Logika és számításelmélet

11. előadás

NP-teljesség

Emlékeztetőül:

NP-teljes nyelv

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

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

Azaz az NP-teljes problémák (ha vannak) az NP-beli problémák legnehezebbjei. Egyikre sem ismeretes polinomiális algoritmus és nem túl valószínű, hogy valaha is lesz ugyanis láttuk, hogy elég egyetlen NP-teljes problémáról bizonyítani, hogy P-beli, ez implikálná, hgy P=NP.
Van-e NP-teljes probléma egyáltalán?

SAT= $\{\langle\varphi\rangle \,|\, \varphi$ kielégíthető nulladrendű KNF$\}$

Tétel (Cook)

SAT NP-teljes.

Cook tétel bizonyítás

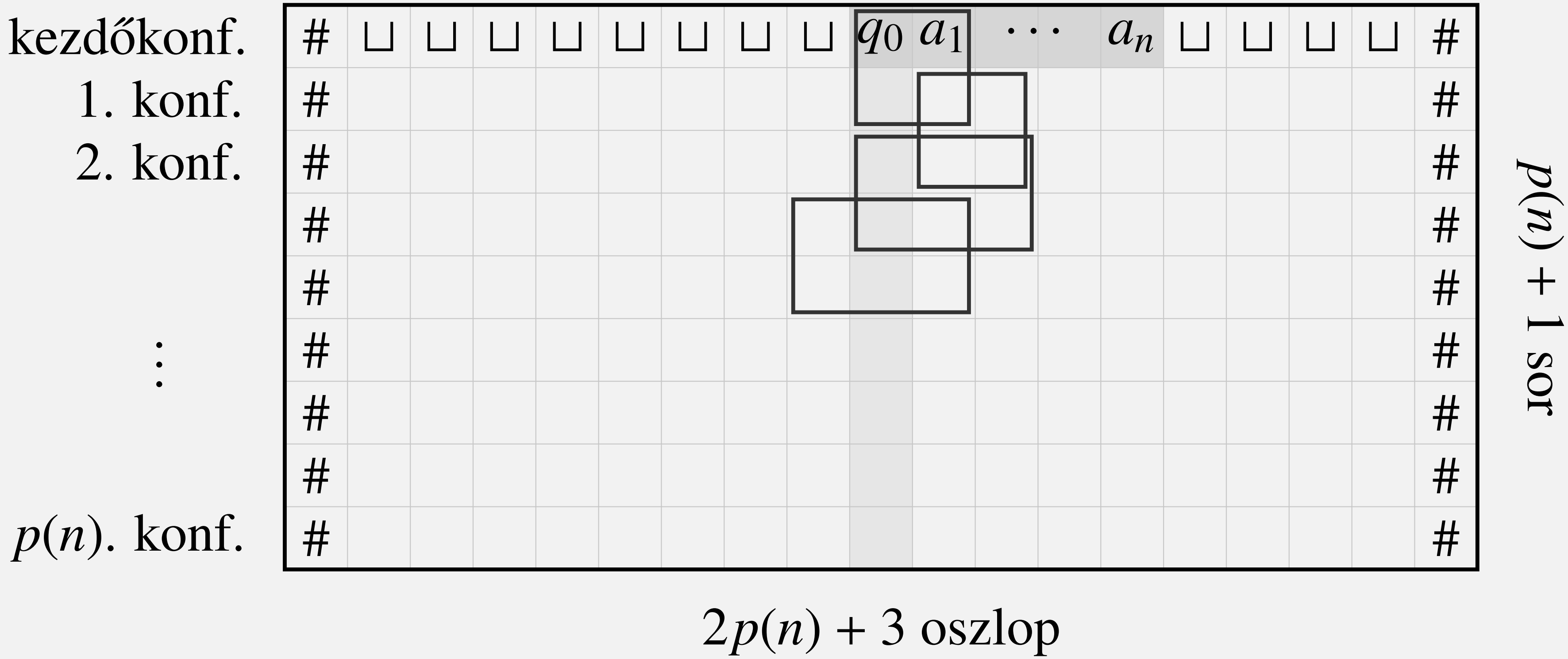
Bizonyítás:

- SAT$\in$ NP: Adott egy φ input. Egy NTG egy számítási ágán polinom időben előállít egy I interpretációt. Majd szintén polinom időben ellenőrzi, hogy ez kielégíti-e φ-t.
- SAT NP-nehéz: ehhez kell, $L \leq_p$ SAT, minden $L \in$ NP-re.

