Algoritmuselmélet

Közelítő algoritmusok

Katona Gyula Y.

Számítástudományi és Információelméleti Tanszék
Budapesti Műszaki és Gazdaságtudományi Egyetem

14. előadás

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is, ha az polinom időben kiszámolható.

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is, ha az polinom időben kiszámolható.

Közelítés additív konstanssal: $OPT - c \leq APPR \leq OPT + c$

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is, ha az polinom időben kiszámolható.

Közelítés additív konstanssal: $OPT - c \leq APPR \leq OPT + c$

Ilyen ritkán van.

Közelítő algoritmusok

C-KÖZÚT

Bemenet: G

Kérdés: Van-e legalább $v(G) - c$ hosszú út G-ben?

Közelítő algoritmusok

C-KÖZÚT

Bemenet: G

Kérdés: Van-e legalább $v(G) - c$ hosszú út G-ben?

Tétel

C-KÖZÚT $\in$ NP-*teljes.*

Bizonyítás.

C-KÖZÚT $\in$ NP, tanú egy út. $\surd$

Közelítő algoritmusok

C-KÖZÚT

Bemenet: G

Kérdés: Van-e legalább $v(G) - c$ hosszú út G-ben?

Tétel

C-KÖZÚT $\in$ NP-*teljes.*

Bizonyítás.

C-KÖZÚT $\in$ NP, tanú egy út. $\surd$

H-ÚT $\prec$ C-KÖZÚT: $G \Longrightarrow G' = G + c$ db izolált pont.

Közelítő algoritmusok

C-KÖZÚT

Bemenet: G

Kérdés: Van-e legalább $v(G) - c$ hosszú út G-ben?

Tétel

C-KÖZÚT $\in$ NP-*teljes.*

Bizonyítás.

C-KÖZÚT $\in$ NP, tanú egy út. $\surd$

H-ÚT $\prec$ C-KÖZÚT: $G \Longrightarrow G' = G + c$ db izolált pont.

Ha G-ben van Hamilton-út, ez G'-ben egy $v(G') - c$ hosszú út. $\surd$

Közelítő algoritmusok

C-KÖZÚT

Bemenet: G

Kérdés: Van-e legalább $v(G) - c$ hosszú út G-ben?

Tétel

C-KÖZÚT $\in$ NP-*teljes.*

Bizonyítás.

C-KÖZÚT $\in$ NP, tanú egy út. $\surd$

H-ÚT $\prec$ C-KÖZÚT: $G \Longrightarrow G' = G + c$ db izolált pont.

Ha G-ben van Hamilton-út, ez G'-ben egy $v(G') - c$ hosszú út. $\surd$

Ha G'-ben van egy $v(G') - c$ hosszú út, akkor az G minden pontját tartalmazza, tehát Hamilton-út. $\surd$ $\square$

Közelítő algoritmusok

Közelítés multiplikatív konstanssal: $\frac{1}{c} OPT \leq APPR \leq c \cdot OPT$

Közelítő algoritmusok

Közelítés multiplikatív konstanssal: $\frac{1}{c} OPT \leq APPR \leq c \cdot OPT$

Ilyen sokszor van. Keressünk 1-hez minél közelebbi konstanst.

Euklideszi utazó ügynök probléma

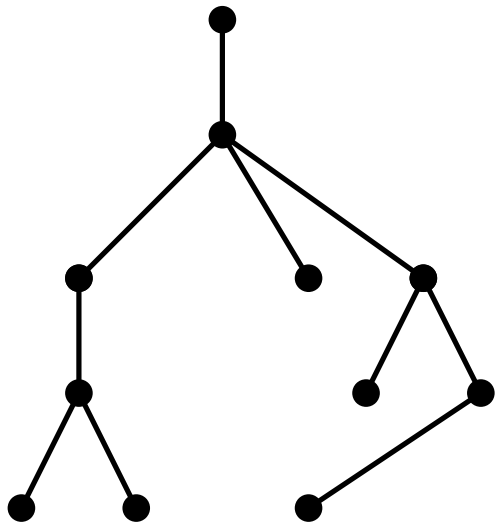
Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

