VĚDA NA HRADĚ

MATEMATICKÁ TEORIE VÝPOČETNÍ SLOŽITOSTI – JE SLOŽITĚJŠÍ PROBLÉM VYŘEŠIT NEŽ ŘEŠENÍ ZKONTROLOVAT?

LIBOR BARTO

5.3.2025

Funded by the European Union (project POCOCOP, ERC Synergy grant No. 101071674). Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ŠÉFOVÁ: Rozdělte zaměstnance do 3 skupin na team building s tím, že

- Alice musí být v jiné skupině než Bertík
- Cecilka —— " —— Dan
- Bertík —— " —— Filoména
- ⋮

Až to budete mít, já to zkontroluju

výpočetní problém

- Máte podat výpověď?

jaká je výpočetní složitost?

- Je úloha šéfové (zkontrolovat řešení) lehčí než vaše?

P versus NP

PLÁN

1. omluvy
2. matematická teorie výpočetní složitosti
   ... a jak vydělat $1'000'000
3. výmluvy
4. sny o symetrii
5. problémy splnitelnosti omezujících podmínek
   ... a jak utrácíme $10'000'000
6. přímluvy

VÝPOČETNÍ SLOŽITOST

- místo konkrétní úlohy
  uvažujeme obecnou úlohu

vynásob 137 a 784

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

NÁSOBENÍ

VSTUP: přirozená čísla a, b
VÝSTUP: $a \cdot b$

```
  1326782104
  2134512312
------------
  2653564208
  1326782104
     .
      .
       .
------------
  ..... 248
```

počet kroků

~ 20
~ 20
⋮
~ 20
~ 20 · 20

~ 600

- algoritmus školské násobení

  vstup velikosti n
  počet kroků $\sim 2n^2$ (nejhůře)

  vstup velikosti ~ 20
  počet kroků ~ 600

  $\Rightarrow$ časová složitost NÁSOBENÍ je $\leq 2n^2$

- otázky
  - je to efektivní? 2× větší vstup ⇒ 4× delší výpočet ✓
  - jde to ještě rychleji? ✓

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

3 SKUPINY

VSTUP : lidi + nekompatibility
(např. Alice, Bertík; Cecilka, Dan ...)

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

VÝSTUP verze 2 : jde to?

naivní algoritmus

pokus	Alice	Bertík	Cecilka ...	počet kroků
1	1	1	1	~n
2	2	1	1	
3	3	1	1	
4	1	2	1	~3^n
⋮				
$3^{\#lidí}$				~n

- naivní algoritmus : vstup velikosti n
  počet kroků ~ 3^n => časová složitost 3SKUPINY je $\leq 3^n$
- – je to efektivní? o 1 větší vstup => 3× delší výpočet ×
  – jde to efektivně? ??? otázka za milion
- správné řešení jde ale rychle zkontrolovat
- varianty : 2SKUPINY (jde efektivně)
  4SKUPINY, 5SKUPIN, ... (???)

$n^{\text{číslo}}$ versus číslo^n

	NÁSOBENÍ			3 SKUPINY
n	n^2	n^3	1.000000001^n	3^n
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	1000000	1000000000	1	asi 500 číslic
⋮				
1000000000	moc	moc	2	straaašně moc
hodně	víc	ještě víc	straaašně moc	straaaašně moc

ROZLOŽ

VSTUP: přirozené číslo a

VÝSTUP: rozklad a na součin prvočísel

VSTUP: 15

VÝSTUP: $3 \cdot 5$

- správné řešení jde efektivně zkontrolovat
  (to je jasné pro jednodušší variantu, kdy víme kolik prvočísel dostaneme)
- naivní algoritmus $\Rightarrow$ časová složitost $\leq 10^{\sqrt{n}}$
- je to efektivní? ✗
- jde to efektivně?
  - snad NE!
  - šifrovací protokol RSA by se dal prolomit

