Ítéletlogika

I. Igazságértékelésfüggvény

A feltételek rekurzív definíciója

- Ha A ítéletváltozó, a φA^i feltételt kielégítő $\mathcal{I}$ interpretációk azok, amelyekre $\mathcal{I}(A) = i$, a φA^h feltételt kielégítők pedig azok, amelyekre $\mathcal{I}(A) = h$.
- A $\varphi(\neg A)^i$ feltétel pontosan akkor teljesül, ha teljesül a φA^h feltétel.
- A $\varphi(\neg A)^h$ feltétel pontosan akkor teljesül, ha teljesül a φA^i feltétel.
- A $\varphi(A \wedge B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^i és a φB^i feltételek.
- A $\varphi(A \wedge B)^h$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^h vagy a φB^h feltételek.
- A $\varphi(A \vee B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^i vagy a φB^i feltételek.
- A $\varphi(A \vee B)^h$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^h és a φB^h feltételek.
- A $\varphi(A \supset B)^i$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^h vagy a φB^i feltételek.
- A $\varphi(A \supset B)^h$ feltételek pontosan akkor teljesülnek, ha teljesülnek a φA^i és a φB^h feltételek.

Tétel: Tetszőleges A ítéletlogikai formula esetén φA^i feltételeket pontosan az A^i-beli interpretációk teljesítik. A φA^h feltételeket pedig pontosan az A^h-beli interpretációk.

II. Formulák és formulahalmazok szemantikus tulajdonságai

- Egy $\mathcal{I}$ interpretáció *kielégít* egy B formulát ($\mathcal{I} \models_0 B$) ha a formula helyettesítési értéke i az $\mathcal{I}$ interpretációban.
- Egy B formula *kielégíthető*, ha legalább egy interpretáció kielégíti.
- Egy B formula *kielégíthetetlen*, ha egyetlen interpretáció sem elégíti ki.
- Egy B formula *tautologia* (ítéletlogikai törvény) ($\models_0 B$), ha minden interpretáció kielégíti.
- Egy $\mathcal{I}$ interpretáció *kielégít* egy $\mathcal{F}$ formulahalmazt ($\mathcal{I} \models_0 \mathcal{F}$), ha a formulahalmaz minden formuláját kielégíti.
- Egy $\mathcal{F}$ formulahalmaz *kielégíthető*, ha legalább egy interpretáció kielégíti.

- Egy $\mathcal{F}$ formulahalmaz *kielégíthetetlen*, ha nincs olyan interpretáció, ami egyszerre minden $\mathcal{F}$-beli formulát kielégít.
- Egy A formulának a B formula *tautologikus következménye*($A \models_0 B$), ha minden A-t kielégítő interpretáció kielégíti B-t is.
- A és B *tautologikusan ekvivalensek* ($A \sim_0 B$), ha $A \models_0 B$ és $B \models_0 A$ is teljesül.
- Egy $\mathcal{F}$ formulahalmaznak a B formula *tautologikus következménye*($\mathcal{F} \models_0 B$), ha minden $\mathcal{F}$-t kielégítő interpretáció kielégíti B-t is.

III. Nevezetes ekvivalenciák ($\top$ tautológia, $\bot$ kielégíthetetlen formula.)

(a) $\neg\neg X \sim_0 X$,

(b) $X \vee X \sim_0 X$ valamint $X \wedge X \sim_0 X$,

(c) $X \vee Y \sim_0 Y \vee X$ valamint $X \wedge Y \sim_0 Y \wedge X$,

(d) $(X \vee Y) \vee Z \sim_0 X \vee (Y \vee Z)$ valamint $(X \wedge Y) \wedge Z \sim_0 X \wedge (Y \wedge Z)$,

(e) $(X \vee Y) \wedge Z \sim_0 (X \wedge Z) \vee (Y \wedge Z)$ valamint $(X \wedge Y) \vee Z \sim_0 (X \vee Z) \wedge (Y \vee Z)$,

(f) $(X \vee Y) \wedge Y \sim_0 Y$ valamint $(X \wedge Y) \vee Y \sim_0 Y$,

(g) $X \supset Y \sim_0 \neg X \vee Y$,

(h) $\neg(X \wedge Y) \sim_0 \neg X \vee \neg Y$ valamint $\neg(X \vee Y) \sim_0 \neg X \wedge \neg Y$,

(i) $X \vee \neg X \sim_0 \top$ valamint $X \wedge \neg X \sim_0 \bot$,

(j) $X \vee \top \sim_0 \top$ valamint $X \wedge \bot \sim_0 \bot$,

(k) $X \vee \bot \sim_0 X$ valamint $X \wedge \top \sim_0 X$.

