

Vybraná témata z algoritmů

Abstrakt

Poznámky k semináři VYTAL v letním semestru 2026. Poslední úprava 27. února 2026.

1 První seminář

Obsah. *formule výrokové logiky a booleovské obvody reprezentují (všechny) booleovské funkce; pravdivost, splnitelnost, sémantická ekvivalence, ekvivalence vzhledem ke splnitelnosti; Tseitsinův algoritmus.*

~

def. *n-ární booleovská funkce* je funkce $f : \{0, 1\}^n \rightarrow \{0, 1\}$. (0 je nepravda, 1 je pravda).

Otázka. *Kolik je n-árních booleovských funkcí?*

Došli jsme k tomu, booleovskou funkci f můžeme reprezentovat řetězcem 2^n bitů, ve kterém je i -tý bit je roven $f(b_1, b_2, \dots, b_n)$, kde $(b_1 b_2 \dots b_n)_2 = i$. (Nejdříve si můžeme přestavit tabulku s $n+1$ sloupci, kde v prvních n sloupcích jsou hodnoty jednotlivých argumentů $b_1, b_2, \dots, b_n$ a v posledním sloupci je hodnota $f(b_1, b_2, \dots, b_n)$. Pokud řádky uspořádáme tak, že číslo $(b_1 b_2 \dots b_n)_2$ roste, jdeme-li tabulkou dolů, tvoří obsah posledního sloupce žádaný řetězec.) n -ární booleovských funkcí je tak tolik, kolik je 2^n -bitových řetězců, tedy 2^{2^n} . $\square$

Příklady booleovských funkcí jsou funkce logických spojek, zejména CON (konjunkce), DIS (disjunkce), NEG (negace).

V dalším použijeme množinu proměnných $VAR = \{x_1, x_2, x_3 \dots\}$, některé z nich budeme občas značit i jinými symboly, např. y, z s případným indexem.

def. *Formule* výrokové logiky je řetězec nad abecedou tvořenou proměnnými, symboly pro logické spojky $\wedge, \vee, \neg$, a závorkami, který je vytvořen podle následujících pravidel.

- Proměnná je formule.
- Jsou-li F, G formule, potom jsou i $(F \wedge G)$, $(F \vee G)$, $\neg F$ formule.

Některé závorky můžeme při zápisu vynechávat (např. vnější závorky, případně místo $(F \wedge G) \wedge H$ psát $F \wedge G \wedge H$, podobně pro disjunkci). Základní definici můžeme rozšířit o symboly dalších spojek zavedením *zkratk*:

- $F \rightarrow G$ je zkratkou $\neg F \vee G$,
- $F \leftrightarrow G$ je zkratkou $(F \rightarrow G) \wedge (G \rightarrow F)$.

Množinu proměnných obsažených ve formuli F označíme $\text{VAR}(F)$.

def. *Ohodnocení proměnných* je částečné zobrazení $\alpha : \text{VAR} \rightarrow \{0, 1\}$. Množinu proměnných, které α ohodnocuje, označíme $\text{VAR}(\alpha)$.

def. Pokud $\text{VAR}(F) \subseteq \text{VAR}(\alpha)$ můžeme hovořit o pravdivosti $F[\alpha]$ formule F . Je definována následovně:

- pro proměnnou x máme $x[\alpha] = \alpha(x)$,
- $(F \wedge G)[\alpha] = \text{CON}(F[\alpha], G[\alpha])$,
- $(F \vee G)[\alpha] = \text{DIS}(F[\alpha], G[\alpha])$,
- $(\neg F)[\alpha] = \text{NEG}(F[\alpha])$.

def. Formule F s proměnnými $\{x_1, \dots, x_n\}$ reprezentuje n -ární booleovskou funkci f , pokud pro každé ohodnocení α ohodnocující všechny tyto proměnné máme $F[\alpha] = f(\alpha(x_1), \alpha(x_2), \dots, \alpha(x_n))$.

Otázka. Existuje ke každé n -ární booleovské funkci formule, která ji reprezentuje?

