Bevezetés a számításelméletbe

9. előadás

Rice tétel

Definíció

Tetszőleges $\mathcal{P} \subseteq RE$ halmazt a rekurzívan felsorolható nyelvek egy **tulajdonságának** nevezzük. $\mathcal{P}$ **triviális**, ha $\mathcal{P} = \emptyset$ vagy $\mathcal{P} = RE$.

$L_{\mathcal{P}} = \{\langle M \rangle \mid L(M) \in \mathcal{P}\}$.

Rice tétele

Ha $\mathcal{P} \subseteq RE$ egy nem triviális tulajdonság, akkor $L_{\mathcal{P}} \notin R$.

Rice tétel

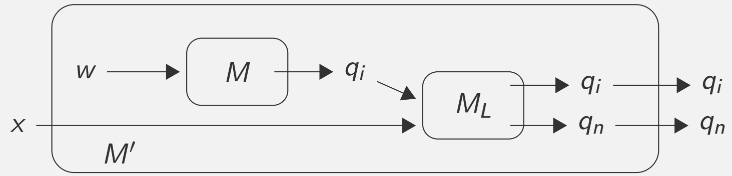
Bizonyítás:

1. eset $\emptyset \notin \mathcal{P}$.
Mivel tudjuk, hogy $L_u \notin R$, elég belátni, hogy $L_u \leq L_{\mathcal{P}}$.
Mivel $\mathcal{P}$ nem triviális, ezért létezik $L \in \mathcal{P}$. ($L \neq \emptyset$).
$L \in RE$, ezért van olyan M_L TG, melyre $L(M_L) = L$.

Egy tetszőleges $\langle M, w \rangle$ TG – bemenet pároshoz elkészítünk egy M' kétszalagos TG-t, mely egy x bemenetén a következőképpen működik:

1. Bemenetétől függetlenül először szimulálja M-et w-re a második szalagján.
2. Így, ha M nem áll meg w-n, akkor M' nem áll meg egyetlen inputjára sem Ez esetben $L(M') = \emptyset$.
3. Ha M elutasítja w-t, akkor M' q_n-be lép és leáll (azaz nem fogadja el x-et). Ez esetben is $L(M') = \emptyset$.
4. Ha M elfogadja w-t, akkor M' szimulálja M_L -et x-en. Ekkor M_L definíciója miatt $L(M') = L$.

Rice tétel



Összefoglalva

- $\langle M, w \rangle \in L_u \Rightarrow L(M') = L \Rightarrow L(M') \in \mathcal{P} \Rightarrow \langle M' \rangle \in L_{\mathcal{P}}$.
- $\langle M, w \rangle \notin L_u \Rightarrow L(M') = \emptyset \Rightarrow L(M') \notin \mathcal{P} \Rightarrow \langle M' \rangle \notin L_{\mathcal{P}}$.

Azaz:
$\langle M, w \rangle \in L_u \Leftrightarrow \langle M' \rangle \in L_{\mathcal{P}}$, tehát $L_u \leq L_{\mathcal{P}}$ és így $L_{\mathcal{P}} \notin R$.

Rice tétel

2. eset $\emptyset \in \mathcal{P}$.

- Alkalmazhatjuk az 1. eset eredményét $\overline{\mathcal{P}} = RE \setminus \mathcal{P}$-re, hiszen ekkor $\overline{\mathcal{P}}$ szintén nem triviális és $\emptyset \notin \overline{\mathcal{P}}$.
- Azt kapjuk, hogy $L_{\overline{\mathcal{P}}} \notin R$.
- $\overline{L_{\mathcal{P}}} = L_{\overline{\mathcal{P}}}$, mivel megállapodásunk szerint minden szó TG kód, a nem kellő alakú szavak egy rögzített, egyetlen szót sem elfogadó TG-et kódolnak.
- $\overline{L_{\mathcal{P}}} \notin R \Rightarrow L_{\mathcal{P}} \notin R$ (tétel volt).

Rice tétel

Alkalmazások

Következmények:
Eldönthetetlen, hogy egy M TG

- az üres nyelvet ismeri-e fel. ($\mathcal{P} = \{\emptyset\}$)
- véges nyelvet ismer-e fel ($\mathcal{P} = \{L \mid L$ véges $\}$)
- környezetfüggetlen nyelvet ismer-e fel ($\mathcal{P} = \{L \mid L$ környezetfüggetlen $\}$)
- elfogadja-e az üres szót ($\mathcal{P} = \{L \in RE \mid \varepsilon \in L\}$)

Post Megfelelkezési Probléma

Definíció

Legyen Σ egy ábécé és legyenek $u_1, \ldots, u_n, v_1 \ldots, v_n \in \Sigma^+$ $(n \geq 1)$. A $D = \left\{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\right\}$ halmazt **dominókészletnek** nevezzük.

(Valójában az i. dominó egy az u_i és v_i szavakból álló rendezett pár. u_i-t a dominó felső, míg v_i-t a dominó alsó szavának nevezzük.)

Definíció

Az $\frac{u_{i_1}}{v_{i_1}} \cdots \frac{u_{i_m}}{v_{i_m}}$ dominósorozat $(m \geq 1, 1 \leq i_1, \ldots, i_m \leq n)$ a $D = \{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\}$ dominókészlet egy **megoldása**, ha $u_{i_1} \cdots u_{i_m} = v_{i_1} \cdots v_{i_m}$.

Post Megfelelkezési Probléma

Példa: A $\{\frac{b}{ca}, \frac{dd}{e}, \frac{a}{ab}, \frac{ca}{a}, \frac{abc}{c}\}$ készlet egy lehetséges megoldása $\frac{a}{ab}\frac{b}{ca}\frac{ca}{a}\frac{a}{ab}\frac{abc}{c}$.

