Logika és számításelmélet

Készítette: Nagy Krisztián

LOGIKA RÉSZ

1. Gondolkodásforma vagy következtetésforma

Egy $F = \{A_1, A_2, \ldots, A_n\}$ állításhalmazból és egy A állításból álló (F, A) pár.

2. Helyes következtetésforma

Egy $F = \{A_1, A_2, \ldots, A_n\}$ állításhalmazból és egy A állításból álló (F, A) pár, ha létezik olyan eset, hogy az F állításhalmazban szereplő mindegyik állítás igaz és minden ilyen esetben az A állítás is igaz.

3. Egyszerű állítás

Egy olyan kijelentés, amelynek tartalmáról eldönthető, hogy igaz-e vagy nem. Egy állításhoz hozzárendeljük az igazságértékét: az i vagy h értéket.

4. Összetett állítás

Egy egyszerű állításokból álló összetett mondat, amelynek az igazságértéke csak az egyszerű állítások igazságértékeitől függ. Az összetett állítások csak olyan nyelvtani összekötőszavakat tartalmaznak, amelyek logikai műveletnek feleltethetők meg.

5. Az ítéletlogika leíró nyelvének ábécéje (V_0)

- Ítéletváltozók (V_v): $X, Y, X_i, \ldots$
- Unér és binér logikai műveleti jelek: $\neg,\ \wedge,\ \vee, \supset$
- Elválasztójelek: ( )

6. Ítéletlogikai formula

1. (alaplépés) Minden ítéletváltozó ítéletlogikai formula. (prímformula)
2. (rekurziós lépés)
   - Ha A ítéletlogikai formula, akkor $\neg A$ is az.
   - Ha A és B ítéletlogikai formulák, akkor $(A \circ B)$ is ítéletlogikai formula, ahol a " $\circ$ " a három binér művelet bármelyike.
3. Minden ítéletlogikai formula az 1.,2., szabályok véges sokszori alkalmazásával áll elő.

7. Közvetlen részformula

1. Prímformulának nincs közvetlen részformulája.
2. $\neg A$ közvetlen részformulája az A formula
3. $Az\ (A \circ B)$ közvetlen részformulái az A (baloldali) és a B (jobboldali).

8. Literál

Ha X ítéletváltozó, akkor az X és a $\neg X$ formulákat literálnak nevezzük. Az ítéletváltozó a literál alapja. (X és $\neg X$ azonos alapú literálok.)

9. Elemi konjunkció

Különböző literálok konjunkciója. Például: $X \wedge Y \wedge \neg Z$

10. Elemi diszjunkció

Különböző literálok diszjunkciója. Például: $X \vee Y \vee \neg Z$

11. Egy *A* formula logikai összetettsége (szerkezeti rekurziót alkalmazó definíció)

1. Alaplépés
   - Ha A ítéletváltozó, akkor $l(A) = 0$
2. Rekurziós lépések
   - $l(\neg A) = l(A) + 1$
   - $l(A \circ B) = l(A) + l(B) + 1$

12. Logikai műveletek hatásköre

Logikai műveletek hatásköre a formula részformulái közül az a legkisebb logikai összetettségű, amelyben az adott logikai összekötőjel előfordul.

13. Fő logikai összekötőjel

Egy formula fő logikai összekötőjele az az összekötőjel, amelynek a hatásköre maga a formula.

14. Interpretáció

$I = V_v \longrightarrow \{i, h\}$

(Annak rögzítését, hogy mely ítéletváltozó igaz és melyik hamis igazságértékű interpretációnak nevezzük.)

15. Szemantikus fa

Egy n-változós szemantikus fa egy n-szintű bináris fa, ahol a szintek a bázisbeli változóknak vannak megfeleltetve. Egy X változó szintjén a csúcsokból kiinduló élpárokhoz $X, \neg X$ cimkéket rendelünk.
X jelentése X igaz, $\neg X$ jelentése X hamis az élhez tartozó interpretációkban, így egy n-szintű szemantikus fa ágain az összes (2^n) lehetséges igazságkiértékelés (I interpretáció) megjelenik.

16. Formula helyettesítési értéke I interpretációban ($B_I(C)$ def. szerkezeti rekurzióval)

1. Ha C formula ítéletváltozó, akkor $B_I(C) = I(C)$
2. Ha C formula negációs, akkor $B_I(\neg C) = \neg B_I(C)$
3. Ha C formula $(A \circ B)$ alakú, akkor $B_I(A \circ B) = B_I(A) \circ B_I(B)$

17. Formula igazságtáblája

Egy n- változós formula igazságtáblája egy olyan $n + 1$ oszlopból és $2^n + 1$ sorból álló táblázat, ahol a fejlécben a bázis (a formula változói rögzített sorrendben) és a formula szerepel. A sorokban a változók alatt az interpretációk (a változók igazságkiértékelései), a formula alatt a formula helyettesítési értékei találhatók.

18. Egy formula igaz/hamis halmaza.

1. Egy formula igazhalmaza azon I interpretációk halmaza, amelyekre a formula helyettesítési értéke igaz.
2. Egy formula hamishalmaza azon I interpretációk halmaza, amelyekre a formula helyettesítési értéke hamis.

19. A φ-igazságértékelés függvény definiálása szerkezeti rekurzióval

1. Ha A prímformula (ítéletváltozó), akkor φA^i feltételt pontosan azok az I interpretációk teljesítik, amelyekben $I(A) = i$, a φA^h feltételt pedig azok, amelyekben $I(A) = h$.
2. A $\varphi(\neg A)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^h feltételek.
3. A $\varphi(A \wedge B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek mind a φA^i, mind a φB^i feltételek.
4. A $\varphi(A \vee B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^i vagy a φB^i feltételek.
5. A $\varphi(A \supset B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^h vagy a φB^i feltételek.

A 2.-5. feltételek hamis változata értelemszerűen adódnak.

20. Interpretáció kielégít egy formulát

Az ítéletlogikában egy I interpretáció kielégít egy B formulát $(I \vDash_0 B)$, ha a formula helyettesítési értéke i az I interpretációban. A formulát kielégítő I interpretációt a formula modelljének is szokás nevezni.

21. Kielégíthetőség/Kielégíthetetlenség/Tautológia formulákra

1. Egy B formula **kielégíthető,** ha legalább egy interpretáció kielégíti.
2. Egy B formula **kielégíthetetlen**, ha egyetlen interpretáció sem elégíti ki.
3. Egy B formula **tautológia** $(\vDash_0 B)$, ha minden interpretáció kielégíti. A tautológiát ítéletlogikai törvénynek is nevezzük.

22. Interpretáció kielégít egy formulahalmazt

Legyen $F = \{A_1, A_2, \dots, A_n\}$ formulahalmaz.
Az ítéletlogikában egy I interpretáció kielégít egy F formulahalmazt $(I \vDash_0 F)$, ha a formulahalmaz minden formulájának helyettesítési értéke i az I interpretációban.

23. Kielégíthetőség/kielégíthetetlenség formulahalmazokra

Legyen $F = \{A_1, A_2, \dots, A_n\}$ formulahalmaz.

1. Egy F formulahalmaz **kielégíthető**, ha legalább egy interpretáció kielégíti.
2. Egy F formulahalmaz **kielégíthetetlen**, ha bármely interpretációban legalább egy formulája h. (Nincs olyan interpretáció, ami kielégítené.)

24. Szemantikus következmény

Egy G formula szemantikus vagy tautologikus következménye az $F = \{F_1, F_2, \dots, F_n\}$ formulahalmaznak, ha minden olyan I interpretációra, amelyre $I \vDash_0 \{F_1, F_2, \dots, F_n\}$ fennáll, $I \vDash_0 G$ is fennáll.
Jelölés: $\{F_1, F_2, \dots, F_n\} \vDash_0 G$

25. Szemantikus következményhez köthető tételek és következtetések

1. Ha egy G formula bármely F feltételhalmaznak következménye, akkor G tautológia $(\vDash_0 G)$
   - Tehát (F, G) akkor helyes következtetésforma, ha teljesül, hogy $F \vDash_0 G$ és létezik olyan I interpretáció, melyre $I \vDash_0 F$
2. Ha F-nek következménye G_1 $(F \vDash_0 G_1)$ és F-nek következménye G_2 $(F \vDash_0 G_2)$ valamint $\{G_1, G_2\}$-nek következménye A $(\{G_1, G_2\} \vDash_0 A)$, akkor F-nek következménye A $(F \vDash_0 A)$

26. Eldöntésprobléma

Eldöntésproblémának nevezik a logikában annak eldöntését, hogy egy (F, G) pár a szemantikus következményfogalom szerint helyes gondolkodásforma-e.

27. Eldöntésproblémához kapcsolódó tételek

1. F-nek akkor és csak akkor következménye G, ha az $F \cup \neg G$ vagy $F_1 \wedge F_2 \wedge \dots \wedge F_n \wedge \neg G$ kielégíthetetlen.
2. (Dedukciós tétel) $\{F_1, F_2, \dots, F_n\} \vDash_0 G$ akkor és csak akkor, ha $\vDash_0 F_1 \supset \left(F_2 \supset \cdots \left(F_{n-1} \supset (F_n \supset G)\right) \dots\right)$

28. Tautologikusan ekvivalens

- (1. változat)
  Két vagy több formula igazságtáblája lehet azonos, ekkor azt mondjuk, hogy a formulák tautologikusan ekvivalensek. Jelölése: $\sim_0$
- (2. változat)
  Az A és B formulák tautologikusan ekvivalensek, ha $A \vDash_0 B$ és $B \vDash_0 A$.
  Ekkor $\vDash_0 (A \supset B) \wedge (B \supset A)$

29. Legszűkebb következmény

Legyen az F feltételhalmazban szereplő változók száma n. Ekkor a legszűkebb következmény az az $\{i, h\}^n \longrightarrow \{i, h\}$ leképezés, amely pontosan azokhoz az interpretációkhoz rendel i értéket, amelyek kielégítik az F-et.

30. Előrekövetkeztetés

Ismert az F feltételhalmaz, és keressük F lehetséges következményeit. Megkeressük F legszűkebb következményét, R-t. Következmény minden olyan G formula, amelyre $R \supset G$ tautológia, azaz R igazhalmaza része G igazhalmazának.

31. Visszakövetkeztetés

Az F feltételhalmaz és a B következményformula ismeretében eldöntjük, hogy B valóban következménye-e F-nek. Mivel $F \vDash_0 B$ pontosan akkor, ha az $F \cup \{\neg B\}$ formulahalmaz kielégíthetetlen.

Más szóval B pontosan akkor következménye F-nek, ha minden olyan interpretációban, ahol B hamis, az F kielégíthetetlen.

32. Matematikai struktúra

A matematikai struktúra egy $\langle U, R, M, K\rangle$ halmaznégyes, ahol

- U: nem üres halmaz, a struktúra értelmezési tartománya (amennyiben U egyfajtájú elemekből áll)
- R: az U-n értelmezett n-változós $(n = 1, 2, \dots, k)$ logikai függvények (alaprelációk) halmaza.
- M: az U-n értelmezett n-változós $(n = 1, 2, \dots, k)$ matematikai függvények (alapműveletek) halmaza.
- K: az U megjelölt elemeinek egy (esetleg üres) részhalmaza.

A **struktúra szignatúrája** (v_1, v_2, v_3 egészértékű függvényegyüttes) megadja az alaprelációk és az alapműveletek aritását, valamint K elemszámát.

33. Termek (Egyfajtájú eset)

1. (alaplépés) Minden individuumváltozó és konstans szimbólum term.
2. (rekurzív lépés) Ha az $f \in F_n$ k-változós függvényszimbólum és $t_1, t_2, \dots, t_k$ termek, akkor $f(t_1, t_2, \dots, t_k)$ is term.
3. Minden term az 1.,2. szabályok véges sokszori alkalmazásával áll elő.

34. Formulák (Egyfajtájú eset)

1. (alaplépés) Ha a $P \in Pr$ k-változós predikátumszimbólum és $t_1, t_2, \dots, t_k$ termek, akkor $P(t_1, t_2, \dots, t_k)$ formula (atomi formula)
2. (rekurzív lépés)
    - Ha A formula, akkor $\neg A$ is az.
    - Ha A és B formulák, akkor $(A \circ B)$ is formula, ahol a " $\circ$ " a három binér művelet bármelyike.
3. Ha A formula, akkor $\forall x A$ és $\exists x A$ is az.
4. Minden formula az 1.,2.,3. szabályok véges sokszori alkalmazásával áll elő.

35. Termek (Többfajtájú eset)

1. (alaplépés) Minden $\pi \in Srt$ fajtájú individuumváltozó és konstans szimbólum π fajtájú term.
2. (rekurzív lépés) Ha az $f \in F_n$ $\left(\pi_1, \pi_2, \dots, \pi_k; \pi_f\right)$ fajtájú függvényszimbólum és $t_1, t_2, \dots, t_k$ rendre $\pi_1, \pi_2, \dots, \pi_k$ fajtájú termek, akkor $f(t_1, t_2, \dots, t_k)$ π_f fajtájú term.
3. Minden term az 1.,2. szabályok véges sokszori alkalmazásával áll elő.

36. Formulák (Többfajtájú eset)

1. (alaplépés) Ha a $P \in Pr\ (\pi_1, \pi_2, \dots, \pi_k)$ fajtájú predikátumszimbólum és $t_1, t_2, \dots, t_k$ rendre $\pi_1, \pi_2, \dots, \pi_k$ fajtájú termek, akkor $P(t_1, t_2, \dots, t_k)$ formula (atomi formula)
2. (rekurzív lépés)
   - Ha A formula, akkor $\neg A$ is az.
   - Ha A és B formulák, akkor $(A \circ B)$ is formula, ahol a " $\circ$ " a három binér művelet bármelyike.
3. Ha A formula, akkor $\forall x A$ és $\exists x A$ is az.
4. Minden formula az 1.,2.,3. szabályok véges sokszori alkalmazásával áll elő.

37. Közvetlen részterm

1. Konstansnak és individuumváltozónak nincs közvetlen résztermje.
2. Az $f(t_1, t_2, \dots, t_k)$ term közvetlen résztermjei a $t_1, t_2, \dots, t_k$ termek.

38. Közvetlen részformula

1. Egy atomi formulának nincs közvetlen részformulája.
2. $\neg A$ közvetlen részformulája az A formula.
3. Az $(A \circ B)$ közvetlen részformulái az A (baloldali) és a B (jobboldali) formulák.
4. A QxA $(Q \in \{\forall, \exists\})$ közvetlen részformulája az A formula.

39. Függvény, reláció, művelet

Legyenek D és R (nemfeltétlenül különböző) halmazok. Függvénynek nevezünk egy $D \longrightarrow R$ leképezést. D a leképezés értelmezési tartománya, R az értékkészlete.

Legyen U egy tetszőleges (individuum)halmaz. Ha $R = \{i, h\}$, akkor a függvény logikai függvény, más néven reláció. Ha $D = R^n$, akkor a függvény matematikai függvény, más néven művelet.

40. Term szerkezeti fája

Egy t term szerkezeti fája egy olyan véges fa, melyre teljesül, hogy

- a gyökeréhez a t term van rendelve,
- ha valamelyik csúcsához egy t' term van rendelve, akkor az adott csúcs gyerekeihez a t' term közvetlen résztermjei vannak rendelve,
- leveleihez individuumváltozók vagy konstansok vannak rendelve.

41. Formula szerkezeti fája

Egy F formula szerkezeti fája egy olyan véges fa, melyre teljesül, hogy

- a gyökeréhez az F formula van rendelve,
- ha valamelyik csúcsához egy F' formula van rendelve, akkor az adott csúcs gyerekeihez az F' formula közvetlen részformulái vannak rendelve,
- leveleihez atomi formulák vannak rendelve.

42. Egy A formula logikai összetettsége

1. Ha A atomi formula, akkor $l(A) = 0$
2. $l(\neg A) = l(A) + 1$
3. $l(A \circ B) = l(A) + l(B) + 1$
4. $l(QxA) = l(A) + 1$

43. Formulában egy x változó egy előfordulása

- **szabad**, ha nem esik x-re vonatkozó kvantor hatáskörébe
- **kötött**, ha x-re vonatkozó kvantor hatáskörébe esik

44. Egy x változó egy formulában

- **kötött változó**, ha x minden előfordulása kötött
- **szabad változó**, ha x minden előfordulása szabad
- **vegyes változó**, ha x-nek van szabad és kötött előfordulása is

45. Formula zártsága

Egy formula

- **zárt**, ha minden változója kötött.
- **nyitott**, ha legalább egy individuumváltozónak van legalább egy szabad előfordulása.
- **kvantormentes**, ha nem tartalmaz kvantort.

46. Alapkifejezés

Alapkifejezés a változót nem tartalmazó L kifejezés (alapformula, alapterm). Ezeket alappéldányoknak is nevezik. Az atomi formulák alappéldányait két csoportba soroljuk:

1. Egy atomi formula **alapatom**, ha argumentumai konstans szimbólumok vagy egy megadott univerzum elemei (Például: $P(c)$)
2. Egy atomi formulát az **atomi formula alappéldányának** nevezzük, ha argumentumai **alaptermek** (Például: $Q(f(a,b),a)$)

47. Elsőrendű logikai nyelv interpretációja

Egy elsőrendű logikai nyelv $L[V_v]$ interpretációja egy, az L nyelvvel azonos szignatúrájú $\langle U, R, M, K\rangle$ matematikai struktúra.

Az I interpretáció működése: $I = \langle I_{Srt}, I_{Pr}, I_{Fn}, I_{Cnst}\rangle$ függvénynégyes, ahol:

- I_{Srt}: $\pi \longmapsto U_\pi$, ahol ha Srt egyértelmű, akkor az interpretáció U univerzuma egyfajtájú elemekből áll
- I_{Pr}: $P \longmapsto P^I$, ahol P^I a struktúra R halmazának egy eleme
- I_{Fn}: $f \longmapsto f^I$, ahol f^I a struktúra M halmazának egy eleme
- I_{Cnst}:$c \longmapsto c^I$, ahol c^I a struktúra K halmazának egy eleme

48. Változókiértékelés

Egy $\kappa: V \longrightarrow U$ leképezés, ahol V a nyelv változóinak halmaza, U pedig az interpretáció univerzuma.