  • Legyen $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ egy L-et eldöntő $p(n)$ polinom időkorlátos NTG. (Feltehető, hogy $p(n) \geq n$.)
  • Legyen továbbá $w = a_1 \cdots a_n \in \Sigma^*$ egy szó.
  • M segítségével megadunk egy polinom időben előállítható φ_w nulladrendű KNF formulát, melyre $w \in L \Leftrightarrow \langle \varphi_w \rangle \in$ SAT.
  • M egy számítása w-n leírható egy T táblázattal, melynek
  – első sora $\# \sqcup^{p(n)} C_0 \sqcup^{p(n)-n} \#$, ahol $C_0 = q_0 w$ M kezdőkonfigurációja w-n
  – T egymást követő két sora M egymást követő két konfigurációja (elegendő $\sqcup$-el kiegészítve, elején és a végén egy #-el). Minden sor $2p(n) + 3$ hosszú.

Cook tétel bizonyítás (folyt.)

– $p(n) + 1$ sor van. Ha hamarabb jut elfogadó konfigurációba, akkor onnantól kezve ismételjük meg az elfogadó konfigurációt.



– a konfigurációátmenet definíciója miatt bármely két sor közötti különbség belefér egy 2x3-as "ablakba"
– T magassága akkora, hogy minden, $\leq p(n)$ lépéses átmenetet tartalmazhasson. A $\sqcup$-ek számát ($\Rightarrow$ T szélességét) pedig úgy, hogy az ablakok biztosan "ne eshessenek le" egyik oldalon se.

Cook tétel bizonyítás (folyt.)

– φ_w ítéletváltozói $X_{i,j,s}$ alakúak, melynek jelentése: T i-ik sorának j-ik cellájában az s szimbólum van, ahol $s \in \Delta = Q \cup \Gamma \cup \{\#\}$.

– φ_w a w bemenetre M minden lehetséges legfeljebb $p(n)$ lépésű működését leírja. Felépítése: $\varphi_w = \varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_{\text{move}} \wedge \varphi_{\text{accept}}$.

– φ_0 akkor és csak akkor legyen igaz, ha minden cellában pontosan 1 betű van:

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

– φ_{start} akkor és csak akkor legyen igaz, ha T első sora a $\sqcup$-okkal és #-ekkel a fent említett módon adott hosszúságúra kiegészített kezdőkonfiguráció.

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

Cook tétel bizonyítás (folyt.)

– φ_{move} akkor és csak akkor legyen igaz, ha minden ablak legális, azaz δ szerinti átmenetet ír le:

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

ahol $$\psi_{i,j} \sim \bigvee_{\substack{(b_1,\ldots,b_6) \\ \text{legális ablak}}} X_{i,j-1,b_1} \wedge X_{i,j,b_2} \wedge X_{i,j+1,b_3} \wedge X_{i+1,j-1,b_4} \wedge X_{i+1,j,b_5} \wedge X_{i+1,j+1,b_6}$$

b_1	b_2	b_3
b_4	b_5	b_6

De: $\psi_{i,j}$ nem elemi diszjunkció!!! Ezért e helyett:

$$\psi_{i,j} := \bigwedge_{\substack{(b_1,\ldots,b_6) \\ \text{illegális ablak}}} \neg X_{i,j-1,b_1} \vee \neg X_{i,j,b_2} \vee \neg X_{i,j+1,b_3} \vee \neg X_{i+1,j-1,b_4} \vee \neg X_{i+1,j,b_5} \vee \neg X_{i+1,j+1,b_6}$$

Cook tétel bizonyítás (folyt.)