Egy másik megoldás: $\frac{a}{ab}\frac{b}{ca}\frac{ca}{a}\frac{a}{ab}\frac{abc}{c}\frac{a}{ab}\frac{b}{ca}\frac{ca}{a}\frac{a}{ab}\frac{abc}{c}$.

Megjegyzés: Tehát egy megoldáshoz a dominók többször felhasználhatók és nem kell minden dominót felhasználni. Egy dominókészletnek több megoldása is lehet.

Megoldás alatt véges (de akármekkora) hosszúságú kirakást értünk.

Vegyük észre, hogy hiába véges maga a készlet, végtelen sok féleképpen lehet a készlet dominóit véges sorozatba egymás után rakni, így megoldás keresése esetén egy végtelen keresési térrel állunk szemben.

Post Megfelelkezési Probléma (PMP):

$L_{\text{PMP}} = \{\langle D \rangle \mid D\text{-nek van megoldása}\}$.

Post Megfelelkezési Probléma

Tétel

$L_{\text{PMP}} \in RE$.

Bizonyítás: Ha D-t egy ábécének tekintjük, akkor éppen a D feletti szavak a potenciális megoldások.

Egy olyan TG, mely a D feletti szavakat hosszlexikografikus sorrendben sorra kipróbálja és ha megoldást talál q_i-ben leáll éppen L_{PMP}-t ismeri fel.

Tétel

$L_{\text{PMP}} \notin R$.

Bizonyítás:
Definiáljuk a PMP egy módosított változatát, MPMP-t. Az MPMP probléma igen-példányai olyan (D, d) (dominókészlet,dominó) párok, melyre D-nek van d-vel kezdődő megoldása.

$L_{\text{MPMP}} = \{\langle D, d\rangle \mid d \in D \wedge D\text{-nek van } d\text{-vel kezdődő megoldása}\}$.

Post Megfelelkezési Probléma

$L_{\text{PMP}} = \{\langle D\rangle \mid D\text{-nek van megoldása}\}$,
$L_{\text{MPMP}} = \{\langle D, d\rangle \mid d \in D \wedge D\text{-nek van } d\text{-vel kezdődő megoldása}\}$.

Először megmutatjuk, hogy $L_{\text{MPMP}} \leq L_{\text{PMP}}$.

Jelölés: ha $u = a_1 \cdots a_n \in \Sigma^+$ és $* \notin \Sigma$ akkor legyen

balcsillag$(u) := *a_1 * a_2 \cdots * a_n$
jobbcsillag$(u) := a_1 * a_2 * \cdots a_n *$.
baljobbcsillag$(u) := *a_1 * a_2 * \cdots a_n *$.

Legyen $D = \{d_1, \ldots, d_n\}$ egy tetszőleges dominókészlet, ahol $d_i = \frac{u_i}{v_i}$ $(1 \leq i \leq n)$.

D' legyen a következő $|D| + 2$ méretű készlet:

$$d'_i = \frac{\text{balcsillag}(u_i)}{\text{jobbcsillag}(v_i)} \qquad (1 \leq i \leq n)$$
$$d'_0 = \frac{\text{balcsillag}(u_1)}{\text{baljobbcsillag}(v_1)}, \qquad d'_{n+1} = \frac{*\#}{\#}$$

.

Post Megfelelkezési Probléma

Példa: Ha

$$D = \left\{\frac{ab}{a}, \ \frac{c}{bc}\right\},$$

akkor

$$D' = \left\{\frac{*a*b}{*a*}, \ \frac{*a*b}{a*}, \ \frac{*c}{b*c*}, \ \frac{*\#}{\#}\right\}$$

Állítás: $\langle D, d_1\rangle \in L_{\text{MPMP}} \iff \langle D'\rangle \in L_{\text{PMP}}$.

Az állítás bizonyítása:

- ha $d_{i_1} \cdots d_{i_m}$ MPMP egy (D, d_1) bemenetének egy megoldása, akkor $d'_0 d'_{i_2} \cdots d'_{i_m} d'_{n+1}$ megoldása a D' PMP inputnak.
- ha $d'_{i_1} \cdots d'_{i_m}$ D'-nek, mint PMP inputnak egy megoldása, akkor az első illetve az utolsó betű egyezése miatt ez csak úgy lehetséges, hogy $d'_{i_1} = d'_0$ és $d'_{i_m} = d'_{n+1}$. Ekkor viszont $d_{i_1} \cdots d_{i_{m-1}}$ megoldása a (D, d_1) MPMP bemenetnek.

Ezzel az állítást bizonyítottuk. Mivel ez a megfeleltetés nyilván TG-pel kiszámítható, ezért $L_{\text{MPMP}} \leq L_{\text{PMP}}$.

Post Megfelelkezési Probléma

Most megmutatjuk, hogy $L_u \leq L_{\text{MPMP}}$.

Minden $\langle M, w\rangle$ (TG, szó) párhoz megadunk egy $\langle D, d\rangle$ (dominókészlet, kezdődominó) párt, úgy hogy

$w \in L(M) \iff D$-nek van d-vel kezdődő megoldása.

Legyen $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ és $w = a_1 \cdots a_n \in \Sigma^*$.
(D, d) konstrukciója:

- $d := \frac{\#}{\#q_0 a_1 \cdots a_n \#}$ (ahol $\# \notin \Sigma$) $\quad d :\in D$
- – ha $\delta(p, a) = (q, b, R)$, akkor $\frac{pa}{bq} :\in D$
  – ha $\delta(p, a) = (q, b, L)$, akkor $(\forall c \in \Gamma:)$ $\frac{cpa}{qcb} :\in D$
  – ha $\delta(p, a) = (q, b, S)$, akkor $\frac{pa}{qb} :\in D$
- $(\forall a \in \Gamma:)$ $\frac{a}{a} :\in D$
- $\frac{\#}{\#}, \ \frac{\#}{\sqcup\#}, \ \frac{\#}{\#\sqcup} :\in D$
- $(\forall a \in \Gamma:)$ $\frac{aq_i}{q_i}, \ \frac{q_i a}{q_i} :\in D$
- $\frac{q_i\#\#}{\#} :\in D$.

