Úvod do teoretické informatiky

Zdeněk Sawa

Katedra informatiky, FEI,
Vysoká škola báňská – Technická universita Ostrava
17. listopadu 15, Ostrava-Poruba 708 33
Česká republika

21. února 2014

Přednášející

Jméno: doc. Ing. Zdeněk Sawa, Ph.D.

E-mail: `zdenek.sawa@vsb.cz`

Místnost: A1024

Web: `http://www.cs.vsb.cz/sawa/uti`

Na těchto stránkách najdete:

- Informace o předmětu
- Učební texty
- Slidy z přednášek
- Zadání příkladů na cvičení
- Aktuální informace
- Odkaz na stránku s animacemi

Požadavky

- **Zápočet** (22 bodů):
  - Zápočtová písemka (22 bodů) — bude se psát na cvičení

  Minimum pro získání zápočtu je 7 bodů.

  Možnost opravy za 14 bodů.

- **Zkouška** (78 bodů)
  - Písemná zkouška skládající se ze tří částí po 26 bodech, přičemž z každé části je nutné získat nejméně 10 bodů.

Algoritmy a problémy

Algoritmus — mechanický postup, jak něco spočítat (může být vykonáván počítačem)

Algoritmy slouží k řešení různých **problémů**.

Příklad algoritmického problému:

Vstup: Přirozená čísla x a y.

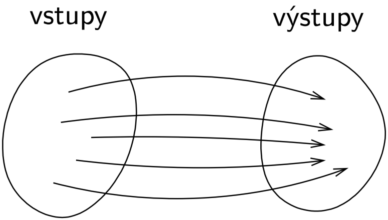
Výstup: Přirozené číslo z takové, že $z = x + y$.

Problémy

Problém

V zadání **problému** musí být určeno:

- co je množinou možných vstupů
- co je množinou možných výstupů
- jaký je vztah mezi vstupy a výstupy



Příklady problémů

Problém „Třídění“

Vstup: Sekvence prvků $a_1, a_2, \ldots, a_n$.

Výstup: Prvky sekvence $a_1, a_2, \ldots, a_n$ seřazené od nejmenšího po největší.

Příklad:

- Vstup: $8, 13, 3, 10, 1, 4$
- Výstup: $1, 3, 4, 8, 10, 13$

Poznámka: Konkrétní vstup nějakého problému se nazývá **instance** problému.

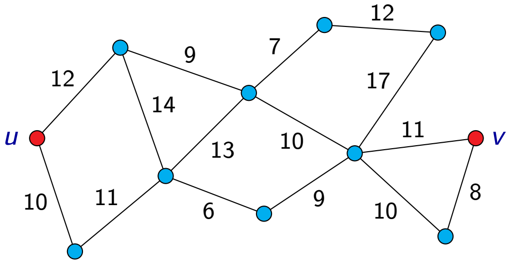
Příklady problémů

Problém „Hledání nejkratší cesty v (neorientovaném) grafu“

Vstup: Neorientovaný graf $G = (V, E)$ s ohodnocením hran, a dvojice vrcholů $u, v \in V$.

Výstup: Nejkratší cesta z vrcholu u do vrcholu v.

Příklad:



Algoritmy a problémy

Algoritmus **řeší** daný problém pokud:

- Se pro každý vstup po konečném počtu kroků zastaví.
- Pro každý vstup vydá správný výstup.

Korektnost algoritmu — ověření toho, že daný algoritmus skutečně řeší daný problém

Výpočetní složitost algoritmu:

- **časová složitost** — jak závisí doba výpočtu na velikosti vstupu
- **paměťová** (nebo též **prostorová**) **složitost** — jak závisí množství použité paměti na velikosti vstupu

Algoritmy a problémy

Teoretická informatika se překrývá se s mnoha dalšími oblastmi matematiky a informatiky:

- teorie grafů
- teorie čísel
- kryptografie
- výpočetní geometrie
- vyhledávání v textu, komprese dat
- teorie her
- ...

Další příklady problémů

Problém „Prvočíselnost"

Vstup: Přirozené číslo n.

Výstup: ANO pokud je n prvočíslo, NE v opačném případě.

Poznámka: Přirozené číslo n je **prvočíslo**, pokud je větší než 1 a je dělitelné beze zbytku pouze čísly 1 a n.

Prvních několik prvočísel: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Rozhodovací problémy

Problémům, kde množina výstupů je $\{\textsc{Ano}, \textsc{Ne}\}$ se říká **rozhodovací problémy**.

Rozhodovací problémy jsou většinou specifikovány tak, že místo popisu toho, co je výstupem, je uvedena otázku.

Příklad:

Problém „Prvočíselnost“

Vstup: Přirozené číslo n.

Otázka: Je n prvočíslo?

