INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

DISKRÉTNÍ MATEMATIKA PRO INFORMATIKY

URČENO PRO VZDĚLÁVÁNÍ V AKREDITOVANÝCH STUDIJNÍCH PROGRAMECH

IVAN KŘIVÝ

ČÍSLO OPERAČNÍHO PROGRAMU: CZ.1.07
NÁZEV OPERAČNÍHO PROGRAMU:
VZDĚLÁVÁNÍ PRO KONKURENCESCHOPNOST
OPATŘENÍ: 7.2
ČÍSLO OBLASTI PODPORY: 7.2.2

INOVACE VÝUKY INFORMATICKÝCH PŘEDMĚTŮ VE STUDIJNÍCH PROGRAMECH OSTRAVSKÉ UNIVERZITY

REGISTRAČNÍ ČÍSLO PROJEKTU: CZ.1.07/2.2.00/28.0245

OSTRAVA 2012

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky

Recenzent: Doc. Ing. František Huňka, CSc.

Název:	Diskrétní matematika pro informatiky
Autor:	Prof. RNDr. Ing. Ivan Křivý, CSc.
Vydání:	první, 2012
Počet stran:	119

Jazyková korektura nebyla provedena, za jazykovou stránku odpovídá autor.

© Ivan Křivý
© Ostravská univerzita v Ostravě

ANOTACE

Předkládaná distanční opora představuje úvod do diskrétní matematiky. Je určena především studentům kombinovaného a distančního studia v následujících bakalářských studijních programech akreditovaných na Přírodovědecké fakultě Ostravské univerzity v Ostravě: *Informatika* a *Aplikovaná informatika*.

Zahrnuje následující témata:

- **základní pojmy** (množiny, relace, funkce, matematická indukce),
- **kombinatorika a její aplikace**,
- **logické funkce**,
- **Booleova algebra a její vlastnosti**,
- **úvod do teorie grafů**.

ÚVOD

Předkládaná distanční opora (modul), která se Vám dostává do ruky, byla vytvořena inovací původní opory v rámci projektu „Inovace výuky informatických předmětů ve studijních programech Ostravské univerzity“, reg. číslo CZ.1.07/2.2.00/28.0245. V souvislosti s inovací byly provedeny následující změny:

Inovace modulu

- upravena struktura celé distanční opory,
- nově zařazeny řešené úlohy, úkoly k procvičení učiva, kontrolní otázky do všech kapitol,
- nově zařazený korespondenční úkoly, autotest a výsledky autotestu.

Inovovaná opora plně pokrývá požadavky učebních osnov povinných předmětů 2DIMA a XDIMA pro posluchače distančního a kombinovaného studia ve studijních programech *Informatika* a *Aplikovaná informatika* na Přírodovědecké fakultě Ostravské univerzity. Tato opora může být samozřejmě použita jako vhodný studijní materiál i pro studenty prezenční formy studia v rámci předmětu DIMAN.

Poslání modulu

Cíle modulu:
Po prostudování tohoto modulu:

- rozšíříte své středoškolské znalosti o množinách, relacích a funkcích,
- osvojíte si základní principy kombinatoriky a schopnost řešit kombinatorické úlohy,
- pochopíte základy teorie logických funkcí a naučíte se využívat je při řešení praktických úloh,
- seznámíte se s Booleovou algebrou a jejími vlastnostmi,
- pochopíte základní pojmy z teorie grafů a osvojíte si postupy k řešení jednodušších úloh z této oblasti.

Celý modul je rozčleněn do následujících lekcí:

Obsah modulu

- základní pojmy diskrétní matematiky a matematická índukce,
- variace, permutace, kombinace, kombinatorické principy,
- kombinační čísla a kombinatorické počítání,
- logické funkce a formule, ekvivalence formulí,

- princip duality a rozklad booleovských funkcí podle proměnných,
- funkcionální úplnost a uzavřenost,
- uspořádané množiny, svazy,
- Booleova algebra a booleovské funkce,
- základní pojmy teorie grafů,
- isomorfismus grafů a reprezentace grafů,
- souvislost grafu a základní typy podgrafů,
- eulerovské grafy.
- opakování učiva a příprava ke zkoušce.

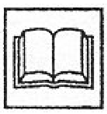
Struktura modulu

U jednotlivých lekcí jsou dodržena následující pravidla:

- specifikace cílů lekce (tedy toho, co by měl student po jejím prostudování umět, znát, pochopit),
- vlastní výklad učiva,
- řešené příklady,
- kontrolní úkoly (otázky, příklady) k procvičení učiva,
- korespondenční úkoly.

Zařazené korespondenční úkoly jsou určeny k ověření Vašich schopností aplikovat získané teoretické znalosti na analýzu řešení konkrétních úloh. Nutnou součástí Vašich studijních povinností je odevzdání korespondenčních úkolů; jejich hodnocení bude započteno do celkového hodnocení kurzu.

V každé kapitole je uvedeno vše potřebné pro samostatné studium, počínaje definicemi základních pojmů a konče využitím teoretických poznatků v praxi. V zájmu správného pochopení probírané látky jsou jednotlivá témata doplněna řešením typových příkladů. Doporučujeme čtenáři, aby se nad každým příkladem důkladně zamyslel. Pochopení principů řešení je totiž nezbytným předpokladem pro porozumění dalšímu výkladu. Čas potřebný k prostudování a procvičení učiva jednotlivých lekcí neuvádíme, neboť z našich zkušeností vyplývá, že rychlost studia značně záleží na Vašich schopnostech a studijních návycích.



Předpokládáme, že si mnozí z Vás budou chtít doplnit a rozšířit poznatky studiem dalších literárních pramenů (učebnic a skript), jež se zabývají jak teorií, tak i aplikacemi. Při výkladu jsme vycházeli především z monografie J. Matouška a J. Nešetřila [15], monografie S. V.

Jablonského [6] a vysokoškolských skript kolegyně Konečné [7, 8]. Některé řešené příklady a úkoly k procvičení učiva jsou převzaty z vysokoškolských skript orientovaných na diskrétní matematiku [1, 2, 3, 5, 10, 11, 12, 14 a 18]. Publikace použité v textu této distanční opory uvádíme v části nazvané „Literatura“. Další publikace a uvedené v části „Doporučená a rozšiřující literatura“, jsou určeny k doplnění Vašich základních znalosti z diskrétní matematiky. Věříme, že předkládaný studijní materiál pomůže pochopit základy diskrétní matematiky, a přejeme Vám hodně úspěchů ve studiu.

Autor

Autor děkuje touto cestou recenzentovi za pečlivé pročtení rukopisu a řadu cenných připomínek směřujících ke zkvalitnění předkládaného učebního textu.

1 ZÁKLADNÍ POJMY

Po prostudování této kapitoly:

- si rozšíříte a doplníte své středoškolské znalosti v oblasti množin, relací a funkcí,
- pochopíte význam matematické indukce a naučíte se jí využívat při dokazování vlastností přirozených čísel.

Klíčová slova: množina, prázdná množina, mohutnost množiny, potenční množina, podmnožina, skládání množin, průnik množin, rozdíl množin, doplněk množiny, kartézský součin množin, binární relace, relace z množiny do množiny, relace na množině, inverzní relace, komplementární relace, skládání relací, kartézský graf, šachovnicový graf, uzlový graf, matice sousednosti, relace reflexivní, relace symetrická, relace asymetrická, relace antisymetrická, relace tranzitivní, ekvivalence, částečné uspořádání, ostré uspořádání, funkce jako relace, skládání funkcí, funkce injektivní, funkce surjektivní, funkce bijektivní, matematická indukce.

V první části této kapitoly si doplníte své znalosti z teorie množin, relací a funkcí. Zvláštní pozornost věnujte relacím, zejména relacím ekvivalence a částečného uspořádání, protože získané poznatky budeme využívat jak při výkladu teorie booleovských (logických) funkcí, tak v úvodu do teorie grafů. Druhá část kapitoly bude věnována problematice matematické indukce. Je velmi důležité, abyste pochopili princip matematické indukce a naučili se ji využívat k dokazování vlastností přirozených čísel.

1.1 Množiny

Množina

Pod pojmem **množiny** se intuitivně rozumí soubor nějakých objektů (prvků množiny). Ve skutečnosti pojem množiny patří k tzv. primitivním pojmům, jež se nedefinují pomocí jiných, dříve zavedených pojmů. Množiny se obvykle označují písmeny velké abecedy (např. A, B, C, ...) a skutečnost, že prvek a patří (nepatří) do množiny A se zapisuje jako $a \in A$ ($a \notin A$). V diskrétní matematice se zpravidla pracuje se třemi číselnými množinami: množinou čísel přirozených ($\mathbb{N}$), čísel celých ($\mathbb{Z}$) a reálných ($\mathbb{R}$).

Množiny se zapisují dvěma způsoby: výčtem prvků (např. {1, 4, 9, ...}) nebo vyznačením vlastnosti, kterou mají všechny prvky dané množiny (např. $\left\{n^2; n \in \mathbb{N}\right\}$).

Prázdná množina

Zvláštní postavení má **množina prázdná**, tj. množina neobsahující žádný prvek. Taková množina existuje pouze jediná a označuje se $\varnothing$.

Mohutnost množiny

Důležitou charakteristikou každé množiny je její **mohutnost** neboli **kardinalita**, která udává počet prvků dané množiny. Mohutnost množiny X se zpravidla označuje $|X|$. Tato charakteristika se definuje i pro nekonečné množiny.

Potenční množina

Často se uvažují i množiny, jejichž prvky jsou samy o sobě také množinami. Typickým příkladem takové množiny je množina všech podmnožin nějaké množiny *X*, tzv. **potenční množina** množiny *X*, jež se označuje $\mathcal{P}(X)$.

Vztahy mezi množinami

Dvě libovolné množiny *A* a *B* jsou si rovny, právě když obsahují identické prvky. Takový vztah se nazývá **rovnost množin** a označuje $A = B$. Jestliže každý prvek množiny *A* je také prvkem množiny *B*, pak říkáme, že množina A je **podmnožinou** množiny *B*, což značíme $A \subseteq B$. Tento vztah (relace) se nazývá množinová inkluze. Pokud platí $A \neq B$, je *A* **vlastní podmnožinou** *B* a píšeme $A \subset B$. Každá neprázdná množina má právě dvě **triviální podmnožiny**: sebe samu a prázdnou množinu.

Operace s množinami

Pro libovolné dvě množiny *A* a *B* můžeme definovat řadu binárních operací. Jejich **průnik** $A \cap B$ je množina všech prvků náležejících současně do *A* i *B*. **Sjednocením** $A \cup B$ těchto množin je množina všech prvků, které náležejí do A nebo do B nebo obou současně. **Rozdíl** $A \backslash B$ uvažovaných množin je množina všech prvků ležících v *A*, ale nikoliv v *B*. **Doplňkem** množiny B v množině A je právě množina $A \backslash B$, tj. množina všech prvků množiny *A*, které nepatří do množiny *B*. **Symetrický rozdíl** obou uvažovaných množin je definován jako $(A \setminus B) \cup (B \setminus A)$. Obě tyto operace mohou být definovány pro libovolný (i nekonečný) počet operandů. Tak např. sjednocení (průnik) množin $A_1, A_2, \ldots, A_n$ se zapisuje $\bigcup_{i=1}^{n} A_i$ ($\bigcap_{i=1}^{n} A_i$).Pro operace průniku a sjednocení platí mimo jiné zákony komutativní i asociativní. Navíc jsou obě zmíněné operace provázány distributivním zákonem, takže platí:

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

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

Platnost uvedených vztahů lze ověřit pomocí Vennova diagramu.

Neuspořádaná dvojice prvků a, b se značí $\{a,b\}$ a představuje obyčejnou dvouprvkovou množinu, v níž na pořadí prvků samozřejmě nezáleží. Naproti tomu v **uspořádané dvojici** těchto prvků, která se označuje (a,b), na tomto pořadí záleží: prvek a je prvním prvkem, kdežto prvek b prvkem druhým.Platí: $(a,b)=(c,d)$, právě když $a=c$ a $b=d$. Tuto uspořádanou dvojici však můžeme zapsat pomocí neuspořádané dvojice takto: $(a,b)=\{\{a\},\{a,b\}\}$. Analogicky se definuje i uspořádaná n-tice prvků.

Uspořádaná dvojice prvků

Kartézský součin množin

Definice 1.1. Kartézský součin $A\times B$ **množin** A a B je množina všech uspořádaných dvojic (a,b), kde $a\in A$ a $b\in B$, tedy

$$A\times B=\{(a,b);a\in A,b\in B\}.$$

Kartézský součin se zavádí nejen pro číselné množiny, ale pro libovolné konečné množiny. Pojem kartézského součinu můžeme rozšířit na libovolných n množin takto:

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

Speciálním případem je n-tá kartézská mocnina množiny A, která se zapisuje ve tvaru

$$A^n=A\times A\times \ ...\ \times A=\{(a_1,a_2,\ ...\ a_n),a_i\in A,i=1,2,\ ...,n\}.$$

Úkoly.

1. Za jakých podmínek platí pro množiny následující rovnosti:
   a) $A\cap B=A,$
   b) $A\cup B\cup C=A,$
   c) $A\cup B=A.$
2. Zjednodušte výraz $(A\cup B)\cap(B\cup C)$.
3. Dokažte platnost množinové rovnosti
   $$(A\cup B)\cap(A\cup C)\cap(B\cup C)=(A\cap B)\cup(A\cap C)\cup(B\cap C).$$
4. Vztah $(A\cup B)\setminus B$ obecně neplatí. Vyšetřete, za jakých podmínek skutečně platí.

1.2 Relace

S využitím pojmu kartézského součinu můžeme definovat jeden ze základních pojmů matematiky, pojem relace.

Relace z množiny A do množiny B

Definice 1.2.1. Nechť A, B jsou množiny. Pak libovolná podmnožina R kartézského součinu $A \times B$ se nazývá (**binární relace**) **z množiny *A* do množiny *B*.** Skutečnost, že uspořádaná dvojice (a,b) je prvkem relace R se zapisuje obvykle ve tvaru $(a,b) \in R$. Je-li $A = B$, pak R se nazývá (**binární**) **relace na množině A**, tedy $R \subseteq A \times A = A^2$.

Relace na množině A

Vedle binární relace existuje i ***n*-ární relace na množině A** definovaná vztahem $R \subseteq A^n$.

Speciální případy relace:

- **relace prázdná**, která neobsahuje žádné uspořádané dvojice ($R = \varnothing$),
- **relace univerzální**, která naopak obsahuje všechny uspořádané dvojice ($R = A \times B$, resp. $R = A^2$),
- **relace identická** (označení *id*) je taková relace na množině A, která obsahuje všechny uspořádané dvojice typu $(a,a) \subseteq A^2$.

Inverzní relace

Nechť $R \subseteq A \times B$. Pak **inverzní relace** (R^{-1}) k relaci R je relace tvořená všemi uspořádanými dvojicemi (b,a) takovými, že uspořádané dvojice $(a,b) \in R$.

Komplementární relace

Podobně **komplementární relace** (R') **k relac**i R je relace tvořená všemi uspořádanými dvojicemi (a,b) takovými, že uspořádané dvojice $(a,b) \notin R$.

Úkol. Je dána relace $R = \{(m,n) \in \mathbb{N}^2; m = n^2\}$. Určete relaci inverzní a komplementární.

Skládání relací

Nechť $R \subseteq A \times B$ a $S \subseteq B \times C$ jsou nějaké relace. Pak **složením** ($R \circ S$) **relací *R* a *S*** v tomto pořadí je relace tvořená všemi uspořádanými dvojicemi (a,c), pro které existuje nějaké $b \in B$ takové, že uspořádané dvojice $(a,b) \in R$ a uspořádané dvojice $(b,c) \in S$.

Úkol. Určete relaci $R \circ S$, jestliže $R = \{(m,n) \in \mathbb{N}^2; m = n^2\}$ a $S = \{(n,p) \in \mathbb{N}^2; p = \sqrt{n}\}$.

*Poznámka***.** Pro skládání relací neplatí obecně komutativní zákon. Složení relací není definováno pro každé dvě relace; vždy musí existovat společná „prostřední“ množina (v našem případě B). Jsou-li obě relace R i S na téže množině, je jejich složení vždy definováno.

Existuje několik způsobů, jak reprezentovat relace:

- grafické (kartézský graf, šachovnicový graf, uzlový graf),
- algebraický (matice sousednosti).

Kartézský graf

Nechť je dána relace $R \subseteq A \times B.$, kde $A = \{a_1, a_2\ ..., a_n\}$ a $B = \{b_1, b_2,\ ..., b_m\}$. Při konstrukci **kartézského grafu** vycházíme z mřížky (v kartézské soustavě souřadnic) definované vertikálními přímkami $x_i = a_i,\ i = 1, 2,\ ...,\ n,$ a horizontálními přímkami $y_j = b_j,\ j = 1, 2,\ ..., m.$ Všechny možné uspořádané dvojice jsou reprezentovány průsečíky těchto přímek. Ty dvojice, které náležejí do dané relace R, se označí např. malými kroužky.

Šachovnicový graf

V případě **šachovnicového grafu** se vychází ze šachovnice, jejíž sloupce odpovídají hodnotám a_i a řady hodnotám b_j. Pak čtvercová pole nacházející se v i-tém sloupci a j-té řadě reprezentují uspořádané dvojice (a_i, b_j). Pro dvojice náležející dané relaci R se příslušná pole vyšrafují, nebo vybarví.

Uzlový graf

Uzlový graf se používá k reprezentaci relace R na množině $A = \{a_1, a_2\ ..., a_n\}$. Jednotlivé prvky množiny A se reprezentují malými kroužky nebo puntíky. Pokud nějaká uspořádané dvojice (a_i, a_j) náleží relaci R, vyznačí se tato skutečnost šipkou směřující od a_i do a_j. V případě $a_i = a_j$ se zakreslí smyčka od a_i do a_i.

Matice sousednosti

Relaci R na množině $A = \{a_1, a_2\ ..., a_n\}$ lze vhodně reprezentovat tzv. **maticí sousednosti**. Je to čtvercová matice $\mathbf{A} = (a_{ij})$, pro jejíž prvky platí:

$$a_{ij} = \begin{cases} 1,\ \text{jestliže}\ (a_i, a_j) \in R, \\ 0,\ \text{jestliže}\ (a_i, a_j) \notin R. \end{cases}$$

Příklad 1.2.1. Pro ilustraci určíme matici sousednosti pro relaci $R = \{(1,2), (1,3), (2,1), (2,4), (3,4), (4,2), (4,4)\}$ na množině $A = \{1, 2, 3, 4\}$. Tato matice má tvar

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Úkol. Vytvořte kartézský, šachovnicový i uzlový graf odpovídající relaci R z předcházejícího příkladu.

Vlastnosti relace

Definice 1.2.2. Relace R na množině A je:

- **reflexivní**, jestliže pro každé $a \in A$ platí $(a,a) \in R$,
- **irreflexivní,** jestliže pro každé $a \in A$ platí $(a,a) \notin R$,
- **symetrická**, jestliže pro každá $a_1, a_2 \in A$ platí: pokud $(a_1, a_2) \in R$, pak $(a_2, a_1) \in R$,
- **asymetrická,** jestliže pro každá $a_1, a_2 \in A$ platí: pokud $(a_1, a_2) \in R$, pak $(a_2, a_1) \notin R$,
- **antisymetrická**, jestliže pro každá $a_1, a_2 \in A$ platí: pokud $(a_1, a_2) \in R$ a současně $(a_2, a_1) \in R$, pak $a_1 = a_2$,
- **tranzitivní,** jestliže pro každá $a_1, a_2, a_3 \in A$ platí: pokud $(a_1, a_2) \in R$ a současně $(a_2, a_3) \in R$, pak $(a_1, a_3) \in R$.

Ekvivalence

Definice 1.2.3. Relace R na množině A je **ekvivalence**, jestliže je reflexivní, symetrická a tranzitivní.

Uvažujme relaci R na množině $\mathbb{Z}$ definovanou předpisem:

$$(a,b) \in R, \text{ právě když } n \mid (a-b),$$

kde n je přirozené číslo. Říkáme, že prvek a je kongruentní s prvkem b modulo n, když rozdíl $(a-b)$ je dělitelný číslem n. Tato relace se nazývá kongruence a zapisuje se ve tvaru $a \equiv b \ (\text{mod}\,\text{ulo}\ n)$.

Příklad 1.2.2. Dokážeme, že takto definovaná relace je ekvivalence, tj. je reflexivní, symetrická a tranzitivní.

Nechť $a \in \mathbb{Z}$, rozdíl $(a-a)$ je dělitelný n, tj. platí $n \mid (a-a)$. To znamená, že prvek a je kongruentní sám se sebou *modulo* n. Relace R je tedy reflexivní.

Nechť $a,b \in \mathbb{Z}$ a rozdíl $(a-b)$ je dělitelný číslem n, tj. $n|(a-b)$. To však platí právě tehdy, když $n|-(a-b)$, což je totéž jako $n|(b-a)$. Relace R je proto symetrická.

Nechť $a,b,c \in \mathbb{Z}$. Nechť dále platí $n|(a-b)$ a současně $n|(b-c)$. Pak existují nějaká $k,l \in \mathbb{Z}$ taková, že platí $a = nk + b = nk + nl + c = n(k+l) + c$, a tudíž $n|(a-c)$. Odtud plyne tranzitivita relace R.

Úkoly.

1. Uvažujte relaci R na množině $\mathbb{R}$ definovanou předpisem $(a,b) \in R$, právě když $a = b$ (rovnost reálných čísel). Dokažte, že tato relace je ekvivalence.
2. Nechť $\mathcal{P}(X)$ je množina všech podmnožin neprázdné množiny X. Uvažujte na této množině relaci R definovanou předpisem $(A,B) \in R$, právě když $A = B$ (množinová rovnost). Dokažte, že tato relace je ekvivalence.

Částečné uspořádání

Definice 1.2.4. Relace R na množině A je **částečné uspořádání (uspořádání)**, jestliže je reflexivní, antisymetrická a tranzitivní.

Příklad 1.2.3. Budeme uvažovat relaci R na množině $\mathbb{Z}$ danou předpisem $(a,b) \in R$, právě když $a \le b$ ("neostrá" nerovnost).

Dokážeme, že tato relace je částečné uspořádání.
Pro libovolné $a \in \mathbb{Z}$ zřejmě platí $a \le a$, takže daná relace je reflexivní,
Nechť jsou dána libovolná $a,b \in \mathbb{Z}$ taková, že $a \le b$. Jestliže zároveň platí také $b \le a$, pak nutně musí platit $a = b$. Odtud plyne, že uvažovaná relace je antisymetrická.
Zvolme libovolná $a,b,c \in \mathbb{Z}$ tak, aby platilo $a \le b$ a současně $b \le c$. To ovšem znamená, že platí $a \le b \le c$, neboli $a \le c$. Tím je dokázáno, že daná relace je tranzitivní.

Úkoly.

1. Uvažujte relaci R na množině všech podmnožin neprázdné množiny X danou takto: $(A,B) \in R$, právě když $A \subseteq B$ (množinová inkluze). Dokažte, že uvedená relace je částečné uspořádání.
2. Nechť je dána relace R na množině všech nenulových celých čísel předpisem $(a,b) \in R$, právě když $a|b$ ("a dělí b"). Dokažte, že tato relace je částečné uspořádání.

Definice 1.2.5. Relace R na množině A je **„ostré“ uspořádání**, jestliže je reflexivní, asymetrická a tranzitivní.

Úkol. Je dána relace R na množině $\mathbb{R}$ definovaná předpisem $(a,b)\in R$, právě když $a<b$. Dokažte, že jde o „ostré“ uspořádání.

1.3 Funkce

Funkce (zobrazení) je jedním ze základních pojmů matematiky. Pojem funkce zde zavedeme netradičně, a to jako speciální typ relace.

Funkce

Definice 1.3.1. **Funkce *f* z množiny *X* do množiny *Y*** ($f : X \to Y$) je binární relace $f \subseteq X \times Y$, která splňuje dodatečnou podmínku, že pro každý prvek $x \in X$ existuje právě jeden prvek $y \in Y$, pro nějž platí $(x,y)\in f$.

Funkce se zpravidla zobrazují obyčejným grafem y vs. x v kartézské soustavě souřadnic, ale v případě diskrétního definičního oboru X lze s výhodou používat stejných prostředků jako při zobrazování relací.

Skládání funkcí

Skládání funkcí se provádí stejně jako u relací, přitom se ovšem používá jiné značení. Jestliže jsou dány dvě funkce $f : X \to Y$ a $g : Y \to Z$, pak můžeme pro každé $x \in X$ definovat novou (složenou) funkci $h : X \to Z$ předpisem $h(x) = g\left(f(x)\right)$. Tato **složená funkce** se zapisuje ve tvaru $(g \circ f)(x)$.

Pro skládání funkcí platí zákon asociativní, ale nikoliv komutativní. Je-li např. definována funkce $g \circ f$, pak funkce $f \circ g$ nemusí být vůbec definována.

Definice 1.3.2. Funkce $f : X \to Y$ se nazývá:

Funkce prostá

- **prostá** (**injektivní**), jestliže pro každá $x_1 \neq x_2$ platí $f(x_1) \neq f(x_2)$,

Funkce surjektivní

- **funkce na** (**surjektivní**), jestliže pro každé $y \in Y$ existuje $x \in X$ takové, že $f(x) = y$,

Funkce bijektivní

- **vzájemně jednoznačná** (**bijektivní**), jestliže je zároveň prostá a na.

Pro skládání funkcí platí následující tvrzení.

Věta 1.3.1. Nechť $f : X \to Y$ a $g : Y \to Z$ jsou funkce. Pak platí:

- jestliže *f* i *g* jsou prosté funkce, je také $f \circ g$ prostá funkce;
- jestliže *f* i *g* jsou surjektivní funkce na, je také $f \circ g$ surjektivní;

- jestliže f i g jsou vzájemně jednoznačné funkce, je také $f \circ g$ vzájemně jednoznačná funkce.

Příklad 1.3.1. Důkazy uvedených tvrzení jsou jednoduché; vycházejí přímo z definice. Pro ilustraci dokážeme druhé z nich. Zvolíme tedy nějaké $z \in Z$ a hledáme $x \in X$, pro které platí $(g \circ f)(x) = z$. Protože g je funkce surjektivní, musí existovat $y \in Y$ takové, že $g(y) = z$. Ale f je také funkce surjektivní, proto musí existovat $x \in X$, které splňuje $f(x) = y$. Takové x je pak hledaný prvek, pro nějž platí $(g \circ f)(x) = z$.

Úkoly.

1. Dokažte obě zbývající tvrzení.
2. Nechť X je konečná množina. Pak funkce $f: X \to X$ je prostá, právě když je surjektivní. Dokažte.
3. Najděte příklad prosté funkce $f: \mathbb{N} \to \mathbb{N}$, která není surjektivní.

Další úlohy k procvičení středoškolských znalostí o množinách, relacích a funkcích lze nalézt v učebních textech [1, 3, 5, 10, 12].

1.4 Matematická indukce

Matematická indukce se užívá pro důkazy vět typu $\forall x \in \mathbb{N}, n \geq n_0 : V(n)$, kde $V(n)$ je výroková forma proměnné n a n_0 pevně zvolené přirozené číslo. Tato metoda důkazu vychází z tzv. principu matematické indukce, který je jedním z Peanových axiomů teorie přirozených čísel.

Peanovy axiomy lze (poněkud zjednodušeně) formulovat takto:

1. Číslo 0 je přirozené číslo.
2. Ke každému přirozenému číslu *n* existuje přirozené číslo *n'*, které je jeho následovníkem.
3. Číslo 0 není následovníkem žádného přirozeného čísla.
4. Různá přirozená čísla mají různé následovníky.
5. Nechť platí, že nějakou vlastnost má číslo 0 a navíc z toho, že ji má přirozené číslo *n*, plyne, že ji má také jeho následovník *n'*, pak tuto vlastnost mají všechna přirozená čísla.

Princip mat. indukce

Princip matematické indukce (viz [15]). Nechť X je množina přirozených čísel, pro kterou platí:

- $1 \in X$.
- Je-li $n \in X$, pak také $n+1 \in X$.

Potom X je množina všech přirozených čísel, tj. $X = \mathbb{N}$.

Důkaz matematickou indukcí se provádí ve dvou krocích:

1. krok. Daná vlastnost se dokáže pro nejmenší přirozené číslo, které přichází v úvahu, zpravidla pro $n = 1$.

2. krok (indukční krok). Vychází se z předpokladu (indukčního předpokladu), že tato vlastnost platí pro nějaké $n = n_0$, a následně se dokáže, že platí též pro $n = n_0 + 1$.

Matematická indukce je jedním ze základních důkazových prostředků v matematice. Použití matematické indukce ilustrujeme na několika jednoduchých příkladech.

Příklad 4.1.1. Dokážeme, že pro všechna $n \geq 1$ platí $\sum_{i=1}^{n} i = 1 + 2 + \ ... \ + n = n(n+1)/2$.

V 1. kroku ověříme platnost vztahu pro $n = 1$. Dostaneme $1 = 1.2/2$, tj. vztah platí..

Předpokládáme, že vztah platí pro nějaké $n = n_0$, takže $\sum_{i=1}^{n_0} i = n_0(n_0+1)/2$.

Dokážeme jeho platnost i pro $n = n_0 + 1$. Postupně dostaneme:

$$\sum_{i=1}^{n_0+1} i = \sum_{i=1}^{n_0} i + (n_0+1) = n_0(n_0+1)/2 + (n_0+1) = (n_0+1)(n_0+2)/2.$$

Tímto je platnost vztahu dokázána pro všechna $n \in \mathbb{N}$.

Příklad 4.1.2. Dokážeme, že pro všechna přirozená čísla $n \geq 1$ je číslo $6^{2n} + 3^{n+2} + 3^{n}$ dělitelné 11.

Pro $n = 1$ platí $6^2 + 3^3 + 3^1 = 36 + 27 + 3 = 66 = 6 \cdot 11$, takže uvedené tvrzení platí.

Nechť toto tvrzení platí pro nějaké $n = n_0$. Potom $6^{2(n_0+1)} + 3^{n_0+3} + 3^{n_0} = 6^{2n_0}.36 + 3^{n_0+2}.3 + 3^{n_0}.3 = 3\left(6^{2n_0} + 3^{n_0+2} + 3^{n_0}\right) + 33 \cdot 6^{2n_0}$.

Výsledné číslo je skutečně dělitelné 11, protože oba sčítance jsou dělitelné 11.

Úkoly.

1. Dokažte matematickou indukcí $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{1.2.3}$.

2. Dokažte mat. indukcí $1.2 + 2.3 + \ \dots\ + n(n+1) = \frac{1}{3} n(n+1)(n+2)$.

3. Dokažte matematickou indukcí, že pro $n \geq 3$ platí $2^n > 2n+1$.

Někdy se může stát, že ve formulaci vlastnosti, kterou je třeba dokázat, vystupují dvě proměnné pro přirozená čísla. V takových případech jednu proměnnou zafixujeme (přidělíme jí pevnou hodnotu) a důkaz provedeme pro druhou.

Kontrolní otázky

1. Kolik prvků má potenční množina množiny *X*, jestliže *X* □*n*?
2. Jaký je rozdíl mezí neuspořádanou a uspořádanou *n*-ticí prvků?
3. Ukažte, že pro skládání binárních relací neplatí obecně komutativní zákon.
4. Jaké jsou základní způsoby grafické reprezentace relace?
5. Je možné reprezentovat relaci z množiny do množiny pomocí matice sousednosti?
6. Jaké jsou základní vlastnosti relací na množině?
7. Srovnejte klasickou (středoškolskou) definici funkce s definicí 1.3.1.
8. Vysvětlete princip matematické indukce.
9. Jaký je postup při důkazu matematickou indukcí?

Pojmy k zapamatování:

- množina,
- prázdná množina,
- mohutnost množiny,
- potenční množina,
- podmnožina,
- sjednocení množin,
- průnik množin,
- rozdíl množin,
- doplněk množiny,
- uspořádaná dvojice prvků,
- kartézský součin,
- relace z množiny do množiny,
- relace na množině,

- inverzní relace,
- komplementární relace,
- skládání relací,
- kartézský graf,
- šachovnicový graf,
- uzlový graf,
- matice sousednosti pro relaci na množině,
- relace reflexivní,
- relace symetrická,
- relace asymetrická,
- relace antisymetrická,
- relace tranzitivní,
- ekvivalence,
- částečné uspořádání,
- ostré uspořádání,
- funkce jako relace,
- skládání funkcí,
- funkce prostá (injektivní),
- funkce na (surjektivní),
- funkce vzájemně jednoznačná (bijektivní),
- matematické indukce.

Shrnutí

V této úvodní kapitole jsou rozšířeny a doplněny středoškolské znalosti o množinách, relacích i funkcích. Zvláštní pozornost je věnována principu matematické indukce a jejímu využití při dokazování vlastností přirozených čísel. Je velmi důležité, abyste vše správně pochopili. Věnujte této části mimořádnou pozornost a teprve, až se ujistíte, že jste všemu porozuměli, přistupte ke studiu dalších kapitol.

2 KOMBINATORIKA

Po prostudování této kapitoly:

- si doplníte znalosti o variacích, permutacích a kombinacích (bez opakování i s opakováním) a naučíte se těchto znalostí využívat při výpočtech klasické pravděpodobnosti jevů,
- pochopíte základní kombinatorické principy (princip součtu, princip součinu, princip inkluze a exkluze) a osvojíte si jejich aplikaci na řešení kombinatorických úloh,
- poznáte základní vlastnosti binomických koeficientů a jejich význam v diskrétní matematice.

Klíčová slova: variace s opakováním, variace bez opakování, permutace bez opakování, permutace s opakováním, kombinační číslo, kombinace bez opakování, kombinace s opakováním, princip součtu, princip součinu, princip inkluze a exkluze, Dirichletův princip, Pascalův trojúhelník, binomická věta, pravděpodobnost jevu.

Tato kapitola je věnována kombinatorice v širším slova smyslu. Naučíte se pracovat s variacemi, permutacemi, kombinacemi a osvojíte si základní kombinatorické principy. Získané znalosti a praktické dovednosti pak oceníte při studiu následujících kapitol věnovaných především logickým funkcím a základům teorie grafů.

