ALGORITMUSOK ÉS BONYOLULTSÁGELMÉLET

Matematika MSc hallgatók számára

9. Előadás

Előadó: Hajnal Péter

Jegyzetelő: Hajnal Péter 2012. április 4.

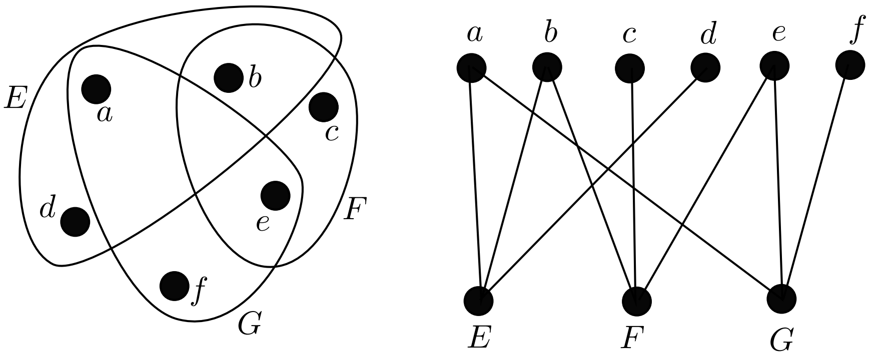
1. További $\mathcal{NP}$-teljes problémák

1.1. Halmazrendszerekkel kapcsolatos problémák

Definíció. $\mathcal{H}$ halmazrendszer a V halmaz felett, ha $\mathcal{H} \subseteq \mathcal{P}(V)$. $\mathcal{H}$ elemei a halmazrendszer élei. k-uniform halmazrendszer olyan halmazrendszer, amely összes éle k elemű. Tehát az egyszerű gráfok pontosan a 2-uninform halmazrendszerek.

Észrevétel. $V, \mathcal{H}$ halmazrendszer könnyen leírható B páros gráffal. A két színosztály V (felső pontok) és $\mathcal{H}$ (alsó pontok). Az alaphalmaz egy v eleme/csúcs akkor és csak akkor van összekötve $\mathcal{H}$ egy E elemével/éllel, ha $v \in E$.

A halmazrendszert lehet kódolni pont-él illeszkedési mátrixszal. Ez egy $n \times m$ méretű 0-1 mátrix, ahol $n = |V|$ és $m = |\mathcal{H}|$



$$\begin{array}{c c} & \begin{array}{ccc} E & F & G \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \\ e \\ f \end{array} & \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

1. ábra. Egy halmazrendszer a középiskolai Venn-diagrammal lerajzolva, a hozzá tartozó, őt kódoló B páros gráf és a pont-él-illeszkedési mátrix

⋆

Definíció. A gráfelmélet független csúcshalmazának fogalmát kétféleképpen terjeszthetjük ki halmazrendszerekre:

- I független, ha minden $E \in \mathcal{H}$ élre $E \not\subseteq I$.
- I független*: ha minden $E \in \mathcal{H}$ élre $|E \cap I| \leq 1$.

Definíció. FGTLEN-CSÚCSOK-HALMAZRENDSZERBEN=

$$\{\lceil V, \mathcal{H}, k\rceil : \text{van olyan } I \text{ független csúcshalmaz, hogy } |I| = k\}.$$

FGTLEN*-CSÚCSOK-HALMAZRENDSZERBEN=

$$\{\lceil V, \mathcal{H}, k\rceil : \text{van olyan } I \text{ független}^* \text{ csúcshalmaz, hogy } |I| = k\}.$$

A páros gráf kódoláson alapulva könnyű leírni a független* halmazokat. Ezeknek B-ben felső pontok egy olyan I halmaza tartozik, amelyekre nem illeszkedik V-alak, azaz olyan $a \in A, f, f' \in I \subset F$ ponthármas, ahol a összekötött f és f'-vel.

Definíció. Legyen B egy halmazrendszert leíró páros gráf. Az alsó/felső szerepek felcserélésével a B^* páros gráfot kapunk. Ez a B^* „elolvasható halmazrendszerként" visszaalakítva halmazrendszerré a $V^* = \mathcal{H}$, $\mathcal{H}^* = V$ duális halmazrendszert kapunk.

A redukciók sorozatát egy trivialitással kezdjük.

