Matematická logika
Přednáška č. 11

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

Rozhodněte a zdůvodněte, zda platí

$$((\exists x)p(x) \Rightarrow (\exists x)q(x)) \models (\exists x)(p(x) \Rightarrow q(x))$$

$$((\forall x)\neg p(x) \vee (\exists x)q(x)) \models (\exists x)(\neg p(x) \vee q(x))$$

$$((\forall x)\neg p(x) \vee (\exists x)q(x)) \wedge (\forall x)(p(x) \wedge \neg q(x))$$

$$((\forall x)\neg p(x) \vee (\exists x)q(x)) \wedge (\forall x)p(x) \wedge (\forall x)\neg q(x)$$

Kontradikce. Tedy se jedná o logický důsledek.

Booleova algebra

Definice

Teorie **Booleových algeber** je v jazyce $L = \{+, \cdot, ', 0, 1, =\}$, kde průsek $\cdot$ a spojení $+$ jsou binární funkce, doplněk $'$ je unární funkce, nejmenší prvek 0 a největší prvek 1 jsou konstanty, $=$ je binární predikát rovnosti.

i) $x + y = y + x$ – komutativní zákony
$x \cdot y = y \cdot x$

ii) $(x + y) + z = x + (y + z)$ – asociativní zákony
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

iii) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ – distributivní zákony
$(x \cdot y) + z = (x + z) \cdot (y + z)$

iv) $x + 0 = x$ – zákony neutrality
$x \cdot 1 = x$

v) $x \cdot x' = 0$ – zákony komplementarity
$x + x' = 1$

Booleova algebra výrokové logiky

Příklad

Nechť S je množina výrokových formulí nad n prvotními formulemi. Spojení $+$ inerpretujeme jako $\vee$, průsek $\cdot$ jako $\wedge$, doplněk $'$ jako $\neg$, konstanty 0 a 1 jako $\bot$ a $\top$ a rovnost jako $\leftrightarrows$. Potom $(S, \vee, \wedge, \neg, \bot, \top, \leftrightarrows)$ je modelem Booleovy algebry.

Důkaz

Pro každé tři formule A, B, C platí:

i) $A \vee B \leftrightarrows B \vee A$ – komutativní zákony
$A \wedge B \leftrightarrows B \wedge A$

ii) $(A \vee B) \vee C \leftrightarrows A \vee (B \vee C)$ – asociativní zákony
$(A \wedge B) \wedge C \leftrightarrows A \wedge (B \wedge C)$

iii) $(A \vee B) \wedge C \leftrightarrows (A \wedge C) \vee (B \wedge C)$ – distributivní zákony
$(A \wedge B) \vee C \leftrightarrows (A \vee C) \wedge (B \vee C)$

iv) $A \vee \bot \leftrightarrows A$ – zákony neutrality
$A \wedge \top \leftrightarrows A$

v) $A \wedge \neg A \leftrightarrows \bot$ – zákony komplementarity
$A \vee \neg A \leftrightarrows \top$

□

Princip duality

Princip duality

Jestliže v Booleově algebře vzájemně zaměníme operace $+$ a $\cdot$ a konstanty 0 a 1, dostaneme opět Booleovu algebru.

Důkaz

Plyne přímo z definice. Všechny axiomy tvoří páry, které jsou zjevně invariantní vůči této záměně. □

Poznámka: Platit budou též všechny odvozené vlastnosti.

Vlastnosti Booleovy algebry

Tvrzení

V Booleově algebře pro každé $x, y \in S$ platí:

i) *doplněk x' je zákony komplementarity určen jednoznačně,*

ii) $x'' = x$ – *zákon dvojí negace*

iii) $x + x = x$ – *idempotence $+$ a $\cdot$*
$x \cdot x = x$

Poznámka: V souladu se zavedenými konvencemi budeme v zápisech uvažovat prioritu $\cdot$ před $+$. Výraz $x \cdot y + z$ tedy znamená $(x \cdot y) + z$.

Důkaz

i) Nechť x_1' splňuje stejné vlastnosti komplementarity k prvku x jako x' (tj. $x \cdot x_1' = 0$ a $x + x_1' = 1$).Potom
$x_1' = x_1' \cdot 1 = x_1' \cdot (x + x') = x_1' \cdot x + x_1' \cdot x' = x_1' \cdot x' = x' \cdot x_1' + x' \cdot x = x' \cdot (x_1' + x) = x'$

ii) $x' \cdot x'' = 0 = x' \cdot x$ a $x' + x'' = 1 = x' + x$.To znamená, že x splňuje stejné vlastnosti komplementarity k x' jako jeho doplněk x''. Tudíž $x'' = x$.

iii) $x = x + 0 = x + x \cdot x' = (x + x) \cdot (x + x') = (x + x) \cdot 1 = x + x$
$x = x \cdot 1 = x \cdot (x + x') = x \cdot x + x \cdot x' = x \cdot x + 0 = x \cdot x$

