Logika i teoria typów

Wykład 5

8 listopada 2022

W poprzednim odcinku: Semantyka Kripkego

Definicja: *Model Kripkego:* struktura $\mathcal{C} = \langle C, \leq, \Vdash \rangle$, gdzie:

- C jest zbiorem *stanów*;
- $\leq$ jest częściowym porządkiem;
- $\Vdash \subseteq C \times \{p, q, r, \dots\}$;
- jeśli $c \Vdash p$ i $c \leq c'$, to $c' \Vdash p$.

Definicja: Rozszerzamy $\Vdash$ na dowolne formuły:

- $c \Vdash \varphi \vee \psi \quad \equiv \quad c \Vdash \varphi$ lub $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi \quad \equiv \quad c \Vdash \varphi$ i $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi \quad \equiv \quad$ jeśli $c \leq c' \Vdash \varphi$, to $c' \Vdash \psi$;
- $c \nVdash \bot$;
- $c \Vdash \neg\varphi \quad \equiv \quad$ jeśli $c \leq c'$, to $c' \nVdash \varphi$.

Monotoniczność:

Jeśli $c \Vdash \varphi$ oraz $c \leq c'$, to $c' \Vdash \varphi$.

Poprawność: Jeśli $\Gamma \vdash \varphi$, to $\Gamma \Vdash \varphi$.

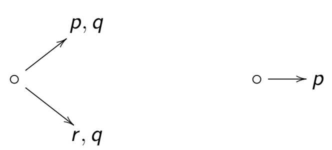
Wnioski z poprawności: kontrprzykłady

Formuły

$(\neg p \to q) \to (\neg r \to q) \to (p \to \neg r) \to q$

$((p \to q) \to p) \to p$

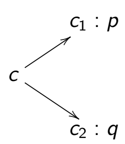
nie są twierdzeniami intuicjonistycznymi.



Wnioski z poprawności: separacja

Twierdzenie: *Żadnego ze spójników $\vee$, $\wedge$, $\to$, $\bot$, nie można zdefiniować z pozostałych.*

1. Alternatywa:

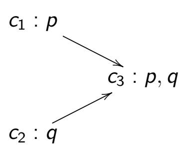


Jeśli φ – formuła bez $\vee$, to $\{c \mid c \Vdash \varphi\} \neq \{c_1, c_2\}$.
Inaczej: żadna formuła bez $\vee$ nie definiuje zbioru $\{c_1, c_2\}$.

Separacja – cd.

Twierdzenie: *Żadnego ze spójników $\vee$, $\wedge$, $\to$, $\bot$, nie można zdefiniować z pozostałych.*

2. Koniunkcja:

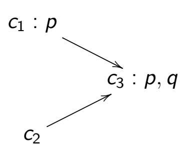


Żadna formuła bez $\wedge$ nie definiuje zbioru $\{c_3\}$.

Separacja – cd.

Twierdzenie: *Żadnego ze spójników $\vee$, $\wedge$, $\to$, $\bot$, nie można zdefiniować z pozostałych.*

3. Implikacja:



Żadna formuła bez $\to$ nie definiuje zbioru $\{c_2, c_3\}$.

Separacja – cd.

Twierdzenie: *Żadnego ze spójników $\vee$, $\wedge$, $\to$, $\bot$, nie można zdefiniować z pozostałych.*

4. Fałsz: Jeśli wszystkie zmienne formuły bez $\bot$ są wymuszone, to ta formuła też. (Formuła pozytywna nie może zawsze definiować zbioru pustego.)

Nagroda pocieszenia

Strzałka Kuzniecowa:
$K(p,q,r) = ((p \vee q) \wedge \neg r) \vee (\neg p \wedge (q \leftrightarrow r))$.

Fakt: Spójniki $\bot$, $\rightarrow$, $\vee$, $\wedge$ są definiowalne z pomocą strzałki Kuzniecowa.

Uwaga: Ale tu nie ma nic takiego, jak funkcyjna zupełność logiki klasycznej.