49. Változókiértékelés variánsa

Legyen x egy változó. A κ^* változókiértékelés a κ változókiértékelés x variánsa, ha $\kappa^*(y) = \kappa(y)$ minden x-től különböző y változó esetén.

50. Termek szemantikája

1. Ha c konstansszimbólum, $|c|^{I,\kappa}$ az U-beli c^I elem
2. Ha x individuumváltozó, $|x|^{I,\kappa}$ a $\kappa(x) \in U$ elem (ahol κ egy változókiértékelés)
3. $|f(t_1, t_2, \dots, t_n)|^{I,\kappa} = f^I\big((|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_n|^{I,\kappa})\big)$

51. Formulák szemantikája

1. $|P(t_1, t_2, \dots, t_n)|^{I,\kappa} = i$, ha $(|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_n|^{I,\kappa}) \in P^I$, ahol P^I jelöli a P^I reláció igazhalmazát.
2. $|\neg A|^{I,\kappa} = \neg|A|^{I,\kappa}$
   $|A \wedge B|^{I,\kappa} = |A|^{I,\kappa} \wedge |B|^{I,\kappa}$
   $|A \vee B|^{I,\kappa} = |A|^{I,\kappa} \vee |B|^{I,\kappa}$
   $|A \supset B|^{I,\kappa} = |A|^{I,\kappa} \supset |B|^{I,\kappa}$
3. $|\forall x A|^{I,\kappa} = i$, ha $|A|^{I,\kappa^*} = i$ κ minden κ^* x variánsára
   $|\exists x A|^{I,\kappa} = i$, ha $|A|^{I,\kappa^*} = i$ κ legalább egy κ^* x variánsára

52. $\boldsymbol{I}, \kappa \vDash A$

Az L egy I interpretációja adott κ változókiértékelés mellett kielégít egy elsőrendű A formulát $(I, \kappa \vDash A)$, ha a formula $|A|^{I,\kappa}$ értéke i. Ha az A formula mondat (zárt formula) és $I \vDash A$, akkor azt mondjuk, hogy az I által megadott S struktúra elégíti ki A-t, így $S \vDash A$. Más szóval S modellje A-nak.

53. $\boldsymbol{I} \vDash F$

Ha L egy I interpretációjára az $F = \{F_1, F_2, \dots, F_n\}$ zárt formulahalmazban $|F_k|^I$ értéke i, minden $1 \leq k \leq n$ értékre, akkor I kielégíti F-et. Jelölés: $I \vDash F$

54. Kielégíthető formula

Azt mondjuk, hogy egy G formula kielégíthető, ha L-hez van legalább egy I interpretáció és κ változókiértékelés, hogy $I, \kappa \vDash G$

55. Kielégíthető formulahalmaz

Azt mondjuk, hogy egy F zárt formulahalmaz kielégíthető, ha L-nek legalább egy I interpretációja kielégíti, azaz $I \vDash F$

56. Logikailag igaz

Azt mondjuk, hogy egy G formula logikailag igaz (logikai törvény), ha G igaz minden lehetséges I interpretációra és minden κ változókiértékelésre. Ez azt jelenti, hogy G igaz minden lehetséges interpretáló struktúrában. Jelölés: $\vDash G$

57. Tautológia

Azt mondjuk, hogy egy G formula tautológia, ha G értéktáblájában a prímkomponensekhez rendelhető összes lehetséges igazságérték hozzárendelés esetén a formula helyettesítési értéke i.

58. Kielégíthetetlenség

Azt mondjuk, hogy G formula illetve F formulahalmaz kielégíthetetlen, ha L-hez nincs olyan I interpretáció, hogy $I \vDash G$ illetve, hogy $I \vDash F$. Más szóval egy G formula kielégíthetetlen, ha minden interpretációban a G értéktáblájának minden sorában G helyettesítési értéke h. Az F formulahalmaz kielégíthetetlen, ha az F közös értéktáblájában minden sorban van legalább egy eleme F-nek, amelynek a helyettesítési értéke h.

59. Logikai vagy szemantikus következmény

Azt mondjuk, hogy a G formula logikai (szemantikus) következménye az F formulahalmaznak, ha minden olyan I interpretációra, amelyre $I \vDash F$ teljesül, az $I \vDash G$ is fennáll.

Más szóval $F \vDash G$ teljesül, ha minden interpretáló struktúrában, az F, G közös értéktáblájában minden olyan sorban, ahol az F elemeinek helyettesítési értéke igaz, a G helyettesítési értéke is igaz.

Jelölés: $F \vDash G$ vagy $\{F_1, F_2, \dots, F_n\} \vDash G$

60. Szemantikus következményhez köthető tételek és fogalmak

- (Logikailag igaz) Ha egy G formula bármely F feltételhalmaznak következménye, akkor G logikailag igaz.
- F-nek szemantikus következménye G, akkor és csak akkor, ha az $F \cup \{\neg G\}$ kielégíthetetlen.
- Ha F-nek következménye G_1 és F-nek következménye G_2 valamint $\{G_1, G_2\}$-nek következménye A, akkor F-nek következménye A

61. Legszűkebb következmény

Ha minden iterpretáló struktúrában, a G a közös értéktáblának pontosan azokban a soraiban igaz, ahol $F_1, F_2, \dots, F_n$ mindegyike igaz, akkor G a legszűkebb következménye F-nek.

62. Ekvivalencia

Az A és B elsőrendű formulák logikailag ekvivalensek, ha $\{A\} \vDash B$ és $\{B\} \vDash A$

63. Ha G tautológia, akkor G logikailag igaz

G elsőrendű formula. Ha $\vDash_0 G$, akkor $\vDash G$.

Bizonyítás

Ha $\vDash_0 G$, akkor G igaz a prímkomponenseinek minden igazságkiértékelésére. Tekintsük a G egy I interpretációját, az individuumváltozók egy κ kiértékelése mellett. Ekkor a prímkomponensek igazságértéke kiszámolható és bármi is lesz a konkrét értékük, ezután a G helyettesítési értéke i lesz (mivel a prímkomponenseinek minden igazságkiértékelésére igaz).

64. Ha $F \vDash_0 G$, akkor $F \vDash G$

Bizonyítás

Az F prímkomponenseinek minden, az F-et kielégítő I interpretációjára $(I \vDash_0 F)$ I kielégíti G-t is. Ha az I interpretáció kielégíti F-et, akkor kielégíti G-t is, mivel az egyidejűleg a prímkomponensekre vonatkozó igazságkiértékelés is.

65. Tautologikusan ekvivalens és logikailag ekvivalens kapcsolata

Ha A és B tautologikusan ekvivalens $(A \sim_0 B)$, akkor A és B logikailag ekvivalens $(A \sim B)$.

66. Dedukciós tétel

- $\{F_1, F_2, \dots, F_n\} \vDash G$ akkor és csak akkor, ha $\{F_1, F_2, \dots, F_{n-1}\} \vDash F_n \supset G$
- $\{F_1, F_2, \dots, F_n\} \vDash G$ akkor és csak akkor, ha $\vDash F_1 \supset \big(F_2 \supset \cdots \big(F_{n-1} \supset (F_n \supset G)\big) \dots\big)$

67. Literál

Egy prímformula (ítéletváltozó) vagy annak negáltja. A literál alapja a benne szereplő prímformula. A literált egységkonjunkciónak vagy egységdiszjunkciónak (egységklóz) is nevezhetünk.

68. Elemi konjunkció/diszjunkció

Egységkonjunkciók/diszjunkciók, illetve különböző alapú literálok konjunkciója/diszjunkciója. Az elemi diszjunkciót klóznak is nevezzük.

69. Teljes elemi konjunkció/diszjunkció

Egy elemi konjunkció/diszjunkció teljes egy adott n változós logikai műveletre nézve, ha mind az n ítéletváltozó alapja valamelyik benne szereplő literálnak.

70. Konjunktív normálforma (KNF) / Kitüntetett konjunktív normálforma (KKNF)

A KNF elemi diszjunkciók (klózok) konjunkciója. KKNF, ha teljes elemi diszjunkciók konjunkciója.

71. Diszjunktív normálforma (DNF) / Kitűntetett diszjunktív normálforma (KDNF)

A DNF elemi konjunkciók diszjunkciója. KDNF, ha teljes elemi konjunkciók diszjunkciója.

72. Egyszerűsítési szabályok

1. $(X \vee d) \wedge (\neg X \vee d) = d$, ahol d elemi diszjunkció
2. $(X \wedge k) \vee (\neg X \wedge k) = k$, ahol k elemi konjunkció

73. Klóz illesztése szemantikus fára

Egy klóz illesztése a szemantikus fára az olyan ágak kiválasztása, amelyeken a klóz minden literálja negálva szerepel. Ezekben az interpretációkban ez a klóz hamis.

74. Cáfoló csúcs

Cáfoló csúcsnak nevezzük a szemantikus fa azon csúcsát, amelyiket elérve egy klóz (amely azt megelőzően még nem volt hamis) hamissá válik.

75. Levezető csúcs

Levezető csúcsnak nevezzük a szemantikus fa azon csúcsát, amelyiket követő mindkét csúcs cáfoló csúcs.

76. Szemantikus fa zártsága

A szemantikus fa egy ága zárt, ha cáfoló csúcsban végződik. A szemantikus fa zárt, ha minden ága zárt.

77. Klózhalmaz kielégíthetetlensége

Ha egy S véges klózhalmaz szemantikus fája zárt, akkor S kielégíthetetlen.

78. Rezolvens

Legyenek C_1, C_2 olyan klózok, amelyek pontosan egy komplemens literálpárt tartalmaznak: $C_1 = C_1{}' \vee L_1$ és $C_2 = C_2' \vee L_2$ és $L_1 = \neg L_2$. Ekkor létezik a rezolvensük: a $res(C_1, C_2) = C$ klóz, ami $C = C_1{}' \vee C_2{}'$

79. Rezolvensképzéshez kapcsolódó tétel

$\{C_1, C_2\} \vDash_0 C$. A rezolvensképzés a rezolúciós kalkulus levezetési szabálya (helyes következtetésforma)

80. Rezolúciós levezetés

Egy S klózhalmazból való rezolúciós levezetés egy olyan véges $k_1, k_2, \dots, k_m$ $(m \geq 1)$ klózsorozat, ahol minden $j = 1,2, \dots, m$-re

1. vagy $k_j \in S$
2. vagy van olyan $1 \leq s, t < j$, hogy k_j a (k_s, k_t) klózpár rezolvense.

A levezetés célja az üres klóz levezetése (ez a megállási feltétel).

81. A rezolúciós kalkulus helyes

1. Lemma: Legyen S tetszőleges klózhalmaz és $k_1, k_2, \dots, k_n$ klózsorozat rezolúciós levezetés S-ből. Ekkor minden $k_j, j = 1,2, \dots, n$-re szemantikus következménye S-nek.
2. Tétel: Legyen S tetszőleges klózhalmaz. Ha S-ből levezethető az üres klóz, akkor S kielégíthetetlen.

82. A rezolúciós kalkulus teljes

Tétel: Ha az S véges klózhalmaz kielégíthetetlen, akkor S-ből levezethető az üres klóz.

Bizonyítás: Tetszőleges zárt szemantikus fa esetén előállítunk egy rezolúciós cáfolatot.

83. Levezetési fa

Egy rezolúciós levezetés szerkezetét mutatja. Olyan gráf, amelynek csúcsaiban klózok vannak. Két csúcsból akkor vezet él egy harmadik csúcsba, ha abban a két csúcsban lévő klózok rezolvense található.

84. Lineáris rezolúciós levezetés

Egy S klózhalmazból egy olyan $k_1, l_1, k_2, l_2, \dots., k_{m-1}, l_{m-1}, k_m$ klózsorozat, ahol $k_1, l_1 \in S$ és minden $i = 2,3, \dots, m$ esetben a k_i a k_{i-1}, l_{i-1} rezolvense, ahol $l_{i-1} \in S$, vagy egy korábban megkapott centrális klóz (rezolvense valamely k_s, l_s $(s < i)$-nek).

85. Lineáris inputrezolúciós levezetés

Egy S klózhalmazból egy olyan $k_1, l_1, k_2, l_2, \dots., k_{m-1}, l_{m-1}, k_m$ klózsorozat, ahol $k_1, l_1 \in S$ és minden $i = 2,3, \dots, m-1$ esetben $l_i \in S$, a k_i pedig a k_{i-1}, l_{i-1} rezolvense

86. Egységrezolúciós stratégia

Rezolvens csak akkor képezhető, ha legalább az egyik klóz egységklóz.

87. Horn klóz

Egy klózt Horn klóznak nevezünk, ha legfeljebb egy literálja nem negált.

88. Horn logika

Horn logika az összes, csak Horn klózokat tartalmazó KNF alakú formulák halmaza.

89. Tétel: Minták teljességre

A lineáris input és az egységrezolúciós stratégia teljes a Horn logikában.

90. Horn klózokkal kapcsolatos tételek

1. Ha az □ levezethető lineáris input rezolúcióval egy K klózhalmazból, akkor K-ban van legalább egy egységklóz.
   Bizonyítás
   Az □t az utolsó lépésben csak egy klózhalmazbeli egységklóz felhasználásával kaphatjuk meg.
2. Kielégíthetetlen Horn klózhalmazban van legalább egy egységklóz.

91. Prenex formula

Legyen Q tetszőleges kvantor, a $Q_1x_1Q_2x_2 \dots Q_nx_nB$ formula. $Q_1x_1Q_2x_2 \dots Q_nx_n$ a prefixum, B, kvantormentes formula a formula magja, törzse.

92. Skolem formula

Skolem formula a $\forall x_1 \forall x_2 \dots \forall x_n A$ formula, ahol a prefixumban csak univerzális kvantorok szerepelnek. Ez eldönthető formulaosztály elsőrendben.

93. Elsőrendű klóz

Olyan zárt Skolem formula, aminek a magja az elsőrendű nyelv literáljainak (azaz atomi formuláinak vagy annak negáltjainak) diszjunkciója. Például: $\forall x \forall y \left(P(x) \vee \neg Q\big(x, f(y)\big)\right)$.

94. Számossággal kapcsolatos tételek

1. Ha egy formula azonosan igaz $|U| = n$ számosságon, akkor ennél kisebb számosságon is azonosan igaz.
2. Ha egy formula kielégíthető $|U| = n$ számosságon, akkor ennél nagyobb számosságon is kielégíthető.

95. Löwenheim-Skolem tétel

Ha egy formula kielégíthető egyáltalán, akkor kielégíthető legfeljebb megszámlálhatóan végtelen U-n.

96. Herbrand-bázis

Legyen S egy elsőrendű klózhalmaz és H a klózhalmazhoz tartozó Herbrand-univerzum. A H Herbrand-univerzum feletti alapatomok egy rögzített sorrendjét Herbrand-bázisnak nevezzük.

97. Herbrand-interpretáció

Legyen az S klózhalmaz leíró nyelve $\langle Pr, Fn, Cnst \rangle$, Herbrand-univerzuma pedig H. Herbrand-interpretációinak nevezzük és I_H-vel jelöljük a nyelv azon interpretációit, melyek univerzuma éppen H, és

- minden $c \in Cnst$ konstansszimbólumhoz a $c \in H$ univerzumelemet (önmagát) rendeli, és
- minden k aritású $f \in Fn$ függvényszimbólumhoz hozzárendeli azt az $f^{I_H}: H^k \longrightarrow H$ művelet, amelyikre minden $h_1, h_2, \dots, h_k \in H$ esetén $f^{I_H}(h_1, h_2, \dots, h_k) = f(h_1, h_2, \dots, h_k)$.

98. Kielégíthetetlenség

- Egy elsőrendű klózhalmaz akkor és csak akkor kielégíthetetlen, ha a Herbrand-univerzuma feletti egyetlen Herbrand-interpretáció sem elégíti ki. Nincs Herbrand-modellje.
- Egy S elsőrendű klózhalmaz kielégíthetetlen akkor és csak akkor, ha S bármely szemantikus fájához van véges zárt szemantikus fája.
- Egy S elsőrendű klózhalmaz kielégíthetetlen akkor és csak akkor, ha S klózai alapelőfordulásainak van véges kielégíthetetlen S' részhalmaza.

SZÁMÍTÁSELMÉLET RÉSZ

1. Kiszámítási problémának

Kiszámítási problémának nevezünk egy olyan, a matematika nyelvén megfogalmazott kérdést, amire egy algoritmussal szeretnénk megadni a választ.

2. Kiszámítható függvény

Egy P kiszámítási probléma reprezentálható egy $f_P : A \longrightarrow B$ függvénnyel. Az A halmaz tartalmazza a probléma egyes bemeneteit, jellemzően egy megfelelő ábébé feletti szavakkal kódolva, míg B halmaz tartalmazza a bemenetekre adott válaszokat, szintén valamilyen alkalmas ábécé feletti szavakkal kódolva.

Egy $f: A \longrightarrow B$ függvényt kiszámíthatónak nevezzük, ha minden $x \in A$ elemre az $f(x) \in B$ érték kiszámítható valamilyen algoritmus modellel. Azt mondjuk, hogy egy P probléma megoldható, ha f_P kiszámítható.

3. Eldöntés probléma

Egy speciális kiszámítási probléma az eldöntés probléma, ahol az f_P értékkészlete egy két elemű halmaz: $\{igen, nem\}, \{1,0\}$. A megoldható eldöntési problémákat eldönthető problémáknak nevezzük.

4. SAT probléma

Az egyik legismertebb eldöntési probléma az úgynevezett SAT probléma, amit a következőképpen definiálunk. Adott egy φ ítéletkalkulusbeli konjunktív normálforma. A kérdés az, hogy kielégíthető-e φ.

A SAT probléma eldönthető, hiszen könnyen adható olyan algoritmus, ami eldönti azt, hogy egy φ formula kielégíthető-e. Ez az algoritmus nem csinál mást, mint a φ-ben szereplő változóknak logikai értéket ad az összes lehetséges módon, majd rendre kiértékeli a formulát.

