SYMETRIE VE VÝPOČETNÍ SLOŽITOSTI

Libor Barto

16.1.2024
Učená společnost ČR

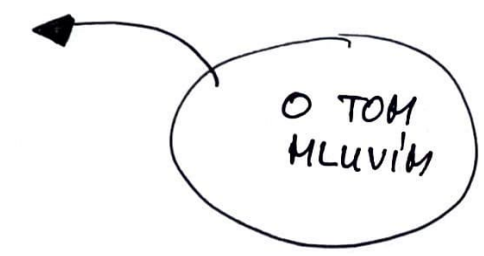
1 O ČEM BUDU MLUVIT

Máme početní úlohu, např.

- vynásob dvě čísla
- spočítej dráhu rakety na Mars
- prolom šifru RSA
- předpověz počasí
- rekonstruuj DNA z nalezených fragmentů
- .....

Základní otázky

- jak zformulovat jako úlohu pro počítač? (vytvořit model)
- jak ji rychle vyřešit? (najít rychlý algoritmus)
  jde to vůbec?
- jak to konkrétně provést? (implementovat)



2 ČASOVÁ SLOŽITOST VÝPOČETNÍCH PROBLÉMŮ

výpočetnú složitost

- místo konkrétní úlohy
  uvažujeme obecnou úlohu

vynásob 137 a 287
dány a, b spočti a·b

výpočetní problém
- specifikovány možné vstupy
- a očekávané výstupy

NÁSOBENÍ

VSTUP: přirozená čísla a, b
VÝSTUP: a·b

- jeho časová složitost:

počet kroků nejlepšího možného algoritmu
v závislosti na velikosti vstupu

počet znaků

v nejhorším případě

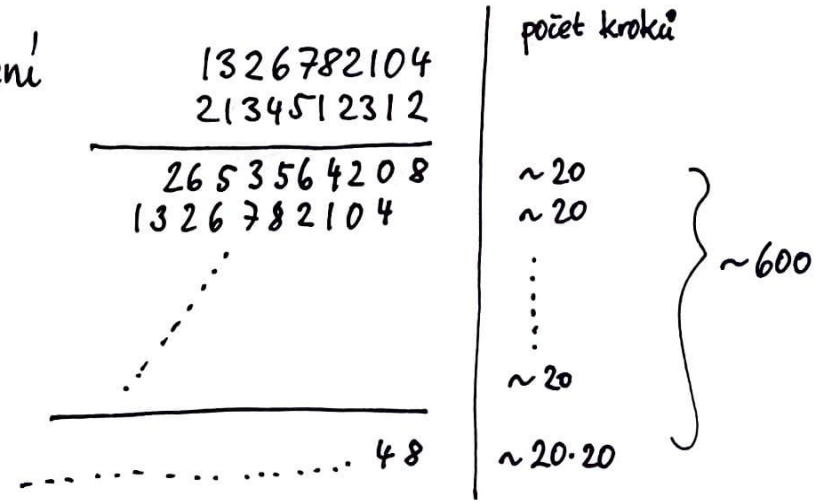
3 NÁSOBENÍ

NÁSOBENÍ

VSTUP: přirozená čísla a, b

VÝSTUP: $a \cdot b$

školské násobení



- algoritmus školského násobení

  vstup velikosti n

  počet kroků $< 2n^2$

  vstup velikosti 20

  počet kroků 600

- nepřesnosti
  - jak je reprezentován vstup?
  - co přesně je „krok algoritmu"? (a „algoritmus"?)

⇒ časová složitost NÁSOBENÍ je $< 2n^2$

- otázky
  - je to rychlé? 2× větší vstup → 4× delší výpočet ✓
  - jde to ještě rychleji? ✓ (!)

4 3 SKUPINY

3 SKUPINY

VSTUP: lidi + kompatibilita
(např. Josef K. může pracovat pouze s Janou A., Petrem B., ...)

