1. 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) 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 $|X|$. **Fontos**, hogy ha nincs teljes párosítás a gráfban, akkor a Hall-tétel értelmében mindig létezik ilyen X halmaz. 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 $|X|$. **Fontos**, hogy ha nincs teljes párosítás a gráfban, akkor a Tutte-tétel értelmében mindig létezik ilyen X halmaz.

   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) 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 komplementere az előbb megadott tulajdonságú gráfokból és a nem gráfot leíró bemenetekből áll, de ez utóbbi eset a korábbiak szerint kezelhető, hiszen felismerhető polinom időben.)

2. Álljon a nyelv az olyan (G, t) párokból, ahol G egy nemnegatív élsúlyokkal rendelkező irányítatlan gráf, $t > 0$ egész, és G-ben minden, t darab élből álló párosítás súlya legalább t^2. Igazolja, hogy ez a nyelv 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 $\Theta(t \log v) \subset O(v^2)$, mert $t < v$ kell legyen, ha v a gráf csúcsainak száma. Amit az L_1-be tartozáshoz ellenőrizni kell: ez valóban $2t$ különböző csúcsa-e a gráfnak és a megfelelő élek a gráfban szerepelnek-e. Ezek mindegyike megvalósítható $O(t) \subseteq O(v)$ lépésben. Ki kell még számolni a súlyaik összegét, ami kisebb kell legyen, mint t^2. Ha legnagyobb súly M, akkor minden súlyban a számjegyek száma legfeljebb $\log M$. Mivel az összeadást lineáris időben el lehet végezni, az összeg kiszámolása $O(t \log M)$ lépést igényel. Így a teljes lépésszám $O(v \log M)$. Az input akár éllistával, akár szomszédossági mátrixszal van megadva, a mérete $n \geq v + \log M$, hiszen szerepelnie kell minden csúcsnak és a legnagyobb súlynak is. Mivel $O(v \log M) \subseteq O(n^2)$, az eljárás polinomiális.

3. Legyen $f : \{0,1\}^* \to \{0,1\}^*$ olyan polinom időben kiszámolható, bijektív függvény, aminél minden $x \in \{0,1\}^*$ szóra teljesül, hogy $|f(x)| = |x|$.
Legyen $L = \{y \mid \text{ van olyan 1-gyel kezdődő } x, \text{ amire } f(x) = y\}$. 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 $L_1 = \{(y, 1z) \mid f(1z) = y\}$. 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 $L_0 = \{(y, 0z) \mid f(0z) = y\}$ nyelv használható, mert a feltétel miatt, ha $f(0z) = y$, akkor nincs másik t szó, amire $f(t) = y$.

4. 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.

5. Igazolja, hogy 3SZÍN $\prec$ 100SZÍN !

   Megoldás: Módosíthatjuk az előadáson látott 3SZÍN $\prec$ 4SZÍN bizonyítást. Tetszőleges G gráfból úgy készül $f(G) = G'$, hogy a csúcshalmazt kiegészítjük 97 további csúccsal, ezek legyenek összekötve G minden csúcsával és egymással is. Ezzel egy polinom időben számolható f függvényt definiáltunk, G szomszédossági mátrixát kiegészítjük 97 további sorral, oszloppal, az új, nem diagonális elemek mind 1-ek.

   Ha $G \in$ 3SZÍN, akkor G'-re egy ilyen színezés kiterjeszthető: az új csúcsok az eddigiektől és egymástól is különböző színt kapnak, amihez összesen 100 szín elég. Másrészt, ha $G' \in$ 100SZÍN, akkor egy jó színezésében a G csúcsai legfeljebb 3 színnel vannak színezve, tehát ilyenkor valóban $G \in$ 3SZÍN.

   Ha precízek akarunk lenni, a Karp-redukció értékét minden bemenetre, a nem gráfokra is meg kell adni. Könnyű látni, hogy ha f nem változtat az ilyen bemeneten, az jó lesz mivel ilyenkor biztos, hogy a bemenet nem gráf, így se a 3SZÍN, se a 100SZÍN nyelvben nincs benne. Az meg, hogy ez az eset áll fenn, polinom időben eldönthető. Tehát az f számolása azzal kezdődik, hogy ellenőrzi, hogy a kapott x bemenet gráfot ad meg vagy sem, ha nem, akkor $f(x) = x$, különben meg a fent leírt módon módosított gráf lesz f értéke.

   Megjegyzés: Mivel általában annak ellenőrzése, hogy a bemenet egy gráf (vagy általában az, hogy formailag jó) általában megy polinom időben, ezért f-et sokszor csak a formailag jó bemeneteken adjuk meg.

6. Igazolja, hogy HAMÚT $\prec$ HAM !
(HAMÚT a Hamilton-utat tartalmazó gráfok nyelve, HAM pedig a Hamilton-kört tartalmazó gráfoké.)

   Megoldás: Tetszőleges G gráfból úgy készül $f(G) = G'$, hogy a csúcshalmazt kiegészítjük egy további v csúccsal, ez legyen összekötve G minden csúcsával. Ezzel egy polinom időben számolható f függvényt definiáltunk, G szomszédossági mátrixát kiegészítjük egy további sorral és oszloppal, az új, nem diagonális elemek mind 1-ek.

