Logika dla informatyków

Jerzy Tiuryn Jerzy Tyszkiewicz Paweł Urzyczyn

Październik 2006

Wnioskowanie o prawdziwości rozmaitych stwierdzeń jest powszednim zajęciem matematyków i nie tylko matematyków. Dlatego filozofowie i matematycy od dawna zajmowali się systematyzacją metod wnioskowania i kryteriów ich poprawności. Oczywiście ostatecznym kryterium poprawności rozumowania pozostaje zawsze zdrowy rozsądek i przekonanie o słuszności wywodu. Logika, która narodziła się jako nauka o rozumowaniu, jest jednak ważnym i potrzebnym narzędziem, które to przekonanie ułatwia.

Szczególną rolę wśród rozmaitych działów logiki zajmuje logika matematyczna, poświęcona opisowi i analizie języka matematyki oraz poprawności wnioskowań matematycznych. Jest to dyscyplina w pewnym sensie paradoksalna: będąc sama częścią matematyki, traktuje matematykę jako swój przedmiot zainteresowania. Dla uniknięcia „błędnego koła" musimy więc tutaj zauważyć, że logika formalna nie opisuje rzeczywistych wywodów matematyka, ale ich uproszczone modele, które bez zastrzeżeń można uważać za zwykłe obiekty matematyczne. Mimo tego ograniczenia, logika matematyczna dostarcza niezwykle ważnych wniosków o charakterze filozoficznym i metamatematycznym.

Logika formalna była kiedyś ezoteryczną nauką z pogranicza filozofii i matematyki, potem stała się pełnoprawnym działem czystej matematyki. Jeszcze później, wraz z narodzinami informatyki, zaczęła być coraz bardziej postrzegana jako dziedzina matematyki stosowanej, a zwłaszcza podstaw informatyki.

Logika matematyczna stosowana jest dziś szeroko w informatyce. Semantyka i weryfikacja programów, teoria złożoności i teoria automatów, programowanie funkcyjne i programowanie w logice — to tylko niektóre z działów informatyki, w których metody logiki formalnej stały się standardowym narzędziem zarówno badacza jak i praktyka.

1 Rachunek zdań

Jak powiedzieliśmy wyżej, logika matematyczna zajmuje się badaniem rozmaitych systemów formalnych, modelujących rzeczywiste sposoby wnioskowania matematycznego. Do najprostszych takich systemów należą różne warianty *logiki zdaniowej* zwanej też *rachunkiem zdań*. Język rachunku zdań jest bardzo prosty. Nie ma w nim wyrażeń stwierdzających jakiś stan rzeczy, zajście jakichś faktów, czy też wyrażeń orzekających o własnościach obiektów. Przedmiotem naszego zainteresowania są tu tylko możliwe zależności pomiędzy stwierdzeniami (zdaniami orzekającymi), oraz to w jaki sposób prawdziwość zdań złożonych zależy od prawdzi-

wości ich składowych. Sens samych składowych pozostaje tu całkowicie dowolny i nieistotny. Dlatego w rachunku zdań odpowiadają im po prostu *zmienne zdaniowe*. Zdania złożone budujemy ze zmiennych za pomocą *spójników logicznych* takich jak *alternatywa* $\vee$, *koniunkcja* $\wedge$, *negacja* $\neg$, czy *implikacja* $\rightarrow$. Wygodne są też *stałe logiczne* $\bot$ (fałsz) i $\top$ (prawda), które można uważać za zeroargumentowe spójniki logiczne. Dlatego nasza pierwsza definicja jest taka:

Definicja 1.1 Ustalamy pewien przeliczalnie nieskończony zbiór ZZ symboli, które będziemy nazywać *zmiennymi zdaniowymi* i zwykle oznaczać literami p, q, itp. Pojęcie *formuły zdaniowej* definiujemy przez indukcję:

- Zmienne zdaniowe oraz $\bot$ i $\top$ są formułami zdaniowymi;
- Jeśli napis φ jest formułą zdaniową, to także napis $\neg\varphi$ jest formułą zdaniową;
- Jeśli napisy φ i ψ są formułami zdaniowymi to napisy $(\varphi \rightarrow \psi)$, $(\varphi \vee \psi)$ i $(\varphi \wedge \psi)$ też są formułami zdaniowymi.

Inaczej mówiąc, formuły zdaniowe to elementy najmniejszego zbioru napisów $\mathcal{F}_Z$, zawierającego $\mathrm{ZZ} \cup \{\bot, \top\}$ i takiego, że dla dowolnych $\varphi, \psi \in \mathcal{F}_Z$ także $\neg\varphi, (\varphi \rightarrow \psi), (\varphi \vee \psi), (\varphi \wedge \psi)$ należą do $\mathcal{F}_Z$.

Konwencje notacyjne: Dla pełnej jednoznaczności składni nasze formuły są w pełni nawiasowane. W praktyce wiele nawiasów pomijamy, stosując przy tym następujące priorytety:

1. Negacja;
2. Koniunkcja i alternatywa;
3. Implikacja.

Zatem na przykład wyrażenie $\neg\varphi \vee \psi \rightarrow \vartheta$ oznacza $((\neg\varphi \vee \psi) \rightarrow \vartheta)$, ale napis $\varphi \vee \psi \wedge \vartheta$ jest niepoprawny.

1.1 Znaczenie formuł

W *logice klasycznej* interpretacją formuły jest wartość logiczna tj. „prawda” (1) lub „fałsz” (0). Aby określić wartość formuły zdaniowej trzeba jednak najpierw ustalić wartości zmiennych.

Definicja 1.2 Przez *wartościowanie zdaniowe* rozumiemy dowolną funkcję ϱ, która zmiennym zdaniowym przypisuje wartości logiczne 0 lub 1. *Wartość formuły* zdaniowej φ przy wartościowaniu ϱ oznaczamy przez $[\![\varphi]\!]_\varrho$ i określamy przez indukcję:

- $[\![\bot]\!]_\varrho = 0$ oraz $[\![\top]\!]_\varrho = 1$;
- $[\![p]\!]_\varrho = \varrho(p)$, gdy p jest symbolem zdaniowym;

- $[\![\neg\varphi]\!]_\varrho = 1 - [\![\varphi]\!]_\varrho$;
- $[\![\varphi \vee \psi]\!]_\varrho = \max\{[\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho\}$;
- $[\![\varphi \wedge \psi]\!]_\varrho = \min\{[\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho\}$;
- $[\![\varphi \to \psi]\!]_\varrho = 0$, gdy $[\![\varphi]\!]_\varrho = 1$ i $[\![\psi]\!]_\varrho = 0$;
- $[\![\varphi \to \psi]\!]_\varrho = 1$, w przeciwnym przypadku.

Łatwo można zauważyć, że $[\![\varphi \to \psi]\!]_\varrho = \max\{[\![\psi]\!]_\varrho, 1 - [\![\varphi]\!]_\varrho\}$, czyli $[\![\varphi \to \psi]\!]_\varrho = [\![\neg\varphi \vee \psi]\!]_\varrho$, dla dowolnego ϱ. A zatem zamiast formuły $\varphi \to \psi$ moglibyśmy z równym powodzeniem używać wyrażenia $\neg\varphi \vee \psi$, lub też odwrotnie: zamiast alternatywy $\varphi \vee \psi$ pisać $\neg\varphi \to \psi$. Nasz wybór spójników nie jest więc „najoszczędniejszy", w istocie w logice klasycznej wystarczy używać np. implikacji i fałszu (Ćwiczenie 6). Czasem i my będziemy korzystać z tego wygodnego uproszczenia, przyjmując, że „oficjalnymi" spójnikami są tylko implikacja i fałsz, a pozostałe to skróty notacyjne, tj. że napisy

$\neg\varphi$	oznaczają odpowiednio	$\varphi \to \bot$;
$\top$		$\neg\bot$;
$\varphi \vee \psi$		$\neg\varphi \to \psi$;
$\varphi \wedge \psi$		$\neg(\varphi \to \neg\psi)$.

Będziemy też czasem pisać $\varphi \leftrightarrow \psi$ zamiast $(\varphi \to \psi) \wedge (\psi \to \varphi)$. Zauważmy, że $[\![\varphi \leftrightarrow \psi]\!]_\varrho = 1$ wtedy i tylko wtedy, gdy $[\![\varphi \to \psi]\!]_\varrho = [\![\psi \to \varphi]\!]_\varrho$.

Często stosowanym skrótem jest notacja $\bigvee_{i\in I} \varphi_i$ oznaczająca alternatywę wszystkich formuł φ_i, gdzie i przebiega skończony zbiór I. Analogicznie stosuje się zapis $\bigwedge_{i\in I} \varphi_i$.

Notacja i terminologia: Jeśli $[\![\varphi]\!]_\varrho = 1$ to piszemy też $\varrho \models \varphi$ lub $\models \varphi[\varrho]$ i mówimy, że φ jest *spełniona* przez wartościowanie ϱ. Jeśli Γ jest zbiorem formuł zdaniowych, oraz $\varrho \models \gamma$ dla wszystkich $\gamma \in \Gamma$, to piszemy $\varrho \models \Gamma$. Wreszcie $\Gamma \models \varphi$ oznacza, że każde wartościowanie spełniające wszystkie formuły z Γ spełnia także formułę φ. Mówimy wtedy, że φ jest *semantyczną konsekwencją* zbioru Γ. Jeśli $\Gamma = \emptyset$ to zamiast $\Gamma \models \varphi$ piszemy po prostu $\models \varphi$. Oznacza to, że formuła φ jest spełniona przez każde wartościowanie. Na koniec powiedzmy jeszcze, że formułami *równoważnymi* nazywamy takie formuły φ i ψ, których wartości przy każdym wartościowaniu są takie same (tj. takie, że równoważność $\varphi \leftrightarrow \psi$ jest tautologią — patrz niżej).

Definicja 1.3 Formuła φ jest *spełnialna*, gdy $\varrho \models \varphi$ zachodzi dla pewnego wartościowania ρ. Jeśli zaś $\models \varphi$ to mówimy, że φ jest *tautologią* (klasycznego) rachunku zdań. Oczywiście $\neg\varphi$ jest spełnialna wtedy i tylko wtedy, gdy φ nie jest tautologią.

1.2 Tautologie rachunku zdań

Niech S będzie funkcją przypisujacą symbolom zdaniowym pewne formuły. Jeśli φ jest formułą zdaniową, to przez $S(\varphi)$ oznaczymy formułę otrzymaną z φ przez jednoczesną zamianę każdego

wystąpienia zmiennej zdaniowej p na formułę $S(p)$. Mówimy, że formuła $S(\varphi)$ jest *instancją* schematu zdaniowego φ. Używamy oznaczenia $S(\Gamma) = \{S(\psi) \mid \psi \in \Gamma\}$.

Fakt 1.4 *Jeżeli Γ jest zbiorem formuł rachunku zdań i $\Gamma \models \varphi$, to także $S(\Gamma) \models S(\varphi)$. W szczególności, jeśli φ jest tautologią to $S(\varphi)$ jest też tautologią.*

Dowód: Ćwiczenie. ∎

Przykład 1.5 Następujące formuły (i wszystkie ich instancje) są tautologiami rachunku zdań:

1. $\bot \to p$;
2. $p \to (q \to p)$;
3. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$;
4. $((p \to q) \to p) \to p$;
5. $p \vee \neg p$;
6. $p \to \neg\neg p$ oraz $\neg\neg p \to p$;
7. $(p \to q) \to (\neg q \to \neg p)$ oraz $(\neg q \to \neg p) \to (p \to q)$;
8. $p \to (p \vee q)$, $q \to (p \vee q)$ oraz $(p \to r) \to ((q \to r) \to (p \vee q \to r))$;
9. $(p \wedge q) \to p$, $(p \wedge q) \to q$ oraz $(r \to p) \to ((r \to q) \to (r \to (p \wedge q)))$;
10. $((p \wedge q) \to r) \leftrightarrow (p \to (q \to r))$;
11. $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$;
12. $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$;
13. $(p \to q) \leftrightarrow (\neg p \vee q)$;
14. $((p \leftrightarrow q) \leftrightarrow r) \leftrightarrow (p \leftrightarrow (q \leftrightarrow r))$;
15. $p \vee \bot \leftrightarrow p$ oraz $p \wedge \top \leftrightarrow p$.

Dowód: Łatwy. ∎

Niektóre z powyższych formuł wskazują na analogię pomiędzy implikacją i uporządkowaniem (np. zawieraniem zbiorów). Implikację $p \to q$ można odczytać tak: „warunek p jest silniejszy (mniejszy lub równy) od q". Formułę (1) czytamy wtedy: „fałsz jest najsilniejszym warunkiem (najmniejszym elementem)". Formuły (8) stwierdzają, że alternatywa $p \vee q$ jest najsilniejszym warunkiem, który wynika zarówno z p jak i z q (czyli jest kresem górnym pary $\{p, q\}$, jak suma zbiorów). Formuły (9) wyrażają dualną własność koniunkcji: to jest kres dolny, czyli najsłabszy warunek implikujący oba argumenty. Prawa de Morgana (11,12) wskazują też

na analogie koniunkcja – iloczyn, alternatywa – suma, negacja – dopełnienie. Ta ostatnia widoczna jest też w prawach wyłączonego środka (5), podwójnej negacji (6) i kontrapozycji (7).

O ile (9) wskazuje na analogię pomiędzy koniunkcją i iloczynem mnogościowym, o tyle warto zauważyć, że koniunkcja ma też własności podobne do iloczynu kartezjańskiego. Jeśli zbiór funkcji z A do B oznaczymy przez $[A \to B]$, to mamy (bardzo naturalną) równoliczność $[A \times B \to C] \sim [A \to [B \to C]]$. Podobieństwo tego związku do formuły (10) nie jest wcale przypadkowe. Wrócimy do tego w Rozdziale 11.

Formuła (13) wyraża implikację z pomocą negacji i alternatywy i jest często bardzo przydatna, gdy np. chcemy przekształcić jakąś formułę do prostszej postaci.

Formuła (2) mówi, że dodatkowe założenie można zawsze zignorować. Formuła (3) (prawo Frege) wyraża dystrybutywność implikacji względem siebie samej i może być odczytywana tak: jeśli r wynika z q w kontekście p, to ten kontekst może być włączony do założenia i konkluzji. Formuła (4) (prawo Peirce'a) wyraża przy pomocy samej implikacji zasadniczą własność logiki klasycznej: możliwość rozumowania przez zaprzeczenie. Sens prawa Peirce'a widać najlepiej gdy q jest fałszem, otrzymujemy wtedy prawo Claviusa: $(\neg p \to p) \to p$.

Warto zauważyć, że formuły w parach (6) i (7) nie są wcale tak symetryczne jak się wydaje na pierwszy rzut oka. Na przykład, pierwsza z formuł (6) to w istocie $p \to ((p \to \bot) \to \bot)$. Wiedząc, że p i $p \to \bot$, natychmiast zgadzamy się na $\bot$. Intuicyjne uzasadnienie drugiej formuły jest zaś w istocie związane z prawem (5).

Własnością, która często uchodzi naszej uwagi, jest łączność równoważności (14). W zwiazku z tym, wyrażenie $\varphi \leftrightarrow \psi \leftrightarrow \vartheta$ można z czystym sumieniem pisać bez nawiasów. Zwróćmy jednak uwagę na to, że oznacza ono zupełnie co innego niż stwierdzenie że φ, ψ i ϑ są sobie nawzajem równoważne!

Ostatnie na liście są dwie równoważności wyrażające taką myśl: fałsz jest „elementem neutralnym" dla alternatywy, a prawda dla koniunkcji. Dlatego $\bot$ możemy uważać za „pustą alternatywę" a $\top$ za „pustą koniunkcję". Powyżej pominięto dobrze znane prawa: łączność i przemienność koniunkcji i alternatywy, ich wzajemną dystrybutywność, przechodniość i zwrotność implikacji itp.

1.3 Postać normalna formuł

Definicja 1.6 Każdą zmienną zdaniową i negację zmiennej zdaniowej nazwijmy *literałem*. Mówimy, że formuła zdaniowa φ jest w *koniunkcyjnej postaci normalnej*, gdy φ jest koniunkcją alternatyw literałów, tj.

$$\varphi = (p_1^1 \vee \cdots \vee p_1^{k_1}) \wedge \cdots \wedge (p_r^1 \vee \cdots \vee p_r^{k_r}), \qquad (*)$$

gdzie $r \geq 0$, $k_i \geq 0$, dla $i = 0, \ldots r$, a wszystkie p_j^i są literałami. Przy tym pustą koniunkcję $(r = 0)$ utożsamiamy w myśl Przykładu 1.5(15) ze stałą $\top$, a stała $\bot$ to tyle co koniunkcja z jednym pustym składnikiem.

