Diszkrét matematika 1.

1. előadás

Juhász Zsófia
jzsofia@inf.elte.hu
jzsofi@gmail.com
Mérai László diái alapján

Komputeralgebra Tanszék

2020 tavasz

Diszkrét matematika

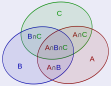
Részterületei:

- Logika
- Halmazelmélet
- Kombinatorika
- Gráfelmélet
- Számelmélet
- Algebra
- Kriptográfia
- Algoritmusok
- Számítástudomány
- Információelmélet
- Játékelmélet
- Diszkrét geometria
- Operációkutatás
- Valószínűségszámítás

Mit tanulunk az idén?

Négy fő témakör:

1. **Alapok:** logika, halmazok, relációk

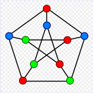


2. **Komplex számok**

$$(\cos t + i*\sin t)^n = \cos n*t + i*\sin n*t$$

3. **Kombinatorika**

4. **Gráfok**



Egy kis matematikai logika . . .

Logikai műveletek

A logikában az állításokat logikai műveletekkel tudjuk összekapcsolni:

- Tagadás (negáció), jele: $\neg A$.
- És (konjunkció), jele: $A \wedge B$.
- Vagy (megengedő vagy/diszjunkció), jele: $A \vee B$.
- Ha ..., akkor ... (implikáció), jele: $A \Rightarrow B$.
- ...pontosan akkor, ha ... (ekvivalencia), jele: $A \Leftrightarrow B$.

Igazságtáblázat

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
I	I	H	I	I	I	I
I	H	H	H	I	H	H
H	I	I	H	I	I	H
H	H	I	H	H	I	I

Logikai műveletek: a **vagy** fajtái

A köznyelvben a **vagy** háromféle értelemmel bírhat:

- Megengedő vagy: $A \vee B$ pontosan akkor igaz, ha A és B közül *legalább* az egyik igaz.

  Pl. „Átok reá ki gyávaságból vagy lomhaságból elmarad,. . . "
- Kizáró vagy: $A \oplus B$ pontosan akkor igaz, ha A és B közül *pontosan* az egyik igaz. ($\oplus$ helyett a XOR jelölés is használatos.)

  Pl. „Most jobbra vagy balra kell fordulnunk."
- Összeférhetetlen vagy: $A||B$ pontosan akkor igaz, ha A és B közül *legfeljebb* egyik igaz.

  Pl. „Iszik vagy vezet!"

A	B	$A \vee B$	$A \oplus B$	$A\|\|B$
I	I	I	H	H
I	H	I	I	I
H	I	I	I	I
H	H	H	H	I

Logikai műveletek

Az implikáció ($A \Rightarrow B$) csak *logikai* összefüggést jelent és nem okozatit!

A	B	$A \Rightarrow B$
I	I	I
I	H	H
H	I	I
H	H	I

Példa

- $2 \cdot 2 = 4 \Rightarrow i^2 = -1$
- $2 \cdot 2 = -3 \Rightarrow$ A kutya emlős állat.

Hamis állításból minden következik:

Példa

- $2 \cdot 2 = 5 \Rightarrow i^2 = -2$

Adott logikai művelet más módon is kifejezhető: $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$

A logikai műveletek tulajdonságai, ítéletlogikai tételek

Állítás (Logikai műveletek tulajdonságai)

1. $A \vee A \Leftrightarrow A$, $A \wedge A \Leftrightarrow A$ *(idempotencia)*
2. $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C, A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ *(asszociativitás)*
3. $A \vee B \Leftrightarrow B \vee A, A \wedge B \Leftrightarrow B \wedge A$ *(kommutativitás)*
4. $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ *(disztributivitás)*
5. $(A \vee B) \wedge A \Leftrightarrow A$, $(A \wedge B) \vee A \Leftrightarrow A$ *(abszorpció, azaz elnyelési tulajdonság)*
6. $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B, \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ *(De Morgan azonosságok)*
7. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ *(kontrapozíció tétele)*
8. $((A \Rightarrow B) \wedge A) \Rightarrow B$ *(modus ponens)*
9. $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ *(szillogizmus)*
10. $((A \Rightarrow B) \wedge (B \Rightarrow A)) \Leftrightarrow (A \Leftrightarrow B)$

Bizonyítás.

Példa:

3. $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$ (a logikai vagy asszociativitása)

A	**B**	**C**	**B ∨ C**	**A ∨ (B ∨ C)**	**A ∨ B**	**(A ∨ B) ∨ C**	**A ∨ (B ∨ C) ⇔ (A ∨ B) ∨ C**
I	I	I	I	I	I	I	I
I	I	H	I	I	I	I	I
I	H	I	I	I	I	I	I
I	H	H	H	I	I	I	I
H	I	I	I	I	I	I	I
H	I	H	I	I	I	I	I
H	H	I	I	I	H	I	I
H	H	H	H	H	H	H	I

□

Kvantorok

Kvantorok

- $\exists$ (egzisztenciális kvantor): „létezik", „van olyan".
- $\forall$ (univerzális kvantor): „bármely", „minden".

