Математичка логика у рачунарству, II колоквијум 2014/15. *13. јануар 2015.*

1. Нека је $\mathbb{M}$ модел језика $\mathcal{L}$. За функцију $f : M^m \longrightarrow M^n$ кажемо да је дефинабилна ако је њен граф

$$\Gamma(f) = \{(\bar{a}, f(\bar{a})) \mid \bar{a} \in M^m\}$$

дефинабилан подскуп од M^{m+n}.

Ако су $f : M^m \longrightarrow M^n$ и $g : M^n \longrightarrow M^k$ дефинабилне функције, доказати да је и $g \circ f$ дефинабилна функција.

Решење. Нека $\phi(\bar{x}, \bar{y})$ дефинише скуп $\Gamma(f)$ и $\psi(\bar{y}, \bar{z})$ дефинише скуп $\Gamma(g)$, где су $\bar{x}, \bar{y}, \bar{z}$ редом дужине m, n, k.

Посматрајмо формулу $\theta(\bar{x}, \bar{z}) = \exists\bar{y}(\phi(\bar{x}, \bar{y}) \wedge \psi(\bar{y}, \bar{z}))$. Тврдимо да $\theta(\bar{x}, \bar{z})$ дефинише $\Gamma(g \circ f)$. Ако је $\models \theta(\bar{a}, \bar{c})$, тада постоји $\bar{b}$ тако да $\models \phi(\bar{a}, \bar{b}) \wedge \psi(\bar{b}\bar{c})$. Из $\models \phi(\bar{a}, \bar{b})$ имамо да је $\bar{b} = f(\bar{a})$, а из $\models \psi(\bar{b}, \bar{c})$ имамо да је $\bar{c} = g(\bar{b})$. Дакле, $\bar{c} = g(f(\bar{a})) = g \circ f(\bar{a})$, па је $\theta(M^{m+k}) \subseteq \Gamma(g \circ f)$.

Обратно, нека је $\bar{c} = g \circ f(\bar{a})$. Означимо $\bar{b} = f(\bar{a})$; тада је $\bar{c} = g(\bar{b})$. Одатле је $\models \phi(\bar{a}, \bar{b}) \wedge \psi(\bar{b}, \bar{c})$, па је и $\models \theta(\bar{a}, \bar{c})$, што доказује $\Gamma(g \circ f) \subseteq \theta(M^{m+k})$. $\dashv$

2. Дати су модели $\mathbb{A} = (\mathbf{Q}, \mathrm{Z})$, $\mathbb{B} = (\mathbf{Q}, \mathrm{Z}, <)$ и $\mathbb{C} = (\mathbf{Q}, \mathrm{Z}, s)$, где:

- $\mathbf{Q}$ је скуп рационалних бројева;
- Z је унарни предикат такав да $\mathrm{Z}(q)$ акко $q \in \mathbf{Z}$ ($\mathbf{Z}$ је скуп целих бројева);
- $<$ је уобичајено уређење рационалних бројева;
- s је функција $s : \mathbf{Q} \longrightarrow \mathbf{Q}$ дата са $s(q) = q + 1$.

Доказати:

(1) $\mathrm{dcl}^{\mathbb{A}}(\emptyset) = \emptyset$, $\mathrm{dcl}^{\mathbb{B}}(\emptyset) = \emptyset$, $\mathrm{dcl}^{\mathbb{C}}(\emptyset) = \emptyset$;

(2) ако $a \in \mathbf{Q}$, онда $\mathrm{dcl}^{\mathbb{A}}(a) = \{a\}$, $\mathrm{dcl}^{\mathbb{B}}(a) = \{a\} \cup \mathbf{Z}$, $\mathrm{dcl}^{\mathbb{C}}(a) = \{a + m \mid m \in \mathbf{Z}\}$;

(3) функција цео део $[-] : \mathbf{Q} \longrightarrow \mathbf{Q}$ је дефинабилна (без параметара) у моделу $\mathbb{B}$;

(4) скуп позитивних рационалних бројева $\mathbf{Q}^+$ није дефинабилан (са параметрима) у моделу $\mathbb{C}$.

Решење.

