Algoritmuselmélet 18. előadás

Katona Gyula Y.
Budapesti Műszaki és Gazdaságtudományi Egyetem
Számítástudományi Tsz.
I. B. 137/b
kiskat@cs.bme.hu

2002 Május 7.

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

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.

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

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-teljes

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

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-teljes

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

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

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-teljes

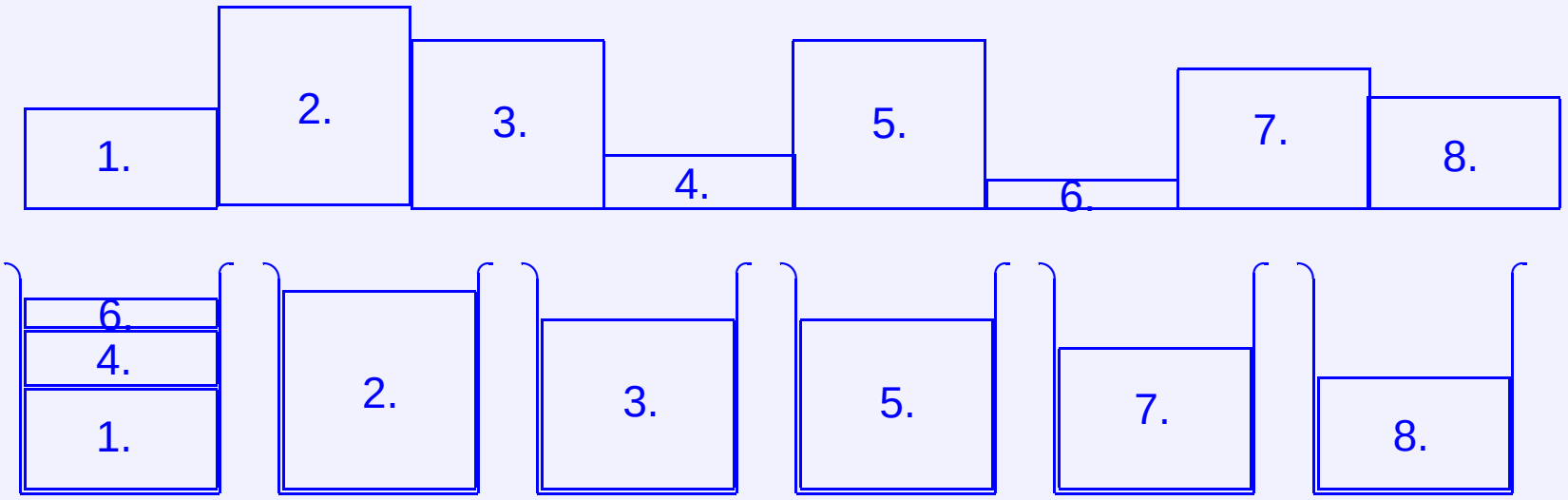
FF-módszer (*first fit*): Vegyünk először üres ládákat, és számozzuk meg őket az $1, 2, \ldots, m$ egészekkel.
Tegyük fel, hogy az $s_1, \ldots, s_{i-1}$ súlyokat már elhelyeztük. Ekkor s_i kerüljön az első (legkisebb sorszámú) olyan ládába, amelybe még befér.

Közelítő algoritmusok

Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

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-teljes

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.



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 $FF(I) \leq 2OPT(I)$.*

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

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, ami nincs félig kitöltve.

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

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

✓

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, ami nincs félig kitöltve.
Felhasználjuk, hogy $\lceil 2x \rceil \leq 2\lceil x \rceil$

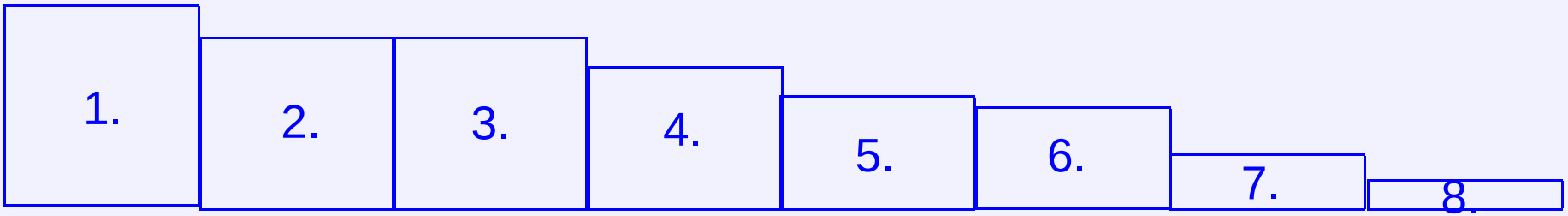
$$FF(I) \leq \lceil 2 \sum_{i=1}^{m} s_i \rceil \leq 2 \lceil \sum_{i=1}^{m} s_i \rceil \leq 2OPT(I)$$