1. Tétel. *(i) FGTLEN-CSÚCSOK $\preceq$ FGTLEN-CSÚCSOK-HRSZBEN*
(ii) FGTLEN-CSÚCSOK $\preceq$ FGTLEN-CSÚCSOK-HRSZBEN*

Valóban, a gráfelméleti problémá gráfja a halmazrendszerek egy speciális esete. A gráfelméleti függetlenség mindkét halmazrendszeres függetlenség fogalom speciális esete.

Definíció. FGTLEN-ÉLEK-HRSZBEN =

$$\{\lceil V, \mathcal{H}, k\rceil : \mathcal{H}\text{-ban } J\ k \text{ db olyan él, amelyek páronként diszjuntak}\}.$$

A következő tétel már kevésbé nyilvánvaló.

2. Tétel. *FGTLEN*-CSÚCSOK-HRSZBEN $\preceq$ FGTLEN-ÉLEK-HRSZBEN*

Bizonyítás. $V, \mathcal{H}, k$-ból képezzük a duális halmazrendszert, a k értékét pedig tartsuk meg: $V^*, \mathcal{H}^*, k$.

Azt kell eldöntenünk, hogy az erdeti halmazrendszert leíró B páros gráfban van-e k felső pont úgy, hogy ne támaszkodjon rá $\vee$ alak. $V^*, \mathcal{H}^*$ páros gráfja éppen a fejetetejére állított B. Azaz az eredeti döntési feladat ekvivalens azzal, hogy fejrefordított B gráfban van-e k alsó csúcs (k darab él), hogy ne támaszkodjon rá $\wedge$, azaz páronként diszjunktak legyenek. Azaz FGTLEN-ÉLEK-HRSZBEN problémát kell megoldani $V^*, \mathcal{H}^*, k$ esetén.

Azaz a kiinduló transzformáció a tételt igazoló redukció. ∎

Megjegyzés. FGTLEN-ÉLEK-GRÁFOKBAN probléma, másképpen PÁROSÍTÁS $= \{\lceil G, k\rceil : \nu(G) \geq k\}$. Az Edmonds-algoritmus alapján ez egy $\mathcal{P}$-beli probléma. Azaz a gráfokra vonatkozó eset könnyen kezelhető.

Definíció. PARKETTÁZÁS =

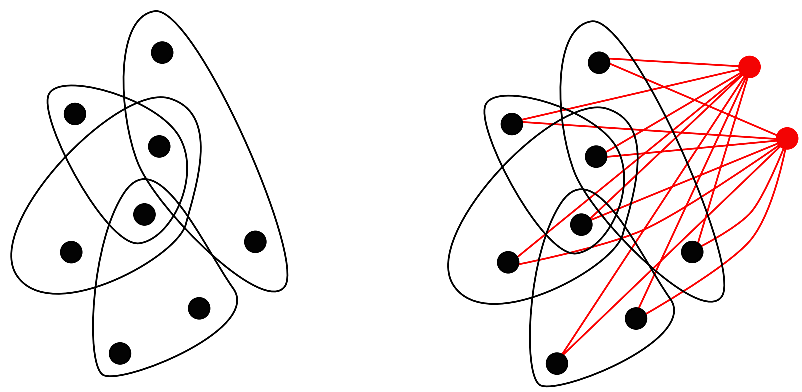
$$\{\lceil V, \mathcal{H}\rceil : \text{ léteznek } E_1, \ldots, E_k \text{ páronként diszjunkt élek, hogy } \dot\cup E_i = V\}$$

3. Tétel. *FGTLEN-ÉLEK-HRSZBEN$\preceq$PARKETTÁZÁS.*

Bizonyítás. Legyen $V, \mathcal{H}, k$ az input. Legyen S a maximális élméret paraméter. El kell dönteni, hogy van-e k db diszjunkt él.

A konstrukciót több lépésben végezzük el. Először $\mathcal{H}$-t úgy transzformáljuk, hogy uniform legyen: Minden E élhez $S - |E|$ sok új pontot veszünk fel (különböző élekhez különböző új pontokat használunk). A módosított halmazrendszerre vonatkozó probléma nyilván ekvivalens a kiinduló problémával.