– végezetül: φ_{accept} akkor és csak akkor legyen igaz, ha az utolsó sorban van q_i-t:

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

.

• $w \in L \Leftrightarrow$ az M NTG-nek van w-t elfogadó számítása$\Leftrightarrow$ T kitölthető úgy, hogy ϕ_w igaz $\Leftrightarrow$ ϕ_w kielégíthető $\Leftrightarrow$ $\langle\varphi_w\rangle \in$ SAT,

• hány literált tartalmaz a φ_w formula? Legyen $k = |\Delta|$.

ϕ_0 : $(p(n) + 1)(2p(n) + 3)(k + k(k - 1)) = O(p^2(n))$,

φ_{start} : $2p(n) + 3 = O(p(n))$,

φ_{move} : $\leq p(n)(2p(n) + 1)k^6 \cdot 6 = O(p^2(n))$,

φ_{accept} : $2p(n) + 1 = O(p(n))$,

azaz φ_w $O(p^2(n))$ méretű, így polinom időben megkonstruálható

• tehát $w \mapsto \langle\varphi_w\rangle$ pol. idejű visszavezetés, így $L \leq_p$ SAT.

• Ez tetszőleges $L \in$ NP nyelvre elmondható. Így SAT NP-nehéz. Mivel NP-beli, ezért NP-teljes is.

További NP-teljes problémák, kSAT

Tétel

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

Bizonyítás: Legyen $L'' \in$ NP tetszőleges. Mivel L NP-teljes, ezért $L'' \leq_p L$. Mivel a feltételek szerint $L \leq_p L'$, ezért a polinom idejű visszavezetések tranzitívitása miatt ($p_1(p_2(n))$ is polinom!) L' NP-nehéz. Ebből és a 3. feltételből kövezkezik az állítás.

Tehát polinom idejű visszavezetéssel további nyelvek NP-teljessége bizonyítható.

kSAT=$\{\langle\varphi\rangle \,|\, \varphi$ kielégíthető KNF és minden tagban pontosan k különböző literál van$\}$.

Az ilyen formulákat kKNF-nek nevezzük a továbbiakban.

3SAT NP-teljessége

Tétel

3SAT NP-teljes.

- 3SAT NP-beli: lásd SAT
- SAT$\leq_p$ 3SAT
  Kell $f : \varphi \mapsto \varphi'$, φ KNF, φ' 3KNF, φ' kielégíthető $\Leftrightarrow \varphi$ kielégíthető, f polinom időben kiszámolható.

$\varphi \mapsto \varphi'$:

ℓ	$\ell \vee X \vee Y,\ \ell \vee X \vee \neg Y,\ \ell \vee \neg X \vee Y,\ \ell \vee \neg X \vee \neg Y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee X,\ \ \ell_1 \vee \ell_2 \vee \neg X$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee X,\ \ \neg X \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \cdots \vee \ell_n$ $(n \geq 5)$	$\ell_1 \vee \ell_2 \vee X_1, \neg X_1 \vee \ell_3 \vee X_2, \ldots, \neg X_{n-2} \vee \ell_{n-1} \vee \ell_n$

$X, Y, X_1, \ldots, X_{n-2}$ új ítéletváltozók. φ' ezek konjunkciója.

Megjegyzés: HORNSAT: mint SAT, de klózonként max. 1 pozitív literál lehet.   HORNSAT és 2SAT $\in$ P.

3 színezhetőség

Egy gráf k**-színezhető**, ha csúcsai k színnel színezhetők úgy, hogy a szomszédos csúcsok színei különbözőek.

