# Számelmélet összefoglaló

Monday, December 11, 2023 10:34 PM

**Definíció**

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

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

**konjukció** $(\wedge)$ **diszjunkció** $(\vee)$

**Definíció**

Egy $I : \mathrm{Var}(\varphi) \rightarrow \{i, h\}$ függvényt $\varphi$ egy **interpretációjának** (változókiértékelésének) nevezünk.

Ha $\mathcal{F}$ egy formulahalmaz, akkor egy $I : \mathrm{Var}(\mathcal{F}) \rightarrow \{i, h\}$ függvényt $\mathcal{F}$ egy **interpretációjának** (változókiértékelésének) nevezünk.

# A formulák igazságértéke

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

### Definíció

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

ahol a műveletek eredményét az alábbi táblázat definiálja.

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

### Definíció

Egy $\varphi$ ítéletlogikai formula **ítélettáblája** egy $2^n \times (n+1)$-es táblázat, ahol $n = |\text{Var}(\varphi)|$. A sorok megfelelnek a lehetséges interpretációknak. Az $I$ interpretációnak megfelelő sor az első $n$ oszlopban tartalmazza az ítéletváltozók $I$ szerinti kiértékelését, míg utolsó, $n+1$. oszlopa $\mathcal{B}_I(\varphi)$-t.

## Definíció

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

## Állítás

Legyen $\varphi$ egy formula és $\varphi_0$ egy részformulája. Tegyük fel, hogy $\varphi_0 \sim_0 \psi_0$ valamely $\psi_0$ formulára és legyen $\psi$ az a formula, amit $\varphi$-ból úgy kapunk, hogy a $\varphi_0$ részformulát $\psi_0$-val helyettesítjük. (Például $\varphi$ szerkezeti fájában az $\varphi_0$-nak megfelelő részfát $\psi_0$ szerkezeti fájával helyettesítjük.) Ekkor $\varphi \sim_0 \psi$.

## Definíció

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

## Tétel

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

- $\varphi$ akkor és csak akkor kielégíthetetlen, ha $\neg\varphi$ tautológia.

### Tétel

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

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

### Definíció

- **Literálnak** nevezünk egy $x$ vagy $\neg x$ alakú formulát, ahol $x \in \mathrm{Var}$. $x$ és $\neg x$ **komplemens literálpár**. Egy literál **alapja** az az ítéletváltozó, amelyik a literálban szerepel.
- **Elemi diszjunkciónak** (vagy röviden **klóznak**) hívunk egy $\ell_1 \vee \cdots \vee \ell_n$ alakú formulát ($n \in \mathbb{N}$), ahol $\ell_1, \ldots \ell_n$ páronként különböző alapú literálok.
- **Konjunktív normálformának** (röviden KNF-nek) nevezünk egy $C_1 \wedge C_2 \wedge \ldots \wedge C_m$ $(m \geqslant 1)$ alakú formulát, ahol minden $1 \leqslant i \leqslant m$-re $C_i$ egy klóz (a KNF egy **tagja**).
- Az **elemi konjunkciót** és a **diszjunktív normálformát** (DNF) ezzel analóg módon definiáljuk $\wedge$ és $\vee$ szerepének felcserélésével.

### Tétel

Minden $\varphi$ ítéletkalkulusbeli formulához megadható egy vele tautologikusan ekvivalens DNF.

### Tétel

Minden $\varphi$ ítéletkalkulusbeli formulához megadható egy vele tautologikusan ekvivalens KNF.

Tehát DNF:
$(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge z) \vee (\neg x \wedge \neg y \wedge z)$.

KNF: $(\neg x \vee \neg y \vee z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y \vee z)$.

## Rezolvens

Legyenek $C_1$ és $C_2$ pontosan 1 komplemens literálpárt tartalmazó klózok. Tehát $C_1 = C_1' \vee \ell_1$, $C_2 = C_2' \vee \ell_2$, ahol $\ell_1$ és $\ell_2$ komplemens literálpár, $C_1'$ és $C_2'$ viszont nem tartalmaz ilyet. A $\mathrm{res}(C_1, C_2) := C_1' \vee C_2'$ klózt (esetleges egyszerűsítés után) a $(C_1, C_2)$ klózpár rezolvensének nevezzük. (Ha $C_1 = \ell_1$, $C_2 = \ell_2$, akkor $\mathrm{res}(C_1, C_2) = \square$.)

## Rezolúciós levezetés

Egy $\mathcal{S}$ klózhalmazból a $C$ klóz rezolúciós levezetése egy olyan véges $K_1, K_2, \ldots, K_m$ $(m \geqslant 1)$ klózsorozat, ahol minden $j = 1, 2, \ldots, m$-re:

- vagy $K_j \in \mathcal{S}$,
- vagy van olyan $1 \leqslant s, t < j$, hogy $K_j = \mathrm{res}(K_s, K_t)$,

és $K_m = C$.

## Tétel

$\mathcal{S}$ klózhalmaz kielégíthetetlen $\Longleftrightarrow$ $\mathcal{S}$-ből levezethető $\square$.

## Lemma

Minden $C_1, C_2$ klózra és $I$ interpretációjukra igaz, hogy ha $I \models_0 \{C_1, C_2\}$, akkor $I \models_0 \mathrm{res}(C_1, C_2)$.

