LOGIKA ÉS SZÁMÍTÁSELMÉLET KIDOLGOZOTT JEGYZET

Készítette:

Butkay Gábor és Gyenes József

A jegyzet a 2013-2014-es tanév 2. felében lévő Logika és számításelmélet előadások alapján született. A jegyzet nem teljes és nem hibátlan. Az esetlegesen kimaradt részekért vagy hibákért a szerkesztők felelősséget nem vállalnak.

Mindenki saját felelősségre használja!

Eötvös Loránd Tudományegyetem
Informatikai Kar

Ha hibát találsz kérlek jelezd a gabor.butkay@windowslive.com e-mail címen!

Gondolkodásforma vagy következtetésforma:

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

Helyes következtetésforma:

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

Ítéletlogika:

Tárgya az egyszerű állítások és a belőlük logikai műveletekkel kapott összetett állítások vizsgálata.

Egyszerű állítás:

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

Összetett állítás:

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

Az ítéletlogika leíró nyelvének ábécéje állhat:

- Ítéletváltozókból (V_v): X, Y, X_i, …
- Unér és binér logikai műveleti jelekből: ¬, ∧, ∨, ⊃
- Elválasztójelekből: ( )

Ítéletlogikai szintaxis

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

Közvetlen részformula:

1) Prímformulának nincs közvetlen részformulája.
2) ¬A közvetlen részformulája az A formula.
3) Az (A∘B) közvetlen részformulái az A (baloldali) és a B (jobboldali).

Literál:

Ha X ítéletváltozó, akkor az X és a ¬X formulákat literálnak nevezzük.

Formula logikai összetettsége:

Egy A formula logikai összetettsége $\ell(A)$

1) (Alaplépés): Ha A ítéletváltozó, akkor $\ell(A)=0$
2) (Rekurzív lépések):
   - $\ell(\neg A) = \ell(A)+1$
   - $\ell(A \circ B) = \ell(A)+\ell(B)+1$

Logikai műveletek hatásköre:

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

Fő logikai összekötőjel:

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

Interpretáció(?):

Annak rögzítését melyik ítéletváltozó i(gaz) és melyik h(amis) igazságértékű interpretációnak nevezzük.

I: $V_v \rightarrow \{ i, h \}$

I(x) jelöli az x ítéletváltozó értékét az I interpretációban. n db ítéletváltozó interpertációinak száma 2^n. Az ítéletváltozók egy adott sorrendjét **bázisnak** nevezzük.

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, ¬X címkéket rendelünk. X jelentése X igaz, ¬X jelentése X hamis, így egy n-szintű szemantikus fa ágain az összes (2^n) lehetséges igazságkiértékelés (interpretáció) megjelenik.

Formula helyettesítési értéke I interpretációban: $B_I(C)$

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

Formula igazságtáblája:

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

Igazhalmaz:

Egy formula igazhalmaza azon I interpretációk halmaza, amelyekre a formula helyettesítési értéke igaz.

Hamishalmaz:

Egy formula hamishalmaza azon I interpretációk halmaza, amelyekre a formula helyettesítési értéke hamis.

φ igazságértékelés függvény:

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 φB^i feltételek.

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.

Kielégíthetőség/kielégíthetetlenség/tautológia formulákra:

Egy B formula kielégíthető, ha legalább egy interpretáció kielégíti.

Egy B formula kielégíthetetlen, ha egyetlen interpretáció sem elégíti ki.

Egy B formula tautológia, ha minden interpretáció kielégíti. A tautológiát ítéletlogikai törvénynek is nevezik.

Interpretáció kielégít egy formula halmazt:

Az ítéletlogikában egy I interpretáció kielégít egy F formulahalmazt ($I \vDash_0 F$) ha a formulahalmaz minden formulájának helyettesítési értéke i az I interpretációban.

Kielégíthetőség/kielégíthetetlenség formulahalmazokra:

Egy F formulahalmaz kielégíthető, ha legalább egy interpretáció kielégíti.

Egy F formulahalmaz kielégíthetetlen, ha bármely interpretációban legalább egy formulája h (nincs olyan interpretáció, ami kielégítené).

Szemantikus következmény:

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

Tétel: Ha egy G formula bármely F feltételhalmaznak következménye, akkor G tautológia.

Tétel: 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 ($F \vDash_0 A$).

Tétel: F-nek akkor és csak akkor következménye G, ha az $F \cup \neg G$ vagy $F_1 \wedge F_2 \wedge \ldots \wedge \neg G$ kielégíthetetlen.

Dedukciós tétel:

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

Eldöntés probléma:

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

Tautologikusan ekvivalens:

Az A és B formukák tautologikusan ekvivalensek, ha $A \vDash_0 B$ és $B \vDash_0 A$.

Legszűkebb következmény:

Legyen az F feltételhalmazban szereplő változók száma n. Ekkor a legszűkebb következmény az az $\{i, h\}^n \rightarrow \{i, h\}$ 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⊃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∪{¬B} formulahalmaz kielégíthetetlen.

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

Nulladrendű állítás:

Ha a kijelentő mondat alanya valamely konkrét dolog, akkor az állítást nulladrendű állításnak hívjuk. Az ilyen állítások formális leírására egy relációt (logikai függvényt) definiálunk.

Elsőrendű állítás:

Ha a kijelentő mondat alanya egy halmaz, akkor az állítást elsőrendű állításnak hívjuk. Ilyenkor az állítás az összes elemre egyidejűleg fennálló megállapítást/általánosítást vagy a halmaz bizonyos elemeire (nem feltétlenül mindre) fennálló megállapítást/létezést fogalmaz meg. Leírásukhoz a kvantorokat (∀,∃) használjuk.

Matematikai struktúra:

A matematikai struktúra egy ⟨U,R,M,K⟩ 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,…,k) logikai függvények (alaprelációk) halmaza
- M: az U-n értelmezett n-változós (n= 1,2,…,k) matematikai függvények (alapműveletek) halmaza
- K: az U megjelölt elemeinek egy (esetleg üres) részhalmaza

A struktúra **szignatúrája** (ν_1, ν_2, ν_3 egészértékű függvényegyüttes) megadja az alaprelációk és az alapműveletek aritását, valamint K elemszámát.

Egyfajtájú struktúrákat leíró nyelvek (?):

Egyféle elemből álló U esetén az ⟨U,R,M,K⟩ struktúra leíró nyelv logikán kívüli része lehet a következő.

Az $\mathcal{L}$ nyelv ábécéje: ⟨Pr, Fn, Cnst⟩, szignatúrája: (ν_1, ν_2, ν_3).

- Pr: predikátumszimbólumok halmaza
  ν_1: P ∈ Pr-re megadja P aritását (k)
- Fn: függvényszimbólumok halmaza
  ν_2: f ∈ Fn-re megadja f aritását (k)
- Cnst: konstansszimbólumok halmaza
  ν_3: megadja a konstansok számát

Többfajtájú struktúrákat leíró nyelvek(?):

Többféle elemből álló U esetén az ⟨U,R,M,K⟩ struktúra leíró nyelv logikán kívüli része lehet a következő.

Az $\mathcal{L}$ nyelv ábécéje: ⟨Srt, Pr, Fn, Cnst⟩, szignatúrája: (ν_1, ν_2, ν_3).

