Számításelmélet

Negyedik előadás

Bonyolultságelmélet – P és NP

- **Definíció:** Legyen $f: \mathbb{N} \to \mathbb{N}$ tetszőleges függvény
  - $\mathrm{TIME}\big(f(n)\big) \coloneqq \{L \mid L \text{ eldönthető } O\big(f(n)\big) \text{ időkorlátos det. Turing-géppel}\}$
  - $\mathrm{NTIME}\big(f(n)\big) \coloneqq \{L \mid L \text{ eldönthető } O\big(f(n)\big) \text{ időkorlátos nemdet. Turing-géppel}\}$
  - $\mathrm{P} = \bigcup_{k=1}^{\infty} \mathrm{TIME}(n^k)$
  - $\mathrm{NP} = \bigcup_{k=1}^{\infty} \mathrm{NTIME}(n^k)$
- **Megjegyzés:** $\mathrm{P} \subseteq \mathrm{NP}$
- **Sejtés:** $\mathrm{P} \subset \mathrm{NP}$
- **Megjegyzés:** P tartalmazza a gyakorlatban is hatékonyan megoldható problémákat
- Milyen problémák vannak NP-ben?

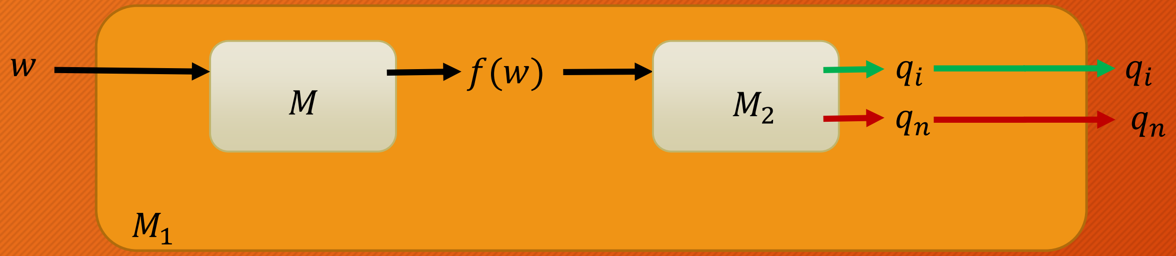
Bonyolultságelmélet – P és NP

- Minden L NP-beli problémára a következő jellemző:
  - Létezik egy polinom idejű nemdeterminisztikus Turin-gép ami
  - L minden I bemenetére „megsejti” (azaz nemdeterminisztikusan generálja) I egy **lehetséges m megoldását** és
  - **polinom időben leellenőrzi** (determinisztikusan), hogy m valóban megoldása-e I-nek
- **Definíció:** Azt mondjuk, hogy egy L nyelv **polinom időben verifikálható,** ha van olyan $K \in \mathrm{P}$ nyelv és k szám, hogy
$$L = \{x \mid \exists y \, (x, y) \in K \text{ és } |y| = O(|x|^k)\}$$
- **Tétel:** Egy nyelv akkor és csak akkor NP-beli, ha polinom időben verifikálható

Bonyolultságelmélet – P és NP

- Milyen visszavezetésre van szükség az NP-n belül?
- Olyanra, ami feltehetőleg nem elég erős, hogy minden NP-beli problémát megoldjon
- **Definíció:** Egy $L_1 \subseteq \Sigma^*$ **nyelv polinom időben visszavezethető** egy $L_2 \subseteq \Delta^*$ nyelvre $(\boldsymbol{L_1 \leq_p L_2})$, ha $L_1 \leq L_2$ és a visszavezetéshez használt függvény polinom időben kiszámítható
- **Tétel:** Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{P}$ $(L_2 \in \mathrm{NP})$, akkor $L_1 \in \mathrm{P}$ $(L_1 \in \mathrm{NP})$
- **Bizonyítás:** Csak az első állítást bizonyítjuk, a másik hasonlóan bizonyítható
  - Legyen $L_2 \in \mathrm{P}$ és tegyük fel, hogy $L_1 \leq_p L_2$
  - Legyen M_2 az L_2-t eldöntő, M pedig a visszavezetést kiszámító Turing-gép
  - Feltehetjük, hogy M és M_2 polinom idejűek
  - Konstruáljuk meg M_1-et:

Bonyolultságelmélet – P és NP



- Világos, hogy $\boldsymbol{M_1}$ **az** $\boldsymbol{L_1}$**-et dönti el,** de polinom idejű-e?
- Igen, mert ha M és M_2 időigénye rendre $p_1(n)$ és $p_2(n)$ polinomok, akkor $\boldsymbol{M_1}$ **időigénye** $\boldsymbol{p_2(p_1(n))}$, ami szintén polinom
  - **Megjegyzés:** ha w n hosszú, akkor $f(w)$ legfeljebb $p_1(n)$ hosszú lehet
- **Megjegyzés:** Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{NP}$, akkor L_1 nem lehet „nehezebben megoldható”, mint L_2

Bonyolultságelmélet – P és NP

- **Definíció:**
  - Legyen $\mathbb{C}$ egy problémaosztály
  - egy L probléma $\mathbb{C}$ -nehéz (a polinom idejű visszavezetésre nézve), ha minden $L' \in \mathbb{C}$ esetén $L' \leq_p L$
  - Egy $\mathbb{C}$ -nehéz L probléma $\mathbb{C}$ -teljes, ha $L \in \mathbb{C}$
- **Tétel:** Legyen L egy NP-teljes probléma. Ha $L \in \mathrm{P}$, akkor $\mathrm{P} = \mathrm{NP}$
- **Bizonyítás:**
  - Elég megmutatni, hogy $\mathrm{NP} \subseteq \mathrm{P}$
  - Legyen $L' \in \mathrm{NP}$ egy tetszőleges probléma
  - Ekkor $L' \leq_p L$
  - Mivel $L \in \mathrm{P}$, az előző tétel alapján $L' \in \mathrm{P}$, azaz $\mathrm{NP} \subseteq \mathrm{P}$

SAT NP-teljes

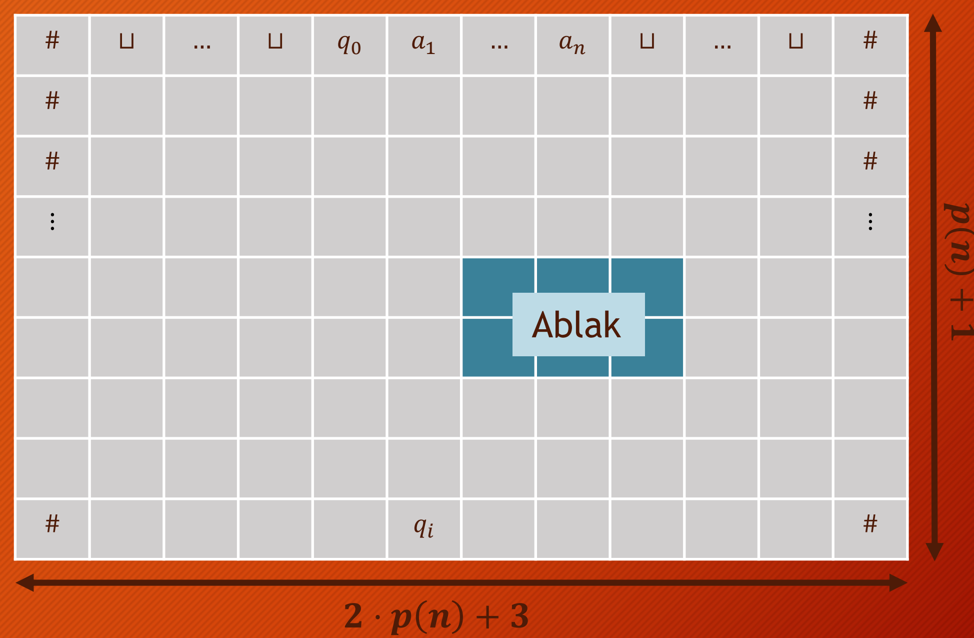
- **Az „első" NP-teljes probléma:**

  $$\mathrm{SAT} := \{\langle\, \varphi \rangle \mid \varphi \text{ kielégíthető zérusrendű KNF}\}$$