Post Megfelelkezési Probléma

Példa:

Ha M-nek $\delta(q_0, b) = (q_2, a, R)$ és $\delta(q_2, a) = (q_i, b, S)$ átmenetei, akkor $q_0bab \vdash aq_2ab \vdash aq_ibb$ egy bab-ot elfogadó konfigurációátmenet.

Az $\langle M, bab\rangle$-hoz tartozó dominókészlet tartalmazza többek között a $\frac{\#}{\#q_0bab\#}$ kezdő-, $\frac{q_0b}{aq_2}$ és $\frac{q_2a}{q_ib}$ átmenet- , $\frac{a}{a}$, $\frac{b}{b}$, $\frac{\sqcup}{\sqcup}$ és $\frac{\#}{\#}$ identikus dominókat valamint a befejezéshez szükséges $\frac{aq_i}{q_i}$, $\frac{q_ib}{q_i}$ és $\frac{q_i\#\#}{\#}$ dominókat.

Ekkor egy kirakás (|-al blokkokra osztva):

$$\frac{\#}{\#q_0bab\#}\ \Big|\ \frac{q_0b}{aq_2}\frac{a}{a}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{a}{a}\frac{q_2a}{q_ib}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{aq_i}{q_i}\frac{b}{b}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{q_ib}{q_i}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{q_ib}{q_i}\frac{\#}{\#}\ \Big|\ \frac{q_i\#\#}{\#}$$

Post Megfelelkezési Probléma

$$\frac{\#}{\#q_0bab\#}\ \Big|\ \frac{q_0b}{aq_2}\frac{a}{a}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{a}{a}\frac{q_2a}{q_ib}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{aq_i}{q_i}\frac{b}{b}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{q_ib}{q_i}\frac{b}{b}\frac{\#}{\#}\ \Big|\ \frac{q_ib}{q_i}\frac{\#}{\#}\ \Big|\ \frac{q_i\#\#}{\#}$$

A fenti példán szemléltetjük, hogy $w \in L(M) \iff D$-nek van d-vel kezdődő megoldása.

Az első blokk csak a $d = \frac{\#}{\#q_0bab\#}$ kezdődominóból áll.

A következő két blokkban alul és felül is konfigurációk következnek, felül mindig eggyel "lemaradva".

A 4.-6. blokkokban a $\frac{aq_i}{q_i}$ (és $\frac{q_ia}{q_i}$) típusú dominókkal egyesével behozható a felső szó lemaradása, egészen addig, amíg az alsó rész már csak $q_i\#$-al hosszabb.

Végül a 7. blokkban csak egy (záró)dominó szerepel, melynek az a szerepe, hogy behozza a még megmaradt lemaradást.

Post Megfelelkezési Probléma

A fenti példa alapján meg lehet általános esetben is konstruálni egy megoldást, így $w \in L(M) \Rightarrow$ van $\langle D, d\rangle$-nak megoldása.

Másrészt ha van d-vel kezdődő megoldás, akkor ez a dominósorozat két szavának hosszára vonatkozó megfontolások alapján csak q_i-t tartalmazó dominók használatával lehetséges. Meggondolható, hogy minden kirakás alsó szava az első q_i-t követő $\#$-ig egy $\#$-ekkel elválasztott elfogadó konfigurációátmenet sorozata kell legyen. és így a w szóhoz tartozó kezdőkonfigurációból el lehet jutni elfogadó konfigurációba, azaz $w \in L(M)$.

Nyilván $\langle D, d\rangle$ $\langle M, w\rangle$-ből TG-pel kiszámítható, így beláttuk, hogy $L_u \leq L_{\mathrm{MPMP}}$.

Innen a tétel bizonyítása: $L_u \leq L_{\mathrm{MPMP}}$, $L_{\mathrm{MPMP}} \leq L_{\mathrm{PMP}}$ és tudjuk már, hogy $L_u \notin R$. Ebből a visszavezetés tranzitivitása és korábbi tételünk alapján $L_{\mathrm{PMP}} \notin R$.

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

(Volt:) Egy G környezetfüggetlen (CF, 2-es típusú) grammatikát **egyértelműnek** neveztünk, ha minden $L(G)$-beli szónak pontosan egy baloldali levezetése van G-ben. (**Baloldali levezetés:** mindig a legbaloldalibb nemterminálist írjuk át a mondatformában.)

$L_{\mathrm{ECF}} := \{\langle G\rangle \mid G \text{ egyértelmű CF grammatika}\}$.

Tétel

$L_{\mathrm{ECF}} \notin R$

Bizonyítás: Megmutatjuk, hogy $L_{\mathrm{PMP}} \leq \overline{L_{\mathrm{ECF}}}$.

Legyen $D = \left\{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\right\}$ egy tetszőleges dominókészlet a Σ ábécé felett.

$\Delta := \{a_1, \ldots, a_n\}$ úgy, hogy $\Sigma \cap \Delta = \emptyset$.

$P_A := \{A \to u_1Aa_1, \ldots, A \to u_nAa_n,\ A \to \varepsilon\}$.
$P_B := \{B \to v_1Ba_1, \ldots, B \to v_nBa_n,\ B \to \varepsilon\}$.

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

$G_A = \langle A, \{A\}, \Sigma \cup \Delta, P_A \rangle$. $G_B = \langle B, \{B\}, \Sigma \cup \Delta, P_B \rangle$.
$G_D = \langle S, \{S, A, B\}, \Sigma \cup \Delta, \{S \to A, S \to B\} \cup P_A \cup P_B \rangle$.