- Srt: nemüres halmaz, melynek π_j elemei fajtákat szimbolizálnak
- Pr: predikátumszimbólumok halmaza
  ν_1: P ∈ Pr-re megadja P aritását (k) és, hogy milyen fajtájúak az egyes argumentumok (π_1, π_2, …, π_k)
- Fn: függvényszimbólumok halmaza
  ν_2: f ∈ Fn-re megadja f aritását (k) és, hogy milyen fajtájúak az egyes argumentumok, valamint a függvény értéke (π_1, π_2, …, π_k ; π_f)
- Cnst: konstansszimbólumok halmaza
  ν_3: megadja minden fajtához a konstansok számát

Termek (egyfajtájú eset) :

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

Formulák (egyfajtájú eset) :

1) (alaplépés) Ha $P \in Pr$ k-változós predikátumszimbólum és $t_1, t_2, \ldots, t_k$ termek, akkor $P(t_1,t_2, \ldots, t_k)$ formula (atomi formula)
2) (rekurzív lépés)
   - Ha A formula, akkor ¬A is az.
   - Ha A és B formulák, akkor (A∘B) is formula, ahol ∘ a három binér művelet bármelyike.
3) Ha A formula, akkor ∀xA és ∃xA is az.
4) Minden formula az 1, 2, 3 szabályok véges sokszori alkalmazásával áll elő.

Termek (többfajtájú eset) :

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

Formulák (többfajtájú eset) :

1) (alaplépés) Ha a $P \in Pr$ $(\pi_1, \pi_2, \ldots, \pi_k)$ fajtájú predikátumszimbólum és $t_1, t_2, \ldots, t_k$ rendre $\pi_1, \pi_2, \ldots, \pi_k$ fajtájú termek, akkor $P(t_1, t_2, \ldots, t_k)$ formula (atomi formula).
2) (rekurzív lépés)
   - Ha A formula, akkor ¬A is az.
   - Ha A és B formulák, akkor (A∘B) is formula, ahol ∘ a három binér művelet bármelyike.
3) Ha A formula, akkor ∀xA és ∃xA is az.
4) Minden formula az 1, 2, 3 szabályok véges sokszori alkalmazásával áll elő.

Közvetlen részterm:

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

Közvetlen részformula:

1) Egy atomi formulának nincs közvetlen részformulája.
2) ¬A közvetlen részformulája az A formula.
3) Az (A∘B) közvetlen részformulái az A (baloldali) és a B (jobboldali) formulák.
4) A QxA (Q ∈ {∀, ∃}) közvetlen részformulája az A formula.

Komponens formula:

Egy formulában egy logikai művelet hatáskörében lévő részformulá(ka)t komponens formuláknak nevezzük.

1) Egy atomi formulának nincs közvetlen komponense (prímformula)
2) ¬A közvetlen komponense az A formula.
3) Az (A∘B) közvetlen komponensei az A és a B formulák.
4) A QxA (Q ∈ {∀, ∃}) formulának nincs közvetlen komponense (prímformula).

Prímformulák:

1) Egy atomi formula prímformula.
2) Egy QxA formula prímformula.

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

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.

Elsőrendű formula logikai összetettsége:

Egy A formula logikai összetettsége: $\ell(A)$

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

Szabad és kötött változók elsőrendű formulákban:

Egy formulában egy x változó egy előfordulása

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

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

Formulák zártsága:

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

Alapkifejezés, alapatom, alapterm:

Alapkifejezés a változót nem tartalmazó $\mathcal{L}$ 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.
2) Egy atomi formulát az atomi formula alappéldányának nevezzük, ha argumentumai **alaptermek**.

Elsőrendű logikai nyelv interpretációja:

Egy elsőrendű logikai nyelv $\mathcal{L}[V_v]$ interpretációja egy, az $\mathcal{L}$ 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:

- $I_{Srt:}$ $\pi \mapsto U_\pi$, ahol ha Srt egyelmű, akkor az interpretáció U univerzuma egyfajtájú elemekből áll
- Az I_{Pr} : $P \mapsto P^I$, ahol P^I a struktúra R halmaza
- Az I_{Fn} : $f \mapsto f^I$, ahol f^I a struktúra M halmaza
- Az I_{Cnst} : $c \mapsto c^I$, ahol c^I a struktúra K halmaza

Változókiértékelés:

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

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 változó kiértékelés)
3) $|f(t_1, t_2, \dots, t_n)|^{I,\kappa} = f^I((|t_1|^{I,\kappa}, |t_2|^{I,\kappa}, \dots, |t_n|^{I,\kappa}))$

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 a 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

Elsőrendű formula értéktáblája:

Egy 1. rendű formula értéktáblájába az első sorba a formula szabad változói, a prímkomponensek és a formula kerülnek. Az individuumváltozók alá a lehetséges változókiértékelések, a prímformulák alá a megfelelő helyettesítési értékek kerülnek. A formula alatt a formulának a prímformulák értékei alapján kiszámított helyettesítési értékei találhatók.

Egy struktúra modellje egy 1. rendű formulának:

Az $\mathcal{L}$ egy I interpretációja adott κ változókiértékelés mellett kielégít egy 1. rendű 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.

Az I interpretáció kielégíti az F 1.rendű formulahalmazt:

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

Kielégíthető 1.rendű formula:

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

Kielégíthető 1.rendű formulahalmaz:

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

Logikailag igaz 1.rendű formula:

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: $\vDash G$.

1.rendű formula tautológia:

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

Kielégíthetetlenség:

Azt mondjuk, hogy G formula illetve F formulahalmaz kielégíthetetlen ha $\mathcal{L}$-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(amis). Az F formulahalmaz kielégíthetetlen, ha az F közös értéktáblájában minden sorban van legalább egy eleme F-nek, amelynek a helyettesítési értéke h(amis).

Elsőrendű szemantikus fa:

Legyenek rendre az $\mathcal{L}$ nyelv szignatúrája szerint (r_1, r_2, …, r_n) a predikátumszimbólumok aritásai.

Előállítjuk minden j = 1, …, n értékre az U^{r_j} értékeinek felhasználásával P_{r_j} összes alapatomját, tekintsük ezek egy rögzített sorrendjét (bázis), a szemantikus fa szintjeihez ebben a sorrendben rendeljük hozzá az alapatomokat. Egy-egy szint minden csúcsából pontosan két él indul ki, az egyik a szinthez rendelt alapatommal, a másik ennek negáltjával van címkézve. A bináris fa ágai adják meg a lehetséges interpretációkat.

Logikai vagy szemantikus következmény az elsőrendű logikában:

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

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

Jelölés: F ⊨ G vagy {F_1, F_2, …, F_n} ⊨ G.

//Tétel (logikailag igaz):

//Ha egy G formula bármely F feltételhalmaznak következménye akkor G logikailag igaz.

Tétel:

F-nek szemantikus következménye G, akkor és csak akkor, ha az F∪{¬G} kielégíthetetlen.

Tétel :

Ha F-nek szemantikus következménye G_1 és F-nek következménye G_2, valamint, {G_1, G_2}-nek következménye A, akkor az F-nek következménye A.

Legszűkebb következmény:

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

Ekvivalencia elsőrendű formulák között:

Az A és B elsőrendű formulák logikailag ekvivalensek, ha {A} ⊨ B és {B} ⊨ A.

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.

Tétel:

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.

Tétel:

Ha A és B tautologikusan ekvivalens, akkor A és B logikailag ekvivalens.

Dedukciós tétel:

$\{F_1, F_2, \ldots, F_n\} \vDash G \Leftrightarrow \{F_1, F_2, \ldots, F_{n-1}\} \vDash F_n \supset G$.