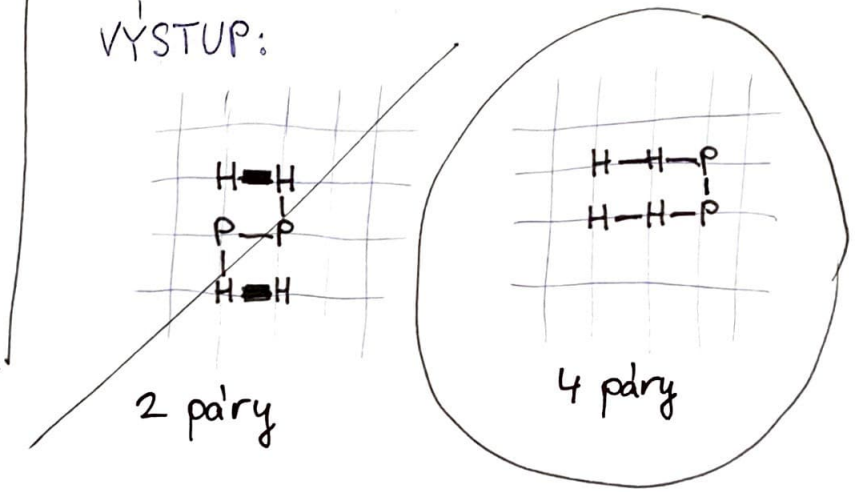
SLOŽ BÍLKOVINU

VSTUP: řetězec písmen H, P

VÝSTUP: složení do čtvercové mřížky s co nejvíce sousedními H–H páry

VSTUP: H-H-P-P-H-H

VÝSTUP:



zjednodušení VSTUP: …., k
VÝSTUP: složení s alespoň k HH páry

- lze efektivně zkontrolovat
- jde vyřešit efektivně? … taky otázka za milion
- přírodě to jde: problém je velmi zjednodušenou variantou skládání bílkovin

$\mathcal{P}$ VERSUS $\mathcal{NP}$

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

$\mathcal{P}$ množina všech efektivně řešitelných výpočetních problémů

obsahuje např. NÁSOBENÍ, 2SKUPINY

$\mathcal{NP}$ množina všech výpočetních problémů, jejichž řešení jde efektivně zkontrolovat

obsahuje např. NÁSOBENÍ, 3SKUPINY, ROZLOŽ, SLOŽ BÍLKOVINU

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

- snad ne (přece řešit je těžší než kontrolovat, RSA, ...)
- I ze 7 matematických „problémů tisíciletí"
- $1'000'000 za vyřešení

REDUKCE

2h

NP

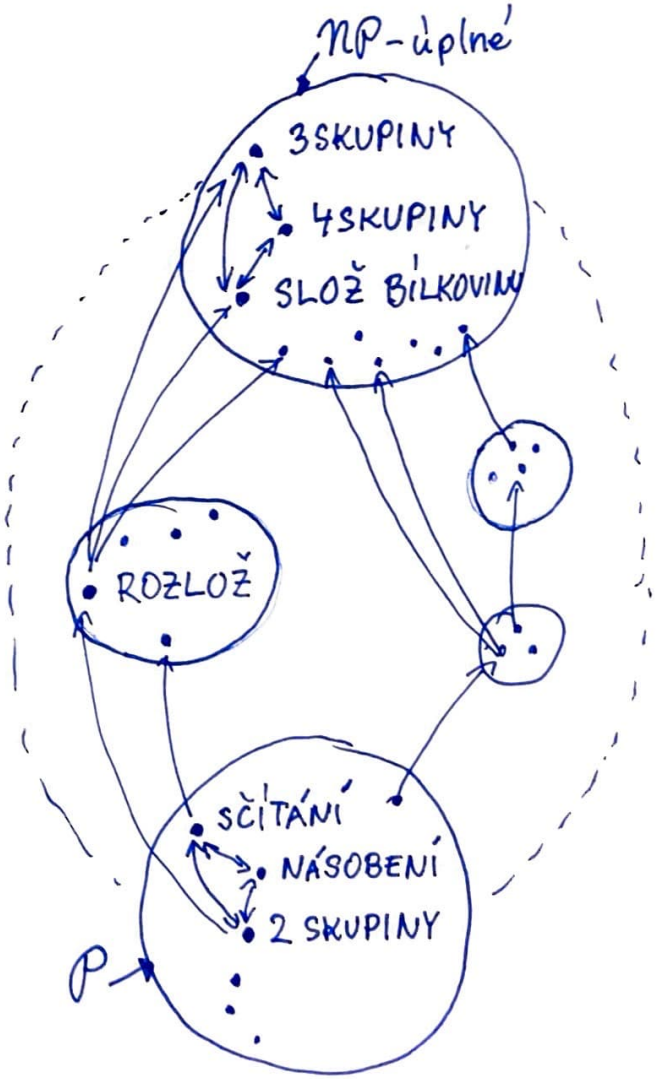
$A \longrightarrow B$ problém A lze efektivně převést (redukovat) na problém B => pak A je „lehčí" než B