Formálisan: $SAT \coloneqq \{\langle\varphi\rangle |\ \varphi$ kielégíthető zérusrendű $KNF\}$

5. Turing-gép

A Turing-gép olyan $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ rendszer, ahol

- Q az állapotok véges, nem üres halmaza,
- $q_0, q_i, q_n \in Q$, q_0 a kezdő-, q_i az elfogadó és q_n az elutasító állapot,
- Σ és Γ rendre a bemenő jelek és a szalagszimbólumok ábécéje, úgy hogy $\Sigma \subseteq \Gamma$ és $\Gamma - \Sigma$ tartalmaz egy speciális $\sqcup$ szimbólumot,
- $\delta: (Q - \{q_i, q_n\}) \times \Gamma \longrightarrow Q \times \Gamma \times \{L, R, S\}$ az átmenet függvény

6. Konfiguráció

Egy M Turing-gép működésének fázisait konfigurációkkal írhatjuk le. Az M konfigurációja egy olyan uqv szó, ahol $q \in Q$ és $u, v \in \Gamma^*$ úgy, hogy $v \neq \varepsilon$. Ez a konfiguráció az M azon állapotát tükrözi, amikor a szalag tartalma uv (uv előtt és után a szalagon már csak $\sqcup$ van) a gép a q állapotban van, és az író-olvasó fej a v első betűjére mutat.

7. Kezdőkonfiguráció

Az M Turing-gép kezdőkonfigurációja egy olyan $q_0u\sqcup$ szó, ahol u csak Σ-beli betűket tartalmaz.

8. Megállási konfiguráció

Az M Turing-gép uqv konfigurációja megállási konfiguráció, ha $q \in \{q_i, q_n\}$. Továbbá $q = q_i$ esetében elfogadó, míg $q = q_n$ esetében elutasító konfigurációról beszélünk.

9. Turing-gép konfiguráció-átmenete

Az M Turing-gép összes konfigurációinak halmazát jelöljük C_M-el.
Az M konfiguráció-átmenete egy olyan $\vdash \subseteq C_M \times C_M$ reláció, amit a következőképpen definiálunk.
Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$ és $u, v \in \Gamma^*$. A következő három esetet különböztetjük meg:

1. Ha $\delta(q, a) = (r, b, S)$, akkor $uqav \vdash urbv$
2. Ha $\delta(q, a) = (r, b, R)$, akkor $uqav \vdash ubrv'$, ahol ha $v \neq \varepsilon$, akkor $v' = v$, különben $v' = \sqcup$
3. Ha $\delta(q, a) = (r, b, L)$, akkor $uqav \vdash u'rcbv$, ahol ha $u \neq \varepsilon$, akkor $u'c = u$ ($u' \in \Gamma^*, c \in \Gamma$), különben $u' = \varepsilon$ valamint $c = \sqcup$

10. Turing-gép által felismert nyelv

Az M Turing-gép által felismert nyelv azoknak az $u \in \Sigma^*$szavaknak a halmaza, melyekre igaz, hogy $q_0u\sqcup \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ szavakra. Jelölése: $L(M)$

11. Turing-felismerhető és eldönthető nyelv

Egy $L \in \Sigma^*$ nyelv Turing-felismerhető, ha $L = L(M)$ valamely M Turing-gépre. Továbbá egy $L \subseteq \Sigma^*$ nyelv eldönthető, ha létezik olyan M Turing-gép, ami felismeri L-et és minden bemeneten megállási konfigurációba jut. A Turing-felismerhető nyelveket szokás rekurzívan felsorolhatónak, az eldönthető nyelveket pedig rekurzívnak is nevezni. Az összes Turing-felismerhető nyelv osztályát RE-vel, az összes rekurzív nyelvét pedig R-rel fogjuk jelölni. Triviális összefüggés: R⊆ RE

12. Turing-gép időigénye

Tekintsünk egy $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ Turing-gépet és annak egy $u \in \Sigma^*$ bemenő szavát. Azt mondjuk, hogy M időigénye az u szón n $(n \in \mathbb{N})$, ha M a $q_0 u \sqcup$ kezdőkonfigurációból n lépésben egy megállási konfigurációba jut.

Legyen $f : \mathbb{N} \longrightarrow \mathbb{N}$ egy függvény. Azt mondjuk, hogy M időigénye $f(n)$ (vagy azt, hogy M egy $f(n)$ időkorlátos gép), ha minden $u \in \Sigma^*$ input szóra, M időigénye az u szón legfeljebb $f\big(l(u)\big)$.

13. Turing-gép időigényének nagyságrendje

Legtöbbször csak arra vagyunk kiváncsiak, hogy mi az általunk vizsgált Turing-gép időigényének nagyságrendje (azaz vajon lineáris, négyzetes, polinomiális vagy exponenciális-e). Erre használjuk a jól ismert O jelölést. Legyen f és g két $\mathbb{N}$-ből a nem negatív valós számok halmazába képző függvény. Azt mondjuk, hogy az f legfeljebb olyan gyorsan nő, mint a g (Jele: $f(n) = \mathrm{O}\big(g(n)\big)$), ha a következő telesül:
Vannak olyan $n_0 \in \mathbb{N}$ és c pozitív valós számok, hogy minden $n \geq n_0$ esetén $f(n) \leq c \cdot g(n)$.

14. Többszalagos Turing-gép

Legyen $k \geq 1$. A k-szalagos Turing-gép olyan $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ rendszer, ahol a komponensek a δ kivételével megegyeznek az egyszalagos Turing-gép komponenseivel, δ pedig a következőképpen adódik: $\delta : (Q - \{q_i, q_n\}) \times \Gamma^k \longrightarrow Q \times \Gamma^k \times \{L, R, S\}^k$.

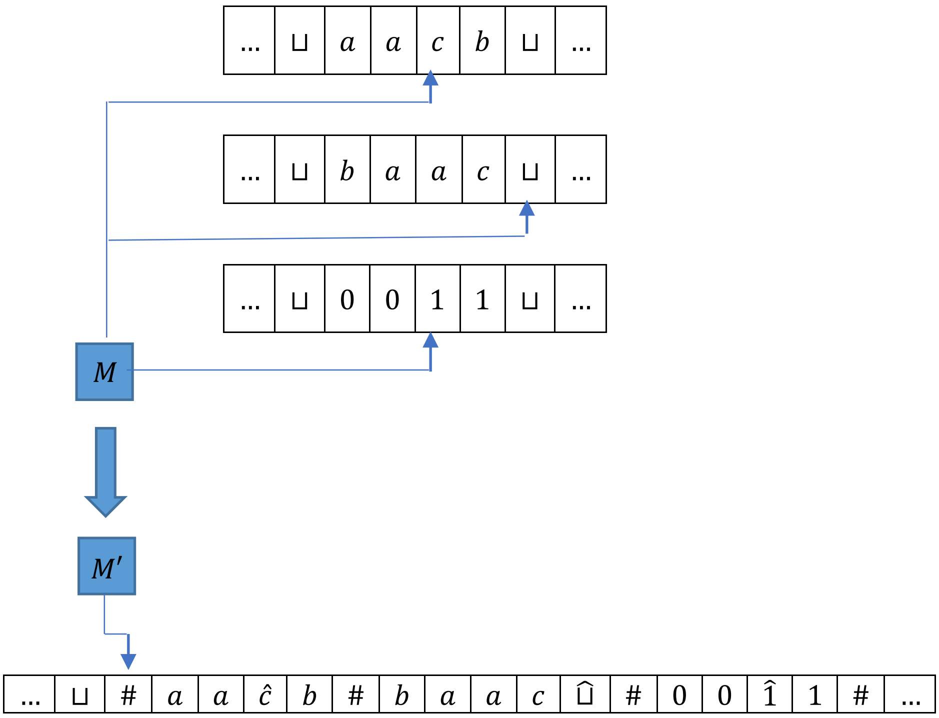
Legyenek $q, p \in Q, a_1, \dots a_k, b_1, \dots, b_k \in \Gamma$ és $D_1, \dots, D_k \in \{L, R, S\}$.
Ha $\delta(q, a_1, \dots a_k) = (p, b_1, \dots, b_k, D_1, \dots, D_k)$, akkor a gép a q állapotból, ha a szalagjain rendre $a_1, \dots a_k$ betűket olvassa, át tud menni a p állapotba, miközben az $a_1, \dots a_k$ betűket átírja $b_1, \dots, b_k$ betűkre és a szalagon a fejeket a $D_1, \dots, D_k$ irányokba mozgatja.

15. Eltérő szalagos Turing-gépek ekvivalenciája

Minden k-szalagos M Turing-géphez van vele ekvivalens egyszalagos M' Turing-gép.

Bizonyítás:

Szemléltetés:



Legyen M k-szalagos Turing-gép. Ha $k = 1$, akkor készen vagyunk. Tegyük fel tehát, hogy $k \geq 2$. Megadunk egy M' egyszalagos Turing-gépet, ami képes szimulálni M működését.

M' egy szalagon, egymás után tárolja az M szalagjainak tartalmát. A különböző szalagokat $\#$ jellel választja el egymástól. Azt, hogy M szalagjain a fejek mely szimbólumokra mutatnak, M' úgy tartja számon, hogy a kérdéses szimbólumokat megjelöli ^ jellel.

A szimuláció lépései a következők. Legyen $w = a_1 \ldots a_n$ az M bemenő szava.

1. M' először előállítja a szalagján M kezdőkonfigurációját, ami így néz ki: $\#\hat{a}_1 a_1 \ldots a_n \# \hat{\sqcup} \# \hat{\sqcup} \ldots \#$.
2. M egy lépésének szimulálásához M' végigolvassa a szalagját az első $\#$-tól kezdve az utolsó (azaz a $k+1$-ik) $\#$-ig. Eközben az állapotában eltárolja a ^ jellel megjelölt szimbólumok ^ nélküli változtait.
3. M' ezután az állapotában eltárolt adatok és M átmenetfüggvénye alapján végrehajtja a sajátszalagján azokat a módosításokat, melyeket M végez a szalagjain.
4. Ha M valamelyik szalagján az utolsó nem $\sqcup$ szimbólum olvasása után jobbra lép, akkor M' a megfelelő $\#$-tól kezdve jobbra mozgatja egy pozícióval a szalagjának tartalmát és a felszabadult helyre beszúr egy $\hat{\sqcup}$ szimbólumot. Hasonlóan jár el M', ha M a legelső nem $\sqcup$ olvasása után balra lép.
5. Ha M valamilyen (elfogadó vagy elutasító) megállási konfigurációba kerül, akkor M' is a megfelelő megállási konfigurációba lép. Egyébként M' folytatja M lépéseinek szimulálását a 2. ponttal.

Látható, hogy M' pontosan akkor lép elfogadó állapotba, amikor M, tehát $L(M) = L(M')$, vagyis a két Turing-gép ekvivalens.

16. Turing-gép egy irányban végtelen szalaggal

Minden többirányú Turing-géphez megadható vele ekvivalens egyirányú Turing-gép.

Bizonyítás (vázlat)

Először szimuláljuk M-et egy olyan M' Turing-géppel, ami két darab egy irányban végtelen szalaggal rendelkezik:

- Az első szalagján szimulálja M-et akkor, amikor az a fej kezdőpozícióján vagy attól jobbra dolgouik,
- A második szalagján pedig akkor, amikor az M a fej kezdőpozíciójától balra dolgozik (ezen a szalagon az ettől a pozíciótól balra levő szó tükörképe van)

Ezután szimuláljuk M'-t egy egy irányban végtelen szalagos Turing-géppel (az eltérő szalagos Turing-gépek ekvivalenciája [15.] tételben látott bizonyításhoz hasonlóan.)

17. Nemdeterminisztikus Turing-gép

A nemdeterminisztikus Turing-gép olyan $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ rendszer, ahol

- Q az állapotok véges, nem üres halmaza,
- $q_0, q_i, q_n \in Q$, q_0 a kezdő-, q_i az elfogadó és q_n az elutasító állapot,
- Σ és Γ rendre a bemenő jelek és a szalagszimbólumok ábécéje, úgy hogy $\Sigma \subseteq \Gamma$ és $\Gamma - \Sigma$ tartalmaz egy speciális $\sqcup$ szimbólumot,
- $\delta: (Q - \{q_i, q_n\}) \times \Gamma \longrightarrow P(Q \times \Gamma \times \{L, R, S\})$ az átmenet függvény.

(A Turing-gép átmeneti függvényét módosíthatjuk úgy, hogy a függvény értéke nem egy konkrét állapot-szalagszimbólum-irány hármas, hanem ezek egy véges halmaza.)

18. Nemdeterminisztikus Turing-gép konfiguráció-átmenete

Egy M nemdeterminisztikus Turing-gép minden konfigurációjából néhány (esetleg nulla) különböző konfigurációba mehet át. Az M konfigurációja a determinisztikus esettel [6.] megeggyezően definiálható.
A konfigurációátmenet pedig a determinisztikus eset [9.] értelemszerű kiterjesztése. Legyen például $uqav$ egy konfiguráció, ahol $a \in \Gamma$ és $u, v \in \Gamma^*$. Ekkor például $uqav \vdash urbv$, ha $(r, b, S) \in \delta(q, a)$

19. Számítási fa

Az M számítási sorozatai egy u szón legegyszerűbben egy fával reprezentálhatók. A fa csúcsa M kezdőkonfigurációja, a szögpontjai pedig M konfigurációi. A fa minden levele megfelel M azon számítási sorozatának az u-n, mely a gyökértől az adott levélig vezető úton előforduló konfigurációkat tartalmazza. M akkor fogadja el u-t, ha a fa valamelyik levele elfogadó konfiguráció. Az így definiált fát nevezzük az M nemdeterminisztikus számítási fájának az u-n.

20. Nemdeterminisztikus Turing-gép eldönt egy nyelvet

Az M nemdeterminisztikus Turing-gép eldönti az $L \subseteq \Sigma^*$ nyelvet, ha felismeri és minden $u \subseteq \Sigma^*$ szóra az M számítási fája véges és minden levele elfogadó vagy elutasító konfiguráció.

21. Nemdeterminisztikus Turing-gép időigénye

Az M nemdeterminisztikus Turing-gép $f(n)$ időigényű, ha minden $u \subseteq \Sigma^*$ n hosszú szóra a számítási fa legfeljebb $f(n)$ magas.

22. Nemdeterminisztikus Turing-gép megfeleltetése determinisztikus Turing-géppel

Minden $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ $f(n)$ idejű nemdeterminisztikus Turing-géphez megadható egy ekvivalens, $2^{O(f(n))}$ idejű M' (determinisztikus) Turing-gép.

Bizonyítás

Legyen M nemdeterminisztikus Turing-gép. Megadunk egy M' háromszalagos, determinisztikus Turing-gépet, ami ekvivalens M-el. Azt már korábban láttuk, hogy M'-höz megadható egy ekvivalens egyszalagos Turing-gép [15.].
M' első szalagja tartalmazza az u bemenő szót. A második szalagon történik az M számítási sorozatainak a szimulációja. Ez a szalag tartalmazza M egy konkrét számítási sorozatának a lépésenkénti eredményét. A harmadik szalagon lévő szó alapján szimulálja M' az M számítási sorozatait, egyesével véve sorra azokat. A szalagon a fej pozíciója mutatja azt, hogy hányadik lépését szimulálja éppen M' az M számítási sorozatának. A harmadik szalagon tulajdonképpen az u-t elfogadó konfigurációk egy szélességi keresése történik a nemdeterminisztikus számítási fában.

Legyen d az M átmenetfüggvénye által megadott halmazok közül a legnagyobb elemszámúnak a számossága. Tegyük fel továbbá, hogy az átmenetfüggvény által megadott halmazokban az elemeknek van egy rögzített sorrendje. Világos, hogy az u számítási fájának minden szögpontjához egyértelműen hozzárendelhető egy $\Sigma = \{1, \dots, d\}$ feletti szó. Nevezetesen az, amelyik megmutatja, hogy a kezdőkunfigurációból az átmenetfüggvény nemdeterminisztikus lehetőségei közül mely választásokkal juthatunk el az adott szögpontban lévő konfigurációkhoz.
Maga a szimuláció a következőképpen történik:

1. Kezdetben az 1-es szalag tartalmazza az u bemenő szót, a 2-es és 3-as szalagok üresek.
2. M' átmásolja az első szalag tartalmát a 2. szalagra
3. M' szimulálja a második szalagon M egy számítási sorozatát. Az hogy melyiket kell szimulálnia a 3-ik szalagján lévő szótól függ. M' a szimuláció minden lépése előtt megnézi a 3-ik szalagján lévő szó kezdőbetűjét és e betű szerint választ M átmenetfüggvényének a lehetőségei közül. ha nincs megfelelő sorszámú választási lehetőség, vagy a 3-ik szalagon már nincs több betű, akkor a szimuláció véget ért és a 4. lépésre ugrunk, Végül, ha M' azt látja, hogy M elfogadó konfigurációba kerül, akkor M' is elfogadó állapotba lép és megáll.
4. M' kicseréli a 3-ik szalagján levő szót az azt lexikografikusan követő szóra, a fejet a szó elejére állítja és a 2-ik pontra ugorva újrakezdi M működésének szimulálását.

Látható, hogy M' pontosan akkor kerül elfogadó konfigurációba egy szón, ha M-nek van ezen a szón elfogadó konfigurációba vezető számítási sorozata. Következik tehát, hogy M és M' ekvivalensek.

23. R és RE kapcsolata

$RE = \{L|L\ Turing\ felismerhető\}$, $R = \{L|L\ eldönthető\}$ Kapcsolatuk: $R \subseteq$ RE

24. Univerzális nyelv (Eldönthetetlen problémák rész)

Azon (M, w) párok halmazát (egy megfelelő bináris szóval kódolva), ahol M egy $\{0,1\}$ bemenő ábécé feletti Turing-gép, w pedig egy $\{0,1\}$-feletti szó, úgy hogy $w \in L(M)$, azaz M elfogadja w-t univerzális nyelvnek nevezzük és L_u-val jelöljük. Tehát $L_u = \{\langle M, w\rangle |\ w \in L(M)\}$, ahol $\langle M, w\rangle$ jelölés a később megadásra kerülő bináris kódolást jelenti.