Algoritmicky řešitelné problémy

Předpokládejme, že máme dán nějaký problém P.

Jestliže existuje nějaký algoritmus, který řeší problém P, pak říkáme, že problém P je **algoritmicky řešitelný**.

Jestliže P je rozhodovací problém a jestliže existuje nějaký algoritmus, který problém P řeší, pak říkáme, že problém P je **(algoritmicky) rozhodnutelný**.

Když chceme ukázat, že problém P je algoritmicky řešitelný, stačí ukázat nějaký algoritmus, který ho řeší (a případně ukázat, že daný algoritmus problém P skutečně řeší).

Algoritmicky neřešitelné problémy

Problém, který není algoritmicky řešitelný, je **algoritmicky neřešitelný**.

Rozhodovací problém, který není rozhodnutelný, je **nerozhodnutelný**.

Kupodivu existuje řada algoritmických problémů (přesně definovaných), o kterých je dokázáno, že nejsou algoritmicky řešitelné.

Teorie vyčíslitelnosti — oblast teoretické informatiky, která se zabývá zkoumáním toho, které problémy jsou a které nejsou algoritmicky řešitelné.

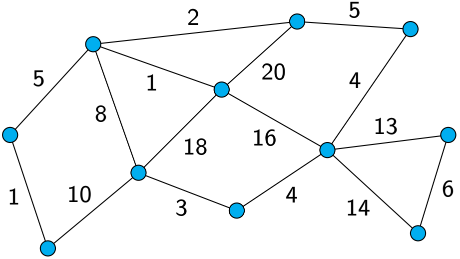
Teorie složitosti

Řada problémů je algoritmicky řešitelných, ale neexistují (nebo nejsou známy) efektivní algoritmy, které by je řešily:

TSP - Problém obchodního cestujícího

Vstup: Neorientovaný graf G s hranami ohodnocenými přirozenými čísly.

Výstup: Nejkratší uzavřená cesta, která projde všemi vrcholy a skončí v tom vrcholu, kde začíná.



Teoretická informatika

Některé další oblasti teoretické informatiky:

- teorie složitosti
- paralelní a distribuované algoritmy
- výpočetní modely

Teorie formálních jazyků

Oblast teoretické informatiky zabývajícími se otázkami týkajícími se **syntaxe**.

- **Jazyk** — množina slov
- **Slovo** — sekvence symbolů z určité abecedy
- **Abeceda** — množina **symbolů** (nebo též **znaků**)

Prostředky používané pro popis jazyků:

- gramatiky
- regulární výrazy
- automaty

Logika

Logika — obor zabývající se otázkami správného vyvozování a argumentace

- formulazace tvrzení přirozeného jazyka pomocí **formulí**
- zkoumání, kdy závěr vyplývá z daných předpokladů
- otázky týkající se důkazů a dokazatelnosti
- souvisí se zkoumáním základů matematiky a s teorií množin

Dva nejdůležitější typy logik:

- výroková logika
- predikátová logika

Výroková logika

Logické vyvozování

- *Jestliže měl vlak zpoždění a na nádraží nebyly taxíky, tak Honza přišel pozdě do práce.*
- *Honza nepřišel do práce pozdě.*
- *Vlak měl zpoždění.*

- *Na nádraží byly taxíky.*

- *Jestliže pršelo a Jana neměla s sebou deštník, tak zmokla.*
- *Jana nezmokla.*
- *Pršelo.*

- *Jana měla s sebou deštník.*

Logické vyvozování

p	Vlak měl zpoždění.	Pršelo.
q	Na nádraží byly taxíky.	Jana měla s sebou deštník.
r	Honza přišel pozdě do práce.	Jana zmokla.

Jestliže p a ne q, tak r.
Ne r.
p.

---

q.

Výroky

Příklady výroků:

- „*Jana zmokla.*“
- „*Jestliže pršelo a Jana neměla s sebou deštník, tak zmokla.*“
- „*Paříž je hlavním městem Japonska.*“
- „*Existuje nekonečně mnoho prvočísel.*“
- „$1 + 1 = 3$“
- „*Číslo* $\sqrt{2}$ *je iracionální.*“

Příklady formulací, které nejsou výroky:

- „*Součet čísel* 2 *a* 5.“
- „*V kolik hodin jede dneska rychlík z Ostravy do Prahy.*“
- „*Vzdálenost Země od Slunce.*“

Výroky

Příklady formulací, které nejsou přímo výroky, ale ze kterých dostaneme výroky dosazením konkrétních hodnot za proměnné:

- „$x > 5$“
- „$x + y = z$“
- „x *je největším prvkem množiny* A“

Toto ovšem jsou výroky:

- „*Existuje přirozené číslo* x *takové, že* $x > 5$*.*“
- „*Pro každé přirozené číslo* x *platí* $x > 5$*.*“

Logické spojky

Atomický výrok — nedá se rozložit na žádné menší výroky

„Jana zmokla."