VÝSTUP: rozdělení do 3 skupin tak, že v každé skupině jsou všichni kompatibilní (nebo info, že nejde)

naivní algoritmus

pokus	Josef K.	Petra M.	Jana A.	....	počet kroků
1	1	1	1	....	n
2	2	1	1	....	n
3	3	1	1	....	n
4	1	2	1	....	⋮
⋮					n

$\sim 3^n$

- naivní algoritmus
  - vstup velikosti n => časová složitost 3 SKUPINY je $< 3^n$
  - počet kroků $< 3^n$
- otázky
  - je to rychlé? o 1 větší vstup → 3× delší výpočet ✗
  - jde to rychleji? ??? otázka za milion
- správné řešení jde ale rychle zkontrolovat

5 $n^{\text{číslo}}$ vs. číslo^n

n	n^2 (NÁSOBENÍ)	n^3	1.00000001^n	3^n (3 SKUPINY)
5	25	125	1	243
10	100	1000	1	59049
20	400	8000	1	3486784401
50	2500	125000	1	nevejde se (asi 25 číslic)
1000	1 000 000	1 000 000 000	1	asi 500 číslic
⋮				
1 000 000 000	moc	moc	2	strašně moc
hodně	víc	ještě víc	strašně moc	strašně moc

6 EFEKTIVNÍ ŘEŠITELNOST

výpočetní problém je efektivně řešitelný, pokud
jeho časová složitost $<$ číslo $\cdot\, n^{\text{číslo}}$ (např. $2n^2$, $37n^3$, ...)

- je $n^{1000000}$ efektivní?
  je 1.00000001^n neefektivní?
- jen složitost v nejhorším případě
- co např. kvantové počítače?

\+ robustní – např. nepřesnosti zmizí
\+ jednoduchý koncept – vhodný pro lepší pochopení výpočetní složitosti

dvě množiny výpočetních problémů

$\mathcal{P}$
efektivně řešitelné
(např. NÁSOBENÍ $\in \mathcal{P}$)

$\mathcal{NP}$
efektivně zkontrolovatelné
(např. 3 SKUPINY $\in \mathcal{NP}$)

$\mathcal{P} \stackrel{?}{=} \mathcal{NP}$

- snad ne (přece řešit je těžší než zkontrolovat, kolaps inf. bezpečnosti....)
- 1 ze 7 matematických „problémů tisíciletí"
- \$1.000.000 za vyřešení

7 USPOŘÁDÁNÍ

- problémy můžeme uspořádat

  $A \leq B$ A jde efektivně převést na B

  např. 3 SKUPINY $\leq$ 4 SKUPINY

  (jak: přidej člověka nekompatibilního s nikým)

  4 SKUPINY $\leq$ 3 SKUPINY

  (těžší)

  dokonce pro všechny $A \in \mathcal{NP}$

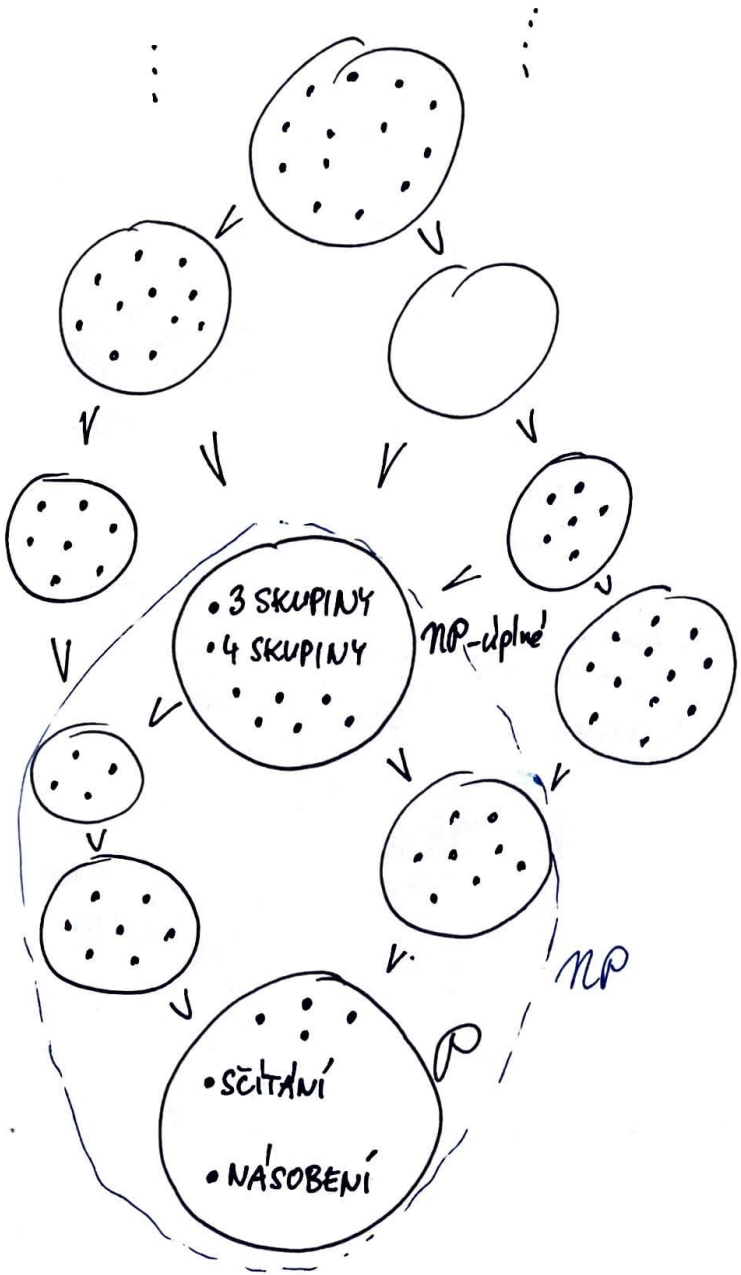
  $A \leq$ 3 SKUPINY ... $\mathcal{NP}$-úplný problém