Tétel:

$\{F_1, F_2, \ldots, F_n\} \vDash G \Leftrightarrow \vDash F_1 \supset (F_2 \supset (\ldots\supset(F_{n-1}\supset(F_n\supset G))\ldots))$ (logikailag igaz).

Egy n változós ítéletlogikai formula tautológia:

Egy n változós 1. rendű B formula tautológia, ha

- hamishalmaza üres. Ez azt jelenti, hogy ¬B kielégíthetetlen.
- Az ítéletváltozók minden kiértékelésére a helyettesítési érték i.

Elsőrendű n változós B formula logikailag igaz:

- minden U univerzumon, a változók minden behelyettesítése mellett kapott B’ alapformulák igazak minden, a nyelvnek megfelelő struktúrában.
- $\neg$B kielégíthetetlen. Egyetlen interpretációban, egyetlen változókiértékelés mellett sem igaz.

Szemantikus eldöntésprobléma megoldhatósága:

A szemantikus eldöntésprobléma algoritmikusan nem oldható meg. Nem létezik univerzális eldöntési algoritmus.

Elemi konjunkció/diszjunkció:

Egységkonjunkció/diszjunkció, illetve különböző alapú literálok konjunkciója/diszjunkciója. Az elemi diszjunkciót klóznak is nevezzük.

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.

Konjunktív normálforma (KNF)/ kitűntetett konjunktív normálforma (KKNF):

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

Diszjunktív normálforma (DNF)/ kitűntetett diszjunktív normálforma (KDNF):

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

Egyszerűsítési szabályok:

1) $(X \vee d) \wedge (\neg X \vee d) = d$
2) $(X \wedge k) \vee (\neg X \wedge k) = k$

ahol d elemi diszjunkció és k elemi konjunkció.

KDNF felírása a formula igazságtáblája alapján:

- A formula igazhalmazbeli interpretációihoz felírjuk az interpretációban igaz teljes elemi konjunkciót
- Felírjuk a kapott teljes elemi konjunkciókból álló diszjunkciós láncformulát.
- Egyszerűsítéssel előállíthatunk egy DNF-et.

KKNF felírása a formula igazságtáblája alapján:

- A formula hamishalmazbeli interpretációihoz felírjuk az interpretációban hamis teljes elemi diszjunkciót.
- Felírjuk a kapott teljes elemi diszjunkciókból álló konjunkciós láncformulát.
- Egyszerűsítéssel előállíthatunk egy KNF-et.

Kalkulus:

Döntési „algoritmus”, levezető eljárás egy olyan algoritmus/lépéssorozat, amely adott input adatokkal dolgozik, azokat a megfelelő szabályok szerint használja fel, a levezetési szabály szerint alakítja át, és akkor áll meg, amikor a kitűzött célt elérte. A megállással egy kétesélyes döntés egyik kimenetét igazolja. Azonban, ha az algoritmus nem éri el a kitűzött célt, az nem feltétlenül jelenti azt, hogy meghozta a másik eshetőségre a döntést. Egy ilyen eljárást kalkulusnak hívunk.

Automatikus tételbizonyító kalkulus:

Egy formula kielégíthetetlenségének eldöntésére több döntési algoritmus ismert. Ezekről bebizonyítható, hogy ha a formula felhasználásával az algoritmus eléri a megállási feltételt, akkor a formula kielégíthetetlen. Azt is mondjuk, hogy az ilyen kalkulusok automatikus tételbizonyító kalkulusok.

Klózok illesztése:

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

Cáfoló csúcs:

Cáfoló csúcsnak nevezzük a szemantikus fa azon csúcsát, amelyiket elérve egy klóz hamissá válik.

Levezető csúcs:

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

Szemantikus fa zártsága:

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

Tétel:

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

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 $C=C_1' \vee C_2'$.

Tétel:

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

Rezolúciós levezetés:

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

Rezolúciós kalkulus helyessége:

Lemma: Legyen S tetszőleges klózhalmaz és $k_1, k_2, \ldots k_n$ klózsorozat rezolúciós levezetés S-ből. Ekkor minden k_j, $j=1, 2, \ldots n$-re szemantikus következménye S-nek.

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

Rezolúciós kalkulus teljes:

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

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.

Lineáris rezolúciós levezetés:

Egy S klózhalmazból egy olyan k_1, l_1, k_2, l_2, …, k_{m-1}, l_{m-1}, k_m klózsorozat, ahol k_1, $l_1 \in S$, és minden i= 2, 3, …, 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.

Lineáris inputrezolúciós levezetés:

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

Egységrezolúciós stratégia:

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

Horn klóz:

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

Horn logika:

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

Tétel:

Ha az □ levezethető lineáris input rezolúcióval egy K klózhalmazból, akkor K-ban van legalább egy egységklóz.

Tétel:

Kielégíthetetlen Horn klózhalmazban van legalább egy egységklóz.

Prenex formula:

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

Skolem formula:

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

Elsőrendű klóz:

Olyan zárt Skolem formula, aminek a magja az elsőrendű nyelv literáljainak diszjunkciója.

A prenex formába való átírás algoritmusa:

1) A logikai összekötőjelek átírása ¬, ∧, ∨-ra.
2) A De Morgan szabályok alkalmazása addig amíg a ¬ hatásköre atomi formula nem lesz.
3) A kvantorkiemelési szabályok alkalmazása addig amíg minden kvantor a formula elejére nem kerül.

Kielégíthetőség és az U számossága:

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

Ha egy formula kielégíthető $|U| = n$ számosságon, akkor ennél nagyobb számosságon is kielégíthető.

Löwenheim-Skolem tétel:

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

Elsőrendű klózhalmaz kielégíthetetlensége:

Egy S elsőrendű klózhalmaz kielégíthetetlen, ha minden interpetációban legalább egy klóza hamis.

Egy elsőrendű klóz hamis egy interpretációban, ha az interpretáló struktúra U univerzumán kifejtve a magból kapott alapklózok közül legalább egy hamis ebben az interpretációban.

Egy S elsőrendű klózhalmaz kielégíthetetlen U felett, ha az U-n definiálható minden struktúrában az alapklózok halmaza kielégíthetetlen. Ha az S elsőrendű klózhalmazból az adott számosságú univerzumon a kifejtéssel megkapott alapklózok halmazából alaprezolúcióval levezethető az üres klóz, akkor a klózhalmaz ezen az univerzumon kielégíthetetlen. Ha egy S kielégíthetetlen egy $|U|=n$ számosságú univerzumon, még lehet nagyobb számosságon kielégíthető.

Herbrand univerzum konstrukciója:

1) H_0={S-ben előforduló konstansok halmaza} vagy ha a klózhalmazban nincs konstans szimbólum, akkor egy szimbolikus konstans {a}.
2) $H_{i+1}=H_i \cup F_i$, ahol F_i azon alaptermek halmaza, amelyeket H_i elemeinek a klózhalmazban lévő függvényszimbólumokba való behelyettesítésével kapjuk.
3) $H_\infty = \bigcup_{k\in\mathbb{N}} H_k$

Ha tekintjük az elsőrendű klózhalmaz leíró nyelvének alaptermjeiből álló halmazt a Herbrand univerzumot (H-t), akkor a klózhalmaz akkor lesz kielégíthetetlen ha H-n kielégíthetetlen. Minden elsőrendű nyelvhez létezik legfeljebb megszámlálhatóan végtelen számosságú Herbrand univerzum.