□

Vlastnosti Booleovy algebry

Tvrzení

V Booleově algebře pro každé $x, y \in S$ platí:

iv) $x + 1 = 1$
$x \cdot 0 = 0$

v) $x + (x \cdot y) = x$ – *zákony absorpce*
$x \cdot (x + y) = x$

vi) $(x + y)' = (x' \cdot y')$ – *de Morganovy zákony*
$(x \cdot y)' = (x' + y')$

Důkaz

iv) $x + 1 = x + x + x' = x + x' = 1$
$x \cdot 0 = x \cdot x \cdot x' = x \cdot x' = 0$

v) $x + x \cdot y = x \cdot (1 + y) = x \cdot 1 = x$
$x \cdot (x + y) = (x + 0) \cdot (x + y) = x + 0 \cdot y = x$

vi) $(x + y)(x' \cdot y') = x \cdot x' \cdot y' + y \cdot x' \cdot y' = 0 \cdot y' + 0 \cdot x' = 0.$
$(x + y) + x' \cdot y' = x + (y + x') \cdot (y + y') = x + (y + x') \cdot 1 = x + x' + y = 1 + y = 1$
To znamená, že $x' \cdot y'$ splňuje stejné vlastnosti komplementarity k $(x + y)$ jako jeho doplněk $(x + y)'$. Tudíž $(x + y)' = x' \cdot y'$.

Počítání v Booleově algebře

Příklad

Zjednodušte následující zápisy výrazů Booleovy algebry tak, aby obsahovaly co nejméně symbolů:

- $abc + \big(b'(a' + c)\big)' = abc + b + (a' + c)' = b + ac'$
- $\big((a' + 1)' + (a + 0)\big)' = (1' + a)' = (0 + a)' = a'$
- $ab'c' + ab'c + abc' + abc = ab'(c + c') + ab(c + c') = ab' + ab = a$

Uspořádání Booleovy algebry

Tvrzení

Pro každé dva prvky x a y Booleovy algebry platí:
$x + y = y$ *právě tehdy, když* $x \cdot y = x$.

Důkaz

S využitím zákonů absorbce dostaneme:

- $\Rightarrow$: $x \cdot y = x \cdot (x + y) = x$.
- $\Leftarrow$: $x + y = x \cdot y + y = y$

□

Definice

Uspořádání na Booleově algebře definujeme takto:

$$x \leq y \quad \text{právě když} \quad x + y = y$$

což je ekvivalentní $x \cdot y = x$.

Vlastnosti uspořádání BA

Tvrzení

Pro každé tři prvky x, y, z Booleovy algebry platí

i) $x \cdot y \leq x, x \leq x + y.$

ii) $0 \leq x, x \leq 1.$

iii) *Uspořádání $\leq$ je částečné uspořádání*

(a) $x \leq x$ – *reflexivita*

(b) $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$ – *transitivita*

(c) $(x \leq y \wedge y \leq x) \Rightarrow x = y$ – *slabá antisymetrie*

Důkaz

i) $(x \cdot y) \cdot x = x \cdot y$, $x + (x + y) = x + y.$

ii) $0 \cdot x = 0$, $x \cdot 1 = x$

iii) (a) $x \leq x$, právě když $x + x = x$.

(b) Jestliže $x \leq y$ a $y \leq z$, pak $x + y = y$ a $y + z = z$, tedy $x + z = x + (y + z) = (x + y) + z = y + z = z$. Tedy $x \leq z$.

(c) Jestliže $x \leq y$ a zároveň $y \leq x$, pak $x + y = y$ a zároveň $y + x = x$. Tedy $x = y + x = x + y = y$.

Infimum a supremum

Definice

Nechť x, y jsou dva prvky Booleovy algebry. Pak definujeme

- $z = \inf\{x, y\}$, **infimum**, největší dolní závora, právě když
  $(z \leq x \wedge z \leq y) \wedge ((\forall u)(u \leq x \wedge u \leq y) \Rightarrow u \leq z)$
- $z = \sup\{x, y\}$, **supremum**, nejmenší horní závora, právě když
  $(x \leq z \wedge y \leq z) \wedge ((\forall u)(x \leq u \wedge y \leq u) \Rightarrow z \leq u)$

Tvrzení

Nechť $x, y \in S$ jsou dva prvky Booleovy algebry. Potom

$$\inf\{x, y\} = x \cdot y \quad \textit{a} \quad \sup\{x, y\} = x + y.$$

Důkaz

- Určitě $(x \cdot y \leq x) \wedge (x \cdot y \leq y)$. Jestliže $(u \leq x) \wedge (u \leq y)$, pak $(u \cdot x = u) \wedge (u \cdot y = u)$, tedy $u \cdot x \cdot y = u$ a tedy $\Rightarrow (u \leq x \cdot y)$.
- Analogicky.

Atomy

Definice

Minimální prvky různé od 0 nazýváme **atomy**. Tj. a je **atom**, právě když

$$\neg(a = 0) \wedge (\forall b)(b \leq a \Rightarrow (b = 0 \vee b = a).$$

Booleova algebra $\{0, 1\}$

Příklad

$S = \{0, 1\}$. Operace jsou definovány jako logické operátory následujícími tabulkami:

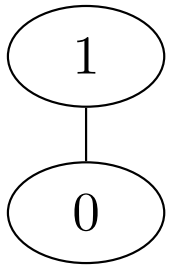
$+$	1	0
1	1	1
0	1	0

$\cdot$	1	0
1	1	0
0	0	0

x	x'
1	0
0	1

Nejmenší prvek je 0 a největší prvek je 1.