25. Diagonális nyelv

Azt a nyelvet, mely azon $\{0,1\}$-feletti Turing-gépek bináris kódjait tartalmazza, melyek nem fogadják el önmaguk kódját mint bemenő szót diagonális nyelvnek nevezzük és $L_{átló}$-val jelöljük.
$L_{átló} = \{\langle M\rangle | \langle M\rangle \notin L(M)\} = \{w_i |\ i \geq 1, w_i \notin L(M_i)\}$

Megjegyzés: Az $L_{átló}$ egy olyan nyelv, ami nem rekurzív, sőt nem is rekurzívan felsorolható.

26. Turing-gépek kódolása (azaz $\langle M, w\rangle$ és $\langle M\rangle$ definíciója)

Legyen $M = (Q, \{0,1\}, \Gamma, \delta, q_0, q_i, q_n)$ és tegyük fel, hogy

- $Q = \{p_1, \dots, p_k\}$ valamely $k \geq 3$-ra úgy, hogy $p_1 = q_0, p_{k-1} = q_i$ és $p_k = q_n$
- $\Gamma = \{X_1, \dots, X_m\}$ valamely $m \geq 3$-ra úgy, hogy $X_1 = 0, X_2 = 1$ és $X_3 = \sqcup$
- A fej irányait D_1-gyel és D_2-vel jelöljük

M egy $\delta(p_i, X_j) = (p_r, X_s, D_t)$ átmenete egyértelműen elkódolható a $0^i10^j10^r10^s10^t$ szóval.

$\langle M\rangle := \langle\delta_1\rangle 11 \langle\delta_2\rangle 11 \dots 11 \langle\delta_l\rangle$, ahol $\delta_1, \dots, \delta_l$ az M összes átmenete
$\langle M, w\rangle := \langle M\rangle 111 w$

(Részletesebben Számelmélet jegyzet 41. oldal 2.4.1. alfejezet)

Megjegyzés: A $\{0,1\}^*$ elemei felsorolhatóak: $\{\varepsilon, 0,1,00,01,10,11,000, \dots 111, \dots\}$
Jelölések: Minden $i \geq 1$-re, w_i jelöli a $\{0,1\}^*$ halmaz i-ik elemét. M_i jelöli a w_i által kódolt Turing-gépet

27. A Diagonális nyelv nem Turing-felismerhető (nem rekurzívan felsorolható)

Tétel: $L_{átló} \notin RE$

Bizonyítás

Tekintsük azt a T táblázatot, melynek oszlopai rendre a $w_1, w_2, \ldots$ szavakkal, a sori pedig az $M_1, M_2, \ldots$ Turing-gépekkel vannak cimkézve (tehát T egy végtelen kétdimenziós mátrix). A T elemei 0 és 1 lehetnek az alábbiak szerint. Minden $i, j \geq 1$-re $T(i, j)$ értéke pontosan akkor 1, ha $w_j \in L(M_i)$.

T	w_1	w_2	w_3	w_4	…
M_1	0	0	0	0	…
M_2	0	1	0	0	…
M_3	1	0	1	0	…
M_4	0	0	1	1	…
…	…	…	…	…	…

Ebben a táblázatban például a második sor második eleme 1, ami azt jelenti, hogy M_2 elfogadja a w_2 szót (ez persze a valóságban nem igaz, hisz w_2 nem kódol legális Turing-gépet, így M_2 nem is ismerhet fel semmilyen szót, de az összefüggések szemléltetéséhez feltesszük, hogy a táblázat helyes).

Minden $i \geq 1$-re a táblázat i-ik sora tekinthető úgy, mint az $L(M_i)$ nyelv karakterisztikus függvénye. Nevezetesen azért, mert minden $j \geq 1$ a w_j szó pontosan akkor eleme $L(M_i)$-nek, ha az i-ik sor j-ik eleme 1. Ebben az értelemben a táblázat átlójában szereplő bitsorozat komplementere pedig nem más, mint az $L_{átló}$ karakterisztikus függvénye. Ezért nyilvánvaló, hogy minden $i \geq 1$-re az $L_{átló}$ karakterisztikus függvénye különbözik $L(M_i)$ karakterisztikus függvényétől. Mivel minden M Turing-géphez van olyan $i \geq 1$ szám, hogy $L(M) = L(M_i)$, kapjuk, hogy az $L_{átló}$ nem lehet egyenlő az $L(M)$-mel semmilyen M Turing-gépre. Adódik tehát, hogy $L_{átló} \notin RE$.

28. Az Univerzális nyelv Turing-felismerhető (rekurzívan felsorolható)

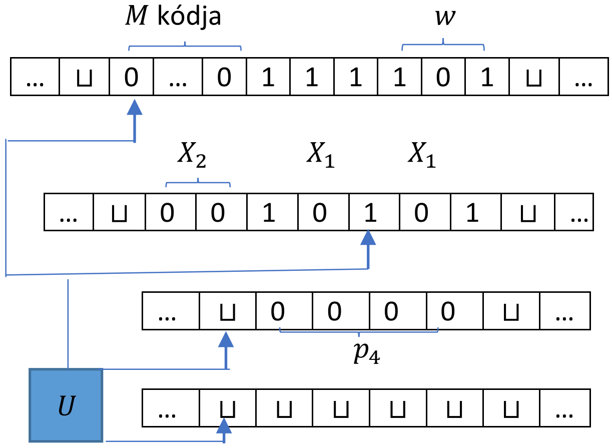
Tétel: $L_u \in RE$

Bizonyítás (vázlat):

L_u-t egy úgynevezett Univerzális Turing-gép ismeri fel

U működése vázlatosan:

- Megnézi, hogy a bemenetén szereplő szó kódol-e Turing-gépet. Ha nem elutasítja a bemenetet.
- Szimulálja M egy lépését:
  - Leolvassa a második szalagról M aktuálisan olvasott szalagszimbólumát
  - Leolvassa a harmadik szalagról M aktuális állapotát
  - Szimulálja M egy lépését (ha kell, használja a segédszalagot)
- Ha M aktuális állapota elfogadó vagy elutasító, akkor U is belép a saját elfogadó vagy elutasító állapotába.



A szalagok rendre felülről-lefele:
M bemenete (u), M szalagja elkódolva,
M állapota elkódolva, Segédszalag

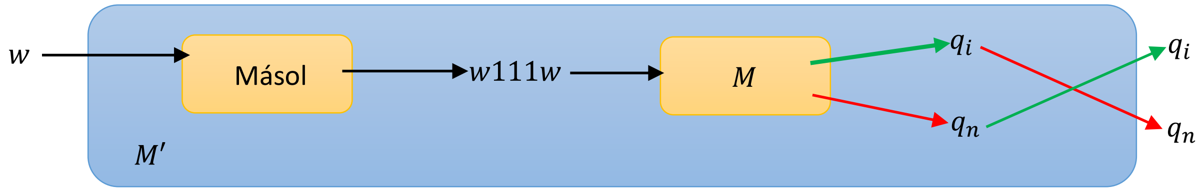
Megjegyzés: Ha M nem áll meg w-n, akkor U sem áll meg $\langle M, w \rangle$-n.

29. Az univerzális nyelv nem eldönthető

Tétel: $L_u \notin R$

Bizonyítás

Az állítást indirekt módon bizonyítjuk. Tegyük fel, hogy L_u eldönthető és legyen M egy Turing-gép, ami eldönti L_u-t. M-ből megkonstruálunk egy olyan M' Turing-gépet, ami $L_{átló}$-t dönti el:



Adott w bemenetre M' a következőképpen működik:

1. Előállítja w-ből $w' = w111w$ szót.
2. w'-n szimulálja M-et.
3. Ha M elfogadja w'-t, akkor M' elutasítja w-t.
4. Ha M elutasítja w'-t, akkor M' elfogadja w-t.

Mivel M minden bemeneten megáll, M' is megáll minden bemeneten. Továbbá $w \in L(M')$ akkor és csak akkor, ha $w' \notin L_u$, azaz ha a w' által kódolt Turing-gép nem fogadja el önmaga kódját bemenetként. Ez azt jelenti, hogy $w \in L(M')$ pontosan akkor teljesül, ha $w \in L_{átló}$. Azt kapjuk tehát, hogy $L(M') = L_{átló}$, vagyis $L_{átló}$ eldönthető. Ez viszont ellentmond a [27.] tételnek, mely szerint $L_{átló} \notin RE$. Ezzel a tétel bizonyítását befejeztük.

30. Komplementer képzés

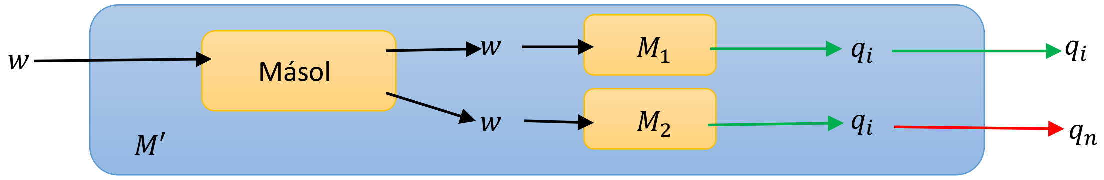
Ha $L \subseteq \Sigma^*$, akkor $\overline{L} \coloneqq \{u \in \Sigma^* \mid u \notin L\}$

31. Ha egy nyelv és a komplementere rekurzívan felsorolható, akkor a nyelv eldönthető

Tétel: Legyen L egy nyelv. Ha $L, \overline{L} \in RE$, akkor $L \in R$

Bizonyítás

Legyen M_1 és M_2 rendre az L-t és $\overline{L}$-t felismerő Turing-gép. Konstruáljuk meg M'-t az alábbi módon:



M' lemásolja w-t a második szalagjára, majd felváltva szimulálja M_1 és M_2 egy-egy lépését addig, amíg valamelyik elfogadó állapotba lép. Így M' az L nyelvet ismeri fel és minden bemeneten meg is áll, azaz $L \in R$

Következmény: A rekurzívan felsorolható nyelvek nem zártak a komplementerképzésre.

32. A rekurzívan felsorolható nyelvek nem zártak a komplementerképzésre.

Következmény: A rekurzívan felsorolható nyelvek nem zártak a komplementerképzésre.

Bizonyítás

Legyen $L \in RE - R$ (Az (L_u) például egy ilyen nyelv)
Ha $\overline{L} \in RE$, akkor a [31.] tétel miatt $L \in R$, ami ellentmondás.

33. A rekurzív nyelvek zártak a komplementer képzésre

Tétel: Ha $L \in R$, akkor $\overline{L} \in R$.

Bizonyítás

Legyen L rekurzív nyelv. Ekkor van olyan M Turing-gép, ami eldönti L-et. Tudjuk, hogy ekkor M olyan, hogy minden L-beli szón q_i-ben áll meg, az összes többi szón pedig q_n-ben, vagyis minden szón megáll. Legyen M' az a Turing-gép, amit úgy kapunk M-ből, hogy M összes olyan átmenetét, ami q_i-be megy q_n-be irányítjuk, a q_n-be menő átmeneteket pedig q_i-be. Nem nehéz belátni, hogy az így definiált M' az $\overline{L}$ nyelvet dönti el.

34. Egy $f: \Sigma^* \longrightarrow \Delta^*$ függvény kiszámíthatósága

Legyen Σ és Δ két ábécé és f egy Σ^*-ból Δ^*-ba képző függvény. Azt mondjuk, hogy f kiszámítható, ha van olyan M Turing-gép, hogy M-et egy $w \in \Sigma^*$ szóval a bemenetén indítva, M úgy áll meg, hogy a szalagján az $f(w)$ szó van.

35. Egy nyelv visszavezethető egy másik nyelvre

Legyen $L_1 \subseteq \Sigma^*$ és $L_2 \subseteq \Delta^*$ két nyelv (azaz eldöntési probléma). Azt mondjuk, hogy L_1 visszavezethető L_2-re (jele: $L_1 \leq L_2$), ha van olyan $f: \Sigma^* \longrightarrow \Delta^*$ kiszámítható függvény, hogy minden $w \in \Sigma^*$ szóra, $w \in L_1$ akkor és csak akkor, ha $f(w) \in L_2$.

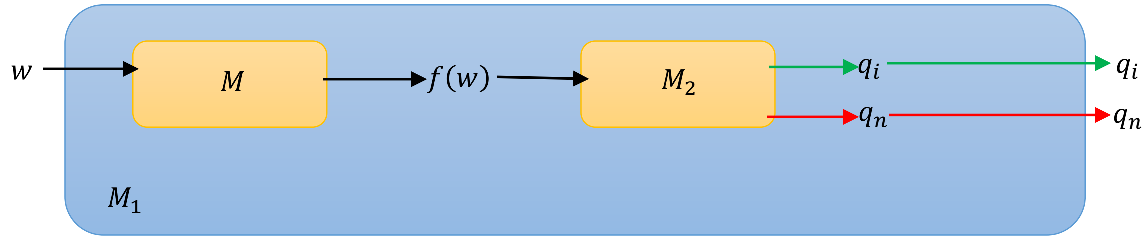
36. Visszavezetéssel kapcsolatos tételek

Tétel: Legyen $L_1 \subseteq \Sigma^*$ és $L_2 \subseteq \Delta^*$ két eldöntés probléma és tegyük fel, hogy $L_1 \leq L_2$. Ekkor igazak az alábbi állítások:

1. Ha $L_1 \notin R$, akkor $L_2 \notin R$.
2. Ha $L_1 \notin RE$, akkor $L_2 \notin RE$

Bizonyítás

Csak a második állítást bizonyítjuk, az első bizonyítása hasonló.
Indirekt módon tegyük fel, hogy L_2 mégis rekurzívan felsorolható. Ekkor van olyan M_2 Turing-gép, hogy $L_2 = L(M_2)$. Továbbá van olyan M Turing-gép, ami kiszámolja az $L_1 \leq L_2$-ben alkalmazott f függvényt. Ezen gépek segítségével megadunk egy olyan M_1 Turing-gépet, ami L_1-et ismeri fel. M_1 szerkezete:



M_1 egy w bemeneten először szimulálja az M gépet. Amikor végez, akkor a szalagján lévő $f(w)$ szón szimulálja M_2 működését. Ha M_2 elfogadja az $f(w)$ szót, akkor M_1 is elfogadja a w-t. Ha M_2 elutasítja $f(w)$-t, akkor M_1 is elutasítja w-t. megjegyezzük, hogy ha M_2 nem áll meg az $f(w)$ bemeneten, akkor M_1 sem áll meg w-n. Könnyen belátható, hogy az így vázolt M_1 gép pontosan az L_1 nyelvet ismeri fel. Felvetésünk szerint azonban az $L_1 \notin RE$, tehát ellentmondáshoz jutottunk. Következtetésképpen L_2 nem lehet rekurzívan felsorolható.

37. Turing-gépek megállási problémája

Legyen $L_h = \{\langle M, w\rangle |\ M\ megáll\ a\ w\ bemeneten\}$, azaz L_h azon $\langle M, w\rangle$ Turing-gép és bemenet párosokat tartalmazza megfelelően kódolva, melyekre teljesül, hogy az M gép megáll a w bemeneten. Nevezzük ezt a nyelvet megállási problémának.

Megjegyzés: $L_u \subseteq L_h$

38. A megállási probléma nem eldönthető

Tétel: $L_h \notin R$

Bizonyítás

Kotábbi tételek alapján elég megmutatni, hogy $L_u \leq L_h$.
Tetszőleges M Turing-gépre, legyen M' az alábbi Turing-gép: M' tetszőleges u bemeneten a következőt teszi:

- Futtatja M-et u-n
- Ha M q_i-be lép, akkor M' is q_i-be lép
- Ha M q_n-be lép, akkor M' egy végtelen ciklusba lép

Belátható, hogy az $f: \langle M\rangle \longrightarrow \langle M'\rangle$ leképezés egy kiszámítható függvény, továbbá az is, hogy tetszőleges $\langle M, w\rangle$ Turing-gép és bemenet párosra:
$\langle M, w\rangle \in L_u \Leftrightarrow M$ elfogadja w-t $\Leftrightarrow$ Az M' megáll w-n $\Leftrightarrow \langle M', w\rangle \in L_h$.
Tehát az M' konstrukciója az L_u visszavezetése L_h-ra. Következik, hogy $L_h \notin R$

39. A megállási probléma rekurzívan felsorolható

Tétel: $L_h \in RE$

Bizonyítás

Kotábbi tételek alapján elég megmutatni, hogy $L_h \leq L_u$.
Tetszőleges M Turing-gépre, legyen M' az alábbi Turing-gép: M' tetszőleges u bemeneten a következőt teszi:

- Futtatja M-et u-n
- Ha M q_i-be vagy q_n-be lép, akkor $M' q_i$-be lép

Belátható, hogy az $f: \langle M\rangle \longrightarrow \langle M'\rangle$ leképezés egy kiszámítható függvény, továbbá az is, hogy tetszőleges $\langle M, w\rangle$ Turing-gép és bemenet párosra:
$\langle M, w\rangle \in L_h \Leftrightarrow$ Az M megáll w-n $\Leftrightarrow$ Az M' elfogadja w-t $\Leftrightarrow \langle M', w\rangle \in L_u$
Tehát az M' konstrukciója az L_h visszavezetése L_u-ra. Következik, hogy $L_h \in RE$

40. Rekurzívan felsorolható nyelek egy tulajdonsága

Ha $\mathcal{P}$ a rekurzívan felsorolható nyelvek egy osztálya, akkor $\mathcal{P}$-t a rekurzívan felsorolható nyelvek egy tulajdonságának nevezzük. Azt mondjuk, hogy egy $L \in RE$ nyelv rendelkezik a $\mathcal{P}$ tulajdonsággal, ha $L \in \mathcal{P}$.
Formálisan: $L_{\mathcal{P}} = \{\langle M \rangle |\ L(M) \in \mathcal{P}\}$

Azt mondjuk, hogy $\mathcal{P}$ triviális tulajdonság, ha minden nyelvre vagy egyetlen nyelvre sem teljesül ($\mathcal{P} = RE$ vagy $\mathcal{P} = \emptyset$).
Azt mondjuk, hogy $\mathcal{P}$ nemtriviális tulajdonság, ha $\mathcal{P} \neq RE$ és $\mathcal{P} \neq \emptyset$.