## Definíció

Egy elsőrendű logika szimbólumhalmaza a következőkből áll

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

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

## Definíció

### Definíció

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

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

### Definíció

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

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

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

### Definíció

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

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

### Definíció

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

### Definíció

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

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

### Definíció

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

### Definíció

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

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

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

### Definíció

Legyen $\varphi$ egy formula, és tekintsük $x \in \text{Ind}$ egy előfordulását $\varphi$-ben. (A kvantorokat közvetlenül követő változókat nem tekintjük ezen változó előfordulásának.) Azt mondjuk, hogy $x$ ezen előfordulása **kötött**, ha $x$ a $\varphi$ egy $\exists x\psi$ vagy $\forall x\psi$ alakú részformulájába esik. Ellenkező esetben $x$ ezen előfordulása **szabad**. Ha $\varphi$ minden individuumváltozójának minden előfordulása kötött, akkor **zárt** formuláról beszélünk. Egyébként a kormula **nyitott**.

### Definíció

- Egy $\varphi$ elsőrendű logikai formula **kielégíthető**, ha van olyan $I$ interpretáció és $\kappa$ változókiértékelés, amelyre $|\varphi|^{I,\kappa} = i$, egyébként **kielégíthetetlen**.
- $\varphi$ **logikailag igaz** (vagy **érvényes**), ha minden $I$, $\kappa$-ra

### Definíció

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

### Church-Turing tézis

Minden formalizálható probléma, ami megoldható algoritmussal, az megoldható Turing géppel is.

### Definíció

A **Turing gép** (továbbiakban sokszor röviden TG) egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendezett hetes , 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,
- $\Sigma$ és $\Gamma$ ábécék, a bemenő jelek illetve a szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \setminus \Sigma$.
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \to Q \times \Gamma \times \{L, S, R\}$ az átmenet függvény. $\delta$ az egész $(Q \setminus \{q_i, q_n\}) \times \Gamma$-n értelmezett függvény.

### Definíció

Az $uqv$ szó az $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ Turing gép egy **konfigurációja** ha $q \in Q$, $u, v \in \Gamma^*$ és $v \neq \varepsilon$.

### Definíció

Egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ Turing gép $\vdash \subseteq C_M \times C_M$ **egylépéses konfigurációátmenet** relációját 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 $c = \sqcup$.

### Definíció

A $\vdash^* \subseteq C_M \times C_M$ **többlépéses konfigurációátmenet** relációját a következőképpen definiáljuk: $C \vdash^* C' \Leftrightarrow$

- ha $C = C'$ vagy
- ha $\exists\, n > 0 \wedge C_1, C_2, \dots C_n \in C_M$, hogy $\forall\, 1 \leqslant i \leqslant n-1$-re $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

### Az $M$ TG által felismert nyelv

$L(M) = \{u \in \Sigma^* \mid q_0 u \sqcup \vdash^* x q_i y$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ -ra$\}$.

### Definíció

Egy $L \subseteq \Sigma^*$ nyelv **Turing-felismerhető**, ha $L = L(M)$ valamely $M$ TG-re.

### Definíció

Egy $L \subseteq \Sigma^*$ nyelv **eldönthető**, ha létezik olyan $M$ TG, mely minden bemeneten megállási konfigurációba jut és $L(M) = L$.

### Definíció

RE=$\{L \mid \exists\, M$ Turing gép, amelyre $L(M) = L\}$.

R=$\{L \mid \exists\, M$ minden inputra megálló Turing gép, melyre $L(M) = L\}$.

### Definíció

Egy $M$ TG **futási ideje** (időigénye) az $u$ szóra $t$ ($t \geqslant 0$), ha $M$ az $u$-hoz tartozó kezdőkonfigurációból $t$ lépésben (konfigurációátmenettel) jut el megállási konfigurációba. Ha nincs ilyen szám, akkor $M$ futási ideje az $u$ szóra végtelen.

### Definíció

Legyen $f : \mathbb{N} \to \mathbb{N}$ egy függvény. Azt mondjuk, hogy $M$ egy $\boldsymbol{f(n)}$ **időkorlátos** gép (vagy $M$ $f(n)$ időigényű), ha minden $u \in \Sigma^*$ input szóra $M$ futási ideje az $u$ szón legfeljebb $f(|u|)$.

### Definíció

Adott egy $k \geqslant 1$ egész szám. A $\boldsymbol{k}$**-szalagos Turing gép** egy olyan $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendezett hetes, 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,
- $\Sigma$ és $\Gamma$ ábécék, a bemenő jelek illetve a szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \backslash \Sigma$,
- $\delta : (Q \backslash \{q_i, q_n\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, S, R\}^k$ az átmenet függvény.

$\delta$ az egész $(Q \backslash \{q_i, q_n\}) \times \Gamma^k$-n értelmezett függvény.

### Definíció

$k$-szalagos TG **konfigurációja** egy $(q, u_1, v_1, \ldots, u_k, v_k)$ szó, ahol $q \in Q$ és $u_i, v_i \in \Gamma^*, v_i \neq \varepsilon$ $(1 \leqslant i \leqslant k)$.

### Definíció

Az $u$ szóhoz tartozó **kezdőkonfiguráció**: $(q_0, u_1, v_1, \ldots, u_k, v_k)$, ahol $u_i = \varepsilon$ $(1 \leqslant i \leqslant k)$, $v_1 = u\sqcup$, és $v_i = \sqcup$ $(2 \leqslant i \leqslant k)$.

