Kiegészítő anyag az Algoritmuselmélet tárgyhoz III.

(a Rónyai–Ivanyos–Szabó: Algoritmusok könyv mellé)

Friedl Katalin
BME SZIT
friedl@cs.bme.hu

2010. május 24.

A bonyolultságelmélet alapjai: a P és az NP osztály

Egy algoritmust (elméleti szempontból) hatékonynak mondunk, ha lépésszáma felülről becsülhető a bemenet hosszának egy polinomjával, azaz ha $f(n)$ jelöli az algoritmus maximális képésszámát az n hosszú bemeneteken, akkor $f(n) = O(n^k)$ teljesül valamilyen k pozitív konstansra. Természetesen, ha a kimenet mondjuk exponenciális hosszú, akkor az algoritmus nem lehet polinom lépésszámú, hiszen pusztán az eredmény kiírásához is több (exponenciális) idő kell. Ez a helyzet például, ha az x pozitív egész bementből a 2^x számot akarjuk kiszámolni, mivel itt a bemenet hossza, az x leírásához szükséges bitek száma $\lceil \log(x+1) \rceil$, míg a kimenet hossza $x+1$ bit. Előfordulhat azonban, hogy bár a kimenet rövid (1 bit), mégsem ismert egy feladatra hatékony algoritmus. (Sőt olyan is előfordul, hogy egyáltalán nincs is algoritmus, de most ezzel az utóbbi esettel nem foglalkozunk – majd az MSc képzésben.)

Mostantól csak olyan típusú feladatokkal foglalkozunk, melyekre a válasz 1 bit, ezek az úgynevezett *eldöntési problémák*. Ilyenek például

- PRÍM
  Bemenet: $m > 0$ egész.
  Kérdés: m prímszám?

- H
  Bemenet: $G = (V, E)$ irányítatlan gráf.
  Kérdés: Van G-ben Hamilton-kör?

- ÚT
  Bemenet: $G = (V, E)$ irányítatlan gráf és két kitüntetett csúcs, $s, t \in V$.
  Kérdés: Van-e s és t között út a gáfban?

1. Megjegyzés. *Egy eldöntési problémához tartozó L* nyelv *azoknak a bemeneteknek a halmaza, amelyekre a válasz* `igen`*. A lehetséges bemeneteket (amik tehát vagy beletartoznak L-be vagy nem),* szavaknak *hívjuk. A következő definíciókat sokszor nyelvekkel és nem eldöntési problémákkal fogalmazzák meg.*

1. Definíció. *Jelölje* P *azoknak az eldöntési problémáknak a halmazát, amelyekhez van olyan $\mathcal{A}$ algoritmus, ami minden x bemenetre helyesen megválaszolja a kérdést, és az algoritmus lépésszáma* polinomiális*, azaz $O(|x|^k)$ valamely k pozitív konstansra. (Itt $|x|$ az x bemenet hosszát jelöli, k független x-től.)*

Jelölés Egy X eldöntési probléma és x bemenet esetén $x \in X$ jelöli, hogy az x bemenetre a válasz `igen`.
Ha egy $\mathcal{A}$ algoritmust az x bemeneten futtatunk, $\mathcal{A}(x)$ jelöli a futás eredményét (ami eldöntési problémáknál `igen` vagy `nem` lehet.)

Az előző példákat vizsgálva könnyen látszik, hogy ÚT $\in$ P, mert például egy szélességi bejárással a kérdés eldönthető, és ez polinom idejű algoritmus. Az is teljesül, hogy PRÍM $\in$P, de ez nem olyan egyszerű, sokáig megoldatlan kérdés volt, csak 2002-ben bizonyították be. A H problémáról nem ismert, hogy P-ben van-e, azaz, hogy van-e rá polinom időben működő algoritmus. (bizonyos speciális gráfosztályok esetén van ilyen).

2. Definíció. *Azt mondjuk, hogy az X eldöntési problémához van* hatékony tanúsítvány*, ha van olyan $\mathcal{T}$ algoritmus, melynek a bemenete (x, t) párokból áll, ahol x az X probléma egy lehetséges bemenete és a következő feltételek teljesülnek: léteznek olyan c és k pozitív konstansok, hogy*

- *ha $x \in X$, akkor* van *olyan t, aminek hossza $|t| = O(|x|^c)$ és $\mathcal{T}(x, t) =$ `igen`,*
- *ha $x \notin X$, akkor* nincs *olyan t, aminek hossza $|t| = O(|x|^c)$ és $\mathcal{T}(x, t) =$ `igen`.*
- *A $\mathcal{T}$ algoritmus polinomiális, azaz a lépésszáma $O((|x| + |t|)^k)$.*

Egy hatékony tanúsítvány lényegében azt jelenti, hogy amennyiben adott x bemenet esetén az eldöntési problémára a válasz `igen`, akkor erre van olyan rövid (polinom hosszú) bizonyíték (t), amiről polinom időben ellenőrizhető, hogy valóban helyes (ezt az ellenőrzést végzi a $\mathcal{T}$). Ha a válasz `nem`, akkor viszont nincs olyan rövid érvelés, amivel be lehet minket (vagy a $\mathcal{T}$ algoritmust) csapni.

