BIK-DML Domácí úkol - řešení

ZS 2021/2022

Příklad 1. *(6 bodů)*

a) Převeďte následující tvrzení z přirozeného jazyka do predikátové logiky. Poté vytvořte negaci v predikátové logice a tu převeďte zpět do přirozeného jazyka. Užijte k tomu unární predikát $p(x)$–x *je fanouškem Agathy Christie*, a binární predikát $r(x, y)$–x *zná* y, pro proměnné z universa všech lidí.

„Každý, kdo zná nějakého fanouška Agathy Christie, je sám fanouškem Agathy Christie."

b) Pomocí DNT nebo KNT vyšetřete, zda je mezi níže uvedenými formulemi vztah logického důsledku nebo dokonce logické ekvivalence. V jednotlivých krocích odvození DNT/KNT uvádějte, jaká pravidla nebo známé logické ekvivalence požíváte. Svůj závěr následně ověřte pomocí pravdivostní tabulky. Pokud některý vztah neplatí, najděte pravdivostní ohodnocení prvotních formulí, které o tom svědčí.

$$(A \wedge B) \Rightarrow (C \vee \neg D), \qquad A \Leftrightarrow C$$

Řešení. a) Odpovídající formule v predikátové logice je

$$(\forall x)((\exists y)(p(y) \wedge r(x, y)) \Rightarrow p(x))$$

nebo logicky ekvivalentní formule

$$(\forall x)(\forall y)((p(y) \wedge r(x, y)) \Rightarrow p(x)).$$

Negací je formule

$$(\exists x)(\exists y)(p(y) \wedge r(x, y) \wedge \neg p(x).$$

Negace v přirozeném jazyku: „Existuje někdo, kdo zná nějakého fanouška Agathy Christie, ale sám není fanouškem Agathy Christie."

b) DNT i KNT první formule:

$$(A \wedge B) \Rightarrow (C \vee \neg D) \overset{\text{zl.pr.}}{\models\!\models} \neg(A \wedge B) \vee (C \vee \neg D) \overset{\text{deMorg}}{\models\!\models} \neg A \vee \neg B \vee C \vee \neg D$$

KNT druhé formule:

$$A \Leftrightarrow C \overset{\text{výz.ekv.}}{\models\!\models} (A \Rightarrow C) \wedge (C \Rightarrow A) \overset{\text{zl.pr.}}{\models\!\models} (\neg A \vee C) \wedge (\neg C \vee A)$$

DNT druhé formule:

$$\begin{aligned}(\neg A \vee C) \wedge (\neg C \vee A) &\overset{\text{distr.z.}}{\models\!\models} (\neg A \wedge \neg C) \vee (\neg A \wedge A) \vee (C \wedge \neg C) \vee (C \wedge A) \\ &\models\!\models (\neg A \wedge \neg C) \vee \bot \vee \bot \vee (C \wedge A) \models\!\models (\neg A \wedge \neg C) \vee (C \wedge A)\end{aligned}$$

Protože platí

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

z KNT obou formulí odvodíme, že formule $(A \wedge B) \Rightarrow (C \vee \neg D)$ je logickým důsledkem formule $A \Leftrightarrow C$ a formule nejsou logicky ekvivalentní. Příkladem pravdivostního ohodnocení prvotních formulí v, které dokazuje že formule nejsou logicky ekvivalentní, je třeba $v(A) = 0, v(B) = 0, v(C) = 1, v(D) = 0$.