2.1 Variace

Základní pojmy variace, permutace a kombinace zavedeme netradičně, s využitím pojmu zobrazení (funkce). Nejprve dokážeme matematickou indukcí následující větu.

Věta 2.1.1. Libovolná *n*-prvková množina *X* má právě 2^n podmnožin.
Důkaz. Nejprve dokážeme, že věta platí pro $n = 0$. Pro $X = \emptyset$ skutečně existuje jediná podmnožina (prázdná množina), tj. $2^0 = 1$.
Nechť pro *n*-prvkovou množinu *X* platí, že má 2^n podmnožin. Uvažujme $(n+1)-$prvkovou množinu $X \cup \{a\}$. V takovém případě se počet podmnožin zvětší o počet všech podmnožin typu $\xi \cup \{a\}$, kde ξ je libovolná podmnožina množiny *X*. Dostaneme tedy:

$$\left| X \cup \{a\} \right| = 2^n + 2^n = 2.2^n = 2^{n+1}. \qquad \square$$

Věta 2.1. 2. Nechť X a Y jsou konečné množiny takové, že $|X| = k$ a $|Y| = n.$ Pak počet všech možných zobrazení $f : X \to Y$ je roven n^k.

Důkaz. Dokážeme matematickou indukcí vzhledem ke k (při pevně zvoleném n). Nechť X je jednoprvková množina, tedy $k = 1$. Z definice zobrazení plyne, že uvažovaný prvek má právě jediný obraz v množině Y. Existuje tedy právě n různých zobrazení, tj. $n^1 = n$.
Nechť uvedená věta platí pro nějakou k-prvkovou množinu X. Přidáme prvek a, tím vytvoříme $(k+1)-$prvkovou množinu $X \cup \{a\}$. Přidáním prvku a se počet zobrazení pro každé původně uvažované zobrazení $f : X \to Y$ zvětší n-krát, takže celkový počet zobrazení bude $n^k.n = n^{k+1}$. Uvedená věta tedy platí pro každé $n \in \mathbb{N}$. □

Variace s opakováním

Definice 2.1.1. Nechť X a Y jsou konečné množiny takové, že $|X| = k$ a $|Y| = n.$ Pak každé zobrazení $f : X \to Y$ se nazývá **variace *k*-té třídy z *n* prvků s opakováním**. Počet všech variací k-té třídy z n prvků s opakováním je podle předcházející věty roven

$$V_k^*(n) = n^k.$$

Poznámka. Variace s opakováním jsou v podstatě uspořádané k-tice prvků (s opakováním) z množiny Y, které jsou obrazem prvků množiny X v daném zobrazení f.

Příklad 2.1.1. Vypočteme, kolik existuje různých třímístných čísel zapsaných v desítkové soustavě. Je zřejmé, že se číslice mohou opakovat, tj. na každé pozici může být obecně libovolná číslice z množiny $\{0,1,2, ...,9\}$. Proto použijeme vzorce pro variace třetí třídy z 10 prvků: $V_3^*(10) = 10^3$. Vyloučíme-li čísla začínající číslicí 0 na první pozici, dostaneme $9.10.10 = 9.10^2$.

Úkoly.

1. Výtah s r pasažéry zastavuje postupně v n podlažích. Kolika různými způsoby mohou pasažéři vystoupit?
2. Kolik existuje různých matic typu $n \times n$ s prvky z množiny $\{0,1,2, ...,9\}$?

Věta 2.1.3. Nechť X a Y jsou konečné množiny, přičemž $|X| = k$ a $|Y| = n.$ Potom počet všech možných prostých (injektivních) zobrazení $f : X \to Y$ je roven $n(n-1)(n-2)\ ...,\ (n-k+1)$.

Důkaz se provádí analogicky jako u věty 2.1.2. □

Variace bez opakování

Definice 2.1.2. Nechť X a Y jsou konečné množiny, přičemž $|X| = k$ a $|Y| = n$. Pak každé prosté zobrazení $f : X \to Y$ se nazývá **variace *k*-té třídy z *n* prvků bez opakování**. Počet všech variací *k*-té třídy z *n* prvků bez opakování je podle předcházející věty roven

$$V_k(n) = n(n-1)(n-2) \;..., \;(n - k + 1).$$

Poznámka. Variace bez opakování jsou v podstatě uspořádané *k*-tice prvků (bez opakování) z množiny *Y*, které jsou obrazem prvků množiny *X* v daném zobrazení *f*.

Příklad 2.1.2. Určíme počet různých třímístných čísel (zapsaných v desítkové soustavě) takových, že se žádná z číslic nemůže opakovat. Jde zřejmě opět o variace třetí třídy z 10 prvků, ale s podmínkou, že se číslice nesmí opakovat. Obecně platí: $V_3(10) = 10.9.8 = 720$. Jestliže vyloučíme čísla začínající číslicí 0 na první pozici, dostaneme $9.9.8 = 646$.

Úkoly.

1. Dokažte větu 2.1.3 matematickou indukcí.
2. Výtah s *r* pasažéry zastavuje postupně v *n* podlažích. Kolika různými způsoby mohou pasažéři vystoupit za předpokladu, že žádní dva z nich nevystoupí ve stejném podlaží?

2.2 Permutace

Pojem permutace zavedeme jako speciální případ variací pro $k = n$.

Permutace bez opakování

Definice 2.2.1. Variace *n*-té třídy z *n* prvků množiny *X* bez opakování se nazývá **permutace množiny *n* prvků bez opakování**. Jejich počet je (podle věty 2.1.3) roven $P(n) = n(n-1)(n-2) \;...\; 2.1 = n!$,

kde *n*! je funkce definovaná na množině ℕ, přičemž 0! = 1.

Poznámka. Permutace je vlastně prosté zobrazení množiny *X* na sebe.

Předpokládejme, že jsou prvky množiny *X* srovnány v nějakém pořadí. Potom permutace představuje pouhé „přerovnání“ prvků. Uvažujme např. množinu $X = \{a, b, c, d\}$. Jednu z jejich možných permutací můžeme zapsat takto:

$$\pi = \begin{pmatrix} a\ b\ c\ d \\ b\ d\ c\ a \end{pmatrix},$$

kde v první řádku jsou seřazeny prvky množiny *X* zpravidla v nějakém „přirozeném“ pořadí a ve druhém řádku jejich obrazy v zobrazení $\pi : X \to X$.. V našem případě platí: $\pi(a) = b,\ \pi(b) = d,\ \pi(c) = c,\ \pi(d) = a.$

Zajímavá je grafická reprezentace permutace pomocí cyklů [15]. V tomto případě se postupuje tak, že prvky množiny X znázorníme jako body v rovině a pak zakreslíme šipky od každého prvku x k prvku $\pi(x)$.

Příklad 2.2.1. Uvažujme skupinu 12 osob stojících v řadě nebo v zástupu. Kolik existuje různých způsobů jejich rozmístění? Je zřejmé, že jde o permutace, přitom na pořadí samozřejmě záleží. Podle definice 2.2.1 je počet různých rozmístění roven $P(12) = 12! = 479001600$.

Příklad 2.2.2. Vyřešme nyní úlohu rozmístění 12 osob kolem „kulatého“ stolu za doplňující podmínky, že rozmístění jsou různá, pokud má každá z osob různé sousedy. V tomto případě musíme uvážit, že vždy 12 rozmístění, které se liší jen „posunutím v kruhu“, lze považovat za stejná. Proto bude celkový počet různých rozmístění podstatně menší, rovný $\frac{12!}{12} = 11! = 39916800$.

Úkoly.

1. Kolika způsoby lze rozmístit 6 lvů v kruhové manéží, pokud se šelmy pohybují po obvodu manéže?
2. Kolik slov (včetně „nesmyslných“) lze vytvořit z 10 různých písmen abecedy, pokud je seřadíme za sebou?

Permutace s opakováním

V řadě kombinatorických úloh se pracuje s pojmem permutace s opakováním, přesněji permutace skupiny (není to množina!) n objektů, z nichž některé jsou stejné (nerozlišitelné). Předpokládejme, že z těchto n objektů je n_1 objektů 1. druhu, n_2 objektů 2. druhu, ..., n_k objektů k-tého druhu. Každé z možných, vzájemně různých rozmístění těchto objektů nazveme **permutace *n* objektů s opakováním**. Jejich celkový počet je dán formulí:

$$P(n; n_1, n_2, \dots, n_k) = \frac{n!}{n_1! n_2! \dots n_k!},$$

kde $\sum_{i=1}^{k} n_i = n$.

Důkaz. Představme si, že objekty téhož druhu nějakým způsobem rozlišíme (např. barvou nebo indexováním). Pak by byl počet permutací (vzájemně různých rozmístění) roven $n!$. Ve skutečnosti bude podstatně menší. Uvážíme-li, že n_i objektů i-tého druhu lze rozmístit $n_i!$ způsoby, $i = 1, 2, .., k$, dostaneme pro celkový počet vzájemně různých rozmístění výše uvedený vzorec. □

Příklad 2.2.3. Vyřešíme následující úlohu: Kolik různých slov (včetně nesmyslných) je možno vytvořit z písmen slova MATEMATIKA? Uvedené slovo sestává z 10 písmen, přitom obsahuje tři písmena A, dvě písmena M, dvě písmena T a po jednom písmena E, I, K. Proto dostaneme

$$P(10;3,2,2,1,1,1)=\frac{10!}{3!2!2!1!1!1!}.$$

Úkol. Kolik různých slov (včetně nesmyslných) je možno vytvořit z písmen následujících slov: INFORMATIKA, PODPROGRAM a PROCEDURA.

2.3 Kombinace

Také kombinace zavedeme netradičně, vyjdeme přitom z definice pojmu kombinační číslo.

Definice 2.3.1. Nechť *n*, *k* jsou nezáporná celá čísla, $n \geq k$. Potom funkce obou proměnných *n*, *k* definovaná vztahem

Kombinační číslo

$$\binom{n}{k}=\frac{\prod_{i=0}^{k-1}(n-i)}{k!}=\frac{n(n-1)(n-2)\ \dots\ (n-k+1)}{k!}=\frac{n!}{(n-k)!k!}$$

se nazývá **kombinační číslo** nebo **binomický koeficient**.
Obě definice jsou přirozeně ekvivalentní. První z nich je ovšem pro praxi vhodnější, protože při výpočtu poskytuje menší mezivýsledky.

Kombinačním číslům a jejich vlastnostem se budeme věnovat později.

Věta 2.3.1. Nechť X je libovolná *n*-prvková množina. Pak počet všech jejích *k*-prvkových podmnožin je roven kombinačnímu číslu $\binom{n}{k}$.

Důkaz (podle [15]). Spočítáme dvěma způsoby všechny uspořádané *k*-tice, které lze vytvořit z prvků množiny *X* (bez opakování). Na jedné straně je tento počet dán počtem variací *k*-té třídy z *n* prvků bez opakování, je tedy roven $n(n-1)(n-2)\ \dots\ (n-k+1)$). Na straně druhé můžeme z jedné *k*-prvkové podmnožiny množiny *X* (takových podmnožin je $\binom{n}{k}$) vytvořit *k*! různých uspořádaných *k*-tic a každou takovou uspořádanou *k*-tici dostaneme z jedné podmnožiny právě jednou. Proto musí platit:

$$n(n-1)(n-2)\ \dots\ (n-k+1)=k!\binom{n}{k}.$$ □

Kombinace bez opakování

Definice 2.3.1. Každá k-prvková podmnožina n-prvkové množiny X se nazývá **kombinace k-té třídy z n prvků bez opakování**. Pro jejich celkový počet $C_k(n)$ platí: $C_k(n) = \binom{n}{k}$.

Poznámka. Při vytváření k-prvkových podmnožin zřejmě nezáleží na pořadí, ve kterém prvky vybíráme

Příklad 2.3.1. Kolika způsoby lze na čtvercové šachovnici (o 64 polích) vybrat tři pole tak, aby všechna vybraná pole neměla stejnou barvu (viz [7])? Je zřejmé, že libovolná tři pole můžeme vybrat celkem $C_3(64) = \binom{64}{3} = 41\,664$ způsoby. Nyní určíme počet všech trojic složených jenom z bílých polí. Takových trojic bude $C_3(32) = \binom{32}{3} = 4\,960$. Právě tolik bude i trojic vytvořených pouze z černých polí. Proto řešením úlohy bude: $\binom{64}{3} - 2.\binom{32}{3} = 31\,744$.

Příklad 2.3.2. Při oslavě se připíjelo na zdraví. Pozorovatel zaregistroval právě 66 ťuknutí. Kolik bylo přítomných za předpokladu, že si každý účastník přiťuknul se všemi ostatními? Nechť x je počet účastníků. Potom musíme řešit rovnici $\binom{x}{2} = 66$ neboli $x^2 - x - 132 = 0$. Uvedená kvadratická rovnice má dva reálné kořeny: 12 a -11. Druhý z kořenů nemá ovšem smysl, takže účastníků bylo 12.

Úkol. Z balíčku 32 karet se náhodně vyberou tři karty. Kolika způsoby lze vybrat:

a) právě jedno eso.
b) nejméně jedno eso,
c) nejvýše jedno eso?

V některých kombinatorických úlohách se vyskytuje pojem kombinace s opakováním. Jde o vytváření kombinací k-té třídy (k prvků) z n prvků za předpokladu, že se každý prvek může ve výběru vyskytovat vícekrát.

Kombinace s opakováním

Definice 2.3.2. **Kombinace k-té třídy z n prvků s opakováním** je libovolný výběr k prvků z n různých druhů prvků, ve kterém nezáleží na pořadí vybíraných prvků. Přitom se předpokládá, že prvky daného druhu jsou nerozlišitelné.

Věta 2.3.2. Počet kombinací k-té třídy z n prvků s opakováním určen vztahem

$$C_k^*(n) = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}.$$

Důkaz. Každý výběr k prvků z n různých druhů zakódujeme řetězcem nul (reprezentují „rozhraní“ mezi objekty různých druhů) a jedniček (reprezentují prvky). Tak např. řetězec 11011101 reprezentuje výběr, jenž zahrnuje dva prvky prvního druhu, tři prvky druhého a jeden prvek třetího druhu. V obecném případě má takový řetězec délku $n+k-1$, protože obsahuje právě k jedniček a $n-1$ rozhraní. Každý řetězec je jednoznačně určen tím, na kterých pozicích jsou jedničky, resp. na kterých pozicích jsou nuly. Úlohu je tedy možno převést na problém určit, kolika způsoby lze vybrat k pozic pro jedničky (nebo $n-1$ pozic pro nuly) z celkového počtu $n+k-1$. Tím je vztah ve větě 2.3.2 dokázán. □

Příklad 2.3.3. Představme si, že v cukrárně mají tři druhy zákusků: věnečky, trubičky a marokánky. Spočteme, kolika různými způsoby je možno zakoupit celkem 7 zákusků. V našem případě je $n=3$ a $k=7$. Řešením dané úlohy je proto $C_7^*(3) = \binom{9}{7} = \binom{9}{2} = 36$.

Úkol. Kolik existuje různých trojúhelníků, jejichž délky stran jsou přirozená čísla z množiny $\{10,11,12,13,14,15,16,17,18,19\}$. Každý trojúhelník je jednoznačně určen délkami svých stran, tj. třemi čísly, které musí splňovat trojúhelníkovou nerovnost.

2.4 Kombinatorické principy

V této části se budeme věnovat třem základním kombinatorickým principům:

A) principu součtu,

B) principu součinu,

C) principu inkluze a exkluze.

Navíc se seznámíte s tzv. Dirichletovým principem a jeho využitím v kombinatorických úvahách.

A. Kombinatorický princip součtu

Tento princip se zakládá na následující větě.

Princip součtu

Věta 2.4.1. Nechť $A_1, A_2, \ldots, A_k$ jsou konečné množiny s mohutností postupně $n_1, n_2, \ldots, n_k$. Jsou-li tyto množiny po dvou disjunktní, pak je mohutnost množiny $\bigcup_{i=1}^{k} A_i$ rovna $\sum_{i=1}^{k} n_i$.

Důkaz této věty je elementární, proto jej ponechávám čtenáři. □

Při aplikaci uvedeného principu se nejprve celek (množina všech možností realizace uvažovaného jevu) rozloží na disjunktní podmnožiny a následně se určí mohutnosti jednotlivých podmnožin. Řešením úlohy je pak součet mohutností všech podmnožin.

Příklad 2.4.1. Určíme počet všech přirozených čísel menších než 200 takových, že končí číslicí 3. Nechť A_1 označuje množinu všech jednociferných čísel končících trojkou, A_2 množinu všech dvouciferných čísel končících trojkou a konečně A_3 množinu všech trojciferných čísel menších než 200 a končících trojkou. Pak zřejmě dostaneme:

$$A_1 = \{3\},\ A_2 = \{13, 23, 33, 43, 53, 63, 73, 83, 93\},$$

$$A_3 = \{103, 113, 123, 133, 143, 153, 163, 173, 183, 193\}.$$

Pro mohutnosti těchto množin platí: $n_1 = 1,\ n_2 = 9,\ n_3 = 10.$ Počet všech přirozených čísel menších než 200 a končících trojkou je roven $\sum_{i=1}^{3} n_i = 20.$

Úkoly.

1. Morseovka. Uvažujte čtyřmístný kód s abecedou $\{.,-\}$. Kolik různých znaků (písmen, číslic, pomocných znaků) lze takto zakódovat?
2. Brailleovo písmo. Představte si, že jednotlivé znaky jsou reprezentovány zvýrazněním různých kombinací různého počtu výstupků na šestibodové matrici. Určete kolik různých znaků lze vyjádřit v Brailleově 6-bodovém systému. Návod: všechny možné znaky nejprve rozdělte do disjunktních množin $A_1, \ldots, A_6$, kde A_k označuje množinu všech možných znaků s právě k zvýrazněnými výstupky.

B. Kombinatorický princip součinu

Princip součinu

Toto kombinatorické pravidlo je založeno na následujícím tvrzení: Počet všech uspořádaných k-tic, jejichž první člen lze vybrat n_1 způsoby a každý další člen postupně $n_2, n_3, \ldots, n_k$ způsoby, je roven $\prod_{i=1}^{k} n_i = n_1.n_2.\cdots.n_k$.

Příklad 2.4.2. Kolik trojciferných čísel lze vytvořit z číslic 0, 1, 2, 3 bez opakování za předpokladu, že číslo nesmí začínat nulou? Je zřejmé, že číslici nejvyššího (druhého) řádu můžeme vybrat 3 způsoby (1, 2 nebo 3), číslici prvního řádu také 3 způsoby (nesmí to být číslice již vybraná) a číslici nultého řádu 2 způsoby (nesmí to být dvě číslice již vybrané).
Celkový počet možností je tedy $3.3.2 = 18$.

Úkoly.

1. Vyjděte z řešení předcházejícího ilustrativního příkladu a určete:
a) kolik z těchto 18 možných trojciferných čísel je dělitelných 10,
b) kolik z těchto 18 čísel je sudých.

2. Určete, kolika způsoby lze sestavit trojčlennou posádku raketoplánu (velitel, pilot, výzkumník), jestliže jsou k dispozici 5 kandidátů na funkci velitele, 3 kandidáti na funkci pilota a 4 kandidáti na funkci výzkumníka.

3. Krotitel má přivést do arény 5 lvů a 4 tygry. Kolika způsoby to lze zařídit za předpokladu, že na pořadí tygrů i lvů záleží a přitom žádní 2 tygři nemohou jít bezprostředně za sebou (musí být mezi nimi lev). Návod: nejprve rozmístěte lvy a pak do 6 zbývajících míst (na počátku, mezi lvy a na konci) umístěte tygry.

C. Kombinatorické princip inkluze a exkluze

Tento princip se používá v případech, kdy chceme spočítat mohutnost sjednocení konečného počtu konečných množin, jestliže známe mohutnosti všech jejich průniků. Vychází se přitom z následující věty.

Princip inkluze a exkluze

Věta 2.4.2. Nechť $A_1, A_2, \ldots, A_n$ je nějaký systém konečných množin. Pak platí:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} \left|A_i \cap A_j\right| + \sum_{i<j<k} \left|A_i \cap A_j \cap A_k\right| - \ \ldots + (-1)^{n-1} \left|A_1 \cap A_2 \cap \ldots \cap A_n\right|.$$

Důkaz této věty, dokonce několika různými metodami, naleznete v monografii [15].

Příklad 2.4.3. Určíme počet přirozených čísel od 1 do 100, které nejsou dělitelné 3 ani 5. Nechť funkce $\lfloor x \rfloor$ značí celou část reálného čísla *x*, t.j.

největší celé číslo, pro nějž $\lfloor x \rfloor < x$. Množiny, s nimiž budeme pracovat, si označíme takto:
$A = \{1, 2, \ ..., \ 100\}$, $|A_3| = \{n \in A;\ 3 \mid n\}$, $|A_5| = \{n \in A;\ 5 \mid n\}$. Pro jejich mohutnosti zřejmě platí: $|A| = 100,\ A_3 = \lfloor 100/3 \rfloor = 33,\ A_5 = \lfloor 100/5 \rfloor = 20$ a $|A_3 \cap A_5| = \lfloor 100/15 \rfloor = 6$. Hledaný počet přirozených čísel splňujících zadání je tedy $|\bar{A}_3 \cap \bar{A}_5| = |A| - |A_3| - |A_5| + |A_3 \cap A_5| = 100 - 33 - 20 + 6 = 53.$

Úkoly.

1. Eratosthenovo síto. Kolik čísel zbude z množiny $\{1, 2, \ ..., \ 1000\}$, když vyloučíme všechny násobky čísel 2, 3, 5, 7 a 11?
2. Kolik existuje přirozených čísel menších než 100, která nejsou dělitelná druhou mocninou žádného přirozeného čísla většího než 1?

Jestliže neznáme mohutnosti všech průniků, nemůžeme určit mohutnost sjednocení všech množin přesně. Představte si, že znáte mohutnosti všech průniků až do *k*-násobných včetně, ale mohutnosti průniků většího počtu množin nikoliv. V takovém případě se k odhadu chyby, které se dopustíte vynecháním členů, jejichž velikost neznáte, používají tzv. **Bonferroniho nerovnosti**. Podle těchto nerovností bude mít uvažovaná chyba stejné znaménko jako první vynechaný člen.

Dirichletův princip

Na závěr této části uvedeme jednoduchou formulaci tzv. **Dirichletova principu** (přihrádkového principu). Jestliže umístíme m objektů do n přihrádek za předpokladu $m > n$, pak musí existovat alespoň jedna přihrádka, v níž budou nejméně dva objekty.

Příklad 2.4.4. Mějme krabicí, jež obsahuje 10 černých a 20 bílých ponožek. Z této krabice budeme naslepo po jedné vytahovat ponožky s cílem získat alespoň jeden pár stejné barvy. Kolik ponožek budeme muset nejméně vytáhnout? V tomto případě máme dvě přihrádky (jednu s černými a druhou s bílými ponožkami), tedy $n = 2$. Abychom dosáhli stanoveného cíle, stačí vytáhnout tři ponožky ($m = 3$).

Podobně lze dokázat, že v Praze existují nejméně dva lidé, kteří mají přesně stejný počet vlasů. Stačí totiž uvážit, že počet vlasů u člověka nepřevyšuje 1000000.

2.5 Kombinační čísla

Pojem **kombinačního čísla** (**binomického koeficientu**) byl již zaveden definicí 2.3.1. Tuto definici je možno rozšířit takto.

Definice 2.5.1. Nechť x je reálné číslo a k nezáporné celé číslo. Pak kombinační číslo $\binom{x}{k}$ je funkce proměnných x a k definované vztahem

$$\binom{x}{k} = \frac{x(x-1)(x-2)\ \dots\ (x-k+1)}{k!}.$$

Pomocí této definice lze psát např.:

$$\binom{x}{3} = \frac{1}{6}x(x-1)(x-2) \text{ nebo } \binom{-1}{3} = \frac{(-1).(-2).(-3)}{3.2.1} = -1.$$

Nyní si dokážeme některé významné vlastnosti kombinačních čísel. Pro celá nezáporná čísla n, k ($n \geq k$) platí

$$\binom{n}{k} = \binom{n}{n-k}. \tag{2.1}$$

Důkaz tohoto tvrzení je triviální. Z hlediska kombinatoriky to znamená, že počet k-prvkových podmnožin n-prvkové množiny je stejný jako počet podmnožin obsahujících $n-k$ prvků. Stačí uvážit, že každé k-prvkové podmnožině lze jednoznačně přiřadit její doplněk. □

V praxi se často používá vzorec pro součet kombinačních čísel

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \tag{2.2}$$

Důkaz (viz [15]). Pravá strana (2.2) udává počet k-prvkových podmnožin n-prvkové množiny X. Vybereme libovolný prvek $a \in X$ a všechny k-prvkové podmnožiny X rozdělíme do dvou skupin podle toho, zda obsahují či neobsahují prvek a. Podmnožiny neobsahující prvek a jsou právě všechny k-prvkové podmnožiny $X \setminus \{a\}$, a je jich celkem $\binom{n-1}{k}$. Je-li A nějaká k-prvková podmnožina X obsahující prvek a, můžeme jí zřejmě jednoznačně přiřadit $(k-1)$-prvkovou množinu $A^* = A \setminus \{a\}$. Proto počet k-prvkových podmnožin X obsahujících prvek a je celkem $\binom{n-1}{k-1}$. Odtud už dostaneme pro celkový počet k-prvkových podmnožin množiny X výraz $\binom{n-1}{k-1} + \binom{n-1}{k}$.

□

Pascalův trojúhelník

Se vztahem (2.2) souvisí tzv. **Pascalův trojúhelník**:

$$\begin{array}{ccccccccccc}
&&&&&1&&&&& \\
&&&&1&&1&&&& \\
&&&1&&2&&1&&& \\
&&1&&3&&3&&1&& \\
&1&&4&&6&&4&&1& \\
1&&5&&10&&10&&5&&1 \\
&&&\vdots&&&&\vdots&&&
\end{array}$$

Vrcholem tohoto trojúhelníku ke kombinační číslo $\binom{0}{0}=1.$ Každý následující řádek schématu se vytváří tak, že pod dvojici čísel předcházejícího řádku se zapíše jejich součet a na okrajích (zleva i zprava) se doplní jedničky.

Binomická věta

Identita (2.2) je vhodná i k důkazu **binomické věty**

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{2.3}$$

matematickou indukcí podle proměnné n.

Důkaz. Pro $n=1$ vztah (2.3) zřejmě platí, neboť $(1+x)^1 = \binom{1}{0} + \binom{1}{1} x = 1+x.$ Předpokládáme, že vztah platí pro libovolné $n_0 \in \mathbb{N}$, a dokážeme jeho platnost i pro $n_0+1.$

$$(1+x)^{n_0+1} = (1+x)^{n_0}(1+x) = \left(\sum_{k=0}^{n_0} \binom{n_0}{k} x^k\right)(1+x) =$$
$$= \sum_{k=0}^{n_0} \binom{n_0}{k} x^k + \sum_{k=0}^{n_0} \binom{n_0}{k} x^{k+1} = \sum_{k=0}^{n_0} \binom{n_0}{k} x^k + \sum_{l=1}^{n_0+1} \binom{n_0}{l-1} x^l =$$
$$= x^l \left[\sum_{l=0}^{n_0} \binom{n_0}{l} + \sum_{l=1}^{n_0+1} \binom{n_0}{l-1}\right] = x^l \sum_{l=0}^{n_0+1} \binom{n_0+1}{l}.$$

Tím je binomická věta dokázána. □

Z binomické věty lze odvodit celou řadu vztahů pro binomické koeficienty. Nejjednodušší z nich dostaneme dosazením $x=1.$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ ... + \binom{n}{n} = 2^n.$$

Celkový počet podmnožin n-prvkové množiny je roven součtu počtů prvků podmnožin s mohutností 0, 1, 2, ..., n.

Z dalších identit platných pro binomické koeficienty uvedeme

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}.$$

Důkaz. Nejprve sumu na levé straně upravíme s použitím identity (2.1) na tvar

$$\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}.$$

Tato suma je rovna počtu n-prvkových podmnožin množiny obsahující $2n$ prvků. Uvažme $2n$-prvkovou množinu X takovou, že n prvků je obarveno červeně a zbývajících n prvků modře. Chceme-li vybrat libovolnou podmnožinu X, pak stačí vybrat nějakou k-prvkovou podmnožinu červených prvků a nějakou $(n-k)$-prvkovou podmnožinu modrých prvků, $k\in\{0,1,\ ...,\ n\}$. Při pevně zvoleném k máme pro výběr červené podmnožiny $\binom{n}{k}$ možností a pro výběr modré podmnožiny $\binom{n}{n-k}$ možností, celkem tedy $\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}$ možností. □

2.6 Kombinatorické počítání

V této části ukážeme, jak aplikovat základní poznatky z kombinatoriky při výpočtu klasické pravděpodobnosti jevů na základě Laplaceovy definice.

Pravděpodobnost jevu

Definice 2.6.1. (**Laplaceova definice pravděpodobnosti**). Nechť určitý náhodný pokus může vykázat celkem n různých, vzájemně se vylučujících výsledků, které jsou na podkladě symetrie a homogenity stejně možné. Jestliže m z těchto výsledků má nevyhnutelně za následek nastoupení určitého jevu A, kdežto zbývajících $n-m$ výsledků jej vylučuje, pak pravděpodobnost jevu A je dána vztahem

$$P(A)=\frac{m}{n}.$$

Poznámka. Na střední škole se tato klasická definice pravděpodobnosti formuluje takto. Pravděpodobnost daného náhodného jevu A je dána poměrem počtu výsledků příznivých nastoupení jevu A a počtu všech možných výsledků náhodného pokusu.

V souladu s Lapalaceovou definicí můžeme pravděpodobnost $P(A)$ považovat za funkci jevu A. Tato funkce má následující vlastnosti. Pro každý jev platí $P(A)\geq 0$.

Vlastnosti pravděpodobnosti

1. Pravděpodobnost jistého jevu Ω je jednotková, tj. $P(\Omega)=1$.
2. Jestliže se nějaký jev *A* skládá z dílčích jevů $A_1, A_2, \ldots, A_n$, pak

$$P(A)=\sum_{i=1}^{n} P(A_i).$$

4. Pravděpodobnost jevu $\overline{A}$ (jevu opačného k *A*) je $P(\overline{A})=1-P(A)$.
5. Pravděpodobnost jevu nemožného $\varnothing$ je rovna nule, tj. $P(\varnothing)=0$.
6. Jestliže z jevu *A* plyne jev *B*, pak platí $P(A)\le P(B)$.
7. Pro pravděpodobnost libovolného jevu platí $0\le P(A)\le 1$.

Poznámka. Na základě uvedených vlastností pravděpodobnosti můžeme řešit jednoduché kombinatorické úlohy. Další vlastnosti klasické pravděpodobnosti jsou popsány např. ve skriptech [13].

Příklad 2.6.1. Někdo má v kapse *N* různých klíčů a chce potmě otevřít dveře svého bytu. Vyjímá naslepo z kapsy jeden klíč po druhém a zkouší jimi otevřít dveře. Určíme pravděpodobnost, že pří *k*-tém pokusu zvolí správný klíč?

Počet všech možných pořadí, jak vyjímat klíče, je zřejmě roven počtu permutací množiny *N* prvků, tedy $N!$. Předpokládejme, že všechny permutace jsou stejně možné. Musíme tedy určit, kolik je takových permutací, při nichž stojí správný klíč na *k*-tém místě. Odpověď je jednoduchá. Existuje právě $(N-1)!$ takových permutací, takže hledaná pravděpodobnost je

$$\frac{(N-1)!}{N!}=\frac{1}{N}.$$

Pravděpodobnosti toho, že správný klíč padne do ruky při prvním, druhém, ..., posledním *N*-tém pokusu, jsou stejné a rovnají se $1/N$.

Příklad 2.6.2. Výtah s *M* pasažéry zastavuje postupně v *N* patrech ($M<N$). Určíme pravděpodobnost jevu *A*, který spočívá v tom, že v žádném patře nevystoupí více než jeden pasažér.
Celkový počet různých rozmístění pasažérů do pater je zřejmě roven počtu variací *M*-té třídy z *N* prvků s opakováním, tj. výrazu N^M. Kolik je však způsobů rozmístění příznivých jevu *A*? Hledaný počet je tentokrát dán počtem variací *M*-té třídy z *N* prvků bez opakování, tj. výrazem $N(N-1)\ldots(N-M+1)$. Pro hledanou pravděpodobnost tedy platí

$$P(A)=\frac{N(N-1)\ldots(N-M+1)}{N^M}=\frac{N!}{N^M(N-M)!}.$$

Příklad 2.6.3. Z hromádky 32 karet (4 barvy po 8 kartách) se náhodně vybere k karet ($k > 1$). Určíme pravděpodobnost toho, že mezi vybranými kartami bude alespoň jedno eso.

Označme symbolem A_i jev, který spočívá v nalezení právě i es mezi k vybranými kartami ($i \le m = \min\{k, 4\}$) a symbolem A jev spočívající v tom, že mezi k vybranými kartami bude nalezeno alespoň jedno eso. Množina všech možných výsledků náhodného pokusu je tvořena všemi kombinacemi k-té třídy z 32 prvků, počet těchto kombinací je roven kombinačnímu číslu $\binom{32}{k}$. Počet výsledků příznivých jevu A_1 určíme takto. Jedno eso lze vybrat $\binom{4}{1}$ různými způsoby a zbývající karty v počtu $k-1$ celkem $\binom{28}{k-1}$ způsoby, takže počet příznivých případů je (podle principu součinu) roven součinu obou uvedených kombinačních čísel. Pro hledanou pravděpodobnost tedy platí

$$P(A_1) = \frac{\binom{4}{1}\binom{28}{k-1}}{\binom{32}{k}}.$$

Analogicky stanovíme i pravděpodobnosti jevů A_i, $i = 2, 3, \ldots, m$. Zřejmě platí:

$$P(A_2) = \frac{\binom{4}{2}\binom{28}{k-2}}{\binom{32}{k}}, \ \ldots, P(A_m) = \frac{\binom{4}{m}\binom{28}{k-m}}{\binom{32}{k}}.$$

Jev A se ovšem skládá ze vzájemně neslučitelných jevů $A_1, A_2, \ldots, A_m$, proto

$$P(A) = \sum_{i=1}^{m} P(A_i).$$

Příklad 2.6.4. Dítě si hraje s písmeny M, M, A, A, A, T, T, E, I, K. Jaká je pravděpodobnost, že se mu podaří při náhodném řazení písmen za sebou vytvořit slovo MATEMATIKA?