Tady jsme si připoměli konstrukci formule v normální formě (konjunktivní nebo disjunktivní). Konstrukci provádíme na základě pravdivostní tabulky. Pravdivostní tabulka, ze které vynecháme všechny sloupce mimo ohodnocení proměnných a pravdivosti dané formule je vlastně zápis booleovské funkce pomocí tabulky (a existuje pro každou booleovskou funkci). Podrobnosti konstrukce lze nalézt v kurzu diskretních struktur. Odpověď je tedy *ano*, navíc umíme potřebnou formuli explicitně zkonstruovat. $\square$

def. n -ární booleovský obvod C je orientovaný graf bez cyklů. Vrcholům říkáme brány, vede-li z brány g hrana do brány h , je h vstupem g . Dále platí následující podmínky.

- Graf obsahuje n bran bez vstupů, každé je přiřazena jiná proměnná z množiny $\{x_1, x_2, \dots, x_n\}$. Jsou to tzv. vstupní brány. (Pak $\text{VAR}(C) = \{x_1, x_2, \dots, x_n\}$)
- Brány s jedním vstupem jsou $\neg$ -brány,
- Brány se dvěma vstupy jsou $\wedge$ -brány nebo $\vee$ -brány.
- V grafu nejsou brány s více než 2 vstupy.
- Jedna brána je navíc označena jako výstupní.

Nyní definujeme pravdivost obvodu pro ohodnocení α takové, že $\{x_1, \dots, x_n\} \subseteq \text{VAR}(\alpha)$. Nejdříve definujeme pravdivost $g[\alpha]$ brány g .

- Pokud je g vstupní brána s proměnou x , pak $g[\alpha] = \alpha(x)$.
- Pokud je g $\neg$ -brána se vstupem h , pak $g[\alpha] = \text{NEG}(h[\alpha])$.
- Pokud je g $\wedge$ -brána se vstupy h_1, h_2 , pak $g[\alpha] = \text{CON}(h_1[\alpha], h_2[\alpha])$.
- Pokud je g $\vee$ -brána se vstupy h_1, h_2 , pak $g[\alpha] = \text{DIS}(h_1[\alpha], h_2[\alpha])$.

Pravdivost obvodu je rovna pravdivosti jeho výstupní brány. Analogicky formulím výrokové logiky můžeme definovat situaci, kdy obvod C reprezentuje booleovskou funkci.

def. Nechť G je booleovský obvod nebo formule výrokové logiky. Pokud existuje ohodnocení α tak, že $\text{VAR}(\alpha) \subseteq \text{VAR}(G)$ a $G[\alpha] = 1$, řekneme, že objekt G je *splnitelný*.

def. Nechť G, F jsou booleovský obvod nebo formule výrokové logiky (mohou to být objekty různého typu). Potom

- G a F jsou *sémanticky ekvivalentní*, pokud pro každé ohodnocení α takové, že $\text{VARS}(G) \cup \text{VARS}(F) \subseteq \text{VARS}(\alpha)$, platí $G[\alpha] = F[\alpha]$.
- G a F jsou *ekvivalentní vzhledem ke splnitelnosti*, pokud je G splnitelná právě když je F splnitelná.

Otázka. Existuje ke každé booleovské funkci booleovský obvod, který ji reprezentuje?

Odpověď je ano. Protože ke každé booleovské funkci existuje formule výrokové logiky, která ji reprezentuje, stačí najít postup transformace formule výrokové logiky na sémanticky ekvivalentní booleovský obvod. Tento postup jsme na semináři našli. $\square$

def. *Literál* je proměnná, nebo její negace. *Klausule* je disjunkcí literálů. Formule je *konjunktivní normální formě* (CNF), pokud je konjunkcí klausulí.

