Számításelmélet

11. előadás

előadó: Kolonits Gábor
kolomax@inf.elte.hu

Lineáris diophantoszi egyenlőtlenségrendszer

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER$=$

$\{\langle \mathbf{A}, \mathbf{b} \rangle \mid \mathbf{A}\mathbf{x} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Lineáris diophantoszi egyenlőtlenségrendszer

Diophantoszi egyenlőtlenségrendszer $=$
$\{\langle \mathbf{A}, \mathbf{b} \rangle \mid \mathbf{Ax} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

Diophantoszi egyenlőtlenségrendszer NP-nehéz.

Lineáris diophantoszi egyenlőtlenségrendszer

Diophantoszi egyenlőtlenségrendszer=
$\{\langle \mathbf{A}, \mathbf{b}\rangle \mid \mathbf{A}\mathbf{x} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

Diophantoszi egyenlőtlenségrendszer NP-nehéz.

Bizonyítás: A 3SAT problémát vezetjük rá vissza polinom időben.

Lineáris diophantoszi egyenlőtlenségrendszer

Diophantoszi egyenlőtlenségrendszer=
$\{\langle \mathbf{A}, \mathbf{b} \rangle \mid \mathbf{A}\mathbf{x} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

Diophantoszi egyenlőtlenségrendszer NP-nehéz.

Bizonyítás: A 3SAT problémát vezetjük rá vissza polinom időben. Legyen φ egy 3KNF, változói $x_1, \ldots, x_n$.

Lineáris diophantoszi egyenlőtlenségrendszer

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER$=$
$\{\langle \mathbf{A}, \mathbf{b}\rangle \mid \mathbf{A}\mathbf{x} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER NP-nehéz.

Bizonyítás: A 3SAT problémát vezetjük rá vissza polinom időben. Legyen φ egy 3KNF, változói $x_1, \ldots, x_n$. Vegyük fel a $0 \leqslant x_i \leqslant 1$ egyenlőtlenségeket.

Lineáris diophantoszi egyenlőtlenségrendszer

Diophantoszi egyenlőtlenségrendszer=

$\{\langle \mathbf{A}, \mathbf{b} \rangle \mid \mathbf{A}\mathbf{x} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

Diophantoszi egyenlőtlenségrendszer NP-nehéz.

Bizonyítás: A 3SAT problémát vezetjük rá vissza polinom időben. Legyen φ egy 3KNF, változói $x_1, \ldots, x_n$. Vegyük fel a $0 \leqslant x_i \leqslant 1$ egyenlőtlenségeket. Továbbá, ha $L_1 \vee L_2 \vee L_3$ φ egy klóza, akkor vegyük fel a $t_1 + t_2 + t_3 \geqslant 1$ egyenlőtlenséget, ahol $t_i = x_j$, ha $L_i = x_j$ és $t_i = 1 - x_j$, ha $L_i = \neg x_j$ $(i = 1, 2, 3)$.

Lineáris diophantoszi egyenlőtlenségrendszer

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER=
$\{\langle \mathbf{A}, \mathbf{b}\rangle \mid \mathbf{Ax} \leqslant \mathbf{b}$ egészegyütthatós egyenlőtlenségrendszernek van egész megoldása$\}$.

Tétel

DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER NP-nehéz.

Bizonyítás: A 3SAT problémát vezetjük rá vissza polinom időben. Legyen φ egy 3KNF, változói $x_1, \ldots, x_n$. Vegyük fel a $0 \leqslant x_i \leqslant 1$ egyenlőtlenségeket. Továbbá, ha $L_1 \vee L_2 \vee L_3$ φ egy klóza, akkor vegyük fel a $t_1 + t_2 + t_3 \geqslant 1$ egyenlőtlenséget, ahol $t_i = x_j$, ha $L_i = x_j$ és $t_i = 1 - x_j$, ha $L_i = \neg x_j$ $(i = 1, 2, 3)$.

Könnyen látható, hogy az így kapott lineáris diophantoszi egyenlőtlenségrendszernek akkor és csak akkor van egész megoldása, ha φ kielégíthető. (Az 1 az igaznak, a 0 a hamisnak felel meg.) $\square$

Lineáris diophantoszi egyenlőtlenségrendszer

1. Megjegyzés: Az is igaz, hogy Diophantoszi egyenlőtlenségrendszer NP-teljes. Az NP-beliség bizonyításához szükségünk lenne egy felső korlátra egy megoldás méretére vonatkozóan. Adható ilyen polinomiális korlát (de ez egyáltalán nem nyilvánvaló állítás, hiszen negatívak is lehetnek az együtthatók).

Lineáris diophantoszi egyenlőtlenségrendszer

1. Megjegyzés: Az is igaz, hogy DIOPHANTOSZI EGYENLŐTLENSÉGRENDSZER NP-teljes. Az NP-beliség bizonyításához szükségünk lenne egy felső korlátra egy megoldás méretére vonatkozóan. Adható ilyen polinomiális korlát (de ez egyáltalán nem nyilvánvaló állítás, hiszen negatívak is lehetnek az együtthatók).

2. Megjegyzés: Tetszőleges (nem feltétlen lineáris) diophantoszi egyenletek megoldhatósága (Hilbert 10. problémája) eldönthetetlen (Jurij Matyijaszevics, 1970). Ez nem meglepő, hiszen a problémaosztály tartalmazza például a Nagy Fermat sejtést/ Wiles tételt is ($a^n + b^n = c^n$-nek nincs pozitív egész megoldása, ha $n > 2$ egész).

Részletösszeg probléma

$$\textsc{Részletösszeg} := \{\langle S, K\rangle \mid S \text{ egész számok egy halmaza, } K \in \mathbb{Z}, \text{ van } S\text{-nek egy olyan } S' \text{ részhalmaza, hogy az } S'\text{-beli számok összege } K\}.$$

Részletösszeg probléma

$\textsc{Részletösszeg} := \{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in \textsc{Részletösszeg}$, mivel 5+9+13=27.

Részletösszeg probléma

$\textsc{Részletösszeg} := \{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in \textsc{Részletösszeg}$, mivel 5+9+13=27.

Tétel

$\textsc{Részletösszeg}$ NP-teljes.

Részletösszeg probléma

$\textsc{Részletösszeg}$:= $\{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in$ $\textsc{Részletösszeg}$, mivel 5+9+13=27.

Tétel

$\textsc{Részletösszeg}$ NP-teljes.

Bizonyítás: Egy S' részhalmaz polinom időben előállítható, majd polinom időben ellenőrizhető, hogy az S'-beli számok összege K-e. Így $\textsc{Részletösszeg} \in$ NP.

Részletösszeg probléma

$\textsc{Részletösszeg}$:= $\{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in$ $\textsc{Részletösszeg}$, mivel 5+9+13=27.

Tétel

$\textsc{Részletösszeg}$ NP-teljes.

Bizonyítás: Egy S' részhalmaz polinom időben előállítható, majd polinom időben ellenőrizhető, hogy az S'-beli számok összege K-e. Így $\textsc{Részletösszeg} \in$ NP.

Megmutatjuk, hogy 3SAT$\leqslant_p$$\textsc{Részletösszeg}$.

Részletösszeg probléma

$\textsc{Részletösszeg} := \{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in$ Részletösszeg, mivel 5+9+13=27.

Tétel

Részletösszeg NP-teljes.

Bizonyítás: Egy S' részhalmaz polinom időben előállítható, majd polinom időben ellenőrizhető, hogy az S'-beli számok összege K-e. Így Részletösszeg$\in$ NP.

Megmutatjuk, hogy 3SAT$\leqslant_p$Részletösszeg.
Legyen φ 3KNF n változóval és m klózzal.

Részletösszeg probléma

$\textsc{Részletösszeg} := \{\langle S, K\rangle \mid S$ egész számok egy halmaza, $K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in \textsc{Részletösszeg}$, mivel 5+9+13=27.

Tétel

$\textsc{Részletösszeg}$ NP-teljes.

Bizonyítás: Egy S' részhalmaz polinom időben előállítható, majd polinom időben ellenőrizhető, hogy az S'-beli számok összege K-e. Így $\textsc{Részletösszeg} \in$ NP.

Megmutatjuk, hogy 3SAT$\leqslant_p$$\textsc{Részletösszeg}$.
Legyen φ 3KNF n változóval és m klózzal.

S $3m + 2n$ darab $n + m$ számjegyű számból fog állni.

Részletösszeg probléma

$\textsc{Részletösszeg}{:=}\ \{\langle S, K\rangle \mid S$ egész számok egy halmaza,
$K \in \mathbb{Z}$, van S-nek egy olyan S' részhalmaza, hogy
az S'-beli számok összege $K\}$.

Példa: $S = \{5, 8, 9, 13, 17\}, K = 27$
Ekkor $\langle S, K\rangle \in$Részletösszeg, mivel 5+9+13=27.

Tétel

Részletösszeg NP-teljes.

Bizonyítás: Egy S' részhalmaz polinom időben előállítható, majd polinom időben ellenőrizhető, hogy az S'-beli számok összege K-e. Így Részletösszeg$\in$ NP.

Megmutatjuk, hogy 3SAT$\leqslant_p$Részletösszeg.
Legyen φ 3KNF n változóval és m klózzal.

S $3m + 2n$ darab $n + m$ számjegyű számból fog állni. j. számjegy alatt a legkisebb helyiértékűtől (azaz hátulról) számított j-edik számjegyet értjük (az 1-es helyiértékű az 1. számegy).