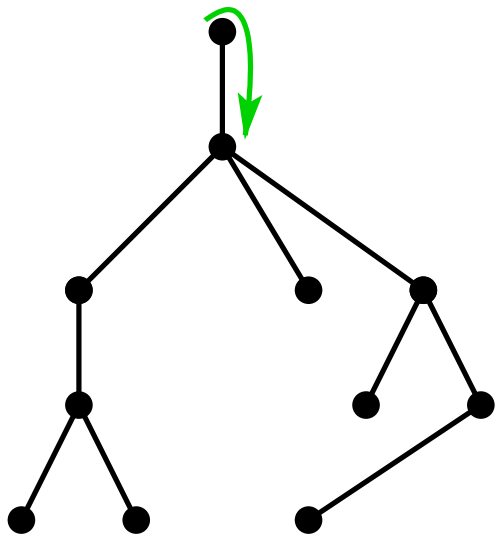


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

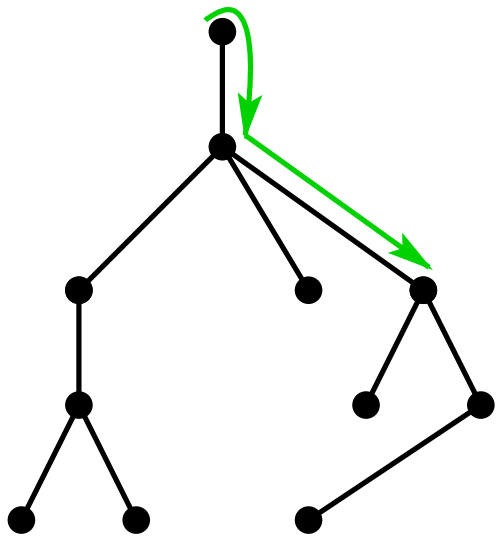


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

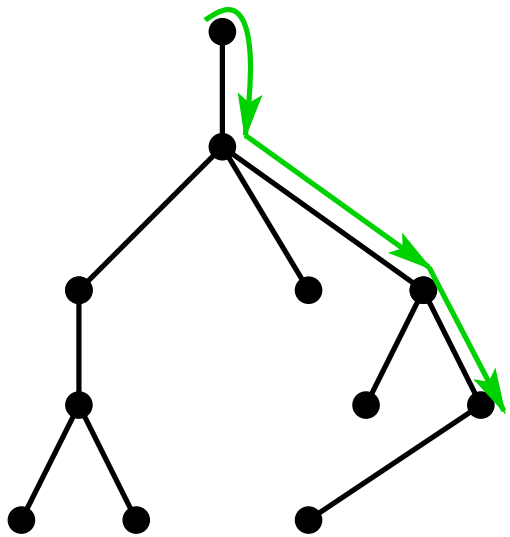


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

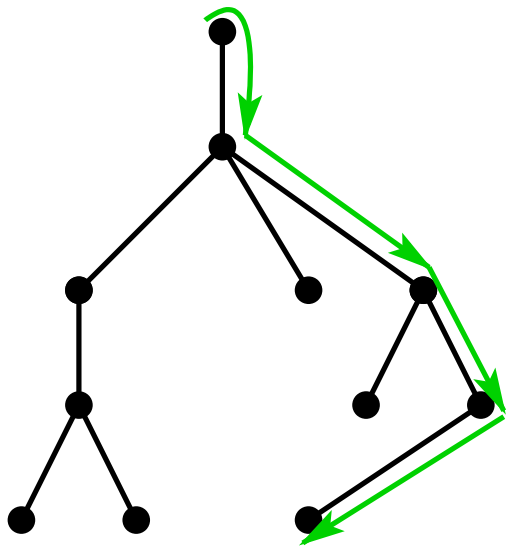


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

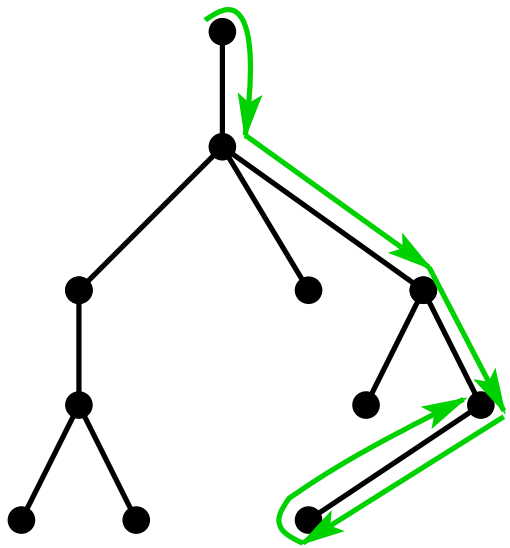


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

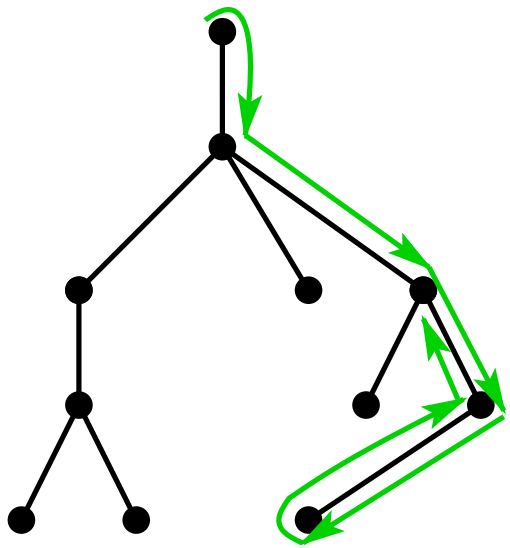


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

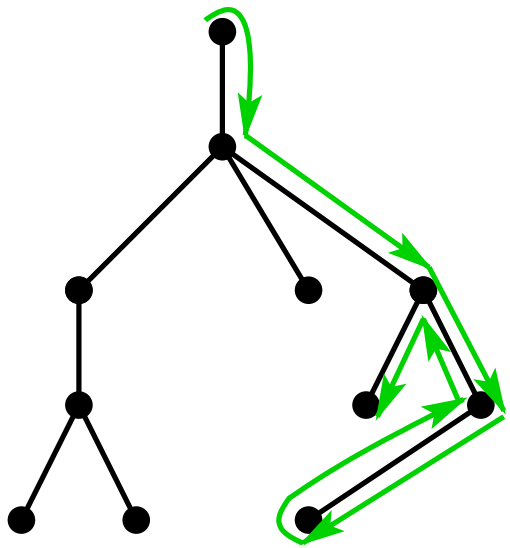


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

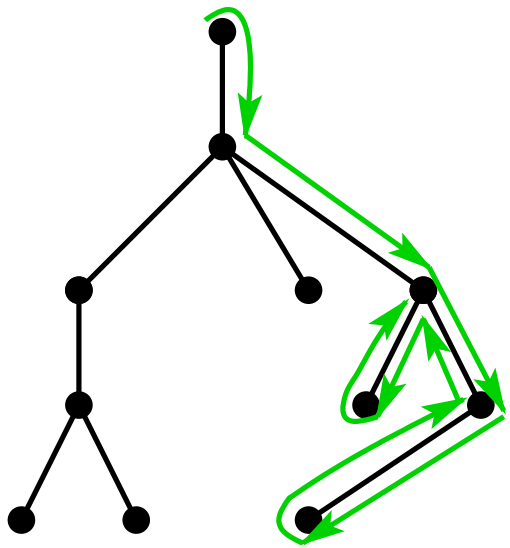


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

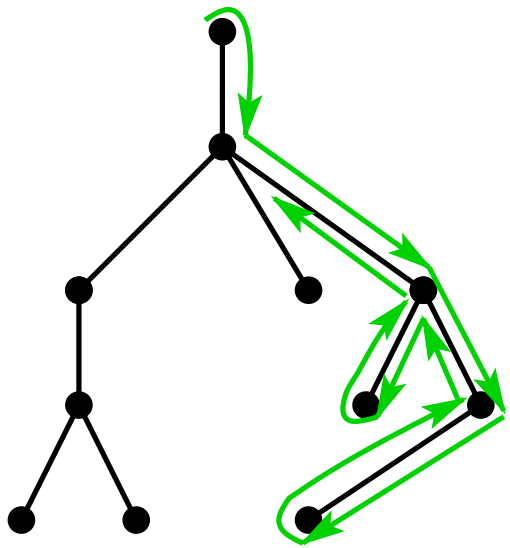


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

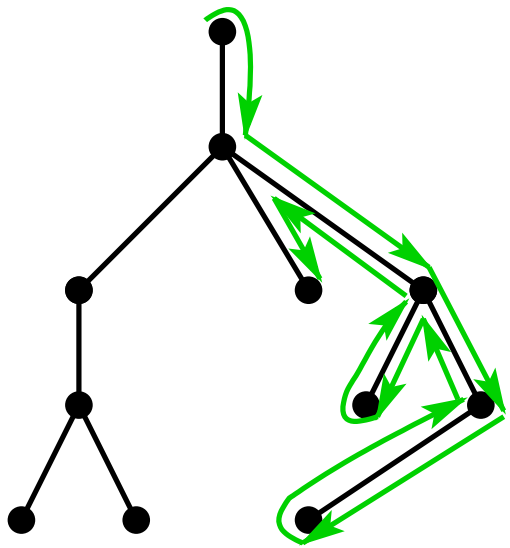


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

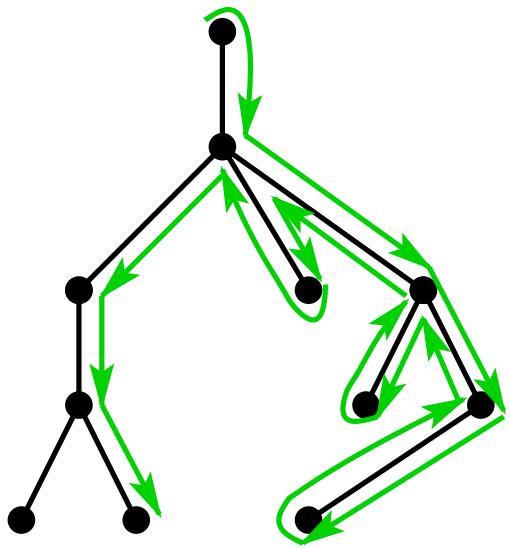


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

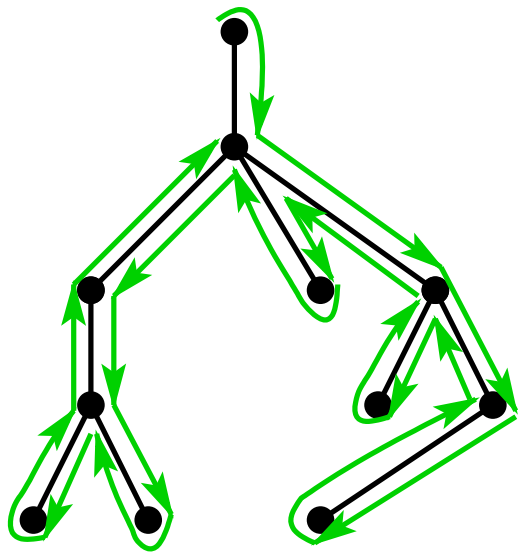


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

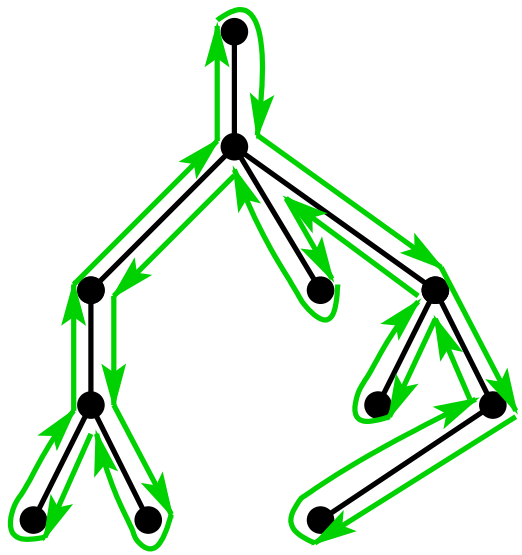


Euklideszi utazó ügynök probléma

Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).

