

Logika intuicjonistyczna

Antoni Kościelski

1 Semantyka Kripke’go

1.1 Wykorzystywany język

Będziemy zajmować się rachunkiem zdań, w którym mamy prawo posługiwać się trzema spójnikami: koniunkcją $\wedge$, alternatywą $\vee$ i implikacją $\rightarrow$ oraz stałą $\perp$ (rozumianą jako „sprzeczność”, czyli takie stwierdzenie, którego nikt nie uzna za prawdziwe).

Rzecz jasna, mamy prawo, oprócz wymienionych symboli, posługiwania się zmiennymi zdaniowymi.

Formuły rachunku zdań definiujemy w zwykły sposób, używając w razie potrzeby nawiasów.

Dodatkowo, będziemy pisać $\neg p$ oraz $p \leftrightarrow q$. Napisy takiej postaci będziemy uważać za skróty następujących formuł, odpowiednio negacji i równoważności:

$$\neg p = p \rightarrow \perp \quad \text{oraz} \quad p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p).$$

1.2 Semantyka Kripke’go

„Prawdziwość” formuł rozważanego języka będziemy ustalać odwołując się do intuicji związanych z pracą ekspertów. Eksperci będą pochodzić z wszystkich krajów, każdy z nich będzie dysponować pewną wiedzą. Dalej V oznacza zbiór zmiennych zdaniowych.

Przyjmijmy, że

- 1) Świat jest zbiorem krajów. Formuła φ jest tautologią (intuicjonistyczną) (symbolicznie: $\Vdash \varphi$), jeżeli w każdym kraju eksperci uznali ją za spełnioną.
- 2) Niech C oznacza kraj. Każdy kraj utożsamiamy ze zbiorem ekspertów tego kraju, czyli C rozumiemy jako zbiór ekspertów danego kraju. Formuła φ jest uważana w kraju C za spełnioną (symbolicznie: $C \Vdash \varphi$), jeżeli wszyscy eksperci tego kraju uznali ją za spełnioną. Tak więc

$$\Vdash \varphi \Leftrightarrow \forall C \, C \Vdash \varphi.$$

- 3) Każdy ekspert jest ekspertem określonego kraju (nie funkcjonuje poza swoim krajem) i dysponuje pewną wiedzą, którą utożsamiamy z zbiorem zmiennych zdaniowych (pewnych, tych, które ekspert uważa za spełnione lub prawdziwe). Formalnie, kraj C możemy uważać za podzbiór $\mathcal{P}(\mathcal{P}(V))$, wtedy ekspert $c \in C$ należy do $\mathcal{P}(V)$, czyli jest podzbiorem V . Mamy więc

$$C \Vdash \varphi \Leftrightarrow \forall c \in C \, c \Vdash \varphi.$$

- 4) Ekspert c z kraju C ustala swoje opinie, czyli stwierdzenia „uważam formułę φ za spełnioną” (symbolicznie: $c \Vdash \varphi$), zgodnie z następującymi zasadami:
- (a) $c \Vdash p \Leftrightarrow p \in c$ w przypadku formuły będącej zmienną zdaniową p ,
 - (b) $c \Vdash \varphi \wedge \psi \Leftrightarrow c \Vdash \varphi$ oraz $c \Vdash \psi$,
 - (c) $c \Vdash \varphi \vee \psi \Leftrightarrow c \Vdash \varphi$ lub $c \Vdash \psi$,
 - (d) $c \nVdash \perp$ (stałej $\perp$ żaden ekspert nie uważa za spełnioną).
- 5) W przypadku implikacji ekspert swoją opinią uzgadnia z innymi ekspertami kraju, z którego pochodzi. Jeżeli bada spełnialność implikacji $\varphi \rightarrow \psi$, to prosi wszystkich ekspertów z jego kraju, takich którzy dysponują wiedzą obszerniejszą od niego, i twierdzą, że formuła φ jest spełniona o odpowiedź na pytanie, czy formuła ψ jest spełniona. Prośbę tę kieruje także do siebie, chyba że uważa φ za niespełnione. Jeżeli uzyska zgodną odpowiedź, że tak, to twierdzi, że implikacja $\varphi \rightarrow \psi$ jest spełniona. Tak więc dla $c \in C$ mamy

$$c \Vdash \varphi \rightarrow \psi \Leftrightarrow \forall c' \in C (c \subseteq c' \wedge c' \Vdash \varphi) \Rightarrow c' \Vdash \psi. \quad (1)$$

1.3 Kilka własności semantyki Kripke’go

Lemat 1.1 *Jeżeli $c, c' \in C$ oraz $c \subseteq c'$, to warunek $c \Vdash \varphi$ pociąga za sobą, że $c' \Vdash \varphi$.*

Dowód. Przez indukcję ze względu na budowę formuły φ . $\square$

Lemat 1.2 *Przypuśćmy, że $c \in C$. Wtedy własność $c \Vdash \neg\varphi$ jest równoważna stwierdzeniu, że $c' \nVdash \varphi$ zachodzi dla wszystkich $c' \in C$ takich, że $c \subseteq c'$.*

Dowód. Wystarczy w równoważności (1) podstawić $\perp$ zamiast ψ . $\square$

Wniosek 1.3 *W kraju C , w którym jest jeden ekspert, wiedza tego eksperta wyznacza wartościowanie zmiennych zdaniowych h : to wartościowanie przyporządkowuje **T** tym zmiennym, które ekspert tego kraju uważa za spełnione, a pozostałym zmiennym przyporządkowuje **F**. W tej sytuacji, dla wszystkich formuł φ zachodzi równoważność*

$$C \Vdash \varphi \Leftrightarrow \varphi[h] = \mathbf{T}. \quad \square$$

Wniosek 1.4 *Tautologie intuicjonistycznego rachunku zdań są tautologiami klasycznego rachunku zdań.* $\square$

Przykład 1.5 Formuła $p \rightarrow \neg\neg p = p \rightarrow ((p \rightarrow \perp) \rightarrow \perp)$ jest tautologią intuicjonistyczną. Aby się o tym przekonać, weźmy dowolny kraj C i dowolnego eksperta c z tego kraju, przekonanego o spełnialności p (takiego, że $p \in c$). Chcemy pokazać, że $c \Vdash \neg\neg p$. W tym celu, zgodnie z lematem 1.2, należy wykazać, że $c' \nVdash \neg p$ dla dowolnego $c' \supset c$. Jest to oczywiste, ponieważ $p \in c'$, więc gdyby c' stwierdzał spełnialność $\neg p = p \rightarrow \perp$, to musiałby także twierdzić, że spełniona jest formuła $\perp$.

Przykład 1.6 Formuła $\neg\neg p \rightarrow p = ((p \rightarrow \perp) \rightarrow \perp) \rightarrow p$ nie jest tautologią intuicjonistyczną. Aby się o tym przekonać, weźmy kraj C , w którym jest tylko dwóch ekspertów: $\emptyset$, przekonany o niespełnialności dowolnego $p \in V$, oraz $\{p\}$,

przekonany wyłącznie o spełnialności zmiennej p . Obaj ci eksperci są przekonani o niespełnialności formuły $\neg p = p \rightarrow \perp$. Drugi dlatego, bo musi uwzględnić swoją opinię o spełnialności formuły $\perp$, która jest oczywiście negatywna. Pierwszy dlatego, bo mimo że sam nie musi się zastanawiać ($p \notin \emptyset$) nad spełnialnością $\perp$, to jednak musi uwzględnić opinię drugiego eksperta, która, rzecz jasna, jest negatywna. W tej sytuacji ekspert $\emptyset$ jest przekonany o spełnialności $\neg\neg p = \neg p \rightarrow \perp$. Zastanawiając się nad spełnialnością tej implikacji musi uwzględnić opinie innych ekspertów, ale tylko przekonanych o spełnialności formuły $\neg p$. W rozważanym kraju takich ekspertów nie ma. Nie usłyszy więc negatywnych opinii, a więc przekona się o słuszności stwierdzenia $\neg\neg p$. Gdy będzie więc rozstrzygać o słuszności implikacji $\neg\neg p \rightarrow p$, będzie przekonany o słuszności jej poprzednika, ale będzie też uważać, że nie zachodzi jej następnik. Odrzuci więc prawdziwość implikacji na podstawie własnej opinii.

Przykład 1.7 Podobnie, jak w poprzednim przykładzie, można wykazać, że w kraju, w którym jest dwóch ekspertów c i c' , takich, że $c \subseteq c'$, nie uważa się prawdziwe prawa wyłączonego środka, a w szczególności formuły $p \vee \neg p$, gdzie $p \in c' \setminus c$. Wynika to z opinii eksperta c .

