Výrokovologické vyplývanie

3. prednáška

Logika pre informatikov a Úvod do matematickej logiky

Ján Kľuka, Ján Mazák

Letný semester 2022/2023

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Obsah 3. prednášky

Výrokovologické vyplývanie

- Výrokovologické ohodnotenia
- Výrokovologické teórie a modely
- Vyplývanie, nezávislosť a nesplniteľnosť

Rekapitulácia

Minulý týždeň sme hovorili o tom,

- čo sú výrokovologické spojky,
- ako zodpovedajú slovenským spojkám,
- čo sú symboly jazyka výrokovologickej časti logiky prvého rádu,
- čo sú formuly tohto jazyka,
- kedy sú formuly pravdivé v danej štruktúre.
- čo je výrokovologická teória a jej model.

Výrokovologické vyplývanie

Logické dôsledky

Na 1. prednáške:

- Hovorili sme o tom, že logiku zaujíma,
  čo a prečo sú zákonitosti správneho usudzovania.
- Správne úsudky odvodzujú z predpokladov (teórií) závery,
  ktoré sú ich logickými dôsledkami.
- *Logickými dôsledkami* teórie sú tvrdenia,
  ktoré sú pravdivé vo všetkých modeloch teórie.

Minulý týždeň sme začali pracovať s výrokovologickou časťou logiky prvého rádu.

Už vieme, čo sú v nej teórie a modely.

Čo sú logické dôsledky?

Výrokovologické vyplývanie

Výrokovologické ohodnotenia

Nekonečne veľa štruktúr

Logickými dôsledkami teórie sú tvrdenia,
ktoré sú pravdivé vo všetkých modeloch teórie.

$$\begin{aligned} T_{\text{party}} = \{&((\texttt{príde(Kim)} \vee \texttt{príde(Jim)}) \vee \texttt{príde(Sarah)}),\\ &(\texttt{príde(Kim)} \to \neg\texttt{príde(Sarah)}),\\ &(\texttt{príde(Jim)} \to \texttt{príde(Kim)}),\\ &(\texttt{príde(Sarah)} \to \texttt{príde(Jim)})\} \end{aligned}$$

Ale štruktúr je nekonečne veľa a ak má teória jeden model,
má aj nekonečne veľa ďalších:

$$\begin{array}{lll} \mathcal{M}_1 = (\{\mathtt{k},\mathtt{j},\mathtt{s}\}, i_1) & \mathcal{M}_1' = (\{\mathtt{k},\mathtt{j},\mathtt{s},0,1\}, i_1') & \mathcal{M}_1'' = (\{2,4,6\}, i_1'') \quad \cdots \\ i_1(\texttt{Kim}) = \mathtt{k} & i_1'(\texttt{Kim}) = \mathtt{k} & i_1''(\texttt{Kim}) = 2 \\ i_1(\texttt{Jim}) = \mathtt{j} & i_1'(\texttt{Jim}) = \mathtt{j} & i_1''(\texttt{Jim}) = 4 \\ i_1(\texttt{Sarah}) = \mathtt{s} & i_1'(\texttt{Sarah}) = \mathtt{s} & i_1''(\texttt{Sarah}) = 6 \\ i_1(\texttt{príde}) = \{\mathtt{k},\mathtt{j}\} & i_1'(\texttt{príde}) = \{\mathtt{k},\mathtt{j},1\} & i_1''(\texttt{príde}) = \{2,4\} \end{array}$$

Rozdiely modelov

V čom sa líšia a čo majú spoločné nasledujúce modely T_{party}?

$\mathcal{M}_1 = (\{\mathtt{k}, \mathtt{j}, \mathtt{s}, \mathtt{e}, \mathtt{h}\}, i_1)$

$i_1(\texttt{Kim}) = \mathtt{k}$

$i_1(\texttt{Jim}) = \mathtt{j}$

$i_1(\texttt{Sarah}) = \mathtt{s}$

$i_1(\texttt{príde}) = \{\mathtt{k}, \mathtt{j}, \mathtt{e}\}$

$\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$

$i_2(\texttt{Kim}) = 1$

$i_2(\texttt{Jim}) = 2$

$i_2(\texttt{Sarah}) = 3$

$i_2(\texttt{príde}) = \{1, 2\}$

$\mathcal{M}_3 = (\{\mathtt{kj}, \mathtt{s}\}, i_3)$

$i_3(\texttt{Kim}) = \mathtt{kj}$

$i_3(\texttt{Jim}) = \mathtt{kj}$

$i_3(\texttt{Sarah}) = \mathtt{s}$

$i_3(\texttt{príde}) = \{\mathtt{kj}\}$

Rozdiely modelov

V čom sa líšia a čo majú spoločné nasledujúce modely T_{party}?