Fakt 1.7 *Dla każdej formuły zdaniowej istnieje równoważna jej formuła w koniunkcyjnej postaci normalnej.*

Dowód: Dowód jest przez indukcję ze względu na długość formuły. Symbole zdaniowe są oczywiście w postaci normalnej. Zgodnie z naszą definicją, także stałe logiczne są postaciami normalnymi. Jeśli φ jest w postaci (*), to $\neg\varphi$ można przekształcić w koniunkcyjną postać normalną stosując prawa De Morgana i prawa dystrybutywności:

$$\psi \vee (\vartheta \wedge \zeta) \leftrightarrow (\psi \vee \vartheta) \wedge (\psi \vee \zeta) \qquad \psi \vee (\vartheta \vee \zeta) \leftrightarrow (\psi \vee \vartheta) \vee (\psi \vee \zeta).$$

Podobnie postępujemy z alternatywą dwóch formuł w postaci normalnej.[1] Przypadek koniunkcji jest oczywisty, a implikację eliminujemy z pomocą prawa 1.5(13). Szczegóły pozostawiamy Czytelnikowi. ∎

Ćwiczenia

1. Zbadać, czy następujące formuły są tautologiami rachunku zdań i czy są spełnialne:

   (a) $(p \to r) \wedge (q \to s) \wedge (\neg p \vee \neg s) \to (\neg p \vee \neg q)$;
   (b) $(p \to q) \vee (q \to r)$;
   (c) $((p \to q) \to r) \wedge \neg(((q \to r) \to r) \to r))$;
   (d) $(p \to q) \wedge (\neg p \to r) \to (r \to \neg q)$;
   (e) $((\neg p \to q) \to r) \to \neg(p \to q)$;
   (f) $p \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$;
   (g) $(p \to q) \vee (p \to \neg q)$;
   (h) $q \vee r \to (p \vee q \to p \vee r)$;
   (i) $(p \vee q \vee r) \wedge (q \vee (\neg p \wedge s)) \wedge (\neg s \vee q \vee r) \to q$.

2. Czy następujące zbiory formuł są spełnialne?

   (a) $\{p \to \neg q, q \to \neg r, r \to \neg p\}$;
   (b) $\{p \to q, q \to r, r \vee s \leftrightarrow \neg q\}$;
   (c) $\{\neg(\neg q \vee p), p \vee \neg r, q \to \neg r\}$;
   (d) $\{s \to q, p \vee \neg q, \neg(s \wedge p), s\}$.

3. Czy zachodzą następujące konsekwencje?

   (a) $p \wedge q \to \neg r, p \models r \to \neg q$;
   (b) $p \to q, p \to (q \to r) \models p \to r$;
   (c) $p \to (q \to r), p \to q \models q \to r$;
   (d) $(p \to q) \to r, \neg p \models r$;
   (e) $(p \to q) \to r, \neg r \models p$;
   (f) $p \to q, r \to \neg q \models r \to \neg p$.

4. Dla dowolnej formuły φ niech $\hat{\varphi}$ oznacza dualizację formuły φ, tzn. formułę powstającą z φ przez zastąpienie każdego wystąpienia $\wedge$ symbolem $\vee$ oraz każdego wystąpienia $\vee$ symbolem $\wedge$.

   (i) Dowieść,że φ jest tautologią wtw, gdy $\neg\hat{\varphi}$ jest tautologią.

   (ii) Dowieść, że $\varphi \leftrightarrow \psi$ jest tautologią wtw, gdy $\hat{\varphi} \leftrightarrow \hat{\psi}$ jest tautologią.

[1] Ta procedura jest niestety wykładnicza (Ćwiczenie 8).

5. Znaleźć formułę zdaniową φ, która jest spełniona dokładnie przy wartościowaniach ϱ spełniających warunki:

   (a) Dokładnie dwie spośród wartości $\varrho(p)$, $\varrho(q)$ i $\varrho(r)$ są równe 1.

   (b) $\varrho(p) = \varrho(q) \neq \varrho(r)$.

   Rozwiązanie: Można to robić na różne sposoby, ale najprościej po prostu wypisać alternatywę koniunkcji, np. $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r)$.

6. Udowodnić, że dla dowolnej funkcji $f : \{0,1\}^k \to \{0,1\}$ istnieje formuła φ, w której występują tylko spójniki $\to$ i $\bot$ oraz zmienne zdaniowe ze zbioru $\{p_1, \ldots, p_k\}$, o tej własności, że dla dowolnego wartościowania zdaniowego ϱ zachodzi równość $[\![\varphi]\!]_\varrho = f(\varrho(p_1), \ldots, \varrho(p_k))$. (Inaczej mówiąc, formuła φ definiuje funkcję zerojedynkową f.)

   Wskazówka: Indukcja ze względu na k.

7. Niech X będzie dowolnym zbiorem niepustym. Dowolną funkcję $v : \mathrm{ZZ} \to \mathbf{P}(X)$ nazwijmy *wartościowaniem* w zbiorze $\mathbf{P}(X)$. Każdej formule zdaniowej φ przypiszemy teraz pewien podzbiór $[\![\varphi]\!]_v$ zbioru X, który nazwiemy jej *wartością* przy wartościowaniu v.

   - $[\![\bot]\!]_v = \emptyset$ oraz $[\![\top]\!]_v = X$;
   - $[\![p]\!]_v = v(p)$, gdy p jest symbolem zdaniowym;
   - $[\![\neg\varphi]\!]_v = X - [\![\varphi]\!]_v$;
   - $[\![\varphi \vee \psi]\!]_v = [\![\varphi]\!]_v \cup [\![\psi]\!]_v$;
   - $[\![\varphi \wedge \psi]\!]_v = [\![\varphi]\!]_v \cap [\![\psi]\!]_v$;
   - $[\![\varphi \to \psi]\!]_v = (X - [\![\varphi]\!]_v) \cup [\![\psi]\!]_v$.

   Udowodnić, że formuła φ jest tautologią rachunku zdań wtedy i tylko wtedy, gdy jest *prawdziwa* w $\mathbf{P}(X)$, tj. gdy dla dowolnego v jej wartością jest cały zbiór X.

8. Uzupełnić szczegóły dowodu Faktu 1.7. Pokazać, że długość postaci normalnej może wzrosnąć wykładniczo w stosunku do rozmiaru formuły początkowej.

9. Niech formuła $\varphi \to \psi$ będzie tautologią rachunku zdań. Znaleźć taką formułę ϑ, że:

   - Zarówno $\varphi \to \vartheta$ jak i $\vartheta \to \psi$ są tautologiami rachunku zdań.
   - W formule ϑ występują tylko te zmienne zdaniowe, które występują zarówno w φ jak i w ψ.

10. Niech $\varphi(p)$ będzie pewną formułą, w której występuje zmienna zdaniowa p i niech q będzie zmienną zdaniową nie występującą w $\varphi(p)$. Przez $\varphi(q)$ oznaczmy formułę powstałą z $\varphi(p)$ przez zamianę wszystkich p na q. Udowodnić, że jeśli
$$\varphi(p), \varphi(q) \models p \leftrightarrow q$$
to istnieje formuła ψ, nie zawierająca zmiennych p ani q, taka że
$$\varphi(p) \models p \leftrightarrow \psi.$$

2 Język logiki pierwszego rzędu.

Język logiki pierwszego rzędu[2] można traktować jak rozszerzenie rachunku zdań, pozwalające formułować stwierdzenia o zależnościach pomiędzy obiektami indywiduowymi (np. relacjach i funkcjach). Dzięki zastosowaniu *kwantyfikatorów*, odwołujących się do całej zbiorowości rozważanych obiektów, można w logice pierwszego rzędu wyrażać własności struktur relacyjnych oraz modelować rozumowania dotyczące takich struktur. Do zestawu symboli rachunku zdań dodajemy następujące nowe składniki syntaktyczne:

- *Symbole operacji i relacji* (w tym symbol równości $=$);
- *Zmienne indywiduowe*, których wartości mają przebiegać rozważane dziedziny;
- *Kwantyfikatory*, wiążące zmienne indywiduowe w formułach.

2.1 Składnia

Symbole operacji i relacji są podstawowymi składnikami do budowy najprostszych formuł, tzw. *formuł atomowych*. Z tego względu w języku pierwszego rzędu rezygnuje się ze zmiennych zdaniowych.

Definicja 2.1 Przez *sygnaturę* Σ rozumieć będziemy rodzinę zbiorów Σ_n^F, dla $n \geq 0$ oraz rodzinę zbiorów Σ_n^R, dla $n \geq 1$. Elementy Σ_n^F będziemy nazywać *symbolami operacji n-argumentowych*, a elementy Σ_n^R będziemy nazywać *symbolami relacji n-argumentowych*. Przyjmujemy, że wszystkie te zbiory są parami rozłączne. Umawiamy się też, że znak równości $=$ nie należy do Σ. Symbol ten nie jest zwykłym symbolem relacyjnym, ale jest traktowany na specjalnych prawach. W praktyce, sygnatura zwykle jest skończona i zapisuje się ją jako ciąg symboli. Np. ciąg złożony ze znaków $+, \cdot, 0, 1$ (o znanej każdemu liczbie argumentów) tworzy sygnaturę języka teorii ciał.

Definicja 2.2 Ustalamy pewien nieskończony przeliczalny zbiór X symboli, które będziemy nazywać *zmiennymi indywiduowymi* i zwykle oznaczać symbolami x, y, z. Zbiór *termów* $\mathcal{T}_\Sigma(X)$ nad sygnaturą Σ i zbiorem zmiennych X definiujemy indukcyjnie:

- Zmienne indywiduowe są termami.
- Dla każdego $n \geq 0$ i każdego symbolu operacji $f \in \Sigma_n^F$, jeśli $t_1, \ldots, t_n$ są termami, to $f(t_1, \ldots, t_n)$ jest też termem.

Zauważmy, że z powyższej definicji wynika iż stałe sygnatury Σ (czyli symbole operacji zeroargumentowych) są termami.

Definicja 2.3 Dla każdego termu $t \in \mathcal{T}_\Sigma(X)$ definiujemy zbiór $FV(t)$ zmiennych *występujących* w t. Definicja jest indukcyjna:

[2] Logika pierwszego rzędu nazywana jest też *rachunkiem predykatów* lub *rachunkiem kwantyfikatorów*.

- $FV(x) = \{x\}$.
- $FV(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} FV(t_i)$.

Definicja 2.4 Następnie zdefiniujemy *formuły atomowe* języka pierwszego rzędu.

- Symbol fałszu $\bot$ jest formułą atomową.
- Dla każdego $n \geq 1$, każdego symbolu $r \in \Sigma_n^R$ relacji n-argumentowej, oraz dla dowolnych termów $t_1, \ldots, t_n \in \mathcal{T}_\Sigma(X)$, napis $r(t_1, \ldots, t_n)$ jest formułą atomową.
- Dla dowolnych termów t_1, t_2, napis $(t_1 = t_2)$ jest formułą atomową.

Konwencja: Niektóre dwuargumentowe symbole relacyjne (np. $\leq$) i funkcyjne (np. $+, \cdot$) są zwyczajowo pisane pomiędzy argumentami. Na przykład formułę atomową $\leq(x, y)$ zwykle piszemy jako „$x \leq y$".

Definicja 2.5 *Formuły* nad sygnaturą Σ i zbiorem zmiennych indywiduowych X definiujemy indukcyjnie.

- Każda formuła atomowa jest formułą.
- Jeśli φ, ψ są formułami, to $(\varphi \to \psi)$ jest też formułą.
- Jeśli φ jest formułą a $x \in X$ jest zmienną indywiduową, to $\forall x \varphi$ jest też formułą.

Ponadto, dla każdej formuły φ definiujemy zbiór *zmiennych wolnych* $FV(\varphi)$ występujących w tej formule:

- $FV(\bot) = \emptyset$;
- $FV(r(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} FV(t_i)$;
- $FV(t_1 = t_2) = FV(t_1) \cup FV(t_2)$;
- $FV(\varphi \to \psi) = FV(\varphi) \cup FV(\psi)$;
- $FV(\forall x \varphi) = FV(\varphi) - \{x\}$.

Formułę bez kwantyfikatorów nazywamy *formułą otwartą*. Natomiast formuła bez zmiennych wolnych nazywa się *zdaniem*, lub *formułą zamkniętą*.

Negację, koniunkcję, alternatywę, symbol prawdy i równoważność formuł definiujemy podobnie jak w przypadku rachunku zdań. Kwantyfikator egzystencjalny zdefiniujemy jako skrót notacyjny przy pomocy *uogólnionego prawa De Morgana*:

$$\exists x \varphi \qquad \text{oznacza} \qquad \neg \forall x \neg \varphi.$$

Zmienne wolne a zmienne związane. W Definicji 2.5 nie zakładamy, że $x \in FV(\varphi)$. Zauważmy też, że zmienna x może występować w formule φ podczas gdy $x \notin FV(\varphi)$. Przez *wystąpienie* zmiennej indywiduowej x rozumiemy tu zwykłe pojawienie się x w jakimkolwiek termie w φ. I tak na przykład w formule[3] $\exists x \forall u(r(x,y) \to \forall y \exists x\, s(x,y,z))$ zmienna u nie występuje, podczas gdy x i y wystepują po dwa razy, a z występuje jeden raz. Bardzo ważną rzeczą jest rozróżnienie wystąpień zmiennych *wolnych* i *związanych* w formułach. Wszystkie wystąpienia zmiennych w formułach atomowych są wolne. Wolne (związane) wystąpienia w formułach φ i ψ pozostają wolne (związane) w formule $\varphi \to \psi$. Wszystkie wolne wystąpienia x w φ stają się związanymi wystąpieniami w formule $\exists x \varphi$ (związanymi przez dopisanie kwantyfikatora $\exists$), a charakter pozostałych wystąpień jest taki sam w φ i w $\exists x \varphi$. Przykładowo w formule $\exists x \forall u(r(x,\underline{y}) \to \forall y \exists x\, s(x,y,z))$ podkreślone wystąpienie y jest wolne, a nie podkreślone jest związane. Obydwa wystąpienia x są zwiazane, ale przez różne kwantyfikatory.

Na koniec uwaga o nazwach zmiennych związanych. Rozróżnienie pomiędzy zmiennymi wolnymi a związanymi jest analogiczne do rozróżnenia pomiedzy identyfikatorami lokalnymi a globalnymi w językach programowania. Globalne identyfikatory, widoczne na zewnątrz, odpowiadają zmiennym wolnym, podczas gdy lokalne identyfikatory (związane np. deklaracją w bloku) nie są widoczne na zewnątrz zakresu ich deklaracji. Intuicyjnie naturalne jest oczekiwanie, że zmiana zmiennej związanej na inną zmienną (tak aby nie wprowadzić konfliktu wynikającego ze zmiany struktury wiązań) nie powinna zmieniać znaczenia formuły.[4] Tak w istocie będzie, jak się przekonamy poniżej (Fakt 2.12).

2.2 Semantyka formuł

Niech Σ będzie sygnaturą. *Struktura* $\mathfrak{A}$ nad sygnaturą Σ (lub po prostu Σ-struktura) to niepusty zbiór A, zwany *nośnikiem*, wraz z interpretacją każdego symbolu operacji $f \in \Sigma_n^F$ jako funkcji n argumentowej $f^{\mathfrak{A}} : A^n \to A$ oraz każdego symbolu relacji $r \in \Sigma_n^R$ jako relacji n-argumentowej $r^{\mathfrak{A}} \subseteq A^n$. (Na przykład, jeśli Σ składa się z jednego symbolu relacji dwuargumentowej, to każdy graf zorientowany jest Σ-strukturą.) W praktyce, strukturę relacyjną przedstawia się jako krotkę postaci $\mathfrak{A} = \langle A, f_1^{\mathfrak{A}}, \ldots, f_n^{\mathfrak{A}}, r_1^{\mathfrak{A}}, \ldots, r_m^{\mathfrak{A}} \rangle$, gdzie $f_1, \ldots, f_n, r_1, \ldots, r_m$ są wszystkimi symbolami danej sygnatury. Często, gdy będzie jasne z kontekstu z jaką strukturą mamy do czynienia, będziemy opuszczać nazwę struktury i pisać po prostu $r, f, \ldots$ zamiast $r^{\mathfrak{A}}, f^{\mathfrak{A}}, \ldots$

Wartościowaniem w Σ-strukturze $\mathfrak{A}$ nazwiemy dowolną funkcję $\varrho : X \to A$. Dla wartościowania ϱ, zmiennej $x \in X$ oraz elementu $a \in A$ definiujemy nowe wartościowanie $\varrho_x^a : X \to A$, będące modyfikacją wartościowania ϱ na argumencie x, w następujący sposób,

$$\varrho_x^a(y) = \begin{cases} \varrho(y), & \text{jeśli } y \neq x; \\ a, & \text{w przeciwnym przypadku.} \end{cases}$$

Najpierw zdefiniujemy znaczenie termów. Wartość termu $t \in \mathcal{T}_\Sigma(X)$ w Σ-strukturze $\mathfrak{A}$ przy wartościowaniu ϱ oznaczamy przez $[\![t]\!]_\varrho^{\mathfrak{A}}$, lub $[\![t]\!]_\varrho$, gdy $\mathfrak{A}$ jest znane. Definicja jest indukcyjna:

[3] Zakładamy tu, że s oraz r są symbolami relacji.

