Prvá písomka z UDML, 15.11.2016 - riešenia
(Celý materiál je neoficiálny, ak tu mám chybu ja, vaše riešenie s rovnakou chybou **nie je** správne!)

1.	a) Uveďte, z čoho sa skladá formálny systém a definujte dôkaz formuly A vo formálnom systéme. b) Definujte štandarnú sémantiku výrokovej logiky pre spojky $\wedge$, $\vee$, $\rightarrow$, $\neg$ (valuáciu a jej rozšírenie) c) Definujte sporný systém. [3b]

a) Formálny systém sa skladá z jazyka, axióm a odvodzovacích pravidiel. Dôkaz formuly A je postupnosť formúl $A_1, A_2, \ldots, A_n$, pričom $A_n = A$ a každá formula postupnosti je buď axióma, alebo je odvodená z predchádzajúcich pomocou niektorého odovdzovacieho pravidla.

b) Valuácia prvotných formúl je funkcia $v\colon \mathcal{P} \rightarrow \{0,1\}$, ktorá každej prvotnej formule priradí pravdivostnú hodnotu. Keď už máme určenú pravdivostnú hodnotu prvotných formúl, môžeme určiť pravdivostnú hodnotu pre všetky formuly. Rozšírenie valuácie označíme $\overline{v}$.

- $\overline{v}(p) = v(p)$ pre prvotné formuly $p \in \mathcal{P}$
- $\overline{v}(A \wedge B) = 1$, ak $\overline{v}(A) = \overline{v}(B) = 1$, inak $\overline{v}(A \wedge B) = 0$
- $\overline{v}(A \vee B) = 0$, ak $\overline{v}(A) = \overline{v}(B) = 0$, inak $\overline{v}(A \vee B) = 1$
- $\overline{v}(A \rightarrow B) = 0$, ak $\overline{v}(A) = 1$ a zároveň $\overline{v}(B) = 0$, inak $\overline{v}(A \rightarrow B) = 1$
- $\overline{v}(\neg A) = 1$, ak $\overline{v}(A) = 0$, inak $\overline{v}(\neg A) = 0$

c) Sporný systém je formálny systém, v ktorom sa dajú dokázať všetky formuly.

2.	Nech G je (konečný) bipartitný graf s partíciami U a V, t.j. všetky hrany vedú medzi U a V. $N(X)$ bude označovať množinu vrcholov, ktoré majú aspoň jedného suseda v množine vrcholov X. Potom platí **Hallova veta**: *Ak má každá množina vrcholov $X \subseteq U$ dosť susedov (ak $\lvert X\rvert \leq \lvert N(X)\rvert$), tak vieme všetky prvky z U popárovať.* Vyslovte vetu o kompaktnosti výrokovej logiky a pomocou nej dokážte nasledujúcu nekonečnú verziu Hallovej vety: *Nech G je nekonečný bipartitný graf s partíciami U a V, pričom každý vrchol má len konečne veľa susedov. Ak pre každú konečnú množinu vrcholov $X \subseteq U$ platí $\lvert X\rvert \leq \lvert N(X)\rvert$, tak vieme prvky z U popárovať.* [4b]

Veta o kompaktnosti VL: Nech T je množina formúl výrokovej logiky. T je splniteľná práve vtedy, keď každá jej konečná $T_0 \supseteq T$ je splniteľná.

Vyrobíme si množinu formúl T, ktorej každý model bude zodpovedať páreniu v grafe, ktoré pokrýva všetky vrcholy v partícií U. Naše prvotné formuly budú

$$p_{u,v} = \textit{hrana } (u,v) \in E \textit{ je v párovaní}$$

Inými slovami, vrcholy u a v tvoria pár. Každá valuácia týchto prvotných formúl bude zodpovedať výberu hrán (ak je $p_{u,v}$ pravdivé, berieme do výberu hranu (u,v))

Naša teória T (pre konkrétny graf) bude obsahovať nasledovné tri sady formúl:

A $= \{p_{u,v_1} \vee p_{u,v_2} \vee \cdots \vee p_{u,v_k} \mid \forall u \in U,\ \{v_1, v_2, \ldots v_k\} = N(u)\}$ - každý vrchol z U chceme s niekým spárovať.