- např. 3SKUPINY $\longrightarrow$ 4SKUPINY (snadné)
  4SKUPINY $\longrightarrow$ 3SKUPINY (těžší – DÚ)

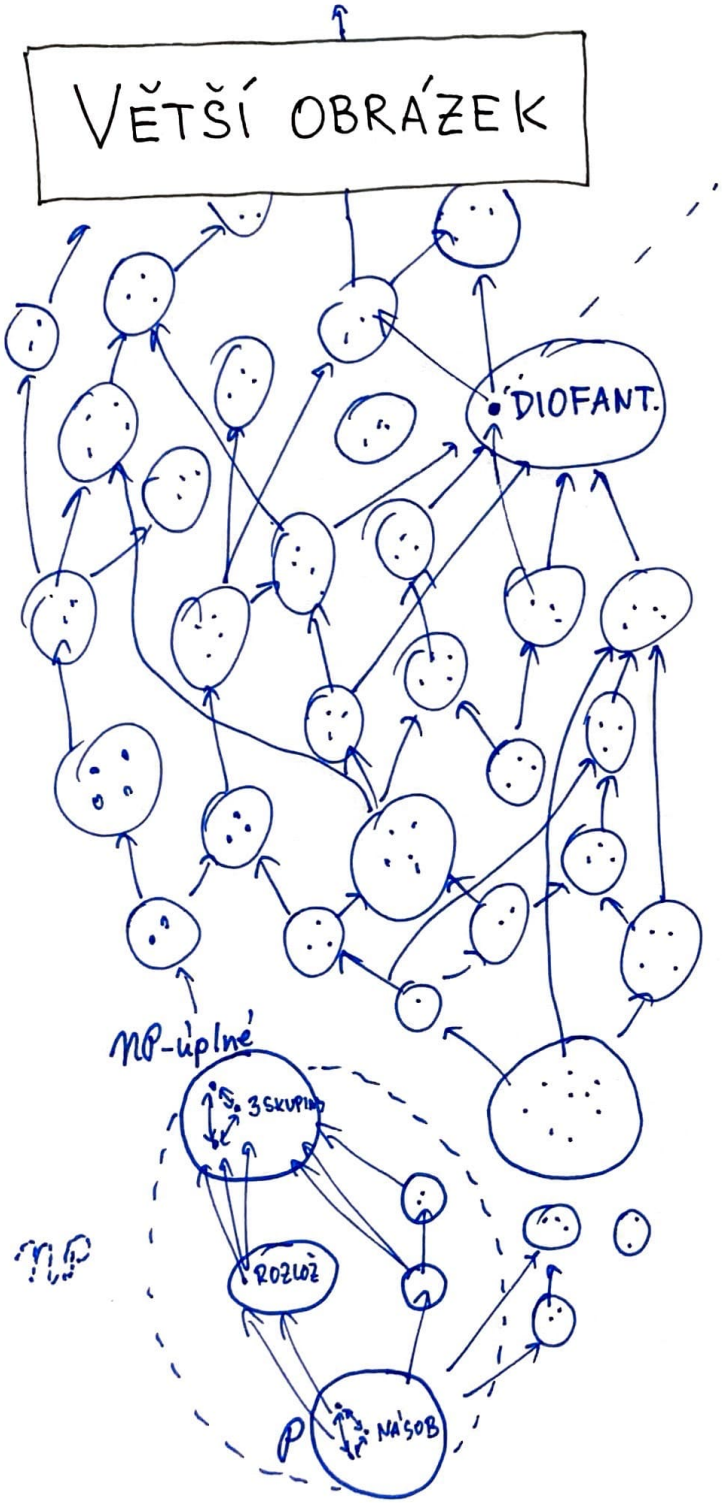
- 3SKUPINY $\leftrightarrow$ 4SKUPINY $\leftrightarrow$ SLOŽ BÍLKOVINU

3SKUPINY jsou *NP-úplný problém*:
pro všechny A v NP je $A \longrightarrow$ 3SKUPINY