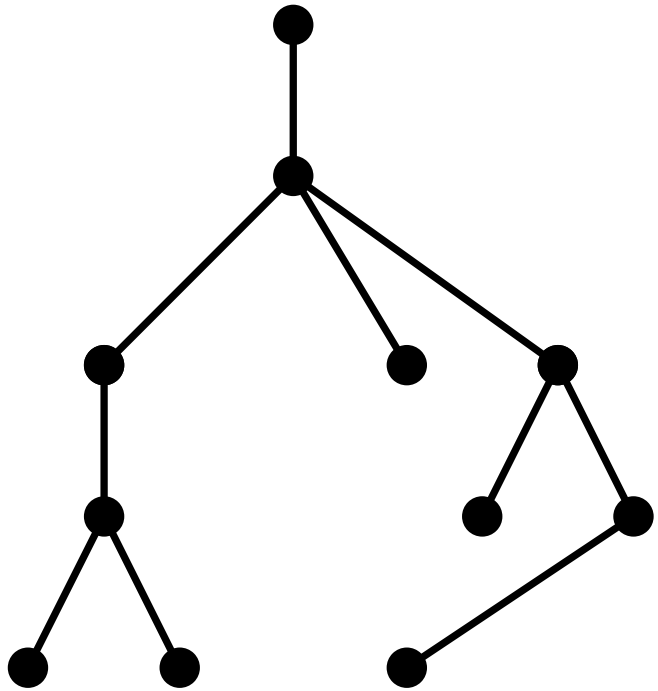
A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal), megkettőzzük az éleit és „körbejárjuk” egy Euler-körsétával.

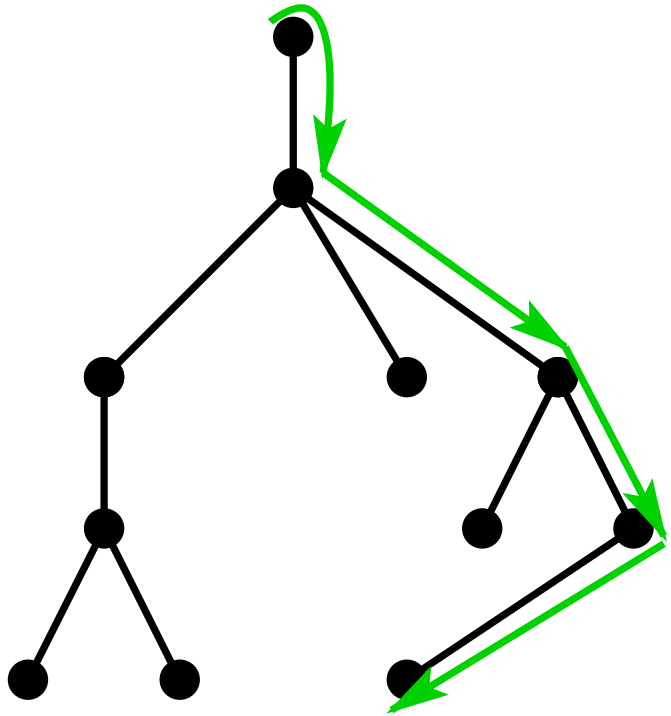


A minimális feszítőfa összsúlya legyen $s \implies$ Euler-séta hossza $2s$.

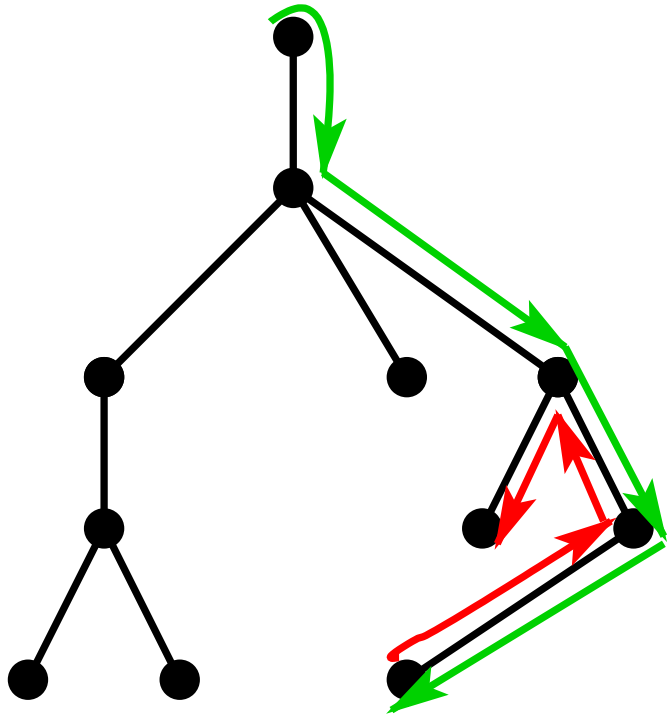
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



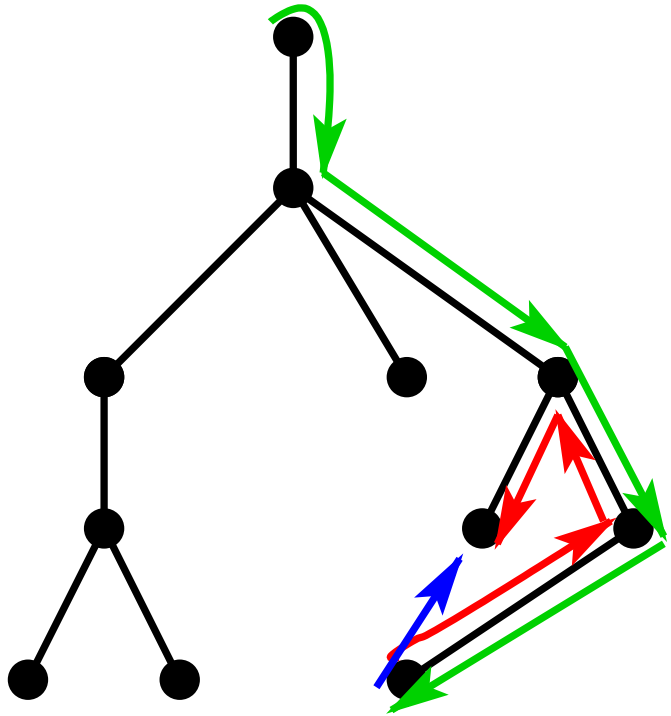
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



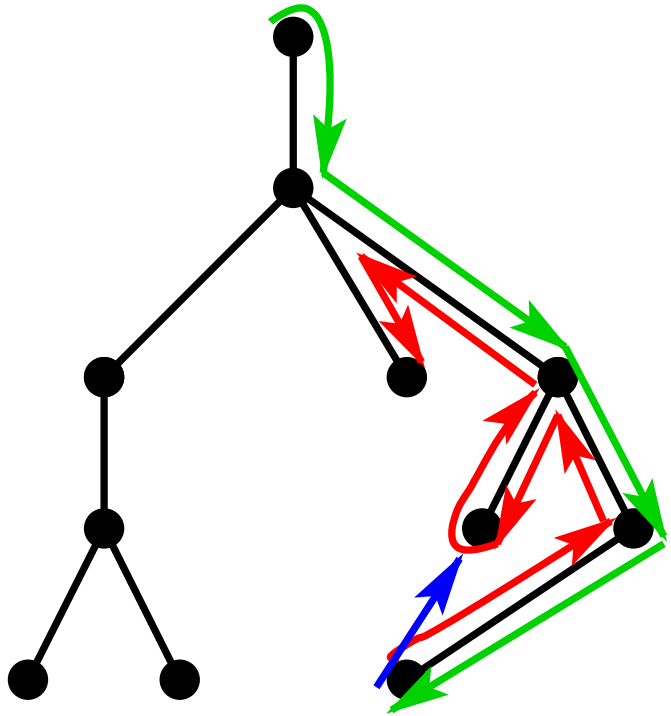
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