2. Megjegyzés. *Mivel t polinom hosszú kell legyen, elég azt kikötni, hogy $\mathcal{T}$ lépésszáma x hosszában polinomiális.*

3. Megjegyzés. *Ha nem kötnénk ki, hogy t polinom hosszú, akkor $\mathcal{T}$ lépésszáma akármilyen nagy lehetne $|x|$-hez képest (csak elég hosszú t-t kell megadni), azaz ily módon amihez van algoritmus, ahhoz lenne tanúsítvány is.*

3. Definíció. *Jelölje* NP *azoknak az eldöntési problémáknak a halmazát, amelyekre van hatékony tanúsítvány.*

4. Megjegyzés. *Az* NP *a* nemdeterminisztikus polinom idő *rövidítése, ami arra utal, hogy t ,,megtalálása" nem feltétlenül determinisztikusan történik, egy* $x \in X$ *esetén elég ha megsejtjük, mi lesz jó. Viszont utána az ellenőrzés, hogy valóban jó a t, amit választottunk (kaptunk valakitől) már polinomidőben megy.*

5. Megjegyzés. *Ha az* X *problémára van hatékony tanúsítvány, akkor ez sugall egy algoritmust is: próbáljuk végig az összes lehetséges* t *bizonyítékot, hiszen mindegyiket polinomidőben ellenőrizhetjük. A baj ezzel az, hogy hiába hatékony (polinom idejű) minden egyes* t *ellenőrzése a* $\mathcal{T}$ *algoritmus segítségével, a lehetséges* t*-k száma exponenciális (*$n = |x|^c$ *hosszú 0-1 sorozatból* 2^n *féle van). Így exponenciális idejű algoritmust kapunk az* X *problémára.*

Példák

- H $\in$ NP, mert egy $G \in$ H gráfhoz jó bizonyíték a gráf csúcsainak egy, a Hamilton-kör mentén való felsorolása. Azaz legyen t a csúcsok felsorolása a megfelelő sorrendben. Ez valóban polinom hosszú lesz. A $\mathcal{T}$ algoritmus a (G, t) bemeneten ellenőrizze, hogy t tényleg a csúcsok egy felsorolása, és hogy a felsorolásban egymás után következő, valamint az utolsó és első elem között van a G gráfban él. Mivel mindez megoldható lineáris számú lépéssel és ilyen t pontosan akkor létezik, ha a gráfnak van Hamilton-köre, tehát $\mathcal{T}$ valóban hatékony tanúsítvány a H problémára.

- Legyen ÖSSZETETT az alábbi eldöntési probléma:

  Bemenet: m pozitív egész szám

  Kérdés: m összetett szám?

  Könnyű látni, hogy ÖSSZETETT $\in$ NP, mert ha $m \in$ ÖSSZETETT, akkor t lehet m egy valódi osztója, a $\mathcal{T}$ algoritus pedig az (m, t) bemenet esetén ellenőrizze, hogy $1 < t < m$ és t osztója m-nek. Vegyük észre, hogy adott m-hez pontosan akkor lesz jó t, ha m egy összetett szám. Ekkor $|t| \leq |m|$ és mivel az oszthatóság ellenőrzésének lépésszáma mindkét szám hosszában polinomiális, tehát valóban van

- Legyen 3SZÍN az alábbi eldöntési probléma:

  Bemenet: $G = (V, E)$ irányítatlan egyszerű gráf

  Kérdés: Kiszínezhetők-e a csúcsai 3 színnel

  Egy G gráfhoz legyen t egy olyan $|V|$ hosszú sorozat, ami az 1, 2, 3 számokból áll. A $\mathcal{T}$ algoritmus egy (G, t) pár esetén ellenőrizze, hogy a t a gráf csúcsainak egy jó, az $\{1, 2, 3\}$ színekkel való színezését írja-e le. Azaz akkor legyen az eredmény `igen`, ha minden olyan esetben, amikor $t_i = t_j$, akkor a gráf megfelelő v_i és v_j csúcsaira $\{v_i, v_j\} \notin E$.

  Ez az ellenőrzés, akár szomszédossági mátrixával, akár éllistával van megadva a gráf, polinom időben megtehető, és világos, hogy pontosan akkor van megfelelő t a G gráfhoz, ha $G \in$ 3SZÍN.

4. Definíció. *Egy X eldöntési probléma komplementere az az $\overline{X}$-sal jelölt probléma, melynek bemenete ugyanolyan mint az X esetén, de a válasz ellentétes. Azaz minden lehetséges x bemenetre*

$$x \in \overline{X} \Leftrightarrow x \notin X.$$

1. Példa. ÖSSZETETT $= \overline{\text{PRÍM}}$

5. Definíció. *Jelölje* co NP *az* NP*-beli problémák* komplementereiből *álló halmazt, azaz $X \in \mathrm{co\,NP} \Leftrightarrow \overline{X} \in \mathrm{NP}$.*

A definíció miatt, míg az NP-beli problémák esetében a definíció szerint az `igen` válaszra van polinom hosszú, polinom időben ellenőrizhető bizonyíték, a co NP-beli problémák azok, ahol a `nem` válaszra van polinom hosszú, polinom időben ellenőrizhető bizonyíték.

1. Állítás. $\mathrm{P} \subseteq \mathrm{NP}$ *és* $\mathrm{P} \subseteq \mathrm{co\,NP}$.

Bizonyítás: Ha $X \in \mathrm{P}$, akkor a hatékony tanúsítvány lehet lényegében az X-et megválaszoló polinom idejű algoritmus (ekkor $|t| = 0$). □

A számítástudomány talán legfontosabb (és legnépszerűbb) nyitott kérdése, hogy vajon P és NP megegyezik vagy nem. Ha $\mathrm{P} \subset \mathrm{NP}$ valódi tartalmazás, akkor ez azt jelentené, hogy vannak olyan kérdések, melyeknél az igaz esetben van rövid (polinom hosszú) bizonyíték, de ezt a bizonyítékot nem lehet polinom időben megtalálni, azaz egy jó válasz ellenőrzése algoritmikusan lehet lényegesen egyszerűbb, mint egy jó válasz megtalálása (ami köznapi logikával elég hihetőnek tűnik). Mint látni fogjuk, sok nevezetes probléma bonyolultsága múlik ezen a kérdésen. Ennek is köszönhető, hogy az ezredfordulón a Clay Mathematics Institute – 6 másik matematikai problémával együtt – a $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ problémára is 1 millió dolláros díjat tűzött ki (lásd www.claymath.org/millennium/).