Tseitsinův algoritmus. Pomocí Tseitsinova algoritmu můžeme transformovat obvod C na formuli F v CNF tak, že C a F jsou ekvivalentní vzhledem ke splnitelnosti. Protože libovolnou formuli umíme převést na jí sémanticky ekvivalentní obvod (viz předchozí otázka), lze provedením Tseitsinova algoritmu na takto získaný obvod převést libovolnou formuli na formuli v CNF, která je s ní ekvivalentní vzhledem ke splnitelnosti. Následují detaily Tseitsinova algoritmu.

Vstupem algoritmu je obvod C , výstupem je formule F . Proměnné obvodu C jsou $x_1, \dots, x_n$ a jeho brány jsou $g_1, \dots, g_m$. Proměnné ve formuli F jsou $x_1, \dots, x_n, g_1, \dots, g_m$. Ve formuli tedy máme jednu proměnnou pro každou proměnnou v C a jednu proměnnou pro každou bránu v C : značíme je stejně, v následujícím bude vždy jasné, kdy se jedná o proměnnou a kdy o bránu.

Algoritmus funguje tak, že projde všechny brány obvodu C a pro každou vytvoří formuli v CNF. Výsledná formule je potom jejich konjunktí. Označme aktuální bránu g , a její případné vstupy označme h_1, h_2 (g, h_1, h_2 tedy patří do množiny $\{g_1, \dots, g_m\}$).

- Je-li g vstupní brána proměnné x (tj. x je z množiny $\{x_1, \dots, x_n\}$), vytvoříme formuli $(\neg g \vee x) \wedge (g \vee \neg x)$. *Princip:* Aby tedy byla formule pravdivá, musí být g a x ohodnoceny stejně. Je totiž sémanticky ekvivalentní $g \leftrightarrow x$: formule $(\neg g \vee x)$ je totiž sémanticky ekvivalentní $(g \rightarrow x)$ a formule $(g \vee \neg x)$ je sémanticky ekvivalentní $(x \rightarrow g)$.
- Je-li g $\neg$ -brána se vstupem h_1 , vytvoříme formuli $(\neg g \vee \neg h_1) \wedge (g \vee h_1)$. (Která je sémanticky ekvivalentní $(g \leftrightarrow h_1)$.)
- Je-li g $\wedge$ -brána se vstupy h_1, h_2 , vytvoříme formuli $(\neg g \vee h_1) \wedge (\neg g \vee h_2) \wedge (\neg h_1 \vee \neg h_2 \vee g)$. (Která je sémanticky ekvivalentní $(h_1 \wedge h_2) \leftrightarrow g$.)
- Je-li g $\vee$ -brána se vstupy h_1, h_2 , vytvoříme formuli $(\neg h_1 \vee g) \wedge (\neg h_2 \vee g) \wedge (h_1 \vee h_2 \vee \neg g)$. (Která je sémanticky ekvivalentní $(h_1 \vee h_2) \leftrightarrow g$.)
- Je-li g výstupní bránou, pak navíc vytvoříme formuli g .

Principem celé konstrukce a základem formálního důkazu toho, že C a F jsou ekvivalentní vzhledem ke splnitelnosti, je fakt, že F kóduje správnost výpočtu pravdivosti bran v C .

Podrobněji. Nechť α je ohodnocení takové, že $\text{VARS}(\alpha) = \text{VARS}(C)$. Pokud $C[\alpha] = 1$, můžeme rozšířit α o ohodnocení proměnných $g_1, \dots, g_m$ tak, že pro výsledné ohodnocení α' máme $F[\alpha'] = 1$. Stačí proměnnou g ohodnotit na pravdivost $g[\alpha]$ v obvodu C .

Obráceně, pokud pro nějaké ohodnocení α máme $F[\alpha] = 1$, potom musí platit, že $\alpha(g)$ je stejně jako pravivost $g[\alpha]$ brány g v obvodu C (pro ohodnocení α). $\square$

2 Druhý seminář

Obsah. transformace CNF na 3CNF; transformace problému barvení na problém splnitelnosti; transformace sudoku na problém splnitelnosti.

