# Základy složitosti a vyčíslitelnosti NTIN090

Petr Kučera

2021/22 (6. přednáška)

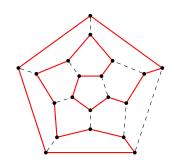
# Problémy ověřitelné v polynomiálním čase

### Hamiltonovská kružnice

#### Hamiltonovská kružnice (HK)

Instance: Neorientovaný graf G = (V, E).

Otázka: Obsahuje G cyklus, který prochází všemi vrcholy?



- Lze navštívit každé město na mapě právě jednou a vrátit se domů?
- Jednoduše ověřitelné zda posloupnost vrcholů určuje hamiltonovskou kružnici
- Obtížné zjistit, zda daný graf obsahuje hamiltonovskou kružnici

### Verifikátor čili ověřovatel

Verifikátorem pro jazyk A je algoritmus V, pro který platí, že

$$A = \{x \mid (\exists y)[V(x, y) \text{ přijme}]\}$$

### Časovou složitost verifikátoru měříme pouze vzhledem k |x|

- Polynomiální verifikátor je takový, který pracuje v polynomiálním čase vzhledem k |x|
- Řetězec y zveme také certifikátem x
- Pokud V(x, y) přijme, přečte jen prefix y polynomiální délky
- Stačí uvažovat polynomiální certifikáty y, které mají délku polynomiální v |x|

### Verifikátor pro hamiltonovskou kružnici

#### Hamiltonovská kružnice (HK)

Instance: Neorientovaný graf G = (V, E).

Otázka: Obsahuje G cyklus, který prochází všemi vrcholy?

### Verifikátor V pro hamiltonovskou kružnici

```
Input: Graf G = (V, E) a posloupnost vrcholů \mathbf{v} = (v_1, \dots, v_\ell)
```

- 1 if  $\ell \neq |V|$  then odmítni
- **2** if  $v_i = v_j$  pro nějakou dvojici indexů  $i \neq j$  then odmítni
- $\mathbf{3}$  for i=1 to n-1 do
- 4 | **if**  $\{v_i, v_{i+1}\} \notin E$  **then** odmítni
- 5 **if**  $\{v_n, v_1\}$  ∉ E **then** odmítni
- 6 přijmi

#### Třída NP

#### **Definice**

NP je třídou jazyků, které mají polynomiální verifikátory.

- Odpovídá třídě úloh, u nichž jsme schopni v polynomiálním čase ověřit, zda daný řetězec je řešením
- NP je třída jazyků, přijímaných nedeterministickými Turingovými stroji v polynomiálním čase
- Nedeterminismus zde odpovídá "hádání" správného certifikátu y pro vstup x

#### P vs. NP

- P jazyky, pro něž je možné rychle rozhodnout, zda do dané slovo patří do jazyka
- NP jazyky, pro něž je možné rychle ověřit že dané slovo patří do jazyka

Triviálně  $P \subseteq NP$ 

Otázka, zda P = NP je otevřená.

## Nedeterministický Turingův stroj

### Nedeterministický Turingův stroj (NTS) je pětice $M = (Q, \Sigma, \delta, q_0, F)$

- $Q, \Sigma, q_0, F$  mají týž význam jako u "obyčejného" deterministického Turingova stroje (DTS).
- Rozdíl oproti DTS je v přechodové funkci, nyní

$$\delta: Q \times \Sigma \mapsto \mathcal{P}(Q \times \Sigma \times \{L, N, R\}).$$

- Možné představy
  - NTS M v každém kroku "uhodne" nebo "vybere" správnou instrukci.
  - NTS M vykonává všechny možné instrukce současně a nachází se během výpočtu ve více konfiguracích současně.

Nedeterministický Turingův stroj není reálný výpočetní model ve smyslu silnější Churchovy-Turingovy teze.

