Számításelmélet

Ötödik előadás

További NP-teljes problémák

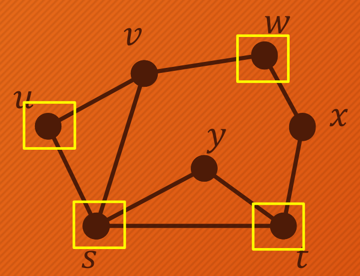
- Legyen $T = \{s_1, \dots, s_n\}$, ahol $s_i \subseteq U$ (U egy tetszőleges halmaz)
- Tudunk-e hatékony algoritmust az alábbi problémákra:
  - Keresni egy minimális elemszámú $H \subseteq U$ halmazt, ami minden s_i halmazból tartalmaz legalább egy elemet, vagy
  - Keresni egy minimális elemszámú részhalmazát T-nek úgy, hogy a T-beli halmazok lefedjék U-t?
- Látni fogjuk, hogy egyik sem könnyebb, mint a CSÚCSLEFEDÉS

HITTING SET és **HALMAZ FEDÉS**

- **HITTING SET (HS)**
  - **Adott** egy U halmaz, $T = \{s_1, \dots, s_n\}$, ahol $s_1, \dots, s_n \subseteq U$, és egy K szám
  - **Kérdés:** Van-e olyan K elemű $H \subseteq U$ halmaz (a *hitting set*) ami tartalmaz minden T-beli halmazból legalább egy elemet?
- **Tétel:** **HITTING SET** NP-teljes
- **Bizonyítás:**
  - Polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{CSL} \leq_{\mathbf{p}} \mathbf{HS}$
    - Legyen $G = (V, E)$ és $K \leq |V|$
    - Konstruáljuk meg T-t a következőképpen:
      - Legyen $U = V$ és minden $\{u, v\} \in E$ élre vegyük fel T-be az $\{u, v\}$ halmazt
    - Belátható, hogy G-ben pontosan akkor van K elemű csúcslefedés, ha T-ben van K elemű hitting set

HITTING SET és HALMAZ FEDÉS

- **Példa:** Végezzük el a konstrukciót az alábbi gráfon



- **Megoldás:**
  - $T = \{\{\boxed{u}, v\}, \{\boxed{u}, s\}, \{v, \boxed{w}\}, \{\boxed{s}, v\}, \{\boxed{w}, x\}, \{x, \boxed{t}\}, \{\boxed{s}, y\}, \{y, \boxed{t}\}, \{\boxed{s}, t\}\}$
  - Egy négy elemű hitting set T-ben: $\boldsymbol{H = \{u, s, t, w\}}$

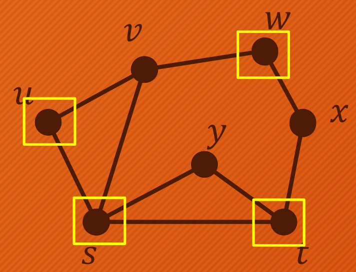
- **Megjegyzés:** A CSL igazából a HS egy speciális esete

HITTING SET és HALMAZ FEDÉS

- **HALMAZ FEDÉS (HF)**
  - **Adott** U részhalmazainak egy $s_1, \dots, s_n$ sorozata és egy K szám
  - **Kérdés:** Van-e ezen halmazok közül K darab olyan melyek uniója U?
- **Tétel:** **HALMAZ FEDÉS** NP-teljes
- **Bizonyítás:**
  - Polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{CSL} \leq_{\mathbf{p}} \mathbf{HF}$
    - Legyen $G = (V, E)$ és $K \leq |V|$
    - Konstruáljuk meg **HF** bemenetét a következőképpen:
      - $U = E$
      - Minden $u \in V$ csúcsra, legyen s_u az u-ból induló E-beli élek halmaza
    - Belátható, hogy G-ben pontosan akkor van K elemű csúcslefedés, ha vannak olyan $\mathrm{u}_1, \dots, u_K$ V-beli csúcsok, hogy $s_{u_1} \cup \dots \cup s_{u_K} = U$