Példák

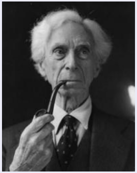
1. $\exists x \in \mathbb{R} : x^2 = 5$
   „Van olyan x valós szám, melyre $x^2 = 5$."
2. $\forall x \in \mathbb{R} : x^2 \geq 0$
   „Minden x valós számra $x^2 \geq 0$."
3. $\forall n \in \mathbb{Z}\ \exists x \in \mathbb{R} : x > n$
   „Minden n egész számhoz létezik olyan x valós szám, amelyre $x > n$."

Halmazok

Egy nevezetes paradoxon a naív halmazelméletben

Russell paradoxon (Bertrand Russell, 1872 - 1970)

Nevezzünk minden olyan halmazt, amely nem eleme önmagának jó halmaznak, és minden olyan halmazt, amely eleme önmagának, rossz halmaznak. Legyen A az összes jó halmazok halmaza. Jó vagy rossz halmaz-e A?



- A jó halmaz. $\Rightarrow$ (A definíciója alapján) A eleme önmagának. $\Rightarrow$ A rossz halmaz. $\lightning$
- A rossz halmaz. $\Rightarrow$ (A definíciója alapján) A nem eleme önmagának. $\Rightarrow$ A jó halmaz. $\lightning$

Körül kell bástyázni a halmazok definiálásának lehetséges módjait $\Rightarrow$ **Axiomatikus halmazelmélet:** Zermelo-Fraenkel-féle axiómarendszer

Halmazok

Halmazelméletben az alapvető fogalmak (ún. predikátumok), nem definiáljuk őket:

- Halmaz (rendszer, osztály, összesség, ...): Informálisan elképzelhető úgy, mint elemeinek gondolati burka.
- $x \in A$, ha az x eleme az A halmaznak.

A halmazok alapvető tulajdonságai axiómák, nem bizonyítjuk őket.

Példa

Meghatározottsági axióma.

Egy halmazt az elemei egyértelműen meghatároznak. $\square$

- Két halmaz pontosan akkor egyenlő, ha ugyanazok az elemeik.
- Egy halmaznak egy elem csak egyszer lehet eleme.

Halmazok

Halmaz megadása elemei felsorolásával:
Véges halmazt definiálhatunk elemei $\{\}$ között történő felsorolásával. Például: Annak a halmaznak, melynek csak az a elem az eleme a jelölése: $\{a\}$. Annak a halmaznak, melynek pontosan az a és b az elemei a jelölése: $\{a, b\}$. (Speciálisan, ha $a = b$, akkor $\{a\} = \{a, b\} = \{b\}$.) ...

Definíció (üres halmaz)

Azt a halmazt, melynek nincs eleme, üres halmaznak nevezzük. Jele: $\emptyset$ vagy $\{\}$.

Megjegyzés

- Figyelem! $\emptyset \neq \{\emptyset\}$.
- A meghatározottsági axióma alapján az üres halmaz egyértelmű.

Részhalmaz fogalma

Definíció (részhalmaz)

Az A halmaz **részhalmaza** a B halmaznak: $A \subseteq B$, ha A minden eleme B-nek is eleme, azaz

$$\forall x : x \in A \Rightarrow x \in B.$$

Ha $A \subseteq B$-nek, de $A \neq B$, akkor A **valódi részhalmaza** B-nek: $A \subsetneq B$.

Megjegyzés:

- Az üres halmaz minden halmaznak részhalmaza.
- Minden halmaz részhalmaza önmagának, de nem valódi részhalmaza.

Állítás (A részhalmaz reláció tulajdonságai; Biz. HF)

Tetszőleges A, B és C halmazokra:

1. $A \subseteq A$ *(reflexivitás).*
2. $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$ *(tranzitivitás).*
3. $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$ *(antiszimmetria).*

Részhalmaz definiálása formula segítségével

Definíció (Részhalmaz axióma)

Legyen A egy halmaz és $\mathscr{F}(x)$ egy formula (azaz $\mathscr{F}$ egy olyan tulajdonság, amely leírható formálisan, a logika nyelvén). Ekkor létezik az a halmaz, amely A-nak pontosan azon x elemeit tartalmazza, melyekre $\mathscr{F}(x)$ igaz (azaz amelyekre az $\mathscr{F}$ tulajdonság teljesül). Ezt a halmazt $\{x \in A : \mathscr{F}(x)\} = \{x \in A \mid \mathscr{F}(x)\}$ jelöli.