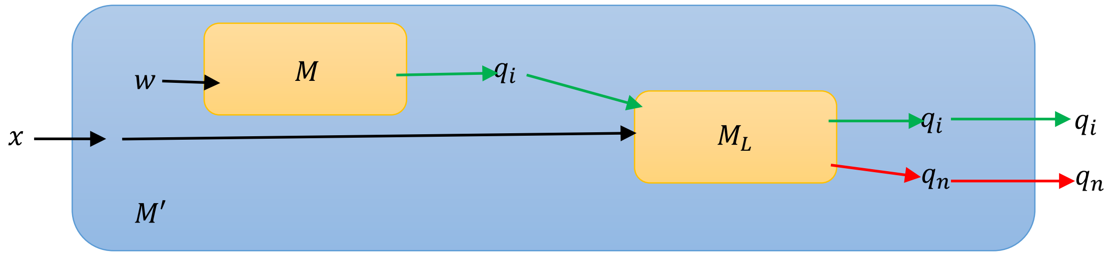
41. Nemtriviális tulajdonsággal kapcsolatos tétel (Rice-tétele)

Tétel: Legyen $\mathcal{P}$ a rekurzívan felsorolható nyelvek egy nemtriviális tulajdonsága. Ekkor az $L_{\mathcal{P}}$ nyelv eldönthetetlen.
Formálisan: Ha $\mathcal{P} \subseteq$ RE egy nemtriviális tulajdonság, akkor $L_{\mathcal{P}} \notin R$

Bizonyítás

Legyen $\mathcal{P}$ egy netriviális tulajdonság. Mivel $L_u \notin R$, elég megmutatni, hogy $L_u \leq L_{\mathcal{P}}$.

- $\emptyset \notin \mathcal{P}$ eset:
  Legyen $L \in \mathcal{P}$ és M_L egy L-et felismerő Turing-gép. Legyen továbbá $\langle M, w \rangle$ egy tetszőleges Turing-gép és bemenet páros, továbbá M' a következő kétszalagos Turing-gép:



  M' működése a következő:
  1. Szimulálja M-et w-n
  2. Ha M nem fogadja el w-t, akkor M' leáll (azaz nem fogadja el x-et $\Longrightarrow L(M') = \emptyset$)
  3. Ha M elfogadja w-t, akkor M' szimulálja M_L-et x-en (azaz $L(M') = L$)

  Belátható tehát, hogy $\langle M, w \rangle \in L_u \Leftrightarrow L(M') = L \Leftrightarrow L(M') \in \mathcal{P} \Leftrightarrow \langle M' \rangle \in L_{\mathcal{P}}$
  Tehát, $L_u \leq L_{\mathcal{P}}$, amiből pedig következik, hogy $L_{\mathcal{P}} \notin R$

- $\emptyset \in \mathcal{P}$ eset:
  Ismételjük meg a fenti bizonyítást $\overline{\mathcal{P}} = RE - \mathcal{P}$-re. Azt kapjuk, hogy $L_{\overline{\mathcal{P}}} \notin R$. Másrészt a $\overline{\mathcal{P}}$-beli nyelveket felismerő Turing-gépek kódjai megegyeznek az olyan Turing-gépek kódjaival, melyek nem $\mathcal{P}$-beli nyelveket ismernek fel ($L_{\overline{\mathcal{P}}} = \overline{L_{\mathcal{P}}}$). Tehát $\overline{L_{\mathcal{P}}} \notin R$, amiből $L_{\overline{\mathcal{P}}} \notin R$, mivel R zárt a komplementer-képzésre.

42. Post megfelelkezési probléma

A PMP-t a következőképpen definiáljuk. Legyen Σ egy legalább két betűt tartalmazó ábécé, és legyen $D = \left\{\left[\frac{u_1}{v_1}\right], \dots, \left[\frac{u_n}{v_n}\right]\right\}$ $(n \geq 1)$ egy dominóhalmaz ahol $u_1, \dots, u_n, v_1, \dots, v_n \in \Sigma^+$. A kérdés az, hogy van-e egy olyan $1 \leq i_1, \dots, i_m \leq m$ $(m \geq 1)$ indexsorozat, melyre teljesül, hogy a $\left[\frac{u_{i_1}}{v_{i_1}}\right], \dots, \left[\frac{u_{i_m}}{v_{i_m}}\right]$ dominókat egymás mellé írva alul és felül is ugyan az a szó adódik, azaz $u_{i_1}, \dots, u_{i_m} = v_{i_1}, \dots, v_{i_m}$. Ebben az esetben a fenti index- vagy dominósorozatot a D egy megoldásának nevezzük. Formális nyelvként a következőképpen definiálhatjuk a PMP-t: $PMP = \{\langle D \rangle | \ D - nek\ van\ megoldása\}$.

43. PMP-hez kapcsolódó tétel

Tétel: A Post megfelelkezési probléma nem eldönthető, de rekurzívan felsorolható.
Formálisan: $L_{PMP} \notin R$, de $L_{PMP} \in RE$

44. Egyértelmű környezetfüggetlen nyelvtan

Egy G környezetfüggetlen (Jelölés: CF; 2-es típusú) grammatika egyértelmű, ha minden $L(G)$-beli szónak pontosan egy baloldali levezetése van G-ben.
Formálisan: $L_{ECF} \coloneqq \{\langle G \rangle | \ G\ egy\ egyértelmű\ CF\ nyelvtan\}$

45. Környezetfüggetlen grammatikák egyértelműségének eldönthetősége

Tétel: A környezetfüggetlen grammatikák egyértelműsége eldönthetetlen.
Formálisan: $L_{ECF} \notin R$

Bizonyítás

Legyen $D = \left\{\left[\frac{u_1}{v_1}\right], \dots, \left[\frac{u_n}{v_n}\right]\right\}$ egy dominókészlet, továbbá legyen $G_D \coloneqq (\{S, A, B\}, \Sigma \cup \Delta, \mathrm{P}, \mathrm{S})$, ahol

- $\Delta = \{a_1, \dots, a_n\}, \Sigma \cap \Delta = \emptyset$
- $P = \{A \to u_1 A a_1, \dots, A \to u_n A a_n, A \to \varepsilon\} \cup \{B \to v_1 B a_1, \dots, B \to v_n B a_n, B \to \varepsilon\}$

Belátható, hogy az $f: \langle D \rangle \longrightarrow \langle G_D \rangle$ konstrukció az L_{PMP} visszavezetése az $\overline{L_{ECF}}$ problémára, azaz $\overline{L_{ECF}} \notin R$. Következik, hogy $L_{ECF} \notin R$, mert R zárt a komplementerképzésre.

46. Környezetfüggetlen nyelvtanokhoz kapcsolódó eldönthetetlen problémák

Tétel: Legyen G_1 és G_2 két környezetfüggetlen grammatika. Ekkor az alábbi problémák mindegyike eldönthetetlen:

1. $L(G_1) \cap L(G_2) = \emptyset$?
2. $L(G_1) = L(G_2)$?
3. $L(G_1) = \Gamma^*$, valamely Γ ábécére?
4. $L(G_1) \subseteq L(G_2)$?

Bizonyítás

Legyen D egy dominókészlet, G_A, G_B a G_D két rész-nyelvtana rendre az A-t és B-t tekintve kezdőszimbólumnak.

1. Legyen $G_1 = G_A$ és $G_2 = G_B$. Ekkor D-nek pontosan akkor van megoldása, ha $L(G_A) \cap L(G_B) = \emptyset$
2. Ismert, hogy $\overline{L(G_A)}$ és $\overline{L(G_B)}$ determinisztikus CF nyelvek
   - $(\Sigma \cup \Delta)^*$ is CF nyelv (Σ és Δ rendre a D-beli dominók ábécéje és az $a_1, \dots, a_n$ halmaz)
   - Legyen G_1 az $\overline{L(G_A)} \cup \overline{L(G_B)}$ nyelvet generáló nyelvta. Ekkor $L(G_1)$-ben pontosan azok a szavak vannak, amik D-nek nem megoldásai.
   - Legyen G_2 a $(\Sigma \cup \Delta)^*$ nyelvet generáló nyelvtan.
   - Ekkor $L(G_1) = L(G_2) \Leftrightarrow D$-nek nincs megoldása
3. Egyszerűen adódik $\Gamma = (\Sigma \cup \Delta)$ választással.
4. Következik abból, hogy $(G_1) = L(G_2) \Leftrightarrow L(G_1) \subseteq L(G_2)$ és $L(G_2) \subseteq L(G_1)$

47. Polinom időkorlátos determinisztikus Turing-géppel eldönthető nyelvek

Legyen $f: \mathbb{N} \longrightarrow \mathbb{N}$ egy függvény.
Ekkor $TIME\big(f(n)\big) = \{L |$ L eldönthető $\mathcal{O}\big(f(n)\big)$ időigényű Turing-géppel $\}$

Továbbá $P = \cup_{k \geq 1} TIME\big(n^k\big)$.

48. P-beli problémák

P tartalmazza a gyakorlatban is hatékonyan megoldható problémákat.

Egy ilyen probléma például:
$ELÉRHETŐSÉG = \{\langle G, s, t\rangle |$ G irányított gráf és G-ben elérhető s-ből $t\}$ ($ELÉRHETŐSÉG \in P$)
$2SAT, HORNSAT \in P$

49. Polinom időkorlátos nemdeterminisztikus Turing-géppel eldönthető nyelvek

Legyen $f: \mathbb{N} \longrightarrow \mathbb{N}$ egy függvény. Ekkor
$NTIME\big(f(n)\big) = \{L |$ L eldönthető $\mathcal{O}\big(f(n)\big)$ időigényű nemdeterminisztikus Turing-géppel $\}$

Továbbá $NP = \cup_{k \geq 1} NTIME\big(n^k\big) = \{L \mid L$ polinom időben ellenőrizhető $\}$

50. P és NP kapcsolata

P ⊆ NP. (Sejtés $P \subset NP$)

51. NP-beli problémák jellemzője

Minden L NP-beli problémára a következő jellemző:
Létezik egy nemdeterminisztikus Turing-gép, ami L egy lehetséges megoldását polinom időben generálja egy munkaszalagján és polinom időben leellenörzi (determinisztikusan), hogy a lehetséges megoldás valóban megoldás-e.

52. Egy nyelv polinom időben verifikálható

Egy L nyelv polinom időben ellenőrizhető, ha van olyan $L_V \in P$ nyelv és $k \geq 1$ szám, hogy
$L = \left\{u \middle| \exists v: (u, v) \in L_V \text{ és } l(v) = O\left(l(u)^k\right)\right\}$.

53. NP-beliség és polinom időben verifikálhatóság kapcsolata

Egy nyelv akkor és csak akkor NP-beli, ha polinom időben verifikálható.

54. Egy nyelv polinom időben visszavezethető egy másik nyelvre

Egy $L_1 \subseteq \Sigma^*$ nyelv polinomidőben visszavezethető egy $L_2 \subseteq \Delta^*$nyelvre $\left(L_1 \leq_p L_2\right)$, ha $L_1 \leq L_2$ és a visszavezetéshez használt függvény polinom időben kiszámítható.

55. Zártság visszavezetésekre nézve

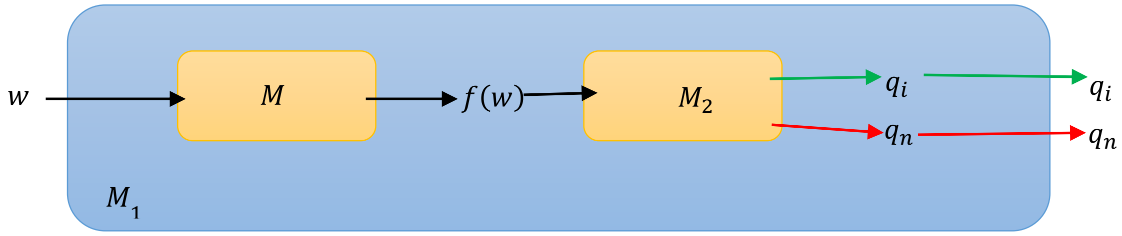
Legyen C problémák, v pedig kiszámítható függvények egy osztálya. Azt mondjuk, hogy C zárt a v-beli visszavezetésekre nézve, ha a következő teljesül. Tetszőleges L_1, L_2 problémák esetén, ha $L_1 \leq_v L_2$ és $L_2 \in C$, akkor $L_1 \in C$.

56. P és NP zártak a polinom idejű visszavezetésekre nézve

Tétel: P és NP zártak a polinom idejű visszavezetésekre nézve.
Formálisan: Ha $L_1 \leq_p L_2$ és $L_2 \in P$ $(L_2 \in NP)$, akkor $L_1 \in P$ $(L_1 \in NP)$

Bizonyítás

Csak az első állítást bizonyítjuk, a másik hasonlóan bizonyítható.
Legyen $L_2 \in P$ és tegyük fel, hogy $L_1 \leq_p L_2$. Legyen M_2 az L_2-t eldöntő, M pedig a visszavezetést kiszámoló Turing-gép. Feltehetjük, hogy M és M_2 polinom idejűek. Konstruáljuk meg M_1-et:



Világos, hogy M_1 az L_1-et dönti el. Polinom idejű lesz, mert ha M és M_2 időigénye rendre $p_1(n)$ és $p_2(n)$ polinomok, akkor M_1 időigénye $p_2(p_1(n))$, ami szintén polinom. (Megjegyzés: ha w n hosszú, akkor $f(w)$ legfeljebb $p_1(n)$ hosszú lehet.)

Megjegyzés: Ha $L_1 \leq_p L_2$ és $L_2 \in NP$, akkor L_1 nem lehet „nehezebben megoldható”, mint L_2.

57. Nehézség és teljesség problémára

Legyen $\mathbb{C}$ egy probléma osztály. Egy L probléma $\mathbb{C}$-nehéz (a polinom idejű visszavezetésre nézve), ha $\forall L' \in \mathbb{C}$ esetén $L' \leq_p L$. Egy $\mathbb{C}$-nehéz probléma $\mathbb{C}$-teljes, ha $L \in \mathbb{C}$.

58. NP-teljes probléma

Legyen L egy probléma. Azt mondjuk, hogy L NP-teljes, ha

1. NP-beli és
2. minden további NP-beli probléma polinom időben visszavezethető L-re.

Ha csak a második pont teljesül, akkor azt mondjuk, hogy L NP-nehéz.

59. NP-teljes problémához köthető tétel

Tétel: Legyen L egy NP-teljes probléma. Ha $L \in P$, akkor $P = NP$.

Bizonyítás

Tegyük fel, hogy L egy P-beli NP-teljes probléma. Legyen $L' \in NP$ egy tetszőleges nyelv. Mivel L NP-teljes, $L' \leq_p L$. Ekkor viszont, mivel P zárt a polinom idejű visszavezetésekre nézve, $L' \in P$ is teljesül. Azt kapjuk tehát, hogy $NP \subseteq$ P. Mivel P $\subseteq$ NP triviálisan teljesül, így $P = NP$.

60. Cook tétele

Tétel: A SAT ($SAT \coloneqq \{\langle\varphi\rangle |\ \varphi$ kielégíthető zérusrendű $KNF\}$) NP-teljes

Bizonyítás (Jegyzet: 68. oldal, dia: 4. EA/7)

61. $kSAT$ probléma

Legyen $k \geq 1$. Ekkor $kSAT$ a következő probléma:

$kSAT = \{\langle\varphi\rangle |\ \langle\varphi\rangle \in SAT, \varphi$ minden tagjában pontosan k literál van $\}$

62. $3SAT$-hoz kapcsolódó tétel

Tétel: A $3SAT$ NP-teljes.

Bizonyítás (Jegyzet: 72. oldal, dia: 4. EA/12)

63. $kSZINEZÉS$ ($k \geq 1$)

Adott $G = (V, E)$ irányítatlan gráf. Ki lehet-e szinezni G csúcsait k különböző színnel, úgy hogy a szomszédos csúcsok különböző színűek?

64. $3SZINEZÉS$-sel kapcsolatos tétel

Tétel: A $3SZINEZÉS$ NP-teljes.

Bizonyítás (dia: 4. EA/14)

65. Teljes részgráf probléma (TELJES RÉSZGRÁF, KLIKK)

Legyen G egy irányítatlan gráf.
$TELJES\ RÉSZGRÁF = \{\langle G, k\rangle |\ k \geq 1, G$-nek létezik k csúcsú teljes részgréfja $\}$

Tehát a $TELJES\ RÉSZGRÁF$ azon G és k párokat tartalmazza egy megfelelő ábécé feletti szavakkal kódolva, melyekre igaz, hogy G-ben van k csúcsú teljes részgráf, azaz olyan részgráf, melyben bármely két csúcs között van él.

66. $\boldsymbol{FÜGGETLEN\ CSÚCSHALMAZ}$ probléma

Legyen G egy irányítatlan gráf.
$FÜGGETLEN\ CSÚCSHALMAZ = \{\langle G, k\rangle |\ k \geq 1, G$-nek van k elemű független csúcshalmaza $\}$

Vagyis a $FÜGGETLEN\ CSÚCSHALMAZ$ azon G és k párokat tartalmazza, melyekre igaz, hogy G-ben van k olyan csúcs, melyek közül egyik sincs összekötve a másikkal.

67. $\boldsymbol{CSÚCSLEFEDÉS}$ probléma

Legyen G egy irányítatlan gráf.
$CSÚCSLEFEDÉS = \{\langle G, k\rangle |\ k \geq 1, G$-nek van olyan k elemű csúcshalmaza, mely tartalmazza G minden élének legalább egyik végpontját $\}$

68. TELJES RÉSZGRÁF-hoz kapcsolódó tétel

Tétel: A $TELJES\ RÉSZGRÁF$ NP-teljes.

Bizonyítás (Jegyzet 73. oldal, dia: 4. EA/22)

69. $\boldsymbol{FÜGGETLEN\ CSÚCSHALMAZ}$-hoz kapcsolódó tétel

Tétel: A $FÜGGETLEN\ CSÚCSHALMAZ$ NP-teljes.

Bizonyítás (Jegyzet 74. oldal, dia: 4. EA/20)

70. $\boldsymbol{CSÚCSLEFEDÉS}$-hez kapcsolódó tétel

Tétel: A $CSÚCSLEFEDÉS$ NP-teljes.