$\mathcal{M}_1 = (\{\mathtt{k}, \mathtt{j}, \mathtt{s}, \mathtt{e}, \mathtt{h}\}, i_1)$	$\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$	$\mathcal{M}_3 = (\{\mathtt{kj}, \mathtt{s}\}, i_3)$
$i_1(\mathtt{Kim}) = \mathtt{k}$	$i_2(\mathtt{Kim}) = 1$	$i_3(\mathtt{Kim}) = \mathtt{kj}$
$i_1(\mathtt{Jim}) = \mathtt{j}$	$i_2(\mathtt{Jim}) = 2$	$i_3(\mathtt{Jim}) = \mathtt{kj}$
$i_1(\mathtt{Sarah}) = \mathtt{s}$	$i_2(\mathtt{Sarah}) = 3$	$i_3(\mathtt{Sarah}) = \mathtt{s}$
$i_1(\mathtt{píde}) = \{\mathtt{k}, \mathtt{j}, \mathtt{e}\}$	$i_2(\mathtt{píde}) = \{1, 2\}$	$i_3(\mathtt{píde}) = \{\mathtt{kj}\}$

Líšia sa doménami aj v interpretáciách.

Rozdiely modelov

V čom sa líšia a čo majú spoločné nasledujúce modely T_{party}?

$\mathcal{M}_1 = (\{\mathtt{k}, \mathtt{j}, \mathtt{s}, \mathtt{e}, \mathtt{h}\}, i_1)$	$\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$	$\mathcal{M}_3 = (\{\mathtt{kj}, \mathtt{s}\}, i_3)$
$i_1(\mathtt{Kim}) = \mathtt{k}$	$i_2(\mathtt{Kim}) = 1$	$i_3(\mathtt{Kim}) = \mathtt{kj}$
$i_1(\mathtt{Jim}) = \mathtt{j}$	$i_2(\mathtt{Jim}) = 2$	$i_3(\mathtt{Jim}) = \mathtt{kj}$
$i_1(\mathtt{Sarah}) = \mathtt{s}$	$i_2(\mathtt{Sarah}) = 3$	$i_3(\mathtt{Sarah}) = \mathtt{s}$
$i_1(\mathtt{pride}) = \{\mathtt{k}, \mathtt{j}, \mathtt{e}\}$	$i_2(\mathtt{pride}) = \{1, 2\}$	$i_3(\mathtt{pride}) = \{\mathtt{kj}\}$

Líšia sa doménami aj v interpretáciách.

Líšia sa v pravdivosti rovnostných atómov, napr. $\mathtt{Kim} \doteq \mathtt{Jim}$.

Rozdiely modelov

V čom sa líšia a čo majú spoločné nasledujúce modely T_{party}?

$\mathcal{M}_1 = (\{\mathtt{k}, \mathtt{j}, \mathtt{s}, \mathtt{e}, \mathtt{h}\}, i_1)$	$\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$	$\mathcal{M}_3 = (\{\mathtt{kj}, \mathtt{s}\}, i_3)$
$i_1(\mathtt{Kim}) = \mathtt{k}$	$i_2(\mathtt{Kim}) = 1$	$i_3(\mathtt{Kim}) = \mathtt{kj}$
$i_1(\mathtt{Jim}) = \mathtt{j}$	$i_2(\mathtt{Jim}) = 2$	$i_3(\mathtt{Jim}) = \mathtt{kj}$
$i_1(\mathtt{Sarah}) = \mathtt{s}$	$i_2(\mathtt{Sarah}) = 3$	$i_3(\mathtt{Sarah}) = \mathtt{s}$
$i_1(\mathtt{pride}) = \{\mathtt{k}, \mathtt{j}, \mathtt{e}\}$	$i_2(\mathtt{pride}) = \{1, 2\}$	$i_3(\mathtt{pride}) = \{\mathtt{kj}\}$

Líšia sa doménami aj v interpretáciách.

Líšia sa v pravdivosti rovnostných atómov, napr. $\mathtt{Kim} \doteq \mathtt{Jim}$.

Zhodujú sa na pravdivosti všetkých predikátových atómov $\mathtt{pride}(\mathtt{Kim})$, $\mathtt{pride}(\mathtt{Jim})$, $\mathtt{pride}(\mathtt{Sarah})$.

V T_{party} na ničom inom nezáleží.

Ohodnotenie atómov

Z každej zo štruktúr

$\mathcal{M}_1 = (\{\mathtt{k}, \mathtt{j}, \mathtt{s}, \mathtt{e}, \mathtt{h}\}, i_1)$ $\quad$ $\mathcal{M}_2 = (\{1, 2, 3\}, i_2)$ $\quad$ $\mathcal{M}_3 = (\{\mathtt{kj}, \mathtt{s}\}, i_3)$

$i_1(\mathtt{Kim}) = \mathtt{k}$ $\quad$ $i_2(\mathtt{Kim}) = 1$ $\quad$ $i_3(\mathtt{Kim}) = \mathtt{kj}$

$i_1(\mathtt{Jim}) = \mathtt{j}$ $\quad$ $i_2(\mathtt{Jim}) = 2$ $\quad$ $i_3(\mathtt{Jim}) = \mathtt{kj}$

$i_1(\mathtt{Sarah}) = \mathtt{s}$ $\quad$ $i_2(\mathtt{Sarah}) = 3$ $\quad$ $i_3(\mathtt{Sarah}) = \mathtt{s}$

$i_1(\mathtt{pride}) = \{\mathtt{k}, \mathtt{j}, \mathtt{e}\}$ $\quad$ $i_2(\mathtt{pride}) = \{1, 2\}$ $\quad$ $i_3(\mathtt{pride}) = \{\mathtt{kj}\}$

môžeme skonštruovať to isté **ohodnotenie predikátových atómov**:

$v(\mathtt{pride}(\mathtt{Kim})) = t$ $\quad$ lebo $\mathcal{M}_j \vDash \mathtt{pride}(\mathtt{Kim})$,

$v(\mathtt{pride}(\mathtt{Jim})) = t$ $\quad$ lebo $\mathcal{M}_j \vDash \mathtt{pride}(\mathtt{Jim})$,

$v(\mathtt{pride}(\mathtt{Sarah})) = f$ $\quad$ lebo $\mathcal{M}_j \nvDash \mathtt{pride}(\mathtt{Sarah})$.