Az sem ismert, hogy vajon $\mathrm{P} \stackrel{?}{=} \mathrm{NP} \cap \mathrm{co\,NP}$. Az előző állítás miatt a bal oldal része a jobb oldalnak, a kérdés, hogy teljesül-e az egyenlőség. Szavakban ez azt a kérdést takarja, hogy ha egy problémánál mind az `igen`, mind a `nem` válaszra van hatékony tanúsítvány, akkor ebből következik-e, hogy az eldöntési kérdésre van hatékony algoritmus. Ha $\mathrm{P} = \mathrm{NP}$, akkor nem nehéz látni, hogy $\mathrm{NP} = \mathrm{co\,NP}$ és így $\mathrm{P} = \mathrm{NP} \cap \mathrm{co\,NP}$ is következik. Fordítva viszont még ha tudnánk is, hogy $\mathrm{P} = \mathrm{NP} \cap \mathrm{co\,NP}$ ebből nem következik, hogy P és NP azonos.

Ahhoz, hogy jobban megérthessük ezt a problémakört, további fogalmakra lesz szükség. Problémák bonyolultságának összehasonlítására szolgál a polinomiális visszavezetés, vagy más néven Karp-redukció.

6. Definíció. *Legyen X és Y két eldöntési probléma. Az X* Karp-redukciója (polinomiális visszavezetése) *az Y problémára egy olyan polinom időben számolható f függvény, amely X minden lehetséges bemenetéhez hozzárendeli Y egy lehetséges bemenetét úgy, hogy*

$$x \in X \Leftrightarrow f(x) \in Y.$$

Jelölése: $X \prec Y$.

A jelölés arra utal, hogy, mint majd mindjárt látni fogjuk, az Y probléma algoritmikusan legalább olyan nehéz, mint az X.

2. Állítás. *Ha* $X \prec Y$ *akkor* $\overline{X} \prec \overline{Y}$.

Bizonyítás: Legyen f az X-nek Y-ra egy Karp-redukciója. Ekkor ugyanez az f egyben az $\overline{X}$-nek is Karp-redukciója $\overline{Y}$-ra, mert a feltevés szerint polinom időben számolható, és $x \in \overline{X} \Leftrightarrow x \notin X \Leftrightarrow f(x) \notin Y \Leftrightarrow f(x) \in \overline{Y}$. $\square$

3. Állítás. *Ha* $Y \in \mathrm{P}$ *és* $X \prec Y$*, akkor* $X \in \mathrm{P}$.

Bizonyítás: A feltétel szerint van egy polinomiális $\mathcal{A}$ algoritmus, ami tetszőleges z bemenetről eldönti, hogy $z \in Y$ vagy $z \notin Y$. Legyen ennek lépésszáma $O(|z|^k)$ Legyen x egy lehetséges bemenete az X problémának. A $\mathcal{B}$ algoritmus előbb az erre szolgáló polinomiális algoritmus segítségével számolja ki $f(x)$-et és erre az $f(x)$-re alkalmazza $\mathcal{A}$-t. Ha az eredmény `igen`, akkor legyen $\mathcal{B}$ eredménye is `igen`, különben pedig `nem`. Mivel $x \in X \Leftrightarrow f(x) \in Y$, ezért $\mathcal{B}$ biztosan helyes választ ad. Az eljárás lépésszáma: $f(x)$ kiszámolása polinomiális, tehát van olyan $d > 0$ konstans, hogy a lépésszáma $O(|x|^d)$. Ezért $f(x)$ hosszára igaz, hogy $|f(x)| = O(|x|^d)$. Az $f(x)$ bemeneten $\mathcal{A}$ lépésszáma $O(|f(x)|^k)$, így tehát a lépésszám összesen $O(|x|^d) + O(|f(x)|^k) = O(|x|^d) + O(|x|^{dk}) = O(|x|^{dk})$, ami valóban polinomja a bemenet $|x|$ hosszának. $\square$

4. Állítás. *Ha* $Y \in \mathrm{NP}$ *és* $X \prec Y$*, akkor* $X \in \mathrm{NP}$.

Bizonyítás: Jelölje $\mathcal{T}$ az Y egy hatékony tanúsítványát és legyen f a Karp-redukció. A $\mathcal{T}'$ algoritmus az (x, t) bemeneten működjön a következőképpen: Előbb kiszámolja az $f(x)$-et és az $(f(x), t)$ párra alkalmazza a $\mathcal{T}$ algoritmust. Ha az eredmény `igen`, akkor legyen $\mathcal{T}'$ eredménye is `igen`, különben pedig `nem`.

Tudjuk, hogy $x \in X \Leftrightarrow f(x) \in Y$ és ez utóbbi pontosan akkor igaz, ha van alkalmas t, azaz, aminek hossza $|t| = O(|f(x)|^c)$ és $\mathcal{T}(f(x), t) = \texttt{igen}$. Ez a t az x hosszához képest is polinomiális, mert ha az $f(x)$ függvény számolása $O(|x|^d)$, akkor $|f(x)| = O(|x|^d)$ és így $|t| = O(|x|^{dc})$.

A $\mathcal{T}'$ algoritmus lépésszáma pedig $O(|x|^d) + O((|f(x)| + |t|)^k) = O(|x|^d) + O(|f(x)|^{ck}) = O(|x|^{dck})$. $\square$

5. Állítás. *Ha* $Y \in \mathrm{co\,NP}$ *és* $X \prec Y$*, akkor* $X \in \mathrm{co\,NP}$.