2 Algebry Heytinga

2.1 Intuicje

Dość trudno powiedzieć, jakie zdania uważamy za prawdziwe. Za to mamy dobrze opracowane metody uzasadniania relatywnej prawdziwości: często przekonywujemy się na wzajem, że prawdziwość jakichś faktów pociąga za sobą prawdziwość innych. Mając zbiór jakiś faktów T , lub zbiór powszechnie przyjętych aksjomatów, możemy w zbiorze wszystkich formuł wprowadzić relację $\sim$, w której są każde dwie formuły, o których ze zbioru T potrafimy wyprowadzić, że są równoważne. Formuły φ i ψ takie, że $\varphi \sim \psi$ możemy uważać za równie prawdziwe (w pewnym sensie). Relacja $\sim$ powinna być relacją równoważności. Jej klasy abstrakcji możemy uważać za „miary prawdziwości” (coś, co oddaje, jak bardzo formuła jest prawdziwa) lub za wartości logiczne. Przyjrzyjmy się tym klasom abstrakcji.

Wraz z relacją $\sim$ w zbiorze jej klas abstrakcji możemy wprowadzić wiele innych działań i relacji. W pierwszym rzędzie możemy wprowadzić porządek częściowy przyjmując, że

$$[\varphi]_{\sim} \leq [\psi]_{\sim} \Leftrightarrow \text{z } T \text{ potrafimy wyprowadzić } \varphi \rightarrow \psi.$$

Relację $[\varphi]_{\sim} \leq [\psi]_{\sim}$ można rozumieć jako stwierdzenie, że formuła ψ jest „bardziej prawdziwa” niż formuła φ . Wśród klas abstrakcji relacji $\sim$ mamy klasę największą (klasa $[\varphi]_{\sim}$ dla $\varphi \in T$ lub formuł φ takich jak $p \rightarrow p$) i najmniejszą (klasa negacji aksjomatów lub formuł takich, jak $p \wedge \neg p$).

Dalej, w zbiorze klas abstrakcji relacji $\sim$ możemy wprowadzić dwa działania $\cap$ i $\cup$ przyjmując

$$[\varphi]_{\sim} \cap [\psi]_{\sim} = [\varphi \wedge \psi]_{\sim} \quad \text{oraz} \quad [\varphi]_{\sim} \cup [\psi]_{\sim} = [\varphi \vee \psi]_{\sim}.$$

Te działania są dobrze określone i pozwalają dla danych stopni „prawdziwości” formuł φ i ψ , wyliczyć, jak bardzo „prawdziwe” są formuły $\varphi \wedge \psi$ i $\varphi \vee \psi$. Jest też widoczny związek między tymi działaniami i porządkiem. Wiemy, że zawsze $\varphi \wedge \psi$ implikuje zarówno φ , jak i ψ . Dla porządku $\leq$ oznacza to, że klasa $[\varphi \wedge \psi]_{\sim}$

ogranicza z dołu obie klasy $[\varphi]_{\sim}$ i $[\psi]_{\sim}$. Z drugiej strony, z faktów $\sigma \rightarrow \varphi$ oraz $\sigma \rightarrow \psi$ potrafimy wywnioskować, że $\sigma \rightarrow \varphi \wedge \psi$. W języku porządku oznacza to, że klasa $[\varphi \wedge \psi]_{\sim}$ jest największym ograniczeniem dolnym klas $[\varphi]_{\sim}$ i $[\psi]_{\sim}$. Tak więc klasa $[\varphi \wedge \psi]_{\sim}$ jest kresem dolnym zbioru klas $\{[\varphi]_{\sim}, [\psi]_{\sim}\}$. Podobnie, klasa $[\varphi \vee \psi]_{\sim}$ jest kresem górnym tego zbioru.

Tak definiowane struktury można uważać za algebry i nazywa się algebrami Lindenbauma.

2.2 Kraty, czyli lattices

Kraty można definiować na dwa sposoby: Są to albo zbiory częściowo uporządkowane, w których każde dwa elementy a i b mają kresy dolny $a \cap b$ i górny $a \cup b$. Albo są to algebry z dwoma działaniami $\cap$ i $\cup$, dwuargumentowymi, łącznymi i przemennymi, spełniającymi dodatkowo prawa absorpcji

$$(a \cap b) \cup b = b \quad \text{oraz} \quad (a \cup b) \cap b = b.$$

Obie definicje są równoważne. W szczególności, w takich algebrach warunki $a \cup b = b$ oraz $a \cap b = a$ są równoważne i definiują porządek ich uniwersów o własnościach wymaganych od krat.

2.3 Relatywne pseudodopełnienie

Przypuśćmy, że mamy daną kratę z porządkiem $\leq$ i operacjami kresu dolnego $\cap$ i górnego $\cup$. Dla dwóch elementów a i b tej kraty relatywnym pseudodopełnieniem a względem b (a do b ?) nazywamy – o ile istnieje – największy element x taki, że $a \cap x \leq b$. Relatywne pseudodopełnienie a względem b będziemy oznaczać symbolem $a \Rightarrow b$. Może zostać scharakteryzowane przez warunek

$$a \cap x \leq b \Leftrightarrow x \leq a \Rightarrow b \tag{2}$$

zachodzący dla wszystkich elementów x należących do rozważanej kraty.

Jeżeli zgodzimy się z tym, że następujące formuły

$$\varphi \wedge (\varphi \rightarrow \psi) \rightarrow \psi \quad \text{oraz} \quad (\varphi \wedge \sigma \rightarrow \psi) \rightarrow (\sigma \rightarrow (\varphi \rightarrow \psi))$$

są prawami logiki, to rozważania z rozdziału 2.1 można uzupełnić o spostrzeżenie, że klasa abstrakcji $[\varphi \rightarrow \psi]_{\sim}$ jest relatywnym pseudodopełnieniem $[\varphi]_{\sim}$ względem $[\psi]_{\sim}$.

Przykład 2.1 Rozważmy pięcioelementowy zbiór uporządkowany, w którym są elementy największy **max** i najmniejszy **min**, a także trzy wzajemnie nieporównywalne elementy pośrednie a , b i c . Jest to krata. Warunek $a \cap x \leq b$ jest w tej kratce spełniony przez dwa elementy $x = b$ i $x = c$. Nie ma wśród nich elementu największego. Inaczej: nie można w niej wskazać takiego elementu $a \Rightarrow b$, aby zachodziła równoważność (1). Tak więc w tej kratce nie można zdefiniować operacji relatywnego pseudodopełnienia.

2.4 Algebry Heytinga

Algebrą Heytinga nazywamy dowolną kratę, w której każde dwa elementy a i b mają relatywne pseudodopełnienie $a \Rightarrow b$, i w której jest element najmniejszy **0**.

W algebrach Heytinga można wprowadzić operację dopełniania przyjmując, że dopełnieniem a jest $\neg a = a \Rightarrow \mathbf{0}$.

Lemat 2.2 *W algebrach Heytinga jest element największy.*

Dowód. Tym elementem – na mocy równoważności (2) – jest $a \Rightarrow a$ (bierzemy dowolne a). $\square$

Element największy w algebrze Heytinga będziemy oznaczać symbolem **1**.

Lemat 2.3 *W algebrach Heytinga, dla dowolnego a mamy $a \cap -a = a \cap (a \Rightarrow 0) = 0$ i – wobec tego – zachodzi także nierówność $a \leq - - a$.*

Dowód. Jeżeli w równoważności (2) wyrażenie b zastąpimy przez **0** i podstawimy dopełnienie $-a$ za x , to lewa strona równoważności okaże się nierównością $a \cap (a \Rightarrow 0) \leq 0$ równoważną tezie, a prawa strona jest oczywiście prawdziwa. Możemy też spowodować, aby lewa strona równoważności (2) była nierównością postaci $(a \Rightarrow 0) \cap a \leq 0$, prawdziwą na mocy pierwszej części dowodu. Wtedy prawa strona będzie nierównością $a \leq (a \Rightarrow 0) \Rightarrow 0$, czyli $a \leq - - a$, i też będzie prawdziwa. $\square$

W algebrach Heytinga na ogół nie zachodzi prawo $a = - - a$. Jeżeli jednak zachodzi w pewnej algebrze Heytinga, to ta algebra staje się algebrą Boole’a.

W kratkach na ogół nie zachodzą prawa rozdzielności: można wykazać tylko jedną nierówność, na przykład

$$(a \cap b) \cup (a \cap c) \leq a \cap (b \cup c).$$

Przeciwna nierówność nie musi zachodzić, podobna sytuacja dotyczy prawa rozdzielności działania $\cup$ względem $\cap$. Przykładem może być pięcioelementowa krata z elementami największym i najmniejszym, i trzema innymi, wzajemnie nieporównywalnymi elementami.

Lemat 2.4 *W algebrach Heytinga zachodzą oba prawa rozdzielności.*

Dowód. Zauważmy, że

- 1) $a \cap b \leq (a \cap b) \cup (a \cap c)$,
- 2) $b \leq a \Rightarrow (a \cap b) \cup (a \cap c)$, na mocy równoważności (2),
- 3) $c \leq a \Rightarrow (a \cap b) \cup (a \cap c)$, z tych samych powodów,
- 4) $b \cup c \leq a \Rightarrow (a \cap b) \cup (a \cap c)$, z własności kresu górnego,
- 5) $a \cap (b \cup c) \leq (a \cap b) \cup (a \cap c)$, na podstawie (2),
- 6) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ ze słabej antysemtryczności $\leq$ (przeciwna relacja w dowolnej kratce jest łatwa do wykazania).

