

Example problems in logic and type theory¹

1. Which of the following formulas are intuitionistic theorems?
 - (a) $(a \rightarrow b \vee c) \rightarrow (a \rightarrow b) \vee (a \rightarrow c)$;
 - (b) $((b \vee c) \rightarrow a) \rightarrow (b \rightarrow a) \wedge (c \rightarrow a)$;
 - (c) $\neg\neg(a \vee \neg a)$;
 - (d) $\neg\neg a \vee \neg\neg\neg a$;
 - (e) $\neg\neg\neg a \rightarrow \neg a$;
2. Show that:
 - (a) $((\neg\neg p \rightarrow p) \rightarrow p) \leftrightarrow \neg\neg p$;
 - (b) $(\neg p \rightarrow p) \leftrightarrow \neg\neg p$;
 - (c) $\neg(\neg\neg p \rightarrow q) \leftrightarrow \neg(p \rightarrow q)$;
 - (d) $(p \rightarrow a) \rightarrow d, (p \rightarrow b) \rightarrow d, p \rightarrow a \vee b \not\vdash p \rightarrow d$;
 - (e) $(p \rightarrow q) \vee (r \rightarrow q) \rightarrow q, \neg(p \wedge r) \vdash q$;
 - (f) $((r \rightarrow a) \rightarrow p) \vee ((d \rightarrow b) \rightarrow q), p \rightarrow x, \neg(a \rightarrow x), b \vdash q$;
 - (g) $(p \vee \neg p) \rightarrow \neg q \vdash \neg q$;
 - (h) $((a \rightarrow c) \rightarrow d) \rightarrow e, ((b \rightarrow c) \rightarrow d) \rightarrow e \not\vdash ((a \vee b \rightarrow c) \rightarrow d) \rightarrow e$;
 - (i) $((p \rightarrow q) \rightarrow r) \rightarrow (p \rightarrow r) \rightarrow r \rightarrow q \vdash q$;
 - (j) $(p \rightarrow q) \leftrightarrow ((p \rightarrow q) \rightarrow p) \rightarrow q$.
- ^R 3. Które z następujących formuł są twierdzeniami intuicjonistycznymi? (Aby uzasadnić odpowiedź pozytywną można np. podać dowód albo odpowiedni λ -term; jeśli odpowiedź jest negatywna można podać kontrprzykład topologiczny, model Kripkego itp.)
 - (a) $(\neg q \rightarrow q) \leftrightarrow \neg\neg q$;
 - (b) $((\neg\neg q \rightarrow q) \rightarrow \neg q) \rightarrow \neg q$;
 - (c) $((\neg\neg p \rightarrow p) \rightarrow p \vee \neg p) \rightarrow \neg p \vee \neg\neg p$. (Scott)
- ^R 4. Które z następujących formuł są intuicjonistycznymi twierdzeniami, a które nie? W przypadku odpowiedzi pozytywnej należy skonstruować dowód (czy można to zrobić bez reguły ex falso?), przy odpowiedzi negatywnej można np. wskazać model Kripkego (wystarczy jeden sposób).
 - (a) $((\neg\neg p \rightarrow p) \rightarrow q) \rightarrow q$.
 - (b) $((\neg\neg p \rightarrow p) \rightarrow \neg q) \rightarrow \neg q$.
- ^R 5. Która z następujących formuł zdaniowych jest twierdzeniem intuicjonistycznym?
 - (a) $(p \rightarrow q \rightarrow r) \rightarrow ((p \rightarrow r) \rightarrow s) \rightarrow ((q \rightarrow r) \rightarrow s) \rightarrow s$;
 - (b) $(p \rightarrow q \rightarrow r) \rightarrow ((p \rightarrow r) \rightarrow s) \rightarrow ((q \rightarrow r) \rightarrow s) \rightarrow (s \rightarrow r) \rightarrow r$.
6. Show that the following formulas are not intuitionistically provable. Are they valid in two-element Kripke models?
 - (a) $p \vee \neg q \vee (p \rightarrow q)$; (Hosoi)
 - (b) $(\neg p \rightarrow q) \rightarrow ((q \rightarrow p) \rightarrow q) \rightarrow q$; (Łukasiewicz)
 - (c) $((p \rightarrow q) \rightarrow r) \rightarrow ((r \rightarrow p) \rightarrow r) \rightarrow r$.
7. Prove that:
 - (a) $\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$;
 - (b) $\neg(p \wedge q) \leftrightarrow \neg(\neg\neg p \wedge \neg\neg q)$;

¹This is a random collection from my old files (in Polish) and handwritten notes. The problems have not been verified and they may include inaccuracies or typographical or other errors. Some questions may be hard to answer. Use at your own risk.

$$(c) \neg(p \rightarrow q) \leftrightarrow (\neg\neg p \wedge \neg q).$$

Conclude that every formula of the form $\neg\alpha$ is equivalent to one without disjunction.

- ^R 8. Show that if $\alpha \rightarrow \beta$ is a propositional classical tautology then $\neg\beta \rightarrow \neg\alpha$ is an intuitionistic theorem. Does it hold in first-order logic?
- ^R 9. Is *ex falso* necessary to prove $\neg\neg(\neg\neg p \rightarrow p)$?
- ^R10. Niech $\alpha = \neg p \rightarrow q$ i niech $\beta = \neg\neg(p \vee q)$. Która z implikacji $\alpha \rightarrow \beta$ i $\beta \rightarrow \alpha$ jest twierdzeniem intuicjonistycznym?
- ^R11. Wykazać, że żadna z następujących formuł nie jest intuicjonistyczną tautologią. Które z nich są wymuszane przez dowolny liniowo uporządkowany model Kripkego?
- (a) $\neg p \vee \neg\neg p$;
 (b) $(p \rightarrow q) \vee (q \rightarrow p)$; (Gödel-Dummett, a właściwie Skolem)
 (c) $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$.
- ^R12. Formuły $\alpha = (((e \rightarrow d) \rightarrow c) \rightarrow b) \rightarrow a$ i $\beta = (e \rightarrow (d \rightarrow a) \rightarrow b) \rightarrow (c \rightarrow b) \rightarrow a$ są klasycznie równoważne. Czy któraś z implikacji $\alpha \rightarrow \beta$, $\beta \rightarrow \alpha$ jest twierdzeniem intuicjonistycznym? W przypadku odpowiedzi pozytywnej należy skonstruować dowód, przy odpowiedzi negatywnej można np. wskazać model Kripkego.²
- ^R13. Rozszerzamy język rachunku zdań o nowy jednoargumentowy spójnik $\sharp$. W modelach Kripkego przyjmujemy, że $c \Vdash \sharp\alpha$, wtedy i tylko wtedy, gdy stany wymuszające α tworzą „przekrój” ponad c , tj. w każdym maksymalnym (skończonym lub nieskończonym) ciągu rosnącym $c = c_0 < c_1 < c_2 < \dots$ jest takie c_n , że $c_n \Vdash \alpha$.
 Proszę udowodnić:
 (a) że $\Vdash \sharp\alpha \rightarrow \neg\neg\alpha$, ale nie na odwrót.
 (b) że spójnik $\sharp$ nie jest definiowalny w intuicjonistycznym rachunku zdań.
- ^R14. Czy każdy zbiór liniowo uporządkowany z elementem pierwszym i ostatnim jest algebrą Heytinga? Czy istnieje związek pomiędzy liniowo uporządkowanymi modelami Kripkego i liniowo uporządkowanymi algebrami Heytinga?
- ^R15. Korzystając ze znanych własności rachunku lambda z typami prostymi, proszę ustalić, czy następujące formuły są intuicjonistycznymi twierdzeniami:
 (a) $((p \rightarrow q) \rightarrow r) \rightarrow (p \rightarrow r) \rightarrow r$;
 (b) $((((p \rightarrow q) \rightarrow r) \rightarrow (p \rightarrow r) \rightarrow r) \rightarrow q) \rightarrow q$.
- ^R16. Dla następujących formuł wskazać kontrprzykłady w modelach Kripkego i kontrprzykłady w algebrach Heytinga:
 (a) $(\neg p \rightarrow q \vee r) \rightarrow ((\neg p \rightarrow q) \vee (\neg p \rightarrow r))$; (Kreisel-Putnam)
 (b) $(q \wedge r \rightarrow \neg p) \rightarrow ((q \rightarrow \neg p) \vee (r \rightarrow \neg p))$.
- ^R17. Niech $\mathcal{H}$ będzie algebrą Heytinga (można założyć, że jest to algebra formuł intuicjonistycznego rachunku zdań) i niech $F = \{a \in \mathcal{H} \mid \neg a = 0\}$. Definiujemy relację $\approx$:
 $a \approx b$ wtedy i tylko wtedy, gdy $a \Rightarrow b \in F$ oraz $b \Rightarrow a \in F$.
 Udowodnić, że
 (a) zbiór F jest filtrem³ w $\mathcal{H}$;
 (b) relacja $\approx$ jest kongruencją w $\mathcal{H}$;
 (c) algebra ilorazowa $\mathcal{H}/\approx$ jest algebrą Boole’a.
- ^R18. Wiedząc, że każda klasyczna tautologia zdaniowa jest prawdziwa w dowolnej algebrze

²Wskazówka: wystarczy model Kripkego o 2 stanach.

³A *filter* is a nonempty set closed under intersections and upward closed.

Boole'a, wywnioskować z zadania 17 twierdzenie Gliwienki.