HITTING SET és HALMAZ FEDÉS

- **Példa:** Végezzük el a konstrukciót az alábbi gráfon



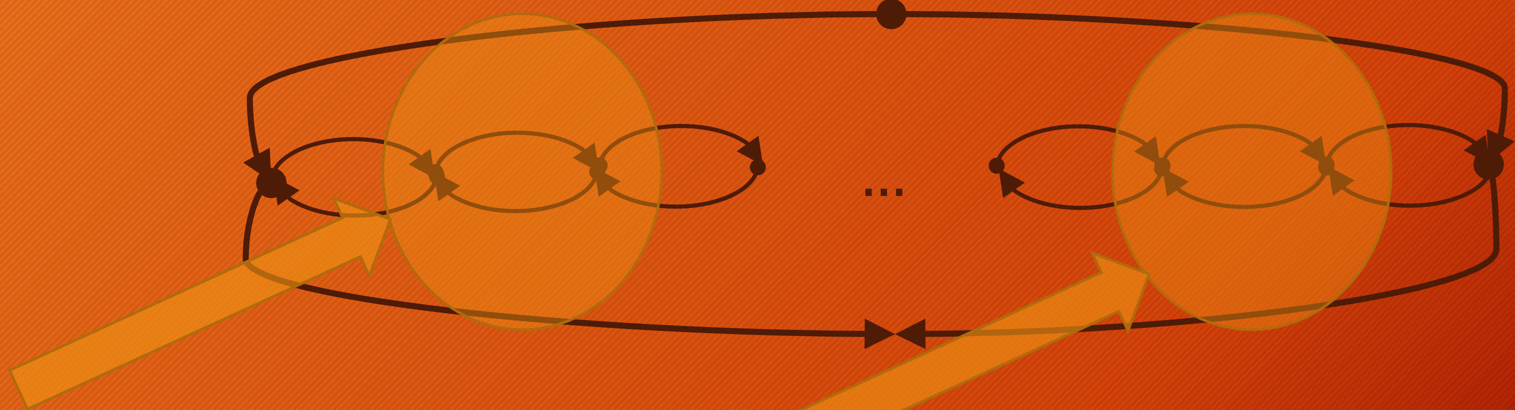
- **Megoldás:**
  - $U = \{\{u,v\},\{u,s\},\{v,w\},\{s,v\},\{w,x\},\{x,t\},\{s,y\},\{y,t\},\{s,t\}\}$
  - $s_u = \{\{u,v\},\{u,s\}\}$, $s_s = \{\{s,u\},\{s.v\},\{s,y\},\{s,t\}\}, \ldots$
  - Egy négy elemű halmaz fedés: $U = s_u \cup s_s \cup s_w \cup s_t$

HAMILTON ÚT

- **Definíció:**
  - $\mathbf{HAMILTON\ ÚT\ (HÚ)}$: Adott egy $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ irányított gráf és $s, t \in V$
  - **Kérdés:** Van-e G-ben s-ből t-be Hamilton út?
- **Tétel:** $\mathrm{HÚ}$ NP-teljes
- **Bizonyítás:**
  - $\mathrm{HÚ}$ polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{SAT} \leq_{\mathbf{p}} \mathbf{HÚ}$
    - Legyen $\boldsymbol{\varphi} = \boldsymbol{c}_1 \wedge \cdots \wedge \boldsymbol{c}_k$ egy tetszőleges KNF-ben adott formula
    - Tegyük fel, hogy a φ-ben használt változók: $X_1, X_2, \dots, X_l$

HAMILTON ÚT

- **Bizonyítás:**
  - Minden X_i változóhoz konstruáljuk meg egy alábbi részgráfot:

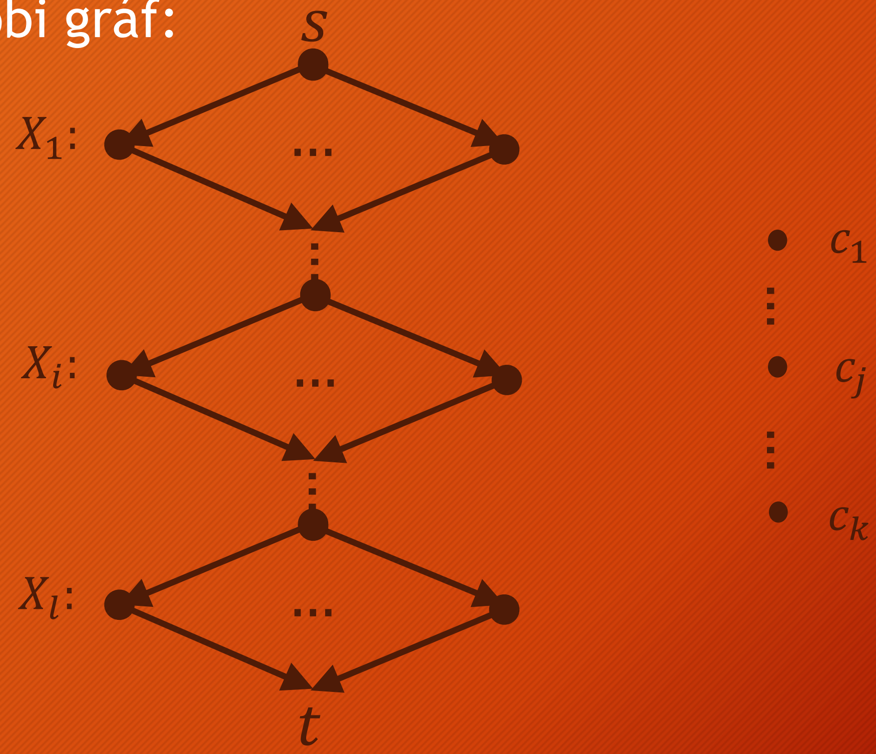


c_1-nek megfeleltetett csúcspár

c_k-nak megfeleltetett csúcspár

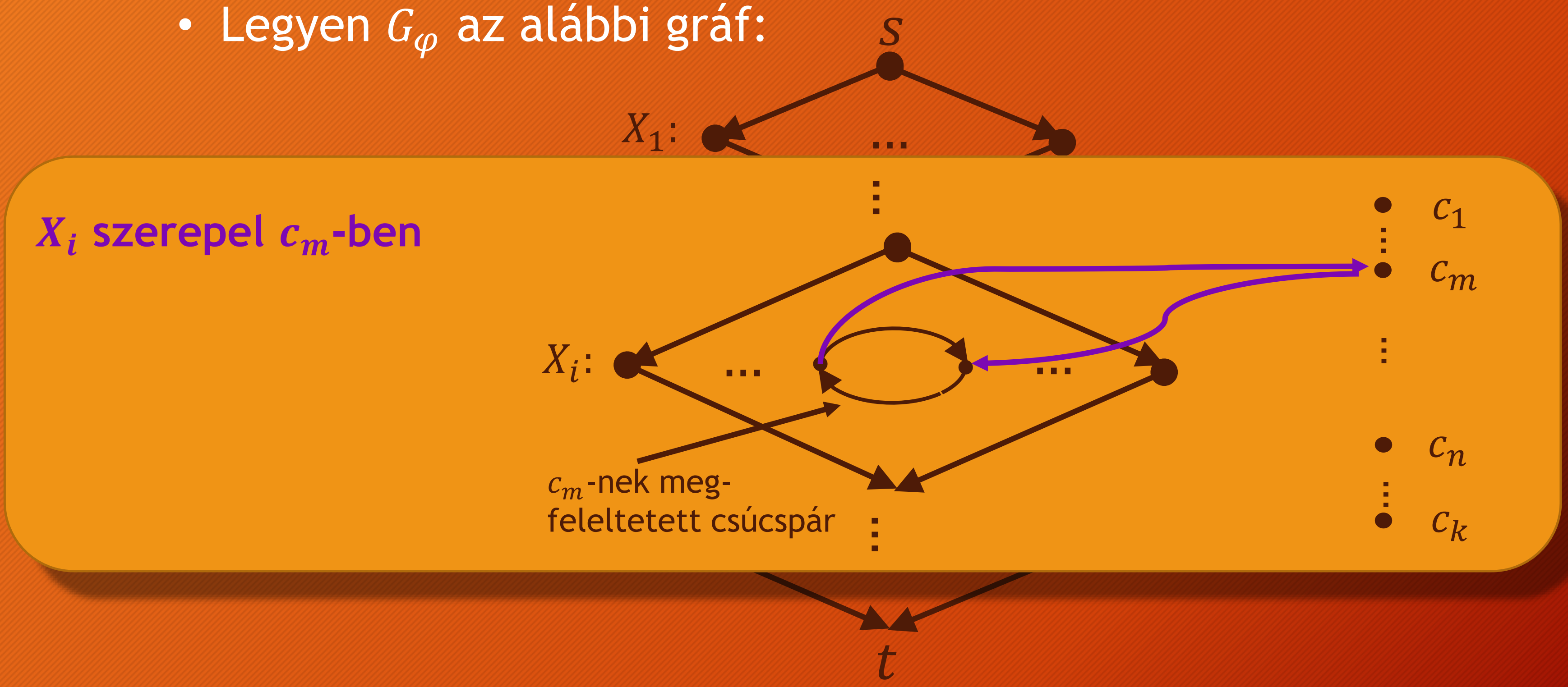
HAMILTON ÚT

- **Bizonyítás:**
  - Legyen G_φ az alábbi gráf:



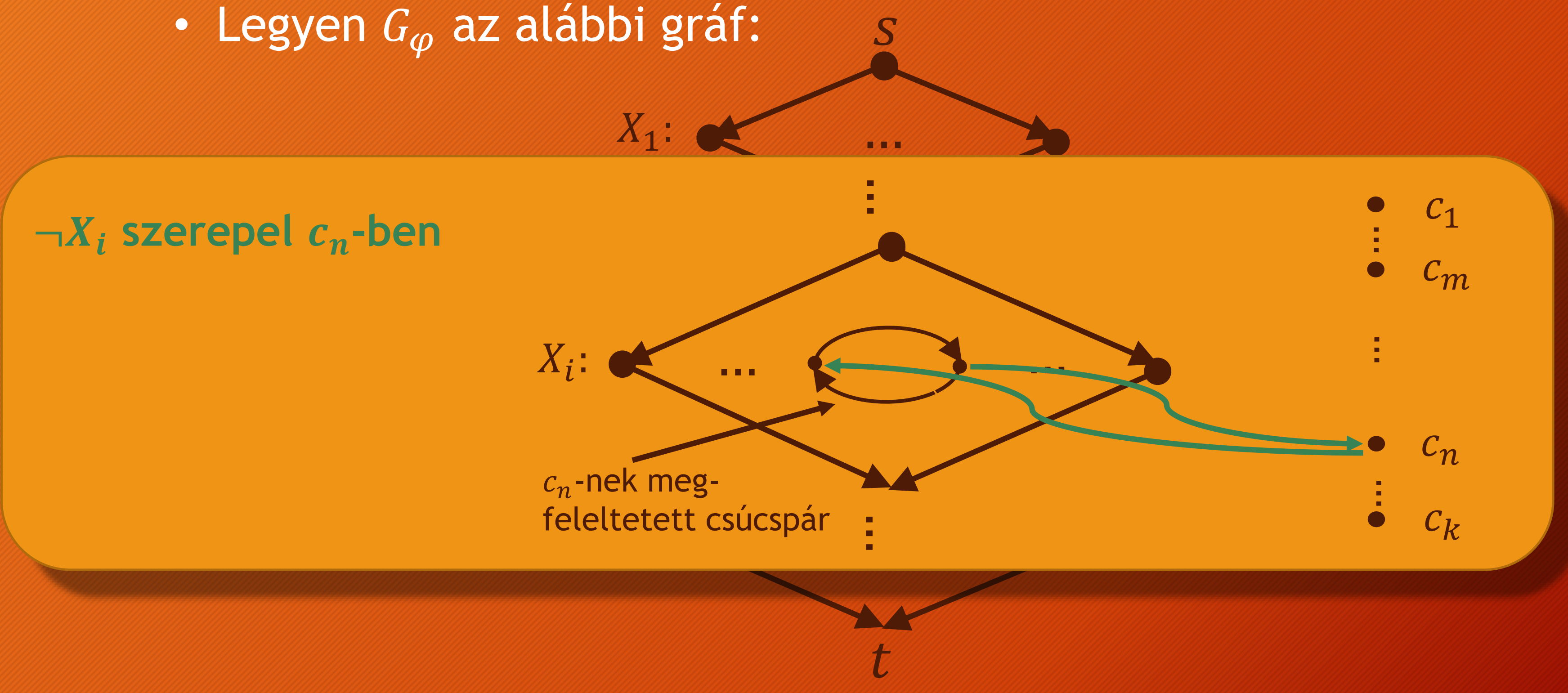
HAMILTON ÚT

- **Bizonyítás:**
  - Legyen G_φ az alábbi gráf:



HAMILTON ÚT

- **Bizonyítás:**
  - Legyen G_φ az alábbi gráf:



HAMILTON ÚT

- **Bizonyítás:**
  - G_φ polinom időben megkonstruálható
  - Belátható, hogy **φ kielégíthető $\Leftrightarrow$ G_φ-ben van Hamilton-út s-ből t-be**
    - **Megjegyzés:**
      - Minden s-ből t-be vezető u út meghatároz egy φ-beli I változóhozzárendelést:
      - u egy X_i-nek megfelelő részgráf tetején pontosan akkor megy balra, ha $I(X_i) = igaz$
      - Ekkor $\mathrm{I} \vDash \varphi \Leftrightarrow u$ Hamilton úttá alakítható