Drugie prawo rozdzielności dowodzimy analogicznie. $\square$

Przykładami algebr Heytinga mogą być zbiory potęgowe $P(X)$ z relacją zawierania (wtedy $A \cup B$ i $A \cap B$ są zwykłymi działaniami mnogościowymi, sumą i przekrojem, zaś $A \Rightarrow B = (X \setminus A) \cup B$), zbiory dzielników ustalonej liczby naturalnej n uporządkowane relacją podzielności (wtedy $a \cup b = NWW(a, b)$, $a \cap b = NWD(a, b)$), a także skończone zbiory liniowo uporządkowane ($a \cup b = \max(a, b)$, $a \cap b = \min(a, b)$, $a \Rightarrow b$ jest elementem największym w przypadku, gdy $a \leq b$, i równa się b w przeciwnym razie).

Ważnym przykładem algebry Heytinga jest rodzina otwartych podzbiorów płaszczyzny R^2 z relacją zawierania. Zbiór $X \subseteq R^2$ jest otwarty, jeżeli wraz z każdym elementem $p \in X$ są w nim wszystkie punkty odległe od p o mniej niż pewne dodatnie ε . Kwadrat jednostkowy z tzw. brzegiem $\{(x, y) \in R^2 : 0 \leq x, y \leq 1\}$ nie jest otwarty, w przeciwieństwie do kwadratu bez brzegu $\{(x, y) \in R^2 : 0 < x, y < 1\}$. Każdy zbiór na płaszczyźnie ma tzw. wnętrze, czyli największy zbiór otwarty w nim zawarty. W tej algebrze $A \cup B$ i $A \cap B$ są równe odpowiednio sumie mnogościowej i przekrojowi A i B , zaś $A \Rightarrow B$ jest wnętrzem zbioru $(R^2 \setminus A) \cup B$.

2.5 Wartościowanie formuł w algebrach Heytinga

Będziemy zajmować się rachunkiem zdań, a formuły tego rachunku będziemy zapisywać używając spójników $\wedge, \vee, \rightarrow$ oraz stałej $\perp$, a także zmiennych zdaniowych ze zbioru V .

Niech $\mathcal{A} = \langle A, \cap, \cup, \Rightarrow, \mathbf{0}, \mathbf{1} \rangle$ będzie algebrą Heytinga. Wartościowaniem zmiennych zdaniowych w algebrze $\mathcal{A}$ będziemy nazywać dowolną funkcję v przyporządkowującą zmiennym ze zbioru V elementy uniwersum algebry $\mathcal{A}$.

Mając wartościowanie zmiennych v definiujemy wartość (logiczną) $[[\varphi]]_v$ formuły φ przy wartościowaniu v przyjmując następujące równania rekurencyjne:

- 1) $[[p]]_v = v(p)$ dla dowolnej zmiennej $p \in V$,
- 2) $[[\varphi \wedge \psi]]_v = [[\varphi]]_v \cap [[\psi]]_v$,
- 3) $[[\varphi \vee \psi]]_v = [[\varphi]]_v \cup [[\psi]]_v$,
- 4) $[[\varphi \rightarrow \psi]]_v = [[\varphi]]_v \Rightarrow [[\psi]]_v$,
- 5) $[[\perp]]_v = \mathbf{0}$.

Formuła φ jest spełniona w algebrze $\mathcal{A}$ przy wartościowaniu v , jeżeli $[[\varphi]]_v = \mathbf{1}$.

Formuła φ jest spełniona w algebrze $\mathcal{A}$, jeżeli jest spełniona w tej algebrze przy wszystkich wartościowaniach. Fakt spełniania formuły φ w algebrze $\mathcal{A}$ zapisujemy wzorem $\mathcal{A} \models \varphi$.

Formuła φ jest (intuicjonistyczną) tautologią, jeżeli jest spełniona we wszystkich algebrach Heytinga, symbolicznie fakt ten będziemy wyrażać wzorem $\models \varphi$.

Formuła φ jest klasyczną tautologią, jeżeli jest spełniona we wszystkich algebrach Boole'a.

3 Intuicjonistyczna dedukcja naturalna w rachunku zdań

Będziemy posługiwać się językiem opisanym w rozdziale 1.1 i zdefiniujemy relację $\Gamma \vdash \varphi$, gdzie φ jest formułą wspomnianego języka, a Γ – zbiorem formuł tego języka. Intuicyjnie, zbiór Γ jest albo zbiorem aksjomatów, albo zbiorem przyjętych założeń, a definiowana relacja może być rozumiana jako stwierdzenia, że z aksjomatów (lub założeń) Γ potrafimy wywnioskować (wyprowadzić) zdanie φ .

W systemach dedukcji naturalnej zwykle nie ma istotnej różnicy między aksjomatami i założeniami, a tzw. twierdzenie o dedukcji jest właściwie częścią definicji systemu. Dowodzenie implikacji $\varphi \rightarrow \psi$ w takich systemach polega na uznaniu

poprzednika φ za dodatkowe założenie i wywnioskowanie z tego założenia i pozostałych, oraz z aksjomatów następnika ψ . Z doświadczenia wynika, że jest to bardzo wygodny sposób uzasadniania twierdzeń.

Relację $\vdash$ definiujemy jako najmniejszą relacją spełniającą następujące reguły:

$$\begin{aligned} & \overline{\Gamma, \varphi \vdash \varphi}, \\ & \frac{\Gamma \vdash \varphi, \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}, \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}, \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}, \\ & \frac{\Gamma, \varphi \vdash \sigma, \Gamma, \psi \vdash \sigma, \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \sigma}, \quad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}, \\ & \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}, \quad \frac{\Gamma \vdash \varphi, \Gamma \vdash \varphi \rightarrow \psi}{\Gamma \vdash \psi}, \\ & \frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}. \end{aligned}$$

Wymienione reguły rozumiemy jako stwierdzenia, jeżeli zachodzą relacje znajdujące się nad kreską, to zachodzi także relacja podana pod kreską.

Zauważmy też, że w tak sformułowanym systemie dedukcji naturalnej nie ma pojęcia dowodu. Drzewo wyprowadzenia relacji postaci $\Gamma \vdash \varphi$ jest metadowodem, czyli dowodem, że coś można udowodnić (bez powiedzenia, jak). Oczywiście, pojęcie dowodu można wprowadzić, ale w systemie dedukcji naturalnej jest nieco bardziej skomplikowane ze względu na konieczność operowania założeniami.

Na koniec zauważmy, że mamy możliwość przeprowadzania dowodów nie wprost. Pierwsza reguła dotycząca implikacji (reguła wprowadzania implikacji) w szczególnym przypadku $\psi = \perp$ przyjmuje postać

$$\frac{\Gamma, \varphi \vdash \perp}{\Gamma \vdash \neg \varphi}.$$

(Pamiętajmy, że formuła $\neg \varphi$ to dokładnie $\varphi \rightarrow \perp$). Jest to właściwie reguła dowodzenia negacji, stwierdza ona, że negację $\neg \varphi$ dowodzimy nie wprost, wyprowadzając sprzeczność z formuły φ .

Bardzo ważne jest to, że w przedstawionym systemie metodą nie wprost możemy dowodzić wyłącznie negacje. Zwykle również nieco inaczej tworzymy dowody nie wprost: Jeżeli chcemy dowieść φ , to wyprowadzamy sprzeczność z $\neg \varphi$. Posługujemy się więc następującą regułą:

$$\frac{\Gamma, \neg \varphi \vdash \perp}{\Gamma \vdash \varphi}. \quad (3)$$

Dołączenie do systemu dedukcji naturalnej powyższej reguły istotnie rozszerza zbiór możliwych do udowodnienia formuł. Rozważany system pozwala na dowiedzenie wszystkich tez intuicjonistycznego rachunku zdań, a po rozszerzeniu umożliwia także dowodzenie tez klasycznego rachunku zdań.

Zadanie 3.1 Pokaż, że $\vdash p \rightarrow \neg \neg p$. Spróbuj dowieść implikację odwrotną $\neg \neg p \rightarrow p$. Pokaż, że $\vdash \neg \neg p \rightarrow p$ w klasycznym rachunku zdań, gdy mamy prawo korzystać także z reguły (3).