Bizonyítás: Mivel $X \prec Y$, ezért $\overline{X} \prec \overline{Y}$ is teljesül. A definíció szerint $Y \in \mathrm{co\,NP}$ pontosan akkor, ha $\overline{Y} \in \mathrm{NP}$. A feltétel szerint $\overline{Y} \in \mathrm{NP}$, tehát a 4. állítás miatt $\overline{X} \in \mathrm{NP}$, azaz $X \in \mathrm{co\,NP}$. $\square$

6. Állítás. *Ha* $X \prec Y$ *és* $Y \prec Z$*, akkor* $X \prec Z$*, azaz a* $\prec$ *reláció tranzitív.*

Bizonyítás: Legyen f az első és g a második Karp-redukció függvénye. Ekkor $g(f(x))$ egy $X \prec Z$ Karp-redukció. Ehhez azt kell csak meggondolni, hogy ha $|f(x)| = O(|x|^d)$ és $|g(z)| = O(|z|^k)$, akkor $|g(f(x))| = O(|x|^{kd})$, ami $|x|$-nek polinomja és $x \in X \quad \Leftrightarrow \quad f(x) \in Y \quad \Leftrightarrow \quad g(f(x)) \in Z$. $\square$

7. Definíció. *Egy Z eldöntési probléma* NP-nehéz*, ha minden $X \in \mathrm{NP}$ problémára teljesül, hogy $X \prec Z$.*

8. Definíció. *Egy Z eldöntési probléma* NP-teljes*, ha az Z probléma* NP*-nehéz és $Z \in \mathrm{NP}$.*

Szemléletesen egy NP-nehéz probléma legalább olyan nehéz mint bármelyik NP-beli probléma (de lehet sokkal nehezebb is), míg az NP-teljes problémák az NP osztály legnehezebb problémái, hisz maguk is NP-ben vannak, és legalább olyan nehezek, mint bármely NP-beli probléma.

A $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ kérdés eldöntéséhez elegendő lenne egyetlen NP-teljes problémáról megmutatni, hogy P-ben van, hiszen ha az Z probléma NP-teljes, akkor minden $X \in \mathrm{NP}$ problémára teljesül, hogy $X \prec Z$, és ha ugyanekkor $Z \in \mathrm{P}$ is igaz, akkor a 3. állítás értelmében $X \in \mathrm{P}$ minden $X \in \mathrm{NP}$ esetén.

Ezért a hátralevő részben NP-teljes problémákkal foglalkozunk. Történetileg az első NP-teljességi bizonyítást Stephen Cook és Leonid Levin egymástól függetlenül, nagyjából egy időben, a 70-es évek elején adta. Az ebben szereplő probléma bizonyos fajta logikai formulákról szól. A későbbiekben azután az NP-teljes problémák száma gyorsan nőtt, már a 70-es évek végén megtöltöttek egy egész könyvet.

Ha már van legalább egy NP-teljes problémánk, akkor a további NP-teljességi bizonyítások a következő séma szerint készíthetőek:

1. Belátjuk, hogy $Z \in \mathrm{NP}$
2. Egy tetszőleges NP-teljes Y problémára megmutatjuk, hogy $Y \prec Z$.

Ez a séma a Karp-redukció tranzitivitása (6. állítás) miatt működik, hiszen az NP-teljesség definíciója szerint minden $X \in \mathrm{NP}$ problémára $X \prec Y$ és így $Y \prec Z$-ből következik, hogy $X \prec Z$ is teljesül minden $X \in \mathrm{NP}$ problémára.

Kiindulási problémaként bizonyítás nélkül fogadjuk el, hogy a már korábban látott 3SZÍN NP-teljes. (Mint már említettük, nem ez volt az első bizonyítottan NP-teljes probléma de nekünk jó kezdőpont lesz.)

1. Tétel. *A* 3SZÍN *probléma* NP*-teljes.*

6. Megjegyzés. *A hasonlóan definiált* 2SZÍN *problémára* 2SZÍN $\in \mathrm{P}$*, hiszen az, hogy egy gráf színezhető-e 2 színnel egyszerűen ellenőrizhető polinom időben (pl. szélességi bejárással kiszínezhetők a csúcsok két színnel, ha egyáltalán van ilyen színezés).*

A 3SZÍN nehézségének felhasználásal már be tudjuk bizonyítani más problémákról is, hogy NP-teljesek. Először azt mutatjuk meg, hogy a legnagyobb független ponthalmaz méretének meghatározása egy gráfban algoritmikusan nehéz feladat. Ehhez előbb ezt át kell fordítani egy eldöntési problémává. Technikai okok miatt ezt úgy célszerű csinálni, hogy az eldöntési problémában nem a maximum értékére kérdezünk rá, hanem arra, hogy van-e elég nagy független ponthalmaz.

MAXFTL

Bemenet: (G, k) pár, ahol G egy gráf és k egy pozitív egész szám.

Kérdés: Van-e G-ben k darab független csúcs?

2. Tétel. *Ha lenne egy $\mathcal{A}$ polinom idejű algoritmus a* MAXFTL *eldöntési problémára, akkor polinom időben meg is lehet határozni egy adott gráfban a maximális független ponthalmaz méretét.*

Bizonyítás: Ha az n pontú G gráfban keresünk maximális független ponthalmazt, akkor alkalmazzuk $\mathcal{A}$-t először a $(G, \lceil n/2 \rceil)$ párra. Ha a válasz `nem`, azaz nincs $\lceil n/2 \rceil$ független pont, akkor próbálkozzunk a $(G, \lceil n/4 \rceil)$ párral. Ellenkező esetben pedig, a $(G, \lceil 3n/4 \rceil)$ párral. Hasonlóan folytatva, bináris kereséssel meghatározhatjuk azt a legnagyob k értéket, amire $(G, k) \in$ MAXFTL. Az eljárás során az $\mathcal{A}$ algoritmus alkalmazásainak száma $\Theta(\log n)$ és mindegyik polinom lépésig tart, tehát összesen is polinom idejű algoritmust kapunk. □

7. Megjegyzés. *Ha nem csak a méretét akarjuk meghatározni, hanem meg is akarunk találni egy legnagyobb független ponthalmazt G-ben, az is megoldható polinom időben az $\mathcal{A}$ algoritmus felhasználásával.*

Most megmutatjuk, hogy a MAXFTL eldöntése valószínűleg nehéz.