- **Feladat:** Konstruáljuk meg G_φ-t, ha $\varphi = (X \vee \neg Y) \wedge (\neg X \vee Y)$

IRÁNYÍTATLAN HAMILTON ÚT

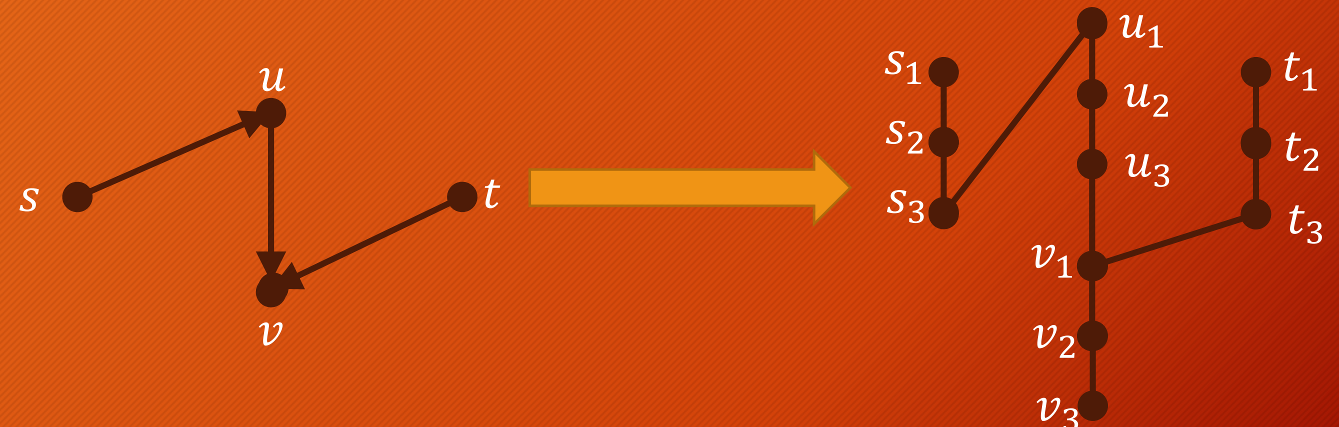
- **Definíció:** IRÁNYÍTATLAN HAMILTON ÚT (IHÚ)
  - **Adott:** $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ irányítatlan gráf és $s, t \in V$
  - **Kérdés:** Van-e G-ben s-ből t-be Hamilton-út?
- **Tétel:** IHÚ NP-teljes
- **Bizonyítás:**
  - IHÚ polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{HÚ} \leq_{\mathbf{p}} \mathbf{IHÚ}$
  - Tetszőleges G-re legyen $G' = (V', E')$ a következő gráf
    - Minden $u \in V$-re, $u_1, u_2, u_3 \in V'$
    - Minden $u \in V$-re, $\{u_1, u_2\}$,$\{u_2, u_3\} \in E'$
    - Minden $(u, v) \in E$-re, $\{u_3, v_1\} \in E'$

IRÁNYÍTATLAN HAMILTON ÚT

- **Bizonyítás:**
  - G' polinom időben megkonstruálható
  - Belátható, hogy

G-ben van Hamilton-út s-ből t-be $\Leftrightarrow$ G'-ben van Hamilton-út s_1-ből t_3-ba

  - **Megjegyzés:** A csúcsok triplázása biztosítja G'-ben azt hogy a G-beli élek az irányításuk elvesztése után is pontosan akkor alkossanak Hamilton-utat, ha G-ben azt alkotnak
  - **Példa:**