- Uspořádání: $0 \leq 1$.
- Atom: $\{1\}$.
- Počet prvků S: $|S| = 2$.



Booleova algebra $\{0,1\}^n$

Příklad

$$S = \{0,1\}^n = \underbrace{\{0,1\} \times \{0,1\} \times \ldots \{0,1\}}_{n \text{ krát}} = \{\langle x_1, \ldots, x_n \rangle | x_1, \ldots, x_n \in \{0,1\}\}.$$

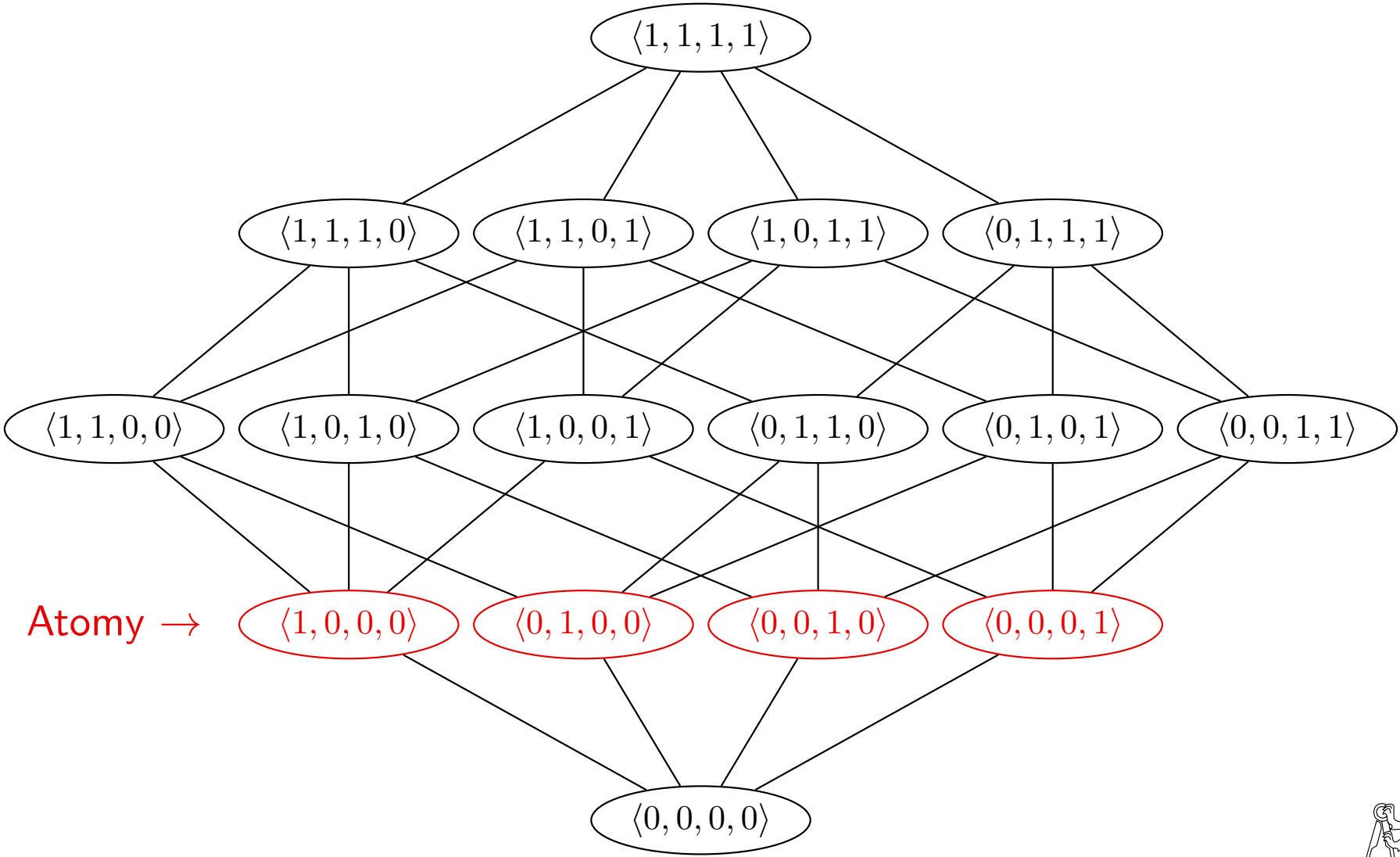
Funkce jsou definovány jako logické operátory po složkách:

- $\langle x_1, x_2, \ldots, x_n \rangle + \langle y_1, y_2, \ldots, y_n \rangle = \langle x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n \rangle$
- $\langle x_1, x_2, \ldots, x_n \rangle \cdot \langle y_1, y_2, \ldots, y_n \rangle = \langle x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n \rangle$
- $\langle x_1, x_2, \ldots, x_n \rangle' = \langle x_1', x_2', \ldots, x_n' \rangle$

Nejmenší prvek: $0 = \langle 0,0,0,0,0 \rangle$.
Největší prvek: $1 = \langle 1,1,1,1,1 \rangle$.