### Definíció

A $(q, u_1, v_1, \ldots, u_k, v_k)$ konfiguráció, ahol $q \in Q$ és $u_i, v_i \in \Gamma^*$, $v_i \neq \varepsilon$ $(1 \leqslant i \leqslant k)$,

- **elfogadó konfiguráció**, ha $q = q_i$,
- **elutasító konfiguráció**, ha $q = q_n$,
- **megállási konfiguráció**, ha $q = q_i$ vagy $q = q_n$.

### Definíció

### Definíció

Egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ $k$-szalagos Turing gép $\vdash \subseteq C_M \times C_M$ **egylépéses konfigurációátmenet** relációját az alábbiak szerint definiáljuk.

Legyen $C = (q, u_1, a_1 v_1, \ldots, u_k, a_k v_k)$ egy konfiguráció, ahol $a_i \in \Gamma$, $u_i, v_i \in \Gamma^*$ $(1 \leqslant i \leqslant k)$. Legyen továbbá $\delta(q, a_1, \ldots, a_k) = (r, b_1, \ldots, b_k, D_1, \ldots, D_k)$, ahol $q, r \in Q$, $b_i \in \Gamma, D_i \in \{L, S, R\}$ $(1 \leqslant i \leqslant k)$. Ekkor $C \vdash (r, u_1', v_1', \ldots, u_k', v_k')$, ahol minden $1 \leqslant i \leqslant k$-ra

- ha $D_i = R$, akkor $u_i' = u_i b_i$ és $v_i' = v_i$ , ha $v_i \neq \varepsilon$, különben $v_i' = \sqcup$,
- ha $D_i = S$, akkor $u_i' = u_i$ és $v_i' = b_i v_i$ ,
- ha $D_i = L$, akkor $u_i = u_i' c$ $(c \in \Gamma)$ és $v_i' = c b_i v_i$ ha $u_i \neq \varepsilon$, különben $u_i' = \varepsilon$ és $v_i' = \sqcup b_i v_i$.

### Definíció

A $k$-szalagos TG-ek **többlépéses konfigurációátmenet** relációját ugyanúgy definiáljuk, mint az egyszalagos esetben, az egylépéses konfigurációátmenet reláció reflexív, tranzitív lezártjaként.
Jelölés: $\vdash^*$.

### Definíció

Az $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ $k$-szalagos TG által **felismert nyelv**:
$L(M) = \{ u \in \Sigma^* \mid (q_0, \varepsilon, u\sqcup, \varepsilon, \sqcup, \ldots, \varepsilon, \sqcup) \vdash^* (q_i, x_1, y_1, \ldots x_k, y_k),$ valamely $x_1, y_1 \ldots, x_k, y_k \in \Gamma^*, y_1, \ldots, , y_k \neq \varepsilon$ -ra$\}$.

### Definíció

Egy $k$-szalagos Turing gép **futási ideje** egy $u$ szóra a hozzá tartozó kezdőkonfigurációból egy megállási konfigurációba megtett lépések száma.

Az **időigény** ($f(n)$ időkorlátos TG) definíciója megegyezik az egyszalagos esetnél tárgyalttal.

### Definíció

Két TG **ekvivalens**, ha ugyanazt a nyelvet ismerik fel.

### Tétel

Minden $M$ $k$-szalagos Turing géphez megadható egy vele ekvivalens $M'$ egyszalagos Turing gép. Továbbá, ha $M$ legalább lineáris időigényű $f(n)$ időkorlátos gép (azaz $f(n) = \Omega(n)$), akkor $M'$ $O(f(n)^2)$ időkorlátos.

### Tétel

Minden egyszalagos $M$ Turing géphez van vele ekvivalens egy irányban végtelen szalagos $M''$ Turing gép.

### Nemdeterminisztikus Turing gép (NTG)

Az egyszalagos **nemdeterminisztikus Turing gép** (továbbiakban röviden NTG) egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendezett hetes, 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,
- $\Sigma$ és $\Gamma$ ábécék, a bemenő jelek illetve a szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \backslash \Sigma$,
- $\delta : (Q \backslash \{q_i, q_n\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, S, R\})$.

### Definíció

Egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ egyszalagos nemdeterminisztikus Turing gép $\vdash \subseteq C_M \times C_M$ **egylépéses konfigurációátmenet** relációját az alábbiak szerint definiáljuk.

Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$, $u, v \in \Gamma^*$ .

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

### Definíció

A $\vdash^* \subseteq C_M \times C_M$ **többlépéses konfigurációátmenet** relációját a következőképpen definiáljuk: $C \vdash^* C' \Leftrightarrow$

- ha $C = C'$ vagy
- ha $\exists\, n > 0 \wedge C_1, C_2, \dots C_n \in C_M$, hogy $\forall\, 1 \leqslant i \leqslant n-1$-re $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

### Definíció

A $\vdash^* \subseteq C_M \times C_M$ **többlépéses konfigurációátmenet** relációját a következőképpen definiáljuk: $C \vdash^* C' \Leftrightarrow$

- ha $C = C'$ vagy
- ha $\exists\, n > 0 \wedge C_1, C_2, \ldots C_n \in C_M$, hogy $\forall\, 1 \leqslant i \leqslant n-1$-re $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

### Definíció

Az $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ nemdeterminisztikus Turing gép által **felismert nyelv**
$L(M) = \{u \in \Sigma^* \mid q_0u\sqcup \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon$ -ra$\}$.