Bizonyítás (Jegyzet 74. oldal, dia: 4. EA/23)

71. $\boldsymbol{HITTING\ SET}$ ($\boldsymbol{HS}$) probléma

Adott halmazok egy $T = \{s_1, \dots, s_n\}$ halmaza és egy K szám.
Kérdés: Van-e olyan K elemű H halmaz (a hitting set), ami tartalmaz minden T-beli halmazból legalább egy elemet?

72. $HITTING\ SET\ (HS)$ problémához kapcsolódó tétel

Tétel: A $HITTING\ SET\ NP$-teljes.

Bizonyítás

- Polinom időben verifikálható.
- Megmutatjuk, hogy $CSÚCSLEFEDÉS \leq_p HITTING\ SET$:
  Legyen $G = (V, E)$ és $K \leq |V|$. Konstruáljuk meg T-t úgy, hogy minden $\{u, v\} \in E$ élre vegyük fel T-be az
  $\{u, v\}$ halmazt. Belátható, hogy G-ben pontosan akkor van K elemű csúcslefedés, ha T-ben van Kelemű hitting set.

Megjegyzés: A $HITTING\ SET$ igazából a $CSÚCSLEFEDÉS$ egy alternatív megfogalmazása.

73. $HALMAZ\ FEDÉS\ (HF)$ probléma

Adott U részhalmazainak egy $s_1, \dots, s_n$ sorozata és egy K szám.
Kérdés: Van-e ezen halmazok közül K darab olyan melyek uniója U?

74. $HALMAZ\ FEDÉS\ (HF)$ problémához kapcsolódó tétel

Tétel: A $HALMAZ\ FEDÉS\ NP$-teljes.

Bizonyítás

1. Polinom időben verifikálható
2. Megmutatjuk, hogy $CSÚCSLEFEDÉS \leq_p HALMAZ\ FEDÉS$:
   Legyen $G = (V, E)$ és $K \leq |V|$. Konstruáljuk meg a $HALMAZ\ FEDÉS$ bemenetét úgy, hogy $U = E$ és minden $u \in V$ csúcsra, legyen s_u az u-ból induló E-beli élek halmaza. Belátható, hogy G -ben pontosan akkor van K elemű csúcslefedés, ha vannak olyan $u_1, \dots, u_K$ V-beli csúcsok, hogy
   $s_{u_1} \cup \dots \cup s_{u_K} = U$

75. $HAMILTON$- $ÚT\ (HÚ)$ probléma

$HAMILTON\text{-}ÚT = \{\langle G, s, t\rangle |\ G = (V, E)$ irányított gráf, $s, t \in V$, és $\exists s$-ből t-be Hamilton-út $\}$

76. $IRÁNYÍTATLAN\ HAMILTON\text{-}ÚT\ (IHÚ)$ probléma

$IRÁNYÍTATLAN\ HAMILTON\text{-}ÚT = \{\langle G, s, t\rangle |\ G = (V, E)$ irányítatlan gráf, $s, t \in V$, és $\exists s$-ből t-be Hamilton-út $\}$

77. $\boldsymbol{IR\acute{A}NY\acute{I}TATLAN\ HAMILTON}$-$\boldsymbol{K\ddot{O}R}$ ($\boldsymbol{IHK}$) probléma

$IRÁNYÍTATLAN\ HAMILTON$-$KÖR = \{\langle G\rangle |\ G$ olyan irányítatlan gráf, amiben van Hamilton-kör $\}$

78. $\boldsymbol{UTAZ\acute{O}\ddot{U}GYN\ddot{O}K}$ probléma

$UTAZÓÜGYNÖK = \{\langle G, k\rangle |\ G$ irányítatlan gráf az éleken egy-egy pozitív egész súllyal, és G-ben van legfeljebb k összsúlyú Hamilton-kör $\}$.

79. $\boldsymbol{HAMILTON}$- $\boldsymbol{\acute{U}T}$ ($\boldsymbol{H\acute{U}}$)-hoz kapcsolódó tétel

Tétel: $HAMILTON$- $ÚT$ probléma NP -teljes.

Bizonyítás (Jegyzet 76. oldal, dia: 5. EA/7)

80. $\boldsymbol{IR\acute{A}NY\acute{I}TATLAN\ HAMILTON}$-$\boldsymbol{\acute{U}T}$-hoz kapcsolódó tétel

Tétel: Az $IRÁNYÍTATLAN\ HAMILTON$-$ÚT$ probléma NP -teljes.

Bizonyítás (Jegyzet 79. oldal, dia: 5. EA/13)

81. $\boldsymbol{IR\acute{A}NY\acute{I}TATLAN\ HAMILTON}$-$\boldsymbol{K\ddot{O}R}$-höz kapcsolódó tétel

Tétel: Az $IRÁNYÍTATLAN\ HAMILTON$-$KÖR$ probléma NP -teljes.

Bizonyítás (Jegyzet 81. oldal, dia: 5. EA/15)

82. $\boldsymbol{UTAZ\acute{O}\ddot{U}GYN\ddot{O}K}$-höz kapcsolódó tétel

Tétel: Az $UTAZÓÜGYNÖK$ probléma NP -teljes.

Bizonyítás

- Polinom időben verifikálható
- Észrevesszük, hogy az $UTAZÓÜGYNÖK$ probléma bemenetét megszorítva úgy, hogy G minden élén 1 súly szerepel, továbbá $K = |V|$ visszakapjuk a $HAMILTON\ KÖR$ problémát.

83. NP-köztes nyelvek

Ha $P \neq NP$, akkor van olyan $L \in NP$ nyelv, hogy $L \notin P$, de L nem is NP-teljes. Ezeket a nyelveket NP-köztes nyelveknek nevezzük.

Egy lehetséges NP-köztes probléma a $GRÁF\ IZOMORFIZMUS = \{\langle G_1, G_2 \rangle |\ G_1$ és G_2 izomorf irányítatlan gráfok $\}$

84. Bonyolultsági osztálybeli problémák komplementer osztálya

Ha $\mathbb{C}$ problémák egy osztálya, akkor $co\mathbb{C} \coloneqq \{\overline{L} |\ L \in \mathbb{C}\}$

85. Egy nyelv és komplementerének a kapcsolata (Teljesség)

Tétel: Legyen $\mathbb{C}$ eldöntési problémák, v pedig kiszámítható függvények egy osztálya. Egy L nyelv akkor és csak akkor $\mathbb{C}$-teljes a v-beli visszavezetésekre nézve, ha $\overline{L}$ $co\mathbb{C}$-teljes a v-beli visszavezetésekre nézve.

Bizonyítás

Mivel $co(co\mathbb{C}) = \mathbb{C}$ elég az egyik irányt bizonyítani. Legyen tehát L egy $\mathbb{C}$-teljes nyelv. Ekkor minden $L' \in \mathbb{C}$-re $L' \leq_v L$. De ez pontosan azt jelenti, hogy minden $L' \in \mathbb{C}$-re $\overline{L'} \leq_v \overline{L}$. Azaz $\overline{L}$ $co\mathbb{C}$-teljes a v-beli visszavezetésekre nézve.

86. Egy nyelv és komplementerének a kapcsolata (Zártság)

Tétel: Legyen $\mathbb{C}$ eldöntési problémák, v pedig kiszámítható függvények egy osztálya. Ha $\mathbb{C}$ zárt a v-beli visszavezetésekre nézve, akkor $co\mathbb{C}$ is az.

Bizonyítás

Legyen L_1 és L_2 két nyelv, úgy hogy $L_1 \leq_v L_2$ és $L_2 \in co\mathbb{C}$. Ekkor nyilvánvalóan $\overline{L_1} \leq_v \overline{L_2}$ valamint $\overline{L_2} \in \mathbb{C}$ is teljesül. De akkor $\mathbb{C}$ zártsága miatt $\overline{L_1} \in \mathbb{C}$, és ebből következik, hogy $L_1 \in co\mathbb{C}$. Tehát $co\mathbb{C}$ is zárt a v-beli visszavezetésekre nézve.

Következmény: $coNP$ zárt a polinom idejű visszavezetésekre nézve. (Megjegyzés: $coNP$ tartalmazza a polinom időben cáfolható problémákat)

87. $coNP$-teljes problémák

Ismert, hogy $ÁLT\_SAT = \{\langle \varphi \rangle |\ \varphi$ kielégíthető zérusrendű formula $\}$ NP-teljes. Ebből következik, hogy a komplementere az $UNSAT = \{\langle \varphi \rangle |\ \varphi$ kielégíthetetlen zérusrendű formula $\}$ $coNP$-teljes. Továbbá a $TAUT = \{\langle \varphi \rangle |\ \varphi$ érvényes zérusrendű formula $\}$ is $coNP$-teljes.

88. Off-line Turing-gép

Off-line Turing-gépnek nevezünk egy olyan többszalagos Turing-gépet, mely a bemenetet tartalmazó szalagot csak olvashatja, a többi, úgynevezett munkaszalagra pedig írhat is. Az off-line Turing-gép tárigényébe csak a munkaszalagokon felhasznált terület számít be.

89. Tárbonyolultsággal kapcsolatos problémaosztályok

Legyen $f: \mathbb{N} \longrightarrow \mathbb{R}_+$ tetszőleges függvény. Ekkor

$SPACE\big(f(n)\big) \coloneqq \{L \mid L$ eldönthető $\mathcal{O}\big(f(n)\big)$ tárkorlátos determinisztikus Off-line Turing-géppel $\}$

$NSPACE\big(f(n)\big) \coloneqq \{L \mid L$ eldönthető $\mathcal{O}\big(f(n)\big)$ tárkorlátos nemdeterminisztikus Off-line Turing-géppel $\}$

$PSPACE = \cup_{k>0} SPACE\big(n^k\big)$ és $NPSPACE = \cup_{k>0} NSPACE\big(n^k\big)$

$L = SPACE(\log_2 n)$ és $NL = NSPACE(\log_2 n)$ (Logaritmikus tárbonyolultságok)

Megjegyzés: $NP \subseteq \mathrm{PSPACE} = \mathrm{NPSPACE}$ és $L \subseteq NL$

90. Savitch tétele

Tétel: Ha $f(n) \geq \log n$, akkor $\mathrm{NSPACE}\big(f(n)\big) \subseteq \mathrm{SPACE}\big(f^2(n)\big)$.

Bizonyítás (Jegyzet: 88. oldal, dia: 5. EA/23.)

Következmény: $PSPACE = NPSPACE$ és $NL \subseteq SPACE(log^2 n)$

91. QBF probléma

Adott egy φ prenex alakú zárt Boole formula. Igaz-e φ?

92. QBF problémával kapcsolatos tétel

Tétel: A QBF probléma $PSPACE$-teljes.

Bizonyítás (dia: 6. EA/2.)

93. FÖLDRAJZI JÁTÉK (FJ) probléma

A $FÖLDRAJZI\ JÁTÉK$ a következő kétszemélyes játék. Adott egy G irányított gráf és annak egy p csúcsa. A két játékos p-ből kiindulva felváltva jelöli meg a G még meg nem jelölt csúcsait, mindig az utoljára megjelölt csúcsokból elérhető csúcsok közül választva. Az veszít, aki nem tud további csúcsot megjelölni.

94. FÖLDRAJZI JÁTÉK problémával kapcsolatos tétel

Tétel: A $FÖLDRAJZI\ JÁTÉK\ PSPACE$-teljes.

Bizonyítás (Jegyzet: 94. oldal, dia: 6. EA/8)

95. ELÉRHETŐSÉG probléma

Az $ELÉRHETŐSÉG$ probléma annak az eldöntése, hogy egy irányított gráfban van-e adott két csúcs között út.
$ELÉRHETŐSÉG = \{\langle G, s, t\rangle |\ G$ irányított gráf és G-ben elérhető s-ből $t\}$

96. $\boldsymbol{ELÉRHETŐSÉG \in NL}$

Tétel: $ELÉRHETŐSÉG \in NL$

Bizonyítás (dia: 6. EA/11)

97. Egy nyelv logaritmikus tárral visszavezethető

Legyen v a determinisztikus (Off-line) Turing-géppel logaritmikus tárral kiszámítható függvények osztálya. A v-szerinti visszavezetéseket logaritmikus tárral való visszavezetéseknek fogjuk hívni, és ha az L_1 logaritmikus tárral visszavezethető L_2-re, akkor ezt így jelöljük: $L_1 \leq_l L_2$.

98. Egy nyelv zárt a logaritmikus tárral való visszavezetésre nézve

Tétel: L és NL zártak a logaritmikus tárral való visszavezetésre nézve.

Bizonyítás (Jegyzet: 98. oldal, dia: 6. EA/12)

99. ELÉRHETŐSÉG problémával kapcsolatos tétel

Tétel: Az $ELÉRHETŐSÉG$ probléma NL-teljes.

Bizonyítás (Jegyzet: 99. oldal, dia: 6. EA/14)

Következmény: $\boldsymbol{NL} \subseteq P$

100. $\boldsymbol{NL} \subseteq P$ következmény és bizonyítása

Tétel: $\boldsymbol{NL} \subseteq P$

Bizonyítás (Jegyzet: 100. oldal, dia: 6. EA/15)

101. Immerman-Szelepcsényi tétel

Tétel: $NL = coNL$

102. Bonyolultsági osztályok kapcsolatai (tétel)

Tétel: $L \subseteq \mathrm{NL} = \mathrm{coNL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} = \mathrm{NPSPACE} \subseteq \mathrm{EXPTIME}$
$\mathrm{EXPTIME} = \bigcup_{k>0} TIME\left(2^{n^k}\right)$

Források:

- Tejfel Máté – Logika EA dia
- Gazdag Zsolt – Számelmélet EA dia
- Gazdag Zsolt – Bevezetés a számításelméletbe jegyzet

Bonyolultsági osztályokhoz kapcsolódó problémák

Bonyolultsági osztályok/ alosztályaik	Problémák
P-beli	$ELÉRHETŐSÉG, 2SAT, HORNSAT, 2SZÍNEZÉS$(páros-e a gráf), $GRÁF\ ÖSSZEFÜGGŐSÉG$
NP-teljes	$SAT, 3SAT, 3SZINEZÉS, FÜGGETLEN\ CSÚCSHALMAZ, TELJES\ RÉSZGRÁF$ $CSÚCSLEFEDÉS, UTAZÓÜGYNÖK, HITTING\ SET, HALMAZFEDÉS,$ $HAMILTON$-$ÚT, IRÁNYÍTATLAN\ HAMILTON$-$ÚT,$ $IRÁNYÍTATLAN\ HAMILTON$-$KÖR, ÁLT\_SAT$
NP-köztes	$GRÁF\ IZOMORFIZMUS$
$coNP$-teljes	$UNSAT, TAUT$
$PSPACE$-teljes	$QBF, FÖLDRAJZI\ JÁTÉK$
NL-teljes	$ELÉRHETŐSÉG, 2SAT$

RÉGEBBI VIZSGÁK

1. Kérdés sor

L1. Adja meg az ítéletlogika leíró nyelvének ábécéjét és szintaxisát!

Az ítéletlogika leíró nyelvének ábécéje:

- Ítéletváltozók (V_v): $X, Y, X_i, \ldots$
- Unér és binér logikai műveleti jelek: $\neg,\ \wedge,\ \vee, \supset$
- Elválasztójelek: ( )

Szintaxisa (Ítéletlogikai formula):

1. (alaplépés) Minden ítéletváltozó ítéletlogikai formula. (prímformula)
2. (rekurziós lépés)
   - Ha A ítéletlogikai formula, akkor $\neg A$ is az.
   - Ha A és B ítéletlogikai formulák, akkor $(A \circ B)$ is ítéletlogikai formula, ahol a " $\circ$ " a három binér művelet bármelyike.
3. Minden ítéletlogikai formula az 1.,2., szabályok véges sokszori alkalmazásával áll elő.

L2. Mi az ítéletlogikai interpretáció (vagy igazságkiértékelés), hogy adjuk meg egy formula helyettesítési értékét egy adott interpretációban?

Annak rögzítését, hogy mely ítéletváltozó igaz és melyik hamis igazságértékű interpretációnak nevezzük.

Egy formula helyettesítési értékét egy adott interpretációban az alábbi módon adjuk meg:

1. Ha C formula ítéletváltozó, akkor $B_I(C) = I(C)$
2. Ha C formula negációs, akkor $B_I(\neg C) = \neg B_I(C)$
3. Ha C formula $(A \circ B)$ alakú, akkor $B_I(A \circ B) = B_I(A) \circ B_I(B)$

L3. Mit értünk gondolkodásforma vagy következtetésforma alatt ítéletlogika esetén és mi a helyes következtetésforma?

Gondolkodásforma vagy következtetésforma alatt egy $F = \{A_1, A_2, \ldots, A_n\}$ állításhalmazból és egy A állításból álló (F, A) pár-t értünk.

Amennyiben létezik olyan eset, hogy az F állításhalmazban szereplő mindegyik állítás igaz és minden ilyen esetben az A állítás is igaz, úgy helyes következtetésformáról beszélhetünk.

L4. Mi a literál, az elemi diszjunkció, illetve az elemi konjunkció definíciója?

Ha X ítéletváltozó, akkor az X és a $\neg X$ formulákat literálnak nevezzük. Az ítéletváltozó a literál alapja. (X és $\neg X$ azonos alapú literálok.)

Elemi konjunkció alatt különböző literálok konjunkcióját értjük (Például: $X \wedge Y \wedge \neg Z$), míg elemi diszjunkció alatt különböző literálok diszjunkcióját. (Például: $X \vee Y \vee \neg Z$)

L5. Mikor elégít ki egy interpretáció egy ítéletlogikai formulát? Mikor tautológia egy ítéletlogikai formula?

Az ítéletlogikában egy I interpretáció kielégít egy B formulát $(I \vDash_0 B)$, ha a formula helyettesítési értéke i az I interpretációban. A formulát kielégítő I interpretációt a formula modelljének is szokás nevezni.

Egy B formula **tautológia** $(\vDash_0 B)$, ha minden interpretáció kielégíti. A tautológiát ítéletlogikai törvénynek is nevezzük.

L6. Adja meg az elsőrendű logika leíró nyelve ábécéjének logikán kívüli részét egyfajtájú univerzum esetén!

