Matematická logika
Přednáška č. 5

RNDr. Kateřina Trlifajová PhD.

katerina.trlifajova@fit.cvut.cz

Katedra aplikované matematiky
Fakulta informačních technologií

České vysoké učení technické v Praze

BI-MLO, ZS 2015/2016

Domácí úkol – řešení

Uvažujme formuli

$$\Big(\cdots\big(\big(\big((A_1 \downarrow A_2) \Rightarrow A_3\big) \downarrow A_4\big) \Rightarrow A_5\big)\cdots \downarrow A_{2k}\Big) \Rightarrow A_{2k+1},$$

kde k je přirozené číslo.

Pro kolik ohodnocení je tato formule pravdivá?

Řešení:

$$\begin{aligned}
&\nvDash \Big(\cdots\big(\big((\neg(A_1 \vee A_2) \Rightarrow A_3\big) \downarrow A_4\big) \Rightarrow A_5\big)\cdots \downarrow A_{2k}\Big) \Rightarrow A_{2k+1}\\
&\nvDash \Big(\cdots\big(\big((A_1 \vee A_2 \vee A_3) \downarrow A_4\big) \Rightarrow A_5\big)\cdots \downarrow A_{2k}\Big) \Rightarrow A_{2k+1}\\
&\nvDash \Big(\cdots\big(A_1 \vee A_2 \vee A_3 \vee A_4 \vee A_5\big)\cdots \downarrow A_{2k}\Big) \Rightarrow A_{2k+1}\\
&\nvDash A_1 \vee A_2 \vee A_3 \vee A_4 \vee A_5 \cdots \vee A_{2k} \vee A_{2k+1}
\end{aligned}$$

Úplný KNT s jednou klausulí a $2k+1$ prvotními formulemi. Tudíž platí pro $2^{2k+1}-1$ ohodnocení.

Obsah čtvrté přednášky

- Resoluční metoda
- Karnaughovy mapy

Logická ekvivalence a důsledek teorií

Definice

Nechť T a S jsou dvě teorie

- Teorie S je **logickým důsledkem** s teorie T, S **vyplývá** z T, právě když pro každé ohodnocení, které splňují všechny formule z T, je splňují i všechny formule S. Píšeme $T \models S$.
- Teorie T je **logicky ekvivalentní** s teorií S, právě když $T \models S$ a $S \models T$. Píšeme $T \models\!\models S$.

Příklad

(i) Konečné teorie převedeme na konjunkce formulí.
$\{A, B, B \Rightarrow C\} \models\!\models \{A \wedge B, C \vee \neg A\}$, neboť
$A \wedge B \wedge (\neg B \vee C) \models\!\models A \wedge B \wedge C \models\!\models A \wedge B \wedge (C \vee \neg A))$

(ii) Nekonečné teorie, například
$\{A_n \Leftrightarrow A_{n+1}, n \in \mathbb{N}\} \models \{A_n \Rightarrow A_{n+1}, n \in \mathbb{N}\}$, neboť
$A_n \Leftrightarrow A_{n+1} \models A_n \Rightarrow A_{n+1}$

Příklady nekonečných teorií

(i) $T_1 = \{A_n, n \in \mathbb{N}\}$ - splnitelná pro ohodnocení $(1, 1, 1, \cdots)$

(ii) $T_2 = \{A_n \Rightarrow A_{n+1}, n \in \mathbb{N}\}$ - splnitelná pro
$(1, 1, 1, 1 \cdots), (0, 1, 1, 1 \cdots), (0, 0, 1, 1 \cdots), (0, 0, 0, 1 \cdots), \cdots, (0, 0, 0, 0 \cdots)$

(iii) $T_3 = \{A_n \Rightarrow A_{n+1}, A_{n+1} \Rightarrow \neg A_n, n \in \mathbb{N}\}$ - splnitelná pro $(0, 0, 0, 0 \cdots)$

(iv) $T_4 = \{A_n \Rightarrow A_{n+1}, A_{n+1} \Rightarrow \neg A_n, A_1, n \in \mathbb{N}\}$ - nesplnitelná

Příklad: Jedná se o logické důsledky? Jsou tyto teorie ekvivalentní?

- $T_1 \models T_2$
- $T_3 \models T_2$
- $T_3 \models\!\models \{\neg A_n, n \in \mathbb{N}\}$
- $T_4 \models T_1, T_2, T_3$
- Pro která m platí $T_1 \models A_m$? - Všechna.
- Pro která m platí $T_2 \models A_m$? - Žádná.

Teorie a její logické důsledky

Věta

Mějme teorii T a formuli B výrokové logiky.

(i) $T \models B$, *právě když* $T \cup \{\neg B\}$ *není splnitelná.*

(ii) $T \models B$, *právě když* $T \rightleftharpoons T \cup \{B\}$.