Označme uvažovaný jev symbolem A. Kdyby byla všechna písmena rozlišitelná (např. velikostí, typem nebo barvou), pak by byl počet všech možných výsledků pokusu roven počtu permutací množiny těchto 10 písmen, tj. 10!. Přirozeně se předpokládá, že mezi uvažovanými písmeny jsou dvě navzájem nerozlišitelná písmena M, tři nerozlišitelná písmena A a dvě nerozlišitelná písmena T. Proto permutace, které se liší transpozicí (záměnou) písmen M (takových je celkem 2!) a/nebo transpozicí písmen A (celkem 3!) a/nebo transpozicí písmen T (celkem 2!) představují jeden a tentýž výsledek pokusu. Z uvedeného je zřejmé, že počet všech vzájemně různých výsledků pokusu je $10!/(2!\ 3!\ 2!)$. Pouze jediná z těchto permutací je příznivá jevu A, takže pro hledanou pravděpodobnost dostaneme

$$P(A) = \frac{2!\ 3!\ 2!}{10!} \approx 0{,}00000066.$$

Metodám řečení kombinatorických úloh jsou věnovány speciální monografie, např. [19].

Úkoly.

1. Číslice 1, 2, ..., n jsou náhodně uspořádány do posloupnosti (řetězce). Jaká je pravděpodobnost toho, že číslice 1 a 2 stojí vedle sebe právě v tomto pořadí?
2. Ve studijní skupině je celkem 30 studentů. Jaká je pravděpodobnost jevu, že žádní dva studenti (popř. více studentů) neslaví narozeniny téhož dne? Předpokládejte, že rok má přesně 365 dnů.
3. V sérii n výrobků je k zmetků. Určete pravděpodobnost jevu, že mezi m náhodně vybranými výrobky bude právě r zmetků.
4. Z deseti losů vyhrávají dva. Určete pravděpodobnost toho, že z pěti náhodně vybraných losů
   a) vyhrává právě jeden,
   b) vyhrává nejméně jeden,
   c) vyhrává nejvýše jeden.
5. V krabici se nachází 15 červených, 9 modrých a 6 zelených kuliček. Jaká je pravděpodobnost toho, že mezi šesti náhodně vybranými kuličkami bude jedna zelená, dvě modré a tři červené?
6. Určete pravděpodobnost výhry první, druhé, třetí a čtvrté ceny v Sazce. Sázkař tipuje výsledky 12 utkání (1 - výhra domácích, 0 – nerozhodně, 2 – výhry hostí). První cenu vyhraje ten, kdo uhodne výsledky všech

utkání. Druhou, třetí, resp. čtvrtou cenu získá sázející, který tipuje nesprávně výsledek jednoho, dvou, resp. tří (libovolných) utkání.

Kontrolní otázky:

1.Vysvětlete rozdíl mezi variacemi s opakováním a variacemi bez opakování.
2. Jaký je vztah mezi variacemi a permutacemi?
3. Jaký je principiální rozdíl mezi variacemi a kombinacemi?
4. Vysvětlete, kdy a jak se používá kombinatorický princip součtu.
5. Vysvětlete, kdy a jak se používá kombinatorický princip součinu.
6. Vysvětlete podstatu a způsob použití kombinatorického principu inkluze a exkluze.
7. Co je to Dirichletův princip?
8. Jak lze rozšířit středoškolskou definici kombinačního čísla?
9. Jak se v praxi využívá binomická věta?
10. Jak je definována pravděpodobnost náhodné jevu podle Laplace?
11. Jaké jsou základní vlastnosti této pravděpodobnosti?
12. Je možno použít Laplaceovu definici při výpočtu pravděpodobnosti náhodného jevu za předpokladu, že příslušný náhodný pokus má nekonečně mnoho různých výsledků?

Pojmy k zapamatování:

- variace s opakováním,
- variace bez opakování,
- permutace bez opakování,
- permutace s opakováním,
- kombinace bez opakování,
- kombinace s opakováním,
- kombinatorický princip součtu,
- kombinatorický princip součinu,
- kombinatorický princip inkluze a exkluze,
- kombinační číslo (binomický koeficient),
- Dirichletův princip,
- Pascalův trojúhelník,
- binomická věta,
- Laplaceova definice pravděpodobnosti jevu,
- aplikace Laplaceovy definice.

Shrnutí

V úvodních odstavcích této kapitoly byly poněkud netradičně (s využitím pojmu zobrazení) zavedeny základní kombinatorické pojmy variace, permutace a kombinace. Následně byla věnována pozornost základním kombinatorickým principům (princip součtu, princip součinu, princip inkluze a exkluze) a některým, často využívaným, vlastnostem kombinačních čísel. Získané znalosti byly využity k řešení jednodušších kombinatorických úloh, konkrétně při výpočtu pravděpodobnosti jevů na základě Laplaceovy definice.

3 LOGICKÉ FUNKCE

Po prostudování této kapitoly:

- osvojíte si základní vlastnosti dvouhodnotových logických funkcí ,
- naučíte se realizovat logické funkce formulemi,
- pochopíte princip duality,
- naučíte se konstruovat úplné normální disjunktivní a konjunktivní formy,
- budete schopni rozhodnout, zda je daná množina logických funkcí funkcionálně úplná, resp. funkcionálně uzavřená .

Klíčová slova: logická funkce, skutečná proměnná, fiktivní proměnná, shodnost funkcí, logická formule, podformule, formule stejné struktury, ekvivalence formulí, tautologie, kontradikce, duální funkce, princip duality, duální formule, úplná disjunktivní normální forma, úplná konjunktivní normální forma, funkcionální úplnost, Žegalkinův polynom, funkcionální uzavřenost, funkce zachovávající konstantu 0, funkce zachovávající konstantu 1, samoduální funkce, monotónní funkce, lineární funkce.

V této kapitole poznáte základy dvouhodnotové logiky. Věnujte pochopení předkládaného učiva náležitou pozornost. Získané znalosti a dovednosti oceníte ve svém dalším studiu, zejména v předmětu „Logické základy umělé inteligence“. Podrobnosti, stejně jako úvod do vícehodnotové logiky, naleznete především v monografii Jablonského [6].

3.1 Základní pojmy

Začneme definicí dvouhodnotové logické funkce.

Logická funkce

Definice 3.1.1. Nechť $E^2 = \{0,1\}$. Pak funkce $f(x_1, x_2, ..., x_n)$ definované zobrazením $f : E^2 \times E^2 \times ... \times E^2 \to E^2$ se nazývají **logické funkce *n* proměnných**. Množinu všech takových funkcí budeme označovat P_2.

Věta 3.1.1. Počet všech logických funkcí z množiny P_2, závisejících na *n* proměnných, je roven 2^{2^n}.

Důkaz. Uvažujme nějakou logickou funkci $f(x_1, x_2, ..., x_n)$. Pak počet všech různých *n*-tic proměnných (a tedy i počet všech různých hodnot funkce) je roven počtu všech variací *n*-té třídy ze 2 prvků s opakováním, tj. $V_n^*(2)=2^n$. Funkce *f* je zobrazením množiny, která má 2^n prvků, do množiny obsahující právě 2 prvky (pro každou *n*-tici proměnných 2 možné hodnoty). Počet všech takových zobrazení je podle věty 2.1.2 roven 2^{2^n}. □

Počet logických funkcí *n* proměnných je samozřejmě konečný, ale s rostoucím *n* roste velmi rychle. Pro $n=1,2,3$, resp. 4, nabývá počet logických funkcí hodnot 4, 16, 256, resp. 65536.

Logické funkce se zadávají (definují) dvěma způsoby:

- tabulkou pravdivostních hodnot,
- analyticky.

Tabulka pravdivostních hodnot funkce $f(x_1,x_2,\ ...,\ x_n)$ má v tzv. standardním uspořádání tvar

x_1	...	x_{n-1}	x_n	$f(x_1,\ ...,\ x_{n-1},\ x_n)$
0	...	0	0	$f(0,\ ...,\ 0,0)$
0	...	0	1	$f(0,\ ...,\ 0,1)$
0	...	1	1	$f(0,\ ...,\ 1,1)$
$\vdots$		$\vdots$	$\vdots$	$\vdots$
1	...	1	1	$f(1,\ ...,\ 1,1)$

Poznámka. V případě standardního uspořádání se *n*-tice hodnot proměnných považuje za zápis čísla ve dvojkové soustavě. Uspořádání *n*-tic pak odpovídá přirozenému uspořádání čísel 0, 1, ..., 2^n-1.

Snaha o minimalizaci počtu proměnných v logické funkci vede k následující definici.

Definice 3.1.2. Logická funkce $f(x_1,x_2,\ ...,\ x_n)\in P_2$ proměnných $x_1,x_2\ ...,\ x_n$ závisí skutečně na proměnné x_i, jestliže existují takové hodnoty $a_1,\ ...,\ a_{i-1},a_{i+1},\ ...,\ a_n$ proměnných $x_1,\ ...,\ x_{i-1},x_{i+1},\ ...,\ x_n$, že platí $f(a_1,\ ...,\ a_{i-1},0,a_{i+1},\ ...,\ a_n)\neq f(a_1,\ ...,\ a_{i-1},1,a_{i+1},\ ...,\ a_n)$. V takovém případě se proměnná x_i nazývá **skutečná proměnná**. V opačném případě se nazývá **fiktivní proměnná**.

Skutečná proměnná
Fiktivní proměnná

Nechť x_i je fiktivní proměnná. Jestliže z tabulky pravdivostních hodnot funkce *f* vynecháme všechny řádky typu $a_1,\ ...,\ a_{i-1},1,a_{i+1},\ ...,\ a_n$ a navíc vynecháme sloupec proměnné x_i, dostaneme tabulku, která definuje novou funkce $g\left(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\right)$ s $n-1$ proměnnými. Hodnoty této nové funkce *g* jsou přitom stejné jako hodnoty funkce *f*.

Shodnost funkcí

Definice 3.1.3. Funkce *f* a *g* se nazývají **shodné**, jestliže funkci *g* lze získat z funkce *f* zavedením nebo vynecháním fiktivních proměnných. Shodnost funkcí *f* a *g* se označuje $f = g$.

Při práci s logickými funkcemi se snažíme najít k dané funkci *f* co nejjednodušší funkci *g* vynecháním všech fiktivních proměnných.

Existují dva typy funkcí, které nemají žádné skutečné proměnné.Jsou to funkce, které se rovnají identicky 0, nebo jsou identicky rovny 1. Tyto funkce se považují za logické konstanty.

Na závěr této části uvedeme úplný přehled logických funkcí jedné a dvou proměnných.

Tab. 3.1. Logické funkce jedné proměnné

x	$f_1 = 0$	$f_2 = 1$	$f_3 = x$	$f_4 = \overline{x}$
0	0	1	0	1
1	0	1	1	0

Poznámka. Funkce f_1 a f_2 jsou logické konstanty, f_3 identická funkce (aserce) a f_4 negace.

Tab.3. 2. Logické funkce dvou proměnných

x_1	x_2	$f_1 = 0$	$f_2 = 1$	$f_3 = x_1$	$f_4 = x_2$	$f_5 = x_1 \wedge x_2$	$f_6 = x_1 \vee x_2$	$f_7 = x_1 \Rightarrow x_2$	$f_8 = x_1 \oplus x_2$
0	0	0	1	0	0	0	0	1	0
0	1	0	1	0	1	0	1	1	1
1	0	0	1	1	0	0	1	0	1
1	1	0	1	1	1	1	1	1	0

Tab.3. 2. Logické funkce dvou proměnných (pokračování)

$f_9 = x_1 \vee \overline{x}_2$	$f_{10} = \overline{x}_1$	$f_{11} = \overline{x}_2$	$f_{12} = \overline{x_1 \wedge x_2}$	$f_{13} = \overline{x_1 \vee x_2}$	$f_{14} = x_1 \Leftrightarrow x_2$	$f_{15} = x_1 \wedge \overline{x}_2$	$f_{16} = \overline{x}_1 \wedge x_2$
1	1	1	1	1	1	0	0
0	1	0	1	0	0	0	1
1	0	1	1	0	0	1	0
1	0	0	0	0	1	0	0

Poznámka. Význam logických funkcí $f_1, f_2, f_3, f_4, f_{10}$ a f_{11} je zřejmý. Pro ostatní funkce se používá následujících názvů:

$f_8 = x_1 \oplus x_2$ součet modulo 2 (funkce XOR),

$f_9 = x_1 \vee \overline{x}_2$,

$f_{12} = \overline{x_1 \wedge x_2} = x_1 / x_2$ Shefferova funkce (funkce NAND),

$f_{13} = \overline{x_1 \vee x_2}$ Pierceova funkce (funkce NOR),

$f_{14} = x_1 \Leftrightarrow x_2$ ekvivalence,

$f_{15} = \overline{x_2 \Rightarrow x_1} = x_1 \wedge \overline{x}_2$ negace implikace,

$f_{16} = \overline{x}_1 \wedge x_2$.

3.2 Formule logiky

Z logických funkcí můžeme vytvářet formule. Nejprve uvedeme definici logické formule pomocí indukce.

Definice 3.2.1. Nechť *P* je nějaká (ne nutně konečná) podmnožina logických funkcí z P_2 (tedy z množiny všech logických funkcí).

a) Indukční předpoklad. Každá funkce $f(x_1, x_2, \ldots, x_m)$ z množiny *P* se nazývá **formule nad množinou *P***.

Formule

b) Indukční krok. Nechť $f(x_1, x_2, \ldots, x_m)$ je funkce z množiny *P* a $A_1, A_2, \ldots, A_m$ jsou výrazy, které jsou buď formulemi nad *P* nebo symboly proměnných z abecedy *U*. Pak výraz $f(A_1, A_2, \ldots, A_m)$ se **nazývá formule nad množinou *P***.

Uvedená indukční definice umožňuje postupně vytvářet z daných formulí formule nové. Je-li formule $\mathcal{A}$ vytvořena pomocí funkcí $f_1, f_2, \ldots, f_n$, můžeme tuto formuli zapsat jako $\mathcal{A}[f_1, f_2. \ldots, f_n]$. Chceme-li však zdůraznit, že se na vytvoření formule $\mathcal{A}$ podílejí proměnné $x_1, x_2, \ldots, x_m$, zapíšeme tuto formuli ve tvaru $\mathcal{A}(x_1, x_2, \ldots, x_m)$.

Podformule

Formule použité při konstrukci nějaké nové formule $\mathcal{A}$ se nazývají **podformule** formule $\mathcal{A}$.

Příklad 3.2.1. Je-li *P* množina elementárních funkcí, pak např. následující výrazy jsou formule nad *P*:

- $x_1 \wedge (x_2 \vee x_3)$,
- $\overline{x}_1 \wedge (x_2 \oplus x_3)$,

- $x_1 \vee ((x_2 \Rightarrow x_3) \wedge (x_3 \Rightarrow x_2))$.

Odpověď na otázku, zda mají či nemají nějaké dvě formule stejnou strukturu, poskytuje následující definice.

Formule stejné struktury

Definice 3.2.2. Nechť $\mathcal{A}[f_1, f_2. ..., f_n]$ je formule nad množinou funkcí P. Nechť $\mathcal{B}[g_1, g_2, ..., g_n]$ je formule vytvořená z formule $\mathcal{A}$ záměnou g_i za f_i, $i = 1, 2, ..., n$. Pak **formule $\mathcal{B}$ má stejnou strukturu jako formule $\mathcal{A}$.**

Příklad 3.2.2. Nechť jsou dány dvě formule: formule $\mathcal{A}$ = $[x_1 \wedge \overline{(x_2 \wedge x_3)}]$ nad množinou funkcí $\{\overline{x}_1, (x_1 \wedge x_2)\}$ a formule $\mathcal{B}$ = $[x_1 \Rightarrow \overline{(x_2 \Rightarrow x_3)}]$ nad množinou funkcí $\{\overline{x}_1, (x_1 \Rightarrow x_2)\}$. Pak podle uvedené definice mají obě formule stejnou strukturu.

Každé formuli $\mathcal{A}(x_1, x_2, ..., x_n)$ nad P můžeme jednoznačně přiřadit funkci $f(x_1, x_2, ..., x_n)$ z P_2, a to na základě následující indukční definice. Díky této definice můžeme s logickou funkcí pracovat stejně jako s formulí a naopak.

Definice 3.2.3 (viz [6]).

a) Indukční předpoklad. Je-li $\mathcal{A}(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$, kde $f \in P$, pak formuli $\mathcal{A}(x_1, x_2, ..., x_n)$ přiřadíme funkci $f(x_1, x_2, ..., x_n)$.

b) Indukční krok. Nechť $\mathcal{A}(x_1, x_2, ..., x_n) = f_0(A_1, A_2, ..., A_m)$, kde A_i, $i = 1, 2, ..., m$, jsou formule nad P nebo symboly proměnných $x_{j(i)}$. Podle indukčního předpokladu je A_i přiřazena funkce f_i z P_2 nebo identická funkce $f_i = x_{j(i)}$. Pak formuli $\mathcal{A}(f_1, f_2, ..., f_n)$ přiřadíme funkci $f(x_1, x_2, ..., x_n) = f_0(f_1, f_2, ..., f_m)$.

Realizace funkcí formulemi

Je-li f funkce přiřazená formuli $\mathcal{A}$, pak říkáme, že **formule $\mathcal{A}$ realizuje funkci f**. Funkce f přiřazená formuli $\mathcal{A}$ se nazývá **superpozicí funkcí z P** a proces vytvoření funkce f z P se nazývá **operací superpozice**.

Příklad 3.2.2. Nechť jsou dány tři formule:

$\mathcal{A}(x) = \overline{x},\ \mathcal{B}(x,y) = x \vee y,\ C(x,z) = x \Rightarrow z$ a k nim po řadě přiřazené funkce $f_1(x) = \overline{x},\ f_2(x,y) = x \vee y,\ f_3(x,z) = x \Rightarrow z.$ Nechť pro nějakou formuli $\mathcal{D}$ platí

$\mathcal{D}(x,y,z) = g(\mathcal{A},\mathcal{B},C)$, kde formuli $\mathcal{A}$ je přiřazena funkce f_1, formuli $\mathcal{B}$ funkce f_2 a formuli C funkce f_3. Pak můžeme formuli $\mathcal{D}$ přiřadit funkci $f(x,y,z) = g(f_1, f_2, f_3)$. Formule $\mathcal{D}$ tedy realizuje funkci f a tato funkce f vznikla superpozicí funkcí g, f_1, f_2 a f_3.

3.3 Ekvivalence formulí

V předcházející části jsme ukázali, že každé formuli nad nějakou množinou logických funkcí $P \subseteq P_2$ můžeme přiřadit logickou funkci, přitom různým formulím mohou být přiřazeny shodné funkce. Tato skutečnost vede k tomu, že je potřebné definovat pojem ekvivalence formulí.

Ekvivalence formulí

Definice 3.3.1. Formule $\mathcal{A}$ a $\mathcal{B}$ nad P jsou **ekvivalentní,** jestliže jim přiřazené logické funkce jsou shodné, tedy $f_{\mathcal{A}} = f_{\mathcal{B}}$. Skutečnost, že formule $\mathcal{A}$ a $\mathcal{B}$ jsou ekvivalentní, se zapisuje ve tvaru $\mathcal{A} = \mathcal{B}$.

Příklad 3.3.1. Příklady ekvivalentních formulí:

- $x \wedge \overline{x} = 0,$
- $x \Leftrightarrow y = (x \Rightarrow y) \wedge (y \Rightarrow x).$

Uvedeme přehled základních ekvivalencí nad množinou logických funkcí $\{0,1,\overline{x},x \wedge y, x \vee y, x \oplus y\}$. Uvedené ekvivalence můžeme klasifikovat podle toho, jaké zákony (jaká pravidla) reprezentují.

1. Zákony komutativní:

$$x \wedge y = y \wedge x,$$
$$x \vee y = y \vee x,$$
$$x \oplus y = x \oplus x.$$

2. Zákony asociativní:

$$(x \wedge y) \wedge z = x \wedge (y \wedge z),$$
$$(x \vee y) \vee z = x \vee (y \vee z),$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z).$$

3. Zákony distributivní:

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z),$$
$$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

4. Zákon dvojité negace (zákon negace negace):

$$\overline{\overline{x}} = x.$$

5. Zákony de Morganovy:

$$\overline{x \wedge y} = \overline{x} \vee \overline{y},$$
$$\overline{x \vee y} = \overline{x} \wedge \overline{y}.$$

6. Zákony idempotence:

$$x \wedge x = x, \qquad x \vee x = x.$$

7. Zákony neutrality:

$$x \wedge 1 = x, \qquad x \vee 0 = x.$$

8. Zákony agresivity:

$$x \wedge 0 = 0, \qquad x \vee 1 = 1.$$

9. Zákony o vyloučení třetího

$$x \wedge \overline{x} = 0, \qquad x \vee \overline{x} = 1.$$

7. Pravidla pro sčítání modulo 2:

$$x \oplus 1 = \overline{x}, \qquad \overline{x} \oplus 1 = \text{ x}$$
$$x \oplus 0 = x, \qquad \overline{x} \oplus 0 = \overline{x}.$$

Jestliže rozšíříme množinu logických funkcí o implikaci a ekvivalenci, přibudou další ekvivalence, např.:

$$x \Rightarrow y = \overline{x} \vee y,$$
$$x \Leftrightarrow y = (x \Rightarrow y) \wedge (y \Rightarrow x) = x \wedge y.$$

Všechny uvedené ekvivalence lze snadno ověřit, když porovnáme funkce stojící na levé a pravé straně těchto ekvivalencí. Na základě těchto ekvivalencí je možno zjednodušovat zápisy formulí nebo dokazovat ekvivalenci dvou formulí.

Přitom je ovšem třeba dodržovat určitá pravidla.

- Pokud se v zápisu formule nepoužívají závorky, má operace $\wedge$ vyšší prioritu než operace $\vee$ a $\oplus$.
- V případě používání závorek je pořadí provádění operací určeno umístěním závorek v zápisu formule.

Příklad 3.3.2. Uvedeme jednoduchý příklad na zjednodušení zadané formule.

$$\mathcal{A}(x,y) = x \vee x \wedge y = x \vee (x \wedge y) = (x \wedge 1) \vee (x \wedge y) =$$
$$= x \wedge (1 \vee y) = x \wedge 1 = x = \mathcal{B}(x,y).$$

Příklad 3.3.3. S použitím uvedených ekvivalencí dokážeme platnost vztahu

$x \wedge [(y \vee x) \vee (x \wedge y)] = x \wedge (x \vee y)$. Řešení je následující:

$$x \wedge [(y \vee x) \vee (x \wedge y)] = x \wedge [y \vee (x \wedge 1) \vee (x \wedge y)] =$$
$$= x \wedge [y \vee x \wedge (1 \vee y)] = x \wedge [y \vee (x \wedge 1)] = x \wedge (x \vee y).$$

Úkoly.

1. Dokažte

   a) $(x \wedge y) \vee (x \wedge \overline{y}) = x,$

   b) $(x \vee y) \wedge (x \vee \overline{y}) = x,$

   c) $(x \wedge \overline{y}) \vee (\overline{x} \wedge \overline{y}) \vee \overline{x} \vee (x \vee \overline{y}) = 1,$

   d) $(x \wedge y \wedge z) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge y \wedge z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z),$

   e) $\left[\left(\overline{\overline{x} \wedge y}\right) \wedge \overline{x}\right] \vee y = (x \wedge y) \vee (\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}).$

Tautologie

2. Rozhodněte, zda následující formule jsou **tautologie**, tj. formule, jejichž hodnota je identicky rovna 1.

   a) $(\overline{\overline{x}} \Rightarrow x) \wedge (x \Rightarrow \overline{\overline{x}}),$

   b) $(\overline{\overline{y}} \vee \overline{x}) \Rightarrow (\overline{x} \vee y),$

   c) $x \Rightarrow (y \Rightarrow z),$

   d) $[x \Rightarrow (y \Rightarrow z)] \Rightarrow [(x \Rightarrow y) \Rightarrow (x \Rightarrow z)].$

Kontradikce

Poznámka. Formule, jejichž hodnota je identicky rovna 0 se nazývá **kontradikce**.

Při dokazování formulí existuje prakticky vždy celá řada různých postupů, které vedou k požadovanému cíli. Snažte se najít takový postup, jenž je co nejkratší v tom smyslu, že vyžaduje použití co nejmenšího počtu v textu uvedených ekvivalencí.

3.4 Princip duality

Jednoduchý způsob, jak získávat nové formule, nabízí tzv. princip duality.

Definice 3.4.1. Funkce $\left[f\left(x_1, x_2,\ ..., x_n\right)\right]^* = \overline{f}\left(\overline{x}_1, \overline{x}_2,\ ..., \overline{x}_n\right)$ se nazývá **duální funkce** k funkci $f\left(x_1, x_2,\ ..., x_n\right)$.

Duální funkce

Poznámka. Duální funkci k funkci *f* můžeme jednoduše označovat f^*.

Tabulku pravdivostních hodnot duální funkce f^* (při daném pořadí vektorů hodnot proměnných) lze snadno odvodit z tabulky pravdivostních hodnot funkce *f*. Stačí invertovat hodnoty funkce *f*, tj. zaměnit 0 za 1 a 1 za 0, a obrátit pořadí vektorů hodnot proměnných.

V následující tabulce (tab. 3.3) jsou k vybraným elementárním funkcím přiřazeny funkce duální.

Tab. 3.3.

f	f^*
0	1
1	0
x	x
$\overline{x}$	$\overline{x}$
$x_1 \wedge x_2$	$x_1 \vee x_2$
$x_1 \vee x_2$	$x_1 \wedge x_2$

Na první pohled je zřejmé, že konstantní funkce 1 je duální k funkci 0 a také funkce 0 je duální k funkci 1. Další vztahy odvodíme přímo z definice duality.

Je-li $f\left(x\right) = x,$ pak $f^*\left(x\right) = \overline{f}\left(\overline{x}\right) = \overline{\left(\overline{x}\right)} = x.$ Podobně, s použitím de Morganova zákona dostaneme:

je-li $f\left(x_1, x_2\right) = x_1 \wedge x_2,$ pak $f^*\left(x_1, x_2\right) = \overline{f}\left(\overline{x}_1, \overline{x}_2\right) = \overline{\left(\overline{x}_1 \wedge \overline{x}_2\right)} = x_1 \vee x_2.$

Přímo z definice duality vyplývá

$$f^{**} = \left(f^*\right)^* = f.$$

Funkce *f* je tedy duální k funkci f^* (tzv. **vlastnost vzájemnosti**).

Představme si, že funkce $f(x_1, x_2, ..., x_n)$ je realizována formulí $\mathcal{A}$. Následující věta (viz [6]) ukazuje, jak vypadá formule $\mathcal{A}^*$, jež realizuje funkci $f^*(x_1, x_2, ..., x_n)$.

Věta 3.4.1 (realizace formule pomocí funkce). Jestliže platí $\mathcal{A}(x_1, ..., x_n) = f\left(f_1(x_{11}, ..., x_{1p_1}), ..., f_m(x_{m1}, ..., x_{mp_m})\right)$, pak bude platit $\mathcal{A}^*(x_1, ..., x_n) = f^*\left(f_1^*(x_{11}, ..., x_{1p_1}), ..., f_m^*(x_{m1}, ..., x_{mp_m})\right)$, kde všechny použité symboly proměnných $x_{11}, ..., x_{mp_m}$ pocházejí z množiny $\{x_1, ..., x_n\}$.

Důkaz je uveden v pracích [6,7].

Z právě uvedené věty vyplývá princip duality pro formule.

Princip duality

Princip duality. Jestliže formule $\mathcal{A} = C[f_1, ..., f_s]$ realizuje funkci $f(x_1, x_2, ..., x_n)$, pak formule $\mathcal{A}^* = C[f_1^*, ..., f_s^*]$, kterou získáme z formule $\mathcal{A}$ záměnou funkcí $f_1, ..., f_s$ odpovídajícími duálními funkcemi $f_1^*, ..., f_s^*$, realizuje funkci $f^*(x_1, x_2, ..., x_n)$. Formule $\mathcal{A}^*$ se nazývá

Duální formule

duální formulí k formuli $\mathcal{A}$.

Ve speciálním případě, kdy $\mathcal{A} = C[0, 1, \overline{x}, x_1 \wedge x_2, x_1 \vee x_2]$, je duální formule $\mathcal{A}^* = C[1, 0, \overline{x}, x_1 \vee x_2, x_1 \wedge x_2]$. To znamená, že pro získání duální formule $\mathcal{A}^*$ k libovolné formuli $\mathcal{A}$ nad množinou funkcí $\{0, 1, \overline{x}, x_1 \wedge x_2, x_1 \vee x_2\}$ je třeba zaměnit ve formuli $\mathcal{A}$ 0 za 1, 1 za 0, $\wedge$ za $\vee$ a $\vee$ za $\wedge$. Pro ilustraci uvádíme několik příkladů.

Příklad 3.4.1.

a) $\mathcal{A}(x_1, x_2) = (x_1 \wedge x_2) \vee (\overline{x}_1 \wedge x_2)$; $\mathcal{A}^*(x_1, x_2) = (x_1 \vee x_2) \wedge (\overline{x}_1 \vee x_2)$,

b) $\mathcal{B}(x_1, x_2) = 1 \wedge (\overline{x}_1 \vee x_2)$; $\mathcal{B}^*(x_1, x_2) = 0 \vee (\overline{x}_1 \wedge x_2)$.

Z principu duality vyplývá i následující tvrzení. Je-li $\mathcal{A} = \mathcal{B}$, pak také $\mathcal{A}^* = \mathcal{B}^*$.

Úkol. Najděte duální výraz k ekvivalenci: $\overline{x_1 \wedge x_2} = \overline{x}_1 \vee \overline{x}_2$.

3.5 Rozklad logických funkcí podle proměnných

V této části ukážeme, že každou logickou funkci lze vyjádřit ve tvaru formule nad nějakou množinou elementárních funkcí. Nejprve zavedeme označení

$$x^{\sigma} = x \wedge \sigma \vee \overline{x} \wedge \overline{\sigma},$$

kde σ je parametr, který může nabývat pouze logických hodnot 0 nebo 1. Odtud bezprostředně plyne

$$x^{\sigma} = \begin{cases} \overline{x} \text{ pro } \sigma = 0, \\ x \text{ pro } \sigma = 1. \end{cases}$$

Nyní dokážeme pomocné tvrzení, že $x^{\sigma} = 1,$ právě když $x = \sigma,$ tj. když hodnota základu mocniny je rovna hodnotě exponentu.

Důkaz. Nechť platí $x = \sigma.$ Pak $x^{\sigma} = (x \wedge x) \vee (\overline{x} \wedge \overline{x}) = x \vee \overline{x} = 1.$ Naopak, nechť platí $x^{\sigma} = 1,$ pak musí být $\overline{x \wedge \sigma} = \overline{x} \wedge \overline{\sigma}$ a také $\overline{x} \vee \overline{\sigma} = \overline{x} \wedge \overline{\sigma},$ ale to je možné pouze tehdy, když $\overline{x} = \overline{\sigma}$ neboli $x = \sigma.$ □

Věta 3.5.1 (věta o rozkladu funkce podle proměnných). Každou logickou funkci je možno pro libovolné m $(1 \le m \le n)$ vyjádřit ve tvaru

$$f(x_1, .., x_m, x_{m+1}, ..., x_n) = \bigvee_{(\sigma_1,...,\sigma_m)} x_1^{\sigma_1} \wedge ... \wedge x_m^{\sigma_m} \wedge f(\sigma_1, .., \sigma_m, x_{m+1}, ..., x_n), \quad (3.1)$$

kde se uvedený logický součet bere přes všechny možné m-tice hodnot proměnných $x_1, ..., x_m.$ Výraz na pravé straně uvedeného vztahu se nazývá **rozklad funkce podle proměnných** $x_1, ..., x_m.$

Rozklad funkce podle proměnných

Důkaz uvedené věty je triviální. Nechť $(\alpha_1, ..., \alpha_n)$ je libovolný vektor proměnných. Pak po dosazení do (3.1) dostaneme

$$f(\alpha_1, ..., \alpha_n) = \bigvee_{(\sigma_1,...,\sigma_m)} \alpha_1^{\sigma_1} \wedge ... \wedge \alpha_m^{\sigma_m} \wedge f(\sigma_1, .., \sigma_m, \alpha_{m+1}, ..., \alpha_n) =$$
$$= \alpha_1^{\alpha_1} \wedge ... \wedge \alpha_m^{\alpha_m} \wedge f(\alpha_1, .., \alpha_m, \alpha_{m+1}, ..., \alpha_n) = f(\alpha_1, ..., \alpha_n).$$
□

V dalším výkladu se zaměříme na rozklad logické funkce podle všech proměnných. Podle věty 3.5.1 má tento rozklad tvar

$$f(x_1, ..., x_n) = \bigvee_{(\sigma_1,...,\sigma_n)} x_1^{\sigma_1} \wedge ... \wedge x_n^{\sigma_n} \wedge f(\sigma_1, ..., \sigma_n), \quad (3.2)$$

což vede k pojmu úplné disjunktní normální formy (ve zkratce úplná DNF).

Věta 3.5.2. Každou logickou funkci je možno vyjádřit jako formuli nad množinou elementárních funkcí negace, konjunkce a disjunkce.

Důkaz. Budeme uvažovat dva případy.

a) Nechť $f\left(x_1,\ ...,\ x_n\right)=0.$ Potom zřejmě platí $f\left(x_1,\ ...,\ x_n\right)=x_i \wedge \overline{x}_i,$ kde i je libovolný prvek množiny $\{1,\ ...,\ n\}$.

b) Nechť $f\left(x_1,\ ...,\ x_n\right)\neq 0.$ V tomto případě, vycházeje ze vztahu (3.2), dostaneme

$$f\left(x_1,\ ...,\ x_n\right)=\bigvee_{(\sigma_1,...,\sigma_n)} x_1^{\sigma_1}\wedge ...\wedge x_n^{\sigma_n}\wedge f\left(\sigma_1,\ ...,\ \sigma_n\right)=\bigvee_{\substack{(\sigma_1,...,\sigma_n)\\ f(\sigma_1,...,\sigma_n)=1}} x_1^{\sigma_1}\wedge ...\wedge x_n^{\sigma_n}.\ \square$$

Úplná DNF

Právě uvedený rozklad se nazývá **úplná disjunktivní forma** (**úplná DNF forma**) funkce $f\left(x_1,\ ...,\ x_n\right)$. Úplná DNF má tedy tvar disjunkce členů spojených operací konjunkce (disjunkce konjunktů).