(1) Јасно је да је пресликавање $x \mapsto x + 1$ аутоморфизам свих ових структура који нема ниједну фиксну тачку, па је $\mathrm{dcl}^{\mathbb{A}}(\emptyset) = \mathrm{dcl}^{\mathbb{B}}(\emptyset) = \mathrm{dcl}^{\mathbb{C}}(\emptyset) = \emptyset$.

(2) Јасно је $a \in \mathrm{dcl}^{\mathbb{A}}(a)$. Нека $b \neq a$. Ако $a \neq b + 1$, онда уочимо пресликавање f дато са: $f(b) = b + 1$, $f(b + 1) = b$ и $f(x) = x$ за $x \neq b, b + 1$. Ако $a = b + 1$, онда $a \neq b - 1$, па уочимо пресликавање f дато са: $f(b) = b - 1$, $f(b - 1) = b$ и $f(x) = x$ за $x \neq b, b - 1$. У сваком случају f је бијекција која чува скуп целих бројева и фиксира a, па $f \in \mathrm{Aut}_a(\mathbb{A})$, али $f(b) \neq b$, па $b \notin \mathrm{dcl}^{\mathbb{A}}(a)$.

Поново је јасно да $a \in \mathrm{dcl}^{\mathbb{B}}(a)$. Такође изаберимо $n \in \mathbf{Z}$ тако да $n \leq a < n + 1$. Тада формула

$$\mathrm{Z}(x) \ \wedge \ x \leq a \ \wedge \ \forall y(\mathrm{Z}(y) \ \wedge \ x \leq y \leq a \Rightarrow y = x)$$

дефинише n и слично

$$\mathrm{Z}(x) \ \wedge a < x \ \wedge \ \forall y(\mathrm{Z}(y) \wedge a < y \leq x \Rightarrow y = x)$$

дефинише $n + 1$. Дакле, $n, n + 1 \in \mathrm{dcl}^{\mathbb{B}}(a)$. Сада индукцијом, ако $n + m \in \mathrm{dcl}^{\mathbb{B}}(a)$, за $m \geq 1$, тада $n+m+1 \in \mathrm{dcl}^{\mathbb{B}}(n+m)$ (према претходно доказаном, за $a = n+m$), па $n+m+1 \in \mathrm{dcl}^{\mathbb{B}}(a)$ (транзитивност dcl-a). И такође, ако $n - m \in \mathrm{dcl}^{\mathbb{B}}(a)$, за $m \geq 0$, тада $n - m - 1 \in \mathrm{dcl}^{\mathbb{B}}(n - m)$ (према претходно доказаном, за $a = n - m$), па $n - m - 1 \in \mathrm{dcl}^{\mathbb{B}}(a)$ (опет транзитивност dcl-a). Дакле, $\mathrm{dcl}^{\mathbb{B}}(a) \supseteq \{a\} \cup \mathbf{Z}$.

Ако $b \neq a$ и $b \notin \mathbf{Z}$, тада можемо направити растућу бијекцију f која чува a, чува $\mathbf{Z}$ тачка по тачка, али не чува b (Нацртајте!). Ови услови нам кажу да $f \in \mathrm{Aut}_a(\mathbb{B})$, али $f(b) \neq b$, па $b \notin \mathrm{dcl}^{\mathbb{B}}(a)$.

Коначно, јасно је да $a \in \mathrm{dcl}^{\mathbb{C}}(a)$. Такође, $x = s(a)$ дефинише $a + 1$, а $s(x) = a$ дефинише $a - 1$, па $a + 1, a - 1 \in \mathrm{dcl}^{\mathbb{C}}(a)$. Индукцијом, ако $a + m \in \mathrm{dcl}^{\mathbb{C}}(a)$, за $m \geq 1$, тада $a + m + 1 \in \mathrm{dcl}^{\mathbb{C}}(a + m)$ (према претходном, за $a = a + m$) па по транзитивности dcl-a $a + m + 1 \in \mathrm{dcl}^{\mathbb{C}}(a)$. Такође, ако $a - m \in \mathrm{dcl}^{\mathbb{C}}(a)$, за $m \geq 1$, тада $a - m - 1 \in \mathrm{dcl}^{\mathbb{C}}(a - m)$ (према претходном, за $a = a - m$) па по транзитивности dcl-a $a - m - 1 \in \mathrm{dcl}^{\mathbb{C}}(a)$. Дакле, $\mathrm{dcl}^{\mathbb{C}}(a) \supseteq \{a + m \mid m \in \mathbf{Z}\}$.