19. Każda klasyczna tautologia zdaniowa zbudowana wyłącznie z $\neg$ i $\wedge$ jest twierdzeniem intuicjonistycznym.⁴
- ^R20. Dany graf skierowany $G = (V, E)$ o k wierzchołkach. Napisać formułę zdaniową, która jest intuicjonistycznym twierdzeniem wtedy i tylko wtedy gdy w G nie ma cyklu Hamiltona. Konstrukcja formuły z grafu G powinna być możliwa w czasie wielomianowym.
- ^R21. Niech $\varphi = \forall x (P(x) \vee \neg P(x))$, $\psi = \neg \forall x P(x)$ oraz $\vartheta = \exists x \neg P(x)$. Która z implikacji $\varphi \wedge \psi \rightarrow \vartheta$ i $\varphi \wedge \vartheta \rightarrow \psi$ jest twierdzeniem intuicjonistycznym?
- ^R22. Która z następujących formuł pierwszego rzędu jest twierdzeniem intuicjonistycznym?
- (a) $\neg \forall x P(x) \rightarrow \neg \forall x \neg \neg P(x)$;
 - (b) $\neg \exists x P(x) \rightarrow \neg \exists x \neg \neg P(x)$.
23. Which of the following formulas are intuitionistic theorems? Which are forced in Kripke models with constant domains? Which are valid in the Heyting algebra $\mathcal{O}(\mathbb{R})$ of open subsets of the real line?
- (a) $\exists x (P(0) \vee P(1) \rightarrow P(x))$;
 - (b) $\forall x ((P(x) \rightarrow P(y)) \rightarrow Q) \rightarrow Q$
 - (c) $(\forall x P(x) \rightarrow \exists y Q(y)) \rightarrow \exists x (P(x) \rightarrow Q(y))$;
 - (d) $\forall y \exists x (P(x) \rightarrow Q(y)) \rightarrow \exists x \forall y (P(x) \rightarrow Q(y))$;
 - (e) $\exists x (P(x) \rightarrow \forall x P(x))$;
 - (f) $\forall x (P(x) \vee Q(x)) \rightarrow \exists x P(x) \vee \forall y Q(y)$
 - (g) $\forall x (P(x) \vee \neg P(x)) \rightarrow \exists x P(x) \vee \forall y \neg P(y)$;
 - (h) $\forall x (P(x) \vee \neg P(x)) \rightarrow \neg \neg \exists x P(x) \rightarrow \exists x P(x)$; (Markov's Principle)
 - (i) $\forall x (P(a, x) \rightarrow P(x, b)) \rightarrow P(a, a) \rightarrow P(b, b)$;
 - (j) $((A \rightarrow \exists x P(x)) \rightarrow B) \leftrightarrow (\forall x ((A \rightarrow P(x)) \rightarrow B))$;
 - (k) $\forall x (P(x) \rightarrow \exists z \neg P(z)) \rightarrow \neg \forall x \neg \neg P(x)$;
 - (l) $\forall x (\neg P(x) \vee \exists x \neg \neg P(x)) \rightarrow \forall x \neg P(x) \vee \exists x \neg \neg P(x)$;
 - (m) $\exists x (\exists x P(x) \rightarrow P(x))$;
 - (n) $(A \rightarrow \exists x P(x)) \leftrightarrow \exists x (A \rightarrow P(x))$;
 - (o) $\neg \neg (\forall x P(x) \vee \exists x \neg P(x))$.
- ^R24. Które implikacje pomiędzy następującymi formułami są intuicjonistycznie prawdziwe?
- (a) $\neg \forall x P(x)$;
 - (b) $\neg \forall x \neg \neg P(x)$;
 - (c) $\neg \neg \exists x \neg P(x)$.
- ^R25. Niech $\gamma = \forall x \exists y (P(y) \wedge (Q(y) \rightarrow Q(x)))$, $\beta = \neg \forall x Q(x)$ oraz $\delta = \forall x (P(x) \rightarrow (Q(x) \vee S))$. Udowodnić, że formuła $\gamma \rightarrow \beta \rightarrow \delta \rightarrow S$ nie jest intuicjonistycznym twierdzeniem, ale jest wymuszana przez wszystkie modele Kripkego o stałych dziedzinach.
- ^R26. Formuły $\gamma = \forall y P(y) \rightarrow \exists x Q(x)$ i $\delta = \exists x (P(x) \rightarrow Q(x))$ są klasycznie równoważne. Czy któraś z implikacji $\gamma \rightarrow \delta$, $\delta \rightarrow \gamma$ jest twierdzeniem intuicjonistycznym? W przypadku odpowiedzi pozytywnej należy skonstruować dowód, w razie odpowiedzi negatywnej proszę podać dwa kontrprzykłady: jeden topologiczny, drugi Kripkego.
- ^R27. Formuła $\neg \neg (\forall x P(x) \vee \exists x \neg P(x))$ nie jest intuicjonistycznym twierdzeniem. Proszę podać kontrprzykład topologiczny i kontrprzykład Kripkego.
- ^R28. Rozpatrzmy następujące schematy aksjomatów:

⁴ Wskazówka: indukcja z użyciem tw. Gliwienki.

- (A) $\forall x(\psi \vee \varphi(x)) \rightarrow \psi \vee \forall x \varphi(x)$; (Grzegorzcyk)
 (B) $(\forall x \varphi(x) \rightarrow \psi) \rightarrow \exists x (\varphi(x) \rightarrow \psi)$;
 (C) $\exists x(\varphi(x) \rightarrow \forall y \varphi(y))$.

Czy w logice intuicjonistycznej pierwszego rzędu rozszerzonej o jeden z tych schematów można udowodnić któryś z pozostałych?

29. Które z następujących formuł są twierdzeniami intuicjonistycznymi?

- (a) $\neg\neg\exists x P(x) \leftrightarrow \exists x\neg\neg P(x)$;
 (b) $\neg\neg\exists x\neg\neg P(x) \leftrightarrow \exists x\neg\neg P(x)$;
 (c) $\neg\neg\exists x P(x) \leftrightarrow \neg\neg\exists x\neg\neg P(x)$;
 (d) $\neg\forall P(x) \leftrightarrow \neg\neg\exists x\neg P(x)$;
^R(e) $\forall x(\neg P(x) \rightarrow \exists y Q(y)) \rightarrow \forall x\exists y(\neg P(x) \rightarrow Q(y))$.

30. Rozpatrzmy sygnaturę złożoną z jednego unarnego symbolu relacyjnego r . Dla tej sygnatury weźmy model Kripkego o trzech stanach a, b, c uporządkowanych tak, że a jest najmniejszym elementem, a dwa pozostałe są nieporównywalne. Z tymi stanami związane są odpowiednio struktury $D_a = \langle \{0\}, \emptyset \rangle$, $D_b = D_c = \langle \{0, 1\}, \{1\} \rangle$. Pokazać, że jeśli $\varrho(x) = 0$ dla dowolnej zmiennej x , a kwantyfikator $\exists$ nie występuje w formule φ , to w naszym modelu warunek $a, \varrho \Vdash \varphi$ jest równoważny każdemu z warunków $b, \varrho \Vdash \varphi$ oraz $c, \varrho \Vdash \varphi$. Wywnioskować stąd, że w logice intuicjonistycznej pierwszego rzędu nie można zdefiniować kwantyfikatora egzystencjalnego za pomocą pozostałych spójników.

^R31. Consider a first-order language with binary predicates P and Q , unary function symbols a and b , and one constant ε . We write terms without parentheses, e.g., $abba(x)$ abbreviates $a(b(b(a(x))))$ and $abba$ abbreviates $a(b(b(a(\varepsilon))))$. Let $w_1, \dots, w_n, v_1, \dots, v_n$ be words over $\{a, b\}$, and let Γ consist of all formulas of the forms:

- $Q(\varepsilon, \varepsilon)$, and $P(\varepsilon, \varepsilon) \rightarrow \perp$;
- $\forall xy(P(w_i(x), v_i(y)) \rightarrow P(x, y))$, for $i = 1, \dots, n$;
- $\forall xy(Q(x, y) \rightarrow P(x, y))$;
- $\forall xy(Q(x, y) \rightarrow Q(a(x), a(y)))$, and $\forall xy(Q(x, y) \rightarrow Q(b(x), b(y)))$.

Is the Post correspondence problem $(w_1, v_1), \dots, (w_n, v_n)$ solvable if and only if $\Gamma \vdash \perp$?

^R32. Dany jest automat dwulicznikowy o zbiorze stanów Q , stanie początkowym q_0 i końcowym q_f . Napisać formułę logiki pierwszego rzędu, która jest twierdzeniem intuicjonistycznym wtedy i tylko wtedy, gdy automat akceptuje konfigurację początkową $(q_0, 0, 0)$. Formuła powinna być efektywnie konstruowalna z automatu. Wskazówka: symbole relacyjne mogą reprezentować stany automatu. Można użyć symboli funkcyjnych dla następnika i zera.

^R33. *Automat z kolejką* ma skończony zbiór stanów i kolejkę (słowo nad ustalonym alfabetem), na której może wykonywać takie operacje:

- $p : \text{insert}(A); \text{goto } q$ (w stanie p wstaw A na koniec kolejki; przejdź do stanu q);
- $p : \text{delete}; \text{goto } q$ (w stanie p usuń literę z początku kolejki; przejdź do q);
- $p : \text{peek}(A); \text{goto } q$ (ze stanu p przejdź do q jeśli na początku kolejki jest A).

Dla danego automatu z kolejką proszę skonstruować formułę pierwszego rzędu, która jest intuicjonistycznym twierdzeniem wtedy i tylko wtedy, gdy automat uruchomiony w stanie q_0 z kolejką $\#$ zatrzyma się w stanie końcowym q_f . Można zakładać, że kolejka nigdy nie jest pusta.⁵

⁵ Wskazówka: Otoczenie Γ kodujące kolejkę $w = A_1 \dots A_n$ może się składać z formuł atomowych $S(x_1, x_2), S(x_2, x_3), \dots, S(x_{n-1}, x_n), A_1(x_1), \dots, A_n(x_n)$ i pewnej ilości śmieci (niepotrzebnych ale nieszkod-

^R34. Niech $\tau = \forall r(\forall q(q \rightarrow r) \rightarrow r)$ i niech $\sigma = \forall p((\tau \rightarrow p) \rightarrow p)$. Napisać takie termy $there : \tau \rightarrow \sigma$ i $back : \sigma \rightarrow \tau$, że w systemie **F** zachodzi równość $\mathbf{I} =_{\beta} \lambda x^{\tau} back(there\ x)$. Czy każdy term zamknięty typu σ jest beta-równy wyrażeniu postaci $there(N)$?

35. Prove the following:

- (a) $\neg \exists p \neg(p \vee \neg p)$;
- (b) $\forall p(\neg \neg p \rightarrow \exists q(p \leftrightarrow (\neg q \vee q)))$;
- (c) $\forall t(((t \rightarrow r) \rightarrow q) \rightarrow (t \rightarrow s) \rightarrow p) \leftrightarrow (((s \rightarrow r) \rightarrow q) \rightarrow p)$;
- (d) $\varphi \leftrightarrow ((\varphi \rightarrow p) \rightarrow p)$, where $\varphi = \forall r(((r \rightarrow p) \rightarrow p) \rightarrow r) \rightarrow r$.
- (e) $\varphi \leftrightarrow ((\varphi \rightarrow p) \rightarrow q)$, where $\varphi = \forall r(((r \rightarrow p) \rightarrow q) \rightarrow r) \rightarrow r$.