=> P = NP právě tehdy, když
3SKUPINY jdou efektivně řešit



VĚTŠÍ OBRÁZEK



DIOFANTICKÉ ROVNICE

VSTUP: soustava rovnic, kde smíme používat $+, \cdot, 0, 1$

např. $x^2 = y$
$y + z = 1$
$x^2 + z^2 + u^2 = 1$
⋮

VÝSTUP: celočíselné řešení

↑ žádný algoritmus neexistuje

CÍL lépe pochopit obrázek

konkrétní otázky
- např. kde je SLOŽ BÍLKOVINU? (odpověď: NP-úplný)
- např. je 3SKUPINY $\in P$? (? ekvivalentní $P = NP$)

obecnější otázky
- jak popsat všechny problémy v ◯? (např. kdy $A \in P$?)
- kdy $A \longrightarrow B$?
- jak řešit všechny problémy v ◯? („superalgoritmus")

VÝMLUVY

námitky proti „efektivně řešitelný"

- je $n^{1000000}$ efektivní?
- je 1.000000001^n neefektivní?
- jen složitost v nejhorším případě
- co např. kvantové počítače?

=> má to svoje výhody, ale je to k ničemu

→ robustní a jednoduchý koncept
(např. zmizí rozdíly v reprezentaci vstupu
konkrétní implementaci)

proč to má smysl?

→ nemyslím si to jen já
($P = NP$ je „problém tisíciletí")

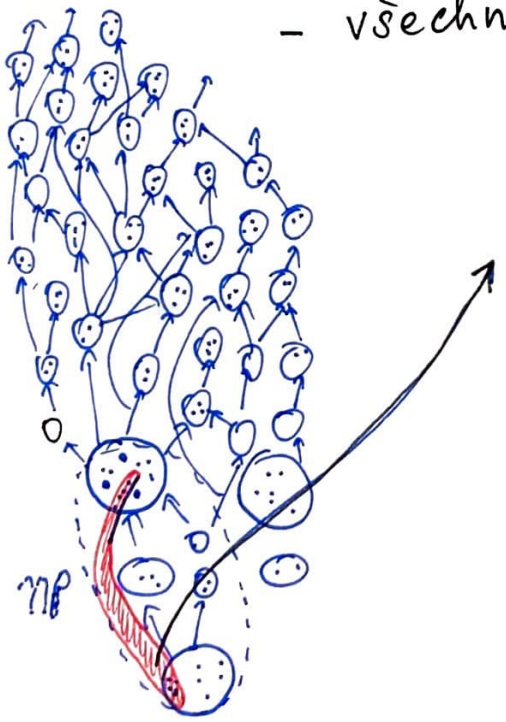
- lepší pochopení světa
- dlouhodobý přínos
- nová matika

SNY O SYMETRII

výpočetní problém ⇝ matematický objekt ⇝ jeho symetrie

odpovědi na obecné otázky

- problém je v ◯ (např. P) právě když je tak a tak symetrický
- $A \to B$ právě když A je symetričtější než B
- všechny problémy v ◯ (např. P) se vyřeší tím a tím superalgoritmem



tady je sen skutečností !

problémy splnitelnosti omezujících podmínek s konečnou šablonou

CSP

5a

Constraint **S**atisfaction **P**roblem
= Problém splnitelnosti omezujících podmínek

CSP

VSTUP: H ... povolené hodnoty proměnných
seznam omezujících podmínek pro proměnné

VÝSTUP: (varianty problému)
- hodnoty pro proměnné, které splňují všechny omezující podmínky
- existují takové hodnoty?
- hodnoty ..... splňují maximum omezujících podmínek
- hodnoty ... splňují 70% maxima ...

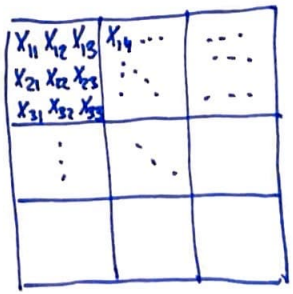
příklady vstupů

- H celá čísla
  $x^2 = y$
  $y + z = 1$
  $x^2 + z^2 + u^2 = 1$
  ⋮
  DIOFANT

- H 1, 2, 3
  $x_{Alice} \neq x_{Bertík}$
  $x_{cecilka} \neq x_{Dan}$
  ⋮
  3SKUPINY

- H 1, 2, ..., 9
  $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}, x_{31}, x_{32}, x_{33}$
  vše různé

SUDOKU



CSP S KONEČNOU ŠABLONOU

příklad

šablona

H povolené hodnoty (konečně mnoho) — H 1,2,3

R seznam dvojic hodnot — R 12, 13, 21, 23, 31, 32

CSP s ŠABLONOU H, R

VSTUP: seznam omezujících podmínek tvaru
xy musí být v R

VÝSTUP: hodnoty pro proměnné, které
splňují všechny omezující podmínky

x_{Alice} $x_{Bertík}$ musí být v R

$x_{Cecilka}$ x_{Dan} — " —

...