3SZÍNEZÉS=$\{\langle G\rangle \mid G$ 3-színezhető$\}$

Tétel

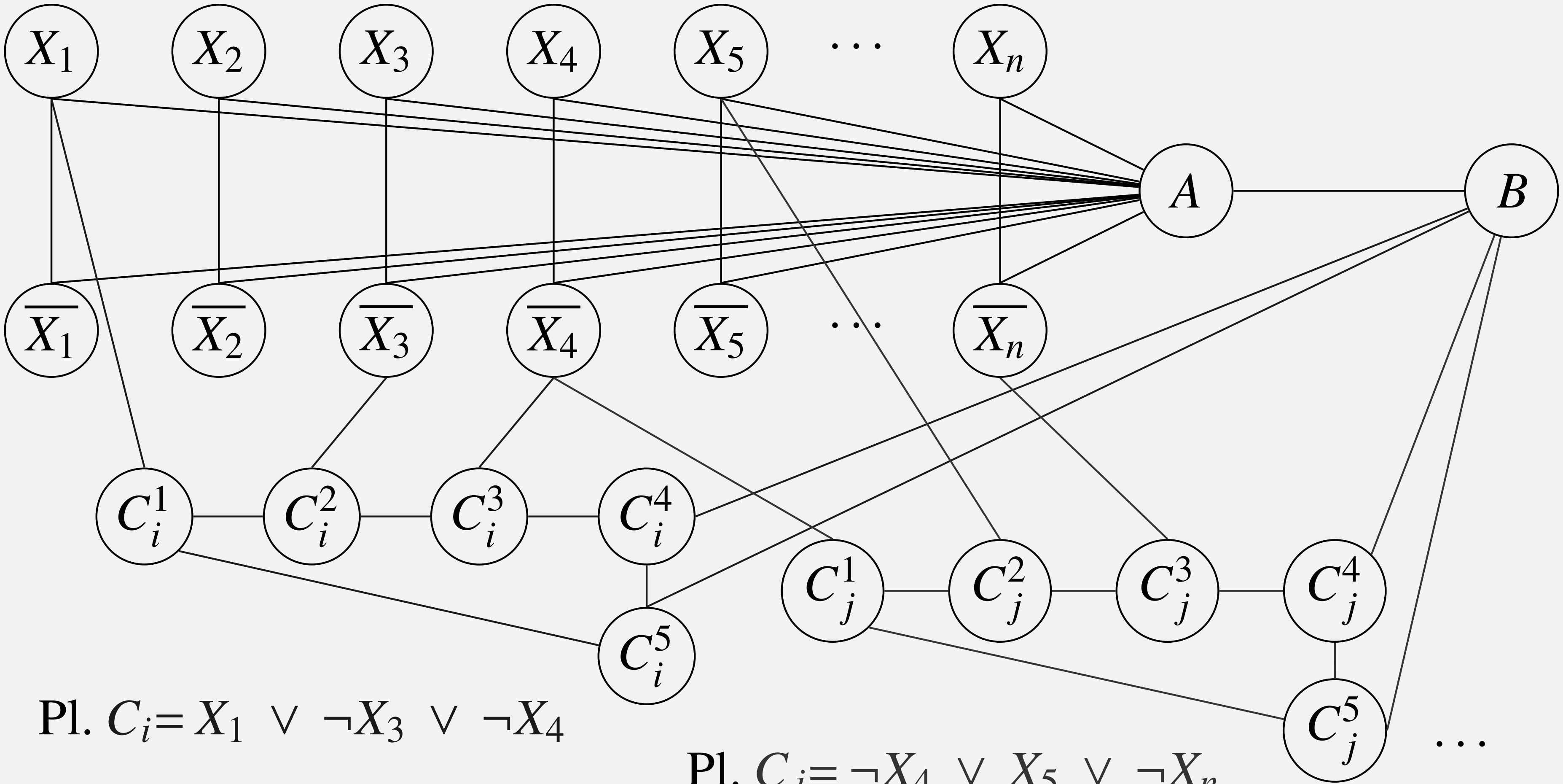
3SZÍNEZÉS NP-teljes.

- 3SZÍNEZÉS NP-beli: egy NTG számítási ágai színezzék ki a gráfot. Egy konkrét színezésről ellenőrizni, hogy helyes-e polinom időben megtehető.
- 3SAT$\leq_p$ 3SZÍNEZÉS

  Elegendő minden φ 3KNF formulához polinom időben elkészíteni egy G_φ gráfot úgy φ kielégíthető $\Leftrightarrow$ G_φ 3 színezhető.