36. Which of the following second-order propositional formulas are intuitionistic theorems?

- (a) $\neg \neg \forall p(p \vee \neg p)$;
- ^R(b) $\forall p(q \vee ((p \rightarrow q) \rightarrow q) \rightarrow p) \rightarrow q \vee \forall p(((p \rightarrow q) \rightarrow q) \rightarrow p)$;⁶
- (c) $\forall p(\neg p \rightarrow q \vee r) \rightarrow \forall p(\neg p \rightarrow q) \vee \forall p(\neg p \rightarrow r)$;
- (d) $\forall p(q \vee (q \rightarrow p)) \leftrightarrow \neg q \vee q$;
- ^R(e) $\forall pq((p \rightarrow q) \vee (q \rightarrow p)) \rightarrow \forall p(\neg p \vee \neg \neg p)$;
- ^R(f) $\forall p(\neg p \vee \neg \neg p) \rightarrow \forall pq((p \rightarrow q) \vee (q \rightarrow p))$;
- (g) $\exists p. ((p \rightarrow q) \rightarrow p) \rightarrow r$;
- (h) $\exists p(((q \rightarrow p) \rightarrow p) \rightarrow r) \leftrightarrow (q \rightarrow r)$;
- (i) $\exists p((r \rightarrow p) \rightarrow q) \leftrightarrow (\neg r \rightarrow q)$;
- (j) $\exists p \neg((p \rightarrow q) \rightarrow p)$;
- (k) $\exists p((p \rightarrow q) \rightarrow r) \leftrightarrow ((q \rightarrow r) \rightarrow q) \rightarrow r$.
- ^R(l) $\neg \neg p \rightarrow \exists q((p \rightarrow \neg q \vee q) \rightarrow p)$. (Połacik)
- (m) $\forall p(q \vee p \vee \neg p) \rightarrow q \vee \forall p(p \vee \neg p)$.
- (n) $\forall p(q \vee \neg p \vee \neg \neg p) \rightarrow q \vee \forall p(\neg p \vee \neg \neg p)$.

^R37. Dla następujących formuł logiki zdaniowej drugiego rzędu znaleźć (intuicjonistycznie) równoważne formuły bez kwantyfikatorów:

- (a) $\exists p((q \rightarrow p) \rightarrow q)$;
- (b) $\exists p(((q \rightarrow p) \rightarrow p) \rightarrow r)$;
- (c) $\forall p(q \vee (q \rightarrow p))$;
- (d) $\exists p(q \vee (q \rightarrow p))$.

^R38. W systemie **F** definiujemy produkt $\tau \times \varrho$ jako $\tau \times \varrho = \forall p((\tau \rightarrow \varrho \rightarrow p) \rightarrow p)$. Para uporządkowana $\langle M^{\tau}, N^{\varrho} \rangle$ to term $\Lambda p \lambda x^{\tau \rightarrow \varrho \rightarrow p}. xMN$. Podać przykład takich typów τ i ϱ , że typ $\tau \times \varrho$ ma „za dużo elementów” tj. istnieje term zamknięty tego typu w postaci normalnej, który nie jest parą uporządkowaną.

^R39. Udowodnić, że system Gödla **T** można interpretować w systemie Girarda **F**. Jak wiadomo, w systemie **F**, (czyli w polimorficznym rachunku lambda) można reprezentować liczby naturalne jako termy zamknięte typu $\omega = \forall p((p \rightarrow p) \rightarrow (p \rightarrow p))$. Należy zdefiniować polimorficzny rekursor, tj. term zamknięty

$$\mathbf{R} : \forall p[(\omega \rightarrow p \rightarrow p) \rightarrow (\omega \rightarrow p \rightarrow p)],$$

który dla dowolnego typu σ spełnia warunki

$$\mathbf{R}\sigma M(succ\ n)N =_{\beta} Mn(\mathbf{R}\sigma MnN) \quad \text{oraz} \quad \mathbf{R}\sigma M0N =_{\beta} N,$$

liwych innych założeń). Cel dowodowy postaci $p(x_1, x_n)$ wskazuje na bieżący stan p i zawiera wskaźniki do końca i początku kolejki. Zadanie polega na dodaniu do Γ dodatkowych założeń Δ , w ten sposób, aby dowód normalny osądu $\Gamma, \Delta \vdash p(x_1, x_n)$ wymagał dowodu osądu $\Gamma', \Delta \vdash p'(x'_1, x'_n)$, gdzie Γ' i $p'(x'_1, x'_n)$ przedstawiają kolejną konfigurację automatu.

⁶Wskazówka: consider the instantiation $p := \neg q$.

gdzie $\mathbf{n}$ jest dowolnym liczebnikiem, a symbol *succ* oznacza term reprezentujący operację następnika. Inaczej mówiąc, term $\mathbf{R}\sigma$ ma się zachowywać jak rekursor $\mathbf{R}_\sigma$ w systemie $\mathbf{T}$.

^{R40.} Obiekty typu *krzak* to drzewa, których liście są etykietowane liczbami naturalnymi, a wierzchołki wewnętrzne mają stopień wyjściowy trzy i nie są etykietowane. Jak można zdefiniować typ *krzak*:

- (a) w składni systemu Coq lub podobnej?
- (b) w systemie $\mathbf{F}$?
- (c) w rachunku lambda z operatorem μ i konstruktorami $\times$, $\oplus$, int ?

Jak wygląda zasada indukcji dla typu *krzak*?

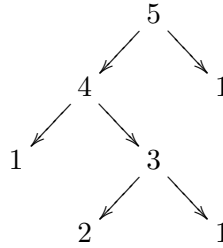
^{R41.} Rozważamy rachunek lambda z typami prostymi, do którego dodajemy nowe stałe typowe i równania między typami. W każdym przypadku należy skonstruować term, który ma nieskończony ciąg redukcji.

- (a) Stałe typowe c_0, c_1, c_2 spełniają równania: $c_0 = c_1 \rightarrow p$, $c_1 = c_2 \rightarrow p$, $c_2 = c_0 \rightarrow p$. Wskazówka: rozpatrzmy termy: $C_0 = \lambda y_1^{c_1}. y_1 C_2$, $C_2 = \lambda y_0^{c_0}. y_0 C_1$, $C_1 = \lambda y_2^{c_2}. y_2 y_0$.
- (b) Teraz równania są $c_0 = c_1 \rightarrow \beta_0$, $c_1 = c_2 \rightarrow \beta_1$, $c_2 = c_0 \rightarrow \beta_2$, gdzie $\beta_0, \beta_1, \beta_2$ są dowolnymi typami.
- (c) A teraz tak: $c_0 = \vec{\alpha}_0 \rightarrow c_1 \rightarrow \beta_0$, $c_1 = \vec{\alpha}_1 \rightarrow c_2 \rightarrow \beta_1$, $c_2 = \vec{\alpha}_2 \rightarrow c_0 \rightarrow \beta_2$, gdzie $\vec{\alpha}_0, \vec{\alpha}_1, \vec{\alpha}_2$ są dowolnymi ciągami typów.
- (d) No to przypuśćmy, że mamy równanie $c_0 = \tau(c_0)$, gdzie c_0 występuje w τ na pozycji negatywnej. Co teraz? (W tej części wystarczy szkic dowodu bez szczegółów.)

^{R42.} Typ $\tau = \forall p((p \rightarrow p \rightarrow \omega \rightarrow p) \rightarrow (\omega \rightarrow p) \rightarrow p)$ jest w systemie $\mathbf{F}$ odpowiednikiem typu indukcyjnego drzew binarnych etykietowanych liczbami naturalnymi:

Inductive $\mathbf{T} : \mathbf{Set} := \mathbf{kons} : \mathbf{T} \rightarrow \mathbf{T} \rightarrow \mathbf{nat} \rightarrow \mathbf{T} \mid \mathbf{leaf} : \mathbf{nat} \rightarrow \mathbf{T}$.

Na przykład term $T = \Lambda p \lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. x \underline{3}$ to samotny liść oznaczony trójką, a drzewo $\lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. f(f(x \underline{1})(f(x \underline{2})(x \underline{1}) \underline{3}) \underline{4})(x \underline{1}) \underline{5}$ widać na obrazku.



- (a) Jakie operacje na drzewach są reprezentowane wyrażeniami:⁷⁸
 - $\lambda t:\tau. t\omega(\lambda p:\omega \lambda q:\omega \lambda x:\omega. p + q + x) \mathbf{I}$?
 - $\lambda t:\tau. t\tau(\lambda p:\tau \lambda q:\tau \lambda x:\omega. p)(\lambda x:\omega. T)$?
- (b) Napisać termy typu $\tau \rightarrow \omega$ reprezentujące takie funkcje:
 - liczba liści drzewa;
 - wysokość drzewa.
- (c) Napisać term typu $\tau \rightarrow \tau$ reprezentujący operację wyzerowania wszystkich etykiet.

^{R43.} Przez *równość Leibniza* w typie τ rozumiemy taki konstruktor $\mathbf{Eq}^\tau : (\forall x:\tau)(\forall y:\tau).*$

$$\mathbf{Eq}^\tau = (\lambda x:\tau)(\lambda y:\tau)(\forall P:\tau \Rightarrow *) (Px \rightarrow Py).$$

⁷⁸Operacje na liczbach naturalnych są takie jak zwykle.

⁸Podpowiedź: pierwszą z funkcji w części 41a można w Coqu zdefiniować tak:

Fixpoint $\mathbf{F}(t:\mathbf{T}) : \mathbf{nat} := \mathbf{match} \ t \ \mathbf{with} \ (\mathbf{kons} \ t1 \ t2 \ k) \Rightarrow (\mathbf{F} \ t1) + (\mathbf{F} \ t2) + k \mid (\mathbf{leaf} \ k) \Rightarrow k \ \mathbf{end}$.

Należy udowodnić, że następujące typy są niepuste:⁹

- $(\forall x:\tau) \mathbf{Eq}^\tau xx$ oraz $(\forall x:\tau)(\forall y:\tau)(\mathbf{Eq}^\tau xy \rightarrow \mathbf{Eq}^\tau yx)$;
- $(\forall x:\tau)(\forall y:\tau)(\forall z:\tau)(\mathbf{Eq}^\tau xy \rightarrow \mathbf{Eq}^\tau yz \rightarrow \mathbf{Eq}^\tau xz)$;
- $(\forall P:\tau \Rightarrow *) (\forall x:\tau)(\forall y:\tau)(\mathbf{Eq}^\tau xy \rightarrow Px \rightarrow Py)$.