Egy elsőrendű klózhalmaz kielégíthetetlen akkor és csak akkor, ha Herbrand univerzumán kielégíthetetlen.

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.

Herbrand interpretáció:

Legyen az S klózhalmaz leíró nyelve ⟨Pr, Fn, Cnst⟩, Herbrand-univerzuma pedig H. Herbrand-interpretációnak nevezzük és I_H-val jelöljük a nyelv azon interpretációit, melyek univerzuma éppen H, és

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

Elsőrendű klózhalmaz kielégíthetetlensége Herbrand interpretációval:

Egy elsőrendű klózhalmaz akkor és csak akkor kielégíthetetlen, ha a Herbrand univerzuma feletti egyetlen Herbrand interpretáció sem elégíti ki. Nincs Herbrand modellje.

Herbrand tételek:

Tétel: Egy S elsőrendű klózhalmaz kielégíthetetlen akkor és csak akkor, ha S bármely szemantikus fájához van véges zárt szemantikus fája.

Tétel: Egy S elsőrendű klózhalmaz kielégíthetetlen akkor és csak akkor, ha S klózai alapelőfordulásainak van véges kielégíthetetlen S' részhalmaza.

Számításelmélet

Definíció: Függvények gyorsasága

Legyenek f; g: N -> N függvények, ahol N a természetes számok halmaza. Azt mondjuk, hogy f legfeljebb olyan gyorsan nő, mint g (jelölése: f (n) = O (g (n))) ha létezik olyan c > 0 szám és $n_0 \in N$, hogy f (n) ≤ c * g (n) minden n ≥ n_0 számra. Az f (n) = Ω(g (n)) jelöli azt, hogy g (n) = O (f (n)) teljesül, és f (n) = Θ (g (n)) jelöli azt, hogy f (n) = O (g (n)) és f (n) = Ω(g (n)) is teljesül.

Tétel: Polinom vs. Exponenciális

Minden polinomiális függvény lassabban nő, mint bármely exponenciális függvény, azaz minden p (n) polinomhoz és c pozitív valós számhoz van olyan n_0 egész szám, hogy minden n ≥ n_0 esetén p (n) ≤ 2^{c*n}.

Definíció: Turing-gép

A Turing-gép egy olyan M = (Q, Σ, Γ, δ, 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 ábécék, a bemenő jelek illetve a szalag szimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma - \Sigma$
-δ : $(Q - \{q_i, q_n\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R, S\}$ az állapot-átmeneti függvény

Definíció: Konfigurációs átmenet

Az M konfiguráció-átmenete egy olyan $\vdash \subseteq C_m \times C_m$ reláció, amit a következőképpen definiálunk. Legyen uqav egy konfiguráció, ahol a ∈ Γ és u; v ∈ Γ* . A következő három esetet különböztetjük meg.

1. Ha δ (q; a) = (r; b; S), akkor uqav ⊢ urbv.
2. Ha δ (q; a) = (r; b;R), akkor uqav ⊢ ubrv', ahol v' = v, ha v≠ε , és v' = ⊔ egyébként
3. Ha δ (q; a) = (r; b; L), akkor uqav ⊢ u'rcbv ahol u'c = u valamely u' ∈ Γ* -ra és c ∈ Γ-ra, ha u ≠ ε és u' = ε , c = ⊔ egyébként.

Definíció: L nyelv felismerhető Turing-géppel

Egy L ∈ Σ* nyelv Turing-felismerhető, ha L = L (M) valamely M Turing-gépre. Továbbá, egy L ⊆ Σ* nyelv eldönthető, ha létezik olyan M Turing-gép, mely minden bemeneten megállási konfigurációba jut és felismeri az L-et. A Turing-felismerhető nyelveket szokás rekurzívan felsorolhatónak, az eldönthető nyelveket pedig rekurzívnak is nevezni.

Definíció: Turing-gép futásának időigénye

Tekintsünk egy M =(Q, Σ, Γ, δ, q_0, q_i, q_n) Turing-gépet és annak egy u ∈ Σ* bemenő szavát. Azt mondjuk, hogy M futási ideje (időigénye) az u szón n (n ≥0), ha M a q0u⊔ kezdő konfigurációból n lépésben el tud jutni egy megállási konfigurációba. Ha nincs ilyen szám, akkor M futási ideje az u-n végtelen.
Legyen f: N -> N egy függvény. Azt mondjuk, hogy M időigénye f (n) (vagy azt, hogy M egy f (n) időkorlátos gép), ha minden u ∈ Σ* input szóra, M időigénye az u szón legfeljebb f (l (u)).

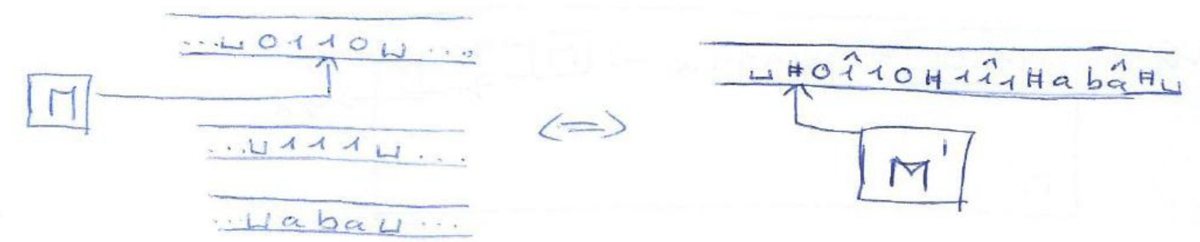
Definíció: Több szalagos Turing- gép

Legyen k≥ 1, k-szalagos Turing-gép: M = (Q, Σ, Γ, δ, q_0, q_i, q_n), ahol a δ kivételével a komponensek ugyanazok, δ pedig a követező: (Q – {q_i, q_n}) × Γ^k → Q × Γ^k × . $\{L, R, S\}^k$

Tétel: Eltérő szalagos Turing-gépek ekvivalenciája

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

Biz:



M' a következőképpen szimulálja M-et:

1. Adott u = a_1, … , a_n bemeneten előállítja az M kezdőkonfigurációját.
2. M' balról jobbra végigmegy a szalagján és eltárolja az állapotában, hogy mely szimbólumok vannak ^-pal megjelölve
3. M' szimulálja M egy lépését. Ha M valamelyik szalagján kiterjeszti a szó hosszát, akkor M' a megfelelő pozíciótól mozgatja 1 cellával a szalag tartalmát
4. Ha M' azt látja, hogy M q_i / q_n –be lép akkor M' is a megfelelő állapotba lép, egyébként folytatja a szimulációt a 2.-tól

Definíció: Turing-gépek ekvivalenciája

M_1 és M_2 Turing-gépek ekvivalensek, ha L (M_1) = L (M_2)

Tétel: Eltérő irányú Turing-gépek ekvivalenciája

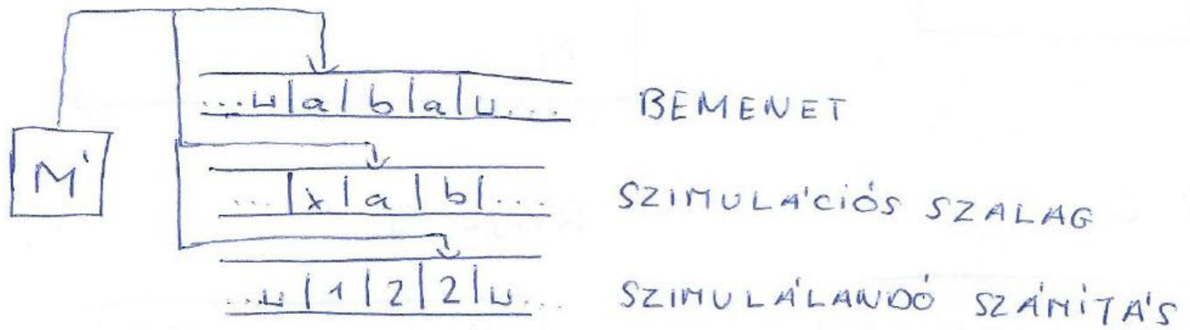
Minden többirányú Turing-géphez van vele ekvivalens egyirányú Turing-gép.