Ověření pomocí pravdivostní tabulky:

A	B	C	D	$A \wedge B$	$C \vee \neg D$	$(A \wedge B) \Rightarrow (C \vee \neg D)$	$A \Leftrightarrow C$
0	0	0	0	0	1	1	1
0	0	0	1	0	0	1	1
0	0	1	0	0	1	1	0
0	0	1	1	0	1	1	0
0	1	0	0	0	1	1	1
0	1	0	1	0	0	1	1
0	1	1	0	0	1	1	0
0	1	1	1	0	1	1	0
1	0	0	0	0	1	1	0
1	0	0	1	0	0	1	0
1	0	1	0	0	1	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	1	1	0
1	1	0	1	1	0	0	0
1	1	1	0	1	1	1	1
1	1	1	1	1	1	1	1

Příklad 2. *(4 body)* Nechť $a, b, m \in \mathbb{Z}$, přičemž $m \geq 2$. Dokažte, že pokud $a \equiv b \pmod{m}$, potom pro každé $n \in \mathbb{N}^+$ platí $a^n \equiv b^n \pmod{m}$.

Řešení. Implikaci dokážeme přímým důkazem za použití slabé matematické indukce.

Mějme tedy $a, b, m \in \mathbb{Z}$ takové, že $a \equiv b \pmod{m}$, t.j. existuje $k \in \mathbb{Z}$ takové, že $a - b = km$. Chceme ukázat, že pak pro každé $n \in \mathbb{N}$ je pravdivý výrok $V(n)$, který říká, že $a^n \equiv b^n \pmod{m}$.
Základní krok: $V(1)$ je pravdivý podle předpokladu tvrzení, neboli volby $a, b, m \in \mathbb{Z}$.
Indukční krok: Nechť $n \in \mathbb{N}$. Ukážeme, že $V(n) \Rightarrow V(n+1)$. Předpokládejme tedy, že $V(n)$ platí, t.j. existuje $l \in \mathbb{Z}$ takové, že $a^n - b^n = lm$. Potom

$$a^{n+1} - b^{n+1} = a \cdot a^n - a \cdot b^n + a \cdot b^n - b \cdot b^n = a(a^n - b^n) + (a-b)b^n = alm + kmb^n = (al + kb^n)m,$$

tedy $a^{n+1} \equiv b^{n+1} \pmod{m}$ a $V(n+1)$ platí.

Alternativně se můžeme v tomto kroku odkázat na tvrzení z přednášky, které říká, že pokud $x \equiv y \pmod{p}$ a $u \equiv v \pmod{p}$ pro nějaká celá čísla x, y, u, v a přirozené číslo p, potom $xu \equiv yv \pmod{p}$. Jeho aplikací, za využití indukčního předpokladu a předpokladu v zadání, dostaneme

$$a^{n+1} = a \cdot a^n \equiv b \cdot b^n = b^{n+1} \pmod{m}.$$

Podle principu matematické indukce proto pro každé $n \in \mathbb{N}^+$ platí $a^n \equiv b^n \pmod{m}$ a implikace je dokázána.

Tvrzení bylo možné dokázat také přímo, použitím vzorce

$$a^n - b^n = (a-b) \sum_{i=0}^{n-1} a^i b^{n-1-i}.$$

Tento vzorec se ale vlastně také dokazuje slabou matematickou indukcí stejným „trikem“ s rozšířením výrazu jako v předešlém postupu.

Příklad 3. *(5 bodů)* Nechť R a S jsou relace na množině $X = \{-2, -1, 1, 2\}$ definované předpisy

$$mRn \Leftrightarrow m \cdot n \geq 0,$$
$$mSn \Leftrightarrow m \cdot n \leq 0.$$

a) O každé z uvedených relací rozhodněte, zda je reflexivní, ireflexivní, tranzitivní, symetrická, antisymetrická, asymetrická. Vlastnost buď dokažte, nebo uveďte protipříklad. Pokud je některá z relací ekvivalencí, napište faktorovou množinu množiny X podle příslušné ekvivalence. Pokud je některá z relací částečným uspořádáním, nakreslete její Hasseův diagram.
b) Odvoďte definující předpis, maticovou reprezentaci a diagram pro složenou relaci $R \circ S$.
c) Popište relaci $R \cup S$ libovolnou reprezentací.

