Algoritmusok bonyolultsága

6. előadás

http://www.ms.sapientia.ro/~kasa/komplex.htm

döntési probléma: *igen* vagy *nem* válasz

Egy Π döntési probléma a D_Π *esetekből* (instances) és az $Y_\Pi \subseteq D_\Pi$ *igen-esetekből* áll.

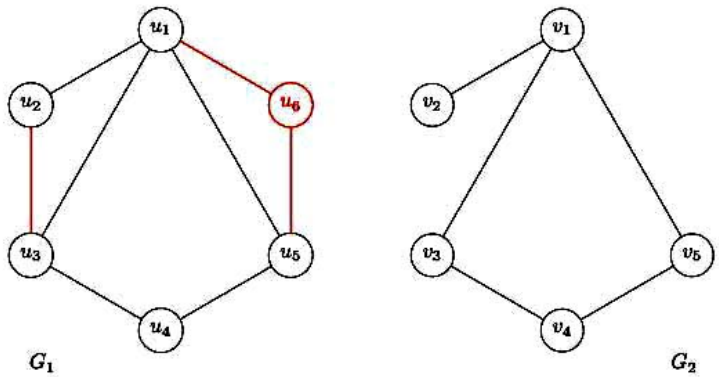
Példák:

Részgráf-izomorfizmus

ÁLTALÁNOS ESET: Adott két gráf: $G_1 = (V_1, E_1)$ és $G_2 = (V_2, E_2)$.

KÉRDÉS: Van-e G_1-nek olyan részgráfja, amelyik izomorf G_2-vel?

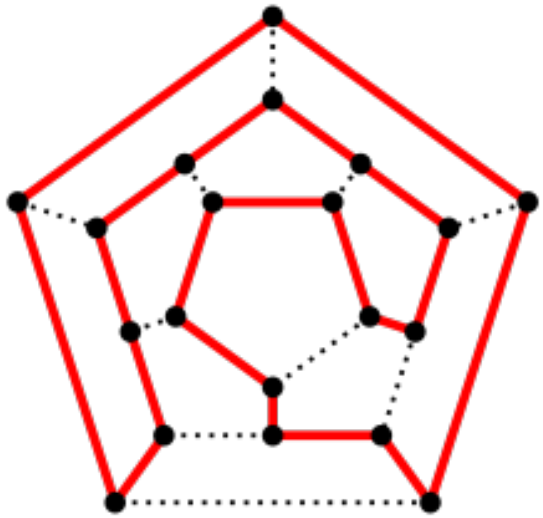
Azaz: létezik-e $V' \subseteq V_1$ és $E' \subseteq E_1$ úgy, hogy $|V'| = |V_2|$, $|E'| = |E_2|$ és létezik egy bijektív $f : V_2 \to V'$, amelyre $\{u, v\} \in E_2$ akkor és csakis akkor, ha $\{f(u), f(v)\} \in E'$?



Utazóügynök

ÁLTALÁNOS ESET: Adott n város:
$C = (c_1, c_2, \ldots, c_n)$, $n \geq 1$; minden várospárra egy $d(c_i, c_j) \in \mathbf{Z}^+$ távolság, és egy $B \in \mathbf{Z}^+$ korlát.
KÉRDÉS: Be lehet-e járni a városokat B-nél nem hosszabb körúttal?
Azaz: Létezik-e a városoknak egy olyan $< c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)} >$ sorrendje úgy, hogy

$$\sum_{i=1}^{n-1} d(c_{\pi(i)}, c_{\pi(i+1)}) + d(c_{\pi(n)}, c_{\pi(1)}) \leq B\,?$$



Feladatok kódolása

Azért használunk *döntési feladatot*, mert azt könnyen megoldhatjuk formális nyelvek segítségével. (Π feladat, e kódolási séma)

$$L[\Pi, e] = \left\{ x \in \Sigma^* \mid x \text{ az } Y_\Pi \text{ egy esetének } e \text{ szerinti kódja} \right\}$$

A kódolási séma hozzárendel minden esethez egy ún. strukturált füzért (stringet).

A *strukturált füzér* rekurzív értelmezése a $\Psi = \{0, 1, -, [,], (,)\} \cup \{,\}$ halmazon:

1. A k egész szám bináris ábrázolásban, esetleg egy $-$ előjellel, strukturált füzér, és a k egész számot jelöli.
2. Ha x strukturált füzér, akkor a $[x]$ is az. Jelölhet egy nevet (pl. csúcs, városnév stb.)
3. Ha $x_1, x_2, \ldots, x_n$ mindegyike strukturált füzér és az $X_1, X_2, \ldots, X_n$ objektumokat jelöli, akkor $(x_1, x_2, \ldots, x_n)$ szintén strukturált füzér, és az $< X_1, X_2, \ldots, X_n >$ sorozatot jelöli.

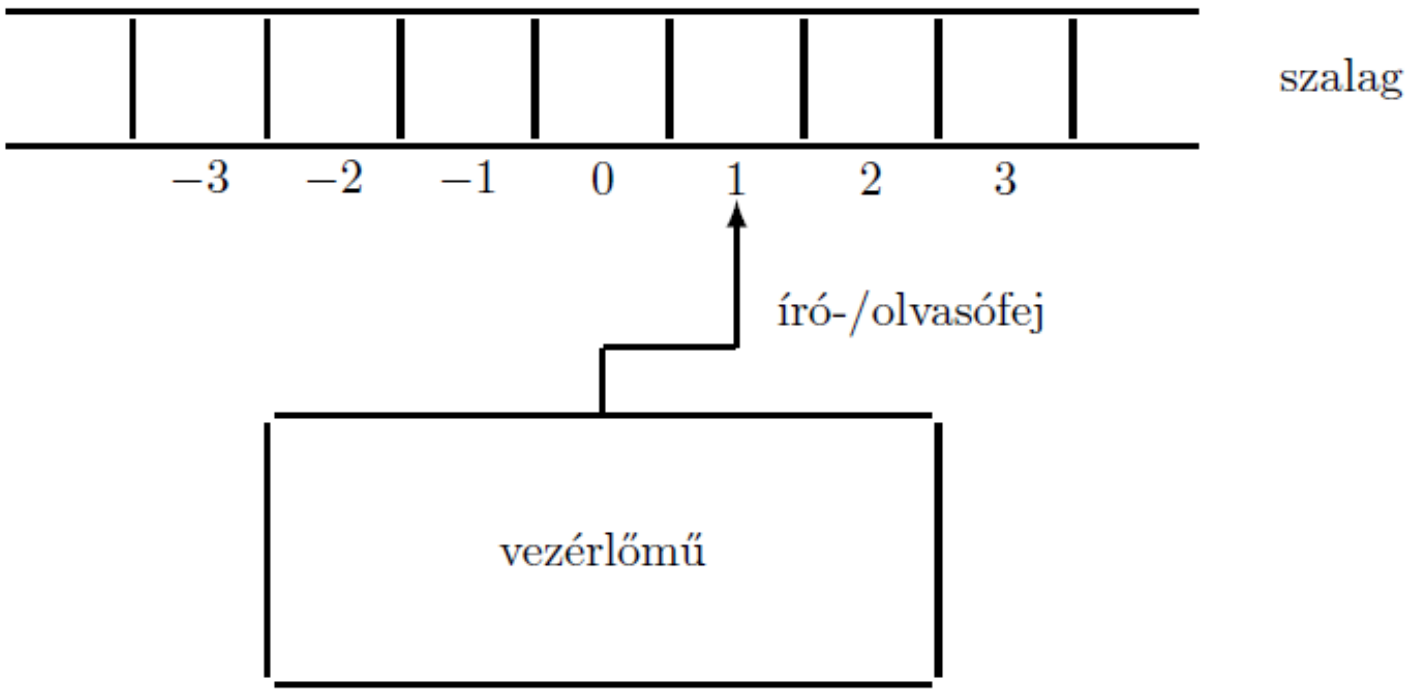
Különböző objektumok ábrázolása:

- halmaz – elemei listája: $< X_1, X_2, \ldots, X_n >$
- gráf – (x, y) strukturált füzér, ahol x a csúcsok strukturált füzére, y az élek strukturált füzére
- véges függvény – $\Big((x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)\Big)$
- racionális szám – (x, y) strukturált füzér, ahol x az a számot jelöli, y a b számot jelöli, ahol $(a, b) = 1$

stb.

A kódolás nem egyérttelmű, egy feladatot különféleképpen lehet kódolni.

Determinisztikus Turing-gép



Determinisztikus Turing-gép

Determinisztikus Turing-gép (Turing-automata) egy változata (Gary-Johnson könyvéből):

Determinisztikus Turing-automatának (DTA) nevezzük a következő rendezett hetest: $M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$, ahol

– Q a belső állapotok véges és nem üres halmaza,
– Σ a bemeneti ábécé,
– Γ a szalagábécé ($\Sigma \subseteq \Gamma$),
– $q_0 \in Q$ a kezdőállapot,
– $B \in \Gamma \setminus \Sigma$ a blank jele (szóköz, üres hely).
– $F = \{q_Y, q_N\}$ a végállapotok halmaza.
– $\delta : \Big(Q \setminus \{q_Y, q_N\}\Big) \times \Gamma \to Q \times \Gamma \times \{-1, +1\}$, átmenetfüggvénynek nevezett leképezés.

