

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

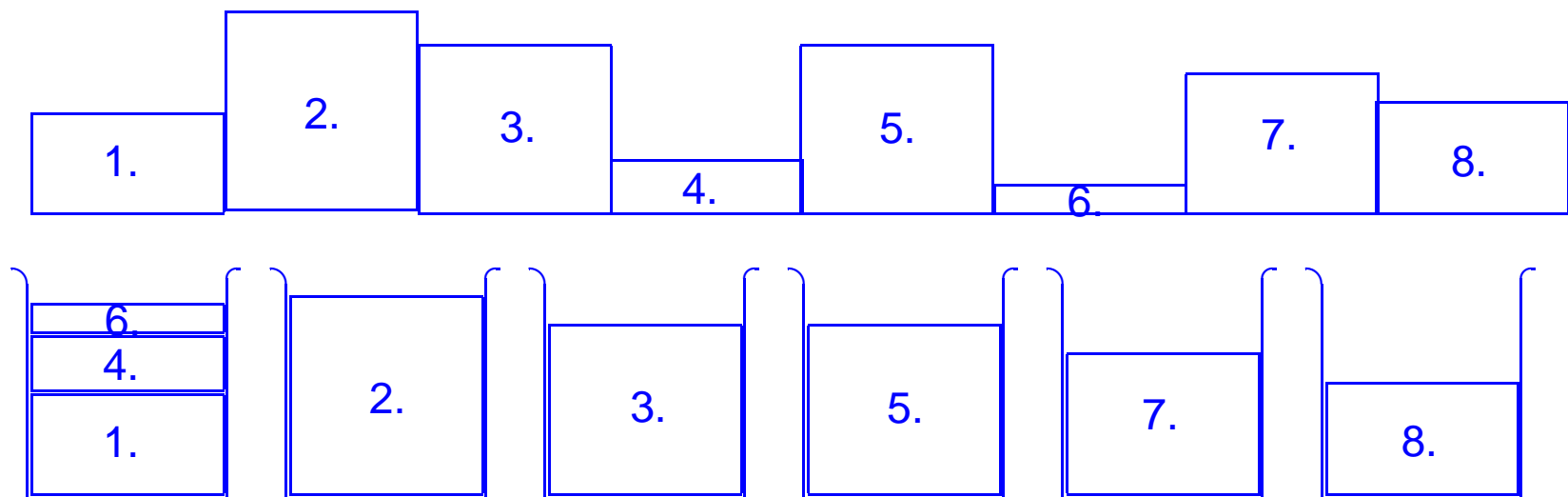
Hátha nem szükséges pontos megoldás, elég az optimumtól nem túl messze levő is.

Ládapakolás: Adottak az s_1, \dots, 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 $1, 2, \dots, m$ egészekkel.

Tegyük fel, hogy az s_1, \dots, 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 $FF(I) \leq 2OPT(I)$.

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 $\lceil 2x \rceil \leq 2\lceil x \rceil$