### Jazyk přijímaný NTS

- Výpočet NTS M nad slovem x je posloupnost konfigurací C<sub>0</sub>, C<sub>1</sub>, C<sub>2</sub>,..., kde
  - C<sub>0</sub> je počáteční konfigurace se vstupem x a
  - z  $C_i$  do  $C_{i+1}$  lze přejít pomocí přechodové funkce  $\delta$
- Výpočet je přijímající, pokud je konečný a v poslední konfiguraci výpočtu se M nachází v přijímajícím stavu
- NTS M přijme slovo x pokud M(x) připouští přijímající výpočet
- Jazyk slov přijímaných NTS M označíme pomocí L(M)

# Časová a prostorová složitost NTS

#### **Definice**

Nechť M je nedeterministický Turingův stroj a nechť  $f: \mathbb{N} \mapsto \mathbb{N}$  je funkce.

- Řekneme, že M pracuje v čase f(n), pokud každý výpočet M nad libovolným vstupem x délky |x| = n skončí po provedení nejvýše f(n) kroků.
- Řekneme, že M pracuje v prostoru f(n), pokud každý výpočet M nad libovolným vstupem x délky |x| = n skončí a využije nejvýše f(n) buněk pracovní pásky.

## Základní nedeterministické třídy složitosti

#### **Definice**

Nechť  $f : \mathbb{N} \to \mathbb{N}$  je funkce, potom definujeme třídy:

- NTIME(f(n)) třída jazyků přijímaných nedeterministickými TS, které pracují v čase O(f(n)).
- NSPACE(f(n)) třída jazyků přijímaných nedeterministickými TS, které pracují v prostoru O(f(n)).

Pro každou funkci  $f: \mathbb{N} \mapsto \mathbb{N}$  platí

$$TIME(f(n)) \subseteq NTIME(f(n))$$
  
 $SPACE(f(n)) \subseteq NSPACE(f(n))$ 

## NP = nedeterministicky polynomiální

### Věta (Alternativní definice třídy NP)

Třída NP je třída jazyků přijímaných nedeterministickými Turingovými stroji v polynomiálním čase, tj.

$$NP = \bigcup_{k \in \mathbb{N}} NTIME(n^k).$$

#### Důkaz.

Ve dvou krocích

- ②  $\bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k) \subseteq \text{NP}$



# Důkaz NP $\subseteq \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$

- Předpokládejme, že  $L \in NP$
- Existuje tedy polynomiální verifikátor V(x, y), který splňuje
  - $L = \{x \mid (\exists y)[V(x, y) \text{ přijme}]\}$
  - V(x, y) pracuje v čase p(|x|) pro nějaký polynom p(n)
- Stačí uvažovat řetězce y délky p(|x|)
  - V nemá čas přečíst více znaků
- Platí tedy

$$L = \{x \mid (\exists y)[|y| \le p(|x|) \land V(x, y) \text{ přijme}]\}$$

# Důkaz NP $\subseteq \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$ (dokončení)

 Polynomiální NTS M, který přijímá L pracuje následujícím způsobem

#### Výpočet M se vstupem x

- 1 Nedeterministicky vyber řetězec y délky p(|x|)
- 2 Pusť V(x, y)
- з if V(x, y) přijme then přijmi else odmítni

$$x \in L \iff (\exists y)[|y| \le p(|x|) \land V(x,y) \text{ přijme}] \iff \text{nějaký výpočet } M(x) \text{ přijme} \iff x \in L(M)$$

M přijímá L v čase O(p(n)).

# Důkaz $\bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k) \subseteq \text{NP}$

- Nechť L je přijímán nějakým NTS  $M = (Q, \Sigma, \delta, q_0, F)$
- Předpokládejme, že M pracuje v polynomiálním čase p(n)
- Označme  $r = \max_{q \in Q, a \in \Sigma} |\delta(q, a)|$ 
  - maximální počet větvení přechodu dle δ
  - $r \leq |Q| \cdot |\Sigma| \cdot 3$
  - r je konstanta, která závisí jen na M a nezávisí na vstupu
- Výpočet M se vstupem x lze popsat řetězcem

$$y \in \{1, \dots, r\}^{p(|x|)}$$

• Pro  $i = 1, ..., p(|x|), y_i$  označuje větev zvolenou v kroku i

# Důkaz $\bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k) \subseteq \text{NP (dokončení)}$

### Výpočet polynomiálního verifikátoru V(x, y) pro jazyk L

- 1 Simuluj M(x) s větvením podle y
- 2 if větev výpočtu M(x) popsaná y přijme then
- 3 přijmi
- 4 else
- 5 odmítni

$$x \in L \iff$$
 nějaký výpočet  $M(x)$  přijme  $\iff (\exists y)[|y| \le p(|x|) \text{ a simulace } M(x)$  s větvením podle  $y$  přijme]  $\iff (\exists y)[|y| \le p(|x|) \text{ a } V(x,y) \text{ přijme}]$ 