IV. Az ítéletlogika eldöntésproblémája:

$$\{A_1, A_2, \ldots, A_n\} \overset{?}{\models_0} B$$

$\{A_1, A_2, \ldots, A_n\} \models_0 B \Leftrightarrow \{A_1, A_2, \ldots, A_n, \neg B\}$ kielégíthetetlen $\Leftrightarrow$
$\Leftrightarrow H = \{\mathrm{KNF}_{A_1}, \mathrm{KNF}_{A_2}, \ldots, \mathrm{KNF}_{A_n}, \mathrm{KNF}_{\neg B}\}$ kielégíthetetlen $\Leftrightarrow$
$\Leftrightarrow$ A H halmaz formuláiban szereplő klózok halmaza kielégíthetetlen

Elsőrendű logika

I. Alapfogalmak
1.a. Egy elsőrendű logika L nyelvének ábécéje:
Logikán kívüli rész:
$\langle \mathrm{Srt}, \mathrm{Pr}, \mathrm{Fn}, \mathrm{Cnst} \rangle$

- Srt, nemüres halmaz melynek elemei fajtákat szimbolizálnak, innentől $|\mathrm{Srt}| = 1$ (egyfajtájú eset).
- Pr, predikátumszimbólumok halmaza. ν_1 minden $P \in \mathrm{Pr}$ -re megadja P aritását ($\in \mathbb{N}$)
- Fn, függvényszimbólumok halmaza. ν_2, minden $f \in \mathrm{Fn}$ -re megadja f aritását ($\in \mathbb{N}$)
- Cnst, konstansszimbólumok halmaza, ν_3 megadja a konstansok számát ($\in \mathbb{N}$).

1.b. Logikai jelek:

- Megszámlálható végtelen sok individuum változó $V = \{x, y, x_1, \ldots\}$
- unér és binér logikai műveleti jelek $\neg, \wedge, \vee, \supset$
- kvantorok $\forall, \exists$
- elválasztójelek $(,)$

Az L nyelv ábécéjére $V[V_v]$-vel hivatkozunk, ahol V_v adja meg a (ν_1, ν_2, ν_3) szignatúrájú $\langle \mathrm{Srt}, \mathrm{Pr}, \mathrm{Fn}, \mathrm{Cnst} \rangle$ halmaznégyest.
2. Term (egyfajtájú eset) $(L_t(V_v))$:

- (alaplépés) minden individuum változó és konstans szimbólum term.
- (rekurzív lépés) Ha $f \in \mathrm{Fn}$ k-aritású függvényszimbólum és $t_1, t_2, \ldots, t_k$ termek, akkor $f(t_1, t_2, \ldots, t_k)$ is term.
- minden term az 1., 2. szabályok véges sokszori alkalmazásával áll elő.

3. Formula (egyfajtájú eset) $(L_f(V_v))$:

- (alaplépés) Ha $P \in \mathrm{Pr}$ k-aritású predikátumszimbólum és $t_1, t_2, \ldots, t_k$ termek, akkor $P(t_1, t_2, \ldots, t_k)$ formula.
- (rekurzív lépés)
  - Ha A formula, akkor $\neg A$ is az.
  - Ha A és B formulák, akkor $(A \circ B)$ is formula ($\circ$ a három binér művelet bármelyike).
  - Ha A formula, akkor $\forall x A$ és $\exists x A$ is az.
- Minden elsőrendű formula az 1., 2. szabályok véges sokszori alkalmazásával áll elő.

