Kapitola 1

Matematické základy

Teoretické základy informatiky vycházejí především z matematiky a matematické logiky. Jazyk matematiky je totiž nejvhodnější při vytváření formálních modelů, které se v informatice využívají nejen jako prostředek teoretického zkoumání, ale současně též jako praktický pracovní nástroj. Tvorba formálních modelů je využitím jednoho z hlavních matematických paradigmat – **abstrakce**. Její důležitost a funkci pro informatiku snad nejlépe vystihli autoři knihy [2] v názvu první kapitoly *Informatika: mechanizace abstrakce*.

V tomto textu budeme často používat základní pojmy diskrétní matematiky, a proto v první kapitole uvádíme stručný přehled vlastností množin, relací, zobrazení a pojmů používaných v asymptotických odhadech. Čtenáři dostatečně seznámenému se zmíněnou problematikou poslouží tato kapitola jen jako zavedení dále používané notace.

1.1 Množiny

Naším cílem není studium teorie množin, a tak se můžeme spokojit s naivním přístupem k zavedení jejích základních pojmů: Za **množinu** považujeme každý souhrn rozlišitelných objektů, které nazýváme **prvky množiny**. Množiny označujeme obvykle velkými písmeny (jako např. $A, B, \ldots, X, \ldots$), v případě potřeby používáme také indexy (např. $A_i, B_j, \ldots$). Prvky množin označujeme nejčastěji malými písmeny (např. $a, b, \ldots, x, \ldots$), popř. také s indexy. Je-li a prvkem množiny A, vyjádříme to zápisem $a \in A$, v opačném případě píšeme $a \notin A$.

Množinu lze určit např. vyjmenováním jejích prvků: obsahuje-li množina A právě n prvků $a_1, a_2, \ldots, a_n (n \geq 1)$, píšeme stručně $A = \{a_1, a_2, \ldots, a_n\}$. Je důležité si uvědomit, že množina nemůže obsahovat žádný prvek více než jednou a že prvky množiny nejsou uvedeným zápisem nijak uspořádány. Dvě **množiny jsou si rovny** (jsou stejné), obsahují-li obě tytéž prvky.

Existuje několik velmi často používaných množin, pro jejichž označení se zavedly zvláštní symboly:

- $\emptyset$ označuje prázdnou množinu, tj. množinu neobsahující žádný prvek
- $\mathbf{N}$ označuje množinu přirozených čísel, tj. množinu $\{0, 1, 2, \ldots\}$
- $\mathbf{Z}$ označuje množinu celých čísel, tj. množinu $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbf{R}$ označuje množinu reálných čísel

Je-li každý prvek množiny A současně prvkem množiny B (tj. pokud z platnosti $a \in A$ plyne platnost $a \in B$), říkáme, že A je **podmnožinou** množiny B, a píšeme $A \subseteq B$. Je zřejmé, že rovnost množin $A = B$ znamená $A \subseteq B$ a $B \subseteq A$. Vztah *být podmnožinou* se označuje také jako **inkluze**. Pro libovolnou množinu A platí $\emptyset \subseteq A$ a $A \subseteq A$. Je-li $A \subseteq B$ a současně $A \neq B$, říkáme, že A je **vlastní podmnožinou** množiny B a píšeme $A \subset B$ ($\subset$ se nazývá **ostrá inkluze**). Je-li $A \subseteq B$ a $B \subseteq C$, potom je i $A \subseteq C$ (stejnou vlastností – označovanou jako **tranzitivita** – se vyznačuje i vztah ostré inkluze $\subset$).

Je-li zadána nějaká množina A, potom lze její podmnožinu B definovat stanovením nějaké podmínky $V(x)$, kterou musí splňovat každý prvek x podmnožiny B. Pro tuto formu zadání používáme zápisy jako

$$B = \{x \in A \ : V(x)\}, \quad B = \{x : x \in A \ \ \& \ V(x)\}, \quad \text{apod.}$$

Při vyjadřování složitějších podmínek při popisu množin a jinde v textu budeme vedle slovního vyjadřování používat také prostředků jazyka logiky (např. logických operátorů $\neg, \&$ a $\vee$ pro negaci, konjunkci a disjunkci, nebo kvantifikátorů $\forall$ a $\exists$).

Pro zadané množiny A, B lze získat další množinu použitím některé ze základních množinových operací:

průnikem množin A a B je množina	$A \cap B = \{x : x \in A \ \ \& \ x \in B\}$
sjednocením množin A a B je množina	$A \cup B = \{x : x \in A \ \ \vee \ x \in B\}$
rozdílem množin A a B je množina	$A - B = \{x : x \in A \ \ \& \ x \notin B\}$
symetrickou diferencí množin A a B je množina	$A \oplus B = (A \cup B) - (A \cap B)$

V určitém kontextu se často stává, že všechny uvažované množiny jsou podmnožinami nějaké výchozí množiny U označované jako **univerzum**. Zabýváme-li se např. pouze celými čísly, pak je univerzem množina celých čísel $\mathbf{Z}$. Pro pevně dané univerzum U nazýváme **doplňkem množiny** A (vzhledem k univerzu U) množinu $\overline{A} = U - A$. Uvedené množinové operace mají řadu všeobecně známých vlastností, z nichž nyní uvedeme pouze několik nejdůležitějších.

Zákony komutativnosti

$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$

Zákony asociativnosti

$$A \cup (B \cup C) = (A \cup B) \cup C \qquad A \cap (B \cap C) = (A \cap B) \cap C$$

Zákony distributivnosti

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Zákony jednotky

$$A \cup \emptyset = \emptyset \cup A = A \qquad A \cap U = U \cap A = A$$

Zákony nuly

$$A \cup U = U \cup A = U \qquad A \cap \emptyset = \emptyset \cap A = \emptyset$$

Zákony doplňku

$$A \cup \overline{A} = \overline{A} \cup A = U \qquad A \cap \overline{A} = \overline{A} \cap A = \emptyset$$

Zákon involuce

$$\overline{(\overline{A})} = A$$

Zákony idempotence

$$A \cup A = A \qquad A \cap A = A$$

Zákony absorpce

$$A \cup (A \cap B) = A \qquad A \cap (A \cup B) = A$$

De Morganovy zákony

$$A - (B \cup C) = (A - B) \cap (A - C) \qquad A - (B \cap C) = (A - B) \cup (A - C)$$

Systémem množin nazýváme množinu, jejíž prvky jsou opět množiny. Takové množiny vyjadřujeme často prostřednictvím indexace, jako např. $\mathcal{A} = \{A_i : i \in I\}$, kde I je nějaká (neprázdná) indexová množina. Je-li indexová množina zřejmá z kontextu, nebo není-li naopak podstatná, píšeme jednoduše $\mathcal{A} = \{A_i\}$.

Množiny A a B nazýváme **disjunktní**, nemají-li společné prvky, tzn. platí-li $A \cap B = \emptyset$. **Mohutností** (nebo též **kardinalitou**) množiny A nazýváme počet jejích prvků a značíme $|A|$.

Dvě množiny mají stejnou mohutnost, pokud lze jejich prvky na sebe vzájemně jednoznačně zobrazit. Mohutnost prázdné množiny je $|\emptyset| = 0$. Má-li množina A za mohutnost nějaké přirozené číslo, nazýváme ji **konečnou množinou**, v opačném případě se jedná o **nekonečnou množinu**. Všechny nekonečné množiny, které mají stejnou mohutnost jako množina přirozených čísel $\mathbf{N}$, nazýváme **spočetné**, ostatní nekonečné množiny jsou **nespočetné**.

Pro dvě konečné množiny A a B platí identita

$$|A \cup B| = |A| + |B| - |A \cap B|, \tag{1.1}$$

odkud lze odvodit vztah $|A \cup B| \leq |A| + |B|$. Pro disjunktní množiny (tj. $A \cap B = \emptyset$) tak dostáváme $|A \cup B| = |A| + |B|$. Je-li $A \subseteq B$, pak platí $B = (B - A) \cup A$ a pomocí výchozího vztahu snadno odvodíme nerovnost $|A| \leq |B|$.