- **Tétel (Cook tétele):** SAT NP-teljes
- **Bizonyítás:**
  - SAT $\in$ NP
    - ***SAT* polinom időben verifikálható:** Megadható olyan M nemdet. Turing-gép, ami egy φ bemenetre nemdeterminisztikusan előállítja φ egy I interpretációját és polinom időben leellenőrzi, hogy I kielégíti-e φ-t
  - Megmutatjuk, hogy **tetszőleges $L \in \mathrm{NP}$-re, $L \leq_p \mathrm{SAT}$**
  - Legyen
    - $L \in \mathrm{NP}$ és $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ egy L-et eldöntő $p(n)$ polinom időkorlátos nemdet Turing-gép, és
    - $w = a_1 \dots a_n \in \Sigma^*$

SAT NP-teljes

- ***M* számítása *w*-n leírható egy *T* táblázattal:**
  - T első sora M kezdőkonfigurációja w-n
  - T egymást követő sora M két egymást követő konfigurációja (a két sor közötti különbség belefér egy 2×3-as ablakba)
  - Egy ilyen ablak **legális,** ha „kompatibilis” δ-val
- ***T* elfogadó,** ha egyik sora elfogadó konfiguráció (feltesszük, hogy az ez utáni sorok megegyeznek ezzel a sorral)



SAT NP-teljes

Polinom időben megkonstruálunk egy olyan φ_w KNF-et, hogy

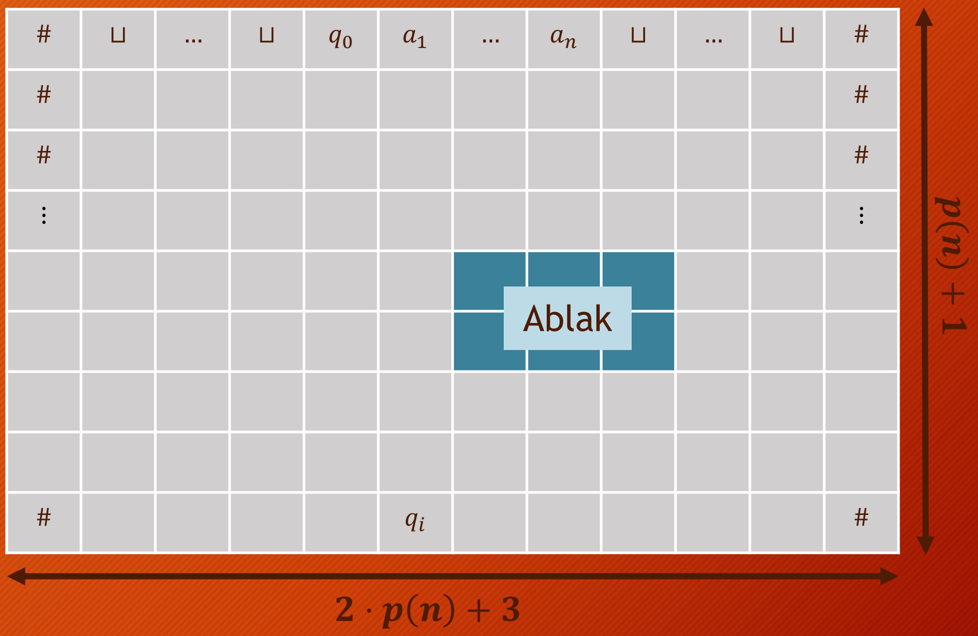
$$\boldsymbol{w \in L \Leftrightarrow \langle \varphi_w \rangle \in \mathrm{SAT}}$$