Példa Turing-automatára

	0	1	B
q_0	$(q_0, 0, +1)$	$(q_0, 1, +1)$	$(q_1, B, -1)$
q_1	$(q_2, B, -1)$	$(q_3, B, -1)$	$(q_N, B, -1)$
q_2	$(q_Y, B, -1)$	$(q_N, B, -1)$	$(q_N, B, -1)$
q_3	$(q_N, B, -1)$	$(q_N, B, -1)$	$(q_N, B, -1)$

Az automata által felismert nyelv

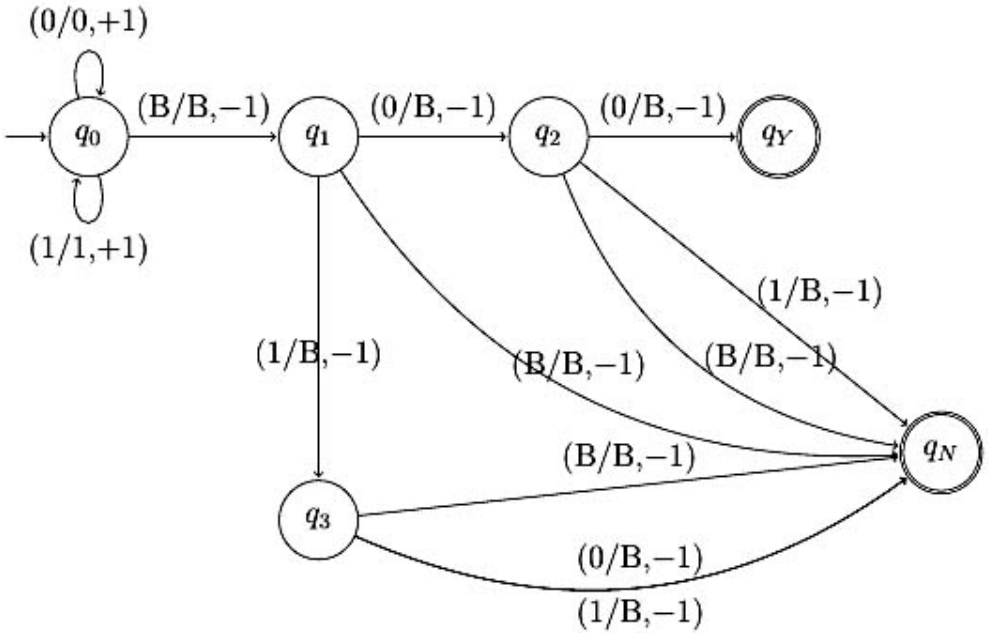
$$L = \left\{ \omega 00 \,\middle|\, \omega \in \{0,1\}^* \right\}$$

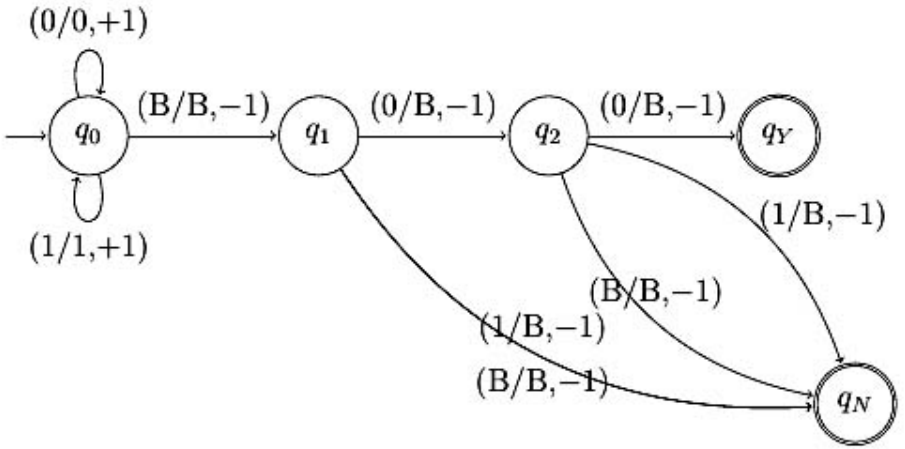
Az M automata által felismert nyelv:

$$L_M = \left\{ x \in \Sigma^* \,\middle|\, M \text{ felismeri } x\text{-et} \right\}$$

Turing-automata = algoritmus (program)

Az előbbi Turing-gép két változatban:





Kapcsolat a döntési feladat és a Turing-gép között

Az M Turing-gép *megoldja* az e sémával kódolt Π döntési feladatot, ha M megáll minden bemenetre, és $L_M = L[\Pi, e]$.

Tekintsük a következő feladatot:

Néggyel való oszthatóság

ÁLTALÁNOS ESET: Adott egy pozitív egész szám: N.

KÉRDÉS: Létezik-e olyan pozitív egész m, amelyre $N = 4m$?

Ha a számokat binárisan ábrázoljuk, a 4-gyel osztható számok utolsó két jegye 0, így az előbbi példa Turing-gépe megoldja ezt a döntési feladatot.

Időbonyolultság

Az *idő* itt az automata lépéseinek a száma a megállásig.

Az (idő)bonyolultság függvény: $T_M : \mathbf{Z}^+ \to \mathbf{Z}^+$, ahol

$$T_M(n) = \max \left\{ m \in \mathbf{Z}^+ \;\middle|\; \begin{array}{l} \exists x \in \Sigma^*, |x| = n, \text{ és az} \\ M \text{ gép } m \text{ lépés után} \\ \text{áll meg az } x \text{ bemenetre} \end{array} \right\}$$

Egy M DTA-program (algoritmus) *polinomiális idejű* (röviden *polinomiális*), ha létezik egy p polinom úgy, hogy minden $n \in \mathbf{Z}^+$ értékre $T_M(n) \leq p(n)$.

P osztály:

$$\mathsf{P} = \left\{ L \subseteq \Sigma^* \;\middle|\; \exists \text{ polinomiális idejű } M \text{ program, amelyre } L = L_M \right\}$$

NP osztály

Tekintsük az UTAZÓÜGYNÖK problémát. Nem ismerünk polinomiális algoritmust a megoldására. De ha valaki megadja a városoknak egy felsorolását, polinomiális időben ellenőrizni tudjuk, hogy az megoldás-e.

Az NP osztály a polinomiális időben ellenőrizhető nyelvek osztálya.
Az NP osztályt értelmezhetjük úgy is, mint a nemdeterminisztikus algoritmusok osztálya.

Egy ilyen algoritmus két részből áll:
– a sejtési fázis: a megoldás megsejtése (sejtés, jóslat, tanú – egy S struktúra)
– az ellenőrző fázis: a sejtés ellenőrzése

NP osztály

Egy nemdeterminisztikus algoritmus megold egy Π döntési feladatot, ha minden $I \in D_\Pi$ esetre fennáll a következő két állítás:

1. Ha $I \in Y_\Pi$, akkor létezik egy S struktúra, amelyet tanúként tekintve, az ellenőrző fázis igen választ ad az adott I-re és S-re.
2. Ha $I \notin Y_\Pi$, akkor nem létezik olyan S struktúra, amelyet tanúként tekintve, az ellenőrző fázis igen választ ad az adott I-re és S-re.

Egy nemdeterminisztikus algoritmus polinomiális időben megold egy Π döntési feladatot, ha létezik olyan p polinom, hogy az ellenőrző fázis legfeljebb $p(n)$ időben történik, ahol n a bemenet hossza.

Informálisan: az NP osztály olyan döntési feladatokból áll, amelyek megfelelő kódolással megoldhatók polinomiális idejű nemdeterminisztikus algoritmusokkal.

Példák NP feladatokra: UTAZÓÜGYNÖK, RÉSZGRÁF-IZOMORFIZMUS stb.

NP osztály

Determinisztikus esetben a komplementer feladat is megoldható polinomiális időben, mivel a Turing-gép minden bemenetre megáll.

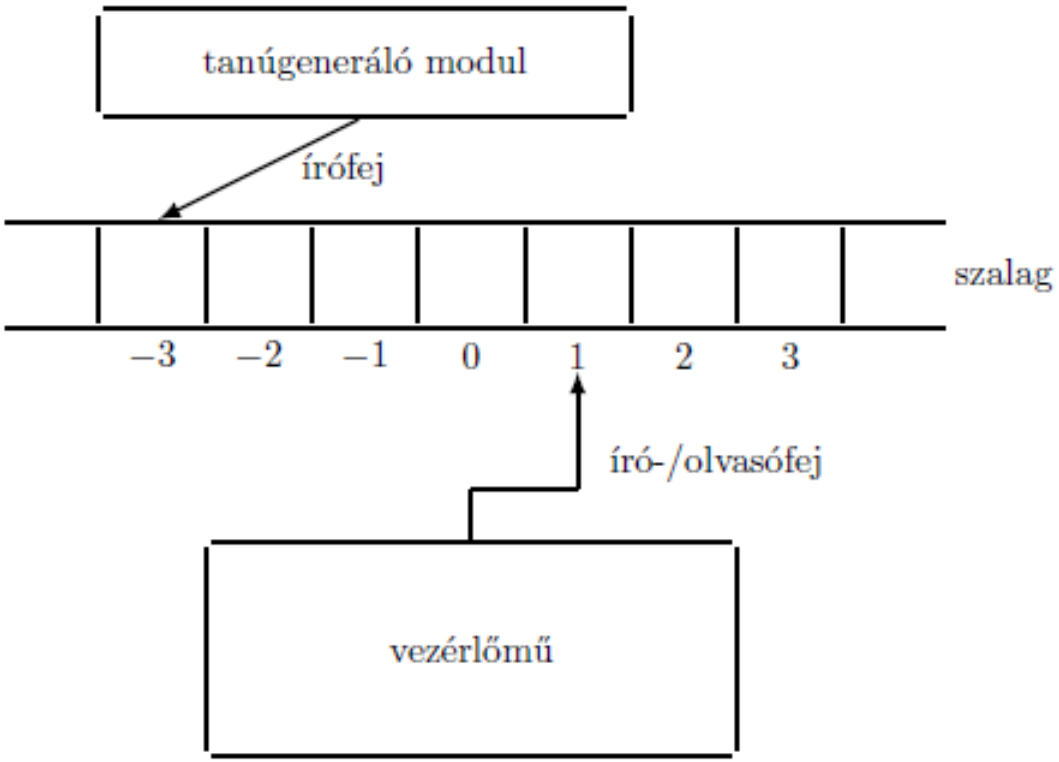
Nemdeterminisztikus esetben ez nem így van.

