Egzamin z logiki i teorii typów, 5 lutego 2025

1. Wiadomo, że schemat $(\neg p \to q \vee r) \to (\neg p \to q) \vee (\neg p \to r)$ nie jest intuicjonistycznym twierdzeniem. Ale jeżeli jakaś formuła postaci $\neg\alpha \to \beta \vee \gamma$ jest twierdzeniem zdaniowej logiki intuicjonistycznej, to jedna z formuł $\neg\alpha \to \beta$ lub $\neg\alpha \to \gamma$ też jest twierdzeniem. Proszę udowodnić ten fakt na dwa sposoby:

   (a) teoriodowodowo (nie odwołując się do semantyki);

   (b) metodami semantyki Kripkego.

2. Które z następujących formuł są twierdzeniami intuicjonistycznej logiki pierwszego rzędu?

   (a) $(\forall x\, \neg\neg P(x)) \to \neg\neg \forall x\, P(x)$

   (b) $\forall x(P(x) \to \exists z\, \neg P(z)) \to \neg\forall x\, \neg\neg P(x)$

   W przypadku odpowiedzi pozytywnej należy skonstruować term dowodowy. Czy odpowiedź się zmieni jeśli kwantyfikatory indywiduowe $\forall x$, $\exists z$ zamienimy na $\forall x{:}\tau$, $\exists z{:}\tau$ i zapytamy czy tak otrzymana formuła rachunku konstrukcji też jest twierdzeniem?

   W przypadku odpowiedzi negatywnej proszę skonstruować kontrmodel Kripkego i kontrprzykład topologiczny. Czy istnieje kontrmodel Kripkego o stałych dziedzinach? Czy istnieje kontrmodel Kripkego o skończonej liczbie stanów?

3. Czy formuła $\forall p(q \vee (p \vee \neg p)) \to q \vee \forall p(p \vee \neg p)$ jest twierdzeniem zdaniowej logiki intuicjonistycznej drugiego rzędu?

4. Dla danego grafu $G = \langle V, E\rangle$ można napisać formułę zdaniową φ, która jest intuicjonistycznym twierdzeniem wtedy i tylko wtedy, gdy G ma cykl Hamiltona. Zakładając, że G ma n wierzchołków, można użyć zmiennych zdaniowych postaci i oraz a_i, gdzie $a \in V$ oraz $i \le n$. Formuła ma kształt $n \to \gamma_1 \to \cdots \to \gamma_N \to 0$, a jej przesłanki γ_j są takie:

   - $(a_1 \to 1) \to 0$, dla $a \in V$;
   - $a_1 \to (b_2 \to 2) \to 1$, dla takich $b, a \in V$, że $b \neq a$ oraz $\langle a, b\rangle \in E$;
   - $a_1 \to b_2 \to (c_3 \to 3) \to 2$, dla takich parami różnych $a, b, c \in V$, że $\langle b, c\rangle \in E$;
   - I tak dalej.

   Tak zdefiniowana formuła jest obliczalna z G, ale jej rozmiary są wykładnicze, bo w zwrocie „i tak dalej" kryją się dowolne ciągi wierzchołków długości nawet n. Zadanie polega na poprawieniu tej konstrukcji w taki sposób, aby otrzymana formuła była obliczalna z grafu G w czasie wielomianowym, co daje redukcję problemu cyklu Hamiltona do intuicjonistycznego rachunku zdań. (Można np. użyć dodatkowych zmiennych.) Czy da się tak otrzymać także wielomianową redukcję problemu cyklu Hamiltona do logiki BCK? (Dowody w BCK to termy „afiniczne": każda zmienna jest używana co najwyżej raz.)

Rozwiązania

1a: Skoro $\neg\alpha \to \beta \vee \gamma$ jest twierdzeniem, to ma dowód normalny, czyli w rozszerzonym rachunku lambda istnieje term zamknięty tego typu w postaci normalnej. Taki term M musi mieć postać $M = \lambda x^{\neg\alpha}.\, N$, gdzie $x : \neg\alpha \vdash N : \beta \vee \gamma$. Jeśli N jest konstruktorem $\mathsf{in}_1(P)$ lub $\mathsf{in}_2(P)$, to term $M = \lambda x^{\neg\alpha}.\, P$ jest dowodem formuły $\neg\alpha \to \beta$ lub formuły $\neg\alpha \to \gamma$. Jeśli zaś N jest eliminatorem, to

musi się zaczynać od aplikacji postaci xR^α, która ma typ $\bot$. Ale wtedy $\neg\alpha \vdash \bot$ i tym bardziej $\neg\alpha \vdash \beta$. Stąd $\vdash \neg\alpha \to \beta$.