~

def. Formule je v 3CNF, pokud je v CNF a každá klauzule obsahuje právě 3 literály. (Někdy definováno i tak, že klauzule obsahují nejvýše 3 literály, pro nás je to nepodstatný rozdíl.)

Transformace CNF na 3CNF. Transformujeme formuli F v CNF na formuli G v 3CNF. Předpokládáme

$$F = C_1 \wedge C_2 \wedge \dots \wedge C_m,$$

kde $C_1, C_2, \dots, C_m$ jsou klauzule. Formuli G vytvoříme jako konjunkci

$$G = G_1 \wedge G_2 \wedge \dots \wedge G_m,$$

kde G_i je formule v 3CNF získaná transformací klauzule C_i . Pokud nemá C_i více než 3 literály, dostaneme G_i dvojením nebo ztrojením některého z literálů, které C_i obsahuje. Jinak nechť

$$C_i = (l_1 \vee l_2 \vee \dots \vee l_k).$$

Potom

$$G_i = (l_1 \vee l_2 \vee z_1) \wedge (\neg z_1 \vee l_3 \vee z_2) \wedge \dots \wedge (\neg z_{k-3} \vee l_{k-1} \vee l_k),$$

kde $z_1, \dots, z_{k-3}$ jsou nové proměnné (budeme jim říkat z -proměnné a jejich literálům z -literály).

Otázka. Jsou F a G ekvivalentní vzhledem ke splnitelnosti?

Pokud je $C_i[\alpha] = 1$, musí existovat j tak, že $l_j[\alpha] = 1$. V G_i si vybereme klauzuli D obsahující l_j a z -literály v ní obsažené ohodnotíme na 0 (tj. jejich proměnné ohodnotíme tak, aby literály byly nepravdivé). Pokud klauzule D' sousedí s D , obsahuje pravdivý literál, který je negací nepravdivého z -literálu z D . Druhý z -literál v klauzuli D' tak ohodnotíme na 0 a v podobném duchu pokračujeme se sousedem D' . Nakonec budou pravdivé všechny klauzule: jedna díky l_j , zbylé díky pravdivosti z -literálů.

Pokud je $G[\alpha] = 1$ pro nějaké ohodnocení α , pak musí existovat literál l tak, že $l[\alpha] = 1$. Kdyby totiž pro všechny literály l bylo $l[\alpha] = 0$, musela by jít G splnit ohodnocením z -proměnných a to nejde. Musíme mít $\alpha(z_1) = 1$ (jinak bychom nesplnili první klauzuli formule G_i), $\alpha(z_2) = 1$ (jinak bychom nesplnili druhou klauzuli formule G_i) atd. Nakonec dostaneme $\alpha(z_{k-3}) = 1$ a poslední klauzule formule G_i tak není pravdivá.

Předchozí dva odstavce ukazují, že formule F a G vzhledem ke splnitelnosti ekvivalentní jsou. $\square$

def. Instancí problému barvení je neorientovaný graf s množinou vrcholů V a množinou hran H a přirozené číslo k . Cílem je zjistit, jestli existuje zobrazení $c : V \rightarrow \{1, 2, \dots, k\}$ takové, že pro každou $(v, w) \in H$ máme $c(v) \neq c(w)$.

Transformace problému barvení na splnitelnost formule v CNF. Na vstupu je graf $G = (V, H)$ a číslo k . Výsledkem je formule F v CNF. Předpokládáme $V = \{1, 2, \dots, n\}$.

Proměnné ve formuli F označíme x_{ij} pro $i = 1, 2, \dots, n$ a $j = 1, 2, \dots, k$. Hlavní myšlenka je, že ohodnocení α takové, že $F[\alpha] = 1$ bude odpovídat barvení: $\alpha(x_{ij}) = 1$ značí, že vrchol i je obarven barvou j .

Musíme zajistit, že formuli splní pouze ohodnocení α , které takto odpovídá korektnímu barvení. Toto vyjádříme pomocí tří podmínek. Platnost každé z nich vyjádříme formulí v CNF, formule F je potom konjunkcí těchto formulí.