3. Tétel. *A* MAXFTL *probléma* NP*-teljes.*

Bizonyítás: MAXFTL $\in$ NP, mert az `igen` válaszra egy jó t bizonyíték lehet egy megfelelő független ponthalmaz pontjainak felsorolása. A $\mathcal{T}$ algoritmus egy (G, k, t) bemenet esetén ellenőrzi, hogy t valóban a G gráfnak k darab csúcsát tartalmazza, úgy hogy semelyik benne szereplő két csúcs között nincs él G-ben. Könnyű látni, hogy ez megvalósítható polinomiális lépésszámmal, és mivel minden jó t polinomiális hosszú G méretében (hiszen legfeljebb annyi csúcsot kell felsorolni, ahány csúcsa van G-nek – nagyoob k értéknél a válasz biztos `nem`) ez egy hatékony tanúsítvány.

Az NP-teljességhez mutatunk egy 3SZÍN $\prec$ MAXFTL Karp-redukciót. Ehhez egy olyan polinom időben számolható függvényt kell megadni, ami minden G gráfhoz hozzárendel egy (H, k) párt úgy, hogy $G \in$ 3SZÍN $\Leftrightarrow$ $(H, k) \in$ MAXFTL. Jelölje a G gráf pontjait $v_1, \ldots, v_n$. A H-nak $3n$ darab pontja lesz, legyenek ezek $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, $c_1, \ldots, c_n$. Ha G-ben van él v_i és v_j között, akkor menjen él az a_i és a_j, a b_i és b_j, valamint a c_i és c_j pontok között is (azaz vettünk 3 példányt a G gráfból). Ezeken felül még minden $1 \leq i \leq n$ indexre húzzuk be mindhárom élet az a_i, b_i és c_i pontok között (azaz egy G-beli pont mindhárom példánya között), k pedig legyen n. Világos, hogy ez a konstrukció adott G-re polinom időben megvalósítható, hiszen a H-nak háromszor annyi pontja lesz mint G-nek, éleinek száma $3e + 3n$, ahol e jelöli G éleinek számát.

Előbb belátjuk, hogy ha $G \in$ 3SZÍN, akkor a H gráfban van n független pont: tekintsük a G gráf egy 3 színnel való színezését. A H-ban vegyük azt a ponthalmazt, mely az a_i-k közül azokat tartalmazza, amik a színezés első színosztályába tartozó pontoknak felelnek meg, a b_i-k közül a második színosztályba tartozó pontok megfelelőit, a c_i-k közül pedig a harmadik színosztály megfelelőit. Ekkor minden i-re az a_i, b_i, c_i csúcsok közül pontosan egyet választottunk, tehát összesen n darabot. Ezek a kiválasztott csúcsok függetlenek H-ban, mert a kiválasztott a_i-k G-ben függetlenek (hiszen azonos színűre voltak színezve G-ben) és ugyanez igaz a b_i-kre illetve a c_i-kre is. Továbbá, mivel egy G-beli pontnak csak egy példánya van benne, ezért a kiválasztott a, b és c pontok között sincsenek élek. Így tehát $(H, n) \in$ MAXFTL.

Még azt kell megmutatni, hogy ha $(H, n) \in$ MAXFTL, akkor $G \in$ 3SZÍN. A H gráf egy F független ponthalmaza minden i-re az a_i, b_i, c_i pontok közül csak egyet tartalmazhat. Mivel n pont van F-ben, ezért minden i-re az a_i, b_i, c_i pontok egyikét tartalmaznia is kell. Az F pontjaiból az a típusúak az eredeti G-nek egy független ponthalmazát adják, és ugyanez igaz a b, illetve a c típusú pontokra is. Egy H-beli n méretű független ponthalmazból az alábbi módon lehet a G gráf egy 3 színnel való színezését megkapni: A független ponthalmazba eső a típusú pontok G-beli megfelelőit színezzük az első színnel, a b típusú pontok megfelelőit a második színnel, a c típusú pontok megfelelőit a harmadik színnel. Ezzel G pontjainak megadtuk egy 3 színnel való színezését, tehát $G \in$ 3SZÍN. $\square$

8. Megjegyzés. *Ha az eldöntési problémát úgy definiáltuk volna, hogy olyan (G, k) párokból áll, melyekre a G-beli maximális független ponthalmaz mérete pontosan k, akkor azzal a nehézséggel néztünk volna szembe, hogy nem világos mi lehetne az* `igen` *válaszra egy rövid bizonyíték, hogyan működhetne egy jó tanúsítvány. Ebben az esetben k pont megadása nem elég, mert bár azt tudjuk polinom időben ellenőrizni, hogy az adott k pont valóban egy független halmazt alkot, de mi garantálja azt, hogy ennél több pontból álló független ponthalmaz nincs a gráfban? (Az így definiált változatról nem ismert, hogy* NP*-ben van-e.)*

A MAXFTL problémához hasonlóan definiálhatjuk a legnagyobb teljes részgráf eldöntési problémáját.

MAXKLIKK

Bemenet: (G, k) pár, ahol G egy gráf és k egy pozitív egész szám.

Kérdés: Van-e G-ben k pontú teljes részgráf?

Erre is hasonlóak igazak, mint a MAXFTL problémára.