Függvények, predikátumok, konstansszimbólumok.

L7. Mikor zárt egy szemantikus fa ítéletlogikában? Mi a cáfoló, illetve a levezető csúcs?

Cáfoló csúcsnak nevezzük a szemantikus fa azon csúcsát, amelyiket elérve egy klóz (amely azt megelőzően még nem volt hamis) hamissá válik.

Levezető csúcsnak nevezzük a szemantikus fa azon csúcsát, amelyiket követő mindkét csúcs cáfoló csúcs.

A szemantikus fa egy ága zárt, ha cáfoló csúcsban végződik. A szemantikus fa zárt, ha minden ága zárt.

L8. Mi egy elsőrendű formula szerkezeti fája?

Egy F formula szerkezeti fája egy olyan véges fa, melyre teljesül, hogy

- a gyökeréhez az F formula van rendelve,
- ha valamelyik csúcsához egy F' formula van rendelve, akkor az adott csúcs gyerekeihez az F' formula közvetlen részformulái vannak rendelve,
- leveleihez atomi formulák vannak rendelve.

L9. Adja meg a Prenex formula, illetve a Skolem formula definícióját!

Prenex formula: Legyen Q tetszőleges kvantor, a $Q_1x_1Q_2x_2 \dots Q_nx_nB$ formula. $Q_1x_1Q_2x_2 \dots Q_nx_n$ a prefixum, B, kvantormentes formula a formula magja, törzse.

Skolem formula: Skolem formula a $\forall x_1 \forall x_2 \dots \forall x_n A$ formula, ahol a prefixumban csak univerzális kvantorok szerepelnek. Ez eldönthető formulaosztály elsőrendben.

L10. Adja meg a rezolúciós levezetés, illetve a lineáris inputrezolúciós levezetés definícióját!

Rezolóciós levezetés: Egy S klózhalmazból való rezolúciós levezetés egy olyan véges $k_1, k_2, \dots, k_m$ $(m \geq 1)$ klózsorozat, ahol minden $j = 1,2, \dots, m$-re

1. vagy $k_j \in S$
2. vagy van olyan $1 \leq s, t < j$, hogy k_j a (k_s, k_t) klózpár rezolvense.

A levezetés célja az üres klóz levezetése (ez a megállási feltétel).

Lineáris inputrezolúciós levezetés: Egy S klózhalmazból egy olyan $k_1, l_1, k_2, l_2, \dots, k_{m-1}, l_{m-1}, k_m$ klózsorozat, ahol $k_1, l_1 \in S$ és minden $i = 2,3, \dots, m-1$ esetben $l_i \in S$, a k_i pedig a k_{i-1}, l_{i-1} rezolvense

L-K-1. Hogyan képezhető két klóz rezolvense? Mi az egységrezolúció definíciója? Mire lehet választ adni a rezolúciós kalkulus segítségével, hogyan? Mit jelent, hogy a rezolúciós kalkulus helyes és teljes? Kalkulus a rezolúciós kalkulus?

Legyenek C_1, C_2 olyan klózok, amelyek pontosan egy komplemens literálpárt tartalmaznak: $C_1 = C_1' \vee L_1$ és $C_2 = C_2' \vee L_2$ és $L_1 = \neg L_2$. Ekkor létezik a rezolvensük: a $res(C_1, C_2) = C$ klóz, ami $C = C_1' \vee C_2'$

$\{C_1, C_2\} \vDash_0 C$. A rezolvensképzés a rezolúciós kalkulus levezetési szabálya (helyes következtetésforma). (Tehát a rezolúciós kalkulus kalkulus)

A **rezolúciós kalkulus helyes**:

1. Lemma: Legyen S tetszőleges klózhalmaz és $k_1, k_2, \dots, k_n$ klózsorozat rezolúciós levezetés S-ből. Ekkor minden $k_j, j = 1,2, \dots, n$-re szemantikus következménye S-nek.
2. Tétel: Legyen S tetszőleges klózhalmaz. Ha S-ből levezethető az üres klóz, akkor S kielégíthetetlen.

A rezolúciós kalkulus teljes:

Ha az S véges klózhalmaz kielégíthetetlen, akkor S-ből levezethető az üres klóz.

Nem teljes a megoldás.

L-K-2. Mit nevezünk eldöntésproblémának? Mi a két eldöntésprobléma ítéletlogikában és elsőrendű logikában? Mi a dedukciós tétel? Mi a kapcsolata az eldöntésproblémával? Milyen eldönthető formulaosztályokat ismer ítéletlogikában? Mi ezek definíciója? Milyen eszközökkel vizsgálható az eldöntésprobléma? Alkalmazható-e a szemantikus fa az eldőntésproblémák vizsgálata során ítéletlogikában? Hogyan?

Eldöntésproblémának nevezik a logikában annak eldöntését, hogy egy (F, G) pár a szemantikus következményfogalom szerint helyes gondolkodásforma-e.

Két eldöntésprobléma az ítéletlogikában és az elsőrendű logikában:

1. F-nek akkor és csak akkor következménye G, ha az $F \cup \neg G$ vagy $F_1 \wedge F_2 \wedge \ldots \wedge F_n \wedge \neg G$ kielégíthetetlen.
2. $\{F_1, F_2, \ldots, F_n\} \vDash_0 G$ akkor és csak akkor, ha $\vDash_0 F_1 \supset \big(F_2 \supset \cdots \big(F_{n-1} \supset (F_n \supset G)\big) \ldots\big)$

Dedukciós tétel: Az $\{F_1, F_2, \ldots, F_n\} \vDash_0 G$, akkor és csak akkor, ha $\{F_1, F_2, \ldots, F_{n-1}\} \vDash_0 (F_n \supset G)$

A dedukciós tételből következik a 2. eldöntésprobléma.

Eldönthető formulaosztályok és definícióik:

A KNF elemi diszjunkciók (klózok) konjunkciója. KKNF, ha teljes elemi diszjunkciók konjunkciója.
A DNF elemi konjunkciók diszjunkciója. KDNF, ha teljes elemi konjunkciók diszjunkciója.

Az eldöntésprobléma az alábbi eszközökkel vizsgálható: előrekövetkeztetéssel, visszakövetkeztetéssel és rezolúcióval.

Szemantikus-fa:

Egy n-változós szemantikus fa egy n-szintű bináris fa, ahol a szintek a bázisbeli változóknak vannak megfeleltetve. Egy X változó szintjén a csúcsokból kiinduló élpárokhoz $X, \neg X$ cimkéket rendelünk. X jelentése X igaz, $\neg X$ jelentése X hamis az élhez tartozó interpretációkban, így egy n-szintű szemantikus fa ágain az összes (2^n) lehetséges igazságkiértékelés (I interpretáció) megjelenik.

A szemantikus fa alkalmazható az eldöntésproblémák vizsgálata során, például a rezolúció esetén tetszőleges zárt szemantikus fa esetén előállítunk egy rezolúciós cáfolatot, mely a rezolúció teljességéhez szükséges.

SZ1. Definiálja az egyszalagos, nemdeterminisztikus Turing-gép konfiguráció-átmenetét és az általa felismert nyelvet!

Egy M nemdeterminisztikus Turing-gép minden konfigurációjából néhány (esetleg nulla) különböző konfigurációba mehet át. Az M konfigurációja a determinisztikus esettel [6.] megeggyezően definiálható. A konfigurációátmenet pedig a determinisztikus eset [9.] értelemszerű kiterjesztése. Legyen például $uqav$ egy konfiguráció, ahol $a \in \Gamma$ és $u, v \in \Gamma^*$. Ekkor például $uqav \vdash urbv$, ha $(r, b, S) \in \delta(q, a)$

A Nemdeterminisztikus Turing-gép által felismert nyelv szintén hasonlóan definiálható, mint a determinisztikus esetben:

az M Turing-gép által felismert nyelv azoknak az $u \in \Sigma^*$szavaknak a halmaza, melyekre igaz, hogy $q_0u \sqcup\vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ szavakra. Jelölése: $L(M)$

SZ2. Mikor mondjuk azt, hogy *M* Turing-gép eldönti az *L* nyelvet?

Egy $L \in \Sigma^*$ nyelv Turing-felismerhető, ha $L = L(M)$ valamely M Turing-gépre. Továbbá egy $L \subseteq \Sigma^*$ nyelv eldönthető, ha létezik olyan M Turing-gép, ami felismeri L-et és minden bemeneten megállási konfigurációba jut.

SZ3. Definiáljon egy olyan nyelvet, ami nem eldönthető, de Turing-felismerhető (rekurzívan felsorolható)! Vajon ennek a nyelvnek a komplementere is felismerhető Turing-géppel? Miért?

Vegyük az $L_u = \{\langle M, w\rangle | \; w \in L(M)\}$ univerzális nyelvet. Az univerzális nyelv Turing-felismerhető, de nem eldönthető. A komplementere nem ismerhető fel Turing-géppel, mivel a rekurzívan felsorolható nyelvek nem zártak a komplementerképzésre.

SZ4. Adja meg a visszavezetés definícióját! Mit jelent az, hogy egy visszavezetés logaritmikus tárral kiszámítható?

Legyen $L_1 \subseteq \Sigma^*$ és $L_2 \subseteq \Delta^*$ két nyelv (azaz eldöntési probléma). Azt mondjuk, hogy L_1 visszavezethető L_2-re (jele: $L_1 \leq L_2$), ha van olyan $f: \Sigma^* \longrightarrow \Delta^*$ kiszámítható függvény, hogy minden $w \in \Sigma^*$ szóra, $w \in L_1$ akkor és csak akkor, ha $f(w) \in L_2$.

Legyen v a determinisztikus (Off-line) Turing-géppel logaritmikus tárral kiszámítható függvények osztálya. A v-szerinti visszavezetéseket logaritmikus tárral való visszavezetéseknek fogjuk hívni, és ha az L_1 logaritmikus tárral visszavezethető L_2-re, akkor ezt így jelöljük: $L_1 \leq_l L_2$.

SZ5. Definiálja az $L_{átló}$ nyelvet. Mit lehet elmondani az L nyelv eldönthetőségéről, ha tudjuk, hogy visszavezethető rá $L_{átló}$? Miért?

Azt a nyelvet, mely azon $\{0,1\}$-feletti Turing-gépek bináris kódjait tartalmazza, melyek nem fogadják el önmaguk kódját mint bemenő szót diagonális nyelvnek nevezzük és $L_{átló}$-val jelöljük.
$L_{átló} = \{\langle M\rangle | \langle M\rangle \notin L(M)\} = \{w_i | \, i \geq 1, w_i \notin L(M_i)\}$

Tétel: Legyen $L_1 \subseteq \Sigma^*$ és $L_2 \subseteq \Delta^*$ két eldöntés probléma és tegyük fel, hogy $L_1 \leq L_2$. Ekkor igazak az alábbi állítások:

1. Ha $L_1 \notin R$, akkor $L_2 \notin R$.
2. Ha $L_1 \notin RE$, akkor $L_2 \notin RE$

A fentebbi tétel alapján elmondható, hogy az L nyelv nem eldönthető, mivel $L_{átló}$ sem.

SZ6. Mit jelent az, hogy a P és az NP osztályok zártak a polinom idejű visszavezetésre nézve?

Ha $L_1 \leq_p L_2$ és $L_2 \in P$ $(L_2 \in NP)$, akkor $L_1 \in P$ $(L_1 \in NP)$

SZ7. Vázolja a P és az NP osztályok valamint az NP-teljes problémák osztályának lehetséges viszonyait! Adjon példát úgynevezett NP-köztes problémára!

P ⊆ NP. (Sejtés $P \subset NP$)

Legyen L egy probléma. Azt mondjuk, hogy L NP-teljes, ha

1. NP-beli és
2. minden további NP-beli probléma polinom időben visszavezethető L-re.

Legyen L egy NP-teljes probléma. Ha $L \in P$, akkor $P = NP$.

Egy példa NP-köztes problémára a $GRÁF\ IZOMORFIZMUS$.

SZ8. Definiáljon egy tetszőleges NP-teljes problémát! Mi a sejtés arra vonatkozóan, hogy ez a probléma benne van-e P-ben? A választ röviden indokolja is!

A $SAT \coloneqq \{\langle\varphi\rangle | \, \varphi$ kielégíthető zérusrendű $KNF\}$ probléma például egy NP-teljes probléma. A sejtés általánosságban az, hogy $P \subset NP$, továbbá tudjuk, ha L_1 NP-teljes és L_2 NP-beli probléma, akkor $L_1 \leq_p L_2$ esetén L_2 is NP-teljes lesz.. (?)

SZ9. Mondja ki Savitch tételét és adja meg annak egy általunk tanult fontos következményét!

Tétel: Ha $f(n) \geq \log n$, akkor $\mathrm{NPSPACE}(f(n)) \subseteq \mathrm{SPACE}(f^2(n))$.

Következmény: $PSPACE = NPSPACE$ és $NL \subseteq SPACE(log^2 n)$

SZ10. Definiálja a FÖLDRAJZI JÁTÉK problémát. Melyik bonyolultsági osztályban teljes ez a probléma?

A $FÖLDRAJZI\ JÁTÉK$ a következő kétszemélyes játék. Adott egy G irányított gráf és annak egy p csúcsa. A két játékos p-ből kiindulva felváltva jelöli meg a G még meg nem jelölt csúcsait, mindig az utoljára megjelölt csúcsokból elérhető csúcsok közül választva. Az veszít, aki nem tud további csúcsot megjelölni.

A $FÖLDRAJZI\ JÁTÉK$ $PSPACE$-teljes.

SZ-K-1. Definiálja az $L_{átló}$ problémát és mutassa meg, hogy ez a probléma nem ismerhető fel Turing-géppel!

Azt a nyelvet, mely azon $\{0,1\}$-feletti Turing-gépek bináris kódjait tartalmazza, melyek nem fogadják el önmaguk kódját mint bemenő szót diagonális nyelvnek nevezzük és $L_{átló}$-val jelöljük.
$L_{átló} = \{\langle M\rangle | \langle M\rangle \notin L(M)\} = \{w_i | \, i \geq 1, w_i \notin L(M_i)\}$

Tétel: $L_{átló} \notin RE$

Bizonyítás

Tekintsük azt a T táblázatot, melynek oszlopai rendre a $w_1, w_2, \ldots$ szavakkal, a sori pedig az $M_1, M_2, \ldots$ Turing-gépekkel vannak cimkézve (tehát T egy végtelen kétdimenziós mátrix). A T elemei 0 és 1 lehetnek az alábbiak szerint. Minden $i, j \geq 1$-re $T(i,j)$ értéke pontosan akkor 1, ha $w_j \in L(M_i)$.

T	w_1	w_2	w_3	w_4	...
M_1	0	0	0	0	...
M_2	0	1	0	0	...
M_3	1	0	1	0	...
M_4	0	0	1	1	...
...	...	...	...	...	...

Ebben a táblázatban például a második sor második eleme 1, ami azt jelenti, hogy M_2 elfogadja a w_2 szót (ez persze a valóságban nem igaz, hisz w_2 nem kódol legális Turing-gépet, így M_2 nem is ismerhet fel semmilyen szót, de az összefüggések szemléltetéséhez feltesszük, hogy a táblázat helyes).

Minden $i \geq 1$-re a táblázat i-ik sora tekinthető úgy, mint az $L(M_i)$ nyelv karakterisztikus függvénye. Nevezetesen azért, mert minden $j \geq 1$ a w_j szó pontosan akkor eleme $L(M_i)$-nek, ha az i-ik sor j-ik eleme 1. Ebben az értelemben a táblázat átlójában szereplő bitsorozat komplementere pedig nem más, mint az $L_{átló}$ karakterisztikus függvénye. Ezért nyilvánvaló, hogy minden $i \geq 1$-re az $L_{átló}$ karakterisztikus függvénye különbözik $L(M_i)$ karakterisztikus függvényétől. Mivel minden M Turing-géphez van olyan $i \geq 1$ szám, hogy $L(M) = L(M_i)$, kapjuk, hogy az $L_{átló}$ nem lehet egyenlő az $L(M)$-mel semmilyen M Turing-gépre. Adódik tehát, hogy $L_{átló} \notin RE$.

SZ-K-2. Definiálja a 3SAT problámát és bizonyítsa be az NP-teljességét!

$3SAT \coloneqq \{\langle\varphi\rangle | \langle\varphi\rangle \in SAT$ és φ minden tagjában pontosan 3 literál van $\}$

Tétel: $3SAT$ NP-teljes.

Bizonyítás: (Jegyzet: 72. oldal, dia: 4. EA/12)

2. Kérdés sor

L1. Adja meg a függvény definícióját! Mi a reláció és mi a művelet?

Legyenek D és R (nemfeltétlenül különböző) halmazok. Függvénynek nevezünk egy $D \longrightarrow R$ leképezést. D a leképezés értelmezési tartománya, R az értékkészlete.

Legyen U egy tetszőleges (individuum)halmaz. Ha $R = \{i, h\}$, akkor a függvény logikai függvény, más néven reláció. Ha $D = R^n$, akkor a függvény matematikai függvény, más néven művelet.

L2. Mi a logikai műveletek hatásköre, melyik egy ítéletlogikai formula fő logikai összekötőjele?

Logikai műveletek hatásköre a formula részformulái közül az a legkisebb logikai összetettségű, amelyben az adott logikai összekötőjel előfordul.

Egy formula **fő logikai összekötőjele** az az összekötőjel, amelynek a hatásköre maga a formula.

L3. Adja meg az igazságtábla definícióját!

Egy n- változós formula igazságtáblája egy olyan $n + 1$ oszlopból és $2^n + 1$ sorból álló táblázat, ahol a fejlécben a bázis (a formula változói rögzített sorrendben) és a formula szerepel. A sorokban a változók alatt az interpretációk (a változók igazságkiértékelései), a formula alatt a formula helyettesítési értékei találhatók.

L4. Adja meg a szemantikus következményfogalom definícióját ítéletlogika esetén!