1b: Przypuśćmy, że $\nVdash \neg\alpha \to \beta$ oraz $\nVdash \neg\alpha \to \gamma$. Są więc takie dwa modele $\langle C_1, \leq_1, \Vdash_1\rangle$ i $\langle C_2, \leq_2, \Vdash_2\rangle$ i takie stany $c_1 \in C_1$, $c_2 \in C_2$, że $C_1, c_1 \Vdash_1 \neg\alpha$, $C_2, c_2 \Vdash_2 \neg\alpha$, $C_1, c_1 \nVdash_1 \beta$ oraz $C_2, c_2 \nVdash_2 \gamma$. Bez straty ogólności można założyć, że c_1 i c_2 są, odpowiednio, elementami najmniejszymi w C_1 i C_2. Wziąwszy $c \notin C_1 \cup C_2$, tworzymy nowy model $\langle C, \leq, \Vdash\rangle$ gdzie $C = C_1 \cup C_2 \cup \{c\}$, relacja $\Vdash$ jest sumą relacji $\Vdash_1$ i $\Vdash_2$, a porządek $\leq$ powstaje z $\leq_1 \cup \leq_2$ przez dodanie c jako elementu najmniejszego. Wtedy $C, c \Vdash \neg\alpha$, oraz $C, c \nVdash \beta$ (bo $C, c_1 \nVdash_1 \beta$) a także $C, c \nVdash \gamma$ (bo $C, c_2 \nVdash_2 \gamma$). Stąd $C, c \nVdash \neg\alpha \to \beta \vee \gamma$.

2a: Ta formuła nie jest twierdzeniem. Kontrmodelem Kripkego (o stałych dziedzinach) jest na przykład struktura $\langle \mathbb{N}, \leq, \{\mathcal{A}_n\}_{n\in\mathbb{N}}\rangle$, gdzie $\mathcal{A}_n = \langle \mathbb{N}, P^n\rangle$ i $P^n = \{0, \ldots, n\}$. Warunek $\neg\neg P(x)$ jest wymuszony w każdym stanie dla każdego elementu, bo każda liczba n należy do P^m dla $m \geq n$. Zatem $0 \Vdash \forall x\, \neg\neg P(x)$. Jednak warunek $\forall x\, P(x)$ nie jest wymuszony nigdzie, skąd $0 \nVdash \neg\neg\forall x\, P(x)$.

Nasza formuła jest jednak wymuszona przez każdy model $\langle C, \leq, \{\mathcal{A}_c\}_{c\in C}\rangle$ o skończonej liczbie stanów. Niech bowiem $c \in C$ i niech $C, d \Vdash \forall x\, \neg\neg P(x)$ dla pewnego $d \geq c$. Wtedy w każdym stanie $e \geq d$ i przy każdym wartościowaniu ϱ zachodzi $C, e, \varrho \Vdash \neg\neg P(x)$. Jeśli e jest stanem końcowym, to mamy po prostu $C, e \Vdash \forall x\, P(x)$. A skoro model jest skończony, to wszystkie drogi prowadzą do stanów końcowych, więc $C, d \Vdash \neg\neg\forall x\, P(x)$.

Kontrprzykładem topologicznym jest $\mathcal{O}(\mathbb{R})$-struktura o dziedzinie $\mathbb{Q}$, gdzie $P(q) = \mathbb{R} - \{q\}$ dla $q \in \mathbb{Q}$. Przy wartościowaniu $v(x) = q$ wartością formuły $\neg\neg P(x)$ jest $\mathbb{R}$ i takie też jest znaczenie zdania uniwersalnego $\forall x\, \neg\neg P(x)$. Ale zdanie $\forall x\, P(x)$ ma wartość zero, bo iloczyn wszystkich zbiorów $\mathbb{R} - \{q\}$ jest brzegowy. Stąd także $\neg\neg\forall x\, P(x)$ ma wartość zero.