Ако $b \notin \{a+m \mid m \in \mathbf{Z}\}$ посматрамо пресликавање f дато са:

$$f(x) = \begin{cases} x & x \in \{a+m \mid m \in \mathbf{Z}\} \\ x+1 & \text{иначе} \end{cases}.$$

Јасно је да је f бијекција која чува скуп целих бројева, и чува функцију s $(f(s(x)) = s(f(x)))$ и $f(a) = a$, па $f \in \mathrm{Aut}_a(\mathbb{C})$. Такође, $f(b) = b+1 \neq b$, па $b \notin \mathrm{dcl}^{\mathbb{C}}(a)$.

(3) Уочимо формулу

$$\phi(x,y) = \mathrm{Z}(y) \ \wedge\ y \leq x \ \wedge\ \forall z(\mathrm{Z}(z) \ \wedge\ y \leq z \leq x \Rightarrow z = y)$$

Приметимо да $\phi(a,y)$ дефинише $[a]$. Према томе $\phi(M,M) = \{(a,[a]) \mid a \in M\} = \Gamma([-])$, тј. $[-]$ је дефинабилна функција.

(4) Претпоставимо супротно да је $\mathbf{Q}^+$ дефинабилан са параметрима $a_1, a_2, \ldots, a_n$. Приметимо да $S = \bigcup_{i=1}^n \{a_i + m \mid m \in \mathrm{Z}\}$ има пресек са $\mathbf{Q}^+$; нека је b у пресеку и изаберимо $N > b$, $N \in \mathbf{Z}$. Посматрамо пресликавање f дато са:

$$f(x) = \begin{cases} x & x \in S \\ x-N & \text{иначе} \end{cases}.$$

Јасно је да је f бијекција која чува скуп целих бројева, чува функцију s и $f(a_i) = a_i$, за $1 \leq i \leq n$, па $f \in \mathrm{Aut}_{\{a_1 \ldots a_n\}}(\mathbb{C})$. Али $f(b) = b - N < 0$, па f не чува $\mathbf{Q}^+$. Контрадикција. $\dashv$

3. Доказати да теорија модела $\mathbb{C}$ из претходног задатка има елиминацију квантификатора.

Решење.

$\dashv$

4. Нека је $\mathcal{K}$ поткласа класе свих коначних модела неког језика. Ако је $\mathcal{K}$ аксиоматска класа, доказати да мора постојати горње ограничење кардиналности њених модела.

Решење. Нека је $\mathcal{K}$ аксиоматизована теоријом T (језика $\mathcal{L}$) и претпоставимо супротно да има неограничено велике коначне моделе. Посматрајмо проширење језика новим константама: $\mathcal{L}' = \mathcal{L} \cup \{c_n \mid n \geq 0\}$, и теорију $T' = T \cup \{c_i \neq c_j \mid i \neq j\}$.

Ако је T_0 коначна подтеорија од T', доказаћемо да она има модел. Довољно је да докажемо да $T_1 = T_0 \cup T$ има модел. Приметимо да T_1 "спомиње" само коначно много константи c_i; нека су то c_i, за $i < N$. Изаберимо модел $\mathbb{M} = (M, s^{\mathbb{M}})_{s \in \mathcal{L}}$ теорије T такав да $|M| > N$ и нека су $m_0, m_1, \ldots, m_N$ различити елементи из M. Посматрамо експанзију $\mathbb{M}'$ модела $\mathbb{M}$ на језик $\mathcal{L}'$ дефинисану са: $c_i^{\mathbb{M}'} = m_i$, за $i < N$ и $c_i^{\mathbb{M}'} = m_N$. Тада је јасно $\mathbb{M}'$ модел теорије T_1.

Дакле, произвољна коначна подтеорија има модел, па по компактности и T' има модел $\mathbb{M}'$, који различито интерпретира бесконачно много константи, па је бесконачан. Његов редукт $\mathbb{M}$ на језик $\mathcal{L}$ је модел теорије T, па $\mathbb{M} \in \mathcal{K}$, што је контрадикција јер $\mathcal{K}$ садржи само коначне моделе. $\dashv$