B $= \{p_{u,v} \rightarrow \neg p_{u,v'} \mid \forall u \in U,\ v, v' \in N(u), v \neq v'\}$ - každý vrchol z U môžeme spárovať najviac s jedným susedom z V.

C $= \{p_{u,v} \rightarrow \neg p_{u',v} \mid \forall v \in V,\ u, u' \in N(v), u \neq u'\}$ - každý vrchol z V môžeme spárovať najviac s jedným susedom z U.

$$T = A \cup B \cup C$$

Teraz chceme dokázať, že ak pre každú konečnú množinu vrcholov $X \subseteq U$ platí $|X| \leq |N(X)|$, tak T má model (a graf G párovanie pokrývajúce partíciu U). Na to použijeme vetu o kompaktnosti.

Stačí dokázať, že každá konečná podmnožina T má model. Zoberme si nejakú konečnú $T_0 \subseteq T$. Množina T_0 hovorí len o konečne veľa vrcholoch grafu G z partície U. Nech sú to vrcholy $U' \subseteq U$. Vytvoríme si podgraf G' indukovaný vrcholmi $U' \cup N(U')$ (sú v ňom vrcholy $U' \cup N(U')$ a hrany pôvodného grafu medzi nimi). Graf G' je konečný a spĺňa podmienku, že pre každé $X \subseteq U'$ platí $|X| \leq |N(X)|$, preto podľa Hallovej vety má graf G' párovanie pokrývajúce U'.

Ak pre graf G' vytvoríme teóriu T' rovnako, ako pre graf G, potom bude platiť

$$T_0 \subseteq T' \subseteq T$$

Keďže graf G' má párovanie, tak T' má model. Ten istý model je aj modelom pre T_0. Tým sme dokázali, že každá konečná $T_0 \subseteq T$ má model. Potom aj T má model (z vety o kompaktnosti) a G má párovanie, ktoré pokrýva U.

3. Definujte disjunktívnu normálnu formu a nájdite ju pre formulu

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

[2b]

Formula je v disjuktívnej normálnej forme, ak je tvaru $A_1 \vee A_2 \vee \cdots \vee A_n$, kde každé A_i je tvaru $(l_{i,1} \wedge l_{i,2} \wedge \cdots \wedge l_{i,k_i})$, pričom každé $l_{i,j}$ je buď prvotná formula alebo jej negácia.

Pri transformovaní formuly do disjuktívnej normánej formy používame nasledujúce ekvivalencie:

(1) $(A \to B) \leftrightarrow \neg(A \wedge \neg B) \leftrightarrow (\neg A \vee B)$ - prepis implikácie

(2) $\neg\neg A \leftrightarrow A$

(3) $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$ - deMorganove pravidlá

(4) $A \wedge (B \vee C) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$
$A \vee (B \wedge C) \leftrightarrow ((A \vee B) \wedge (A \vee C))$ - distributívne zákony

1.	$(a \to \neg(b \vee c)) \wedge ((\neg d \to a) \to \neg(b \wedge c))$	
2.	$(\neg a \vee \neg(b \vee c)) \wedge ((\neg\neg d \vee a) \to \neg(b \wedge c))$	(1) 2x
3.	$(\neg a \vee \neg(b \vee c)) \wedge (\neg(d \vee a) \vee \neg(b \wedge c))$	(2)+(1)
4.	$(\neg a \vee (\neg b \wedge \neg c)) \wedge ((\neg d \wedge \neg a) \vee \neg b \vee \neg c))$	(3) 3x
5.	$(\neg a \wedge ((\neg d \wedge \neg a) \vee \neg b \vee \neg c) \vee ((\neg b \wedge \neg c) \wedge ((\neg d \wedge \neg a) \vee \neg b \vee \neg c))$	(4)
6.	$(\neg a \wedge \neg d \wedge \neg a) \vee (\neg a \wedge \neg b) \vee (\neg a \wedge \neg c) \vee (\neg b \wedge \neg c \wedge \neg d \wedge \neg a) \vee (\neg b \wedge \neg c \wedge \neg b) \vee (\neg b \wedge \neg c \wedge \neg c)$	(4) 2x
7.	$(\neg a \wedge \neg d) \vee (\neg a \wedge \neg b) \vee (\neg a \wedge \neg c) \vee (\neg b \wedge \neg c \wedge \neg d \wedge \neg a) \vee (\neg b \wedge \neg c) \vee (\neg b \wedge \neg c)$	
8.	$(\neg a \wedge \neg d) \vee (\neg a \wedge \neg b) \vee (\neg a \wedge \neg c) \vee (\neg b \wedge \neg c)$	