Definíció: Nemdeterminisztikus Turing-gép

Egy $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ nemdeterminisztikus Turing-gép komponensei az átmenetfüggvény kivételével megegyeznek.
Az átmenetfüggvénye: $\delta: (Q - \{q_i, q_n\}) \times \Gamma \to P(Q \times \Gamma \times \{L, R, S\})$.
Az M nemdeterminisztikus Turing-gép által felismert nyelv ugyanaz, mint determinisztikus esetben.

Tétel: Nemdeterminisztikus Turing-gép megfeleltetése determinisztikussal

Minden M nemdeterminisztikus Turing-géphez adható ekvivalens determinisztikus M' Turing-gép. Ha M f(n) időigényű volt, akkor M' legfeljebb $2^{O(f(n))}$ időigényű lesz.
Biz: (Ide van írva, hogy lásd jegyzetben M' lépéseit)



Legyen $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ d:= { δ(q,a)}.
Tegyük fel hogy minden $(q,a) \in Q \times M$ esetén a δ(q,a) elemeinek van egy rögzített sorrendje.
Ekkor egy q bementen az M számítási fájának minden konfigurációjához egyértelműen hozzárendelhető egy T-feletti szó ahol T: = {1,…,d}.
Belátható hogy M' akkor és csak akkor fogad el egy szót, ha M is elfogadja.

Definíció: Nemdeterminisztikus Turing-géppel való eldöntés

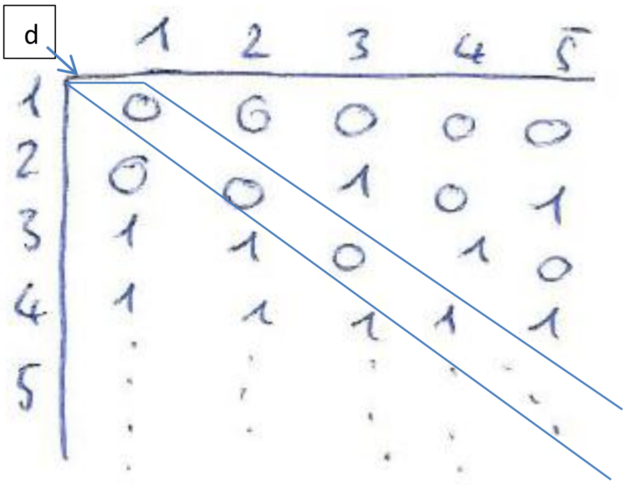
Az M nemdeterminisztikus Turing-gép eldönti az L nyelvet, ha felismeri (L = L (M)) és $\forall u \in \Sigma^*$ szóra az M számítási fája u-n véges és ∀ levele elutasító vagy elfogadó konfiguráció

Definíció: Időigény és számítási fa kapcsolata
Az M f(n) időigényű, ha $u \in \Sigma^*$ esetén az M számítási fája legfeljebb f(l(u)) magas.

Definíció: R és RE kapcsolata
RE= { L | L Turing felismerhető }
R = { L | L eldönthető }
Kapcsolatuk: $R \subseteq RE$

Tétel: Az Látló nem rekurzívan felsorolható, ahol Látló = { <M,w> | w ∈ L(M) }

Biz:
Legyen T a következő táblázat: T(i,j) = 1 ⇔ $w_j \in L(M_i)$. d a táblázat bal felső sarkából indított átló.



1. T i-ik sora $L(M_i)$ nyelv karakterisztikus függvénye
2. $\overline{d}$ az Látló karakterisztikus függvénye
3. Az összes RE-beli nyelv karakterisztikus függvénye megegyezik a T valamelyik sorával
4. $\overline{d}$ különböző T összes sorától

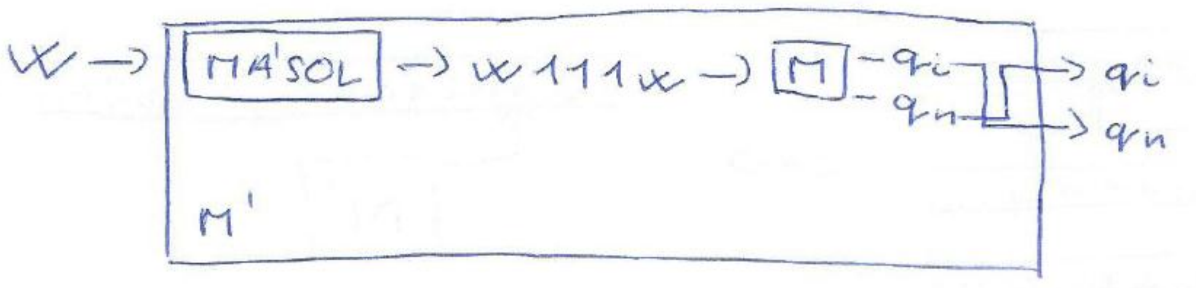
Látló karakterisztikus függvénye különbözik az összes RE-beli nyelv karakterisztikus függvényétől => Látló ∉ RE

Tétel: Lu ∈ RE, ahol Lu= { <M,w> | w ∈ L (M) }

Biz: Könyvet írtunk EA-n

Tétel: Lu ∉ R.

Biz:

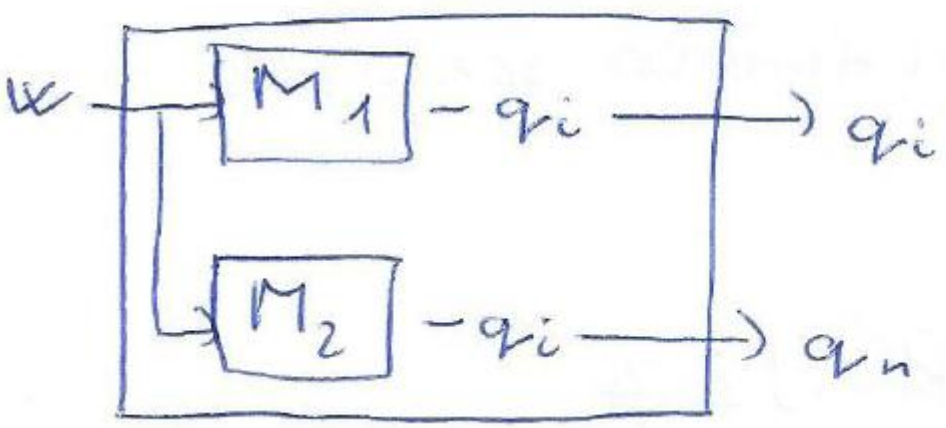


Indirekt módon tegyük fel, hogy Lu ∈ R és legyen M az a Turing-gép, ami eldönti Lu –t.
Konstruáljuk meg a következő M'-t:
Ekkor w ∈ L(M') ⇔ w111w ∉ L(M) ⇔ w111w ∈ Lu ⇔ w által kódolt Turing-gép nem fogadja el w-t ⇔ w ∈ Látló .
Azt kapjuk, hogy L(M') = Látló => ellentmondás