A konstrukció második lépésében már feltesszük, hogy $\mathcal{H}$ egy S-uniform halmazrendszer. Ebben a lépésben $V(H)$-hoz hozzáveszünk $|V(H)| - k \cdot S$ darab új csúcsot (legyen $\widetilde{V}$ a kapott ponthalmaz), $\widetilde{\mathcal{H}}$ elemei pedig $\mathcal{H}$ elemei és minden régi-új csúcspárra egy-egy őket tartalmazó kételemű halmaz.



2. ábra. Az 5. Tétel redukciója. $|V| - kS = 8 - 2 \cdot 3 = 2$. A két új pont és a hozzájuk tartozó gráfélek a jobb oldalon szerepelnek pirosban.

Észrevétel. $(\widetilde{V}, \widetilde{\mathcal{H}})$ parkettázásához le kell fedni a $|V| - kS$ darab új csúcsot, ami csak a $|V| - kS$ darab új csúcskettőssel lehet. A maradék parkettázó élek csak régi élek lehetnek, amelyek kS csúcsot fednek le. Azaz a parkettázás ad k független elt $\mathcal{H}$-ban.

Az észrevétel gondolatmenetének megfordításá teszi teljessé a bizonyítás elméleti részét. ∎

⋆ ⋆ ⋆

Definíció. HALMAZRENDSZEREK SZÍNEZÉSI PROBLÉMÁJA: adott egy H halmazrendszer és egy k természetes szám. Kiszínezhetők-e $V(H)$ elemei k színnel, hogy semelyik H-beli halmaz ne legyen monokromatikus?

4. Tétel. *HALMAZRENDSZEREK SZÍNEZÉSI PROBLÉMÁJA $\mathcal{NP}$-teljes.*

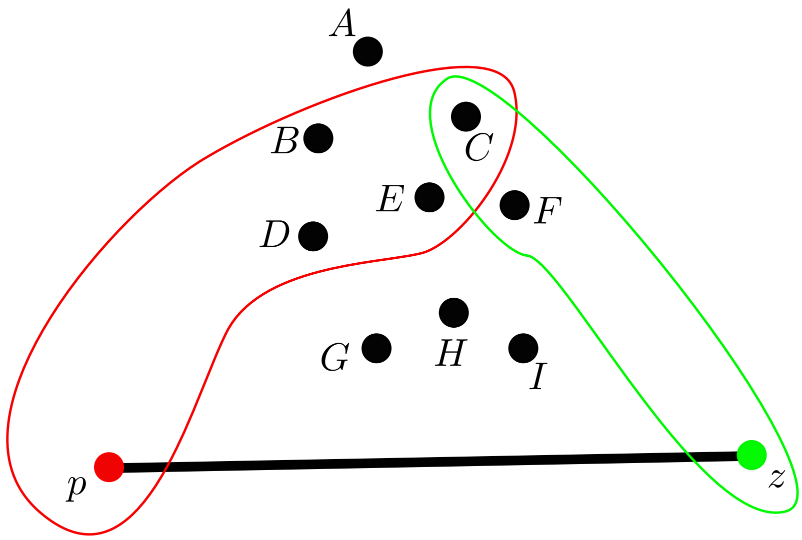
Bizonyítás. A gráfelméleti színezési probléma általánosítása. ∎

Gráfok esetén a 2-színezhetőség esete könnyen kezelhető volt.

Definíció. HALMAZRENDSZEREK-2-SZÍNEZHETŐSÉGE: Adott egy $\mathcal{H}$ halmazrendszer. Döntsük el: kiszínezhetők-e $V(H)$ elemei 2 színnel úgy, hogy semelyik H-beli halmaz ne legyen monokromatikus.

5. Tétel. *PARKETTÁZÁS* $\preceq$ *HALMAZRENDSZEREK-2-SZÍNEZHETŐSÉGE.*

Bizonyítás. Adott egy $V, \mathcal{H}$ input a parkettázás problémához.
Konstrukció: $\widetilde{V} = \mathcal{H} \cup \{p, z\}$. $\widetilde{H}$-hoz minden E, F metsző $\mathcal{H}$-beli élpárra legyen $Z_{E,F} = \{E, F, z\}$ egy él. Minden $v \in V$ esetén legyen $R_v = \{E : v \in E \in \mathcal{H}\} \cup \{p\}$ egy $\widetilde{\mathcal{H}}$-beli él. Továbbá legyen $\{p, z\}$ is egy $\widetilde{\mathcal{H}}$-beli él.