II. Szemantika (egyfajtájú eset)
1. Interpretáció
Egy elsőrendű logikai nyelv $L(V_v)$ *interpretációja* egy
$\mathcal{I} = \langle \mathcal{I}_{\mathrm{Srt}}, \mathcal{I}_{\mathrm{Pr}}, \mathcal{I}_{\mathrm{Fn}}, \mathcal{I}_{\mathrm{Cnst}} \rangle$ függvénynégyes, ahol

- $\mathcal{I}_{\mathrm{Srt}}$ egy U halmaz (univerzum) megjelölése,
- $\mathcal{I}_{\mathrm{Pr}} : P \mapsto P^{\mathcal{I}}$, minden $P \in$Pr-re, ha P k-aritású, akkor $P^{\mathcal{I}} \subseteq U^k$, (Logikai fv-es megfogalmazás: $P^{\mathcal{I}}(u_1, \ldots, u_k) = i \Leftrightarrow (u_1, \ldots, u_k) \in P^{\mathcal{I}}$)
- $\mathcal{I}_{\mathrm{Fn}} : f \mapsto f^{\mathcal{I}}$, minden $f \in$Fn-re, ha f k-aritású, akkor $f^{\mathcal{I}} : U^k \to U$ egy k változós művelet U-n,

- $\mathcal{I}_{\text{Cnst}} : c \mapsto c^{\mathcal{I}} \in U$.

2. Változókiértékelés
   $\kappa : V \to U$.
3. Termek értéke egy $\mathcal{I}$ interpretációban, egy κ változókiértékelés mellett:

   - Ha x_s individuumváltozó, $|x_s|^{\mathcal{I},\kappa}$ a $\kappa(x) \in U$ individuum.
     Ha c konstansszimbólum $|c|^{\mathcal{I},\kappa}$ az U-beli $c^{\mathcal{I}}$ individuum.
   - $|f(t_1, t_2, \ldots, t_n)|^{\mathcal{I},\kappa} = f^{\mathcal{I}}(|t_1|^{\mathcal{I},\kappa}, |t_2|^{\mathcal{I},\kappa}, \ldots, |t_n|^{\mathcal{I},\kappa})$.

4. Formulák igazságértéke egy $\mathcal{I}$ interpretációban, egy κ változókiértékelés mellett:

   - $|P(t_1, t_2, \ldots, t_n))|^{\mathcal{I},\kappa} = i, \Leftrightarrow (|t_1|^{\mathcal{I},\kappa}, |t_2|^{\mathcal{I},\kappa}, \ldots, |t_n|^{\mathcal{I},\kappa}) \in P^{\mathcal{I}}$
   - $|\neg A|^{\mathcal{I},\kappa} = \neg |A|^{\mathcal{I},\kappa}$
     $|A \circ B|^{\mathcal{I},\kappa} = |A|^{\mathcal{I},\kappa} \circ |B|^{\mathcal{I},\kappa} \qquad \circ \in \{\wedge, \vee, \supset\}$
   - $|\forall x A|^{\mathcal{I},\kappa} = i$, ha $|A|^{\mathcal{I},\kappa^*} = i$ minden κ^* x variánsára
     $|\exists x A|^{\mathcal{I},\kappa} = i$, ha $|A|^{\mathcal{I},\kappa^*} = i$ legalább egy κ^* x variánsára

(κ^* a κ x-variánsa, ha $\kappa^*(y) = \kappa(y)$, ha $y \neq x$.)

III. Elsőrendű formulák szemantikus tulajdonságai

- Egy A elsőrendű logikai formula *kielégíthető*, ha van az elsőrendű logika nyelvének olyan $\mathcal{I}$ interpretációja, és $\mathcal{I}$-ben olyan κ változókiértékelés, melyre $|A|^{\mathcal{I},\kappa} = i$, egyébként *kielégíthetetlen*.
- A *logikailag igaz*, ha minden $\mathcal{I}, \kappa$-ra, $|A|^{\mathcal{I},\kappa} = i$, ennek jelölése $\models A$.
- A és B elsőrendű logikai formulák *logikailag ekvivalensek*, ha ha minden $\mathcal{I}, \kappa$-ra, $|A|^{\mathcal{I},\kappa} = |B|^{\mathcal{I},\kappa}$. Jelölése $A \sim B$.
- *Quine-táblázat*: A prímkomponenseket ítéletváltozónak tekintő ítélettábla.
- Egy A elsőrendű logikai formula *tautologikusan igaz*, ha Quine-táblázatában A oszlopában csupa i áll. Jelölése $\models_0 A$.