[4] Taka zamiana zmiennych bywa nazywana *α-konwersją*.

- $[\![x]\!]^{\mathfrak{A}}_{\varrho} = \varrho(x)$.
- $[\![f(t_1, \ldots, t_n)]\!]^{\mathfrak{A}}_{\varrho} = f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{A}}_{\varrho}, \ldots, [\![t_1]\!]^{\mathfrak{A}}_{\varrho})$.

Znaczenie formuł definiujemy poniżej. Napis

$$(\mathfrak{A}, \varrho) \models \varphi.$$

czytamy: formuła φ jest *spełniona* w strukturze $\mathfrak{A}$ przy wartościowaniu ϱ. Zakładamy tu, że φ oraz $\mathfrak{A}$ są nad tą samą sygnaturą. Spełnianie definiujemy przez indukcję ze względu na budowę formuły φ.

- Nie zachodzi $(\mathfrak{A}, \varrho) \models \bot$.
- Dla dowolnego $n \geq 1$, $r \in \Sigma^R_n$ oraz dla dowolnych termów $t_1, \ldots, t_n$, przyjmujemy, że $(\mathfrak{A}, \varrho) \models r(t_1, \ldots, t_n)$ wtedy i tylko wtedy, gdy $\langle [\![t_1]\!]^{\mathfrak{A}}_{\varrho}, \ldots [\![t_1]\!]^{\mathfrak{A}}_{\varrho} \rangle \in r^{\mathfrak{A}}$.
- $(\mathfrak{A}, \varrho) \models t_1 = t_2$, wtedy i tylko wtedy, gdy $[\![t_1]\!]^{\mathfrak{A}}_{\varrho} = [\![t_2]\!]^{\mathfrak{A}}_{\varrho}$.
- $(\mathfrak{A}, \varrho) \models \varphi \to \psi$, gdy nie zachodzi $(\mathfrak{A}, \varrho) \models \varphi$ lub zachodzi $(\mathfrak{A}, \varrho) \models \psi$.
- $(\mathfrak{A}, \varrho) \models \forall x \varphi$ wtedy i tylko wtedy, gdy dla dowolnego $a \in A$ zachodzi $(\mathfrak{A}, \varrho^a_x) \models \varphi$.

Nastepujące twierdzenie pokazuje, że spełnianie formuły φ w dowolnej strukturze zależy jedynie od wartości zmiennych wolnych $FV(\varphi)$. Uzasadnia ono następującą konwencję notacyjną: napiszemy na przykład $(\mathfrak{A}, x : a, y : b) \models \varphi$ zamiast $(\mathfrak{A}, \varrho) \models \varphi$, gdy $\varrho(x) = a$ i $\varrho(y) = b$, a przy tym wiadomo, że w formule φ występują wolno tylko zmienne x i y. Jeśli φ jest zdaniem, to wartościowanie można całkiem pominąć.

Fakt 2.6 *Dla dowolnej Σ-struktury $\mathfrak{A}$ i dowolnej formuły φ jeśli wartościowania ϱ i ϱ' przyjmują równe wartości dla wszystkich zmiennych wolnych w φ, to*

$$(\mathfrak{A}, \varrho) \models \varphi \qquad \textit{wtedy i tylko wtedy, gdy} \qquad (\mathfrak{A}, \varrho') \models \varphi.$$

Dowód: Ćwiczenie. ∎

2.3 Prawdziwość i spełnialność formuł

Powiemy, że formuła φ jest *spełnialna w* $\mathfrak{A}$, gdy istnieje wartościowanie ϱ w strukturze $\mathfrak{A}$ takie, że zachodzi $(\mathfrak{A}, \varrho) \models \varphi$. Formuła φ jest *spełnialna*, gdy istnieje struktura $\mathfrak{A}$, w której φ jest spełnialna.

Formuła φ jest *prawdziwa* w $\mathfrak{A}$, gdy dla każdego wartościowania ϱ w $\mathfrak{A}$ zachodzi $(\mathfrak{A}, \varrho) \models \varphi$. W tym przypadku mówimy też, że $\mathfrak{A}$ jest *modelem* dla formuły φ (oznaczamy to przez $\mathfrak{A} \models \varphi$). Dla zbioru formuł Γ i Σ-struktury $\mathfrak{A}$ powiemy, że $\mathfrak{A}$ jest modelem dla Γ (piszemy $\mathfrak{A} \models \Gamma$), gdy dla każdej formuły $\varphi \in \Gamma$, zachodzi $\mathfrak{A} \models \varphi$. Formuła φ jest *tautologią* (oznaczamy to przez $\models \varphi$), gdy jest ona prawdziwa w każdej Σ-strukturze.

Oczywiście jeśli weźmiemy dowolną tautologię rachunku zdań to po podstawieniu na miejsce zmiennych zdaniowych dowolnych formuł logiki pierwszego rzędu dostaniemy tautologię logiki pierwszego rzędu. Poniżej podajemy przykłady tautologii logiki pierwszego rzedu, których nie da się w ten sposób otrzymać.

Fakt 2.7 *Następujące formuły są tautologiami logiki pierwszego rzedu:*

1. $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$.
2. $\varphi \to \forall x\varphi$, *o ile* $x \notin FV(\varphi)$.
3. $\forall x\varphi \to \varphi$.
4. $x = x$.
5. $x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \cdots)$, *dla* $f \in \Sigma_n^F$, $n \geq 0$.
6. $x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to r(x_1, \ldots, x_n) \to r(y_1, \ldots, y_n)) \cdots)$, *dla* $r \in \Sigma_n^R$, $n \geq 1$.

Dowód: Aby się przekonać, że formuła (1) jest tautologią, rozpatrzmy dowolną strukturę $\mathfrak{A}$ i jakieś wartościowanie ϱ. Załóżmy najpierw, że $(\mathfrak{A}, \varrho) \models \forall x(\varphi \to \psi)$ oraz $(\mathfrak{A}, \varrho) \models \forall x\, \varphi$. Oznacza to, że dla dowolnego $a \in A$ zachodzi $(\mathfrak{A}, \varrho_x^a) \models \varphi$ oraz $(\mathfrak{A}, \varrho_x^a) \models \varphi \to \psi$. Musi więc zajść $(\mathfrak{A}, \varrho_x^a) \models \psi$. Z dowolności a mamy $(\mathfrak{A}, \varrho) \models \forall x\, \psi$, a stąd $(\mathfrak{A}, \varrho) \models \forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$.

Jeśli $(\mathfrak{A}, \varrho) \not\models \forall x(\varphi \to \psi)$ lub $(\mathfrak{A}, \varrho) \not\models \forall x\, \varphi$, to nasza formuła jest spełniona przez ϱ wprost z definicji. Uzasadnienie części (3–6) pozostawiamy czytelnikowi. ∎

Ponadto mamy następujący

Fakt 2.8 *Dla dowolnej tautologii* φ *i dowolnej zmiennej* x, *formuła* $\forall x\varphi$ *jest też tautologią.*

Dowód: Ćwiczenie. ∎

Uzasadnienie, że dana formuła jest tautologią polega na analizie jej spełniania w dowolnych modelach (por. Fakt 2.7). Natomiast wykazanie, że tak nie jest polega na podaniu odpowiedniego kontrprzykładu. Takiego jak ten:

Przykład 2.9 Zdanie $(\forall x p(x) \to \forall x q(x)) \to \forall x(p(x) \to q(x))$ nie jest tautologią. Rozpatrzmy bowiem model $\mathfrak{A} = \langle \mathbb{N}, p^{\mathfrak{A}}, q^{\mathfrak{A}} \rangle$, w którym:

- $n \in p^{\mathfrak{A}}$, wtedy i tylko wtedy, gdy n jest parzyste;
- $n \in q^{\mathfrak{A}}$, wtedy i tylko wtedy, gdy n jest nieparzyste;

Ponieważ $p^{\mathfrak{A}} \neq \mathbb{N}$, więc $\mathfrak{A} \not\models \forall x p(x)$. (Mamy tu do czynienia ze zdaniem, więc wartościowanie jest nieistotne i dlatego je pomijamy.) Stąd otrzymujemy $\mathfrak{A} \models \forall x p(x) \to \forall x q(x)$. Z drugiej strony $\mathfrak{A} \not\models \forall x(p(x) \to q(x))$, ponieważ $(\mathfrak{A}, x : 2) \not\models p(x) \to q(x)$. Rzeczywiście, $2 \in p^{\mathfrak{A}} - q^{\mathfrak{A}}$.

2.4 Podstawianie termów

Dla formuły φ, termu t i zmiennej x, napis $\varphi(t/x)$ oznacza wynik podstawienia t na wszystkie *wolne* wystąpienia x w φ. Wykonywanie takiego podstawienia bez dodatkowych zastrzeżeń może prowadzić do kłopotów. Na przykład sens formuł $\forall y(y \leq x)$ oraz $\forall z(z \leq x)$ jest taki sam. Tymczasem „naiwne" podstawienie y w miejsce x w obu tych formułach daje w wyniku odpowiednio $\forall y(y \leq y)$ i $\forall z(z \leq y)$, a te dwie formuły znaczą całkiem co innego. Przyczyną jest to, że w pierwszym przypadku zmienną y wstawiono w zasięg kwantyfikatora $\forall y$.

Źródłem problemu w powyższym przykładzie było to, że po wykonaniu podstawienia pojawiały się nowe wiązania kwantyfikatorem. Sugeruje to następującą definicję. Powiemy, że term t jest *dopuszczalny* dla zmiennej x w formule φ (lub, że podstawienie $\varphi(t/x)$ jest *dopuszczalne*) jeśli dla każdej zmiennej y występującej w t, żadne wolne wystąpienie x w φ nie jest zawarte w zasięgu kwantyfikatora $\forall y$ lub $\exists y$. Mamy więc następującą indukcyjną definicję dopuszczalnego podstawienia,[5] w której każda lewa strona jest dopuszczalna pod warunkiem, że prawa strona jest dopuszczalna.

- $\bot(t/x) = \bot$, gdy $x \notin FV(\varphi)$;
- $r(t_1, \ldots, t_n)(t/x) = r(t_1(t/x), \ldots, t_n(t/x))$;
- $(t_1 = t_2)(t/x) = (t_1(t/x) = t_2(t/x))$;
- $(\varphi \to \psi)(t/x) = \varphi(t/x) \to \psi(t/x)$;
- $(\forall x\, \varphi)(t/x) = \forall x\, \varphi$;
- $(\forall y\, \varphi)(t/x) = \forall y\, \varphi(t/x)$, gdy $y \neq x$, oraz $y \notin FV(t)$;
- W pozostałych przypadkach podstawienie jest niedopuszczalne.

W dalszym ciągu będziemy rozważać jedynie podstawienia dopuszczalne.

Lemat 2.10 (o podstawieniu) *Niech $\mathfrak{A}$ będzie dowolną strukturą oraz $\varrho : X \to A$ dowolnym wartościowaniem w $\mathfrak{A}$. Niech t będzie dowolnym termem.*

1. *Dla dowolnego termu s i zmiennej x mamy*

$$[\![s(t/x)]\!]^{\mathfrak{A}}_{\varrho} = [\![s]\!]^{\mathfrak{A}}_{\varrho^a_x}$$

   gdzie $a = [\![t]\!]^{\mathfrak{A}}_{\varrho}$.

2. *Dla dowolnej formuły φ, jeśli term t jest dopuszczalny dla x w φ, to*

$$(\mathfrak{A}, \varrho) \models \varphi(t/x) \qquad \text{wtedy i tylko wtedy, gdy} \qquad (\mathfrak{A}, \varrho^a_x) \models \varphi,$$

   gdzie $a = [\![t]\!]^{\mathfrak{A}}_{\varrho}$.

[5] Podstawianie termu t do termu s na miejsce zmiennej x oznaczamy podobnie: $s(t/x)$. Takie podstawienie jest zawsze wykonalne.

Dowód: Część 1 dowodzimy przez indukcję ze względu na budowę termu s. Jeśli s jest zmienną x, to obie strony są równe $[\![t]\!]^{\mathfrak{A}}_{\varrho}$. Jeśli s jest zmienną y (różną od x), to obie strony są równe $\varrho(y)$. Jeśli s jest postaci $f(s_1, \ldots, s_n)$, to mamy następujące równości.

$$\begin{aligned}
[\![s(t/x)]\!]^{\mathfrak{A}}_{\varrho} &= [\![f(s_1(t/x), \ldots, s_n(t/x))]\!]^{\mathfrak{A}}_{\varrho} \\
&= f^{\mathfrak{A}}([\![s_1(t/x)]\!]^{\mathfrak{A}}_{\varrho}, \ldots, [\![s_n(t/x)]\!]^{\mathfrak{A}}_{\varrho}) \\
&= f^{\mathfrak{A}}([\![s_1]\!]^{\mathfrak{A}}_{\varrho^a_x}, \ldots, [\![s_n]\!]^{\mathfrak{A}}_{\varrho^a_x}) \\
&= [\![f(s_1, \ldots, s_n)]\!]^{\mathfrak{A}}_{\varrho^a_x} = [\![s]\!]^{\mathfrak{A}}_{\varrho^a_x}.
\end{aligned}$$

Dowód części 2 przeprowadzamy przez indukcję ze względu na budowę formuły φ. Jeśli φ jest postaci $\bot$ to teza jest oczywista. Jeśli φ jest formułą atomową, to tezę natychmiast dostajemy z wyżej udowodnionej części 1. Na przykład, jeśli φ jest postaci $s_1 = s_2$ to mamy:

$$\begin{array}{lll}
(\mathfrak{A}, \varrho) \models \varphi(t/x) & \text{wtedy i tylko wtedy, gdy} & [\![s_1(t/x)]\!]^{\mathfrak{A}}_{\varrho} = [\![s_1(t/x)]\!]^{\mathfrak{A}}_{\varrho} \\
& \text{wtedy i tylko wtedy, gdy} & [\![s_1]\!]^{\mathfrak{A}}_{\varrho^a_x} = [\![s_2]\!]^{\mathfrak{A}}_{\varrho^a_x} \\
& \text{wtedy i tylko wtedy, gdy} & (\mathfrak{A}, \varrho^a_x) \models s_1 = s_2.
\end{array}$$

Druga z powyższych równoważności wynika z części 1.

Krok indukcyjny dla przypadku, gdy φ jest postaci $\psi \to \vartheta$ jest oczywisty i pozostawimy go czytelnikowi. Rozważymy przypadek gdy φ jest postaci $\forall y \psi$. Jeśli zmienne x oraz y są równe, to x nie występuje wolno w φ i wówczas teza wynika natychmiast z Faktu 2.6. Tak więc przyjmijmy, że x oraz y są różnymi zmiennymi. Wówczas z dopuszczalności t dla x w φ wynika, że y nie występuje w t. Ponadto $\varphi(t/x)$ jest identyczne z $\forall y \psi(t/x)$. Mamy następujące równoważności:

$$\begin{array}{lll}
(\mathfrak{A}, \varrho) \models \forall y \psi(t/x) & \text{wtedy i tylko wtedy, gdy} & \text{dla każdego } d \in A,\ (\mathfrak{A}, \varrho^d_y) \models \psi(t/x) \\
& \text{wtedy i tylko wtedy, gdy} & \text{dla każdego } d \in A,\ (\mathfrak{A}, \varrho^{d\,a'}_{y\,x}) \models \psi,
\end{array}$$

gdzie $a' = [\![t]\!]^{\mathfrak{A}}_{\varrho^d_y}$. Ponieważ y nie występuje w t, więc $a' = [\![t]\!]^{\mathfrak{A}}_{\varrho^d_y} = [\![t]\!]^{\mathfrak{A}}_{\varrho} = a$. Skoro zmienne x oraz y są różne, to $\varrho^{d\,a}_{y\,x} = \varrho^{a\,d}_{x\,y}$. Tak więc warunek $(\mathfrak{A}, \varrho^{d\,a'}_{y\,x}) \models \psi$ jest równoważny warunkowi $(\mathfrak{A}, \varrho^{a\,d}_{x\,y}) \models \psi$, dla każdego $d \in A$. Czyli

$$(\mathfrak{A}, \varrho^a_x) \models \forall y \psi. \qquad \blacksquare$$

Natychmiastowym wnioskiem z Lematu 2.10 jest następujący przykład tautologii.