Pl. az UTAZÓÜGYNÖK feladatnál a kérdés az, hogy létezik-e olyan bejárás, amely B-nél nem hosszabb.

A komplementer feladat az lenne, hogy be kell bizonyítani, hogy nem létezik olyan bejárás, amely nem hosszabb mint B. Ezt nem tudjuk megoldani polinomiális idejű nemdeterminisztikus algoritmussal.

NP osztály — formalizálva

Nemdeterminisztikus Turing-gép



Két fázis:

1. Kezdetben a vizsgálandó szó a szalagon van az 1. rekesztől jobbra. A tanút ráírja a szalagra -1-től balra.

2. Ellenőrzés (amikor csak a vezérlőmű működik, de vizsgálja a tanút is.)

Nemdeterminisztikus számítás

Egy M NDTM program esetében sok teljes számítási folyamat létezik. Akkor fogadja el (ismeri fel) a szót, ha ezek közül legalább egy végállapotban végződik. Az M által felismert nyelv

$$L_M = \left\{ x \in \Sigma^* \mid M \text{ elfogadja } x\text{-et} \right\}$$

Az x elfogadásának ideje a legkevesebb lépesből álló teljes elfogadó számítási folyamat lépésszáma.
Az időbonyolultság függvény $T_M : \mathbf{Z}^* \to \mathbf{Z}^*$

$$T_M(n) = \max \left\{ \{1\} \cup \left\{ m \in \mathbf{Z}^* \;\middle|\; \begin{array}{l} \exists x \in L_M, |x| = n, \text{és } M \text{ az } x\text{-et} \\ m \text{ lépesben fogadja el} \end{array} \right\} \right\}$$

Abban az esetben, ha M egyetlen n hosszúságú szót sem ismer fel, akkor a fenti érték 1.

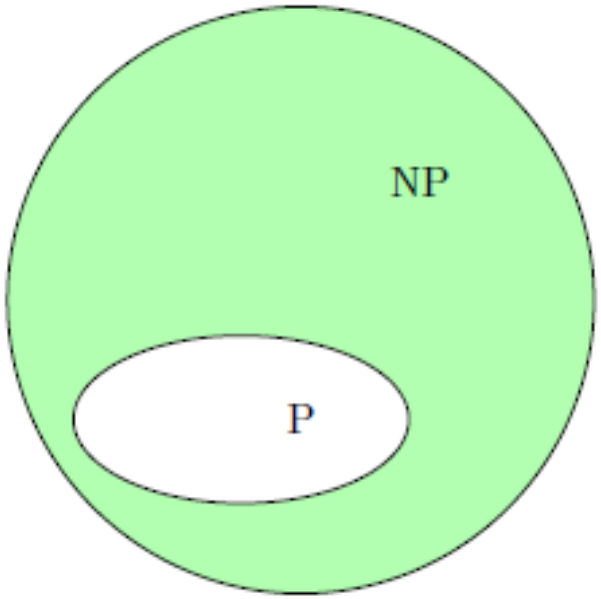
NP osztály — formális definíció

Ha létezik egy p polinom úgy, hogy $T_M(n) \leq p(n)$ tetszőleges $n \geq 1$-re, akkor M polinomiális idejű nemdeterminisztikus (NDTM) program.

Az NP osztály formális definíciója:

$$\text{NP} = \left\{ L \subseteq \Sigma^* \;\middle|\; \exists \,\text{polinomiális idejű NDTM program, amelyre } L_M = L \right\}$$

P és NP osztályok kapcsolata



$P \subseteq NP$

Tétel

Ha $\Pi \in$ NP, akkor létezik egy p polinom, és Π megoldható olyan determinisztikus algoritmussal, amelynek az időbonyolultsága $O\left(2^{p(n)}\right)$, ahol n a bemenet nagysága.

A $L_1 \subseteq \Sigma_1^*$ nyelv polinomiálisan átalakítható az $L_2 \subseteq \Sigma_2^*$ nyelvvé, ha létezik egy $f : \Sigma_1^* \to \Sigma_2^*$ függvény, amelyre a következő két feltétel teljesül:

1. Létezik egy polinomiális idejű DTM program, amely kiszámítja az f függvényt.
2. Minden $x \in \Sigma_1^*$-re $x \in L_1$ akkor és csakis akkor, ha $f(x) \in L_2$.

Jelölése: $L_1 \propto L_2$.

Lemma

Ha $L_1 \propto L_2$, akkor $L_2 \in P$-ből következik, hogy $L_1 \in P$
(vagy ami ezzel egyenértékű: ha $L_1 \notin P$, akkor $L_2 \notin P$).

Ha Π_1 és Π_2 döntési feladatok, $\Pi_1 \propto \Pi_2$ (polinomiálisan átalakítható) ha létezik $f : D_{\Pi_1} \to D_{\Pi_2}$ úgy, hogy

1. f polinomiálisan kiszámítható algoritmus,
2. Minden $I \in D_{\Pi_1}$-re $I \in Y_{\Pi_1}$ akkor és csakis akkor, ha $f(I) \in Y_{\Pi_2}$.

Példa:

Hamilton-kör

ÁLTALÁNOS ESET: Adott egy $G = (V, E)$ gráf.
KÉRDÉS: Létezik-e G-ben Hamilton-kör?

Bebizonyítjuk, hogy HAMILTON-KÖR $\propto$ UTAZÓÜGYNÖK.
Ehhez definiálni kell egy f függvényt, amely a HAMILTON-KÖR minden esetéhez hozzárendeli az UTAZÓÜGYNÖK egy esetét.

Ha $|V| = n$, legyen adott egy Hamilton-kör a G gráfban. Ugyanezek a csúcsok lesznek az UTAZÓÜGYNÖK feladat csúcsai. Definiáljuk a távolságot: $d(v_i, v_j) = 1$ ha $(v_i, v_j) \in E$ és 2 különben. Legyen $B = n$.

Könnyű belátni, hogy ez az átalakítás polinomiális. A második követelmény: egy Hamilton-kör egyben egy megfelelő bejárás és fordítva.

Lemma

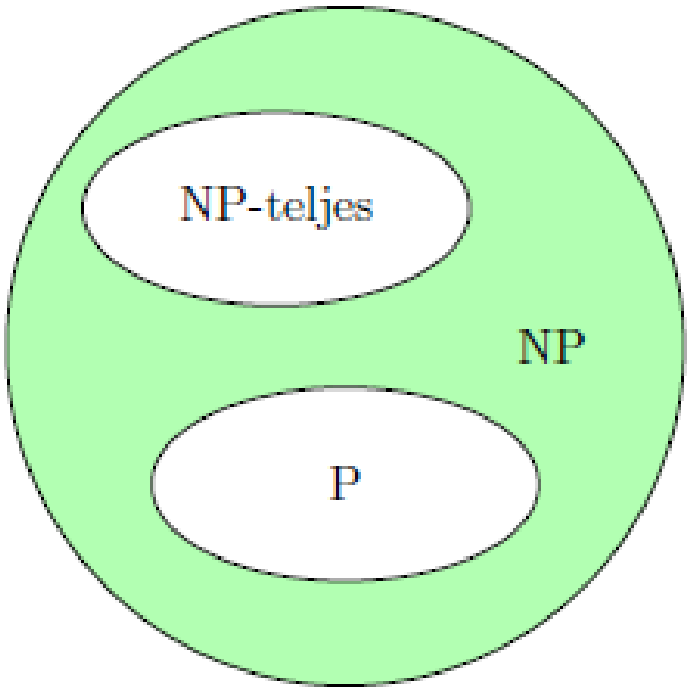
Ha $L_1 \propto L_2$ és $L_2 \propto L_3$, akkor $L_1 \propto L_3$.

Egy L nyelv NP-teljes, ha $L \in$ NP és minden $L' \in$ NP-re $L' \propto L$.

Egy Π döntési feladat NP-teljes, ha $\Pi \in$ NP és minden $\Pi' \in$ NP-re $\Pi' \propto \Pi$.

Az NP-teljes feladatok a legnehezebbek. Ha egy NP-teljes feladat *megoldható lenne* polinomiális időben, akkor minden NP-beli feladat polinomiális lenne.

Ha P $\neq$ NP, akkor ha Π NP-teljes, akkor $\Pi \in$ NP $\setminus$ P.



Lemma

Ha $L_1 \in NP$, $L_2 \in NP$, L_1 NP-teljes és $L_1 \propto L_2$, akkor L_2 is NP-teljes.

Ahhoz, hogy bebizonyítsuk, hogy egy Π döntési feladat NP-teljes a következőket kell bizonyítani:

1. $\Pi \in$ NP, és
2. létezik egy NP-teljes Π' feladat úgy, hogy $\Pi' \propto \Pi$.