V je polynomiální verifikátor pro L, tedy  $L \in NP$ .

# Základní vztahy

# Nedeterministický čas a deterministický prostor

#### Věta

Pro každou funkci  $f: \mathbb{N} \mapsto \mathbb{N}$  platí, že

$$NTIME(f(n)) \subseteq SPACE(f(n))$$

- Nechť L je přijímán NTM M v čase g(n) = O(f(n))
- Předpokládejme, že  $M = (Q, \Sigma, \delta, q_0, F)$
- Označme  $r = \max_{q \in Q, a \in \Sigma} |\delta(q, a)|$ 
  - maximální počet větvení přechodu dle  $\delta$
  - $r \le |Q| \cdot |\Sigma| \cdot 3$  je konstanta, která závisí jen na M
- Výpočet M se vstupem x lze popsat řetězcem  $y \in \{1, ..., r\}^{g(|x|)}$
- Pro  $i = 1, ..., g(|x|), y_i$  označuje větev zvolenou v kroku i
- Popíšeme TM M', který rozhoduje L v prostoru O(f(n))

## Důkaz (část 2)

### První nápad

### Výpočet M' se vstupem x

```
1 forall y \in \{1, ..., r\}^{g(|x|)} do
```

- Simuluj M(x) s větvením podle y
- if větev výpočtu M(x) popsaná y přijme then
- 4 přijmi
- 5 reject

M' by musel znát hodnotu g(|x|).

Co když g(|x|) není vyčíslitelná v prostoru O(g(|x|))?

## Důkaz (část 3)

### Výpočet M' se vstupem x

```
1 k \leftarrow 1
2 repeat
3 | forall y \in \{1, \dots, r\}^k do
4 | Simuluj M(x) s větvením podle y
5 | if větev výpočtu M(x) popsaná y přijme then přijmi
6 | k \leftarrow k + 1
7 until všechny simulace M(x) větvící podle y odmítly
```

- M pracuje v čase g(n) = O(f(n))
- $\implies$  každý výpočet M(x) skončí do g(n) kroků
- $\implies M'(x)$  skončí výpočet s  $k \le g(|x|)$

8 odmítni

# Důkaz (část 4)

### Prostorové nároky

- Vždy platí  $k \le g(|x|)$
- Prostor O(g(n)) = O(f(n)) je potřeba pro uložení y
- Prostor O(g(n)) = O(f(n)) je potřeba k simulaci M(x) podle y
- Dohromady M' pracuje v prostoru O(f(n))

## Důkaz (část 5)

$$L=L(M')$$

- Pokud M(x) má přijímající výpočet
  - Simulace M(x) přijme s nějakým y,  $|y| \le g(|x|)$
  - M'(x) přijme
- Pokud M(x) nemá přijímající výpočet
  - Pro hodnotu k = g(|x|), simulace M(x) s každým y odmítne
  - M'(x) odmítne

M' rozhoduje L v prostoru O(f(n))

### NP and PSPACE

#### Věta

Pro každou funkci  $f: \mathbb{N} \mapsto \mathbb{N}$  platí, že

 $\mathrm{NTIME}(f(n))\subseteq \mathrm{SPACE}(f(n))$ 

### Důsledek

 $\mathrm{NP}\subseteq\mathrm{PSPACE}$ 

### Model TS s menším než lineárním prostorem

Pro prostor menší než lineární uvažujeme vícepáskový TS:

Vstupní páska je jen pro čtení

Pracovní pásky jsou pro čtení i zápis

### Výstupní páska je jen pro zápis a hlava se hýbe jen vpravo

- Do prostoru se počítá jen obsah pracovních pásek.
- Součástí konfigurace je
  - stav,
  - poloha hlavy na vstupní pásce,
  - polohy hlav na pracovních páskách a
  - obsah pracovních pásek.
- Konfigurace neobsahuje vstupní slovo.