(iii) *Nechť* $T \models B$. *Potom* T *je splnitelná, právě když* $T \cup \{B\}$ *je splnitelná.*

(iv) $T \models \bot$, *právě když* T *není splnitelná.*

Důkaz

(i) $T \models B$, právě když pro každé ohodnocení v platí, že jestliže splňuje T, pak $v(B) = 1$, právě když neexistuje ohodnocení, které splňuje T a zároveň $v(B) = 0$, což je právě tehdy, když neexistuje ohodnocení, které splňuje T a zároveň $v(\neg B) = 1$, což je právě když $T \cup \{\neg B\}$ není splnitelná.

(ii) Nechť $T \models B$. Potom také $T \models T$, tedy $T \models T \cup \{B\}$. Na druhou stranu jistě $T \cup \{B\} \models T$.
Nechť nyní $T \rightleftharpoons T \cup \{B\}$, pak jistě $T \models T \cup \{B\}$, tedy i $T \models B$.

(iii) Podle (ii) $T \rightleftharpoons T \cup \{B\}$. Tedy jsou splnitelné pro stejná ohodnocení.

(iv) Podle (ii) $T \models \bot$, právě když $T \rightleftharpoons T \cup \{\bot\}$, právě když T není splnitelná.

Resoluční metoda

Vycházíme z KNT, hledáme jednoduché logické důsledky plynoucí z klausulí.

Věta

Nechť T je teorie. Potom k ní existuje ekvivalentní teorie T', $T \rightleftarrows T'$, taková, že všechny její formule jsou klausule.

Důkaz. Ke každé formuli existuje KNT, užijeme všechny klausule všech formulí.

Tvrzení

Pro libovolné formule A, B, C platí

i) $A \wedge (\neg A \vee B) \models B$

ii) $(A \vee B) \wedge (\neg A \vee C) \models (B \vee C)$

iii) $A \wedge \neg A \models \bot$.

Důkaz

i) $A \wedge (\neg A \vee B) \wedge \neg B$ je kontradikce,

ii) $(A \vee B) \wedge (\neg A \vee C) \wedge \neg(B \vee C)$ je kontradikce.

iii) $A \wedge \neg A \rightleftarrows \bot$.

Resolventy a resloučení obal

Definice

Logický důsledek dvou klausulí, který odvodíme způsobem popsaným v předchozí větě, se nazývá **resolventa**. Označme **resoluční obal** $\mathcal{R}(T) = T \cup$ resolventy vzniklé z T, přičemž přidané resolventy můžeme využívat k vytváření ostatních.

Příklad. Nechť $T = \{A \Rightarrow B, C \Rightarrow D, A \vee C\} \rightleftarrows \{\neg A \vee B, \neg C \vee D, A \vee C\}$

- $\neg A \vee B, A \vee C \vDash B \vee C$
- $\neg C \vee D, A \vee C \vDash A \vee D$
- $A \vee D, \neg A \vee B \vDash B \vee D$
- $\mathcal{R}(T) = T \cup \{B \vee C, A \vee D, B \vee D\}$

Resoluční metoda

Tvrzení

Nechť T je teorie.

- *$\mathcal{R}(T)$ je logicky ekvivalentní s T, $\mathcal{R}(T) \models\!\!\models T$.*
- *Je-li T konečná, pak $\mathcal{R}(T)$ je též konečná množina.*

Důkaz

Po konečně krocích se počet resolvent stabilizuje. Existuje totiž jen konečně mnoho navzájem různých klauzulí nad konečně mnoha literály z formulí v T. □

Věta (Herbrandova)

Konečná množina klauzulí T je splnitelná právě tehdy, když její resoluční obal $\mathcal{R}(T)$ neobsahuje kontradikci.

Resoluční metoda - příklad I.

Příklad

Určete, zda je množina $\{(A \Rightarrow B), (B \Rightarrow C), (C \Rightarrow D), (D \Rightarrow \neg A), A\}$ splnitelná.

Klausule: $(\neg A \vee B), (\neg B \vee C), (\neg C \vee D), (\neg D \vee \neg A), A$

Resolventy:

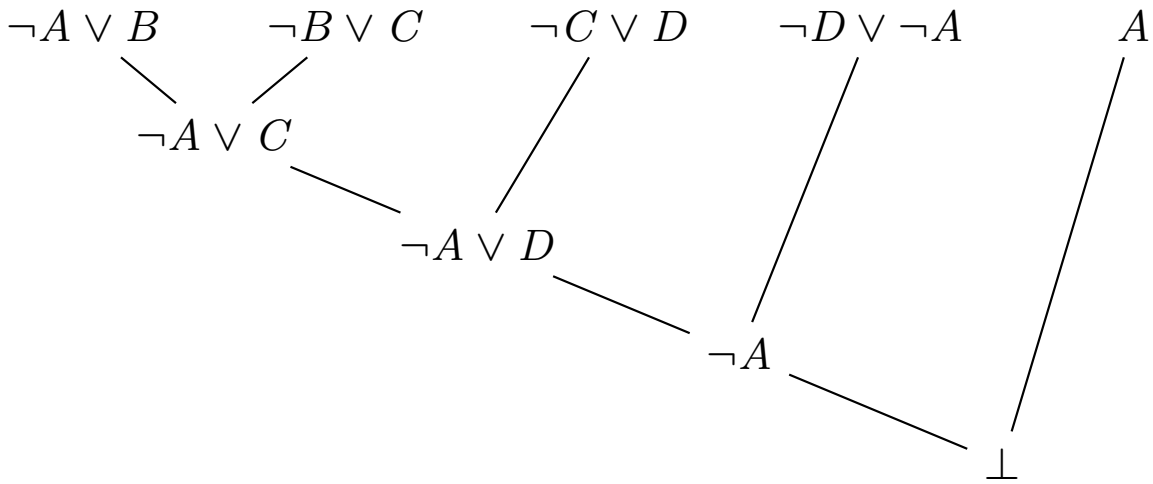
i) $(\neg A \vee B), (\neg B \vee C) \models \neg A \vee C$,