NP-teljesség

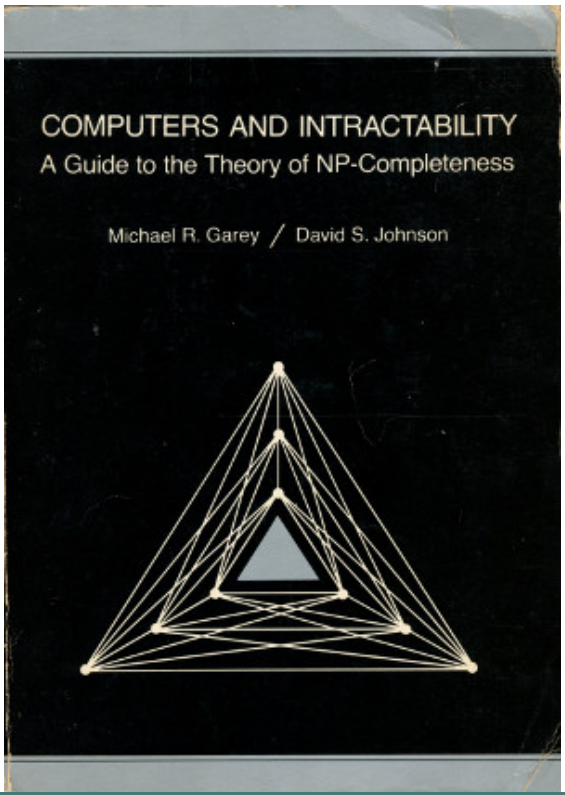
Egy L nyelv NP-teljes, ha $L \in$ NP és minden $L' \in$ NP-re $L' \propto L$.

Egy Π döntési feladat NP-teljes, ha $\Pi \in$ NP és minden $\Pi' \in$ NP-re $\Pi' \propto \Pi$.

Ahhoz, hogy bebizonyítsuk, hogy egy Π döntési feladat NP-teljes a következőket kell bizonyítani:

1. $\Pi \in$ NP, és
2. létezik egy NP-teljes Π' feladat úgy, hogy $\Pi' \propto \Pi$.

Megnézzük a Garey–Johnson-könyvben!



[GT12] PARTITION INTO ISOMORPHIC SUBGRAPHS

INSTANCE: Graphs $G=(V,E)$ and $H=(V',E')$ with $|V|=q|V'|$ for some $q \in Z^+$.

QUESTION: Can the vertices of G be partitioned into q disjoint sets $V_1, V_2, \ldots, V_q$ such that, for $1 \leqslant i \leqslant q$, the subgraph of G induced by V_i is isomorphic to H?

Reference: [Kirkpatrick and Hell, 1978]. Transformation from 3DM.

Comment: Remains NP-complete for any fixed H that contains at least 3 vertices. The analogous problem in which the subgraph induced by V_i need only have the same number of vertices as H and contain a subgraph isomorphic to H is also NP-complete, for any fixed H that contains a connected component of three or more vertices. Both problems can be solved in polynomial time (by matching) for any H not meeting the stated restrictions.

[GT13] PARTITION INTO HAMILTONIAN SUBGRAPHS

INSTANCE: Directed graph $G=(V,A)$.

QUESTION: Can the vertices of G be partitioned into disjoint sets $V_1, V_2, \ldots, V_k$, for some k, such that each V_i contains at least three vertices and induces a subgraph of G that contains a Hamiltonian circuit?

Reference: [Valiant, 1977a]. Transformation from 3SAT. (See also [Herrmann, 1973]).

Comment: Solvable in polynomial time by matching techniques if each V_i need only contain at least 2 vertices [Edmonds and Johnson, 1970]. The analogous problem for undirected graphs can be similarly solved, even with the requirement that $|V_i| \geqslant 3$. However, it becomes NP-complete if we require that $|V_i| \geqslant 6$ [Papadimitriou, 1978d] or if the instance includes an upper bound K on k.

SATISFIABILITY (KIELÉGÍTHETŐSÉG) — SAT: az első NP-teljes feladat

$U = \{u_1, u_2, \ldots, u_m\}$ Boole-változók halmaza

$t : U \to \{T, F\}$ T igaz, F hamis (vagy: 1 igaz, 0 hamis) (értékadás)

literál: u és $\overline{u}$ ($\overline{u}$ az u tagadása)

klóz: literálok halmaza, pl: $\{u_1, \overline{u_2}, u_3\}$

Egy klóz akkor igaz, ha valamelyik literálja igaza.
(A klóz tulajdonképpen a literálok diszjunkciója.)

Pl. a fenti klóz csak akkor hamis, ha $u_1 = F$, $u_2 = T$, $u_1 = F$, minden más esetben igaz, azaz minden más értékadás kielégíti a klózt.

A változók akkor elégítenek ki egy klózhalmazt, ha minden elemét (minden egyes klózt) kielégítenek (tulajdonképpen klózok konjunkciójáról van szó).

Kielégíthetőség

ÁLTALÁNOS ESET: Adott a változók U halmaza, és az U elemeiből képzett C klózhalmaz.

KÉRDÉS: Létezik-e a változóknak olyan értékadása, amely kielégíti C-t?

Példa:

1. $U = \{u_1, u_2\}$, $C = \left\{\{u_1, \overline{u}_2\}, \{\overline{u_1}, u_2\}\right\}$

   $t(u_1) = t(u_2) = T$ kielégíti C-t.

2. $U = \{u_1, u_2\}$, $C = \left\{\{u_1, u_2\}, \{u_1, \overline{u}_2\}, \{\overline{u_1}\}\right\}$

   Egyetlen értékadás sem elégíti ki.

u_1	u_2	$\{u_1, u_2\}$	$\{u_1, \overline{u}_2\}$	$\{\overline{u_1}\}$	C
T	T	T	T	F	F
T	F	T	T	F	F
F	T	T	F	T	F
F	F	F	T	T	F

Cook tétele (1971)

Tétel

A KIELÉGÍTHETŐSÉG *probléma NP-teljes.*

Bizonyítás:
Könnyű belátni, hogy a feladat NP osztálybeli.

$L_{SAT} = L[SAT, e]$ egy megfelelő kódolással. Be kell bizonyítani, hogy minden $L \in NP$ nyelvre, $L \propto L_{SAT}$. Minden nyelv NP-ből megadható egy polinomiális idejű NDTM programmal, amely felismeri.
A bizonyításhoz meg kell adjuk egy tetszőleges polinomiális idejű NDTM programot és annak polinomiális idejű transzformációját L_{SAT}-ra. Ekkor ez a transzformáció átalakít egy tetszőleges M polinomiális idejű NDTM program által felismert L_M nyelvet az L_{SAT}-ra. Így egyszerre bizonyítjuk, hogy minden $L \in NP$ nyelvre, $L \propto L_{SAT}$.

Cook tétele — folytatás

Legyen M az L nyelvet felismerő polinomiális idejű NDTM program ($L = L_M$). Ennek adatai: $Q, \Sigma, \Gamma, \delta, q_0, q_Y, q_N, B$. Legyen p egy polinom, amelyre $T_M(n) \leq p(n)$. (Feltehetjük, hogy $T_M(n) \geq p(n)$). Az általános átalakító f_L függvényt a fentiek függvényében adjuk meg.

Legyen f_L olyan függvény, amely Σ^* elemeit alakítja a SAT egy esetévé (és nem a SAT egy kódolt esetévé, mivel ez a kódolás könnyen megoldható).
Tehát az f_L azzal a tulajdonsággal rendelkezik, hogy

$$x \in L \subseteq \Sigma^* \iff f_L(x) \text{ kielégíthető.}$$

Cook tétele — folytatás

Az f_L változóinak halmaza legyen U. Legyenek

Q elemei: $q_0, q_1 = q_Y, q_2 = q_N, q_3, \ldots, q_r \left(r = |Q| - 1\right)$,

Γ elemei: $s_0 = B, s_1, s_2 \ldots, s_\nu \left(\nu = |\Gamma| - 1\right)$.

Az f_L változói és azok jelentése:

változó	hatáskör	jelentés
$Q[i,k]$	$0 \le i \le p(n)$ $0 \le k \le r$	Az i időpontban M a q_k állapotban van.
$H[i,j]$	$0 \le i \le p(n)$ $-p(n) \le j \le p(n)+1$	Az i időpontban az író/olvasófej a szalag j-edik elemét viszgálja.
$S[i,j,k]$	$0 \le i \le p(n)$ $-p(n) \le j \le p(n)+1$ $0 \le k \le \nu$	Az i időpontban a szalag j-edik eleme s_k-t tartalmazza.

A 0-dik pillanatban a szalagon az $1..n$ elemek tartalmazzák az x bemenetet ($n = |x|$), a $-1..-|w|$ elemek pedig a w tanút.

Cook tétele — folytatás

Az M egy számítása megfelel egy, az U változókkal képzett igaz értékű logikai formulának Fordítva nem igaz). Ha a számítás hamarabb megáll, mint $p(n)$, akkor úgy tekintjük, hogy az automata abban a végállapotban marad, ugyazon az elemen, és megmarad a szalag tartalma.

Az f_L függvény ezekkel változókkal egy olyan klózhalmazt hoz létre, amely csak akkor és csakis akkor kielégíthtő, ha a megfelelő számítási folyamat felismeri x-et. Tehát:

$x \in L$ $\Leftrightarrow$ Létezik M-nek egy x-et elfogadó számítási folyamata.

$\Leftrightarrow$ Létezik M-nek egy x-et elfogadó számítási folyamata, amely legfeljebb $p(n)$ lépésben végzi az ellenőrző fázist, ha a tanú pontosan $p(n)$ hosszúságú.

$\Leftrightarrow$ Az $f_L(x)$ klózhalmaz kielégíthető.

Cook tétele — folytatás

Az $f_L(x)$ klózai 6 csoportba oszthatók:

klózcsoport	megszorítások
G_1	Minden i-edik időpontban M egyetlen egy állapotban van.
G_2	Minden i-edik időpontban az író/olvasófej egy elemet vizsgál.
G_3	Minden i-edik időpontban a szalag minden eleme egy betűt tartalmaz.
G_4	A 0-dik időpontban az automata kezdő konfigurációban van.
G_5	A $p(n)$ időpontban az automata q_Y állapotban van.
G_6	Minden i-edik időpontban $\Big(0 \leq i < p(n)\Big)$ egyetlen átmenet van a következő időpontba.