Megjegyzés: $\{x \in A : \mathscr{F}(x)\}$ helyett az $\{x : x \in A \wedge \mathscr{F}(x)\}$ vagy $\{x : x \in A, \mathscr{F}(x)\}$ jelölés is szokásos.

Példa

- $\{n \in \mathbb{Z} : \exists m \, (m \in \mathbb{Z} \wedge n = m^2)\}$: a négyzetszámok halmaza.
- $\{x \in \mathbb{R} : x^2 = 3\}$: az $x^2 = 3$ egyenlet valós megoldásainak halmaza, azaz $\{\sqrt{3}, -\sqrt{3}\}$.

Műveletek halmazokkal: halmazok uniója

Definíció (halmazok uniója)

Az A és B halmazok **uniója:** $A \cup B$ az a halmaz, mely pontosan A és B összes elemét tartalmazza:

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Általában: Legyen $\mathscr{A}$ egy olyan halmaz, melynek az elemei is halmazok (**halmazrendszer**). Ekkor $\bigcup \mathscr{A} = \cup\{A : A \in \mathscr{A}\} = \cup_{A \in \mathscr{A}} A$ az a halmaz, mely $\mathscr{A}$ összes elemének elemeit tartalmazza:

$$\cup\mathscr{A} = \{x \mid \exists A \in \mathscr{A} : x \in A\}.$$

Speciálisan: $A \cup B = \cup\{A, B\}$.

Példák

- $\{a, b, c\} \cup \{b, c, d\} = \{a, b, c, d\}$
- $\{x \in \mathbb{R} : 0 < x\} \cup \{x \in \mathbb{R} : x < 0\} = \{x \in \mathbb{R} : x \neq 0\}$

Műveletek halmazokkal: az unió tulajdonságai

Állítás (Az unió tulajdonságai)

Minden A, B, C halmazra:

1. $A \cup \emptyset = A$
2. $A \cup (B \cup C) = (A \cup B) \cup C$ *(asszociativitás)*
3. $A \cup B = B \cup A$ *(kommutativitás)*
4. $A \cup A = A$ *(idempotencia)*
5. $A \subseteq B \Leftrightarrow A \cup B = B$

Bizonyítás.

1. $x \in A \cup \emptyset \Leftrightarrow x \in A \vee x \in \emptyset \Leftrightarrow x \in A$.
2. $x \in A \cup (B \cup C) \Leftrightarrow x \in A \vee x \in B \cup C \Leftrightarrow x \in A \vee (x \in B \vee x \in C) \Leftrightarrow (x \in A \vee x \in B) \vee x \in C \Leftrightarrow x \in A \cup B \vee x \in C \Leftrightarrow x \in (A \cup B) \cup C$
3. 2-höz hasonló.
4. 2-höz hasonló.
5. $\Rightarrow$: $A \subseteq B \Rightarrow A \cup B \subseteq B$, de $B \subseteq A \cup B$ mindig teljesül, így $A \cup B = B$.
   $\Leftarrow$: Ha $A \cup B = B$, akkor A minden eleme eleme B-nek.

□

Műveletek halmazokkal: halmazok metszete

Definíció (halmazok metszete)

Az A és B halmazok metszete: $A \cap B$ az a halmaz, mely pontosan az A és B *közös* elemeit tartalmazza:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

.

Általában: Legyen $\mathscr{A}$ egy olyan halmaz, melynek az elemei is halmazok (halmazrendszer). Ekkor $\cap\mathscr{A} = \cap\{A : A \in \mathscr{A}\} = \cap_{A\in\mathscr{A}} A$ a következő halmaz:

$$\cap\mathscr{A} = \{x \mid \forall A \in \mathscr{A} : x \in A\}.$$

Speciálisan: $A \cap B = \cap\{A, B\}$.

Példa

- $\{a, b, c\} \cap \{b, c, d\} = \{b, c\}$.
- Ha $I_n = \{x \in \mathbb{R} : n \leq x \leq n+1\}$, $\forall\, n \in \mathbb{Z}$-re és $\mathscr{I} = \{I_n : n \in \mathbb{Z}\}$, akkor
  - $I_2 \cap I_3 = \{3\}$
  - $I_8 \cap I_{11} = \emptyset$
  - $I_n \cap I_{n+1} = \{n+1\}$
  - $\cap\mathscr{I} = \emptyset$

Diszjunkt és páronként diszjunkt halmazrendszerek

Definíció ((páronként) diszjunkt halmazrendszer)

Ha $A \cap B = \emptyset$, akkor A és B diszjunktak.
Általánosabban: Ha $\mathscr{A}$ egy halmazrendszer, és $\cap \mathscr{A} = \emptyset$, akkor $\mathscr{A}$ diszjunkt, illetve $\mathscr{A}$ elemei diszjunktak.
Ha $\mathscr{A}$ egy halmazrendszer, és $\mathscr{A}$ bármely két eleme diszjunkt, akkor $\mathscr{A}$ elemei páronként diszjunktak.