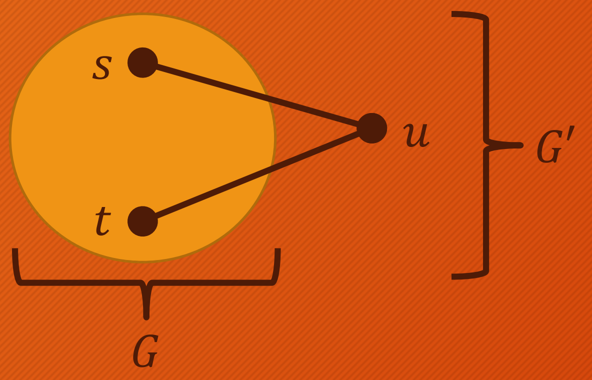


IRÁNYíTATLAN HAMILTON KÖR

- **Definíció:** IRÁNYíTATLAN HAMILTON KÖR (IHK)
  - **Adott:** $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ irányítatlan gráf
  - **Kérdés:** Van-e G-ben Hamilton-kör?
- **Tétel:** IHK NP-teljes
- **Bizonyítás:**
  - IHK polinom időben verifikálható
  - Megmutatjuk, hogy $\mathbf{IHÚ} \leq_{\mathbf{p}} \mathbf{IHK}$
  - Tetszőleges G-re és $s, t \in V$ csúcsokra, legyen $G' = (V', E')$ a következő gráf
    - $V' = V \cup \{u\}$, ahol u egy új, V-ben nem szereplő csúcs
    - $E' = E \cup \{\{s, u\}, \{t, u\}\}$

IRÁNYíTATLAN HAMILTON KÖR

- A konstrukció:



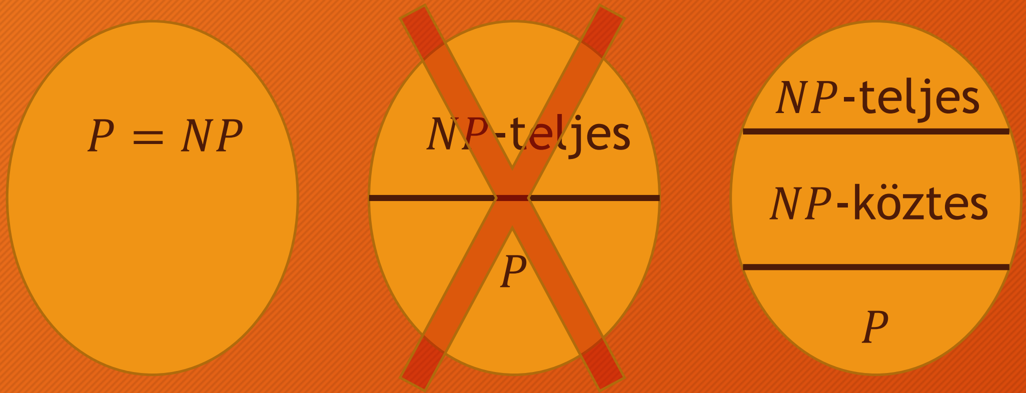
- Belátható, hogy G-ben pontosan akkor van Hamilton-út s-ből t-be, ha G'-ben van Hamilton-kör

UTAZÓÜGYNÖK

- **Definíció:** UTAZÓÜGYNÖK
  - **Adott:** $G = (V, E)$ irányítatlan gráf az éleken pozitív egész súlyokkal és K természetes szám
  - **Kérdés:** Van-e G-ben legfeljebb K súlyú Hamilton-kör?
- **Tétel:** UTAZÓÜGYNÖK NP-teljes
- **Bizonyítás:**
  - Polinom időben verifikálható
  - Észrevesszük, hogy az **UTAZÓÜGYNÖK probléma bemenetét a következőképpen megszorítva:**
    - G minden élén 1 súly szerepel
    - $K = |V|$

    visszakapjuk a HAMILTON KÖR problémát

A P és NP osztályok lehetséges viszonyai



- **Tétel:** Ha $\mathrm{P} \neq \mathrm{NP}$, akkor van olyan L, hogy $L \in \mathrm{NP}, L \notin \mathrm{P}$ és L nem NP-teljes (azaz L NP-köztes)
- **Sejtés:** egy ilyen probléma a $\mathrm{GRÁF\ IZOMORFIZMUS}$:
  - Adottak G_1 és G_2 irányítatlan gráfok
  - Kérdés: Izomorfak-e?
- **Megjegyzés:** Babai László, magyar matematikus friss eredménye: $\mathrm{GRÁF\ IZOMORFIZMUS}$ kvázipolinom időben megoldható