IV. Elsőrendű logikai törvények

- ha $x \notin \text{Par}(A)$:
  $\forall x A \sim A$ és $\exists x A \sim A$,
- $\forall x \forall y A \sim \forall y \forall x A$ és $\exists x \exists y A \sim \exists y \exists x A$,
- $\neg \exists x A \sim \forall x \neg A$ és $\neg \forall x A \sim \exists x \neg A$,
- ha $x \notin \text{Par}(A)$:
  $A \wedge \forall x B \sim \forall x (A \wedge B)$ és $A \wedge \exists x B \sim \exists x (A \wedge B)$,
  $A \vee \forall x B \sim \forall x (A \vee B)$ és $A \vee \exists x B \sim \exists x (A \vee B)$,
  $A \supset \forall x B \sim \forall x (A \supset B)$ és $A \supset \exists x B \sim \exists x (A \supset B)$,
  $\forall x B \supset A \sim \exists x (B \supset A)$ és $\exists x B \supset A \sim \forall x (B \supset A)$,
- $\forall x A \wedge \forall x B \sim \forall x (A \wedge B)$ és $\exists x A \vee \exists x B \sim \exists x (A \vee B)$.

Függvények aszimptotikus növekedési üteme

I. Általános összefüggések

A. Definíciók

Legyenek $f, g : \mathbb{N} \to \mathbb{R}^+$ függvények, ahol $\mathbb{N}$ a természetes számok, $\mathbb{R}^+$ pedig a nemnegatív valós számok halmaza.

- f-nek g aszimptotikus felső korlátja (jelölése: $f(n) = O(g(n))$; ejtsd: $f(n) =$ nagyordó $g(n)$) ha létezik olyan $c > 0$ konstans és $N \in \mathbb{N}$ küszöbindex, hogy $f(n) \leq c \cdot g(n)$ minden $n \geq N$-re.
- f-nek g aszimptotikus alsó korlátja (jelölése: $f(n) = \Omega(g(n))$) ha létezik olyan $c > 0$ konstans és $N \in \mathbb{N}$ küszöbindex, hogy $f(n) \geq c \cdot g(n)$ minden $n \geq N$-re.
- f-nek g aszimptotikus éles korlátja (jelölése: $f(n) = \Theta(g(n))$) ha léteznek olyan $c_1, c_2 > 0$ konstansok és $N \in \mathbb{N}$ küszöbindex, hogy $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$ minden $n \geq N$-re.

A definíció $f : \mathbb{N} \to \mathbb{R}$ függvényekre is kiterjeszthető, ekkor tekintsük f helyett a $\max\{f, 0\}$ függvényt.

B. Tulajdonságok

O, Ω, Θ 2-aritású relációnak is felfogható a $\mathbb{N} \to \mathbb{R}^+$ függvények univerzumán, pl. $f = O(g)$-ra $O(f, g)$ relációként gondolhatunk (de ilyet általában nem írunk). Az alábbiakban néha így gondolunk rájuk.

1. O, Ω, Θ tranzitív (pl. $f = O(g),\ g = O(h) \ \Rightarrow \ f = O(h)$)
2. O, Ω, Θ reflexív
3. Θ szimmetrikus
4. O, Ω fordítottan szimmetrikus ($f = O(g) \ \Leftrightarrow g = \Omega(f)$)
5. (köv.) Θ ekvivalenciareláció, a $\mathbb{N} \to \mathbb{R}^+$ függvények egy osztályozását adja. Az egyes függvényosztályokat általában "legegyszerűbb" tagjukkal reprezentáljuk. Pl. 1 (korlátos függvények), n (lineáris függvények), n^2 (négyzetes függvények).
6. $f, g = O(h) \ \Rightarrow \ f + g = O(h)$, hasonlóan Ω-ra, Θ-ra. (Összeadásra való zártság)
7. Legyen $c > 0$ konstans $f = O(g) \ \Rightarrow \ c \cdot f = O(g)$, hasonlóan Ω-ra, Θ-ra. (Pozitív konstanssal szorzásra való zártság)
8. $f + g = \Theta(\max\{f, g\})$ (szekvencia tétele). A domináns tag határozza meg egy összeg aszimptotikus nagyságrendjét.

C. Ha létezik az f/g határérték

- ha $f(n)/g(n) \to +\infty \quad \Rightarrow f(n) = \Omega(g(n))$ és $f(n) \neq O(g(n))$
- ha $f(n)/g(n) \to c \quad (c > 0) \Rightarrow f(n) = \Theta(g(n))$
- ha $f(n)/g(n) \to 0 \quad \Rightarrow f(n) = O(g(n))$ és $f(n) \neq \Omega(g(n))$

II. Konkrét függvények

- $p(n) = a_k n^k + \cdots + a_1 n + a_0$ ($a_k > 0$), ekkor $p(n) = \Theta(n^k)$,
- Minden $p(n)$ polinomra és $c > 1$ konstansra $p(n) = O(c^n)$, de $p(n) \neq \Omega(c^n)$,
- Minden $c > d > 1$ konstansokra $d^n = O(c^n)$, de $d^n \neq \Omega(c^n)$,
- Minden $a, b > 1$-re $\log_a n = \Theta(\log_b n)$,
- Minden $c > 0$ -ra $\log n = O(n^c)$, de $\log n \neq \Omega(n^c)$.