ii) $(\neg A \vee C), (\neg C \vee D) \models \neg A \vee D$,

iii) $(\neg A \vee D), (\neg D \vee \neg A) \models \neg A$,

iv) $\neg A, A \models \bot$. Tedy $\bot \in \mathcal{R}(T)$.

$T \cup \{\neg A \vee C, \neg A \vee D, \neg A, \bot\} \subseteq \mathcal{R}(T)$, tedy T není splnitelná.

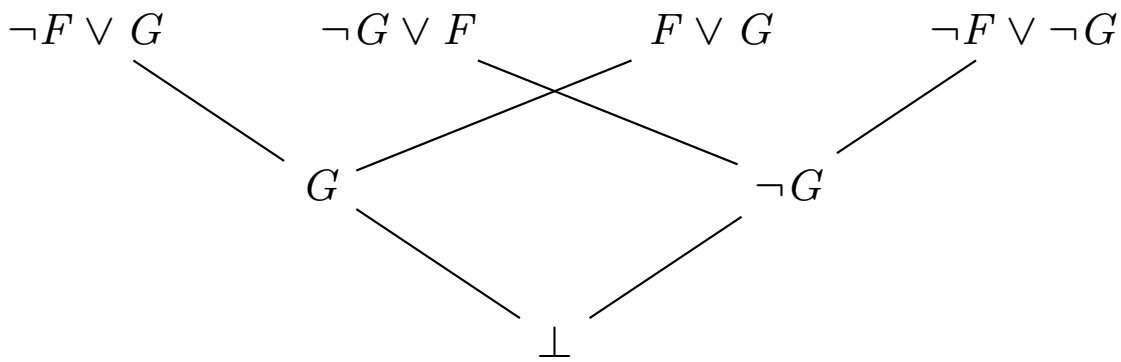


Resoluční metoda - příklad II.

Příklad

Ukažte, že platí $F \Leftrightarrow G, F \vee G \models F \wedge G$.

Upravíme: $(F \Rightarrow G) \wedge (G \Rightarrow F) \wedge (F \vee G) \models F \wedge G$
Zajímá nás: Je $T = (\neg F \vee G) \wedge (\neg G \vee F) \wedge (F \vee G) \wedge (\neg F \vee \neg G)$ splnitelná?



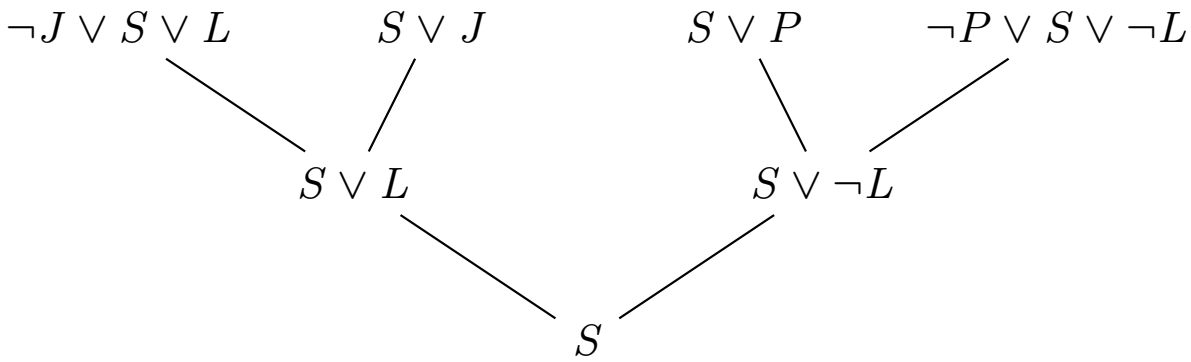
$\mathcal{R}(T) = \{\neg F \vee G, \neg G \vee F, F \vee G, \neg F \vee G, \neg G, F, \neg F, \bot\}$ není splnitelná, tedy platí!

Resoluční metoda - příklad III.