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá:

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.
- A j. klózhoz 3 számot rendelünk.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.
- A j. klózhoz 3 számot rendelünk. Mindegyiknek 1 számjegy kivételével minden számjegye 0, az egyetlen kivétel a j. számjegy, ez a 3 számban legyen rendre 5,6 és 7.

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.
- A j. klózhoz 3 számot rendelünk. Mindegyiknek 1 számjegy kivételével minden számjegye 0, az egyetlen kivétel a j. számjegy, ez a 3 számban legyen rendre 5,6 és 7.

Példa: $\varphi = (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee \neg x_3 \vee \neg x_4)$.

Részletösszeg probléma

Az $1-m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1)-(m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1-m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1-m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.
- A j. klózhoz 3 számot rendelünk. Mindegyiknek 1 számjegy kivételével minden számjegye 0, az egyetlen kivétel a j. számjegy, ez a 3 számban legyen rendre 5,6 és 7.

Példa: $\varphi = (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee \neg x_3 \vee \neg x_4)$.

A számok:

000101 001000 010000 100001
000100 001010 010011 100010

Részletösszeg probléma

Az $1 - m$. számjegyeket megfeleltetjük a klózoknak, az $(m+1) - (m+n)$. számjegyeket pedig a változóknak.

- az i. változóhoz két számot rendelünk hozzá: mindkettőben az $m+i$. bit 1-es. Ezen felül az első számban azon $1 - m$. számjegyek 1-esek, ahol x_i, míg a másik számban azon $1 - m$. számjegyek 1-esek, ahol $\neg x_i$ szerepel a helyiértéknek megfelelő klózban. A többi számjegy 0.
- A j. klózhoz 3 számot rendelünk. Mindegyiknek 1 számjegy kivételével minden számjegye 0, az egyetlen kivétel a j. számjegy, ez a 3 számban legyen rendre 5,6 és 7.

Példa: $\varphi = (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee \neg x_3 \vee \neg x_4)$.

A számok:

000101 001000 010000 100001
000100 001010 010011 100010
000005 000006 000007
000050 000060 000070

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1 - m$. számjegyek mindegyike 21, az $(m+1) - (m+n)$. számjegyek mindegyike 2.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1 - m$. számjegyek mindegyike 21, az $(m+1) - (m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1 - m$. számjegyek mindegyike 21, az $(m+1) - (m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg. Legyen K minden $1 - m$. számjegye 8, minden $(m+1) - (m+n)$. számjegye pedig 1-es.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1-m$. számjegyek mindegyike 21, az $(m+1)-(m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg. Legyen K minden $1-m$. számjegye 8, minden $(m+1)-(m+n)$. számjegye pedig 1-es. Mivel 21<32, ezért K csak úgy érhető el, ha minden helyiértéken 8 illetve 1 az összeg.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1 - m$. számjegyek mindegyike 21, az $(m+1) - (m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg. Legyen K minden $1 - m$. számjegye 8, minden $(m+1) - (m+n)$. számjegye pedig 1-es. Mivel 21<32, ezért K csak úgy érhető el, ha minden helyiértéken 8 illetve 1 az összeg.

Ha φ kielégíthető, akkor van egy I interpretáció, ami igazra értékeli. Válasszuk az első $2n$ szám közül azt az n-et, ami I igaz literáljainak felel meg.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1 - m$. számjegyek mindegyike 21, az $(m+1) - (m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg. Legyen K minden $1 - m$. számjegye 8, minden $(m+1) - (m+n)$. számjegye pedig 1-es. Mivel 21<32, ezért K csak úgy érhető el, ha minden helyiértéken 8 illetve 1 az összeg.

Ha φ kielégíthető, akkor van egy I interpretáció, ami igazra értékeli. Válasszuk az első $2n$ szám közül azt az n-et, ami I igaz literáljainak felel meg. Ekkor az $(m+1) - (m+n)$. számjegyeknél 1 az összeg, míg az $1 - m$. számjegyeknél 1, 2, vagy 3 aszerint, hogy klózonként hány literál igaz.

Részletösszeg probléma

Vegyük észre, hogyha minden számot összeadunk akkor az $1-m$. számjegyek mindegyike 21, az $(m+1)-(m+n)$. számjegyek mindegyike 2.

Nem választottuk még meg a K számot, ehhez válasszunk egy 21-nél nagyobb számot, pl. 32-t. K-t 32-es számrendszerben adjuk meg. Legyen K minden $1-m$. számjegye 8, minden $(m+1)-(m+n)$. számjegye pedig 1-es. Mivel 21<32, ezért K csak úgy érhető el, ha minden helyiértéken 8 illetve 1 az összeg.

Ha φ kielégíthető, akkor van egy I interpretáció, ami igazra értékeli. Válasszuk az első $2n$ szám közül azt az n-et, ami I igaz literáljainak felel meg. Ekkor az $(m+1)-(m+n)$. számjegyeknél 1 az összeg, míg az $1-m$. számjegyeknél 1, 2, vagy 3 aszerint, hogy klózonként hány literál igaz. A további $3m$ számmal minden 1 és m közötti számjegy 8-cá egészíthető ki.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et. Ha az i. változóhoz rendelt 2 szám közül az első S'-beli, akkor legyen x_i igaz, különben hamis.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et. Ha az i. változóhoz rendelt 2 szám közül az első S'-beli, akkor legyen x_i igaz, különben hamis. S' minden $1 \leqslant j \leqslant m$-re pontosan 1-et tartalmaz a j. klózhoz rendelt 3 számból, hiszen ha egyet se tartalmazna, akkor legfeljebb 3, ha legalább 2-t akkor legalább 11 lenne a j. számjegy.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et. Ha az i. változóhoz rendelt 2 szám közül az első S'-beli, akkor legyen x_i igaz, különben hamis. S' minden $1 \leqslant j \leqslant m$-re pontosan 1-et tartalmaz a j. klózhoz rendelt 3 számból, hiszen ha egyet se tartalmazna, akkor legfeljebb 3, ha legalább 2-t akkor legalább 11 lenne a j. számjegy. Ez azt jelenti, hogy 8-at csak úgy kaphatunk, hogy 1,2 vagy 3 darab 1-es szerepel az összegben.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et. Ha az i. változóhoz rendelt 2 szám közül az első S'-beli, akkor legyen x_i igaz, különben hamis. S' minden $1 \leqslant j \leqslant m$-re pontosan 1-et tartalmaz a j. klózhoz rendelt 3 számból, hiszen ha egyet se tartalmazna, akkor legfeljebb 3, ha legalább 2-t akkor legalább 11 lenne a j. számjegy. Ez azt jelenti, hogy 8-at csak úgy kaphatunk, hogy 1,2 vagy 3 darab 1-es szerepel az összegben. Ez viszont azt jelenti, hogy minden klózban 1,2 vagy 3 literál igaz, tehát φ kielégíthető.

Részletösszeg probléma

Fordítva, tegyük fel, hogy az S' részhalmazbeli számok összege K. Ez csak úgy lehetséges, ha az első $2n$ számból pontosan n-et választottunk, minden változóra 1-et. Ha az i. változóhoz rendelt 2 szám közül az első S'-beli, akkor legyen x_i igaz, különben hamis. S' minden $1 \leqslant j \leqslant m$-re pontosan 1-et tartalmaz a j. klózhoz rendelt 3 számból, hiszen ha egyet se tartalmazna, akkor legfeljebb 3, ha legalább 2-t akkor legalább 11 lenne a j. számjegy. Ez azt jelenti, hogy 8-at csak úgy kaphatunk, hogy 1,2 vagy 3 darab 1-es szerepel az összegben. Ez viszont azt jelenti, hogy minden klózban 1,2 vagy 3 literál igaz, tehát φ kielégíthető.

Mivel S $O(n+m)$ darab $O(n+m)$ jegyű számból áll és K is $O(n+m)$ jegyű ezért a $\varphi \mapsto (S, K)$ függvény polinom időben kiszámítható, tehát 3SAT polinom időben visszavezethető RÉSZLETÖSSZEG-re, így RÉSZLETÖSSZEG NP-teljes. $\square$

Hátizsák probléma

A HÁTIZSÁK nyelv olyan $a_1, \ldots, a_n, b, p_1, \ldots p_n, k$ rendezett $(2n+2)$-esekből áll, ahol ezen számok mindegyike nemnegatív és van egy olyan $I \subseteq \{1, \ldots n\}$ halmaz, amelyre $\sum_{i \in I} a_i \leqslant b$ és $\sum_{i \in I} p_i \geqslant k$.

Hátizsák probléma

A HÁTIZSÁK nyelv olyan $a_1, \dots, a_n, b, p_1, \dots p_n, k$ rendezett $(2n+2)$-esekből áll, ahol ezen számok mindegyike nemnegatív és van egy olyan $I \subseteq \{1, \dots n\}$ halmaz, amelyre $\sum_{i \in I} a_i \leqslant b$ és $\sum_{i \in I} p_i \geqslant k$.

Story: Adott egy kincsesbarlangban n kincs, az i. kincs térfogata a_i, eladása p_i profitot hoz. Ki tudunk-e hozni a b kapacitású hátizsákunkban legalább k profitot hozó kincset? (Feltesszük, hogy ha a kincsek össztérfogata legfeljebb b, akkor azt valahogy be tudjuk zsúfolni a hátizsákba.)