^{R44}. Strumień można reprezentować w rachunku lambda na kilka sposobów. Pierwszy używa operatora największego punktu stałego ν . Definiujemy typ $\mathbf{stream} := \nu p. \mathbf{int} \times p$ z operacjami $\mathit{Coit}_\sigma : (\sigma \rightarrow \mathbf{int} \times \sigma) \rightarrow \sigma \rightarrow \mathbf{stream}$ i $\mathit{Unfold} : \mathbf{stream} \rightarrow \mathbf{int} \times \mathbf{stream}$, dla których przyjmujemy regułę redukcji $\mathit{Unfold}(\mathit{Coit}_\sigma f M^\sigma) \Rightarrow \mathit{Lift}_\sigma(\mathit{Coit}_\sigma f)(f M^\sigma)$. Operacja $\mathit{Lift}_\sigma : (\sigma \rightarrow \mathbf{stream}) \rightarrow (\mathbf{int} \times \sigma) \rightarrow (\mathbf{int} \times \mathbf{stream})$ „podnosi” typ argumentu: $\mathit{Lift}_\sigma(\varphi)$ działa jak φ na prawej współrzędnej, tj. $\mathit{Lift}_\sigma(\varphi)(\langle n, s \rangle) := \langle n, \varphi s \rangle$.

Wyrażenie $\mathit{Nats} := \mathit{Coit}_{\mathbf{int}}(\lambda n. \langle n, n+1 \rangle)0$ przedstawia strumień wszystkich liczb naturalnych. Jeśli zdefiniujemy $\mathit{head}(s) := \pi_1(\mathit{Unfold}(s))$ i $\mathit{tail}(s) := \pi_2(\mathit{Unfold}(s))$, to aplikacja $\mathit{head}(\mathit{Nats})$ zredukuje się do zera, a aplikacja $\mathit{tail}(\mathit{Nats})$ zredukuje się do strumienia $\mathit{Coit}_{\mathbf{int}}(\lambda n. \langle n, n+1 \rangle)1$, który zaczyna się od jedynki.

- (a) Proszę zdefiniować operację $\mathit{razydwa} : \mathbf{stream} \rightarrow \mathbf{stream}$, która mnoży wszystkie wyrazy strumienia przez dwa. Powinno być tak, że $\mathit{head}(\mathit{razydwa} s) = 2 \cdot \mathit{head}(s)$ oraz $\mathit{tail}(\mathit{razydwa} s) = \mathit{razydwa}(\mathit{tail} s)$. Symbol równości oznacza konwersję.

Drugi sposób wymaga użycia typu egzystencjalnego $\mathbf{stream} := \exists p. p \times (p \rightarrow \mathbf{int} \times p)$. Teraz strumień wszystkich liczb naturalnych to np. $\mathit{Nats} := [\mathbf{int}, \langle 0, \lambda n. \langle n, n+1 \rangle]$.

- (b) Proszę zdefiniować operacje head , tail i $\mathit{razydwa}$ dla takich strumieni.

Trzeci sposób to definicja typu $\mathbf{stream}$ w systemie $\mathbf{F}$.

- (c) Proszę zdefiniować $\mathbf{stream}$ w systemie $\mathbf{F}$ używając tylko operatorów $\rightarrow$ i $\forall$. Dla takiego typu $\mathbf{stream}$ proszę zdefiniować Nats i operacje head , tail i $\mathit{razydwa}$.

Rozwiązania

3a: To jest twierdzenie. Równoważność to koniunkcja dwóch implikacji, więc λ -term reprezentujący dowód tej formuły jest parą $\langle \lambda x^{-q \rightarrow q} \lambda y^{-q}. y(xy), \lambda x^{-q \rightarrow q} \lambda y^{-q}. \varepsilon_q(xy) \rangle$.

3b: To też twierdzenie. Inhabitantem jest term $\lambda x^{(\neg \neg q \rightarrow q) \rightarrow \neg q} \lambda y^q. x(\lambda z^{\neg \neg q}. y)$.

3c: To nie twierdzenie. Jako kontrprzykład można podać model Kripkego o 4 stanach uporządkowanych tak, że $c_0 \leq c_1 \leq c_2$ oraz $c_0 \leq c_3$, ale c_3 jest nieporównywalne z c_1 i z c_2 . W tym modelu p jest wymuszone tylko w stanie c_2 . Wtedy $c_3 \Vdash \neg p$, i mamy $c_0 \not\Vdash \neg p \vee \neg \neg p$. Ponieważ $c_1 \Vdash \neg \neg p$, więc $\neg \neg p \rightarrow p$ jest wymuszone tylko w c_2 i c_3 . Zatem $c_0 \Vdash (\neg \neg p \rightarrow p) \rightarrow p \vee \neg p$.

4a: Rozpatrzmy model Kripkego o dwóch stanach 0 i 1, przy tym niech $0 \not\Vdash p, q$ i $1 \Vdash p, q$. Wtedy $0 \Vdash \neg \neg p$, więc $0 \not\Vdash (\neg \neg p \rightarrow p)$. Ale $0 \Vdash (\neg \neg p \rightarrow p) \rightarrow q$ więc (4a) nie jest wymuszone w stanie 0.

4b: Dowód: $\lambda x^{(\neg \neg p \rightarrow p) \rightarrow \neg q} \lambda y^q. x(\lambda z^{\neg \neg p}. \varepsilon_p(z(\lambda u^p. x(\lambda v^{\neg \neg p}. u)y))y)$. Co się tyczy dowodu bez ex falso, przypomnijmy, że negacja $\neg \alpha$ to w istocie skrót implikacji $\alpha \rightarrow \perp$. Reguła ex falso nadaje stałej $\perp$ szczególną rolę; jeśli ją usuniemy, to $\perp$ staje się taką samą zmienną zdaniową jak inne. Jeśli więc formuła ma dowód bez reguły ex falso, to ma też dowód formuła otrzymana z niej przez zamianę każdej negacji $\neg \alpha$ na $\alpha \rightarrow r$, gdzie r jest nową zmienną. W naszym przypadku byłaby to formuła $((p \rightarrow r) \rightarrow r) \rightarrow p \rightarrow q \rightarrow r$. Kontrmodel dla tej formuły ma trzy stany 0, 1 i 2, a relację $\Vdash$ określimy tak: $0, 1, 2 \not\Vdash p$, $0 \not\Vdash q, r$, $1, 2 \Vdash q$, $2 \Vdash r$, $1 \not\Vdash r$. Wtedy jedynym stanem, który forsuje formułę $(p \rightarrow r) \rightarrow r$ jest 2 i żaden stan nie wymusza $((p \rightarrow r) \rightarrow r) \rightarrow p$. Stąd $0 \Vdash (((p \rightarrow r) \rightarrow r) \rightarrow p) \rightarrow q \rightarrow r$. Ale $0 \not\Vdash q \rightarrow r$.

⁹Wskazówka: Jeśli $P : \tau \Rightarrow *$ oraz $x : \tau$, to $(\lambda z:\tau)(Pz \rightarrow Px)$ jest konstruktorem rodzaju $\tau \Rightarrow *$

Inaczej: Dowód formuły $((p \rightarrow r) \rightarrow r) \rightarrow p \rightarrow q \rightarrow r$, to lambda-term tego typu, który ma postać normalną $\lambda x^{((p \rightarrow r) \rightarrow r) \rightarrow p} \rightarrow q \rightarrow r \lambda y^q.M^r$. Term M musi wyglądać tak: $M = xN^{((p \rightarrow r) \rightarrow r) \rightarrow p}Q^q$, gdzie $N = \lambda z^{(p \rightarrow r) \rightarrow r}.P^p$. Ale w otoczeniu, w którym typy wszystkich zmiennych x, y, z kończą się na r lub q , nie istnieje term typu p .

5a: Nie. Kontrmodel Kripkego składa się z trzech stanów a, b, c , gdzie $a \leq b, c$ ale stany b i c są nieporównywalne. Stan a nie wymusza żadnych atomów, natomiast $b \Vdash q, s$ oraz $c \Vdash p, s$. Wtedy formuła $p \rightarrow r$ jest wymuszona tylko w stanie b a formuła $q \rightarrow r$ jest wymuszona tylko w stanie c . A więc stan a wymusza wszystkie trzy założenia i nie wymusza konkluzji s .

Inny sposób: przyjmijmy $v(p) = (-\infty, 0)$, $v(q) = (0, \infty)$, $v(r) = \emptyset$, $v(s) = \mathbb{R} - \{0\}$ w algebrze otwartych podzbiorów prostej $\mathbb{R}$. Wtedy $\llbracket p \rightarrow r \rrbracket_v = \llbracket \neg p \rrbracket_v = (0, \infty) \subseteq \llbracket s \rrbracket_v$ i podobnie $\llbracket q \rightarrow r \rrbracket_v \subseteq \llbracket s \rrbracket_v$. Ponadto $\llbracket p \rightarrow q \rightarrow r \rrbracket_v = \llbracket p \wedge q \rightarrow r \rrbracket_v = \mathbb{R}$, tymczasem $\llbracket s \rrbracket_v \neq \mathbb{R}$.

5b: Tak, bo to jest typ termu: $\lambda x^{p \rightarrow q \rightarrow r} \lambda y^{(p \rightarrow r) \rightarrow s} \lambda z^{(q \rightarrow r) \rightarrow s} \lambda u^{s \rightarrow r}. u(y(\lambda v^p. u(z(\lambda w^q. xvw))))$.

Inny sposób: rozpatrzmy stan c modelu Kripkego, w którym wymuszone są wszystkie założenia, ale nie konkluzja r . Skoro $c \Vdash s \rightarrow r$, to $c \nVdash s$. Zatem $c \nVdash p \rightarrow r$, jest więc taki stan $d \geq c$, że $d \Vdash p$ oraz $d \nVdash r$, skąd też $d \nVdash s$. Wtedy także $d \nVdash q \rightarrow r$, jest więc taki stan $e \geq d$, że $e \Vdash q$ i $e \nVdash r$. Ale $e \Vdash p$ i mamy sprzeczność z powodu pierwszego założenia.

8: This property easily follows from Glivenko's theorem. And conversely (take $\alpha = \top$), hence it does not hold at first-order.