- φ_w ítéletváltozói $\boldsymbol{X_{i,j,s}}$ alakúak, melynek jelentése: $\boldsymbol{T}$ $\boldsymbol{i}$-ik sorának $\boldsymbol{j}$-ik cellájában $\boldsymbol{s}$ szimbólum van, ahol $s \in C := Q \cup \Gamma \cup \{\#\}$
- $\varphi_w = \varphi_0 \wedge \varphi_{start} \wedge \varphi_{move} \wedge \varphi_{accept}$

$$\varphi_0 = \bigwedge_{\substack{1 \le i \le p(n)+1 \\ 1 \le j \le 2p(n)+3}} \left(\left(\bigvee_{s \in C} X_{i,j,s} \right) \wedge \bigwedge_{s,t \in C, s \neq t} (\neg X_{i,j,s} \vee \neg X_{i,j,t}) \right)$$

$T(i,j)$-ben van valamilyen betű

$T(i,j)$-ben nincs két különböző betű



SAT NP-teljes

$$\varphi_w = \varphi_0 \wedge \varphi_{start} \wedge \varphi_{move} \wedge \varphi_{accept}$$

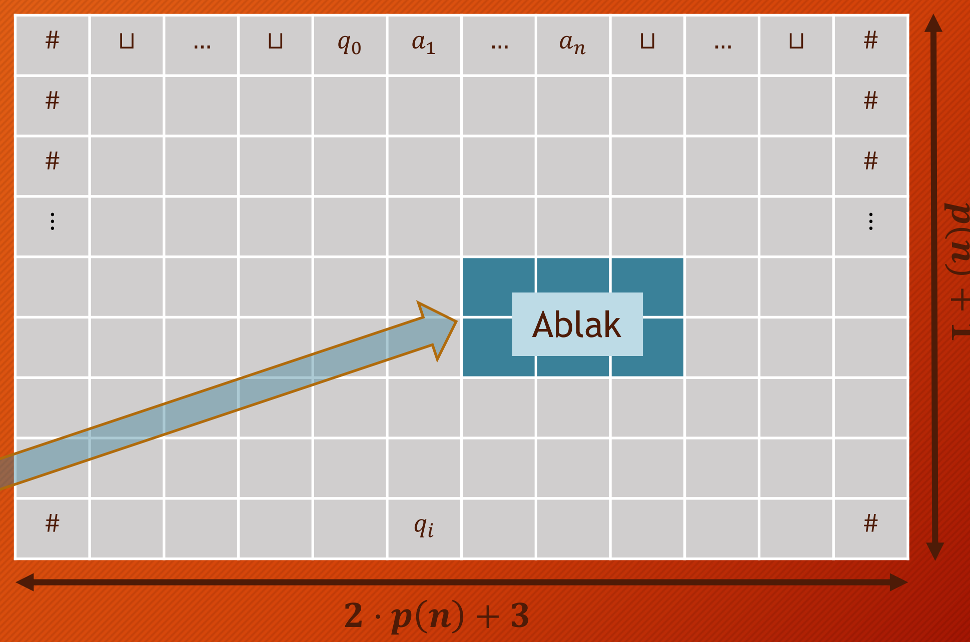
$$\varphi_{start} = X_{1,1,\#} \wedge X_{1,2,\sqcup} \wedge \cdots \wedge X_{1,2p(n)+3,\#}$$

$$\varphi_{accept} = \bigvee_{j=2}^{2p(n)+2} X_{p(n)+1,j,q_i}$$

$$\varphi_{move} = \bigwedge_{\substack{1 \le i \le p(n) \\ 2 \le j \le 2p(n)+2}} \psi_{i,j} \text{ , ahol}$$