Eldönthetlenség

A. Definíciók

- Egy $L \subseteq \Sigma^*$ nyelv **Turing-felismerhető**, vagy **rekurzívan felsorolható** ha $L = L(M)$ valamely M Turing-gépre. A rekurzívan felsorolható nyelvek osztályát RE -vel jelüljük.
- Egy $L \subseteq \Sigma^*$ nyelv **eldönthető**, vagy **rekurzív** ha létezik olyan M Turing-gép, mely minden bemeneten megáll és $L = L(M)$. A rekurzív (eldönthető) nyelvek osztályát pedig R-rel jelöljük.
- Egy M Turing-gép **kódja** (jelölése $\langle M \rangle$): Ha $M = (Q, \{0,1\}, \Gamma, \delta, q_0, q_i, q_n)$, ahol $Q = \{p_1, \ldots, p_k\}, \Gamma = \{X_1, \ldots, X_m\}, D_1 = R, D_2 = L, D_3 = S$, akkor egy $\delta(p_i, X_j) = (p_r, X_s, D_t)$ átmenet kódja $0^i10^j10^r10^s10^t$. $\langle M \rangle$ az átmenetek kódjainak felsorolása 11-el elválasztva.
- $\langle M, w \rangle = \langle M \rangle 111 w$
- Néhány az előadáson tanult nevezetes nyelv:

  $L_{\text{átló}} = \{\langle M \rangle \mid \langle M \rangle \notin L(M)\}$.

  $L_u = \{\langle M, w \rangle \mid w \in L(M)\}$.

  $L_{\text{halt}} = \{\langle M, w \rangle \mid M \text{ megáll a } w \text{ bemeneten}\}$.

B. Tételek

- $L_{\text{átló}} \notin RE$
- $L_u \in RE, \;\; L_u \notin R$
- $L_{\text{halt}} \in RE, \;\; L_{\text{halt}} \notin R$
- Ha $L \in R$, akkor $\bar{L} \in R$.
- Ha $L \in RE$ és $\bar{L} \in RE$, akkor $L \in R$.

C. Visszavezetés

C1. Definíció

- $f : \Sigma^* \to \Delta^*$ **kiszámítható**, ha van olyan Turing-gép, ami kiszámítja. (lásd szófüggvényt kiszámító TG-ek)
- $L_1 \subseteq \Sigma^*$ **visszavezethető** $L_2 \subseteq \Delta^*$-ra, ha van olyan $f : \Sigma^* \to \Delta^*$ kiszámítható szófüggvény, hogy $w \in L_1 \Leftrightarrow f(w) \in L_2$. Jelölés: $L_1 \leq L_2$

C2. Tételek

- Ha $L_1 \leq L_2$ és $L_1 \notin RE$, akkor $L_2 \notin RE$.
- Ha $L_1 \leq L_2$ és $L_1 \notin R$, akkor $L_2 \notin R$.

D. Egy konkrét eldönthetetlen nyelv

Post megfelelkezési probléma: Legyen Σ egy véges abc. Post megfelelkezési problémájának egy bemenete egy (s,t) $(s,t \in \Sigma^*)$ alakú rendezett párokból álló véges H halmaz. A megfelelkezési feladat egy H bemenetét megoldhatónak nevezzük, ha vannak olyan (nem feltétlenül különböző) H-beli $(s_1,t_1),(s_2,t_2),\ldots,(s_n,t_n)$ párok úgy, hogy $s_1s_2\ldots s_n = t_1t_2\ldots t_n$, Ilyenkor az $s_1s_2\ldots s_n$, vagy ami ugyanaz, a $t_1t_2\ldots t_n$ szót a H megoldásának nevezzük.