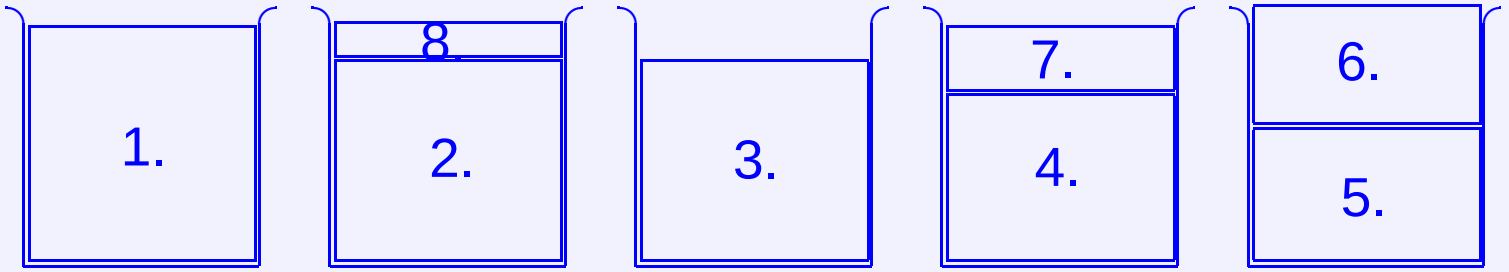
✓

Tétel. [D. S. Johnson és munkatársai, 1976]
A probléma tetszőleges I inputjára teljesül, hogy $FF(I) \leq \lceil 1.7OPT(I) \rceil$. Továbbá vannak tetszőlegesen nagy méretű I inputok, melyekre $FF(I) \geq 1.7(OPT(I) - 1)$.

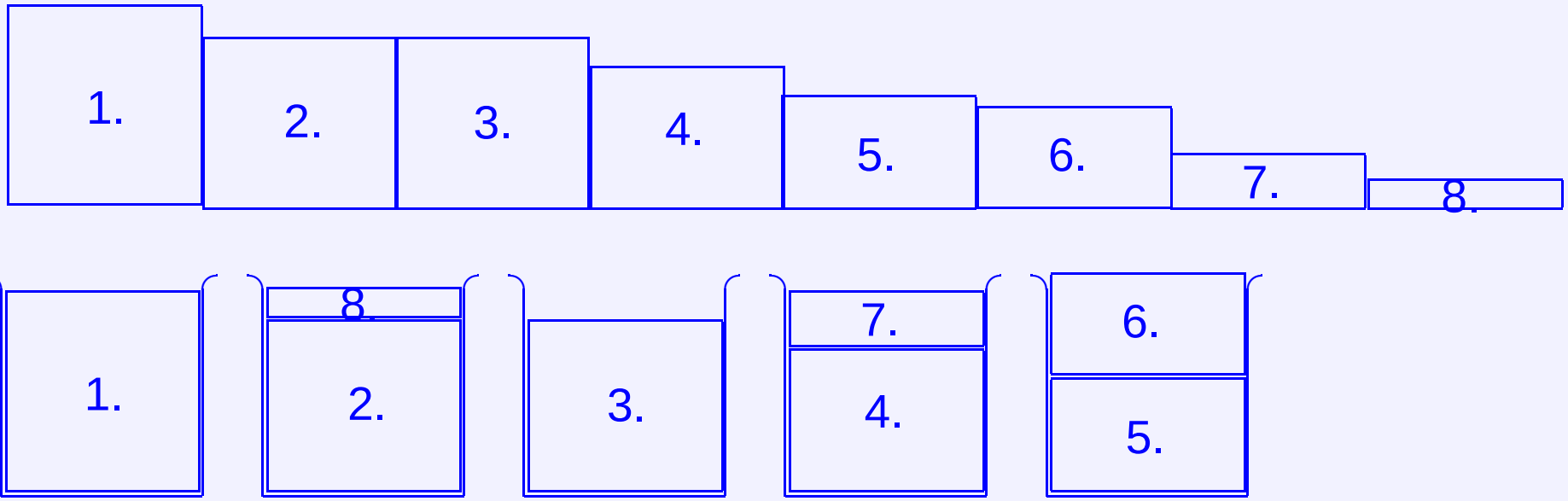
FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az FF-módszert.

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



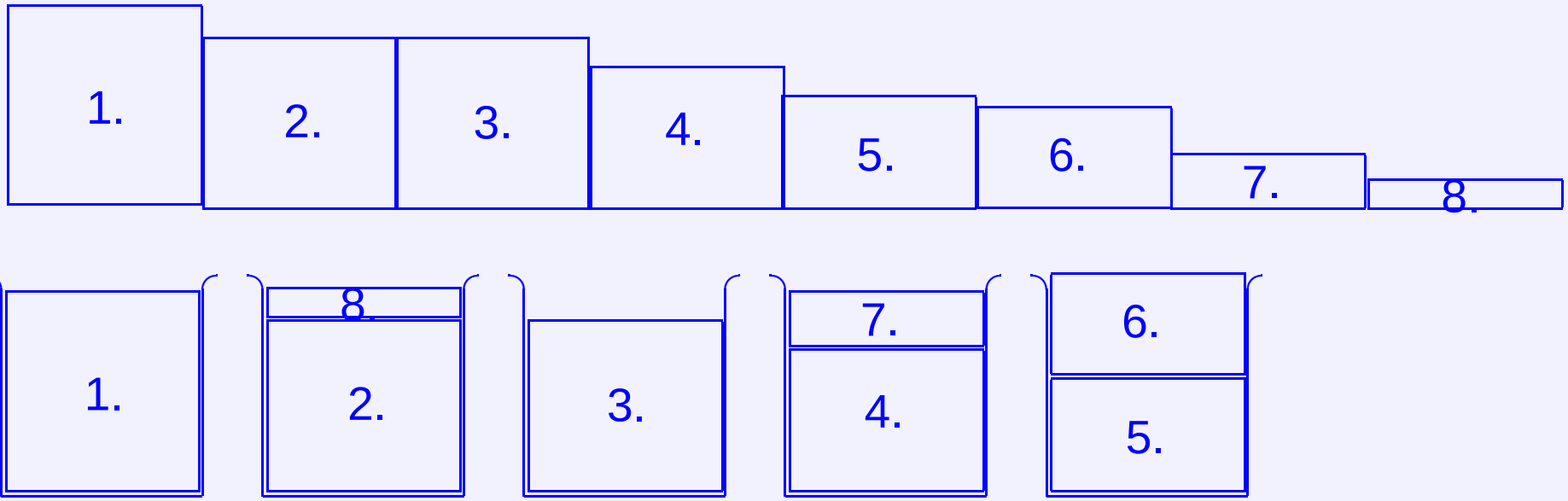


FFD-módszer (first fit decreasing): először rendezzük a súlyokat nem növő sorrendbe, utána alkalmazzuk az FF-módszert.