Věta 3.5.2 má konstruktivní charakter, protože umožňuje formulovat algoritmus pro konstrukci úplné DNF.

Algoritmus pro konstrukci úplné DNF

Algoritmus pro konstrukci úplné DNF sestává z následujících pěti kroků.

1. Sestavit pro danou funkci $f\left(x_1,\ ...,\ x_n\right)$ tabulku pravdivostních hodnot.
2. Ověřit, zda platí $f\left(x_1,\ ...,\ x_n\right)\neq 0.$
3. Vybrat všechny řádky hodnot $\sigma_1,\ ...,\ \sigma_n$ proměnných $x_1,\ ...,\ x_n$, pro něž platí $f\left(\sigma_1,\ ...,\ \sigma_n\right)=1.$
4. Pro každý vybraný řádek vytvořit konjunkci (konjunkt) ve tvaru $x_1^{\sigma_1}\wedge ...\wedge x_n^{\sigma_n}$.
5. Získané konjunkce spojit operací disjunkce do výsledné úplné DNF.

Příklad 3.5.1. Konstrukci úplné DNF ukážeme na příkladě logické funkce $f\left(x_1, x_2, x_3\right)$ zadané tabulkou pravdivostních hodnot (viz tab. 3.4).

Tab. 3.4.

x_1	x_2	x_3	$f\left(x_1,\ x_2, x_3\right)$
0	0	0	1

0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Pro danou funkci zřejmě platí $f\left(x_1, x_2, x_3\right) \neq 0.$ Ve 3. kroku algoritmu vybereme řádky 1, 2, 6 a 8. Pro tyto řádky vytvoříme konjunkce $\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3,$ $\overline{x}_1 \wedge \overline{x}_2 \wedge x_3,$ $x_1 \wedge \overline{x}_2 \wedge x_3$ a $x_1 \wedge x_2 \wedge x_3.$ V posledním kroku vytvoříme úplnou disjunktivní normální formu $f\left(x_1, x_2, x_3\right) = \left(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right) \vee \left(\overline{x}_1 \wedge \overline{x}_2 \wedge x_3\right) \vee \left(x_1 \wedge \overline{x}_2 \wedge x_3\right) \vee \left(x_1 \wedge x_2 \wedge x_3\right).$

Poznámky.

a) Jednotlivé konjunkce není nutno uzavírat do závorek, protože konjunkce má vyšší prioritu než disjunkce.

b) Pro zjednodušení zápisu se operátory $\wedge$ a $\vee$ obvykle nahrazují běžnými algebraickými operátory pro násobení a sčítání, takže výsledná úplná DNF se zapisuje takto: $f\left(x_1,\ x_2, x_3\right) = \overline{x}_1\overline{x}_2\overline{x}_3 + \overline{x}_1\overline{x}_2 x_3 + x_1\overline{x}_2 x_3 + x_1 x_2 x_3.$

Princip duality nám umožňuje vyjádřit libovolnou logickou funkci ve tvaru konjunkce členů spojených operací disjunkce. Nechť $f\left(x_1,\ ...,\ x_n\right) \neq 1,$ potom pro funkci duální zřejmě platí $f^*\left(x_1,\ ...,\ x_n\right) \neq 0.$ Jestliže na duální funkci aplikujeme větu 3.5.2, dostaneme

$$f^*\left(x_1,\ ...,\ x_n\right) = \bigvee_{\substack{(\sigma_1,\dots,\sigma_n) \\ f^*(\sigma_1,\dots,\sigma_n)=1}} x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n}.$$

Na základě principu duality postupně odvodíme

$$f\left(x_1,\ ...,\ x_n\right) = f^{**}\left(x_1,\ ...,\ x_n\right) = \bigwedge_{\substack{(\sigma_1,\dots,\sigma_n) \\ f^*(\sigma_1,\dots,\sigma_n)=1}} \left(x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n}\right) =$$

$$= \bigwedge_{\substack{(\sigma_1,\dots,\sigma_n) \\ f(\overline{\sigma}_1,\dots,\overline{\sigma}_n)=0}} \left(x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n}\right) = \bigwedge_{\substack{(\sigma_1,\dots,\sigma_n) \\ f(\sigma_1,\dots,\sigma_n)=0}} \left(x_1^{\overline{\sigma}_1} \wedge \dots \wedge x_n^{\overline{\sigma}_n}\right).$$

Úplná KNF

Výraz $\bigwedge\limits_{\substack{(\sigma_1,\dots,\sigma_n) \\ f(\sigma_1,\dots,\sigma_n)=0}} \left(x_1^{\bar{\sigma}_1} \wedge \dots \wedge x_n^{\bar{\sigma}_n} \right)$ se nazývá **úplná konjunktivní normální forma** (**úplná KNF forma**). Úplná KNF má tedy tvar konjunkce disjunktů.

Algoritmus pro konstrukci úplné KNF

Algoritmus pro konstrukci úplné KNF je podobný algoritmu pro konstrukci úplné DNF. Sestává z následujících kroků.

1. Sestavit pro danou funkci $f\left(x_1, \dots, x_n\right)$ tabulku pravdivostních hodnot.
2. Ověřit, zda platí $f\left(x_1, \dots, x_n\right) \neq 1.$
3. Vybrat všechny řádky hodnot $\sigma_1, \dots, \sigma_n$ proměnných $x_1, \dots, x_n$, pro něž platí $f\left(\sigma_1, \dots, \sigma_n\right) = 0.$
4. Pro každý vybraný řádek vytvořit disjunkci (disjunkt) ve tvaru $x_1^{\bar{\sigma}_1} \vee \dots \vee x_n^{\bar{\sigma}_n}$.
5. Získané disjunkce spojit operací konjunkce do výsledné úplné KNF.

Příklad 3.5.2. Sestrojíme úplnou KNF pro funkci zadanou tabulkou pravdivostních hodnot (viz tab. 3.4).

Pro danou funkci zřejmě platí $f\left(x_1, x_2, x_3\right) \neq 1.$ Ve 3. kroku algoritmu vybereme řádky 3, 4, 5 a 7. Pro tyto řádky vytvoříme disjunkce $x_1 \vee \bar{x}_2 \wedge x_3$, $x_1 \vee \bar{x}_2 \wedge \bar{x}_3$, $\bar{x}_1 \wedge x_2 \wedge x_3$ a $\bar{x}_1 \wedge \bar{x}_2 \wedge x_3$. V posledním kroku vytvoříme úplnou KNF $f\left(x_1, x_2, x_3\right) = \left(x_1 \vee \bar{x}_2 \vee x_3\right) \wedge \left(x_1 \vee \bar{x}_2 \vee \bar{x}_3\right) \wedge \left(\bar{x}_1 \vee x_2 \vee x_3\right) \wedge \left(\bar{x}_1 \vee \bar{x}_2 \vee x_3\right).$

Ve zkratce: $f\left(x_1, x_2, x_3\right) = \left(x_1 + \bar{x}_2 + x_3\right)\left(x_1 + \bar{x}_2 + \bar{x}_3\right)\left(\bar{x}_1 + x_2 + x_3\right)\left(\bar{x}_1 + \bar{x}_2 + x_3\right).$

Příklad 3.5.3. Závěrem uvedeme alternativní postup (algoritmus) pro konstrukci úplné KNF funkce $f\left(x_1, x_2, x_3\right)$ definované tabulkou pravdivostních hodnot uvedenou v tab. 3.4. Nejprve vytvoříme tabulku 3.5 pravdivostních hodnot negace této funkce, tj. funkce $\bar{f}\left(x_1, x_2, x_3\right).$ Pak sestrojíme úplnou DNF této funkce postupem popsaným při řešení příkladu 3.5.1. Dostaneme ve zkratce $\bar{f}\left(x_1, x_2, x_3\right) = \bar{x}_1 x_2 \bar{x}_3 + \bar{x}_1 x_2 x_3 + x_1 \bar{x}_2 \bar{x}_2 + x_1 x_2 \bar{x}_3.$ Nakonec pomocí de Morganova zákona získáme stejný výsledek jako v příkladě 3.5.2, tj. $f\left(x_1, x_2, x_3\right) = \left(x_1 + \bar{x}_2 + x_3\right)\left(x_1 + \bar{x}_2 + \bar{x}_3\right)\left(\bar{x}_1 + x_2 + x_3\right)\left(\bar{x}_1 + \bar{x}_2 + x_3\right).$

Tab. 3.5.

x_1	x_2	x_3	$\overline{f}(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Úlohy.

1. Vyberte tabulku pravdivostních hodnot libovolné logické funkce dvou proměnných a určete příslušné úplné DNF a KNF.
2. Vyberte tabulku pravdivostních hodnot libovolné logické funkce tří proměnných a určete příslušné úplné DNF a KNF.
3. Určete úplné DNF a KNF logické funkce $f(x_1, x_2) = x_1 \Rightarrow x_2$.

3.6 Funkcionální úplnost

Cílem této části je ukázat, jak nalézt množiny elementárních logických funkcí, pomocí nichž je možno vyjádřit libovolnou funkci z množiny P_2 všech logických funkcí.

Funkcionální úplnost

Definice 3.6.1. Množina funkcí $P = \{f_1, f_2, ..., f_i, ...\} \in P_2$ se nazývá **funkcionálně úplná**, jestliže každá logická funkce z P_2 může být reprezentována ve tvaru formule nad funkcemi množiny P.

Příklad 3.6.1. Problematiku funkcionální úplnosti ilustrujeme na několika příkladech.

1. Množina všech logických funkcí P_2 je zřejmě funkcionálně úplná.
2. Podle věty 3.5.2 je také funkcionálně úplná množina $\{\overline{x}, x_1 \wedge x_2, x_1 \vee x_2\}$.
3. Ne každá množina logických funkcí je funkcionálně úplná. Např. množina logických konstant $\{0,1\}$ nemůže být funkcionálně úplná,

protože pomocí ní není možno vyjádřit žádnou logickou funkci, která není konstantní.

Při rozhodování o funkcionální úplnosti dané množiny funkcí se využívá následující věty.

Věta 3.6.1. Nechť jsou dány dvě množiny funkcí z P_2: $P=\{f_1, f_2, ...\}$ a $G=\{g_1, g_2, ...\}$ takové, že množina P je funkcionálně úplná a každou její funkci je možno reprezentovat formulí nad funkcemi množiny G. Pak také množina G je funkcionálně úplná.

Důkaz (viz [jab]). Nechť h je libovolná funkce z P_2. Z úplnosti množiny P vyplývá, že funkci h lze reprezentovat nějakou formulí nad P, což znamená

$$h=C_h[f_1, f_2, ...].$$

Z předpokladů věty dále vyplývají následující formule nad G:

$$f_1=C_1[g_1, g_2, ...],$$
$$f_2=C_2[g_1, g_2, ...], \; ... \, .$$

Jestliže nyní ve formuli $h=C_h[f_1, f_2, ..., f_i, ...]$ nahradíme funkce $f_1, f_2, ...$ formulemi nad G, dostaneme

$$h=C_h[f_1, f_2, ...]=C_h\left[C_1[g_1, g_2, ...], C_2[g_1, g_2, ...], ...\right]=C[g_1, g_2, ...].$$

Výraz $C[g_1, g_2, ...]$ je formule nad množinou G, čímž je věta dokázána.

□

Použití věty 3.6.1 ilustrujeme na několika příkladech.

Příklad 3.6.2. Dokážeme, že množina $G=\{\overline{x}, x_1 \wedge x_2\}$ je funkcionálně úplná. K důkazu použijeme množinu $P=\{\overline{x}, x_1 \wedge x_2, x_1 \vee x_2\}$, o které již víme, že je skutečně funkcionálně úplná. Nyní funkce f_i množiny P vyjádříme formulemi nad funkcemi g_j množiny G.

$$f_1=\overline{x}=g_1=C_1[g_1],$$
$$f_2=x_1 \wedge x_2=g_2=C_2[g_2],$$
$$f_3=x_1 \vee x_2=\overline{\overline{x}_1 \wedge \overline{x}_2}=C_3[g_1, g_2].$$

Tím je důkaz ukončen.

Příklad 3.6.3. Dokážeme, že množina $G = \{\overline{x}, x_1 \vee x_2\}$ je funkcionálně úplná. K důkazu opět použijeme množinu $P = \{\overline{x}, x_1 \wedge x_2, x_1 \vee x_2\}$. Jestliže vyjádříme funkce f_i množiny P formulemi nad funkcemi g_j množiny G, dostaneme

$$\begin{aligned} f_1 &= \overline{x} = g_1 = C_1[g_1], \\ f_2 &= x_1 \wedge x_2 = \overline{\overline{x}_1 \vee \overline{x}_2} = C_2[g_1, g_2], \\ f_3 &= x_1 \vee x_2 = g_2 = C_3[g_2]. \end{aligned}$$

Množina $G = \{\overline{x}, x_1 \vee x_2\}$ je tedy funkcionálně úplná.

Příklad 3.6.4. Dokážeme, že jednoprvková množina $G = \{x_1 / x_2\}$, kde x_1 / x_2 je tzv. Shefferova funkce (funkce NAND) uvedená v tab. 3.2 pod označením f_{12}, je funkcionálně úplná.

Tentokrát použijeme k důkazu množinu $P = \{\overline{x}, x_1 \wedge x_2\}$. V tomto případě můžeme psát

$$\begin{aligned} f_1 &= \overline{x}_1 = x_1 / x_1 = C_1[g_1], \\ f_2 &= x_1 \wedge x_2 = \overline{x_1 / x_2} = (x_1 / x_2)/(x_1 / x_2) = C_2[g_1], \end{aligned}$$

takže množina $G = \{x_1 / x_2\}$ je skutečně funkcionálně úplná.

Příklad 3.6.6. Dokážeme, že množina $\mathrm{G} = \{0, 1, x_1 \wedge x_2, x_1 \oplus x_2\}$ je funkcionálně úplná. K důkazu použijeme množinu $\mathrm{P} = \{\overline{x}, x_1 \wedge x_2\}$. Zřejmě platí:

$$\begin{aligned} f_1 &= \overline{x} = x \oplus 1 = C_1[g_2, g_4], \\ f_2 &= x_1 \wedge x_2 = g_3 = C_2[g_3]. \end{aligned}$$

a tím je důkaz dokončen.

Úlohy.

1. Dokažte, že množina $G = \{0, 1, x_1 \wedge x_2, x_1 \oplus x_2\}$ je funkcionálně úplná. Zvolte $P = \{\overline{x}, x_1 \wedge x_2, x_1 \vee x_2\}$.
2. Dokažte, jednoprvková množina $G = \{\overline{x_1 \vee x_2}\}$, tzv. Pierceova funkce NOR uvedená v tab. 3.2 pod označením f_{13}, je funkcionálně úplná. Návod: zvolte $P = \{\overline{x}, x_1 \vee x_2\}$.

Výsledek příkladu 3.6.5, tj. množina $G=\{0,1,x_1\wedge x_2,x_1\oplus x_2\}$ je funkcionálně úplná, vede k formulaci Žegalkinovy věty.

Věta 3.6.2. (Žegalkinova věta). Každá funkce z množiny P_2 (množiny všech logických funkcí) může být vyjádřena ve tvaru Žegalkinova polynomu.

Žegalkinův polynom

Žegalkinův polynom je logická funkce ve tvaru

$$f\left(x_1,\ \dots,x_n\right)=\sum_{(i_1,\dots,i_s)}^{\oplus} a_{i_1,\dots,i_s}\wedge x_{i_1}\wedge\dots\wedge x_{i_s},$$

kde $i_1,\ \dots,\ i_s$ jsou indexy z množiny $\{1,\ \dots,\ n\}$, koeficienty $a_{i_1,\dots,i_s}$ nabývají hodnot z množiny $\{0,1\}$ a naznačená sumace představuje sčítání modulo 2. Jednoduchou kombinatorickou úvahou zjistíme, že celkový počet Žegalkinových polynomů je 2^{2^n}, tj. právě tolik, kolik je všech logických funkcí *n* proměnných. Z toho ovšem vyplývá, že daná logická funkce je vyjádřena Žegalkinovým polynomem jednoznačně.

Při konstrukci Žegalkinova polynomu pro danou funkci se vychází z tabulky pravdivostních hodnot této funkce. Obecný tvar Žegalkinova polynomu pro funkce dvou proměnných je

$$f\left(x_1,x_2\right)=a\wedge x_1\wedge x_2\oplus b\wedge x_1\oplus c\wedge x_2\oplus d, \tag{3.3}$$

kde koeficienty a,b,c,d nabývají hodnot z množiny $\{0,1\}$. Postupným dosazováním hodnot z jednotlivých řádků tabulky pravdivostních hodnot dané funkce za proměnné x_1,x_2 spočteme hodnoty koeficientů a,b,c,d. Postup ukážeme na jednoduchém příkladu (viz [Kon]).

Příklad 3.6.5. Určíme tvar Žegalkinova polynomu pro funkci dvou proměnných $f\left(x_1,x_2\right)=x_1\vee x_2$. Tabulka pravdivostních hodnot této funkce (jednoduché disjunkce) je uvedena v tab. 3.2 pod označením f_6. K vyjádření obecného tvaru Žegalkinova polynomu (3.3) použijeme zkrácené notace

$$f\left(x_1,x_2\right)=ax_1x_2\oplus bx_1\oplus cx_2\oplus d.$$

Postupným dosazováním z jednotlivých řádků tabulky pravdivostních hodnot funkce $f\left(x_1,x_2\right)=x_1\vee x_2$ dostaneme

$$f\left(0,0\right)=a00\oplus b0\oplus c0\oplus d=0\oplus 0\oplus 0\oplus d=d=0,$$
$$f\left(0,1\right)=a01\oplus b0\oplus c1\oplus 0=0\oplus 0\oplus c\oplus 0=c=1,$$
$$f\left(1,0\right)=a10\oplus b1\oplus 10\oplus 0=0\oplus b\oplus 0\oplus 0=b=1,$$
$$f\left(1,1\right)=a11\oplus 11\oplus 11\oplus 0=a\oplus 1\oplus 1\oplus 0=a\oplus 0=a=1.$$

Žegalkinův polynom pro funkci $f\left(x_1,x_2\right)=x_1\vee x_2$ má tedy tvar $x_1x_2\oplus x_1\oplus x_2$.

3.7 Funkcionální uzavřenost

Začneme definicí pomocného pojmu uzávěr množiny.

Uzávěr množiny

Definice 3.7.1. Nechť P je nějaká podmnožina množiny všech logických funkcí P_2. **Uzávěr množiny** P (označení $[P]$) je množina všech logických funkcí, jež lze vyjádřit formulemi nad množinou P. Je zřejmé, že obecně platí $P\subseteq\left[P\right]$.

Základní vlastnosti uzávěru množiny je možno formulovat takto:

1. $\left[P\right]=P,$
2. $\left[\left[P\right]\right]=\left[P\right],$
3. Jestliže $M_1\subseteq M_2$, pak $\left[M_1\right]\subseteq\left[M_2\right]$.
4. $\left[M_1\cup M_2\right]\supseteq\left[M_1\right]\cup\left[M_2\right]$.

Příklad 3.7.1. Pro ilustraci pojmu uzávěr množiny uvedeme pár příkladů.

1. Nechť $P=P_2$, pak $\left[P\right]=P_2$,
2. Nechť $P=\left\{1,x_1\oplus x_2\right\}$, pak uzávěrem množiny P je množina (třída) všech lineárních funkcí, jež mají ve zkrácené notaci tvar $f\left(x_1,\ ...,\ x_n\right)=c_0\oplus c_1x_1\oplus ...\oplus c_nx_n$, $c_i\in\left\{0,1\right\}$, $i=0,1,\ ...,\ n.$

Pomocí uzávěru můžeme definovat funkcionální úplnost množiny funkcí.

Funkcionální úplnost

Definice 3.7.2. Množina logických funkcí P je **funkcionálně úplná**, jestliže platí $[P] = P_2$. Tato definice je ekvivalentní definici 3.6.1, uvedené již dříve v části 3.6.

Teprve v tomto okamžiku uvedeme definici funkcionální uzavřenosti množiny logických funkcí.

Funkcionální uzavřenost

Definice 3.7.3. Třída (množina) logických funkcí P je **funkcionálně uzavřená**, jestliže platí $[P] = P$.

Následuje přehled nejdůležitějších funkcionálně uzavřených tříd funkcí. Podrobnější charakteristiku těchto tříd nalezne čtenář v pracích [6, 7].

3.7.1 Třída logických funkcí zachovávajících konstantu 0

Tato třída (T_0) je definována předpisem $T_0 = \{ f \in P_2; f(0, \ldots, 0) = 0 \}$. Patří do ní elementární funkce $0, x, x_1 \wedge x_2, x_1 \vee x_2, x_1 \oplus x_2$, ale nepatří elementární funkce 1 a $\overline{x}$. Počet funkcí patřících do T_0 je zřejmě roven polovině všech logických funkcí z P_2, tj. $\left(\frac{1}{2}\right) 2^{2^n} = 2^{2^n - 1}$.

Věta 3.7.1. Třída T_0 je funkcionálně uzavřená.

Důkaz. Musíme dokázat, že platí $[T_0] = T_0$. Platnost vztahu $T_0 \subseteq [T_0]$ je evidentní. Zbývá tedy dokázat $[T_0] \subseteq T_0$, tj. že každá funkce patřící do $[T_0]$ patří také do T_0. Každá funkce $F \in T_0$ může být vyjádřena formulí nad množinou T_0, která realizuje nějakou funkci $f(f_1, \ldots, f_n)$, kde $f, f_1, \ldots, f_n$ jsou funkce ze třídy T_0, tj. funkce zachovávající konstantu 0.

$$F(0, \ldots, 0) = f(f_1(0, \ldots, 0), \ldots, f_n(0, \ldots, 0)) = f(0, \ldots, 0) = 0.$$

Tím je důkaz dokončen. □

3.7.2. Třída logických funkcí zachovávajících konstantu 1

Tato třída (T_1) je definována předpisem $T_1 = \{ f \in P_2; f(1, \ldots, 1) = 1 \}$. Náleží do ní elementární funkce $1, x, x_1 \wedge x_2, x_1 \vee x_2$, ale nikoliv elementární funkce $0, \overline{x}, x_1 \oplus x_2$. Počet funkcí patřících do T_1 je zřejmě roven také polovině všech logických funkcí z P_2, tj. $\left(\frac{1}{2}\right) 2^{2^n} = 2^{2^n - 1}$. Funkce patřící do T_1 jsou duální k funkcím, jež náležejí do třídy T_0.

Věta 3.7.2. Třída T_1 je funkcionálně uzavřená.

Úkol. Dokažte samostatně toto tvrzení. Postup je analogický tomu, který jsme použili při důkazu věty 3.7.1.

3.7.3. Třída samoduálních funkcí

Samoduální funkce

Definice 3.7.4. Funkce $f \in P_2$, která je rovna své duální funkci f^*, se nazývá **samoduální funkce**. Množina všech samoduálních funkcí se nazývá třída samoduálních funkcí a značí se obvykle S. Zřejmě platí: $S = \left\{ f \in P_2;\, f = f^* \right\}$.

Do uvedené třídy patří např. elementární funkce $x, \bar{x}$ nebo $(x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$. Samoduálnost funke se snadno ověřuje v tabulce pravdivostních hodnot.

Pro samoduální funkce platí ekvivalence $\bar{f}(\bar{x}_1, ..., \bar{x}_n) = f(x_1, ..., x_n)$. To znamená, že na vektorech hodnot proměnných $(\alpha_1, ..., \alpha_{\mathrm{n}})$ a $(\bar{\alpha}_1, ..., \bar{\alpha}_{\mathrm{n}})$, které se nazývají opačné, nabývá samoduální funkce opačné hodnoty. Z toho vyplývá, že samoduální funkce je plně určena hodnotami uvedenými v první polovině sloupce svých pravdivostních hodnot. Proto je počet samoduálních funkcí n proměnných roven $2^{2^{n-1}} = \sqrt{2^{2^n}}$.

Věta 3.7.3. Třída S všech samoduálních funkcí je funkcionálně uzavřená.

Důkaz. Zřejmě platí $S \subseteq [S]$. Je nutno dokázat obrácenou inkluzi, tj. $[S] \subseteq S$. Protože S obsahuje identickou funkci x, stačí dokázat, že libovolnou funkci F z $[S]$ je možno reprezentovat formulí, která je realizována superpozicí logických funkcí z S. Nechť $F = f(f_1, ..., f_m)$, kde $f, f_1, ..., f_m \in$ S. Potom platí

$$\begin{aligned} F^*(x_1, ..., x_m) &= f^*\left(f_1^*(x_1, ..., x_m), ..., f_m^*(x_1, ..., x_m)\right) = \\ &= f\left(f_1(x_1, ..., x_m), ..., f_m(x_1, ..., x_m)\right) = F(x_1, ..., x_m). \end{aligned}$$

Tím je tvrzení dokázáno. □

Úkoly. Rozhodněte, zda následující funkce jsou samoduální:

a) $f(x_1, x_2) = x_1 \wedge x_2$,

b) $f(x_1, x_2) = x_1 \vee x_2$,

c) $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$.

3.7.4. Třída monotónních funkcí

Nejprve zavedeme relaci předcházení.

Relace předcházení

Definice 3.7.5. Nechť $\boldsymbol{\alpha}=(\alpha_1,\ ...,\ \alpha_n)$ a $\boldsymbol{\beta}=(\beta_1,\ ...,\ \beta_n)$ jsou dva vektory hodnot proměnných $x_1,...,x_n$. Vektor $\boldsymbol{\alpha}$ předchází vektor $\boldsymbol{\beta}$ $(\boldsymbol{\alpha}\prec\boldsymbol{\beta})$, právě když pro jednotlivé složky obou vektorů platí $\alpha_i \le \beta_i\ (i=1,...,n)$. Uvedená relace se nazývá **relace předcházení**.

Příklad 3.7.2. Např. vektor $\boldsymbol{\alpha}=(1,1,0,1)$ předchází vektor $\boldsymbol{\beta}=(1,1,1,1)$, protože $\alpha_1=1\le 1=\beta_1$, $\alpha_2=1\le 1=\beta_2, \alpha_3=0\le 1=\beta_3$ a $\alpha_4=1\le 1=\beta_4$.

Relace předcházení je příkladem relace částečného uspořádání na množině n-složkových vektorů pravdivostních hodnot, je tedy reflexivní, antisymetrická a tranzitivní.

Monotónní funkce

Definice 3.7.6. Logická funkce $f(x_1,...,x_m)$ se nazývá **monotónní**, jestliže pro každé dva vektory hodnot proměnných $\boldsymbol{\alpha}$ a $\boldsymbol{\beta}$ takové, že $\boldsymbol{\alpha}\prec\boldsymbol{\beta}$, platí $f(\boldsymbol{\alpha})\le f(\boldsymbol{\beta})$. Množina všech takových funkcí se nazývá třída monotónních funkcí a označuje se M.

Do třídy monotónních funkcí patří např. elementární funkce 0,1, x a $x_1\wedge x_2$. Pro ověření monotónnosti se používá tabulka pravdivostních hodnot.

Relace předcházení je částečné uspořádání, ale toto uspořádání není úplné. Existují takové vektory hodnot proměnných, které jsou nesrovnatelné. Ukážeme to na jednoduchém příkladě.

Příklad 3.7.3. Ověříme monotónnost logické funkce $f(x_1,x_2)=x_1\wedge x_2$. Pravdivostní hodnoty této funkce jsou uvedeny v tab. 3.2. Odtud zjistíme, že existují právě dvě posloupnosti vektorů v relaci předcházení:

$(0,0)\prec(0,1)\prec(1,1)$ a $(0,0)\prec(1,0)\prec(1,1)$. V prvním případě pro pravdivostní hodnoty uvažované funkce platí $f(0,0)\le f(0,1)\le f(1,1)$, ve druhém $f(0,0)\le f(1,0)\le f(1,1)$. Vektory $(0,1)$ a $(1,0)$ jsou v relaci předcházení nesrovnatelné. Funkce $f(x_1,x_2)=x_1\wedge x_2$ je zřejmě monotónní.

Věta 3.7.4. Třída všech monotónních funkcí je funkcionálně uzavřená.

Důkaz. Zřejmě platí $M\subseteq[M]$ a navíc identická funkce patří také do $[M]$.Abychom dokázali obrácenou inkluzi, dokážeme, že libovolná funkce $F(x_1,\ ...,x_n)=f\left(f_1(x_1,\ ...,x_n),\ ...,f_m(x_1,\ ...,x_n)\right)\in[M]$ je monotónní, jestliže všechny funkce $f_1, \ldots, f_m$ jsou monotónní. Nechť $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ a $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ jsou dva vektory hodnot proměnných $x_1, \ldots, x_n$ takové, že platí $\boldsymbol{\alpha} \prec \boldsymbol{\beta}$. Jsou-li funkce $f_i,\ i = 1, \ldots, n,$ monotónní, pak musí být $f_i(\boldsymbol{\alpha}) \le f_i(\boldsymbol{\beta})$. Z definice relace předcházení vyplývá $\left(f_1(\boldsymbol{\alpha}), \ldots, f_m(\boldsymbol{\alpha})\right) \prec \left(f_1(\boldsymbol{\beta}), \ldots, f_m(\boldsymbol{\beta})\right)$. Funkce f je podle předpokladu také monotónní, takže dostaneme

$$f\left(f_1(\boldsymbol{\alpha}), \ldots, f_m(\boldsymbol{\alpha})\right) \le f\left(f_1(\boldsymbol{\beta}), \ldots, f_m(\boldsymbol{\beta})\right), \text{ tj. } F(\boldsymbol{\alpha}) \le F(\boldsymbol{\beta}). \qquad \square$$

Úkoly. Rozhodněte, zda následující funkce jsou monotónní:

a) $f(x_1, x_2) = x_1 \vee x_2,$

b) $f(x_1, x_2) = x_1 \Rightarrow x_2,$

c) $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3.$

3.7.5. Třída lineárních funkcí

Definice 3.7.7. Každá logická funkce ve tvaru (zkrácená notace)

$$f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n\,,$$

Lineární funkce

kde koeficienty $c_0, \ldots, c_n \in \{0,1\}$, se nazývá **lineární funkce.** Množina všech takových lineárních funkcí se nazývá třída lineárních funkcí a označuje se L.

Do této třídy patří např. elementární funkce 0,1, $x, \overline{x}, x_1 \oplus x_2,$ ale nepatří tam funkce $x_1 \wedge x_2$ a $x_1 \vee x_2$. Je to speciální třída funkcí, konkrétně Žegalkinovy polynomy obsahující nejvýše lineární členy.

Věta 3.7.5. Třída lineárních funkcí je funkcionálně uzavřená.

Důkaz. Je zřejmé, že lineární výraz vytvořený z lineárních výrazů je nutně lineární. □

Úkoly. Rozhodněte, zda následující funkce jsou lineární:

a) $f(x_1, x_2) = x_1 \wedge x_2,$

b) $f(x_1, x_2) = x_1 \Rightarrow x_2,$

c) $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3.$

Lze snadno ukázat, že třídy logických funkcí T_0, T_1, S, M *a* L jsou po dvou disjunktní (vzájemně různé).

Vycházeje z vlastností základních funkcionálně uzavřených tříd logických funkcí, můžeme formulovat nutné a postačující podmínky pro funkcionální úplnost dané množiny logických funkcí.

NP podmínky pro funkcionální úplnost

Věta 3.7.6. Množina logických funkcí $P \subseteq P_2$ je **funkcionálně úplná**, právě když není plně obsažena v žádné ze tříd $T_0, T_1, S, M \ a\ L$.

Důkaz této věty je poněkud zdlouhavý. Čtenář jej najde jednak v monografii [6], jednak ve skriptech [7].

Použití věty 3.7.6 jako nástroje pro rozhodování, zda daná množina logických funkcí je nebo není funkcionálně úplná, ilustrujeme na příkladě převzatém z monografie [6].

Příklad 3.7.4. Dokážeme, že množina logických funkcí $P = \{0, 1, x_1 \wedge x_2, x_1 \oplus x_2 \oplus x_3\}$ je funkcionálně úplná. Je nutno dokázat, že daná množina P není plně obsažena v žádné ze tříd $T_0, T_1, S, M \ a\ L$. Stačí ovšem, když dokážeme, že v množině P existuje alespoň jedna funkce, která nepatří do $T_0, T_1, S, M \ a\ L$. Postupně zjistíme:

- konstantní funkce 0 nepatří do třídy T_1,
- konstantní funkce 1 nepatří do třídy T_0,
- obě konstantní funkce 0 a 1 nepatří do třídy S,
- funkce $x_1 \wedge x_2$ nepatří do třídy L (není lineární v proměnných x_1, x_2).

Zbývá tedy určit funkci, jež není monotónní. Takovou funkcí je právě funkce $f(x_1, x_2 x_3) = x_1 \oplus x_2 \oplus x_3$. Pravdivostní hodnoty této funkce jsou uvedeny v tab. 3.6.

Tab. 3.6. Pravdivostní hodnoty funkce $f(x_1, x_2 x_3) = x_1 \oplus x_2 \oplus x_3$.

x_1	x_2	x_3	$x_1 \oplus x_2 \oplus x_3$.
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Pro vektory hodnot proměnných $\boldsymbol{\alpha} = (1, 0, 0)$ a $\boldsymbol{\beta} = (1, 0, 1)$ zřejmě platí $\boldsymbol{\alpha} \prec \boldsymbol{\beta}$. Pak pro příslušné hodnoty uvažované funkce dostaneme $f(1,0,0) = 1 > 0 = f(1,0,1)$, což znamená, že funkce $x_1 \oplus x_2 \oplus x_3$ nepatří do třídy *M.* Z uvedeného vyplývá, že množina $P=\{0,1,x_1 \wedge x_2, x_1 \oplus x_2 \oplus x_3\}$ je funkcionálně úplná.