2b: Ta formuła jest twierdzeniem, a jej dowód można zapisać w postaci takiego termu:

$$\lambda X^{\forall x(P(x)\to\exists z\,\neg P(z))}\lambda Y^{\forall x\,\neg\neg P(x)}.\, Yx_0(\lambda Z^{P(x_0)}.\, \mathbf{let}\ Xx_0Z = [z, V : \neg P(z)]\ \mathbf{in}\ YzV).$$

Ten term ma zmienną wolną x_0, co jest dozwolone w logice pierwszego rzędu („dogmat o niepustości dziedziny"). Jednak dowód w rachunku konstrukcji musi być termem zamkniętym, a to nie zawsze jest możliwe. Na przykład formuła $\forall x^\bot\,(P(x) \to \exists z^\bot.\, \neg P(z)) \to \neg\forall x^\bot.\, \neg\neg P(x)$, gdzie $\bot = \forall p{:}*\,.\, p$, nie jest twierdzeniem rachunku konstrukcji. Istotnie, na mocy *ex falso*, zarówno $\forall x^\bot\,(P(x) \to \exists z^\bot.\, \neg P(z))$ jak i $\forall x^\bot.\, \neg\neg P(x)$ są twierdzeniami, a zatem z naszej formuły natychmiast wynika sprzeczność. Tymczasem rachunek konstrukcji nie jest sprzeczny, bo ma własność silnej normalizacji.

3: Tak. Jeśli $x : \forall p(q \vee (p \vee \neg p))$, to aplikacja xq ma typ $q \vee (q \vee \neg q)$ równoważny alternatywie $q \vee \neg q$. Oczywiście $q \vdash q \vee \forall p(p \vee \neg p)$, więc wystarczy sprawdzić, że także $\forall p(q \vee (p \vee \neg p)), \neg q \vdash \forall p(p \vee \neg p)$. A to łatwe, bo dla x jak wyżej mamy $xp : q \vee (p \vee \neg p)$, a pierwszy składnik alternatywy jest sprzeczny z $\neg q$. Ten dowód można zapisać w postaci lambda-termu:

$$\lambda x^{\forall p(q\vee(p\vee\neg p))}.\, xq[z^q.\, \mathsf{in}_1(z);\ w^{q\vee\neg q}.\, w[z^q.\, \mathsf{in}_1(z);\ y^{\neg q}.\, \mathsf{in}_2(\Lambda p.\, xp[v^q.\, yv[p \vee \neg p];\ u^{p\vee\neg p},\ u\,])]].$$

4: Dodajemy zmienne a^i o znaczeniu „wierzchołek a nie został wybrany w i-tym kroku" i dla każdego $i = 1, \ldots, n$ piszemy składowe $a^1 \to a^2 \to \cdots \to a^{i-1} \to b_{i-1} \to (a_i \to b^i \to \cdots \to z^i \to i) \to i - 1$, gdzie $\langle b, a\rangle \in E$ oraz $b, \ldots, z$ to wszystkie wierzchołki oprócz a.

Czyli zaczynamy od $(a_1 \to b^1 \to \cdots \to z^1 \to 1) \to 0$, a potem na przykład dla $i = 6$ mamy założenia postaci $a^1 \to a^2 \to \cdots \to a^6 \to b_6 \to (a_7 \to b^7 \to \cdots \to z^7 \to 7) \to 6$. Wszystkich takich założeń jest n^3, każde długości $\mathcal{O}(n)$. Każde jest w dowodzie użyte najwyżej raz. Także dodawane do otoczenia założenia postaci a^i, a_i, są używane co najwyżej raz: zmienna typu a^i, gdy dla pewnego $j > i$ wprowadzamy założenie a_j, a zmienna typu a_j, gdy wprowadzamy jakieś b_{j+1}.

Żeby to był naprawdę cykl, i żeby nie popsuć afiniczności, trzeba:
(1) zamienić założenia $(a_1 \to b^1 \to \cdots \to z^1 \to 1) \to 0$ na $(a_1 \to a'_1 \to b^1 \to \cdots \to z^1 \to 1) \to 0$;
(2) zamiast n przyjąć założenia postaci $b_n \to a'_1 \to n$, dla każdej krawędzi $\langle b, a\rangle$.