$$\psi_{i,j} \sim \bigvee_{\substack{(b_1,\dots,b_6) \\ \text{legális ablak}}} X_{i,j-1,b_1} \wedge \cdots \wedge X_{i+1,j+1,b_6}$$

b_1	b_2	b_3	i
b_4	b_5	b_6	
	j		



SAT NP-teljes

- **Belátható, hogy**
    - φ_w egy KNF-ben adott formula
    - φ_w polinom időben megkonstruálható
    - $w \in L \Leftrightarrow \langle \varphi_w \rangle \in \mathrm{SAT}$
  - Tehát, a fenti konstrukció L polinom idejű visszavezetése SAT-ra
  - Mivel L tetszőleges NP-beli nyelv volt kapjuk, hogy **SAT NP-teljes**
- Hogyan lehet további problémák NP-teljességét belátni?
- **Tétel:** Ha L NP-teljes, $L' \in \mathrm{NP}$ és $L \leq_p L'$, akkor L' is NP-teljes
- **Bizonyítás:**
  - Az állítás egyszerű következménye annak, hogy a polinom idejű visszavezetések tranzitívak
  - **Emlékeztetőül:** Ha $p_1(n)$ és $p_2(n)$ polinomok, akkor $p_2(p_1(n))$ szintén polinom

3SAT NP-teljes

- **Definíció:** $k\mathrm{SAT}$
  - Adott egy φ zérusrendű KNF, melynek minden tagjában pontosan k darab (páronként különböző változót tartalmazó) literál szerepel
  - **Kérdés:** kielégíthető-e φ?
- **Tétel:** $3\mathrm{SAT}$ NP-teljes
- **Bizonyítás:**
  - Világos, hogy $3\mathrm{SAT} \in \mathrm{NP}$
  - Megmutatjuk, hogy $\mathrm{SAT} \leq_p 3\mathrm{SAT}$

3SAT NP-teljes

- **Bizonyítás:**
  - Tetszőleges φ KNF-ben lévő formulához konstruáljuk meg φ'-t a következő táblázat alapján:

φ egy C tagja	φ' klózai
l	$(l \vee X \vee Y) \wedge (l \vee \neg X \vee Y) \wedge (l \vee X \vee \neg Y) \wedge (l \vee \neg X \vee \neg Y)$
$l_1 \vee l_2$	$(l_1 \vee l_2 \vee X) \wedge (l_1 \vee l_2 \vee \neg X)$
$l_1 \vee l_2 \vee l_3$	$l_1 \vee l_2 \vee l_3$
$l_1 \vee l_2 \vee l_3 \vee l_4$	$(l_1 \vee l_2 \vee X) \wedge (\neg X \vee l_3 \vee l_4)$
$l_1 \vee \cdots \vee l_n$ $(n \geq 5)$	$(l_1 \vee l_2 \vee X_1) \wedge (\neg X_1 \vee l_3 \vee X_2) \wedge \cdots \wedge (\neg X_{n-2} \vee l_{n-1} \vee l_n)$