9: Yes, if $\sim \alpha := \alpha \rightarrow q$ then $\nVdash \sim \sim (\sim p \rightarrow p)$.

10: Pierwsza tak: dla $x : \alpha$, $y : \neg(p \vee q)$ jest $y[\text{inr}(x(\lambda z^p. y(\text{inl } z)))] : \perp$. Druga nie: kontrmodel Kripkego ma dwa stany $c < d$, w stanie c nic nie jest wymuszone, w stanie d jest wymuszone q .

11: Jeśli w algebrze otwartych podzbiorów $\mathbb{R}$ zinterpretujemy p jako $(-\infty, 0)$, oraz q jako $(0, \infty)$, to znaczeniem formuł (11a) i (11b) będzie zbiór $\mathbb{R} - \{0\}$. Obie te formuły są jednak wymuszane przez dowolny liniowo uporządkowany model Kripkego. Formuła (11b) dlatego, że jeden ze zbiorów $\{c \mid c \Vdash p\}$ i $\{c \mid c \Vdash q\}$ musi (z powodu monotoniczności) zawierać drugi. A formuła (11a) dlatego, że $c \nVdash \neg p$ jest możliwe tylko wtedy, gdy $c' \Vdash p$ dla pewnego $c' \geq c$. Ale wtedy dla dowolnego stanu c'' istnieje takie c''' , że $c''' \Vdash p$, skąd wynika $c \Vdash \neg \neg p$.

Natomiast dla formuły (11c) kontrprzykładem liniowym jest model dwuelementowy, w którym $c < c'$, a relacja $\Vdash$ jest taka, że $c \nVdash p, q$ oraz $c' \Vdash p, q$.

12: Żadna z implikacji $\alpha \rightarrow \beta$, $\beta \rightarrow \alpha$ nie jest twierdzeniem intuicjonistycznym. Kontrmodel Kripkego dla $\alpha \rightarrow \beta$ ma 2 stany, w pierwszym stanie nic nie jest wymuszone, w drugim wymuszone są atomy e, b, a . Kontrmodel dla $\beta \rightarrow \alpha$ jest podobny, ale w drugim stanie wymuszone są e, d, a .

$(\alpha \rightarrow \beta)$ Implikacje $c \rightarrow b$, $d \rightarrow a$ są wymuszone wszędzie, $e \rightarrow d$ nigdzie, więc $(e \rightarrow d) \rightarrow c$ wszędzie, natomiast $((e \rightarrow d) \rightarrow c) \rightarrow b$ tylko w stanie 2. Ale $2 \Vdash a$, więc α jest wymuszone wszędzie. Ponadto $e \rightarrow (d \rightarrow a) \rightarrow b$ i $c \rightarrow b$ są wymuszone wszędzie, tymczasem $1 \nVdash a$.

$(\beta \rightarrow \alpha)$ Implikacje $c \rightarrow b$, $d \rightarrow a$, $e \rightarrow d$ są wymuszone wszędzie, zatem $(e \rightarrow d) \rightarrow c$ nigdzie i dalej $((e \rightarrow d) \rightarrow c) \rightarrow b$ wszędzie, więc $1 \nVdash \alpha$. Formuła $e \rightarrow (d \rightarrow a) \rightarrow b$ nie jest wymuszona nigdzie, bo w stanie 2 jest e . Zatem $1 \Vdash \beta$.

Inna metoda: pokazać, że nie istnieje term w postaci normalnej.

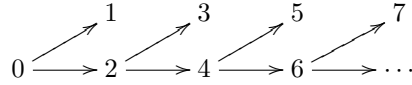
$(\alpha \rightarrow \beta)$ Jeśli $\Gamma = \{X : \alpha, Y : e \rightarrow (d \rightarrow a) \rightarrow b, Z : c \rightarrow b\}$, to trzeba wyprowadzić $\Gamma \vdash a$. Trzeba użyć X i udowodnić $\Gamma, (e \rightarrow d) \rightarrow c \vdash b$. Żeby użyć Y , trzeba udowodnić $\Gamma, (e \rightarrow d) \rightarrow c \vdash e$, co jest niemożliwe, bo żadne założenie nie kończy się na e . No to trzeba użyć zmiennej Z i udowodnić $\Gamma, (e \rightarrow d) \rightarrow c, e \vdash d$, a to się też nie da, z podobnego powodu.

$(\beta \rightarrow \alpha)$ Niech $\Delta = \{V : ((e \rightarrow d) \rightarrow c) \rightarrow b, W : \beta\}$. Chcemy udowodnić $\Delta \vdash a$ i musimy użyć W . To wymaga dowodu dla $\Delta, e, d \rightarrow a \vdash b$ z użyciem V , czyli chcemy $\Delta, e, d \rightarrow a \vdash c$ i tu znowu nie ma założenia kończącego się na c .

13: Jeśli stan c wymusza $\sharp \alpha$, to żaden przyszły stan $c_1 > c$ nie może wymuszać formuły $\neg \alpha$. Inaczej moglibyśmy zbudować rosnący ciąg stanów, który „omiija” α . A zatem $\Vdash \sharp \alpha \rightarrow \neg \neg \alpha$.

Rozpatrzmy teraz model Kripkego o zbiorze stanów $\mathbb{N}$ i z takim porządkiem: liczby parzyste są uporządkowane jak zwykle, a każda liczba nieparzysta $2k + 1$ jest większa od liczb $2n$ dla $n \leq k$

i nieporównywalna ze wszystkimi pozostałymi liczbami. Atom p jest wymuszony we wszystkich stanach nieparzystych. Wtedy $0 \Vdash \neg\neg\alpha$, ale $0 \nVdash \# \alpha$, bo ciąg stanów parzystych „omija” α .



Ten efekt jest możliwy tylko w modelu nieskończonym. W modelach skończonych stany końcowe tworzą przekrój, w takich modelach mamy więc wymuszoną równoważność $\neg\neg p \leftrightarrow \# p$. Gdyby $\# p$ było równoważne jakiejś formule β , to w każdym modelu skończonym mielibyśmy też $\beta \leftrightarrow \neg\neg p$. Ponieważ intuicjonistyczny rachunek zdań ma własność skończonego modelu, formuła $\beta \leftrightarrow \neg\neg p$ byłaby intuicjonistycznym twierdzeniem i w konsekwencji formuły $\neg\neg p$ i $\# p$ też byłyby równoważne.

14: Porządek liniowy jest oczywiście kratą. Jeśli $a \leq b$, to pseudodopełnieniem $a \Rightarrow b$ jest 1, w przeciwnym razie mamy $a \Rightarrow b = b$. Zatem mamy algebrę Heytinga (krata jest dystrybutywna, bo zawsze istnieje pseudodopełnienie).

Formuła zdaniowa jest wymuszana we wszystkich liniowo uporządkowanych modelach Kripkego wtedy i tylko wtedy, gdy jest prawdziwa we wszystkich liniowo uporządkowanych algebrach Heytinga. Implikacja z lewej do prawej wynika stąd, że filtrami pierwszymi w liniowo uporządkowanej algebrze Heytinga są wszystkie podzbiory zamknięte w górę. Zatem filtry te są liniowo uporządkowane przez inkluzję i jeśli zbudujemy z nich model Kripkego jak w dowodzie twierdzenia o pełności, to będzie on liniowo uporządkowany.

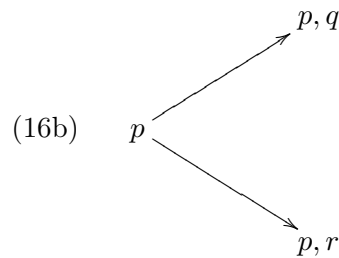
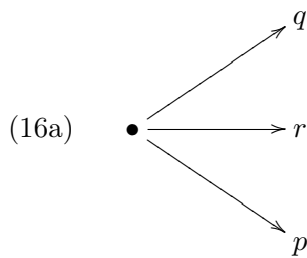
Aby udowodnić implikację z prawej do lewej należy zauważyć, że zamknięte w górę podzbiory liniowo uporządkowanego modelu Kripkego C też są liniowo uporządkowane i tworzą algebrę Heytinga H . Jeśli teraz określimy $\varrho(p) = \{c \mid c \Vdash p\}$ to przez łatwą indukcję uzyskamy równoważność warunków $H, \varrho \models \varphi$ oraz $C \Vdash \varphi$.

15: Formuła (15a) nie ma inhabitanta w postaci normalnej, więc nie może być tautologią. W otoczeniu $y : (p \rightarrow q) \rightarrow r$, $z : p \rightarrow r$ każdy term normalny typu r musiałby być postaci $yM^{p \rightarrow q}$ lub postaci zN^p . Takiego M ani N nie da się skonstruować, bo w naszym otoczeniu nie ma zmiennej typu kończącego się na p ani na q . Niech teraz $\tau = ((p \rightarrow q) \rightarrow r) \rightarrow (p \rightarrow r) \rightarrow r$. Wtedy term

$$\lambda x^{\tau \rightarrow q} x(\lambda y^{(p \rightarrow q) \rightarrow r} \lambda z^{p \rightarrow r} y(\lambda u^p x(\lambda y^{(p \rightarrow q) \rightarrow r} \lambda z^{p \rightarrow r} zu))),$$

ma typ $(\tau \rightarrow q) \rightarrow q$, więc formuła (15b) jest tautologią.

16: Kontraprzykłady Kripkego są na rysunku. Strzałki oznaczają relację $\leq$ w zbiorze stanów. Zaznaczono wszystkie zmienne zdaniowe wymuszone w poszczególnych stanach. Kontraprzykłady Heytinga



wyberzemy w algebrze otwartych podzbiorów prostej rzeczywistej. W części 16a niech $v(p) = (-\infty, 0)$, $v(q) = (0, \infty) - \{\frac{1}{2^n} \mid n \geq 2\}$, $v(r) = (0, \infty) - \{\frac{1}{3^n} \mid n \geq 2\}$. W części 16b weźmy $v(p) = \mathbb{R}$ oraz $v(q) = (-\infty, 0)$, $v(r) = (0, \infty)$.

17a: Warunek $-a = 0$ oznacza tyle co $\forall x(x \sqcap a = 0 \rightarrow x = 0)$. Jeśli $a, b \in F$ oraz $x \sqcap a \sqcap b = 0$, to wtedy $x \sqcap a = 0$, bo $b \in F$, i dalej $x = 0$, bo $a \in F$. Jeśli $a \in F$ oraz $a \leq b$ to $x \sqcap a \geq x \sqcap b$, jeśli więc $x \sqcap b = 0$, to tym bardziej $x \sqcap a = 0$, skąd $x = 0$. Ponadto $F \neq \emptyset$, bo $-1 = 0$, a więc F jest filtrem.