$L_D = \{\langle D \rangle \mid \text{a } D \text{ dominókészletnek van megoldása}\} \notin R$

Bonyolultságelmélet

I. Időbonyolultság

A. Determinisztikus és nemdeterminisztikus időbonyolultsági osztályok

- $\mathrm{TIME}(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ időigényű determinisztikus Turing-géppel$\}$
- $\mathrm{NTIME}(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ időigényű nemdeterminisztikus Turing-géppel$\}$
- $\mathrm{P} = \bigcup_{k\geq 1} \mathrm{TIME}(n^k)$.
- $\mathrm{NP} = \bigcup_{k\geq 1} \mathrm{NTIME}(n^k)$.
- Észrevétel: $\mathrm{P} \subseteq \mathrm{NP}$.
- Sejtés: $\mathrm{P} \neq \mathrm{NP}$ (sejtjük, hogy igaz, de bizonyítani nem tudjuk).

B. Visszavezetés polinom időben

B1. Definíció

- $f : \Sigma^* \to \Delta^*$ **polinom időben kiszámítható**, ha van olyan Turing-gép, ami polinom időben kiszámítja. (lásd szófüggvényt kiszámító TG-ek)
- $L_1 \subseteq \Sigma^*$ **polinom időben visszavezethető** $L_2 \subseteq \Delta^*$-ra, ha van olyan $f : \Sigma^* \to \Delta^*$ polinom időben kiszámítható szófüggvény, hogy $w \in L_1 \Leftrightarrow f(w) \in L_2$. Jelölés: $L_1 \leq_p L_2$.

B2. Tételek

- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{P}$, akkor $L_1 \in \mathrm{P}$.
- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{NP}$, akkor $L_1 \in \mathrm{NP}$.

C. NP-teljesség

C1. Definíció

Egy L probléma **NP-teljes**, ha NP-beli és minden NP-beli probléma polinom időben visszavezethető rá.

C2. Tételek

- Ha L NP-teljes és $L \in \mathrm{P}$ akkor P=NP.
- Ha L_1 NP-teljes, $L_2 \in \mathrm{NP}$ és $L_1 \leq_p L_2$ akkor L_2 NP-teljes.

C3. Logika gyorstalpaló

- A logika **ítéletlogika** (nulladrendű logika) nevű modelljében egy logikai formula **ítéletváltozók**ból és **logikai műveletek**ből (pl. tagadás ($\neg$, negáció), logikai és ($\wedge$, konjunkció), megengedő vagy ($\vee$, diszjunkció)) épül fel. Az ítéletváltozókat **igaz**ra vagy **hamis**ra értékelhetjük ki. Egy formula **igazságértéké**t az ítéletváltozók adott kiértékelése mellett a formula felépítésére vonatkozó rekurzió alapján kapjuk meg. Egy formula **kielégíthető**, ha van olyan kiértékelés, ami igazra értékeli ki.
- Tétel: Minden formulához van vele ekvivalens KNF.
- **Literál**: egy ítéletváltozó vagy egy negált ítéletváltozó. **Tag**: literálok (lehet 1 darab is) diszjukciója. **Konjunktív normálforma (KNF)**: Tagok (lehet 1 darab is) konjunkciója.
- Példa: $\varphi = (X \vee \neg Y) \wedge (\neg X \vee \neg Y \vee Z) \wedge \neg Z$ kielégíthető KNF, például ha mindhárom ítéletváltozó hamis, akkor φ igaz. $X \wedge (\neg X \vee \neg Y) \wedge Y$ kielégíthetetlen KNF.

C4. Egy NP-teljes nyelv

- Legyen $\textsc{Sat} = \{\langle\varphi\rangle \mid \varphi$ kielégíthető KNF$\}$, ahol $\langle\phi\rangle$ a ϕ formula valamilyen dekódolható kódja $\{0,1\}$ felett.
- Tétel (Cook): $\textsc{Sat}$ NP-teljes.

D. Nevezetes (előadáson ismertetett) NP-teljes nyelvek
($\langle\,\rangle$ mindig valamilyen kellően tömör dekódolható kódolást jelent $\{0,1\}$ felett, most nem a kódolásra fókuszálunk.)