Problém minimalizace počtu funkcí ve funkcionálně úplných množinách řeší následující věta.

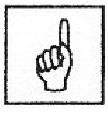
Věta 3.7.7. Z každé funkcionálně úplné množiny funkcí lze vybrat funkcionálně úplnou podmnožinu, která je čtyřprvková.

Důkaz nalezne čtenář v publikacích [6, 7].

Poznámka. V části 3.6 jsme ukázali, že existují funkcionálně úplné množiny s menším počtem prvků.

Kontrolní otázky:

1. Vysvětlete rozdíl mezi skutečnou a fiktivní proměnnou v logické funkci.
2. Jaký je princip definice pomocí indukce?
3. Kdy jsou dvě logické formule _ a _ ekvivalentní?
4. Jaké zákony se nejčastěji používají při zjednodušování formulí nebo při dokazování ekvivalence dvou formulí?
5. Co jsou tautologie a kontradikce?
6. Vysvětlete princip duality formulí.
7. Vysvětlete postup při konstrukci úplné disjunktivní a úplné konjunktivní normální formy.
8. Mohou úplná disjunktivní nebo úplná konjunktivní normální forma obsahovat fiktivní proměnné?
9. Jaký je alternativní postup při konstrukci úplné konjunktivní normální formy?
10. Jak se dokazuje funkcionální úplnost dané množiny logických funkcí?
11. Jaké jsou nejznámější funkcionálně úplné množiny logických funkcí?
12. V čem spočívá výjimečnost Shefferovy funkce (funkce NAND) a Pierceovy funkce (funkce NOR)?
13. Jak se dokazuje, že daná třída (množina) logických funkcí je funkcionálně uzavřená?
14. Jaké znáte funkcionálně uzavřené třídy funkcí?
15. Jaké jsou nutné a postačující podmínky pro funkcionální úplnost dané množiny logických funkcí?



Pojmy k zapamatování:

- logická funkce,
- skutečná proměnná,
- fiktivní proměnná,
- shodnost funkcí,

- logická formule,
- formule stejné struktury,
- realizace funkcí formulemi,
- ekvivalence formulí,
- funkce duální,
- princip duality,
- rozklad funkce podle proměnných,
- úplná disjunktivní normální forma (úplná DNF),
- úplná konjunktivní normální forma (úplná KNF),
- funkcionální úplnost,
- Žegalkinův polynom,
- funkcionální uzavřenost,
- funkce zachovávající konstantu 0,
- funkce zachovávající konstantu 1,
- samoduální funkce,
- relace předcházení,
- monotónní funkce,
- lineární funkce.

Shrnutí

Tato kapitola je věnována základům dvouhodnotové logiky. V úvodních odstavcích jsou definovány základní pojmy (logická funkce, skutečná proměnná, fiktivní proměnná, logická formule, ekvivalence formulí), objasněna jednoznačná souvislost mezi logickými funkcemi a formulemi (realizace funkcí formulemi) a uveden přehled nejvýznamnějších ekvivalencí vhodných pro manipulaci s logickými funkcemi nebo formulemi (důkazy jejich vlastnosti, jejich zjednodušování). Zvláštní pozornost se věnuje především vysvětlení principu duality, algoritmům pro konstrukci úplné DNF, resp. úplné KNF, a striktnímu zavedení pojmů funkcionální úplnost a funkcionální uzavřenost.

Korespondenční úkol pro studenty XDIMA

1. Dokažte matematickou indukcí, že pro každé $n \in \mathbb{N}$ platí rovnost:

$$\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ \dots\ \frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}.$$

2. Ve studijní skupině je 30 studentů. Určete počet možností, že žádní dva studenti neslaví narozeniny téhož dne v roce. Předpokládejte, ýe rok má přesně 365 dnů.

3. Dokažte s použitím ekvivalencí, že formule

$$(\overline{y} \wedge x) \vee (\overline{x} \vee y)$$

je tautologie. Ověření pomocí tabulky pravdivostních hodnot bude hodnoceno polovičním počtem bodů.

4. Zvolte si libovolnou logickou funkci tří proměnných. Vytvořte příslušnou tabulku pravdivostních hodnot a určete úplnou disjunktivní i úplnou konjunktivní normální formu této funkce.

Korespondenční úkol prostudenty 2DIMA

1. Dokažte matematickou indukcí Moivreovu větu:

$$2.\ (\cos\alpha + i\sin\beta)^n = \cos(n\alpha) + \sin(n\alpha).$$

Návod: použijte vzorec pro násobení komplexních jednotek

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos(\alpha+\beta) + i\sin(\alpha+\beta).$$

2. Z hromádky karet (obsahující 4 esa) se náhodně vybere 5 karet. Kolika způsoby lze vybrat nejvýše 2 esa? Návod: použijte kombinatorických principů součtu a součinu.

3. Dokažte s použitím ekvivalencí, že formule

$$(\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}) \vee \overline{x} \vee (x \vee \overline{y})$$

je tautologie. Ověření pomocí tabulky pravdivostních hodnot bude hodnoceno polovičním počtem bodů.

4. Zvolte si libovolnou logickou funkci tří proměnných. Vytvořte příslušnou tabulku pravdivostních hodnot a určete úplnou disjunktivní i úplnou konjunktivní normální formu této funkce.

4 USPOŘÁDANÉ STRUKTURY

Po prostudování této kapitoly:

- si rozšíříte své znalosti o uspořádaných množinách,
- pochopíte základní vlastnosti svazů a Booleových algeber,
- poznáte booleovské funkce a osvojíte si postupy pro minimalizaci booleovských polynomů.

Klíčová slova: částečně uspořádaná množina, ostře uspořádaná množina, lineárně uspořádaná množina, Hasseův diagram, minimální prvek, maximální prvek, nejmenší prvek, největší prvek, infimum množiny, supremum množiny, svaz, úplný svaz, distributivní svaz, ohraničený svaz, komplement, komplementární svaz, Booleova algebra, axiomy Booleovy algebry, booleovská funkce, booleovský polynom, minimalizace booleovského polynomu, minimalizační kritéria, Karnaughova mapa, Quinneův – McCluskeiův algoritmus.

Úvodní část této kapitoly je věnována definici základních pojmů teorie uspořádaných množin (nejmenší a největší prvek, maximální a minimální prvek, infimum a supremum). V dalším výkladu budete sledovat postupný přechod od uspořádaných množin ke složitějším uspořádaným strukturám, jakými jsou svazy a Booleovy algebry. Doporučuji k prostudování také učební text [9]. Základními tématy této kapitoly jsou Booleova algebra a booleovké polynomy. V nich poznáte strukturu a vlastnosti Booleovy algebry a základní metody pro minimalizaci booleovských polynomů (metoda přímá, metoda založená na využití tzv. Karnaughovy mapy a Quinneův-McCluskeiův algoritmus).

4.1 Uspořádané množiny

Relace částečného uspořádání a ostrého uspořádání byly již podrobně vysvětleny v kapitole 1, části 1.2.

Částečně uspořádaná množina

Definice 4.1.1. Nechť R je relace částečného uspořádání na množině A. Pak dvojice (A,R) se nazývá **částečně uspořádaná množina** (**poset**).

Příklady částečně uspořádaných množin:

a) číselné množiny $(\mathbb{N},\leq)$, $(\mathbb{Z},\leq)$, $(\mathbb{Q},\leq)$ a $(\mathbb{R},\leq)$,

b) množinová inkluze $\subseteq$ na nějaké systému množin např. na potenční množině $\mathcal{P}(A)$ nějaké neprázdné množiny X, tj. $(\mathcal{P}(A) \subseteq)$,

c) dvojice $(\mathbb{N},|)$, kde $a|b$ značí „a dělí b“.

Ostře uspořádaná množina

Definice 4.1.2. Nechť R je relace ostrého uspořádání na množině A. Pak dvojice (A, R) se nazývá **ostře uspořádaná množina.**

Příklady částečně uspořádaných množin:
a) číselné množiny $(\mathbb{N},<)$, $(\mathbb{Z},<)$, $(\mathbb{Q},<)$ a $(\mathbb{R},<)$,
b) ostrá množinová inkluze $\subset$ na nějaké systému množin např. na potenční množině $\mathcal{P}(A)$ nějaké neprázdné množiny X, tj. $(\mathcal{P}(A)\subset)$.

Lineárně uspořádaná množina

Definice 4.1.3. Částečné uspořádání na množině A se nazývá **lineární** (**úplné**), jestliže platí $\forall a,b: a \leq b$ nebo $b \geq a$. Dvojice $(A,\leq)$ se pak nazývá **lineárně uspořádaná množina**.

Příklady na lineárně uspořádané množiny:
a) číselné množiny $(\mathbb{N},\leq)$, $(\mathbb{Z},\leq)$, $(\mathbb{Q},\leq)$ a $(\mathbb{R},\leq)$,
b) množina $(\mathcal{P}(A)\subseteq)$., kde $\mathcal{P}(A)$ je potenční množina nějaké neprázdné množiny X, není obecně lineárně uspořádaná.

Konečné částečně uspořádané (ostře uspořádané, lineárně uspořádané) množiny je možno znázorňovat pomocí šipek jako kterékoliv jiné relace. Takové znázornění však bývá často nepřehledné, zvláště u množin s velkým počtem prvků. Proto se při znázorňování částečně uspořádaných množin zakresluje šipkami jen relace tzv. bezprostředního předchůdce.

Relace bezprostředního předchůdce

Definice 4.1.4. Nechť $(A,\leq)$ je částečně uspořádaná množina. Pak prvek a je bezprostředním předchůdcem prvku b, jestliže platí:
a) $a \leq b$,
b) neexistuje žádný prvek $t \in A$ takový, že $a \leq t \leq b$.
Taková relace se nazývá **relace bezprostředního předchůdce**.

Hasseův diagram

Znázornění částečně uspořádaných množin s použitím relace bezprostředního předchůdce se nazývá **Hasseův diagram**. Na obrázku 4.1. je pro ilustraci uveden Hasseův diagram částečně uspořádané množiny $(\mathcal{P}(\{1,2,3\}),\subseteq)$.

Nyní zavedeme pojmy minimální a maximální prvek uspořádané množiny.

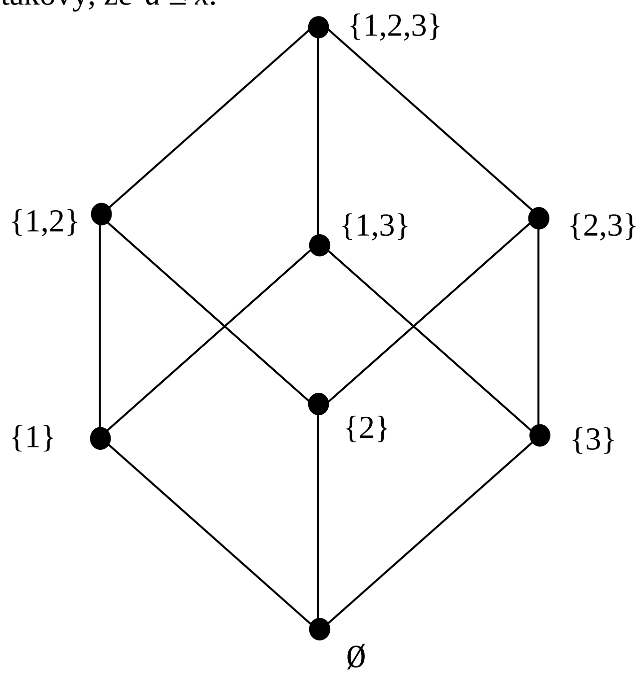
Definice 4.1.5. Nechť $(A,\leq)$ je částečně uspořádaná množina. Prvek $a \in A$ se nazývá

a) **minimální prvek uspořádané množiny** $(A,\leq)$, jestliže neexistuje žádný prvek $x\in A$ takový, že $x\leq a$;

Minimální prvek

b) **maximální prvek uspořádané množiny** $(A,\leq)$, jestliže neexistuje žádný prvek $x\in A$ takový, že $a\leq x$.

Maximální prvek



Obr. 4.1. Hasseův diagram uspořádané množiny $(\mathcal{P}(\{1,2,3\}),\subseteq)$.

S právě zavedenými pojmy na první pohled souvisejí pojmy nejmenší a největší prvek uspořádané množiny.

Definice 4.1.6. Nechť $(A,\leq)$ je částečně uspořádaná množina. Prvek $a\in A$ se nazývá

a) **nejmenší prvek** uspořádané **množiny** $(A,\leq)$, jestliže pro každý prvek $x\in A$ platí $a\leq x$;

Nejmenší prvek

b) **největší prvek** uspořádané **množiny** $(A,\leq)$, jestliže pro každý prvek $x\in A$ platí $x\leq a$.

Největší prvek

Pojem minimální, resp. maximální, prvek je pouze zdánlivě příbuzný pojmu nejmenší, resp. největší, prvek uspořádané množiny. Tyto pojmy je nutno striktně rozlišovat.

Každá neprázdná konečná (částečně) uspořádaná množina má alespoň jeden minimální, resp. maximální, prvek. Pokud je takový prvek právě jeden, pak je zároveň prvkem nejmenším, resp. největším. Minimálních a maximálních prvků může být v neprázdné konečné (částečně) uspořádané množině více, kdežto nejmenší a největší prvek, pokud existuje, je právě jeden.

Příklad 4.1.1. Uvažujme částečně uspořádanou množinu $(\mathcal{P}(\{1,2,3\}),\subseteq)$, jejíž Hasseův diagram je uveden na obr. 4.1. V tomto případě existuje jediný maximální (a tedy i největší prvek) $\{1,2,3\}$ a také jediný minimální (nejmenší) prvek $\emptyset$. Jestliže odstraníme z potenční množiny $\mathcal{P}(\{1,2,3\})$ prvek $\{1,2,3\}$, situace se podstatně změní: v množině jsou tři maximální prvky $\{1,2\}, \{1,3\}$a $\{2,3\}$, ale žádný z nich není největší.

Úkol. Nechť $(A,\prec)$ je částečně uspořádaná množina, kde A je množina trojsložkových vektorů $A=\{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1)(0,1,1)\}$ a $\prec$ relace předcházení definovaná v části 3.7.4. Načrtněte Hasseův diagram této uspořádané množiny a určete její minimální a maximální prvky, popř. nejmenší a největší prvek, pokud ovšem existuje.

Pro teorii svazů a Booleových algeber jsou důležité pojmy infimum a supremum uspořádané množiny.

Infimum množiny

Definice 4.1.7. Nechť $(A,\leq)$ je částečně uspořádaná množina a B libovolná podmnožina A. Pak prvek $a\in A$ se nazývá **dolní závora množiny *B* v množině *A***, jestliže pro každý prvek $x\in B$ platí $a\leq x$. Nechť Z je množina všech dolních závor množiny B v množině A. Největší prvek množiny Z, pokud existuje, se nazývá i**nfimum množiny *B* v množině *A*** a značí se $\inf B$.

Supremum množiny

Definice 4.1.8. Nechť $(A,\leq)$ je částečně uspořádaná množina a B libovolná podmnožina A. Pak prvek $a\in A$ se nazývá **horní závora množiny *B* v množině *A***, jestliže pro každý prvek $x\in B$ platí $x\leq a.$. Nechť Z je množina všech horních závor množiny B v množině A. Nejmenší prvek množiny Z, pokud existuje, se nazývá **supremum množiny *B* v množině *A*** a značí se $\sup B$.

Příklad 4.1.2. Uvažujme částečně uspořádanou množinu $(\mathbb{R},\leq)$ a v ní uzavřený interval $\langle a,b\rangle, a<b$. Určení infima a suprema je v tomto případě triviální. Zřejmě platí: $\inf\langle a,b\rangle=a$, $\sup\langle a,b\rangle=b$. Stejný výsledek dostaneme i pro intervaly $(a,b),(a,b\rangle,\langle a,b)$.

Příklad 4.1.3. Uvažujme částečně uspořádanou množinu $(\mathbb{N},\leq)$, tj. množinu přirozených čísel při uspořádání podle velikosti, a v ní dvouprvkovou množinu $B=\{m,n\}$, $m\leq n$. Určíme infimum a supremum množiny B.

Všechny dolní závory množiny $B=\{m,n\}$ jsou přirozená čísla menší nebo rovna m. Pro největší dolní závoru, tedy infimum, zřejmě platí $\inf B=m.$ Analogicky pro supremum dostaneme $\sup B=n.$

Příklad 4.1.4. Uvažujme částečně uspořádanou množinu $(\mathbb{N},|)$, kde | představuje relaci dělitelnosti, a v ní dvouprvkovou množinu $B=\{m,n\}$, kde $m,n\in\mathbb{N}$. Určíme infimum a supremum množiny B.

Všechny dolní závory množiny $B=\{m,n\}$, jsou takové prvky množiny $(\mathbb{N},|)$, které jsou dělitelné současně čísly m i n. Největší dolní závora, tj. infimum, množiny dolních závor je zřejmě největší společný dělitel (greatest common divisor) čísel m a n, tj. platí $\inf\{m,n\}=\gcd(m,n)$. Analogicky, všechny horní závory množiny $B=(m,n)$ jsou takové prvky množiny $(\mathbb{N},|)$, které jsou současně násobkem obou čísel m i n. Nejmenší horní závora, tj. supremum, množiny horních závor je nejmenší společný násobek (least common multiple) obou čísel, tedy $\sup\{m,n\}=\operatorname{lcm}(m,n)$.

Úkoly.

1. Uvažujte částečně uspořádanou množinu $(\mathcal{P}(X),\subseteq)$, kde $\mathcal{P}(X)$ je potenční množina nějaké neprázdné množiny X, a v ní dvouprvkovou množinu $\{A,B\}$. Určete infimum a supremum této dvouprvkové množiny.
2. Uvažujte částečně uspořádanou množinu $(A,\leq)$, kde A je uzavřený interval $\langle c,d\rangle\in\mathbb{R},\ c<d$. Určete infimum a supremum prázdné množiny.

4.2 Svazy

V této části zavedeme pojem svazu a vysvětlíme některé základní pojmy z teorie svazů.

Definice 4.2.1. Částečně uspořádané množina se nazývá **svaz**, jestliže každá její dvouprvková podmnožina $\{a,b\}$ má infimum a supremum. V tomto případě značíme $\inf\{a,b\}=a\wedge b;\ \ \sup\{a,b\}=a\vee b.$ Svaz

Poznámka. Operace infimum a supremum se považují za základní binární operace svazu a označují se $\wedge$, resp. $\vee$.

Příklady svazu.

a) Částečně uspořádaná množina $(\mathbb{N},|)$ je svaz, protože (viz příklad 4.1.4) pro každou dvouprvkovou množinu platí $\inf\{m,n\} = m \wedge n = \gcd(m,n)$ a také $\sup\{m,n\} = m \vee n = \mathrm{lcm}(m,n)$.

b) Částečně uspořádaná množina $(\mathcal{P}(X),\subseteq)$, kde $\mathcal{P}(X)$ je potenční množina neprázdné množiny X, je také svaz, protože pro každou dvouprvkovou množinu $\{A,B\} \in \mathcal{P}(X)$ platí $\inf\{A,B\} = A \wedge B = A \cap B$ a $\sup\{A,B\} = A \vee B = A \cup B$.

c) Každá lineárně uspořádaná množina je svaz. Toto tvrzení vychází přímo z definice lineárního uspořádání.

d) Jednoprvková množina je triviální svaz.

Úplný svaz

Definice 4.2.2. Částečně uspořádané množina se nazývá **úplný svaz** (**řetězec**), jestliže každá její podmnožina (nejen dvouprvková) má infimum a supremum.

Příklady úplného svazu.

a) Částečně uspořádaná množina $(\mathbb{N},|)$ je úplný svaz, protože pro libovolnou k-tici přirozených čísel existuje největší společný dělitel i nejmenší společný násobek.

a) Částečně uspořádaná množina $(\mathcal{P}(X),\subseteq)$ je také úplný svaz, protože pro libovolnou k-tici množin existuje jejich průnik i sjednocení.

Svazy se obvykle zapisují ve tvaru $(X,\wedge,\vee,\leq)$, kde X reprezentuje množinu, $\leq$ relaci uspořádání a $\wedge,\vee$ operace infima, resp. suprema. To znamená, že pro libovolná $a,b \in X$ platí $a \wedge b = \inf\{a,b\}$ a $a \vee b = \sup\{a,b\}$ v dané relaci $\leq$.

Poznámka. V libovolném svazu platí pro operace infima a suprema zákony komutativní a asociativní.

Distributivní svaz

Definice 4.2.3. Svaz $(X,\wedge,\vee,\leq)$ se nazývá **distributivní**, jestliže pro libovolnou trojici prvků $a,b,c \in X$ platí distributivní zákony, tj.

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \text{ a } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Příklad 4.2.1. Dokážeme, že částečně uspořádaná množina $(\mathcal{P}(X),\subseteq)$ je distributivní svaz $S = (\mathcal{P}(X),\cap,\cup,\subseteq)$. V takovém svazu se operace infima (suprema) interpretují jako množinové operace průniku (sjednocení). Stačí tedy dokázat, že pro libovolné množiny $A,B,C \in \mathcal{P}(X)$ platí rovnost $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. To znamená, že když pro nějaký prvek x platí $x \in A \cap (B \cup C)$, pak platí $x \in (A \cap B) \cup (A \cap C)$, a také naopak, jestliže platí $x \in (A \cap B) \cup (A \cap C)$, pak musí platit $x \in A \cap (B \cup C)$. Důkaz rovnosti dvou množin je záležitostí elementární, proto jej přenechávám čtenáři.

Příklad 4.2.2. Dokážeme, že částečně uspořádaná množina $(\mathbb{N}, \leq)$ je distributivní svaz. Připomínáme, že v tomto svazu se operace infima a suprema interpretují takto: pro libovolná $m, n \in \mathbb{N}$ platí $\inf\{m,n\} = \min\{m,n\}$ a $\sup\{m,n\} = \max\{m,n\}$. V této interpretaci se podmínka distributivity zapisuje ve tvaru rovnosti $\min\{m, \max\{n, p\}\} = \max\{\min\{m,n\}, \min\{m, p\}\}$. Pak stačí dokázat, že pro libovolná $m, n, p \in \mathbb{N}$ je levá strana rovnosti rovna pravé straně. Nechť např. $m \leq n \leq p$. Pak po dosazení do uvedené rovnosti dostaneme $\min\{m, p\} = \max\{m, m\}$, a tedy $m = m$. Analogicky dokážeme platnost této rovnosti i pro všechna ostatní (celkem 5) uspořádání přirozených čísel m, n, p.

Úkol. Dokažte, že částečně uspořádaná množina $(\mathbb{N}, |)$ je distributivní svaz. Návod: operace infima (suprema) interpretujte jako největší společný dělitel (nejmenší společný násobek).

Poznámka. Lze dokázat i obecnější tvrzení, že každá lineárně uspořádaná množina je distributivní svaz.

Ohraničený svaz

Definice 4.2.4. Svaz $(X, \wedge, \vee, \leq)$ se nazývá **ohraničený**, jestliže obsahuje nejmenší i největší prvek. Nejmenší prvek se označuje symbolem 0, největší prvek symbolem 1.

V případě svazu $(\mathcal{P}(X), \subseteq)$ je nejmenším prvkem prázdná množina a největším prvkem celá množina X. Ve svazu $(\mathbb{N}, \leq)$ zřejmě neexistuje největší prvek.

Nechť $(X, \wedge, \vee, \leq)$ je ohraničený svaz. Pak pro libovolný prvek $a \in X$ platí

$$a \wedge 0 = 0, \quad a \vee 0 = a,$$
$$a \wedge 1 = a, \quad a \vee 1 = 1.$$

Komplement

Definice 4.2.5. Prvek $\overline{a} \in X$ svazu $S = (X, \wedge, \vee, \leq)$ se nazývá **komplement** prvku $a \in X$, jestliže platí $a \wedge \overline{a} = 0$ a $a \vee \overline{a} = 1$.

Komplementární svaz

Definice 4.2.6. Ohraničený svaz, v němž ke každému prvku existuje jeho komplement, se nazývá **komplementární**.

Příkladem komplementárního svazu je např. svaz $(\mathcal{P}(X),\cap,\cup,\subseteq)$. V tomto případě je komplementem každého prvku jeho doplněk do množiny *X*. Naproti tomu svazy $(\mathbb{N},\leq)$ a $(\mathbb{N},|)$ nejsou komplementární, protože neobsahují největší prvek.

4.3 Booleova algebra

V předcházejících částech kapitoly 4 jsme připravili vše potřebné k zavedení pojmu Booleova algebra.

Booleova algebra

Definice 4.3.1. Svaz $(X,\wedge,\vee,\leq)$ se nazývá **Booleova algebra**, právě když je distributivní a komplementární.

Věta 4.3.1. V libovolné Booleově algebře má každý prvek právě jeden komplement.

Důkaz provedeme sporem. Předpokládejme, že k prvku $a\in X$ existují dva různé komplementy $\overline{a}_1$ a $\overline{a}_2$. Z definice komplementu plyne

$$a\wedge\overline{a}_1=a\wedge\overline{a}_2=0 \text{ a } a\vee\overline{a}_1=a\vee\overline{a}_2=1.$$

S využitím vlastností distributivnosti a komplementarity dostaneme:

$$\overline{a}_1=\overline{a}_1\wedge 1=\overline{a}_1\wedge(a\vee\overline{a}_2)=(\overline{a}_1\wedge a)\vee(\overline{a}_1\wedge\overline{a}_2)=0\vee(\overline{a}_1\wedge\overline{a}_2)=\overline{a}_1\wedge\overline{a}_2=\inf\{\overline{a}_1,\overline{a}_2\},$$

z čehož vyplývá $\overline{a}_1\leq\overline{a}_2$. Vycházeje z komplementu $\overline{x}_2$ dostaneme analogicky:

$$\overline{a}_2=\overline{a}_2\wedge 1=\overline{a}_2\wedge(a\vee\overline{a}_1)=(\overline{a}_2\wedge a)\vee(\overline{a}_2\wedge\overline{a}_1)=0\vee(\overline{a}_2\wedge\overline{a}_1)=\overline{a}_2\wedge\overline{a}_1=\inf\{\overline{a}_2,\overline{a}_1\},$$

a tedy $\overline{a}_2\leq\overline{a}_1$. Relace částečného uspořádání je antisymetrická, proto musí platit $\overline{a}_1=\overline{a}_2$. Tím je tvrzení dokázáno. □

Booleovu algebru označujeme $B=(X,\wedge,\vee,-,0,1)$, kde *X* je nosič této algebry, $\wedge$ a $\vee$ binární operace infimum a supremum, $-$ unární operace komplement, 0 a 1 nejmenší a největší prvek. Přitom pro každé tři prvky $a,b,c\in X$ platí následující **axiomy** (zákony):

I. komutativní zákony $a\wedge b=b\wedge a$, $\quad a\vee b=b\vee a$;

II. asociativní zákony $(a\wedge b)\wedge c=a\wedge(b\wedge c)$,

$(a\wedge b)\wedge c=a\wedge(b\wedge c)$;

III. distributivní zákony

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$

Axiomy Booleovy algebry

IV. zákony idempotence $a \wedge a = a$, $\quad a \vee a = a$;

V. zákony neutrality $a \wedge 1 = a$, $\quad a \vee 0 = a$;

VI. zákony agresivity $a \wedge 0 = 0$, $\quad a \vee 1 = 1$;

VII. zákony absorpce $a \wedge (a \vee b) = a$, $\quad a \vee (a \wedge b) = a$;

VIII. zákony o vyloučení třetího $a \wedge \overline{a} = 0$, $\quad a \vee \overline{a} = 1$.

Poznámka. Axiomy uvedené v pravém sloupci lze odvodit na základě principu duality, tj. nahrazením operace infimum za operaci supremum, nejmenšího prvku za největší a také naopak. Axiomy v levém sloupci představují **úplný axiomatický systém Booleovy algebry**.

Příklady struktur, které jsou Booleovou algebrou.

a) **Množinová algebra** $(\mathcal{P}(X), \cap, \cup, \overline{A}, \emptyset, X)$, kde $\mathcal{P}(X)$ je potenční množina nějaké neprázdné množiny *X*, množinový průnik (operace $\cap$) definuje operaci infimum, množinové sjednocení (operace $\cup$) je operací supremum, $\overline{A}$ doplněk množiny $A \in \mathcal{P}(X)$ (komplement prvku *A*), prázdné množina ($\emptyset$) nejmenší a celá množina *X* největší prvek algebry.

b) **Algebra jevů** $(\mathbb{A}, \cap, \cup, \overline{A}, \emptyset, \Omega)$**,** kde $\mathbb{A}$ je množina všech elementární jevů spjatých s daným náhodným procesem. Infimum je definováno jako průnik jevů, supremum jako sjednocení jevů, komplement jako komplementární (doplňkový) jev $\overline{A}$ k danému jevu *A*, nejmenší prvek jako nemožný jev $\emptyset$ a největší prvek jako jistý jev Ω. Tato algebra je v podstatě shodná s množinovou algebrou, protože jevy jsou chápány jako množiny.

c) **Algebra výrokové logiky** $(\{0,1\}, \wedge, \vee, -, 0, 1)$**,** kde infimum je definováno jako logický součin (konjunkce), supremum jako logický součet (disjunkce), komplement jako negace, nejmenší prvek je logická konstanta 0 a největší prvek jako logická konstanta 1. S využitím logických funkcí konjunkce, disjunkce a negace lze tedy vytvořit z množiny $\{0,1\}$ Booleovu algebru.

d) **Triviální Booleova algebra** $(\{0\}, \wedge, \vee, -, 0, 0)$**.** V této algebře platí: $0 \wedge 0 = 0$, $0 \vee 0 = 0$, $\overline{0} = 0$, nejmenším i největším prvkem je 0.

Dále dokážeme některé významné vlastnosti Booleovy algebry, především platnost de Morganových zákonů a zákona dvojité negace.

Zákon dvojité negace

Věta 4.3.2. Nechť B je Booleova algebra. Pak pro každý prvek $a \in X$ platí: $\overline{(\overline{a})} = a,$ tedy **zákon dvojité negace**.

Důkaz. Označme $\overline{a}$ komplement prvku a. Pak z axiomů VIII dostaneme $a \wedge \overline{a} = 0$ a $a \wedge \overline{a} = 0.$ Podle komutativního zákona (axiom I) musí platit také $\overline{a} \wedge a = 0$ a $\overline{a} \wedge a = 0.$ Z definice komplementu je zřejmé, že prvek a je komplementem prvku $\overline{a}$, takže $\overline{(\overline{a})} = a.$ □

de Morganovy zákony

Věta 4.3.3. Nechť B je Booleova algebra. Pak pro každé dva prvky $a, b \in X$ platí: $\overline{(a \wedge b)} = \overline{a} \vee \overline{b}$ a $\overline{(a \vee b)} = \overline{a} \wedge \overline{b},$ tj. **de Morganovy zákony**.

Důkaz. Stačí dokázat pouze první formuli, protože platnost druhé formule vyplývá z principu duality. Na základě axiomu VIII je zřejmé, že rovnost $\overline{(a \wedge b)} = \overline{a} \vee \overline{b}$ platí, právě když současně platí $(a \wedge b) \wedge \left(\overline{a} \wedge \overline{b}\right) = 0$ a $(a \wedge b) \vee \left(\overline{a} \wedge \overline{b}\right) = 1.$ Platnost obou posledně uvedených formulí snadno dokážeme pomocí axiomů I, II, III, VI, VII a VIII. Pro první formuli postupně dostaneme

$$(a \wedge b) \wedge \left(\overline{a} \wedge \overline{b}\right) = \left((a \wedge b) \wedge \overline{a}\right) \vee \left((a \wedge b) \wedge \overline{b}\right) =$$
$$= (a \wedge \overline{a} \wedge b) \vee \left(a \wedge b \wedge \overline{b}\right) = (0 \wedge b) \vee (a \wedge 0) = 0 \vee 0 = 0.$$

Analogicky pro druhou formuli

$$(a \wedge b) \vee \left(\overline{a} \wedge \overline{b}\right) = \left(\overline{a} \wedge \overline{b}\right) \vee (a \wedge b) = \left(\left(\overline{a} \wedge \overline{b}\right) \vee a\right) \wedge \left(\left(\overline{a} \wedge \overline{b}\right) \vee b\right) =$$
$$= \left(\overline{a} \vee a \vee \overline{b}\right) \wedge \left(\overline{a} \vee b \vee \overline{b}\right) = \left(1 \vee \overline{b}\right) \wedge (\overline{a} \vee 1) = 1 \wedge 1 = 1.$$

Tím je platnost první formule dokázána. □

Pomocí základních axiomů I – VIII, jakož i formulí dříve odvozených (např. de Morganových zákonů a zákonu dvojité negace) je možno dokázat celou řadu vlastností Booleovy algebry.

Úkoly.

1. Dokažte, že pro každé dva prvky $a, b \in X$ platí:
   a) $a \wedge b = a \wedge (\overline{a} \vee b),$
   b) $a \vee b = a \vee (\overline{a} \wedge b).$
2. Dokažte, že pro každé dva prvky $a, b \in X$ platí:
   a) $a \vee b = 0 \Leftrightarrow a = 0$ a současně $b = 0,$

b) $a \wedge b = 1 \Leftrightarrow a = 1$ a současně $b = 1$.

3. Dokažte, že pro každé dva prvky $a, b \in X$ platí:

   a) $a = b \Leftrightarrow \left(a \wedge \overline{b}\right) \vee \left(\overline{a} \wedge b\right)$,

   b) $a = b \Leftrightarrow \left(a \vee \overline{b}\right) \wedge \left(\overline{a} \vee b\right)$.

4.4 Booleovské funkce

Nejprve uvedeme definici booleovské funkce (Booleovy funkce).

Booleovská funkce

Definice 4.4.1. Nechť $B = \left(X, \wedge, \vee, -, 0, 1\right)$ je Booleova algebra. Pak libovolné zobrazení $F : X^n \to X$ se nazývá **booleovská funkce** (**Booleova funkce**) ***n*** **proměnných**.

*Poznámky***.**

1. Někteří autoři definují booleovskou funkci n proměnných takto: libovolné zobrazení $F : \{0,1\}^n \to \{0,1\}$ se nazývá booleovské funkce.
2. Každá logická funkce z kapitoly 3 je booleovská funkce.