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 $FFD(I) \geq \frac{11}{9}OPT(I)$. ($\frac{11}{9} = 1.222\ldots$)

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 $FFD(I) \geq \frac{11}{9}OPT(I)$. ($\frac{11}{9} = 1.222\ldots$)

Tétel. [F. de la Vega, G. S. Lueker]
Tetszőleges $\varepsilon > 0$-hoz van olyan P lineáris algoritmus, amire $P(I) \leq (1+\varepsilon)OPT(I)$.

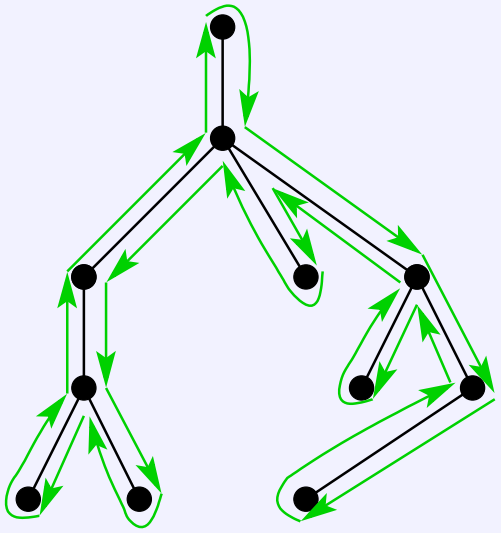
Euklideszi utazó ügynök probléma

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.

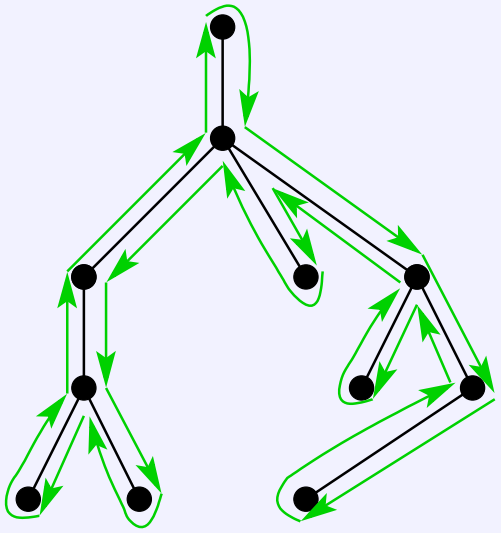
Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal). $\Longrightarrow$



Euklideszi utazó ügynök probléma

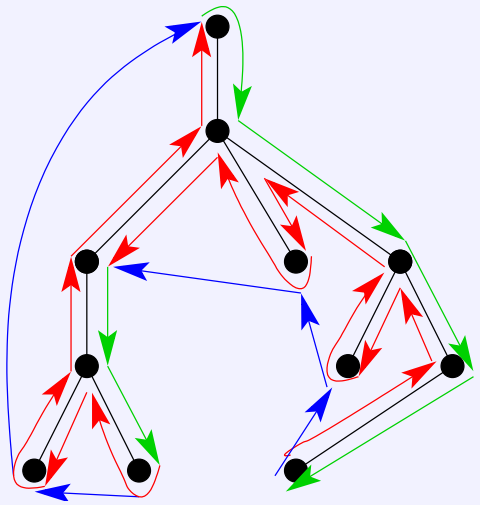
Az n pontú K_n teljes gráf élein adott a nemnegatív értékű d súlyfüggvény. Erre teljesül a háromszög-egyenlőtlenség: tetszőleges különböző u, v, w csúcsokra érvényes a $d(u, w) \leq d(u, v) + d(v, w)$ egyenlőtlenség (az euklideszi feltétel).
A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal). $\Longrightarrow$

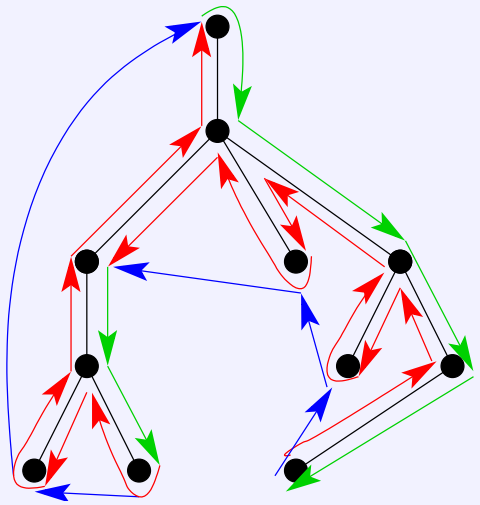


Ennek összsúlya legyen s $\Longrightarrow$ Euler séta hossza $2s$.