Cook tétele — folytatás

A G_1 csoport klózai:

$$\Big\{Q[i,0], Q[i,1], \ldots, Q[i,r]\Big\}, \; 0 \leq i \leq p(n)$$

$$\Big\{\overline{Q[i,j]}, \overline{Q[i,j']}\Big\}, \; 0 \leq i \leq p(n), \; 0 \leq j < j' \leq r$$

Az első $p(n)+1$ klóz egyidejűleg igaz, ha M minden i időpontban *legalább egy állapotban* van.

A következő $\big(p(n)+1\big)\big(r(r+1)/2\big)$ klóz egyidejűleg igaz, ha nincs olyan i időpont, hogy M *egynél több állapotban* van.

Cook tétele — folytatás

A G_2 csoport klózai:

$$\Big\{H[i,-p(n)], H[i,-p(n)+1], \ldots, H[i,p(n)+1]\Big\}, \; 0 \leq i \leq p(n)$$

$$\Big\{\overline{H[i,j]}, \overline{H[i,j']}\Big\}, \; 0 \leq i \leq p(n), \; -p(n) \leq j < j' \leq p(n)+1$$

Az első $p(n)+1$ klóz egyidejűleg igaz, ha M minden i időpontban *legalább egy szalagelemet* vizsgál.

A következő klózok egyidejűleg igazak, ha nincs olyan i időpont, hogy M *egynél több szalagelemet* vizsgál.

Cook tétele — folytatás

A G_3 csoport klózai:

$$\Big\{S[i,j,0], S[i,j,1], \ldots, S[i,j,\nu]\Big\}, \; 0 \leq i \leq p(n), \; -p(n) \leq j \leq p(n)+1$$

$$\Big\{\overline{S[i,j,k]}, \overline{S[i,j,k']}\Big\}, \; 0 \leq i \leq p(n), \; -p(n) \leq j \leq p(n)+1, \; 0 \leq k < k' \leq \nu$$

Az első sorbeli klózok egyidejűleg igazak, ha minden i időpontban minden szalagcella *legalább egy betűt* tartalmaz Γ-ból.

A következő klózok egyidejűleg igazak, ha nincs olyan i időpont és szalagcella, hogy *egynél több betű* legyen abban a cellában.

Cook tétele — folytatás

A G_4 csoport klózai:

$$\Big\{Q[0,0]\Big\},\ \Big\{H[0,1]\Big\},\ \Big\{S[0,0,0]\Big\}$$

$$\Big\{S[0,1,k_1], S[0,2,k_2], \ldots, S[0,n,k_n]\Big\},$$

$$\Big\{S[0,n+1,0], S[0,n+2,0], \ldots, S[0,p(n)+1,0]\Big\},$$

ahol $x = s_{k_1} s_{k_2} \ldots s_{k_n}$

Cook tétele — folytatás

A G_5 csoport klózai:

$Q[p(n), 1]$

A $p(n)$ időpontban az automata végállapotban van ($q_1 = q_Y$).

Cook tétele — folytatás

A G_6 csoport klózai esetében azt kell leírni, hogy a számítási folyamat mindegyik konfigurációjából egyetlen lépéssel jutunk a következő konfigutrációba.

A klózok két alcsoportba oszthatók.

Az első alcsoport klózai azt biztosítják, hogy ha az automata az i-edik időpontban nem vizsgálja a j-edik cellát, akkor a j-edik cella tartalma nem változik, amikor áttérünk i-ről $(i+1)$-re:

$$\left\{\overline{S[i,j,l]}, H[i,j], S[i+1,j,l]\right\}, 0 \leq i < p(n), -p(n) \leq j \leq p(n)+1, 0 \leq l \leq \nu$$

Cook tétele — folytatás

Az következő alcsoport klózai azt biztosítják, hogy az átmenet egyik konfigurációból a másikba a δ átmenetfüggvény szerint történik.
Ha $0 \leq i < p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq r$ és $0 \leq l \leq \nu$, akkor

$$\left\{\overline{H[i,j]}, \overline{Q[i,k]}, \overline{S[i,j,l]}, H[i+1, j+\Delta]\right\}$$

$$\left\{\overline{H[i,j]}, \overline{Q[i,k]}, \overline{S[i,j,l]}, Q[i+1, k']\right\}$$

$$\left\{\overline{H[i,j]}, \overline{Q[i,k]}, \overline{S[i,j,l]}, S[i+1, j, l']\right\}$$

ahol ha $q \in Q \setminus \{q_y, q_N\}$, akkor Δ, k', l' értékei olyanok, hogy $\delta(q_k, s_l) = (q_{k'}, s_{l'}, \Delta)$, ha pedig $q_k \in \{q_Y, q_N\}$, akkor $\delta(q_k, s_l) = (q_k, s_l, 0)$

Cook tétele — folytatás

$C = G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5 \cup G_6$

Ha $x \in L$, akkor létezik egy legfeljebb $p(n)$ hosszúságú elfogadó számítási folyamat, amelyre a C klózhalmaz kielégíthető (C igaz), és fordítva minden olyan értékekre, amelyekre C igaz, a számítási folyamat elfogadó.

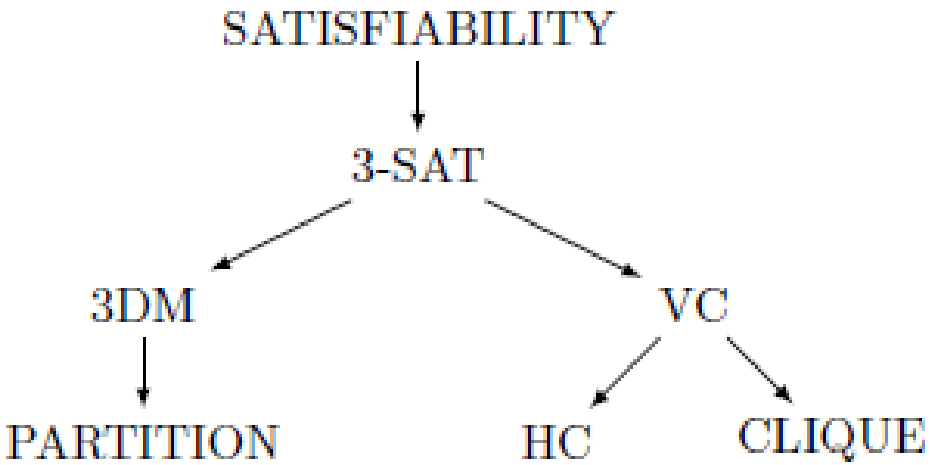
Még bizonyítani kell, hogy $f_L(x)$ polinomiális időben előállítható. Bebizonyítható, hogy $|f_L)(x)| = O(p(n)^4)$.

qu.e.d.

NP-teljesség bizonyítása

Egy Π feladat NP-teljességének bizonyítása:

1. bizonyítani kell, hogy $\Pi \in$ NP,
2. keresni kell egy ismert Π' NP-teljes feladatot,
3. meg kell adni egy $f : \Pi' \to \Pi$ függvényt,
4. bizonyítani kell, hogy f polinomiális idejű átalakítás.



SATISFIABILITY = KIELÉGÍTHETŐSÉG
3SAT = 3-változós KIELÉGÍTHETŐSÉG
3DM = 3-dimenziós PÁROSÍTÁS
VC = CSÚCSLEFEDÉS
CLIQUE = TELJES RÉSZGRÁF (KLIKK)
HC = HAMILTON-KÖR
PARTITION = FELBONTÁS (PARTÍCIÓ)

3SAT

ÁLTALÁNOS ESET: Adott a $C = \{c_1, c_2, \ldots, c_m\}$ klózhalmaz egy véges U változóhalmazon, ahol $|c_i| = 3$, $1 \leq i \leq m$.

KÉRDÉS: Kielégíthető-e C?

3-DIMENSIONAL MATCHING (3DM)

ÁLTALÁNOS ESET: Adott $M \subseteq W \times X \times Y$, ahol W, X, Y mindegyike q-elemű halmaz, és diszjunktak.

KÉRDÉS: Létezik-e M-ben teljes párosítás, azaz olyan $M' \subseteq M$, hogy $|M'| = q$, és M' elemei minden koordinátában különböznek?

VERTEX COVER (VC)

ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf és egy pozitív $K \leq |V|$.

KÉRDÉS: Létezik-e egy legfeljebb K elemű csúcslefedés? Azaz $\exists V' \subseteq V$ úgy, hogy $|V'| \leq K$ és a gráf minden $\{u, v\}$ éle esetében vagy $u \in V'$ vagy $v \in V'$?

CLIQUE

ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf és egy pozitív $J \leq |V|$.
KÉRDÉS: Létezik-e G-ben egy legalább J csúcsú teljes részgráf? Azaz, $\exists V' \subseteq V$ úgy, hogy $|V'| \geq J$ és V' bármely két csúcsát az E egy éle köti össze?

HAMILTONIAN CIRCUIT (HC)

ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf.
KÉRDÉS: Van-e G-ben Hamilton-kör? Azaz, $\exists < v_1, v_2, \ldots, v_n >$, $v_i \in V$, $1 \leq i \leq n$, $n = |V|$ úgy, hogy $\{v_n, v_1\} \in E$ és $\{v_i, v_{i+1}\} \in E$, $1 \leq i < n$?

PARTITION

ÁLTALÁNOS ESET: Adott egy A véges halmaz, és egy súlyfüggvény $s : A \to \mathbf{Z}^+$.
KÉRDÉS: Létezik-e $A' \subseteq A$ úgy, hogy $\sum_{a \in A'} s(a) = \sum_{a \in A \setminus A'} s(a)$?

Tétel

A 3SAT feladat NP-teljes.

Bizonyítás:
Legyen $U = \{u_1, u_2, \ldots, u_n\}$ a változók, $C = \{c_1, c_2, \ldots, c_m\}$ a klózok halmaza. C megfelel egy elfogadó számítási folyamatnak.