Příklad

Jestliže Jones nepotkal Smithe (J), pak Smith je vrahem (S) nebo Jones lže (L). Jestli Smith není vrahem, pak ho Jones nepotkal a vražda se stala po půlnoci (P). Jestli se vražda stala po půlnoci, pak byl Smith vrahem nebo Jones mluví pravdu. Co se tedy stalo?

Teorie: $J \Rightarrow (S \vee L), \neg S \Rightarrow (J \wedge P), P \Rightarrow (S \vee \neg L)$



$\mathcal{R}(T) = \{\neg J \vee S \vee L, S \vee J, S \vee P, \neg P \vee S \vee \neg L, S \vee L, S \vee \neg L, S, \neg J \vee S \vee \neg P, S \vee \neg J, \neg P \vee S\}$
- Smith je vrahem.

Resoluční metoda - příklad IV.

Příklad

Buď svědek mluvil pravdu nebo, jestli Henry spáchal sebvraždu, pak se zápisky nenašly. Jestli svědek mluvil pravdu, pak Henry nespáchal sebvraždu. Jestli se zápisky nalezly, pak se Henry zabil. Je to splnitelná množina formulí? Co je její logický důsledek?

Teorie: $S \vee (H \Rightarrow \neg Z), S \Rightarrow \neg H, Z \Rightarrow H$
Zajímá nás: $(S \vee \neg H \vee \neg Z) \wedge (\neg S \vee \neg H) \wedge (\neg Z \vee H)$

- $(\neg S \vee \neg H) \wedge (\neg Z \vee H) \models (\neg S \vee \neg Z)$
- $(S \vee \neg H \vee \neg Z) \wedge (\neg S \vee \neg Z) \models (\neg H \vee \neg Z)$
- $(\neg H \vee \neg Z) \wedge (\neg Z \vee H) \models \neg Z$

$\mathcal{R}(T) = \{S \vee \neg H \vee \neg Z, \neg S \vee \neg H, \neg Z \vee H, \neg S \vee \neg Z, \neg H \vee \neg Z, S \vee \neg Z, \neg Z\}$

Zápisky se nenašly.

P versus NP problém

Výpočetní složitost.

- P-problém: existuje algoritmus, který nalezne řešení v polynomiálním čase.
- NP-problém: existuje algoritmus, který ověří řešení v polynomiálním čase.

Platí $P \subseteq NP$, ale platí též $P = NP$?

Příklad

Existuje k dané množině celých čísel její podmnožina taková, že součet čísel v ní obsažených je 0?

Například pro množinu $\{-2, -3, 15, 14, 7, -10\}$ to je $\{-2, -3, 15, -10\}$.

- Známý algoritmus má $2^n - 1$ kroků.
- Lehko ověříme dosazením. NP-problém.

SAT problém

SAT problém - problém splnitelnosti *(satisfiability)* formule výrokové logiky .

- tabulková metoda
- sémantické stromy
- resoluční metoda

NP-úplný problém: NP-problém, na nějž může být převedeno (resp. na nějž lze v polynomiálním čase redukovat pomocí deterministického Turingova stroje) řešení všech ostatních NP-problémů.

Věta Cook-Levinova věta

SAT problém je NP-úplný.