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

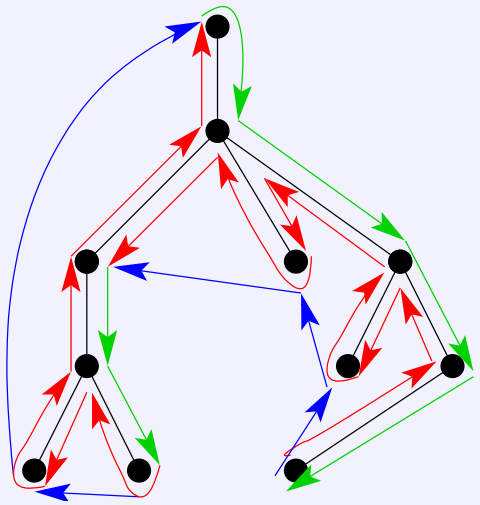


Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ha az optimális Hamilton-körből elhagyunk egy élet $\Longrightarrow$ egy legalább s súlyú feszítőfa

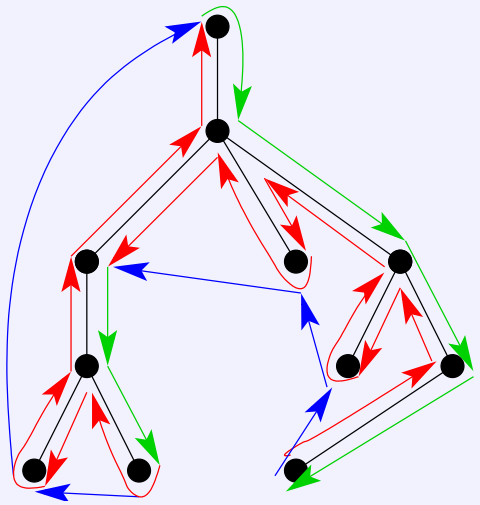
Ez nem Hamilton-kör $\Longrightarrow$ levágjuk a fölösleges részeket, közben rövidítünk is.



Ha az optimális Hamilton-körből elhagyunk egy élet $\Longrightarrow$ egy legalább s súlyú feszítőfa

A módszer legfeljebb $\mathbf{2}$-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 feszítőfa

A módszer legfeljebb $\mathbf{2}$-szer akkora utat ad, mint az optimális.

JAVA animáció: TSP

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.

Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n-változós $f \in \mathbb{Z}[x_1, \ldots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

Véletlent használó módszerek

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

Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n-változós $f \in \mathbb{Z}[x_1, \ldots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

Példa: $f(x_1, x_2, \ldots, x_{2n}) = (x_1 + x_2)(x_3 + x_4) \cdots (x_{2n-1} + x_{2n})$

Véletlent használó módszerek

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

Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n-változós $f \in \mathbb{Z}[x_1, \ldots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

Példa: $f(x_1, x_2, \ldots, x_{2n}) = (x_1 + x_2)(x_3 + x_4) \cdots (x_{2n-1} + x_{2n})$

$$D = \det \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}$$

Véletlent használó módszerek

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

Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n-változós $f \in \mathbb{Z}[x_1, \ldots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

Példa: $f(x_1, x_2, \ldots, x_{2n}) = (x_1 + x_2)(x_3 + x_4) \cdots (x_{2n-1} + x_{2n})$

$$D = \det \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix}$$

Mminél hamarabb szeretnénk találni egy $\alpha = (\alpha_1, \ldots, \alpha_n)$-t, amire $f(\alpha) \neq 0$.

Véletlent használó módszerek

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

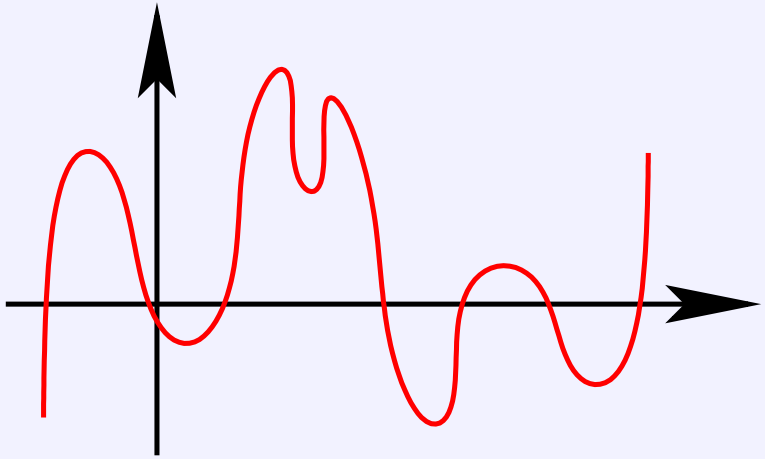
Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n-változós $f \in \mathbb{Z}[x_1, \ldots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