$f : \langle D \rangle \to \langle G_D \rangle$ visszavezetés, mert:

- ha $\frac{u_{i_1}}{v_{i_1}} \cdots \frac{u_{i_m}}{v_{i_m}}$ megoldása D-nek, akkor $u_{i_1} \cdots u_{i_m} = v_{i_1} \cdots v_{i_m}$. De ekkor $u_{i_1} \cdots u_{i_m} a_{i_m} \cdots a_{i_1} = v_{i_1} \cdots v_{i_m} a_{i_m} \cdots a_{i_1}$ kétféleképpen is levezethető, így G_D nem egyértelmű.
- ha G_D nem egyértelmű, akkor van olyan szó, aminek két baloldali levezetése van. De ezek $S \to A$-val illetve $S \to B$-vel kell kezdődjenek, hiszen G_A és G_B egyértelmű. A generált szavak xy, $x \in \Sigma^*, y \in \Delta^*$ alakúak, így ugyanaz a generált Σ feletti prefix is. Így a két levezetés D egy megoldását adja.

f nyilván TG-pel kiszámítható. Mivel $L_{\text{PMP}} \notin R$, következik, hogy $\overline{L_{\text{ECF}}} \notin R$, amiből kapjuk, hogy $L_{\text{ECF}} \notin R$.

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

Lemma

Az előző tétel bizonyításában definiált G_A és G_B grammatikák esetén $\overline{L(G_A)}$ és $\overline{L(G_B)}$ környezetfüggetlen.

Bizonyítás: Az állítás nem nyilvánvaló, mivel a környezetfüggetlen nyelvek nem zártak a komplementer képzésre. Elég G_A-ra belátni az állítást, G_B-re ugyanígy bizonyítható.

Legyen $n_i := |u_i|$ $(1 \leq i \leq |D|)$. $L(G_A)$-hoz adható determinisztikus veremautomata.
Ötlet: Amíg Σ-beli betűk jönnek az inputon pakoljuk őket bele a verembe. Ha $a_i \in \Delta$-beli betű jön, akkor próbáljuk meg kivenni u_i^{-1}-et a veremből. Megvalósítás:
$A = \langle \Sigma \cup \{\#\}, Q, T, \delta, q_0, \#, \{s\} \rangle$, ahol

$$Q = \{q_0, r, s\} \cup \bigcup_{i=1}^{|D|} \{q_{i1}, \ldots, q_{i(n_i-1)}\}$$

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

és M_δ:

$\#q_0 t \to \#t q_0 \quad (t \in \Sigma)$

$t_1 q_0 t_2 \to t_1 t_2 q_0 \quad (t_1, t_2 \in \Sigma)$

$t_{n_i} x a_i \to q_{i(n_i-1)} \quad (1 \leq i \leq |D|, x \in \{q_0, r\}, u_i = t_1 \cdots t_{n_i}, n_i \geq 2)$

$t_j q_{ij} \to q_{i(j-1)} \quad (1 \leq i \leq |D|, 2 \leq j \leq n_i - 1, u_i = t_1 \cdots t_{n_i}, n_i \geq 2)$

$t_1 q_{i1} \to r \quad (1 \leq i \leq |D|, u_i = t_1 \cdots t_{n_i}, n_i \geq 2)$

$t r a_i \to r \quad (1 \leq i \leq |D|, u_i = t, t \in \Sigma)$

$\#r \to \#s$

Az veremautomata determinisztikus (teljessé tehető egy zsákutcaállapot és a hiányzó átmenetek hozzávételével.) A determisztikus veremautomatával felismerhető nyelvek osztálya zárt a komplementerképzésre, ugyanis $Q \setminus F$-re változtatva az elfogadó állapothalmazt a veremautomata épp a komplementer nyelvet ismeri fel.

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

Tétel

Eldönthetetlenek az alábbi, G_1 és G_2 környezetfüggetlen grammatikákkal kapcsolatos kérdések.

(1) $L(G_1) \cap L(G_2) \stackrel{?}{=} \emptyset$

(2) $L(G_1) \stackrel{?}{=} L(G_2)$

(3) $L(G_1) \stackrel{?}{=} \Gamma^*$ valamely Γ ábécére

(4) $L(G_1) \stackrel{?}{\subseteq} L(G_2)$

Bizonyítás:

(1) L_{PMP}-t vezethetjük vissza rá. Legyen $D = \left\{ \frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n} \right\}$ a dominókészlet. Készítsük el a fenti G_A és G_B grammatikákat. Könnyen látható, hogy D-nek akkor és csak akkor van megoldása, ha $L(G_A)$-nak és $L(G_B)$-nek a metszete nemüres.

Környezetfüggetlen grammatikákkal kapcsolatos eldönthetetlen algoritmikus problémák

(2) $L := \overline{L(G_A) \cap L(G_A)} = \overline{L(G_A)} \cup \overline{L(G_B)} \in \mathcal{L}_2$, mivel az előző Lemma szerint $\overline{L(G_A)} \in \mathcal{L}_2$ és $\overline{L(G_B)} \in \mathcal{L}_2$ az, és $\mathcal{L}_2$ zárt az unióra.

Legyenek G_1 és G_2 olyan környezetfüggetlen grammatikák, amelyekre $L(G_1) = L$ és $L(G_2) = (\Sigma \cup \Delta)^*$.
$L(G_1) = L(G_2) \Leftrightarrow L(G_A) \cap L(G_B) = \emptyset$, így ha (2) eldönthető volna, akkor (1) is az lenne, de az imént láttuk, hogy nem az.

(3) Legyen G_1 ugyanaz,mint (2)-ben és $\Gamma = \Sigma \cup \Delta$. Pont úgy, mint előbb, (3) eldönthetősége (1) eldönthetőségét implikálná.

(4) Mivel $L(G_1) = L(G_2) \Leftrightarrow L(G_1) \subseteq L(G_2) \wedge L(G_2) \subseteq L(G_1)$, ezért a tartalmazás eldönthetősége (2) eldönthetőségét implikálná.