3. ábra. $A, B, C, \ldots, H, I$ pontosan a halmazrendszerünk élei. B, C, D, E pontosan az a elemet tartalamzó élek. C és F élek metszőek. A fenti információkból kiolvasható éleket rajzoltuk be az ábrába, amely a redukció megfelelő töredékét tartalmazza.

Észrevétel. $\widetilde{V}, \widetilde{\mathcal{H}}$ egy 2-színezése esetén legyen p színe piros, z színe zöld (a $\{p, z\}$ él kényszerít a teljes paletta használatára). Az eredeti éleknek megfelelő csúcsok közül a zöld szín kijelöl egy élhalmazt. Ezek parkettázzák az eredti halmazrendszert.

Valóban, köztük két metsző él egy $Z_{E,F}$ típusú zöld-homogén élhez vezetne a redukció eredményében. Míg egy lefedetlen v csúcs (az eredeti halmazrendszerben) adna egy R_v piros-homogén élt.

A gondolatmenet megfordítható, a bizonyítás teljes. ■

⋆ ⋆ ⋆

Az alábbi problémák mindegyike $\mathcal{NP}$-teljes. Ezek nem szerepeltek előadáson. Csak megemlítjük az érdeklődő olvasóknak és ötletet adunk az igazoláshoz.

Definíció. HÁRMASÍTÁS: adott három azonos méretű halmaz és ennek transzverzálisaiból álló 3-uniform halmazrendszer. Van-e a halmazrendszernek olyan részhalmaza, amely a három halmaz uniójának partícióját adja?

Ötlet. Szokásos visszavezetés: 3-SAT.

Definíció. 3-UNIFORM HALMAZRENDSZER PARTÍCIÓ: adott egy 3-uniform halmazrendszer. Van-e olyan részhalmaza, ami az alaphalmaz partíciója?

Ötlet. HÁRMASÍTÁS általánosítása.

1.2. Egyéb problémák

Definíció. DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER: adott egy $Ax \le b$ egész együtthatós lineáris egyenlőtlenségrenszer. Van-e megoldása egész számokban?

6. Tétel. *DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER $\mathcal{NP}$-teljes.*

Bizonyítás. $\mathcal{NP}$-beliségre tanú egy megoldás.

Az $\mathcal{NP}$-nehézség bizonyításához a SAT-ot vezetjük vissza a problémára: adott egy konjunktív normálforma. Minden x_i változóra bevezetjük a $0 \le x_i \le 1$, és minden $\langle z_1, \ldots, z_k\rangle$ klózra a $t_1 + \ldots + t_k$ egyenlőtlenséget, ahol $t_i = x_j$, ha $t_i = x_j$ és $t_i = 1 - x_j$, ha $t_i = \overline{x}_j$. Könnyű látni, hogy az egyenlőtlenségrendszer polinom időben megkonstruálható, és pontosan akkor megoldható, ha a konjunktív normálforma kielégíthető. ■

Definíció. RÉSZLETÖSSZEG=

$$\{\lceil A, b\rceil : A \subset \mathbb{N}, b \in \mathbb{N}, \text{van olyan } R \subset A, \text{ hogy az } R\text{-beli számok összege } b\}.$$

A feladat egy egyszerű értelmezése: A a pénztárcánkban lévő érmék értékeit összegyűjtő halmaz . A, b kódja akkor tartozik az elfogadandó nyelvhez, ha b összeget pontosan ki tudunk fizetni a pénztárcánkból.

7. Tétel. *RÉSZLETÖSSZEG $\mathcal{NP}$-teljes.*

Bizonyítás. RÉSZLETÖSSZEG nyilván $\mathcal{NP}$-beli. Belátjuk, hogy PARKETTÁZÁS $\preceq$ RÉSZLETÖSSZEG.

Legyen $V, \mathcal{H}$ a PARKETTÁZÁS egy inputja. Ki lehet-e választani olyan parkettahalmazt/élhalmazt, amivel ki lehet parkettázni a V-t/padlót?

Konstrukció: Legyen $w : V \to \{1, a, a^2, \ldots, a^{|V|-1}\}$ tetszőleges bijekció. Az értékkészletre gondoljunk mint az a alapú számrendszer helyiértékei.