(totéž jako $x_{Alice} \neq x_{Bertík}$, $x_{Cecilka} \neq x_{Dan}$)

pro každou šablonu máme jeden výpočetní problém

3 SKUPINY

SYMETRIE

5c

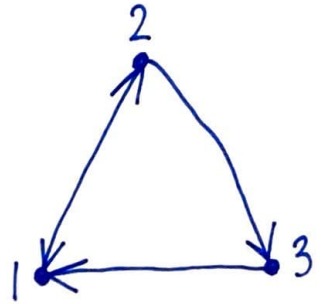
- šablona ⇝ obrázek

  puntíky ... hodnoty z H

  šipky ... dvojice z R

H 1,2,3

R 12, 21, 23, 31



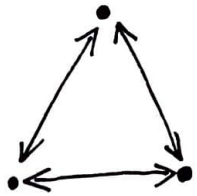
- složitost CSP s šablonou H, R závisí pouze na symetriích obrázku

  ... ale jsou to i symetrie, které nejsou očividné

  více: L. Barto: Symetrie ve výpočetní složitosti, Vesmír 101, 2022/9

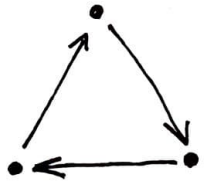
Ⓐ

2 SKUPINY

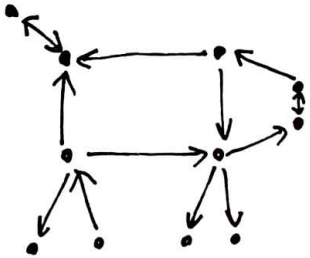


Ⓑ

3 SKUPINY



Ⓒ



Ⓓ

očividně symetrické

A, B > C > D

symetrické

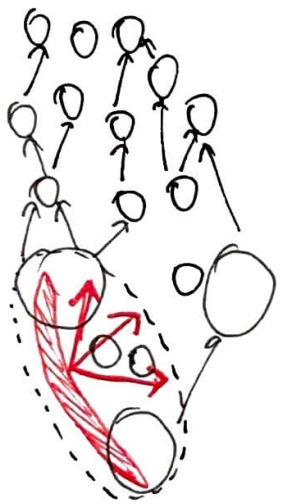
A, C, D > B

POCOCOP

5d

POlynomial-time COmputation: Opening the Black boxes in COnstraint Problems

L. B.
M. Bodirsky (TU Dresden)
M. Pinsker (TU Wien)



optimalizace

aproximace

∞ hodnot

MAX CUT

VSTUP: lidi + nekompatibilita

VÝSTUP: 2 skupiny, aby bylo co nejméně nekompatibilit

3 vs 5 SKUPINY

VSTUP: —"— jdou správně rozdělit do 3 skupin

VÝSTUP: rozdělení do 5 skupin

MEZI

VSTUP: události, omezení typu A se musí stát mezi B a C

VÝSTUP: pořadí událostí, aby omezení byla splněna

novinka

našli jsme symetrie

nevíme:

3 vs 6 : ?

KRÁSNÁ FIRMA

5e

- máme 100 lidských vlastností
- člověk každou z nich buď má nebo nemá
- krásná firma: – pro každých 49 z těchto 100 vlastností je ve firmě člověk, který má právě tyto vlastnosti
  – žádní jiní lidé ve firmě nejsou

  (firma je dooost velká)
  – nekompatibilní = žádné společné vlastnosti
- ukažte, že jdou správně rozdělit do 4 skupin (toto je DÚ)
- nejdou správně rozdělit do 3 skupin (toto není DÚ)

  – jedna z ingrediencí pro důkaz, že 3 vs 5 SKUPINY je NP-úplný

ZÁVĚREM

- symetrie výpočetního problému určují jeho výpočetní složitost

- je mnoho aspektů výpočetní složitosti i matematické teorie —"—, které jsem nezmínil

přímluvy