A matematikai logika formális modelljei

I. **Ítéletkalkulus** (nulladrendű logika)

A modell formális kereteket biztosít olyan következtetések helyességének eldöntésére, melyek elemi állításokból (ítéletekből) épülnek fel. Az ítéletek fontos jellemzője, hogy igazságértékük (igaz/hamis) egyértelműen eldönthető. Ítéletek például a „Süt a nap" vagy a „Lemegyek a térre" de nem tekinthető ítéletnek például a „Laci magas" (mihez képest?), „Lejössz a térre?" (kérdő mondat) vagy „Bárcsak itt lennél" (óhajtó mondat). Az elemi állításokból logikai műveleteknek megfeleltethető nyelvi összekötők segítségével összetett állítások építhetők. Például „Süt a nap, de mégis otthon maradok." (logikai és kapcsolat, konjunkció) vagy „Ha süt a nap, lemegyek a térre." (ha ... akkor, implikáció).

Beláthatók olyan következtetések, mint:

(1) ‚Ha süt a nap, lemegyek a térre."
(2) „Süt a nap."
(3) Tehát „Lemegyek a térre."

Ítéletkalkulus

Definíció

Adott **ítéletváltozók** egy előre rögzített megszámlálhatóan végtelen $\mathrm{Var} = \{x_1, x_2, \ldots\}$ halmaza. Az **ítéletlogikai formulák** Form halmaza a legszűkebb halmaz melyre

- Minden $x \in \mathrm{Var}$ esetén $x \in \mathrm{Form}$,
- Ha $\varphi \in \mathrm{Form}$, akkor $\neg\varphi \in \mathrm{Form}$,
- Ha $\varphi, \psi \in \mathrm{Form}$, akkor $(\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi) \in \mathrm{Form}$.

A műveleti jelek elnevezése: **negáció** ($\neg$), **konjukció** ($\wedge$), **diszjunkció** ($\vee$), **implikáció** ($\rightarrow$). Ez egyben egy csökkenő precedenciasorrend is zárójelek elhagyásához.

Szemantika:

Definíció

Egy $I : \mathrm{Var} \rightarrow \{i, h\}$ függvényt **interpretációnak** (változókiértékelésnek) nevezünk.

Ítéletkalkulus

Egy I interpretációban egy $\varphi \in \mathrm{Form}$ formula $\mathcal{B}_I(\varphi)$ **igazságértékét** (Boole értékét) a következő rekurzóval definiáljuk:

Definíció

- ha $x \in \mathrm{Var}$ akkor $\mathcal{B}_I(x) := I(x)$,
- ha $\varphi \in \mathrm{Form}$ formula, akkor $\mathcal{B}_I(\neg\varphi) := \neg\mathcal{B}_I(\varphi)$,
- ha $\varphi, \psi \in \mathrm{Form}$ formulák, akkor $\mathcal{B}_I(\varphi \circ \psi) := \mathcal{B}_I(\varphi) \circ \mathcal{B}_I(\psi)$, ahol $\circ \in \{\wedge, \vee, \rightarrow\}$,

ahol a műveleteket az alábbi táblázat definiálja.

$\mathcal{B}_I(\varphi)$	$\mathcal{B}_I(\psi)$	$\mathcal{B}_I(\neg\varphi)$	$\mathcal{B}_I(\varphi \wedge \psi)$	$\mathcal{B}_I(\varphi \vee \psi)$	$\mathcal{B}_I(\varphi \rightarrow \psi)$
i	i	h	i	i	i
i	h	h	h	i	h
h	i	i	h	i	i
h	h	i	h	h	i

Ítéletkalkulus

Egy formula igazságértéke csak a benne szereplő ítéletváltozók kiértékelésétől függ.

n ítéletváltozó esetén 2^n lehetséges interpretáció van (ha nem törődünk a formulában nem szereplő ítéletváltozók kiértékelésével).

Definíció

Egy φ ítéletlogikai formula **igazságtáblája** egy $2^n \times (n+1)$-es táblázat, ha $x_1, \dots, x_n$ a φ formulában szereplő ítéletváltozók. A sorok megfelelnek a lehetséges interpretációknak. Az első n oszlop tartalmazza az ítéletváltozók kiértékelését. Egy I interpretációhoz tartozó sor $n+1$. oszlopa pedig $\mathcal{B}_I(\varphi)$-t.

Példa:

x	y	$\neg x \vee y$
i	i	i
i	h	h
h	i	i
h	h	i

Ítéletkalkulus

Definíció

- Egy $\mathcal{I}$ interpretáció **kielégít** egy φ formulát ($I \models_0 \varphi$) ha a formula helyettesítési értéke i az I interpretációban.
- Egy φ formula **kielégíthető**, ha legalább egy interpretáció kielégíti.
- Egy φ formula **kielégíthetetlen**, ha egyetlen interpretáció sem elégíti ki.
- Egy φ formula **tautologia** (ítéletlogikai törvény) ($\models_0 \varphi$), ha minden interpretáció kielégíti.
- Egy φ formulának a ψ formula **tautologikus következménye**($\varphi \models_0 \psi$), ha minden φ-t kielégítő interpretáció kielégíti ψ-t is.
- φ és ψ **tautologikusan ekvivalensek** ($\varphi \sim_0 \psi$), ha $\varphi \models_0 \psi$ és $\psi \models_0 \varphi$ is teljesül.

Példák: $\varphi \to \psi \sim_0 \neg\varphi \vee \psi$, $\quad \neg(\varphi \wedge \psi) \sim_0 \neg\varphi \vee \neg\psi$ (De Morgan)

Ítéletkalkulus

Definíció

- Egy I interpretáció **kielégít** egy $\mathcal{F}$ formulahalmazt ($I \models_0 \mathcal{F}$), ha a formulahalmaz minden formuláját kielégíti.
- Egy $\mathcal{F}$ formulahalmaz **kielégíthető**, ha legalább egy interpretáció kielégíti.
- Egy $\mathcal{F}$ formulahalmaz **kielégíthetetlen**, ha nincs olyan interpretáció, ami egyszerre minden $\mathcal{F}$-beli formulát kielégít.
- Egy $\mathcal{F}$ formulahalmaznak a φ formula **tautologikus következménye**($\mathcal{F} \models_0 \varphi$), ha minden $\mathcal{F}$-t kielégítő interpretáció kielégíti φ-t is.