Pro neprázdnou množinu A nazýváme systém $\mathcal{A} = \{A_i : i \in I\}$ neprázdných podmnožin množiny A **rozkladem na množině** A, pokud splňuje následující dvě podmínky:

- $\bigcup_{i \in I} A_i = A$ (**podmínka pokrytí**)
- $A_i \cap A_j = \emptyset$ pro všechna $i, j \in I, i \neq j$ (**podmínka disjunkce**)

Prvky A_i tohoto systému nazýváme **třídami rozkladu** na množině A.

Pro libovolné přirozené k označujeme symbolem $\binom{A}{k}$ systém všech k-prvkových podmnožin množiny A, tedy

$$\binom{A}{k} = \{A' : A' \subseteq A \ \& \ |A'| = k\}.$$

Speciálně platí $\binom{A}{0} = \{\emptyset\}$ a $\binom{A}{k} = \emptyset$ pro $k > |A|$. Systém $\binom{A}{1}$ je velmi podobný původní množině A – je tvořen všemi jejími jednoprvkovými podmnožinami. Většinou můžeme považovat tento systém za shodný s původní množinou A.

Systém všech podmnožin množiny A nazýváme **potencí** (nebo **exponenciální množinou**) množiny A a značíme 2^A. Platí tedy

$$2^A = \{A' : A' \subseteq A\} = \binom{A}{0} \cup \binom{A}{1} \cup \binom{A}{2} \cup \dots$$

Je vidět, že potence libovolné množiny je neprázdná, speciálně $2^\emptyset = \{\emptyset\}$. Tak např. pro $A = \{a, b\}$ máme $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Velmi často vytváříme ze dvou nebo více objektů složitější objekty, u kterých chceme rozlišit jejich vytvářecí složky podle pořadí. **Uspořádaná dvojice** prvků a a b se vyjadřuje zápisem (a, b) a formálně lze zavést vztahem $(a, b) = \{a, \{a, b\}\}$. Je zřejmé, že $(a, b) \neq (b, a)$, zatímco $\{a, b\} = \{b, a\}$.

Zobecněním postupu použitého při zavedení uspořádaných dvojic je možné pro libovolné přirozené n zavést uspořádanou n-tici prvků $a_1, a_2, \dots, a_n$, kterou budeme zapisovat jako $(a_1, a_2, \dots, a_n)$. V určitém kontextu (jsou-li např. a_i symboly nějaké abecedy) se taková n-tice pro zjednodušení zapisuje jako řetězec $a_1 a_2 \dots a_n$. Pro úplnost připustíme i (uspořádané!) 1-tice (a) a také jedinou 0-tici $\emptyset$.

Pro zadané množiny A a B nazýváme množinu uspořádaných dvojic, jejichž první složka je z množiny A a druhá z množiny B, **kartézským součinem** množin A a B, značíme $A \times B$. Je tedy

$$A \times B = \{(a, b) : a \in A \ \& \ b \in B\}$$

Pro kartézský součin konečných množin A a B platí $|A \times B| = |A| \cdot |B|$. Pro přirozené n a množiny $A_1, A_2, \dots, A_n$ zavádíme obdobně n-násobný kartézský součin pomocí vztahu

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_i \in A_i, i = 1, 2, \dots, n\}$$

Pro mohutnost n-násobného kartézského součinu konečných množin platí

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$$

Zvolíme-li všechny množiny A_i rovné jediné množině A, nazýváme součin $A \times A \times \cdots \times A$ **n-tou kartézskou mocninou** množiny A a značíme A^n. Podle naší předchozí poznámky o uspořádaných n-ticích je vidět, že pro libovolnou množinu A platí $A^1 = A$ a $A^0 = \{\emptyset\}$.

Kromě uspořádaných dvojic je pro zavedení neorientovaných grafů zapotřebí rovněž pojem **neuspořádané dvojice**. Jsou-li $a, b \in A$ libovolné (ne nutně různé) prvky, pak zápisem $[a, b]$ vyjadřujeme v tomto textu neuspořádanou dvojici prvků a, b. Pro neuspořádané dvojice tedy platí $[a, b] = [b, a]$ a množinu neuspořádaných dvojic prvků z množiny A označujeme $A \otimes A$. Zřejmě je možné psát

$$A \otimes A = \binom{A}{1} \cup \binom{A}{2}.$$

Cvičení

1.1-1. De Morganovy zákony se zpravidla uvádějí ve tvaru

(a) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ (b) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

Jaký je vztah mezi tímto zněním a formulací uvedenou dříve v textu?

(*Odpověď:* Ve dříve uvedené formulaci stačí za množinu A považovat univerzum U, použít definici doplňku a vhodně změnit označení proměnných.)

1.1-2. S použitím definice sjednocení a průniku dokažte vztahy

(a) $(A \cap B) \subseteq A \subseteq (A \cup B)$ (b) $(A \cap B) \subseteq B \subseteq (A \cup B)$

(*Odpověď:* Každý prvek z A (a rovněž každý prvek z B) je současně prvkem $(A \cup B)$, takže platí $A \subseteq (A \cup B), B \subseteq (A \cup B)$. Každý prvek z $A \cap B$ je prvkem množiny A a současně prvkem množiny B, takže $A \cap B \subseteq A$ a zároveň $A \cap B \subseteq B$.)

1.1-3. S použitím definice inkluze, předchozího cvičení a v textu uvedených zákonů platných pro množinové operace dokažte ekvivalenci následujících pěti vztahů :

(a) $A \subseteq B$ (b) $A \cup B = B$ (c) $A \cap B = A$
(d) $\overline{A} \cup B = U$ (e) $A \cap \overline{B} = \emptyset$

Odpověď:

(a) $\Rightarrow$ (b) : $A \cup B = \{x : (x \in A)$ **or** $(x \in B)\} =$
$= \{x : x \in A\} \cup \{x : x \in B\} \subseteq \{x : x \in B\} \cup \{x : x \in B\} = \{x : x \in B\} = B,$
takže $B \subseteq (A \cup B) \subseteq B \Rightarrow (A \cup B) = B$

(b) $\Rightarrow$ (c) : $A \cap B = A \cap (A \cup B) = (A \cap A) \cup (A \cap B) = A \cup (A \cap B) \supseteq A,$
takže $A \supseteq (A \cap B) \supseteq A \Rightarrow (A \cap B) = A$

(c) $\Rightarrow$ (d) : $\overline{A} \cup B = \overline{(A \cap B)} \cup B = (\overline{A} \cup \overline{B}) \cup B = \overline{A} \cup (\overline{B} \cup B) = \overline{A} \cup U = U$

(d) $\Rightarrow$ (e) : $\emptyset = \overline{U} = \overline{(\overline{A} \cup B)} = A \cap \overline{B}$

(e) $\Rightarrow$ (a) : $(A \cap B) = (A \cap B) \cup \emptyset = (A \cap B) \cup (A \cap \overline{B}) = A \cap (B \cup \overline{B}) = A \cap U = A,$
takže je $B \supseteq (A \cap B) = A$

1.1-4. Zjistěte, zda platí následující rovnosti, které bychom mohli nazvat distributivními zákony pro průnik a rozdíl množin ((a) ,(b)), distributivními zákony pro sjednocení a rozdíl množin ((c), (d)) a asociativními zákony pro rozdíl množin ((e), (f)):

(a) $A \cap (B - C) = (A \cap B) - (A \cap C)$ (b) $(A \cap B) - C = (A - C) \cap (B - C)$
(c) $A \cup (B - C) = (A \cup B) - (A \cup C)$ (d) $(A \cup B) - C = (A - C) \cup (B - C)$
(e) $(A - B) - C = A - (B \cup C)$ (f) $A - (B - C) = (A - B) \cup (A \cap B \cap C)$

(*Návod:* Pomocí pravdivostních tabulek se ukáže, že vztahy (a), (b), (d), (e) a (f) platí, kdežto vztah (c) nikoliv.)