### Definíció

Egy $M$ TG egy $u \in \Sigma^*$ inputjához tartozó **nemdeterminisztikus számítási fa** egy gyökeres fa, melynek csúcsai $M$ konfigurációival címkézettek. $q_0u\sqcup$ a gyökér címkéje. Ha $C$ egy csúcs címkéje, akkor $|\{C' \mid C \vdash C'\}|$ gyereke van és ezek címkéi éppen $\{C' \mid C \vdash C'\}$ elemei.

### Definíció

Az $M$ NTG **felismeri** az $L \subseteq \Sigma^*$ nyelvet, ha $L(M) = L$.

Az $M$ NTG **eldönti** az $L \subseteq \Sigma^*$ nyelvet, ha felismeri továbbá minden $u \in \Sigma^*$ input szóhoz tartozó nemdeterminisztikus számítási fa véges és a fa minden levele elfogadó vagy elutasító konfiguráció.

### Definíció

Az $M$ NTG $\boldsymbol{f(n)}$ **időkorlátos** (időigényű), ha minden $u \in \Sigma^*$ $n$ hosszú szóra $u$ számítási fája legfeljebb $f(n)$ magas.

### Definíció

Legyen $X = \{x_1 < x_2 < \cdots < x_s\}$ egy rendezett ábécé. Ekkor $X^*$ szavainak **hossz-lexikografikus** (shortlex) rendezése alatt azt a $\prec_{\text{shortlex}}$ rendezést értjük, melyre a következők teljesülnek. Minden $u_1 \cdots u_n, v_1 \cdots v_m \in X^*$-ra
$u_1 \cdots u_n \prec_{\text{shortlex}} v_1 \cdots v_m \Leftrightarrow (n < m) \vee$
$((n = m) \wedge (u_k < v_k)$, ahol $k$ a legkisebb olyan $i$, melyre $u_i \neq v_i)$.

## Tétel

Minden $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ $f(n)$ időkorlátos NTG-hez megadható egy ekvivalens, $2^{O(f(n))}$ időkorlátos $M'$ determinisztikus TG.

## Definíció

- $A$ és $B$ halmazoknak **megegyezik a számosságuk**, ha $\exists$ bijekció köztük. Jelölése: $|A| = |B|$.
- $A$-nak **legalább annyi a számossága**, mint $B$-nek, ha $\exists$ $B$-ből injekció $A$-ba. Jelölése: $|A| \geqslant |B|$.
- $A$-nak **nagyobb a számossága, mint $B$-nek**, ha $\exists$ $B$-ből $A$-ba injekció, de $\nexists$ bijeckió. Jelölése: $|A| > |B|$.

## Cantor-Bernstein-Schröder tétel

Ha $\exists$ injekció $A$-ból $B$-be és $B$-ből $A$-ba is, akkor $\exists$ bijekció $A$ és $B$ között, azaz ha $|A| \leqslant |B|$ és $|A| \geqslant |B|$, akkor $|A| = |B|$.

## Definíció

Egy $A$ halmaz **megszámlálhatóan végtelen számosságú**, ha létezik $A$ és $\mathbb{N}$ között bijekció.

## Definíció

Egy $A$ halmaz **continuum számosságú**, ha létezik $A$ és $\mathbb{R}$ között bijekció.

## Tétel

$|\mathbb{R}| > |\mathbb{N}|$

## Következmény

A $\{0, 1\}$ feletti nyelvek halmazának számossága nagyobb, mint a $\{0, 1\}$ feletti szavak számossága.

## Tétel

Minden $H$ halmazra $|\mathcal{P}(H)| > |H|$.

## Következmény

Minden számosságnál van nagyobb számosság, tehát végtelen sok számosság van.

### Definíció

Egy $M$ Turing-gép **kódja** (jelölése $\langle M \rangle$) a következő:
Legyen $M = (Q, \{0,1\}, \Gamma, \delta, q_0, q_i, q_n)$, ahol

- $Q = \{p_1, \ldots, p_k\}$, $\Gamma = \{X_1, \ldots, X_m\}$, $D_1 = R$, $D_2 = S$, $D_3 = L$
- $k \geqslant 3$, $p_1 = q_0$, $p_{k-1} = q_i$, $p_k = q_n$,
- $m \geqslant 3$, $X_1 = 0$, $X_2 = 1$, $X_3 = \sqcup$.
- 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.

### Tétel

Létezik nem Turing-felismerhető nyelv.

### Tétel

$L_{\text{átló}} := \{w_i \mid w_i \notin L(M_i)\} \notin RE$.

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

### Tétel

$L_u \in RE$

### Tétel

$L_u \notin R$.

### Tétel

Ha $L$ és $\overline{L} \in RE$, akkor $L \in R$.

### Tétel

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

### Definíció

Azt mondjuk, hogy az $M = \langle Q, \Sigma, \Delta, \delta, q_0, q_i, (q_n) \rangle$ TG **kiszámítja** az $f : \Sigma^* \to \Delta^*$ szófüggvényt, ha minden $u \in \Sigma^*$-beli szóra megáll, és ekkor $f(u) \in \Delta^*$ olvasható az utolsó szalagján.

### Definíció

Az $f : \Sigma^* \to \Delta^*$ szófüggvény **kiszámítható**, ha van olyan Turing-gép, ami kiszámítja. [lásd szófüggvényt kiszámító TG]

### Definíció

$L_1 \subseteq \Sigma^*$ **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: $L_1 \leqslant L_2$

**Tétel**

- Ha $L_1 \leqslant L_2$ és $L_2 \in RE$, akkor $L_1 \in RE$.
- Ha $L_1 \leqslant L_2$ és $L_2 \in R$, akkor $L_1 \in R$.