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

Biz:

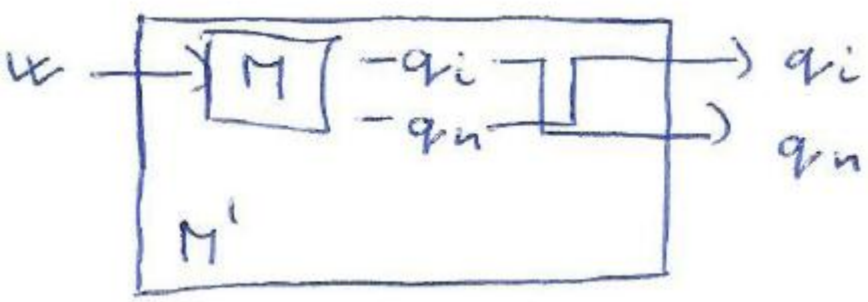
Legyen M_1 és M_2 2 Turing-gép, ami rendre az L és $\overline{L}$ nyelveket ismeri fel. Legyen M a következő Turing-gép.



M felváltva szimulálja az 1-es és 2-es szalagján az M_1 és M_2 gépeket a w szón.
Az M minden bemeneten megáll és L(M) =L, azaz L ∈ R.

Tétel: Legyen L ∈ R. Akkor $\overline{L}$ ∈ R.

Biz:



Legyen M az L-et eldöntő Turing-gép és konstruáljuk meg M'-t.
L(M) = $\overline{L}$ és M minden bemeneten megáll, vagyis $\overline{L}$ ∈ R

Definíció:

Ha L ⊆ Σ*, akkor $\overline{L}$ = { u ∈ Σ* | u ∉ L}

Definíció: Függvény kiszámítása

Egy f: Σ*→ Δ* függvény kiszámítható, ha van olyan M determinisztikus Turing-gép, ami egy w ∈ Σ* szóval a bementén indítva véges sok lépésben megáll, és ekkor az utolsó szalagján f(w) van.

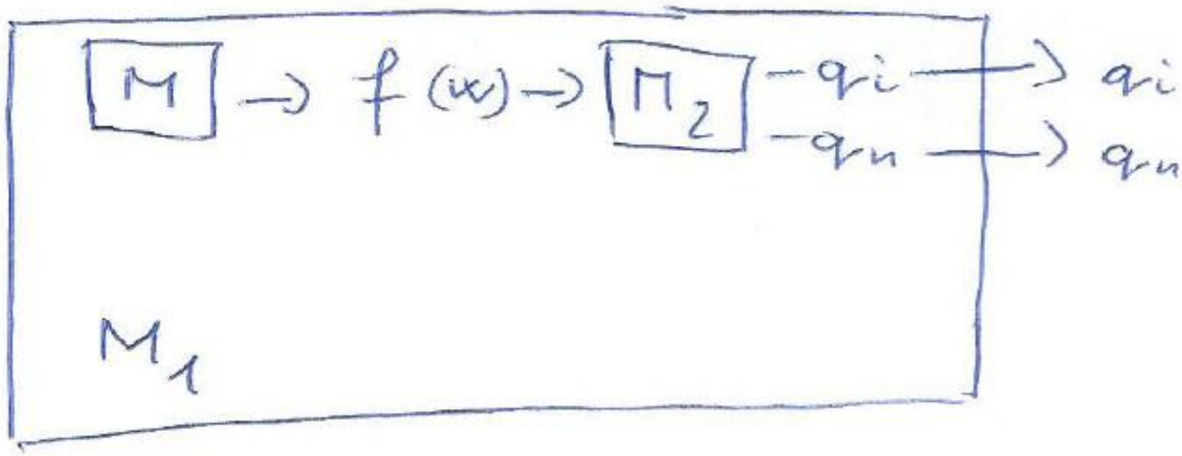
Definíció: Visszavezetés

Legyen $L_1 \subseteq \Sigma^*$, $L_2 \subseteq \Delta^*$. L_1 visszavezethető L_2-re ($L_1 \subseteq L_2$), ha létezik $f: \Sigma^* \rightarrow \Delta^*$ kiszámítható függvény, hogy $w \in \Sigma^*$: $w \in L_1 \Leftrightarrow f(w) \in L_2$.

Tétel: L_1 visszavezethető L_2
Ha $L_1 \subseteq L_2$ és
- $L_2 \in R$, akkor $L_1 \in R$.
- $L_2 \in RE$, akkor $L_1 \in RE$.

Ha $L_1 \notin R$, akkor $L_2 \notin R$.

Biz: Ha $L_1 \notin R$, akkor $L_2 \notin R$ bizonyítjuk be.
Tegyük fel, hogy $L_2 \in R$ és legyen M_2 egy Turing-gép, ami eldönti L_2 –t Legyen továbbá M az f-et kiszámító Turing-gép. Legyen M_1 a következő



Mivel $L_1 \subseteq L_2$ $L(M_1) = L_1$. Továbbá M_2 minden bemeneten megáll vagyis $L_1 \in R$.
Ami ellentmondás.

Definíció: L_h nyelv

$L_h = \{ \langle M,w \rangle \mid M \text{ megáll } w\text{-n} \}$

Tétel: $L_h \notin R$.

Biz:
Elég megmutatni, hogy $L_u \leq L_h$
Legyen f: $\langle M \rangle \rightarrow \langle M' \rangle$ ahol M' az a Turing-gép, amit úgy kapunk M-ből, hogy amikor q_n-be lép akkor M' belép egy végtelen ciklusba.

1. f kiszámítható függvény
2. Tetszőleges M,w párosra teljesül:
   $\langle M,w \rangle \in L_u \Leftrightarrow$ M megáll q_i-ben a w-n $\Leftrightarrow$ M' megáll w-n $\Leftrightarrow$ $\langle M',w \rangle \in L_h$
   $L_u \notin R$ így $L_h \notin R$

Tétel: $L_h \in$ RE.

Biz:

Legyen U az L_u –t felismerő univerzális Turing-gép. Konstruáljuk meg U'-t:
U' úgy működik, mint U kivéve hogy U'-ben minden U-beli qn-be vezető átmenet qi-be irányítunk.
M megáll w-n ⇔ <M,w> $\in L_h$

Tétel: Rice tétel

Egy P ⊆ RE halmazt RE-beli nyelvek egy tulajdonságának nevezzük. A P triviális, ha P = ∅ vagy P = RE. Lp = {<M> | L(M) ∈ P}.

Tétel: Ha P ∈ RE nem triviális, akkor $L_p \notin$ R.

Definíció: Nevezetes időbonyolultságú osztályok

P azon nyelveket tartalmazza, amelyek eldönthetőek polinom időkorlátos determinisztikus Turing-géppel.
NP eldönthető polinom idejű nemdeterminisztikus Turing-géppel.
Kapcsolat: P ⊂ NP

TIME(f(n)) = { L | L eldönthető O(f(n)) időigényű Turing-géppel }
NTIME(f(n)) = { L | L eldönthető O(f(n)) időigényű nemdeterminisztikus Turing-géppel}
ahol f : N -> N függvény.