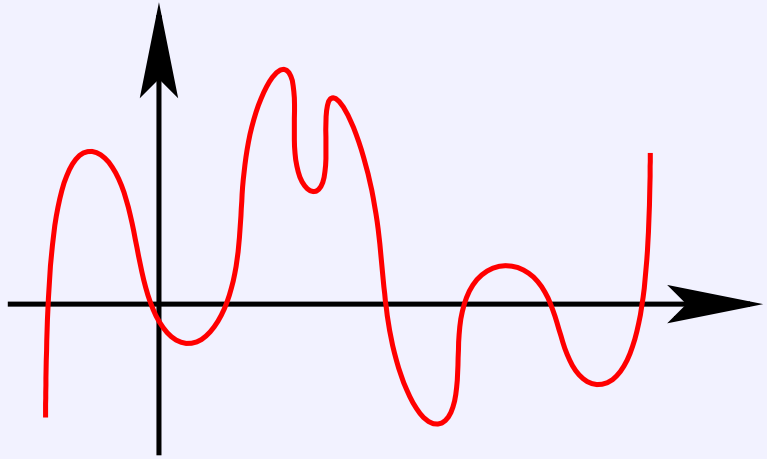
Példa: $f(x_1, x_2, \ldots, x_{2n}) = (x_1 + x_2)(x_3 + x_4) \cdots (x_{2n-1} + x_{2n})$

$$D = \det \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix}$$

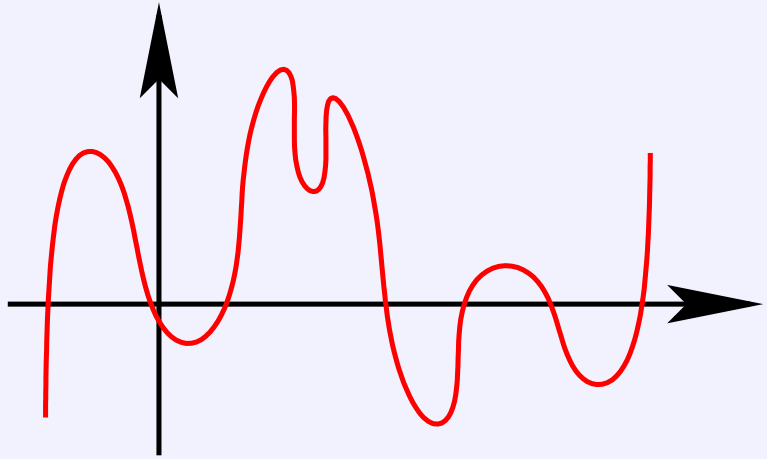
Mminél hamarabb szeretnénk találni egy $\alpha = (\alpha_1, \ldots, \alpha_n)$-t, amire $f(\alpha) \neq 0$.

Pl. egy változóra jól látszik





Tétel. [J. Schwartz lemmája] *Ha* $\deg f \leq d$, *és* $\alpha_1, \ldots, \alpha_n$ *egyenletes eloszlású, egymástól független véletlen elemei az* $\{1, \ldots, N\}$ *számhalmaznak, akkor* $f \not\equiv 0$ *esetén* $Prob(f(\alpha) = 0) \leq \frac{d}{N}$.



Tétel. [J. Schwartz lemmája] *Ha* $\deg f \leq d$, *és* $\alpha_1, \ldots, \alpha_n$ *egyenletes eloszlású, egymástól független véletlen elemei az* $\{1, \ldots, N\}$ *számhalmaznak, akkor* $f \not\equiv 0$ *esetén* $Prob(f(\alpha) = 0) \leq \frac{d}{N}$.

Tétel. *Az* $\{1, 2, \ldots, 2d\}$ *halmazból vett véletlen* n*-komponensű* α *vektor esetén* $Prob(f(\alpha) \neq 0) \geq 1/2$, *ha* $f \not\equiv 0$. *Ekkora halmazból választva tehát legalább* $1/2$ *valószínűséggel adódik tanú. Ha* t*-szer függetlenül választunk ilyen helyettesítést, akkor legalább* $1 - \frac{1}{2^t}$ *valószínűséggel kapunk tanút.*

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$ $M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás
Ha tehát G-ben nincs teljes párosítás, $\Longrightarrow \det M = 0$.

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás
Ha tehát G-ben nincs teljes párosítás, $\Longrightarrow \det M = 0$.
Ha viszont van G-ben teljes párosítás $\Longrightarrow \exists$ nem 0 kifejtési tag

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás
Ha tehát G-ben nincs teljes párosítás, $\Longrightarrow \det M = 0$.
Ha viszont van G-ben teljes párosítás $\Longrightarrow \exists$ nem 0 kifejtési tag
nem ejthetik ki egymást, mert bármely kettőben van két különböző változó.

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás
Ha tehát G-ben nincs teljes párosítás, $\Longrightarrow \det M = 0$.
Ha viszont van G-ben teljes párosítás $\Longrightarrow \exists$ nem 0 kifejtési tag
nem ejthetik ki egymást, mert bármely kettőben van két különböző változó.

Az előző módszerrel eldönthetjük, hogy $\det M = 0$ igaz-e.

Alkalmazás

Randomizált módszer teljes párosítás keresésére páros gráfban.

Legyen $G = (L, U; E)$ páros gráf, $L = \{l_1, \ldots, l_n\}$ és $U = \{u_1, \ldots, u_n\}$
$M = (m_{ij})$ n-szer n-es mátrix $\Longrightarrow$

$$m_{ij} = \begin{cases} x_{ij} & \text{ha } (l_i, u_j) \in E, \\ 0 & \text{különben.} \end{cases}$$

Tétel. *G-ben akkor és csak akkor van teljes párosítás ha $\det M \neq 0$.*

Bizonyítás: A determináns egy tagja $\Longrightarrow \pm m_{1\pi(1)} m_{2\pi(2)} \cdots m_{n\pi(n)}$
Ha nem 0 $\Longrightarrow (l_i, u_{\pi(i)}) \in E$, $i = 1, \ldots, n$, $\Longrightarrow$ teljes párosítás
Ha tehát G-ben nincs teljes párosítás, $\Longrightarrow \det M = 0$.
Ha viszont van G-ben teljes párosítás $\Longrightarrow \exists$ nem 0 kifejtési tag
nem ejthetik ki egymást, mert bármely kettőben van két különböző változó.