17b: Niech $a \approx a'$ oraz $b \approx b'$. Chcemy pokazać, że $-a \approx -a'$ oraz $a \circ b \approx a' \circ a'$ dla każdego działania $\circ \in \{\sqcap, \sqcup, \Rightarrow\}$. W tym celu potrzebne są nam takie nierówności, prawdziwe w każdej algebrze Heytinga, a oczywiste w algebrze Lindenbauma:

- $a \Rightarrow a' \leq -a' \Rightarrow -a$;
- $(a \Rightarrow a') \sqcap (b \Rightarrow b') \leq (a \sqcap b \Rightarrow a' \sqcap b')$;
- $(a \Rightarrow a') \sqcap (b \Rightarrow b') \leq (a \sqcup b \Rightarrow a' \sqcup b')$;
- $(a' \Rightarrow a) \sqcap (b \Rightarrow b') \leq (a \Rightarrow b) \Rightarrow (a' \Rightarrow b')$.

Jeśli lewe strony tych nierówności należą do filtru, to prawe strony też i to już cały dowód.

17c: Aby pokazać, że $\mathcal{H}/\approx$ jest algebrą Boole'a, trzeba sprawdzić, że $a \sqcup -a \approx 1$, dla dowolnego a , inaczej mówiąc, że $a \sqcup -a \in F$. Przypuśćmy więc, że $x \sqcap (a \sqcup -a) = 0$. Wtedy $x \sqcap a = x \sqcap -a = 0$ czyli $x \leq -a$ oraz $x \leq - -a$. Stąd $x \leq (-a \sqcap - -a) = 0$.

18: Jeśli $\mathcal{H}$ jest algebrą Lindenbauma i α jest klasyczną tautologią, to α jest spełniona przez trywialne wartościowanie w $\mathcal{H}/\approx$ zadane wzorem $v(p) = [[p]_{\sim}]_{\approx}$. To wartościowanie ma tę własność, że $[[\alpha]]_v = [[\alpha]_{\sim}]_{\approx}$, gdzie $[\alpha]_{\sim}$ oznacza element algebry Lindenbauma wyznaczony przez formułę α (klasę abstrakcji ze względu na intuicjonistyczną równoważność formuł.) A więc mamy $[\alpha]_{\sim} \approx 1$ czyli $[\alpha]_{\sim} \in F$. Jeszcze inaczej, $\vdash \neg\alpha \rightarrow \perp$ czyli $\vdash \neg\neg\alpha$.

19: Problem cyklu Hamiltona jest w klasie NP, istnieje więc formuła zdaniowa klasycznie wyrażająca istnienie cyklu Hamiltona. Negacja tej formuły wyraża nieistnienie. Można więc zastosować translację Kołmogorowa. Ale my skonstruujemy naszą formułę wprost. Użyjemy zmiennych zdaniowych s_{ℓ}^i, v_{ℓ}^i , gdzie $\ell \in V$ oraz $i = 1, \dots, k$. Formuła ma postać $\vec{\alpha} \rightarrow s_{\ell_0}^1$, gdzie ℓ_0 to wybrany wierzchołek początkowy, a założenia $\vec{\alpha}$ są takie:

- $v_{\ell_1}^{i+1} \rightarrow \dots \rightarrow v_{\ell_m}^{i+1} \rightarrow s_{\ell}^i$, gdzie $\ell \in V$, $i < k$ oraz $\ell_1, \dots, \ell_m$ to wszystkie wierzchołki, do których prowadzą krawędzie z ℓ .
- $(v_{\ell}^i \rightarrow v_{\ell}^{i+1} \rightarrow \dots \rightarrow v_{\ell}^k \rightarrow s_{\ell}^i) \rightarrow v_{\ell}^i$, gdzie $\ell \in V$, $i < k$.
- $v_{\ell^1}^k, \dots, v_{\ell^d}^k$, gdzie $\ell^1, \dots, \ell^d$ to wszystkie wierzchołki, z których nie ma krawędzi do ℓ_0 .

Każda droga w G rozpoczynająca się od ℓ_0 odpowiada jednej gałęzi potencjalnego dowodu, w którym kolejne cele dowodowe są postaci s_{ℓ}^i , gdy ℓ jest i -tym kolejnym wierzchołkiem na tej drodze. Jeśli wierzchołek ℓ był odwiedzany w chwili i , to do założeń dodaje się atomy $v_{\ell}^{i+1}, \dots, v_{\ell}^k$. W razie kolejnego wybrania tego samego wierzchołka, ta gałąź w dowodzie się kończy. Pozostają jeszcze te gałęzie, w których udało się wybrać k różnych wierzchołków. Wtedy dowód można zakończyć, jeśli nie istnieje przejście do ℓ_0 .

20: Pierwsza nie. Kontrmodel Kripkego ma dwa stany $c < d$ i dziedziny $\mathcal{A}_c = \{0\}$, $\mathcal{A}_d = \{0, 1\}$. W obu strukturach do relacji P należy tylko 0. Kontrmodel topologiczny to $\mathcal{H}$ -struktura o dziedzinie $\mathcal{A} = \mathbb{R} - \mathbb{Q}$, gdzie $\mathcal{H}$ jest algebrą otwartych podzbiorów $\mathbb{Q}$. Relację P interpretujemy jako funkcję określoną tak: $P^{\mathcal{A}}(r) = \mathbb{Q} \cap (-r, r)$. Druga tak. Dowód można zapisać jako lambda term

$$\lambda X^{\varphi \wedge \vartheta}. \text{unpack } X\{2\} \text{ as } [x, Y: \neg P(x)] \text{ in } \lambda Z^{\forall x P(x)}. Y(Zx)$$

21a: Nie. Rozpatrzmy $\mathcal{O}(\mathbb{R})$ -strukturę $\mathcal{A} = \langle \mathbb{R}, P^{\mathcal{A}} \rangle$, gdzie $P^{\mathcal{A}}(r) = \mathbb{R} - \{r\}$ dla dowolnego $r \in \mathbb{R}$. Wtedy $[[\forall x P(x)]] = \emptyset$, ale $[[\forall x \neg \neg P(x)]] = \mathbb{R}$, bo $\sim(\sim(\mathbb{R} - \{r\})) = \mathbb{R}$ dla każdego $r \in \mathbb{R}$. Zatem znaczeniem formuły $\neg \forall x P(x)$ jest cała prosta a znaczeniem formuły $\neg \forall x \neg \neg P(x)$ jest zbiór pusty. Inny sposób: rozpatrzmy model Kripkego o zbiorze stanów $\mathbb{N}$ i stałych dziedzinach $D_n = \mathbb{N}$. Relację P zdefiniujemy w dziedzinie D_n jako zbiór $\{k \mid k \leq n\}$. Nie ma takiego stanu, który wymusza $\forall x P(x)$, bo zawsze jest element, który nie należy do relacji. Za to formuła $\forall x \neg \neg P(x)$ jest wymuszona w każdym stanie, bo każdy element prędzej czy później do relacji wpadnie.

21b: Tak. To jest typ takiego termu:

$$\lambda X^{\neg \exists x P(x)} \lambda Y^{\exists x \neg \neg P(x)}. \text{unpack } Y \text{ as } [a, V: \neg \neg P(a)] \text{ in } V(\lambda Z^{P(a)}. X[a, Z]^{\exists x P(x)}).$$

Inny sposób: rozpatrzmy dowolny model Kripkego i dowolny stan c . Jeśli $c \Vdash \neg \exists x P(x)$, to znaczy, że w każdym stanie $d \geq c$ relacja P jest pusta. Tymczasem $c \Vdash \exists x \neg \neg P(x)$ oznacza, że dla pewnego elementu a dziedziny D_c zachodzi $c, a \Vdash \neg \neg P(x)$, w szczególności $c, a \not\Vdash \neg P(x)$. Inaczej: element a musi w jakimś przyszłym stanie należeć do relacji P .

23: Z „dobrego” prawa De Morgana $\forall x \neg Q(x) \leftrightarrow \neg \exists x Q(x)$ wynika równoważność formuł (23b) i (23c). Formuła (23b) implikuje formułę (23a), bo $P(x)$ implikuje $\neg \neg P(x)$, a schemat $(p \rightarrow q) \rightarrow \neg q \rightarrow \neg p$

jest intuicjonistycznie prawdziwy. Pozostaje zauważyć, że formuła (23a) nie implikuje pozostałych. Jeśli znaczeniami predykatu $P(x)$ są zbiory $\mathbb{R} - \{x\}$ dla $x \in \mathbb{R}$, to w algebrze otwartych podzbiorów prostej wartością formuły (23a) będzie 1, a wartością formuły (23c) będzie 0.

24: Dowód w Coqu przy założeniu schematu Grzegorzcyka:

Variable A: Set.

Variable a: A.

Variable S: Prop.

Variables P Q : A $\rightarrow$ Prop.

Hypothesis Grzegorzcyk: forall (R: A $\rightarrow$ Prop) (S: Prop),
(forall x, R x $\vee$ S) $\rightarrow$ (forall x, R x) $\vee$ S.

Hypothesis Gamma: forall x, exists y, P y $\wedge$ (Q y $\rightarrow$ Q x).

Hypothesis Beta: not (forall x, Q x).

Hypothesis Delta: forall x, P x $\rightarrow$ (Q x $\vee$ S).

Goal S.

assert (forall x, Q x $\vee$ S).

+ intro.

destruct (Gamma x).

destruct H.

destruct (Delta x0 H).

- left.

apply H0.

assumption.

- right.

assumption.

+ destruct (Grzegorzcyk Q S H).

- contradiction.

- assumption.

Qed.

Weźmy model Kripkego o dwóch stanach $0 < 1$, i strukturach relacyjnych $\mathcal{A}_0 = \langle \{0\}, P^0, Q^0, S^0 \rangle$, $\mathcal{A}_1 = \langle \{0, 1\}, P^1, Q^1, S^1 \rangle$, gdzie $Q^0 = Q^1 = \{0\}$, $P^0 = \{0\}$, $P^1 = \{0, 1\}$, zeroargumentowa relacja S^0 nie zachodzi, a S^1 zachodzi. Atom $P(y)$ jest wymuszany wszędzie, więc $0 \Vdash \forall x (P(x) \wedge (Q(x) \rightarrow Q(x)))$, i tym bardziej $0 \Vdash \gamma$. Ponieważ $1 \notin Q^1$, więc $0 \nVdash \beta$. Dalej $0 \Vdash \forall x (Q(x) \vee S)$, bo w stanie 0 mamy Q , a w stanie 1 mamy S . Stąd $0 \Vdash \delta$. Ostatecznie $0 \nVdash \gamma \rightarrow \beta \rightarrow \delta \rightarrow S$, bo $0 \nVdash S$.