  $A \sim B$ $A \leq B$ a $B \leq A$

- důležité pro praxi: kde je konkrétní problém na obrázku?

- důležité pro lepší pochopení složitosti:

  - jak popsat všechny problémy v $\bigcirc$? (např. kdy $A \in \mathcal{P}$?)
  - kdy $A \leq B$?
  - jak řešit všechny problémy v $\bigcirc$? ("superalgoritmus")



8 SYMETRIE

3 zásadní otázky
- jak popsat všechny problémy v $\bigcirc$?
- kdy $A \in B$?
- jak řešit všechny problémy v $\bigcirc$?

mají překvapivě dobré odpovědi v jisté množině výpočetních problémů! ~2000–now
(problémy splnitelnosti omezujících podmínek s pevnou konečnou šablonou)

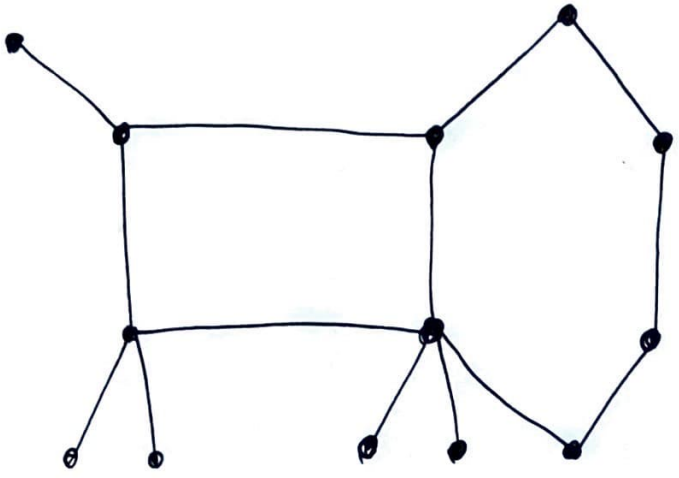
problém ⟶ matematická struktura ⟶ její symetrie

v té množině:
- v $\mathcal{P}$ jsou dostatečně symetrické problémy, ostatní NP-úplné
- $A \leq B$ pokud A je symetričtější (čím symetričtější problém, tím jednodušší)
- superalgoritmus pro všechny $A \in \mathcal{P}$.

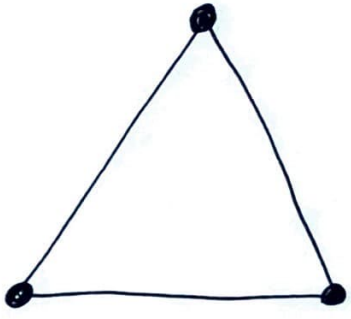
cíl ERC Sy6 POCOCOP (LB, Manuel Bodirsky TU Dresden, Michael Pinsker TU Wien)
- rozšířit na větší množinu
- zlepšit odpovědi

(9) CO JE SYMETRIČTĚJŠÍ?

odpovídá problému 3 SKUPINY



(A)



(B)

správně je (B) ... symetrie, se kterými pracujeme, nejsou úplně očividné

10 ZÁVĚR

co matematici umí: položit zásadní, přesné, konkrétní a krásné otázky (jako $P \stackrel{?}{=} NP$)

co —"— neumí: odpovědět

ale, ale, ale, ... : ...