### Další prostorové třídy

Třída problémů řešitelných v logaritmickém prostoru

$$L = SPACE(\log_2 n)$$

Třída jazyků přijímaných NTS v logaritmickém prostoru

$$NL = NSPACE(log_2 n)$$

Třída jazyků přijímaných NTS v polynomiálním prostoru

$$NPSPACE = \bigcup_{k \in \mathbb{N}} NSPACE(n^k)$$

# Vztah prostoru a času

### Věta (Vztah prostoru a času)

Pro každou funkci  $f(n) \ge \log_2 n$  a každý jazyk L platí, že

$$L \in \mathrm{NSPACE}(f(n)) \implies (\exists c_L \in \mathbb{N}) \left[ L \in \mathrm{TIME}(2^{c_L f(n)}) \right].$$

#### Důsledek

Je-li f(n) funkce, pro kterou platí  $f(n) \ge \log_2 n$  a je-li g(n) funkce, pro kterou platí f(n) = o(g(n)), pak

$$NSPACE(f(n)) \subseteq TIME(2^{g(n)}).$$

### Vztah prostoru a času

### Věta (Vztah prostoru a času)

Pro každou funkci  $f(n) \ge \log_2 n$  a každý jazyk L platí, že

$$L \in \mathrm{NSPACE}(f(n)) \implies (\exists c_L \in \mathbb{N}) \left[ L \in \mathrm{TIME}(2^{c_L f(n)}) \right].$$

#### ldea důkazu

- L je přijímán nějakým NTS M v prostoru O(f(n))
- Pro vstup x, definujeme graf konfigurací G<sub>M,x</sub>
  - Vrcholy = možné konfigurace výpočtu M(x)
  - Hrany = možné přechody mezi konfiguracemi
- Popíšeme TS M', který rozhoduje L
  - M' se vstupem x hledá v G<sub>M,x</sub> cestu z počáteční konfigurace do nějaké přijímající konfigurace

# Graf konfigurací

#### **Definice**

Nechť  $M=(Q,\Sigma,\delta,q_0,F)$  je NTS pracující v prostoru f(n) a x vstupní řetězec. Graf konfigurací výpočtů M nad x je orientovaný graf  $G_{M,x}=(V,E)$ , kde

- Vrcholy V reprezentují možné konfigurace výpočtů M(x)
- $(C_1, C_2) \in E$  je-li možné z  $C_1$  do  $C_2$  přejít přechodem dle  $\delta$
- Označme  $C_0^x$  počáteční konfiguraci výpočtu M(x)

M(x) přijme, právě když v  $G_{M,x}$  obsahuje cestu z  $C_0^x$  do nějaké přijímající konfigurace  $C_F$ .

# Velikost grafu konfigurací

#### Lemma

- Uvažme funkci  $f(n) \ge \log_2 n$
- Uvažme NTS  $M = (Q, \Sigma, \delta, q_0, F)$ , který pracuje v prostoru f(n)
- Nechť x je vstup délky n = |x|
- Nechť  $G_{M,x} = (V, E)$  je odpovídající graf konfigurací

Pak  $|V| \le 2^{c_M f(n)}$  pro nějakou konstantu  $c_M$ 

Budeme předpokládat, že M má jednu vstupní pásku jen pro čtení a jednu pracovní pásku.