V siedmom a ôsmom riadku sa len odstránili nadbytočné literály a klauzuly. Tieto kroky už neboli potrebné, ale výsledná formula vyzerá krajšie. :-)

Bola aj iná cesta, ako nájsť disjunktívnu normálu formu. Mohli sme nájsť boolovskú funkciu, ktorá zodpovedá našej formule (urobiť veľkú tabuľku) a opísať, kedy nadobúda pravdivostnú hodnotu 1.

a	b	c	d	$\neg(b \vee c)$	$a \to \neg(b \vee c)$	$\neg d \to a$	$\neg(b \wedge c)$	$(\neg d \to a) \to \neg(b \wedge c)$	φ
0	0	0	0	1	1	0	1	1	1
0	0	0	1	1	1	1	1	1	1
0	0	1	0	0	1	0	1	1	1
0	0	1	1	0	1	1	1	1	1
0	1	0	0	0	1	0	1	1	1
0	1	0	1	0	1	1	1	1	1
0	1	1	0	0	1	0	0	1	1
0	1	1	1	0	1	1	0	0	0
1	0	0	0	1	1	1	1	1	1
1	0	0	1	1	1	1	1	1	1
1	0	1	0	0	0	1	1	1	0
1	0	1	1	0	0	1	1	1	0
1	1	0	0	0	0	1	1	1	0
1	1	0	1	0	0	1	1	1	0
1	1	1	0	0	0	1	0	0	0
1	1	1	1	0	0	1	0	0	0

Z nej potom môžeme spraviť napríklad úplnú disjunktívnu normálnu formu:

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

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

4. Nech $\mathcal{B}$ je formálny systém definovaný rovnako ako formálny systém výrokovej logiky (FS VL) až na axiómy:
$(B1) = (A1)$
$(B2) = (A2)$
$(B3)\ \ A \to (B \to (B \to A))$
Predpokladajte, že pre formálny systém $\mathcal{B}$ platí veta o dedukcii.
Sformulujte slabú formu vety o úplnosti výrokovej logiky. Definujte vlastnosti (slabá) korektnosť a (slabá) úplnosť.
Zistite a dokážte, či je tento systém (slabo) úplný, a zistite a dokážte, či je aj (slabo) korektný – všetko vzhľadom ku klasickej sémantike. Môžete pritom využiť, že FS VL je úplný aj korektný a že vynechaním ľubovoľnej axiómy dostaneme neúplný systém. [6b]

Slabá forma vety o úplnoti výrokovej logiky: $\vdash \varphi \iff \models \varphi$ - formula je dokázateľná práve vtedy, keď je tautológia.

Korektnosť: $\vdash \varphi \Rightarrow \models \varphi$ - všetky dokázateľné sú tautológie.

Úplnosť: $\models \varphi \Rightarrow \vdash \varphi$ - všetky tautológie sa dajú dokázať.

Overenie korektnosti: Systém výrokovej logiky je korektný, preto vieme, že modus ponens je korektné pravidlo a axiómy $(B1)$ a $(B2)$ sú tautológie. Ak je aj axióma $(B3)$ tautológia, potom je celý systém korektný. Ak nie je tautológia, potom nie je korektný.