25: Implikacja $\delta \rightarrow \gamma$ jest twierdzeniem, którego dowód można zapisać w postaci lambda-termu:

$\lambda X^\delta \lambda Y^{\forall y P(y)}. \text{unpack } X \text{ as } [x, Z : P(x) \rightarrow Q(x)] \text{ in } [x, Z(Yx)]$.

Implikacja $\gamma \rightarrow \delta$ nie jest twierdzeniem, co najłatwiej zauważyć zamieniając $Q(x)$ na $\perp$. Wtedy $\gamma \rightarrow \delta$ to po prostu prawo De Morgana $\neg \forall y P(y) \rightarrow \exists x \neg P(x)$. Kontrprzykładem topologicznym jest $\mathcal{O}(\mathbb{R})$ -struktura $\mathcal{A} = \langle \mathbb{Q}, P^{\mathcal{A}}, Q^{\mathcal{A}} \rangle$, w której $P^{\mathcal{A}}(w) = \mathbb{R} - \{w\}$ i $Q^{\mathcal{A}}(w) = \emptyset$, dla $w \in \mathbb{Q}$. Znaczeniem formuły $\forall y P(y)$ jest wtedy wnętrze zbioru $\mathbb{R} - \mathbb{Q}$ czyli zbiór pusty. A więc znaczeniem γ jest cała prosta, podczas gdy znaczenie δ jest puste. Kontrprzykład Kripkego dla formuły $\gamma \rightarrow \delta$ ma postać $\mathcal{C} = \langle \mathbb{N}, \leq, \{\mathcal{A}_n \mid n \in \mathbb{N}\} \rangle$, gdzie $\mathcal{A}_n = \langle \mathbb{N}, P^n, Q^n \rangle$ oraz $P^n = \{0, \dots, n\}$, $Q^n = \emptyset$, dla $n \in \mathbb{N}$. Ponieważ w każdym stanie n są elementy nie należące do P^n , więc $n \nVdash \forall y P(y)$ czyli walkowerem $0 \Vdash \gamma$. Ale $0 \nVdash \delta$, bo każda liczba naturalna należy do pewnego P^n .

26: Kontrprzykładem topologicznym jest $\mathcal{O}(\mathbb{R})$ -struktura $\mathcal{A} = \langle \mathbb{Q}, P^{\mathcal{A}} \rangle$, w której $P^{\mathcal{A}}(w) = \mathbb{R} - \{w\}$ dla $w \in \mathbb{Q}$. Znaczeniem formuły $\forall y P(y)$ jest wtedy wnętrze zbioru $\mathbb{R} - \mathbb{Q}$ czyli zbiór pusty. Znaczeniem formuły $\exists x \neg P(x)$ też jest zbiór pusty, a podwójna negacja z przodu nic tu nie zmienia.

Kontrprzykład Kripkego dla tej formuły ma postać $\mathcal{C} = \langle \mathbb{N}, \leq, \{\mathcal{A}_n \mid n \in \mathbb{N}\} \rangle$, gdzie $\mathcal{A}_n = \langle \mathbb{N}, P^n \rangle$ oraz $P^n = \{0, \dots, n\}$, dla $n \in \mathbb{N}$. Ponieważ w każdym stanie n są elementy nie należące do P^n , więc

$n \not\models \forall y P(y)$. Ale nie ma też elementów spełniających $\neg P(x)$, bo każdy prędzej czy później znajdzie się w zbiorze P^m dla pewnego $m \geq n$. Zatem $n \not\models \exists x \neg P(x)$. A więc w każdym stanie n wymuszona jest formuła $\neg(\forall x P(x) \vee \exists x \neg P(x))$, co oczywiście wyklucza podwójną negację.

27: Schematy (B) i (C) są równoważne. W schemacie (B) możemy przyjąć $\forall x \varphi(x)$ jako ψ i otrzymamy (C). Mamy też oczywiste wynikanie $\varphi(x) \rightarrow \forall x \varphi(x), \forall x \varphi(x) \rightarrow \psi \vdash \varphi(x) \rightarrow \psi$, a więc (C) po prostu implikuje (B). Dalej, z paradoksu pijaka (C) wynika schemat Grzegorzcyka (A). Mamy bowiem $\varphi(x_0) \rightarrow \forall y \varphi(y), \psi \vee \varphi(x_0) \vdash \psi \vee \forall y \varphi(y)$. Natomiast schematy (B) i (C) nie są konsekwencjami (A), bo (B) ma kontrprzykład o stałych dziedzinach (prosta adaptacja rozwiązania 16b).

28e: To nie twierdzenie. Rozpatrzmy dziedzinę $D = \{1, 2\}$ i algebrę otwartych podzbiorów $\mathbb{R}^2$. Zinterpretujmy $Q(1)$ jako I ćwiartkę płaszczyzny, $Q(2)$ jako III ćwiartkę, a $P(1)$ i $P(2)$ jako sumę II i IV ćwiartki. Wtedy lewa strona to cała płaszczyzna, a po prawej stronie brakuje punktu $\langle 0, 0 \rangle$.

30: No, there is always a proof corresponding to the empty word. To fix it, replace the third axiom by two: $\forall xy(Q(x, y) \rightarrow P(a(x), a(y)))$, and $\forall xy(Q(x, y) \rightarrow P(b(x), b(y)))$.

31: Formuła ma postać $\alpha_1 \rightarrow \alpha_2 \rightarrow \dots \rightarrow \alpha_n \rightarrow \perp$, a jej przesłanki α_i są następujące:

- $q_0(0, 0) \rightarrow \perp$ oraz $\forall xy(q_f(x, y))$;
- $\forall xy(p(s(x), y) \rightarrow q(x, y))$, dla instrukcji postaci „ $q : c_1 := c_1 + 1; \text{goto } p$ ”;
- $\forall xy(p(x, s(y)) \rightarrow q(x, y))$, dla instrukcji postaci „ $q : c_2 := c_2 + 1; \text{goto } p$ ”;
- $\forall xy(p(x, y) \rightarrow q(s(x), y))$, dla instrukcji postaci „ $q : c_1 := c_1 - 1; \text{goto } p$ ”;
- $\forall xy(p(x, y) \rightarrow q(x, s(y)))$, dla instrukcji postaci „ $q : c_2 := c_2 - 1; \text{goto } p$ ”;
- $\forall xy(p(0, y) \rightarrow q(0, y))$, oraz $\forall xy(r(s(x), y) \rightarrow q(s(x), y))$,
dla instrukcji postaci „ $q : \text{if } c_1 = 0 \text{ then goto } p \text{ else goto } r$ ”;
- $\forall xy(p(x, 0) \rightarrow q(y, 0))$, oraz $\forall xy(r(x, s(y)) \rightarrow q(x, s(y)))$,
dla instrukcji postaci „ $q : \text{if } c_2 = 0 \text{ then goto } p \text{ else goto } r$ ”.

32: W zbiorze Δ mamy formułę $\forall xy q_f(x, y)$ i po jednej formule dla każdej instrukcji automatu:

- $\forall xyz(S(z, y) \rightarrow q(x, z) \rightarrow p(x, y))$, dla instrukcji $p : \text{delete}; \text{goto } q$;
- $\forall xy(\forall z(S(z, x) \rightarrow A(z) \rightarrow q(z, y)) \rightarrow p(x, y))$, dla instrukcji $p : \text{insert}(A); \text{goto } q$;
- $\forall xy(A(y) \rightarrow q(x, y) \rightarrow p(x, y))$, dla instrukcji $p : \text{peek}(A); \text{goto } q$.

Powiemy, że otoczenie $\Gamma(x_1, \dots, x_n)$ koduje kolejkę $w = A1 \dots A_n$, gdy należą do niego formuły jak we wskazówce, a wszystkie pozostałe formuły są atomowe i nie zawierają zmiennych $x_1, \dots, x_n$, z co najwyżej jednym wyjątkiem postaci $S(x_n, y)$ gdzie $y \neq x_1, \dots, x_n$. Wtedy osąd postaci $\Gamma, \Delta \vdash q(x_1, x_n)$ można tylko udowodnić z pomocą formuły związanej z instrukcją dla stanu q . Na przykład jeśli to jest instrukcja $p : \text{insert}(A); \text{goto } q$, to musimy udowodnić $\Gamma, \Delta \vdash \forall z(S(z, x_1) \rightarrow A(z) \rightarrow p(z, x_n))$, co prowadzi do zadania $\Gamma, S(z, x_1), A(z), \Delta \vdash p(z, x_n)$. Otoczenie $\Gamma S(z, x_1), A(z)$ koduje kolejkę $AA1 \dots A_n$ z pomocą ciągu zmiennych $z, x_1, \dots, x_n$ (mogą tam też być nowe „śmieci” ale to nic nie szkodzi) i możemy przez indukcję pokazywać, że osąd ma dowód wtedy i tylko wtedy, gdy maszyna uruchomiona w odpowiedniej konfiguracji dojdzie do stanu końcowego. (Dla konfiguracji końcowej dowód jest trywialny.) Automat uruchomiony w stanie q_0 z kolejką $\#$ zatrzyma się więc w stanie q_f wtedy i tylko wtedy, gdy istnieje dowód osądu $\Delta, \#(x_1) \vdash q_0(x_1, x_1)$. A zatem jeśli $\Delta = \{\alpha_1, \dots, \alpha_N\}$, to nasza formuła ma postać $\alpha_1 \rightarrow \dots \rightarrow \alpha_N \rightarrow \#(x_1) \rightarrow q_0(x_1, x_1)$,

33: Niech $there = \lambda z^\tau \Lambda p \lambda y^{\tau \rightarrow p}. yz$ i $back = \lambda x^\sigma. x\tau \mathbf{I}$. Term $\Lambda p \lambda y^{\tau \rightarrow p}. y(\Lambda r \lambda u^{\forall q (q \rightarrow r)}. u(\tau \rightarrow p) y)$ ma typ σ i nie jest postaci $there(N)$.