Booleovský polynom

Definice 4.4.2. Nechť B je Booleova algebra. Pak **booleovský polynom** (**Booleův polynom**) je řetězec vytvořený ze všech prvků množiny X (včetně prvků 0 a 1) pomocí konečného počtu operací infimum, supremum a komplement.

Příklady booleovských polynomů:

$\overline{x}$, $\overline{\left(x_1 \vee \overline{x}_2\right)}$, $\left(\overline{x}_1 \wedge x_2 \wedge \overline{x}_3\right) \vee \left(x_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right)$,

$\left(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right) \vee \left(\overline{x}_1 \wedge x_2 \wedge \overline{x}_3\right) \vee \left(x_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right)$.

Existuje jednoznačná korespondence mezi množinou všech booleovských funkcí n proměnných a množinou booleovských polynomů n proměnných ve tvaru úplné DNF. To nám umožňuje omezit se jen na studium booleovských polynomů. Podle věty 3.5.2 lze pro každou logickou funkce zkonstruovat její úplnou DNF. Jestliže zobecníme tuto větu na množinu všech booleovských funkcí, pak je možno zkonstruovat úplnou DNF i pro každý booleovský polynom. K vytvoření úplné DNF booleovského polynomu můžeme využít algoritmu popsaného v části 3.5. Vedle tohoto algoritmu (tzv. nepřímé metody) existuje i metoda přímá, jejíž algoritmus popíšeme.

Přímá metoda pro konstrukci úplné DNF

Algoritmus přímé metody pro konstrukci DNF

1. Aplikovat na vybranou booleovskou funkci F de Morganovy zákony.
2. Aplikovat distributivní zákony.
3. Využít zákony idempotence, neutrality, agresivity a vyloučení třetího.

4. Pokud v některé části získané booleovského výrazu chybí proměnná x_i, vytvořit infimum této části s $\left(x_i \vee \overline{x}_i\right)$.
5. Eventuálně uspořádat jednotlivé členy, popř. proměnné, ve vytvořené úplné DNF booleovského polynomu.

Uvedený postup ilustrujeme na příkladě převzatém ze skript [7].

Příklad 4.4.1. Sestrojíme booleovský polynom ve tvaru úplné DNF pro funkci $F\left(x_1, x_2\right) = \left(\overline{\left(\overline{x}_1 \wedge x_2\right)} \wedge \overline{x}_1\right) \vee x_2$.

$$\left(\overline{\left(\overline{x}_1 \wedge x_2\right)} \wedge \overline{x}_1\right) \vee x_2 = \left(\left(\overline{\overline{x}}_1 \vee \overline{x}_2\right) \wedge \overline{x}_1\right) \vee x_2 = \left(\left(x_1 \vee \overline{x}_2\right) \wedge \overline{x}_1\right) \vee x_2 =$$
$$= \left(\left(x_1 \wedge \overline{x}_1\right) \vee \left(\overline{x}_2 \wedge \overline{x}_1\right)\right) \vee x_2 = \left(0 \vee \left(\overline{x}_2 \wedge \overline{x}_1\right)\right) \vee x_2 = \left(\overline{x}_2 \wedge \overline{x}_1\right) \vee x_2 =$$
$$= \left(\overline{x}_2 \wedge \overline{x}_1\right) \vee \left(x_1 \vee \overline{x}_1\right) \wedge x_2 = \left(\overline{x}_2 \wedge \overline{x}_1\right) \vee \left(x_1 \wedge x_2\right) \vee \left(\overline{x}_1 \wedge x_2\right) =$$
$$= \left(x_1 \wedge x_2\right) \vee \left(\overline{x}_1 \wedge x_2\right) \vee \left(\overline{x}_1 \wedge \overline{x}_2\right).$$

Hledaný booleovský polynom je tedy $\left(x_1 \wedge x_2\right) \vee \left(\overline{x}_1 \wedge x_2\right) \vee \left(\overline{x}_1 \wedge \overline{x}_2\right)$, ve zkrácené notaci $x_1 x_2 + \overline{x}_1 x_2 + \overline{x}_1 \overline{x}_2$.

Hlavním úkolem této části je popsat metody vhodné k **minimalizaci booleovských funkcí**. Problém minimalizace booleovské funkce spočívá v nahrazení této funkce její ekvivalentní, co nejjednodušší, formou. Minimalizace se provádí ve dvou krocích:

1. konstrukce booleovského polynomu pro danou funkci,
2. minimalizace tohoto polynomu pomocí jednoho z následujících kritérií.

Minimalizační kritérium 1

Kritérium 1 (podle počtu literálů, tj. počtu proměnných nebo jejich komplementů). Součet konjunktů booleovského polynomu *f* je minimální vzhledem k počtu literálů, právě když pro každý booleovský polynom *f* platí: je-li $g = f$, pak počet literálů v polynomu *g* je větší nebo roven počtu literálů v polynomu *f* (včetně násobnosti).

Minimalizační kritérium 2

Kritérium 2 (podle počtu konjunktů). Součet konjunktů booleovského polynomu v DNF formě je minimální vzhledem k počtu konjunktů, právě když pro každý booleovský polynom *f* platí: je-li $g = f$, pak polynom *g* neobsahuje menší počet konjunktů než polynom *f*. Jestliže oba mají stejný počet konjunktů, pak polynom *g* neobsahuje menší počet literálů než polynom *f* (včetně násobnosti).

Existuje několik metod pro minimalizaci booleovských polynomů:

a) metody algebraická,
b) metody grafické (např. Karnaughova mapa),

c) metoda Quinneova - McCluskeiova.

4.4.1 Algebraická metoda

Tato metoda je nejjednodušší z minimalizačních metod, ale hodí se pouze pro minimalizaci velmi jednoduchých booleovských polynomů. V principu je založena na využívání základních ekvivalencí. Použití algebraické metody ilustrujeme na následujícím příkladu.

Příklad 4.4.2. Minimalizujeme booleovský polynom se třemi proměnnými $(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge \overline{x}_3)$. Postupně dostaneme

$$
\begin{aligned}
&(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge \overline{x}_3) = \\
&= \left[(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3)\right] \vee \left[(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge \overline{x}_3)\right] = \\
&= \left[(\overline{x}_1 \wedge \overline{x}_3) \wedge (\overline{x}_2 \vee x_2)\right] \vee \left[(\overline{x}_2 \wedge \overline{x}_3) \wedge (\overline{x}_1 \vee x_1)\right] = \\
&= \left[(\overline{x}_1 \wedge \overline{x}_3) \wedge 1\right] \vee \left[(\overline{x}_2 \wedge \overline{x}_3) \wedge 1\right] = (\overline{x}_1 \wedge \overline{x}_3) \vee (\overline{x}_2 \wedge \overline{x}_3).
\end{aligned}
$$

Hledaný minimální booleovský polynom je tedy $(\overline{x}_1 \wedge \overline{x}_3) \vee (\overline{x}_2 \wedge \overline{x}_3)$, ve zkrácené notaci $\overline{x}_1\overline{x}_3 + \overline{x}_2\overline{x}_3$.

Úkol.
Minimalizujte následující booleovské polynomy:

a) $(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$,

b) $(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge \overline{x}_2 \wedge x_3) \vee (x_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$.

4.4.2 Karnaughova mapa

Karnaughova mapa

Karnaughova mapa je tabulka, která má právě tolik políček, kolik je „kombinací“ vstupních proměnných, tedy 2^n pro *n* proměnných. Každé políčko odpovídá jedné z možných „kombinací“ a zapisujeme do něj odpovídající funkční hodnotu. V případě Karnaughovy mapy se sousední políčka od sebe liší hodnotou jediné proměnné.

Pro Karnaughovu mapu platí následující konvence:

- V případě dvou proměnných používáme tabulku 2×2, přičemž řádky odpovídají jedné proměnné (např. x_1) a sloupce druhé proměnné (např. x_2). Pro tři proměnné se používá zpravidla tabulka 2×4, v níž řádky odpovídají jedné proměnné (např. x_1) a sloupce zbývajícím dvěma proměnným (např. x_2, x_3). Analogicky se postupuje i pro více proměnných.

- Řádky nebo sloupce, v nichž je hodnota proměnné rovna 1 se označují názvem proměnné. V neoznačených řádcích nebo sloupcích je hodnota příslušných proměnných rovna 0.
- Pravá hrana tabulky sousedí s levou hranou, stejně tak i horní hrana sousedí s dolní hranou. Tabulka se tedy považuje v obou směrech (vertikálním i horizontálním) za souvislou.
- Do tabulky se zpravidla vkládají pouze hodnoty 1.

Poznámka. Karnaughova mapa je vhodná pro reprezentaci hodnot dané logické funkce namísto prosté tabulky pravdivostních hodnot, a to zejména u funkcí s větším počtem proměnných.

Při minimalizaci booleovského polynomu se sdružují políčka Karnaughovy mapy do větších souvislých oblastí podle následujících pravidel:

- Sdružuje se 2, 4, 8, ... políček, které všechny obsahují hodnotu 1.
- Tato políčka musí vytvářet souvislou oblast ve tvaru obdélníka.
- V tomto obdélníku se nesmí vyskytovat žádná 0.
- Každé souvislé oblasti odpovídá nějaká logická funkce ve tvaru součinu (konjunktu) proměnných.
- V takovém konjunktu chybí ta proměnná (ty proměnné), které v příslušné souvislé oblasti mění svou hodnotu.

Pokud splníme všechna uvedená pravidla, bude výsledný součet (supremum) funkcí odpovídajících jednotlivým souvislým oblastem hledaným minimálním booleovským polynomem.

Příklad 4.4.3. Použití Karnaughovy mapy ilustrujeme při řešení příkladu 4.4.2. Nejprve zapíšeme do Karnaughovy mapy pravdivostní hodnoty polynomu $(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2 \wedge \overline{x}_3)$. Dostaneme

Tab. 4.1. Karnaughova mapa k příkladu 4.4.3.

			x_2	
		x_3		
	1	0	0	1
x_1	1	0	0	0

V uvedené mapě nalezneme právě dvě souvislé (vyšrafované) oblasti, které obsahují výhradně hodnotu 1:

1. Levý sloupec tabulky o rozměrech 2×1. V této oblasti mění svou hodnotu proměnná x_1, proto bude v zápisu příslušné logické funkce chybět. Hodnoty zbývajících dvou proměnných se nemění, přitom obě jsou nulové. Odpovídající logická funkce bude mít tedy tvar $\bar{x}_2 \wedge \bar{x}_3$.
2. Oblast o rozměrech 1×2 tvořená prvním a čtvrtým prvkem prvého řádku tabulky. Tentokrát mění svou hodnotu proměnná x_2 a obě zbývající proměnné mají hodnotu 0. Odpovídající funkce bude má proto tvar $\bar{x}_1 \wedge \bar{x}_3$.

Hledaný minimální polynom je $\left(\bar{x}_1 \wedge \bar{x}_3\right) \vee \left(\bar{x}_2 \wedge \bar{x}_3\right)$. Tento výsledek se přirozeně shoduje s výsledkem příkladu 4.4.2.

Úkol. Minimalizujte následující booleovské polynomy pomocí Karnaughovy mapy:

a) $\left(x_1 \wedge x_2 \wedge x_3\right) \vee \left(x_1 \wedge x_2 \wedge \bar{x}_3\right) \vee \left(x_1 \wedge \bar{x}_2 \wedge x_3\right) \vee \left(x_1 \wedge x_2 \wedge x_3\right)$,

b) $\left(\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right) \vee \left(\bar{x}_1 \wedge \bar{x}_2 \wedge x_3\right) \vee \left(x_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right) \vee \left(x_1 \wedge \bar{x}_2 \wedge x_3\right) \vee \left(x_1 \wedge x_2 \wedge x_3\right)$.

4.4.3 Metoda Quinneova - McCluskeiova

Tato metoda je patrně nejznámější a v praxi nejčastěji používaná. Dříve než vysvětlíme podstatu metody, zavedeme několik nových pojmů. Ostatní pojmy byly již vysvětleny v části 3.5.

Definice 4.4.3.1. Každý konkunkt v úplné DNF booleovského polynomu *f* se nazývá **minterm** (**term nultého řádu**) tohoto polynomu. Jestliže z daného mintermu odstraním *n* literálů, tj. proměnných nebo jejich doplňků (negací) dostaneme **term *n*-tého řádu**.

Minterm

Term *n*-tého řádu

Příklad 4.4.4. Konjunkty $\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$, $\bar{x}_1 \wedge x_2 \wedge \bar{x}_3$, a $x_1 \wedge \bar{x}_2 \wedge \bar{x}_3$ jsou podle definice všechny mintermy následujícího booleovského polynomu v úplné DNF $f\left(x_1, x_2, x_3\right) = \left(\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right) \vee \left(\bar{x}_1 \wedge x_2 \wedge \bar{x}_3\right) \vee \left(x_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right)$.

Definice 4.4.3.2. Každý konjunkt, který implikuje úplnou DNF daného booleovského polynomu *f* je jeho **implikant**. Přitom polynom *p* implikuje polynom *f*, právě když neexistuje taková *n*-tice proměnných $\left(\alpha_1,\ \ldots,\ \alpha_n\right)$, že $p\left(\alpha_1,\ \ldots,\ \alpha_n\right) = 1$ a současně $f\left(\alpha_1,\ \ldots,\ \alpha_n\right) = 0$.

Implikant

Příklad 4.4.5. Dokážeme, že $p\left(x_1, x_3\right) = \bar{x}_1 \wedge \bar{x}_3$ je implikantem polynomu $f\left(x_1, x_2, x_3\right) = \left(\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right) \vee \left(\bar{x}_1 \wedge x_2 \wedge \bar{x}_3\right) \vee \left(x_1 \wedge \bar{x}_2 \wedge \bar{x}_3\right)$. Zřejmě platí $p(0,0) = 1$. Pro jinou kombinaci hodnot proměnných x_1 a x_3 má polynom $p\left(x_1, x_3\right)$ nulovou hodnotu. Jestliže dosadíme za x_1 a x_2 do polynomu *f*, dostaneme $f\left(0,x_2,0\right)=\overline{x}_2 \vee x_2 \vee 0 = 1$. Tím je důkaz ukončen. □

Prostý implikant

Definice 4.4.3.3. Implikant *p* polynomu *f* se nazývá **prostý implikant**, právě když přestane být implikantem polynomu *f* , když z něj odstraníme libovolný literál (proměnnou nebo její komplement).

Úkol. Dokažte, že $p\left(x_1,x_3\right)=\overline{x}_1 \wedge \overline{x}_3$ je dokonce prostý implikant polynomu $f\left(x_1,x_2,x_3\right)=\left(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right) \vee \left(\overline{x}_1 \wedge x_2 \wedge \overline{x}_3\right) \vee \left(x_1 \wedge \overline{x}_2 \wedge \overline{x}_3\right)$.

Nezkratitelný součet konjunktů

Definice 4.4.3.4. Součet (disjunkce) konjunktů (polynom *f*) pro nějakou booleovskou funkci *F* je **nezkratitelný**, právě když jsou splněny dvě podmínky:

1. Každý konjunkt je prostým implikantem funkce *F*.
2. Jestliže v polynomu *f* vynecháme libovolný konjunkt, pak polynom *f* už nebude definovat funkci *F*.

Quinneův – McCluskeiův algoritmus pro konstrukci minimálního polynomu booleovské funkce *F* sestává ze čtyř kroků:

1. Převést booleovskou funkci *F* na booleovský polynom *f* ve tvaru úplné DNF.
2. Vytvořit množinu *P* všech prostých implikantů polynomu *f*.
3. Vytvořit z množiny *P* množinu všech nezkratitelných polynomů.
4. Vybrat z množiny nezkratitelných polynomy právě ty, jež splňují minimalizační kritéria.

Příklad 4.4.6. Vyřešíme příklad 4.4.2 pomocí Quinneova–McCluskeiova algoritmu**. Z**adaný polynom je už ve tvaru úplné DNF. Každý z konjunktů $\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3$, $\overline{x}_1 \wedge x_2 \wedge \overline{x}_3$ a $x_1 \wedge \overline{x}_2 \wedge \overline{x}_3$ je minterm (viz příklad 4.4.4). Následně sestavíme tabulku mintermů (viz tab. 4.2) a vepíšeme do ní hodnoty jejich základních charakteristik: dvojkové číslo (hodnoty proměnných, pro něž minterm nabývá hodnoty 1), index (počet hodnot 1 ve dvojkovém čísle) a stavový index (hodnota dvojkového čísla v desítkové soustavě).

Tab. 4.2. Tabulka mintermů k příkladu 4.4.6.

Minterm	Dvojkové číslo	Index	Stavový index
$\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$	000	0	0
$\bar{x}_1 \wedge x_2 \wedge \bar{x}_3$	010	1	2
$x_1 \wedge \bar{x}_2 \wedge \bar{x}_3$	100	1	4

Nyní přikročíme k určení prostých implikantů, a to pomocí tzv. krácení termů. Krátit můžeme pouze termy, které se liší o jednotku v počtu hodnot 1 a přitom se liší v hodnotě na stejné pozici. Krácením minitermů $\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$ (000) a $\bar{x}_1 \wedge x_2 \wedge \bar{x}_3$ (010) dostaneme term 1. řádu $\bar{x}_1 \wedge \bar{x}_3$ s dvojkovým číslem $0-0$. Analogicky krácením minitermů $\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$ (000) a $x_1 \wedge \bar{x}_2 \wedge \bar{x}_3$ (100) získáme term 1. řádu $\bar{x}_2 \wedge \bar{x}_3$ s dvojkovým číslem -00. Termy získané krácením představují prosté implikanty. Množina prostých implikantů obsahuje tedy dva termy, tj. $P = \{\bar{x}_1 \wedge \bar{x}_3, \bar{x}_2 \wedge \bar{x}_3\}$. K určení nezkratitelných polynomů se používá tzv. mřížka prostých implikantů (viz tab. 4.3).

Tab. 4.3. Mřížka prostých implikantů k příkladu 4.4.6.

Prostý implikant	$\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$	$\bar{x}_1 \wedge x_2 \wedge \bar{x}_3$	$x_1 \wedge \bar{x}_2 \wedge \bar{x}_3$
$\bar{x}_1 \wedge \bar{x}_3$	+	+	–
$\bar{x}_2 \wedge \bar{x}_3$	+	–	+

Tabulka má formu znaménkové matice, přičemž v buňce na *i*-tém řádku a v *j*-tém sloupci je znaménko +, právě když všechny literály prostého implikantu na *i*-tém řádku jsou také literály minitermu v *j*-tém sloupci. Je-li v dané buňce znaménko +, říkáme, že příslušný miniterm je pokrytý příslušným prostým implikantem. Při konstrukci minimálního polynomu se snažíme o to, aby každý miniterm byl pokrytý aspoň jedním prostým implikantem. V našem případě je řešení jednoznačné, minimální polynom má tvar $(\bar{x}_1 \wedge \bar{x}_3) \vee (\bar{x}_2 \wedge \bar{x}_3)$, ve zkrácené notaci $\bar{x}_1\bar{x}_3 + \bar{x}_2\bar{x}_3$. Tento výsledek se samozřejmě shoduje s výsledky příkladů 4.4.2 i 4.4.3.

Kontrolní otázky:

1. Jak je definován lineární uspořádání?
2. Co je to Hasseův diagram a k čemu slouží?

3. Jaký je rozdíl mezi minimálním a nejmenším prvkem dané uspořádané množiny?
4. Jaký je rozdíl mezi maximálním a největším prvkem dané uspořádané množiny?
5. Jak jsou definovány infimum a supremum uspořádané množiny?
6. Jak je definován svaz, resp. úplný svaz?
7. Jak je definována Booleova algebra?
8. Jaké jsou základní vlastnosti (axiomy) Booleovy algebry?
9. Jak je definována booleovská funkce a speciálně booleovský polynom?
10. Co je cílem minimalizace booleovského polynomu a jaká jsou minimalizační kritéria?
11. Co je Karnaughova mapa a k čemu slouží?
12. Jak se postupuje při minimalizaci booleovského polynomu s využitím Karnaughovy mapy?
13. Jak se postupuje při minimalizaci booleovského polynomu pomocí Quinneovy-McCluskeiovy metody?

Pojmy k zapamatování:

- uspořádaná (částečně uspořádaná) množina,
- ostře uspořádaná množina,
- lineárně uspořádaná množina,
- Hasseův diagram,
- minimální prvek množiny,
- maximální prvek množiny,
- nejmenší prvek množiny,
- největší prvek množiny,
- infimum množiny,
- supremum množiny,
- svaz,
- úplný svaz,
- distributivní svaz,
- ohraničený svaz,
- komplementární svaz,
- Booleova algebra,
- axiomy Booleovy algebry,
- booleovská funkce,
- booleovský polynom,
- minimalizace booleovské funkce (booleovského polynomu),
- minimalizační kritéria,
- algebraická minimalizace,

- Karnaughova mapa,
- Quinneův - McCluskeiův algoritmus.

Shrnutí

Tato kapitola je věnována výkladu základních pojmů teorie uspořádaných algebraických struktur (uspořádané množiny, svazy a Booleovy algebry). Zvláštní pozornost je přitom zaměřena jednak na strukturu a axiomy Booleovy algebry, jednak na problematiku minimalizace booleovských funkcí.

5 ÚVOD DO TEORIE GRAFŮ

Po prostudování této kapitoly:

- pochopíte základní pojmy z teorie grafů,
- naučíte se jednoznačně reprezentovat graf pomocí matic,
- dovedete rozlišit isomorfní a neisomorfní grafy,
- pochopíte pojem souvislého grafu a naučíte se hledat nejkratší cestu v grafu,
- poznáte základní typy podgrafů daného grafu (zejména stromy) a jejich vlastnosti,
- seznámíte se podrobněji s eulerovskými grafy.

Klíčová slova: graf, vrchol grafu, hrana grafu, násobnost hrany, orientace hrany, ohodnocení hrany, úplný graf, kružnice, bipartitní graf, stupeň vrcholu, skóre grafu, rovnost grafů, isomorfismus grafů, matice sousednosti, Laplaceova matice sousednosti, matice incidence, sled v grafu, cesta v grafu, souvislost grafu, komponenta grafu, metrika grafu, vzdálenost vrcholů, Dijkstrův algoritmus, podgraf, indukovaný podgraf, faktor grafu, strom, kostra grafu, minimální kostra grafu, Kruskalův algoritmus, eulerovský graf.

Úvodní část této kapitoly je věnována definici základních pojmů teorie grafů (např. graf, vrchol grafu, hrana grafu, stupeň vrcholu, skóre grafu) a některým významným typům grafů. Další výklad je postupně zaměřen na způsoby reprezentace grafu, vysvětlení pojmů isomorfismus grafů a souvislost grafu, klasifikaci podgrafů daného grafu, základní vlastnosti stromů a konečně eulerovské a hamiltonovské grafy. Zvláštní pozornost se přitom věnuje vybraným grafickým algoritmům (např. Dijkstrovu algoritmu pro nalezení nejkratší cesty v grafu nebo algoritmu pro nalezení minimální kostry grafu). Při výkladu budeme vycházet především z monografie [15], některé příklady jsou převzaty z monografie [17].

5.1 Pojem grafu

Graf je jedním ze základních pojmů diskrétní matematiky. Představuje matematickou abstrakci celé řady schémat, v nichž se vyskytují nějaké (zpravidla konečné) množiny bodů a spojnice mezi vybranými dvojicemi bodů. Typickým příkladem jsou dopravní sítě nebo tzv. síťové grafy.

Graf

Definice 5.1.1. **Graf** *G* je uspořádaná dvojice (V,E), kde *V* představuje nějakou neprázdnou množinu a *E* množinu dvouprvkových podmnožin množiny *V*. Prvky množiny *V* se nazývají **vrcholy** (**uzly**) grafu G prvky množiny *E* **hrany** grafu *G*.

Vrchol grafu
Hrana grafu

Grafy se zakreslují do roviny, přičemž vrcholům odpovídají body (zpravidla „puntíky“) a hranám spojnice mezi příslušnými dvojicemi bodů (úsečky nebo oblouky). Zpravidla se požaduje, aby se spojnice nekřížily.

Při studiu grafů jsou užitečné některé binární relace.

1. Relace sousednosti $\alpha \subseteq V \times V$; dvojice vrcholů $\{a,b\} \in \alpha$, resp. uspořádaná dvojice vrcholů $(a,b) \in \alpha$, (tj. vrchol *a* sousedí s vrcholem *b*), právě když existuje hrana spojující vrcholy *a* a *b*.

2. Relace incidence $i \subseteq E \times V$; uspořádaná dvojice $(e,v) \in i$, právě když vrchol *v* leží na hraně *e* (vrchol *v* je incidentní s hranou *e*).

Násobnost hrany

Orientace hrany

Ohodnocení hran nebo vrcholů

Pro jednoduchost nebudeme uvažovat **smyčky**, tj. hrany spojující daný vrchol se sebou samým. Počet hran spojujících dané dva vrcholy grafu se nazývá **násobnost hrany**. Podle toho, zda záleží nebo nezáleží na orientaci hrany, tj. ne tom, který z vrcholů je počáteční a který koncový, se rozlišují **hrany orientované** a **hrany neorientované**. Každé hraně grafu (vrcholu grafu) může být přiřazeno ohodnocení, tj. zobrazení $o_E : E \to \mathbb{R}$ ($o_V : V \to \mathbb{R}$), jež každé hraně (vrcholu) přiřazuje nějaké (zpravidla nezáporné) reálné číslo. Taková hrana (vrchol) se nazývá **hranově ohodnocená (vrcholově ohodnocený)**.

Grafy je možno klasifikovat podle různých hledisek.
Podle počtu vrcholů rozeznáváme:

a) **konečné grafy**, které obsahují konečný počet vrcholů,

b) **nekonečné grafy**, které mají nekonečný počet vrcholů.

Podle četnosti hran se rozlišují:

c) **prosté grafy**, které obsahují pouze hrany s násobností rovnou 1,

d) **multigrafy**, které obsahují aspoň jednu hranu s násobností větší než 1.

Podle orientace hran rozlišujeme:

a) **orientované grafy**, které obsahují pouze orientované hrany, tj. uspořádané dvojice vrcholů $(a,b) \subseteq V \times V$,

b) **neorientované grafy**, které obsahují pouze neorientované hrany, tj. dvouprvkové podmnožiny $\{a,b\} \subseteq \binom{V}{2}$.

Podle ohodnocení hran můžeme klasifikovat grafy na:

a) **hranově ohodnocené grafy**, jež obsahují pouze ohodnocené hrany,
b) **vrcholově ohodnocené grafy**, jež obsahují pouze ohodnocené vrcholy,
c) **neohodnocené grafy**, v nichž neexistují ani ohodnocené hrany, ani ohodnocené vrcholy.

Podle toho, zda lze graf zakreslit do roviny bez křížení jeho hran, rozeznáváme:

a) **rovinné** (planární) **grafy**,
b) **nerovinné grafy.**

Poznámka. Klasifikaci grafů podle jiných hledisek (např. podle souvislosti grafu) uvedeme později.

Zavedeme několik významných typů grafu (viz [15]), jež se často vyskytují v teorii grafů a pro něž existuje jednotné označení i terminologie.

Úplný graf K_n na n vrcholech $(n \geq 1)$. Pro tento typ grafu platí: $V = \{1, 2, \ldots, n\}$ a $E = \binom{V}{2}$, tj. množina hran E je množina všech dvouprvkových podmnožin množiny vrcholů V. Úplný graf K_n obsahuje tedy maximálně možný počet hran. Úplný graf

Kružnice C_n **na** n vrcholech $(n \geq 3)$. V tomto případě platí: $V = \{1, 2, \ldots, n\}$ a $E = \{\{i, i+1\}, i = 1, \ldots, n-1\} \cup \{\{1, n\}\}$. Kružnice je tedy graf, v němž je každý vrchol spojen hranou se svým následovníkem a poslední n-tý vrchol s vrcholem prvním. Pokud jsou hrany znázorněny úsečkami, představuje kružnice C_n uzavřený n-úhelník. Kružnice

Cesta P_n s n vrcholy $(n \geq 0)$. Pro tento typ grafu platí: $V = \{1, 2, \ldots, n\}$ a $E = \{\{i-1, i\}, i = 1, \ldots, n\}$. Cesta tedy představuje graf, v němž je každý vrchol spojen hranou se svým následovníkem. Pokud jsou hrany znázorněny úsečkami, představuje cesta P_n neuzavřenou „lomenou“ čáru tvořenou n úsečkami. Cesta

Úplný bipartitní graf

Úplný bipartitní graf $K_{m,n}$ s $(m+n)$ vrcholy $(m \geq 1, n \geq 1)$. Pak $V = \{u_1, \ ..., u_m\} \cup \{v_1, \ ..., v_n\}$, $E = \{\{u_i, v_j\}; i = 1, \ ..., m, j = 1, \ ..., n\}$. Množina vrcholů bipartitního grafu sestává ze dvou disjunktních množin V_1 a V_2, přitom každý vrchol z V_1 je spojen s hranou s každým vrcholem z V_2.

Úkoly. Znázorněte:

a) úplný graf K_n pro $n = 1, 3, 4, 5$ a 6,

b) kružnici C_n pro $n = 3, 4, 5$ a 6,

c) cestu P_n pro $n = 3, 5, 6$ a 8,

d) úplný bipartitní graf $K_{m,n}$ pro následující dvojice přirozených čísel *m* a *n*: $(1,1), (1,2), (1,3), (2,3)$ a $(3,3)$.

Stupeň vrcholu

Definice 5.1.2. Nechť $G = (V, E)$ je neorientovaný graf a *v* jeho vrchol. Pak počet hran grafu *G* obsahujících vrchol *v* se nazývá **stupeň vrcholu *v* v grafu *G*** a označuje $d_G(v)$.

Poznámky.

1. V orientovaném grafu se rozlišuji výstupní stupeň vrcholu ($d_G^+(v)$) a vstupní stupeň vrcholu ($d_G^-(v)$), které označují počet hran vystupujících z vrcholu *v*, resp. vstupujících do tohoto vrcholu. Celkový stupeň daného vrcholu je součtem jeho výstupního a vstupního stupně.
2. Izolovaný bod v grafu má přirozeně stupeň 0.

Úkol. Určete stupně všech vrcholů v grafech z předcházejícího úkolu.

Pro nově zavedený pojem stupeň grafu platí velmi důležité věty.

Věta 5.1.1. Nechť $G = (V, E)$ je libovolný graf. Pak součet stupňů všech jeho vrcholů je roven dvojnásobku počtu jeho hran, tj. $\sum_{v \in V} d_G(v) = 2|E|$.

Důkaz této věty (tzv. principu sudosti) je triviální. Stupeň vrcholu *v* je roven počtu hran obsahujících vrchol *v*. Každá hrana však obsahuje právě dva vrcholy. Jestliže sečteme všechny stupně, dostaneme dvojnásobek počtu hran. □

Úkol. Dokažte větu 5.1.1 matematickou indukcí podle počtu hran.

Věta 5.1.2. Nechť $G=(V,E)$ je libovolný konečný graf. Pak počet vrcholů lichého stupně je vždy číslo sudé.

Důkaz vyplývá přímo z věty 5.1.1.

S pojmem stupně vrcholu úzce souvisí pojem skóre grafu.

Skóre grafu

Definice 5.1.3. Nechť $G=(V,E)$ je graf a $v_1,v_2,\ ...,v_n$ jeho vrcholy v nějakém libovolně zvoleném pořadí. Pak posloupnost $d_G(v_1),d_G(v_2),\ ...,d_G(v_n)$ se nazývá **skóre grafu *G***.

Poznámka. Skóre nezávisí na zvoleném pořadí vrcholů. Dvě skóre jsou tedy stejná, jestliže jedno z nich můžeme získat z druhého pouze změnou pořadí čísel.

Grafová posloupnost

Definice 5.1.4. Posloupnost přirozených čísel $(d_1,d_2,\ ...,d_n)$ se nazývá **grafová**, když existuje graf s n vrcholy takový, že stupně jeho vrcholů se rovnají právě těmto číslům.

Každá posloupnost přirozených čísel není samozřejmě grafová. Např. posloupnosti $(1,2)$ nebo $(1,3)$ nejsou zcela jistě grafové. Pří rozhodování, zda je daná posloupnost grafové či nikoliv, se používá následující věta.

Věta 5.1.3 (věta o skóre). Nechť $(d_1,d_2,\ ...,d_n)$ je nějaká neklesající posloupnost přirozených čísel. Pak je tato posloupnost grafová (skórem nějakého grafu) právě tehdy, když je grafová také posloupnost $\left(d_1,d_2,\ ..,d_{n-d_n-1},d_{n-d_n}-1,\ ...,d_{n-1}-1\right)$.

Důkaz je poněkud zdlouhavý. Naleznete jej v monografii [15].

Někteří autoři (např. [8]) formulují právě uvedenou větu v modifikovaném (ovšem ekvivalentním) tvaru.

Věta 5.1.4 (věta o skóre). Nechť $(d_1,d_2,\ ...,d_n)$ je nějaká nerostoucí posloupnost přirozených čísel, kde $n\geq 2$ a $1\leq d_1\leq n-1$. Pak je tato posloupnost grafová (skórem nějakého grafu), právě když je grafová také posloupnost $\left(d_2-1,d_3-1,\ ...,d_{d_1+1},d_{d_1+2},\ ...,d_n\right)$.

Obě věty o skóre představují relativně jednoduchý algoritmus, jenž umožňuje rychle rozhodnout, zda je či není daná posloupnost posloupností grafickou.

Příklad 5.1.1 (viz [15]) . Dokážeme, že posloupnost $(1,1,1,2,2,3,4,5,5)$ je grafová. Opakovanou aplikací věty 5.1.3 dostaneme postupně posloupnosti:

1. $(1,1,1,1,1,1,2,3,4)$,

2. $(1,1,1,0,0,1,2)$, po přerovnání $(0,0,1,1,1,1,2)$,

3. $(0,0,1,1,0,0)$, po přerovnání $(0,0,0,0,1,1)$,

4. $(0,0,0,0,0)$.

Posloupnost $(0,0,0,0,0)$ je grafová (skóre grafu s pěti izolovanými vrcholy), proto také posloupnost $(1,1,1,2,2,3,4,5,5)$ je posloupností grafovou.