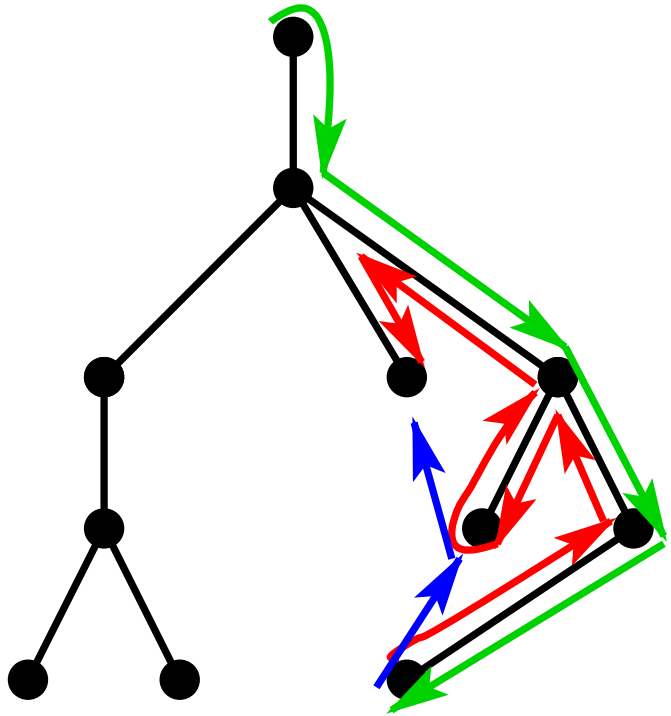
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



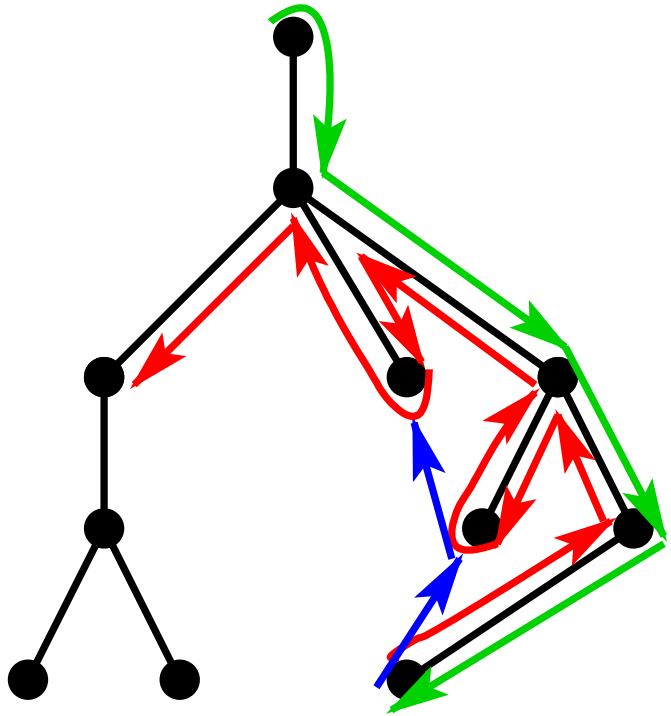
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



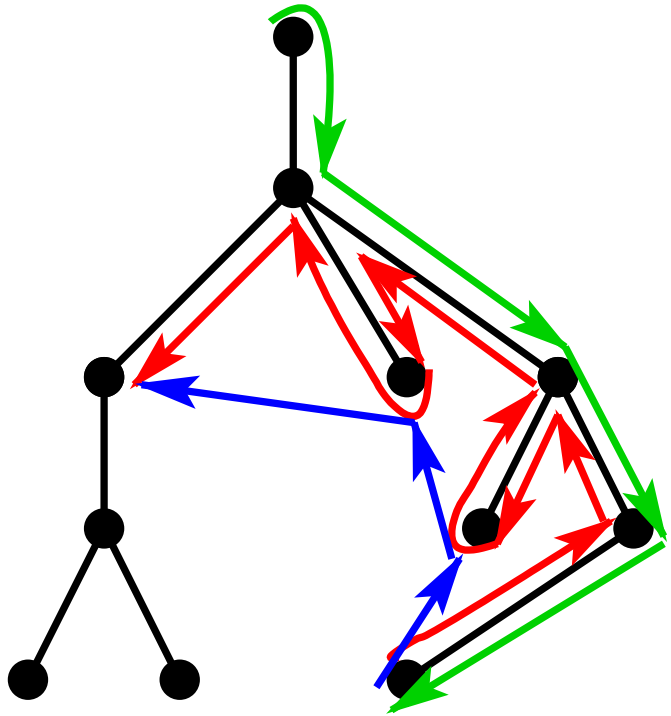
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



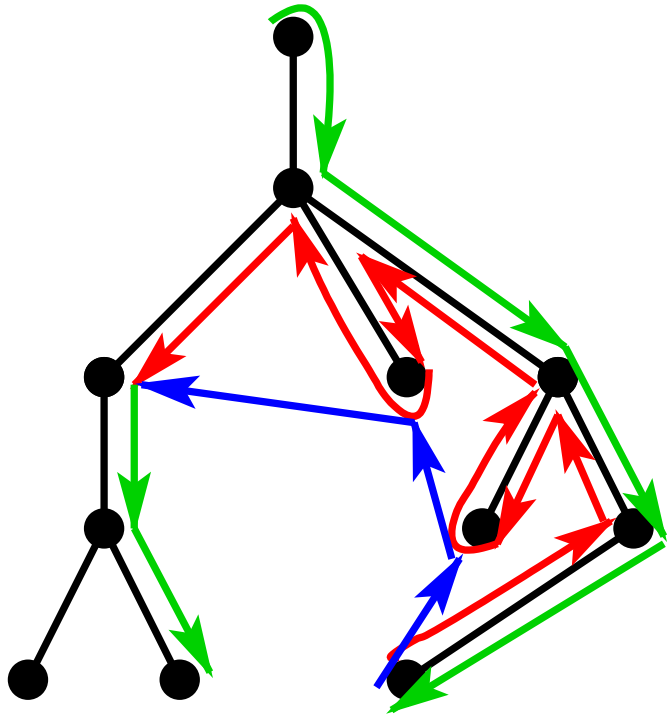
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



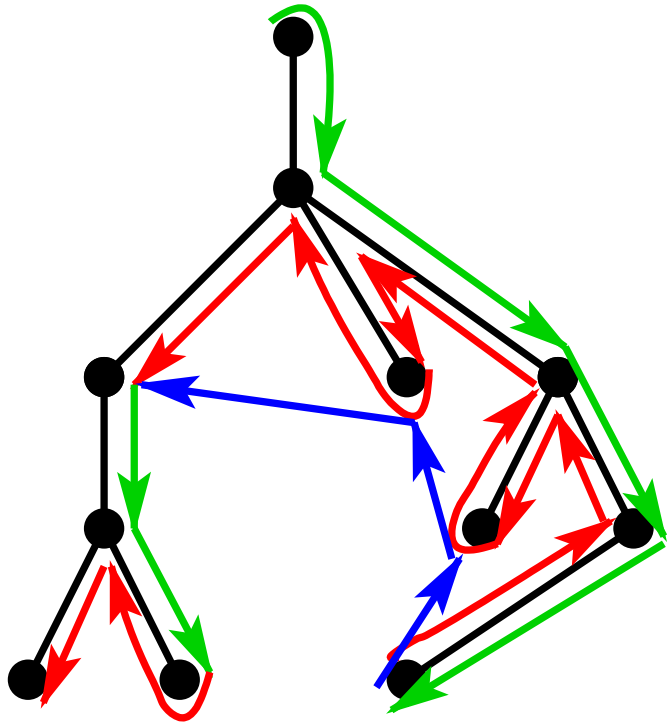
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



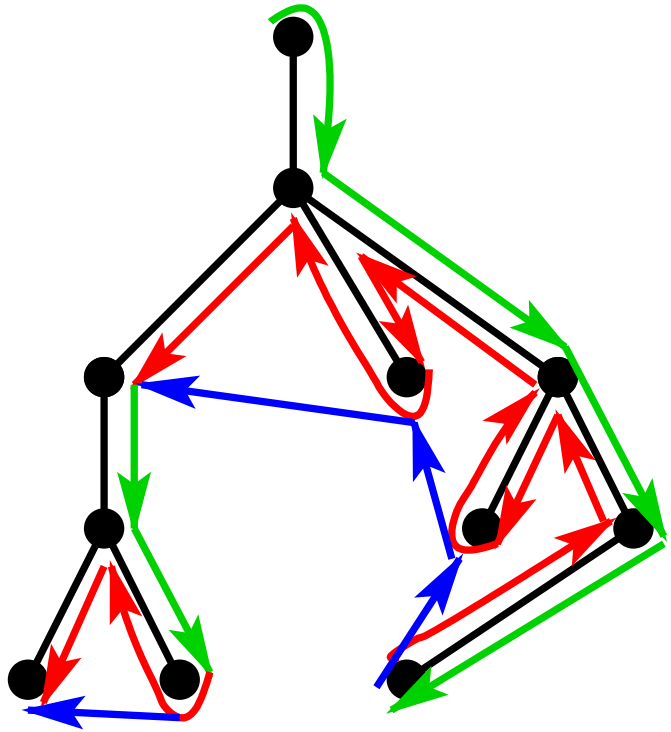
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