1.1-5. Ověřte následující vlastnosti operace symetrické diference:

(a) $A \oplus B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$ (b) $A \oplus B = B \oplus A$
(c) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (d) $A \oplus A = \emptyset$ (e) $A \oplus \emptyset = A$

(*Návod:* Postupujeme buď pomocí pravdivostních tabulek nebo použijeme známých vlastností množinových operací. Tak např. důkaz (a) provedeme úpravami pravé strany takto:

$(A \cap \overline{B}) \cup (\overline{A} \cap B) =$	podle definice doplňku
$= (A \cap (U - B)) \cup ((U - A) \cap B) =$	použitím vztahu (a) ve cvič. 1.1-4
$= ((A \cap U) - (A \cap B)) \cup ((U \cap B) - (A \cap B)) =$	použitím zákona jednotky
$= (A - (A \cap B)) \cup (B - (A \cap B)) =$	použitím vztahu (d) ve cvič. 1.1-4
$= (A \cup B) - (A \cap B))$	definice symetrické diference

1.1-6. Určete nutnou a postačující podmínku platnosti vztahu $A \oplus B = A \cup B$ pro obecné množiny A, B.

1.1-7. Pro $A = \{1, 2, 3\}$ a $B = \{a, b, c, d\}$ určete
(a) všechny prvky potencí 2^A a 2^B
(b) všechny prvky kartézských součinů $A \times B,\ B \times A,\ A \times A$
(c) všechny prvky množin $A \otimes A, B \otimes B$

1.1-8. Nechť $|A| = m,\ |B| = n$. Určete mohutnost množin $2^A,\ A \times B, A \otimes A$.

1.1-9. Dokažte zobecněné de Morganovy zákony pro konečné systémy množin
(a) $\overline{(A_1 \cup A_2 \cup \ \ldots\ \cup A_n)} = \overline{A_1} \cap \overline{A_2} \cap \ \ldots\ \cap \overline{A_n}$
(b) $\overline{(A_1 \cap A_2 \cap \ \ldots\ \cap A_n)} = \overline{A_1} \cup \overline{A_2} \cup \ \ldots\ \cup \overline{A_n}$

1.1-10. Dokažte následující zobecnění vztahu (1.1):

$$|A_1 \cup A_2 \cup \ \ldots\ \cup A_n| = |A_1| + |A_2| + \ \ldots\ + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| - \ \ldots \\ + |A_1 \cap A_2 \cap A_3| + \ \ldots\ + (-1)^{n-1} |A_1 \cap A_2 \cap \ \ldots\ \cap A_n|$$

1.2 Relace a zobrazení

Binární relací R **z množiny** A **do množiny** B nazýváme libovolnou podmnožinu kartézského součinu $A \times B$. Skutečnost, že uspořádaná dvojice (a, b) je v relaci R, zapisujeme kromě běžného $(a, b) \in R$ také v jednodušší infixové podobě jako aRb. Jsme např. zvyklí na zápis $1 < 10$, který vyjadřuje náležení uspořádané dvojice čísel $(1, 10)$ do binární relace $<$: $(1, 10) \in <$. Binární relaci $R^{-1} \subseteq B \times A$ definovanou vztahem

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

nazýváme **inverzní relací** k relaci $R \subseteq A \times B$.

Binární relací R **na množině** A rozumíme podmnožinu kartézského součinu $A \times A$. **Identická relace** Δ_A **na množině** A (též diagonála) se zavádí vztahem $\Delta_A = \{(a, a) : a \in A\}$. **Prázdnou relací** 0_A rozumíme prázdnou množinu uspořádaných dvojic.

V tomto textu se sice věnujeme téměř výhradně binárním relacím, pojem relace je však možno zobecnit. Pro přirozené kladné n nazýváme n**-ární** relací R na množinách $A_1, A_2, \ldots, A_n$ libovolnou podmnožinu kartézského součinu $A_1 \times A_2 \times \cdots \times A_n$. Pojem n-ární relace je nezbytný např. jako matematický model pro relační databáze.

Jsou-li $R \subseteq A \times B$ a $S \subseteq B \times C$ binární relace, potom **součinem (složením) relací** R a S nazýváme relaci $R \circ S \subseteq A \times C$ definovanou vztahem

$$a\ (R \circ S)\ c \ \Leftrightarrow_{df}\ \exists b \in B :\ (aRb\ \&\ bSc).$$

Omezíme-li se na binární relace na (jediné) množině A, pak je operace složení definována pro libovolné dvě relace a platí pro ni asociativní zákon

$$R \circ (S \circ T) = (R \circ S) \circ T. \tag{1.2}$$

Při určování inverze k součinu relací narazíme na zákonitost, která je dobře známá z dalších oblastí matematiky:

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}. \tag{1.3}$$

Díky asociativnosti a existenci inverze má pro relaci $R \subseteq A \times A$ smysl zavést celočíselnou mocninu R^n pomocí vztahů

$$R^n = \begin{cases} \Delta_A & \text{pro } n = 0 \\ R \circ R \circ \cdots \circ R \ (n\text{-krát}) & \text{pro } n > 0 \\ (R^{-n})^{-1} & \text{pro } n < 0 \end{cases} \tag{1.4}$$

Tranzitivní uzávěr R^+, resp. **reflexivně-tranzitivní uzávěr** R^* relace R jsou definovány vztahy

$R^+ = \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \cdots \qquad R^* = \bigcup_{i=0}^{\infty} R^i = \Delta_A \cup R \cup R^2 \cup R^3 \cup \cdots$

Binární relace mohou mít různé vlastnosti, připomeneme si jen následující (předpokládáme $R \subseteq A \times A$):

(RE)	**reflexivita**:	aRa pro všechna $a \in A$	$\Delta_A \subseteq R$
(SY)	**symetrie**:	$aRb \Rightarrow bRa$	$R^{-1} = R$
(TR)	**tranzitivita**:	$aRb \ \& \ bRc \Rightarrow aRc$	$(R \circ R) \subseteq R$
(AN)	**antisymetrie**:	$aRb \ \& \ bRa \Rightarrow a = b$	$(R \cap R^{-1}) \subseteq \Delta_A$
(AS)	**asymetrie**:	$aRb \Rightarrow \neg bRa$	$R \cap R^{-1} = 0_A$
(IR)	**ireflexivita**:	$\neg aRa$ pro všechna $a \in A$	$R \cap \Delta_A = 0_A$

Je dobré vědět, že všechny uvedené vlastnosti jsou invariantní vůči přechodu k inverzní relaci (viz cvič. 1.2-5). Jestliže nějaká relace nemá některou z požadovaných vlastností, můžeme se zabývat otázkou, jak zadanou relaci R co nejméně změnit, aby tuto vlastnost měla. Pro vlastnosti reflexivity, symetrie a tranzitivity se toho snažíme dosáhnout přidáváním potřebných uspořádaných dvojic, u zbývajících tří vlastností je toho možné dosáhnout pouze odebíráním nežádoucích uspořádaných dvojic. Téměř úplným vodítkem v takových úpravách je následující tvrzení, jehož poslední část vyjadřuje nejednoznačnost úprav směřujících k redukování relace na relaci asymetrickou.

Věta 1.1: Nechť $R \subseteq A \times A$ je binární relace. Potom platí:
(a) $R \cup \Delta_A$ je nejmenší reflexivní relací obsahující R
(b) $R \cup R^{-1}$ je nejmenší symetrickou relací obsahující R
(c) R^+ je nejmenší tranzitivní relací obsahující R
(d) $R - \Delta_A$ je největší ireflexivní relací obsaženou v R
(e) $R - S - \Delta_A$ je (v sobě) maximální asymetrickou relací obsaženou v R pro každou relaci S takovou, že $\{S, S^{-1}\}$ je rozklad relace $(R \cap R^{-1}) - \Delta_A$.