3 színezhetőség

Legyenek $X_1, \ldots, X_n$ a φ-ben előforduló ítéletváltozók. Továbbá $\varphi = C_1 \wedge \ldots \wedge C_m$, azaz $C_1, \ldots C_m$ φ pontosan 3 literálból álló klózai.
G_φ konstrukciója:



Pl. $C_i = X_1 \vee \neg X_3 \vee \neg X_4$

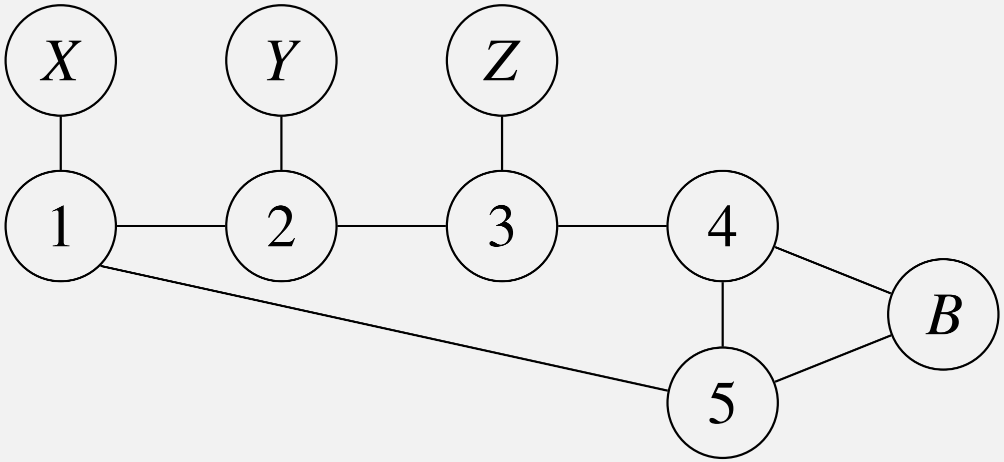
Pl. $C_j = \neg X_4 \vee X_5 \vee \neg X_n$

Minden klózhoz tartozik egy ötszög a fenti módon.

3 színezhetőség

Lemma: Legyen G_0 az alábbi gráf és tegyük fel, hogy az X, Y, Z, B csúcsokat 2 színnel kiszíneztük. Akkor és csak akkor létezik ehhez a parciális színezéshez az egész G_0-ra kiterjeszthető 3-színezés, ha X, Y, Z, B nem mind egyszínű.

G_0



A lemma bizonyítása:

- Ha X, Y, Z, B egyszínű, akkor a maradék 2 színnel kéne az ötszöget kiszínezni, amit nem lehet.
- Egyébként megadunk egy színezést. *1. lépés:* első körben csak 2 színt használunk, 1,2,3,4,5-öt színezzük az $\{X, Y, Z, B\}$-beli szomszédjával ellentétes színűre.

3 színezhetőség

Ez persze még nem jó, mert 1,2,3,4,5 között lehetnek azonos színű szomszédok.

2. lépés: bevetjük a 3. színt: ha 1,2,3,4,5 között van ciklikusan, az óramutató járása szerint valahány egymás utáni egyszínű csúcs, akkor minden párosadikat színezzük át a 3. színre.

A visszavezetés bizonyítása:

- Tegyük fel hogy φ kielégíthető, ekkor meg kell adnunk G_φ egy 3-színezését. Legyenek a színek piros, zöld és kék. Ha X_i igaz, akkor legyen az X_i csúcs zöld, az $\overline{X_i}$ csúcs piros. Ha hamis, akkor épp fordítva. A legyen kék és B legyen piros. Mivel minden klóz ki van elégítve, így minden ötszöghöz van zöld (az igaz literál) és piros szomszéd (B) is, így a lemma miatt a színezés minden ötszögre kiterjeszthető.