Definíció: A PMP probléma

A PMP problémát a következőképpen definiáljuk. Legyen Σ egy legalább két betűt tartalmazó ábécé és legyen D = $\{\left[\frac{u_1}{v_1}\right], \dots, \left[\frac{u_n}{v_n}\right]\}$ egy dominóhalmaz melyben n ≥ 1, $u_1, \dots, u_n, v_1, \dots v_n \in \Sigma^+$. A kérdés az, hogy van-e olyan $1 \leq i_1, \dots, i_m \leq m$ ($m \geq 1$) indexsorozat amelyre teljesül, hogy $\left[\frac{u_{i1}}{v_{i1}}\right], \dots, \left[\frac{u_{im}}{v_{im}}\right]$ dominókat egymás mellé írva alul és felül ugyanaz a szó adódik, azaz $u_{i1},\dots,u_{im} = v_{i1},\dots v_{im}$. Ebben az esetben a fenti dominósorozatot a D egy megoldásának nevezzük.

Fromális nyelvként a következőképpen definiáljuk a PMP-t:
PMP = { <D> | D-nek van megoldása}

Definíció: Függvény kiszámíthatóságának viszonyítása Turing-géppel

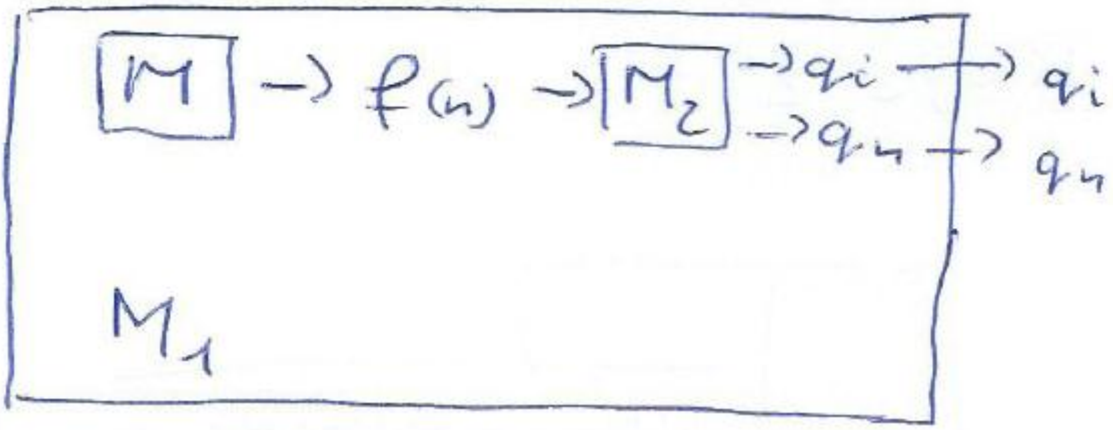
Legyen Σ és Δ két ábécé és f egy Σ *-ból Δ*-ba képező függvény. Azt mondjuk, hogy f polinom időben kiszámítható, ha kiszámítható egy polinom időigényű Turing-géppel.

Definíció: Visszavezethetőség

Legyen $L_1 \in \Sigma^*$ és $L_2 \in \Delta^*$ két nyelv. Azt mondjuk, hogy L_1 polinom időben visszavezethető L_2-re (jele: $L_1 \leq_p L_2$), ha $L_1 \leq L_2$ és felhasznált f függvény polinom időben kiszámítható.

Tétel: Két polinom időben visszavezethető probléma kapcsolata
Legyen L_1 és L_2 két probléma, úgy, hogy $L_1 \leq_p L_2$
- $L_2 \in P$, akkor $L_1 \in P$
- $L_2 \in NP$, akkor $L_1 \in NP$.

Biz: (2. állítást kell csak belátni)



M az $L_1 \leq_p L_2$ visszavezetést kiszámoló M_2 pedig az L_2 –t eldöntő Turing-gép (M determinisztikus, M_2 nemdeterminisztikus). Belátható, hogy $L(M_2) = L_2$ azaz $L_2 \in NP$

Definíció: NP teljesség, NP egy fontos részosztálya

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.

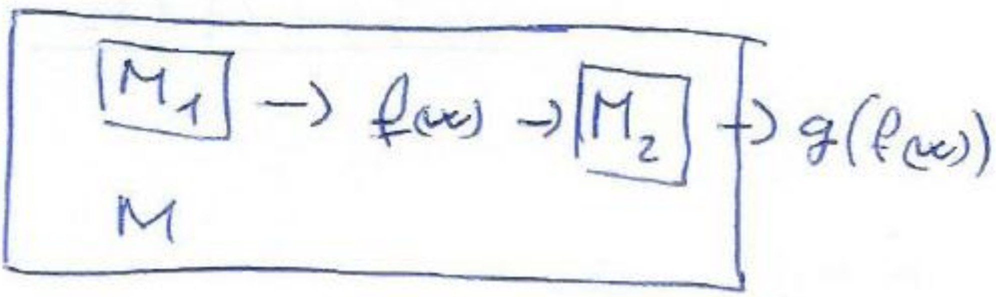
Tétel: Legyen L egy NP-teljes probléma. Ha $L \in P$, akkor $P = NP$.

Biz:
Elég megmutatni, hogy ebben az esetben $NP \subseteq P$. Legyen $L' \in NP$. Mivel L NP-teljes, azt kapjuk, hogy $L' \leq_p L$. $L \in P$ így $L' \in P$

Tétel: NP-beli problémákról belátható hogy NP-teljes

Legyen L_1 egy NP-teljes és L_2 egy NP-beli probléma. Ha $L_1 \leq_p L_2$, akkor L_2 is NP-teljes.

Biz:



Elég megmutatni, hogy tetszőleges $L'' \in$ NP-re $L'' \leq_p L$.
Legyen M_1 és M_2 rendre az $L'' \leq_p L$ és $L \leq_p L'$ visszavezetést kiszámító Turing-gép. tegyük fel hogy M_1 az f M_2 a g függvényt számolja ki.
Legyen M a következő Turing-gép.

Belátható hogy M is polinom idejű, továbbá az $L'' \leq_p L'$-t számítja ki. Következménye hogy L' Np-teljes.

Definíció: Sat probléma definíciója

SAT = { <φ> | φ egy kielégíthető zérusrendű KNF}

Tétel: Cook tétel : Sat NP-teljes.

Biz:

1. SAT ∈ NP
2. Legyen L ∈ NP és M egy P(n) polinom idejű nemdeterminisztikus Turing-gép melyre L(M) = L. Tetszőleges w szóhoz megadható egy φ w KNF, hogy w ∈ L ⇔ < φw> ∈ SAT
   φw-vel leírható M működése

A φw ítéletváltozói $X_{i,j,c}$ alakúak ami annak az ítéletnek felel meg hogy a táblázat i-ik sorának j-edik mezőjében c szimbólum van.

Tétel: 3SAT NP-teljes, ahol 3SAT={ <ϕ>: ϕ ∈ SAT, ϕ minden tagjában pontosan 3 literál van}

Definíció:

Legyen $k \geq 1$. kSAT = { <ϕ> : < ϕ> ∈ SAT, ϕ minden tagjában k literál van}

Definíció: Teljes részgráf

Teljes részgráf ={ <G,k> | G véges gráf, k ≥ 1, G-nek létezik k csúcsú teljes részgráfja }

Definíció: Független csúcshalmaz

Független csúcshalmaz = {⟨G; k⟩| G véges gráf, k ≥ 1; G-nek van k elemű független csúcshalmaza}

Definíció: Csúcslefedés

Csúcslefedés = {⟨G; k⟩ | G véges gráf, k ≥ 1;G-nek van olyan k elemű csúcshalmaza, mely tartalmazza G minden élének legalább egy végpontját }

Tétel: Teljes részgráf NP-teljes.