Důkaz: Platnost částí (a) a (d) je zřejmá.
(b) Relace $R \cup R^{-1}$ je zjevně symetrická; nechť $S \supseteq R$ je rovněž symetrická relace, potom $S = S^{-1} \supseteq R^{-1}$, takže $S \supseteq R \cup R^{-1}$.
(c) Relace R^+ je tranzitivní, neboť $R^+ \circ R^+ = R^+$; nechť $S \supseteq R$ je rovněž tranzitivní relace, potom platí $S = S^+ \supseteq R^+$.
(e) Relace $R - S - \Delta_A$ je zřejmě asymetrická a je obsažena v R. K této relaci nelze již přidat žádnou uspořádanou dvojici $(a, b) \in S$, neboť dvojice (b, a) je v S^{-1} a tedy i v $R - S - \Delta_A$, takže $R - S - \Delta_A$ je i maximální. △

Binární relaci, která je reflexivní, symetrická a tranzitivní, nazýváme **ekvivalencí**. Je-li R ekvivalence na množině A, potom pro každý prvek $a \in A$ nazýváme **třídou prvku** a v ekvivalenci R podmnožinu

$$[a]_R = \{x \in A : xRa\}. \tag{1.5}$$

Velmi důležitou charakterizaci vzájemného vztahu ekvivalencí a rozkladů na množině podává následující tvrzení.

Věta 1.2: Každá ekvivalence na neprázdné množině A definuje rozklad na této množině a každý rozklad na A definuje ekvivalenci.

Důkaz: (a) Od ekvivalence $R \subseteq A \times A$ k rozkladu na A dojdeme takto: uvažujme všechny různé třídy prvků $[a]_R$ pro $a \in A$. Ukážeme, že tyto třídy představují požadovaný rozklad.

(*podmínka pokrytí*) – Vzhledem ke vztahu 1.5 platí $\emptyset \neq [a]_R \subseteq A$, neboť je vždy alespoň $a \in [a]_R$. Potom ale sjednocení všech tříd $[a]_R$ pro $a \in A$ pokrývá celé A.

(*podmínka disjunkce*) – Disjunktnost dvou různých tříd $[a]_R, [b]_R$ dokážeme sporem. Nechť $[a]_R \cap [b]_R \neq \emptyset$, tedy existuje $c \in A : (c \in [a]_R)$ & $(c \in [b]_R)$. Pro libovolné $x \in [a]_R$ potom platí xRa, aRc (to plyne z cRa a ze symetrie R) a cRb. Díky tranzitivitě je tedy i xRb. Platí tedy $[a]_R \subseteq [b]_R$. Obdobně dokážeme i opačný vztah $[b]_R \subseteq [a]_R$, takže jsou obě třídy shodné, což je spor s původním předpokladem.

(b) Přechod od rozkladu $\{X_i : i \in I\}$ k ekvivalenci je snazší. Definujeme relaci R na A takto:

$$xRy \Leftrightarrow_{df} \exists i \in I : (x \in X_i) \ \& \ (y \in X_i)$$

Potom je R zřejmě ekvivalencí, neboť má zjevně vlastnosti (RE), (SY) a (TR). △

Binární relaci R na množině A, která je reflexivní, antisymetrická a tranzitivní, nazýváme **(částečným) uspořádáním** množiny A, dvojici $\langle A, R\rangle$ pak nazýváme **uspořádanou množinou**. Příkladem takové relace je (neostré) uspořádání $\leq$ na množině přirozených čísel $\mathbf{N}$ podle velikosti. Symbolu $\leq$ se proto používá k označení obecné relace uspořádání na libovolné množině A a symbolem $\geq$ vyjadřujeme inverzní relaci k tomuto uspořádání (což je opět uspořádání na A).

Dva různé prvky $x, y \in A$ nazýváme **srovnatelné** v uspořádání $\leq$, pokud platí $x \leq y$ nebo $y \leq x$. Je-li $\leq$ uspořádání na A, pak binární relaci $<$ definovanou vztahem

$$x < y \Leftrightarrow_{df} (x \leq y) \ \& \ (x \neq y)$$

nazýváme **ostrým uspořádáním** odpovídajícím uspořádání $\leq$. Ostré uspořádání je zjevně asymetrická tranzitivní relace, je tedy současně ireflexivní. Inverzní relaci k ostrému uspořádání $<$ označujeme symbolem $>$ – zjevně je to opět ostré uspořádání, které odpovídá uspořádání $\geq$.

Minimálním prvkem uspořádané množiny $\langle A, \leq\rangle$ nazýváme takový prvek $c \in A$ (pokud existuje), pro který nelze v A nalézt prvek x ostře menší než c, tj. $x < c$. **Nejmenším prvkem** uspořádané množiny $\langle A, \leq\rangle$ nazýváme takový prvek $d \in A$ (pokud existuje), který je menší nebo roven všem ostatním prvkům množiny A, tj. $d \leq x$ pro všechna $x \in A$. Použitím inverzních uspořádání se obdobně definují i **maximální** a **největší prvek** množiny A.

Mějme např. množinu přirozených čísel $\{2, 3, 5, 6, 10, 15, 30\}$ uspořádanou dělitelností. Pak jsou čísla 2, 3 a 5 jejími minimálními prvky a číslo 30 je největším (a současně jediným maximálním) prvkem, nejmenší prvek zde neexistuje.

Uspořádání $\leq$ na množině A se nazývá **úplné** (též **lineární**), pokud pro libovolná $x, y \in A$ platí $(x \leq y) \ \vee \ (y \leq x)$, jinými slovy, jsou-li každé dva prvky srovnatelné.

Jsou-li $\langle A, R\rangle$ a $\langle B, S\rangle$ uspořádané množiny, je možné uspořádat i kartézský součin $A \times B$ tak, že se srovnání provádí „po složkách“. Vzniklé uspořádání se nazývá **direktním součinem**, má však tu nepříjemnou vlastnost, že direktní součin dvou úplných uspořádání nevytváří úplné uspořádání. Častěji se proto setkáme s vytvářením uspořádání na lexikografickém principu.

Pro uspořádanou množinu $\langle A, \leq \rangle$ nazýváme **lexikografickým uspořádáním** $\preceq$ indukovaným uspořádáním $\leq$ na množině A^* všech n-tic libovolné délky [1]

$$A^* = \bigcup_{i=0}^{\infty} A^i = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \ \ldots \tag{1.6}$$

relaci definovanou takto: Pro $x = (x_1, x_2, \ldots, x_k),\ y = (y_1, y_2, \ldots, y_n)$ pokládáme

$$x \preceq y \ \Leftrightarrow_{df}\ \exists i \ \leq k\ (x_i < y_i\ \&\ (\forall j < i\ (x_j = y_j)))\ \vee\ (k < n\ \&\ (\forall i\ \leq k\ (x_i = y_i))) \tag{1.7}$$

Lexikografické uspořádání dovoluje srovnávat n-tice s různým počtem prvků a je-li výchozí uspořádání úplné, potom je úplné i jím indukované lexikografické uspořádání. Definiční vztah jen vyjadřuje postup, který dobře známe z abecedního řazení slov – je to totiž lexikografické uspořádání indukované uspořádáním písmen v abecedě.

Nechť jsou dány (neprázdné) množiny A, B. **Zobrazením** množiny A do množiny B nazýváme každou binární relaci $f \subseteq A \times B$, pro kterou ke každému $a \in A$ existuje nejvýše jedno $b \in B$ tak, že $(a, b) \in f$. Množina A je **levým oborem** zobrazení f, množina B je jeho **pravým oborem**. Pro takové zobrazení f používáme zápis $f : A \mapsto B$ a je-li $(a, b) \in f$, vyjadřujeme to zápisem $b = f(a)$ nebo $f : a \ \mapsto b$.

Definiční obor $\mathcal{D}(f)$ zobrazení f tvoří množina všech prvků $a \in A$, pro které existuje (podle předpokladu jediný) prvek $b \in B$ tak, že $(a, b) \in f$. Podobně **obor hodnot** $\mathcal{H}(f)$ zobrazení f tvoří množina všech prvků $b \in B$, pro které existuje prvek $a \in A$ tak, že $(a, b) \in f$. Zobrazení $f : A \mapsto B$ se nazývá **totální**, jestliže $\mathcal{D}(f) = A$, jinak je **parciální**. Dvě zobrazení jsou si rovna, pokud mají stejné levé i pravé obory a jsou si navíc rovna jako binární relace. Zobrazení f je :

surjektivní	– pokud $\mathcal{H}(f) = B$
injektivní	– pokud platí $a_1 \neq a_2 \ \Rightarrow\ f(a_1) \neq f(a_2)$
bijektivní	– pokud je totální, surjektivní a injektivní (píšeme $f : A \leftrightarrow B$)
permutací na A	– pokud je bijektivní a $\mathcal{D}(f) = \mathcal{H}(f) = A$

Inverzí zobrazení $f : A \mapsto B$ dostaneme obecně pouze relaci $f^{-1} \subseteq B \times A$. Pro injektivní zobrazení je inverze zobrazením, pro bijektivní zobrazení $f : A \leftrightarrow B$ dostaneme inverzí opět bijektivní zobrazení $f^{-1} : B \leftrightarrow A$.