# Velikost $G_{M,x}$ (důkaz)

$$|V| \leq |Q| \cdot (n+2) \cdot f(n) \cdot |\Sigma|^{f(n)}$$

#### Konfigurace se skládá z následujících prvků

- stav
  - |Q| různých stavů
- poloha hlavy na vstupní pásce
  - n + 2 možných poloh
  - včetně prázdných políček kolem vstupu
- poloha hlavy na pracovní pásce
  - f(n) možných poloh
- obsah pracovní pásky
  - slovo  $w \in \Sigma^*$  na pásce má délku  $|w| \le f(n)$
  - $|\Sigma|^{f(n)}$  různých slov

### Počet konfigurací

$$\begin{split} |V| &\leq |Q| \cdot (n+2) \cdot f(n) \cdot |\Sigma|^{f(n)} \\ &= 2^{\log_2 |Q|} \cdot 2^{\log_2 (n+2)} \cdot 2^{\log_2 f(n)} \cdot 2^{f(n) \log_2 |\Sigma|} \\ &= 2^{\log_2 |Q| + \log_2 (n+2) + \log_2 f(n) + f(n) \log_2 |\Sigma|} \\ &\leq 2^{f(n)(\log_2 |Q| + 2 + 1 + \log_2 |\Sigma|)} & (f(n) \geq \log_2 n) \end{split}$$

Položíme-li 
$$c_M=\log_2|Q|+2+1+\log_2|\Sigma|$$
, pak
$$|V|\leq 2^{c_Mf(n)}$$
 
$$|E|\leq |V|^2\leq 2^{2c_Mf(n)}$$

### Vztah prostoru a času

### Věta (Vztah prostoru a času)

Pro každou funkci  $f(n) \ge \log_2 n$  a každý jazyk L platí, že

$$L \in \mathrm{NSPACE}(f(n)) \implies (\exists c_L \in \mathbb{N}) \left[ L \in \mathrm{TIME}(2^{c_L f(n)}) \right].$$

#### Idea důkazu

- Předpokládejme, že L je přijímán nějakým M v prostoru O(f(n))
- Pro vstup x, definujeme graf konfigurací G<sub>M,x</sub>
  - Vrcholy = možné konfigurace výpočtu M(x)
  - Hrany = možné přechody mezi konfiguracemi
- Popíšeme TS M', který rozhoduje L
  - M' se vstupem x hledá v G<sub>M,x</sub> cestu z počáteční konfigurace do nějaké přijímající konfigurace

# Vztah prostoru a času (důkaz)

### Výpočet M' se vstupem x

- 1 Sestav počáteční konfiguraci  $C_0^x$  výpočtu M(x)
- 2 Projdi graf  $G_{M,x}$  prohledáváním do hloubky (DFS) počínaje ve vrcholu  $C_0^x$
- 3 if DFS narazí přijímající konfiguraci then
- 4 přijmi
- 5 else
- 6 odmítni
  - DFS nepotřebuje mít před spuštěním zkonstruovaný graf  $G_{M,x}$ 
    - zná počáteční vrchol C<sub>0</sub><sup>x</sup>
    - seznam sousedů  $\Gamma(C)$  aktuálního vrcholu C lze zkonstruovat v každém kroku pomocí přechodové funkce  $\delta$  stroje M

M' nemusí znát hodnotu f(|x|).

## Vztah prostoru a času (důkaz)

- DFS lze provést v polynomiálním čase na RAMu i TS
- Turingův stroj M' pracuje v polynomiálním čase vzhledem k velikosti grafu  $G_{M,x}$
- Pracuje v čase

$$O(|V|^k) = O(2^{kc_M f(n)}) = O(2^{c_L f(n)})$$

pro nějaké konstanty  $k \ge 1$  a  $c_L \ge kc_M$ 

# Vztah prostoru a čase (poznámky)

### Věta (Vztah prostoru a času)

Pro každou funkci  $f(n) \ge \log_2 n$  a každý jazyk L platí, že

$$L \in \mathrm{NSPACE}(f(n)) \implies (\exists c_L \in \mathbb{N}) \left[ L \in \mathrm{TIME}(2^{c_L f(n)}) \right].$$

- $c_L$  závisí na jazyku L
- Různé jazyky mají různé konstanty

### Z věty **NEPLYNE**

- $NSPACE(f(n)) \subseteq TIME(2^{f(n)})$
- NSPACE $(f(n)) \subseteq \text{TIME}(2^{cf(n)})$  pro nějakou konstantu c