Az NP és coNP osztályok

- **Definíció:**
  - Ha $\mathbb{C}$ problémák egy osztálya, akkor $\mathbf{co}\mathbb{C} \coloneqq \{\bar{\boldsymbol{L}} \mid \boldsymbol{L} \in \mathbb{C}\}$
  - $\mathbb{C}$ **zárt a polinom idejű visszavezetésre nézve**, ha tetszőleges $\mathrm{L}_2 \in \mathbb{C}$ és L_1 problémák esetén, $L_1 \leq_p L_2$-ből következik, hogy $L_1 \in \mathbb{C}$
- **Megjegyzés:** korábbi tételünk alapján P és NP zártak a polinom idejű visszavezetésre nézve
- **Tétel:** Ha $\mathbb{C}$ zárt a polinom idejű visszavezetésre nézve, akkor $\mathrm{co}\mathbb{C}$ is zárt
- **Bizonyítás:**
  - Tegyük fel, hogy $\mathbb{C}$ zárt a polinom idejű visszavezetésre nézve, $L_1 \leq_p L_2$ és $L_2 \in \mathrm{co}\mathbb{C}$
  - Ekkor $\overline{L_1} \leq_p \overline{L_2}$ és $\overline{L_2} \in \mathbb{C}$

Az NP és coNP osztályok

- **Bizonyítás:**
  - Következik, hogy $\overline{L_1} \in \mathbb{C}$ (mert $\mathbb{C}$ zárt), azaz $L_1 \in \mathrm{co}\mathbb{C}$
  - Tehát $\mathrm{co}\mathbb{C}$ is zárt a polinom idejű visszavezetésre nézve
- **Következmény:** coNP zárt a polinom idejű visszavezetésre nézve
- **Tétel:** Egy L nyelv akkor és csak akkor $\mathbb{C}$-teljes, ha $\bar{L}$ $\mathrm{co}\mathbb{C}$-teljes
- **Bizonyítás:**
  - Mivel $\mathrm{co}(\mathrm{co}\mathbb{C}) = \mathbb{C}$, elég az egyik irányt bizonyítani
  - Tegyük fel, hogy L $\mathbb{C}$-teljes, azaz $L \in \mathbb{C}$ és minden $L' \in \mathbb{C}$-re, $L' \leq_p L$
  - Akkor $\bar{L} \in \mathrm{co}\mathbb{C}$ és minden $\overline{L'} \in \mathrm{co}\mathbb{C}$-re, $\overline{L'} \leq_p \bar{L}$, azaz $\bar{L}$ $\mathrm{co}\mathbb{C}$-teljes

Az NP és coNP osztályok

- ÁLT_SAT $= \{\langle\varphi\rangle \mid \varphi$ kielégíthető zérusrendű formula$\}$ is NP-teljes
- **Következik, hogy**
  - $\overline{\text{ÁLT\_SAT}}$ = **UNSAT** $= \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen zérusrendű formula$\}$ és
  - **TAUT** $= \{\langle\varphi\rangle \mid \varphi$ érvényes zérusrendű formula$\}$ coNP-teljesek (triviálisan UNSAT $\leq_p$ TAUT)
- **Megjegyzés:**
  - coNP tartalmazza **polinom időben cáfolható** problémákat
  - Nem ismert, hogy NP = coNP, de az a **sejtés, hogy a két osztály összehasonlíthatatlan**
  - Viszont, ha egy coNP-teljes problémáról kiderülne, hogy NP-beli, akkor NP = coNP

Tárbonyolultság

- A **tárbonyultság** vizsgálatához ún. **off-line Turing-gépeket** használunk:
  - A bemenetet csak olvassa
  - A kimenetet csak írja
  - A felhasznált tárba csak a munkaszalagokon felhasznált cellák száma számít bele
- **Megjegyzés:**
  - Off-line Turing-gépek használatával **szublineáris** tárbonyultságnak is van értelme
  - A tár újra felhasználható
- **Definíció:** Legyen $f: \mathbb{N} \to \mathbb{R}_+$ tetszőleges függvény
  - $\mathbf{SPACE}\big(\boldsymbol{f}(\boldsymbol{n})\big) \coloneqq \{L \mid L \text{ eldönthető } O\big(f(n)\big) \text{ tárkorlátos det. Turing - géppel}\}$
  - $\mathbf{NSPACE}\big(\boldsymbol{f}(\boldsymbol{n})\big) \coloneqq \{L \mid L \text{ eldönthető } O\big(f(n)\big) \text{ tárkorlátos nemdet. Turing - géppel}\}$
  - $\mathbf{PSPACE} = \bigcup_{k=1}^{\infty} \mathrm{SPACE}(n^k)\,, \mathbf{NPSPACE} = \bigcup_{k=1}^{\infty} \mathrm{NSPACE}(n^k)$
- **Megjegyzés:**
  - $\mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{NPSPACE}$
  - Később látni fogjuk, hogy $\mathrm{PSPACE} = \mathrm{NPSPACE}$ és az a sejtés, hogy $\mathrm{NP} \subset \mathrm{PSPACE}$