- SAT=$\{\langle\varphi\rangle \mid \varphi$ kielégíthető KNF$\}$ (Cook tétel)
- 3SAT=$\{\langle\varphi\rangle \mid \varphi$ kielégíthető KNF és minden tagban pontosan 3 literál van$\}$
- 3SZÍNEZÉS=$\{\langle G\rangle \mid G$ 3-színezhető$\}$
  (egy gráf 3-színezhető, ha csúcsai 3 színnel színezhetők úgy, hogy a szomszédos csúcsok színei különbözőek)
- KLIKK=$\{\langle G\rangle \mid G$-nek van k méretű teljes részgráfja$\}$
  (G irányítatlan gráf; $k \in \mathbb{N}$ előre rögzített)
- FÜGGETLEN CSÚCSHALMAZ=$\{\langle G\rangle \mid G$-nek van k méretű üres részgráfja$\}$
  (G irányítatlan gráf; $k \in \mathbb{N}$ előre rögzített)
- CSÚCSLEFEDÉS=$\{\langle G\rangle \mid$ van k méretű részhalmaza $V(G)$-nek, ami az összes élt lefogja$\}$
  (G irányítatlan gráf; $k \in \mathbb{N}$ előre rögzített; egy $S \subseteq V(G)$ lefog egy E élt, ha $S \cap E \neq \emptyset$)
- HITTING SET=$\{\langle T\rangle \mid$ van olyan k méretű S halmaz, ami az összes T-beli halmazt lefogja$\}$
  (T halmazok halmaza; $k \in \mathbb{N}$ előre rögzített; egy S halmaz lefog egy X halmazt, ha $S \cap X \neq \emptyset$)
- HALMAZFEDÉS=$\{\langle U, T\rangle \mid$ van k darab T-beli halmaz, aminek uniója $U\}$
  (U egy halmaz; T U részhalmazainak egy halmaza; $k \in \mathbb{N}$ előre rögzített)
- HÚ=$\{\langle G\rangle \mid$ van a G irányított gráfban s-ből t-be Hamilton út$\}$
  (A Hamilton út olyan út, ami minden csúcsot bejár; s és t előre rögzítettek)
- IHÚ=$\{\langle G\rangle \mid$ van a G irányítatlan gráfban s-ből t-be Hamilton út$\}$
  (s és t előre rögzítettek)
- IHK=$\{\langle G\rangle \mid$ van a G irányítatlan gráfban Hamilton kör$\}$
- UTAZÓÜGYNÖK=$\{\langle G\rangle \mid$ van-e a G-ben legfeljebb k súlyú Hamilton kör$\}$
  (G pozitív egészekkel élsúlyozott irányítatlan gráf; $k \in \mathbb{N}$ előre rögzített)

II. Tárbonyolultság

E. A tárbonyolultság mértékegysége

A tárbonyultság vizsgálatához ún. **off-line Turing-gép**eket használunk. Az első szalag a bemeneti szalag, ezt csak olvashatja, az utolsó szalag a kimeneti szalag, erre csak írhat. A Turing-gép **tárigénye** a többi szalagon (ún. munkaszalagokon) felhasznált cellák száma. Egy Turing-gép $f(n)$ **tárkorlátos**, ha bármely u inputra legfeljebb $f(|u|)$ tárat használ.

F. Determinisztikus és nemdeterminisztikus tárbonyolultsági osztályok

- $\mathrm{SPACE}\,(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ tárkorlátos determinisztikus Turing-géppel$\}$
- $\mathrm{NSPACE}\,(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ tárkorlátos nemdeterminisztikus Turing-géppel$\}$
- PSPACE=$\bigcup_{k\geq 1}\mathrm{SPACE}\,(n^k)$.
- NPSPACE=$\bigcup_{k\geq 1}\mathrm{NSPACE}\,(n^k)$.
- NL=$\mathrm{NSPACE}\,(\log n)$.

G. Savitch tétele és következményei

- (Savitch tétele) Ha $f(n) \geq \log n$, akkor $\mathrm{NSPACE}\,(f(n)) \subseteq \mathrm{SPACE}\,(f^2(n))$
- PSPACE=NPSPACE
- $\mathrm{NL} \subseteq \mathrm{SPACE}\,(\log^2 n)$

(Determinisztikus) Turing-gépek

- A **Turing-gép** egy olyan $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendszer, ahol
  - Q az állapotok véges, nemüres 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 szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \setminus \Sigma$.
  - $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \to Q \times \Gamma \times \{L, R, S\}$ az átmenet függvény.
- A Turing-gép működésének fázisait a gép konfigurációival írjuk le. A Turing-gép **konfigurációja** egy uqv szó, ahol $q \in Q$ és $u, v \in \Gamma^*, v \neq \varepsilon$.