Hátizsák probléma

A Hátizsák nyelv olyan $a_1, \dots, a_n, b, p_1, \dots p_n, k$ rendezett $(2n+2)$-esekből áll, ahol ezen számok mindegyike nemnegatív és van egy olyan $I \subseteq \{1, \dots n\}$ halmaz, amelyre $\sum_{i \in I} a_i \leqslant b$ és $\sum_{i \in I} p_i \geqslant k$.

Story: Adott egy kincsesbarlangban n kincs, az i. kincs térfogata a_i, eladása p_i profitot hoz. Ki tudunk-e hozni a b kapacitású hátizsákunkban legalább k profitot hozó kincset? (Feltesszük, hogy ha a kincsek össztérfogata legfeljebb b, akkor azt valahogy be tudjuk zsúfolni a hátizsákba.)

Tétel

Hátizsák NP-teljes.

Hátizsák probléma

A Hátizsák nyelv olyan $a_1, \ldots, a_n, b, p_1, \ldots p_n, k$ rendezett $(2n+2)$-esekből áll, ahol ezen számok mindegyike nemnegatív és van egy olyan $I \subseteq \{1, \ldots n\}$ halmaz, amelyre $\sum_{i \in I} a_i \leqslant b$ és $\sum_{i \in I} p_i \geqslant k$.

Story: Adott egy kincsesbarlangban n kincs, az i. kincs térfogata a_i, eladása p_i profitot hoz. Ki tudunk-e hozni a b kapacitású hátizsákunkban legalább k profitot hozó kincset? (Feltesszük, hogy ha a kincsek össztérfogata legfeljebb b, akkor azt valahogy be tudjuk zsúfolni a hátizsákba.)

Tétel

Hátizsák NP-teljes.

Bizonyítás: Hátizsák NP-beli, mivel a tárgyak egy I részhalmazát előállítani és arra a 2 egyenlőtlenség teljesülését ellenőrizni az input méretében polinomiális.

Hátizsák probléma

RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK:
Legyen (S, K) RÉSZLETÖSSZEG egy bemenete, ahol $S = \{s_1, \ldots, s_n\}$.

Hátizsák probléma

RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK:
Legyen (S, K) RÉSZLETÖSSZEG egy bemenete, ahol
$S = \{s_1, \ldots, s_n\}$.

$a_i := s_i, p_i := s_i, b := K, k := K$ minden $1 \leqslant i \leqslant n$-re.

Hátizsák probléma

RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK:
Legyen (S, K) RÉSZLETÖSSZEG egy bemenete, ahol $S = \{s_1, \ldots, s_n\}$.

$a_i := s_i, p_i := s_i, b := K, k := K$ minden $1 \leqslant i \leqslant n$-re.

Ha valamely $I \subseteq \{1, \ldots n\}$-re $\sum_{i \in I} s_i = K$, akkor $\sum_{i \in I} a_i = K = b \leqslant b$ és $\sum_{i \in I} p_i = K = k \geqslant k$.

Hátizsák probléma

RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK:
Legyen (S, K) RÉSZLETÖSSZEG egy bemenete, ahol $S = \{s_1, \ldots, s_n\}$.

$a_i := s_i, p_i := s_i, b := K, k := K$ minden $1 \leqslant i \leqslant n$-re.

Ha valamely $I \subseteq \{1, \ldots n\}$-re $\sum_{i \in I} s_i = K$, akkor $\sum_{i \in I} a_i = K = b \leqslant b$ és $\sum_{i \in I} p_i = K = k \geqslant k$.

Ha valamely $I \subseteq \{1, \ldots n\}$-re $\sum_{i \in I} a_i \leqslant b = K$ és $\sum_{i \in I} p_i \geqslant k = K$, akkor $\sum_{i \in I} s_i = K$, mivel $a_i = p_i = s_i$ minden $1 \leqslant i \leqslant n$-re.

Hátizsák probléma

RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK:
Legyen (S, K) RÉSZLETÖSSZEG egy bemenete, ahol $S = \{s_1, \ldots, s_n\}$.

$a_i := s_i, p_i := s_i, b := K, k := K$ minden $1 \leqslant i \leqslant n$-re.

Ha valamely $I \subseteq \{1, \ldots n\}$-re $\sum_{i\in I} s_i = K$, akkor $\sum_{i\in I} a_i = K = b \leqslant b$ és $\sum_{i\in I} p_i = K = k \geqslant k$.

Ha valamely $I \subseteq \{1, \ldots n\}$-re $\sum_{i\in I} a_i \leqslant b = K$ és $\sum_{i\in I} p_i \geqslant k = K$, akkor $\sum_{i\in I} s_i = K$, mivel $a_i = p_i = s_i$ minden $1 \leqslant i \leqslant n$-re.

(S, K)-ból $a_1, \ldots, a_n, b, p_1, \ldots p_n, k$ polinom időben kiszámítható, tehát RÉSZLETÖSSZEG $\leqslant_p$ HÁTIZSÁK, így HÁTIZSÁK NP-nehéz, és NP-belisége miatt NP-teljes is. $\square$

Partíció probléma

$\textsc{Partíció}$:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Partíció probléma

PARTÍCIÓ:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Partíció probléma

Partíció:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

Partíció NP-teljes.

Partíció probléma

PARTÍCIÓ:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. $2+2+4=2+3+3$.

Tétel

PARTÍCIÓ NP-teljes.

Bizonyítás: PARTÍCIÓ NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

Partíció probléma

PARTÍCIÓ:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

PARTÍCIÓ NP-teljes.

Bizonyítás: PARTÍCIÓ NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

RÉSZLETÖSSZEG $\leqslant_p$ PARTÍCIÓ. Legyen $S = \{s_1, \ldots, s_m\}$ és b a RÉSZLETÖSSZEG egy bemenete, feltehető, hogy $b \leqslant s = \sum_{i=1}^{m} s_i$.

Partíció probléma

$\textsc{Partíció}{:=}\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

Partíció NP-teljes.

Bizonyítás: Partíció NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

Részletösszeg $\leqslant_p$ Partíció. Legyen $S = \{s_1, \ldots, s_m\}$ és b a Részletösszeg egy bemenete, feltehető, hogy $b \leqslant s = \sum_{i=1}^{m} s_i$.
$B := \{s_1, \ldots, s_m, s+1-b, b+1\}$.

Partíció probléma

$\textsc{Partíció}$:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

$\textsc{Partíció}$ NP-teljes.

Bizonyítás: $\textsc{Partíció}$ NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

$\textsc{Részletösszeg} \leqslant_p \textsc{Partíció}$. Legyen $S = \{s_1, \ldots, s_m\}$ és b a $\textsc{Részletösszeg}$ egy bemenete, feltehető, hogy $b \leqslant s = \sum_{i=1}^{m} s_i$.
$B := \{s_1, \ldots, s_m, s+1-b, b+1\}$. Ekkor
$\langle B\rangle \in \textsc{Partíció} \Longleftrightarrow \langle S, b\rangle \in \textsc{Részletösszeg}$.

Partíció probléma

PARTÍCIÓ:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

PARTÍCIÓ NP-teljes.

Bizonyítás: PARTÍCIÓ NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

RÉSZLETÖSSZEG $\leqslant_p$ PARTÍCIÓ. Legyen $S = \{s_1, \ldots, s_m\}$ és b a RÉSZLETÖSSZEG egy bemenete, feltehető, hogy $b \leqslant s = \sum_{i=1}^m s_i$.
$B := \{s_1, \ldots, s_m, s+1-b, b+1\}$. Ekkor
$\langle B\rangle \in$ PARTÍCIÓ $\Longleftrightarrow \langle S, b\rangle \in$ RÉSZLETÖSSZEG.
Ehhez elég annyit észrevenni, hogy B-ben $2s+2$ a számok összege, az utolsó kettőé pedig $s+2$, ami több, mint az összeg fele, így ez a két szám másik félben kell legyen.

Partíció probléma

$\textsc{Partíció}$:=$\{\langle B\rangle \mid B$ olyan pozitív számok multihalmaza, amely két egyenlő összegű részre particionálható$\}$.

Példa: A 2,2,2,3,3,4 multihalmaz ilyen, hiszen pl. 2+2+4=2+3+3.

Tétel

$\textsc{Partíció}$ NP-teljes.

Bizonyítás: $\textsc{Partíció}$ NP-beli, egy részhalmazt előállítani és a két részhalmaz elemeit összeadni polinom időben megy.

$\textsc{Részletösszeg} \leqslant_p \textsc{Partíció}$. Legyen $S = \{s_1, \ldots, s_m\}$ és b a $\textsc{Részletösszeg}$ egy bemenete, feltehető, hogy $b \leqslant s = \sum_{i=1}^{m} s_i$.
$B := \{s_1, \ldots, s_m, s + 1 - b, b + 1\}$. Ekkor
$\langle B\rangle \in \textsc{Partíció} \Longleftrightarrow \langle S, b\rangle \in \textsc{Részletösszeg}$.

Ehhez elég annyit észrevenni, hogy B-ben $2s + 2$ a számok összege, az utolsó kettőé pedig $s + 2$, ami több, mint az összeg fele, így ez a két szám másik félben kell legyen.

A visszavezetés nyilván polinomiális. $\square$

Ládapakolás

Számítási feladat: Hány egységnyi súlykapacitású ládába lehet bepakolni az $s_1, \ldots, s_n \, (\leqslant 1)$ súlyú tárgyakat?

Ládapakolás

Számítási feladat: Hány egységnyi súlykapacitású ládába lehet bepakolni az $s_1, \ldots, s_n \, (\leqslant 1)$ súlyú tárgyakat?

Eldöntési probléma: Bele lehet-e pakolni az $s_1, \ldots, s_n$ súlyú tárgyakat k darab egységnyi súlykapacitású ládába?