Konečná posloupnost délky $n \in \mathbf{N}$ je zobrazení, jehož definičním oborem je množina $\{0, 1, \ \ldots\ , n-1\}$. **Nekonečná posloupnost** je zobrazení, jehož definičním oborem je množina přirozených čísel $\mathbf{N}$. Pro zobrazení $f : A_1 \times A_2 \times \ \ldots\ \times A_n \mapsto B$ píšeme $b = f(a_1, a_2, \ \ldots\ , a_n)$ a každé a_i nazýváme **argumentem** zobrazení f, přestože – striktně vzato – má f jediný argument, kterým je celá uspořádaná n-tice. Zobrazení, jehož obor(-y) argumentů i obor hodnot jsou nějaké číselné množiny, nazýváme **funkcí**.

Vlastnosti relací, zobrazení a funkcí se v potřebné míře studují v základních kurzech matematiky, zde si tedy na závěr připomeneme ještě jeden důležitý pojem, s nímž se budeme v rozličných podobách setkávat dále v textu.

Nechť A je libovolná množina a $R \subseteq A^{n+1} (n \geq 0)$ nějaká $(n+1)$-ární relace na A. Potom říkáme, že $B \subseteq A$ je **uzavřená vzhledem k relaci** R, pokud platí

$$b_1, b_2, \ldots, b_n \in B\ \&\ (b_1, b_2, \ldots, b_n, b_{n+1}) \in R \ \ \Rightarrow \ \ b_{n+1} \in B$$

Libovolnou vlastnost tvaru „množina B je uzavřená vzhledem k relacím $R_1, R_2, \ldots, R_m$“ nazýváme **uzávěrovou vlastností** množiny B.

Tak např. množina sudých celých čísel $\mathbf{I}_S \subseteq \mathbf{I}$ je uzavřená vzhledem k binární relaci dělitelnosti, neboť jestliže sudé celé číslo i dělí nějaké celé číslo j, pak také j musí být sudé.

[1] Je třeba upozornit, že symboly $\leq$ a $<$ použité ve vztahu 1.6 mají dvojí význam – vyjadřují totiž jednak obecnou relaci uspořádání a odpovídajícího ostrého uspořádání na množině A, jednak obvyklé uspořádání přirozených čísel podle velikosti.

Podmnožina lichých čísel vzhledem k této relaci uzavřená není. Pro pevně zvolenou množinu C je vlastnost inkluze této množiny, tedy „C je podmnožinou B“, uzávěrovou vlastností. Za relaci R podle definice uvedené výše stačí totiž uvažovat unární relaci $R = \{(x) : x \in C\}$.

Jelikož n-ární zobrazení na množině (tzv. **operace**) je speciálním případem $(n+1)$-ární relace, můžeme se zabývat i uzavřeností množin vzhledem k operacím. Např. množina sudých celých čísel je uzavřená vzhledem k operacím sčítání i odčítání, množina lichých čísel jen vzhledem k násobení.

Podobně je ovšem i libovolná relace také (pod-)množinou, takže může být uzavřená vzhledem k jiným relacím. Tak např. uvažujme následující ternární relaci T nad binárními relacemi na množině A, tedy $T \subseteq A^2 \times A^2 \times A^2$:

$$T = \{((a,b),(b,c),(a,c)) : a,b,c \in A\}.$$

Potom je binární relace R uzavřená vzhledem k T, právě když je R tranzitivní relací na A, jinými slovy tranzitivita je uzávěrová vlastnost. Podobně i reflexivita je uzávěrová vlastnost, neboť to plyne z uzávěrovosti inkluze identické (diagonální) relace $\Delta_A = \{(a,a) : a \in A\}$.

V matematice se často setkáme s konstrukcí, při níž se přejde od nějaké množiny B s vlastností P k **minimální množině C, která obsahuje B a má vlastnost P**. Minimálností se zde rozumí, že neexistuje vlastní podmnožina C obsahující B, která by rovněž měla vlastnost P. Pro zajištění korektnosti takové konstrukce je ovšem třeba, aby P byla uzávěrová vlastnost, jak ukazuje následující tvrzení.

Věta 1.3: Nechť P je uzávěrová vlastnost definovaná nějakými relacemi $R_1, \ldots, R_m$ na množině A a nechť B je podmnožina množiny A. Potom existuje jediná minimální množina C, která obsahuje B a má vlastnost P (množinu C nazýváme **uzávěrem množiny** B vzhledem k relacím $R_1, \ldots, R_m$ a značíme B^*).

Důkaz: Uvažujme systém S všech podmnožin množiny A, které jsou uzavřené vzhledem k relacím $R_1, \ldots, R_m$ a mají B za podmnožinu. Potom je S neprázdný – obsahuje totiž alespoň množinu A. Položíme nyní $C = \cap S$, kde průnik probíhá přes všechny prvky systému S.

C je korektně definovaná, neboť je to průnik neprázdného systému množin. C rovněž obsahuje B, neboť jej obsahují všechny množiny systému S. C je také uzavřená vzhledem ke každé relaci R_i, což plyne z následující úvahy: nechť $a_1, \ldots, a_{n_i-1} \in C$ a $(a_1, \ldots, a_{n_i-1}, a_{n_i}) \in R_i$. Potom všechny množiny systému S obsahují $a_1, \ldots, a_{n_i-1}$ a protože jsou uzavřené vzhledem k R_i, obsahují také prvek a_{n_i}. Také C tedy obsahuje a_{n_i}, a je tedy uzavřená vzhledem k R_i.

C je konečně i minimální, neboť nemůže existovat žádná vlastní podmnožina $C' \subset C$ s těmito vlastnostmi – C' by totiž musela být obsažena v systému S, a tedy by musela být nadmnožinou k C. △

Je vidět, že právě uvedené chápání pojmu *uzávěr* je zcela v souladu např. s tím, jak jsme dříve zavedli tranzitivní a reflexivně-tranzitivní uzávěr relace. Pro konečnou množinu B lze výpočet jejího uzávěru B^* vzhledem k zadaným relacím $R_1 \subseteq A^{n_1}, \ldots, R_k \subseteq A^{n_k}$ provést pomocí následujícího generického algoritmu.

Algoritmus 1.4 Uzávěr množiny vzhledem k soustavě relací

UZAVER$(A, R_1, \ldots, R_k)$

```
1   A* := A                                   Počáteční nastavení uzávěru
2   while                                     Přidáváme, dokud je co
3       „existuje index i(1 ≤ i ≤ k) a r_i prvků a_1, ..., a_{r_i-1} ∈ B*
4       a a_{r_i} ∈ A − B* takových, že (a_1, ..., a_{r_i}) ∈ R_i"
5       do A* := A* ∪ {a_{r_i}}
```

V odstavci 7.2 se seznámíme s efektivní implementací uzávěrového algoritmu určeného k výpočtu vzdáleností mezi uzly grafu.

Cvičení

1.2-1. Dokažte platnost vztahu (1.2) vyjadřujícího asociativnost součinu binárních relací.

(*Odpověď:* Pro libovolná $x, v \in A$ platí

$x\ R \circ (S \circ T)\ v\ \Leftrightarrow$
$\Leftrightarrow\ \exists y : (xRy$ **and** $(y\ S \circ T\ v))$
$\Leftrightarrow\ \exists y : (xRy$ **and** $(\exists z : (ySz$ **and** $zTv)))$
$\Leftrightarrow\ \exists y, z : (xRy$ **and** ySz **and** $zTv)$
$\Leftrightarrow\ \exists z : (\exists y : (xRy$ **and** $ySz)$ **and** $zTv)$
$\Leftrightarrow\ \exists z : (x\ R \circ S\ z)$ **and** $zTv)$
$\Leftrightarrow\ x\ ((R \circ\ S) \circ T)\ v)$

1.2-2. Dokažte platnost vztahu (1.3) o inverzi součinu binárních relací.