Příklad 5.1.2. Vyřešíme příklad 5.1,1 pomocí věty 5.1.4. Nejprve přerovnáme čísla $1,1,1,2,2,3,4,5,5$ do nerostoucí posloupnosti $(5,5,4,3,2,2,1,1,1)$. Pak opakovaným použitím věty 5.1.4 dostaneme:

1. $(4,3,2,1,1,1,1,1)$,

2. $(2,1,0,0,1,1,1)$, po přerovnání $(2,1,1,1,1,0,0)$,

3. $(0,0,1,1,0,0)$, po přerovnání $(1,1,0,0,0,0)$,

4. $(0,0,0,0,0)$.

Dostali jsme samozřejmě stejný výsledek jako v příkladu 5.1.1.

Úkol. Rozhodněte, zda jsou následující posloupnosti grafové:

a) $(4,4,4,4,3,3,2)$,

b) $(5,5,5,5,5,4,4,3)$,

c) $(6,6,6,6,5,4,3)$.

5.2 Isomorfismus grafů

Začneme definicí jednoduchého pojmu rovnost dvou grafů.

Rovnost grafů

Definice 5.2.1. Dva grafy $G=(V,E)$ a $G'=(V',E')$ jsou **stejné** (**identické**), právě když mají identické množiny vrcholů i hran, tj. jestliže platí: $V=V'$ a $E=E'$. Rovnost grafů v tomto smyslu se značí $G=G'$.

Některé grafy se však liší pouze označením svých vrcholů a hran. Tuto skutečnost vystihuje pojem isomorfismus grafů.

Isomorfismus grafů

Definice 5.2.2. Dva grafy $G=(V,E)$ a $G'=(V',E')$ jsou **isomorfní**, jestliže existuje bijektivní zobrazení $F:V\to V'$ takové, že platí:

$\{a,b\}\in E,$ právě když $\{F(a),F(b)\}\in E'$ pro neorientované grafy, resp.

$(a,b)\in E,$ právě když $(F(a),F(b))\in E'$ pro orientované grafy.

Takové zobrazení F se nazývá **isomorfismus grafů** G a G' a označuje zápisem $G \cong G'$.

Poznámky.

1. V případě neorientovaných grafů se hrany považují za dvouprvkové podmnožiny vrcholů, v případě orientovaných grafů za uspořádané dvojice vrcholů.
2. Isomorfismus grafů je speciálním případem homomorfismu (viz např. [8]).

Úkol. Dokažte, že relace „být isomorfním“ je na nějaké množině grafů $\mathcal{G}$ ekvivalence.

Příklad 5.2.1. Najdeme isomorfismus neorientovaných grafů G a G' znázorněných na obrázku 5.1. Oba grafy mají stejný počet vrcholů, počet hran i stejné skóre. Použijeme např. bijektivní zobrazení F takové, že

$$F(1)=a,\ F(2)=d,\ F(3)=b,\ F(4)=e,\ F(5)=c,\ F(6)=f.$$

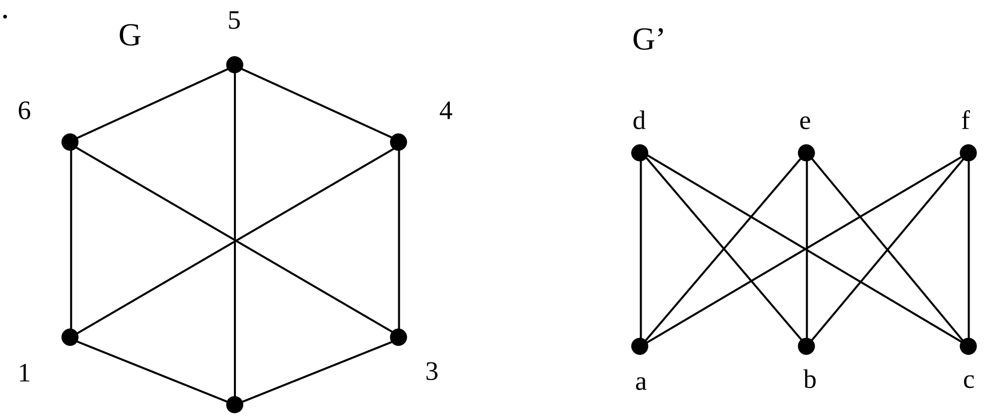
Zobrazení F představuje také bijektivní zobrazení hran grafu G na hrany grafu G'. Vzhledem k tomu, že oba grafy jsou neorientované, můžeme psát:

$\{F(1),F(2)\}=\{a,d\},\ \{F(1),F(4)\}=\{a,e\},\ \{F(1),F(6)\}=\{a,f\},$

$\{F(2)F(3)\}=\{b,d\},\ \{F(2),F(5)\}=\{c,d\},\ \{F(3),F(4)\}=\{b,e\},$

$\{F(3),F(6)\}=\{b,f\},\ \{F(4),F(5)\}=\{c,e\},\ \{F(5),F(6)\}=\{c,f\}.$

Na závěr můžeme říci, že G a G' jsou isomorfní úplné bipartitní grafy $K_{3,3}$..



Obr. 5.1. Neorientované grafy G a G' k příkladu 5.2.1.

Úkol. Příklad 5.2.1 má více řešení. Nalezněte nějaký jiný isomorfismus grafů G a G' na obrázku 5.1.

Poznámka. Úloha rozhodnout, zda dva grafy jsou či nejsou isomorfní, je v obecném případě obtížná. Podle [15] dosud neexistuje pro takové rozhodování efektivní algoritmus, tj. algoritmus použitelný ve všech případech.

Celkový počet prostých grafů bez smyček na *n*-prvkové množině vrcholů *V* je $2^{\binom{n}{2}}$. Důkaz tohoto tvrzení je jednoduchý. Maximální počet hran takového grafu se rovná počtu dvouprvkových podmnožin *n*-prvkové množiny, tedy $\binom{n}{2}$. Pro každou hranu existují právě dvě možnosti: buď se v grafu skutečně vyskytuje nebo nikoliv. Na základě kombinatorického principu součinu je proto celkový počet grafů $2^{\binom{n}{2}}$. Mezi těmito grafy jsou určitě grafy, které nejsou navzájem isomorfní. Počet neisomorfním grafů na *n* vrcholech lze odhadnout následující úvahou.

1. Takových grafů nemůže být více než $2^{\binom{n}{2}}$.
2. Uvažme jeden určitý graf *G* na množině *n* vrcholů. Určíme počet grafů G', které jsou s grafem *G* isomorfní. Je-li G' takový isomorfní graf, pak podle definice 5.2.2 existuje bijektivní zobrazení $F : V \to V$, které je isomorfismem G a G'**.** Takových bijekcí je podle věty 2.1.3 právě $n!$. Odtud dostaneme, že graf *G* je isomorfní nejvýše s $n!$ grafy na množině *V*, a proto existuje nejméně $2^{\binom{n}{2}} / n!$ navzájem neisomorfních grafů na *n* vrcholech.

5.3 Reprezentace grafu

Grafy můžeme reprezentovat různými prostředky. V podstatě rozlišujeme dva základní způsoby reprezentace grafů:

a) grafická reprezentace (znázornění grafu v rovině),
b) algebraická reprezentace.

Dále se budeme zabývat jen algebraickými formami reprezentace konečných prostých grafů bez smyček.

Nejjednodušším způsobem algebraické reprezentace je prostý **seznam vrcholů a hran**. Takový seznam se zpravidla zadává ve tvaru množiny $\{|V|, |E|, e_1, e_2, \ldots, e_i, \ldots\}$, kde $e_i \in E$, $i \in \mathbb{N}$. Tento způsob reprezentace obsahuje celkem $2|E| + 2$ údaje.

Pro informatiky je důležité vědět, jak se grafy reprezentují v paměti počítače. Předpokládejme, že je dán graf, který má právě *n* vrcholů. V takovém případě se jeho vrcholy uspořádají do pole velikosti *n* a do *i*-tého prvku tohoto pole se vloží ukazatel (pointer) na spojový seznam vrcholů, jež s vrcholem *i* sousedí. Graf se tedy reprezentuje **seznamem sousedů pro každý z vrcholů**.

V praxi se grafy nejčastěji reprezentují pomocí matic. Nejvýznamnější a také nejčastěji používanou formou maticové reprezentace je matice sousednosti.

Definice 5.3.1. Nechť $G=(V,E)$ je graf s n vrcholy: $v_1, v_2, ..., v_n$ v nějakém libovolném pořadí. Pak matice $A_G=\left(a_{ij}\right)_{i,j=1}^{n}$ definovaná předpisem

$$a_{ij}=\begin{cases}1 \text{ pro } \{v_i,v_j\}\in E\\ 0 \qquad\qquad \text{jinak}\end{cases}$$

Matice sousednosti grafu

se nazývá **matice sousednosti grafu G**.

Matice A_G je symetrická čtvercová matice (typu $n\times n$) s prvky 0 a 1; na hlavní diagonále jsou přitom samé 0. Souvisí s dříve zavedenou relací sousednosti. Je definována pro neorientované i orientované grafy a závisí přirozeně na zvoleném očíslování vrcholů grafu. Každá matice s uvedenými vlastnostmi je maticí sousednosti nějakého grafu. Vedle takto zavedené matice sousednosti A_G se někdy používá i jiných matic sousednosti: **znaménkové matice sousednosti** $Z_G=\left(z_{ij}\right)_{i,j=1}^{n}$, pro jejíž prvky platí:

$$z_{ij}=\begin{cases}+ \text{ pro } \{v_i,v_j\}\in E\\ - \text{ pro } \{v_i,v_j\}\notin E\,,\\ 0 \qquad\quad \text{pro } i=j\end{cases}$$

Lapcaceova matice sousednosti

a také **Laplaceovy matice souvislosti** $L_G=\left(l_{ij}\right)_{i,j=1}^{n}$ definované předpisem

$$l_{ij}=\begin{cases}-1 \quad \text{pro } \{v_i,v_j\}\in E\\ \;\;0 \quad\; \text{pro } \{v_i,v_j\}\notin E\,.\\ d_G(v_i) \quad \text{pro } i=j\end{cases}$$

Obě modifikované matice souslednosti jsou také kvadratické (typu $n\times n$) a použitelné pro neorientované i orientované grafy, ale nejsou symetrické.

Další velmi významnou reprezentací neorientovaného grafu $G=(V,E)$ je matice incidence.

Definice 5.3.2. Nechť $G=(V,E)$ je neorientovaný graf s n vrcholy a m hranami. Pak matice $I_G=\left(a_{ij}\right)_{i=1,j=1}^{m,n}$ definovaná předpisem

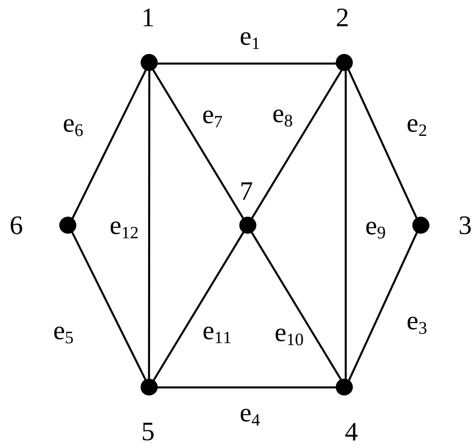
$$a_{ij}=\begin{cases}1, \text{ jestliže } v_j \in e_i,\\ 0 \text{ jinak.}\end{cases}$$

Matice incidence

se nazývá **matice incidence grafu G**.

Poznámka. Ve výše uvedené definici platí $a_{ij}=1$, právě když vrchol v_j je incidentní s hranou e_i.

Matice incidence je obdélníkové matice typu $m \times n$. Každý její řádek obsahuje právě dvě 1, protože libovolná hrana spojuje dva vrcholy.



Obr. 5.2. Graf k příkladu 5.3.1.

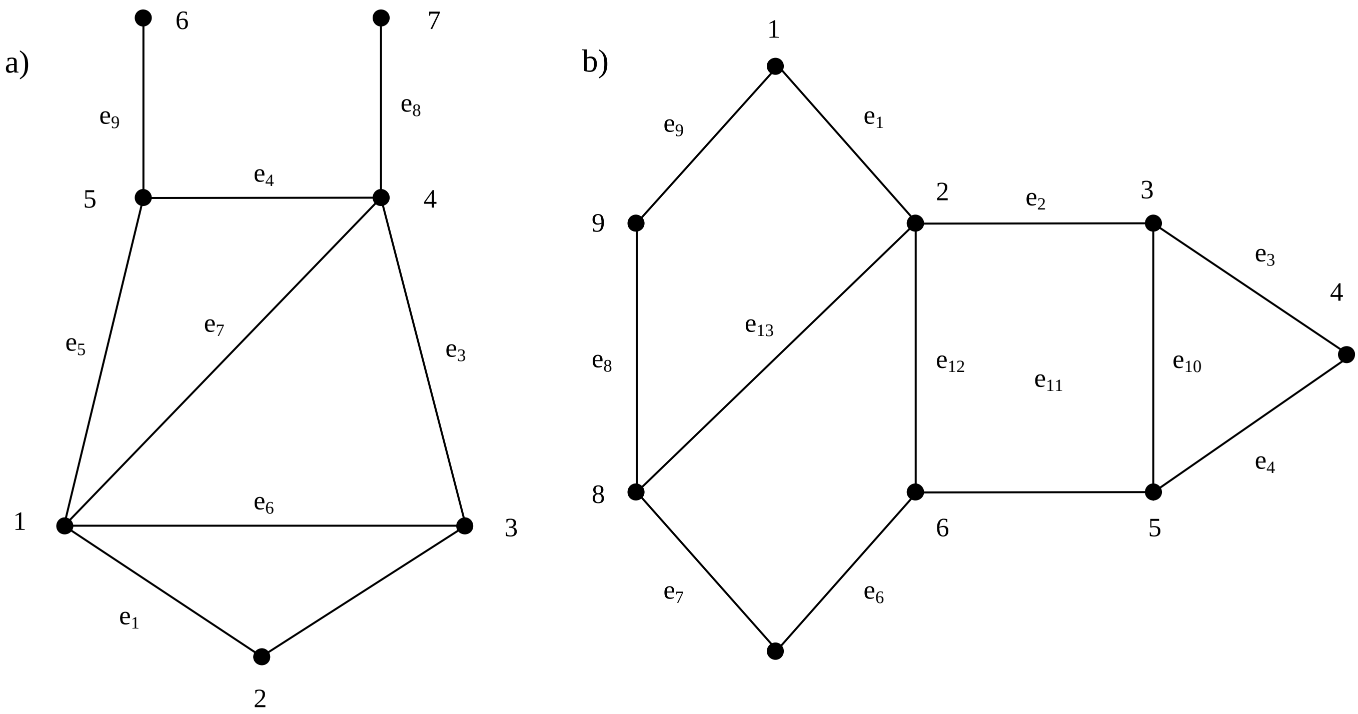
Příklad 5.3.1. Pro ilustraci vytvoříme matici sousednosti, Laplaceovu matici sousednosti a matici incidence pro neorientovaný graf na obrázku 5.2.

$$A_G=\begin{pmatrix}0&1&0&0&1&1&1\\1&0&1&1&0&0&1\\0&1&0&1&0&0&0\\0&1&1&0&1&0&1\\1&0&0&1&0&1&1\\1&0&0&0&1&0&0\\1&1&0&1&1&0&0\end{pmatrix},$$

$$L_G = \begin{pmatrix} 4 & -1 & 0 & 0 & -1 & -1 & -1 \\ -1 & 4 & -1 & -1 & 0 & 0 & -1 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 4 & -1 & 0 & -1 \\ -1 & 0 & 0 & -1 & 4 & -1 & -1 \\ -1 & 0 & 0 & 0 & -1 & 2 & 0 \\ -1 & -1 & 0 & -1 & -1 & 0 & 4 \end{pmatrix},$$

$$I_G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Úkol. Vytvořte matice A_G, L_G a I_G pro grafy znázorněné na obrázku 5.3a a 5.3b.



Obr. 5.3

5. 4 Souvislost grafu

Nejprve definujeme základní pojmy sled a cesta v grafu.

Sled grafu

Definice 5.4.1. Nechť $G=(V,E)$ je nějaký graf. Pak posloupnost $(v_0,e_1,v_1,e_2,\ ...,\ e_n,v_n)$, pro níž platí $e_i=\{v_{i-1},v_i\}\in E,\ i=1,2,...,\ n,$ se nazývá **sled z vrcholu** v_0 **do vrcholu** v_n **v grafu *G***. Vrchol v_0 **(**v_n**)** se nazývá **počáteční** (**koncový**) **vrchol sledu** a číslo $n\in\mathbb{N}$ **délka sledu**.

Ve sledu se mohou některé vrcholy i hrany opakovat. Jestliže existuje v grafu *G* sled z vrcholu v_0 do vrcholu v_n, pak v něm také existuje sled z vrcholu v_n do vrcholu v_0 definovaný posloupností $(v_n,e_n,v_{n-1},\ ...,\ v_1,e_1,v_0)$.

Úkol. Existuje-li v grafu *G* sled délky *n* sled z vrcholu v_0 do vrcholu v_n, pak je možno tento sled prodloužit tak, že vznikne nový sled délky $n+2$. Dokažte.

Cesta v grafu

Definice 5.4.2. Nechť $G=(V,E)$ je nějaký graf. Pak posloupnost $(v_0,e_1,v_1,e_2,\ ...,\ e_n,v_n)$, kde $v_0,v_1,\ ...,\ v_n$ jsou vzájemně různé vrcholy grafu *G* a pro každé $i=1,2,...,\ n$ platí $e_i=\{v_{i-1},v_i\}\in E$, se nazývá **cesta z vrcholu** v_0 **do vrcholu** v_n **v grafu *G*.** Vrchol v_0 **(**v_n**)** se nazývá **počáteční** (**koncový**) **vrchol cesty** a číslo $n\in\mathbb{N}$ **délka cesty**.

V případě cesty (na rozdíl od sledu) se nemohou vrcholy ani hrany opakovat. Souvislost mezi sledem a cestou vystihuje následující věta.

Věta 5.4.1. V grafu G existuje cesta z vrcholu v_0 do vrcholu v_n právě tehdy, když v něm existuje sled z vrcholu v_0 do vrcholu v_n.

Důkaz. Každá cesta představuje v daném grafu sled. Naopak, každý sled mezi dvěma danými vrcholy, který má nejmenší možnou délku, je cesta. □

Nyní přistoupíme k definici souvislosti grafu.

Souvislost grafu

Definice 5.4.3. Neorientovaný graf $G=(V,E)$ je **souvislý**, jestliže pro každé dva jeho vrcholy x a y existuje cesta z vrcholu *x* do vrcholu *y*.

Poznámky.

1. Na základě definice 5.4.3 můžeme zavést klasifikaci grafů podle souvislosti na souvislé a nesouvislé.

2. Na množině vrcholů V grafu $G=(V,E)$ můžeme zavést speciální relaci „~“ vztahem $x \sim y$, právě když v grafu G existuje cesta z vrcholu x do vrcholu y.
3. V případě orientovaného grafu je situace složitější (viz např. [8]).

Úkol. Dokažte, že relace „~“ je na množině vrcholů V grafu $G=(V,E)$ ekvivalence.

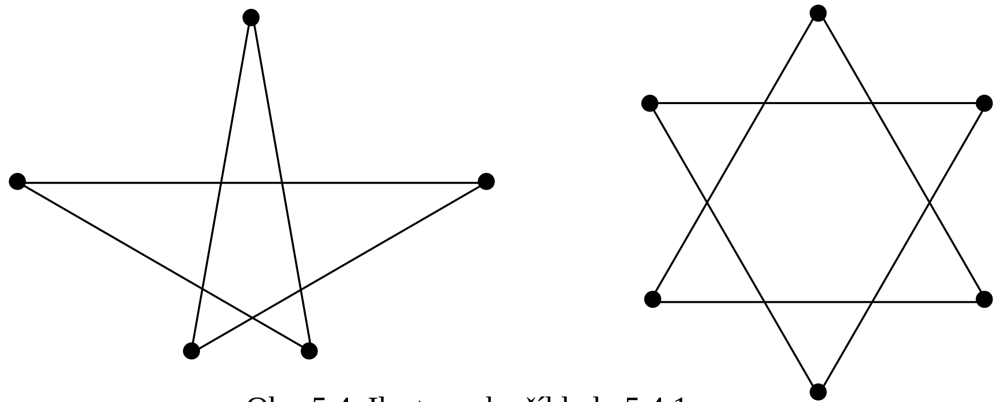
S pojmem souvislosti grafu úzce souvisí pojem komponenta grafu.

Komponenta grafu

Definice 5.4.4. Nechť $G=(V,E)$ je neorientovaný graf a $V=V_1 \cup V_2 \cup \ldots \cup V_k$ rozklad množiny vrcholů V na třídy ekvivalence „□ “ (navzájem disjunktní množiny ekvivalentních vrcholů). Pak množiny $V_i,\ i=1,2,\ldots,k,$ se nazývají **komponenty grafu** G. Graf G je tedy sjednocením svých komponent $V_i,\ i=1,2,\ldots,k$.

Pomocí zavedeného pojmu komponenta grafu lze definovat souvislost grafu takto: graf G je souvislý, právě když pro počet jeho komponent platí $k=1$.

Příklad 5.4.1. Pro ilustraci nově zavedených pojmů uvádíme na obrázku 5.4 dva neorientované grafy G_1 a G_2. První z nich je zřejmě souvislý, kdežto druhý nesouvislý, tvořený dvěma komponentami.



Obr. 5.4. Ilustrace k příkladu 5.4.1.

V celé řadě aplikací je třeba určovat vzdálenosti vrcholů v daném grafu.

Vzdálenost vrcholů

Definice 5.4. Nechť $G=(V,E)$ je souvislý graf. Pak číslo $\rho_G(x,y)$ udávající délku nejkratší cesty z vrcholu x do vrcholu y v grafu G se nazývá **vzdálenost vrcholů *x* a *y* v grafu *G***.

V případě neohodnocených grafů se měří délka cesty počtem hran této cesty, zatímco u hranově ohodnocených grafů je délka cesty rovna součtu ohodnocení všech hran uvažované cesty.

Metrika grafu

Zobrazení $\rho_G : V \times V \to \mathbb{R}$ (tzv. **metrika grafu**) má samozřejmě obecné vlastnosti metriky:

1. $\rho_G(x,y) \geq 0$ a $\rho_G(x,y) = 0,$ právě když $x = y$,
2. pro každou dvojici $x, y \in V$ platí $\rho_G(x,y) = \rho_G(y,x)$ (vlastnost symetrie),
3. pro každou trojici $x, y, z \in V$ platí $\rho_G(x,z) \leq \rho_G(x,y) + \rho_G(y,z)$ (tzv. trojúhelníková nerovnost).

V případě hranově neohodnocených grafů má zobrazení ρ_G navíc ještě speciální vlastnosti:

4. pro každou dvojici $x, y \in V$ je $\rho_G(x,y)$ je nezáporné celé číslo,
5. je-li $\rho_G(x,z) > 1,$ pak existuje vrchol $y,\ x \neq y \neq z$, takový, že $\rho_G(x,y) + \rho_G(y,z) = \rho_G(x,z).$

Na závěr této části uvedeme nejznámější algoritmus pro určení nejkratší cesty ze zvoleného počátečního vrcholu do všech ostatních vrcholů grafu, tzv. Dijkstrův algoritmus. Budeme přitom vycházet z předpokladu, že daný graf $G = (V, E)$ má všechny hrany ohodnocené kladnými reálnými čísly, tj. existuje zobrazení $w : E \to (0, \infty)$, které každé hraně $e \in E$ přiřazuje její ohodnocení $w(e).$ Popis algoritmu včetně značení proměnných je převzat z monografie [15].

Dijkstrův algoritmus

Popis Dijkstrova algoritmu

Vstupy: graf $G = (V, E)$ daný seznamem sousedů každého z vrcholů $v \in V,$ ohodnocení $w(e)$ všech hran $e \in E$ a počáteční (startovní) vrchol s.

Proměnné:

- $d(v), v \in V$ - reálné proměnné udávající aktuální vzdálenosti vrcholu v od počátečního vrcholu s (při započtení ohodnocení jednotlivých hran),
- δ – reálné číslo,
- $A \subseteq V$ - množina tzv. aktivních vrcholů, tj. vrcholů, pro které ještě nebyla hodnota $d(v)$ definitivně určena,
- $N \subseteq V$ - množina vrcholů, pro něž je hodnota $d(v)$ nejmenší možná mezi všemi vrcholy $v \in A$.

Výstup: definitivní hodnoty $d(v)$ pro všechny vrcholy $v \in V$.

1. krok (inicializace proměnných)

$d(s) := 0$; $d(v) := \infty$ pro $x \in V \setminus \{s\}$; $A := V$

2. krok (podmínka pro ukončení výpočtu)

Jestliže pro všechna $x \in A$ platí $d(x) = \infty$, algoritmus končí, jinak pokračuje 3. krokem. Algoritmus končí jednak v případě, kdy $A = \emptyset$, jednak v případě, kdy množina *A* obsahuje pouze vrcholy nedosažitelné cestou z počátečního vrcholu *s*.

3. krok (výběr množiny *N* a aktualizace množiny *A*)

$\delta := \min\{d(y); y \in A\}$

$N := \{v \in A; d(v) = \delta\}$

$A := A \setminus N$

4. krok (aktualizace hodnot $d(v)$ pro sousedy vrcholů z množiny *N*)

Pro každou hranu $e = \{v, y\}, v \in N$ a $y \in A$ se provede příkaz

$d(y) := \min\{d(y), d(v) + w(e).\}$

Po vyčerpání všech takových hran e se pokračuje 2.krokem.

Poznámky.

1. Dijkstrův algoritmus je použitelný i pro orientované grafy.
2. Při programování se symbol ∞ nahrazuje nějakým číslem s hodnotou zaručeně vyšší než je délka nejdelší cesty v uvažovaném grafu.
3. Správnost Dijkstrova algoritmu je dokázána např. v monografii [15].

Úkol. Zkuste naprogramovat v jazyku, který znáte (např. v Pascalu) Dijkstrův algoritmus a ověřte jeho správnost na nějakém jednoduchém neorientovaném grafu.

5.5 Podgrafy

Nejprve zavedeme základní pojmy podgraf a indukovaný podgraf.

Podgraf

Definice 5.5.1. Graf *H* je **pografem** grafu *G*, jestliže $V(H) \subseteq V(G)$ a $E(H) \subseteq E(G)$.

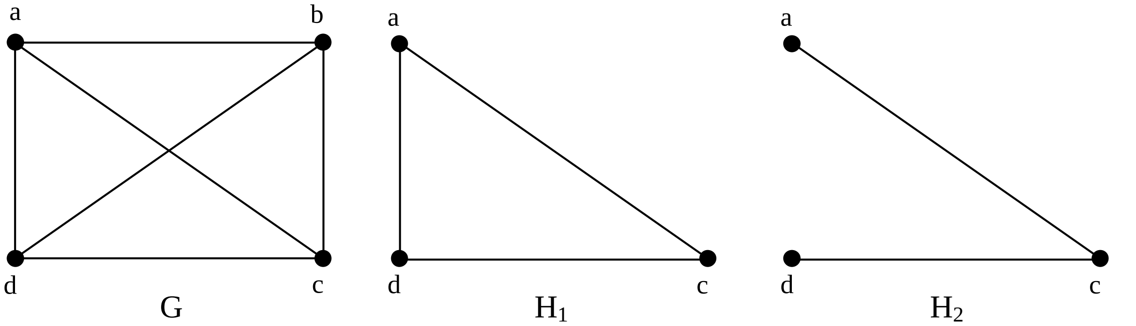
Indukovaný podgraf

Definice 5.5.2. Graf *H* je **indukovaným pografem** grafu *G*, jestliže $V(H) \subseteq V(G)$ a $E(H) = E(G) \cap \binom{|V(H)|}{2}$.

Poznámka. Symboly $V(G)$ a $V(H)$ označují v tomto pořadí množiny vrcholů grafů *G* a *H*.

Indukovaný podgraf grafu *G* vytvoříme tak, že z grafu G odstraníme některé vrcholy a všechny takové hrany, jež obsahují odstraněné vrcholy. V případě podgrafu můžeme z grafu *G* navíc odstranit některé další hrany, i když neodstraníme žádny z jejich koncových vrcholů.

Příklad 5.5.1. Souvislosti mezi grafem, podgrafem a indukovaným podgrafem ukážeme ne jednoduchém příkladu (viz obr. 5.5).



Obr. 5.5. Ilustrace k příkladu 5.5.

Výchozí graf G má čtyři vrcholy a,b,c,d a šest hran $\{a,b\},\{a,c\},\{a,d\}$, $\{b,c\},\{b,d\},\{c,d\}$. Graf H_1 je podle definice 5.5.2 indukovaným podgrafem grafu *G*; vznikl z grafu *G* odstraněním vrcholu *b* a hran $\{a,b\},\{b,c\}$ a $\{c,d\}$. Naproti tomu graf H_2 je podle definice 5.5.1 podgrafem grafu *G*; byl vytvořen z grafu H_1 odstraněním hrany $\{a,d\}$, aniž by byly odstraněny vrcholy *a* a *d*.

Příkladem podgrafu jsou již dříve zavedené grafy cesta a kružnice. Podgraf nějakého grafu *G*, který je isomorfní s cestou P_n**,** se nazývá **cesta v grafu *G* délky *n***. Podobně podgraf isomorfní s kružnicí C_n se nazývá **kružnice v grafu *G* délky *n***.

Zvláštní význam mají podgrafy mající stejnou množinu vrcholů jako výchozí graf.

Faktor grafu

Definice 5.5.3. Podgraf H grafu G takový, že $V(H)=V(G)$ a $E(H)\subseteq E(G)$ se nazývá **faktorem grafu G**. Speciálně, každý graf je svým vlastním faktorem.

Příklad 5.5.2. Určíme počet různých faktorů grafu G na obrázku 5.5. Zmíněný graf má právě šest hran. Faktory vznikají z výchozího grafu tak, že z něj odstraňujeme hrany. Pro každou hranu máme právě dvě možnosti:

buď ji odstraníme nebo neodstraníme. Proto (na základě kombinatorického principu součinu) existuje právě $2^6 = 64$ různých faktorů grafu *G*.

Úkol. Kolik faktorů má úplný graf K_n na *n* vrcholech $(n \geq 2)$? Návod: určete nejprve počet hran uvažovaného grafu.

Jedním z nejběžnějších útvarů v přírodě i matematice jsou objekty se stromovou strukturou. Pomocí stromů lze popsat např. rodokmeny, elektrické rozvody, hierarchické struktury v řízení apod. Stromy jsou také významným typem podgrafů.

Strom

Definice 5.5.5. Souvislý prostý graf, který neobsahuje žádnou kružnici, se nazývá **strom**.

Poznámka. Jakýkoliv prostý graf (ne nutně souvislý) neobsahující žádnou kružnici se nazývá **les**. Strom můžeme proto definovat jako souvislý les.

Definice stromu není příliš šikovná. Není totiž jasné, jak ověřit, že daný graf je skutečně stromem. Ověření souvislosti je úloha snadná, ale potíže vznikají při ověřování neexistence kružnice. Proto jsou velmi důležité alternativní popisy stromu.

Koncový vrchol stromu

Věta 5.5.1 (věta o koncovém bodu). Každý strom na *n* vrcholech $(n \geq 2)$ obsahuje nejméně dva vrcholy 1. stupně. Takové vrcholy se nazývají **koncové vrcholy** (**listy**).

Důkaz. Nechť $P = (v_0, e_1, v_1, \ldots, e_n, v_n)$ je cesta maximální délky v uvažovaném stromu. Dokážeme sporem, že v_0 a v_n jsou koncové vrcholy. Nechť např. vrchol v_0 není koncovým vrcholem. Pak nutně musí existovat ještě jiná hrana $e \neq e_1$ obsahující vrchol v_0. Označme ji $e = \{v_0, v\}$. Rozlišíme dvě možnosti.

a) Vrchol *v* je některým z vrcholů cesty *P* , tj. $v = v_i$, $2 \leq i \leq n-1$. V tomto případě hrana *e* spolu s úsekem cesty *P* od vrcholu v_0 do vrcholu v_i tvoří kružnici, což vede ke sporu.

b) Vrchol *v* není vrcholem cesty *P*, tj. $v \notin \{v_0, v_1, \ldots, v_n\}$. Pak bychom mohli cestu *P* prodloužit o hranu *e*, a to je opět spor s předpokladem věty. □

Poznámka. Věta 5.5.1 neplatí pro nekonečné stromy.

Pro ověřování faktu, že daný graf je strom se používá následující tvrzení.

Věta 5.5.2. Nechť G je graf a v jeho koncový vrchol. Pak G je strom, právě když $G-v$ je také strom.

Poznámka. Zápis $G-v$ označuje graf, jenž vznikne z grafu G odstraněním koncového vrcholu v a všech hran obsahujících vrchol v.

Důkaz.

a) Nechť G je strom a x, y dva jeho vrcholy různé od koncového vrcholu v. Uvažujme libovolnou cestu P z vrcholu x do vrcholu y. Tato cesta nemůže obsahovat žádný vrchol 1. stupně kromě vrcholů x a y, tedy ani vrchol v. Proto je cesta P celá obsažena v grafu $G-v$, což znamená, že graf $G-v$ je také souvislý. Jelikož graf G neobsahuje podle předpokladu žádnou kružnici, ani graf $G-v$ nemůže obsahovat kružnici. Tím je dokázáno, že graf $G-v$ je také strom.

b) Nechť $G-v$ je strom. Přidáním koncového vrcholu v zřejmě nemůže vzniknout kružnice. Zbývá tedy dokázat, že graf G je souvislý. Podle předpokladu už existuje cesta mezi libovolnými dvěma vrcholy grafu $G-v$. Cesta z libovolného vrcholu x do vrcholu v vznikne prodloužením cesty spojující vrcholy x a y o hranu $\{y, v\}$, kde y je jediný soused vrcholu v v grafu G. □

Z věty 5.5.2 vyplývá, že graf G je strom, právě když ho můžeme převést postupným odstraňováním koncových vrcholů ne jeden vrchol. Přitom můžeme v každém kroku odebrat libovolný koncový vrchol.