Ládapakolás

Számítási feladat: Hány egységnyi súlykapacitású ládába lehet bepakolni az $s_1, \dots, s_n\,(\leqslant 1)$ súlyú tárgyakat?

Eldöntési probléma: Bele lehet-e pakolni az $s_1, \dots, s_n$ súlyú tárgyakat k darab egységnyi súlykapacitású ládába?

$\textsc{Ládapakolás}{:=}\{\langle s_1, \dots, s_n, k\rangle \mid s_i \in \mathbb{Q}^+ (1 \leqslant i \leqslant n)$ súlyok particionálhatók $k \in \mathbb{N}^+$ részre úgy, hogy minden particióban a súlyok összege $\leqslant 1\}$.

Ládapakolás

Számítási feladat: Hány egységnyi súlykapacitású ládába lehet bepakolni az $s_1, \ldots, s_n$ $(\leqslant 1)$ súlyú tárgyakat?

Eldöntési probléma: Bele lehet-e pakolni az $s_1, \ldots, s_n$ súlyú tárgyakat k darab egységnyi súlykapacitású ládába?

$\textsc{Ládapakolás}$:=$\{\langle s_1, \ldots, s_n, k\rangle \mid s_i \in \mathbb{Q}^+ (1 \leqslant i \leqslant n)$ súlyok particionálhatók $k \in \mathbb{N}^+$ részre úgy, hogy minden particióban a súlyok összege $\leqslant 1\}$.

Példa: 0,34; 0,44; 0,54; 0,64 súlyú tárgyak esetén nem járunk jól, ha a 2 legksebb súlyút egy ládába rakjuk, ekkor ugyanis 3 láda kell. Könnyű találni csak 2 ládát használó ládapakolást.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

PARTÍCIÓ $\leqslant_p$ LÁDAPAKOLÁS:

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

PARTÍCIÓ $\leqslant_p$ LÁDAPAKOLÁS:

Legyenek $b_1, \ldots, b_n$ a B multihalmaz elemei és $b = \sum_{i=1}^{n} b_i$.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

PARTÍCIÓ $\leqslant_p$ LÁDAPAKOLÁS:

Legyenek $b_1, \ldots, b_n$ a B multihalmaz elemei és $b = \sum_{i=1}^{n} b_i$.
Legyenek az L multihalmaz elemei $2b_1/b, \ldots, 2b_n/b$.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

PARTÍCIÓ $\leqslant_p$ LÁDAPAKOLÁS:

Legyenek $b_1, \ldots, b_n$ a B multihalmaz elemei és $b = \sum_{i=1}^{n} b_i$.
Legyenek az L multihalmaz elemei $2b_1/b, \ldots, 2b_n/b$. Ekkor könnyen láthatóan $\langle B \rangle \in$ PARTÍCIÓ $\iff \langle L, 2 \rangle \in$ LÁDAPAKOLÁS.

Ládapakolás

Tétel

LÁDAPAKOLÁS NP-teljes.

Bizonyítás: NP-beli, hiszen egy partíció előállítása, majd a partíciókra a súlyhatár betartásának ellenőrzése polinomiális időben megy.

PARTÍCIÓ $\leqslant_p$ LÁDAPAKOLÁS:

Legyenek $b_1, \ldots, b_n$ a B multihalmaz elemei és $b = \sum_{i=1}^{n} b_i$.
Legyenek az L multihalmaz elemei $2b_1/b, \ldots, 2b_n/b$. Ekkor könnyen láthatóan $\langle B \rangle \in$ PARTÍCIÓ $\iff \langle L, 2 \rangle \in$ LÁDAPAKOLÁS.

A visszavezetés nyilván polinomiális. $\square$

NP lehetséges szerkezete

Definíció

L **NP-köztes**, ha $L \in \mathrm{NP}$, $L \notin \mathrm{P}$ és L nem NP-teljes.

NP lehetséges szerkezete

Definíció

L **NP-köztes**, ha $L \in \mathrm{NP}$, $L \notin \mathrm{P}$ és L nem NP-teljes.

Ladner tétele

Ha $\mathrm{P} \neq \mathrm{NP}$, akkor létezik NP-köztes nyelv.

NP lehetséges szerkezete

Definíció

L **NP-köztes**, ha $L \in \mathrm{NP}$, $L \notin \mathrm{P}$ és L nem NP-teljes.

Ladner tétele

Ha $\mathrm{P} \neq \mathrm{NP}$, akkor létezik NP-köztes nyelv.

(biz. nélkül)

Mivel nem tudjuk, hogy $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$, ezért nem tudjuk, hogy léteznek-e NP-köztes nyelvek. Valószínűleg igen, hiszen azt gondoljuk, hogy $\mathrm{P} \neq \mathrm{NP}$.

NP lehetséges szerkezete

Definíció

L **NP-köztes**, ha $L \in \mathrm{NP}$, $L \notin \mathrm{P}$ és L nem NP-teljes.

Ladner tétele

Ha $\mathrm{P} \neq \mathrm{NP}$, akkor létezik NP-köztes nyelv.

(biz. nélkül)

Mivel nem tudjuk, hogy $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$, ezért nem tudjuk, hogy léteznek-e NP-köztes nyelvek. Valószínűleg igen, hiszen azt gondoljuk, hogy $\mathrm{P} \neq \mathrm{NP}$.

Vannak azonban olyan nyelvek, amelyeknek se a P-beliségét, se az NP-teljességét nem sikerült eddig igazolni az intenzív próbálkozások ellenére sem, így erős NP-köztes jelölteknek számítanak.

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

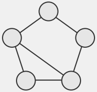
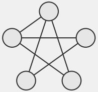
$\textsc{Gráfizomorfizmus} = \{\langle G_1, G_2\rangle \mid G_1 \text{ és } G_2 \text{ irányítatlan izomorf gráfok}\}.$

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

$$\textsc{Gráfizomorfizmus} = \{\langle G_1, G_2\rangle \mid G_1 \text{ és } G_2 \text{ irányítatlan izomorf gráfok}\}.$$

Példa:  és  izomorfak.

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

$\textsc{Gráfizomorfizmus} = \{\langle G_1, G_2\rangle \mid$ G_1 és G_2 irányítatlan izomorf gráfok$\}$.

Példa:

és izomorfak.

Megjegyzés: A gráfizomorfizmus probléma számos, gyakorlatban előforduló speciális esete P-beli. Például:

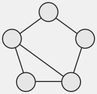
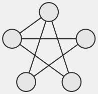
- fák

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

$\textsc{Gráfizomorfizmus} = \{\langle G_1, G_2 \rangle \mid G_1$ és G_2 irányítatlan izomorf gráfok$\}$.

Példa:  és  izomorfak.

Megjegyzés: A gráfizomorfizmus probléma számos, gyakorlatban előforduló speciális esete P-beli. Például:

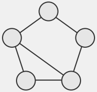
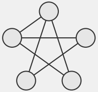
- fák
- síkba rajzolható gráfok

NP-köztes jelöltek – Gráfizomorfizmus

Definíció

A $G_i = (V_i, E_i)$ $(i = 1, 2)$ irányítatlan gráfok **izomorfak**, ha van olyan $f : V_1 \to V_2$ bijekció, hogy $\forall u, v \in V_1$ esetén $\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$.

$\textsc{Gráfizomorfizmus} = \{\langle G_1, G_2\rangle \mid G_1$ és G_2 irányítatlan izomorf gráfok$\}$.

Példa:  és  izomorfak.

Megjegyzés: A gráfizomorfizmus probléma számos, gyakorlatban előforduló speciális esete P-beli. Például:

- fák
- síkba rajzolható gráfok
- korlátos fokszámú gráfok

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

Egy új eredmény: Babai László, magyar matematikus 2017-es eredménye:

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

Egy új eredmény: Babai László, magyar matematikus 2017-es eredménye:

Tétel: $\textsc{Gráfizomorfizmus} \in$ QP,

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

Egy új eredmény: Babai László, magyar matematikus 2017-es eredménye:

Tétel: $\textsc{Gráfizomorfizmus} \in$ QP, ahol

$$\mathrm{QP} = \bigcup_{c \in \mathbb{N}} \mathrm{TIME}(2^{(\log n)^c})$$

a „kvázipolinom időben” megoldható problémák osztálya.

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

Egy új eredmény: Babai László, magyar matematikus 2017-es eredménye:

Tétel: $\textsc{Gráfizomorfizmus} \in \mathrm{QP}$, ahol

$$\mathrm{QP} = \bigcup_{c \in \mathbb{N}} \mathrm{TIME}(2^{(\log n)^c})$$

a „kvázipolinom időben” megoldható problémák osztálya.

A gráfizomorfizmus probléma alábbi általánosítása viszont már NP-teljes.

NP-köztes jelöltek – Gráfizomorfizmus

Nehéz eset például, ha nagyméretű gráfokban minden fokszám $\sqrt{|V|}$ körüli.

Egy új eredmény: Babai László, magyar matematikus 2017-es eredménye:

Tétel: $\textsc{Gráfizomorfizmus} \in \mathrm{QP}$, ahol

$$\mathrm{QP} = \bigcup_{c \in \mathbb{N}} \mathrm{TIME}(2^{(\log n)^c})$$

a „kvázipolinom időben” megoldható problémák osztálya.

A gráfizomorfizmus probléma alábbi általánosítása viszont már NP-teljes.

