P, NP

1. Álljon az L nyelv azokból az irányítatlan gráfokból, melyekben nincs kör. Igazolja, hogy $L \in \mathrm{P}$.

   Megoldás: Elegendő azt megmutatni, hogy erre az eldöntési feladatra van polinom idejű algoritmus. A szélességi (vagy mélységi) bejárás alkalmas erre: egy tetszőleges pontból indítjuk és akkor hagyjuk abba, hogy ha vagy minden pontot bejárt vagy talált egy élet, ami nem faél. Az utóbbi esetben van kör a gráfban. Ha viszont minden él faél, akkor a gráf egy erdő, tehát nincs benne kör.

   Az algoritmus lépésszáma n csúcsú gráfokon mátrixos megadás esetén $O(n^2)$, ami lineáris a bemenet $N = n^2$ hosszában.

   Megjegyzés: Ha ezt Turing-géppel akarjuk megvalósítani, akkor több lépés kell. Hiszen míg a mátrixból két pont közötti él létezését eldönteni $O(1)$ lépés, addig a Turing-gép szalagján oda kell menjünk a megfelelő helyre, ami n^2-tel arányos lépést is jelenthet. De az ebből adódó $O(n^4)$ összes lépésszám is polinomiális n-ben (és így N-ben is).

2. Az L nyelv álljon az olyan (G, s, t) hármasokból, ahol G egy irányított gráf, s és t a gráfnak két csúcsa és G-ben van út s-ből t-be. Igazolja, hogy $L \in \mathrm{P}$.

   Megoldás: Egy s-ből induló szélességi bejárással megválaszolható a kérdés. (A bejárás leállhat, ha elérünk t-be vagy ha bejártuk s komponensének összes csúcsát.) Mivel a BFS polinom idejű, ezért $L \in \mathrm{P}$.

3. Álljon az L nyelv azokból az (n, m) párokból, amelyekben n és m egy-egy pozitív egész szám bináris alakja, és ez a két szám relatív prím. Igaz-e, hogy $L \in \mathrm{P}$?

   Megoldás: Itt a bemenet hossza $\Theta(\log n + \log m)$, de az euklideszi algoritmus, amivel két szám legnagyobb közös osztója meghatározható, ebben is polinom idejű algoritmus.

4. Bizonyítsa be az alábbi két nyelvről, hogy NP-beliek! Melyikről tudja belátni, hogy P-ben van? Melyikről látja, hogy co NP-beli?

   (a) G irányítatlan gráfok nyelve, amelyekben van legfeljebb 100 élből álló kör.

   (b) (G, k) párokból álló nyelv, ahol a G irányítatlan gráfban van legfeljebb k élből álló kör.

   Megoldás: (a) A tanú tétel alapján NP-ben van, hiszen legyen az L_1 nyelv az olyan (G, y) párok nyelve, ahol G egy irányítatlan gráf és y egy legfeljebb 100 élű kör csúcsai a kör mentén sorban felsorolva. Világos, hogy G pontosan akkor van benne a feladatbeli L nyelvben, ha van hozzá olyan y, hogy $(G, y) \in L_1$. Ennek az y-nak a hossza, ha a körbeli csúcsok sorszámát binárisan felírjuk, $\Theta(\log n)$, ahol n a G csúcsainak száma, tehát $|y|$ kisebb mint a G megadásának hossza, ezért belefér a polinom korlátba. Még az kell, hogy $L_1 \in P$. Ez azért igaz, mert az L_1-be tartozáshoz azt kell ellenőrizni, hogy a bemenet y részében legfeljebb 100 csúcs szerepel, ezek mind különbözőek és hogy a szomszédos csúcsok, valamint az első és utolsó csúcs között megy él. (Igazából azt is megengedhetnénk, hogy a felsorolásban legyenek ismétlődő csúcsok, azaz egy zárt élsorozatot adjanak, mert ha ilyen van, akkor legfeljebb 100 élű kör is van.)