Értelmezünk egy C' 3-literálos klózhalmazt, amelynek változói U'-ből vannak: $U' = U \cup \left\{ \bigcup_{j=1}^{m} U'_j \right\}$, $C = \bigcup_{j=1}^{m} C'_j$.

Meg kell mutatnunk, hogyan készül C'_j és U'_j a c_j klózokból.

Legyen $c_j = \{z_1, z_2, \ldots, z_k\}$, ahol minden z_i az U változóiból képzett literál.

A C'_j és U'_j előállítása függ k értékétől:

1. eset $k = 1$: $U'_j = \{y_j^1, y_j^2\}$
$$C'_j = \{\{z_1, y_j^1, y_j^2\}, \{z_1, y_j^1, \overline{y}_j^2\}, \{z_1, \overline{y}_j^1, y_j^2\}, \{z_1, \overline{y}_j^1, \overline{y}_j^2\}\}$$

2. eset $k = 2$: $U'_j = \{y_j^1\}$, $C'_j = \{z_1, z_2, y_j^1\}, \{z_1, z_2, \overline{y}_j^1\}$

3. eset $k = 3$: $U'_j = \emptyset$, $C'_j = \{c_j\}$

4. eset $k > 3$: $U'_j = \{y_j^i \mid 1 \leq i \leq k-3\}$
$$C'_j = \{\{z_1, z_2, y_j^1\}\} \cup \{\{\overline{y}_j^i, z_{i+2}, y_j^{i+1}\} \mid 1 \leq i \leq k-4\} \cup \{\{y_j^{k-3}, z_{k-1}, z_k\}\}$$

Be kell bizonyítani, hogy C' akkor és csakis akkor kielégíthető, ha C kielégíthető.

Legyen $t : U \to \{T, F\}$ egy olyan értékadás, amely kielégíti C-t. Értelmezzük a $t' : U' \to \{T, F\}$ (t-t kiterjesztő) értékadást, amely kielégíti C'-t. Elég, ha a t' függvényt U'_j-n értelmezzük.

Az 1. és 2. esetben: C'_j-t már t kielégíti, ezért a kiterjesztés tetszőleges lehet, pl. $t'(y) = T$, $\forall y \in U'_j$.

A 3. esetben U'_j üres, ezért t kielégíti C'_j-et.

4. eset: Mivel t kielégíti C-t, kell léteznie olyan l egésznek, amelyre $t(z_l) = T$.

Ha $l = 1$ vagy 2, legyen $t'(y^i_j) = F$, ha $1 \leq i \leq k - 3$.

Ha $l = k - 1$ vagy k, legyen $t'(y^i_j) = T$, ha $1 \leq i \leq k - 3$.

Különben legyen $t'(y^i_j) = T$, ha $1 \leq i \leq l - 2$ és $t'(y^i_j) = F$, ha $l - 1 \leq i \leq k - 3$.

Könnyű belátni, hogy ez az értékadás kielégíti C'-et.
Fordítva: Ha t' kielégíti C'-et, akkor t' leszűkítése U-ra kielégíti C-t.

Az átalakítás polinomiális időben elvégezhető.

Érdekes, hogy a 2SAT probléma polinomiális, azaz P-ben van (ez a rezolúciós módszerrel könnyen belátható).

Vertex Cover és Clique

Ez a két feladat nagyon hasonlít egymáshoz, és a következőhöz.

INDEPENDENT SET (független csúcshalmaz)
ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf, és $J \leq |V|$ pozitív szám.
KÉRDÉS: Létezik-e $V' \subseteq V$, $|V'| \geq J$ úgy, hogy ha $u, v \in V'$, akkor $\{u, v\} \notin E$?

Lemma

Tetszőleges $G = (V, E)$ gráfra és $V' \subseteq V$-re a következő kijelentések egyenértékűek:

- *V' lefedő csúcshalmaz G-ben.*
- *$V \setminus V'$ független csúcshalmaz.*
- *$V \setminus V'$ teljes gráf (klikk) a G gráf komplementerében.*

Tétel

A VERTEX COVER feladat NP-teljes.

Bizonyítás.

íKönnyű belátni, hogy a feladat NP-ben van, hisz csak azt kell megvizsgálni polinomiális időben, hogy egy adott csúcshalmaz (a tanú) illeszkedik-e minden élhez.

A 3SAT feladatot transzformáljuk VC feladattá. Legyen a 3SAT egy esete: $U = \{u_1, u_2, \ldots, u_n\}$, $C = \{c_1, c_2, \ldots, c_m\}$.

Meghatározunk egy $G = (V, E)$ gráfot és egy pozitív $K \leq |V|$ számot úgy, hogy G-ben van egy legfeljebb K csúcsú lefedő halmaz, akkor és csakis akkor, ha C kielégíthető.

A gráfot részenként hozzuk létre.

A gráf első része:

Minden $u_i \in U$ változóra legyen $T_i = (V_i, E_i)$, ahol $V_i = \{u_i, \overline{u}_i\}$, $E_i = \big\{\{u_i, \overline{u}_i\}\big\}$.

A gráf második része:

Minden $c_j \in C$ klózra legyen $S_j = (V'_j, E'_j)$:

$$V'_j = \big\{a_1[j], a_2[j], a_3[j]\big\}$$
$$E'_j = \big\{\{a_1[j], a_2[j]\}, \{a_1[j], a_3[j]\}, \{a_2[j], a_3[j]\}\big\}$$

A gráf harmadik része:

Minden $c_j \in C$ klóz esetében legyen x_j, y_j, z_j a három használt literál. Ekkor S_j csúcsai között definiáljuk a következő éleket:

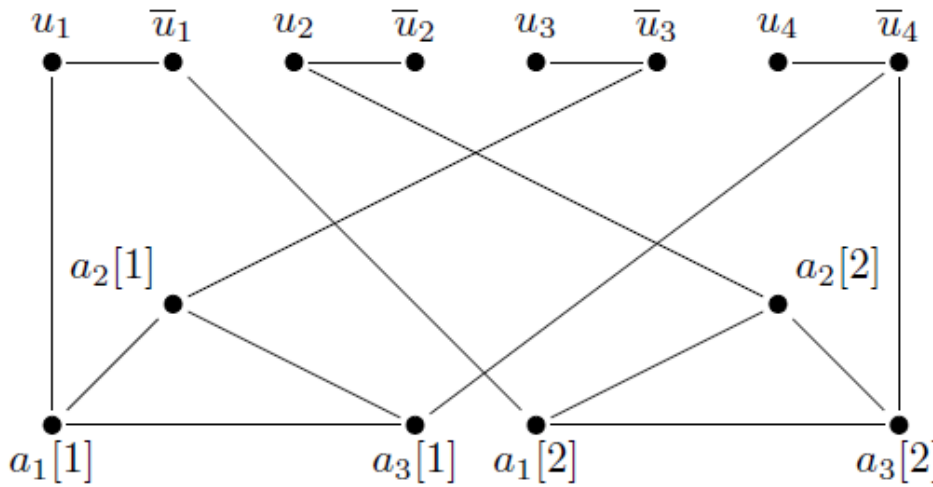
$$E''_j = \Big\{\{a_1[j], x_j\}, \{a_2[j], y_j\}, \{a_3[j], z_j\}\Big\}$$

Legyen $K = n + 2m$ és $G = (V, E)$, ahol

$$V = \left(\bigcup_{i=1}^{n} V_i\right) \cup \left(\bigcup_{j=1}^{m} V'_j\right)$$

$$E = \left(\bigcup_{i=1}^{n} E_i\right) \cup \left(\bigcup_{j=1}^{m} E'_j\right) \cup \left(\bigcup_{j=1}^{m} E''_j\right)$$

Példa:



$U = \{u_1, u_2, u_3, u_4\}$, $C = \{\{u_1, \overline{u}_3, \overline{u}_4\}, \{\overline{u}_1, u_2, \overline{u}_4\}\}$

Könnyű belátni, hogy az átalakítás polinomiális.
Elég bizonyítani, hogy C akkor és csakis akkor kielégíthető, ha G-ben létezik legfeljebb K csúcsból álló lefedés.

V' lefedő csúcshalmaz $\Rightarrow$ C kielégíthető

Legyen $V' \subseteq V$, $|V'| \leq K$ egy lefedő csúcshalmaz. Ennek tartalmazni kell legalább egy csúcsot minden T_i-ből, és legalább kettőt minden S_j-ből. Ez legalább $n + 2m = K$ csúcs, ezért V' pontosan egy csúcsot tartalmaz minden T_i-ből, és pontosan kettőt minden S_j-ből.

Legyen $t(u_i) = T$, ha $u_i \in V'$ és $t(u_i) = F$, ha $\overline{u}_i \in V'$.

Tekintsük az E''_j éleit (összesen 3 van), ezek közül csak kettőt tudnak lefedni a $V'_j \cap V'$ halmazból.

Ezért legalább egy élt ezek közül egy $V_i \cap V'$ halmazból való csúcs fed le. Ez vagy u_i vagy $\overline{u}_i$, de t értelmezése szerint ennek értéke mindig T.

Ezért minden c_j kielégíthető, tehát kielégíthető C is.

C kielégíthető $\Rightarrow$ V' lefedő csúcshalmaz

Legyen $t : U \to \{T, F\}$, amely kielégíti C-t. A megfelelő lefedő csúcshalmaz tartalmaz egy csúcsot minden T_i-ből, és kettőt minden S_j-ből. A $T_i \cap V'$-beli csúcs u_i ha $t(u_i) = T$, és $\overline{u}_i$ ha $t(u_i) = F$.

Ez biztosítja, hogy E''_j három éle közül legalább egy le van fedve. A másik kettő végpontjait bevesszük V'-be.

A kapott V' egy lefedő csúcshalmaz.