- Uspořádání: $\left(\langle a_1, \ldots, a_n \rangle \leq \langle b_1, \ldots, b_n \rangle\right) \Leftrightarrow (\forall i = 1, \ldots, n)(a_i \leq b_i)$.
- Atomy: $\{\langle 1,0,...,0 \rangle, \langle 0,1,...,0 \rangle, \ldots, \langle 0,0,...,1 \rangle\}$.
  Počet atomů: n.
- Počet prvků v S: $|S| = 2^n$.

Příklad – Booleova algebra $\{0,1\}^4$



Booleova algebra $P(M)$

Příklad

Nechť M je množina. Množina všech podmnožin $P(M)$ (potenční množina) množiny M je $P(M) = \{a | a \subseteq M\}$.

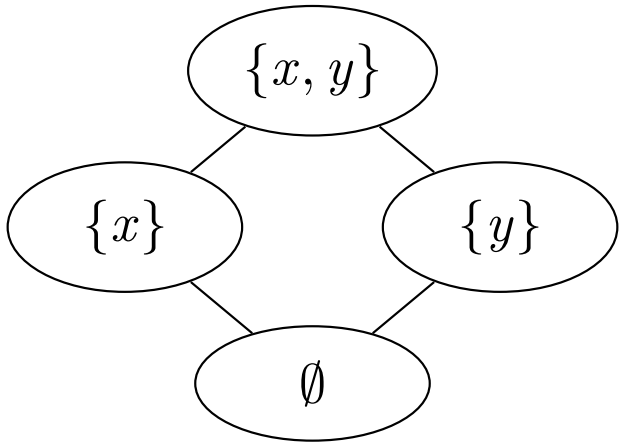
Zaveďme Booleovu algebru na $S = P(M)$:

- $a + b = a \cup b$
- $a \cdot b = a \cap b$
- $a' = M \setminus a$
- Nejmenší prvek: $\emptyset$
- Největší prvek: M

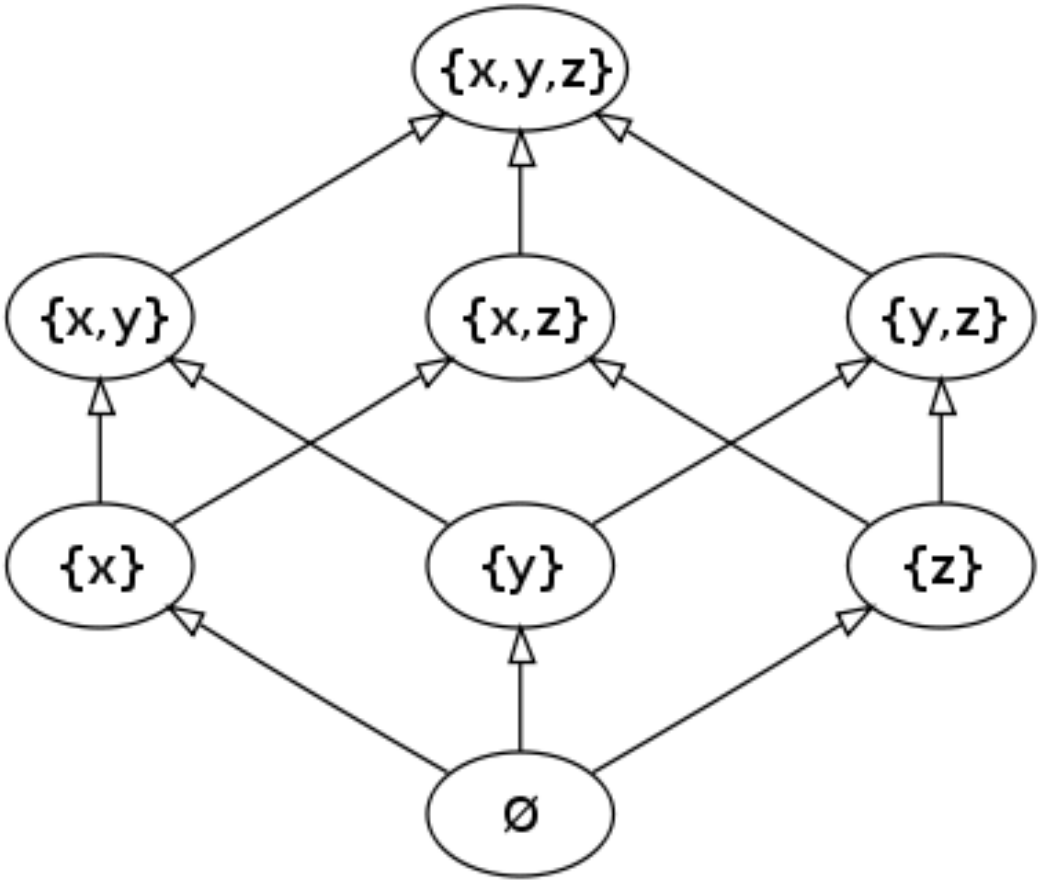
- Uspořádání: $(a \leq b) \Leftrightarrow \big((a \cap b) = a\big) \Leftrightarrow (a \subseteq b)$
- Atomy: jednoprvkové podmnožiny M.
  Počet atomů: $|M|$
- Počet prvků v BA: $|P(M)| = 2^{|M|}$