   (b) Ahhoz, hogy ez NP-ben van, az előző bizonyítást csak kicsit kell módosítani: az y tanú most egy kört alkotó legfeljebb k darab csúcs felsorolása. A bemenetben k binárisan van leírva, azaz a bemenet hossza $\Theta(n^2 + \log k)$. Formálisan nézve egy $k \log n$ hosszú tanú ebben nem polinomiális. De vegyük észre, hogy csak $k \leq n$ esetben lehet megoldás, és ekkor $k \log n \leq n \log n < n^2$, tehát a tanú valóban polinom hosszú (sőt, lineáris) a bemenet hosszához viszonyítva. Mivel az L_1-be tartozáshoz legfeljebb $k \leq n$ csúcs különbözőségét és ennyi él meglétét kell ellenőrizni, ez megoldható polinom időben, azaz $L_1 \in \mathrm{P}$.

   Az (a)-ban megadott nyelv világos, hogy P-ben is benne van, hiszen egy n csúcsú gráf esetén a lehetséges 100 élű körök száma nem több, mint n^{100}, ami polinomiális. Adott 100 pontra annak ellenőrzése, hogy az adott sorrendben kört alkotnak konstans sok lépés, tehát minden lehetőség ellenőrzése összesen $O(n^{100})$ és így polinom idő.

   A (b)-nél nem alkalmazhatjuk az előző eljárást, mert a lehetőségek száma most n^k nagyságrendű, ami nem polinomiális n-ben és $\log k$-ban, és itt még az a feltevés sem segít, hogy $k \leq n$. Ennek ellenére ez a nyelv is P-ben van. Ehhez azt kell észrevenni, hogy egy gráfban egy legrövidebb kör megtalálható polinom sok lépésben. Egymás után minden csúcsból indítsunk egy-egy BFS-t, mindegyiket az első nem faélig csináljuk. Ezzel minden esetben kapunk egy olyan kört, ami legfeljebb olyan hosszú, mint a kezdőpontot tartalmazó legrövidebb kör. Az így megtalált körök közül a legrövidebb a gráfban egy legkevesebb élű kör.

Az n darab BFS lépéseinek száma $O(n^3)$, a keletkező körök hosszának meghatározása összesen megoldható $O(n^2)$ lépésben, tehát az egész polinomiális.

Mivel $\mathrm{P} \subseteq \mathrm{co\,NP}$, következik, hogy mindkét nyelv co NP-ben is benne van.

5. Igazolja, hogy a
   (a) MAXKLIKK $= \{(G, k) : G$ irányítatlan gráfban van k pontú klikk$\}$ nyelv NP-ben van.
   (b) 5KLIKK $= \{G : G$ irányítatlan gráfban van 5 pontú klikk$\}$ nyelv
   - NP-ben van,
   - co NP-ben van,
   - P-ben van.

Megoldás: (a) A tanú tételt használjuk: az L_1 nyelv álljon az olyan (G, k, y) hármasokból, ahol G egy irányítatlan gráf, k egy pozitív egész és y olyan k darab csúcs felsorolása, melyek G-ben egy teljes gráfot alkotnak. Ha $(G, k) \in$ MAXKLIKK, akkor $k \leq n$, tehát a megfelelő y hossza polinomiális. Azt kell ellenőrizni, hogy y valóban k darab különböző csúcsot tartalmaz, és hogy bármely kettő között megy él (ami kevesebb, mint $k^2 \leq n^2$ él ellenőrzését jelenti), és ez megoldható polinom időben. Ha $(G, k) \notin$ MAXKLIKK, akkor nincs olyan y, ami megfelel ennek az ellenőrzésnek.

(b) Az előző bizonyítás a $k = 5$ esetre alkalmazva jó az NP-beliség bizonyításához.

Az, hogy 5KLIKK $\in$ P abból következik, hogy összesen $\binom{n}{5}$ lehetséges 5 pontú klikk van, ezek ellenőrizhetők összesen $O(n^5)$ lépésben.

Ebből, mivel $\mathrm{P} \subseteq \mathrm{co\,NP}$, következik, hogy 5KLIKK $\in$ co NP.