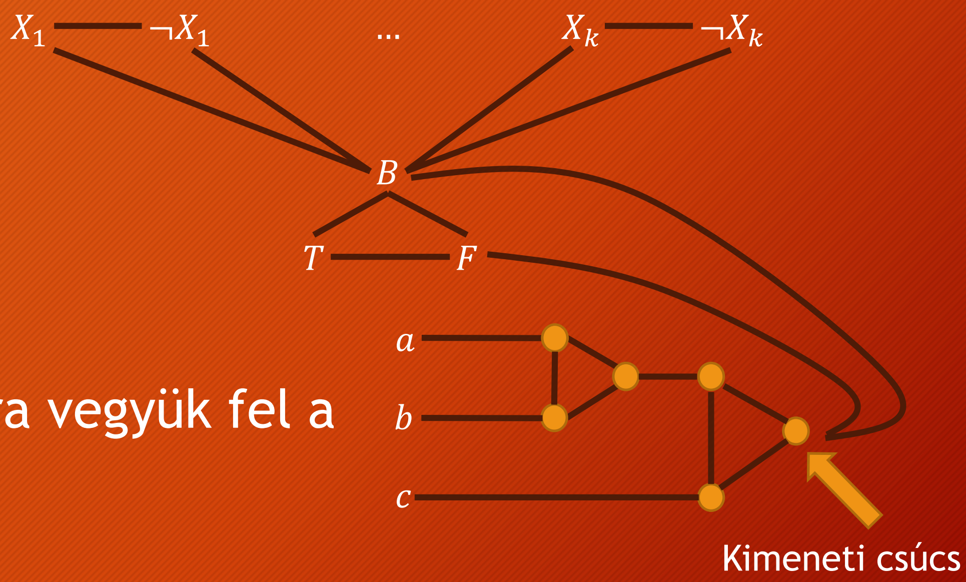
  - $X, Y, X_1, \dots, X_{n-2}$ mindig új, korábban nem használt ítéletváltozók
  - Belátható, hogy φ kielégíthető $\Leftrightarrow$ φ' kielégíthető
- **Megjegyzés:** $\mathrm{2SAT}, \mathrm{HORNSAT} \in \mathrm{P}$

3SZINEZÉS NP-teljes

- **Definíció:** $\boldsymbol{k}\mathbf{SZINEZÉS}\ (\boldsymbol{k} \geq \mathbf{1})$
  - **Adott:** $G = (V, E)$ irányítatlan gráf
  - **Kérdés:** Ki lehet-e szinezni G csúcsait k különböző színnel úgy, hogy a szomszédos csúcsok különböző színűek?
- **Tétel:** $\mathbf{3SZINEZÉS}$ NP-teljes
- **Bizonyítás:**
  - Világos, hogy $3\mathrm{SZINEZÉS}$ polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{3SAT} \leq_{\boldsymbol{p}} \mathbf{3SZINEZÉS}$

3SZINEZÉS NP-teljes

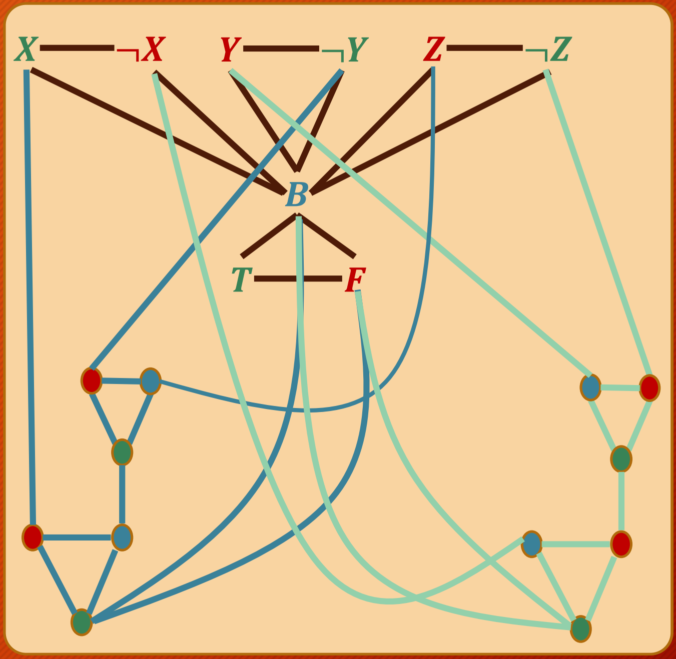
- Legyen φ egy 3SAT alakú formula és tfh. a φ-beli változók $X_1, \dots, X_k$
- Konstruáljuk meg G_φ-t:



- Plusz minden $a \vee b \vee c$ klózra vegyük fel a következő éleket:

3SZINEZÉS NP-teljes

- **Példa:** ha $\varphi = (X \vee \neg Y \vee Z) \wedge (\neg X \vee Y \vee \neg Z)$, akkor G_φ:
- **Egy tetszőleges $\boldsymbol{\varphi}$ formulára**
- **Ha $\boldsymbol{\varphi}$ kielégíthető, akkor** vegyük φ egy kiértékelését
- Ha ebben egy literál *igaz*, akkor G_φ-ben színezzük őt *zöld*re, a komplementerét pedig *piros*ra
- Mivel így egy klóz legalább egy literálja *zöld*, a klóznak megfelelő háromszög színezhető úgy, hogy a „kimeneti” csúcsa *zöld*
- Ezután B-t színezhetjük *kékre*, azaz **$\boldsymbol{G_\varphi}$ három színezhető**
- **Ha $\boldsymbol{G_\varphi}$ három színezhető, akkor** vegyük G_φ egy színezését
- Feltehetjük, hogy F-et *piros*ra, T-t pedig *zöld*re színezzük;
- Legyen I a következő: $I(X_i) = igaz \Leftrightarrow X_i$ *zöld*re van színezve; ekkor I jól definiált
- Tfh. I nem elégíti ki φ-t; akkor van olyan c klóz, aminek minden literálja *hamis* I-ben, azaz a megfelelő csúcsok mind *pirosak* G_φ-ben;
- Ekkor a c-nek megfelelő részgráfban a kimeneti kapu *piros* lehet csak, ami ellentmondás, tehát **$\boldsymbol{\varphi}$ kielégíthető**

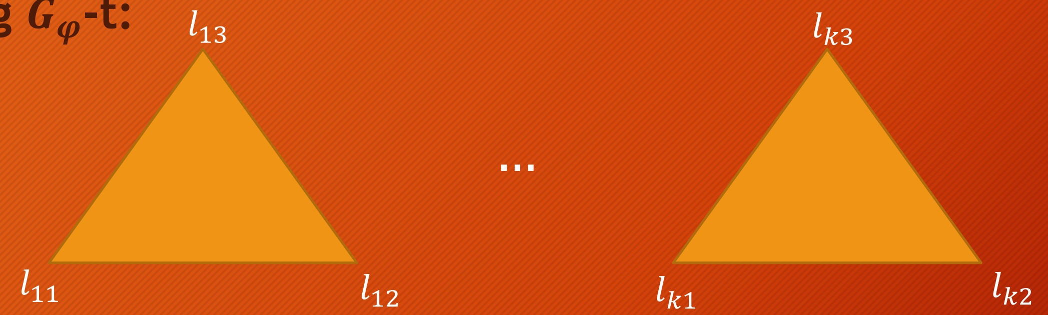


További NP-teljes problémák

- **Definíció:** Legyen adott egy $G = (V, E)$ irányítatlan gráf és $K \leq |V|$
  - **KLIKK**
    - **Kérdés:** Van-e G-ben K darab olyan csúcs, melyek teljes gráfot alkotnak?
  - **FÜGGETLEN CSÚCSHALMAZ**
    - **Kérdés:** Van-e G-ben K darab olyan csúcs, melyek egyikéből sincs a másikba vezető él?
  - **CSÚCSLEFEDÉS**
    - **Kérdés:** Van-e G-ben K darab olyan csúcs, hogy G minden élének egyik végpontja ezen csúcsok valamelyikére esik?
- **Tétel:** A fenti problémák mindegyike NP-teljes
- **Bizonyítás:**
  - **Mindhárom probléma polinomidőben verifikálható:** Megadható olyan M nemdet. Turing-gép, ami egy $\langle G, K\rangle$ bemenetre nemdeterminisztikusan felsorolja G K darab csúcsát és polinom időben leellenőrzi, hogy ezek rendelkeznek-e a kérdéses tulajdonsággal