4 Twierdzenia o pełności

Lemat 4.1 (o poprawności) *Niech $C \subseteq \mathcal{P}(\mathcal{P}(V))$ (patrz rozdział 1.2). Załóżmy, że $\Gamma \vdash \varphi$. Jeżeli zgodnie z semantyką Kripke’go wszystkie formuły $\gamma \in \Gamma$ są uważane za spełnione w kraju C ($C \Vdash \gamma$ dla wszystkich $\gamma \in \Gamma$), to także formuła φ jest uważana za spełnioną w kraju C (także $C \Vdash \varphi$).*

Dowód. Dość łatwy, przez indukcję wynikającą z definicji relacji $\vdash$. $\square$

Lemat 4.2 (o poprawności) *Weźmy algebrę Heytinga $\mathcal{A}$ i wartościowanie v w tej algebrze. Załóżmy, że $\Gamma \vdash \varphi$. Jeżeli wszystkie formuły $\gamma \in \Gamma$ są spełnione przy wartościowaniu v w algebrze $\mathcal{A}$ ($[[\gamma]]_v = \mathbf{1}$ dla wszystkich $\gamma \in \Gamma$), to także formuła φ jest spełnioną w $\mathcal{A}$ przy wartościowaniu v (także $[[\varphi]]_v = \mathbf{1}$).*

Dowód. Łatwy, przez indukcję wynikającą z definicji relacji $\vdash$. $\square$

Twierdzenie 4.3 (o pełności) *Przypuśćmy, że formuła φ jest uważana za spełnioną w każdym kraju, w którym uważane za spełnione są wszystkie formuły $\gamma \in \Gamma$. Wtedy $\Gamma \vdash \varphi$. Albo inaczej, jeżeli $C \Vdash \varphi$ dla dowolnego C takiego, że wszystkie $\gamma \in \Gamma$ są w C uważane za spełnione (zachodzi $C \Vdash \gamma$), to $\Gamma \vdash \varphi$. $\square$*

Twierdzenie 4.4 (o pełności) *Przypuśćmy, że formuła φ jest spełniona w każdej algebrze Heytinga, w której przy wszystkich wartościowaniach są spełnione wszystkie formuły $\gamma \in \Gamma$. Wtedy $\Gamma \vdash \varphi$. Albo inaczej, jeżeli $\mathcal{A} \models \varphi$ dla dowolnej algebry Heytinga $\mathcal{A}$, w której wszystkie $\gamma \in \Gamma$ są spełnione (zachodzi $\mathcal{A} \models \gamma$), to $\Gamma \vdash \varphi$.*

Dowód. Konstruujemy i wykorzystujemy w dowodzie tzw. algebrę Lindenbauma, opisaną w rozdziale 2.1. Jeżeli w algebrze Lindenbauma dla zbioru Γ spełniona jest formuła φ przy wartościowaniu $v(p) = [p]_{\sim}$, to na mocy definicji tej algebry, ze zbioru Γ można wyprowadzić φ . $\square$

Wniosek 4.5 *Dla dowolnej formuły φ równoważne są następujące warunki*

- 1) $\vdash \varphi$ (czyli φ daje się dowieść w rozważanym, intuicjonistycznym systemie dedukcji naturalnej),
- 2) $\Vdash \varphi$ (czyli φ jest tautologią według Kripke’go),
- 3) $\models \varphi$ (czyli tautologią według Heytinga). $\square$

5 Implikacyjny fragment rachunku zdań

5.1 Dowody w stylu Hilberta

Ciąg formuł $\varphi_1, \varphi_2, \dots, \varphi_n$ jest dowodem (w stylu Hilberta, zgodnie z definicją postulowaną i analizowaną przez Hilberta) formuły φ , jeżeli $\varphi_n = \varphi$ oraz dla wszystkich $i = 1, 2, \dots, n$

- 1) φ_i jest aksjomatem (logicznym lub pozalogicznym) lub też
- 2) φ_i jest wnioskiem z niektórych formuł φ_j dla $j < i$ (z przesłanek takiej postaci) otrzymanym za pomocą jednej z przyjętych reguł dowodzenia.

Oczywiście przyjęta definicja pojęcia dowodu jest nieprecyzyjna, wymaga jeszcze wyjaśnienia, jakie formuły uważamy za aksjomaty, i wskazania reguł dowodzenia, którymi mamy prawo się posługiwać.

Aksjomaty logiczne będziemy uważać za część definicji dowodu, muszą zostać wskazane (bez nich niczego nie dowiedzimy), ale w zasadzie nie będą ulegać zmianie. Aksjomaty pozallogiczne będziemy dobierać zależnie od potrzeb. Zapis $\Gamma \vdash_H \varphi$, gdzie Γ jest dowolnym zbiorem formuł, będzie oznaczać, że formuła φ ma dowód (czyli istnieje ciąg spełniający wyżej podane warunki) korzystający z określonych aksjomatów logicznych i ze zbioru aksjomatów pozallogicznych Γ .

5.2 Implikacyjny fragment intuicjonistycznego rachunku

Można go zdefiniować na dwa równoważne, niewiele różniące się sposoby. Albo jako te formuły rachunku zdań, które można zapisać używając jedynie implikacji (i zmiennych zdaniowych), i które można dowieść w systemie dedukcji naturalnej, albo jako te formuły, które można dowieść w systemie dedukcji naturalnej posługując się jedynie trzema regułami:

$$\frac{}{\Gamma, \varphi \vdash \varphi}, \quad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}, \quad \frac{\Gamma \vdash \varphi, \quad \Gamma \vdash \varphi \rightarrow \psi}{\Gamma \vdash \psi}.$$

Zauważmy, że

$$\vdash (\sigma \rightarrow \tau \rightarrow \rho) \rightarrow (\sigma \rightarrow \tau) \rightarrow (\sigma \rightarrow \rho) \quad \text{oraz} \quad \vdash \sigma \rightarrow \tau \rightarrow \sigma.$$

5.3 Implikacyjny fragment według Hilberta

Będziemy rozważać też system hilbertowski, w którym formuły zapisujemy używając (poza zmiennymi zdaniowymi) wyłącznie znaku implikacji $\rightarrow$. Aksjomatami logicznymi tego systemu będą wszystkie formuły dwóch, niżej wymienionych postaci:

$$(\sigma \rightarrow \tau \rightarrow \rho) \rightarrow (\sigma \rightarrow \tau) \rightarrow (\sigma \rightarrow \rho) \quad \text{oraz} \quad \sigma \rightarrow \tau \rightarrow \sigma.$$

Posługujemy się w nim jedną regułą dowodzenia, a mianowicie regułą odrywania

$$\frac{\varphi, \quad \varphi \rightarrow \psi}{\psi}.$$

Przykład 5.1 Weźmy formułę φ . Pokażemy, że w opisanym systemie można dowieść formułę $\varphi \rightarrow \varphi$, a więc pokażemy, że $\vdash_H \varphi \rightarrow \varphi$. Dowodem tej formuły jest następujący ciąg formuł

- 1) $(\varphi \rightarrow (\varphi \rightarrow \varphi) \rightarrow \varphi) \rightarrow (\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow \varphi \rightarrow \varphi$ (jest to pierwszy z aksjomatów pozallogicznych, wzięliśmy jego wersję, w której użyliśmy φ zamiast σ i ρ oraz $\varphi \rightarrow \varphi$ zamiast τ),
- 2) $\varphi \rightarrow (\varphi \rightarrow \varphi) \rightarrow \varphi$ (jest to drugi z aksjomatów pozallogicznych, użyliśmy φ zamiast σ oraz $\varphi \rightarrow \varphi$ zamiast τ),
- 3) $(\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow \varphi \rightarrow \varphi$ (jest to wniosek wynikający za pomocą reguły odrywania z dwóch poprzedzających stwierdzeń),
- 4) $\varphi \rightarrow (\varphi \rightarrow \varphi)$ (jest to drugi z aksjomatów pozallogicznych, użyliśmy φ zamiast σ oraz τ),

- 5) $\varphi \rightarrow \varphi$ (jest to wniosek otrzymany za pomocą reguły odrywania z dwóch ostatnich stwierdzeń).

Twierdzenie 5.2 (o dedukcji) *Dla dowolnych formuł φ i ψ , i zbioru γ , warunek $\Gamma, \varphi \vdash_H \psi$ zachodzi wtedy i tylko wtedy, gdy $\Gamma \vdash_H \varphi \rightarrow \psi$.*

Dowód. Mając dowód $\psi_1, \dots, \psi_n$ formuły ψ korzystający z aksjomatu φ tworzymy ciąg $\varphi \rightarrow \psi_1, \dots, \varphi \rightarrow \psi_n$ i pokazujemy, że dodając do niego odpowiednie formuły możemy uzupełnić go do dowodu formuły $\varphi \rightarrow \psi$. Implikacja odwrotna jest oczywista. Zauważmy jeszcze, że jako aksjomaty logiczne wzięliśmy formuły niezbędne w dowodzie twierdzenia o dedukcji. $\square$

Twierdzenie 5.3 *Dla dowolnej formuły zapisanej tylko z użyciem implikacji i dla dowolnego Γ , warunek $\Gamma \vdash \varphi$ jest równoważny z $\Gamma \vdash_H \varphi$.*

Dowód. Implikację „z lewej do prawej” dowodzimy przez indukcję wynikającą z definicji relacji $\vdash$. W najtrudniejszym momencie korzystamy z twierdzenia o dedukcji. Implikację odwrotną dowodzimy przez łatwą indukcję ze względu na długość dowodu. Musimy tylko sprawdzić, że aksjomaty logiczne można dowieść w systemie dedukcji naturalnej. $\square$

6 Rachunek zdań drugiego rzędu

6.1 Formuły

Formuły rachunku zdań II rzędu, jak zwykle, definiujemy przez indukcję przyjmując, że

- 1) zmienne zdaniowe są formułami rachunku zdań II rzędu,
- 2) stała $\perp$ jest formułą rachunku zdań II rzędu,
- 3) jeżeli φ i ψ są formułami rachunku zdań II rzędu, to $\varphi \wedge \psi$, $\varphi \vee \psi$ oraz $\varphi \rightarrow \psi$ też są formułami rachunku zdań II rzędu,
- 4) jeżeli φ jest formułą rachunku zdań II rzędu, a p jest zmienną zdaniową to $\forall p \varphi$ oraz $\exists p \varphi$ też są formułami rachunku zdań II rzędu.