6. Bizonyítsa be, hogy az alábbi nyelvek co NP-beliek!
   (a) Az olyan páros gráfok nyelve, amelyekben van teljes párosítás.
   (b) Az olyan gráfok nyelve, amelyekben van teljes párosítás.
   (c) A síkbarajzolható gráfok nyelve.
   (d) Az olyan gráfok nyelve, amelyekben akárhogyan színezzük ki az éleket 2 színnel, mindig keletkezik egyszínű háromszög.

Megoldás: Mindegyik esetben azt kell megmutatni, hogy a nyelv komplementere NP-ben van. Ehhez a tanú tétel értelmében elegendő egy hatékony tanúsítványt mutatnunk a komplementer nyelvre, ami lényegében azt jelenti, hogy a nyelvbe nem tartozáshoz kell rövid tanú és ezt ellenőrző polinom idejű eljárás.

(a) A nyelv polinom időben felismerhető, ennek bizonyítása is jó megoldás, de itt most, a gyakorlás kedvéért, egy tanút mutatunk a komplementerre.

Arra, hogy egy páros gráfban nincs teljes párosítás tanú egy olyan X ponthalmaz, ami megsérti a Hall-feltételt. Ha megadjuk a pontoknak egy ilyen részhalmazát, akkor ellenőrizni kell, hogy ezek a pontok mind a páros gráf egyik pontosztályából kerültek ki. A szomszédaik meghatározásának lépésszáma $O(n^2)$, és ennyi időben azt is ellenőrizni tudjuk, hogy a számuk valóban több mint $|X|$. Amennyiben van teljes párosítás a gráfban, akkor világos, hogy ilyen X nem létezik.

Szigorúan véve a nyelv komplementerébe azok a bemenetek is beletartoznak, amelyek nem páros gráfot írnak le. Ilyenkor az üres szó is megfelel tanúnak, hiszen polinom időben meg tudunk győződni róla, ha egy gráf nem páros gráf (BFS), és arról is, ha a bemenet nem gráfot ír le (mert nem négyzetszám hosszú 0/1 sorozat vagy a megfelelő mátrix nem lenne szimmetrikus – nem irányítatlan a gráf).

A későbbiekben ilyen esetekben a nem megfelelő alakú bemenet (tehát nem gráf vagy ha irányítatlan gráf kellene, akkor nem ilyet leíró) esetére általában nem fogunk kitérni. Ezek az előbb vázolt módon egyszerűen kezelhetők.

(b) A Hall-tétel helyett itt a Tutte-tételt kell alkalmazni: arra, hogy nincs teljes párosítás tanú egy olyan X ponthalmaz, hogy ezt elhagyva a gráfból, a megmaradt részben a páratlan pontszámú komponensek száma több, mint $|X|$. Tehát L_1 állhat a (G, x) párokból, ahol x az X halmaz pontjainak felsorolása, aminek n csúcsú gráf esetén a hossza $O(n \log n)$. Az L_1-be tartozáshoz ellenőrizni kell, hogy x a gráf k különböző csúcsának a felsorolása. Az elhagyásukkal keletkező gráf (mátrixa) polinom időben megkonstruálható. Ennek a maradék gráfnak a komponensei (és azok mérete) egy szélességi bejárással polinom időben meghatározhatók, és innen a Tutte-tételbeli feltétel ellenőrizhető.

Azt is tudjuk, hogy ha van teljes párosítás akkor nincs megfelelő x.

(c) Itt a Kuratowski-tételt használjuk: tanú a gráfban található K_5 vagy $K_{3,3}$ gráf csúcsai és annak leírása, hogy ezek éleinek a gráfban mely utak felelnek meg. (Kizárólag a pontok megadása nem elég, mert nagyon sokféle út lehet közöttük.) Amit az L_1-be tartozás során ellenőrizni kell: ezek tényleg utak az eredeti gráfban, a gráf minden csúcsa legfeljebb az egyikhez tartozik, és persze, hogy valóban az egyik Kuratowski-gráf leírásával van dolgunk. Ez polinom idejű eljárással megvalósítható.

Tudjuk, hogy ha a gráf síkbarajzolható, akkor nincs jó tanú.