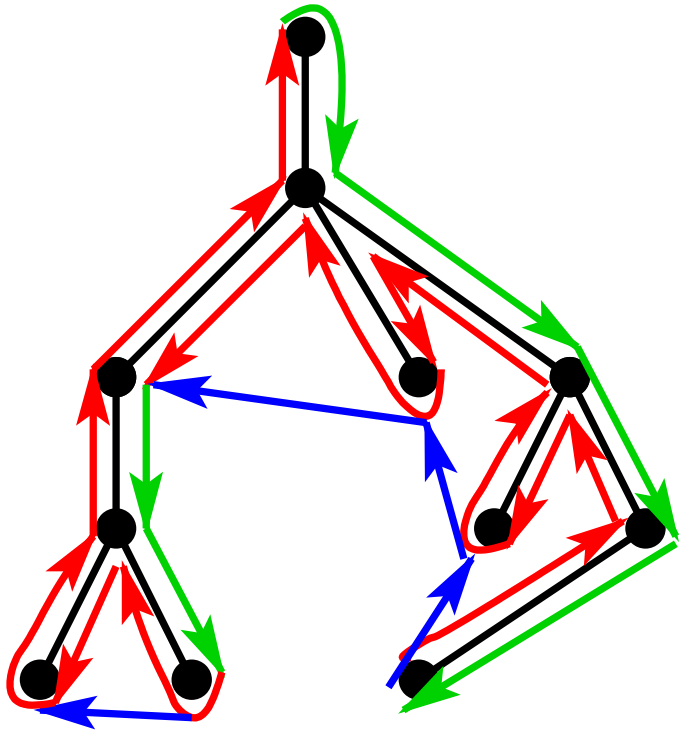
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



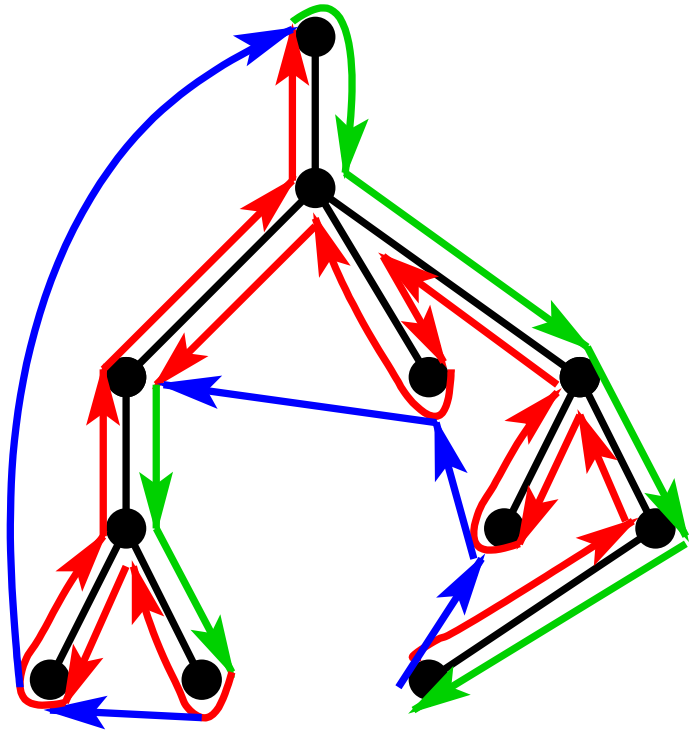
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.

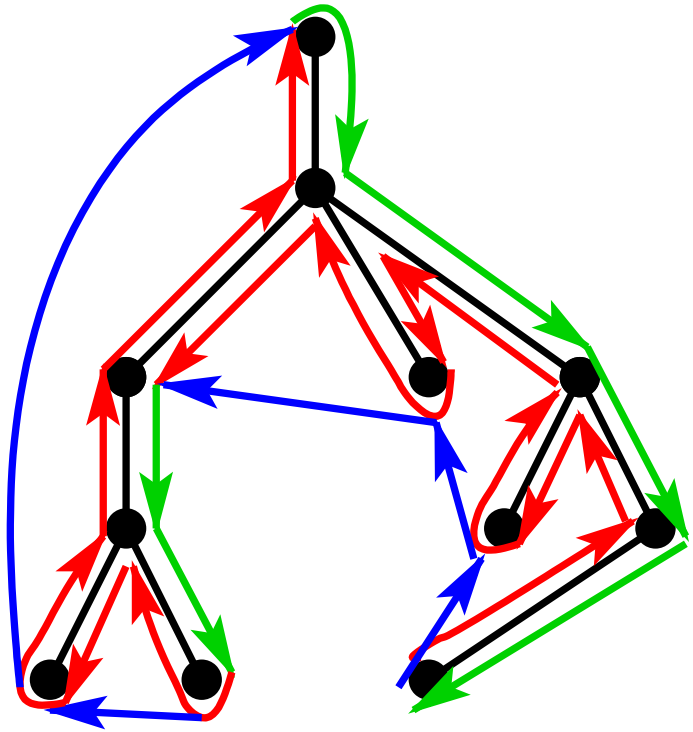


Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ha az optimális Hamilton-körből elhagyunk egy élet $\Longrightarrow$ egy legalább s súlyú feszítőfát kapunk.

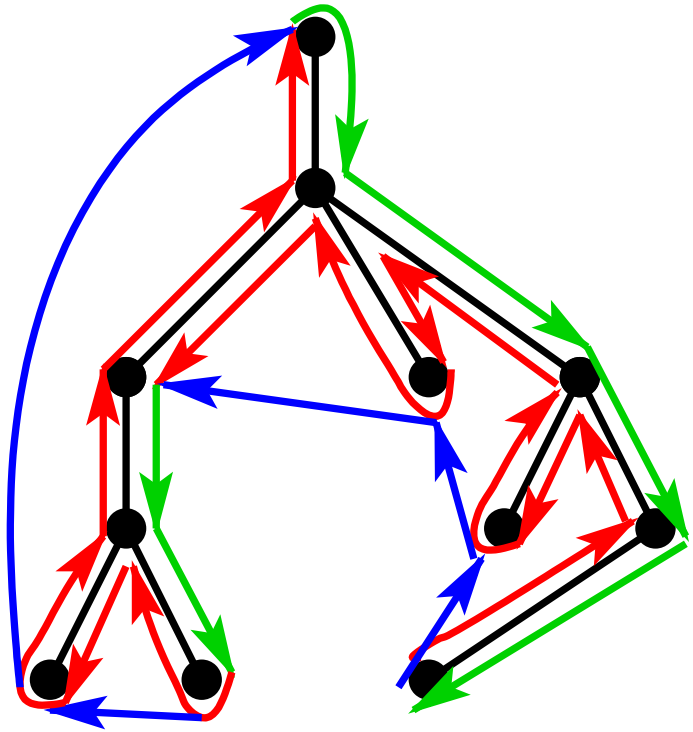
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ha az optimális Hamilton-körből elhagyunk egy élet $\Longrightarrow$ egy legalább s súlyú feszítőfát kapunk.

A módszer legfeljebb 2-szer akkora utat ad, mint az optimális.

Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ha az optimális Hamilton-körből elhagyunk egy élet $\Longrightarrow$ egy legalább s súlyú feszítőfát kapunk.

A módszer legfeljebb 2-szer akkora utat ad, mint az optimális.

Ládapakolás

Ládapakolás: Adottak az $s_1, \ldots, s_m$ (racionális) súlyok, $0 \leq s_i \leq 1$. A cél a súlyok elhelyezése minél kevesebb 1 súlykapacitású ládába.