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



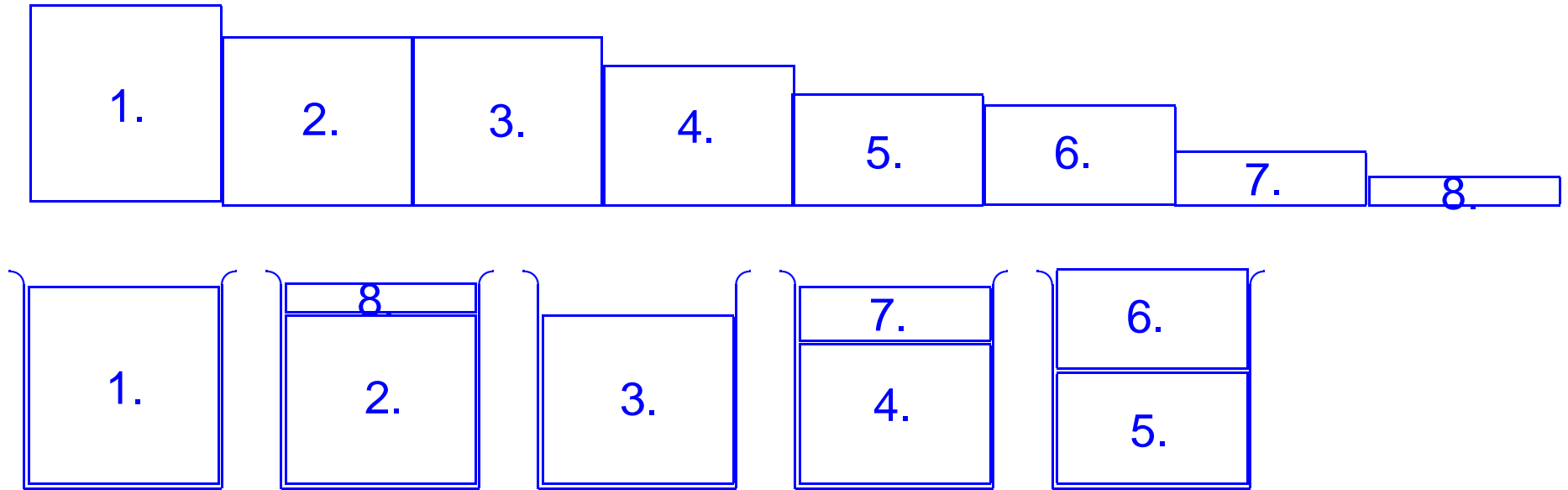
Tétel. [D. S. Johnson és munkatársai, 1976]

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

Tétel. [F. de la Vega, G. S. Lueker]

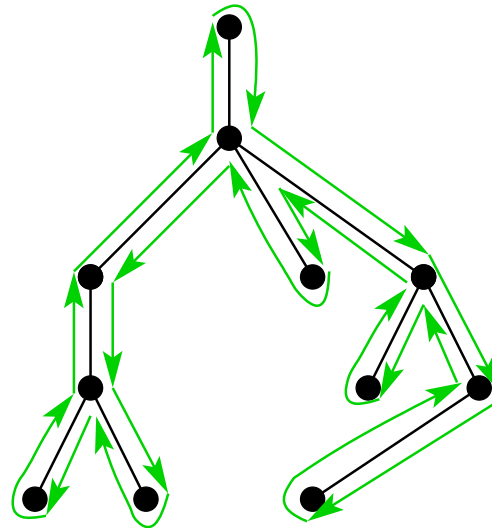
Tetszőleges $\epsilon > 0$ -hoz van olyan P lineáris algoritmus, amire $P(I) \leq (1 + \epsilon)OPT(I)$.

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).

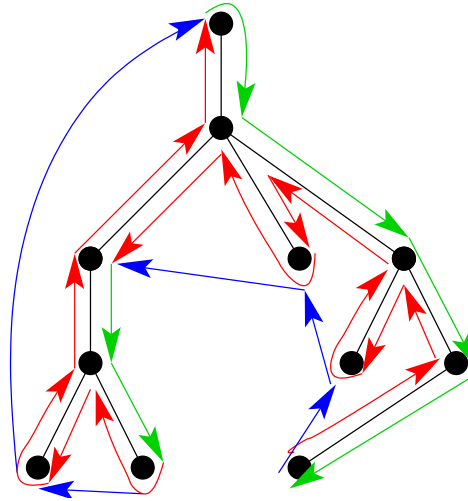
A cél egy minimális összsúlyú Hamilton-kör keresése.

Keresünk egy minimális összsúlyú feszítőfát (pl. Kruskal). \implies



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

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



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

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

JAVA animáció: TSP

Véletlent használó módszerek

Előny: Gyorsabb lehet.

Hátrány: Kis valószínűséggel hibás választ kapunk.