Fakt 2.11 *Dla dowolnej formuły φ, zmiennej x i termu t dopuszczalnego dla x w φ, formuła*

$$\forall x \varphi \to \varphi(t/x)$$

jest tautologią logiki pierwszego rzędu.

Dowód: Ćwiczenie. $\blacksquare$

Fakt 2.12 *Jeśli zmienna y jest dopuszczalna dla x w φ oraz $y \notin FV(\varphi)$, to*

$$\models (\forall x\varphi) \leftrightarrow (\forall y\varphi(y/x)).$$

Dowód: Z Faktu 2.11 oraz Faktu 2.8 otrzymujemy

$$\models \forall y(\forall x\varphi \rightarrow \varphi(y/x)).$$

Zatem na mocy Faktu 2.7(1) wnioskujemy, że

$$\models (\forall y\forall x\varphi) \rightarrow (\forall y\varphi(y/x)).$$

Na mocy Przykładu 2.7(2) otrzymujemy implikację $\rightarrow$. Odwrotna implikacja wynika z już udowodnionej implikacji oraz z następujących prostych obserwacji:

- Jeśli y jest dopuszczalna dla x w φ, to x jest dopuszczalna dla y w $\varphi(y/x)$.
- Jeśli $y \notin FV(\varphi)$, to x nie występuje wolno w $\varphi(y/x)$.
- Wynik podstawienia $\varphi(y/x)(x/y)$ jest identyczny z φ. ∎

Fakt 2.12 pozwala zamieniać zmienne związane dowolnie, tak długo jak są spełnione założenia. W szczególności jeśli chcemy wykonać podstawienie termu do formuły w sytuacji, gdy ten term nie jest dopuszczalny to wystarczy zamienić nazwy pewnych zmiennych związanych, tak aby term stał się dopuszczalny. Łatwo jest uogólnić Fakt 2.12: znaczenie formuły nie ulega zmianie także przy wymianie zmiennych związanych kwantyfikatorami wystepującymi wewnątrz formuły.

Ćwiczenia

1. Niech $\mathfrak{A} = \langle \mathbb{N}, p^{\mathfrak{A}}, q^{\mathfrak{A}} \rangle$, gdzie:
   $\langle a, b \rangle \in p^{\mathfrak{A}}$ wtedy i tylko wtedy, gdy $a + b \geq 6$;
   $\langle a, b \rangle \in q^{\mathfrak{A}}$ wtedy i tylko wtedy, gdy $b = a + 2$.

   Zbadać czy formuły

   (a) $\forall x p(x, y) \rightarrow \exists x q(x, y)$;
   (b) $\forall x p(x, y) \rightarrow \forall x q(x, y)$;
   (c) $\forall x p(x, y) \rightarrow \exists x q(x, z)$;

   są spełnione przy wartościowaniu $v(y) = 7$, $v(z) = 1$ w strukturze $\mathfrak{A}$.

2. Niech $\mathfrak{A} = \langle \mathbb{Z}, f^{\mathfrak{A}}, r^{\mathfrak{A}} \rangle$ i $\mathfrak{B} = \langle \mathbb{Z}, f^{\mathfrak{B}}, r^{\mathfrak{B}} \rangle$, gdzie
   $f^{\mathfrak{A}}(m, n) = \min(m, n)$, dla $m, n \in \mathbb{Z}$, a $r^{\mathfrak{A}}$ jest relacją $\geq$;
   $f^{\mathfrak{B}}(m, n) = m^2 + n^2$, dla $m, n \in \mathbb{Z}$, a $r^{\mathfrak{B}}$ jest relacją $\leq$.

   Zbadać czy formuły

   (a) $\forall y(\forall x(r(z, f(x, y)) \rightarrow r(z, y)))$;
   (b) $\forall y(\forall x(r(z, f(x, y))) \rightarrow r(z, y))$,

są spełnione przy wartościowaniu $v(z) = 5$, $v(y) = 7$ w strukturach $\mathfrak{A}$ i $\mathfrak{B}$.

3. Czy formuła $\forall x(\neg r(x, y) \to \exists z(r(f(x, z), g(y))))$ jest spełniona przy wartościowaniu $v(x) = 3$, $w(x) = 6$ i $u(x) = 14$

   (a) w strukturze $\mathfrak{A} = \langle \mathbb{N}, r^{\mathfrak{A}} \rangle$, gdzie $r^{\mathfrak{A}}$ jest relacją podzielności?
   (b) w strukturze $\mathcal{B} = \langle \mathbb{N}, r^{\mathfrak{B}} \rangle$, gdzie $r^{\mathfrak{B}}$ jest relacją przystawania modulo 7?

4. W jakich strukturach prawdziwa jest formuła $\exists y(y \neq x)$? A formuła $\exists y(y \neq y)$ otrzymana przez „naiwne" podstawienie y na x?

5. Podaj przykład modelu i wartościowania, przy którym formuła
$$p(x, f(x)) \to \forall x \exists y\, p(f(y), x)$$
jest: a) spełniona; b) nie spełniona.

6. Zbadać, czy następujące formuły są tautologiami i czy są spełnialne:

   (a) $\exists x \forall y(p(x) \vee q(y)) \to \forall y(p(f(y)) \vee q(y))$;
   (b) $\forall y(p(f(y)) \vee q(y)) \to \exists x \forall y(p(x) \vee q(y))$;
   (c) $\exists x(\forall y q(y) \to p(x)) \to \exists x \forall y(q(y) \to p(x))$;
   (d) $\exists x(\forall y q(y) \to p(x)) \to \exists x(q(x) \to p(x))$.

7. Niech f będzie jednoargumentowym symbolem funkcyjnym, który nie występuje w formule φ. Pokazać, że formuła $\forall x \exists y \varphi$ jest spełnialna wtedy i tylko wtedy gdy formuła $\forall x \varphi(f(x)/y)$ jest spełnialna.

8. Udowodnić, że zdanie
$$\forall x \exists y\, p(x, y) \wedge \forall x \neg p(x, x) \wedge \forall x \forall y \forall z(p(x, y) \wedge p(y, z) \to p(x, z))$$
ma tylko modele nieskończone.

9. Dla każdego n napisać takie zdanie φ_n, że $\mathfrak{A} \models \varphi_n$ zachodzi wtedy i tylko wtedy, gdy $\mathfrak{A}$ ma dokładnie n elementów.

10. Czy jeśli $\mathfrak{A} \models \exists x\, \varphi$, to także $\mathfrak{A} \models \varphi[t/x]$, dla pewnego termu t?

3 Logika pierwszego rzędu. Sposób użycia.

Przyjrzyjmy się teraz kilku ważnym tautologiom.

Fakt 3.1 *Następujące formuły są tautologiami (dla dowolnych φ i ψ).*

1. $\forall x(\varphi \to \psi) \to (\exists x\varphi \to \exists x\psi)$;
2. $\exists x\varphi \to \varphi$, *o ile* $x \notin FV(\varphi)$;
3. $\varphi(s/x) \to \exists x\varphi$;
4. $\neg\forall x\varphi \leftrightarrow \exists x\neg\varphi$;
5. $\neg\exists x\varphi \leftrightarrow \forall x\neg\varphi$;
6. $\forall x(\varphi \wedge \psi) \leftrightarrow \forall x\varphi \wedge \forall x\psi$;
7. $\exists x(\varphi \vee \psi) \leftrightarrow \exists x\varphi \vee \exists x\psi$;
8. $\forall x(\varphi \vee \psi) \leftrightarrow \varphi \vee \forall x\psi$, *o ile* $x \notin FV(\varphi)$;
9. $\exists x(\varphi \wedge \psi) \leftrightarrow \varphi \wedge \exists x\psi$, *o ile* $x \notin FV(\varphi)$;
10. $\forall x\varphi \to \exists x\varphi$;
11. $\forall x\forall y\varphi \leftrightarrow \forall y\forall x\varphi$;
12. $\exists x\exists y\varphi \leftrightarrow \exists y\exists x\varphi$;
13. $\exists x\forall y\varphi \to \forall y\exists x\varphi$.

Dowód: Ćwiczenie. ∎

Formuły (1)–(3) powyżej wyrażają własności kwantyfikatora szczegółowego i są odpowiednikami formuł z Faktu 2.7. Zauważmy, że zamiast rozdzielności kwantyfikatora szczegółowego, mamy tu jeszcze jedno prawo rozkładu kwantyfikatora ogólnego. Zakłóca to nieco symetrię pomiędzy $\forall$ i $\exists$, wyrażoną prawami de Morgana (4) i (5).

Kolejne dwie tautologie przypominają o bliskim związku kwantyfikatora ogólnego z koniunkcją i kwantyfikatora szczegółowego z alternatywą. (Uwaga: zmienna x może być wolna w φ i ψ.) Analogiczna rozdzielność kwantyfikatora ogólnego względem alternatywy (8) i kwantyfikatora szczegółowego względem koniunkcji (9) nie zawsze jest prawdą, ale zachodzi pod warunkiem, że zmienna wiązana kwantyfikatorem nie występuje w jednym z członów formuły. (Prawo (8) nazywane bywa prawem Grzegorczyka.)

Formuła (10) jest odbiciem naszego założenia o niepustości świata. Jest to tautologia, ponieważ umówiliśmy się, że rozważamy tylko struktury o niepustych nośnikach.

Prawa (11)–(13) charakteryzują możliwości permutowania kwantyfikatorów. Implikacja odwrotna do (13) zazwyczaj nie jest tautologią.

Stosując równoważności (4–9) możemy każdą formułę sprowadzić do postaci, w której wszystkie kwantyfikatory znajdują się na początku.

Definicja 3.2 Mówimy, że formuła φ jest w *preneksowej postaci normalnej*, gdy

$$\varphi = Q_1 y_1 Q_2 y_2 \dots Q_n y_n \, \psi,$$

gdzie każde z Q_i to $\forall$ lub $\exists$, a ψ jest formułą otwartą. (Oczywiście n może być zerem.)

Fakt 3.3 *Dla każdej formuły pierwszego rzędu istnieje równoważna jej formuła w preneksowej postaci normalnej.*

Dowód: Indukcja (ćwiczenie). ∎

Przykład 3.4 Formuła $\exists y p(y) \to \forall z q(z)$ jest równoważna każdej z następujących formuł:

$$\neg\exists y \, p(y) \vee \forall z \, q(z);$$

$$\forall y \, \neg p(y) \vee \forall z \, q(z);$$

$$\forall y (\neg p(y) \vee \forall z \, q(z));$$

$$\forall y \forall z (\neg p(y) \vee q(z));$$

$$\forall y \forall z (p(y) \to q(z)).$$

3.1 Logika formalna i język polski

Systemy logiki formalnej są, jak już mówiliśmy, tylko pewnymi modelami, czy też przybliżeniami rzeczywistych sposobów wyrażania różnych stwierdzeń i wnioskowania o ich poprawności. Poziom dokładności takich przybliżeń może być większy lub mniejszy. Większy tam, gdzie mamy do czynienia z dobrze określoną teorią matematyczną, lub językiem programowania. Mniejszy wtedy, gdy używamy logiki do weryfikacji poprawności stwierdzeń języka potocznego, choćby takiego jak podręcznikowy przykład: *„Janek idzie do szkoły."* Oczywiście przypisanie temu stwierdzeniu wartości logicznej jest zgoła niemożliwe, nie wiemy bowiem, który Janek do jakiej ma iść szkoły i czy może już doszedł? Więcej sensu ma zastosowanie logiki predykatów do analizy np. takiego rozumowania:

Każdy cyrulik sewilski goli tych wszystkich mężczyzn w Sewilli, którzy się sami nie golą.
Ale nie goli żadnego z tych, którzy golą się sami.
A zatem w Sewilli nie ma ani jednego cyrulika.

W tym przypadku aparat logiki formalnej może być pomocny. Łatwiej zrozumieć o co chodzi, tłumacząc nasz problem na język logiki predykatów, i przedstawiając go jako pytanie o poprawność pewnego stwierdzenia postaci $\Gamma \models \varphi$. Można więc zapytać, czy

$$\forall x(C(x) \wedge S(x) \to \forall y(G(x,y) \leftrightarrow S(y) \wedge \neg G(y,y))) \models \neg\exists x(C(x) \wedge S(x))?$$

Stwierdziwszy poprawność powyższego stwierdzenia, wywnioskujemy, że w Sewilli cyrulika nie ma. I będzie to wniosek... błędny, bo cyrulik być może jest kobietą.

W powyższym przykładzie po prostu źle ustalono logiczną interpretację naszego zadania, zapominając o jednym z jego istotnych elementów. Błąd ten można łatwo naprawić, co jest zalecane jako ćwiczenie. Ale nie zawsze język logiki formalnej wyraża ściśle to samo, co potoczny język polski, a nawet język w którym pisane są prace matematyczne. Zarówno składnia jak i semantyka tych języków rządzi się zupełnie innymi prawami, i o tym należy pamiętać tłumacząc jeden na drugi.

Implikacja materialna i związek przyczynowo-skutkowy

Implikacja, o której mówimy w logice klasycznej to tzw. *implikacja materialna*. Wartość logiczna, którą przypisujemy wyrażeniu „$\varphi \to \psi$" zależy wyłącznie od wartości logicznych przypisanych jego częściom składowym φ i ψ. Nie zależy natomiast zupełnie od treści tych wyrażeń, czy też jakichkolwiek innych związków pomiędzy φ i ψ. W szczególności, wypowiedzi φ i ψ mogą mówić o zajściu jakichś zdarzeń i wtedy wartość logiczna implikacji „$\varphi \to \psi$" nie ma nic wspólnego z ich ewentualnym następstwem w czasie, lub też z tym, że jedno z tych zdarzeń spowodowało drugie. W języku polskim stwierdzenie *„jeśli φ to ψ"* oczywiście sugeruje taki związek, np. w zdaniu:

Jeśli zasilanie jest włączone, to terminal działa.

Tymczasem implikacja materialna nie zachodzi, o czym dobrze wiedzą użytkownicy terminali. Co więcej, w istocie materialną prawdą jest stwierdzenie odwrotne:

Jeśli terminal działa to zasilanie jest włączone.

Natomiast zdanie

Terminal działa, ponieważ zasilanie jest włączone,

stwierdza nie tylko związek przyczynowo-skutkowy, ale też faktyczne zajście wymienionych zdarzeń i w ogóle nie ma odpowiednika w logice klasycznej.

Inne spójniki w mniejszym stopniu grożą podobnymi nieporozumieniami. Ale na przykład spójnik „i" w języku polskim może też sugerować następstwo czasowe[6] zdarzeń: *„Poszedł i zrobił."* A wyrażenie *„A, chyba że B"* ma inny odcień znaczeniowy niż proste *„A lub B"*. Przy tej okazji zwróćmy uwagę na to, że słowo *„albo"* bywa czasem rozumiane w znaczeniu alternatywy wykluczającej. My jednak umawiamy się, że rozumiemy je tak samo jak *„lub"*.

Konfuzje składniowe

Przy tłumaczeniu z języka polskiego na język logiki formalnej i na odwrót można łatwo popełnić błąd nawet wtedy gdy nie powstają problemy semantyczne. Składnia tych języków jest oparta na innych zasadach. Na przykład te dwa zdania mają bardzo podobną budowę:

[6] W językach programowania jest podobnie, ale to już inna historia.

Każdy kot ma wąsy.
Pewien kot ma wąsy.

Ale ich tłumaczenia na język rachunku predykatów nie są już takie podobne:

$$\forall x(Kot(x) \to MaWąsy(x));$$
$$\exists x(Kot(x) \wedge MaWąsy(x)).$$

Dość częstym błędem jest właśnie mylenie koniunkcji z implikacją w zasięgu działania kwantyfikatora. A oto inny przykład: Zdania

Liczba n jest parzysta;

Liczba n jest dwukrotnością pewnej liczby

oznaczają to samo. Zaprzeczeniem pierwszego z nich jest oczywiście zdanie

Liczba n nie jest parzysta,

ale zaprzeczeniem drugiego nie jest zdanie

Liczba n nie jest dwukrotnością pewnej liczby,

otrzymane przecież przez analogiczną operację „podstawienia". Użycie słowa „pewnej" powoduje bowiem, że to zdanie rozumiemy jako $\exists x(\neg n = 2x)$, a nie jako $\neg\exists x(n = 2x)$.

Innym popularnym błędem jest mylenie koniunkcji z alternatywą w przesłance implikacji, zwłaszcza gdy występuje tam negacja. Mamy bowiem skłonność do powtarzania słowa „nie" w obu członach założenia i nie razi nas zdanie

Kto nie ma biletu lub nie jest pracownikiem teatru, ten nie wejdzie na przedstawienie.