$\textsc{Részgráfizomorfizmus} = \{\langle G_1, G_2 \rangle \mid$ G_1 és G_2 irányítatlan gráfok és G_1 izomorf G_2 egy részgráfjával$\}$.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő,

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

RÉSZGRÁFIZOMORFIZMUS NP-teljes.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

Részgráfizomorfizmus NP-teljes.

Bizonyítás: Részgráfizomorfizmus NP-beli, hiszen egy NTG polinom időben előllíthat egy f bijekciót $V(G_1)$ és $V(G_2)$ egy $|V(G_1)|$ méretű részhalmaza között, majd polinom időben ellenőrizhető, hogy f izomorfizmus-e.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

Részgráfizomorfizmus NP-teljes.

Bizonyítás: Részgráfizomorfizmus NP-beli, hiszen egy NTG polinom időben elő́llíthat egy f bijekciót $V(G_1)$ és $V(G_2)$ egy $|V(G_1)|$ méretű részhalmaza között, majd polinom időben ellenőrizhető, hogy f izomorfizmus-e.

IHK$\leqslant_p$Részgráfizomorfizmus.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

Részgráfizomorfizmus NP-teljes.

Bizonyítás: Részgráfizomorfizmus NP-beli, hiszen egy NTG polinom időben előllíthat egy f bijekciót $V(G_1)$ és $V(G_2)$ egy $|V(G_1)|$ méretű részhalmaza között, majd polinom időben ellenőrizhető, hogy f izomorfizmus-e.

IHK$\leqslant_p$Részgráfizomorfizmus. Legyen G egy irányítatlan gráf. G_1 legyen egy $|V(G)|$ csúcsú kör, $G_2 := G$.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

RÉSZGRÁFIZOMORFIZMUS NP-teljes.

Bizonyítás: RÉSZGRÁFIZOMORFIZMUS NP-beli, hiszen egy NTG polinom időben előllíthat egy f bijekciót $V(G_1)$ és $V(G_2)$ egy $|V(G_1)|$ méretű részhalmaza között, majd polinom időben ellenőrizhető, hogy f izomorfizmus-e.

IHK$\leqslant_p$RÉSZGRÁFIZOMORFIZMUS. Legyen G egy irányítatlan gráf. G_1 legyen egy $|V(G)|$ csúcsú kör, $G_2 := G$. Ekkor G-ben van Hamilton kör, akkor és csak akkor, ha G_2-nek van G_1-gyel izomorf részgráfja.

Részgráfizomorfizmus NP-teljes

Megjegyzés: A részgráf nem feszítetten értendő, tehát például $G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$ 2 élből álló út részgráfja $G_2 = (\{A, B, C, D\}, \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\})$ teljes 4 csúcsú gráfnak, hiszen G_1 izomorf $G_3 = (\{A, B, C\}, \{\{A, B\}, \{B, C\}\})$-mal, ami részgráfja G_2-nek annak ellenére, hogy $\{A, C\} \in E(G_2)$.

Tétel

Részgráfizomorfizmus NP-teljes.

Bizonyítás: Részgráfizomorfizmus NP-beli, hiszen egy NTG polinom időben előllíthat egy f bijekciót $V(G_1)$ és $V(G_2)$ egy $|V(G_1)|$ méretű részhalmaza között, majd polinom időben ellenőrizhető, hogy f izomorfizmus-e.

IHK$\leqslant_p$Részgráfizomorfizmus. Legyen G egy irányítatlan gráf. G_1 legyen egy $|V(G)|$ csúcsú kör, $G_2 := G$. Ekkor G-ben van Hamilton kör, akkor és csak akkor, ha G_2-nek van G_1-gyel izomorf részgráfja. A visszavezetés nyilván polinomiális. $\square$

NP-köztes jelöltek – Prímfaktorizáció

Számítási feladat:

Prímfaktorizáció: adjuk meg egy egész szám prímtényezős felbontását!

NP-köztes jelöltek – Prímfaktorizáció

Számítási feladat:

Prímfaktorizáció: adjuk meg egy egész szám prímtényezős felbontását!

A probléma eldöntési változata:

$$\textsc{Prímfaktorizáció} = \{\langle n, k\rangle \mid n\text{-nek van } k\text{-nál kisebb prímtényezője}\}$$

NP-köztes jelöltek – Prímfaktorizáció

Számítási feladat:

Prímfaktorizáció: adjuk meg egy egész szám prímtényezős felbontását!

A probléma eldöntési változata:

$$\textsc{Prímfaktorizáció} = \{\langle n, k \rangle \mid n\text{-nek van } k\text{-nál kisebb prímtényezője}\}$$

Alkalmazás:

NP-köztes jelöltek – Prímfaktorizáció

Számítási feladat:

Prímfaktorizáció: adjuk meg egy egész szám prímtényezős felbontását!

A probléma eldöntési változata:

$$\textsc{Prímfaktorizáció} = \{\langle n, k\rangle \mid n\text{-nek van } k\text{-nál kisebb prímtényezője}\}$$

Alkalmazás:

RSA eljárás: 1976-ban Ron Rivest, Adi Shamir és Len Adleman kifejlesztett egy nyílt kulcsú titkosító algoritmust, amely két nagy prím összeszorzásával azt használja ki, hogy nem ismeretes polinomiális algoritmus egy összetett szám prímtényezőinek meghatározására.

NP-köztes jelöltek – Prímfaktorizáció

Számítási feladat:

Prímfaktorizáció: adjuk meg egy egész szám prímtényezős felbontását!

A probléma eldöntési változata:

$$\textsc{Prímfaktorizáció} = \{\langle n, k\rangle \mid n\text{-nek van } k\text{-nál kisebb prímtényezője}\}$$

Alkalmazás:

RSA eljárás: 1976-ban Ron Rivest, Adi Shamir és Len Adleman kifejlesztett egy nyílt kulcsú titkosító algoritmust, amely két nagy prím összeszorzásával azt használja ki, hogy nem ismeretes polinomiális algoritmus egy összetett szám prímtényezőinek meghatározására.

Bár bizonyítani nem tudjuk, hogy $\textsc{Prímfaktorizáció}$ nem P-beli, mégis az RSA algoritmus adatok biztonságos továbbítására a mai napig az egyik leggyakrabban használt algoritmus.

co$\mathcal{C}$ bonyolutsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \bar{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \bar{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor co$\mathcal{C}$ is.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \bar{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor co$\mathcal{C}$ is.

Bizonyítás: Legyen $L_2 \in \mathrm{co}\mathcal{C}$ és L_1 tetszőleges nyelvek, melyekre $L_1 \leqslant_p L_2$.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor co$\mathcal{C}$ is.

Bizonyítás: Legyen $L_2 \in$ co$\mathcal{C}$ és L_1 tetszőleges nyelvek, melyekre $L_1 \leqslant_p L_2$. Utóbbiból következik, hogy $\overline{L}_1 \leqslant_p \overline{L}_2$ (ugyananaz a visszavezetés jó!).

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor co$\mathcal{C}$ is.

Bizonyítás: Legyen $L_2 \in$ co$\mathcal{C}$ és L_1 tetszőleges nyelvek, melyekre $L_1 \leqslant_p L_2$. Utóbbiból következik, hogy $\overline{L}_1 \leqslant_p \overline{L}_2$ (ugyananaz a visszavezetés jó!). Mivel $\overline{L}_2 \in \mathcal{C}$, ezért a tétel feltétele miatt $\overline{L}_1 \in \mathcal{C}$.

co$\mathcal{C}$ bonyolultsági osztályok

Definíció

Ha $\mathcal{C}$ egy bonyolultsági osztály co$\mathcal{C} := \{L \mid \overline{L} \in \mathcal{C}\}$.

Definíció

$\mathcal{C}$ **zárt a polinomidejű visszavezetésre nézve**, ha minden esetben ha $L_2 \in \mathcal{C}$ és $L_1 \leqslant_p L_2$ teljesül következik, hogy $L_1 \in \mathcal{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

Tétel

Ha $\mathcal{C}$ zárt a polinomidejű visszavezetésre nézve, akkor co$\mathcal{C}$ is.

Bizonyítás: Legyen $L_2 \in \mathrm{co}\mathcal{C}$ és L_1 tetszőleges nyelvek, melyekre $L_1 \leqslant_p L_2$. Utóbbiból következik, hogy $\overline{L}_1 \leqslant_p \overline{L}_2$ (ugyananaz a visszavezetés jó!). Mivel $\overline{L}_2 \in \mathcal{C}$, ezért a tétel feltétele miatt $\overline{L}_1 \in \mathcal{C}$. Azaz $L_1 \in \mathrm{co}\mathcal{C}$. □

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP?

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP?

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathcal{C}$-teljes.

co$\mathcal{C}$ bonyolultsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathcal{C}$-teljes.

Bizonyítás:

- Ha $L \in \mathcal{C}$, akkor $\overline{L} \in$ co$\mathcal{C}$.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathcal{C}$-teljes.

Bizonyítás:

- Ha $L \in \mathcal{C}$, akkor $\overline{L} \in$ co$\mathcal{C}$.
- Legyen $L' \in \mathcal{C}$, melyre $L' \leqslant_p L$. Ekkor $\overline{L'} \leqslant_p \overline{L}$.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathcal{C}$-teljes.

Bizonyítás:

- Ha $L \in \mathcal{C}$, akkor $\overline{L} \in$ co$\mathcal{C}$.
- Legyen $L' \in \mathcal{C}$, melyre $L' \leqslant_p L$. Ekkor $\overline{L'} \leqslant_p \overline{L}$.
  Ha L' befutja $\mathcal{C}$-t akkor $\overline{L'}$ befutja co$\mathcal{C}$-t.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathcal{C}$-teljes.