Egy L nyelv NP-teljes, ha $L \in$ NP és minden $L' \in$ NP-re $L' \propto L$.

Egy Π döntési feladat NP-teljes, ha $\Pi \in$ NP és minden $\Pi' \in$ NP-re $\Pi' \propto \Pi$.

Ahhoz, hogy bebizonyítsuk, hogy egy Π döntési feladat NP-teljes a következőket kell bizonyítani:

1. $\Pi \in$ NP, és
2. létezik egy NP-teljes Π' feladat úgy, hogy $\Pi' \propto \Pi$.

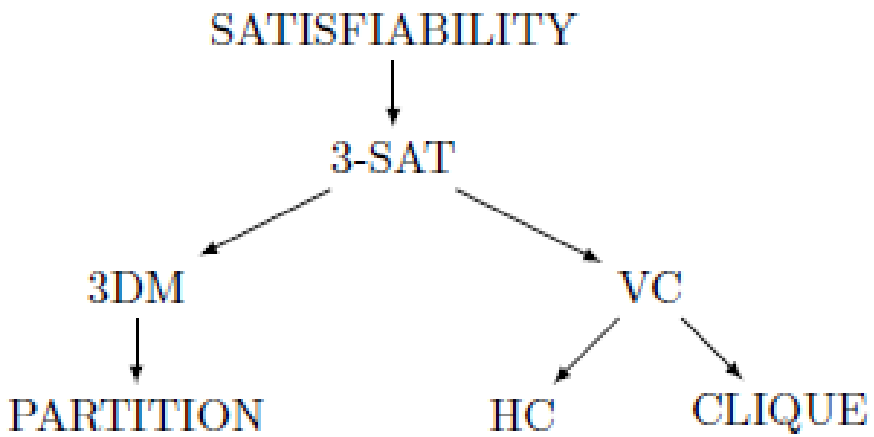
Tétel

A Hamilton-út feladat NP-teljes.

HAMILTONIAN CIRCUIT (HC)

ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf.

KÉRDÉS: Van-e G-ben Hamilton-kör? Azaz, $\exists < v_1, v_2, \ldots, v_n >$, $v_i \in V$, $1 \leq i \leq n$, $n = |V|$ úgy, hogy $\{v_n, v_1\} \in E$ és $\{v_i, v_{i+1}\} \in E$, $1 \leq i < n$?



VERTEX COVER (VC)

ÁLTALÁNOS ESET: Adott a $G = (V, E)$ gráf és egy pozitív $K \leq |V|$.

KÉRDÉS: Létezik-e egy legfeljebb K elemű csúcslefedés? Azaz $\exists V' \subseteq V$ úgy, hogy $|V'| \leq K$ és a gráf minden $\{u, v\}$ éle esetében vagy $u \in V'$ vagy $v \in V'$?

HC feladat NP-teljességének bizonyítása

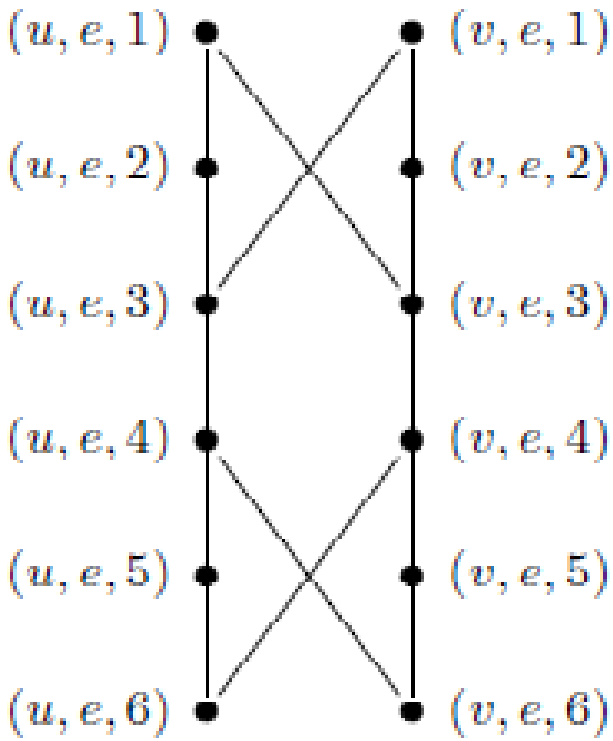
Hogy $HC \in$ NP, könnyű belátni.

A $G = (V, E)$ gráfhoz, amelyben van K lefog csúcs, hozzárendeljük a $G' = (V', E')$ gráfot, amelyben van HC. Legyenek $a_1, a_2, \ldots, a_K$ csúcsok.
Legyen minden $e = \{u, v\}$ élre:

$$V'_e = \{(u, e, i), (v, e, i)\} \mid 1 \leq i \leq 6\} \text{ és}$$

$$E'_e = \left\{\{u, e, i), (u, e, i+1)\} \mid 1 \leq i \leq 5\right\}$$
$$\cup \left\{\{(u, e, 3), (v, e, 1)\}, \{(v, e, 3), (u, e, 1)\right.$$
$$\cup \left\{\{(u, e, 6), (v, e, 4)\}, \{(v, e, 6), (u, e, 4)\right.$$

Minden $\{u, v\}$ élre:



A $v \in V$ csúcshoz illeszkedő élek: $e_{v[1]}, e_{v[2]}, \ldots, e_{v[deg(v)]}$, és ekkor

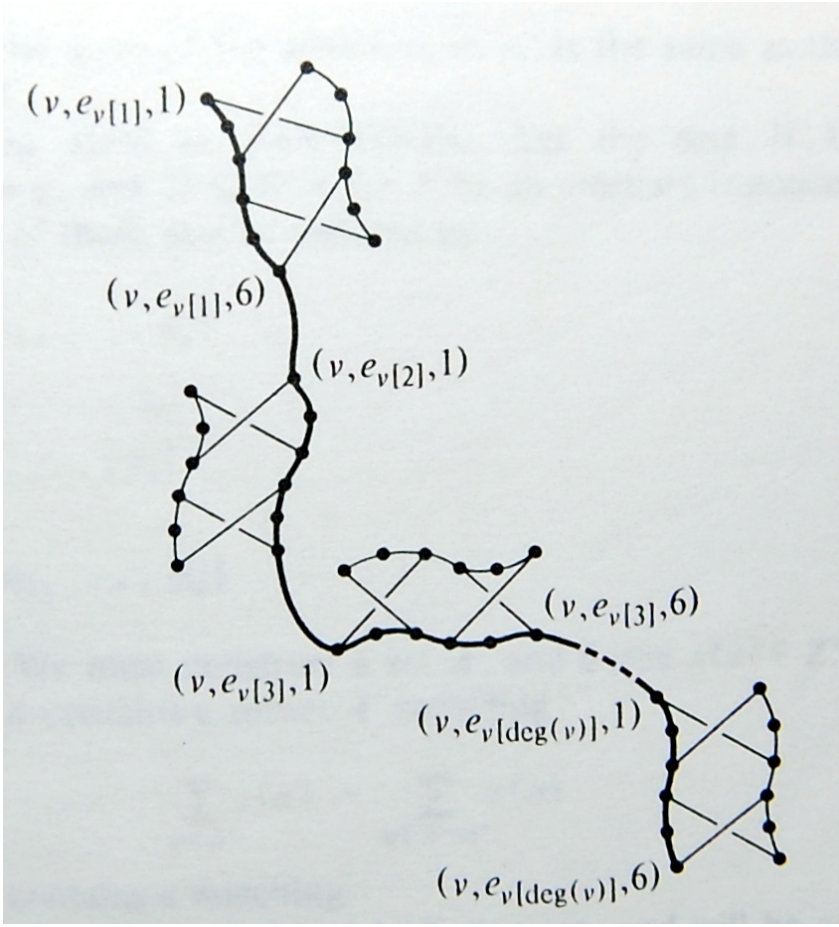
$$E'_v = \left\{ \{(v, e_{v[i]}, 6), (v, e_{v[i+1]}, 1)\} \,\middle|\, 1 \leq i < deg(v) \right\}$$

$$E'' = \left\{ \{a_i, (v, e_{v[1]}, 1)\}, \{a_i, (v, e_{v[deg(v)]}, 6)\} \,\middle|\, 1 \leq i \leq K, v \in V \right\}$$

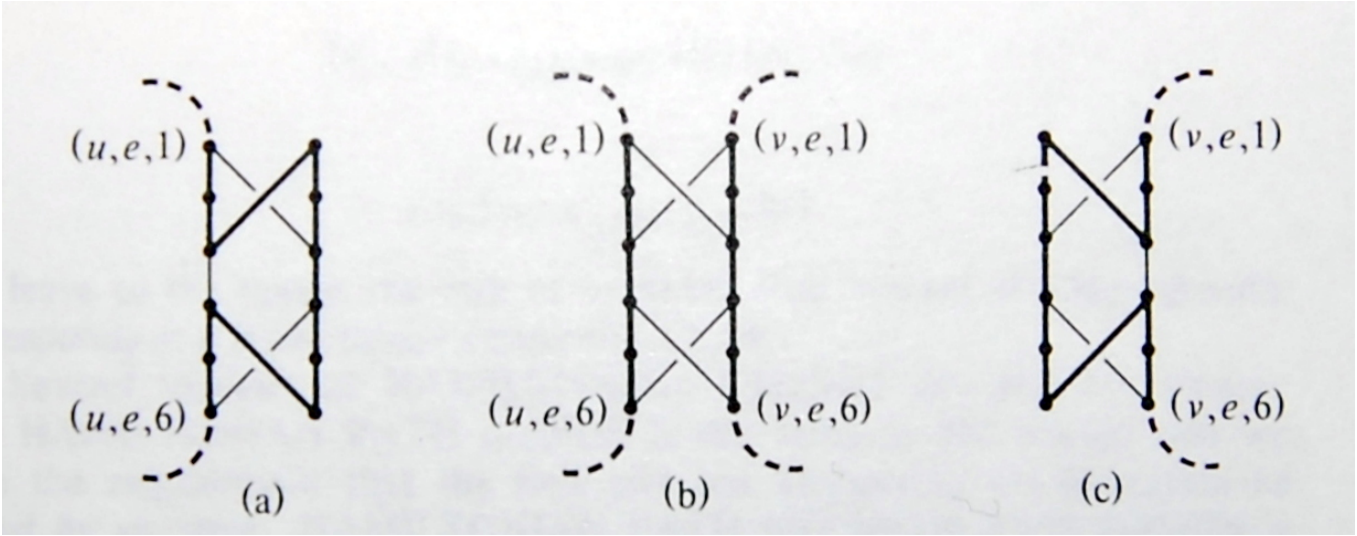
A $G' = (v'', E')$ gráf tehát:

$$V' = \{a_i \mid 1 \leq i \leq K\} \cup \left(\bigcup_{e \in E} V'_e \right)$$

$$E' = \left(\bigcup_{e \in E} E'_e \right) \cup \left(\bigcup_{v \in V} E'_v \right) \cup E''$$