Ale od tekstu matematycznego oczekujemy więcej ścisłości i w takim tekście zdanie:

Jeśli x nie jest równe 2 *lub nie jest równe* 3*, to* $x^2 - 5x + 6$ *nie jest zerem.*

może wprowadzić czytelnika w błąd. „Dosłowne" tłumaczenie tego zdania na język logiki predykatów, to przecież formuła

$$\neg(x = 2) \vee \neg(x = 3) \to \neg(x^2 - 5x + 6 = 0),$$

a nie formuła

$$\neg(x = 2 \vee x = 3) \to \neg(x^2 - 5x + 6 = 0).$$

Wielu takich dwuznaczności unikniemy, gdy przypomnimy sobie, że w języku polskim istnieją takie słowa jak *ani* i *żaden*.

3.2 Siła wyrazu logiki pierwszego rzędu

Język logiki pierwszego rzędu, dzięki możliwości używania kwantyfikatorów, jest dość elastyczny. Można z jego pomocą wyrazić wiele nietrywialnych własności obiektów matematycznych. W szczególności interesować nas może *definiowanie* elementów i wyodrębnianie struktur

o pewnych szczególnych własnościach, czy też formułowanie kryteriów *odróżniających* jakieś struktury od innych.

Przykład 3.5 Przypuśćmy, że sygnatura składa się z dwóch jednoargumentowych symboli relacyjnych R i S i dwuargumentowego symbolu funkcyjnego f. Wtedy formuła

$$\forall x \forall y (R(x) \wedge S(y) \rightarrow R(f(x,y)) \wedge S(f(x,y))$$

jest prawdziwa dokładnie w tych modelach $\mathcal{A} = \langle A, f^{\mathcal{A}}, R^{\mathcal{A}}, S^{\mathcal{A}} \rangle$, w których obraz iloczynu kartezjańskiego $R^{\mathcal{A}} \times S^{\mathcal{A}}$ przy przekształceniu f zawiera się w zwykłym iloczynie $R^{\mathcal{A}} \cap S^{\mathcal{A}}$.

Przykład 3.6 Teraz niech nasza sygnatura składa się z jednej operacji dwuargumentowej $\cdot$ i z jednej stałej ε. Zdanie

$$\exists x_1 \exists x_2 \forall y (\forall z_1 \forall z_2 (y = z_1 \cdot z_2 \rightarrow y = z_1 \vee y = z_2) \rightarrow y = x_1 \vee y = x_2 \vee y = \varepsilon)$$

jest prawdziwe w strukturze $\langle \{a,b\}^*, \cdot, \varepsilon \rangle$ słów nad alfabetem $\{a,b\}^*$ z konkatenacją i słowem pustym, ale nie w modelu słów nad alfabetem trzyliterowym $\langle \{a,b,c\}^*, \cdot, \varepsilon \rangle$. Inaczej mówiąc, nasze zdanie *rozróżnia* te dwie struktury.

3.3 Nierozstrzygalność

Niestety, konsekwencją znacznej siły wyrazu logiki pierwszego rzędu jest jej nierozstrzygalność. Dokładniej, nierozstrzygalny jest następujący problem decyzyjny:[7] *Czy dana formuła logiki pierwszego rzędu jest tautologią?* Aby wykazać, że tak jest, posłużymy się znaną nam nierozstrzygalnością problemu stopu dla maszyn Turinga.

Przypomnijmy, że (deterministyczną, jednotaśmową) *maszynę Turinga nad alfabetem* $\mathcal{A}$ można zdefiniować jako krotkę $\mathcal{M} = \langle \Delta, Q, \delta, q_0, q_a \rangle$, gdzie:

- Δ jest skończonym alfabetem, zawierającym $\mathcal{A}$ oraz symbol $\mathsf{B} \notin \mathcal{A}$ (blank);
- Q jest skończonym zbiorem *stanów*;
- $q_0 \in Q$ jest stanem *początkowym*;
- $q_f \in Q$ jest stanem *końcowym* lub *akceptującym*;
- $\delta : (Q - \{q_f\}) \times \Delta \rightarrow \Delta \times Q \times \{-1, 0, +1\}$ jest *funkcją przejścia*.

Zakładając, że zbiory Δ i Q są rozłączne, można zdefiniować *konfigurację* maszyny jako słowo postaci wqv, gdzie $q \in Q$ oraz $w, v \in \Delta^*$, przy czym utożsamiamy konfiguracje wqv i $wqv\mathsf{B}$. Interpretacja tej definicji jest następująca. Taśma maszyny jest nieskończona w prawo. Na początku taśmy zapisane jest słowo wv, dalej w prawo są same blanki, a głowica maszyny „patrzy" na pierwszy znak na prawo od w. Konfigurację postaci $\mathcal{C}_w = q_0 w$, gdzie $w \in \mathcal{A}^*$, nazywamy *początkową*, a konfigurację postaci $wq_f v$ nazywamy *końcową* lub *akceptującą*.

[7] W istocie, nazwa „problem decyzyjny" (Entscheidungsproblem) została użyta po raz pierwszy właśnie w tym kontekście.

Relację $\rightarrow_{\mathcal{M}}$ na konfiguracjach definiuje się tak:

- Jeśli $\delta(q,a) = (b,p,+1)$ to $wqav \rightarrow_{\mathcal{M}} wbpv$;
- Jeśli $\delta(q,a) = (b,p,0)$ to $wqav \rightarrow_{\mathcal{M}} wpbv$;
- Jeśli $\delta(q,a) = (b,p,-1)$ to $wcqav \rightarrow_{\mathcal{M}} wpcbv$ oraz $qav \rightarrow_{\mathcal{M}} pbv$ (gdy ruch w lewo jest niemożliwy.)

Symbolem $\twoheadrightarrow_{\mathcal{M}}$ oznaczamy przechodnio-zwrotne domknięcie relacji $\rightarrow_{\mathcal{M}}$. Jeżeli $\mathcal{C}_w \twoheadrightarrow_{\mathcal{M}} \mathcal{C}'$, gdzie $\mathcal{C}'$ jest konfiguracją akceptującą to mówimy, że maszyna *akceptuje* słowo w.

W naszej konstrukcji skorzystamy z następującej postaci problemu stopu: *Czy dana maszyna Turinga akceptuje słowo puste?* Nietrudno jest zredukować do niego ogólny przypadek problemu stopu (ćwiczenie).

Następujący lemat będzie przydatny w dowodzie nierozstrzygalności.

Lemat 3.7 *Niech ϑ oznacza koniunkcję następujących formuł*

- $\forall y \neg P(y,c)$
- $\forall x \exists y P(x,y)$
- $\forall x \forall y (P(x,y) \rightarrow R(x,y))$
- $\forall x \forall y \forall z (R(x,y) \rightarrow (R(y,z) \rightarrow R(x,z)))$
- $\forall x \neg R(x,x)$

Zdanie ϑ jest spełnialne, a każdy jego model $\mathfrak{A}$ zawiera nieskończony ciąg różnych elementów $c^{\mathfrak{A}} = a_0, a_1, a_2, \ldots$, takich że $(a_i, a_{i+1}) \in P^{\mathfrak{A}}$ dla każdego i.

Dowód: Ćwiczenie. ∎

Twierdzenie 3.8 *Nie istnieje algorytm rozstrzygający czy dana formuła logiki pierwszego rzędu jest tautologią.*

Dowód: Naszym celem jest efektywna konstrukcja, która dla dowolnej maszyny Turinga $\mathcal{M}$ utworzy formułę $\varphi_{\mathcal{M}}$ o takiej własności:

$$\mathcal{M} \textit{ akceptuje słowo puste} \quad \text{wtedy i tylko wtedy, gdy} \quad \varphi_{\mathcal{M}} \textit{ jest tautologią.}$$

Stąd natychmiast wynika teza twierdzenia. W przeciwnym razie taka konstrukcja pozwalałaby bowiem na rozstrzyganie problemu stopu.

W istocie, wygodniej będzie skonstruować taką formułę $\psi_{\mathcal{M}}$, że

$$\mathcal{M} \textit{ zapętla się na słowie pustym} \quad \text{wtedy i tylko wtedy, gdy} \quad \psi_{\mathcal{M}} \textit{ jest spełnialna,}$$

i na koniec przyjąć $\varphi_{\mathcal{M}} = \neg\psi_{\mathcal{M}}$. Sygnatura naszej formuły będzie zależała od maszyny $\mathcal{M}$ (bo tak jest łatwiej) chociaż tak być nie musi (Ćwiczenie 13). Składa się ona z:

- jednoargumentowych symboli relacyjnych S_q, dla wszystkich stanów $q \in Q$;
- dwuargumentowych symboli relacyjnych C_a, dla wszystkich symboli $a \in \Delta$;
- dwuargumentowego symbolu relacyjnego G;
- stałej c i symboli P i Q występujących w formule ϑ z Lematu 3.7.

Formuła $\varphi_{\mathcal{M}}$ jest koniunkcją złożoną z wielu składowych, które teraz opiszemy. Pierwszą składową jest formuła ϑ z Lematu 3.7. Każdy model tej formuły zawiera różnowartościowy ciąg $a_0, a_1, a_2, \ldots$, który posłuży nam jako substytut ciągu liczb naturalnych (o elemencie a_i myślimy jak o liczbie i). Intuicyjny sens formuł atomowych naszej sygnatury jest taki:

- Formułę $S_q(x)$ czytamy: po x krokach obliczenia maszyna jest w stanie q.
- Formułę $G(x, y)$ czytamy: po x krokach głowica maszyny znajduje się w pozycji y.
- Formułę $C_a(x, y)$ czytamy: po x krokach na pozycji y znajduje się symbol a.

Dalsze składowe naszej formuły $\varphi_{\mathcal{M}}$ są tak dobrane, aby każdy jej model reprezentował nieskończone obliczenie maszyny zaczynające się od słowa pustego. Oto te składowe:

1. $S_{q_0}(c) \wedge G(c, c) \wedge \forall x\, C_{\mathsf{B}}(c, x)$;
2. $\forall x(\bigvee_{q \in Q} S_q(x))$;
3. $\forall x(S_q(x) \to \neg S_p(x))$, dla $q, p \in Q$, $q \neq p$;
4. $\forall x \forall y(\bigvee_{a \in \Delta} C_a(x, y))$;
5. $\forall x \forall y(C_a(x, y) \to \neg C_b(x, y))$, dla $a, b \in \Delta$, $a \neq b$;
6. $\forall x \exists y\, G(x, y)$;
7. $\forall x \forall y \forall z(G(x, y) \wedge G(x, z) \to y = z)$;
8. $\forall x \forall y \forall z(S_q(x) \wedge G(x, y) \wedge C_a(x, y) \wedge P(x, z) \to S_p(z) \wedge C_b(z, y))$, gdy $\delta(q, a) = (p, b, i)$;
9. $\forall x \forall y \forall z(\neg G(x, y) \wedge C_a(x, y) \wedge P(x, z) \to C_a(z, y))$;
10. $\forall x \forall y \forall z \forall v(S_q(x) \wedge G(x, y) \wedge P(x, z) \wedge P(y, v) \to G(z, v))$, gdy $\delta(q, a) = (p, b, +1)$;
11. $\forall x \forall y \forall z(S_q(x) \wedge G(x, y) \wedge P(x, z) \to G(z, y))$, gdy $\delta(q, a) = (p, b, 0)$;
12. $\forall x \forall y \forall z \forall v(S_q(x) \wedge G(x, y) \wedge P(x, z) \wedge P(v, y) \to G(z, v))$, gdy $\delta(q, a) = (p, b, -1)$;
13. $\forall x \forall y \forall z \forall v(S_q(x) \wedge G(x, c) \wedge P(x, z) \to G(z, c))$, gdy $\delta(q, a) = (p, b, -1)$;
14. $\forall x \neg S_{q_f}(x)$.

Przypuśćmy teraz, że maszyna $\mathcal{M}$ ma nieskończone obliczenie dla pustego słowa wejściowego. Zbudujemy model $\mathfrak{A}$ dla formuły $\varphi_{\mathcal{M}}$. Dziedziną tego modelu jest zbiór $\mathbb{N}$ liczb naturalnych. Stałą c interpretujemy jako zero, relacja $P^{\mathfrak{A}}$ to relacja następnika, a $R^{\mathfrak{A}}$ to (ostra) relacja

mniejszości. Relacje $S_q^{\mathcal{A}}$, $C_a^{\mathcal{A}}$ i $G^{\mathcal{A}}$ określamy zgodnie z ich intuicyjną interpretacją na podstawie przebiegu nieskończonego obliczenia maszyny. Nietrudno się przekonać, że wszystkie człony koniunkcji są prawdziwe w $\mathfrak{A}$, czyli zdanie $\varphi_{\mathcal{M}}$ jest spełnialne.

Przystąpmy więc do trudniejszej części dowodu. Załóżmy mianowicie, że $\mathfrak{A} \models \varphi_{\mathcal{M}}$ dla pewnej struktury $\mathfrak{A}$. Wtedy także $\mathfrak{A} \models \vartheta$, niech więc a_i będą elementami $\mathfrak{A}$, o których mowa w Lemacie 3.7. Struktura $\mathfrak{A}$ spełnia też wszystkie pozostałe składowe formuły $\varphi_{\mathcal{M}}$. Składowe (2) i (3) gwarantują, że każdy z elementów a_i należy do dokładnie jednej z relacji S_q. Podobnie, każda para (a_i, a_j) należy do dokładnie jednej z relacji C_a, oraz każde a_i jest w relacji G z dokładnie jednym elementem struktury $\mathfrak{A}$ — tu używamy składowych (4)–(7).

Rozpatrzmy obliczenie maszyny $\mathcal{M}$ dla słowa pustego. Pokażemy, że jest to obliczenie nieskończone.

Jeśli obliczenie maszyny $\mathcal{M}$ składa się z co najmniej n kroków, to przez q_n oznaczmy stan, w którym znajduje się maszyna $\mathcal{M}$ po wykonaniu tych n kroków, a przez k_n pozycję głowicy w tym momencie. Zawartością m-tej komórki taśmy po n-tym kroku obliczenia niech zaś będzie symbol b_{nm}.

Przez indukcję ze względu na n dowodzimy, że dla dowolnego $n \in \mathbb{N}$ obliczenie składa się z co najmniej n kroków, oraz:

$$a_n \in S_{q_n}^{\mathfrak{A}} \qquad (a_n, a_m) \in C_{b_{nm}}^{\mathfrak{A}} \qquad (a_n, a_{k_n}) \in G^{\mathfrak{A}}.$$

Inaczej mówiąc, model $\mathfrak{A}$ prawidłowo reprezentuje kolejne konfiguracje maszyny. Dla $n = 0$ powyższe związki wynikają wprost z prawdziwości członu (1) naszej koniunkcji. W kroku indukcyjnym skorzystamy przede wszystkim z członu (14), który gwarantuje, że stan q_n nie jest końcowy. Określona jest więc wartość funkcji przejścia $\delta(q_n, b_{mk_n})$. Możemy więc odwołać się do składowych (9–12), które zapewniają poprawną zmianę stanu i symbolu pod głowicą (8), zachowanie bez zmian reszty taśmy (9) i przesunięcie głowicy (10–12). Szczegóły dowodu pozostawiamy Czytelnikowi. ∎

Twierdzenie 3.8 można wzmocnić, pokazując (Ćwiczenie 13), że problem jest nierozstrzygalny nawet dla formuł nad pewną ustaloną sygnaturą. W istocie, jest tak dla większości sygnatur, z wyjątkiem bardzo „ubogich" przypadków. Dwa takie przypadki są przedmiotem Ćwiczeń 3 i 5 do Rozdziału 13.

Ćwiczenia

1. Stosując schematy (6–9) z Faktu 3.1, pokazać, że następujące formuły są tautologiami:
   (a) $(\exists y p(y) \to \forall z q(z)) \to \forall y \forall z (p(y) \to q(z))$;
   (b) $(\forall x \exists y r(x, y) \to \exists x \forall y r(y, x)) \to \exists x \forall y (r(x, y) \to r(y, x))$;
   (c) $\forall x \exists y ((p(x) \to q(y)) \to r(y)) \to ((\forall x p(x) \to \forall y q(y)) \to \exists y r(y))$;
   (d) $\forall x (p(x) \to \exists y q(y)) \to \exists y (\exists x p(x) \to q(y))$.
2. Jak rozumiesz następujące zdania? Jak je sformułować, żeby nie budziły wątpliwości?
   (a) *Nie wolno pić i grać w karty.*
   (b) *Nie wolno pluć i łapać.*

(c) *Zabrania się zaśmiecania i zanieczyszczania drogi.*[8]

(d) *Zabrania się zaśmiecania lub zanieczyszczania drogi.*[9]

(e) *Wpisać, gdy osoba ubezpieczona nie posiada numerów identyfikacyjnych NIP lub PESEL.*[10]

(f) *Podaj przykład liczby, która jest pierwiastkiem pewnego równania kwadratowego o współczynnikach całkowitych i takiej, która nie jest.*

(g) *Warunek zachodzi dla każdego x i dla pewnego y.*

3. Czy następujące definicje można lepiej sformułować?

   (a) *Zbiór A jest* dobry*, jeśli ma co najmniej 2 elementy.*

   (b) *Zbiór A jest* dobry*, jeśli dla każdego $x \in A$, jeśli x jest parzyste, to x jest podzielne przez* 3.