Ládapakolás

Ládapakolás: Adottak az $s_1, \ldots, s_m$ (racionális) súlyok, $0 \leq s_i \leq 1$. A cél a súlyok elhelyezése minél kevesebb 1 súlykapacitású ládába.

NP-nehéz,

Ládapakolás

Ládapakolás: Adottak az $s_1, \ldots, s_m$ (racionális) súlyok, $0 \leq s_i \leq 1$. A cél a súlyok elhelyezése minél kevesebb 1 súlykapacitású ládába.

NP-nehéz, a PARTÍCIÓ probléma visszavezethető rá.

Ládapakolás

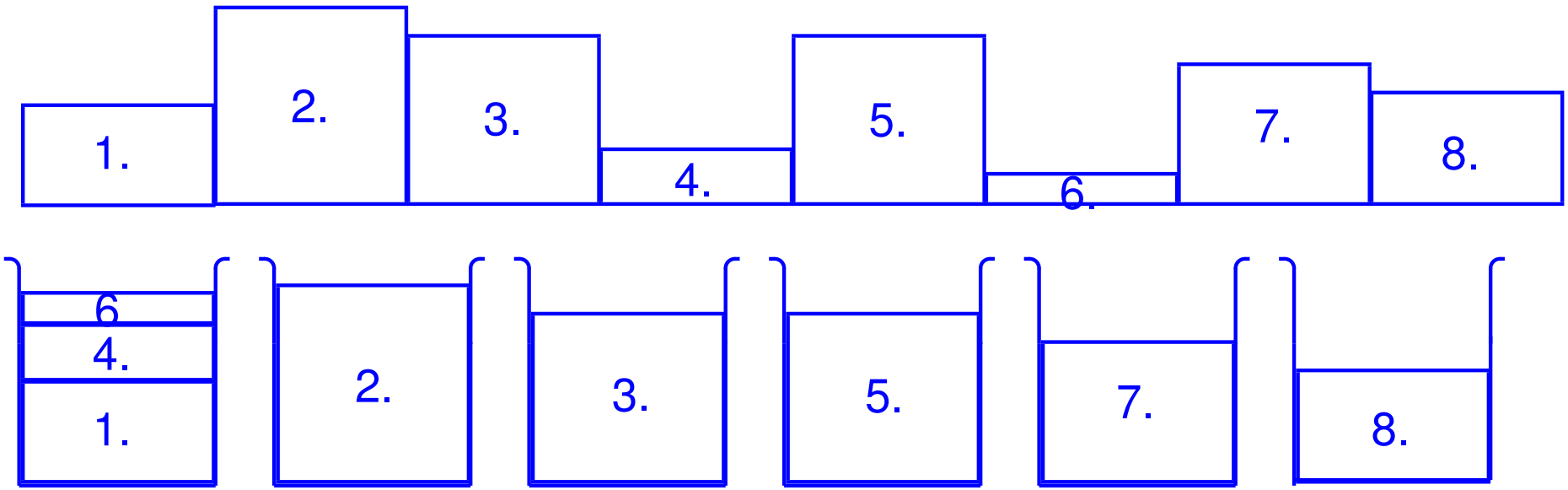
FF-módszer (*first fit*): Vegyünk először üres ládákat, és számozzuk meg őket az $1, 2, \ldots, m$ egészekkel.

Ládapakolás

FF-módszer (*first fit*): Vegyünk először üres ládákat, és számozzuk meg őket az $1, 2, \ldots, m$ egészekkel.
Tegyük fel, hogy az $s_1, \ldots, s_{i-1}$ súlyokat már elhelyeztük. Ekkor s_i kerüljön az első (legkisebb sorszámú) olyan ládába, amelybe még befér.

Ládapakolás

FF-módszer (*first fit*): Vegyünk először üres ládákat, és számozzuk meg őket az $1, 2, \ldots, m$ egészekkel.
Tegyük fel, hogy az $s_1, \ldots, s_{i-1}$ súlyokat már elhelyeztük. Ekkor s_i kerüljön az első (legkisebb sorszámú) olyan ládába, amelybe még befér.



First Fit

Tétel

Jelölje a Ládapakolás probléma egy I inputjára $OPT(I)$ az optimális (minimálisan elegendő), $FF(I)$ pedig az FF-módszer által eredményezett ládaszámot. A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq 2OPT(I)$.

First Fit

Tétel

Jelölje a Ládapakolás probléma egy I inputjára $OPT(I)$ az optimális (minimálisan elegendő), $FF(I)$ pedig az FF-módszer által eredményezett ládaszámot. A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq 2OPT(I)$.

Bizonyítás.

$\lceil \sum_{i=1}^{m} s_i \rceil \leq OPT(I)$

First Fit

Tétel

Jelölje a Ládapakolás probléma egy I inputjára $OPT(I)$ az optimális (minimálisan elegendő), $FF(I)$ pedig az FF-módszer által eredményezett ládaszámot. A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq 2OPT(I)$.

Bizonyítás.

$\lceil \sum_{i=1}^{m} s_i \rceil \leq OPT(I)$
$FF(I) \leq \lceil 2 \sum_{i=1}^{m} s_i \rceil \iff$ nincs két olyan láda, amely nincs félig kitöltve.

First Fit

Tétel

Jelölje a Ládapakolás probléma egy I inputjára $OPT(I)$ az optimális (minimálisan elegendő), $FF(I)$ pedig az FF-módszer által eredményezett ládaszámot. A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq 2OPT(I)$.

Bizonyítás.

$\lceil \sum_{i=1}^{m} s_i \rceil \leq OPT(I)$
$FF(I) \leq \lceil 2 \sum_{i=1}^{m} s_i \rceil \iff$ nincs két olyan láda, amely nincs félig kitöltve.
Felhasználjuk, hogy $\lceil 2x \rceil \leq 2\lceil x \rceil$:

$$FF(I) \leq \lceil 2 \sum_{i=1}^{m} s_i \rceil \leq 2 \lceil \sum_{i=1}^{m} s_i \rceil \leq 2OPT(I).$$

$\surd$ □

First Fit

Tétel (D. S. Johnson és munkatársai, 1976)

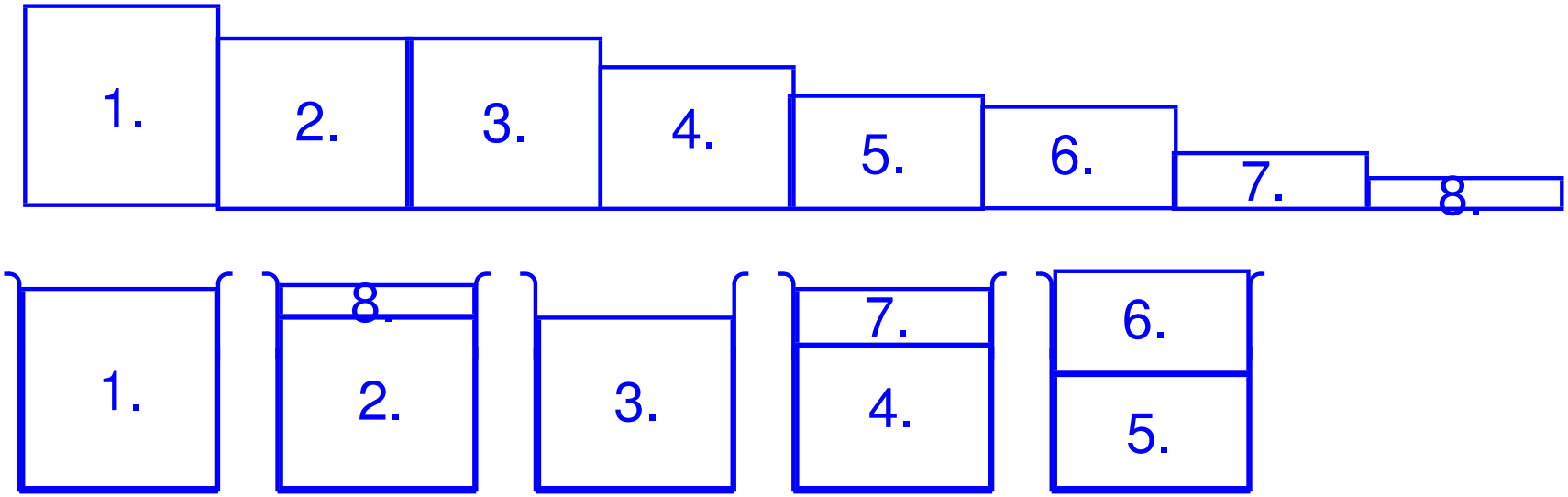
A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq \lceil 1.7 OPT(I) \rceil$. Továbbá vannak tetszőlegesen nagy méretű I inputok, melyekre $FF(I) \geq 1.7(OPT(I) - 1)$.