35b: To jest twierdzenie. Podstawiając $p := \neg q$ i korzystając z zadań (3a–3b) widzimy, że z lewej strony implikacji wynika $q \vee \neg q$. A zatem dowód naszej formuły można zapisać z pomocą termu:

$$\lambda x^{\forall p (q \vee \alpha)}. \text{case } x(\neg q) \quad \text{of } [u^q] \text{inleft}(u) \\ \text{or } [w^{\alpha'}] \text{inright}(\Lambda p. \text{case } xp \quad \text{of } [s^q] \varepsilon_\alpha(w(\lambda z^{\neg q \rightarrow q} s) \\ \text{or } [r^\alpha] r))$$

gdzie użyto skrótów $\alpha = ((p \rightarrow q) \rightarrow q) \rightarrow p$ i $\alpha' = \alpha[p := \neg q] = ((\neg q \rightarrow q) \rightarrow q) \rightarrow \neg q$.

35e: Yes, use the instantiation $p := p, q := \neg p$.

35f: No, consider a standard model¹⁰ of four states a, b, c, d with $a \leq b, c \leq d$ and incomparable b, c .

¹⁰All upward-closed subsets are values.

Take $v(p) = \{a, d\}$ and $v(q) = \{b, d\}$. Then $a \not\models (p \rightarrow q) \vee (q \rightarrow p)$, while $a \models \forall p(\neg p \vee \neg \neg p)$.

35l: No. Consider the algebra of open sets of $\{0\} \cup \{1/n \mid n \in \mathbb{N}_+\}$ and take $v(p) = \{1/n \mid n \in \mathbb{N}_+\}$.

36a: $\neg q \rightarrow q$ czyli $\neg \neg q$ (bo $\vdash \neg q \rightarrow (q \rightarrow p)$); **36b:** $q \rightarrow r$ (bo z jednej strony $q \vdash (q \rightarrow p) \rightarrow p$, a z drugiej $\vdash q \leftrightarrow (q \rightarrow q) \rightarrow q$); **36c:** $q \vee \neg q$ (bo z jednej strony $\neg q \vdash q \rightarrow p$, a z drugiej strony można przyjąć $p := \perp$); **36d:** $\top$ (bo wystarczy $p := q$).

37: Przyjmiemy τ jak w zadaniu 33 i $\varrho = \forall r(r \rightarrow r)$. Wtedy wyrażenie

$$\Lambda p \lambda x^{\tau \rightarrow \varrho \rightarrow p}. x(\Lambda r \lambda u^{\forall q(q \rightarrow r)}. u(\tau \rightarrow \varrho \rightarrow p)x) \mathbf{I}$$

ma typ $\tau \times \varrho$ i nie jest parą uporządkowaną.

38: Należy najpierw zdefiniować iloczyn kartezjański typów $\sigma \times \tau$, pary uporządkowane i rzutowania. Definicja rekursora jest taka:

$$\Lambda p \lambda f^{\omega \rightarrow p \rightarrow p} \lambda n^{\omega} \lambda y^p \pi_1(n(p \times \omega)(\lambda v^{p \times \omega} \langle f(\pi_2(v))(\pi_1(v)), \text{succ}(\pi_2(v)) \rangle))(y, \mathbf{0})).$$

39: W Coqu napiszemy

```
Inductive krzak : Set :=
| node : krzak -> krzak -> krzak -> krzak
| leaf : nat -> krzak
```

i dostaniemy taką zasadę indukcji:

```
krzak_ind
: forall P : krzak -> Prop,
  (forall k : krzak,
    P k ->
    forall k0 : krzak,
      P k0 -> forall k1 : krzak, P k1 -> P (node k k0 k1)) ->
  (forall n : nat, P (leaf n)) -> forall k : krzak, P k
```

W systemie **F** zdefiniujemy $\text{krzak} = \forall p((\omega \rightarrow p) \rightarrow (p \rightarrow p \rightarrow p \rightarrow p) \rightarrow p)$, a trzecia możliwość to $\text{krzak} = \mu p. \text{int} \oplus (p \times p \times p)$.

40a: $C_2 C_0 \rightarrow C_2 C_0$.

40b: Niech $C_0 = \lambda y_1^{c_1}. f_0(y_1 C_2)$, $C_2 = \lambda y_0^{c_0}. f_2(y_0 C_1)$, $C_1 = \lambda y_2^{c_2}. f_1(y_2 y_0)$, gdzie $f_0 : \beta_1 \rightarrow \beta_0$, $f_2 : \beta_0 \rightarrow \beta_2$, $f_1 : \beta_2 \rightarrow \beta_1$ są zmiennymi. Teraz $C_2 C_0 \rightarrow f_2(f_0(f_1(C_2 C_0)))$.

40c: Skoro tak, to $C_0 = \lambda \vec{x}_0 y_1. f_0(y_1 \vec{z}_1 C_2)$, $C_2 = \lambda \vec{x}_2 y_0. f_2(y_0 \vec{z}_0 C_1)$, $C_1 = \lambda \vec{x}_1 y_2. f_1(y_2 \vec{z}_2 y_0)$ (tutaj zmienne $\vec{z}_1, \vec{z}_2, \vec{z}_0$ są wolne) i mamy redukcję: $C_2 \vec{z}_2 C_0 \rightarrow f_2(f_0(f_1(C_2 \vec{z}_2 C_0)))$.

40d: Jest droga w drzewie τ od korzenia do negatywnej pozycji, na której znajduje się c_0 . Ta droga skręca w lewo nieparzystą liczbę razy, powiedzmy $2k + 1$. To wyznacza ciąg typów $c_0, c_1, \dots, c_{2k}, c_0$ spełniających równania podobne do tych w części (c), gdzie było $k = 1$.

41b: Term $\lambda t:\tau. t\omega(\lambda p:\omega \lambda q:\omega \lambda x:\omega. p+q)(\lambda x:\omega. \Lambda p \lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. x \underline{1})$ liczy liście, natomiast wysokość dostaniemy z pomocą termu $\lambda t:\tau. t\omega(\lambda p:\omega \lambda q:\omega \lambda x:\omega. 1 + \max\{p, q\})(\lambda x:\omega. \Lambda p \lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. x \underline{0})$

41c: Zdefiniujmy najpierw funkcje $\text{kons} = \lambda t:\tau \lambda s:\tau \lambda n:\omega. \Lambda p \lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. f(tpfx)(spfx)(xn)$ i $\text{leaf} : \lambda n:\omega \Lambda p \lambda f^{p \rightarrow p \rightarrow \omega \rightarrow p} \lambda x^{\omega \rightarrow p}. xn$. Zerowanie etykiet można teraz napisać tak:

$$\lambda t:\tau. t\tau(\lambda y:\tau \lambda z:\tau \lambda u:\omega. \text{kons} y z \underline{0})(\lambda u:\omega. \text{leaf} \underline{0}).$$

42: Trudna jest tylko symetria. Przyjmiemy otoczenie, w którym

$$x : \tau, \quad y : \tau, \quad \zeta : \mathbf{Eq}^\tau xy, \quad P : \tau \Rightarrow *.$$

Niech $W = (\lambda z:\tau)(Pz \rightarrow Px)$. Ponieważ $\mathbf{Eq}^\tau xy = (\forall P:\tau \Rightarrow *) (Px \rightarrow Py)$, więc aplikacja ζW ma typ $Wx \rightarrow Wy$ czyli typ $(Px \rightarrow Px) \rightarrow (Py \rightarrow Px)$. Zatem term $\zeta W \mathbf{I}$ (gdzie $\mathbf{I}$ to odpowiedni kombinatory identycznościowy) ma typ $(Py \rightarrow Px)$. Ostatecznie, term $(\lambda x:\tau)(\lambda y:\tau)(\lambda \zeta:\mathbf{Eq}^\tau xy)(\Lambda P:\tau \Rightarrow *).\zeta W \mathbf{I}$ ma typ $(\forall x:\tau)(\forall y:\tau)(\mathbf{Eq}^\tau xy \rightarrow \mathbf{Eq}^\tau yx)$.

43a: $\text{razydwa} := \lambda s^{\text{stream}}. \text{Coit}_{\text{stream}}(\lambda t^{\text{stream}} \langle 2 \cdot (\text{head } t), \text{tail } t \rangle) s$.

43b: $\text{head} := \lambda s^{\text{stream}}. \text{unpack } s \text{ as } [p, X^{p \times (p \rightarrow \text{int} \times p)}] \text{ in } \pi_1((\pi_2 X)(\pi_1 X))$,
 $\text{tail} := \lambda s^{\text{stream}}. \text{unpack } s \text{ as } [p, X^{p \times (p \rightarrow \text{int} \times p)}] \text{ in } [p, \langle \pi_2((\pi_2 X)(\pi_1 X)), \pi_2 X \rangle]$,

$razydwa := \lambda s^{\text{stream}}. \text{unpack } s \text{ as } [p, X^{p \times (p \rightarrow \text{int} \times p)}] \text{ in } [p, \langle \pi_1 X, \lambda x^p \langle 2 \cdot \pi_1(\pi_2 X x), \pi_2(\pi_2 X x) \rangle \rangle]$.

43c: Kwantyfikator $\exists$ jest definiowalny w systemie **F**, a currying eliminuje iloczyn kartezjański.

$\text{stream} := \forall q(\forall p(p \rightarrow (p \rightarrow \text{int}) \rightarrow (p \rightarrow p) \rightarrow q) \rightarrow q)$,

$Nats := \Lambda q \lambda z^{\forall p(\dots)}. z \text{ int } 0 \text{ id succ}$,

$head := \lambda s^{\text{stream}}. s \text{ int } (\Lambda p \lambda u^p \lambda v^{p \rightarrow \text{int}} \lambda w^{p \rightarrow p}. vu)$,

$tail := \lambda s^{\text{stream}}. s \text{ stream } (\Lambda p \lambda u^p \lambda v^{p \rightarrow \text{int}} \lambda w^{p \rightarrow p}. \Lambda q \lambda z^{\forall p(\dots)}. zp(wu)vw)$,

$razydwa := \lambda s^{\text{stream}}. s \text{ stream } (\Lambda p \lambda u^p \lambda v^{p \rightarrow \text{int}} \lambda w^{p \rightarrow p}. \Lambda q \lambda z^{\forall p(\dots)}. zpu(\lambda u. 2 \cdot (vu))w)$.