Řešení. a) *Relace R:*
- ◇ je reflexivní: Pro každé $x \in \mathbb{Z}$ platí $x^2 \geq 0$, tedy i $\forall m \in X : mRm$.
- ◇ není ireflexivní: Např. $1R1$.
- ◇ je tranzitivní: Pokud pro nějaké $m, n, p \in X$ platí $mRp \wedge pRn$, potom m a p mají stejné znaménko a taky p a n mají stejné znaménko. Z toho plyne, že i m a n mají stejné znaménko a $m \cdot n \geq 0$, tedy mRn.
- ◇ je symetrická: Plyne to z komutativity operace násobení.
- ◇ není antisymetrická: Např. $2R1$ a $1R2$ ale $2 \neq 1$.
- ◇ není asymetrická: Není ani antisymetrická.

Relace R je ekvivalence a faktorová množina X podle R je

$$X/R = \{[-2]_R = [-1]_R, [1]_R = [2]_R\} = \{\{-2, -1\}, \{1, 2\}\}.$$

Relace S:
- ◇ není reflexivní: Např. $\neg 1S1$.
- ◇ je ireflexivní: Pro každé $x \in \mathbb{Z} \setminus \{0\}$ platí $x^2 > 0$, tedy $\forall m \in X : \neg mSm$.
- ◇ není tranzitivní: Např. $-1S1 \wedge 1S-2$ ale $\neg -1S-2$.
- ◇ je symetrická: Plyne to z komutativity operace násobení.
- ◇ není antisymetrická: Např. $-2S1$ a $1S-2$ ale $-2 \neq 1$.
- ◇ není asymetrická: Není ani antisymetrická.

Relace S není ani ekvivalence ani částečné uspořádání.

b) Hledáme složenou relaci $R \circ S$.
Definující předpis:

$$\forall m, n \in X : m(R \circ S)n \Leftrightarrow (\exists p \in X : mSp \wedge pRn) \Leftrightarrow (\exists p \in X : m \cdot p \leq 0 \wedge p \cdot n \geq 0)$$
$$\Leftrightarrow m \cdot n \leq 0 \Leftrightarrow mSn.$$

Dokažme předposlední ekvivalenci podrobně. Pokud existuje $p \in X$ takové, že $m \cdot p \leq 0$ a $p \cdot n \geq 0$, potom m a p mají opačná znaménka, zatímco n má stejné znaménko jako p. Tedy m a n mají opačná znaménka a platí $m \cdot n \leq 0$. Naopak, pokud $m \cdot n \leq 0$, potom můžeme zvolit $p = n$ a bude platit, že $m \cdot p \leq 0$ a $p \cdot n \geq 0$.

Tedy $R \circ S = S$.

Matice:

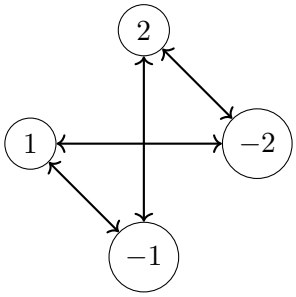
$$M_R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad M_S = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad M_S \cdot M_R = \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{pmatrix},$$

tedy

$$M_{R \circ S} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

a opět vidíme, že $R \circ S = S$.

Diagram:



Stačilo jedním způsobem ukázat, že $R \circ S = S$ a reprezentace pak odvodit od toho. Tady uvádím každý argument zvlášť jako možnosti.

c) Relace R obsahuje všechny dvojice čísel z X se stejnými znaménkami a relace S obsahuje všechny dvojice čísel z X s opačnými znaménkami, proto $R \cup S$ bude obsahovat všechny dvojice, tedy bude to úplná relace:

$$R \cup S = X \times X.$$

Příklad 4. *(4 body)* Kolika způsoby lze z padesáti fotbalistů sestavit tři týmy po jedenácti hráčích? Výsledek nemusíte vyčíslit, stačí podrobně vysvětlený vzorec.