Az előző módszerrel eldönthetjük, hogy $\det M = 0$ igaz-e.

Hasonlóan megy nem páros gráfokra is.

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 $a^{m-1} \equiv 1 \pmod{m}$, 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 $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

gyors hatványozással ez 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 $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

gyors hatványozással ez 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 $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

gyors hatványozással ez gyorsan végrehajtható

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

Pl.: $m = 21 = 7 \cdot 3$ és $a = 2 \Longrightarrow a$ 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 $a^{m-1} \equiv 1 \pmod{m}$, akkor a válasz „$m$ valószínűleg prím”, különben a válasz „m összetett”.

gyors hatványozással ez gyorsan végrehajtható

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

Pl.: $m = 21 = 7 \cdot 3$ és $a = 2 \Longrightarrow a$ az m Fermat-tanúja, hiszen $2^{20} \equiv 4 \pmod{21}$.

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.*

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 $\Longrightarrow c_i^{m-1} \equiv 1 \pmod m$

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.

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

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
ac_i mind különbözőek lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú ✓

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
ac_i mind különbözőek lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú ✓

Vannak olyan számok, amiknek nincs tanújuk $\Longrightarrow$ Carmichael-számok

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
ac_i mind különbözőek lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú ✓

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

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
ac_i mind különbözőek lesznek $\Longrightarrow$ legalább annyi tanú, mint nem tanú ✓

Vannak olyan számok, amiknek nincs tanújuk $\Longrightarrow$ 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

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.

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

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.

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

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.

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

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.

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

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.

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”.

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?

Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel*

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$
írógép-paradoxon

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$
írógép-paradoxon

$n = 2^k - 10$ alakú számok bináris kódja $k = \log_2 n$ hosszú

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$
írógép-paradoxon

$n = 2^k - 10$ alakú számok bináris kódja $k = \log_2 n$ hosszú
Viszont a $2^k - 10$ kifejezés hossza csak $\log_2 \log_2 n +$ konstans.

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$
írógép-paradoxon

$n = 2^k - 10$ alakú számok bináris kódja $k = \log_2 n$ hosszú
Viszont a $2^k - 10$ kifejezés hossza csak $\log_2 \log_2 n +$ konstans.

Rögzítsünk egy U univerzális Turing-gépet, és értelmezzük az $x \in I^*$ szó bonyolultságát mint a legrövidebb $y\#z$ input szó hosszát, melyre U az x szót számítja ki.

Kolmogorov-bonyolultság

Milyen röviden lehet leírni valamit?
Tekintsük azokat a természetes számokat, amelyeket magyar nyelven legfeljebb 100 billentyű-leütéssel definiálni lehet.
A billentyűk száma véges $\Longrightarrow$ ezen számok halmaza is véges $\Longrightarrow$ Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.
$\Longrightarrow$ *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* $\Longleftarrow$ egy száznál rövidebb jelsorozat $\lightning$
írógép-paradoxon

$n = 2^k - 10$ alakú számok bináris kódja $k = \log_2 n$ hosszú
Viszont a $2^k - 10$ kifejezés hossza csak $\log_2 \log_2 n +$ konstans.

Rögzítsünk egy U univerzális Turing-gépet, és értelmezzük az $x \in I^*$ szó bonyolultságát mint a legrövidebb $y\#z$ input szó hosszát, melyre U az x szót számítja ki.
Az U gép választásától nagy mértékben független, és aszimptotikus értelemben jó közelítését adja az „optimumnak”.

Definíció. *Legyen M egy TG ami az $f_M : I^* \to I^*$ parciális függvényt számolja ki. Jelöljük $C_M(x)$-szel annak a legrövidebb bemenő szónak a hosszát, mellyel elindítva M az x szót adja eredményül:*

$$C_M(x) = \begin{cases} \min\{|y| : \ y \in I^*, \ f_M(y) = x\} & \text{ha ilyen } y \text{ létezik,} \\ \infty & \text{különben.} \end{cases}$$

Definíció. *Legyen M egy TG ami az $f_M : I^* \to I^*$ parciális függvényt számolja ki. Jelöljük $C_M(x)$-szel annak a legrövidebb bemenő szónak a hosszát, mellyel elindítva M az x szót adja eredményül:*

$$C_M(x) = \begin{cases} \min\{|y| : \ y \in I^*, \ f_M(y) = x\} & \text{ha ilyen } y \text{ létezik,} \\ \infty & \text{különben.} \end{cases}$$

A $C_M(x)$ szám méri, hogy x mennyire nyomható össze akkor, ha a kibontást, vagyis az összenyomott szó visszafejtését az M algoritmus végzi.