   (c) *Zbiór A jest* dobry*, jeśli dla pewnego $x \in A$, jeśli x jest parzyste, to x jest podzielne przez* 3.

4. Wskazać błąd w rozumowaniu:

   (a) *Aby wykazać prawdziwość tezy*
   „Dla dowolnego n, jeśli zachodzi warunek $W(n)$ to zachodzi warunek $U(n)$"
   załóżmy, że dla dowolnego n zachodzi $W(n)$...

   (b) *Aby wykazać prawdziwość tezy*
   „Dla pewnego n, jeśli zachodzi warunek $W(n)$ to zachodzi warunek $U(n)$"
   załóżmy, że dla pewnego n zachodzi $W(n)$...

5. Sformułować poprawnie zaprzeczenia stwierdzeń:

   - *Liczby m i n są pierwsze.*
   - *Liczby m i n są względnie pierwsze.*

6. Czy zdanie *„Liczba a nie jest kwadratem pewnej liczby całkowitej"*jest poprawnym zaprzeczeniem zdania *„Liczba a jest kwadratem pewnej liczby całkowitej"*?

7. Sygnatura Σ składa się z symboli $r, s \in \Sigma_1^R$, $R, S \in \Sigma_2^R$ i $g \in \Sigma_2^F$. Napisać takie zdania φ i ψ, że:

   (a) zdanie φ jest prawdziwe dokładnie w tych modelach $\mathcal{A} = \langle A, R^{\mathcal{A}}, S^{\mathcal{A}}, r^{\mathcal{A}}, s^{\mathcal{A}}, g^{\mathcal{A}} \rangle$, w których obie relacje $R^{\mathcal{A}}$, $S^{\mathcal{A}}$ są przechodnie, ale ich suma nie jest przechodnia;

   (b) zdanie ψ jest prawdziwe dokładnie w tych modelach $\mathcal{A} = \langle A, R^{\mathcal{A}}, S^{\mathcal{A}}, r^{\mathcal{A}}, s^{\mathcal{A}}, g^{\mathcal{A}} \rangle$, w których $s^{\mathcal{A}}$ jest obrazem iloczynu kartezjańskiego $r^{\mathcal{A}} \times r^{\mathcal{A}}$ przy funkcji $g^{\mathcal{A}}$.

8. Sygnatura Σ składa się z dwuargumentowych symboli relacyjnych r i s oraz dwuargumentowego symbolu funkcyjnego f. Napisać (możliwie najkrótsze) zdanie, które jest prawdziwe dokładnie w tych modelach$\mathcal{A} = \langle A, r^{\mathcal{A}}, s^{\mathcal{A}}, f^{\mathcal{A}} \rangle$, w których:

   (a) Złożenie relacji $r^{\mathcal{A}}$ i $s^{\mathcal{A}}$ zawiera się w ich iloczynie $r^{\mathcal{A}} \cap s^{\mathcal{A}}$;

   (b) Zbiór wartości funkcji $f^{\mathcal{A}}$ jest rzutem sumy $r^{\mathcal{A}} \cup s^{\mathcal{A}}$ na pierwszą współrzędną;

   (c) Relacja $r^{\mathcal{A}}$ nie jest funkcją z A w A;

   (d) Obraz $r^{\mathcal{A}}$ przy funkcji $f^{\mathcal{A}}$ jest podstrukturą w $\mathcal{A}$;

   (e) Obraz zbioru $A \times A$ przy funkcji $f^{\mathcal{A}}$ jest pusty.

9. Dla każdej z par struktur:

   (a) $\langle \mathbb{N}, \leq \rangle$ i $\langle \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}, \leq \rangle$;

[8] Kodeks Drogowy przed nowelizacją w roku 1997.
[9] Kodeks Drogowy po nowelizacji w roku 1997.
[10] Instrukcja wypełniania formularza ZUS ZCZA (Zgłoszenie danych o członkach rodziny...)

(b) $\langle \mathbb{N}, + \rangle$ i $\langle \mathbb{Z}, + \rangle$;

(c) $\langle \mathbb{N}, \leq \rangle$ i $\langle \mathbb{Z}, \leq \rangle$,

wskaż zdanie prawdziwe w jednej z nich a w drugiej nie.

10. Napisać takie zdania φ i ψ, że:

    (a) zdanie φ jest prawdziwe w modelu $\mathcal{A} = \langle \mathbb{Z}, +, 0 \rangle$, ale nie w modelu $\mathcal{B} = \langle \mathbb{N}, +, 0 \rangle$;

    (b) zdanie ψ jest prawdziwe w modelu $\mathcal{B} = \langle \mathbb{Z}, +, 0 \rangle$, ale nie w modelu $\mathcal{C} = \langle \mathbb{Q}, +, 0 \rangle$.

11. Wskazać formułę pierwszego rzędu:

    (a) spełnialną w ciele liczb rzeczywistych ale nie w ciele liczb wymiernych;

    (b) spełnialną w algebrze $\mathbb{N}$ z mnożeniem, ale nie w algebrze $\mathbb{N}$ z dodawaniem;

    (c) spełnialną w $\langle \{a, b\}^*, \cdot, \varepsilon \rangle$ ale nie w $\langle \{a, b, c\}^*, \cdot, \varepsilon \rangle$.

12. Zmodyfikować konstrukcję z dowodu Twierdzenia 3.8 w ten sposób, aby w formule $\psi_{\mathcal{M}}$ nie występował symbol równości ani stała c.

13. Zmodyfikować konstrukcję z dowodu Twierdzenia 3.8 w ten sposób, aby $\psi_{\mathcal{M}}$ była zawsze formułą ustalonej sygnatury (niezależnej od maszyny $\mathcal{M}$). Wywnioskować stąd, że logika pierwszego rzędu nad tą ustaloną sygnaturą jest nierozstrzygalna.

4 Ograniczenia logiki pierwszego rzędu

Ten rozdział poświęcony jest ograniczeniom, którym podlega język logiki pierwszego rzędu. Okazuje się, że nie każde pojęcie da się w nim wyrazić, a także, że są pojęcia, które dają się wyrazić, ale odpowiednie zdanie lub formuła z konieczności musi być skomplikowane. Rozważania w tym rozdziale będziemy prowadzić przy założeniu, że w sygnaturze występują wyłącznie symbole relacyjne. Wyniki dają się zastosować do sygnatur z symbolami funkcyjnymi, ale wymaga to zakodowania wszystkich funkcji jako relacji.

Zaczniemy od miary skomplikowania formuł, która będzie przydatna w dalszym ciągu.

Definicja 4.1 *Rangę kwantyfikatorową* $QR(\varphi)$ formuły φ definiujemy jak następuje:

- $QR(\bot) = QR(t_1 = t_2) = QR(r(t_1, \ldots, t_k)) = 0$ dla dowolnych termów $t_1, \ldots, t_k$ oraz $r \in \Sigma_k^R$.
- $QR(\varphi \to \psi) = \max(QR(\varphi), QR(\psi))$.
- $QR(\forall x \varphi) = 1 + QR(\varphi)$.

Intuicyjnie QR to głębokość zagnieżdżenia kwantyfikatorów w formule. Jest to jedna z wielu możliwych miar stopnia komplikacji formuły φ. Parametr ten ma następujące znaczenie: jeśli struktura $\mathfrak{A}$ ma n elementów, to pesymistyczny czas sprawdzenia, czy dla zdania φ zachodzi $\mathfrak{A} \models \varphi$ jest asymptotycznie proporcjonalny do $n^{QR(\varphi)}$, gdy użyjemy naturalnego algorytmu do wykonania tego zadania, który dla każdego kwantyfikatora w formule przegląda wszystkie elementy struktury.

Teraz możemy wyjaśnić, dlaczego nie dopuszczamy symboli funkcyjnych w sygnaturze. Otóż ich obecność zakłóca potrzebne nam własności funkcji QR. Tytułem przykładu, formuła $R(x, f(f(x)))$ jest atomowa i jej ranga kwantyfikatorowa powinna wynosić 0. Tymczasem gdy f będziemy reprezentować w strukturze jako dwuargumentową relację F, ta sama formuła przybierze postać $\exists y \exists z (F(x, y) \wedge F(y, z) \wedge R(x, z))$, której ranga kwantyfikatorowa wynosi 2. Twierdzenia, których dalej dowodzimy, odwołują się do wartości QR zdefiniowanych powyżej dla logiki bez symboli funkcyjnych. To właśnie jest przyczyna, dla której funkcje wykluczamy z rozważań.

4.1 Charakteryzacja Fraïssé

Definicja 4.2 Jeśli $\mathfrak{A}$ jest strukturą relacyjną oraz $\emptyset \neq B \subseteq A$, to struktura $\mathfrak{A}_{|B}$ tej samej sygnatury Σ co $\mathfrak{A}$, nazywana *podstrukturą indukowaną przez* B *w* $\mathfrak{A}$, ma nośnik B, zaś dla każdego $r \in \Sigma_n^R$

$$r^{\mathfrak{A}_{|B}} = r^{\mathfrak{A}} \cap B^n.$$

Definicja 4.3 Niech $\mathfrak{A}, \mathfrak{B}$ będą strukturami relacyjnymi tej samej sygnatury Σ, ponadto niech $A' \subseteq A$ i $B' \subseteq B$. Jeśli funkcja $h : A' \to B'$ jest izomorfizmem podstruktur indukowanych $h : \mathfrak{A}_{|A'} \cong \mathfrak{B}_{|B'}$, to mówimy, że h jest *częściowym izomorfizmem z* $\mathfrak{A}$ *w* $\mathfrak{B}$. Jego *dziedzina* to $dom(h) = A'$, a *obraz* to $rg(h) = B'$.

Na zasadzie konwencji umawiamy się, że $\emptyset$ jest częściowym izomorfizmem z $\mathfrak{A}$ w $\mathfrak{B}$ o pustej dziedzinie i pustym obrazie.

Dla dwóch częściowych izomorfizmów g, h z $\mathfrak{A}$ w $\mathfrak{B}$ piszemy $g \subseteq h$ gdy $dom(g) \subseteq dom(h)$ oraz $g(a) = h(a)$ dla wszystkich $a \in dom(g)$, to jest wtedy, gdy g jest zawarte jako zbiór w h.

Definicja 4.4 Niech m będzie dodatnią liczbą naturalną. Dwie struktury relacyjne tej samej sygnatury są *m-izomorficzne*, co oznaczamy $\mathfrak{A} \cong_m \mathfrak{B}$, gdy istnieje rodzina $\{I_n \mid n \leq m\}$ w której każdy I_n jest niepustym zbiorem częściowych izomorfizmów z $\mathfrak{A}$ w $\mathfrak{B}$, oraz spełniająca następujące dwa warunki:

Tam Dla każdego $h \in I_{n+1}$ oraz każdego $a \in A$ istnieje takie $g \in I_n$, że $h \subseteq g$ oraz $a \in dom(g)$.

Z powrotem Dla każdego $h \in I_{n+1}$ oraz każdego $b \in B$ istnieje takie $g \in I_n$, że $h \subseteq g$ oraz $b \in rg(g)$.

Samą rodzinę $\{I_n \mid n \leq m\}$ nazywamy wówczas *m-izomorfizmem* struktur $\mathfrak{A}$ i $\mathfrak{B}$, co oznaczamy $\{I_n \mid n \leq m\} : \mathfrak{A} \cong_m \mathfrak{B}$.

Nieformalne wyjaśnienie jest takie: I_n to zbiór częściowych izomorfizmów, które mogą być rozszerzone n-krotnie o dowolne elementy w dziedzinie i obrazie, a kolejne rozszerzenia leżą w $I_{n-1}, \ldots, I_0$.

Definicja 4.5 Dwie struktury relacyjne tej samej sygnatury są *skończenie izomorficzne*, symbolicznie $\mathfrak{A} \cong_{fin} \mathfrak{B}$, gdy istnieje rodzina $\{I_n \mid n \in \omega\}$, taka, że każda podrodzina $\{I_n \mid n \leq m\}$ jest m-izomorfizmem.

Jeśli $\{I_n \mid n \leq m\}$ ma powyższe własności, to piszemy $\{I_n \mid n \leq m\} : \mathfrak{A} \cong_{fin} \mathfrak{B}$, a samą rodzinę nazywamy *skończonym izomorfizmem.*

Fakt 4.6

- *Jeśli* $\mathfrak{A} \cong \mathfrak{B}$, *to* $\mathfrak{A} \cong_{fin} \mathfrak{B}$.
- *Jeśli* $\mathfrak{A} \cong_{fin} \mathfrak{B}$ *oraz nośnik* $\mathfrak{A}$ *jest zbiorem skończonym, to* $\mathfrak{A} \cong \mathfrak{B}$.

Dowód: Ćwiczenie. ∎

Definicja 4.7 Dwie struktry $\mathfrak{A}$ i $\mathfrak{B}$ tej samej sygnatury są *elementarnie równoważne*, co zapisujemy symbolicznie $\mathfrak{A} \equiv \mathfrak{B}$, gdy dla każdego zdania φ logiki pierwszego rzędu nad tą samą sygnaturą, $\mathfrak{A} \models \varphi$ wtedy i tylko wtedy, gdy $\mathfrak{B} \models \varphi$.

Dwie struktry $\mathfrak{A}$ i $\mathfrak{B}$ tej samej sygnatury są *m-elementarnie równoważne*, symbolicznie $\mathfrak{A} \equiv_m \mathfrak{B}$, gdy dla każdego zdania φ logiki pierwszego rzędu nad tą samą sygnaturą, o randze kwantyfikatorowej nie przekraczającej m, zachodzi $\mathfrak{A} \models \varphi$ wtedy i tylko wtedy, gdy $\mathfrak{B} \models \varphi$.

Fakt 4.8 $\mathfrak{A} \cong_{fin} \mathfrak{B}$ *wtedy i tylko wtedy, gdy dla każdego naturalnego* m *zachodzi* $\mathfrak{A} \cong_m \mathfrak{B}$.

Dowód: Wynikanie z lewej do prawej jest oczywiste. Załóżmy teraz, że dla każdego m istnieje rodzina $\{I_n^m \mid n \leq m\}$ spełniająca warunki z definicji relacji $\cong_m$. Rozważmy rodzinę $\{J_n \mid n \in \omega\}$, gdzie $J_n = \bigcup_{m \in \omega} I_n^m$. Bezpośrednie sprawdzenie pokazuje natychmiast, że spełnia ona warunki definicji relacji $\cong_{fin}$. ∎

Twierdzenie 4.9 (Fraïssé) *Niech* Σ *będzie dowolną sygnaturą relacyjną zawierającą skończenie wiele symboli, oraz niech* $\mathfrak{A}, \mathfrak{B}$ *będą dowolnymi strukturami nad* Σ.

- *Dla każdego* $m \in \mathcal{N}$ *zachodzi równoważność:* $\mathfrak{A} \cong_m \mathfrak{B}$ *wtedy i tylko wtedy gdy* $\mathfrak{A} \equiv_m \mathfrak{B}$.
- $\mathfrak{A} \cong_{fin} \mathfrak{B}$ *wtedy i tylko wtedy gdy* $\mathfrak{A} \equiv \mathfrak{B}$.

Dowód: Jest oczywiste, że druga równoważnośc wynika z pierwszej. Pierwszą z kolei udowodnimy tylko z lewej do prawej strony. Dowód w stronę przeciwną jest bardziej zawiły technicznie, a w dodatku ta implikacja jest rzadko używana w praktyce. Wyraża za to istotną z metodologicznego punktu widzenia informację: jeśli dwie struktury są (m-)elementarnie równoważne, to fakt ten można na pewno udowodnić posługując się metodą Fraïssé, choć oczywiście nie ma gwarancji, że będzie to metoda najprostsza.