Példa: $\{x, x \to y\} \models_0 y$

Ítéletkalkulus

Tétel

Legyen $\mathcal{F}$ egy formulahalmaz és φ egy formula. Akkor a következők teljesülnek.

- φ akkor és csak akkor kielégíthetetlen, ha $\neg\varphi$ tautológia.
- $\mathcal{F} \models_0 \varphi$ akkor és csak akkor, ha $\mathcal{F} \cup \{\neg\varphi\}$ kielégíthetetlen.

Ítéletkalkulus

Definíció

- **Literálnak** nevezünk egy x vagy $\neg x$ alakú formulát, ahol $x \in \mathrm{Var}$. Egy literál **alapja** az az ítéletváltozó, amelyik a literálban szerepel.
- **Klóznak** hívunk egy $\ell_1 \vee \cdots \vee \ell_n$ alakú formulát ($n \in \mathbb{N}$), ahol $\ell_1, \ldots \ell_n$ páronként különböző alapú literálok.
- **Konjunktív normálformának** (röviden KNF-nek) nevezünk egy $C_1 \wedge C_2 \wedge \ldots \wedge C_m$ $(m \geq 1)$ alakú formulát, ahol minden $1 \leq i \leq m$-re C_i egy klóz (a KNF egy **tagja**).

Példa:

$x \vee \neg y \vee z$ egy klóz (és 1-tagú KNF is egyben)
$(x \vee \neg y \vee z) \wedge (\neg x \vee z) \wedge \neg y$ egy 3-tagú KNF.

Tétel

Minden ítéletkalkulusbeli formulához megadható egy vele tautologikusan ekvivalens KNF.

Eldönthető problémák a nulladrendű logikában

Állítás: Eldönthetőek az ítéletkalkulus alábbi algoritmikus kérdései:

- egy φ ítéletkalkulusbeli formula kielégíthető-e,
- egy φ ítéletkalkulusbeli formula kielégíthetetlen-e,
- egy φ ítéletkalkulusbeli formula tautológia-e,
- φ és ψ ítéletkalkulusbeli formulákra $\varphi \sim_0 \psi$ fennáll-e,
- egy $\mathcal{F}$ véges ítéletkalkulusbeli formulahalmaz és egy φ formula esetén $\mathcal{F} \models_0 \varphi$ fennáll-e.

Bizonyítás: Készítsük el az ítélettáblákat a szóban forgó formulákra és olvassuk le belőlük.

Megjegyzés: A kérdések eldönthetősége valójában azon múlik, hogy véges sok lehetséges interpretáció van, így megoldhatóak „brute force" módszerrel. Mivel n ítéletváltozó esetén az ítélettáblának 2^n, azaz exponenciális sok sora van, ez nem hatékony. Ugyan ismeretesek az ítélettáblánál jobb módszerek, azonban ezek mindegyike a legrosszabb esetben szintén exponenciális műveletigényű.

A matematikai logika formális modelljei

II. **Elsőrendű logika**

A nulladrendű logika korlátozottan alkalmas a világ leírására, az egyszerű állítások belső szerkezetét nem vizsgálja. Például a „Minden ember halandó.", „Szókrátész ember.", „Szókrátész halandó." állítások nulladrendű formalizálása esetén nincs más lehetőségünk, mint x, y és z-ként formalizálni a fenti állítás-hármast. Ugyanakkor mivel az emberek halmaza részhalmaz a halandók halmazának és Szókrátész az ember-halmaz egy eleme, ezért jó lenne egy olyan modell, ahol a 3. állítás az első 2 következménye.

Egy elsőrendű logikában (nem véletlen a határozatlan névelő!) az állítások belső szerkezetét is figyelembe tudjuk venni. Tudunk egy halmaz összes elemére illetve legalább egy elemére vonatkozó állításokat formalizálni.

Elsőrendű logika

Definiálni fogunk két nyelvet a termek Term és a formulák Form nyelvét. Ehhez előbb definálunk egy megszámlálhatóan végtelen szimbólumhalmazt, a szavak betűinek a halmazát.

Definíció

Egy elsőrendű logika szimbólumhalmaza a következőkből áll

- Pred, a **predikátumszimbólumok** véges halmaza,
- Func, a **függvényszimbólumok** véges halmaza,
- Cnst, a **konstansszimbólumok** véges halmaza,
- $\mathrm{Ind} = \{x_1, x_2, \ldots\}$, az **individuumváltozók** megszámlálhatóan végtelen halmaza
- $\{\neg, \wedge, \vee, \rightarrow, \forall, \exists\}$ műveleti jelek és kvantorok. $\forall$ neve **univerzális kvantor**, míg $\exists$ neve **egzisztenciális kvantor**
- **(,)** és **,** (vessző).

Minden $s \in \mathrm{Pred} \cup \mathrm{Func} \cup \mathrm{Cnst}$-hez hozzá van rendelve egy $\mathrm{ar}(s) \in \mathbb{N}$ szám, a szimbólum **aritása** (a konstansokhoz mindig 0).

Elsőrendű logika

Definíció

A **termek** Term nyelve az a legszűkebb halmaz, amelyre

- minden $x \in \mathrm{Ind}$ esetén $x \in \mathrm{Term}$
- minden $c \in \mathrm{Cnst}$ esetén $c \in \mathrm{Term}$
- minden $f \in \mathrm{Func}$ és $t_1, \dots t_{\mathrm{ar}(f)} \in \mathrm{Term}$ esetén $f(t_1, \dots t_{\mathrm{ar}(f)}) \in \mathrm{Term}$.