További NP-teljes problémák

- **FÜGGETLEN CSÚCSHALMAZ (FCS) NP-nehéz**
  - Megmutatjuk, hogy $\mathbf{3SAT} \leq_{\mathbf{p}} \mathbf{FCS}$
    - Legyen $\varphi = (l_{11} \vee l_{12} \vee l_{13}) \wedge \cdots \wedge (l_{k1} \vee l_{k2} \vee l_{k3})$
    - **Konstruáljuk meg G_φ-t:**



    - Plusz l_{ij} és l_{mn} között pontosan akkor van él ha ezek egymás komplementerei
  - **Belátható, hogy** a konstrukció polinom időben elvégezhető
  - **Megmutatjuk, hogy** φ kielégíthető $\Leftrightarrow$ G_φ-ben van k csúcsú független csúcshalmaz

További NP-teljes problémák

- **φ kielégíthető $\Leftrightarrow$ G_φ-ben van k csúcsú független csúcshalmaz:**
  - **φ kielégíthető** $\Leftrightarrow$
    - Van olyan I interpretáció, hogy minden $i = 1, \ldots, k$-ra, az i-ik klózból ki lehet választani olyan l_{ij_i} literált, hogy $\mathrm{I} \vDash \{l_{1j_1}, \ldots, l_{kj_k}\}$

      $\Leftrightarrow$
    - Minden $i = 1, \ldots, k$-ra, az i-ik háromszögből ki lehet választani olyan l_{ij_i} csúcsot, hogy az $\{l_{1j_1}, \ldots, l_{kj_k}\}$ csúcshalmaz független csúcshalmaz G_φ-ben

      $\Leftrightarrow$
  - **G_φ-ben van k csúcsú független csúcshalmaz**
- **Feladat:** Alkalmazzuk a fenti konstrukciót a következő formulára

$$\varphi = (\neg X \vee \mathrm{Y} \vee \neg Z) \wedge (\neg X \vee \neg Y \vee Z) \wedge (X \vee \neg Y \vee \neg Z)$$

További NP-teljes problémák

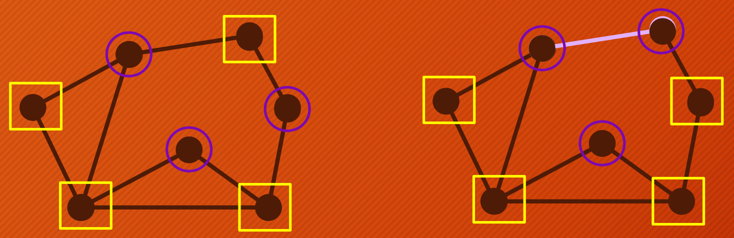
- **KLIKK NP-nehéz**
  - Megmutatjuk, hogy $\mathbf{FCS} \leq_p \mathbf{KLIKK}$
    - Legyen $G = (V, E)$
    - **Konstruáljuk meg $\boldsymbol{G' = (V, E')}$-t:**
      - Minden $a, b \in V$-re, $\{a, b\} \in E' \Leftrightarrow \{a, b\} \notin E$
  - **Belátható, hogy**
    - a konstrukció polinom időben elvégezhető és
    - tetszőleges $K \leq |V|$-re,

    G-ben van K csúcsú független csúcshalmaz $\Leftrightarrow$
    G'-ben van K csúcsú teljes részgráf

További NP-teljes problémák

- **CSÚCSLEFEDÉS (CSL) NP-nehéz**
  - Megmutatjuk, hogy **FCS** $\leq_p$ **CSL**
    - Legyen $G = (V, E)$ és $K \leq |V|$
    - **Vegyük észre, hogy**

    G-ben van K csúcsú független csúcshalmaz $\Leftrightarrow$
    G-ben van $|V| - K$ csúcsú csúcslefedés
    - **Például:**



- A bekarikázott csúcsok független csúcshalmazt alkotnak $\Leftrightarrow$
- A bekeretezett csúcsok csúcslefedést alkotnak