  A konfiguráció a gép 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 a gép író-olvasó feje a v szó első betűjén áll.
- A gép **kezdőkonfigurációja** egy olyan q_0u szó, ahol u csak Σ-beli betűket tartalmaz.
- Egy Turing-gép **konfigurációátmenetét** az alábbiak szerint definiáljuk. Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$, $u, v \in \Gamma^*$.
  - Ha $\delta(q, a) = (r, b, R)$, akkor $uqav \vdash ubrv'$, ahol $v' = v$, ha $v \neq \varepsilon$, különben $v' = \sqcup$,
  - ha $\delta(q, a) = (r, b, S)$, akkor $uqav \vdash urbv$,
  - ha $\delta(q, a) = (r, b, L)$, akkor $uqav \vdash u'rcbv$, ahol $c \in \Gamma$ és $u'c = u$, ha $u \neq \varepsilon$, különben $u' = u$ és $c = \sqcup$.
- Azt mondjuk, hogy M **véges sok lépésben eljut** a C konfigurációból a C' konfigurációba (jele $C \vdash^* C'$), ha van olyan $n \geq 1$ és $C_1, \ldots, C_n$ konfigurációsorozat, hogy $C_1 = C, C_n = C'$ és minden $1 \leq i < n$-re, $C_i \vdash C_{i+1}$.
- Ha $q \in \{q_i, q_n\}$, akkor azt mondjuk, hogy az uqv konfiguráció egy **megállási konfiguráció**. $q = q_i$ esetében **elfogadó**, míg $q = q_n$ esetében **elutasító konfigurációról** beszélünk.
- Az M által **felismert nyelv** (amit $L(M)$-mel jelölünk) azoknak az $u \in \Sigma^*$ szavaknak a halmaza, melyekre igaz, hogy $q_0u \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ szavakra.
- Egy $L \subseteq \Sigma^*$ nyelv **Turing-felismerhető**, ha $L = L(M)$ valamely M

  Turing-gépre. Továbbá, egy $L \subseteq \Sigma^*$ nyelv **eldönthető**, ha létezik olyan M

  Turing-gép, 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. A rekurzívan felsorolható nyelvek osztályát RE -vel, a rekurzív nyelvek osztályát pedig R-rel jelöljük.
- Tekintsünk egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ Turing-gépet és annak egy $u \in \Sigma^*$ bemenő szavát. Azt mondjuk, hogy M **futási ideje (időigénye)** az u szón n ($n \geq 0$), ha M a q_0u kezdőkonfigurációból n lépésben (konfigurációátmenettel) jut el megállási konfigurációba. Ha nincs ilyen szám, akkor M futási ideje az u-n végtelen.
- Legyen $f : \mathbb{N} \to \mathbb{N}$ egy függvény. Azt mondjuk, hogy M **időigénye** $f(n)$ (vagy, hogy M egy $f(n)$ időkorlátos gép), ha minden $u \in \Sigma^*$ input szóra, M időigénye az u szón legfeljebb $f(|u|)$.
- A **k-szalagos Turing-gép** egy olyan $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendszer, ahol
  - Q az állapotok véges, nemüres 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 szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \setminus \Sigma$,
  - $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, R, S\}^k$ az átmenet függvény.
- A k szalagos Turing-gép **konfigurációja** egy $\begin{matrix} u_1 & & v_1 \\ \vdots & q & \vdots \\ u_k & & v_k \end{matrix}$ szó, ahol $q \in Q$ és $u_i, v_i \in \Gamma^*, v_i \neq \varepsilon$ $(1 \leq i \leq k)$. Az u szóhoz tartozó **kezdőkonfiguráció:** $u_i = \varepsilon$ $(1 \leq i \leq k)$, $v_1 = u$, és $v_i = \sqcup$ $(2 \leq i \leq k)$. Időigény: mint az egyszalagosnál (konfigurációátmenetek száma alapján).
- **Szófüggvényt kiszámító Turing-gép**:

  Az M (determinisztikus) Turing-gép kiszámítja az $f : \Sigma^* \to \Gamma^*$ szófüggvényt, ha M minden $u \in \Sigma^*$-ra olyan vqw megállási konfigurációba jut ($q \in \{q_i, q_n\}$), ahol $vw = f(u)$ (szóeleji és szóvégi $\sqcup$-ektől eltekintve). Időigény: mint fent (konfigurációátmenetek száma alapján).