Bizonyítás:

- Ha $L \in \mathcal{C}$, akkor $\overline{L} \in$ co$\mathcal{C}$.
- Legyen $L' \in \mathcal{C}$, melyre $L' \leqslant_p L$. Ekkor $\overline{L'} \leqslant_p \overline{L}$.
  Ha L' befutja $\mathcal{C}$-t akkor $\overline{L'}$ befutja co$\mathcal{C}$-t. Azaz minden co$\mathcal{C}$-beli nyelv polinom időben visszavezethető $\overline{L}$-re.

co$\mathcal{C}$ bonyolutsági osztályok

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Igaz-e, hogy P = coP? Igen. (L-et polinom időben eldöntő TG q_i és q_n állapotát megcseréljük: $\overline{L}$-t polinom időben eldöntő TG.)
Igaz-e, hogy NP = coNP? A fenti konstrukció NTG-re nem feltétlen $\overline{L}$-t dönti el. Valójában azt sejtjük, hogy NP$\neq$coNP.

Tétel

L $\mathcal{C}$-teljes $\iff$ $\overline{L}$ co$\mathcal{C}$-teljes.

Bizonyítás:

- Ha $L \in \mathcal{C}$, akkor $\overline{L} \in$ co$\mathcal{C}$.
- Legyen $L' \in \mathcal{C}$, melyre $L' \leqslant_p L$. Ekkor $\overline{L'} \leqslant_p \overline{L}$.
  Ha L' befutja $\mathcal{C}$-t akkor $\overline{L'}$ befutja co$\mathcal{C}$-t. Azaz minden co$\mathcal{C}$-beli nyelv polinom időben visszavezethető $\overline{L}$-re.

Tehát $\overline{L}$ co$\mathcal{C}$-beli és co$\mathcal{C}$-nehéz, így co$\mathcal{C}$-teljes. $\square$

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \mid$ a φ nulladrendű formula tautológia$\}$.

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \,|\, \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \,|\,$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \mid$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Bizonyítás: $\textsc{Áltsat} = \{\langle\varphi\rangle \mid \varphi$ kielégíthető nulladrendű formula$\}$ is NP-teljes (NP-beli és $\textsc{Sat}$ speciális esete neki.)

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \,|\, \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \,|\,$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Bizonyítás: $\textsc{Áltsat} = \{\langle\varphi\rangle \,|\, \varphi$ kielégíthető nulladrendű formula$\}$ is NP-teljes (NP-beli és $\textsc{Sat}$ speciális esete neki.)

$\overline{\textsc{Áltsat}} := \textsc{Unsat}$, az előző tétel alapján $\textsc{Unsat}$ coNP-teljes.

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \,|\, \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \,|\,$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Bizonyítás: $\textsc{Áltsat} = \{\langle\varphi\rangle \,|\, \varphi$ kielégíthető nulladrendű formula$\}$ is NP-teljes (NP-beli és $\textsc{Sat}$ speciális esete neki.)

$\overline{\textsc{Áltsat}} := \textsc{Unsat}$, az előző tétel alapján $\textsc{Unsat}$ coNP-teljes.
$\textsc{Unsat} \leqslant_p \textsc{Taut}$, hiszen $\varphi \mapsto \neg\varphi$ polinom idejű visszavezetés. $\square$

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \mid$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Bizonyítás: $\textsc{Áltsat} = \{\langle\varphi\rangle \mid \varphi$ kielégíthető nulladrendű formula$\}$ is NP-teljes (NP-beli és $\textsc{Sat}$ speciális esete neki.)

$\overline{\textsc{Áltsat}} := \textsc{Unsat}$, az előző tétel alapján $\textsc{Unsat}$ coNP-teljes.

$\textsc{Unsat} \leqslant_p \textsc{Taut}$, hiszen $\varphi \mapsto \neg\varphi$ polinom idejű visszavezetés. $\square$

Informálisan: coNP olyan nyelveket tartalmaz, amelyekbe való tartozás **polinom időben cáfolható**.

Példák coNP teljes nyelvekre

$\textsc{Unsat} := \{\langle\varphi\rangle \,|\, \varphi$ kielégíthetetlen nulladrendű formula$\}$.

$\textsc{Taut} := \{\langle\varphi\rangle \,|\,$ a φ nulladrendű formula tautológia$\}$.

Tétel

$\textsc{Unsat}$ és $\textsc{Taut}$ coNP-teljesek.

Bizonyítás: $\textsc{Áltsat} = \{\langle\varphi\rangle \,|\, \varphi$ kielégíthető nulladrendű formula$\}$ is NP-teljes (NP-beli és $\textsc{Sat}$ speciális esete neki.)

$\overline{\textsc{Áltsat}} := \textsc{Unsat}$, az előző tétel alapján $\textsc{Unsat}$ coNP-teljes.
$\textsc{Unsat} \leqslant_p \textsc{Taut}$, hiszen $\varphi \mapsto \neg\varphi$ polinom idejű visszavezetés. $\square$

Informálisan: coNP olyan nyelveket tartalmaz, amelyekbe való tartozás **polinom időben cáfolható**.

Például egy φ-t kielégítő interpretáció cáfolja, hogy φ kielégíthetetlen lenne. Egy φ-t hamisra értékelő interpretáció cáfolja, hogy φ tautológia lenne. Egy interpretáció polinom időben előállítható és adott interpretációban a formula igazságértéke polinom időben kiszámítható.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$,

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

Legyen most $L \in \mathrm{NP}$ tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in \mathrm{coNP}$.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor NP = coNP.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

Legyen most $L \in \mathrm{NP}$ tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in \mathrm{coNP}$. $\mathrm{coNP} \subseteq \mathrm{NP}$ miatt $\overline{L} \in \mathrm{NP}$,

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

Legyen most $L \in \mathrm{NP}$ tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in \mathrm{coNP}$. $\mathrm{coNP} \subseteq \mathrm{NP}$ miatt $\overline{L} \in \mathrm{NP}$, majd ismét coNP definíciója miatt $L \in \mathrm{coNP}$.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor NP = coNP.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

Legyen most $L \in \mathrm{NP}$ tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in \mathrm{coNP}$. $\mathrm{coNP} \subseteq \mathrm{NP}$ miatt $\overline{L} \in \mathrm{NP}$, majd ismét coNP definíciója miatt $L \in \mathrm{coNP}$. Tehát $\mathrm{NP} \subseteq \mathrm{coNP}$ is teljesül. $\square$

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in$ NP, akkor NP $=$ coNP.

Bizonyítás: Legyen $L' \in$ coNP tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in$ NP. Tehát coNP $\subseteq$ NP.

Legyen most $L \in$ NP tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in$ coNP. coNP $\subseteq$ NP miatt $\overline{L} \in$ NP, majd ismét coNP definíciója miatt $L \in$ coNP. Tehát NP $\subseteq$ coNP is teljesül. $\square$

Sejtés: NP $\neq$ coNP.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in \mathrm{NP}$, akkor $\mathrm{NP} = \mathrm{coNP}$.

Bizonyítás: Legyen $L' \in \mathrm{coNP}$ tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in \mathrm{NP}$. Tehát $\mathrm{coNP} \subseteq \mathrm{NP}$.

Legyen most $L \in \mathrm{NP}$ tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in \mathrm{coNP}$. $\mathrm{coNP} \subseteq \mathrm{NP}$ miatt $\overline{L} \in \mathrm{NP}$, majd ismét coNP definíciója miatt $L \in \mathrm{coNP}$. Tehát $\mathrm{NP} \subseteq \mathrm{coNP}$ is teljesül. $\square$

Sejtés: $\mathrm{NP} \neq \mathrm{coNP}$.

Amennyiben a sejtés igaz, akkor UNSAT és TAUT még csak nem is NP-beliek.

coNP-teljes nyelvek egy tulajdonsága

Tétel

Ha L coNP-teljes és $L \in$ NP, akkor NP $=$ coNP.

Bizonyítás: Legyen $L' \in$ coNP tetszőleges. Mivel L coNP-teljes, ezért $L' \leqslant_p L$, de mivel L NP-beli, ezért korábbi tételünk szerint $L' \in$ NP. Tehát coNP $\subseteq$ NP.

Legyen most $L \in$ NP tetszőleges, ekkor coNP definíciója miatt $\overline{L} \in$ coNP. coNP $\subseteq$ NP miatt $\overline{L} \in$ NP, majd ismét coNP definíciója miatt $L \in$ coNP. Tehát NP $\subseteq$ coNP is teljesül. $\square$

Sejtés: NP $\neq$ coNP.

Amennyiben a sejtés igaz, akkor Unsat és Taut még csak nem is NP-beliek. Mindenesetre nem ismeretes ezen nyelvekhez való tartozásra polinom időben kiszámítható és ellenőrizhető bizonyíték (tanú).

NP $\cap$ coNP

Ha NP $\neq$ coNP egy érdekes osztály lehet NP $\cap$ coNP.

$\mathsf{NP} \cap \mathsf{coNP}$

Ha $\mathsf{NP} \neq \mathsf{coNP}$ egy érdekes osztály lehet $\mathsf{NP} \cap \mathsf{coNP}$. Nyilván $\mathsf{P} \subseteq \mathsf{NP} \cap \mathsf{coNP}$.