Řešení. Nejdřív vyřešíme úlohu pro tři rozlišitelné týmy, tedy když záleží na "pořadí" týmů (můžeme si třeba představit, že mají různé barvy dresů). V prvním kroku vybereme 11 hráčů z 50 do prvního týmu (kombinace bez opakování), možností je $\binom{50}{11}$. Potom vybereme ze zbývajících 39 fotbalistů 11 členů druhého týmu, možností je $\binom{39}{11}$. A nakonec vybereme 11 hráčů ze zbylých 28 do třetího týmu, možností je $\binom{28}{11}$. Tyto tři kroky tvoří nezávislé fáze procesu, tedy podle násobícího principu je celkový počet možných výběrů hráčů do seřazených týmů roven

$$\binom{50}{11} \cdot \binom{39}{11} \cdot \binom{28}{11}.$$

Na pořadí týmů ale nezáleží, jsou určeny pouze svými členy. Proto musíme všechny výběry, které se liší pouze pořadím týmů, spojit do jedné možnosti. Počet takových výběrů je vždy roven počtu permutací týmů, tedy 3!. Proto předešlý výsledek vydělíme 3! a celkový výsledek je

$$\binom{50}{11} \cdot \binom{39}{11} \cdot \binom{28}{11} \cdot \frac{1}{3!} = \frac{50!}{11! \cdot 11! \cdot 11! \cdot 17! \cdot 3!}.$$

Jinými slovy, úloha odpovídá rozdělování 50 různých objektů do 4 stejných krabiček s předepsanými objemy (tři týmy po 11 hráčích a jedna skupina se 17 nezačleněnými fotbalisty).

Příklad 5. *(2 body)* Vyřešte lineární kongruenci

$$133^{1623} \,.\, x \equiv 55 \pmod{10}.$$

Řešení. Nejdřív nahradíme základ mocniny a pravou stranu kongruence jejich zbytky po celočíselném dělení modulem, se kterými jsou kongruentní, čímž se množina všech řešení lineární kongruence nezmění. Tedy $133 \equiv 3 \pmod{10}$ a $55 \equiv 5 \pmod{10}$, proto

$$133^{1623} \,.\, x \equiv 55 \pmod{10} \quad \Leftrightarrow \quad 3^{1623} \,.\, x \equiv 5 \pmod{10}.$$

Jelikož $\gcd(10, 3) = 1$ a $\Phi(10) = \Phi(2 \cdot 5) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$, podle Eulerovy věty platí $3^4 \equiv 1 \pmod{10}$. Proto

$$3^{1623} = (3^4)^{405} \cdot 3^3 \overset{Eu.v.}{\equiv} 1^{405} \cdot 3^3 = 27 \equiv 7 \pmod{10}$$

a dále

$$133^{1623} \,.\, x \equiv 55 \pmod{10} \quad \Leftrightarrow \quad 3^{1623} \,.\, x \equiv 5 \pmod{10} \quad \Leftrightarrow \quad 7 \,.\, x \equiv 5 \pmod{10}.$$

Řešíme tedy úlohu lineární kongruence na pravé straně ekvivalencí. Řešení existuje, protože $\gcd(7, 10) = 1$ dělí 5, a v $\mathbb{Z}_{10}$ je právě jedno. Řešení můžeme buď uhodnout nebo najít počítáním lineární diofantické rovnice $7x + 10y = 5$ pomocí rozšířeného Eukleidova algoritmu:

$$1 = \gcd(7, 10) = 3 \cdot 7 + (-2) \cdot 10 \qquad / \cdot \frac{5}{\gcd(7, 10)}$$
$$5 = 15 \cdot 7 + (-10) \cdot 10.$$