Savitch tétele

- **Tétel (Savitch):** Ha $f(n) \geq \log n$, akkor $\mathrm{NSPACE}\big(f(n)\big) \subseteq SPACE(f^2(n))$
- **Bizonyítás:**
  - Először megmutatjuk, hogy az $\mathbf{ELÉR}$ probléma $SPACE(\log^2 n)$-ben van
    - $\mathbf{ELÉR}$: Adott $G = (V, E)$ irányított gráf és $s, t \in V$
    - **Kérdés:** Van-e G-ben út s-ből t-be
  - Legyen $G = (V, E)$ egy irányítatlan gráf, és tekintsük a következő Boole-függvényt:
    - $\mathbf{MAXELÉR}(\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{i}) = \mathbf{igaz} \Leftrightarrow$ G-ben van olyan út s-ből t-be ami legfeljebb i darab csúcsot érint
  - **Megjegyzés:** G-ben van út s-ből t-be $\Leftrightarrow \mathrm{MAXELÉR}(s, t, |V|) = \mathrm{igaz}$
  - $\mathrm{MAXELÉR}(s, t, |V|)$ kiszámítható egy olyan N algoritmussal, aminek tárigénye $O(\log^2 n)$
    - **Ötlet:** $\mathrm{MAXELÉR}(s, t, i) = igaz \Leftrightarrow$

      $\exists u \in V\colon \mathrm{MAXELÉR}\left(s, u, \left\lceil \frac{i}{2} \right\rceil\right) = igaz \wedge \mathrm{MAXELÉR}\left(u, t, \left\lceil \frac{i}{2} \right\rceil\right) = igaz$

Savitch tétele

- **Bizonyítás:**
    - A számításhoz legfeljebb $\log n$ mélységű rekurziót kell alkalmazni
    - A rekurzió minden szintjén $O(\log n)$ méretű adatot kell eltárolni
    - Következik, hogy N $\log^2 n$ tárral képes kiszámítani az $\mathbf{EL\acute{E}R}$ problémát
  - **Ezek után a tétel bizonyítása:**
    - Legyen M egy $f(n)$ tárigényű nemdeterminisztikus Turing-gép és w az M egy n hosszú bemenete
    - Ekkor M egy konfigurációjának tárolásához
      - El kell tárolni a fejek pozícióját, a munkaszalagok tartalmát és M állapotát
      - Ez megtehető $O(f(n))$ tárral, azaz
      - M konfigurációs gráfjának a mérete w-n $2^{df(n)}$ egy alkalmas d konstansra
    - Ebben a gráfban kell keresni egy utat a kezdő és az elfogadó konfiguráció között (feltehető, hogy M-nek csak egy elfogadó konfigurációja van)
    - Azaz az N algoritmussal ki kell számolni a $\mathrm{MAXEL\acute{E}R}(c_{kezdő}, c_{elfogadó}, 2^{d \cdot f(n)})$ értéket az M konfigurációs gráfjában
    - N tárigénye $O\left(\log^2 2^{d \cdot f(n)}\right) = O(f^2(n))$
- **Következmény:** $\mathrm{PSPACE} = \mathrm{NPSPACE}$

PSPACE-teljes problémák

- **Definíció:**
  - QBF: Adott egy φ prenex alakú zárt Boole formula
  - Kérdés: Igaz-e φ?
- **Példa:**
  - $\exists X \forall Y \exists Z((X \vee Y) \wedge (Y \vee Z) \wedge (\neg Y \vee \neg Z))$ igaz
  - $\exists X \forall Y((X \vee Y) \wedge (\neg X \vee \neg Y))$ nem igaz
- **Tétel:** QBF PSPACE-teljes
- **Megjegyzés:** QBF akkor is PSPACE-teljes ha a bemenetét megszorítjuk:
  - A kvantorok alternálnak, az első (és az utolsó kvantor) $\exists$, a formula magja KNF
  - Ekkor QBF felfogható kétszemélyes játékként:
    - Az első játékos választja a páratlan változók értékét és célja a formula igazzá tétele
    - A második játékos választja a páros változók értékét és célja a formula hamissá tétele