6.2 Intuicje

W klasycznym rachunku zdań, w którym dodatkowo mamy prawo posługiwać się zdaniem sprzecznym $\perp$ i zdaniem „absolutnie prawdziwym” $\top$, rachunek zdań II rzędu definiuje się tak, aby zachodziły równoważności

$$\forall p \varphi \leftrightarrow \varphi[p := \top] \wedge \varphi[p := \perp] \quad \text{oraz} \quad \exists p \varphi \leftrightarrow \varphi[p := \top] \vee \varphi[p := \perp].$$

Albo mniej formalnie: zdanie $\forall p \varphi$ jest prawdziwe, jeżeli zdanie φ jest prawdziwe bez względu na treść lub wartość logiczną zdania p , a zdanie $\exists p \varphi$ jest prawdziwe, jeżeli w pewnych sytuacjach, czyli dla odpowiednio dobranych p o odpowiedniej wartości logicznej, zdanie φ jest prawdziwe.

6.3 Dedukcja naturalna dla języka II rzędu

System dedukcji naturalnej dla języka II rzędu dopuszcza korzystanie z wszystkich reguł wnioskowania wymienionych w rozdziale 3 i dodatkowo pozwala stosować następujące reguły:

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall p \varphi} \text{ o ile } p \notin FV(\Gamma), \quad \frac{\Gamma \vdash \forall p \varphi}{\Gamma \vdash \varphi[p := \sigma]},$$

$$\frac{\Gamma \vdash \varphi[p := \sigma]}{\Gamma \vdash \exists p \varphi}, \quad \frac{\Gamma \vdash \exists p \varphi, \quad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi} \text{ o ile } p \notin FV(\Gamma, \varphi).$$

W powyższych regułach, wzór $FV(\Gamma)$ oznacza zbiór zmiennych wolnych występujących w Γ , czyli sumę zbiorów zmiennych wolnych występujących w poszczególnych formułach z Γ .

6.4 Semantyka oparta o algebry Heytinga

Aby zdefiniować semantykę dla języka II rzędu potrzebne są zupełne algebry Heytinga. Algebry Heytinga to zbiory uporządkowane. Zupełne algebry Heytinga to zupełne zbiory uporządkowane, a więc takie, że każdy zbiór elementów tego zbioru, także nieskończony, ma kresy: dolny i górny.

Jest sporo zupełnych algebr Heytinga. Takimi są algebry skończone, algebra otwartych podzbiorów płaszczyzny, a także odcinek $[0, 1]$ ze zwykłym porządkiem.

Pojęcie wartościowania i wartości logicznej formuły II rzędu definiujemy podobnie jak definiowaliśmy odpowiedniki tych pojęć w przypadku rachunku rzędu I w rozdziale 2.5. Są jednak pewne różnice. Po pierwsze, wartościowania przyjmują wartości w zupełnych algebrach Heytinga. Po drugie, podane w rozdziale 2.5 warunki definiujące wartość logiczną muszą zostać uzupełnione o warunki pozwalające obliczać wartości formuł rozpoczynających się kwantyfikatorami, czyli o warunki:

$$6) [[\forall p \varphi]]_v = \text{kres dolny zbioru } \{[[\varphi]]_w : \forall q \neq p \ w(q) = v(q)\},$$

$$7) [[\exists p \varphi]]_v = \text{kres górny zbioru } \{[[\varphi]]_w : \forall q \neq p \ w(q) = v(q)\}.$$

Licząc zgodnie z tymi wzorami np. wartość formuły $\forall p \varphi$ przy wartościowaniu v , znajdujemy najpierw wartości logiczne $[[\varphi]]_w$ dla wszystkich wartościowań w , które zmiennym różnym od p przypisują te same wartości, co wartościowanie v , a następnie znajdujemy odpowiedni kres.

Jak zwykle, dość łatwo dowodzi się lemat o poprawności semantyki:

Lemat 6.1 *Niech $\mathcal{A}$ będzie ustaloną, zupełną algebrą Heytinga. Jeżeli $\Gamma = \{\psi_1, \psi_1, \dots, \psi_n\}$ oraz $\Gamma \vdash \varphi$, to dla wszystkich wartościowań v w algebrze $\mathcal{A}$ zachodzi nierówność*

$$[[\psi_1]]_v \cap [[\psi_2]]_v \cap \dots \cap [[\psi_n]]_v \leq [[\varphi]]_v. \quad \square$$

6.5 $\{\forall, \rightarrow\}$ -fragment rachunku zdań II rzędu

W $\{\forall, \rightarrow\}$ -fragmencie rachunku zdań II rzędu można zdefiniować wszystkie spójniki logiczne i kwantyfikator $\exists$. Przyjmijmy, że

$$1) \perp = \forall \alpha \alpha,$$

- 2) $\varphi \wedge \psi = \forall \alpha ((\varphi \rightarrow \psi \rightarrow \alpha) \rightarrow \alpha)$ o ile $\alpha \notin FV(\varphi) \cup FV(\psi)$,
- 3) $\varphi \vee \psi = \forall \alpha ((\varphi \rightarrow \alpha) \rightarrow (\psi \rightarrow \alpha) \rightarrow \alpha)$ o ile $\alpha \notin FV(\varphi) \cup FV(\psi)$,
- 4) $\exists \alpha \varphi = \forall \beta ((\forall \alpha (\varphi \rightarrow \beta)) \rightarrow \beta)$ o ile $\beta \notin FV(\varphi)$.

Zadanie 6.1 Następujące fakty wydają się prawdziwe, a więc spróbuj je dowieść:

- 1) Jeżeli w wyżej podanych równościach symbol $=$ zastąpimy przez $\leftrightarrow$, to otrzymamy formuły, które można dowieść w rozważanym rachunku zdań II rzędu.
- 2) Przyjmujemy wyżej podane definicje spójników i kwantyfikatorów. Dla każdej reguły opisującej naturalną dedukcję w rachunku zdań II rzędu, w $\{\forall, \rightarrow\}$ -fragmencie tego rachunku dowiedz, że przy takich definicjach, z prawdziwości przesłanek wynika prawdziwość wniosków (z prawdziwości stwierdzeń nad kreską wynika prawdziwość stwierdzeń pod kreską).

7 Prosty system typów

7.1 Podstawowe pojęcia i notacja

Zapis $M : \sigma$ będziemy uważać za stwierdzenie, że „term M jest typu σ ”. W takim kontekście M zwykle będzie termem rachunku λ , czasem nieco zmodyfikowanym, a σ – typem. Czasem zapis ten będzie rozumieć jako parę uporządkowaną złożoną z termu M i typu σ .

Typy będą napisami zbudowanymi ze zmiennych typowych, zbiór zmiennych typowych będziemy oznaczać symbolem $\mathbf{V}$, oraz z symbolu $\rightarrow$. Zbiór typów $\mathbf{T}$ będzie najmniejszym zbiorem zawierającym $\mathbf{V}$ i spełniającym warunek

jeżeli $\sigma, \tau \in \mathbf{T}$, to $(\sigma \rightarrow \tau) \in \mathbf{T}$.

Zapisując typy będziemy opuszczać niepotrzebne nawiasy. Przyjmujemy, że napis $\sigma_1 \rightarrow \sigma_2 \rightarrow \sigma_3$ oznacza typ $(\sigma_1 \rightarrow (\sigma_2 \rightarrow \sigma_3))$.

Kontekstem nazywamy skończony i jednoznaczny zbiór par postaci $x : \sigma$, gdzie x jest zmienną rachunku λ , a σ – typem. Kontekst Γ musi więc spełniać warunek

jeżeli $x : \sigma_1, x : \sigma_2 \in \Gamma$, to $\sigma_1 = \sigma_2$.

Konteksty są więc funkcjami, będziemy też w odniesieniu do kontekstów stosować notacje związane z funkcjami. Tak więc $\Gamma(x) = \sigma$ oznacza, że $x : \sigma \in \Gamma$, $dom(\Gamma)$ to dziedzina Γ , czyli zbiór zmiennych występujących w Γ , $\Gamma[dom(\Gamma)]$ to zbiór wartości przyjmowanych przez Γ , albo typów występujących w Γ . Zapis $\Gamma, x : \sigma$ oznacza $\Gamma \cup \{x : \sigma\}$.