Charakteristiku stromů rozšíříme následujícím tvrzením.

Věta 5.5.3. Graf $G(V, E)$ je strom, právě když platí:

1. Pro každé dva vrcholy $x, y \in V$ existuje právě jediná cesta z vrcholu x do vrcholu y.
2. Graf G je souvislý, ale vynecháním libovolné hrany vznikne nesouvislý graf.
3. Graf G neobsahuje žádnou kružnici, ale každý graf vytvořený z grafu G přidáním hrany, tj. graf $G+e$, kde $e \in \binom{|V|}{2} \setminus E$, bude kružnici obsahovat.
4. Graf G je souvislý a splňuje Eulerův vztah $|V| = |E| + 1$.

Důkaz je poněkud zdlouhavý (viz [M+N]).

V praxi se často řeší úloha propojit daná místa nějakým vedením tak, aby celková délka propojení byla co nejkratší. Přitom se předpokládá, že se tato propojení (v teorii grafů tzv. síť) nebude větvit nikde mimo propojovaná místa.

Úloha nalézt takové propojení se v teorii grafů formuluje následujícím způsobem.

Je dán souvislý graf $G(V, E)$ s nezáporným ohodnocením hran $w: E \to \langle 0, \infty)$. Je třeba určit souvislý podgraf $T = (V, E^*)$ takový, aby výraz $\sum_{e \in E^*} w(e)$ nabýval minimální hodnoty. Řešením této úlohy je vždy nějaký strom. V případě kladného ohodnocení hran může být řešením jenom strom.

V souvislosti s řešením propojovacího problému se zavádí pojem kostra grafu.

Definice 5.5.3. Nechť $G(V, E)$ je graf. Pak libovolný strom (V, E^*), kde $E^* \subseteq E$, se nazývá **kostra grafu *G***.

Kostra grafu

Je zřejmé, že kostra může existovat pouze tehdy, když graf *G* je souvislý. Daný graf může mít samozřejmě více koster. Problém nalezení minimální kostry je algebraicky dobře zvládnutý.

Formulujeme precizně úlohu nalezení minimální kostry grafu a podrobně popíšeme jednoduchý Kruskalův algoritmus (tzv. hladový algoritmus) k jejímu určení.

Problém minimální kostry. Nechť $G(V, E)$ je souvislý graf s nezáporným ohodnocením hran *w*. Úkolem je nalézt kostru $T = (V, E^*)$ grafu *G* s nejmenší možnou hodnotou $\sum_{e \in E^*} w(e)$.

Minimální kostra

Kruskalův algoritmus (viz [15]).

Kruskalův algoritmus

Je dán souvislý graf $G(V, E)$ s *n* vrcholy, *m* hranami a ohodnocením *w*.

Nejprve je nutno očíslovat hrany $e_1, e_2, \ldots, e_m$ tak aby platilo $w(e_1) \le w(e_2) \le \ldots \le w(e_m)$, tj. setřídit hrany podle ohodnocení do neklesající posloupnosti.

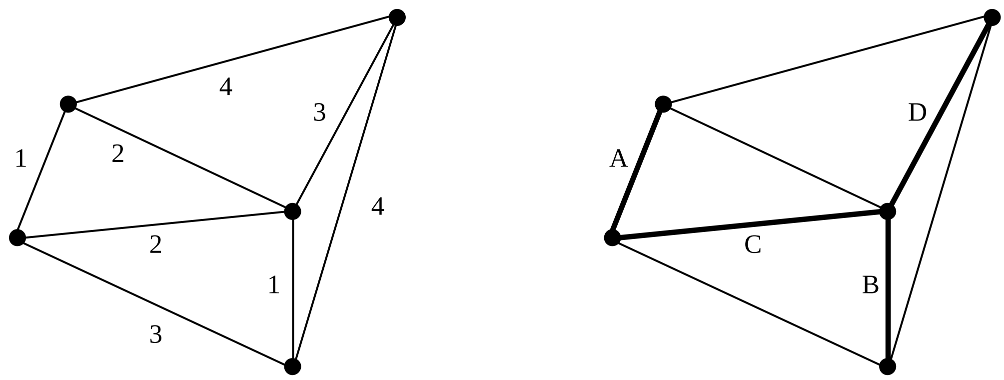
Dále se v cyklu postupně konstruují množiny hran $E_0, E_1, E_2, \ldots \subseteq E$, přičemž $E_0 = \emptyset$. Je-li už nalezena množina E_{i-1}, určí se množina E_i předpisem

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\}, \text{ jestliže graf } G(V, E_{i-1} \cup \{e_i\}) \text{ neobsahuje kružnici,} \\ E_{i-1} \text{ jinak.} \end{cases}$$

Algoritmus se zastaví, jestliže množina E_i má $n-1$ hran nebo $i=m$, tj. všechny hrany grafu $G(V,E)$ jsou už zpracovány.

Jestliže E_t značí množinu hran, pro níž se Kruskalův algoritmus zastavil, pak $T=(V,E_t)$ představuje hledanou minimální kostru grafu $G(V,E)$.

Příklad 5.5.3. Pro ilustraci určíme minimální kostru hranově ohodnoceného grafu na znázorněného obrázku 5.6a. Setřídíme-li hrany zadaného grafu podle jejich ohodnocení, dostaneme neklesající posloupnost 1, 1, 2, 2, 3, 3, 4, 4. Graf má celkem pět vrcholů a osm hran. Existuje více možností, jak postupně konstruovat množinu hran E_0, E_1, E_2, E_3, E_4. Jeden z možných postupů je znázorněn na obrázku 5.6b; pořadí, v němž byly hrany přidávány, je vyznačeno písmeny A,B,C a D.



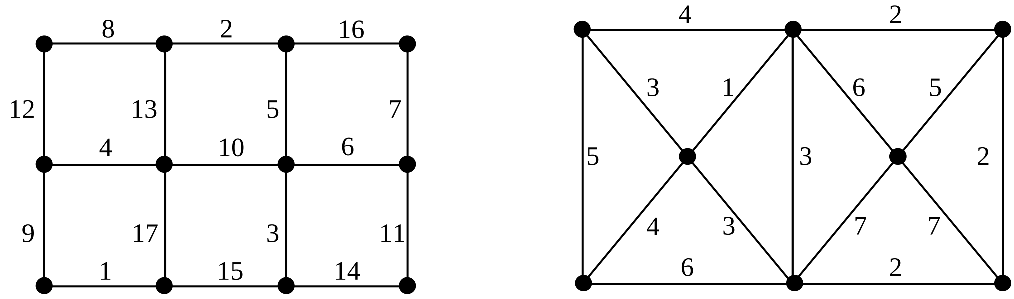
a) b)

Obr. 5.6. Ilustrace k příkladu 5.5.3:
a) výchozí graf; b) postup při konstrukci minimální kostry.

Kruskalův algoritmus řeší problém minimální kostry v tom smyslu, že vždy nalezne minimální kostru daného grafu vzhledem k ohodnocení. Pokud existuje pro daný graf více minimálních koster, pak nalezne jednu z nich. Důkaz správnosti Kruskalova algoritmu je uveden v monografii [15].

Úkoly.

1. Příklad 5.5.3 má více řešení. Nalezněte jinou minimální kostru grafu na obrázku 5.6a.
2. Určete všechny různé minimální kostry hranově ohodnocených grafu na obrázcích 5.7a a 5.7b.
3. Určete všechny různé minimální kostry hranově ohodnocených grafu na obrázcích 5.7a a 5.7b.



a) b)

Obr. 5.7. Ilustrace k úloze 2.

Existuje několik sofistikovanějších algoritmů k nalezení minimální kostry grafu, např. Jarníkův (Primův) algoritmus a Borůvkův algoritmus. Popis těchto algoritmů lze nalézt v monografii [15].

5.6 Eulerovské grafy

Jednou z nejstarších úloh je úloha zvaná „jednotažka“, kterou lze laicky formulovat takto: Nakreslete daný graf jedním uzavřeným tahem tak, že se žádná jeho hrana neopakuje dvakrát.

Uzavřený eulerovský tah
Eulerovský graf

Definice 5.6.1. Nechť G je nějaký souvislý neorientovaný graf. Pak uzavřený sled $(v_0, e_1, v_1, \, ..., \, e_{n-1}, v_{n-1}, v_n, e_n, v_0)$ takový, že se v něm každá hrana vyskytuje právě jednou a každý vrchol nejméně jednou, se nazývá **uzavřený eulerovský tah**. Graf G je **eulerovský**, právě když má alespoň jeden uzavřený eulerovský tah.

Eulerovská cesta

Poznámka. Pro uzavřený eulerovský tah se někdy používá název **eulerovská cesta**.

Nejprve se budeme zabývat neorientovanými grafy. Odpověď na otázku, za jakých podmínek je graf eulerovský, tj. kdy existuje v grafu uzavřený eulerovský tah, dává následující věta.

Věta 5.6.1. Souvislý neorientovaný graf G je eulerovský, právě když každý jeho vrchol je sudého stupně.

Poznámka. Věta platí i pro grafy s vícenásobnými hranami.

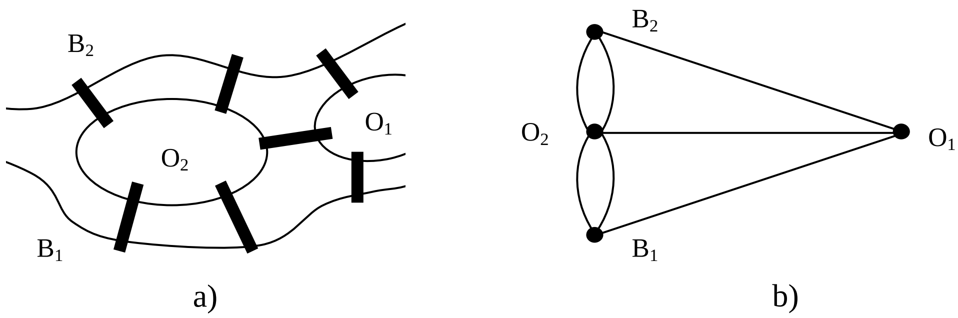
Důkaz. Předpokládejme, že graf G je eulerovský. Pak každý jeho vrchol musí být sudého stupně, protože pro každý vrchol platí: kdykoliv uzavřený eulerovský tah vstoupí do nějakého vrcholu, musí ho zase opustit.

Naopak, nechť souvislý graf $G(V, E)$ má všechny vrcholy sudého stupně. Uvažme v tomto grafu nějaký uzavřený tah $T = (v_0, e_1, v_1, \, ..., \, , e_m, v_m)$, který má maximální délku m. Nejprve dokážeme, že $v_0 = v_m$. Kdyby uvedený vztah neplatil, pak by do vrcholu v_0 zasahoval lichý počet hran. Stupeň vrcholu v_0 je podle předpokladu sudý. Proto existuje nějaká hrana $e \in E$, která není v tahu T obsažena, a o tuto hranu bychom mohli tah prodloužit, což vede ke sporu.

Vyjdeme tedy z předpokladu $v_0 = v_m$ a dokážeme, že $\{e_1, e, \ldots, e_m\} = E$. Definujme pomocný graf $G^* = (V^*, E^*)$, kde V^* je množina všech vrcholů a E^* množina všech hran tahu T.

Předpokládejme, že $V^* \neq V$. Graf G je podle předpokladu souvislý, a tak existuje hrana $e = \{v_k, v^*\} \in E$, kde $v_k \in V^*$ a $v^* \notin V^*$. V takovém případě tah $(v^*, e, v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1 \ldots, e_k, v_k)$ má délku $m+1$, a to vede ke sporu.

Nechť tedy $V^* = V$ a přitom $E^* \neq E$. Uvažujme nějakou „nadbytečnou“ hranu $e = \{v_k, v_t\} \in E \setminus E^*$. Také v tomto případě, podobně jako v předchozím případě, vede tah $(v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1 \ldots, e_k, v_t)$ ke sporu. □



Obr. 5.8. Ilustrace k Eulerovu problému o sedmi mostech v Kőnigsbergu: a) schematické rozmístění mostů, b) příslušný graf.

Příklad 5.6.1. Pokusíme se vyřešit jednu z nejstarších úloh teorie grafů, tzv. problém sedmi mostů v Kőnigsbergu (dnes Kaliningradu). Městem protéká řeka a v ní jsou dva ostrovy O_1 a O_2. V 18. století stálo ve městě sedm mostů, jak je znázorněno na obr. 5.8a. Úloha byla formulována takto: Je možno projít městem tak, abychom přešli všechny mosty právě jednou a vrátili se tam, odkud jsme vyšli? Situaci můžeme popsat grafem na obr. 5.8b, jehož vrcholy O_1, O_2 představují ostrovy a vrcholy B_1, B_2 břehy zmíněné řeky. Všechny vrcholy grafu jsou lichého stupně, a proto (podle věty 5.6.2) úloha nemá řešení.

Vycházejíce z právě dokázané věty, popíšeme algoritmus pro nalezení uzavřeného eulerovského tahu (eulerovské cesty). V průběhu algoritmu budeme postupně konstruovat sled T jako posloupnost vrcholů a hran grafu $G(V,E)$.

Algoritmus pro konstrukci uzavřeného eulerovského tahu.

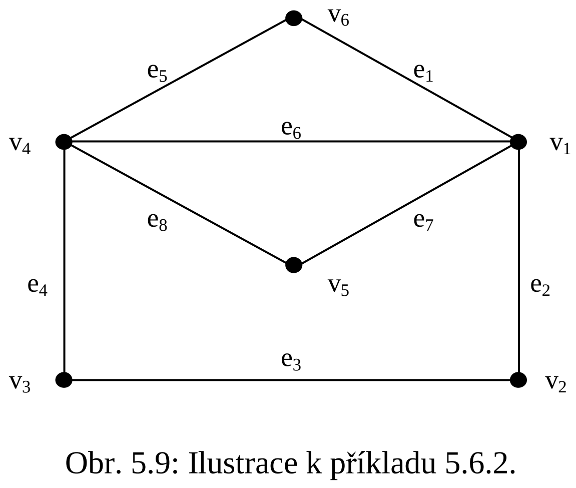
Algoritmus pro konstrukci eulerovské cesty

1. krok. Vybereme libovolný vrchol grafu $G(V,E)$ a označíme jej v_0. Dále vybereme hranu $e_i = \{v_0, v_i\} \in E$, položíme $T = (v_0, e_i, v_i)$ a posuneme se do bodu v_i.

2. krok. Vybereme další hranu $e_j = \{v_i, v_j\} \in E \setminus e_i$. Jestliže taková hrana existuje, pak $T = (v_0, e_i, v_i, e_j, v_j)$ a ověřujeme, zda je tah T uzavřený. Pokud není uzavřený, položíme $j := i$ a pokračujeme ve výběru další hrany. V případě, že je tah T uzavřený, zjišťujeme, zda je T také hledaným uzavřeným tahem. Pokud ano, algoritmus skončí, v opačném případě pokračujeme 3. krokem.

3. krok. Vybereme vrchol v_k, pro nějž platí, že existuje hrana $e_k = \{v_k, v_l\}$ dosud nezařazená do žádného sledu, položíme $T_k = (v_k, e_k, v_l)$. Postupně vybíráme další takové hrany a „připojujeme“ je do sledu T_k, a to do té doby, než se stane uzavřeným sledem.

4. krok. Vložíme sled T_k do sledu T a ověříme, zda je vytvořený sled skutečně uzavřeným eulerovským tahem (eulerovskou cestou). Pokud ano, algoritmus skončí, v opačném případě pokračuje krokem 3.



Obr. 5.9: Ilustrace k příkladu 5.6.2.

Příklad 5.6.2. Pomocí popsaného algoritmu nalezneme uzavřený eulerovský tah (eulerovskou cestu) v grafu na obr. 5.9.

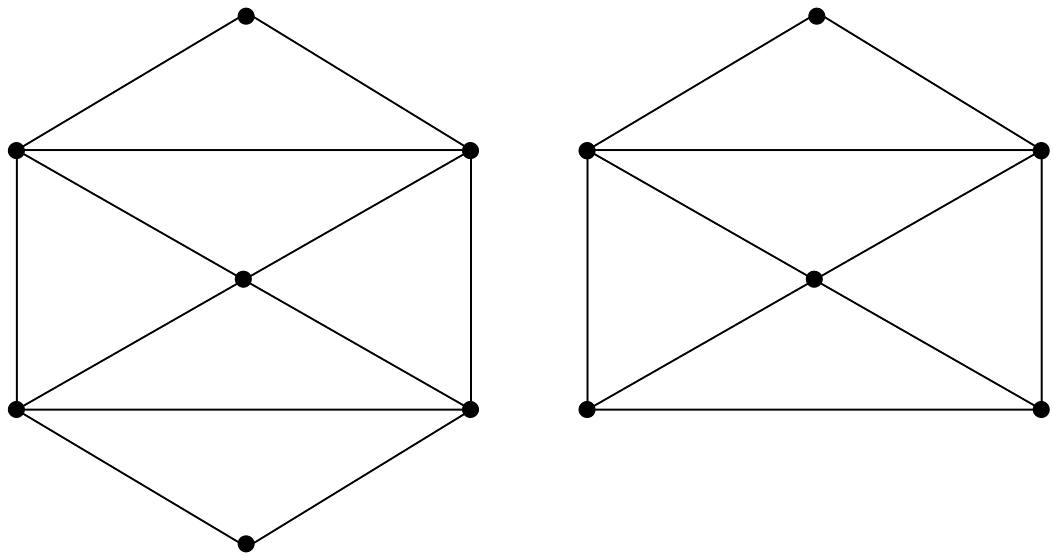
1. krok. Vybereme např. vrchol v_0 a hranu $e_1 = \{v_0, v_1\}$. Vytvoříme sled $T = (v_0, e_1, v_1)$ a přejdeme do vrcholu v_1.

2. krok. Vybereme další hranu $e_2 = \{v_1, v_2\}$, přidáme ji do sledu T a posuneme se do vrcholu v_2. Sled $T = (v_0, e_1, v_1, e_2, v_2)$ není uzavřený, proto vybereme další (dosud nezařazenou) hranu $e_3 = \{v_2, v_3\}$, přidáme ji do sledu T a přejdeme do vrcholu v_3. Ani sled $T = (v_0, e_1, v_1, e_2, v_2, e_3, v_3)$ není uzavřený, a tak pokračujeme ve výběru dalších dosud nezařazených hran $e_4 = \{v_3, v_4\}$ a $e_5 = \{v_4, v_0\}$. Dostaneme sled $T = (v_0, e_1, v_1, e_2, v_2, e_3, v_3, e_4, v_4, e_5, v_0)$, který je již uzavřený, ale neobsahuje všechny hrany grafu, a proto není hledanou eulerovskou cestou.

3. krok. Vezmeme vrchol v_1, pro nějž existuje dosud nezařazená hrana $e_6 = \{v_1, v_4\}$ a tuto hranu vložíme do sledu T_1. Dostaneme $T_1 = (v_1, e_6, v_4)$. Postupně vybereme další nezařazené hrany $e_6 = \{v_4, v_5\}$ a $e_7 = \{v_5, v_1\}$. Tak získáme sled $T_1 = (v_1, e_6, v_4, e_8, v_5, e_7, v_1)$, který je už uzavřený.

4. krok. Vložíme sled T_1 do sledu T a dostaneme sled $(v_0, e_1, v_1, e_6, v_4, e_8, v_5, e_7, v_1, e_2, v_2, e_3, v_3, e_4, v_4, e_5, v_0)$. Tento sled je, jak snadno ověříme, hledanou eulerovskou cestou.

Úkol. Rozhodněte, zda graf na obr. 5.10a je eulerovský, a pokud ano, nalezněte v něm eulerovskou cestu.



a) b)

Obr 5.10: Ilustrace k úlohám o nalezení eulerovské cesty (5.10a), resp. otevřeného eulerovského tahu (5.10b).

V některých úlohách se hledá namísto uzavřeného eulerovského sledu (eulerovské cesty) otevřený eulerovský sled.

Definice 5.6.2. Nechť G je nějaký souvislý neorientovaný graf. Pak otevřený sled $\left(v_0, e_1, v_1, \ ..., e_{n-1}, v_{n-1}, v_n\right)$ takový, že se v něm každá hrana vyskytuje právě jednou a každý vrchol nejméně jednou, se nazývá **otevřený eulerovský tah**.

Otevřený eulerovský tah

V tomto případě můžeme formulovat podmínku pro existenci otevřeného eulerovského sledu takto.

Věta 5.6.2. V souvislém neorientovaném grafu G existuje otevřený eulerovský tah, právě když graf G obsahuje dva vrcholy lichého stupně.

Důkaz. Uvažujme graf $G(V,E)$, jehož dva vrcholy (označme je např. v^* a v^{**}) jsou lichého stupně. Do tohoto grafu přidáme fiktivní vrchol $x \notin V$ a hrany $\{v^*, x\}$, $\{x, v^{**}\}$, které spojují vrchol x s oběma vrcholy lichého stupně. Tím dostaneme graf, jehož všechny vrcholy mají sudý stupeň. Pro tento graf můžeme použít větu 5.6.1, podle níž právě v takovém grafu existuje uzavřený euklidovský tah. Pak jen stačí odstranit fiktivní vrchol $x \notin V$ a hrany $\{v^*, x\}$, $\{x, v^{**}\}$ a dostaneme hledaný otevřený euklidovský tah. □

Úkol. Rozhodněte, zda v grafu na obr. 5.10b existuje otevřený eulerovský tah, a pokud ano, tak jej nalezněte.

Rozšíříme pojem eulerovského grafu na grafy orientované. Nejprve musíme zavést některé nové pojmy: uzavřený orientovaný tah a symetrizaci grafu G.

Definice 5.6.3. Nechť G je nějaký souvislý orientovaný graf. Pak uzavřený sled $\left(v_0, e_1, v_1, \ ..., e_{n-1}, v_{n-1}, v_n, e_n, v_0\right)$, pro nějž platí $e_i = \left(v_{i-1}, v_i\right) \in E$ pro $i = 1, 2, \ .., n$ a $e_i \neq e_j$ pro $i \neq j$ (takový, že se v něm každá hrana vyskytuje právě jednou a každý vrchol nejméně jednou), se nazývá **uzavřený orientovaný tah**. Orientovaný graf G je **eulerovský**, právě když má alespoň jeden uzavřený orientovaný tah.

Uzavřený orientovaný tah

Každému orientovanému grafu $G(V,E)$ lze přiřadit neorientovaný graf sym $(G) = \left(V, \tilde{E}\right)$, kde $\tilde{E} = \left\{\{x, y\};\ (x, y) \in E \text{ nebo } (y, x) \in E\ \right\}$. Graf sym (G) se nazývá **symetrizace grafu *G***.

Věta 5.6.3. Orientovaný graf $G(V,E)$ je eulerovský, právě když pro každý vrchol $v \in V$ platí, že jeho vstupní a výstupní stupně se rovnají a navíc jeho symetrizace je souvislý graf.

Kontrolní otázky:

1. Jaký je principiální rozdíl mezi neorientovanými a orientovanými grafy?
2. Jaké charakteristiky se v praxi připisují hranám v hranově ohodnocených grafech?
3. Popište algoritmus používaný při rozhodování, zda daná posloupnost je posloupností grafovou.
4. Jakým způsobem se obvykle reprezentuje daný graf v paměti počítače?
5. Porovnejte matici sousednosti a Laplaceovu matici sousednosti daného grafu.
6. Jaký je rozdíl mezi sledem a cestou v neorientovaném grafu?
7. Jaké obecné vlastnosti má metrika grafu?
8. Jaké vlastnosti navíc má metrika hranově neohodnoceného grafu?
9. Popište Dijkstrův algoritmus pro určení nejkratší cesty v daném grafu.
10. Popište souvislosti mezi daným grafem, jeho podgrafem a jeho indukovaným podgrafem.
11. Jaké významné typy podgrafů znáte?
12. Jaký je rozdíl základní mezi stromem a lesem?
13. Jaký postup se používá při ověřování skutečnosti, že daný graf je stromem?
14. Jaké jsou základní charakteristiky stromu?
15. Formulujte problém minimální kostry graf.
16. Popište Kruskalův algoritmus pro stanovení minimální kostry.
17. Jaké jsou nutné a postačující podmínky pro existenci uzavřeného eulerovského tahu (eulerovské cesty) v neorientovaném grafu?
18. Popište algoritmus pro nalezení eulerovské cesty v neorientovaném grafu?
19. Jaké jsou nutné a postačující podmínky pro existenci otevřeného eulerovského tahu v neorientovaném grafu?

Pojmy k zapamatování:

- graf,
- vrchol grafu,
- hrana grafu,
- orientace hrany,

- ohodnocení hrany,
- úplný graf,
- kružnice,
- bipartitní graf,
- stupeň vrcholu,
- skóre grafu (grafová posloupnost),
- rovnost grafů,
- isomorfismus grafů,
- matice sousednosti,
- Laplaceova matice sousednosti,
- matice incidence,
- sled v grafu,
- cesta v grafu,
- souvislost grafu,
- komponenta grafu,
- vzdálenost vrcholů,
- metrika grafu,
- Dijkstrův algoritmus,
- podgraf,
- indukovaný podgraf,
- faktor grafu,
- strom,
- kostra grafu,
- minimální kostra grafu,
- Kruskalův algoritmus,
- eulerovský graf,
- uzavřený eulerovský tah (eulerovská cesta),
- algoritmus pro konstrukci eulerovské cesty,
- otevřený eulerovský tah,
- uzavřený orientovaný (eulerovský) tah.

Shrnutí

Tato kapitola představuje pouze úvod do teorie grafů. V úvodní části jsou definovány základní pojmy (graf, vrchol grafu, hrana grafu, stupeň vrcholu, skóre grafu), nastíněna klasifikace grafů a uvedeny některé významné typy grafů. Následující části jsou věnovány isomorfismu grafů, základním způsobům reprezentace grafů (matice sousednosti, Laplaceova matice sousednosti a matice incidence), problematice spojené se souvislostí grafu (sled a cesta v grafu, komponenta grafu, metrika grafu), významným typům podgrafů (především stromům) a eulerovským grafům.

Zvláštní pozornost je přitom zaměřena na grafické algoritmy (Dijkstrův algoritmus pro nalezení nejkratší cesty v grafu, Kruskalův algoritmu pro určení minimální kostry grafu, algoritmus pro konstrukci eulerovské cesty). Některé možnosti aplikace grafů jsou uvedeny v monografiích [4,16].

Autotest

1. Určete počet přirozených čísel od 1 do 100 takových, že nejsou dělitelné 3 ani 7.
2. Najděte duální formuli k následujícím formulím:

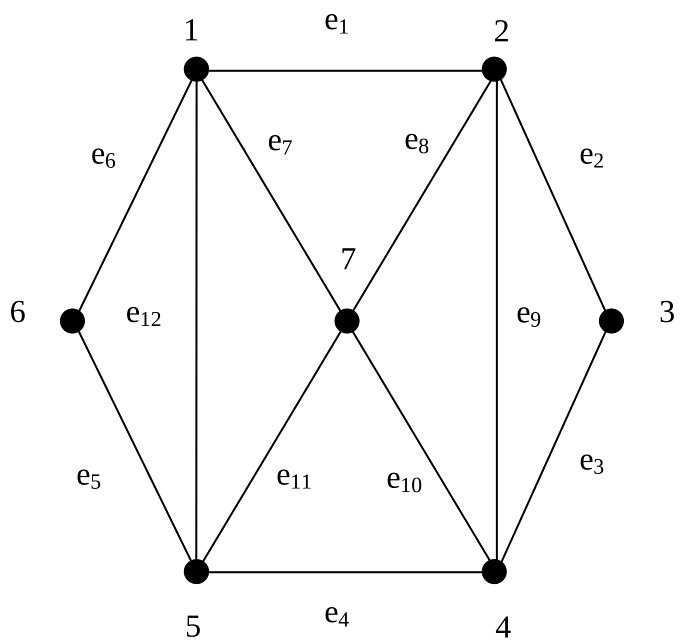
   a) $(x \vee \overline{y}) \wedge (x \vee y)$,

   b) $y \Leftrightarrow x$.
3. Dokažte, že platí $x \wedge [(y \vee x) \vee (x \wedge y)] = x \wedge (x \vee y)$. Uveďte, které ekvivalence jste při důkazu použili.
4. Je dána tabulka pravdivostních hodnot funkce $f(x, y, z)$.

x	y	z	$f(x, yz)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Určete úplnou disjunktivní i úplnou konjunktivní normální formu této funkce.

5. Rozhodněte, zda posloupnost (7, 6, 6, 5, 4, 4, 4, 3, 3, 3, 2) je skóre grafu (grafová posloupnost).
6. Je dán prostý graf s očíslovanými vrcholy a hranami. Určete příslušnou matici incidence.



Výsledky autotestu

1. 57

2. a) $\left(x \wedge \overline{y}\right) \vee \left(\overline{x} \wedge y\right)$; b) $\left(\overline{y} \wedge x\right) \vee \left(\overline{x} \wedge y\right)$

3. Např. : $$\begin{aligned} & x \wedge \big(\left(y \vee x\right) \vee \left(x \wedge y\right)\big) = x \wedge \big(y \vee \left(x \wedge 1\right) \vee \left(x \wedge y\right)\big) = \\ & = x \wedge \big(y \vee x \wedge \left(1 \vee y\right)\big) = x \wedge \big(y \vee \left(x \wedge 1\right)\big) = x \wedge \left(y \vee x\right). \end{aligned}$$

4. DNF: $\overline{x}\,\overline{y}\,\overline{z} \vee \overline{x}\,\overline{y}z \vee x\overline{y}\,\overline{z} \vee x\overline{y}z$;

   KNF: $\left(x + \overline{y} + z\right) \wedge \left(x + \overline{y} + \overline{z}\right) \wedge \left(\overline{x} + \overline{y} + z\right) \wedge \left(\overline{x} + \overline{y} + \overline{z}\right)$

5. Posloupnost není grafová.

6. $$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

LITERATURA

[1] BĚLOHLÁVEK, R., VYCHODIL, V. *Diskrétní matematika pro informatiky I.* [Učební text.]. Olomouc: PřF UP Olomouc, 2006.

[2] BĚLOHLÁVEK, R., VYCHODIL, V. *Diskrétní matematika pro informatiky II.* [Učební text.]. Olomouc: PřF UP Olomouc, 2006.

[3] ČADA, R., KAISER, T., RYJÁČEK, Z. *Diskrétní matematika.* [Učební text.]. Plzeň: FAV ZU Plzeň, 2004.

[4] DEMEL, J. *Grafy a jejich aplikace*. SNTL Praha, 1988.

[5] HLÍNĚNÝ, P. *Diskrétní matematika.* [Učební text.]. Ostrava: VŠB-TU Ostrava, 2004.

[6] JABLONSKIJ,S. V. *Úvod do diskrétní matematiky*. Bratislava: ALFA, 1984.

[7] KONEČNÁ, P. *Diskrétní matematika*. [Učební text.].Ostrava: PřF OU Ostrava, 2004.

[8] KONEČNÁ, P. *Úvod do teorie grafů.* [Učební text.].Ostrava: PřF OU Ostrava, 2006.

[9] KOPKA, J. Svazy a Booleovy algebry. [Učební text.]. Ústí nad Labem: Univerzita J. E. Purkyně, 1991.

[10]KOUCKÝ, M., ZELINKA, B. *Diskrétní matematika I.* [Učební text.]. Liberec: PdF TU Liberec, 2004.

[11]KOUCKÝ, M. *Diskrétní matematika II.* [Učební text.]. Liberec: PdF TU Liberec, 2002.

[12]KOVÁŘ, P. Cvičení z diskrétní matematiky. [Učební text.]. Ostrava: VŠB-TU Ostrava, 2009.

[13]KŘIVÝ, I. *Úvod do teorie pravděpodobnosti.* [Učební text.]. Ostrava: Pedagogická fakulta, 1983.

[14]KŘIVÝ, I. *Sbírka úloh z teorie pravděpodobnosti.* [Učební text.]. Ostrava: Pedagogická fakulta, 1981.

[15]MATOUŠEK, J., NEŠETŘIL, J. *Kapitoly z diskrétní matematiky*. Praha: Karolímum, 2007.

[16]NEČAS, J. Grafy a jejich použití. Praha: SNTL, 1978.

[17]SEDLÁČEK, J. *Úvod do teorie grafů*. Academia Praha, 1977.

[18]VELEBIL, J. *Diskrétní matematika. Sbírka řešených příkladů.* [Učební text.]. Praha: FEL ČVUT Praha, 2007.

[19]VILENKIN, N. J. *Kombinatorika.* Praha: SNTL, 1977.

Doporučená a rozšiřující literatura

BALAKRISHNAN, V. K. *Introductory Discrete Mathematics*New York: Dover, 1997.

DOSSEY, J. A. et al. *Discrete Mathematics*, 3rd edition. Reading: Addison-Wesley, 1997.

FUCHS, E. *Diskrétní matematika pro učitele*. Brno: Přírodovědecká fakulta MU, 2001. ISBN 80-210-2703-7.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O. *Concrete Mathematics. A Foundation for Computer Science.*. New York: Addison Wesley, 2008.

HAVLÍČEK, I. Diskrétní matematika. [Učební text]. Praha: Vysoká škola finanční a právní, 2007.

JOHNSONBAUGH,, R. *Discrete Mathematics*. 7th Edition. Pearson Education Ltd., 2008. ISBN 01-313-5430-2.

LIPSCHITZ, S., LIPSON, M. L. *2000 Solved Problems in Discrete Mathematics.* New York: McGraw-Hill Company, 1991.

MEZNÍK, I. Diskrétní matematika pro užitou informatiku. Brno: Siemens Industrial Turbomachinery, 2009.

ROSEN, K. H. *Discrete Mathematics and Its Applications*, 6th Edition. New York: McGraw-Hill Higher Education, 2007. ISBN 0-07-288008-2.

STEIN, C., DRYSDALE, R., BOGART, K. *Discrete Mathematics for Computer Scientists*. Addison Wesley, 2010. ISBN 0-132-12271-5.

NÝDL, V. *Diskrétní matematika v příkladech, díl 1.* [Učební text]. České Budějovice: Jihočeská univerzita, 2006.

NÝDL, V. *Diskrétní matematika v příkladech, díl 2.* Č. [Učební text]. České Budějovice: Jihočeská univerzita, 2007.