4. Tétel. *Ha lenne egy $\mathcal{A}$ polinom idejű algoritmus, amely eldönti a* MAXKLIKK *problémát, akkor polinom időben meg is lehetne határozni egy adott gráfban egy maximális méretű teljes részgráf pontjainak számát.*

Bizonyítás: A bizonyítás itt is hasonlóan megy, a legnagyobb klikk mérete az $\mathcal{A}$ algoritmus segítségével bináris kereséssel meghatározható. $\square$

5. Tétel. *A* MAXKLIKK *probléma* NP*-teljes.*

Bizonyítás: Az világos, hogy MAXKLIKK $\in$ NP, mert bizonyítékként a t-ben most k olyan csúcsot sorolunk fel, amelyek közül bármelyik kettő között van él, könnyű olyan hatékony tanúsítványt készíteni, ami ezt ellenőrzi.

Az NP-teljesség bizonyításához mutatunk egy MAXFTL $\prec$ MAXKLIKK Karp-redukciót. Legyen $f(G,k) = (\overline{G},k)$, ahol $\overline{G}$ a G gráf komplementerét jelöli. Ez egy, a gráf méretében polinom időben számolható függvény és nyilván

$$(G,k) \in \text{MAXFTL} \quad \Leftrightarrow \quad (\overline{G},k) \in \text{MAXKLIKK}.$$

□

További NP-teljes problémák (bizonyítás nélkül)

- H
  Bemenet: G irányítatlan gráf.
  Kérdés: Van G-ben Hamilton-kör?

- HÚT
  Bemenet: G irányítatlan gráf.
  Kérdés: Van G-ben van Hamilton-út?

- S-T-HÚT
  Bemenet: G irányítatlan gráf, és két kitüntetett csúcsa, s és t.
  Kérdés: Van G-ben olyan Hamilton-út, aminek végpontjai s és t?

6. Tétel. *A* RÉSZGRÁFIZO *probléma* NP*-teljes, ahol* RÉSZGRÁFIZO
Bemenet: G_1 *és* G_2 *irányítatlan gráfok.*
Kérdés: Van-e G_1*-nek* G_2*-vel izomorf részráfja?*

Bizonyítás: Az NP-beliséghez a t bizonyíték lehet egy leírás, hogy G_2 melyik csúcsának melyik G_1-beli csúcs felel meg, a hozzá tartozó tanúsítvány ellenőrzi, hogy ez a megfeleltetés jó-e, azaz különböző csúcsok képe különböző, és G_2-ben összekötött csúcsoknak olyan csúcsok felelnek meg, melyek között an G_1-ben él. A megfeleltetés, azaz t hossza G_2 csúcsszámával arányos, az ellenőrzés is polinomiális.

Az NP-teljesség bizonyításához mutassuk meg hogy van H $\prec$ RÉSZGRÁFIZO Karp-redukció. Ehhez definiáljuk azt a függvényt, mely minden n pontú G gráfhoz a (C,G) párt rendeli, ahol C egy n pontú kör. Ez a függvény kiszámolható polinom időben. Mivel G-ben pontosan akkor van Hamilton-kör, ha van benne C-vel izomorf részgráf, ezért $G \in$H $\Leftrightarrow$ $(C,G) \in$ RÉSZGRÁFIZO. □

A H helyett használhattuk volna például a MAXKLIKK problémát is.

9. Megjegyzés. *A hasonlónak tűnő* GRÁFIZO *probléma:*
Bemenet: G_1 *és* G_2 *irányítatlan gráfok.*
Kérdés: $G_1 \simeq G_2$*?*
szintén NP*-ben van (Házi feladat), de nem ismert, hogy* NP*-teljes-e, vagy hogy esetleg van-e rá polinom idejű algoritmus.*

Néhány fontos, nem gráfokról szóló NP-teljes eldöntési feldat (bizonyítás nélkül)

- 3DH: Tekintsünk három azonos méretű diszjunkt véges halmazt, ezek $|A| = |B| = |C|$, és tekintsünk néhány olyan három elemű halmazt, melyek mindhárom halmazból egy-egy elemet tartalmaznak. Kérdés, hogy kiválasztható-e ezekből a 3 elemű halmazokból néhány úgy, hogy az alaphalmaz ($A \cup B \cup C$) minden eleme pontosan egy kiválasztott halmazban legyen benne. Formálisabban:

  Bemenet: $(A, B, C; F_1, F_2, \cdots, F_n)$, ahol $|A| = |B| = |C|$ és $F_i \subseteq A \times B \times C$.
  Kérdés: Van-e olyan $I \subseteq \{1, 2, \ldots, n\}$, hogy az F_j halmazok $j \in I$ esetén az $A \cup B \cup C$ minden elemét pontosan egyszer fedik le.

10. Megjegyzés. *A hasonlóan definiálható* 2DH *esetében 2 elemű halmazok szerepelnek. Ezek felfoghatók egy páros gráf éleinek, és ilyen szemlélettel az a kérdés, hogy az adott páros gráfban van-e teljes párosítás, tehát* $2\mathrm{DH} \in \mathrm{P}$ *(magyar módszer).*

- X3C: Itt egyetlen A véges alaphalmaz van és ennek adottak bizonyos 3 elemű részhalmazai. Az eldöntési feladat itt is az, hogy ezekből néhányat ki tudunk-e választani úgy, hogy A minden eleme pontosan egy kiválasztott halmazban legyen benne.

  Bemenet: $(A; F_1, F_2, \cdots, F_n)$, ahol $F_i \subseteq A$ és $|F_i| = 3$.
  Kérdés: Van-e olyan $I \subseteq \{1, 2, \ldots, n\}$, hogy az F_j halmazok $j \in I$ esetén az A minden elemét pontosan egyszer fedik le?

11. Megjegyzés. *A hasonlón definiálható* X2C *probléma megfelel annak a kérdésnek, hogy adott gráfban van-e teljes párosítás. Ismert, hogy a teljes párosítás létezése eldönthető polinom időben, így tehát* $\mathrm{X2C} \in \mathrm{P}$.

- RH (részhalmazösszeg):

  Bemenet: $s_1, s_2, \ldots, s_n$ pozitív egész számok, és még egy b pozitív egész.
  Kérdés: Az s_i-k közül kiválasztható-e néhány úgy, hogy összegük épp b-vel legyen egyenlő?