$\mathsf{NP} \cap \mathsf{coNP}$

Ha $\mathsf{NP} \neq \mathsf{coNP}$ egy érdekes osztály lehet $\mathsf{NP} \cap \mathsf{coNP}$. Nyilván $\mathsf{P} \subseteq \mathsf{NP} \cap \mathsf{coNP}$. Először nézzünk néhány példát $\mathsf{NP} \cap \mathsf{coNP}$-beli nyelvre.

$\mathrm{NP} \cap \mathrm{coNP}$

Ha $\mathrm{NP} \neq \mathrm{coNP}$ egy érdekes osztály lehet $\mathrm{NP} \cap \mathrm{coNP}$. Nyilván $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP}$. Először nézzünk néhány példát $\mathrm{NP} \cap \mathrm{coNP}$-beli nyelvre.

1. példa

NP $\cap$ coNP

Ha NP $\neq$ coNP egy érdekes osztály lehet NP $\cap$ coNP. Nyilván P $\subseteq$ NP $\cap$ coNP. Először nézzünk néhány példát NP $\cap$ coNP-beli nyelvre.

1. példa

$\textsc{Összefüggő} := \{\langle G\rangle \mid G = (V, E)$ összefüggő, irányítatlan gráf$\}$

NP $\cap$ coNP

Ha NP $\neq$ coNP egy érdekes osztály lehet NP $\cap$ coNP. Nyilván P $\subseteq$ NP $\cap$ coNP. Először nézzünk néhány példát NP $\cap$ coNP-beli nyelvre.

1. példa

ÖSSZEFÜGGŐ$:= \{\langle G \rangle \mid G = (V, E)$ összefüggő, irányítatlan gráf$\}$

ÖSSZEFÜGGŐ NP-beli, hiszen egy n csúcsú gráf összefüggőségére bizonyíték $\binom{n}{2}$ út a pontpárok között. Egy út hossza legfeljebb n. Így egy NTG előállíthat $\binom{n}{2}$ darab legfeljebb n csúcsból álló sorozatot polinom idő alatt, majd polinom időben ellenőrizheti, hogy ezek tényleg utak-e a pontpárok között.

$\mathrm{NP} \cap \mathrm{coNP}$

Ha $\mathrm{NP} \neq \mathrm{coNP}$ egy érdekes osztály lehet $\mathrm{NP} \cap \mathrm{coNP}$. Nyilván $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP}$. Először nézzünk néhány példát $\mathrm{NP} \cap \mathrm{coNP}$-beli nyelvre.

1. példda

ÖSSZEFÜGGŐ$:= \{\langle G \rangle \mid G = (V, E)$ összefüggő, irányítatlan gráf$\}$

ÖSSZEFÜGGŐ NP-beli, hiszen egy n csúcsú gráf összefüggőségére bizonyíték $\binom{n}{2}$ út a pontpárok között. Egy út hossza legfeljebb n. Így egy NTG előállíthat $\binom{n}{2}$ darab legfeljebb n csúcsból álló sorozatot polinom idő alatt, majd polinom időben ellenőrizheti, hogy ezek tényleg utak-e a pontpárok között.

ÖSSZEFÜGGŐ coNP-beli is, hiszen a csúcsok egy olyan X részhalmaza cáfolat, hogy X és $V \backslash X$ között nem megy él. V egy X részhalmazának előállítása és annak ellenőrése hogy X és $V \backslash X$ között nem megy él polinom időben megvalósítható.

NP $\cap$ coNP

Ha NP $\neq$ coNP egy érdekes osztály lehet NP $\cap$ coNP. Nyilván P $\subseteq$ NP $\cap$ coNP. Először nézzünk néhány példát NP $\cap$ coNP-beli nyelvre.

1. példa

ÖSSZEFÜGGŐ$:= \{\langle G\rangle \mid G = (V, E)$ összefüggő, irányítatlan gráf$\}$

ÖSSZEFÜGGŐ NP-beli, hiszen egy n csúcsú gráf összefüggőségére bizonyíték $\binom{n}{2}$ út a pontpárok között. Egy út hossza legfeljebb n. Így egy NTG előállíthat $\binom{n}{2}$ darab legfeljebb n csúcsból álló sorozatot polinom idő alatt, majd polinom időben ellenőrizheti, hogy ezek tényleg utak-e a pontpárok között.

ÖSSZEFÜGGŐ coNP-beli is, hiszen a csúcsok egy olyan X részhalmaza cáfolat, hogy X és $V \setminus X$ között nem megy él. V egy X részhalmazának előállítása és annak ellenőrése hogy X és $V \setminus X$ között nem megy él polinom időben megvalósítható.

ÖSSZEFÜGGŐ P-ben van, például szélességi kereséssel polinom időben ellenőrizhető egy gráf összefüggősége.

NP $\cap$ coNP

2. példa

NP $\cap$ coNP

2. példa

Definíció

Legyen $G = (A, B, E)$ (irányítatlan) páros gráf. Egy $M \subseteq E$ élhalmaz **teljes párosítás**, ha az $(A \cup B, M)$ gráfban minden csúcs foka pontosan 1.

$\mathrm{NP} \cap \mathrm{coNP}$

2. példa

Definíció

Legyen $G = (A, B, E)$ (irányítatlan) páros gráf. Egy $M \subseteq E$ élhalmaz **teljes párosítás**, ha az $(A \cup B, M)$ gráfban minden csúcs foka pontosan 1.

$\textsc{Teljes Párosítás} := \{\langle G \rangle \mid G =$ (A, B, E) páros gráfban van teljes párosítás$\}$

$\mathrm{NP} \cap \mathrm{coNP}$

2. példa

Definíció

Legyen $G = (A, B, E)$ (irányítatlan) páros gráf. Egy $M \subseteq E$ élhalmaz **teljes párosítás**, ha az $(A \cup B, M)$ gráfban minden csúcs foka pontosan 1.

Teljes Párosítás:$= \{\langle G \rangle \mid G = (A, B, E)$ páros gráfban van teljes párosítás$\}$

Teljes Párosítás NP-beli, hiszen $(a, b) \in A \times B$ párok egy $|A|$ méretű listája polinom időben előállítható, és polinom időben ellenőrizhető, hogy ez teljes párosítást ad.

NP $\cap$ coNP

TELJES PÁROSÍTÁS coNP-belisége Frobenius tételéből adódik.

NP $\cap$ coNP

Teljes Párosítás coNP-belisége Frobenius tételéből adódik.

Tétel: A $G = (A, B, E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha $|A| = |B|$ és minden $X \subseteq A$ halmazra legalább $|X|$ olyan B-beli csúcs van, amelyik valamelyek X-beli csúccsal szomszédos.

$\mathrm{NP} \cap \mathrm{coNP}$

TELJES PÁROSÍTÁS coNP-belisége Frobenius tételéből adódik.

Tétel: A $G = (A, B, E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha $|A| = |B|$ és minden $X \subseteq A$ halmazra legalább $|X|$ olyan B-beli csúcs van, amelyik valamelyek X-beli csúccsal szomszédos.

A egy X részhalmaza polinom időben előállítható és szintén polinom időben ellenőrizhető, hogy nem teljesül-e a rá a tétel feltétele.

$\mathrm{NP} \cap \mathrm{coNP}$

Teljes Párosítás coNP-belisége Frobenius tételéből adódik.

Tétel: A $G = (A, B, E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha $|A| = |B|$ és minden $X \subseteq A$ halmazra legalább $|X|$ olyan B-beli csúcs van, amelyik valamelyek X-beli csúccsal szomszédos.

A egy X részhalmaza polinom időben előállítható és szintén polinom időben ellenőrizhető, hogy nem teljesül-e a rá a tétel feltétele.

Teljes Párosítás P-ben van, amit a **magyar módszer** nevű Kőnig Dénes és Egerváry Jenő munkássága nyomán Harold Kuhn által adott polinomiális algoritmus mutat, mely egy páros gráfban keres maximális méretű (részleges) párosítást.

NP $\cap$ coNP

Teljes Párosítás coNP-belisége Frobenius tételéből adódik.

Tétel: A $G = (A, B, E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha $|A| = |B|$ és minden $X \subseteq A$ halmazra legalább $|X|$ olyan B-beli csúcs van, amelyik valamelyek X-beli csúccsal szomszédos.

A egy X részhalmaza polinom időben előállítható és szintén polinom időben ellenőrizhető, hogy nem teljesül-e a rá a tétel feltétele.

Teljes Párosítás P-ben van, amit a **magyar módszer** nevű Kőnig Dénes és Egerváry Jenő munkássága nyomán Harold Kuhn által adott polinomiális algoritmus mutat, mely egy páros gráfban keres maximális méretű (részleges) párosítást.

Ötlete: vegyünk független éleket, amíg tudunk, majd keressünk javító alternáló utat, azaz olyan utat ami egy A-beli és egy B-beli párosításon kívüli csúcs között fut és az élei váltakozva párosításon kívüliek illetve belüliek.

$\mathbf{NP} \cap \mathbf{coNP}$

3. példa Prímtesztelés

NP $\cap$ coNP

3. példa Prímtesztelés

$\textsc{Prímek} := \{p \mid p \text{ prím}\}.$

$\mathbf{NP} \cap \mathbf{coNP}$

3. példa Prímtesztelés

$\textsc{Prímek} := \{p \mid p \text{ prím}\}$.

Fontos észrevétel, hogy egy $p \in \textsc{Prímek}$ hossza p számjegyeinek száma, azaz $\Theta(\log p)$.

$\mathrm{NP} \cap \mathrm{coNP}$

3. példa Prímtesztelés

$\textsc{Prímek} := \{p \mid p \text{ prím}\}$.