$L_h = \{\langle M, w\rangle \mid M$ megáll a $w$ bemeneten$\}$ $L_u \subseteq L_h$

**Tétel**

$L_h \notin R$.

**Tétel**

$L_h \in RE$.

**Definíció**

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

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

**Rice tétele**

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

**Definíció**

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

**Definíció**

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

**Post Megfelelkezési Probléma (PMP):**

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

**Tétel**

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

**Tétel**

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

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

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

**Tétel**

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

**Tétel**

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

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

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

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

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

**Definíció**

$\textsc{ValidityPred} := \{\langle\varphi\rangle \mid \varphi$ logikailag igaz elsőrendű formula$\}$.
$\textsc{UnsatPred} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen elsőrendű formula$\}$.
$\textsc{SatPred} := \{\langle\varphi\rangle \mid \varphi$ kielégíthető elsőrendű formula$\}$.
$\textsc{EqivPred} := \{\langle\varphi, \psi\rangle \mid \varphi, \psi$ elsőrendű formulák, melyekre $\varphi \sim \psi\}$.
$\textsc{ConsPred} := \{\langle\mathcal{F}, \varphi\rangle \mid \mathcal{F}$ véges elsőrendű formulahalmaz, $\varphi$ elsőrendű formula, $\mathcal{F} \models \varphi\}$.

**Tétel**

$\textsc{ValidityPred} \notin \mathrm{R}$

**Következmény**

$\textsc{UnsatPred}$, $\textsc{SatPred}$, $\textsc{EquivPred}$, $\textsc{ConsPred} \notin \mathrm{R}$

**Tétel**

$\textsc{UnsatPred} \in \mathrm{RE}$.

**Következmény**

$\textsc{SatPred} \notin \mathrm{RE}$

**Tétel**

Minden $G$ grammatikához megadható egy $L(G)$-t felismerő NTG.

**Tétel**

Minden $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n\rangle$ determinisztikus TG-hez megadható egy $L(M)$-et generáló $G$ grammatika.

### Definíció

A **lineárisan korlátolt automata** (LKA) olyan **nemdeterminisztikus** TG, melynek $\Sigma$ bemeneti ábécéje két speciális szimbólumot tartalmaz $\rhd$-et (baloldali végejel/endmarker) és $\lhd$-et (jobboldali végejel/endmarkert). Ezen felül

- a bemenetek $\rhd(\Sigma \setminus \{\rhd, \lhd\})^* \lhd$-beliek,
- $\rhd$ és $\lhd$ nem írhatók felül
- $\rhd$-tól balra illetve $\lhd$-től jobbra nem állhat a fej.
- a fej kezdőpozíciója a $\rhd$ tartalmú cella jobb-szomszédja

### Tétel

(1) Minden $G$ 1-es típusú grammatikához megadható egy $A$ LKA, melyre $L(A) = L(G)$.

(2) Minden $A$ LKA-hoz megadható egy $G$ 1-es típusú grammatika, melyre $L(G) = L(A)$.

### Tétel

Ha $A$ LKA, akkor $L(A)$ eldönthető.

| | |
|---|---|
| $\mathcal{L}_3$ | 3-típusú grammatika<br>determinisztikus véges automata<br>nemdeterminisztikus véges automata<br>reguláris kifejezés |
| | determinisztikus veremautomata |
| $\mathcal{L}_2$ | 2-típusú grammatika<br>verematomata |
| $\mathcal{L}_1$ | 1-típusú grammatika<br>lineárisan korlátolt automata |
| R | minden inputra megálló Turing gép |
| RE<br>=<br>$\mathcal{L}_0$ | Turing gép<br>nemdeterminisztikus Turing gép<br>0-típusú grammatika |

### Tétel

$\mathcal{L}_1 \subset$ R.

### Definíció

- $\mathrm{TIME}\,(f(n)) =$
  $\{L \mid L$ eldönthető $O(f(n))$ időkorlátos determinisztikus TG-pel$\}$
- $\mathrm{NTIME}\,(f(n)) =$
  $\{L \mid L$ eldönthető $O(f(n))$ időkorlátos NTG-pel$\}$
- $\mathrm{P}=\bigcup_{k\geqslant 1}\mathrm{TIME}\,(n^k)$.
- $\mathrm{NP}=\bigcup_{k\geqslant 1}\mathrm{NTIME}\,(n^k)$.

### Definíció

Az $f:\Sigma^* \to \Delta^*$ szófüggvény **polinom időben kiszámítható**, ha van olyan polinom időkorlátos Turing gép, amelyik kiszámítja.

### Definíció

$L_1 \subseteq \Sigma^*$ **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: $L_1 \leqslant_p L_2$.

### Tétel

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

### Definíció

Legyen $\mathcal{C}$ egy bonyolultsági osztály. Egy $L$ nyelv **$\mathcal{C}$-nehéz** (a polinom idejű visszavezetésre nézve), ha minden $L' \in \mathcal{C}$ esetén $L' \leqslant_p L$.

### Definíció

Legyen $\mathcal{C}$ egy bonyolultsági osztály. Egy $L$ nyelv **$\mathcal{C}$-teljes**, ha $L \in \mathcal{C}$ és $L$ $\mathcal{C}$-nehéz.