P = NP

Millennium Prize Problems, Clay Mathematics Institute, 2000, 1.000.000 US$

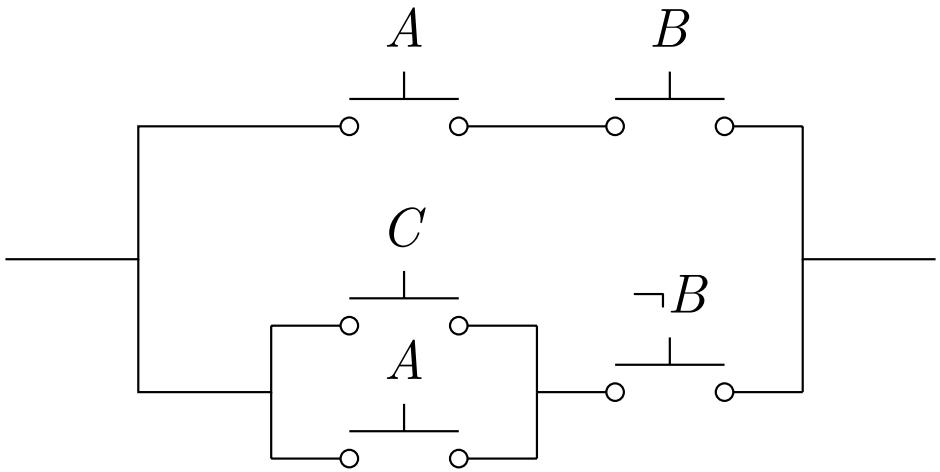
Minimální DNT

Definice

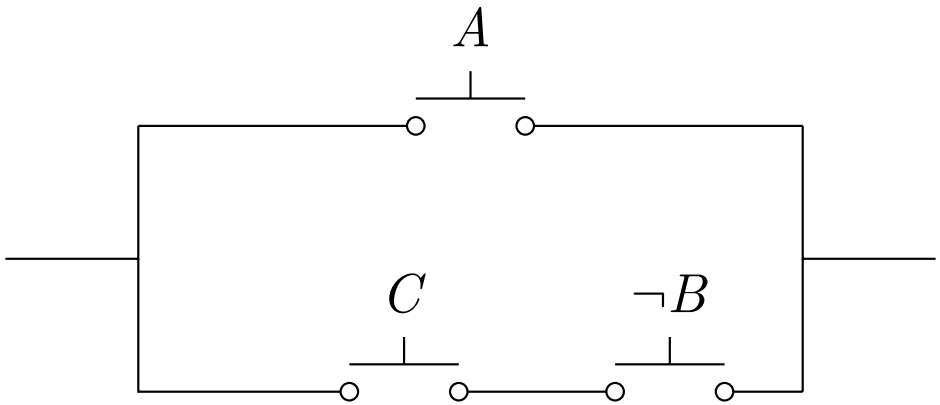
Disjunktivní tvar je **minimální**, právě když žádný jiný ekvivalentní disjunktivní tvar nemá méně mintermů nebo méně literálů.

- $(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C)$
- $(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge \neg C) \bowtie (\neg B \wedge \neg C)$
- $(A \wedge B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \bowtie (B \wedge \neg C)$
- $(\neg B \wedge \neg C) \vee (B \wedge \neg C) \bowtie \neg C$
- $(A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \bowtie (A \wedge B)$
- $(A \wedge B) \vee \neg C$

Elektrické obvody



Zapojení obvodu $(A \wedge B) \vee ((A \vee C) \wedge \neg B) \rightleftharpoons (A \wedge B) \vee (A \wedge \neg B) \vee (C \wedge \neg B)$
Minimalizace $\rightleftharpoons A \vee (C \wedge \neg B)$



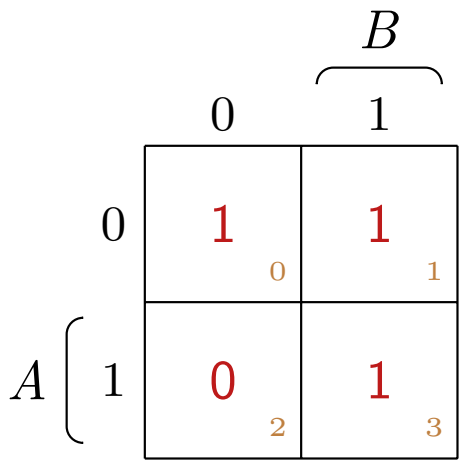
Karnaughova mapa pro 2 prvotní formule

Sestrojíme Karnaughovu mapu $A \Rightarrow B$.

Pravdivostní tabulka:

dec. index	A	B	$A \Rightarrow B$
0	0	0	1
1	0	1	1
2	1	0	0
3	1	1	1

Karnaughova mapa:



Formule odpovídá funkci $f(A, B) = \sum(0, 1, 3)$.

Úplné DNT: $(\neg A \wedge \neg B) \vee (\neg A \wedge B) \vee (A \wedge B)$

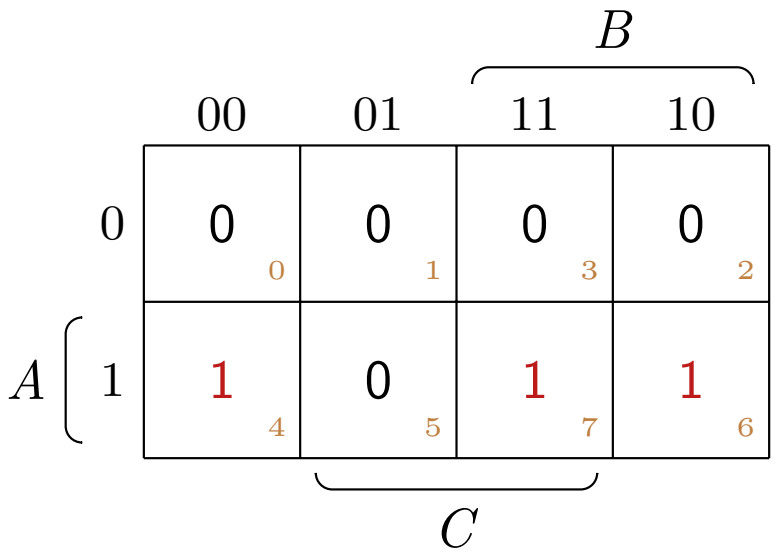
Karnaughova mapa pro 3 prvotní formule

Sestrojíme Karnaughovu mapu formule $\neg\big(A \Rightarrow (\neg B \wedge C)\big)$.