Složený výrok — složen z menších jednodušších výroků

„Jestliže pršelo a Jana neměla s sebou deštník, tak zmokla."

Složeno z výroků:

- *„Pršelo."*
- *„Jana měla s sebou deštník."*
- *„Jana zmokla."*

Logické spojky

Reprezentace výroků pomocí **formulí**:

Symbol	Log. spojka	Příklad použití	Neformální význam
$\neg$	negace	$\neg p$	*„není pravda p"*
$\wedge$	konjunkce	$p \wedge q$	*„p a q"*
$\vee$	disjunkce	$p \vee q$	*„p nebo q"*
$\rightarrow$	implikace	$p \rightarrow q$	*„jestliže p, pak q"*
$\leftrightarrow$	ekvivalence	$p \leftrightarrow q$	*„p právě tehdy, když q"*

Atomické výroky — p, q, r, ...
(případně s indexy — p_0, p_1, p_2, ...)

Logické spojky

„Jestliže pršelo a Jana neměla s sebou deštník, tak zmokla."

Zápis pomocí formule:

$$(p \land \neg q) \rightarrow r$$

Atomické výroky:

- p — *„Pršelo."*
- q — *„Jana měla s sebou deštník."*
- r — *„Jana zmokla."*

Pravdivostní hodnoty

pravda	nepravda
1	0
P	N
true	false
T	F
ano	ne
yes	no

Pro označení pravdivostních hodnot budeme používat 0 a 1.

Pravdivostní hodnoty se též označují jako hodnoty **booleovské**.

Negace

Negací výroku φ je výrok *„není pravda, že* φ*“*. Například negací výroku

„číslo 5 *je prvočíslo“*

je výrok

„není pravda, že číslo 5 *je prvočíslo“*

nebo

„číslo 5 *není prvočíslo“*.

Ve formulích se negace označuje symbolem “$\neg$”.

Formální zápis: $\neg\varphi$ příklad: $\neg p$

φ	$\neg\varphi$
0	1
1	0

Negace

Příklad: Negací výroku

„Karel je ze všech žáků ve třídě nejvyšší"

je třeba výrok

„Karel není ze všech žáků ve třídě nejvyšší"

nebo

„není pravda, že Karel je ze všech žáků ve třídě nejvyšší".

Ne ovšem výrok

„Karel je ze všech žáků ve třídě nejmenší".

Negace

Příklad:

„Není pravda, že číslo 5 *není kladné."*

lze formalizovat jako

$$\neg\neg p \qquad \text{nebo} \qquad \neg(\neg p)$$

Podobně

„není pravda, že není pravda, že číslo 5 *není kladné"*

je možné zapsat

$$\neg\neg\neg p \qquad \text{nebo} \qquad \neg(\neg(\neg p))$$

p — *„číslo* 5 *je kladné"*

Konjunkce

Konjunkcí výroků φ a ψ je výrok „φ *a* ψ“.

Příklad: Konjunkcí výroků *„Kodaň je hlavním městem Dánska“* a „$2+2=4$“ je výrok

„Kodaň je hlavním městem Dánska a $2+2=4$.“

Ve formulích se konjunkce označuje pomocí symbolu „$\wedge$“.

$$p \wedge q$$

- p — *„Kodaň je hlavním městem Dánska“*
- q — „$2+2=4$“

Konjunkce

φ	ψ	$\varphi \wedge \psi$
0	0	0
0	1	0
1	0	0
1	1	1

Příklady nepravdivých výroků:

- *„Helsinky jsou hlavním městem Itálie a Karlova univerzita byla založena v roce 1348.“*
- *„Asie je světadíl s největší rozlohou a* $3 + 5 = 14$*.“*
- *„Existuje jen konečně mnoho prvočísel a Plzeň je hlavním městem USA.“*

Konjunkce

Příklad:

„chtěl jsem přijet, ale ujel mi vlak"

lze formalizovat jako $p \wedge q$.

Příklad:

„číslo 12 je dělitelné čísly 3 a 4"

lze formalizovat jako $p \wedge q$, kde

- p — *„číslo 12 je dělitelné číslem 3"*
- q — *„číslo 12 je dělitelné číslem 4"*

Konjunkce

Příklady výroků, kde „a“ **nemá** význam konjunkce:

- *„Levý a pravý břeh řeky byly spojeny mostem.“*
- *„Číslo* 3 *je největším společným dělitelem čísel* 12 *a* 15*.“*
- *„Bod A leží na průsečíku přímek p_1 a p_2.“*

Konjunkce

Výrok *„ani* φ*, ani* ψ*“* říká to samé, co

„není pravda φ *a není pravda* ψ*“.*

Je tedy možné ho formalizovat jako

$$\neg\varphi \wedge \neg\psi$$

Příklad: Výrok *„přímka p neprochází ani bodem A ani bodem B“* je možné formalizovat jako

$$\neg r \wedge \neg s\,,$$

kde

- r — *„přímka p prochází bodem A“*
- s — *„přímka p prochází bodem B“*

Disjunkce

Disjunkcí výroků φ a ψ je výrok „φ *nebo* ψ“.