### NP-teljes nyelv

Egy $L$ nyelv **NP-teljes** (a polinom idejű visszavezetésre nézve), ha

- $L \in \mathrm{NP}$
- $L$ NP-nehéz, azaz minden $L' \in \mathrm{NP}$ esetén $L' \leqslant_p L$.

### Tétel

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

**Definíció**

$\mathrm{SAT} := \{\langle\varphi\rangle \mid \varphi$ kielégíthető nulladrendű KNF$\}$

**Cook-Levin tétel**

SAT NP-teljes.

**Tétel**

Ha $L$ NP-teljes, $L \leqslant_p L'$ és $L' \in$ NP, akkor $L'$ NP-teljes.

**Definíció**

*k*KNF-nek nevezünk egy olyan KNF-t, ahol minden klóz pontosan $k$ darab páronként különböző alapú literál diszjunkciója.

**Példák** 4KNF:

$(\neg x_1 \vee x_3 \vee x_5 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_3 \vee x_4 \vee \neg x_6) \wedge (x_1 \vee x_2 \vee \neg x_4 \vee \neg x_6)$.

2KNF: $(\neg x_1 \vee x_3) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3)$.

**Definíció:**

$k\mathrm{SAT}=\{\langle\varphi\rangle \mid \varphi$ kielégíthető $k$KNF$\}$

**Tétel**

3SAT NP-teljes.

**Tétel**

$2\mathrm{SAT} \in \mathrm{P}$.

**Definíció**

**Horn formula**: olyan KNF, amelynek minden tagja legfeljebb egy pozitív (azaz negálatlan) literált tartalmaz.

**Definíció**

$\mathrm{HORNSAT}=\{\langle\varphi\rangle \mid \varphi$ kielégíthető Horn formula$\}$

**Tétel**

$\mathrm{HORNSAT} \in \mathrm{P}$.

**Definíció**

Legyen $k \geqslant 1$ egész szám. Egy (irányítatlan) gráf **$k$-színezhető**, ha kiszínezhetők a csúcsai $k$ színnel úgy, hogy bármely két szomszédos csúcsnak a színe különböző.

Formálisan: $G = (V, E)$ $k$-színezhető, ha $\exists\, f : V \to \{1, \dots, k\}$ leképezés, melyre $\forall x, y \in V : f(x) = f(y) \Rightarrow \{x, y\} \notin E$.

$k\textsc{Színezés}{:=}\{\langle G\rangle \mid G$ $k$-színezhető$\}$

**Tétel**

$3\textsc{Színezés}$ NP-teljes.

**Tétel**

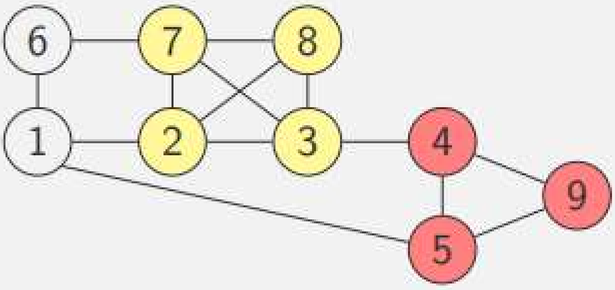
$2\textsc{Színezés} \in \mathrm{P}$


**Definíció**

Egy $G$ egyszerű, irányítatlan gráf egy teljes részgráfját **klikknek** nevezzük.

KLIKK:= $\{\langle G, k\rangle \mid G$-nek van $k$ méretű klikkje$\}$

**Példa:**



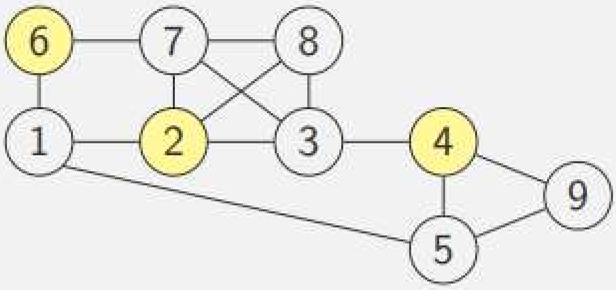

$\{2, 3, 7, 8\}$ és $\{4, 5, 9\}$ klikk. $\{1, 2, 6, 7\}$ nem klikk.

**Definíció**

Egy $G$ egyszerű, irányítatlan gráf egy üres részgráfját **független ponthalmaznak** mondjuk.

FÜGGETLEN PONTHALMAZ:=
$\{\langle G, k\rangle \mid G$-nek van $k$ méretű független ponthalmaza$\}$

**Példa:**




$\{2, 6, 4\}$ független. $\{1, 7, 3, 9\}$ nem független a $\{3, 7\}$ él miatt.

**Definíció**

Legyen $S \subseteq V(G)$ és $E \in E(G)$. Ha $S \cap E \neq \emptyset$, akkor a csúcshalmaz **lefogja** $E$-t. Ha $S$ minden $E \in E(G)$ élt lefog, akkor $S$ egy **lefogó ponthalmaz**.