(*Odpověď:* Pro libovolná $x, y \in A$ platí

$x\ (R \circ S)^{-1}\ y\ \Leftrightarrow$
$\Leftrightarrow\ y\ (R \circ S)\ x$
$\Leftrightarrow\ \exists z : (yRz$ **and** $zSx)$
$\Leftrightarrow\ \exists z : (zR^{-1}y$ **and** $xS^{-1}z)$
$\Leftrightarrow\ \exists z : (xS^{-1}z$ **and** $zR^{-1}y)$
$\Leftrightarrow\ x\ (S^{-1} \circ R^{-1})\ y)$

1.2-3. Proč je při zavedení mocniny relace důležitá asociativnost součinu relací?

(*Odpověď:* Bez asociativnosti by zápis n-násobného součinu ve tvaru $R \circ R \circ\ \ldots\ \circ R$ (n-krát) neměl smysl, neboť by výsledek součinu závisel na rozmístění vnitřních závorek.)

1.2-4. Pro $R, S, T \subseteq A \times A$ dokažte následující vlastnosti operací s binárními relacemi:
(a) $(R \cup S) \circ T = (R \circ T) \cup (S \circ T),\ \ R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$
(b) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$, $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
(c) $R \subseteq S\ \Rightarrow\ (R \circ T \subseteq S \circ T)$ **and** $(T \circ R \subseteq T \circ S)$

(*Odpověď:* Při důkazu vztahu (a) postupujeme např. takto:

$x\ (R \cup S) \circ T\ z\ \Leftrightarrow$
$\Leftrightarrow\ \exists y : (x\ (R \cup S)\ y$ **and** $yTz)$
$\Leftrightarrow\ \exists y : ((xRy$ **or** $xSy)$ **and** $yTz)$
$\Leftrightarrow\ \exists y : ((xRy$ **and** $yTz)$ **or** $(xSy$ **and** $yTz)$
$\Leftrightarrow\ (\exists y : (xRy$ **and** $yTz))$ **or** $(\exists y : (xSy$ **and** $yTz))$
$\Leftrightarrow\ (x\ R \circ T\ z)$ **or** $(x\ S \circ T\ z)$
$\Leftrightarrow\ x\ ((R \circ T) \cup (S \circ T))\ z$

Důkaz dalších vztahů je analogický.)

1.2-5. Dokažte, že má-li relace R některou z vlastností (RE) až (IR), potom má tutéž vlastnost i relace R^{-1}.

(*Odpověď:* Důkaz se provede využitím množinové charakterizace vlastností a vztahů uvedených v předchozím cvičení. Tak např. platí

(TR) $R \circ R \subseteq R\ \Rightarrow\ (R \circ R)^{-1} \subseteq R^{-1}\ \Leftrightarrow\ R^{-1} \circ R^{-1} \subseteq R^{-1}$,

neboli R^{-1} je rovněž tranzitivní. Podobně postupujeme i u dalších vlastností.)

1.2-6. Které z vlastností (RE) až (IR) má prázdná relace 0_A? Vyjmenujte všechny kombinace vlastností (RE) až (IR), které se mohou současně vyskytnout u nějaké neprázdné relace.

1.2-7. Jak se pro danou relaci $R \subseteq A \times A$ určí nejmenší ekvivalence, která obsahuje R?

1.2-8. Vyslovte tvrzení analogické části (e) věty 1.1 pro vlastnost antisymetrie.

1.2-9. Zjistěte, zda sjednocení, průnik a součin dvou ekvivalencí na množině A jsou opět ekvivalencemi na A.

1.2-10. Pro libovolné kladné celé číslo p definujeme relaci '$\equiv \pmod p$'(nazývanou **kongruence modulo** p) vztahem

$$a \equiv b \pmod p \;\Leftrightarrow_{df}\; \exists k \in \mathbf{Z} : \; (a - b = k.p),$$

Dokažte, že tato relace je ekvivalencí na množině celých čísel $\mathbf{Z}$. Určete třídy rozkladu množiny $\mathbf{Z}$ podle této ekvivalence.

1.2-11. Je možné z libovolné relace $R \subseteq A \times A$ případným doplněním získat relaci uspořádání na A?

1.2-12. Považujeme-li (konečnou) uspořádanou množinu $\langle A, \leq \rangle$ za abecedu, pak můžeme prvky množiny A^* považovat za slova (libovolné délky) nad danou abecedou. Lexikografické uspořádání množiny slov je sice úplné, má však jednu nepříjemnou vlastnost, kterou lze poznat již pro $A = \{a, b\}$: mezi dvěma slovy jako jsou aaa a baa se v lexikografickém uspořádání nachází nekonečně mnoho slov $aaaa, aaab, aaaaa, aaaab, aaaba, aaabb, \ldots$
Zaveďte na A^* jiné úplné uspořádání, které zajistí, že pro libovolná dvě slova $w_1 \preceq w_2$ existuje jen konečně mnoho slov w takových, že $w_1 \preceq w \preceq w_2$.

1.2-13. Potvrďte nebo vyvraťte správnost následující úvahy. Každá symetrická tranzitivní relace $R \subseteq A \times A$ je také reflexivní. Jestliže totiž platí aRb, potom platí i bRa (symetrie) a odtud díky tranzitivitě dostáváme aRa.

1.2-14. Nechť $R \subseteq A \times A$ je tranzitivní a ireflexivní relace. Určete, jakou další vlastnost pak R zaručeně má.

1.2-15. Nechť $\langle A, \leq \rangle$ je neprázdná a konečná uspořádaná množina. Dokažte, že A má alespoň jeden minimální a jeden maximální prvek.

1.2-16. Nechť A, B jsou konečné množiny, $f : A \mapsto B$. Ukažte, že
(a) je-li f injektivní, potom je $|A| \leq |B|$ (b) je-li f surjektivní, potom je $|A| \geq |B|$

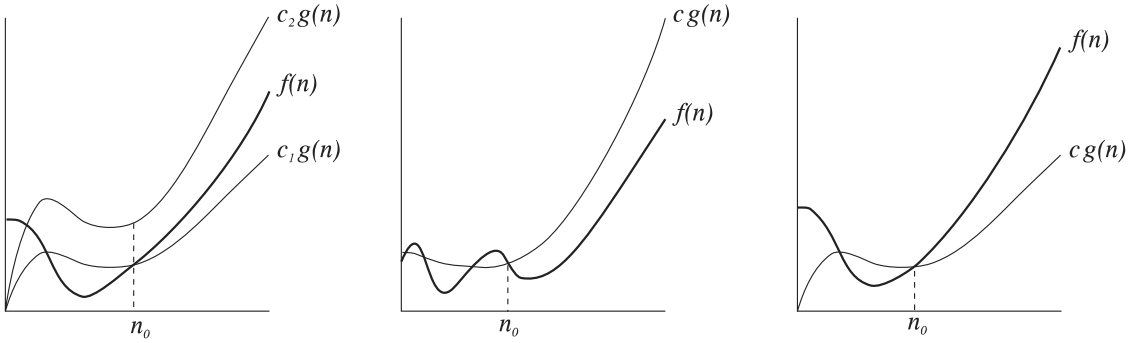
1.2-17. Určete, zda je zobrazení f vyjádřené výrazem $f(x) = x + 1$
(a) bijekcí na množině přirozených čísel $\mathbf{N}$ (b) bijekcí na množině celých čísel $\mathbf{Z}$

1.2-18. Nechť A, B jsou konečné množiny, $|A| = m, |B| = n$. Určete
(a) počet totálních zobrazení $f : A \mapsto B$
(b) počet bijekcí $f : A \mapsto A$
(c) počet totálních injektivních zobrazení $f : A \mapsto B$ (platí-li $m \leq n$)

1.2-19. Nalezněte nějakou bijekci
(a) množiny celých čísel $\mathbf{Z}$ na množinu přirozených čísel $\mathbf{N}$
(b) množiny $\mathbf{N} \times \mathbf{N}$ na $\mathbf{N}$
(c) množiny $\mathbf{Z} \times \mathbf{Z}$ na $\mathbf{N}$

1.3 Řád růstu funkcí

Při určování časové složitosti algoritmů není často možné určit přesnou závislost počtu operací na rozsahu vstupních dat n. Při stejné hodnotě parametru n může navíc délka výpočtu záviset na samotných hodnotách vstupních dat, analyzovat v takovém případě průměrný případ bývá velmi náročné. Spokojíme se proto i s tím, když dokážeme určit asymptotické chování délky nejhoršího výpočtu $T(n)$, tedy jeho závislost na argumentu pro dostatečně veliké hodnoty n. Připomeneme si nyní přesný význam základní matematické notace používané v asymptotických odhadech.