Pravdivostní tabulka:

dec.	A	B	C	$\neg\big(A \Rightarrow (\neg B \wedge C)\big)$
0	0	0	0	0
1	0	0	1	0
2	0	1	0	0
3	0	1	1	0
4	1	0	0	1
5	1	0	1	0
6	1	1	0	1
7	1	1	1	1

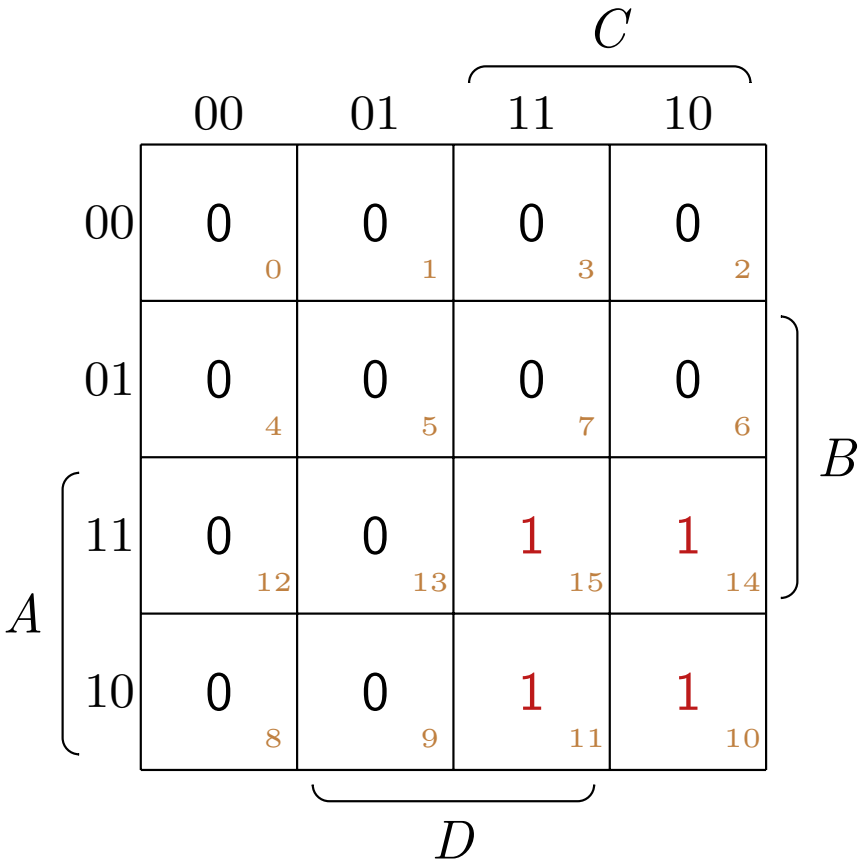
Karnaughova mapa:



Úplné DNT: $(A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$ nebo $\sum(4, 6, 7)$

Karnaughova mapa pro 4 prvotní formule

Sestrojíme Karnaughovu mapu formule $A \wedge C$ jako funkci prvotních formulí A, B, C a D.

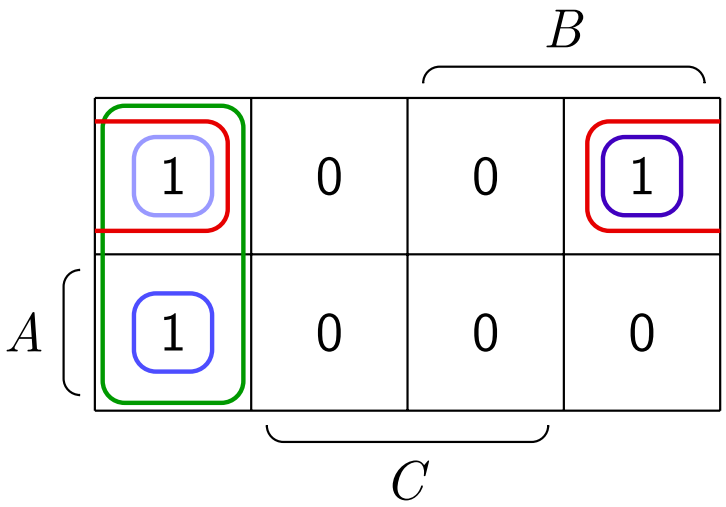


$(A \wedge B \wedge C \wedge D) \vee (A \wedge B \wedge C \wedge \neg D) \vee (A \wedge \neg B \wedge C \wedge D) \vee (A \wedge \neg B \wedge C \wedge \neg D)$

$\sum(10, 11, 14, 15)$

Karnaughovy množiny - příklad 1.

Karnaughova množina je skupina buněk v Karnaughově mapě, která odpovídá mintermu. Karnaughova množina má vždy tvar obdélníku, jehož každá strana obsahuje 2^k buněk.