Všetky tieto štruktúry (a nekonečne veľa ďalších) vieme pri vyhodnocovaní formúl jazyka $\mathcal{L}_{\text{party}}$ nahradiť týmto ohodnotením.

Výrokovologické formuly, teórie a ohodnotenia

Definícia 3.1

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.

Množinu všetkých predikátových atómov jazyka $\mathcal{L}$ označujeme $\mathcal{PA}_{\mathcal{L}}$.

Výrokovologickými formulami jazyka $\mathcal{L}$ nazveme všetky formuly jazyka $\mathcal{L}$, ktoré **neobsahujú symbol rovnosti**. Množinu všetkých výrokovologických formúl jazyka $\mathcal{L}$ označujeme $\mathcal{PE}_{\mathcal{L}}$.

Definícia 3.2

Nech (f, t) je usporiadaná dvojica *pravdivostných hodnôt*, $f \neq t$, kde f predstavuje *nepravdu* a t predstavuje *pravdu*.
Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.

Výrokovologickým ohodnotením pre $\mathcal{L}$, skrátene *ohodnotením*, nazveme každé zobrazenie $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$.

Pravdivé formuly v ohodnotení

Ako vyhodnotíme, či je formula pravdivá v nejakom ohodnotení?

Definícia 3.3

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech (f, t) sú pravdivostné hodnoty a nech $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$. Reláciu ***výrokovologická formula A je pravdivá v ohodnotení v*** ($v \vDash_{\mathrm{p}} A$) definujeme **induktívne** pre všetky predikátové atómy a a všetky výrokovologické formuly A, B jazyka $\mathcal{L}$ nasledovne:

- $v \vDash_{\mathrm{p}} a$ vtt $v(a) = t$,
- $v \vDash_{\mathrm{p}} \neg A$ vtt $v \nvDash_{\mathrm{p}} A$,
- $v \vDash_{\mathrm{p}} (A \wedge B)$ vtt $v \vDash_{\mathrm{p}} A$ a zároveň $v \vDash_{\mathrm{p}} B$,
- $v \vDash_{\mathrm{p}} (A \vee B)$ vtt $v \vDash_{\mathrm{p}} A$ alebo $v \vDash_{\mathrm{p}} B$,
- $v \vDash_{\mathrm{p}} (A \to B)$ vtt $v \nvDash_{\mathrm{p}} A$ alebo $v \vDash_{\mathrm{p}} B$,

kde **vtt** skracuje *vtedy a len vtedy* a $v \nvDash_{\mathrm{p}} A$ skracuje *A nie je pravdivá vo v*.

Vyhodnotenie formuly v ohodnotení

Príklad 3.4

Vyhodnoťme formulu

$$X = ((\texttt{príde}(\texttt{Jim}) \vee \neg\texttt{príde}(\texttt{Kim})) \rightarrow \texttt{príde}(\texttt{Sarah}))$$

vo výrokovologickom ohodnotení

$$v = \{\texttt{príde}(\texttt{Kim}) \mapsto t,\ \texttt{príde}(\texttt{Jim}) \mapsto t,\ \texttt{príde}(\texttt{Sarah}) \mapsto f\}$$

zdola nahor:

	p(Kim)	p(Jim)	p(Sarah)	¬p(Kim)	(p(Jim) ∨ ¬p(Kim))	X
v	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$

príde sme skrátili na p.

Ohodnotenie zhodné so štruktúrou

Definícia 3.5

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech (f, t) sú pravdivostné hodnoty, $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$ a $S \subseteq \mathcal{PA}_{\mathcal{L}}$ je množina predikátových atómov.

Ohodnotenie v a štruktúra $\mathcal{M}$ sú navzájom ***zhodné na*** S vtt pre každý predikátový atóm $A \in S$ platí

$$v(A) = t \text{ vtt } \mathcal{M} \models A.$$

Ohodnotenie v a štruktúra $\mathcal{M}$ sú navzájom ***zhodné*** vtt sú zhodné na $\mathcal{PA}_{\mathcal{L}}$.

Konštrukcia ohodnotenia zhodného so štruktúrou

Ohodnotenie zhodné so štruktúrou zostrojíme ľahko:

Tvrdenie 3.6

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a (f, t) sú pravdivostné hodnoty. Zobrazenie $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ definované pre každý atóm $A \in \mathcal{PA}_{\mathcal{L}}$ nasledovne:

$$v(A) = \begin{cases} t, & \text{ak } \mathcal{M} \vDash A, \\ f, & \text{ak } \mathcal{M} \nvDash A \end{cases}$$

je výrokovologické ohodnotenie zhodné s $\mathcal{M}$.