Definíció

Az **elsőrendű formulák** Form nyelve az a legszűkebb halmaz, amelyre

- minden $p \in \mathrm{Pred}$ és $t_1, \dots t_{\mathrm{ar}(p)} \in \mathrm{Term}$ esetén $p(t_1, \dots t_{\mathrm{ar}(p)}) \in \mathrm{Form}$. Ezek az **atomi formulák**.
- Ha $\varphi \in \mathrm{Form}$, akkor $\neg\varphi \in \mathrm{Form}$.
- Ha $\varphi, \psi \in \mathrm{Form}$, akkor $(\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi) \in \mathrm{Form}$.
- Ha $\varphi \in \mathrm{Form}$, akkor $\forall x\varphi \in \mathrm{Form}$ és $\exists x\varphi \in \mathrm{Form}$.

Elsőrendű logika

Példa

$\mathrm{Pred} = \{p, q\}, \quad \mathrm{Func} = \{f\}, \quad \mathrm{Cnst} = \{a\}.$

$\mathrm{ar}(p) = \mathrm{ar}(q) = \mathrm{ar}(f) = 2.$

$x,\ a,\ f(x, y),\ f(x, f(a, x)) \in \mathrm{Term}.$

$p(x, y),\ q(x, f(a, a)),\ \neg p(x, f(y, z)),\ (\exists x p(x, y) \to q(x, z)) \in \mathrm{Form}.$

$\varphi_1 = \forall x p(x, a) \in \mathrm{Form},$

$\varphi_2 = \forall x \exists y q(f(x, y), a) \in \mathrm{Form},$

$\varphi_3 = \forall x(\forall y q(f(y, x), y) \to p(x, a)) \in \mathrm{Form}.$

Precedenciasorrend zárójelelhagyáshoz: $\forall, \exists, \neg, \wedge, \vee, \to$.

Elsőrendű logika

Egy elsőrendű logika szemantikáját a szimbólumainak interpretációja és a változók kiértékelése adja meg.

Definíció

Egy elsőrendű logikai szimbólumainak **interpretációja** alatt egy $I = \langle U, I_{\mathrm{Pred}}, I_{\mathrm{Func}}, I_{\mathrm{Cnst}} \rangle$ rendezett négyest értünk, ahol

- U egy tetszőleges, nemüres halmaz (univerzum),
- I_{Pred} minden $p \in \mathrm{Pred}$-hez hozzárendel egy $p^I \subseteq U^{\mathrm{ar}(p)}$ $\mathrm{ar}(p)$-változós relációt U felett,
- I_{Func} minden $f \in \mathrm{Func}$-hez hozzárendel egy $f^I : U^{\mathrm{ar}(p)} \to U$ $\mathrm{ar}(p)$-változós műveletet U-n,
- I_{Cnst} minden $c \in \mathrm{Cnst}$-hez hozzárendel egy $c^I \in U$-t.

Definíció

Változókiértékelés alatt egy $\kappa : \mathrm{Ind} \to U$ leképezést értünk.

Vegyük észre, hogy κ függ az U univerzumtól.

Elsőrendű logika

Példa Az előző példát folytatva legyen $I = \langle \mathbb{N}, I_{\mathrm{Pred}}, I_{\mathrm{Func}}, I_{\mathrm{Cnst}} \rangle$ egy interpretáció, ahol
$I_{\mathrm{Pred}}(p) = p^I, \quad (m, n) :\in p^I \Leftrightarrow m \geq n$
$I_{\mathrm{Pred}}(q) = q^I, \quad (m, n) :\in q^I \Leftrightarrow m = n$
$I_{\mathrm{Func}}(f) = f^I, \quad f^I(m, n) := m + n$
$I_{\mathrm{Cnst}}(a) := 0,$
legyen továbbá κ egy változókiértékelés, amelyre
$\kappa(x) = 5, \kappa(y) = 3.$

Definíció

Egy $t \in \mathrm{Term}$ **értékét** egy I interpretációban a κ változókiértékelés mellett $|t|^{I,\kappa}$ jelöli és a következőképpen definiáljuk

- Ha $x \in \mathrm{Ind}$, akkor $|x|^{I,\kappa} := \kappa(x)$,
- Ha $c \in \mathrm{Cnst}$, akkor $|c|^{I,\kappa} := c^I$,
- $|f(t_1, t_2, \dots, t_{\mathrm{ar}(f)})|^{I,\kappa} := f^I(|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_{\mathrm{ar}(f)}|^{I,\kappa})$.

Példa Az előző példát folytatva $|f(f(x, y), y)|^{I,\kappa} = 11$.

Elsőrendű logika

Definíció

A κ^* változókiértékelés a κ változókiértékelés x-variánsa, ha $\kappa^*(y) = \kappa(y)$ minden $y \in \text{Ind}, y \neq x$ esetén.

Definíció

Egy $\varphi \in$ Form formula **igazságértékét** egy I interpretációban a κ változókiértékelés mellett $|\varphi|^{I,\kappa}$ jelöli és így definiáljuk:

- $|p(t_1, t_2, \dots, t_{\text{ar}(p)})|^{I,\kappa} = i \Leftrightarrow$ $(|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_{\text{ar}(p)}|^{I,\kappa}) \in p^I$,
- $|\neg\varphi|^{I,\kappa} := \neg|\varphi|^{I,\kappa}$
- $|\varphi \circ \psi|^{I,\kappa} := |\varphi|^{I,\kappa} \circ |\psi|^{I,\kappa}$ $\quad \circ \in \{\wedge, \vee, \rightarrow\}$
- $|\forall x\varphi|^{I,\kappa} = i \Leftrightarrow$ ha $|\varphi|^{I,\kappa^*} = i$ κ-nak minden κ^* x-variánsára,
- $|\exists x\varphi|^{I,\kappa} = i \Leftrightarrow$ ha $|\varphi|^{I,\kappa^*} = i$ κ-nak legalább egy κ^* x-variánsára.