Legyen $E \in \mathcal{H}$ esetén $a_E = \sum_{v:v\in E} w(v)$. Legyen $A = \{a_E : E \in \mathcal{H}\}$ és $b = 11\ldots1_a = \sum_{v:v\in V} w(v)$. Ezzel leírtuk a részletösszeg probléma egy inputját.

Észrevétel. Ha a értékét $|\mathcal{H}| + 1$-nek választjuk, akkor $a_i \in A$ számok olyanok, hogy minden részletösszeg az a alapú számrendszerben maradék továbbvitele nékül kiszámolható.

Az észrevétel egyből adja, hogy a csupa 1-es számjegyből álló szám előállítása mint részletösszeg ekvivalens az eredeti halmazrendszerre vonatkozó PARKETTÁZÁS feladattal (alkalmasan nagy a esetén).

A redukció során előforduló legnagyobb szám $S = \sum_{i=0}^{|V|-1} a^i = \frac{a^{|V|-1}}{a-1} < a^{|V|}$. Kódjának hossza $|V| \log a = |V| \log(|\mathcal{H}| + 1)$. Redukciónk polinomiális. ■

⋆ ⋆ ⋆

Az alábbi problémák mindegyike $\mathcal{NP}$-teljes. Ezek nem szerepeltek előadáson. Csak megemlítjük az érdeklődő olvasóknak és ötletet adunk az igazoláshoz.

Definíció. HÁTIZSÁK: Adott tárgyak T halmaza. Minden $t \in T$ tárgyhoz tartozik egy V_t térfogat és egy v_t érték ($v_t, V_t \in \mathbb{N}$). Adott egy hátizsák, amelybe legfeljebb H össztérfogatú tárgyakat pakolhatunk. Továbbá adott egy L értékhatár. ($H, L \in \mathbb{N}$.) Kiválasztható-e T egy részhalmaza úgy, hogy elférjen a hátizsákban és összértéke legalább L legyen?

Ötlet. Szokásos visszavezetés: 3-UNIFORM HALMAZRENDSZER PARTÍCIÓ.

Definíció. LÁDAPAKOLÁS: adott egész számok A halmaza, egy b és egy c egész szám. Meg lehet-e adni A egy legfeljebb b osztályú partícióját, amelyben minden osztály összege legfeljebb c?

Ötlet. Szokásos visszavezetés: HÁRMASÍTÁS.

2. Egy $PSPACE$-teljes probléma

Definíció (kvantifikált Boole-formula probléma, QBF). Legyen a φ Boole-formula a következő alakú: $\varphi(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$. Ekkor a

$$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n \varphi(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$$

vagy igaz, vagy hamis. A probléma az, hogy döntsük el, hogy melyik.

8. Tétel. *QBF $\mathcal{PSPACE}$-teljes, vagyis*

- *(i) QBF $\in \mathcal{PSPACE}$*
- *(ii) $\forall L \in \mathcal{PSPACE} : L \prec_{\mathcal{P}} QBF$*

Bizonyítás. Azt látjuk be, hogy QBF $\mathcal{NPSPACE}$-teljes. Ez a tétel állítása, hiszen tudjuk, hogy $\mathcal{NPSPACE} = \mathcal{PSCPACE}$.

(i) Könnyen belátható.

(ii) Ahogy általában a tár korlátozott döntéseknél tettük, egy tetszőleges $L \in_T \mathcal{NPSPACE}$ nyelvre az ω L-hez tartozásának döntési feladatát visszavezethetjük az ELÉRHETŐSÉG eldöntésére a ($G_{T,\omega}$, START, ELFOGAD) input esetén, ahol $G_{T,\omega}$ a redukált konfigurációk gráfja:

$$\omega \in L \Leftrightarrow \text{ létezik START-ELFOGAD (irányított) út } G_{T,\omega}\text{-ban.}$$

$G_{T,\omega}$ egy 2^{n^α} pontszámú gráf. Egy csúcs kódja logaritmikus a csúcsok számában. Vagyis mindegyik csúcs n^α hosszban kódolható.

Persze nem az ELÉRHETŐSÉG inputját gyártjuk le. Ennek „költsége" $\mathcal{PSPACE}$, ami megegyezik L bonyolultságával, így nincs értelme. (A gondolatmenet $\mathcal{NL}$ és $\mathcal{L}$ viszonyában működött.)