Ustalmy $m \in \mathcal{N}$. Dowód tego, że z $\mathfrak{A} \cong_m \mathfrak{B}$ wynika $\mathfrak{A} \equiv_m \mathfrak{B}$ sprowadza się do wykazania następującego faktu za pomocą indukcji ze względu na budowę φ:

> *Niech* $\{I_n \mid n \leq m\}$ *będzie rodziną o której mowa w definicji* $\mathfrak{A} \cong_m \mathfrak{B}$*, niech* φ *będzie formułą o co najwyżej* r *zmiennych wolnych (bez utraty ogólności niech będą to* $x_1, \ldots, x_r$*) i spełniającą* $QR(\varphi) \leq n \leq m$ *oraz niech* $g \in I_n$*. Wówczas dla dowolnych* $a_1, \ldots, a_r \in dom(g)$ *następujące dwa warunki są równoważne:*
>
> $$\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r \models \varphi$$
>
> $$\mathfrak{B}, x_1 : g(a_1), \ldots, x_r : g(a_r) \models \varphi.$$

Dla formuł atomowych, powyższa teza wynika wprost z faktu, że g jest częściowym izomorfizmem (przypomnijmy że w sygnaturze nie ma symboli funkcyjnych i co za tym idzie jedynymi termami są zmienne).

Gdy φ ma postać $\psi \to \xi$, to mamy następujący ciąg równoważnych warunków:

- $\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r \models \psi \to \xi$
- $\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r \not\models \psi$ lub $\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r \models \xi$
- $\mathfrak{A}, x_1 : g(a_1), \ldots, x_r : g(a_r) \not\models \psi$ lub $\mathfrak{A}, x_1 : g(a_1), \ldots, x_r : g(a_r) \models \xi$

- $\mathfrak{A}, x_1 : g(a_1), \ldots, x_r : g(a_r) \models \psi \to \xi$,

przy czym druga równoważność wynika z założenia indukcyjnego, a pierwsza i trzecia z definicji semantyki.

Gdy φ ma postać $\forall x\psi$, to, jako że $x_{r+1} \notin FV(\varphi)$ i co za tym idzie $\models (\forall x\psi) \leftrightarrow \forall x_{r+1}\psi(x_{r+1}/x)$ (patrz Fakt 2.12), możemy bez utraty ogólności założyć, że φ ma postać $\forall x_{r+1}\psi$. Z założenia $QR(\varphi) \leq n$ wynika, że $QR(\psi) \leq n-1$. Mamy teraz następujący ciąg równoważnych warunków:

- $(\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r) \models \varphi$
- Dla każdego $a \in A$ zachodzi $(\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r, x_{r+1} : a) \models \psi$
- Dla każdego $a \in A$ istnieje takie $h \in I_{n-1}$, że $g \subseteq h$, $a \in dom(h)$ oraz $(\mathfrak{A}, x_1 : a_1, \ldots, x_r : a_r, x_{r+1} : a) \models \psi$
- Dla każdego $a \in A$ istnieje takie $h \in I_{n-1}$, że $g \subseteq h$, $a \in dom(h)$ oraz $(\mathfrak{B}, x_1 : g(a_1), \ldots, x_r : g(a_r), x_{r+1} : h(a)) \models \psi$
- Dla każdego $b \in B$ istnieje takie $h \in I_{n-1}$, że $g \subseteq h$, $b \in rg(h)$ oraz $(\mathfrak{B}, x_1 : g(a_1), \ldots, x_r : g(a_r), x_{r+1} : b) \models \psi$
- Dla każdego $b \in B$ zachodzi $(\mathfrak{B}, x_1 : g(a_1), \ldots, x_r : g(a_r), x_{r+1} : b) \models \psi$
- $(\mathfrak{B}, x_1 : g(a_1), \ldots, x_r : g(a_r)) \models \varphi$.

Równoważności druga i czwarta zachodzą na mocy warunków **Tam** i **Z powrotem**, trzecia na mocy założenia indukcyjnego, a pozostałe na mocy definicji spełniania. ∎

Pokażemy teraz pierwszy przykład inherentnego ograniczenia logiki pierwszego rzędu.

Fakt 4.10 *Jeśli $\mathfrak{A}, \mathfrak{B}$ są dwoma skończonymi liniowymi porządkami o mocach większych niż 2^m, to $\mathfrak{A} \equiv_m \mathfrak{B}$.*

Dowód: Bez utraty ogólności możemy założyć, że $A = \{0, \ldots, N\}$, $B = \{0, \ldots, M\}$, przy czym $2^m < N \leq M$, a porządek jest porządkiem naturalnym. Dowód przeprowadzamy wykorzystując Twierdzenie 4.9, czyli w istocie wykazujemy, że $\mathfrak{A} \cong_m \mathfrak{B}$.

Dla danego $k \leq m$ określmy „odległość" d_k pomiędzy elementami naszych struktur jak następuje:

$$d_k(a,b) = \begin{cases} |b-a| & \text{jeśli } |b-a| < 2^k \\ \infty & \text{wpp.} \end{cases}$$

Niech I_k dla $k \leq m$ będzie zbiorem wszystkich częściowych izomorfizmów g z $\mathfrak{A}$ w $\mathfrak{B}$ takich, że $\{\langle 0,0\rangle, \langle N,M\rangle\} \subseteq g$ oraz $d_k(a,b) = d_k(g(a), g(b))$ dla wszystkich $a, b \in dom(g)$. Oczywiście $I_k \neq \emptyset$ bo $\{\langle 0,0\rangle, \langle N,M\rangle\} \in I_k$.

Pokazujemy własność **Tam** dla rodziny $\{I_k \mid k \leq m\}$. Niech $g \in I_{k+1}$. Niech $a \in \{0, \ldots, N\}$. Mamy wskazać w I_k częściowy izomorfizm $h \supseteq g$ taki, że $a \in dom(h)$.

Rozróżniamy dwa przypadki:

(i) Jeśli istnieje takie $b \in dom(g)$, że $d_k(a, b) < \infty$, to w B jest dokładnie jeden element a', który jest tak samo położony względem $g(b)$ jak a względem b, oraz spełnia $d_j(a', g(b)) = d_j(a, b)$. Kładziemy wówczas $h(a) := a'$ i h jest wtedy częściowym izomorfizmem zachowującym odległości d_j.

(ii) Jeśli natomiast takiego b nie ma, to niech $a' < a < a''$, gdzie a', a'' są najbliższymi b elementami po lewej i po prawej, które należą do $dom(g)$. Wówczas $d_j(a', a) = d_j(a, a'') = \infty$, co w myśl definicji d_j oznacza, że $d_{j+1}(a', a'') = \infty$. Zatem na mocy założenia indukcyjnego także $d_{j+1}(g(a'), g(a'')) = \infty$. Istnieje więc $g(a') < b < g(a'')$ takie, że $d_j(g(a'), b) = d_j(b, g(a'')) = \infty$, i wówczas kładąc $h(a) := b$ uzyskujemy żądane rozszerzenie. ∎

Przykład powyższy wskazuje na kilka istotnych ograniczeń logiki pierwszego rzędu. Po pierwsze, nie da się żadnym zdaniem zdefiniować nawet tak prostego pojęcia jak „porządek liniowy o parzystej liczbie elementów", i to bez względu na to, jak byśmy je rozumieli dla modeli nieskończonych. Istotnie, zdanie które miałoby definiować taką własność musiałoby mieć jakąś rangę kwantyfikatorową, powiedzmy q. Jednak w myśl poprzedniego twierdzenia, porządki o mocach $2^q + 1$ i $2^q + 2$ są q-elementarnie równoważne i nasze hipotetyczne zdanie jest albo prawdziwe w obu, albo fałszywe w obu, podczas gdy powinno być w jednym fałszywe, a w drugim prawdziwe.

Drugim ograniczeniem jest fakt, że każda specyfikacja porządku liniowego o mocy n w logice pierwszego rzędu musi z konieczności mieć rangę kwantyfikatorową co najmniej $\log_2 n$, a więc sugeruje algorytm sprawdzenia, czy dany obiekt mocy m istotnie spełnia tę specyfikację, którego czas działania ma rząd wielkości $m^{\log_2 n}$, co jest wynikiem fatalnym.[11] Bierze się to stąd, że prawdziwość zdania o randze kwantyfikatorowej q sprawdza się w danej skończonej strukturze za pomocą q zagnieżdżonych pętli, z których każda przegląda cały nośnik struktury i odpowiada jednemu kwantyfikatorowi.

4.2 Gra Ehrenfeuchta

Charakteryzacja Fraïssé jest dość skomplikowana i odpychająca w bezpośrednim użyciu. W praktyce jej popularność ogromnie zwiększyło podanie przez Andrzeja Ehrenfeuchta jej równoważnego opisu w terminach dwuosobowej gry, którą teraz zdefiniujemy. Gra ta doskonale sprawdza się w rozumowaniach intuicyjnych. Praktyczne doświadczenie wskazuje, że próby napisania bardzo formalnego dowodu przy użyciu gry kończą się zwykle wskazaniem rodziny zbiorów częściowych izomorfizmów w duchu Fraïssé.

Niech Σ będzie sygnaturą relacyjną i niech $\mathfrak{A}, \mathfrak{B}$ będą strukturami sygnatury Σ.

Dla uproszczenia zakładamy, że $A \cap B = \emptyset$.

[11] Na szczęście znamy lepsze algorytmy wykonujące to zadanie.

Definicja 4.11 *Gra Ehrenfeuchta* $G_m(\mathfrak{A}, \mathfrak{B})$ jest rozgrywana przez dwóch graczy, oznaczanych I i II. Trwa ona przez m rund.

W i-tej rundzie ($i = 1, \ldots, m$) najpierw wykonuje ruch gracz I, wybierając jedną ze struktur oraz jeden z elementów jej nośnika. Jest on oznaczany a_i jeśli pochodzi z A, zaś b_i, jeśli z B. Jako drugi wykonuje ruch gracz II, który musi wybrać element w pozostałej strukturze (czyli w $\mathfrak{A}$, jeśli I wybrał element w $\mathfrak{B}$, oraz w $\mathfrak{B}$, jeśli I wybrał element w $\mathfrak{A}$) i oznaczyć go a_i lub b_i, zależnie od tego, skąd wybierał.

W ciągu m rund wybrane zostają elementy $a_1, \ldots, a_m \in A$ oraz $b_1, \ldots, b_m \in B$.

Gracz II wygrywa rozgrywkę, jeśli funkcja $h = \{\langle a_i, b_i \rangle \mid i = 1, \ldots, m\}$ jest częściowym izomorfizmem z $\mathfrak{A}$ w $\mathfrak{B}$. W przeciwnym wypadku wygrywa gracz I.

Mówimy, że gracz II ma *strategię wygrywającą* w grze $G_m(\mathfrak{A}, \mathfrak{B})$, jeśli może wygrać każdą rozgrywkę, niezależnie od posunięć gracza I.

Definicja powyższa dopuszcza powtarzanie ruchów przez obu graczy, czyli wybieranie elementów, które poprzednio były już wybrane. Jest to dogodne, gdyż upraszcza definicję. Gdybyśmy bowiem zakazali tego, to albo niemożliwe byłoby rozegranie gry $G_m(\mathfrak{A}, \mathfrak{B})$ gdy choć jedna ze struktur ma moc mniejszą niż m, albo trzeba by było wprowadzić w definicji specjalny warunek służący do rozstrzygania zwycięstwa w sytuacjach, gdy brak możliwości dalszych ruchów.

W praktyce jednak w dowodach prawie nigdy nie rozpatruje się takich ruchów, gdyż jest oczywiste, że wykonanie takiego posunięcia przez gracza I nie przybliża go do zwycięstwa, zaś gdy wykona je gracz II mimo że nie zrobił tego gracz I, powoduje to jego natychmiastową przegraną.

Twierdzenie 4.12 (Ehrenfeucht)

- *Gracz II ma strategię wygrywającą w grze* $G_m(\mathfrak{A}, \mathfrak{B})$ *wtedy i tylko wtedy, gdy* $\mathfrak{A} \cong_m \mathfrak{B}$.
- *Gracz II ma dla każdego* m *strategię wygrywającą w grze* $G_m(\mathfrak{A}, \mathfrak{B})$ *wtedy i tylko wtedy, gdy* $\mathfrak{A} \cong_{fin} \mathfrak{B}$.

Dowód: Ćwiczenie. ∎

Poniższe twierdzenie ilustruje, w jaki sposób gra może zostać wykorzystana dla wskazania ograniczeń możliwości logiki pierwszego rzędu.

Twierdzenie 4.13 *Jeśli* $\mathfrak{A} = \langle A, \leq^{\mathfrak{A}} \rangle$ *i* $\mathfrak{B} = \langle B, \leq^{\mathfrak{B}} \rangle$ *są dwoma porządkami liniowymi, gęstymi, bez elementu pierwszego i ostatniego, to* $\mathfrak{A} \equiv \mathfrak{B}$.

Dowód: W myśl Twierdzenia 4.12 należy pokazać, że dla każdego m gracz II ma strategię wygrywającą w grze $G_m(\mathfrak{A}, \mathfrak{B})$. Opiszemy teraz tę strategię. Jej postać nie zależy od

liczby rund do rozegrania. Pokażemy też, że jeśli po zakończeniu poprzedniej rundy warunek wygrywający dla gracza II był spełniony, to po wykonaniu ruchu zgodnie ze wskazaną strategią pozostanie on nadal spełniony. Wówczas na mocy zasady indukcji po rozegraniu dowolnej ilości rund, w których gracz II będzie się stosował do tej strategii, pozostanie on zwycięzcą.

Zauważmy, że warunek o częściowym izomorfizmie w naszej sytuacji oznacza tyle, że zbiory $\{a_1, \ldots, a_k\}$ i $\{b_1, \ldots, b_k\}$ elementów wybranych w każdej ze struktur, po posortowaniu rosnąco zgodnie z porządkiem odpowiednio $\leq^{\mathfrak{A}}$ oraz $\leq^{\mathfrak{B}}$ prowadzą do identycznych ciągów indeksów swoich oznaczeń. Dokładnie, jeśli $a_{i_1} <^{\mathfrak{A}} a_{i_2} <^{\mathfrak{A}} \cdots <^{\mathfrak{A}} a_{i_k}$ i $b_{j_1} <^{\mathfrak{B}} b_{j_2} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{j_k}$, to zachodzą równości $i_\ell = j_\ell$ dla $\ell = 1, \ldots, k$.

- Na pierwszy ruch gracza I gracz II odpowiada w dowolny sposób.

  Przed tą rundą nie było wybranych elementów, czyli przekształcenie opisane w definicji gry było przekształceniem pustym, które na mocy konwencji jest częściowym izomorfizmem. Po wykonaniu ruchu zgodnie ze strategią ciągi indeksów w obu strukturach są oczywiście identyczne.

- We wszystkich kolejnych rundach gracz II określa swój ruch następująco. Niech $a_{i_1} <^{\mathfrak{A}} a_{i_2} <^{\mathfrak{A}} \cdots <^{\mathfrak{A}} a_{i_k}$ i $b_{i_1} <^{\mathfrak{B}} b_{i_2} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{i_k}$ będą (identycznymi na mocy założenia indukcyjnego) ciągami indeksów przed wykonaniem tego ruchu. Ze względu na symetrię sytuacji, możemy bez utraty ogólności założyć, że gracz I wybiera strukturę $\mathfrak{A}$. Może symbolem a_{k+1} oznaczyć:

  - Element mniejszy od a_{i_1}. Wówczas gracz II wybiera element mniejszy od b_{i_1} w $\mathfrak{B}$, który istnieje na mocy założenia, że w $\mathfrak{B}$ nie ma elementu najmniejszego. Widać, że nowe ciągi indeksów pozostaną równe.
  - Element większy od a_{i_k}. Wówczas gracz II wybiera element większy od b_{i_k} w $\mathfrak{B}$, który istnieje na mocy założenia, że w $\mathfrak{B}$ nie ma elementu ostatniego. Widać, że także teraz nowe ciągi indeksów pozostaną równe.
  - Element a spełniający $a_{i_\ell} <^{\mathfrak{A}} a <^{\mathfrak{A}} a_{i_{\ell+1}}$ dla pewnego ℓ. W $\mathfrak{B}$ istnieje element b spełniający $b_{i_\ell} <^{\mathfrak{B}} b <^{\mathfrak{B}} b_{i_{\ell+1}}$, gdyż $\mathfrak{B}$ jest porządkiem gęstym. Gracz II wybiera taki element i również w tym wypadku widać, że nowe ciągi indeksów pozostaną równe.

Na tym dowód istnienia strategii wygrywającej dla gracza II jest zakończony. ∎

Z powyższego wynika między innymi, że $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$. Zatem nie ma zdania logiki pierwszego rzędu, które definiuje pojęcie porządku ciągłego (tzn. takiego, w którym wszystkie niepuste ograniczone podzbiory mają kres górny i kres dolny), bo musiałoby ono być prawdziwe w pierwszej ze struktur, a fałszywe w drugiej.