Definíció. *Legyen M egy TG ami az $f_M : I^* \to I^*$ parciális függvényt számolja ki. Jelöljük $C_M(x)$-szel annak a legrövidebb bemenő szónak a hosszát, mellyel elindítva M az x szót adja eredményül:*

$$C_M(x) = \begin{cases} \min\{|y| : \ y \in I^*, \ f_M(y) = x\} & \text{ha ilyen } y \text{ létezik,} \\ \infty & \text{különben.} \end{cases}$$

A $C_M(x)$ szám méri, hogy x mennyire nyomható össze akkor, ha a kibontást, vagyis az összenyomott szó visszafejtését az M algoritmus végzi.
konkrét x-re $\Longrightarrow \exists\ M_1$ gép, hogy $C_{M_1}(x) = 0$

Definíció. *Legyen M egy TG ami az $f_M : I^* \to I^*$ parciális függvényt számolja ki. Jelöljük $C_M(x)$-szel annak a legrövidebb bemenő szónak a hosszát, mellyel elindítva M az x szót adja eredményül:*

$$C_M(x) = \begin{cases} \min\{|y| : \ y \in I^*, \ f_M(y) = x\} & \text{ha ilyen } y \text{ létezik,} \\ \infty & \text{különben.} \end{cases}$$

A $C_M(x)$ szám méri, hogy x mennyire nyomható össze akkor, ha a kibontást, vagyis az összenyomott szó visszafejtését az M algoritmus végzi.
konkrét x-re $\Longrightarrow \exists\ M_1$ gép, hogy $C_{M_1}(x) = 0$
és $\exists\ M_2$ gép, hogy $C_{M_2}(x) = \infty$.

Definíció. *Legyen M egy TG ami az $f_M : I^* \to I^*$ parciális függvényt számolja ki. Jelöljük $C_M(x)$-szel annak a legrövidebb bemenő szónak a hosszát, mellyel elindítva M az x szót adja eredményül:*

$$C_M(x) = \begin{cases} \min\{|y| : \ y \in I^*, \ f_M(y) = x\} & \text{ha ilyen } y \text{ létezik,} \\ \infty & \text{különben.} \end{cases}$$

A $C_M(x)$ szám méri, hogy x mennyire nyomható össze akkor, ha a kibontást, vagyis az összenyomott szó visszafejtését az M algoritmus végzi.
konkrét x-re $\Longrightarrow \exists\ M_1$ gép, hogy $C_{M_1}(x) = 0$
és $\exists\ M_2$ gép, hogy $C_{M_2}(x) = \infty$.

Tétel. [invariancia-tétel] *Legyen U egy univerzális Turing-gép. Ekkor tetszőleges M Turing-gépre létezik egy (csak M-től függő) $c_M \in \mathbb{Z}^+$ állandó, mellyel minden $x \in I^*$ szóra teljesül a következő egyenlőtlenség:*

$$C_U(x) \leq C_M(x) + c_M.$$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

legyen y egy legrövidebb szó, amiből M az x-et bontja ki:

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

legyen y egy legrövidebb szó, amiből M az x-et bontja ki:

$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

legyen y egy legrövidebb szó, amiből M az x-et bontja ki:

$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$

$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

legyen y egy legrövidebb szó, amiből M az x-et bontja ki:

$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$

$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$

legyen y egy legrövidebb szó, amiből M az x-et bontja ki:

$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$

$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

$\Longrightarrow c_M = |w\#|$ ✓

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$
legyen y egy legrövidebb szó, amiből M az x-et bontja ki:
$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$
$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

$\Longrightarrow c_M = |w\#|$ $\surd$

Tétel. *Legyenek U_1 és U_2 univerzális Turing-gépek, melyek input abc-je $I = \{0,1\}$. Ekkor van olyan $c = c_{U_1,U_2}$ állandó, hogy minden $x \in I^*$ szóra*

$$|C_{U_1}(x) - C_{U_2}(x)| \leq c.$$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$
legyen y egy legrövidebb szó, amiből M az x-et bontja ki:
$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$
$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

$\Longrightarrow c_M = |w\#|$ $\surd$

Tétel. *Legyenek U_1 és U_2 univerzális Turing-gépek, melyek input abc-je $I = \{0,1\}$. Ekkor van olyan $c = c_{U_1,U_2}$ állandó, hogy minden $x \in I^*$ szóra*

$$|C_{U_1}(x) - C_{U_2}(x)| \leq c.$$

Bizonyítás: $C_{U_1}(x) \leq C_{U_2}(x) + c_{U_2}$ és $C_{U_2}(x) \leq C_{U_1}(x) + c_{U_1}$ $\surd$

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$
legyen y egy legrövidebb szó, amiből M az x-et bontja ki:
$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$
$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

$\Longrightarrow c_M = |w\#|$ $\surd$

Tétel. *Legyenek U_1 és U_2 univerzális Turing-gépek, melyek input abc-je $I = \{0,1\}$. Ekkor van olyan $c = c_{U_1,U_2}$ állandó, hogy minden $x \in I^*$ szóra*

$$|C_{U_1}(x) - C_{U_2}(x)| \leq c.$$

Bizonyítás: $C_{U_1}(x) \leq C_{U_2}(x) + c_{U_2}$ és $C_{U_2}(x) \leq C_{U_1}(x) + c_{U_1}$ $\surd$

Definíció. *Rögzítsünk egy U univerzális Turing gépet. Legyen $x \in I^*$. A $C(x) := C_U(x)$ mennyiség az x szó* Kolmogorov-bonyolultsága.

Bizonyítás: M gép leírása $\Longrightarrow w \in I^*$
legyen y egy legrövidebb szó, amiből M az x-et bontja ki:
$\Longrightarrow y \in I^*$, $f_M(y) = x$, és $|y| = C_M(x)$
$\Longrightarrow U$ a $w\#y$ bemeneten x-et adja eredményül $\Longrightarrow$

$$C_U(x) \leq |w\#y| = |w\#| + |y| = |w\#| + C_M(x)$$

$\Longrightarrow c_M = |w\#|$ $\surd$

Tétel. *Legyenek U_1 és U_2 univerzális Turing-gépek, melyek input abc-je $I = \{0,1\}$. Ekkor van olyan $c = c_{U_1,U_2}$ állandó, hogy minden $x \in I^*$ szóra*

$$|C_{U_1}(x) - C_{U_2}(x)| \leq c.$$

Bizonyítás: $C_{U_1}(x) \leq C_{U_2}(x) + c_{U_2}$ és $C_{U_2}(x) \leq C_{U_1}(x) + c_{U_1}$ $\surd$

Definíció. *Rögzítsünk egy U univerzális Turing gépet. Legyen $x \in I^*$. A $C(x) := C_U(x)$ mennyiség az x szó* Kolmogorov-bonyolultsága.