First Fit Decreasing

FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az *FF*-módszert.

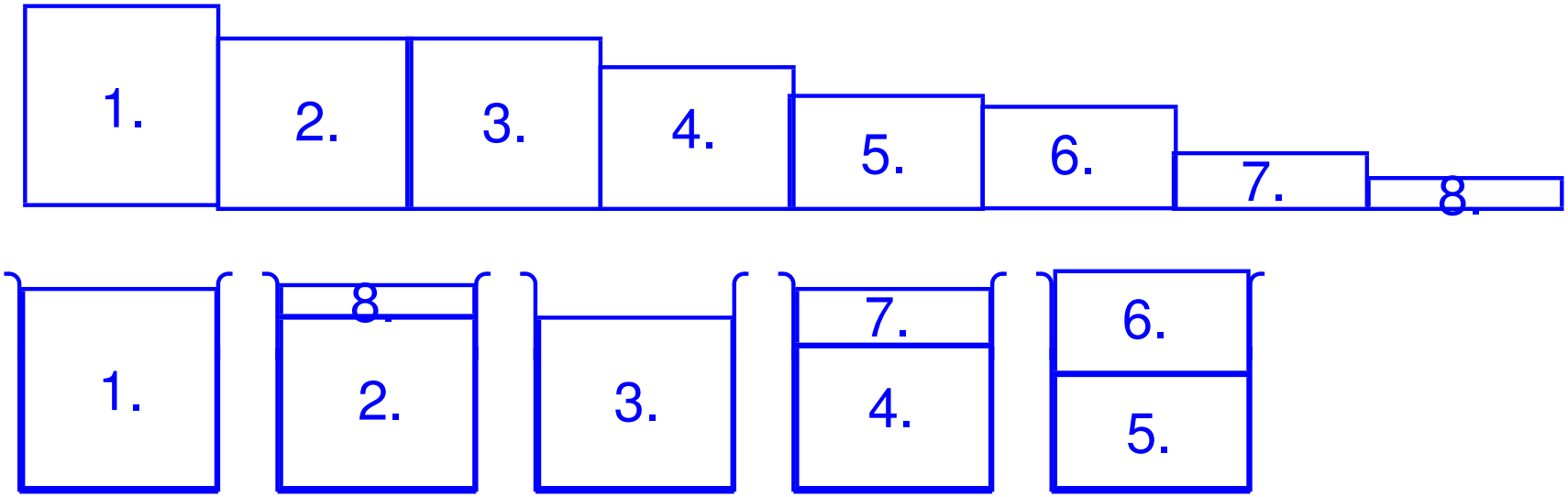
First Fit Decreasing

FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az *FF*-módszert.



First Fit Decreasing

FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az *FF*-módszert.

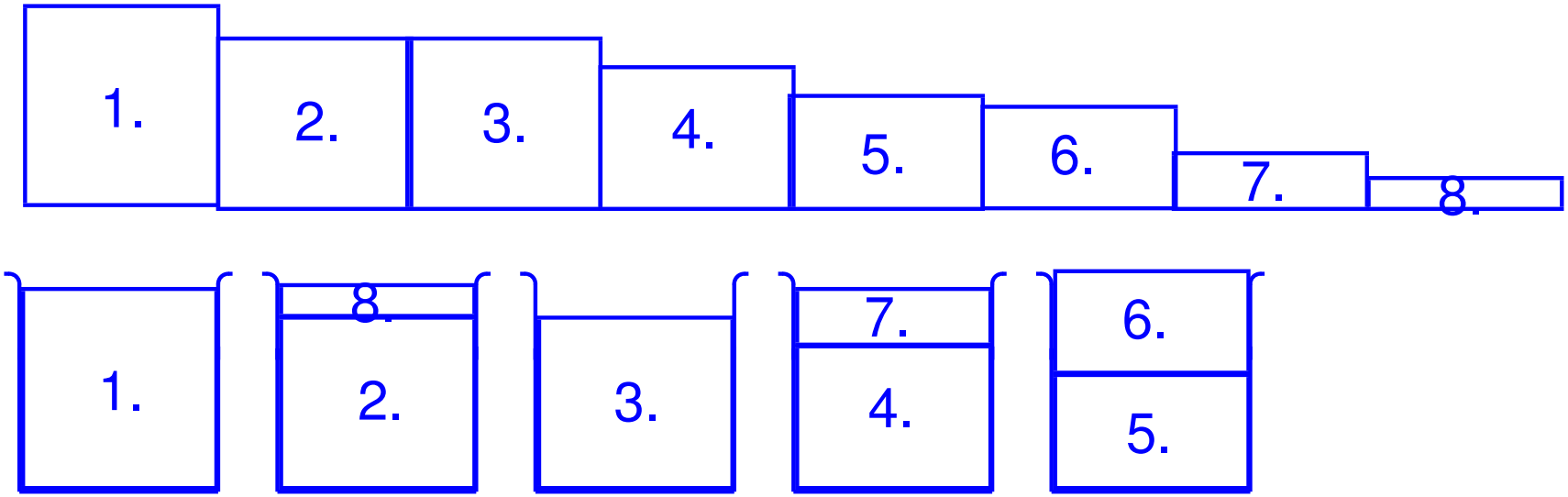


Tétel (D. S. Johnson, 1973)

Tetszőleges I inputra teljesül, hogy $FFD(I) \leq \frac{11}{9} OPT(I) + 4$, *és tetszőlegesen nagy méretű I inputok vannak, melyekre* $FFD(I) \geq \frac{11}{9} OPT(I)$. ($\frac{11}{9} = 1.222\ldots$)

First Fit Decreasing

FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az *FF*-módszert.



Tétel (D. S. Johnson, 1973)

Tetszőleges I inputra teljesül, hogy $FFD(I) \leq \frac{11}{9} OPT(I) + 4$, *és tetszőlegesen nagy méretű I inputok vannak, melyekre* $FFD(I) \geq \frac{11}{9} OPT(I)$. ($\frac{11}{9} = 1.222\ldots$)

Jobb approximáció

Tétel (W. Fernandez de la Vega, G. S. Lueker)

Tetszőleges $\varepsilon > 0$-hoz van olyan P lineáris algoritmus, amire $P(I) \leq (1+\varepsilon)OPT(I) + 1$.

Jobb approximáció

Tétel (W. Fernandez de la Vega, G. S. Lueker)

Tetszőleges $\varepsilon > 0$-hoz van olyan P lineáris algoritmus, amire $P(I) \leq (1+\varepsilon)OPT(I) + 1$.

Futásideje: $O(n) + 2^{2^{O((1/\varepsilon)\log(1/\varepsilon))}}$

Véletlent használó módszerek

Előny: Gyorsabb lehet.

Véletlent használó módszerek

Előny: Gyorsabb lehet.
Hátrány: Kis valószínőséggel hibás választ kapunk.

Véletlent használó módszerek

Előny: Gyorsabb lehet.
Hátrány: Kis valószínőséggel hibás választ kapunk.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.

Fermat-teszt (m)

1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha lnko$(a, m) \neq 1$, akkor a válasz „m összetett”.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.

Fermat-teszt (m)

1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.
Fermat-teszt (m)
1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

2. Euklideszi algoritmussal gyorsan végrehajtható.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.
Fermat-teszt (m)
1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha lnko$(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

2. Euklideszi algoritmussal gyorsan végrehajtható.
3. Gyors hatványozással gyorsan végrehajtható.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.
Fermat-teszt (m)
1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

2. Euklideszi algoritmussal gyorsan végrehajtható.
3. Gyors hatványozással gyorsan végrehajtható.

Ha azt kapjuk, hogy „m összetett” $\Longrightarrow$ ez biztos igaz.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.
Fermat-teszt (m)
1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

2. Euklideszi algoritmussal gyorsan végrehajtható.
3. Gyors hatványozással gyorsan végrehajtható.

Ha azt kapjuk, hogy „m összetett” $\implies$ ez biztos igaz.
Pl.: $m = 21 = 7 \cdot 3$ és $a = 2 \implies a$ az m Fermat-tanúja, hiszen $2^{20} \equiv 4 \pmod{21}$.