Dôkaz.

Pre každý atóm $A \in \mathcal{PA}_{\mathcal{L}}$ musíme dokázať, že $v(A) = t$ vtt $\mathcal{M} \vDash A$:
($\Leftarrow$) Priamo: Ak $\mathcal{M} \vDash A$, tak $v(A) = t$ podľa jeho definície v leme.
($\Rightarrow$) Nepriamo: Ak $\mathcal{M} \nvDash A$, tak $v(A) = f$ podľa jeho definície v leme, a pretože $t \neq f$, tak $v(A) \neq t$. □

Dokážeme zostrojiť aj štruktúru z ohodnotenia, aby boli zhodné?

Príklad 3.7 (Konštrukcia štruktúry zhodnej s ohodnotením)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, kde $\mathcal{C}_{\mathcal{L}} = \{\mathtt{Kim}, \mathtt{Jim}, \mathtt{Sarah}\}$ a $\mathcal{P}_{\mathcal{L}} = \{\mathtt{príde}\}$.

Nech v je výrokovologické ohodnotenie pre $\mathcal{L}$, kde

$$v(\mathtt{príde}(\mathtt{Kim})) = t \quad v(\mathtt{príde}(\mathtt{Jim})) = t \quad v(\mathtt{príde}(\mathtt{Sarah})) = f$$

Zostrojme štruktúru pre $\mathcal{L}$ zhodnú s v.

Dokážeme zostrojiť aj štruktúru z ohodnotenia, aby boli zhodné?

Príklad 3.7 (Konštrukcia štruktúry zhodnej s ohodnotením)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, kde $\mathcal{C}_\mathcal{L} = \{\texttt{Kim}, \texttt{Jim}, \texttt{Sarah}\}$ a $\mathcal{P}_\mathcal{L} = \{\texttt{príde}\}$.

Nech v je výrokovologické ohodnotenie pre $\mathcal{L}$, kde

$$v(\texttt{príde}(\texttt{Kim})) = t \quad v(\texttt{príde}(\texttt{Jim})) = t \quad v(\texttt{príde}(\texttt{Sarah})) = f$$

Zostrojme štruktúru pre $\mathcal{L}$ zhodnú s v.

Možnosťou, ktorú ľahko zovšeobecníme na všetky jazyky, je použiť ako doménu množinu konštánt:

$$\mathcal{M} = (\underbrace{\{\texttt{Kim}, \texttt{Jim}, \texttt{Sarah}\}}_{\mathcal{C}_\mathcal{L}}, i)$$

Každú konštantu interpretujeme ňou samou:

$$i(\texttt{Kim}) = \texttt{Kim} \qquad i(\texttt{Jim}) = \texttt{Jim} \qquad i(\texttt{Sarah}) = \texttt{Sarah}$$

predikát $\texttt{príde}$ ako množinu tých c, pre ktoré $v(\texttt{príde}(c)) = t$:

$$i(\texttt{príde}) = \{\texttt{Kim}, \texttt{Jim}\}$$

Konštrukcia štruktúry zhodnej s ohodnotením

Ako zostrojíme štruktúru zhodnú s ohodnotením pre hocijaký jazyk?

Tvrdenie 3.8

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu,
nech (f, t) sú pravdivostné hodnoty
a $v : \mathcal{PA}_{\mathcal{L}} \to \{f, t\}$ je výrokovologické ohodnotenie pre $\mathcal{L}$.

Nech $\mathcal{M} = (D, i)$ je štruktúra pre $\mathcal{L}$ s doménou $D = \mathcal{C}_{\mathcal{L}}$
a interpretačnou funkciou definovanou pre všetky $n > 0$, všetky
konštanty c a všetky predikátové symboly $P \in \mathcal{P}_{\mathcal{L}}$ s aritou n takto:

$$i(c) = c$$
$$i(P) = \{ (c_1, \dots, c_n) \in \mathcal{C}_{\mathcal{L}}^n \mid v(P(c_1, \dots, c_n)) = t \}$$

Potom $\mathcal{M}$ je zhodná s v.

Štruktúram zo syntaktického materiálu sa hovorí herbrandovské.

Zhoda na všetkých výrokovologických formulách

Tvrdenie 3.9

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a υ je výrokovologické ohodnotenie pre $\mathcal{L}$ zhodné s $\mathcal{M}$. Potom pre každú výrokovologickú formulu $X \in \mathcal{PE}_{\mathcal{L}}$ platí, že $\upsilon \models_{\mathrm{p}} X$ vtt $\mathcal{M} \models X$.

Zhoda na všetkých výrokovologických formulách

Tvrdenie 3.9

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a v je výrokovologické ohodnotenie pre $\mathcal{L}$ zhodné s $\mathcal{M}$. Potom pre každú výrokovologickú formulu $X \in \mathcal{PE}_{\mathcal{L}}$ platí, že $v \vDash_{\mathrm{p}} X$ vtt $\mathcal{M} \vDash X$.