Tétel: Független csúcshalmaz NP-teljes.

Tétel: Csúcslefedés NP-teljes

Biz: (Előző Három tétel egybe megy)

1. Mindhárman NP-ben vannak:
   - Egy M nemdeterminisztikus Turing-gép „megsejti” a probléma egy megoldását
   - polinom időben leellenőrzi, hogy a sejtés tényleg helyes megoldás-e
2.
   a.) 3Sat ≤p FCS f : $<\varphi> \,-\!> <G\varphi>$, ahol φ 3SAT alakú $\varphi = (l_{11} \vee l_{12} \vee l_{13}) \wedge \ldots \wedge (l_{k1} \vee l_{k2} \vee l_{k3})$ és $G\varphi$. Az élek: a Δ-ek + koplemens literálpárok között. Ekkor f polinom időben kiszámítható és $<\varphi> \in$ 3SAT ⇔ $<G\varphi> \in$ FCS

   b.) FCS ≤p KLIKK
   f: $<G> \,-\!> <\overline{G}>$ $\overline{G}$: csúcsai mint G csúcsai élei {a,b} él: $\overline{G}$-ben ⇔{a,b} nem él G-ben, G-ben akkor és csak akkor van két csúcs között él ha ugyanezen csúcsok között $\overline{G}$-ben nincs. Ekkor $<G, K> \in$ FCS ⇔ $<\overline{G}, K> \in$ KLIKK

   c.) FCS ≤p CSL
   f: $<G, K> \,-\!> <G, n\text{-}k>$, ahol n=M

Definíció: Hamilton-út

Hamilton-út = {⟨G; s; t⟩ | G véges irányított gráf, s; t csúcsok, ∃ s-ből t-be Hamilton-út}

Tétel: Hamilton út NP-teljes.

Biz:
SAT≤p HÚ
f: $<\varphi> \,-\!> G\varphi$, ahol $\varphi = d_1 \wedge d_2 \wedge \ldots \wedge d_k$. Tegyük fel hogy φ-ben az $x_1,\ldots x_k$ változok szerepelnek(tagadva vagy anélkül)
Ekkor $<\varphi> \in$ SAT ⇔ $<G\varphi,s,t> \in$ HÚ

Definíció: Irányítatlan Hamilton-út

Irányítatlan Hamilton-út = {⟨G; s; t⟩ | G véges irányított gráf, s; t csúcsok, ∃ s-ből t-be Hamilton-út}

Tétel: Az Irányítatlan Hamilton-út probléma NP-teljes.

Biz:

1. IHÚ ∈ NP
2. HÚ ≤p IHÚ f: G —> G’
   A G’ csúcsai: G csúcsai „duplázva”: u —> u_1,u_2,u_3
   élei: u_1 —u_2 és u_2 – u_3 automatikusan, + ha van u—>v él G-ben , akkor G’-be felvesszük az u_3—v_1 élt.
   Ekkor: <G,s,t>∈ HÚ ⇔ <G’,s_4,t_3>∈ IHÚ

Tétel: HK NP-teljes

Biz:

1. HK ∈ NP
2. IHÚ ≤p HK

f: <G, s ,t> —> <G’>. Ekkor <G, s, t>∈ IHÚ ⇔ <G’>∈ HK

Definíció: Utazóügynök

Utazóügynök = {⟨G; k⟩ | G véges irányítatlan gráf az éleken egy-egy pozitív egész súllyal és G-ben van legfeljebb k összsúlyú Hamilton kör}

Tétel: Az Utazóügynök probléma NP-teljes.

Biz:

1. UÜ ∈ NP

Ha lekorlátozzuk UÜ bemenetét úgy, hogy G minden élén 1 súly szerepel és K|V|, akkor megkapjuk a HK-t. Ezért UÜ is NP-teljes

Tétel: P Beli és NP-teljes problémák viszonya

Ha P=NP, akkor van olyan L ∈ NP, hogy L ∉ P és L nem NP-teljes.

Definíció: Legyen C egy nyelvosztály coC = { $\overline{\mathrm{L}}$ | L ∈ C}

Tétel: C és coC zártsága polinom idejű visszavezetésekre

Ha C zárt a polinom idejű visszavezetésre, azaz ha L ∈ C és L' ≤p L akkor L'∈ C , akkor coC is zárt.

Biz:

Tegyük fel hogy L' ≤p L és L ∈ coC. Ekkor $\overline{L'}$ ≤p L és $\overline{L}$ ∈ C. Mivel C zárt a polinom idejű visszavezetésre következik, hogy $\overline{L'}$ ∈ C => L'∈ coC.

Definíció: C-teljesség

Egy L nyelv C- nehéz, ha ∀ L′ ∈ L: L'≤p L. Ha L ∈ C, akkor L C-teljes

Tétel: Ha L C-nehéz, akkor $\overline{L}$ coC-nehéz

Biz:
Elég megmutatni, hogy a következő teljesül:
Legyen L C-nehéz. Ekkor ∀ L′ ∈ C : L' ≤p L => ∀ $\overline{L'}$: $\overline{L'}$ ≤p $\overline{L}$ => $\overline{L}$ coC-nehéz.

Tétel: TAUT coNP-teljes, ahol TAUT = { <φ > | φ egy érvényes zérusrendű formula }

Biz:

ÁLT.SAt = { <φ> | φ kielégíthető zérus rendű formula}
UNSAT = { <φ> | φ kielégíthetetlen zérusrendű formula}
UNSAT = $\overline{\text{ÁLT.SAT}}$
ÁLT.SAT NP-nehéz => UNSAT coNP-nehéz
Továbbá UNSAT ≤p TAUT : f :< φ> −> < ¬φ>
Ebből következik: TAUT is coNP-nehéz: Belátható, hogy TAUT ∈ coNP => TAUT coNP-teljes

Definíció: Off-line Turing-gép

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

Definíció: Tárbonyolultsággal kapcsolatos nyelvosztályok

SPACE(f(n)) = { L | L eldönthető O(f(n)) tárigényű determinisztikus Turing-géppel }

NSPACE(f(n)) = { L |L eldönthető O(f(n)) tárigényű nemdeterminisztikus Turing-géppel}

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

Kapcsolat: L⊆ NL ⊆ P ⊆ NP ⊆ PSPACE

Definíció: Tárbonyolultsági osztályok

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

Tétel: Savitch tétel

Ha f (n)≥ log n, akkor NSPACE (f (n)) ⊆ SPACE(f^2(n)).
Következmény PSPACE=NPSPACE

Tétel: QBF PSPACE-teljessége

QBF PSPACE-teljes, ahol QBF= { <φ> | φ egy kielégíthető kvantifikált Boole-formula}. Sőt QBF PSPACE-teljes marad a következő megszorításokkal is:

- a kvantorok alternálnak
- a kvantormentes rész KNF-ben van
- az első és utolsó kvantor a ∃

Tétel: FJ PSPACE-teljes, FJ=Földrajz játék

Biz: QBF ≤p FJ