A $\neg, \wedge, \vee, \rightarrow$ műveletek ugyanazok, mint az ítéletlogikánál.

Elsőrendű logika

Példa Az előző példát folytatva

$|p(f(y,y),x)|^{I,\kappa} = i.$
$|q(f(y,y),x)|^{I,\kappa} = h.$
$|p(x,y) \rightarrow q(x,y)|^{I,\kappa} = h.$

$\varphi_1 = \forall x p(x,a)$,
Minden természetes szám ≥ 0. $\quad |\varphi_1|^{I,\kappa} = i$,

$\varphi_2 = \forall x \exists y q(f(x,y),a)$,
Minden természetes számhoz hozzá tudjuk adni egy természetes számot úgy, hogy 0-t kapjunk. $\quad |\varphi_2|^{I,\kappa} = h$,

$\varphi_3 = \forall x(\forall y q(f(y,x),y) \rightarrow p(x,a))$,
Ha a természetes számoknak van nulleleme, akkor az egyenlő 0-val, $|\varphi_3|^{I,\kappa} = i$.

Ha $U = \mathbb{Z}$ lenne, akkor φ_2 is igaz lenne.

Elsőrendű logika

Definíció

Legyen φ egy formula, és tekintsük $x \in$ Ind egy előfordulását φ-ben. Azt mondjuk, hogy x ezen előfordulása **kötött**, ha x a φ egy $\exists x\psi$ vagy $\forall x\psi$ alakú részformulájába esik. Ellenkező esetben x ezen előfordulása **szabad**. Ha φ minden individuumváltozójának minden előfordulása kötött, akkor **zárt** formuláról beszélünk.Egyébként a kormula **nyitott**.

Észrevétel: Ha φ zárt, ekkor bármely I interpretáció esetén $|\varphi|^{I,\kappa}$ értéke nem függ κ-tól. Ilyenkor $|\varphi|^{I,\kappa}$ helyett $|\varphi|^I$ írható.

Példa Az előző példában φ_1, φ_2, φ_3 zárt formulák, míg $\forall x p(x,x) \rightarrow q(x,x)$ nyitott, mert x 3. és 4. előfordulását nem tartalmazza kvantált részformula. (A formula részformulái: $\forall x p(x,x) \rightarrow q(x,x)$, $\forall x p(x,x)$, $p(x,x)$, $q(x,x)$.)

Elsőrendű logika

Definíció

- Egy φ elsőrendű logikai formula **kielégíthető**, ha van olyan I interpretáció és κ változókiértékelés, amelyre $|\varphi|^{I,\kappa} = i$, egyébként **kielégíthetetlen**.
- φ **logikailag igaz** (vagy **érvényes**), ha minden I, κ-ra, $|\varphi|^{I,\kappa} = i$, ennek jelölése $\models \varphi$.
- φ és ψ elsőrendű logikai formulák **logikailag ekvivalensek**, ha ha minden I, κ-ra, $|\varphi|^{I,\kappa} = |\psi|^{I,\kappa}$. Jelölése $\varphi \sim \psi$.
- Az $\mathcal{F}$ formulahalmaz **kielégíthető**, ha van olyan I interpretáció és κ változókiértékelés, amelyre $|\varphi|^{I,\kappa} = i$ teljesül minden $\varphi \in \mathcal{F}$-re, egyébként **kielégíthetetlen**.
- Az $\mathcal{F}$ formulahalmaznak φ **logikai következménye** (jelölés: $\mathcal{F} \models \varphi$) ha minden I, κ-ra ha minden $\psi \in \mathcal{F}$-re $|\psi|^{I,\kappa} = i$ teljesül, akkor $|\varphi|^{I,\kappa} = i$ is teljesül.

Eldönthetetlen problémák az elsőrendű logikában

Tétel

Legyen $\textsc{ValidityPred} = \{\langle\varphi\rangle \mid \varphi \text{ logikailag igaz}\}$. Ekkor

(1) $\textsc{ValidityPred} \notin \mathrm{R}$

Nem bizonyítjuk, a bizonyítás megtalálható Gazdag Zsolt: Bevezetés a számításelméletbe elektronikus jegyzetének 61. oldalán.

A bizonyítás egyébként L_{PMP}-t vezeti vissza a fenti problémának megfelelő formális nyelvre. Azaz minden D dominókészlethez megadható egy φ_D elsőrendű formula, amelyre teljesül, hogy D-nek akkor és csak akkor van megoldása, ha $\models \varphi_D$.

(Vagyis egy dominókészlet megoldásának fogalmát formálisan le lehet írni egy elsőrendű logikai formulával.)

Eldönthetetlen problémák az elsőrendű logikában

Következmény

Legyen $\mathcal{F}$ egy elsőrendű formulahalmaz és φ egy elsőrendű formula. Eldönthetetlen, hogy

(2) φ kielégíthetetlen-e

(3) φ kielégíthető-e

(4) $\mathcal{F} \models \varphi$ teljesül-e

Bizonyítás:

(2) $\models \neg\varphi \Leftrightarrow \varphi$ kielégíthetetlen.

(3) Eldönthetetlen nyelv komplementere eldönthetetlen.

(4) $\mathcal{F} \models \varphi \Leftrightarrow \mathcal{F} \cup \{\neg\varphi\}$ kielégíthetetlen

Megjegyzés: Van olyan algoritmus, amely egy tetszőleges φ elsőrendű formulára pontosan akkor áll meg igen válasszal, ha φ kielégíthetetlen (ilyen például az elsőrendű logika rezolúciós algoritmusa). Ezért a kielégíthetetlenség rekurzíve felsorolható. $\Rightarrow$ a kielégíthetőség nem rekurzíve felsorolható.