Pełność w sensie Kripkego

Twierdzenie: $\Gamma \vdash \varphi$ *wtedy i tylko wtedy, gdy* $\Gamma \Vdash \varphi$

Możliwy dowód: Pokazać, że $\Gamma \Vdash \varphi$ implikuje $\Gamma \models \varphi$ i skorzystać z pełności w sensie Heytinga.

W tym celu buduje się model Kripkego z *filtrów* danej algebry Heytinga.

Ale my to zrobimy inaczej...

Rachunek zdań jako gra (politycznie niepoprawna)

Mamy dwoje graczy: $\forall$frodytę i $\exists$rosa. $\exists$ros próbuje skonstruować dowód, $\forall$frodyta szuka błędu.

Przykład: $(p \to \neg q) \to (\neg p \to \neg q) \to \neg q$

Inaczej: $x : p \to \neg q, \quad y : \neg p \to \neg q, \quad z : q \quad \vdash \quad \bot$

Player ($\exists$): *I will prove* $\bot$ *using assumption* y!

Opponent ($\forall$): *Can you prove the 1st assumption* $\neg p$ *of* y? *That is, can you prove* $\bot$ *using an assumption* $v : p$?

Player ($\exists$): *Yes, I will use assumption* x!

Opponent ($\forall$): *Can you prove the 2nd assumption* q *of* x?

Player ($\exists$): *Sure, take* z!

Proof = strategy = inhabitant: $\lambda xyz.\, y(\lambda v.\, xvz)z$

Inny przykład: $\neg\neg(p \vee \neg p)$

$\exists$: $\neg\neg(p \vee \neg p)$!

$\forall$: $x : (p \vee \neg p) \to \bot \quad \vdash \bot$?

$\exists$: apply x!

$\forall$: $x : (p \vee \neg p) \to \bot \quad \vdash p \vee \neg p$?

$\exists$: $x : (p \vee \neg p) \to \bot \quad \vdash \neg p$!

$\forall$: $x : (p \vee \neg p) \to \bot, \quad y : p \quad \vdash \bot$?

$\exists$: apply x!

$\forall$: $x : (p \vee \neg p) \to \bot, \quad y : p \quad \vdash p \vee \neg p$?!

$\exists$: $x : (p \vee \neg p) \to \bot, \quad y : p \quad \vdash p$!

Rachunek zdań jako gra

Pozycja w grze to osąd $\Gamma \vdash \tau$. Jeśli $\tau = \alpha \vee \beta$, to α i β nazywamy *celami* w tej pozycji, w przeciwnym przypadku całe τ jest *celem*.

Mamy dwoje graczy: $\forall$frodytę i $\exists$rosa. $\exists$ros próbuje skonstruować dowód, $\forall$frodyta szuka błędu.

Każda runda gry to ruch $\exists$rosa i odpowiedź $\forall$frodyty. $\exists$ros wybiera (a) założenie $\alpha \in \Gamma$, lub (b) cel α w τ, po czym $\forall$frodyta ustala następną pozycję.

$\exists$ros wygrywa w *pozycji końcowej*: gdy $\bot \in \Gamma$, lub $\tau \in \Gamma$ (można żądać aby τ było atomem).

$\forall$frodyta wygrywa, jeśli rozgrywka jest nieskończona.

Strategia $\exists$rosa to dowód

W pozycji $\Gamma \vdash \tau$:

- wybór założenia $\alpha \in \Gamma$ to wybór dowodu przez eliminację typu zmiennej $x : \alpha$.
- wybór celu α w τ, to wybór dowodu przez wprowadzenie (konstrukcję) α.

Jak to jest w Coqu

Ruch $\exists$rosa, to użycie taktyki.

Ruch $\forall$frodyty, to wybór jednego z *subgoals*.