Příklad – Booleova algebra $P(M)$ pro $M = \{x, y\}$

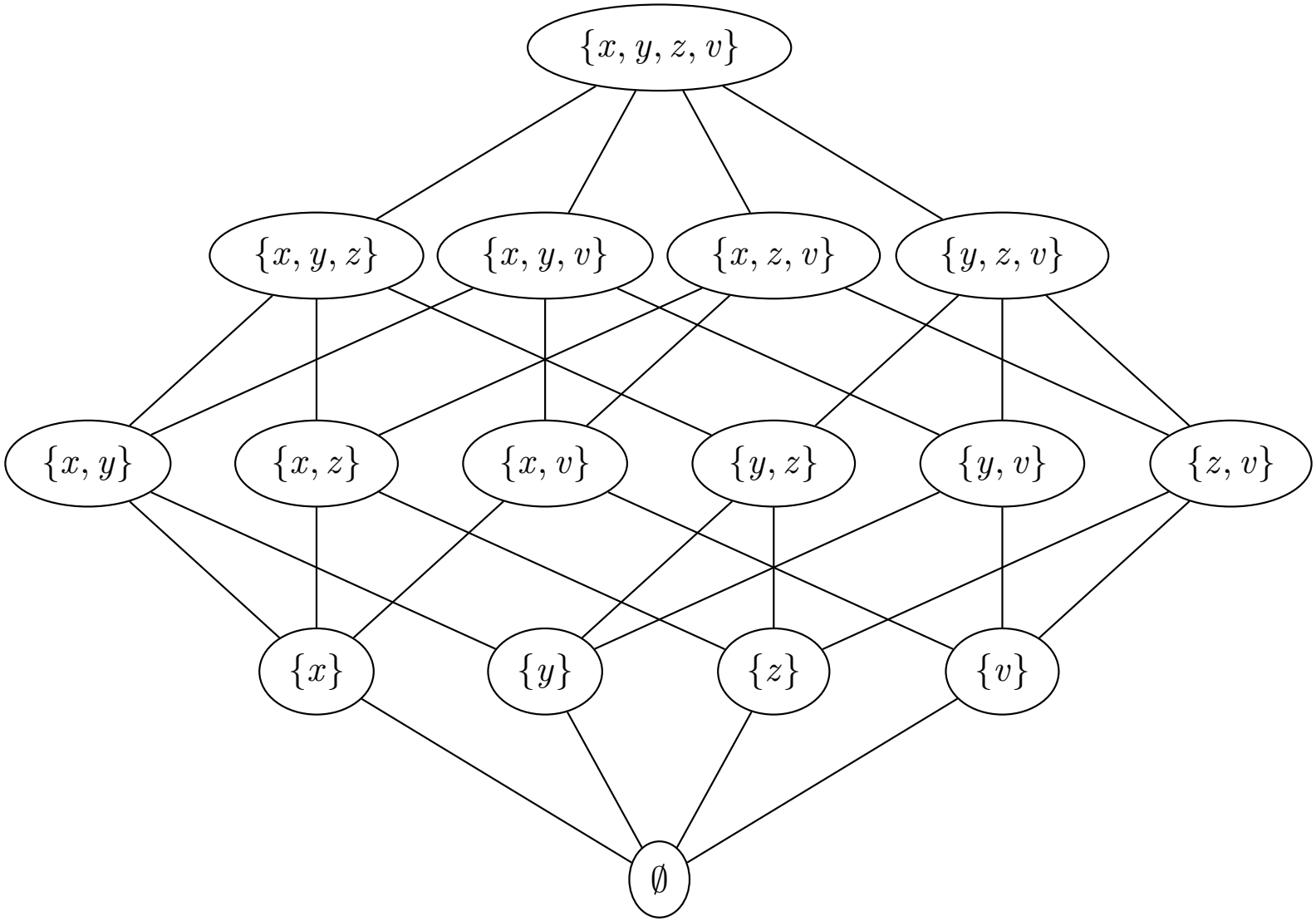
$$P(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$$



Příklad – Booleova algebra $P(M)$ pro $M = \{x, y, z\}$



Příklad – Booleova algebra $P(M)$ pro $M = \{x, y, z, v\}$



Booleova algebra výrokové logiky

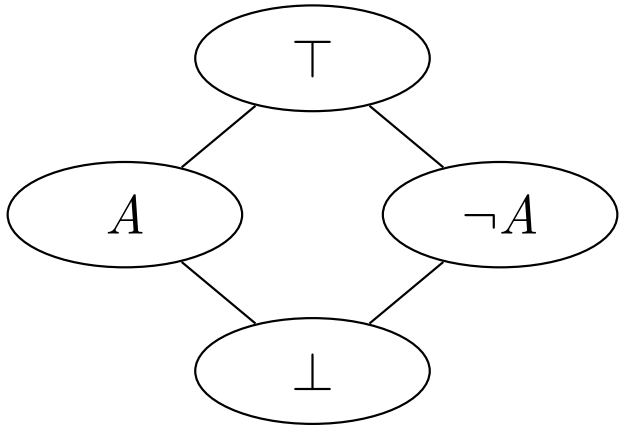
Příklad

$S =$ množina výrokových formulí nad prvotními formulemi $\{A_1, ..., A_n\}$.