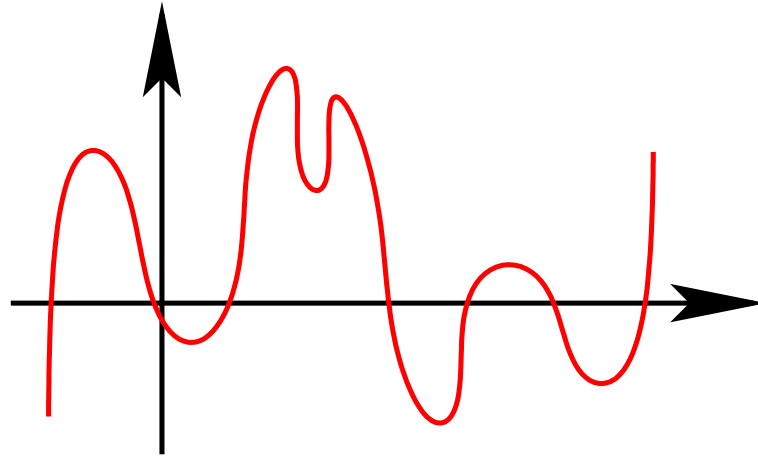
Probléma: Adott behelyettesítéssel (**fekete dobozzal**) egy n -változós $f \in \mathbb{Z}[x_1, \dots, x_n]$ egész együtthatós polinom. Tudjuk, hogy $\deg f \leq d$. El akarjuk dönteni, hogy f azonosan nulla-e.

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

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

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

Pl. egy változóra jól látszik



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

Tétel. Az $\{1, 2, \dots, 2d\}$ halmazból vett véletlen n -komponensű α vektor esetén $\text{Prob}(f(\alpha) \neq 0) \geq 1/2$, 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.

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

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

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

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

Ha nem 0 $\implies (l_i, u_{\pi(i)}) \in E, i = 1, \dots, n, \implies$ teljes párosítás

Ha tehát G -ben nincs teljes párosítás, $\implies \det M = 0$.

Ha viszont van G -ben teljes párosítás $\implies \exists$ 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.

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” \implies ez biztos igaz


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

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 $\implies a^{m-1} \not\equiv 1 \pmod{m}$ és

c_1, c_2, \dots, c_s nem tanúk $\implies c_i^{m-1} \equiv 1 \pmod{m}$

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

$\implies (ac_i)^{m-1} \equiv a^{m-1}c_i^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m} \implies ac_i$ tanú
 ac_i mind különbözőek lesznek \implies legalább annyi tanú, mint nem tanú 

Vannak olyan számok, amiknek nincs tanújuk \implies Carmichael-számok

Pl. $561 = 3 \cdot 11 \cdot 17$

Alford, Granville, Pomerance, 1992 \implies 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

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

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

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

A billentyűk száma véges \implies ezen számok halmaza is véges \implies Van tehát egy legkisebb természetes szám, amit nem lehet definiálni a fenti módon.

\implies *az a legkisebb szám, amely nem definiálható magyar nyelven legfeljebb száz billentyű-leütéssel* \iff egy száznál rövidebb jelsorozat \downarrow
írógép-paradoxon

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

Viszont a $2^k - 10$ kifejezés hossza csak $\log_2 \log_2 n + \text{konstans}$.

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 $f_M : I^* \rightarrow I^*$ 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 $\implies \exists M_1$ 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 $\implies w \in I^*$

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

$$\implies y \in I^*, f_M(y) = x, \text{ és } |y| = C_M(x)$$

$$\implies U \text{ a } w\#y \text{ bemeneten } x\text{-et adja eredményül } \implies$$

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

$$\implies c_M = |w\#| \quad \checkmark$$

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 $C_{U_2}(x) \leq C_{U_1}(x) + c_{U_1}$ \checkmark

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

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

Vizsgálhatjuk a $C(x_n)$ alakú sorozatok növekedési rendjét, ahol x_1, x_2, \dots 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. 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.

\implies legfeljebb annyi k -nál nem hosszabb kódú x lehet, amennyi k -nál nem hosszabb szó van: $1 + 2 + \dots + 2^{k-1} + 2^k = 2^{k+1} - 1$

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

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

\implies Van legalább n hosszú kódú szó. ✓

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

\implies A kedvezőtlen esetek aránya az n hosszú szavak között legfeljebb $2^{n-7}/2^n = 1/128 < 1/100$. ✓