Reguły gry (w pozycji $\Gamma \vdash \tau$)

a1) Jeśli α jest założeniem $\beta \to \gamma$, to $\forall$frodyta wybiera jedną z pozycji $\Gamma, \gamma \vdash \tau$ and $\Gamma \vdash \beta$.

a2) Jeśli α jest założeniem $\beta \vee \gamma$, to $\forall$frodyta wybiera jedną z pozycji $\Gamma, \beta \vdash \tau$ and $\Gamma, \gamma \vdash \tau$.

a3) Jeśli α jest założeniem $\beta \wedge \gamma$, to $\forall$frodyta nie ma wyboru i następną pozycją jest $\Gamma, \beta, \gamma \vdash \tau$.

b1) Jeśli α jest celem $\beta \to \gamma$, to $\forall$frodyta nie ma wyboru i następną pozycją jest $\Gamma, \beta \vdash \gamma$.

b2) Jeśli α jest celem $\beta \wedge \gamma$, to $\forall$frodyta wybiera jedną z pozycji $\Gamma \vdash \beta$ and $\Gamma \vdash \gamma$.

b3) Jeśli α is celem atomowym albo celem $\beta \vee \gamma$, to $\forall$frodyta nie ma wyboru i następną pozycją jest $\Gamma \vdash \alpha$.

Strategia ∃rosa to dowód

Fakt: *Jeśli ∃ros ma strategię wygrywającą w pozycji $\Gamma \vdash \tau$, to osąd $\Gamma \vdash \tau$ ma dowód.*

Dowód: Indukcja ze względu na rozmiary strategii ∃rosa.

Pozycje końcowe:

- $\Gamma, x : \tau \vdash x : \tau$;
- $\Gamma, x : \bot \vdash x[\tau] : \tau$;

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa.

∃ros wybiera założenie $(x : \alpha) \in \Gamma$:

a1) Jeśli α jest założeniem $\beta \to \gamma$, to ∀frodyta wybiera jedną z pozycji $\Gamma, \gamma \vdash \tau$ and $\Gamma \vdash \beta$.

Jeśli ∃ros wygrywa w obu pozycjach $\Gamma, \gamma \vdash \tau$ i $\Gamma \vdash \beta$, to są termy $\Gamma, y : \gamma \vdash M : \tau$ oraz $\Gamma \vdash N : \beta$.

Wtedy $\Gamma \vdash M[y := x^{\beta\to\gamma}N] : \tau$.

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa:

∃ros wybiera założenie $(x : \alpha) \in \Gamma$:

a2) Jeśli α jest założeniem $\beta \vee \gamma$, to ∀frodyta wybiera jedną z pozycji $\Gamma, \beta \vdash \tau$ and $\Gamma, \gamma \vdash \tau$.

Jeśli ∃ros wygrywa w obu pozycjach $\Gamma, \beta \vdash \tau$ i $\Gamma, \gamma \vdash \tau$, to są termy $\Gamma, y : \beta \vdash M : \tau$ oraz $\Gamma, z : \gamma \vdash N : \tau$

Wtedy $\Gamma \vdash x^{\beta\vee\gamma}[y.\, M; z.\, N] : \tau$.

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa.

∃ros wybiera założenie $(x : \alpha) \in \Gamma$:

a3) Jeśli α jest założeniem $\beta \wedge \gamma$, to ∀frodyta nie ma wyboru i następną pozycją jest $\Gamma, \beta, \gamma \vdash \tau$.

Jeśli $\Gamma, y : \beta, z : \gamma \vdash M : \tau$, to

$$\Gamma \vdash M[y := x^{\beta\wedge\gamma}\{1\}][z := x^{\beta\wedge\gamma}\{2\}] : \tau.$$

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa.

∃ros wybiera cel α w pozycji $\Gamma \vdash \alpha \vee \rho$:

b1) Jeśli α jest celem $\beta \to \gamma$, to ∀frodyta nie ma wyboru i następną pozycją jest $\Gamma, \beta \vdash \gamma$.

Przypuśćmy że $\Gamma, y : \beta \vdash M : \gamma$. Wtedy $\Gamma \vdash \lambda x : \beta.\, M^\gamma : \alpha$.

Jeśli $\tau = \alpha \vee \rho$, to $\Gamma \vdash \mathrm{in}_1(\lambda x : \beta.\, M) : \tau$.

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa.