Dôkaz indukciou na konštrukciu formuly.

1.1: Nech X je rovnostný atóm. Potom nie je výrokovologickou formulou a tvrdenie preň triviálne platí.
1.2: Nech X je predikátový atóm. Potom $v \vDash_{\mathrm{p}} X$ vtt $v(X) = t$ vtt $\mathcal{M} \vDash X$.
2.1: Indukčný predpoklad: Nech tvrdenie platí pre formulu X.
Dokážme tvrdenie pre $\neg X$. Ak X neobsahuje symbol rovnosti $\doteq$, potom $v \vDash_{\mathrm{p}} \neg X$ vtt $v \nvDash_{\mathrm{p}} X$ vtt (podľa IP) $\mathcal{M} \nvDash X$ vtt $\mathcal{M} \vDash \neg X$. Ak X obsahuje $\doteq$, $\neg X$ ho obsahuje tiež, teda nie je výrokovologická a tvrdenie pre ňu platí triviálne.
2.2: IP: Nech tvrdenie platí pre formuly X a Y. Ak X alebo Y obsahuje $\doteq$, tvrdenie platí pre $(X \wedge Y)$, $(X \vee Y)$, $(X \to Y)$ triviálne, lebo nie sú výrokovologické. Nech teda X ani Y neobsahuje $\doteq$. Potom platí $v \vDash_{\mathrm{p}} (X \to Y)$ vtt $v \nvDash_{\mathrm{p}} X$ alebo $v \vDash_{\mathrm{p}} Y$ vtt (podľa IP) vtt $\mathcal{M} \nvDash X$ alebo $\mathcal{M} \vDash Y$ vtt $\mathcal{M} \vDash (X \to Y)$. Podobne pre ďalšie spojky. □

Výrokovologické vyplývanie

Výrokovologické teórie a modely

Výrokovologické teórie

Vráťme sa naspäť k teóriám, modelom a vyplývaniu.

Definícia 3.10

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Každú množinu výrokovologických formúl jazyka $\mathcal{L}$ budeme nazývať *výrokovologickou teóriou* v jazyku $\mathcal{L}$.

Príklad 3.11

Výrokovologickou teóriou je

$$\begin{aligned} T_{\text{party}} = \{&((\texttt{príde}(\texttt{Kim}) \vee \texttt{príde}(\texttt{Jim})) \vee \texttt{príde}(\texttt{Sarah})),\\ &(\texttt{príde}(\texttt{Kim}) \to \neg\texttt{príde}(\texttt{Sarah})),\\ &(\texttt{príde}(\texttt{Jim}) \to \texttt{príde}(\texttt{Kim})),\\ &(\texttt{príde}(\texttt{Sarah}) \to \texttt{príde}(\texttt{Jim}))\}, \end{aligned}$$

ale nie

$$T_{\text{party}} \cup \{\texttt{Kim} \doteq \texttt{Sarah}\}.$$

Príklad výrokovologického modelu

Príklad 3.12 (Výrokovologický model teórie o party)

$$v = \{\texttt{príde(Kim)} \mapsto t, \texttt{príde(Jim)} \mapsto t, \texttt{príde(Sarah)} \mapsto f\}$$

$$\left.\begin{aligned} v &\vDash_{\mathrm{p}} ((\texttt{príde(Kim)} \vee \texttt{príde(Jim)}) \vee \texttt{príde(Sarah)}) \\ v &\vDash_{\mathrm{p}} (\texttt{príde(Kim)} \to \neg\texttt{príde(Sarah)}) \\ v &\vDash_{\mathrm{p}} (\texttt{príde(Jim)} \to \texttt{príde(Kim)}) \\ v &\vDash_{\mathrm{p}} (\texttt{príde(Sarah)} \to \texttt{príde(Jim)}) \end{aligned}\right\} v \vDash_{\mathrm{p}} T_{\text{party}}$$

Výrokovologický model

Definícia 3.13 (Výrokovologický model)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je teória v jazyku $\mathcal{L}$ a υ je výrokovologické ohodnotenie pre jazyk $\mathcal{L}$.

Teória T je ***pravdivá*** v ohodnotení υ, skrátene $\upsilon \vDash_{\mathrm{p}} T$, vtt **každá** formula X z T je pravdivá vo υ (teda $\upsilon \vDash_{\mathrm{p}} X$ pre každú $X \in T$).

Hovoríme tiež, že υ je ***výrokovologickým modelom*** T.

Teória T je ***nepravdivá*** vo υ, skrátene $\upsilon \nvDash_{\mathrm{p}} T$, vtt T nie je pravdivá vo υ.

Zrejme $\upsilon \nvDash_{\mathrm{p}} T$ vtt $\upsilon \nvDash_{\mathrm{p}} X$ pre **nejakú** $X \in T$.

Definícia 3.14 (Splniteľnosť a nesplniteľnosť)

Teória je *výrokovologicky splniteľná* vtt
má aspoň jeden výrokovologický model.

Teória je *výrokovologicky nesplniteľná* vtt
nemá žiaden výrokovologický model.

Zrejme teória nie je splniteľná vtt keď je nesplniteľná.

Príklad 3.15

T_{party} je evidentne splniteľná.