Az „igazi" visszavezetés egy formulát gyárt le. Ehhez szükségünk lesz néhány jelölésre.

Jelölés. Legyen $N := n^\alpha$.

$u \overset{\rightarrow}{\sim} v$ jelölje azt, hogy alapgráfunkban u-ból elérhető (irányított értelemben) a v csúcs.

$u \overset{\rightarrow}{\sim}_{\leq i} v$ jelölje azt, hogy alapgráfunkban u-ból legfeljebb i lépéssel elérhetünk v-be.

Esetünkben az alapgráf $G_{T,\omega}$, pontszáma 2^N. Így $u \overset{\rightarrow}{\sim} v$ akkor és csak akkor, ha $u \overset{\rightarrow}{\sim}_{\leq 2^N} v$.

Az alapötletünk az, hogy felosztjuk az utunkat két részre egy középső k csúccsal, előbb csak egy k csúcsig megyünk el START-ból maximum 2^{N-1} lépésben, majd onnan szintén maximum 2^{N-1} lépésben ELFOGAD-ig.

Eddigi ötleteink formalizálva:

$\omega \in L \Leftrightarrow \mathrm{START} \rightsquigarrow_{\leq 2^N} \mathrm{ELFOGAD}$,

$\mathrm{START} \rightsquigarrow_{\leq 2^N} \mathrm{ELFOGAD} \Leftrightarrow \exists_V k (\mathrm{START} \rightsquigarrow_{\leq 2^{N-1}} k) \wedge (k \rightsquigarrow_{\leq 2^{N-1}} \mathrm{ELFOGAD})$.

Az összes csúcs (START,k,ELFOGAD) N (n-ben polinomiális) hosszú bitsorozattal kódolt. A $\exists_V k$ azt jelenti, hogy N hosszú kódszavak (csúcsokat kódoló bitsorozatok) között létezik. Azaz N darab, bitekre vonatkozó egzisztenciális kvantor sorozata.

Gondolhatunk arra, hogy nincs mit tenni csak iterálni kell ezeket az ötleteket. Formulánkban két helyen is szerepel az $\rightsquigarrow_{\leq 2^{N-1}}$ reláció. Iterálásnál (N mélységre van szükségünk) a formula nagysága exponenciálisan nagy lenne. Még egy ötletre van szükségünk. A fenti formulánk ekvivalens azzal, hogy

$$\exists_V k \forall_V c \forall_V c' : (c = \mathrm{START} \wedge c' = k) \vee (c = k \wedge c' = \mathrm{ELFOGAD}) \rightarrow c \rightsquigarrow_{\leq 2^{N-1}} c'.$$

Ezt a gondolatmenetet iterálva már a kapott formula mérete polinomiális lesz. $N = n^\alpha$ iterálás kell és mindegyik csak hozzáad a fomrulához egy polinomiális hosszú új részt. A bizonyítás befejezéseként csak ellenőrizzük, hogy az iteráció elindul: Az iteráció legmélyén lévő formulák: $u \rightsquigarrow_{\leq 1} v$ azt jelentik, hogy '$u = v$ vagy u-ból vezet él v-hez'. Ez egy egyszerű (kvantor nélküli) Boole-formulával megfogalmazható reláció.

Az $\exists_V v$ jelölés csalóka. v N darab bittel kódolt, ezek mindegyike létezik kvantorral kötött. Úgy tűnik, hogy az alternáló kvantorok feltétele nem teljesül. Nincs probléma. Új változók bevezetésével a kvantorok alternálása megoldható. Ha az új változókat csak kvantifikált formában használjuk, akkor nem befolyásolják a formula logikai értékét. ■

Megjegyzés. A QBF feladat inputjában nem az volt a fontos, hogy a létezik kvantor után egy minden kvantor következik és fordítva, hanem az, hogy kvantorok váltakozásának száma tetszőlegesen nagy lehet.

Ezzel a legfontosabb nyelvosztályokra találtunk teljes problémákat. Azaz olyan problémákat, amelyek tükrözik a nyelvosztály teljes nehézségét. Ha ezekről a teljes problámákról tudunk valami „okosat" mondani, akkor az egész osztályról kapunk fontos információt.