Obrázek 1.1: Řád růstu funkcí

Θ-notace

Pro zadanou funkci $g(n)$ vyjadřuje zápis $\Theta(g(n))$ soubor (množinu) funkcí definovanou vztahem

$$\Theta(g(n)) = \{f(n) : \exists\ c_1, c_2, n_0 > 0\ (0 \leq c_1.g(n) \leq f(n) \leq c_2.g(n) \text{ pro všechna } n \geq n_0)\}$$

Uvedená podmínka vyjadřuje, že od určité hodnoty argumentu n jsou hodnoty funkce $f(n)$ omezeny zdola i shora v pásu ohraničovaném vhodně zvolenými násobky funkce $g(n)$. Přestože je $\Theta(g(n))$ množinou funkcí, píšeme obvykle $f(n) = \Theta(g(n))$, když chceme vyjádřit, že f náleží do příslušné množiny takto omezitelných funkcí. Říkáme také, že $f(n)$ **roste řádově stejně rychle** jako $g(n)$. Obr. 1.1a intuitivně znázorňuje situaci, kdy $f(n) = \Theta(g(n))$.

Vzhledem k podmínce použité v definici $\Theta(g(n))$ je zřejmé, že funkce $g(n)$ musí být asymptoticky nezáporná, jinak by byla množina $\Theta(g(n))$ prázdná. Podobně musí být asymptoticky nezáporná i každá funkce $f(n)$, která roste řádově stejně rychle jako $g(n)$. Tuto vlastnost budeme tedy předpokládat vždy, když použijeme asymptotickou notaci.

Smyslem charakterizace funkcí prostřednictvím zápisu $\Theta(g(n))$ je možnost zanedbat ve vyjádření funkce členy nižších řádů stejně jako koeficient u členu nejvyššího řádu. Ukážeme to na jednoduchém příkladu. Nechť $f(n) = 0.5 * n^2 + 2n + n * \lg n$, potom je $f(n) = \Theta(n^2)$. Abychom to dokázali, musíme nalézt vhodné konstanty c_1, c_2 a n_0 tak, aby platilo [2]

$$c_1 * n^2 \leq 0.5 * n^2 + 2n + n * \lg n \leq c_2 * n^2$$

pro všechna $n \geq n_0$. Můžeme předpokládat kladné n, takže po dělení n^2 dostáváme

$$c_1 \leq 0.5 + 2/n + (\lg n)/n \leq c_2.$$

Bez ohledu na n stačí tedy vzít hodnotu $c_1 = 0.5$, hodnotu c_2 můžeme nastavit libovolně blízko výše, pokud posuneme n_0 dostatečně daleko. Na druhé straně ovšem můžeme ověřit, že platí

$$0.5 * n^2 + 2n + n^2 * \lg n \neq \Theta(n^2), \quad 0.5 * n^2 + 2n + n^2 * \lg n \neq \Theta(n^3).$$

Kdyby totiž existovala c_2 a n_0 splňující podmínku

$$0.5 * n^2 + 2n + n^2 * \lg n \leq c_2 * n^2 \quad \text{pro } n \geq n_0,$$

pak by musela být hodnota výrazu $0.5 + 2/n + \lg n \leq c_2$, což je nemožné, protože hodnota logaritmu roste nade všechny meze. Podobně nelze nalézt kladná c_1 a n_0 tak, aby platilo

$$c_1 * n^3 \leq 0.5 * n^2 + 2n + n^2 * \lg n \quad \text{pro } n \geq n_0.$$

[2] V tomto textu budeme symboly log, ln a lg označovat po řadě dekadický, přirozený a dvojkový logaritmus. S ohledem na asymptotické chování není ovšem mezi těmito funkcemi žádný rozdíl.

Hodnota výrazu $c_1 \leq 0.5/n + 2/n^2 + \lg n/n$ totiž pro rostoucí n klesá k nule.

Snadno lze ukázat, že pro každý polynom $f(n)$ stupně k platí $f(n) = \Theta(n^k)$. Jelikož libovolnou konstantu můžeme považovat za polynom stupně 0, bude mít její asymptotická charakterizace tvar $\Theta(n^0)$ neboli $\Theta(1)$. V posledním zápisu se ovšem nevyskytuje explicite proměnná, při jejímž růstu chování funkce sledujeme – musíme tedy předpokládat, že bude zřejmá z kontextu.

O-notace

V řadě případů bývá obtížné – někdy dokonce nemožné – nalézt asymptotické omezení zkoumané funkce zdola i shora. Při analýze nejhoršího případu se pak snažíme nalézt asymptotickou horní hranici, což odpovídá použití O-notace. Pro zadanou funkci $g(n)$ vyjadřuje zápis $O(g(n))$ soubor (množinu) funkcí definovanou vztahem

$$O(g(n)) = \{f(n) : \exists c, n_0 > 0 \ (0 \leq f(n) \leq c.g(n) \text{ pro všechna } n \geq n_0)\}$$

Stejně jako v případě Θ-notace používáme i zde zápisu $f(n) = O(g(n))$ a říkáme, že funkce $f(n)$ **roste řádově nejvýše tak rychle** jako $g(n)$. Tuto situaci intuitivně znázorňuje obr. 1.1b – pro všechny hodnoty n počínaje n_0 je hodnota $f(n)$ nižší nebo nejvýše rovna hodnotě $c.g(n)$. Z definice i z obrázku je zřejmé, že $f(n) = \Theta(g(n))$ implikuje $f(n) = O(g(n))$, takže je z množinového hlediska možné psát $\Theta(g(n)) \subseteq O(g(n))$. Rozdíl mezi $\Theta(g(n))$ a $O(g(n))$ můžeme ilustrovat na tom, že platí např.

$$0.5 * n^2 + 2n + n^2 * \lg n = O(n^3).$$

Volbu konstant požadovaných podle definice lze provést např. hodnotami $c = 2.5$ a $n_0 = 1$ (při dostatečném zvětšení hodnoty n_0 můžeme konstantu c libovolně snížit).

Pro každý polynom $f(n)$ stupně k platí $f(n) = O(n^s)$, kde $s \geq k$. Při použití O-notace se tedy nemusí nutně jednat o těsnou asymptotickou charakterizaci, ale jen o základní určení horní hranice řádu růstu funkce, která vyjadřuje výpočetní složitost nejhoršího případu výpočtu nějakého algoritmu.

Složitost konkrétního výpočtu běžných algoritmů nezávisí ovšem pouze na délce vstupních dat, ale také na skutečných hodnotách těchto dat. Tak může např. řazení vkládáním proběhnout v čase $O(n)$ (pro seřazenou vstupní posloupnost) nebo v čase $O(n^2)$ (pro opačně seřazenou vstupní posloupnost). Prohlásíme-li tedy, že složitost řazení vkládáním je v nejhorším případě $O(n^2)$, omezujeme tím dobu výpočtu shora pro libovoná vstupní data. Naproti tomu oceněním nejhoršího případu řazení vkládáním jako $\Theta(n^2)$ omezujeme shora a zdola pouze a jen případy nejhorších možných hodnot vstupních dat.

Ω-notace

Při asymptotickém odhadu chování algoritmů v nejlepším případě je užitečné používat Ω-notace. Pro zadanou funkci $g(n)$ vyjadřuje zápis $\Omega(g(n))$ soubor (množinu) funkcí definovanou vztahem

$$\Omega(g(n)) = \{f(n) : \exists c, n_0 > 0 (0 \leq c.g(n) \leq f(n) \text{ pro všechna } n \geq n_0)\}$$

Vztah mezi třemi zavedenými formami asymptotických charakterizací udává následující tvrzení, jehož důkaz vyplyne bezprostředním použitím definic.