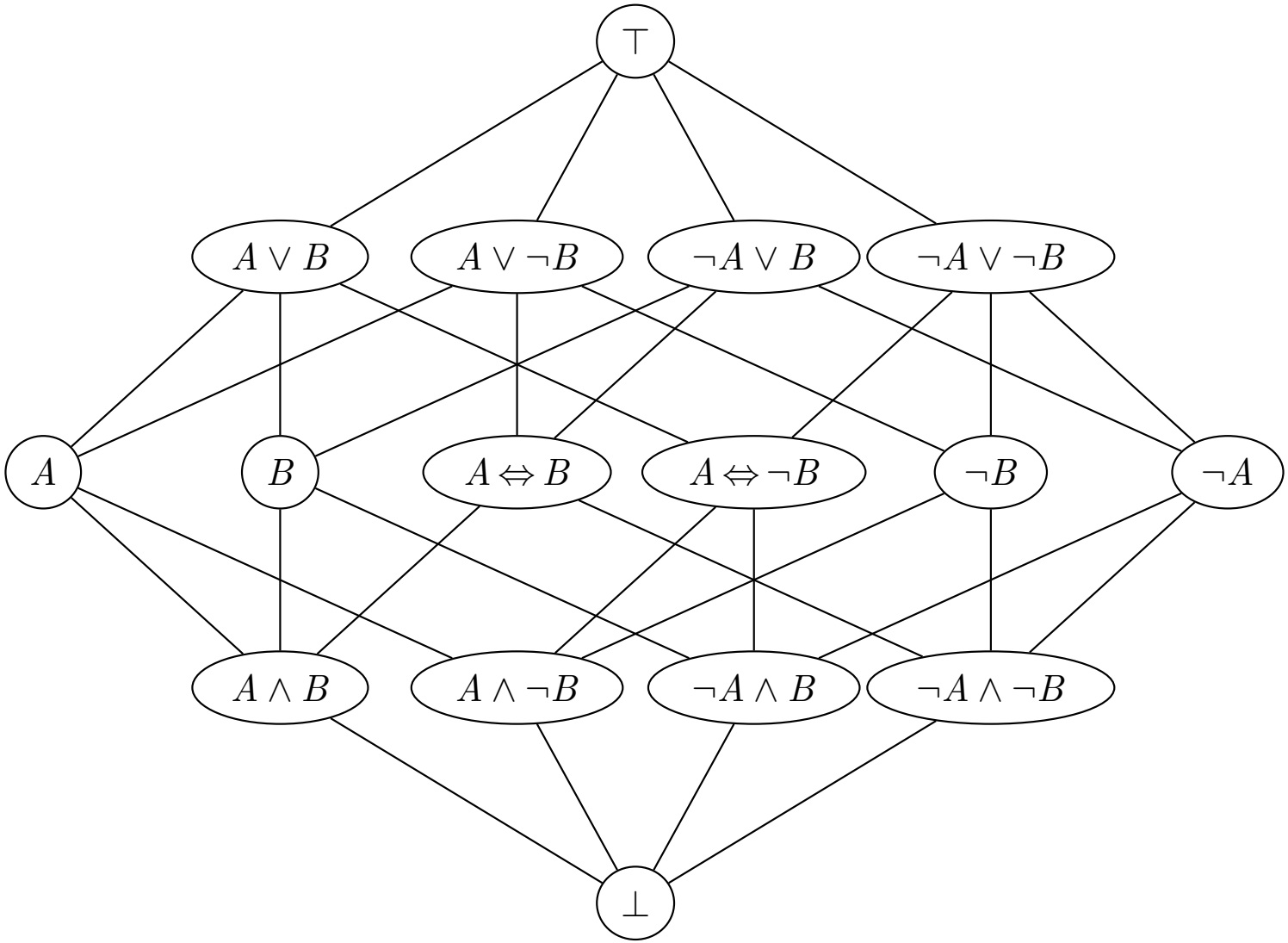
- $A + B = A \vee B$
- $A \cdot B = A \wedge B$
- $A' = \neg A$
- Rovnost definujeme jako $\rightleftharpoons$.
- $0 = \bot, \quad 1 = \top$

- Uspořádání: $A \leq B$ odpovídá $A \vDash B$, neboť to je právě, když $A \wedge B \rightleftharpoons A$ $\Leftrightarrow$ úplné mintermy A tvoří podmnožinu úplných mintermů B
- Atomy– úplné mintermy: $(A_1 \wedge A_2 \wedge \ldots \wedge A_n)$, $(\neg A_1 \wedge A_2 \wedge \ldots \wedge A_n)$, $(A_1 \wedge \neg A_2 \wedge \ldots \wedge A_n), \ldots, (A_1 \wedge A_2 \wedge \ldots \wedge \neg A_n), \ldots, (\neg A_1 \wedge \neg A_2 \wedge \ldots \wedge \neg A_n)$ Atomů je 2^n.
- Počet prvků Booleovy algebry: $|S| = 2^{2^n}$.