A	B	$B \to A$	$B \to (B \to A)$	$A \to (B \to (B \to A))$
0	0	1	1	1
0	1	0	0	1
1	0	1	1	1
1	1	1	1	1

Z tabuľky vidíme, že $(B3)$ je tautológia, preto je systém $\mathcal{B}$ korektný.

Overenie úplnosti: Vidíme, že v žiadnej axióme sa nevyskytuje negácia a to je podozrivé. Intuitívne tušíme, že náš systém asi nebude úplný. Skúsime to teda dokázať. Dajú sa použiť dva postupy (a možno aj viac).

Prvý spôsob je cez sémantiku. Definujeme si sémantiku:

A	$\neg A$
0	1
1	1

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

Ďalej definujeme *dúhovosť* formuly. Formula je *dúhová*, ak má hodnotu 1 pre ľubovoľné ohodnotenie prvotných formúl v. Všetky axiómy $\mathcal{B}$ systému sú dúhové, lebo sú to tautológie a správanie implikácie sme nezmenili. Modus ponens prenáša dúhovosť. Ak A je dúhová a $A \to B$ je dúhová, tak aj B musí mať stále hodnotu 1 a tiež je dúhová. Pozrime sa teraz na axiómu výrokovej logiky $(A3)$ $(\neg B \to \neg A) \to (A \to B)$.

$\overline{v}(A)$	$\overline{v}(B)$	$\overline{v}(\neg A)$	$\overline{v}(\neg B)$	$\overline{v}(\neg B \to \neg A)$	$\overline{v}(A \to B)$	$\overline{v}((\neg B \to \neg A) \to (A \to B))$
0	0	1	1	1	1	1
0	1	1	1	1	1	1
1	0	1	1	1	0	0
1	1	1	1	1	1	1

Ak $\overline{v}(A) = 1$ a $\overline{v}(B) = 0$, tak $\overline{v}((\neg B \to \neg A) \to (A \to B)) = 0$. Z toho dostávame, že $(A3)$ nie je dúhová, preto nemôže byť v systéme $\mathcal{B}$ dokázateľná. V $\mathcal{B}$ nie sú dokázateľné všetky tautológie, takže nie je úplný.

Druhý spôsob je nájsť dôkaz $(B3)$ z axióm $(B1)$ a $(B2)$. Ja som napríklad našla takýto dôkaz:

1.		$\vdash$	$A \to (B \to A)$	$(B1)$
2.	A	$\vdash$	$B \to A$	$(VD\ 1.)$
3.		$\vdash$	$(B \to A) \to (B \to (B \to A))$	$(B1)$
4.	A	$\vdash$	$B \to (B \to A)$	$(MP\ 2., 3.)$
5.		$\vdash$	$A \to (B \to (B \to A))$	$(VD\ 4.)$

Axióma $(B3)$ je dokázateľná z $(B1) = (A1)$ a $(B2) = (A2)$. To znamená, že v tomto systéme je dokázateľné iba to, čo je dokázateľné iba z prvých dvoch axióm. Keďže systém iba s prvými dvoma axiómami nie je úplný, ani systém $\mathcal{B}$ nemôže byť úplný.

Bonus. V úlohe č. 1 ste definovali sporný systém. Nájdite nejaký sporný systém a dokážte o ňom, že je naozaj sporný. Je zakázané používať axiómu typu A. Inak môžete používať všetko, čo viete o výrokovej logike. [2b]

Jedno z veľa možných riešení je napríklad:

- jazyk: rovnaký ako pre výrokovú logiku.
- axióma: (AX) $A \to B$.
- odvodzovacie pravidlo: modus ponens: $\frac{A, A \to B}{B}$

Aby sme dokázali, že tento systém je sporný, musíme nájsť dôkaz pre ľubovolnú formulu. Napríklad takýto:

1.	$\vdash A \to B$	(AX)
2.	$\vdash (A \to B) \to A$	(AX)
3.	$\vdash A$	$(MP\ 1., 2.)$