∃ros wybiera cel α w pozycji $\Gamma \vdash \alpha \vee \rho$:

b2) Jeśli α jest celem $\beta \wedge \gamma$, to ∀frodyta wybiera jedną z pozycji $\Gamma \vdash \beta$ and $\Gamma \vdash \gamma$.

Jeśli $\Gamma \vdash M : \beta$ oraz $\Gamma \vdash N : \gamma$, to $\Gamma \vdash \langle M, N\rangle : \alpha$.

Dla $\tau = \alpha \vee \rho$ mamy $\Gamma \vdash \mathrm{in}_1(\langle M, N\rangle) : \tau$.

Strategia ∃rosa to dowód

Indukcja ze względu na rozmiary strategii ∃rosa.

∃ros wybiera cel α w pozycji $\Gamma \vdash \alpha \vee \rho$:

b3) Jeśli α is celem atomowym albo celem $\beta \vee \gamma$, to ∀frodyta nie ma wyboru i następną pozycją jest $\Gamma \vdash \alpha$.

Jeśli $\Gamma \vdash M : \alpha$ oraz $\tau = \alpha \vee \rho$, to $\Gamma \vdash \mathrm{in}_1(M) : \tau$.

A jeśli ∃ros nie ma strategii?

Co to znaczy, że ∃ros ma strategię w pozycji $\mathcal{P}$?

- Pozycja $\mathcal{P}$ jest końcowa, lub istnieje taki ruch ∃rosa, że każda odpowiedź ∀frodyty prowadzi do pozycji, w której ∃ros ma strategię.

Co to znaczy, że ∃ros nie ma strategii w pozycji $\mathcal{P}$?

- Pozycja $\mathcal{P}$ nie jest końcowa, oraz dla każdego ruchu ∃rosa, istnieje odpowiedź ∀frodyty, która prowadzi do pozycji, gdzie ∃ros nie ma strategii.

To znaczy, że ∀frodyta umie grać nieskończenie długo.
Czyli to ona ma strategię. Ta gra jest *zdeterminowana*.

Strategia ∀frodyty, czyli *refutacja*

Strategia ∀frodyty, to drzewo S etykietowane pozycjami niekońcowymi, spełniające taki warunek:

- Dla każdego ruchu ∃rosa w dowolnym wierzchołku $\mathcal{P}$, istnieje odpowiedź ∀frodyty, prowadząca do pewnego następnika wierzchołka $\mathcal{P}$ w drzewie S.

Dygresja: własność skończonej strategii

Strategia ∀frodyty jest nieskończonym drzewem zbudowanym ze skończenie wielu różnych pozycji. Na każdej gałęzi pozycje się od pewnego miejsca powtarzają. Po pierwszym takim powtórzeniu sędzia powinien przerwać grę.

Zatem strategia (refutacja) to w istocie skończony obiekt.

Strategia ∀frodyty: notacja

Niech S będzie strategią wygrywającą ∀frodyty.

- Jeśli $\mathcal{P} = (\Gamma \vdash \tau)$, to $\Gamma_\mathcal{P} = \Gamma$ i $\tau_\mathcal{P} = \tau$.
- Jeśli pozycja $\mathcal{P}'$ jest w S następnikiem pozycji $\mathcal{P}$, to piszemy $S : \mathcal{P} \to \mathcal{P}'$.

Strategia ∀frodyty to kontrmodel Kripkego

Pierwsze koty za płoty:

– Stany modelu to pozycje w strategii;
– porządek to $\twoheadrightarrow$;
– wymuszanie $\mathcal{P} \Vdash p$, gdy $p \in \Gamma_\mathcal{P}$;
– chcemy $\mathcal{P} \Vdash \alpha$, gdy $\alpha \in \Gamma_\mathcal{P}$.

Tak jest niedobrze: Niech $\mathcal{P} = (p \to q,\ p \vdash r)$.
Wtedy $\mathcal{P} \nVdash p \to q$, bo $\mathcal{P} \Vdash p$, ale $\mathcal{P} \nVdash q$.

Dopiero w następnej pozycji $\mathcal{P}' = (p \to q, p, q \vdash r)$ mamy $\mathcal{P}' \Vdash p \to q$.