7.2 Relacja typowania à la Curry

Zdefiniujemy teraz relację $\Gamma \vdash M : \sigma$, gdzie Γ jest kontekstem, M – termem rachunku λ , a σ – typem. Jest to najmniejsza relacja mająca następujące własności:

$$\frac{}{\Gamma, x : \sigma \vdash x : \sigma}, \quad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x M : \sigma \rightarrow \tau}, \quad \frac{\Gamma \vdash M : \sigma \rightarrow \tau, \quad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}.$$

W powyższej definicji termy powinny być rozumiane jako klasy abstrakcji relacji α -konwersji.

7.3 Najprostsze własności

Lemat 7.1 *Założmy, że $\Gamma \vdash M : \sigma$. Wtedy*

- 1) *jeżeli $\Gamma \subseteq \Gamma'$, to $\Gamma' \vdash M : \sigma$,*
- 2) *$FV(M) \subseteq \text{dom}(\Gamma)$,*
- 3) *jeżeli Γ' jest kontekstem Γ ograniczonym do zbioru $FV(M)$, to $\Gamma' \vdash M : \sigma$.*
□

Lemat 7.2 1) *Jeżeli $\Gamma \vdash M : \sigma$, to $\Gamma[\alpha := \tau] \vdash M : \sigma[\alpha := \tau]$ (α to zmienna typowa, chyba wiadomo, jak podstawiamy typ w innym typie za zmienną typową, podstawianie w Γ to podstawianie we wszystkich typach występujących w Γ).*

- 2) *Jeżeli $\Gamma, x : \tau \vdash M : \sigma$ i $\Gamma \vdash N : \tau$, to $\Gamma \vdash M[x := N] : \sigma$.* □

Chyba najważniejszy lemat stwierdza, że β -redukcja zachowuje typ termu:

Lemat 7.3 *Jeżeli $\Gamma \vdash M : \sigma$ i $M \rightarrow_{\beta} N$, to $\Gamma \vdash N : \sigma$.* □

7.4 Problem rekonstrukcji typu

Będziemy badać, czy dla danego termu M istnieją Γ i σ takie, że $\Gamma \vdash M : \sigma$. Prezentuję tutaj jedno z możliwych rozwiązań, pochodzące od Berengregta, inne, niż prezentowane na wykładzie.

Podstawieniem nazywamy funkcję $\theta : \mathbf{T} \rightarrow \mathbf{T}$ taką, że $\theta(\sigma \rightarrow \tau) = (\theta\sigma) \rightarrow (\theta\tau)$. Zwykle będziemy rozważać podstawienia, które poza skończonym zbiorem zmiennych typowych α spełniają równość $\theta(\alpha) = \alpha$.

Zdefiniujemy teraz (przez indukcję ze względu na M) zbiór $E(\Gamma, M, \sigma)$ dla kontekstu Γ , termu M takiego, że $FV(M) \subseteq \text{dom}(\Gamma)$, i typu σ . Będzie to zbiór równości typów, niekoniecznie prawdziwych, jednak takich, których odpowiednie spełnienie zagwarantuje prawdziwość relacji $\Gamma \vdash M : \sigma$. Przyjmujemy, że

- 1) $E(\Gamma, x, \sigma) = \{\Gamma(x) = \sigma\}$, gdzie x jest zmienną λ -rachunku,
- 2) $E(\Gamma, \lambda x M, \sigma) = E(\Gamma \cup \{x : \alpha\}, M, \alpha \rightarrow \beta) \cup \{\alpha \rightarrow \beta = \sigma\}$, gdzie α i β są „świeżymi” zmiennymi typowymi,
- 3) $E(\Gamma, MN, \sigma) = E(\Gamma, M, \alpha \rightarrow \sigma) \cup E(\Gamma, N, \alpha)$, gdzie α jest „świeżą” zmienną typową.

Podstawienie θ unifikuje zbiór równości X , jeżeli $\theta(\sigma) = \theta(\tau)$ (jeżeli termy $\theta(\sigma)$ i $\theta(\tau)$ są identyczne) dla wszystkich równości $\sigma = \tau \in X$. Fakt, że θ unifikuje X będziemy wyrażać wzorem postaci $\theta \models X$.

Jeżeli $\Gamma = \{x_1 : \sigma_1, \dots, x_n : \sigma_n\}$, to $\theta(\Gamma) = \{x_1 : \theta(\sigma_1), \dots, x_n : \theta(\sigma_n)\}$ (θ to podstawienie).

Lemat 7.4 *Jeżeli $\theta \models E(\Gamma, M, \sigma)$, to $\theta(\Gamma) \vdash M : \theta(\sigma)$.* □

Lemat 7.5 *Jeżeli $\theta(\Gamma) \vdash M : \theta(\sigma)$, to $\theta' \models E(\Gamma, M, \sigma)$ dla pewnego podstawienia θ' takiego, że $\theta(\alpha) = \theta'(\alpha)$ dla wszystkich zmiennych typowych α występujących w Γ i σ .* □

Wniosek 7.6 Niech M będzie dowolnym λ -termem ze zmiennymi wolnymi $x_1, \dots, x_n$, a $\alpha_1, \dots, \alpha_n$ i β będą zmiennymi typowymi. Wtedy

- 1) Jeżeli $\theta \models E(\{x_1 : \alpha_1, \dots, x_n : \alpha_n\}, M, \beta)$, to $\{x_1 : \theta(\alpha_1), \dots, x_n : \theta(\alpha_n)\} \vdash M : \theta(\beta)$.
- 2) Warunek $\Gamma \vdash M : \sigma$ zachodzi dla pewnych Γ i σ wtedy i tylko wtedy, gdy zbiór $E(\{x_1 : \alpha_1, \dots, x_n : \alpha_n\}, M, \beta)$ ma unifikator. $\square$

Lemat 7.7 Problem, czy M ma typ (w pewnym kontekście, jeżeli jest potrzebny), jest rozstrzygalny. $\square$

Dla termu M najogólniejszym typem (a właściwie najgólniejszą parą, chyba że M nie ma zmiennych wolnych), nazywamy parę Γ i σ taką, że

- 1) $\Gamma \vdash M : \sigma$,
- 2) jeżeli $\Gamma' \vdash M : \sigma'$, to $\theta(\Gamma) \subseteq \Gamma'$ oraz $\theta(\sigma) = \sigma'$ dla pewnego podstawienia θ .

Lemat 7.8 Jeżeli term M ma typ (być może w pewnym kontekście), to M ma najogólniejszy typ.

Dowód. Konstruując najogólniejszy typ postępujemy tak, jak we wniosku 7.6: ale teraz bierzemy najogólniejszy unifikator zbioru $E(\{x_1 : \alpha_1, \dots, x_n : \alpha_n\}, M, \beta)$. $\square$

Do zagadnienia rekonstrukcji typu można też podejść inaczej, dowodząc lematy takie, jak poniższy, stanowiące podstawę algorytmu rekurencyjnego.

Lemat 7.9 Przypuśćmy, że $\Gamma_M \vdash M : \sigma_M$ oraz $\Gamma_N \vdash N : \sigma_N$. Przyjmijmy, że $\Gamma_M = \{x_1 : \alpha_{1,M}, \dots, x_n : \alpha_{n,M}\}$, podobnie Γ_N , oraz $FV(M) \cap FV(N) = \{x_1, \dots, x_k\}$. Wtedy term MN ma typ wtedy i tylko wtedy, gdy można zunifikować układ równości

$$\alpha_{1,M} = \alpha_{1,N}, \dots, \alpha_{k,M} = \alpha_{k,N}, \sigma_M = \sigma_N \rightarrow \beta.$$

Jeżeli θ jest unifikatorem tego układu, to

$$\theta(\Gamma_M) \cup \theta(\Gamma_N) \vdash MN : \theta(\beta). \quad \square$$

7.5 Relacja typowania à la Church

Zdefiniujemy teraz relację $\Gamma \vdash M : \sigma$, gdzie Γ jest kontekstem, σ – typem, a M termem rachunku λ , ale z pewnymi dopiskami.

Musi więc najpierw zmodyfikować pojęcie termu: w zwykłej definicji λ -termu warunek dotyczący abstrakcji zastępujemy następującym:

jeżeli M jest termem, x - zmienną, a $\sigma \in \mathbf{T}$, to $\lambda x : \sigma M$ też jest termem.

Jest to najmniejsza relacja mająca następujące własności:

$$\frac{}{\Gamma, x : \sigma \vdash x : \sigma}, \quad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x : \sigma M : \sigma \rightarrow \tau}, \quad \frac{\Gamma \vdash M : \sigma \rightarrow \tau, \quad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}.$$

W powyższej definicji termy też powinny być rozumiane jako klasy abstrakcji relacji α -konwersji.

Oba systemy typów mają podobne własności:

Lemat 7.10 1) Jeżeli $\Gamma \vdash_{Church} M : \sigma$, to $\Gamma \vdash_{Curry} |M| : \sigma$ ($|M|$ to term M pozbawiony adnotacji o typach wymaganych w systemie à la Church).