Karnaughovy množiny pokrývající 1 buňku:

- $\neg A \wedge \neg B \wedge \neg C$
- $A \wedge \neg B \wedge \neg C$
- $\neg A \wedge B \wedge \neg C$

Karnaughovy množiny pokrývající 2 buňky:

- $\neg B \wedge \neg C$
- $\neg A \wedge \neg C$

Úplné DNT: $\bowtie (\neg A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C)$

Minimální DNT: $\bowtie (\neg B \wedge \neg C) \vee (\neg A \wedge \neg C)$

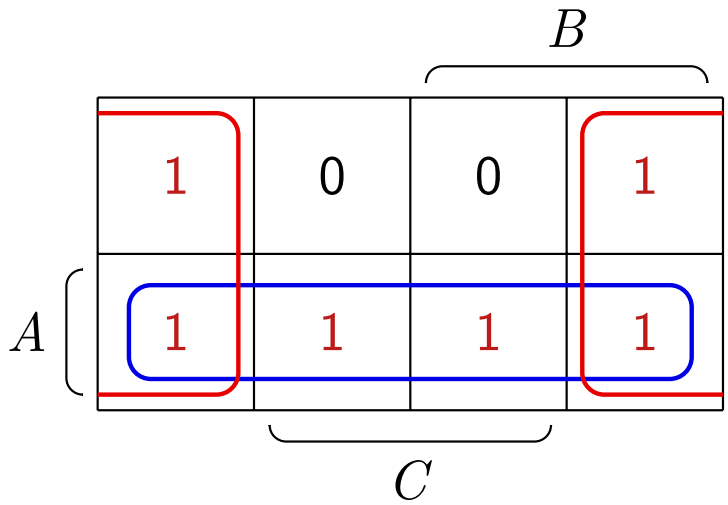
Minimální DNT získáme pokrytím všech 1 co největšími Karnaughovými množinami, které se mohou překrývat.

Karnaughovy množiny - příklad 2.

Příklad

Nalezněte minimální DNT formule $\neg(A \Rightarrow B) \vee (A \Leftrightarrow C) \vee (A \wedge B \wedge \neg C)$.

Upravíme: $(A \wedge \neg B) \vee (A \wedge C) \vee (\neg A \wedge \neg C) \vee (A \wedge B \wedge \neg C)$

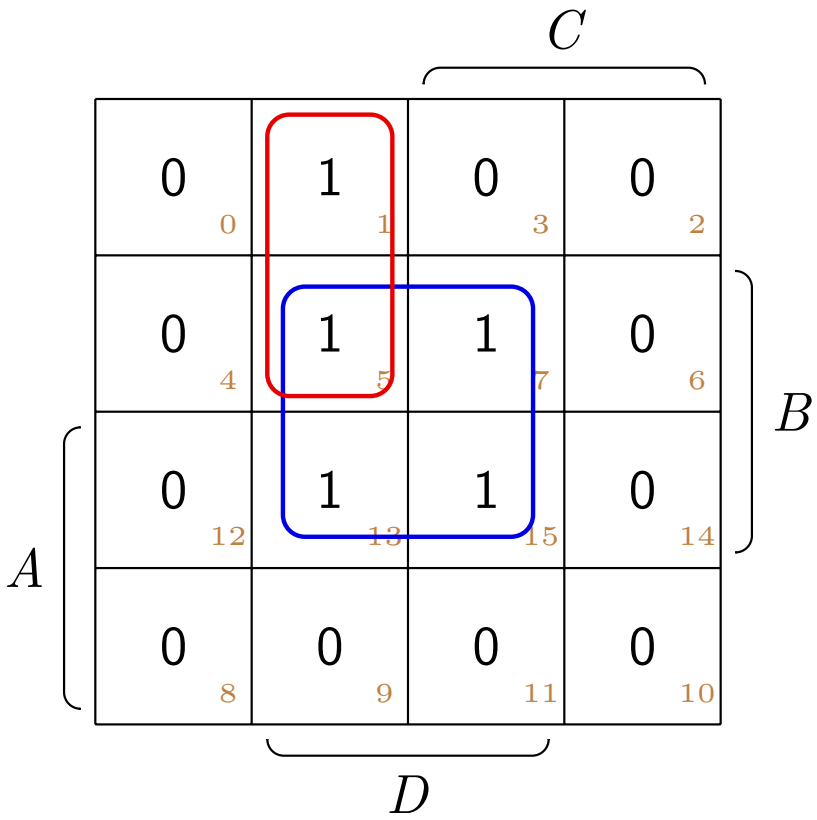


Minimální DNT: $\bowtie A \vee \neg C$ To je vlastně $C \Rightarrow A$

Karnaughovy množiny - příklad 3.