3 színezhetőség

- Tegyük fel most, hogy G_φ ki van színezve 3 színnel. Ámnfth. A kék. Mivel $X_1, \ldots, X_n, \overline{X_1}, \ldots, \overline{X_n}$ mind A szomszédai, így egyikük se lehet kék. Továbbá az $(X_i, \overline{X_1})$ párok össze vannak kötve, így minden párban pontosan egy piros és pont egy zöld csúcs van. Ámnfth. B piros (a zöld eset analóg). Mivel az ötszögek ki vannak színezve, ezért a lemma miatt minden ötszögnek van zöld szomszédja. Az "X_i:=igaz $\Leftrightarrow$ X_i csúcs zöld" interpretáció tehát kielégíti φ-t.

Tehát beláttuk, hogy $\varphi \mapsto G_\varphi$ visszavezetés. Mivel G_φ φ ismeretében az input méretének polinomja időben legyártható, ezért a visszavezetés polinom idejű.

Mivel 3SAT NP-teljes korábbi tételünk miatt 3SZÍNEZÉS is az.

Megjegyzés: 2SZÍNEZÉS $\in$ P

3 irányítatlan gráfokkal kapcsolatos probléma

Az alábbi nyelvek esetén G egyszerű, irányítatlan gráf k pedig egy nemnegatív egész. G egy teljes részgráfját **klikknek**, egy üres részgráfját **független ponthalmaznak** mondjuk.

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

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

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: LEFOGÓ PONTHALMAZ a Gazdag jegyzetben CSÚCSLEFEDÉS néven szerepel]

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

Ha G-nek van k méretű klikkje/független ponthalmaza, akkor bármely kisebb k-ra is van. Ha van k méretű lefogó ponthalmaz, akkor bármely nagyobb k-ra is van ($k \leq |V(G)|$).

Független ponthalmaz

Tétel

Klikk,Független ponthalmaz,Lefogó ponthalmaz NP-teljes.

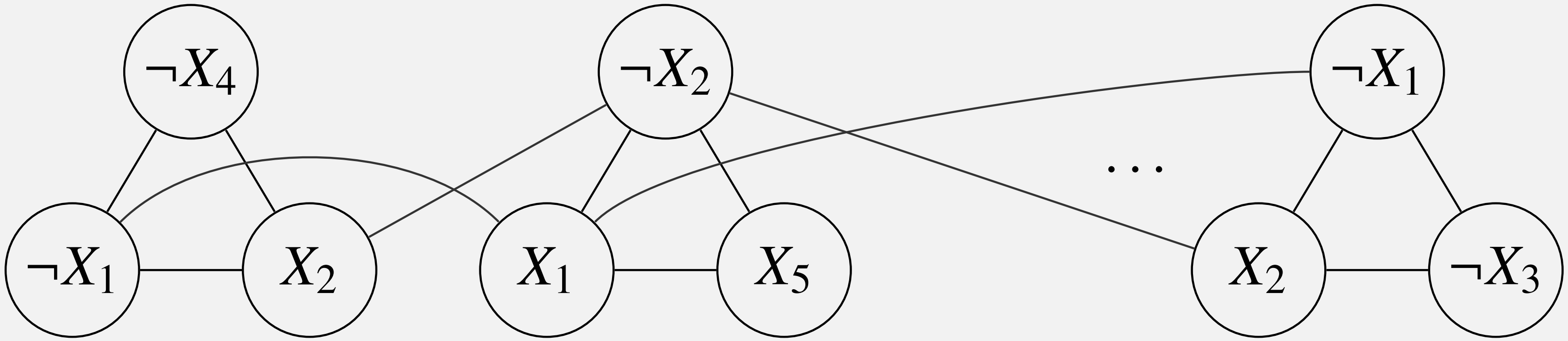
- Egy NTG egy számítási ágán vizsgáljon meg egy k elemű ponthalmazt. Mindhárom esetben az ellenőrzés polinomiális.
- 3SAT$\leq_p$ Független csúcshalmaz

  Kell: $f : \varphi \mapsto (G_\varphi, k)$, φ 3KNF, G_φ-ben van k független akkor és csak akkor ha φ kielégíthető.