Věta 1.5: Pro libovolné funkce $f(n)$ a $g(n)$ platí $f(n) = \Theta(g(n))$, právě když $f(n) = O(g(n))$ a současně $f(n) = \Omega(g(n))$.

Analogicky jako v případě analýzy nejhoršího případu, jestliže oceníme např. nejlepší případ při řazení vkládáním jako $\Omega(n)$, pak i všechny doby výpočtu řazení vkládáním patří do $\Omega(n)$.

Uvedeme nyní stručně další vlastnosti a vzájemné vztahy mezi zavedenými notacemi. Předpokládáme přitom, že všechny používané funkce jsou asymptoticky kladné.

Reflexivita:	$f(n) = \Theta(f(n)) \qquad f(n) = O(f(n)) \qquad f(n) = \Omega(f(n))$
Symetrie:	$f(n) = \Theta(g(n)) \;\Leftrightarrow\; g(n) = \Theta(f(n))$
Tranzitivita:	$f(n) = \Theta(g(n))$ & $g(n) = \Theta(h(n)) \;\Rightarrow\; f(n) = \Theta(h(n))$ $f(n) = O(g(n))$ & $g(n) = O(h(n)) \;\Rightarrow\; f(n) = O(h(n))$ $f(n) = \Omega(g(n))$ & $g(n) = \Omega(h(n)) \;\Rightarrow\; f(n) = \Omega(h(n))$
Inverze:	$f(n) = O(g(n)) \;\Leftrightarrow\; g(n) = \Omega(f(n))$

Funkci $f(n)$ nazýváme **polynomiálně omezenou**, jestliže platí $f(n) = O(n^k)$ pro nějakou konstantu k, což můžeme zapsat také jako $f(n) = n^{O(1)}$. Funkci $f(n)$ nazýváme **polylogaritmicky omezenou**, jestliže platí $f(n) = \log_{O(1)} n$. Je známo, že pro každé $a > 0$ je

$$\lim_{n\to\infty} \log^b n/n^a = 0 \quad \text{pro libovolné } b > 0,$$

tedy logaritmus v libovolné mocnině roste pomaleji než libovolně malá (kladná) mocnina n.

Při odhadech složitosti se používá také iterovaného (dvojkového) logaritmu $\lg^* n$, který se zavede takto: nechť platí

$$\lg^i n = \begin{cases} n & \text{pro } i = 0 \\ \lg(\lg^{(i-1)} n) & \text{pro } i > 0 \text{ a } \lg^{(i-1)} n > 0 \\ \text{nedefinováno} & \text{pro } i > 0 \text{ a } \lg^{(i-1)} n \leq 0 \text{ nebo } \lg^{(i-1)} n \text{ není definováno} \end{cases}$$

Potom pokládáme $\lg^* n = \min\{i \geq 0 : \lg^{(i)} n \leq 1\}$. Iterovaný logaritmus je velmi pomalu rostoucí funkce, což je vidět z několika hodnot uvedených v následující tabulce.

n	2	4	16	65536	2^{65536}
$\lg^* n$	1	2	3	4	5

Pro asymptotické odhady je užitečná rovněž Stirlingova aproximace faktoriálu, která využívá Θ-notaci:

$$n! = \sqrt{2\pi n} * \left(\frac{n}{e}\right)^n * \left(1 + \Theta\left(\frac{1}{n}\right)\right)$$

Odtud vyplývá např. $\lg(n!) = \Theta(n * \lg n)$.

Cvičení

1.3-1. Je funkce $\lfloor \lg n \rfloor !$ polynomiálně omezená? Je funkce $\lfloor \lg \lg n \rfloor !$ polynomiálně omezená? Která funkce je asymptoticky větší: $\lg(\lg^* n)$ nebo $\lg^*(\lg n)$?

Odpověď: Aby bylo $[\lg n]! = O(n^k)$ pro nějaké přirozené k, muselo by platit $[\lg n]! \leq c.n^k$ pro všechna n počínaje nějakým $n_0 > 0$. S použitím Stirlingovy aproximace a po vynechání přechodu na celou část logaritmu dostaneme, že by muselo postupně platit:

$$\begin{aligned} \sqrt{2\pi \lg n} * \left(\frac{\lg n}{e}\right)^{\lg n} &\leq c.n^k \\ \left(\frac{\lg n}{e}\right)^{\lg n} &\leq c.n^k \\ (\lg n)^{\lg n} &\leq c.n^k.e^{\lg n} \\ (\lg n).(\lg \lg n) &\leq \lg c + k.\lg n + (\lg n).\lg e \\ \lg \lg n &\leq K \end{aligned}$$

Hodnoty funkce $\lg \lg n$ však nelze omezit žádnou konstantou, takže původní funkce $[\lg n]!$ nemůže být polynomiálně omezená. Podobným postupem se dokáže, že funkce $[\lg \lg n]!$ již polynomiálně omezená je. Asymptoticky větší je funkce $\lg^*(\lg n)$, jinak řečeno platí

$$\lg(\lg^* n) = O(\lg^*(\lg n)).$$

1.3-2. Mějme polynom $p(n) = a_0 + a_1 * n + a_2 * n^2 + \ \ldots\ + a_r * n^r,\ a_r > 0$ a konstantu $k > 0$. Dokažte platnost vztahů:
(a) je-li $k \geq r$, potom $p(n) = O(n^k)$
(b) je-li $k \leq r$, potom $p(n) = \Omega(n^k)$
(c) je-li $k = r$, potom $p(n) = \Theta(n^k)$

1.3-3. Předpokládejte, že $k \geq 1$ a $b > 1$ jsou konstanty. Pro každou dvojici funkcí $(f(n), g(n))$ v následující tabulce určete, zda platí $f(n) = O$ nebo Ω nebo $\Theta(g(n))$:

$f(n)$	$g(n)$	$f(n) = O(g(n))$	$f(n) = \Omega(g(n))$	$f(n) = \Theta(g(n))$
n^k	b^n	.	.	.
$\sqrt{n}$	$n^{\cos n}$	.	.	.
2^n	$2^{(n/2)}$	.	.	.

(*Odpověď:* (ano, ne, ne), (ne, ne, ne), (ne, ano, ne))

1.3-4. Seřaďte následujících 30 funkcí do pořadí $f_1, f_2, \ \ldots\ , f_{30}$ tak, aby platilo $f_i = \Omega(f_{i+1})$.

$\lg(\lg^* n)$	$2^{\lg^* n}$	$(\sqrt{2})^{\lg n}$	n^2	$n!$	$(\lg n)!$	$(\frac{3}{2})^n$	n^3
$\lg^2 n$	$\lg(n!)$	2^{2^n}	$n^{1/\lg n}$	$\ln\ln n$	$\lg^* n$	$n \cdot 2^n$	$n^{\lg\lg n}$
$\ln n$	1	$2^{\lg n}$	$(\lg n)^{\lg n}$	e^n	$4^{\lg n}$	$(n+1)!$	$\sqrt{\lg n}$
$\lg^*(\lg n)$	$2^{\sqrt{2\lg n}}$	n	2^n	$n \lg n$	$2^{2^{n+1}}$		

1.3-5. Nechť $f(n)$ a $g(n)$ jsou asymptoticky kladné funkce. Dokažte nebo vyvraťte platnost následujících vztahů:
(a) pokud je $f(n) = O(g(n))$, potom je $g(n) = O(f(n))$
(b) $f(n) + g(n) = \Theta(\min(f(n), g(n)))$
(c) nechť $\lg(g(n)) > 0$ a $f(n) > 1$ pro všechna dostatečně veliká n, potom z $f(n) = O(g(n))$ plyne $\lg(f(n)) = O(\lg(g(n)))$
(d) pokud $f(n) = O(g(n))$, potom je $2^{f(n)} = O(2^{g(n)})$
(e) $f(n) = O((f(n))^2)$
(f) $f(n) = \Theta(f(n/2))$