Egy G formula szemantikus vagy tautologikus következménye az $F = \{F_1, F_2, \dots, F_n\}$ formulahalmaznak, ha minden olyan I interpretációra, amelyre $I \vDash_0 \{F_1, F_2, \dots, F_n\}$ fennáll, $I \vDash_0 G$ is fennáll.
Jelölés: $\{F_1, F_2, \dots, F_n\} \vDash_0 G$

L5. Mi a legszűkebb következmény, az előre- és a visszakövetkeztetés definíciója ítéletlogika esetén?

Legyen az F feltételhalmazban szereplő változók száma n. Ekkor a **legszűkebb következmény** az az $\{i,h\}^n \longrightarrow \{i,h\}$ leképezés, amely pontosan azokhoz az interpretációkhoz rendel i értéket, amelyek kielégítik az F-et.

Előrekövetkeztetés: Ismert az F feltételhalmaz, és keressük F lehetséges következményeit. Megkeressük F legszűkebb következményét, R-t. Következmény minden olyan G formula, amelyre $R \supset G$ tautológia, azaz R igazhalmaza része G igazhalmazának.

Visszakövetkeztetés: Az F feltételhalmaz és a B következményformula ismeretében eldöntjük, hogy B valóban következménye-e F-nek. Mivel $F \vDash_0 B$ pontosan akkor, ha az $F \cup \{\neg B\}$ formulahalmaz kielégíthetetlen.

Más szóval B pontosan akkor következménye F-nek, ha minden olyan interpretációban, ahol B hamis, az F kielégíthetetlen.

L6. Adja meg az elsőrendű logika leíró nyelve ábécéjének logikai részét!

Indiviidum-változók, Elválasztó jelek: $(,)$,Unér és binér logikai műveleti jelek: $\neg, \wedge, \vee, \supset, \leftrightarrow$, Kvantorok: $\forall, \exists$; (ítélet változók)

L7. Mi egy term szerkezeti fája?

Egy t term szerkezeti fája egy olyan véges fa, melyre teljesül, hogy

- a gyökeréhez a t term van rendelve,
- ha valamelyik csúcsához egy t' term van rendelve, akkor az adott csúcs gyerekeihez a t' term közvetlen résztermjei vannak rendelve,
- leveleihez individuumváltozók vagy konstansok vannak rendelve.

L8. Adja meg az elsőrendű formulák szemantikáját!

1. . $|P(t_1,t_2,\dots,t_n)|^{I,\kappa} = i$, ha $(|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_n|^{I,\kappa}) \in P^I$, ahol P^I jelöli a P^I reláció igazhalmazát.
2. $|\neg A|^{I,\kappa} = \neg |A|^{I,\kappa}$
   $|A \wedge B|^{I,\kappa} = |A|^{I,\kappa} \wedge |B|^{I,\kappa}$
   $|A \vee B|^{I,\kappa} = |A|^{I,\kappa} \vee |B|^{I,\kappa}$
   $|A \supset B|^{I,\kappa} = |A|^{I,\kappa} \supset |B|^{I,\kappa}$
3. $|\forall x A|^{I,\kappa} = i$, ha $|A|^{I,\kappa^*} = i$ κ minden κ^* x variánsára
   $|\exists x A|^{I,\kappa} = i$, ha $|A|^{I,\kappa^*} = i$ κ legalább egy κ^* x variánsára

L9. Mi két formula rezolvense?

Legyenek C_1, C_2 olyan klózok, amelyek pontosan egy komplemens literálpárt tartalmaznak: $C_1 = C_1' \vee L_1$ és $C_2 = C_2' \vee L_2$ és $L_1 = \neg L_2$. Ekkor létezik a rezolvensük: a $res(C_1, C_2) = C$ klóz, ami $C = C_1' \vee C_2'$

L10. Adja meg a Herbrand univerzum definícióját!

Az elsőrendű klózhalmaz leíró nyelvének alaptermjeiből álló halmazt Herbrand univerzumnak nevezzük.

L-K-1. Mi az ítéletlogika leíró nyelvének ábécéje, szintaxisa és szemantikája? Milyen módszereket ismer az ítéletlogikai formulák jelentésének megadására? Mi az igazságkiértékelés.? Mi a kapcsolat az ítéletlogika leíró nyelvének szemantikája és a formulák hamishalmaza között?

Az **ítéletlogika leírónyelvének ábécéje**:

- Ítéletváltozók (V_v): $X, Y, X_i, \ldots$
- Unér és binér logikai műveleti jelek: $\neg, \ \wedge, \ \vee, \supset$
- Elválasztójelek: ( )

Szintaxisa (Formulák):

1. (alaplépés) Minden ítéletváltozó ítéletlogikai formula. (prímformula)
2. (rekurziós lépés)
    - Ha A ítéletlogikai formula, akkor $\neg A$ is az.
    - Ha A és B ítéletlogikai formulák, akkor $(A \circ B)$ is ítéletlogikai formula, ahol a „ $\circ$ ” a három binér művelet bármelyike.
3. Minden ítéletlogikai formula az 1.,2., szabályok véges sokszori alkalmazásával áll elő.

Ítéletlogikai formulák jelentésének megadására: Igazságtábla, szemantikus fa

Interpretáció: Annak rögzítését, hogy mely ítéletváltozó igaz és melyik hamis igazságértékű interpretációnak nevezzük.)

Igazsághalmaz:

1. Egy formula igazhalmaza azon I interpretációk halmaza, amelyekre a formula helyettesítési értéke igaz.
2. **Egy formula hamishalmaza azon *I* interpretációk halmaza, amelyekre a formula helyettesítési értéke hamis.**

Nem teljes!

L-K-2. Mi a Prenex formula a Skolem formula, illetve az elsőrendű klóz definíciója? Hogyan lehet előállítani egy formulát elsőrendű klózok konjunkciójaként? Mi az alaprezolúció? Miért érdemes a Herbrand univerzumot használni az alaprezolúcióhoz?

Prenex formula: Legyen Q tetszőleges kvantor, a $Q_1x_1Q_2x_2 \ldots Q_nx_nB$ formula. $Q_1x_1Q_2x_2 \ldots Q_nx_n$ a prefixum, B, kvantormentes formula a formula magja, törzse.

Skolem formula: Skolem formula a $\forall x_1 \forall x_2 \ldots \forall x_n A$ formula, ahol a prefixumban csak univerzális kvantorok szerepelnek. Ez eldönthető formulaosztály elsőrendben.

Elsőrendű klóz: Olyan zárt Skolem formula, aminek a magja az elsőrendű nyelv literáljainak (azaz atomi formuláinak vagy annak negáltjainak) diszjunkciója. Például: $\forall x \forall y \left(P(x) \vee \neg Q(x, f(y))\right)$.

Alaprezolúció: A feladat tetszőleges elsőrendű formula átírása elsőrendű klózok konjunkciós formulájává. Az eldöntésprobléma elsőrendű klózhalmaz kielégíthetetlenségének eldöntése.

Azért érdemes Herbrand univerzumot használni, mert egy elsőrendű klózhalmaz akkor és csak akkor kielégíthetetlen, ha a Herbrand-univerzuma feletti egyetlen Herbrand-interpretáció sem elégíti ki.

SZ1. Hogyan lehet egy eldöntési problémát formális nyelvként megadni? Adja meg a konjunktív normálformában adott ítéletkalkulusbeli formulák kielégíthetőségének problémáját

Egy P kiszámítási probléma reprezentálható egy $f_P : A \longrightarrow B$ függvénnyel. Egy speciális kiszámítási probléma az eldöntés probléma, ahol az f_P értékkészlete egy két elemű halmaz: $\{igen, nem\}, \{1,0\}$. A megoldható eldöntési problémákat eldönthető problémáknak nevezzük

$SAT \coloneqq \{\langle\varphi\rangle \mid \varphi$ kielégíthető zérusrendű $KNF\}$

SZ2. Mikor mondjuk azt, hogy M Turing-gép felismeri az L nyelvet? Mikor mondjuk, hogy M eldönti L-t (+ $L(M)$)

Egy $L \in \Sigma^*$ nyelv Turing-felismerhető, ha $L = L(M)$ valamely M Turing-gépre. Továbbá egy $L \subseteq \Sigma^*$ nyelv eldönthető, ha létezik olyan M Turing-gép, ami felismeri L-et és minden bemeneten megállási konfigurációba jut.

Az M Turing-gép által felismert nyelv azoknak az $u \in \Sigma^*$szavaknak a halmaza, melyekre igaz, hogy $q_0u \sqcup \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ szavakra. Jelölése: $L(M)$

SZ3. Definiálja az L_u nyelvet! Mit tanultunk a bonyolultságáról?

$L_u = \{\langle M, w\rangle | \; w \in L(M)\}$ univerzális nyelv. Az univerzális nyelv Turing-felismerhető, de nem eldönthető.

SZ4. Adja meg a visszavezetés definícióját! Mit mondhatunk el egy L nyelv eldönthetőségéről, ha tudjuk, hogy visszavezethető rá az L_u

Legyen $L_1 \subseteq \Sigma^*$ és $L_2 \subseteq \Delta^*$ két nyelv (azaz eldöntési probléma). Azt mondjuk, hogy L_1 visszavezethető L_2-re (jele: $L_1 \leq L_2$), ha van olyan $f: \Sigma^* \longrightarrow \Delta^*$ kiszámítható függvény, hogy minden $w \in \Sigma^*$ szóra, $w \in L_1$ akkor és csak akkor, ha $f(w) \in L_2$.

Azt mondhatjuk, hogy rekurzívan felsorolható (Turing-felismerhető).

SZ5. Definiáljon egy tetszőleges nyelvet, amit nem lehet felismerni Turing-géppel! Vajon a megadott nyelv komplementere eldönthető? Miért?

Azt a nyelvet, mely azon $\{0,1\}$-feletti Turing-gépek bináris kódjait tartalmazza, melyek nem fogadják el önmaguk kódját mint bemenő szót diagonális nyelvnek nevezzük és $L_{átló}$-val jelöljük.
$L_{átló} = \{\langle M\rangle | \langle M\rangle \notin L(M)\} = \{w_i | \; i \geq 1, w_i \notin L(M_i) \}$

A megadott nyelv komplementere nem eldönthető, mert az eldönthetőség zárt a komplementerképzésre nézve és $L_{átló}$ nem eldönthető.

SZ6. Definiálja az NP-teljességet! Mit mondhatnánk el a P és az NP osztályok viszonyáról, ha kiderülne, hogy a *SAT* probléma *P*-ben van.

Legyen L egy probléma. Azt mondjuk, hogy L NP-teljes, ha

1. NP-beli és
2. minden további NP-beli probléma polinom időben visszavezethető L-re.

Ha kiderülne, hogy a SAT probléma P-ben van, akkor: $P = NP$.

SZ7. Vázolja a P és az NP osztályok valamint az NP-teljes problémák osztályának lehetséges viszonyait! Adjon példát úgynevezett NP-köztes problémára!

P ⊆ NP. (Sejtés $P \subset NP$)

Legyen L egy probléma. Azt mondjuk, hogy L NP-teljes, ha

1. NP-beli és
2. minden további NP-beli probléma polinom időben visszavezethető L-re.

Legyen L egy NP-teljes probléma. Ha $L \in P$, akkor $P = NP$.

Egy példa NP-köztes problémára a $GRÁF\ IZOMORFIZMUS$.

SZ8. Definiálja a coNP osztályt és adjon meg egy coNP-teljes problémát!

$coNP \coloneqq \{\overline{L} \mid L \in NP\}$. $coNP$-teljes problémák például az $UNSAT, TAUT$

SZ9. Definiálja a PSPACE és NPSPACE osztályokat! Milyen tartalmazási viszony áll fenn a két osztály között?

Legyen $f\colon \mathbb{N} \longrightarrow \mathbb{R}_+$ tetszőleges függvény. Ekkor
$SPACE\big(f(n)\big) \coloneqq \{L \mid L$ eldönthető $\mathcal{O}\big(f(n)\big)$ tárkorlátos determinisztikus Off-line Turing-géppel $\}$
$NSPACE\big(f(n)\big) \coloneqq \{L \mid L$ eldönthető $\mathcal{O}\big(f(n)\big)$ tárkorlátos nemdeterminisztikus Off-line Turing-géppel $\}$

$PSPACE = \cup_{k>0} SPACE\big(n^k\big)$ és $NPSPACE = \cup_{k>0} NSPACE\big(n^k\big)$

Savitch tételének következménye miatt tudjuk, hogy $PSPACE = NPSPACE$.

SZ10. Definiáljon egy tanult PSPACE-teljes problémát!

QBF: Adott egy φ prenex alakú zárt Boole formula. Igaz-e φ?
(Lehetne a FÖLDRAJZI JÁTÉKOT is írni.)

SZ-K-1. Definiálja az L_h problémát és mutassa meg, hogy ez a probléma Turing-felismerhető. de nem eldönthető.

Legyen $L_h = \{\langle M, w\rangle | \; M \; megáll \; a \; w \; bemeneten\}$, azaz L_h azon $\langle M, w\rangle$ Turing-gép és bemenet párosokat tartalmazza megfelelően kódolva, melyekre teljesül, hogy az M gép megáll a w bemeneten. Nevezzük ezt a nyelvet megállási problémának.

Megjegyzés: $L_u \subseteq L_h$

Tétel: $L_h \in RE$

Bizonyítás

Kotábbi tételek alapján elég megmutatni, hogy $L_h \leq L_u$.
Tetszőleges M Turing-gépre, legyen M' az alábbi Turing-gép: M' tetszőleges u bemeneten a következőt teszi:

- Futtatja M-et u-n
- Ha M q_i-be vagy q_n-be lép, akkor $M' q_i$-be lép

Belátható, hogy az $f: \langle M\rangle \longrightarrow \langle M'\rangle$ leképezés egy kiszámítható függvény, továbbá az is, hogy tetszőleges $\langle M, w\rangle$ Turing-gép és bemenet párosra:
$\langle M, w\rangle \in L_h \Leftrightarrow$ Az M megáll w-n $\Leftrightarrow$ Az M' elfogadja w-t $\Leftrightarrow \langle M', w\rangle \in L_u$
Tehát az M' konstrukciója az L_h visszavezetése L_u-ra. Következik, hogy $L_h \in RE$

Tétel: $L_h \notin R$

Bizonyítás

Kotábbi tételek alapján elég megmutatni, hogy $L_u \leq L_h$.
Tetszőleges M Turing-gépre, legyen M' az alábbi Turing-gép: M' tetszőleges u bemeneten a következőt teszi:

- Futtatja M-et u-n
- Ha M q_i-be lép, akkor M' is q_i-be lép
- Ha M q_n-be lép, akkor M' egy végtelen ciklusba lép

Belátható, hogy az $f: \langle M\rangle \longrightarrow \langle M'\rangle$ leképezés egy kiszámítható függvény, továbbá az is, hogy tetszőleges $\langle M, w\rangle$ Turing-gép és bemenet párosra:
$\langle M, w\rangle \in L_u \Leftrightarrow M$ elfogadja w-t $\Leftrightarrow$ Az M' megáll w-n $\Leftrightarrow \langle M', w\rangle \in L_h$.
Tehát az M' konstrukciója az L_u visszavezetése L_h-ra. Következik, hogy $L_h \notin R$

SZ-K-2. Definiálja a Független csúcshalmaz és Klikk problémákat + NP teljesség biz.

Legyen G egy irányítatlan gráf.
$FÜGGETLEN\ CSÚCSHALMAZ = \{\langle G, k\rangle \mid k \geq 1, G$-nek van k elemű független csúcshalmaza $\}$

Vagyis a $FÜGGETLEN\ CSÚCSHALMAZ$ azon G és k párokat tartalmazza, melyekre igaz, hogy G-ben van k olyan csúcs, melyek közül egyik sincs összekötve a másikkal.

Tétel: A $FÜGGETLEN\ CSÚCSHALMAZ$ NP-teljes.

Bizonyítás (Jegyzet 74. oldal, dia: 4. EA/20)

Legyen G egy irányítatlan gráf.
$TELJES\ RÉSZGRÁF\ (KLIKK) = \{\langle G, k\rangle \mid k \geq 1, G$-nek létezik k csúcsú teljes részgréfja $\}$

Tehát a $TELJES\ RÉSZGRÁF$ azon G és k párokat tartalmazza egy megfelelő ábécé feletti szavakkal kódolva, melyekre igaz, hogy G-ben van k csúcsú teljes részgráf, azaz olyan részgráf, melyben bármely két csúcs között van él.

Tétel: A $TELJES\ RÉSZGRÁF$ NP-teljes.

Bizonyítás (Jegyzet 73. oldal, dia: 4. EA/22)

Csoportokban felmerülő kérdések

Kérdés: Tegyük fel, hogy M egy det. Turing gép, ami eldönti az L nyelvet. u egy tetszőleges szó. Milyen számításai lehetnek az u-n, ha u eleme L és akkor, ha u nem eleme L ?

Válasz: Mindkét esetben véges a számítás, és értelemszerűen elfogadó vagy elutasító állapotban áll meg a gép. Tehát ha u benne van L-ben akkor elfogadó, ha nem, akkor elutasító állapotban áll meg.

Kérdés: Polinom idejű visszavezetés: Ha L1<= L2 <= L2 akkor L1<= L3 is teljesül. Miért?

Válasz: A polinom idejű visszavezetés másik neve Karp-redukció. A Karp-redukcióban résztvevő "felek" pedig relációban állnak egymással, amely reláció egyik tulajdonsága, hogy tranzitív.

Kérdés: Vajon minden NP teljes probléma visszavezethető a 3SAT problémára polinom időben? Miért?

Válasz: Igen, mert 3SAT is NP-teljes.

Kérdés: Miért nem triviális tulajdonsága egy rekurzívan felsorolható nyelvnek, hogy véges-e vagy sem?

Válasz: Azért nem triviális tulajdonsága, mert annak a felismerése, hogy egy rekurzívan felsorolható nyelv mikor üres, véges, rekurzív algoritmikusan megoldhatatlan problémát jelent.

Források

Tejfel Máté – Logika dia
Gazdag Zsolt – Számításelmélet dia
Gazdag Zsolt – Bevezetés a számításelméletbe jegyzet (2015) (Aki teheti olvassa el legalább egyszer!)

Javítási javaslatok – „Több szem többet lát"

Lestár Norbert (Logika 50, 78), Bálint Ádám (Szám.elm 26.), Rózsa Dávid (Szám.elm 90.)