Fontos észrevétel, hogy egy $p \in \textsc{Prímek}$ hossza p számjegyeinek száma, azaz $\Theta(\log p)$.

$\textsc{Prímek}$ coNP-belisége könnyen látható, hiszen egy n szám legfeljebb $\sqrt{n}$ méretű osztója cáfolja, hogy n prím lenne. A cáfolat mérete $O(\log n)$, a maradékos osztás $O(\log^3 n)$ időben végrehajtható.

NP $\cap$ coNP

3. példa Prímtesztelés

$\textsc{Prímek}$:= $\{p \mid p \text{ prím}\}$.

Fontos észrevétel, hogy egy $p \in \textsc{Prímek}$ hossza p számjegyeinek száma, azaz $\Theta(\log p)$.

$\textsc{Prímek}$ coNP-belisége könnyen látható, hiszen egy n szám legfeljebb $\sqrt{n}$ méretű osztója cáfolja, hogy n prím lenne. A cáfolat mérete $O(\log n)$, a maradékos osztás $O(\log^3 n)$ időben végrehajtható.

Megjegyzés: $\sqrt{n}$-ig determinisztikusan kipróbálni minden számot túl lassú, $\log n$-ben exponenciális.

NP $\cap$ coNP

3. példa Prímtesztelés

$\textsc{Prímek}$:= $\{p \mid p \text{ prím}\}$.

Fontos észrevétel, hogy egy $p \in \textsc{Prímek}$ hossza p számjegyeinek száma, azaz $\Theta(\log p)$.

$\textsc{Prímek}$ coNP-belisége könnyen látható, hiszen egy n szám legfeljebb $\sqrt{n}$ méretű osztója cáfolja, hogy n prím lenne. A cáfolat mérete $O(\log n)$, a maradékos osztás $O(\log^3 n)$ időben végrehajtható.

Megjegyzés: $\sqrt{n}$-ig determinisztikusan kipróbálni minden számot túl lassú, $\log n$-ben exponenciális.

$\textsc{Prímek}$ NP-belisége már nem ilyen egyszerű, szükség van egy gyorsan ellenőrizhető prímtesztre.

$\mathbf{NP} \cap \mathbf{coNP}$

Tétel (Lucas prímtesztje) n prím $\Leftrightarrow$ létezik $1 \leqslant x \leqslant n-1$, melyre $x^{n-1} \equiv 1 \pmod{n}$, de $x^{(n-1)/p} \not\equiv 1 \pmod{n}$ $(n-1)$-nek minden p prímosztójára.

NP $\cap$ coNP

Tétel (Lucas prímtesztje) n prím $\Leftrightarrow$ létezik $1 \leqslant x \leqslant n-1$, melyre $x^{n-1} \equiv 1 \pmod{n}$, de $x^{(n-1)/p} \not\equiv 1 \pmod{n}$ $(n-1)$-nek minden p prímosztójára.

Ez alapján a következő $(\log n)$-ben polinom idejű rekurzív nemdeterminisztikus algoritmus készíthető:

$\mathrm{NP} \cap \mathrm{coNP}$

Tétel (Lucas prímtesztje) n prím $\Leftrightarrow$ létezik $1 \leqslant x \leqslant n-1$, melyre $x^{n-1} \equiv 1 \pmod{n}$, de $x^{(n-1)/p} \not\equiv 1 \pmod{n}$ $(n-1)$-nek minden p prímosztójára.

Ez alapján a következő $(\log n)$-ben polinom idejű rekurzív nemdeterminisztikus algoritmus készíthető:

Nemdeterminisztikus prímfelismerés(n)
if $n = 2$ **then return** 'igen';
if $n = 1$ vagy $n > 2$ páros **then return** 'nem';
if $n > 2$ páratlan **then**
legyen $1 < x < n$;
ellenőrizzük, hogy $x^{n-1} \equiv 1 \pmod{n}$ igaz-e
tippelünk $n-1$ prímfelbontására: $p_1, \ldots p_k$
ellenőrizzük, hogy $n - 1 = p_1 \cdots p_k$
ellenőrizzük, minden $1 \leqslant i \leqslant k$-ra, hogy p_i prím és
hogy $x^{(n-1)/p_i} \not\equiv 1 \pmod{n}$
return 'igen', ha minden ellenőrzés rendben

$\mathbf{NP} \cap \mathbf{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

$\mathbf{NP} \cap \mathbf{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

$\mathrm{NP} \cap \mathrm{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$

$\mathbf{NP} \cap \mathbf{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

NP $\cap$ coNP

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$\mathbf{NP} \cap \mathbf{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} cm_i^5$

$\mathbf{NP} \cap \mathbf{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} cm_i^5 \leqslant cm^4 + c(m-1)^4 \sum_{i=1}^{k} m_i$

NP $\cap$ coNP

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m-1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} cm_i^5 \leqslant cm^4 + c(m-1)^4 \sum_{i=1}^{k} m_i = cm(m^3 + (m-1)^4)$

$\mathrm{NP} \cap \mathrm{coNP}$

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} cm_i^5 \leqslant cm^4 + c(m-1)^4 \sum_{i=1}^{k} m_i = cm(m^3 + (m-1)^4) \leqslant cm^5$

NP $\cap$ coNP

Egy potenciális prímfelbontás $O(\log n)$ prímből áll, melyek mindegyike $O(\log n)$ hosszú. Egy mod n hatványozás végrehajtható $O(\log^3 n)$, az összes $O(\log^4 n)$, időben.

Összességében az algoritmus lépésszámára $m = \lceil \log_2 n \rceil$ jegyű bemenet esetén

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} T(m_i)$ alakú rekurzió adódik, ahol m_i a p_i számjegyeinek száma $(1 \leqslant i \leqslant k)$.

Nyilván $\sum_{i=1}^{k} m_i \leqslant m$ és $m_i \leqslant m - 1$ minden $1 \leqslant i \leqslant k$-ra.

Innen teljes indukcióval $T(m) \leqslant cm^5$ bizonyítható:

$T(m) \leqslant cm^4 + \sum_{i=1}^{k} cm_i^5 \leqslant cm^4 + c(m-1)^4 \sum_{i=1}^{k} m_i = cm(m^3 + (m-1)^4) \leqslant cm^5$

Az algoritmus $O(\log^5 n)$ időkorlátos, így PRÍMEK NP-beli.

$\mathbf{NP} \cap \mathbf{coNP}$

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy PRÍMEK P-beli-e.

$\mathbf{NP} \cap \mathbf{coNP}$

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy PRÍMEK P-beli-e.

AKS-prímteszt: 2002-ben M. Agrawal, N. Kayal, N. Saxena indiai tudósok készítettek egy $O(\log^{12} n \log^{k} \log n)$ idejű determinisztikus prímtesztet (k egy konstans), amivel bebizonyították, hogy PRÍMEK P-beli.

NP $\cap$ coNP

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy PRÍMEK P-beli-e.

AKS-prímteszt: 2002-ben M. Agrawal, N. Kayal, N. Saxena indiai tudósok készítettek egy $O(\log^{12} n \log^k \log n)$ idejű determinisztikus prímtesztet (k egy konstans), amivel bebizonyították, hogy PRÍMEK P-beli. Munkájukkal elnyerték a Gödel- és Fulkerson-díjakat 2006-ban.

$\mathbf{NP} \cap \mathbf{coNP}$

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy PRÍMEK P-beli-e.

AKS-prímteszt: 2002-ben M. Agrawal, N. Kayal, N. Saxena indiai tudósok készítettek egy $O(\log^{12} n \log^k \log n)$ idejű determinisztikus prímtesztet (k egy konstans), amivel bebizonyították, hogy PRÍMEK P-beli. Munkájukkal elnyerték a Gödel- és Fulkerson-díjakat 2006-ban. Később a hatékonyságot $O(\log^6 n \log^k \log n)$-re sikerült javítani.

NP $\cap$ coNP

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy $\textsc{Prímek}$ P-beli-e.

AKS-prímteszt: 2002-ben M. Agrawal, N. Kayal, N. Saxena indiai tudósok készítettek egy $O(\log^{12} n \log^k \log n)$ idejű determinisztikus prímtesztet (k egy konstans), amivel bebizonyították, hogy $\textsc{Prímek}$ P-beli. Munkájukkal elnyerték a Gödel- és Fulkerson-díjakat 2006-ban. Később a hatékonyságot $O(\log^6 n \log^k \log n)$-re sikerült javítani.

A fenti példák azt sugallják, hogy egy NP $\cap$ coNP-beli problémáról végül mindig kiderül, hogy P-beli, ám ez valószínűleg nem igaz.

NP $\cap$ coNP

Sokáig nyitott kérdés volt a számjegyek számában polinomiális determinisztikus prímteszt létezése, azaz, hogy $\textsc{Prímek}$ P-beli-e.

AKS-prímteszt: 2002-ben M. Agrawal, N. Kayal, N. Saxena indiai tudósok készítettek egy $O(\log^{12} n \log^k \log n)$ idejű determinisztikus prímtesztet (k egy konstans), amivel bebizonyították, hogy $\textsc{Prímek}$ P-beli. Munkájukkal elnyerték a Gödel- és Fulkerson-díjakat 2006-ban. Később a hatékonyságot $O(\log^{6} n \log^k \log n)$-re sikerült javítani.

A fenti példák azt sugallják, hogy egy NP $\cap$ coNP-beli problémáról végül mindig kiderül, hogy P-beli, ám ez valószínűleg nem igaz.

Sejtés: P $\neq$ NP $\cap$ coNP.