2) Jeżeli $\Gamma \vdash_{Curry} M : \sigma$, to $\Gamma \vdash_{Church} M' : \sigma$ dla pewnego termu M' z adnotacjami, takiego że $|M'| = M$. $\square$

Oba systemy typów różni natępujący lemat:

Lemat 7.11 Jeżeli $\Gamma \vdash_{Church} M : \sigma$ i $\Gamma \vdash_{Church} M : \tau$, to $\sigma = \tau$. $\square$

7.6 Izomorfizm Currego-Howarda

Lemat 7.12 1) Jeżeli $\{x_1 : \tau_1, \dots, x_n : \tau_n\} \vdash M : \sigma$, to $\{\tau_1, \dots, \tau_n\} \vdash \sigma$ (w systemie dedukcji naturalnej).

2) Jeżeli $\{\tau_1, \dots, \tau_n\} \vdash \sigma$ (w systemie dedukcji naturalnej), to istnieją zmienne $x_1, \dots, x_n$ i term M takie, że $\{x_1 : \tau_1, \dots, x_n : \tau_n\} \vdash M : \sigma$. $\square$

8 Polimorficzny rachunek lambda¹

8.1 Typy

Niech $\mathbf{V}$ będzie zbiorem zmiennych typowych. Jak zwykle, przez indukcję, zdefiniujemy zbiór typów $\mathbf{T}$: jest to najmniejszy ze zbiorów spełniających następujące warunki:

- 1) $\mathbf{V} \subseteq \mathbf{T}$,
- 2) jeżeli $\tau, \sigma \in \mathbf{T}$, to także $\tau \rightarrow \sigma \in \mathbf{T}$,
- 3) jeżeli $\alpha \in \mathbf{V}$ i $\tau \in \mathbf{T}$, to także $\forall \alpha \tau \in \mathbf{T}$.

Nietrudno zauważyć, że typy polimorficzne można uważać za formuły rachunku zdań II rzędu zapisane za pomocą spójnika $\rightarrow$ i kwantyfikatora $\forall$. Oczywiście, zapisując typy musimy też używać nawiasów. Przyjmujemy zasady opuszczania nawiasów analogiczne do stosowanych w rachunku lambda. Przyjmujemy też zasadę, że zmienne typowe będą oznaczane początkowymi literami alfabetu greckiego.

8.2 Termy polimorficznego rachunku lambda à la Church

Termy polimorficznego rachunku λ są tworzone ze zmiennych ze zbioru V , zmiennych typowych należących do $\mathbf{V}$ i dwóch operatorów lambda: zwykłego λ i polimorficznego λ , ten ostatni często jest zapisywany jako Λ .

Zbiór wszystkich termów (à la Church) polimorficznego rachunku lambda $\mathcal{T}$ jest najmniejszym zbiorem spełniającym następujące warunki:

- 1) $V \subseteq \mathcal{T}$,
- 2) jeżeli $M, N \in \mathcal{T}$, to $MN \in \mathcal{T}$ (zwykła aplikacja),
- 3) jeżeli $M \in \mathcal{T}$, $x \in V$ i $\tau \in \mathbf{T}$, to $\lambda x : \tau M \in \mathcal{T}$ (zwykła abstrakcja),
- 4) jeżeli $M \in \mathcal{T}$ i $\tau \in \mathbf{T}$, to $M\tau \in \mathcal{T}$ (aplikacja typu (?)),

¹Według: Sørensen, Urzyczyn, *Curry-Howard Isomorphism*

5) jeżeli $M \in \mathcal{T}$ i $\alpha \in \mathbf{V}$, to $\lambda\alpha M \in \mathcal{T}$ (polimorficzna abstrakcja).

Czytanie długich termów z adnotacjami bywa uciążliwe. Wtedy czytanie może ułatwić inny zapis, postaci $\lambda x^\tau M$, wyrażający to samo, co $\lambda x : \tau M$.

W polimorficznym systemie typów à la Curry warunek 3) przyjmuje zwykłą postać

3) jeżeli $M \in \mathcal{T}$ i $x \in V$, to $\lambda x M \in \mathcal{T}$ (zwykła abstrakcja),

8.3 Odrobina intuicji

Będziemy analizować procedurę sortowania S . Procedura ta wymaga danych (właściwie jednej danej), przyjmijmy, że danymi są ciągi, czyli, dla ustalenia uwagi, elementy typu postaci $Nat \rightarrow X$. Taka procedura pozwala na sortowanie danych typu X . Jeżeli zostanie dobrze napisana, to powinna pozwalać na sortowanie danych różnych typów (dla różnych typów X). Można na przykład napisać procedurę sortowania, która oprócz zwykłych danych wymaga procedury P porównującej dane, zapewne typu $X \rightarrow X \rightarrow Bool$. Wobec tego procedura S powinna być typu

$$(X \rightarrow X \rightarrow Bool) \rightarrow (Nat \rightarrow X) \rightarrow Nat \rightarrow X.$$

Jeżeli jest rzeczywiście dobrze napisana i może być stosowana dla danych różnych typów X , to możemy przypisać jej typ polimorficzny

$$\forall\alpha ((\alpha \rightarrow \alpha \rightarrow Bool) \rightarrow (Nat \rightarrow \alpha) \rightarrow Nat \rightarrow \alpha),$$

dodając jednocześnie do jej treści stosowną informację o polimorfizmie $\forall\alpha S$. Jeżeli teraz chcemy ją zastosować w konkretnym przypadku, na przykład do sortowania ciągu liczb typu Nat , to powinniśmy użyć procedury $(\forall\alpha S) Nat$, czyli właściwie procedury S z dodatkową informacją, że powinna być wykorzystana do sortowania danych typu Nat . Tak więc procedura $(\forall\alpha S) Nat$ powinna być typu

$$(Nat \rightarrow Nat \rightarrow Bool) \rightarrow (Nat \rightarrow Nat) \rightarrow Nat \rightarrow Nat,$$

wymagać procedury typu $Nat \rightarrow Nat \rightarrow Bool$ porównującej dane i ciągu typu $Nat \rightarrow Nat$.

8.4 Polimorficzny system typów $\lambda 2$, czyli system F

Aby zdefiniować polimorficzny system typów, pamiętając, że posługujemy się rozszerzonym pojęciem termu, reguły prostego systemu typów (à la Church):

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}, \quad \frac{\Gamma \vdash M : \sigma \rightarrow \tau, \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}, \quad \frac{\Gamma, x : \tau \vdash M : \sigma}{\Gamma \vdash \lambda x : \tau M : \tau \rightarrow \sigma}$$

uzupełniamy o dwie reguły:

$$\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \lambda\alpha M : \forall\alpha \sigma} \quad \text{o ile} \quad \alpha \notin FV(\Gamma), \quad \frac{\Gamma \vdash M : \forall\alpha \sigma}{\Gamma \vdash M\tau : \sigma[\alpha := \tau]}.$$

W polimorficznym systemie typów à la Curry posługujemy się zwykłym pojęciem λ -termu i regułami typowania, wśród których zamiast wyżej podanych reguł dotyczących polimorfizmu znajdują się dwie następujące:

$$\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash M : \forall\alpha \sigma} \quad \text{o ile} \quad \alpha \notin FV(\Gamma), \quad \frac{\Gamma \vdash M : \forall\alpha \sigma}{\Gamma \vdash M : \sigma[\alpha := \tau]}.$$

8.5 Kilka uwag i β -redukcja

Zadanie 8.1 Pokaż, że

- 1) $\vdash \lambda\beta (\lambda x^{\forall\alpha (\alpha \rightarrow \alpha)}. x(\beta \rightarrow \beta)(x\beta) : \forall\beta ((\forall\alpha (\alpha \rightarrow \alpha)) \rightarrow \beta \rightarrow \beta)$
- 2) $\vdash \lambda\alpha. \lambda f^{\alpha \rightarrow \alpha} \lambda x^\alpha. f(fx) : \forall\alpha ((\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)),$
- 3) $\vdash \lambda f^{\forall\alpha (\alpha \rightarrow \beta \rightarrow \alpha)} \lambda\alpha \lambda x^\alpha. f(\beta \rightarrow \alpha)(f\alpha x) :$
 $(\forall\alpha (\alpha \rightarrow \beta \rightarrow \alpha)) \rightarrow \forall\alpha (\alpha \rightarrow \beta \rightarrow \beta \rightarrow \alpha)$

Twierdzenie 8.1 (Izomorfizm Curre’go-Howarda)

- 1) *Jeżeli $\Gamma \vdash M : \varphi$ w polimorficznym systemie typów $\lambda 2$, to $\Gamma[\text{dom}(\Gamma)] \vdash \varphi$ w (intuicjonistycznym) rachunku zdań II rzędu.*
- 2) *Jeżeli w $\{\forall, \rightarrow\}$ -fragmencie intuicjonistycznego rachunku zdań II rzędu zachodzi $\Delta \vdash \varphi$, to w polimorficznym systemie typów $\lambda 2$ mamy $\Gamma \vdash M : \varphi$ dla pewnych Γ i $M \in \mathcal{T}$. $\square$*

Twierdzenie 8.2 *Problem dowodliwości w intuicjonistycznym rachunku zdań II rzędu jest nierozstrzygalny. $\square$*

W związku ze zmianą pojęcia λ -termu musi ulec zmianie pojęcie β -redukcji. Ogólna postać definicji tego pojęcia pozostaje bez zmian. Mamy jednak dwa rodzaje aplikacji i tym samym dwa rodzaje redeksów. Oba rodzaje redukujemy podobnie:

- 1) $(\lambda x : \tau M)N \rightarrow_\beta M[x := N]$ dla $N \in \mathcal{T}$ i $x \in V$,
- 2) $(\lambda\alpha M)\tau \rightarrow_\beta M[\alpha := \tau]$ dla $\tau \in \mathbf{T}$ i $\alpha \in \mathbf{V}$.