Příklad: Disjunkcí výroků *„velryby patří mezi savce“* a *„ČR leží v mírném podnebném pásu“* je výrok

„velryby patří mezi savce nebo ČR leží v mírném podnebném pásu“.

Ve formulích se disjunkce označuje symbolem “$\vee$”.

$$p \vee q$$

- p — *„velryby patří mezi savce“*
- q — *„ČR leží v mírném podnebném pásu“*

Disjunkce

Disjunkce je „*nebo*“ v **nevylučujícím** smyslu.

φ	ψ	$\varphi \vee \psi$
0	0	0
0	1	1
1	0	1
1	1	1

Implikace

Implikace — *„jestliže* φ, *pak* ψ*“*

- φ — předpoklad
- ψ — závěr

Příklad:

> *„ Jestliže se Petr dobře připravil na zkoušku, pak z této zkoušky dostal dobrou známku.“*

Implikace se označuje symbolem “$\rightarrow$”.

$$p \rightarrow q$$

- p — *„Petr se dobře připravil na zkoušku“*
- q — *„Petr dostal z této zkoušky dobrou známku“*

Implikace

φ	ψ	$\varphi \rightarrow \psi$
0	0	1
0	1	1
1	0	0
1	1	1

Poznámka: Formule $p \rightarrow q$ je pravdivá právě v těch případech, kdy je pravdivá formule

$$\neg p \vee q\,.$$

Implikace

Implikace **nevyjařuje** příčinnou souvislost.

Příklad:

- *„Jestliže je Washington hlavním městem USA, tak* $1 + 1 = 2$*."*
- *„Jestliže je Washington hlavním městem USA, tak* $1 + 1 = 3$*."*
- *„Jestliže je Tokio hlavním městem USA, tak* $1 + 1 = 2$*."*
- *„Jestliže je Tokio hlavním městem USA, tak* $1 + 1 = 3$*."*

Implikace

Příklady různých způsobů vyjádření tvrzení $p \rightarrow q$ v přirozené řeči:

- *„pokud p, pak q"*
- *„když p, tak q"*
- *„q, pokud p"*
- *„z p plyne q"*
- *„za předpokladu p platí q"*
- *„p implikuje q"*
- *„q platí tehdy, když platí p"*
- *„p platí jen tehdy, když platí q"*
- *„p je postačující podmínka pro q"*
- *„q je nutná podmínka pro p"*

Implikace

Pokud platí $\varphi \rightarrow \psi$ a zároveň platí φ, je možné z toho vyvodit, že platí i ψ.

Příklad: Pokud platí

- *„jestliže je dnes úterý, pak je zítra středa“*
- *„dnes je úterý“*

lze z toho vyvodit, že platí

- *„zítra je středa“*

Ekvivalence

Ekvivalence — *„φ právě tehdy, když ψ“*

Příklad:

> *„Trojúhelník ABC má všechny tři strany stejně dlouhé právě tehdy, když má všechny tři úhly stejně velké.“*

Logická spojka ekvivalence se označuje symbolem “$\leftrightarrow$”

$$p \leftrightarrow q$$

- p — *„trojúhelník ABC má všechny tři strany stejně dlouhé“*
- q — *„trojúhelník ABC má všechny tři úhly stejně velké“*

Ekvivalence

φ	ψ	$\varphi \leftrightarrow \psi$
0	0	1
0	1	0
1	0	0
1	1	1

Poznámka: Formule $p \leftrightarrow q$ říká v podstatě to samé co formule

$$(p \rightarrow q) \wedge (q \rightarrow p)$$

Ekvivalence

Alternativní způsoby vyjádření ekvivalence $p \leftrightarrow q$ v přirozené řeči:

- *„p tehdy a jen tehdy když q“*
- *„p je nutnou a postačující podmínkou pro to, aby platilo q“*

Ekvivalence se často používá v **definicích** nových pojmů:

Příklad:

- *„Trojúhelník je rovnoramenný právě tehdy, když alespoň dvě jeho strany jsou stejně dlouhé.“*
- *„Trojúhelník je rovnoramenný, jestliže alespoň dvě jeho strany jsou stejně dlouhé.“*