Příklad – BA nad jednou prvotní formulí A



Příklad – BA nad dvěma prvotními formulemi A, B



Isomorfismus Booleových algeber

Definice

Isomorfismus Booleových algeber S a T je zobrazení $f : S \to T$, které je prosté a na a pro každé $x, y \in S$ platí:

i) $f(x)' = f(x')$

ii) $f(x + y) = f(x) + f(y)$

iii) $f(x \cdot y) = f(x) \cdot f(y)$

Tvrzení

Je-li f isomorfismus Booleových algeber S a T, potom

i) $f(0) = 0$

ii) $f(1) = 1$

Důkaz

i) $f(0) = f(x \cdot x') = f(x) \cdot f(x') = f(x) \cdot f(x)' = 0$

ii) $f(1) = f(x + x') = f(x) + f(x') = f(x) + f(x)' = 1$

□

Věta o isomorfismu

Věta

Každá konečná Booleova algebra S je isomorfní s Booleovou algebrou $P(A)$, kde A je množina atomů S. Booleova algebra má 2^m prvků, kde m je počet atomů.

Důkaz

Každému prvku x lze přiřadit množinu atomů, které jsou menší nebo rovné než x.
Nechť A je množina všech atomů algebry S. Pro $x \in S$ definujme
$f(x) = \{a \in A | a \leq x\} \in P(A)$. Zjevně f je prosté a na.
Inverzní zobrazení je $f^{-1}\big(\{a_1, \ldots, a_k\}\big) = a_1 + a_2 + \ldots + a_k$ a $f^{-1}(\emptyset) = 0$.

- $x \neq y \Leftrightarrow \{a \in A | a \leq x\} \neq \{a \in A | a \leq y\}$
- $f(x \cdot y) = \{a \in A | a \leq x \cdot y\} = \{a \in A | a \leq x \wedge a \leq y\} = \{a \in A | a \leq x\} \cap \{a \in A | a \leq y\}$, neboť $a \leq x \cdot y \Leftrightarrow (a \leq x) \wedge (a \leq y)$
- $f(x+y) = \{a \in A | a \leq x+y\} = \{a \in A | a \leq x \vee a \leq y\} = \{a \in A | a \leq x\} \cup \{a \in A | a \leq y\}$, neboť $a \leq x + y \Leftrightarrow (a \leq x) \vee (a \leq y)$
- $f(x') = \{a \in A | a \leq x'\} = A \setminus \{a \in A | a \leq x\} = f(x)'$, neboť
  $x \cdot x' = 0 \Rightarrow \{a \in A | a \leq x\} \cap \{a \in A | a \leq x'\} = \emptyset$
  $x + x' = 0 \Rightarrow \{a \in A | a \leq x\} \cup \{a \in A | a \leq x'\} = A$