Prímtesztelés

Bemenő adatként adott (binárisan) egy m páratlan egész; szeretnénk eldönteni, hogy m prímszám-e.
Fermat-teszt (m)
1. Válasszunk egy véletlen a egészet az $[1, m)$ intervallumból.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor a válasz „m összetett”.
3. Ha $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

2. Euklideszi algoritmussal gyorsan végrehajtható.
3. Gyors hatványozással gyorsan végrehajtható.

Ha azt kapjuk, hogy „m összetett” $\implies$ ez biztos igaz.
Pl.: $m = 21 = 7 \cdot 3$ és $a = 2 \implies a$ az m Fermat-tanúja, hiszen $2^{20} \equiv 4 \pmod{21}$.

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ *és* $a^{m-1} \not\equiv 1 \pmod{m}$*), melyre lnko*$(a, m) = 1$*, akkor az* $[1, m)$ *intervallum egészeinek legalább a fele Fermat-tanú.*

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ *és* $a^{m-1} \not\equiv 1 \pmod{m}$*), melyre lnko*$(a, m) = 1$*, akkor az* $[1, m)$ *intervallum egészeinek legalább a fele Fermat-tanú.*

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ *és* $a^{m-1} \not\equiv 1 \pmod{m}$*), melyre lnko*$(a, m) = 1$*, akkor az* $[1, m)$ *intervallum egészeinek legalább a fele Fermat-tanú.*

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Feltehetjük, hogy a, c_i relatív prímek m-hez.

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre $lnko(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Feltehetjük, hogy a, c_i relatív prímek m-hez.

$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre lnko$(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Feltehetjük, hogy a, c_i relatív prímek m-hez.

$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.

Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow$

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre lnko$(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Feltehetjük, hogy a, c_i relatív prímek m-hez.

$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.

Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow m | ac_i - ac_j = a(c_i - c_j) \Longrightarrow m | c_i - c_j$, hiszen lnko$(a, m) = 1$.

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre lnko$(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk $\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$

Feltehetjük, hogy a, c_i relatív prímek m-hez.

$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.

Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow m | ac_i - ac_j = a(c_i - c_j) \Longrightarrow m | c_i - c_j$, hiszen lnko$(a, m) = 1$. $\Longrightarrow ac_1, ac_2, \ldots, ac_s$ mind különbözőek lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú. $\surd$

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre lnko$(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk
$\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$
Feltehetjük, hogy a, c_i relatív prímek m-hez.
$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.
Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow m | ac_i - ac_j = a(c_i - c_j) \Longrightarrow m | c_i - c_j$,
hiszen lnko$(a, m) = 1$. $\Longrightarrow ac_1, ac_2, \ldots, ac_s$ mind különbözőek
lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú. $\surd$ $\square$

Vannak olyan számok, amelyeknek nincs tanújuk: Carmichael-számok

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre $\text{lnko}(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk
$\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$
Feltehetjük, hogy a, c_i relatív prímek m-hez.
$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.
Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow m | ac_i - ac_j = a(c_i - c_j) \Longrightarrow m | c_i - c_j$,
hiszen $\text{lnko}(a, m) = 1$. $\Longrightarrow ac_1, ac_2, \ldots, ac_s$ mind különbözőek
lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú. $\surd$ $\square$

Vannak olyan számok, amelyeknek nincs tanújuk: Carmichael-számok
Pl. $561 = 3 \cdot 11 \cdot 17$

Prímtesztelés

Tétel

Ha m-nek van olyan a Fermat-tanúja ($1 \leq a < m$ és $a^{m-1} \not\equiv 1 \pmod{m}$), melyre $\text{lnko}(a, m) = 1$, akkor az $[1, m)$ intervallum egészeinek legalább a fele Fermat-tanú.

Bizonyítás.

Legyen a tanú $\Longrightarrow a^{m-1} \not\equiv 1 \pmod{m}$ és $c_1, c_2, \ldots, c_s$ nem tanúk
$\Longrightarrow c_i^{m-1} \equiv 1 \pmod{m}$
Feltehetjük, hogy a, c_i relatív prímek m-hez.
$\Longrightarrow (ac_i)^{m-1} \equiv a^{m-1} c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \Longrightarrow ac_i$ tanú.
Ha $ac_i \equiv ac_j \pmod{m} \Longrightarrow m | ac_i - ac_j = a(c_i - c_j) \Longrightarrow m | c_i - c_j$,
hiszen $\text{lnko}(a, m) = 1$. $\Longrightarrow ac_1, ac_2, \ldots, ac_s$ mind különbözőek
lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú. $\surd$ $\square$

Vannak olyan számok, amelyeknek nincs tanújuk: Carmichael-számok
Pl. $561 = 3 \cdot 11 \cdot 17$
Alford, Granville, Pomerance, 1992 $\Longrightarrow$ végtelen sok ilyen szám van

Rabin-Miller teszt

Definíció

Legyen m egy páratlan természetes szám. Írjuk fel $m-1$-et $m-1=2^k n$ alakban, ahol n páratlan. Az $1 \leq a < m$ egész Rabin–Miller-tanú *(m összetettségére), ha az*

$$a^n - 1,\ a^n + 1,\ a^{2n} + 1, \ldots,\ a^{2^{k-1}n} + 1$$

számok egyike sem osztható m-mel.

Rabin-Miller teszt

Tétel

Ha m prím, akkor m-hez nincs Rabin–Miller-tanú.

Rabin-Miller teszt

Tétel

Ha m prím, akkor m-hez nincs Rabin–Miller-tanú.

Bizonyítás.

$$a^{m-1} - 1 = (a^n - 1)(a^n + 1)(a^{2n} + 1) \cdots (a^{2^{k-1}n} + 1)$$

Rabin-Miller teszt

Tétel

Ha m prím, akkor m-hez nincs Rabin–Miller-tanú.

Bizonyítás.

$$a^{m-1} - 1 = (a^n - 1)(a^n + 1)(a^{2n} + 1) \cdots (a^{2^{k-1}n} + 1)$$

m prím $\implies$ a kis Fermat-tétel szerint m osztja a bal oldalt.

Rabin-Miller teszt

Tétel

Ha m prím, akkor m-hez nincs Rabin–Miller-tanú.

Bizonyítás.

$$a^{m-1} - 1 = (a^n - 1)(a^n + 1)(a^{2n} + 1) \cdots (a^{2^{k-1}n} + 1)$$

m prím $\implies$ a kis Fermat-tétel szerint m osztja a bal oldalt.
$\implies$ m osztja a jobb oldal valamelyik tényezőjét $\implies$ a nem Rabin–Miller-tanú.

Rabin-Miller teszt

Tétel

Ha m prím, akkor m-hez nincs Rabin–Miller-tanú.

Bizonyítás.

$$a^{m-1} - 1 = (a^n - 1)(a^n + 1)(a^{2n} + 1) \cdots (a^{2^{k-1}n} + 1)$$

m prím $\implies$ a kis Fermat-tétel szerint m osztja a bal oldalt.
$\implies$ m osztja a jobb oldal valamelyik tényezőjét $\implies$ a nem Rabin–Miller-tanú. □

Tétel

Ha m összetett, akkor az $1 \leq a < m$ feltételt teljesítő a egészeknek legalább a fele Rabin–Miller-tanú.

Rabin-Miller teszt

$RM(m)$
1. Írjuk fel $m-1$-et $m-1=2^k n$ alakban, ahol n páratlan.
2. Válasszunk egy véletlen a egészet az $[1,m)$ intervallumból.
3. Ha az $a^n-1,\ a^n+1,\ a^{2n}+1,\ldots,\ a^{2^{k-1}n}+1$ számok egyike sem osztható m-mel, akkor megállunk azzal a válasszal, hogy „m összetett”, különben megállunk azzal a válasszal, hogy „m valószínűleg prím”.