Mam nadzieję, że definicje obu rodzajów podstawień występujących w podanych wzorach są dostatecznie jasne.

8.6 Termy typu $\varphi \wedge \psi$

Przyjmijmy następujące definicje:

- 1) $\langle M, N \rangle = \lambda\alpha \lambda z^{\varphi \rightarrow \psi \rightarrow \alpha}. zPQ,$
- 2) $\pi_1(M^{\varphi \wedge \psi}) = M\varphi(\lambda x^\varphi \lambda y^\psi. x),$
- 3) $\pi_2(M^{\varphi \wedge \psi}) = M\psi(\lambda x^\varphi \lambda y^\psi. y).$

Wtedy zachodzą następujące reguły typowania odpowiadające regułom naturalnej dedukcji:

$$\frac{\Gamma \vdash M\varphi, \Gamma \vdash N\psi}{\Gamma \vdash \langle M, N \rangle : \varphi \wedge \psi}, \quad \frac{\Gamma \vdash M : \varphi \wedge \psi}{\Gamma \vdash \pi_1(M) : \varphi}, \quad \frac{\Gamma \vdash M : \varphi \wedge \psi}{\Gamma \vdash \pi_2(M) : \psi}.$$

8.7 Termy typu $\varphi \vee \psi$

Przyjmijmy następujące definicje:

- 1) $in_1(M^\varphi) = \lambda\alpha \lambda u^{\varphi \rightarrow \alpha} \lambda v^{\psi \rightarrow \alpha}. uM,$
- 2) $in_2(M^\psi) = \lambda\alpha \lambda u^{\varphi \rightarrow \alpha} \lambda v^{\psi \rightarrow \alpha}. vM,$
- 3) $case(L^{\varphi \vee \psi}; x^\varphi.M^\rho; y^\psi.N^\rho) = L\rho(\lambda x^\varphi.M)(\lambda x^\psi.N).$

Wtedy zachodzą następujące reguły typowania odpowiadające regułom naturalnej dedukcji:

$$\frac{\Gamma, \varphi \vdash M : \sigma, \quad \Gamma, \psi \vdash N : \sigma, \quad \Gamma \vdash L : \varphi \vee \psi}{\Gamma \vdash case(L; x.M; y.N) : \sigma}, \quad \frac{\Gamma \vdash M : \varphi}{\Gamma \vdash in_1(M) : \varphi \vee \psi}, \quad \frac{\Gamma \vdash M : \psi}{\Gamma \vdash in_2(M) : \varphi \vee \psi},$$

8.8 Typy Bool i Nat

W systemie **F** można implementować typ **Bool** w następujący sposób:

- 1) **Bool** = $\forall\alpha(\alpha \rightarrow \alpha \rightarrow \alpha),$
- 2) **true** = $\lambda\alpha \lambda x^\alpha \lambda y^\alpha x,$
- 3) **false** = $\lambda\alpha \lambda x^\alpha \lambda y^\alpha y.$

A teraz implementacja typu odpowiadającego liczbom naturalnym:

- 1) **Nat** = $\forall\alpha((\alpha \rightarrow \alpha) \rightarrow \alpha \rightarrow \alpha),$
- 2) $c_n = \lambda\alpha \lambda f^{\alpha \rightarrow \alpha} \lambda x^\alpha f^n(x)$ (polimorficzne literały Churcha),
- 3) **succ** = $\lambda n^{\mathbf{Nat}} \lambda\alpha \lambda f^{\alpha \rightarrow \alpha} \lambda x^\alpha f(n\alpha f x).$

Lemat 8.3 Dla danego typu σ definiujemy term $\mathbf{r}_\sigma$ typu $\sigma \rightarrow (\sigma \rightarrow \mathbf{Nat} \rightarrow \sigma) \rightarrow \mathbf{Nat} \rightarrow \sigma$ jako

$$\lambda y^\sigma \lambda f^{\sigma \rightarrow \mathbf{Nat} \rightarrow \sigma} \lambda n^{\mathbf{Nat}} \pi_1(n(\sigma \wedge \mathbf{Nat})(\lambda v^{\sigma \wedge \mathbf{Nat}} \langle f(\pi_1(v))(\pi_2(v)), \mathbf{succ}(\pi_2(v)) \rangle \langle y, c_0 \rangle)).$$

Ten term spełnia dwie następujące równości:

$$\mathbf{r}_\sigma M N c_0 =_\beta M \quad \text{oraz} \quad \mathbf{r}_\sigma M N (\mathbf{succ} n) =_\beta N (\mathbf{r}_\sigma M N n). \quad \square$$

Zadanie 8.2 Pokaż, że term $\lambda zy. y(z\mathbf{I})(z\mathbf{K})(\lambda x x)$ nie ma typu w systemie **F**.

Twierdzenie 8.4 Problem rekonstrukcji typu w systemie **F** jest nierozstrzygalny.

□

9 Silna normalizacja dla prostego systemu typów

9.1 Potrzebne definicje

- 1) $SN = \{M \in \Lambda : M \text{ jest silnie normalizowalny}\}$
- 2) $A \Rightarrow B = \{F \in \Lambda : \forall X \in A \ FX \in B\}$, gdzie $A, B \subseteq \Lambda$
- 3) $[[\alpha]] = SN$ oraz $[[\sigma \rightarrow \tau]] = [[\sigma]] \Rightarrow [[\tau]]$ dla zmiennych typowych α i typów prostych $\sigma \rightarrow \tau$
- 4) Zbiór $X \subseteq SN$ jest nasycony, jeżeli
 - (a) $xM_1 \dots M_n \in X$ dla $n \geq 0$, $M_1, \dots, M_n \in SN$ i dowolnej zmiennej x ,
 - (b) jeżeli $M_1[x := M_0]M_2 \dots M_n \in X$, to $(\lambda x M_0)M_1M_2 \dots M_n \in X$, gdzie $n \geq 1$ i $M_1, \dots, M_n \in SN$
- 5) $\mathbf{S} = \{X \subseteq \Lambda : X \text{ jest nasycony}\}$

Lemat 9.1 $SN \in \mathbf{S}$.

Lemat 9.2 Jeżeli $A, B \in \mathbf{S}$, to $A \Rightarrow B \in \mathbf{S}$.

Wniosek 9.3 Dla dowolnego typu prostego σ mamy $[[\sigma]] \in \mathbf{S}$.

- 6) wartościowaniem nazywamy funkcję $\rho : V \rightarrow \Lambda$
- 7)

$$\rho(x := N)(y) = \begin{cases} N & \text{jeżeli } y = x \\ \rho(y) & \text{w przeciwnym przypadku} \end{cases}$$

- 8) $[[M]]_\rho = M[x_1 := \rho(x_1), \dots, x_n := \rho(x_n)]$, gdzie ρ jest wartościowaniem i $FV(M) = \{x_1, \dots, x_n\}$.
- 9) $\rho \models M : \sigma$ iff $[[M]]_\rho \in [[\sigma]]$,
- 10) $\rho \models \Gamma$ iff $\rho(x) \in [[\sigma]]$ dla wszystkich $x : \sigma \in \Gamma$,
- 11) $\Gamma \models M : \sigma$ iff $\forall \rho \ \rho \models \Gamma \Rightarrow \rho \models M : \sigma$,

Lemat 9.4 Jeżeli $\Gamma \vdash M : \sigma$, to $\Gamma \models M : \sigma$.

Twierdzenie 9.5 Jeżeli $\Gamma \vdash M : \sigma$, to $M \in SN$.

Dowód. Załóżmy, że $\Gamma \vdash M : \sigma$. Z poprzedniego lematu $\Gamma \models M : \sigma$. Weźmy ρ takie, że $\rho(x) = x$ przynajmniej dla x takich, że $x : \tau \in \Gamma$. $x \in [[\tau]]$, ponieważ $[[\tau]] \in \mathbf{S}$. Wobec tego, $\rho \models \Gamma$ i mamy $M = [[M]]_\rho \in [[\sigma]] \subseteq SN$. $\square$