  (G_φ, k) konstrukciója: minden egyes $L_1 \vee L_2 \vee L_3$ klózhoz vegyünk fel egy a többitől diszjunkt háromszöget, a csúcsokhoz rendeljük hozzá a literálokat. Így m darab klóz esetén $3m$ csúcsot kapunk. Kössük össze éllel ezen felül a komplemens párokat is. $k := m$.

Független ponthalmaz

Egy példa:



$\neg X_1 \vee X_2 \vee \neg X_4$ $\quad$ $X_1 \vee \neg X_2 \vee X_5$ $\quad$ $\neg X_1 \vee X_2 \vee \neg X_3$

* Ha φ kielégíthető, akkor minden klózban van kielégített literál, válasszunk klózonként egyet, ezeknek megfelelő csúcsok m elemű független csúcshalmazt alkotnak.

* Ha G_φ-ben van m független csúcs, akkor ez csak úgy lehet, ha háromszögenként 1 van. Vegyünk egy ilyet, ezen csúcsoknak megfelelő literálok között nem lehet komplemens pár, hiszen azok össze vannak kötve. Így a független halmaznak megfelelő, (esetleg csak parciális) interpretáció kielégít minden klózt. Ha nincs minden változó kiértékelve, egészítsük ki tetszőlegesen egy interpretációvá.

KLIKK, LEFOGÓ PONTHALMAZ

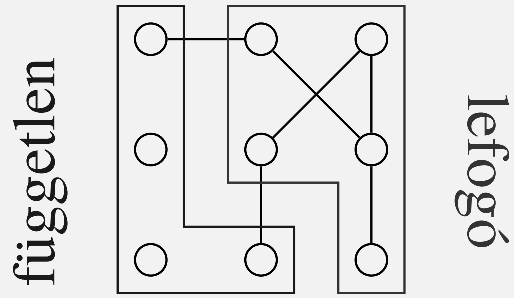
- FÜGGETLEN PONTHALMAZ $\leq_p$ KLIKK

  $f : (G, k) \mapsto (\bar{G}, k)$

  Ez jó visszavezetés, mert ami G-ben klikk az $\bar{G}$-ban független ponthalmaz és viszont.

- FÜGGETLEN PONTHALMAZ $\leq_p$ LEFOGÓ PONTHALMAZ
  $f : (G, k) \mapsto (G, |V(G)| - k)$
  Ha G-ben van k méretű F független ponthalmaz, akkor van $|V(G)| - k$ méretű lefogó ponthalmaz (F komplementere).
  Ha G-ben van $|V(G)| - k$ méretű L lefogó ponthalmaz, akkor van k méretű független ponthalmaz (L komplementere).

Mindkét visszavezetés polinom időben kiszámítható.



Lefogó ponthalmaz hipergráfokban

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

HIPERGRÁF LEFOGÓ PONTHALMAZ$=\{\langle \mathcal{S}, k\rangle \,|\, \mathcal{S}$ egy hipergráf és $\mathcal{S}$-hez van k elemű lefogó ponthalmaz$\}$.

Tétel

HIPERGRÁF LEFOGÓ PONTHALMAZ NP-teljes.

Bizonyítás: HIPERGRÁF LEFOGÓ PONTHALMAZ NP-beli, hiszen polinom időben ellenőrizhető, hogy U egy részhalmaza minden $\mathcal{S}$-beli halmazt metsz-e.

LEFOGÓ PONTHALMAZ a HIPERGRÁF LEFOGÓ PONTHALMAZ speciális esete, hiszen a gráf a hipergráf speciális esete: egy gráf éleire úgy gondolunk, mint 2-elemű halmazokra, így a gráf éleinek halmaza egy hipergráf. (A visszavezetés az identikus leképezés.
$U := V(G)$, $\mathcal{S} := E(G)$, k ugyanaz).
[Megjegyzés: a Gazdag jegyzetben HITTING SET]