**Megjegyzés:** A fenti fogalom **csúcsfedés** néven is ismeretes.

LEFOGÓ PONTHALMAZ:=

## Definíció

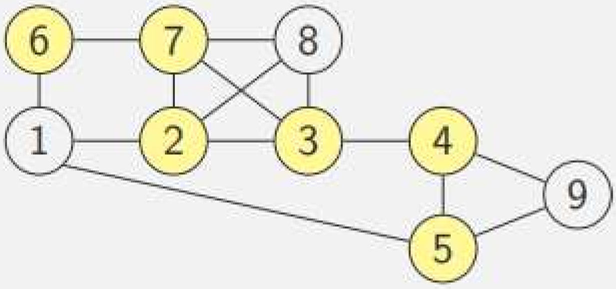
Legyen $S \subseteq V(G)$ és $E \in E(G)$. Ha $S \cap E \neq \emptyset$, akkor a csúcshalmaz **lefogja** $E$-t. Ha $S$ minden $E \in E(G)$ élt lefog, akkor $S$ egy **lefogó ponthalmaz**.

**Megjegyzés:** A fenti fogalom csúcsfedés néven is ismeretes.

LEFOGÓ PONTHALMAZ:=

$\{\langle G, k\rangle \mid G\text{-nek van } k \text{ méretű lefogó ponthalmaza}\}$

**Példa:**




$\{2, 3, 4, 5, 6, 7\}$ lefogó ponthalmaz.

## Tétel

KLIKK, FÜGGETLEN PONTHALMAZ, LEFOGÓ PONTHALMAZ NP-teljes.

## Definíció

$\mathcal{S}$ egy **hipergráf** (vagy halmazrendszer), ha $\mathcal{S} = \{A_1, \ldots, A_n\}$, ahol $A_i \subseteq U$, $(1 \leqslant i \leqslant n)$ valamely $U$ alaphalmazra. $H \subseteq U$ egy **hipergráf lefogó ponthalmaz**, ha $\forall 1 \leqslant i \leqslant n : H \cap A_i \neq \emptyset$.

HIPERGRÁF LEFOGÓ PONTHALMAZ:=

$\{\langle \mathcal{S}, k\rangle \mid \mathcal{S}$ egy hipergráf és van $k$ elemű $\mathcal{S}$-et lefogó ponthalmaz$\}$.

## Tétel

HIPERGRÁF LEFOGÓ PONTHALMAZ NP-teljes.

## Definíció

Adott egy $G$ gráf. Egy a $G$ összes csúcsát pontosan egyszer tartalmazó utat **Hamilton útnak**, egy a $G$ összes csúcsát pontosan egyszer tartalmazó kört **Hamilton körnek** nevezünk. Ha a gráf irányított, a Hamilton útnak/körnek irányítottnak kell lennie.

HÚ$=\{\langle G, s, t\rangle \mid$ van a $G$ irányított gráfban $s$-ből $t$-be H-út$\}$.

IHÚ$=\{\langle G, s, t\rangle \mid$ van a $G$ irányítatlan gráfban $s$ és $t$ végpontokkal H-út$\}$.

IHK$=\{\langle G\rangle \mid$ van a $G$ irányítatlan gráfban H-kör$\}$.

**Tétel**

HÚ NP-teljes

**Tétel**

IHÚ NP-teljes

**Tétel**

IHK NP-teljes

**Eldöntési verzió:**
TSP=$\{\langle G, K\rangle \mid G$-ben van $\leqslant K$ súlyú H-kör$\}$.

**Tétel**

TSP NP-teljes

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER=
$\{\langle \mathbf{A}, \mathbf{b}\rangle \mid \mathbf{Ax} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

**Tétel**

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER NP-nehéz.

RÉSZLETÖSSZEG:= $\{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van $S$-nek egy olyan $S'$ részhalmaza, hogy az $S'$-beli számok összege $K\}$.

**Példa:** $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in$RÉSZLETÖSSZEG, mivel 5+9+13=27.

**Tétel**

RÉSZLETÖSSZEG NP-teljes.

A HÁTIZSÁK nyelv olyan $a_1, \ldots, a_n, b, p_1, \ldots p_n, k$ rendezett $(2n+2)$-esekből áll, ahol ezen számok mindegyike nemnegatív és van egy olyan $I \subseteq \{1, \ldots n\}$ halmaz, amelyre $\sum_{i\in I} a_i \leqslant b$ és $\sum_{i\in I} p_i \geqslant k$.

**Tétel**

HÁTIZSÁK NP-teljes.

PARTÍCIÓ:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

**Példa:** A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

**Tétel**

PARTÍCIÓ NP-teljes.

LÁDAPAKOLÁS:=$\{\langle s_1, \ldots, s_n, k\rangle \mid s_i \in \mathbb{Q}^+ (1 \leqslant i \leqslant n)$ súlyok particionálhatók $k \in \mathbb{N}^+$ részre úgy, hogy minden partícióban a súlyok összege $\leqslant 1\}$.

### Tétel

LÁDAPAKOLÁS NP-teljes.

### Definíció

$L$ **NP-köztes**, ha $L \in$ NP, $L \notin$ P és $L$ nem NP-teljes.

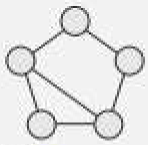
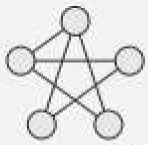
### Ladner tétele

Ha P $\neq$ NP, akkor létezik NP-köztes nyelv.

### Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

GRÁFIZOMORFIZMUS $= \{\langle G_1, G_2\rangle \mid$ $G_1$ és $G_2$ irányítatlan izomorf gráfok$\}$.

**Példa:**  és  izomorfak.

**Tétel:** GRÁFIZOMORFIZMUS $\in$ QP, ahol

$$\text{QP} = \bigcup_{c \in \mathbb{N}} \text{TIME}(2^{(\log n)^c})$$

a „kvázipolinom időben" megoldható problémák osztálya.