### $NL \subseteq P$

$$NL = NSPACE(\log_2 n)$$

$$\mathbf{P} = \bigcup_{k \in \mathbb{N}} \mathrm{TIME}(n^k)$$

#### Důsledek

 $NL \subseteq P$ 

- Předpokládejme, že  $L \in \text{NSPACE}(\log_2 n)$
- Podle věty o vztahu prostoru a času existuje konstanta  $c_L \in \mathbb{N}$ , prokterou platí

$$L \in \text{TIME}(2^{c_L \log_2 n}) = \text{TIME}(n^{c_L}) \subseteq P$$

#### NPSPACE ⊆ EXPTIME

$$\text{NPSPACE} = \bigcup_{k \in \mathbb{N}} \text{NSPACE}(n^k)$$

EXPTIME = 
$$\bigcup_{k \in \mathbb{N}} \text{TIME}(2^{n^k})$$

#### Důsledek

#### NPSPACE ⊆ EXPTIME

- Předpokládejme, že  $L \in NPSPACE$
- $\implies L \in \text{NSPACE}(n^k)$  pro nějaké  $k \in \mathbb{N}$ 
  - Podle věty o vztahu prostoru a času existuje konstanta  $c_L \in \mathbb{N}$ , prokterou platí

$$L \in \text{TIME}(2^{c_L n^k}) \subseteq \text{TIME}(2^{n^{k+1}}) \subseteq \text{EXPTIME}$$

#### Věta

Platí následující řetězec inkluzí:

LCNLCPCNPCPSPACECNPSPACECEXPTIME

- $L \subseteq NL$ ,  $P \subseteq NP$ ,  $PSPACE \subseteq NPSPACE$  plyne z
  - Pro každou funkci f(n)
    - TIME(f(n))  $\subseteq$  NTIME(f(n))
    - $SPACE(f(n)) \subseteq NSPACE(f(n))$
- NP ⊆ PSPACE plyne z
  - NTIME(f(n)) ⊆ SPACE(f(n)) pro každou funkci f(n)
- NL ⊆ P, NPSPACE ⊆ EXPTIME plyne ze vztahu prostoru a času

#### Věta

Platí následující řetězec inkluzí:

LCNLCPCNPCPSPACECNPSPACECEXPTIME

- $L \subseteq NL$ ,  $P \subseteq NP$ ,  $PSPACE \subseteq NPSPACE$  plyne z
  - Pro každou funkci f(n)
    - TIME(f(n))  $\subseteq$  NTIME(f(n))
    - SPACE(f(n))  $\subseteq$  NSPACE(f(n))
- NP ⊆ PSPACE plyne z
  - NTIME(f(n)) ⊆ SPACE(f(n)) pro každou funkci f(n)
- NL ⊆ P, NPSPACE ⊆ EXPTIME plyne ze vztahu prostoru a času

#### Věta

Platí následující řetězec inkluzí:

LCNLCPCNPCPSPACECNPSPACECEXPTIME

- L  $\subseteq$  NL, P  $\subseteq$  NP, PSPACE  $\subseteq$  NPSPACE plyne z
  - Pro každou funkci f(n)
    - TIME(f(n))  $\subseteq$  NTIME(f(n))
    - SPACE $(f(n)) \subseteq NSPACE(f(n))$
- NP ⊆ PSPACE plyne z
  - NTIME(f(n)) ⊆ SPACE(f(n)) pro každou funkci f(n)
- NL ⊆ P, NPSPACE ⊆ EXPTIME plyne ze vztahu prostoru a času

#### Věta

Platí následující řetězec inkluzí:

L⊆NL⊆P⊆NP⊆PSPACE⊆NPSPACE⊆EXPTIME

- $L \subseteq NL$ ,  $P \subseteq NP$ ,  $PSPACE \subseteq NPSPACE$  plyne z
  - Pro každou funkci f(n)
    - TIME(f(n))  $\subseteq$  NTIME(f(n))
    - SPACE(f(n))  $\subseteq$  NSPACE(f(n))
- NP ⊆ PSPACE plyne z
  - NTIME(f(n)) ⊆ SPACE(f(n)) pro každou funkci f(n)
- NL ⊆ P, NPSPACE ⊆ EXPTIME plyne ze vztahu prostoru a času