Tedy

$$x \equiv 15 \equiv 5 \pmod{10}.$$

Příklad 6. *(5 bodů)* Do sedmého ročníku Základní školy v Dlouhé ulici chodí téměř 300 žáků, přičemž dívek je dvakrát tolik co chlapců. Celý ročník se společně chystá na lyžařský zájezd. Když se chlapci ubytují do pokojů po šesti, v posledním pokoji zbydou dvě volná místa. Pokud se děvčata rozdělí do pokojů po osmi, v posledním pokoji budou jenom čtyři dívky. Nakonec však tři dívky účast odřekly a tak bude možné alespoň děvčata ubytovat do pokojů po pěti tak, že žádné lůžko nezůstane prázdné. Kolik dětí je v sedmém ročníku Základní školy v Dlouhé ulici?

Řešení. Označme x počet všech chlapců v sedmém ročníku. Zadání můžeme vyjádřit následující soustavou lineárních kongruencí:

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ 2x &\equiv 4 \pmod{8} \\ 2x - 3 &\equiv 0 \pmod{5} \end{aligned}$$

Nejdřív vyřešíme druhou a třetí kongruenci samostatně, abychom získali soustavu, kterou umíme řešit podle Čínské věty o zbytcích. Druhou kongruenci skrátím dvěma:

$$2x \equiv 4 \pmod{8} \quad \Leftrightarrow \quad x \equiv 2 \pmod{\frac{8}{\gcd(2, 8)}} \quad \Leftrightarrow \quad x \equiv 2 \pmod{4}.$$

Řešení třetí kongruence buď uhodeme nebo najdeme počítáním lineární diofantické rovnice $2x+5y = 3$ pomocí rozšířeného Eukleidova algoritmu:

$$1 = \gcd(2, 5) = (-2) \cdot 2 + 1 \cdot 5 \qquad / \cdot \frac{3}{\gcd(2, 5)}$$
$$3 = (-6) \cdot 2 + 3 \cdot 5.$$

Řešením třetí kongruence je tak

$$x \equiv -6 \equiv 4 \pmod{5}.$$

Platí tedy

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ 2x &\equiv 4 \pmod{8} \\ 2x - 3 &\equiv 0 \pmod{5} \end{aligned} \qquad \Leftrightarrow \qquad \begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

a budeme řešit soustavu na pravé straně.

Máme $\gcd(6, 4) = 2|(4 - 2)$, $\gcd(6, 5) = 1|(4 - 4)$ a $\gcd(4, 5) = 1|(2 - 4)$. Podle zobecněné Čínské věty o zbytcích tedy řešení existuje a je určeno jednoznačne modulo $\operatorname{lcm}(6, 4, 5) = 60$.

Z první rovnice dostáváme:

$$x \equiv 4 \pmod{6} \quad \rightarrow \quad x = 4 + 6.t, \ t \in \mathbb{Z}.$$

Dosadíme do druhé rovnice:

$$\begin{aligned} 4 + 6.t &\equiv 2 \pmod 4 \\ 2.t &\equiv 2 \pmod 4 \\ t &\equiv 1 \pmod 2 \quad \rightarrow \quad t = 1 + 2.k,\ k \in \mathbb{Z}. \end{aligned}$$

Tedy pro x máme $x = 4 + 6.(1 + 2.k) = 10 + 12.k$ pro nějaké $k \in \mathbb{Z}$.
Dosadíme do poslední rovnice:

$$\begin{aligned} 10 + 12.k &\equiv 4 \pmod 5 \\ 2.k &\equiv 4 \pmod 5 \\ k &\equiv 2 \pmod 5 \quad \rightarrow \quad k = 2 + 5.\ell,\ \ell \in \mathbb{Z}. \end{aligned}$$

Dostáváme, že $x = 10+12.(2+5.\ell) = 34+60.\ell$ pro nějaké $\ell \in \mathbb{Z}$. Celkový počet žáků je $3x$. Volbou $\ell = 1$ se nejvíce přiblížíme číslu 300 zdola, tedy žáků v sedmém ročníku je 282.