Výrokovologické vyplývanie

Vyplývanie, nezávislosť a nesplniteľnosť

Ak sú množiny konštánt a predikátových symbolov jazyka konečné, jazyk má konečne veľa predikátových atómov a teda aj konečne veľa ohodnotení.

Uvažovať o všetkých ohodnoteniach a modeloch teórie nie je také odstrašujúce. Napríklad si ľahšie predstavíme logický dôsledok:

Definícia 3.16

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je ***výrokovologickým dôsledkom*** teórie T vtt pre každé ohodnotenie v pre jazyk $\mathcal{L}$ platí, že ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$.

Hovoríme tiež, že X ***vyplýva*** z T a píšeme $T \vDash_{\mathrm{p}} X$.

Ak X nevyplýva z T, píšeme $T \nvDash_{\mathrm{p}} X$.

Príklad výrokovologického vyplývania

Príklad 3.17

Vyplýva $\texttt{príde(Kim)}$ výrokovologicky z T_{party}?

Pretože vieme vymenovať všetky ohodnotenia pre $\mathcal{L}_{\text{party}}$, zistíme to ľahko:

	v_i			$((\texttt{p(K)} \vee \texttt{p(J)}) \vee \texttt{p(S)})$	$(\texttt{p(K)} \to \neg\texttt{p(S)})$	$(\texttt{p(J)} \to \texttt{p(K)})$	$(\texttt{p(S)} \to \texttt{p(J)})$	T_{party}	$\texttt{p(K)}$
	$\texttt{p(K)}$	$\texttt{p(J)}$	$\texttt{p(S)}$						
v_0	f	f	f	$\nvDash_{\text{p}}$				$\nvDash_{\text{p}}$	
v_1	f	f	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$	$\nvDash_{\text{p}}$	
v_2	f	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_3	f	t	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_4	t	f	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$
v_5	t	f	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	
v_6	t	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$
v_7	t	t	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	

Skrátili sme `príde` na `p`, `Kim` na `K`, `Jim` na `J`, `Sarah` na `S`.

Logický záver: Formula $\texttt{príde(Kim)}$ výrokovologicky vyplýva z T_{party}.

Praktický záver: Aby boli všetky požiadavky splnené, Kim musí prísť na párty.

Príklad nezávislosti

Príklad 3.18

Vyplýva $\texttt{príde(Jim)}$ výrokovologicky z T_{party}?

	v_i			$((\texttt{p(K)} \vee \texttt{p(J)}) \vee \texttt{p(S)})$	$(\texttt{p(K)} \to \neg\texttt{p(S)})$	$(\texttt{p(J)} \to \texttt{p(K)})$	$(\texttt{p(S)} \to \texttt{p(J)})$	T_{party}	$\texttt{p(J)}$
	$\texttt{p(K)}$	$\texttt{p(J)}$	$\texttt{p(S)}$						
v_0	f	f	f	$\nvDash_{\text{p}}$				$\nvDash_{\text{p}}$	
v_1	f	f	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$	$\nvDash_{\text{p}}$	
v_2	f	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_3	f	t	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_4	t	f	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$
v_5	t	f	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	
v_6	t	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$
v_7	t	t	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	

Logický záver: Formula $\texttt{príde(Jim)}$ nevyplýva z T_{party}.

Výrokovologická nezávislosť

Vzťahu medzi $\texttt{príde(Jim)}$ a T_{party} hovoríme nezávislosť.

Definícia 3.19

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je *výrokovologicky nezávislá* od teórie T vtt existujú také ohodnotenia v_0 a v_1 pre jazyk $\mathcal{L}$, že $v_0 \vDash_{\text{p}} T$ aj $v_1 \vDash_{\text{p}} T$, ale $v_0 \nvDash_{\text{p}} X$ a $v_1 \vDash_{\text{p}} X$.

Príklad 3.20 (pokračovanie príkladu 3.18)

Logický záver: Formula $\texttt{príde(Jim)}$ je nezávislá od T_{party}.

Praktický záver: Všetky požiadavky budú naplnené bez ohľadu na to, či Jim príde alebo nepríde na párty. Nie je nutné, aby bol prítomý ani aby bol neprítomý. Môže, ale nemusí prísť. Jeho prítomnosť od požiadaviek nezávisí.

Príklad vyplývania negácie

Príklad 3.21

Je $\texttt{príde(Sarah)}$ výrokovologickým dôsledkom T_{party} alebo nezávislá od T_{party}?

	v_i			$((\texttt{p(K)} \vee \texttt{p(J)}) \vee \texttt{p(S)})$	$(\texttt{p(K)} \to \neg\texttt{p(S)})$	$(\texttt{p(J)} \to \texttt{p(K)})$	$(\texttt{p(S)} \to \texttt{p(J)})$	T_{party}	$\texttt{p(S)}$
	$\texttt{p(K)}$	$\texttt{p(J)}$	$\texttt{p(S)}$						
v_0	f	f	f	$\nvDash_{\text{p}}$				$\nvDash_{\text{p}}$	
v_1	f	f	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$	$\nvDash_{\text{p}}$	
v_2	f	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_3	f	t	t	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$		$\nvDash_{\text{p}}$	
v_4	t	f	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$
v_5	t	f	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	
v_6	t	t	f	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$
v_7	t	t	t	$\vDash_{\text{p}}$	$\nvDash_{\text{p}}$			$\nvDash_{\text{p}}$	

Logický záver: Formula $\texttt{príde(Sarah)}$ nevyplýva z T_{party}, ale ani nie je nezávislá od T_{party}.