Példa

- Az $\{1, 2\}$ és $\{3, 4\}$ halmazok diszjunktak.
- Az $\{1, 2\}$, $\{2, 3\}$ és $\{1, 3\}$ halmazok diszjunktak, de nem páronként diszjunktak.
- Az $\{1, 2\}$, $\{3, 4\}$ és $\{5, 6\}$ halmazok páronként diszjunktak.
- Ha $I_n = \{x \in \mathbb{R} : n \leq x \leq n + 1\}$, $\forall\, n \in \mathbb{Z}$-re és $\mathscr{I} = \{I_n : n \in \mathbb{Z}\}$, akkor $\mathscr{I}$ diszjunkt halmazrendszer, de elemei nem páronként diszjunktak.

Műveletek halmazokkal: a metszet tulajdonságai

Állítás (A metszet tulajdonságai; Biz. HF)

Minden A, B, C *halmazra:*

1. $A \cap \emptyset = \emptyset$
2. $A \cap (B \cap C) = (A \cap B) \cap C$ *(asszociativitás)*
3. $A \cap B = B \cap A$ *(kommutativitás)*
4. $A \cap A = A$ *(idempotencia)*
5. $A \subseteq B \Leftrightarrow A \cap B = A$

Disztributivitás

Állítás (Az unió és metszet disztributivitási tulajdonságai)

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Bizonyítás.

1. $x \in A \cap (B \cup C) \Leftrightarrow x \in A \wedge x \in B \cup C \Leftrightarrow$
   $\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Leftrightarrow x \in A \cap B \vee x \in A \cap C \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$
2. HF. hasonló

$\square$

Halmazok különbsége, komplementere

Definíció (halmazok különbsége)

Az A és B halmazok **különbsége** az $A \setminus B = \{x \in A : x \notin B\}$ halmaz.

Definíció (halmaz komplementere)

Egy rögzített X alaphalmaz és $A \subseteq X$ részhalmaz esetén az A halmaz **komplementere** az $\overline{A} = A' = X \setminus A$ halmaz.

Állítás (Különbség kifejezése komplementer segítségével)

$A \setminus B = A \cap \overline{B}$.

Bizonyítás.

$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B \Leftrightarrow x \in A \wedge x \in \overline{B} \Leftrightarrow x \in A \cap \overline{B}$ $\square$

Komplementer tulajdonságai

Állítás (Komplementer tulajdonságai; Biz. HF)

Legyen X az alaphalmaz. Ekkor minden $A, B \subseteq X$ halmazra:

1. $\overline{\overline{A}} = A$;
2. $\overline{\emptyset} = X$;
3. $\overline{X} = \emptyset$;
4. $A \cap \overline{A} = \emptyset$;
5. $A \cup \overline{A} = X$;
6. $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$;
7. $\overline{A \cap B} = \overline{A} \cup \overline{B}$;
8. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

A 7. és 8. összefüggések az ún. de Morgan szabályok.

Komplementer tulajdonságai

Bizonyítás.

Példa

$\vdots$

7. $x \in \overline{A \cap B} \Leftrightarrow \neg(x \in A \cap B) \Leftrightarrow \neg(x \in A \wedge x \in B) \Leftrightarrow$
   $\Leftrightarrow \neg(x \in A) \vee \neg(x \in B) \Leftrightarrow x \in \overline{A} \vee x \in \overline{B} \Leftrightarrow x \in \overline{A} \cup \overline{B}$

$\vdots$

$\square$

Halmazok szimmetrikus differenciája

Definíció (szimmetrikus differencia)

Az A és B halmazok szimmetrikus differenciája az

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

halmaz.

Állítás (Szimmetrikus differencia másik előállítása; Biz. HF)

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

Halmaz hatványhalmaza

Definíció (hatványhalmaz)

Ha A egy halmaz, akkor azt a halmazrendszert, melynek elemei pontosan az A halmaz részhalmazai az A hatványhalmazának mondjuk, és 2^A-val jelöljük. (A $\mathscr{P}(A)$ jelölés is szokásos.)

- $A = \emptyset$, $2^\emptyset = \{\emptyset\}$
- $A = \{a\}$, $2^{\{a\}} = \{\emptyset, \{a\}\}$
- $A = \{a, b\}$, $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Jelölés: Egy véges A halmaz elemszámát $|A|$ jelöli.

Állítás (Hatványhalmaz elemszáma; biz. később)

Tetszőleges A véges halmazra: $|2^A| = 2^{|A|}$.