C$. V prvem primeru je $x \in A$ in $y \in B$, v drugem pa je $x \in A$ in $y \in C$. V obeh primerih pa je $(x, y) \in A \times (B \cup C)$. Sklepamo na vsebovanost $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.

  Sledi, da velja $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

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

  Dokaz. Velja $(A \cap B) \times (C \cap D) \subseteq A \times (C \cap D) \subseteq A \times C$. Podobno $(A \cap B) \times (C \cap D) \subseteq B \times D$. Sledi $(A \cap B) \times (C \cap D) \subseteq (A \times C) \cap (B \times D)$.

  Vzemimo poljuben $(x, y) \in (A \times C) \cap (B \times D)$. Sledi $(x, y) \in A \times C$ in $(x, y) \in B \times D$. Velja $x \in A$, $y \in C$ in $x \in B, y \in D$. Torej je $x \in A \cap B$ in $y \in C \cap D$. Sklepamo $(x, y) \in (A \cap B) \times (C \cap D)$ in zato $(A \times C) \cap (B \times D) \subseteq (A \cap B) \times (C \cap D)$.

  Obe vsebovanosti implicirata enakost $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

- $A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$

- $A \times B \subseteq C \times D \ \wedge \ A \times B \neq \emptyset \implies A \subseteq C \wedge B \subseteq D$
- $A$ končna z $m$ elementi in $B$ končna z $n$ elementi $\Longrightarrow$ $A \times B$ končna z $m \cdot n$ elementi.

Če v tretjo lastnost vstavimo $C = D$, pridelamo

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

Podobno, če vstavimo $A = B$.
Toda v splošnem

$$(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D).$$

Protiprimer. $A = C = [0, 1]$, $B = D = [1, 2]$. Velja

$$(A \cup B) \times (C \cup D) = [0, 2] \times [0, 2],$$

toda

$$(A \times C) \cup (B \times D) = [0, 1] \times [0, 1] \cup [1, 2] \times [1, 2].$$

Naj bosta $A, B$ množici, $X$ pa neznana množica, ki zadošča

$$X \cup A = B \setminus X,$$
$$X \cup B = X.$$

Obravnavaj rešljivost zgornjega sistema in v primeru rešljivosti sistem tudi reši.

- Iz $X \cup A = B \setminus X = B \cap X^c$ sklepamo $X \subseteq B$, $X \subseteq X^c$ in $A \subseteq B$, $A \subseteq X^c$. Iz $X \subseteq X^c$ sklepamo, da je $X = \emptyset$.
- Iz $X \cup B = X$ sklepamo, z upoštevanjem $X = \emptyset$, $B = \emptyset$.
- Iz $A \subseteq B$ sklepamo, z upoštevanjem $B = \emptyset$, $A = \emptyset$.
- Torej je sistem rešljiv samo za $A = B = \emptyset$, pri čemer je kandidat za rešitev $X = \emptyset$.
- Na koncu samo še preverimo, da je $A = B = X = \emptyset$ res rešitev: $\emptyset \cup \emptyset = \emptyset \setminus \emptyset$ in $\emptyset \cup \emptyset = \emptyset$.

Naj bodo $A, B, C$ množice, $X$ pa neznana množica, ki zadošča

$$A \cup X = B,$$
$$A \cap X = C.$$

Obravnavaj rešljivost zgornjega sistema in v primeru rešljivosti sistem tudi reši.

- Iz $A \cup X = B$ sklepamo $A \subseteq B$, $X \subseteq B$ in $X$ vsebuje $B \setminus A$.
- Iz $A \cap X = C$ sklepamo, $C \subseteq A$, $C \subseteq X$ in $C$ je natanko množica točk, kjer se $A$ in $X$ ujemata.
- Dobili smo pogoj $C \subseteq A \subseteq B$ in edinega kandidata za $X = C \cup (B \setminus A)$.
- Preverimo, da je pri pogoju rešljivosti sistem res zadoščen:
  $A \cup X = A \cup (C \cup (B \setminus A)) = A \cup C \cup (B \setminus A) = A \cup (B \setminus A) = A \cup (B \cap A^c) = (A \cup B) \cap (A \cup A^c) = B$,
  pri čemer smo v tretji enakosti upoštevali $A \subseteq C$, v peti distributivnost in v šesti $A \subseteq B$.
  $A \cap X = A \cap (C \cup (B \setminus A)) = A \cap (C \cup (B \cap A^c)) = A \cap ((C \cup B) \cap (C \cup A^c)) =$
  $$= A \cap (B \cap (C \cup A^c) = A \cap B \cap (C \cup A^c) = A \cap (C \cup A^c) = (A \cap C) \cap (A \cap A^c) = C,$$
  kjer smo v tretji enakosti upoštevali distributivnost, v četrti $C \subseteq B$, v šesti $A \subseteq B$, v sedmi distributivnost in v zadnji $C \subseteq A$.