Pozycja nasycona

Pozycja $\mathcal{P}$ jest *nasycona*, gdy każda runda „statyczna'' (bez zmiany tezy) jest trywialna (nie wprowadza nowych założeń).

Lemat: *W strategii wygrywającej ∀frodyty, dla dowolnej pozycji $\mathcal{P}$ istnieje taka nasycona pozycja $\mathcal{Q}$, że $\mathcal{P} \twoheadrightarrow \mathcal{Q}$ i $\tau_\mathcal{Q} = \tau_\mathcal{P}$.*

Dowód: Strategia przewiduje wszystkie ruchy ∃rosa.
Jest ścieżka, gdzie każda runda jest statyczna.
Dodawanie nowych założeń musi się skończyć.

Model

- Stany modelu to pozycje nasycone w strategii.
- Porządek to $\twoheadrightarrow$.
- Wymuszanie $\mathcal{P} \Vdash p$, gdy $p \in \Gamma_P$.

Lemat: *Let $\mathcal{P} = (\Gamma \vdash \tau)$ be a saturated position in a winning strategy S.*

If α is an assumption in $\mathcal{P}$ then $\mathcal{P} \Vdash \alpha$, and if α is a goal in $\mathcal{P}$, then $\mathcal{P} \nVdash \alpha$.

Dowód: Indukcja ze względu na α.

Dowód lematu

Lemat: *Jeśli $\mathcal{P}$ nasycona, to $\mathcal{P} \Vdash \Gamma_\mathcal{P}$ i $\mathcal{P} \nVdash \tau_\mathcal{P}$*

Dowód: Przypadek założenia $\alpha = \beta \to \gamma$.

Niech $\mathcal{P} \leq \mathcal{Q}$ i $\mathcal{Q} \Vdash \beta$. Formuła α jest założeniem w $\mathcal{Q}$, więc ∃ros może wskazać α w pozycji $\mathcal{Q}$. Jeśli ∀frodyta odpowie $\Gamma_\mathcal{Q} \vdash \beta$, to istnieje taka nasycona pozycja $\mathcal{R} \geq \mathcal{Q}$, że $\tau_\mathcal{R} = \tau_\mathcal{Q} = \beta$. Wtedy $\mathcal{R} \nVdash \beta$ z założenia indukcyjnego o β oraz $\mathcal{R} \Vdash \beta$, ponieważ $\mathcal{Q} \leq \mathcal{R}$. Sprzeczność.

Zatem ∀frodyta musi przejść do $\Gamma_\mathcal{Q}, \gamma \vdash \tau_\mathcal{Q}$.
To jest runda statyczna, a $\mathcal{Q}$ jest nasycona, więc $\gamma \in \Gamma_\mathcal{Q}$.
Zatem $\mathcal{Q} \Vdash \gamma$ z założenia indukcyjnego o γ.

Dowód lematu

Lemat: *Jeśli $\mathcal{P}$ nasycona, to $\mathcal{P} \Vdash \Gamma_\mathcal{P}$ i $\mathcal{P} \nVdash \tau_\mathcal{P}$*

Dowód: Przypadek $\tau_\mathcal{P} = \beta \wedge \gamma$. Wtedy jedna z pozycji $\Gamma \vdash \beta$, $\Gamma \vdash \gamma$ należy do strategii i rozszerza się do nasyconej pozycji $\mathcal{R}$, gdzie $\tau_\mathcal{R} = \beta$ lub $\tau_\mathcal{R} = \gamma$. Z założenia indukcyjnego $\mathcal{R} \nVdash \beta$ lub odpowiednio $\mathcal{R} \nVdash \gamma$.
Ponieważ $\mathcal{P} \leq \mathcal{R}$, więc tym bardziej $\mathcal{P} \nVdash \beta$ lub $\mathcal{P} \nVdash \gamma$.

Przypadek celu atomowego p: pozycja należy do strategii wygrywającej ∀frodyty, więc $p \notin \Gamma_\mathcal{P}$.