- PARTÍCIÓ

  Bemenet: $s_1, s_2, \ldots, s_n$ pozitív egész számok.
  Kérdés: Két részre oszthatóak-e úgy, hogy a két rész összege azonos legyen?

  Azaz van-e olyan $I \subseteq \{1, 2, \ldots, n\}$, melyre $\sum_{j \in I} s_j = \sum_{j \notin I} s_j$.

- HÁTIZSÁK

  Bemenet: $s_1, s_2, \ldots, s_n$ és $v_1, v_2, \ldots, v_n$ pozitív egész számok, valamint b, k pozitív egészek.
  Kérdés: Van-e olyan $I \subseteq \{1, 2, \ldots, n\}$, melyre $\sum_{j \in I} s_j \leq b$ és $\sum_{j \in I} v_j \geq k$

Kevésbé formálisan: van n tárgy, az i-ediknek s_i a súlya és v_i az értéke. Továbbá van egy hátizsákunk, aminek teherbírása b. Kérdés, hogy ki tudunk-e választani úgy néhány tárgyat, hogy összességében ne lépjük túl a hátizsák teherbírását, de legalább k értéket elpakoljunk. (Az eredeti változatban ez egy maximalizálási feladat, adott b súlykorláthoz határozzuk meg a lehető legnagyobb összértéket, ami elpakolható – a fenti ennek az eldöntési változata.)

- LÁDAPAKOLÁS

  Bemenet: n tárgy, az i-edik mérete $0 < s_i \leq 1$ racionális szám.
  Kérdés: Belepakolható-e az összes tárgy k darab ládába akkor, ha minden ládába legfeljebb 1 összméretnyi tárgyat tehetünk?

- EP (azaz egész értékű programozás) Tekintsük a $\sum_{j=1}^{n} a_{ij}x_j \leq b_i$, $x_j \geq 0$ egyenlőtlenségrendszert, ahol a_{ij}, b_i adott egész számok. Kérdés, hogy ha adottak még a c_j $(1 \leq j \leq n)$ egész számok is, akkor mennyi lesz a $\sum_{j=1}^{n} c_j x_j$ maximális értéke, ha minden x_j egész szám kell legyen. Az EP ennek a maximalizálási feladatnak az eldöntési változata.

12. Megjegyzés. *Ha az EP problémánál nem kötjük ki, hogy minden x_j egész szám kell legyen, akkor kapjuk a* lineáris programozás *(röviden* LP*) feladatot. Az ehhez tartozó eldöntési feladat a* P *osztályban van (és van rá több, a gyakorlatban is hatékonyan működő programcsomag). Viszont, ha megköveteljük, hogy a megoldás egész legyen, akkor már a feladat* NP*-teljes lesz. Ez utóbbi tény nem meglepő, mivel a korábban felsorolt problémák mindegyike megfogalmazható egész programozás feladatként is.*

2. Példa. *Vegyük a* MAXFTL *problémát. Ebből úgy kaphatunk* EP *feladatot, ha a gráf minden i csúcsának megfeleltetünk egy x_i változót. Az egyenlőtlenségek legyenek az alábbiak: minden $\{i, j\}$ élére a gráfnak legyen $x_i + x_j \leq 1$ és minden változóra $x_i \leq 1$, $x_i \geq 0$. Ezen feltételek mellett a kérdés, hogy lehet-e $\sum x_i \geq k$ (eldöntési változat).*

A két utóbbi feltételtípus garantálja, hogy a változók értéke csak 0 vagy 1 lehet. Könnyű látni, hogy az élekre vonatkozó feltételek pontosan azt írják le, hogy azok a csúcsok, melyekhez tartozó változó értéke 1 a gráfban egy független halmazt alkotnak.

Feladatok

1. Jelölje X_1 azt a problémát, hogy egy adott irányítatlan gráf összefüggő-e és X_2 azt, hogy van-e benne Hamilton-kört. Lehetséges-e, hogy $X_1 \prec X_2$, illetve hogy $X_2 \prec X_1$?

   Megoldás: Az, hogy egy gráf összefüggő-e, polinom időben eldönthető (pl. egy szélességi vagy mélységi bejárással), tehát $X_1 \in$ P. Tudjuk, hogy az X_2 probléma NP-teljes (X_2 =H). Mivel P $\subseteq$ NP, ezért az NP-teljesség definíciója miatt $X_1 \prec X_2$.

Másrészt viszont, ha létezik az $X_2 \prec X_1$ Karp-redukció, akkor a 3. állítás miatt $X_2 \in$ P, és így P = NP. Nem kizárt, hogy ez igaz legyen, de a tudomány mai állása szerint nem ismert, hogy P $\stackrel{?}{=}$ NP.

2. Igazolja, hogy ha 3SZÍN benne van co NP-ben, akkor NP = co NP.

   Megoldás: Mivel a 3SZÍN probléma NP-teljes, tehát minden $X \in$ NP probléma visszavezethető rá, azaz $X \prec$ 3SZÍN. A feltétel szerint 3SZÍN $\in$ co NP, és ezért az 5. állítás miatt $X \in$ co NP, amiből NP $\subseteq$ co NP következik. Másrészt, ha $X \in$ co NP, akkor $\overline{X} \in$ NP, tehát $\overline{X} \prec$ 3SZÍN. A feltevés szerint 3SZÍN $\in$ co NP, ezért az 5. állítás miatt $\overline{X} \in$ co NP, azaz $X \in$ NP.

3. Legyen SÍKMAXKLIKK

   Bemenet: (G, k), ahol G egy síkbarajzolható gráf
   Kérdés: Van-e G-ben k pontú klikk

   Mutassa meg, hogy ez NP-teljes, vagy mutassa meg, hogy a probléma P-ben van.