Vyplývanie negácie

Tvrdenie 3.22

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X nevyplýva z teórie T a nie je výrokovologicky nezávislá od T vtt $\neg X$ vyplýva z T.

Príklad 3.23 (pokračovanie príkladu 3.21)

Logický záver: Z T_{party} vyplýva $\neg\texttt{príde}(\texttt{Sarah})$.

Praktický záver: Aby boli všetky požiadavky naplnené, Sarah **nesmie** prísť na party.

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

Buď $v \vDash_{\mathrm{p}} X$, alebo $v \nvDash_{\mathrm{p}} X$.

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \vDash_{\mathrm{p}} X$	pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$
existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \nvDash_{\mathrm{p}} X$	X je nezávislá od T $T \nvDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	$T \vDash_{\mathrm{p}} \neg X$
pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$	$T \vDash_{\mathrm{p}} X$	

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

Buď $v \vDash_{\mathrm{p}} X$, alebo $v \nvDash_{\mathrm{p}} X$.

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \vDash_{\mathrm{p}} X$	pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$
existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \nvDash_{\mathrm{p}} X$	X je nezávislá od T $T \nvDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	$T \vDash_{\mathrm{p}} \neg X$ a $T \nvDash_{\mathrm{p}} X$
pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$	$T \vDash_{\mathrm{p}} X$	

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

Buď $v \vDash_{\mathrm{p}} X$, alebo $v \nvDash_{\mathrm{p}} X$.

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \vDash_{\mathrm{p}} X$	pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$
existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \nvDash_{\mathrm{p}} X$	X je nezávislá od T $T \nvDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	$T \vDash_{\mathrm{p}} \neg X$ a $T \nvDash_{\mathrm{p}} X$
pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$	$T \vDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

$$\text{Buď } v \vDash_{\mathrm{p}} X, \text{ alebo } v \nvDash_{\mathrm{p}} X.$$

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \vDash_{\mathrm{p}} X$	pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$
existuje v také, že $v \vDash_{\mathrm{p}} T$ a $v \nvDash_{\mathrm{p}} X$	X je nezávislá od T $T \nvDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	$T \vDash_{\mathrm{p}} \neg X$ a $T \nvDash_{\mathrm{p}} X$
pre všetky v, ak $v \vDash_{\mathrm{p}} T$, tak $v \vDash_{\mathrm{p}} X$	$T \vDash_{\mathrm{p}} X$ a $T \nvDash_{\mathrm{p}} \neg X$	T je **nesplniteľná** $T \vDash_{\mathrm{p}} X$ aj $T \vDash_{\mathrm{p}} \neg X$

Nesplniteľná teória

Príklad 3.24

Je teória $T'_{\text{party}} = T_{\text{party}} \cup \{(\neg \texttt{príde(Sarah)} \rightarrow \neg \texttt{príde(Kim)})\}$ splniteľná?

	v_i			$((\texttt{p(K)} \vee \texttt{p(J)}) \vee \texttt{p(S)})$	$(\texttt{p(K)} \rightarrow \neg\texttt{p(S)})$	$(\texttt{p(J)} \rightarrow \texttt{p(K)})$	$(\texttt{p(S)} \rightarrow \texttt{p(J)})$	$(\neg\texttt{p(S)} \rightarrow \neg\texttt{p(K)})$	T'_{party}
	p(K)	p(J)	p(S)						
v_0	f	f	f	$\not\models_p$					$\not\models_p$
v_1	f	f	t	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$
v_2	f	t	f	$\models_p$	$\models_p$	$\not\models_p$			$\not\models_p$
v_3	f	t	t	$\models_p$	$\models_p$	$\not\models_p$			$\not\models_p$
v_4	t	f	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_5	t	f	t	$\models_p$	$\not\models_p$				$\not\models_p$
v_6	t	t	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_7	t	t	t	$\models_p$	$\not\models_p$				$\not\models_p$

Logický záver: T'_{party} je nesplniteľná, vyplýva z nej každá formula.

Praktický záver: T'_{party} nemá praktické dôsledky, lebo nevypovedá o žiadnom stave sveta. Na jej základe nevieme rozhodnúť, kto musí alebo nesmie prísť na párty.

Nesplniteľnosť ale nie neužitočná vlastnosť.

Tvrdenie 3.25

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X výrokovologicky vyplýva z teórie T vtt $T \cup \{\neg X\}$ je výrokovologicky nesplniteľná.

Podľa tohto tvrdenia sa rozhodnutie vyplývania dá zredukovať na rozhodnutie splniteľnosti.

Výrokovologickú splniteľnosť rozhoduje SAT solver.