   Ha G-ben van egy Hamilton-út, akkor G'-ben lesz Hamilton-kör, hiszen v szomszédos a Hamilton-út két végpontjával. Ha G'-ben van Hamilton-kör, akkor ez tartalmazza v-t. Ha most a Hamilton-körből töröljük v-t, akkor egy Hamilton-út marad, ami G mindent pontját tartalmazza.

7. Mutassa meg, hogy ha $X \prec Y$, akkor $\overline{X} \prec \overline{Y}$ is igaz.

   Megoldás: Ugyanaz az f függvény jó lesz, hiszen $x \in X \Leftrightarrow f(x) \in Y$ pontosan akkor teljesül, amikor $x \notin X \Leftrightarrow f(x) \notin Y$.

8. Bizonyítsa be, hogy ha $L_1 \prec L_2$ és $L_2 \in \mathrm{NP}$, akkor $L_1 \in \mathrm{NP}$.

   Megoldás: Ha $L_1 \prec L_2$, akkor van olyan M_1 DTG, ami $O(n^k)$ időben kiszámolja a redukció $f(x)$ függvényét. Mivel $L_2 \in \mathrm{NP}$, van olyan M_2 NTG, aminek nyelve L_2 és futásideje $O(n^l)$. Legyen M az a NTG, ami x inputon először kiszámítja $f(x)$-et, majd $f(x)$-en futtatja M_2-t. A f tulajdonságai miatt világos, hogy M nyelve L_1, futásideje pedig $O(n^{kl})$ lesz. Ezért $L_1 \in \mathrm{NP}$.

9. Bizonyítsa be, hogy ha $L_1 \prec L_2$ és $L_2 \in \mathrm{co\,NP}$, akkor $L_1 \in \mathrm{co\,NP}$.

   Megoldás: Ha $L_2 \in \mathrm{co\,NP}$, akkor $\overline{L_2} \in \mathrm{NP}$. Mivel $L_1 \prec L_2$, a 7. feladat miatt teljesül $\overline{L_1} \prec \overline{L_2}$ is. Így a 8. feladat miatt $\overline{L_1} \in \mathrm{NP}$. Ebből viszont következik $L_1 \in \mathrm{co\,NP}$.

10. Tegyük fel, hogy van egy eljárásunk, ami egy tetszőleges Boole-formuláról polinom időben eldönti, hogy a SAT nyelvnek eleme vagy nem. Hogyan lehet ezt felhasználva polinom időben megtalálni egy adott $\varphi(x_1, x_2, \cdots, x_m)$ formulához a változóknak egy olyan értékelését, amelyet ha a φ-be behelyettesítünk, akkor a formula értéke igaz lesz?

    Megoldás: Először adjuk be az eljárásnak magát a φ formulát. Ha a válasz az, hogy nincs megoldás, akkor készen vagyunk. Ellenkező esetben legyen $i = 1$ és helyettesítsünk x_i helyébe hamis értéket. Legyen φ_0 az a formula, amit így φ-ből kapunk. Adjuk oda ezt az eljárásnak. Ha a válasz az, hogy továbbra is van megoldás, akkor legyen $\varphi = \varphi_0$, különben pedig $\varphi = \varphi_1$, ahol az utóbbi azt jelzi, amit az x_i helyébe igazat behelyettesítve kapunk. (Vegyük észre, hogy ha φ_0 nem, akkor φ_1 biztos kielégíthető.) Hajtsuk végre ugyanezt az $i = 2, 3, \ldots, m$ választással.

    Ezen a módon a változóknak sorban értéket adunk. Mivel minden i esetén x_i-nek olyan értéket választunk, amihez a hátralevő változók megválaszthatók úgy, hogy a formula igaz legyen, a végén, amikor minden változót rögzítettünk, az érték igaz lesz.

    Lépésszám: legyen az eredeti eljárás lépéspészáma az n méretű formulákon $O(n^c)$. Ezt m-szer hívjuk meg (minden változóra egyszer), mindig legfeljebb n méretű formulára. Mivel $m \leq n$, ezért a lépésszáma $O(n^{c+1})$.

    Megjegyzés: lehet, hogy az eredeti formulához több jó kiértékelés is van, ez a módszer ezekből egyet fog megtalálni, a lexikografikusan legelsőt.

11. Igazolja, hogy ha egy X eldöntési probléma NP-teljes és $X \in \mathrm{NP} \cap \mathrm{co\,NP}$, akkor $\mathrm{NP} = \mathrm{co\,NP}$.

    Megoldás: Mivel X NP-teljes, ezért minden $L \in \mathrm{NP}$ probléma esetén $L \prec X$, amiből $X \in \mathrm{co\,NP}$ miatt $L \in \mathrm{co\,NP}$ jön, tehát $\mathrm{NP} \subseteq \mathrm{co\,NP}$.

    A fordított irányú tartalmazást hasonlóan láthatjuk be, mint az előbb: tetszőleges $L \in \mathrm{co\,NP}$ problémára teljesül, hogy $\overline{L} \in \mathrm{NP}$, tehát $\overline{L} \prec X$ az X NP-teljessége miatt, amiből $\overline{L} \in \mathrm{co\,NP}$ következik. Tehát $L \in \mathrm{NP}$, azaz $\mathrm{co\,NP} \subseteq \mathrm{NP}$, és így $\mathrm{NP} = \mathrm{co\,NP}$.