(Garey-Johnson)



(Garey-Johnson)

Ha H Hamiltom-út: két a_i közötti rész azon élekből készült, amelyek egy csomóponthoz illeszkednek. Tehát ezek a csúcsok lefogó csúcsok lesznek.

Fordítva: Legyen V^* egy lefogó csúcshalmaz, $|V^*| = k$. $\{u, v\} \in E$, és ha $\{u, v\} \cap V^*$ rendre egyenő $\{u\}$, $\{u, v\}$ vagy $\{u, v\}$, akkor rendre válasszuk az ábra a), b) vagy c) szerinti csúcsait, majd a következőket:

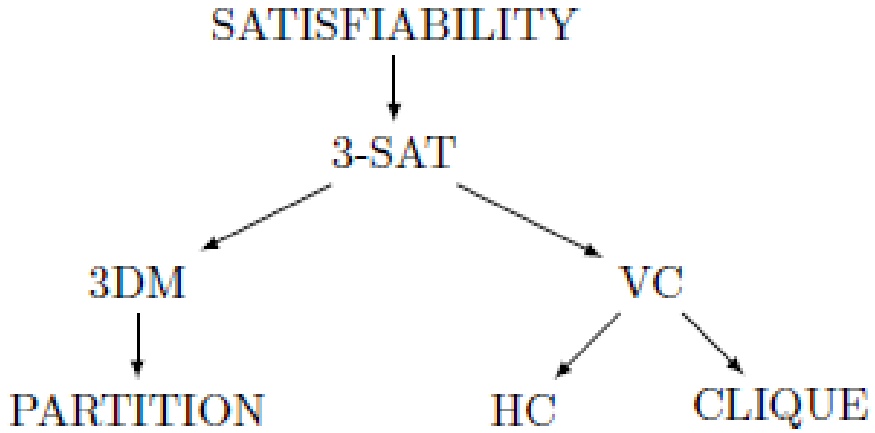
$\{a_i, (v_i, e_{v_i[1]}, 1)\}$, $1 \leq i \leq K$,
$\{a_{i+1}, (v_i, e_{v_i[deg(v_i)]}, 6)\}$, $1 \leq i \leq K$ és
$\{a_1, (v_K, e_{v_K[deg(v_K)]}, 6)\}$.

Ezek Hamilton-útat képeznek.

3-DIMENSIONAL MATCHING (3DM)

ÁLTALÁNOS ESET: Adott $M \subseteq W \times X \times Y$, ahol W, X, Y mindegyike q-elemű halmaz, és diszjunktak.

KÉRDÉS: Létezik-e M-ben teljes párosítás, azaz olyan $M' \subseteq M$, hogy $|M'| = q$, és M' elemei minden koordinátában különböznek?



Tétel

A 3DM feladat NP-teljes.

Bizonyítás.

Könnyű belátni, hogy 3DM $\in$ NP.

A 3SAT-ot alakítjuk 3DM-mé. Legyen $U = \{u_1, u_2, \ldots, u_n\}$ a változók halmaza, $C = \{c_1, c_2, \ldots, c_m\}$ a klózok halmaza.

Létrehozzuk a W, X, Y halmazokat és az $M \subseteq W \times X \times Y$ halmazt úgy, hogy M-ben akkor és csakis akkor van teljes párosítás, ha C kielégíthető.

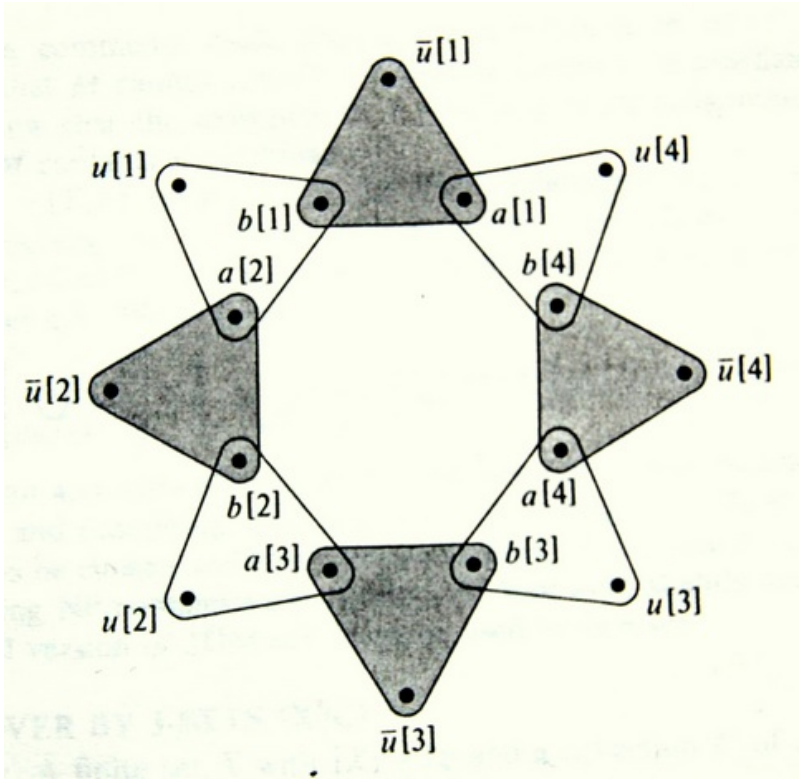
Minden változóhoz és minden klózhoz rendelünk bizonyos halmazokat:

$$T_i^t = \left\{ (\overline{u}_i[j], a_i[j], b_i[j]) \mid 1 \leq j \leq m \right\}$$

$$T_i^f = \left\{ (u_i[j], a_i[j+1], b_i[j]) \mid 1 \leq j < m \right\} \cup \left\{ (u_i[m], a_i[1], b_i[m]) \right\}$$

ahol $u_i[j], \overline{u}_i[j] \in W, a_i[j] \in X, b_i[j] \in Y$

és legyen $T_i = T_i^t \cup T_i^f$, $1 \leq i \leq n$



(Garey–Johnson)

(felső indexek jelentése:
– t: truth-setting component
– f: fan-out component)

Egy teljes párosítás vagy T_i^t vagy T_i^f minden elemét tartalmazza.

Értelmezzük a következőket is: Minden c_j klózhoz:

$$C_j = \Big\{ \big(u_i[j], s_1[j], s_2[j]\big) \,\big|\, u_i \in c_j \Big\}, \quad \text{ahol} \;\; s_1[j] \in X, s_2[j] \in Y$$

$$G = \Big\{ \big(u_i[j], g_1[k], g_2[k]\big), \big(\overline{u}_i[j], g_1[k], g_2[k]\big) \,\big|\, 1 \le k \le m(n-1), 1 \le i \le n, 1 \le j \le m \Big\},$$

ahol $g_1[k] \in X, g_2[k] \in Y$

Legyen

$$W = \Big\{ u_i[j], \overline{u}_i[j] \,\big|\, 1 \le i \le n, 1 \le j \le m \Big\}$$

$X = A \cup S_1 \cup G_1$ ahol

$A = \{a_i[j] \,|\, 1 \le i \le n, 1 \le j \le m\}$

$S_1 = \{s_1[j] \,|\, 1 \le j \le m\}$

$G_1 = \{g_1[j] \,|\, 1 \le j \le m(n-1)\}$

$Y = B \cup S_2 \cup G_2$ ahol

$B = \{b_i[j] \,|\, 1 \le i \le n, 1 \le j \le m\}$

$S_2 = \{s_2[j] \,|\, 1 \le j \le m\}$

$G_2 = \{g_2[j] \,|\, 1 \le j \le m(n-1)\}$

és

$$M = \left(\bigcup_{i=1}^{n} T_i\right) \cup \left(\bigcup_{j=1}^{m} C_j\right) \cup G$$

Mivel $M \subseteq W \times X \times Y$ és $|M| = 2mn + 3m + 2m^2 n(n-1)$,
M polinomiális időben előállítható.
Az M előállításából látszik, hogy csak akkor van benne teljes párosítás, ha C kielégíthető.
Fordítva: ha C kielégíthető, akkor minden c_j klózra legyen z_i vagy u_i vagy $\overline{u}_i$. és legyen igaz. Ekkor

$$M' \subseteq \left(\bigcup_{t(u_i)=T} T_i^t\right) \cup \left(\bigcup_{t(u_i)=F} T_i^f\right) \cup \left(\bigcup_{j=1}^{m} \left\{(z_j, s_1[j], s_2[j])\right\}\right) \cup G'$$

ahol $G' \subseteq G$ egy megfelelően választott részhalmaz. M' egy teljes párosítás.