Množina atómov formuly a teórie

Definícia 3.26

Množinu atómov $\text{atoms}(X)$ formuly $X \in \mathcal{E}_{\mathcal{L}}$ definujeme pre všetky formuly $A, B \in \mathcal{E}_{\mathcal{L}}$ nasledovne:

- $\text{atoms}(A) = \{A\}$, ak A je atóm,
- $\text{atoms}(\neg A) = \text{atoms}(A)$,
- $\text{atoms}((A \wedge B)) = \text{atoms}((A \vee B)) = \text{atoms}((A \to B)) = \text{atoms}(A) \cup \text{atoms}(B)$.

Množinou atómov teórie T je

$$\text{atoms}(T) = \bigcup_{X \in T} \text{atoms}(X).$$

Ohodnotenia zhodné na atómoch teórie

Definícia 3.27

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $M \subseteq \mathcal{PA}_{\mathcal{L}}$. Ohodnotenia v_1 a v_2 sa ***zhodujú*** na množine M vtt $v_1(A) = v_2(A)$ pre každý atóm $A \in M$.

Tvrdenie 3.28

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Pre každú výrokovologickú teóriu T a formulu X jazyka $\mathcal{L}$ a všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine $\mathrm{atoms}(T) \cup \mathrm{atoms}(X)$ platí

- $v_1 \models_{\mathrm{p}} T$ *vtt* $v_2 \models_{\mathrm{p}} T$,
- $v_1 \models_{\mathrm{p}} X$ *vtt* $v_2 \models_{\mathrm{p}} X$.

Ohodnotenia postačujúce na skúmanie teórií

Inak povedané: Pravdivosť formuly/teórie v ohodnotení závisí **iba** od pravdivostných hodnôt tých atómov, ktoré sa v nej vyskytujú.

Takže na zistenie vyplývania, nezávislosti, splniteľnosti stačí preskúmať všetky ohodnotenia, ktoré sa **líšia** na atómoch **vyskytujúcich** sa vo formule a teórii.

Pokiaľ je teória je konečná, stačí skúmať konečne veľa ohodnotení, aj keby bol jazyk nekonečný.

Výrokovologické vyplývanie

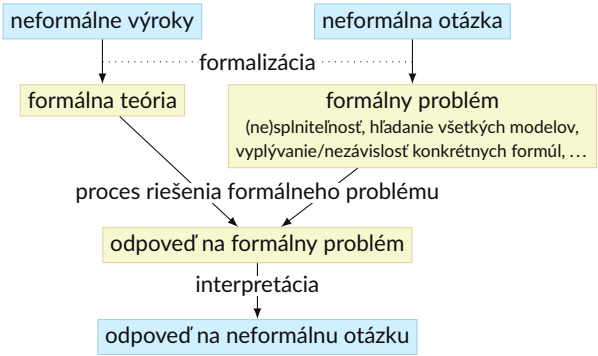
Rekapitulácia

Rekapitulácia

Dnes sme sa naučili:

- ako zjednodušiť štruktúry na výrokovologické ohodnotenia,
- čo je logické vyplývanie z teórie a logický dôsledok teórie,
- čo je nezávislosť formuly od teórie,
- štyri situácie vo vzťahoch teórií a formúl a ich praktické dôsledky,
- čo sú splniteľné a nesplniteľné teórie,
- ako súvisí nesplniteľnosť a vyplývanie.

Schéma riešenia problémov pomocou logiky



XOR

Logická spojka exlusive or (XOR):

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- zodpovedá sčítaniu v poli $\mathbb{Z}_2$
- komutatívna a asociatívna
- rýchlo vypočítateľná, aj na úrovni hardvéru
- dôležitá v kryptológii

XOR

Ideálna šifra: vezmeme náhodný reťazec (kľúč) rovnako dlhý ako správa a spravíme XOR bit po bite. Použitý kľúč zahodíme. Všetky zašifrované texty sú rovnako pravdepodobné.

Reálne šifry: kľúč je krátky (napr. 1024 B). Ak by sme ho nakopírovali veľakrát za sebou, bity správy šifrované tým istým bitom kľúča vytvoria slabinu (možno dešifrovať aj bez znalosti kľúča, stačí uhádnuť jeho dĺžku). Preto napr. použijeme kľúč ako seed do pseudonáhodného generátora a vygenerujeme reťazec potrebnej dĺžky.

Útoky na šifry: o.i. pomocou SAT solvera, ktorý vie pracovať s XOR (aktívna oblasť výskumu).

XOR

Ku XOR existuje prepis do CNF, napr. z $a \oplus b \oplus c$ sa stane

$$(a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (b \vee \neg a \vee \neg c) \wedge (c \vee \neg a \vee \neg b)$$

XOR

Ku XOR existuje prepis do CNF, napr. z $a \oplus b \oplus c$ sa stane

$$(a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (b \vee \neg a \vee \neg c) \wedge (c \vee \neg a \vee \neg b)$$

Ale s počtom premenných rastie dĺžka ekvivalentnej CNF formuly exponenciálne. Preto sa oplatí predspracovanie: XOR formuly vnímame ako súčty nad $\mathbb{Z}_2$ a použijeme Gaussovu elimináciu.

$$a_1 \oplus a_2 \oplus a_3 = 0$$
$$a_1 \oplus a_3 \oplus a_4 = 0$$

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{array}\right)$$