Příklad

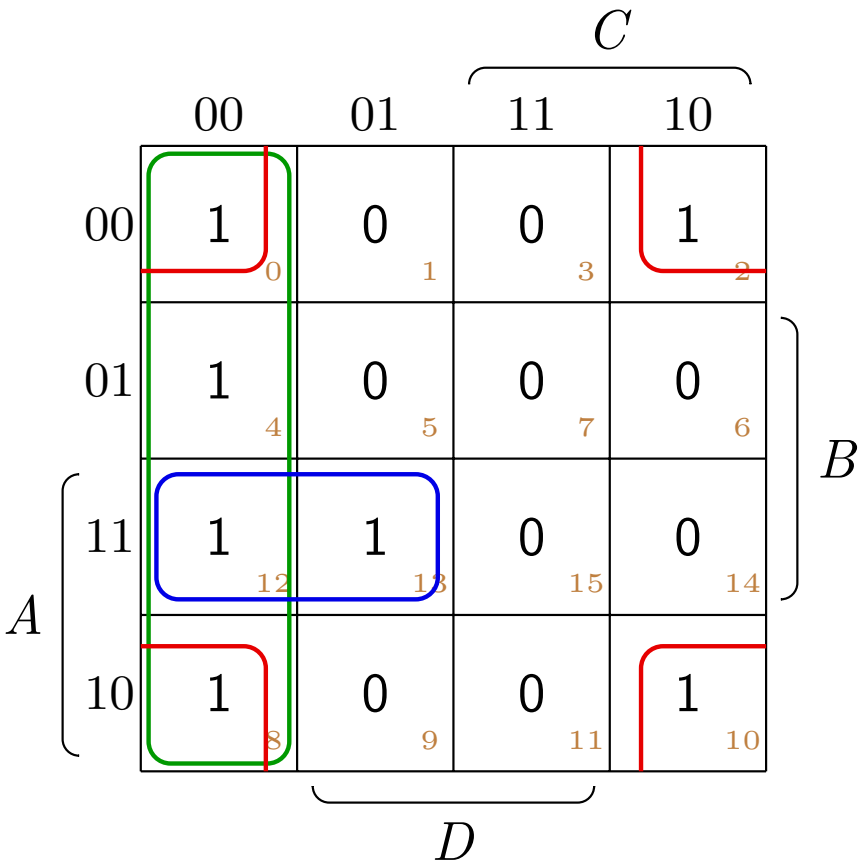
Nalezněte minimální DNT Booleovy funkce $\sum(1, 5, 7, 13, 15)$.



Minimální DNT: $(B \wedge D) \vee (\neg A \wedge \neg C \wedge D)$

Karnaughova mapa - příklad 4.

Nalezněte minimální DNT formule $\sum(0, 2, 4, 8, 10, 12, 13)$.



Minimální DNT: $(\neg C \wedge \neg D) \vee (\neg B \wedge \neg D) \vee (A \wedge B \wedge \neg C)$

Karnaughovy množiny pro 4 prvotní formule

Pro formuli se 4 prvotními formulemi:

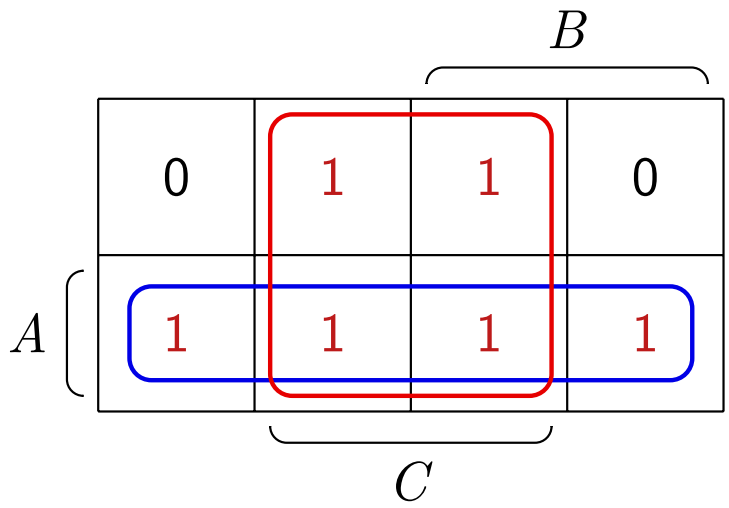
- 1 buňka - minterm se 4 literály - minterm úplného DNT.
- 2 buňky - minterm se 3 literály
- 4 buňky - minterm se 2 literály
- 8 buněk - minterm se 1 literály
- 16 buněk (celá tabulka) - tautologie

Karnaughova mapa - příklad 5.

Příklad

Nalezněte minimální KNT formule $\neg A \wedge (A \Leftrightarrow C)$.

Upravíme: $\neg A \wedge (A \vee \neg C) \wedge (\neg A \vee C)$
Hledáme minimální DNT negace formule, tj. $A \vee (\neg A \wedge C) \vee (A \wedge \neg C)$



Minimální DNT negace: $\dashv\vdash A \vee C$
Minimální KNT formule $\dashv\vdash \neg A \wedge \neg C$

Domácí úkol

Nechť $\{A_1, A_2, \cdots\}$ je množina prvotních formulí. Pro která ohodnocení je splněna teorie

$$\mathcal{T} = \{A_n \Rightarrow \neg(A_{n+1} \wedge A_{n+2}), \neg A_n \Rightarrow (A_{n+1} \vee A_{n+2}), \neg A_{n+2} \Rightarrow A_n\}$$