   Megoldás: Tudjuk, hogy egy síkgráfban nem lehet 4-nél több pontú teljes részgráf, hiszen K_5 nem rajzolható síkba. Ekkor viszont a probléma az alábbi módon eldönthető:

   Ha $k > 4$, akkor a válasz `nem`, és készen vagyunk;

   Ha $k \leq 4$, akkor ellenőrizzük a gráf pontjainak az összes k elemű részhalmazát. Amennyiben találunk közöttük olyat, amin a gráf teljes, akkor a válasz `igen`, egyébként pedig `nem`. Mivel egy n pontú gráfból kevesebb mint $n^k \leq n^4$ féleképpen tudunk $k \leq 4$ pontot kiválasztani, és egy választás ellenőrzése $O(k^2) = O(4^2) = O(1)$ lépés, az algoritmusnak ez a része is polinomiális.

4. P-beli vagy NP-teljes az alábbi probléma?

   Bemenet: (G, k), ahol G egy gráf, $k > 0$ egész.
   Kérdés: Van-e a G gráfban legalább k élű kör?

   Megoldás: Belátjuk, hogy NP-teljes. Az NP-beliséget mutatja hogy az `igen` válaszra bizonyíték lehet egy keresett kör pontjainak a kör mentén való felsorolása. A tanúsítvány feladata ellenőrizni, hogy valóban egy k pontú kört ír le a t bizonyíték.

   Ezután megadunk egy visszaezetést a H problémáról. Egy tetszőleges G gráfhoz rendeljük hozzá az $f(G) = (G, n)$ párt, ahol n a G pontjainak száma. Ekkor $G \in$ H $\Leftrightarrow f(G) = (G, n)$ esetén a válasz `igen`. Mivel f polinom időben számolható, ezért ez egy jó Karp-redukció.

5. P-beli vagy NP-teljes az alábbi X probléma?

   Bemenet: G gráf.
   Kérdés: Kiszínezhetőek-e a csúcsai 4 színnel?

Megoldás: Megmutatjuk, hogy az X probléma NP-teljes. Polinom időben ellenőrizhető, hogy ha adott egy G gráf, aminek minden csúcsához 4 féle szín valamelyikét rendeltük, akkor ez vajon helyes színezés-e. Ezzel kapunk egy hatékony tanúsítványt (a színek hozzárendelésének leírása, azaz t hossza lineáris).

Az NP-teljességhez megadunk egy 3szín $\prec$ 4szín visszavezetést. Egy tetszőleges G gráfból készítsük el azt a G' gráfot, amit úgy kapunk, hogy egy új x pontot hozzáveszünk a gráfhoz, és ezt az x pontot minden régivel összekötjük. Ez a konstrukció polinom időben végrehajtható. Világos, hogy ha $G \in$ 3szín, akkor $G' \in$ 4szín. A másik irányhoz tegyük fel, hogy G' kiszínezhető 4 színnel. Ekkor az x pont színe egyetlen másik pont színezésére sem használható, hiszen x minden más ponttal össze van kötve. Ez azt jelenti, hogy a G' gráf többi része (ami az eredeti G-vel izomorf) 3 színnel van kiszínezve, tehát $G \in$ 3szín.

6. Legyen X az a kérdés, hogy adott G gráf csúcsai kiszínezhetőek-e 3 színnel úgy, hogy az egyik színt csak egyszer használjuk. Ez P-beli vagy NP-teljes?

   Megoldás: Megmutatjuk, hogy ez P-ben van. Egy gráf akkor és csak akkor rendelkezik a kívánt tulajdonsággal, ha van egy olyan pontja, amit elhagyva páros gráfot kapunk. Ezt viszont tudjuk polinom időben ellenőrizni, mert annak eldöntésére, hogy egy gráf páros gráf-e, van polinom idejű algoritmus (egy szélességi bejárás mentén osztjuk a pontokat két osztálya, ha ellentmondásra jutunk, akkor a gráf nem páros), és ezt kell minden egyes pont elhagyása után a maradék gráfra végrehajtani.

7. Egy hivatal új épületbe fog költözni. Az épület minden emeletén ugyanakkora terület használható fel irodák kialakítására. Minden részleg megmondta, hogy összesen mekkora irodaterületre tart igényt. Azt akarjuk eldönteni, hogy meg lehet-e oldani a költözést úgy, hogy egyetlen részleg se legyen kettévágva, azaz egy részleg teljes egészében egy emeleten legyen (de egy emeletre kerülhet több részleg is). Igazolja, hogy a probléma P-ben van, vagy azt, hogy NP-teljes.

   Megoldás: A feladat kicsit formálisabb leírása: Adottak a részlegek igényei: $a_1, a_2, \ldots, a_n$ pozitív egészek; az egy szinten használható terület nagysága: b pozitív egész; az épület szintjeinek száma: k pozitív egész. A cél, hogy az a_i-ket k csoportba osszuk úgy, hogy minden csoport összege legfeljebb b legyen.

   Ez nyilván NP-ben van, hiszen egy jó beosztás lehet a bizonyíték a megoldhatóságra, aminek helyességét polinom időben ellenőrizni tudjuk (és persze a hossza is polinomiális).

   Megmutatjuk, hogy van partíció $\prec X$ Karp-redukció.

   Legyen $(s_1, s_2, \ldots, s_n)$ a partíció feladat egy lehetséges bemenete. Ennek feleltessük meg azt a feladatot, amikor a hivatal épületében 2 szint van, $b = (\sum_{s_i})/2$ és az i-edik részleg helyigénye $a_i = s_i$. Ezzel a megfeleltetéssel $(s_1, s_2, \ldots, s_n) \in$ PARTÍCIÓ $\Leftrightarrow$ a költözés megoldható. Tehát az X-re visszavezethető egy NP-teljes probléma, és $X \in$ NP, ezért X maga is NP-teljes.