1. *Každý vrchol je obarven alespoň jednou barvou.*

Pro vrchol i to znamená, že alespoň jedna proměnná z $\{x_{i1}, x_{i2}, \dots, x_{ik}\}$ musí být pravdivá. To zajistíme pomocí formule

$$\varphi_i = (x_{i1} \vee x_{i2} \vee \dots \vee x_{ik}).$$

(Pokud je pravdivá, alespoň jedna z proměnných je pravdivá).

2. *Každý vrchol je obarven nejvýše jednou barvou.*

Pro vrchol i to znamená, že nejvýše jedna proměnná z $\{x_{i1}, x_{i2}, \dots, x_{ik}\}$ je pravdivá. To zajistíme pomocí formule

$$\psi_i = \bigwedge_{1 \leq s < t \leq k} (\neg x_{is} \vee \neg x_{it})$$

(Pokud je pravdivá, nejvýše jedna z proměnných je pravdivá).

3. *Sousední vrcholy nejsou obarveny stejnou barvou*

Pro každou hranu $\{v, w\} \in H$ musí platit, že pro každou barvu j nejsou proměnné x_{vj} a x_{wj} obě pravdivé. To zajistíme pomocí formule

$$\kappa_{vw} = \bigwedge_{1 \leq j \leq k} (\neg x_{vj} \vee \neg x_{wj}).$$

Celkem tedy

$$F = \left(\bigwedge_{i=1}^n \varphi_i \wedge \psi_i \right) \wedge \bigwedge_{\{v,w\} \in H} \kappa_{vw}.$$

Z principu konstrukce plyne, že graf G lze obarvit k barvami, právě když je formule F splnitelná. Navíc každému ohodnocení α takové, že $F[\alpha] = 1$ odpovídá jedno barvení.

Formule JUST-ONE. Z výše uvedené konstrukce je užitečná formule

$$\text{JUST-ONE}(\{x_1, x_2, \dots, x_n\}) = (x_1 \vee x_2 \vee \dots \vee x_n) \wedge \left(\bigwedge_{1 \leq i < j \leq n} (\neg x_i \vee \neg x_j) \right).$$

Tato formule je pravdivá jenom pro ohodnocení, které splní právě jednu proměnnou z množiny $\{x_1, x_2, \dots, x_n\}$.

Otázka. Lze podobně transformovat sudoku na splnitelnost formule v CNF?

Ano. Vstupem transformančního algoritmu je částečně doplněná sudoku tabulka o délce strany n . Výsledkem je formule F v CNF.

Zavedeme proměnné x_{ijk} pro $i, j, k = 1, 2, \dots, n$. Ohodnocení proměnné x_{ijk} na 1 značí, že na políčku na pozici i, j je zapsána hodnota k .

Dále pomocí konjunkce JUST-ONE formulí vyjádříme, že v každém sloupci, řádku a podtabulce je každá z hodnot $1, 2, \dots, n$ právě jednou. Ohodnocení, které splní tuto formuli, odpovídá správnému vyplnění tabulky hodnotami.

Počáteční hodnoty v tabulce doplníme pomocí dalších jednoprvkových klausulí. Je-li na pozici i, j hodnota k , dodáme k doposud vytvořené formuli klausuli (x_{ijk}) . $\square$

3 Třetí seminář

Obsah. význam problému splnitelnosti v teorii výpočetní složitosti; sat solvery; rezoluce;

~

Krátce jsme diskutovali složitostní třídy P, NP a roli problému splnitelnosti a (některých) transformací z minulých seminářů v otázce, jestli se tyto třídy rovnají.

~

V dalším se budeme na formuli v CNF dívat jako na množinu klausulí, přičemž klausule je množina literálů. V dalším narazíme na prázdnou množinu ve dvou situacích:

- jako na prázdnou formuli v CNF, tj. formuli neobsahující žádnou klausuli,
- jako na prázdnou klausuli, tj. klausuli neobsahující žádný literál.