$C(0010) = ?$

$C(0010) = ? \implies C$ függvény nem rekurzív

$C(0010) = ?$ $\Longrightarrow$ C függvény nem rekurzív

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol $x_1, x_2, \ldots$ növekvő hosszúságú I^*-beli szavak sorozata.

$C(0010) = ?$ $\Longrightarrow$ C függvény nem rekurzív

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol $x_1, x_2, \ldots$ növekvő hosszúságú I^*-beli szavak sorozata.

Pl. az $n = 2^k - 10$ alakú számokra $C(n) \leq \log_2 \log_2 n + c'$ teljesül alkalmas c' állandóval.

$C(0010) = ?$ $\Longrightarrow$ C függvény nem rekurzív

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol $x_1, x_2, \ldots$ növekvő hosszúságú I^*-beli szavak sorozata.

Pl. az $n = 2^k - 10$ alakú számokra $C(n) \leq \log_2 \log_2 n + c'$ teljesül alkalmas c' állandóval.

Tétel. *Legyen $x \in I^*$. Ekkor $C(x) \leq |x| + k$, ahol k egy x-től független állandó.*

$C(0010) = ?$ $\Longrightarrow$ C függvény nem rekurzív

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol $x_1, x_2, \ldots$ növekvő hosszúságú I^*-beli szavak sorozata.

Pl. az $n = 2^k - 10$ alakú számokra $C(n) \leq \log_2 \log_2 n + c'$ teljesül alkalmas c' állandóval.

Tétel. *Legyen $x \in I^*$. Ekkor $C(x) \leq |x| + k$, ahol k egy x-től független állandó.*

Bizonyítás: x-hez hozzá kell írni egy semmit nem csináló TG kódját.

$C(0010) = ?$ $\Longrightarrow$ C függvény nem rekurzív

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol $x_1, x_2, \ldots$ növekvő hosszúságú I^*-beli szavak sorozata.

Pl. az $n = 2^k - 10$ alakú számokra $C(n) \leq \log_2 \log_2 n + c'$ teljesül alkalmas c' állandóval.

Tétel. *Legyen $x \in I^*$. Ekkor $C(x) \leq |x| + k$, ahol k egy x-től független állandó.*

Bizonyítás: x-hez hozzá kell írni egy semmit nem csináló TG kódját.

Definíció. *Az $x \in I^*$ szó* összenyomhatatlan*, ha $C(x) \geq |x|$.*

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó.*

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1}-1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n-8$.*

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van:

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

$$H_k = \{x \in I^* : \ C(x) \leq k\}$$

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

$$H_k = \{x \in I^* : \ C(x) \leq k\}$$

$k = n - 1 \implies n$ hosszú szavak száma $2^n \implies H_{n-1}$-ben legfeljebb $2^n - 1$ szó van

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1} - 1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n - 8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

$$H_k = \{x \in I^* : \ C(x) \leq k\}$$

$k = n - 1 \implies n$ hosszú szavak száma $2^n \implies H_{n-1}$-ben legfeljebb $2^n - 1$ szó van
$\Longrightarrow$ Van legalább n hosszú kódú szó. $\surd$

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1}-1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n-8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

$$H_k = \{x \in I^* : \ C(x) \leq k\}$$

$k = n-1 \implies n$ hosszú szavak száma $2^n \implies H_{n-1}$-ben legfeljebb $2^n - 1$ szó van
$\Longrightarrow$ Van legalább n hosszú kódú szó. $\surd$

A H_{n-8} halmaznak legfeljebb $2^{n-7} - 1 < 2^{n-7}$ eleme van.

Tétel. *Legyen $k \in \mathbb{Z}^+$. Legfeljebb $2^{k+1}-1$ $x \in I^*$ szó van, melyre $C(x) \leq k$. Következésképpen minden $n \geq 1$ egészre létezik n hosszúságú összenyomhatatlan szó. Ha $n > 8$, akkor az n hosszú I^*-beli szavak több, mint 99 százalékának a Kolmogorov-bonyolultsága nagyobb, mint $n-8$.*

Bizonyítás: Egyforma y-okra egyforma lesz $f_U(y) = x$ is.
$\Longrightarrow$ legfeljebb annyi k-nál nem hosszabb kódú x lehet, amennyi k-nál nem hosszabb szó van: $1 + 2 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$

$$H_k = \{x \in I^* : \ C(x) \leq k\}$$

$k = n-1 \Longrightarrow n$ hosszú szavak száma $2^n \Longrightarrow H_{n-1}$-ben legfeljebb $2^n - 1$ szó van
$\Longrightarrow$ Van legalább n hosszú kódú szó. $\surd$

A H_{n-8} halmaznak legfeljebb $2^{n-7} - 1 < 2^{n-7}$ eleme van.
$\Longrightarrow$ A kedvezőtlen esetek aránya az n hosszú szavak között legfeljebb $2^{n-7}/2^n = 1/128 < 1/100$. $\surd$