(d) Nézzük a komplementer tulajdonságot: a gráf éleihez lehet úgy két színt rendelni, hogy minden háromszögben mindkét szín előforduljon. Erre tanú egy megfelelő színezés, amit $O(n^2)$ bittel leírhatunk (n a gráf csúcsainak száma). A gráfbeli összes háromszög ellenőrzése $O(n^3)$ lépés, ezért $L_1 \in \mathrm{P}$. (A nyelv komplemetere az előbb megadott tulajdonságú gráfokból és a nem gráfot leíró bemenetekből áll, de ez utóbbi eset a korábbiak szerint kezelhető, hiszen felismerhető polinom időben.)

7. Álljon a nyelv az olyan (G, t) párokból, ahol G egy súlyozott, irányítatlan gráf, $t > 0$ egész, és G-ben minden, t darab élből álló párosítás súlya legalább t^2. Igazolja, hogy ez a nyelv $\mathrm{co\,NP}$-ben van!

   Megoldás: A komplementer tulajdonság: a gráfban van olyan t élű párosítás, melynek súlya kisebb, mint t^2. Ehhez tanú egy ilyen párosítás, amihez $2t$ csúcsot kell megadni. Ennek hossza $\Theta(t \log n) \subset O(n^2)$, mert $t < n$ kell legyen. Amit az L_1-be tartozáshoz ellenőrizni kell: ez valóban $2t$ különböző csúcsa a gráfnak, a megfelelő élek a gráfban szerepelnek és ki kell számolni a súlyaik összegét, ami kisebb kell legyen, mint t^2. Ezek mindegyike megvalósítható $O(t) \subseteq O(n)$ lépésben, tehát az eljárás polinomiális.

8. Legyen $f : \{\mathtt{0},\mathtt{1}\}^* \to \{\mathtt{0},\mathtt{1}\}^*$ olyan polinom időben kiszámolható, bijektív függvény, aminél minden $x \in \{\mathtt{0},\mathtt{1}\}^*$ szóra teljesül, hogy $|f(x)| = |x|$. Legyen $L = \{y : \text{ van olyan 1-gyel kezdődő } x, \text{ amire } f(x) = y\}$. Igaz-e, hogy $L \in \mathrm{NP} \cap \mathrm{co\,NP}$?

   Megoldás: A függvény bijektív, tehát van inverze, de ez nem feltétlenül jelenti azt, hogy ezt az inverzet polinom időben ki is tudjuk számolni.

   Azt viszont, hogy $L \in \mathrm{NP}$ elég egy megfelelő tanúsítvánnyal igazolni. Legyen $L_1 = \{(y, 1z) : f(1z) = y\}$. Ekkor az $x = 1z$ tanú hossza a feltétel szerint $|y|$, az ellenőrzése pedig az $f(x)$ kiszámolásából áll, ami polinomiális.

   A $\mathrm{co\,NP}$-beliséghez az $L_0 = \{(y, 0z) : f(0z) = y\}$ nyelv használható, mert a feltétel miatt, ha $f(0z) = y$, akkor nincs másik t szó, amire $f(t) = y$.

9. Igazolja, hogy az a nyelv, ami az összes olyan M determinisztikus véges automata leírásából áll, melyre $L(M) \neq \emptyset$ teljesül, NP-ben van.

   Megoldás: Arra, hogy $L(M) \neq \emptyset$ egy tanú lehet egy $x \in L(M)$. Az ellenőrzés lépésszáma $O(|x|)$. Azt kell még meggondolni, hogy van olyan $x \in L(M)$, amire $|x|$ polinomiális az automata leírásának hosszában, azaz, hogy ha a nyelv nem üres, akkor van rövid eleme. Ehhez vegyük észre, hogy ha $x \in L(M)$ egy legrövidebb szó, akkor a neki megfelelő állapotátmenetek sorozatában nem ismétlődhet állapot (különben az ismétlődések közötti rész kihagyható lenne a szóból). Ez viszont azt jelenti, hogy $|x|$ kisebb, mint az állapotok száma, tehát polinomiális (valójában lineáris).

   Megjegyzés: igazából ez a nyelv P-ben is benne van: azt kell eldönteni, hogy az automatában a kezdő állapotból elérhető egy elfogadó állapot, ami egy, a gráfon végrehajtott bejárással megoldható.