RÉSZGRÁFIZOMORFIZMUS $= \{\langle G_1, G_2\rangle \mid$ $G_1$ és $G_2$ irányítatlan gráfok és $G_1$ izomorf $G_2$ egy részgráfjával$\}$.

### Tétel

RÉSZGRÁFIZOMORFIZMUS NP-teljes.

PRÍMFAKTORIZÁCIÓ $=$
$\{\langle n, k\rangle \mid n$-nek van $k$-nál kisebb prímtényezője$\}$

### Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály $\text{co}\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

### Definíció

$\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

### Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor $\text{co}\mathcal{C}$ is.

### Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

P = coP  NP$\neq$coNP

### Tétel

$L$ $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ $\text{co}\mathcal{C}$-teljes.

$\textsc{Unsat} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \mid$ a $\varphi$ nulladrendű formula tautológia$\}$.

### Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

### Tétel

Ha $L$ coNP-teljes és $L \in$ NP, akkor NP = coNP.

### Definíció

Az offline Turing gép (OTG) egy olyan TG, melynek az első szalagja csak olvasható, a többi írható is. Első szalagját bemeneti szalagnak, további szalagjait munkaszalagoknak nevezzük.

### Tétel

Minden TG-hez megadható vele ekvivalens offline TG.

### Definíció

A nemdeterminisztikus offline Turing gép (NOTG) egy nemdeterminisztikusan működő offline Turing gép.

### Definíció

A **számító offline Turing gép** olyan legalább 2 szalagos számító Turing gép, amelynek az első szalagja csak olvasható, az utolsó szalagja csak írható. Az első szalagot bemeneti szalagnak, utolsó szalagot kimeneti szalagnak, a többi szalagot munkaszalagnak nevezzük.

### Definíció

Egy offline TG **többlet tárigénye** egy adott inputra azon celláknak a száma, amelyeken a működés során valamelyik munkaszalag feje járt.

Egy offline TG $f(n)$ **többlet tárkorlátos**, ha bármely $u$ inputra legfeljebb $f(|u|)$ a többlet tárigénye.

### Definíció

Egy nemdeterminisztikus offline TG **többlet tárigénye** egy adott inputra a legnagyobb többlet tárigényű számításának az többlet tárigénye.

Egy nemdeterminisztikus offline TG $f(n)$ **többlet tárkorlátos**, ha bármely $u$ inputra legfeljebb $f(|u|)$ az többlet tárigénye.

- $\text{SPACE}(f(n)) := \{L \mid L$ eldönthető $O(f(n))$ többlet tárkorlátos determinisztikus offline TG-pel$\}$
- $\text{NSPACE}(f(n)) := \{L \mid L$ eldönthető $O(f(n))$ többlet tárkorlátos nemdeterminisztikus offline TG-pel$\}$
- $\text{PSPACE}:=\bigcup_{k\geqslant 1}\text{SPACE}(n^k)$.
- $\text{NPSPACE}:=\bigcup_{k\geqslant 1}\text{NSPACE}(n^k)$.
- $\text{L}:=\text{SPACE}(\log n)$.
- $\text{NL}:=\text{NSPACE}(\log n)$.

$\text{ELÉR} = \{\langle G, s, t\rangle \mid$ A $G$ irányított gráfban van $s$-ből $t$-be út$\}$.

### Tétel

$\text{ELÉR} \in \text{TIME}(n^2)$.

### Tétel

$\text{ELÉR} \in \text{SPACE}(\log^2 n)$.

### Definíció

Egy $M$ NTG $G_M$ **konfigurációs gráfjának** csúcsai $M$ konfigurációi és $(C, C') \in E(G_M) \Leftrightarrow C \vdash_M C'$.

### Savitch tétele

Ha $f(n) \geqslant \log n$, akkor $\mathrm{NSPACE}(f(n)) \subseteq \mathrm{SPACE}(f^2(n))$.

### Következmény

PSPACE = NPSPACE

### Tétel

NL $\subseteq$ P

### Tétel

ELÉR $\in$ NL

### Definíció

Egy $L_1 \subseteq \Sigma^*$ nyelv **logaritmikus tárral visszavezethető** egy $L_2 \subseteq \Delta^*$ nyelvre, ha $L_1 \leqslant L_2$ és a visszavezetéshez használt függvény kiszámítható logaritmikus többlet tárkorlátos determinisztikus offline Turing géppel. Jelölése: $L_1 \leqslant_\ell L_2$.

### Definíció

Egy $L$ nyelv **NL-nehéz** (a log. táras visszavezetésre nézve), ha minden $L' \in$ NL nyelvre, $L' \leqslant_\ell L$. Ha ezen felül $L \in$ NL is teljesül, akkor $L$ **NL-teljes** (a log. táras visszavezetésre nézve)

### Tétel

Az L osztály zárt a logaritmikus tárral való visszavezetésre nézve.

### Tétel

ELÉR NL-teljes a logaritmikus tárral történő visszavezetésre nézve.

### Immerman-Szelepcsényi tétel

NL = coNL

EXPTIME:=$\bigcup_{k\in\mathbb{N}}\mathrm{TIME}(2^{n^k})$.

### Hierarchia tétel

(I) NL $\subset$ PSPACE és P $\subset$ EXPTIME.

(II) L $\subseteq$ NL=coNL $\subseteq$ P $\subseteq$ NP $\subseteq$ NPSPACE=PSPACE $\subseteq$ EXPTIME