Booleova algebra výrokové logiky

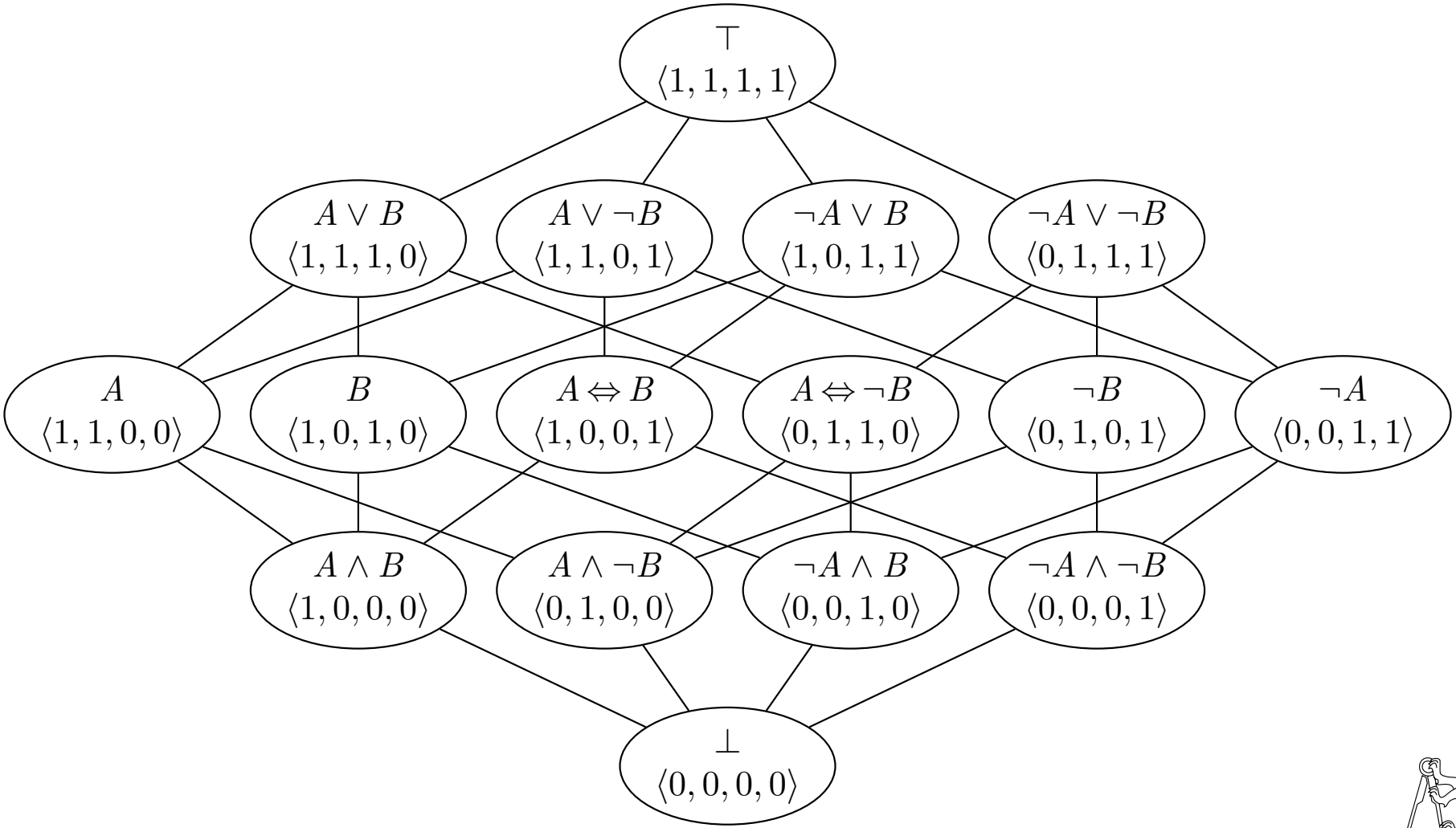
Důsledek

Booleova algebra nad n prvotními formulemi má 2^n atomů a 2^{2^n} výrokových formulí.

Důkaz

Atomy jsou všechny úplné mintermy, je jich 2^n. Každou formuli jednoznačně vyjádříme jako disjunkci konečné množiny mintermů (z jednoznačnosti úplného DNT). Podmnožin množiny mintermů je 2^{2^n}. □

Isomorfismus $\{0,1\}^4$ a BA nad prvotními formulemi A, B



Booleovská funkce

Definice

Booleovská funkce je funkce z množiny $\{0,1\}^n$ do množiny $\{0,1\}$.

Booleovské funkce na $\{0,1\}^2$

x	y	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
1	1	1	1	1	1	0	1	1	1
1	0	1	1	1	0	1	1	0	0
0	1	1	1	0	1	1	0	0	1
0	0	1	0	1	1	1	0	1	0

x	y	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	0	0	0	1	0	0	0	0
1	0	1	1	0	0	1	0	0	0
0	1	1	0	1	0	0	1	0	0
0	0	0	1	1	0	0	0	1	0

Booleovské funkce nad 2 prvotními formulemi

Každá formule výrokové logiky se 2 prvotními proměnnými odpovídá právě jedné booleovské funkci z množiny $\{0,1\}^2$ do množiny $\{0,1\}$.

Logicky ekvivalentní formule odpovídají stejné booleovské funkci.

A	B	T	$A \vee B$	$B \Rightarrow A$	$A \Rightarrow B$	$\neg A \vee \neg B$	A	$A \Leftrightarrow B$	B
1	1	1	1	1	1	0	1	1	1
1	0	1	1	1	0	1	1	0	0
0	1	1	1	0	1	1	0	0	1
0	0	1	0	1	1	1	0	1	0

$A \Leftrightarrow \neg B$	$\neg B$	$\neg A$	$A \wedge B$	$A \wedge \neg B$	$\neg A \wedge B$	$\neg A \wedge \neg B$	$\bot$
0	0	0	1	0	0	0	0
1	1	0	0	1	0	0	0
1	0	1	0	0	1	0	0
0	1	1	0	0	0	1	0

Celkem $2^{2^2} = 16$ možných booleovských funkcí (logicky neekvivalentních formulí)

Domácí úkol pro 2. paralelku

Tři lidé sedí kolem stolu. Každý z nich ví, že má na hlavě buď bílý nebo černý klobouk, a každý vidí klobouky svých sousedů, ale nikoli svůj. Ve skutečnosti mají všichni bílý klobouk. Vyzveme je, aby se přihlásil, kdo vidí bílý klobouk. Všichni zvednou ruku. Dále je vyzveme, aby ten kdo ví, jakou barvu má jeho klobouk, ruku sundal. Po chvíli ten nejchytřejší ruku sundá. Jak na to přišel?

Domácí úkol pro 3. paralelku

Představte si, že máme šachovnici, z níž jsou vyříznuta dvě políčka v rozích proti sobě na diagonále.

Rozmístěte na ni kostky domina (kostka domina zabere dvě sousední políčka šachovnice) tak, aby pokryly všechna zbylá políčka šachovnice.