Abychom tyto dvě situace odlišily, budeme v prvním případě používat značení $\emptyset$ a v druhém případě $\diamond$.

Otázka. Pro libovolné ohodnocení proměnných α máme $\emptyset[\alpha] = 1$ a $\diamond[\alpha] = 0$. Proč?

Disjunkce je pravdivá, když existuje alespoň jeden pravdivý disjunkt, přitom $\diamond$ nemůže žádný pravdivý disjunkt obsahovat pro žádné ohodnocení. Konjunkce je nepravdivá, pokud existuje alespoň jeden nepravdivý konjunkt. Ovšem $\emptyset$ neobsahuje nepravdivý konjunkt pro žádné ohodnocení, proto musí být pro všechna ohodnocení pravdivá. $\square$

def. Pro formuli F a ohodnocení α definujeme $F[\alpha]$ jako formuli, kterou získáme z F následovně:

- odstraníme všechny klauzule, které obsahují alespoň jeden literál, který α ohodnotí na 1.
- ze zbylých klausulí odstraníme všechny literály, které α ohodnotí na 0.

V případě, že $\text{vars}(\alpha) \supseteq \text{vars}(F)$, je značení zavedené předchozí definicí nejednoznačné. Podle dřívějších definic totiž máme $F[\alpha] \in \{0, 1\}$, ale podle nové definice je $F[\alpha] \in \{\emptyset, \{\diamond\}\}$. O kterou možnost se jedná, vždy poznáme z definice.

def. Nechť C_1, C_2 jsou klauzule a x je proměnná taková, že $x \in C_1$ a $\neg x \in C_2$. Rezolučním pravidlem aplikovaným na x, C_1, C_2 odvodíme klausuli

$$r(x, C_1, C_2) = (C_1 - \{x\}) \cup (C_2 - \{\neg x\}).$$

Této klausuli říkáme *resolventa*, klauzule C_1, C_2 jsou její *rodiče*. (Kromě označení *resolventy*, $r(x, C_1, C_2)$ také říká, že C_1 a C_2 obsahují různé literály proměnné x .)

def. Nechť F je množina klausulí. *Rezolučním odvozením* klauzule C z F je posloupnost klausulí

$$C_1, C_2, \dots, C_m$$

taková, že pro $i = 1, 2, \dots, m$ je buď $C_i \in F$, nebo $C_i = r(x, C_j, C_k)$ pro $j, k < i$; a navíc $C_m = C$. Délka odvození je rovna $m - |F|$.

def. Rezolučnímu odvození $\diamond$ z formule F říkáme *rezoluční zamítnutí* formule F .

Příklad. Mějme $F = \{C_1, C_2, C_3, C_4, C_5\}$, kde

$$\begin{aligned}C_1 &= \{x, \neg z\}, \\C_2 &= \{x, y, z\}, \\C_3 &= \{\neg x, \neg y, \neg z\}, \\C_4 &= \{\neg x, y\}, \\C_5 &= \{\neg y, z\}.\end{aligned}$$

Potom máme

$$\begin{aligned}C_6 &= r(z, C_1, C_2) = \{x, y\}, \\C_7 &= r(x, C_1, C_3) = \{\neg y, \neg z\}, \\C_8 &= r(x, C_6, C_4) = \{y\}, \\C_9 &= r(z, C_7, C_5) = \{\neg y\}, \\C_{10} &= r(y, C_8, C_9) = \diamond.\end{aligned}$$

Posloupnost $C_1, \dots, C_{10}$ je rezolučním zamítnutím F , má délku 5. □

Naším cílem je dokázat následující větu.

Věta 1 (O rezoluci). *Formule F je nesplnitelná, právě když existuje její rezoluční zamítnutí.*

Na promyšlení do příštího semináře jsme si nechali důkaz jedné z implikací ve větě o rezoluci, kterou zachycuje následující lemma.

Lemma 1 (O korektnosti rezoluce). *Pokud existuje rezoluční zamítnutí formule F , je formule F nesplnitelná.*