Inne przypadki podobnie.

Główny lemat

Lemat: *Jeśli ∀frodyta ma strategię w pozycji $\mathcal{P} = (\Gamma_{\mathcal{P}} \vdash \tau_{\mathcal{P}})$, to $\Gamma_{\mathcal{P}} \not\Vdash \tau_{\mathcal{P}}$.*

Dowód: Istnieje pozycja nasycona $\mathcal{Q} \geq \mathcal{P}$, gdzie $\Gamma_{\mathcal{P}} \subseteq \Gamma_{\mathcal{Q}}$ oraz $\tau_{\mathcal{Q}} = \tau_{\mathcal{P}}$.

Uwaga:
I na odwrót: kontrmodel wyznacza pewną strategię ∀frodyty.

Pełność Kripkego

Twierdzenie: *Dla dowolnego osądu $\Gamma \vdash \tau$:*

– albo istnieje dowód $\Gamma \vdash M : \tau$,

– albo istnieje kontrmodel, tj. $\Gamma \not\Vdash \tau$.

Wniosek: *Jeśli $\Gamma \Vdash \tau$, to $\Gamma \vdash \tau$.*

Wnioski z twierdzenia o pełności

Prawo alternatywy (disjunction property)

Twierdzenie: Jeśli $\vdash \alpha \vee \beta$, to $\vdash \alpha$ lub $\vdash \beta$.

Dowód: Przypuśćmy, że $\nvdash \alpha$ i $\nvdash \beta$.
Wtedy $\mathcal{C}_1, c_1 \not\Vdash \alpha$ oraz $\mathcal{C}_2, c_2 \not\Vdash \beta$.

Nowy model: $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \{c_0\}$, gdzie c_0 nowy i najmniejszy. Relacja $\Vdash$ jest sumą relacji z $\mathcal{C}_1$ i $\mathcal{C}_2$. W stanie c_0 nie są wymuszane żadne zmienne zdaniowe.

Jeśli $\vdash \alpha \vee \beta$, to także $c_0 \Vdash \alpha \vee \beta$, skąd $c_0 \Vdash \alpha$ lub $c_0 \Vdash \beta$. Ale wtedy także $c_1 \Vdash \alpha$ lub $c_2 \Vdash \beta$.

Własność podformuł dla gier

Lemat: *Wszystkie formuły używane w grze rozpoczętej w pozycji początkowej $\varnothing \vdash \tau$ są podformułami formuły τ.*

W szczególności spójniki logiczne występujące w takiej grze to są tylko te spójniki, które są w τ.

Dowód: Indukcja.

Własność skończonego modelu

Twierdzenie:

Jeśli $\mathcal{C} \Vdash \varphi$ dla wszystkich skończonych modeli $\mathcal{C}$, to $\Vdash \varphi$.

Dowód: Model otrzymany ze strategii ∀frodyty jest nieskończony, ale od pewnego miejsca stany się powtarzają, bo jest tylko skończenie wiele mozliwych pozycji. Można obcinać nieskończone gałęzie po pierwszych powtórzeniach.

Twierdzenie Gliwienki

Twierdzenie:

Formuła zdaniowa α jest klasyczną tautologią wtedy i tylko wtedy, gdy $\neg\neg\alpha$ jest twierdzeniem intuicjonistycznym.

Dowód: ($\Leftarrow$) Oczywiste.

($\Rightarrow$) Wtedy α jest wymuszona w każdym stanie końcowym.

Konserwatywność

Wniosek: *Jeśli ∃ros ma strategię w pozycji $\varnothing \vdash \tau$, gdzie τ jest formułą implikacyjną (typem prostym), to τ ma inhabitanta w zwykłym rachunku lambda.*

Dowód: Wszystkie formuły są implikacyjne
(bo mamy własność podformuł),
więc każda runda ma postać (a1) lub (b1).
Term, który opisuje strategię ∃rosa zawiera więc
tylko abstrakcje i aplikacje.

Wniosek: *Typ prosty jest niepusty wtedy i tylko wtedy, gdy jest tautologią intuicjonistyczną.*