Definicja 4.14 *Teorią* nazywamy dowolny zbiór zdań, zamknięty ze względu na konsekwencje semantyczne, tj. taki zbiór zdań Δ, że $\Delta \models \varphi$ zachodzi tylko dla $\varphi \in \Delta$. Przykładem teorii jest każdy zbiór postaci $\{\varphi \mid \Gamma \models \varphi\}$, zwany *teorią aksjomatyczną* wyznaczoną przez Γ, czy też postaci $\mathbf{Th}(\mathcal{K}) = \{\varphi \mid \mathfrak{A} \models \varphi, \text{ dla każdego } \mathfrak{A} \in \mathcal{K}\}$ (teoria klasy struktur $\mathcal{K}$) albo $\mathbf{Th}(\mathfrak{A}) = \{\varphi \mid \mathfrak{A} \models \varphi\}$ (teoria modelu $\mathfrak{A}$). Teorię Δ nazywamy *zupełną*, gdy dla każdego

zdania φ, dokładnie jedno ze zdań φ i $\neg\varphi$ należy do Δ. Zbiór zdań prawdziwych w ustalonym modelu jest oczywiście zawsze teorią zupełną.

Wniosek 4.15 *Teoria klasy $\mathcal{A}$ wszystkich porządków liniowych, gęstych, bez elementu pierwszego i ostatniego jest zupełna.*

Dowód: Teoria o której mówimy nie ma modeli skończonych. W myśl Twierdzenia 4.13 wszystkie jej modele nieskończone są elementarnie równoważne. Zatem $\mathbf{Th}(\mathcal{A}) = \mathbf{Th}(\langle\mathbb{Q}, \leq\rangle)$, a teoria pojedynczego modelu jest zawsze zupełna. ∎

Ćwiczenia

1. Wykazać, że dla dostatecznie dużych q istnieje zdanie o randze kwantyfikatorowej q definiujące porządek liniowy o mocy 2^q.

2. Adaptując dowód Faktu 4.10 udowodnić, że struktury $\langle\{1 - 1/n \mid n = 1, 2, \dots\}, \leq\rangle$ oraz $\langle\bigcup_{n=1}^{\infty}\{1-1/n, 1+1/n, 3-1/n\}, \leq\rangle$, gdzie $\leq$ jest w obu wypadkach standardowym porządkiem liczb wymiernych, są elementarnie równoważne.

   Wywnioskować stąd, że pojęcie dobrego porządku nie jest wyrażalne w logice pierwszego rzędu. (Zupełnie inny dowód tego faktu poznamy w Rozdziale 8.)

3. Niech R będzie jednoargumentowym symbolem relacyjnym. Udowodnić, że klasa wszystkich takich struktur $\mathfrak{A} = \langle A, R\rangle$, że $|R| = |A - R|$, nie jest aksjomatyzowalna żadnym zbiorem zdań pierwszego rzędu.

4. Udowodnić, że klasa wszystkich (skończonych lub nieskończonych) grafów $\mathfrak{A} = \langle A, E\rangle$, w których istnieją dwa wierzchołki o równych sobie, skończonych stopniach, nie jest aksjomatyzowalna żadnym zdaniem pierwszego rzędu.

5. Udowodnić, że klasa wszystkich (skończonych lub nieskończonych) grafów $\mathfrak{A} = \langle A, E\rangle$, których każdy skończony podgraf jest planarny, nie jest aksjomatyzowalna żadnym zdaniem pierwszego rzędu.

6. Pokazać, że klasa wszystkich relacji równoważności, których wszystkie skończone klasy abstrakcji mają parzystą moc, nie jest aksjomatyzowalna żadnym zdaniem pierwszego rzędu.

7. Dane są dwie struktury relacyjne $\mathfrak{A} = \langle U, R^{\mathfrak{A}}\rangle$ i $\mathfrak{B} = \langle U, R^{\mathfrak{B}}\rangle$ nad sygnaturą złożoną z jednego dwuargumentowego symbolu relacyjnego. Ich nośnikiem jest $U = \{1, 2, \dots, 15\}$, relacja $R^{\mathfrak{A}}(x, y)$ zachodzi wtedy i tylko wtedy, gdy $x|y$, a relacja $R^{\mathfrak{B}}(x, y)$ wtedy i tylko wtedy, gdy $x \equiv y \pmod 2$.

   Ustalić, jaką minimalną rangę kwantyfikatorową ma zdanie φ takie, że $\mathfrak{A} \models \varphi$ i $\mathfrak{B} \not\models \varphi$.

8. Dane są dwie sześcioelementowe struktury relacyjne $\mathfrak{A}$ i $\mathfrak{B}$ nad sygnaturą złożoną z jednego dwuargumentowego symbolu relacyjnego. Struktury są narysowane poniżej jako grafy skierowane:

   Ustalić, jaką minimalną rangę kwantyfikatorową ma zdanie φ takie, że $\mathfrak{A} \models \varphi$ i $\mathfrak{B} \not\models \varphi$.

5 Paradygmaty dowodzenia

Sprawdzenie, czy dana formuła rachunku zdań jest tautologią, polega zwykle na obliczeniu jej wartości dla 2^n różnych wartościowań, gdzie n jest liczbą zmiennych zdaniowych tej formuły. Jak dotąd nie są znane radykalnie szybsze metody. Dla rachunku predykatów nie istnieje w ogóle żaden algorytm sprawdzania czy dana formuła jest tautologią (Twierdzenie 3.8). W obu przypadkach istnieją jednak metody *dowodzenia* pozwalające na wyprowadzanie prawdziwych formuł za pomocą ustalonych procedur syntaktycznych.

Każdy system dowodzenia zawiera dwa składniki:

- początkowy zbiór formuł (lub wyrażeń zbudowanych z wielu formuł) zwanych *aksjomatami*;
- zbiór operacji przekształcających wyrażenia w wyrażenia — operacje te są nazywane *regułami dowodzenia*.

Reguły dowodzenia opisują warunki, przy pomocy których można otrzymać nowe wyrażenie (nazywane *konkluzją*) z otrzymanych już wyrażeń (nazywanych *przesłankami*). Dowody w systemach formalnych są ciągami wyrażeń, być może posiadającymi dodatkową strukturę pozwalającą na lepszą wizualizację.

W dalszej części opiszemy trzy systemy dowodzenia: system typu hilbertowskiego (od nazwiska Davida Hilberta), system naturalnej dedukcji oraz rachunek sekwentów. Ostatnie dwa systemy znajdują zastosowanie w pewnych działach sztucznej inteligencji oraz w systemach automatycznego dowodzenia twierdzeń.

5.1 System hilbertowski

Poniższy system dowodzenia dotyczy formuł zbudowanych przy użyciu jedynie spójnika $\rightarrow$, stałej $\bot$ oraz zmiennych zdaniowych. Przypomnijmy, że dla dowolnej formuły φ, napis $\neg\varphi$ jest skrótem zapisu $\varphi \rightarrow \bot$. Symbole φ, ψ, ϑ w poniższym systemie oznaczają dowolne formuły.

Aksjomaty

(A1) $\varphi \rightarrow (\psi \rightarrow \varphi)$
(A2) $(\varphi \rightarrow (\psi \rightarrow \vartheta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \vartheta))$
(A3) $\neg\neg\varphi \rightarrow \varphi$

Reguła dowodzenia

$$\text{(MP)} \qquad \frac{\varphi \qquad \varphi \rightarrow \psi}{\psi}$$

Reguła (MP) jest nazywana *regułą odrywania* lub też regułą *modus ponens*.

Dowodem w powyższym systemie nazywamy taki ciąg formuł, w którym każda formuła albo jest aksjomatem, albo też została otrzymana z wcześniej występujących formuł w wyniku

zastosowania reguły odrywania. Powiemy, że formuła φ *ma dowód*, lub jest *twierdzeniem* systemu hilbertowskiego, co zapiszemy $\vdash_H \varphi$, gdy istnieje dowód zawierający φ. Powyższą definicję możemy nieco uogólnić. Niech Δ będzie dowolnym zbiorem formuł. Powiemy, że formuła φ ma dowód ze zbioru hipotez Δ (notacja $\Delta \vdash_H \varphi$), gdy φ jest twierdzeniem systemu, w którym zbiór aksjomatów został poszerzony o formuły ze zbioru Δ.

Przykład 5.1 Niech p będzie zmienną zdaniową. Pokażemy, że formuła $p \to p$ jest twierdzeniem systemu hilbertowskiego. Poniżej podajemy dowód dla tej formuły. W nawiasach podajemy nazwę aksjomatu, jeśli dana formuła jest instancją tego aksjomatu, lub też numery formuł z wcześniejszych kroków dowodu, do których jest stosowana reguła odrywania.

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ (A2)
2. $p \to ((p \to p) \to p)$ (A1)
3. $(p \to (p \to p)) \to (p \to p)$ (1,2)
4. $p \to (p \to p)$ (A1)
5. $p \to p$ (3,4)

Zauważmy, że w powyższym przykładzie możemy wszędzie zastąpić zmienną p przez dowolną formułę φ dostając dowód formuły $\varphi \to \varphi$.

Następujące twierdzenie jest bardzo użyteczne, gdy trzeba uzasadnić, że jakaś formuła jest twierdzeniem.

Twierdzenie 5.2 (o dedukcji) *Dla dowolnego zbioru formuł Δ oraz dowolnych formuł φ, ψ, jeśli $\Delta \cup \{\varphi\} \vdash_H \psi$, to $\Delta \vdash_H \varphi \to \psi$.*

Dowód: Dowód jest indukcyjny ze względu na liczbę kroków w dowodzie formuły ψ ze zbioru hipotez $\Delta \cup \{\varphi\}$. Przypuśćmy najpierw, że dowód ten składa się tylko z jednego kroku. Jeśli $\psi = \varphi$, to stosując wyprowadzenie z Przykładu 5.1 dostajemy dowód formuły $\varphi \to \varphi$. Możemy oczywiście przyjąć, że formuła ta jest wyprowadzona ze zbioru hipotez Δ. Druga możliwość jest taka, że $\psi \in \Delta$ lub też, że ψ jest aksjomatem. W każdym z tych przypadków mamy $\Delta \vdash_H \psi$. Wówczas stosując regułę odrywania do ψ oraz aksjomatu $\psi \to (\varphi \to \psi)$ dostajemy formułę $\varphi \to \psi$.

Załóżmy teraz, że ostatnim krokiem w wyprowadzeniu formuły ψ jest zastosowanie reguły (MP) do formuł $\vartheta \to \psi$ oraz ϑ, dla pewnej formuły ϑ. Z założenia indukcyjnego mamy $\Delta \vdash_H \varphi \to (\vartheta \to \psi)$ oraz $\Delta \vdash_H \varphi \to \vartheta$. Stosując regułę odrywania do $\varphi \to (\vartheta \to \psi)$ oraz do aksjomatu (A2): $(\varphi \to (\vartheta \to \psi)) \to ((\varphi \to \vartheta) \to (\varphi \to \psi))$ dostajemy formułę $(\varphi \to \vartheta) \to (\varphi \to \psi)$. Ponownie stosując regułę odrywania do tej formuły oraz do $\varphi \to \vartheta$ dostajemy żądaną formułę $\varphi \to \psi$. To kończy dowód twierdzenia o dedukcji. ∎

Twierdzenie 5.3 (o poprawności) *Jeśli $\Delta \vdash_H \varphi$, to $\Delta \models \varphi$. W szczególności, jeśli $\vdash_H \varphi$, to φ jest tautologią.*

Dowód: Dowód jest indukcyjny ze względu na liczbę kroków w wyprowadzeniu formuły φ w systemie hilbertowskim ze zbioru hipotez Δ. Jeśli dowód ten składa się tylko z jednego kroku to albo $\varphi \in \Delta$ albo φ jest aksjomatem. W obu przypadkach oczywiście zachodzi $\Delta \models \varphi$.

Załóżmy teraz, że φ jest otrzymana przez zastosowanie reguły odrywania do formuł $\psi \to \varphi$ oraz ψ. Z założenia indukcyjnego mamy

$$\Delta \models \psi \to \varphi \text{ oraz } \Delta \models \psi. \tag{1}$$

Niech ϱ będzie dowolnym wartościowaniem spełniającym wszystkie formuły z Δ. Na mocy (1), wartościowanie ϱ spełnia $\psi \to \varphi$ oraz spełnia ψ. Wynika stąd, że ϱ spełnia φ. Tym samym udowodniliśmy, że $\Delta \models \varphi$. To kończy dowód. ∎

Lemat 5.4 *Dla dowolnych formuł φ, ψ zbudowanych przy użyciu $\to$ oraz $\bot$, następujące formuły są twierdzeniami systemu hilbertowskiego.*

1. $\varphi \to (\neg\psi \to \neg(\varphi \to \psi))$;
2. $\bot \to \varphi$;
3. $(\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$;

Dowód: (1) Niech $\Delta = \{\varphi, \psi \to \bot, \varphi \to \psi\}$. Stosując regułę odrywania do formuł φ oraz $\varphi \to \psi$ dostajemy ψ. Przez ponowne zastosowanie (MP) do tej formuły oraz do $\psi \to \bot$ otrzymujemy wyprowadzenie $\bot$. Tym samym pokazaliśmy, że $\Delta \vdash_H \bot$. Stosując teraz trzy razy twierdzenie o dedukcji dostajemy

$$\vdash_H \varphi \to ((\psi \to \bot) \to ((\varphi \to \psi) \to \bot)),$$

czyli

$$\vdash_H \varphi \to (\neg\psi \to \neg(\varphi \to \psi)).$$

(2) Ponieważ $\{\bot, \neg\varphi\} \vdash_H \bot$, więc z twierdzenia o dedukcji wynika $\bot \vdash_H \neg\neg\varphi$. Stosując teraz (MP) do tej formuły oraz do aksjomatu (A3) w postaci $\neg\neg\varphi \to \varphi$ otrzymujemy $\bot \vdash_H \varphi$. Ponowne zastosowanie twierdzenia o dedukcji daje nam $\vdash_H \bot \to \varphi$.

(3) Niech $\Delta = \{\varphi \to \psi, \neg\varphi \to \psi\}$. Zaczynamy od zbioru hipotez $\Delta \cup \{\varphi, \neg\psi\}$. Stosując (MP) do formuł φ oraz $\varphi \to \psi$ dostajemy ψ. Ponowne zastosowanie (MP) do tej formuły oraz do $\neg\psi$ daje nam $\bot$. Używając teraz twierdzenia o dedukcji do formuły $\bot$ otrzymujemy

$$\Delta \cup \{\neg\psi\} \vdash_H \neg\varphi.$$

Ponieważ mamy $\Delta \cup \{\neg\psi\} \vdash_H \neg\varphi \to \psi$, to stosując (MP) otrzymujemy $\Delta \cup \{\neg\psi\} \vdash_H \psi$. Jeszcze raz używamy (MP) aby z $\neg\psi$ i ψ otrzymać $\bot$ i mamy

$$\Delta \cup \{\neg\psi\} \vdash_H \bot.$$

Na mocy twierdzenia o dedukcji $\Delta \vdash_H \neg\neg\psi$. Stosując (MP) do formuły $\neg\neg\psi$ oraz do aksjomatu $\neg\neg\psi \to \psi$ otrzymujemy $\Delta \vdash_H \psi$. Dwukrotne zastosowanie twierdzenia o dedukcji daje nam $\vdash_H (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$. To kończy dowód lematu. ∎

Powyższy system można łatwo rozszerzyć do systemu dla formuł opartych o pozostałe spójniki logiczne. Wystarczy w tym celu dodać aksjomaty wyrażające równoważności definiujące te spójniki.

(B1) $\varphi \wedge \psi \to \neg(\varphi \to \neg\psi)$
(B2) $\neg(\varphi \to \neg\psi) \to \varphi \wedge \psi$
(B3) $\varphi \vee \psi \to (\neg\varphi \to \psi)$
(B4) $(\neg\varphi \to \psi) \to \varphi \vee \psi$

Tak otrzymany system oznaczymy przez $\vdash_{H^+}$.

Twierdzenie 5.5 (o poprawności dla $\vdash_{H^+}$) *Dla dowolnego zbioru formuł Δ i dla dowolnej formuły φ w języku z $\vee, \wedge, \to, \bot$, jeśli $\Delta \vdash_{H^+} \varphi$ to $\Delta \models \varphi$.*

Dowód: Wystarczy sprawdzić, że aksjomaty (B1)–(B4) są tautologiami. Konkluzja wynika z Twierdzenia 5.3 o poprawności dla $\vdash_H$. ∎

Lemat 5.6 *Dla dowolnej formuły φ istnieje formuła $\tilde{\varphi}$ zbudowana przy użyciu jedynie $\to$ oraz $\bot$, taka że $\vdash_{H^+} \varphi \to \tilde{\varphi}$ oraz $\vdash_{H^+} \tilde{\varphi} \to \varphi$.*

Dowód: W danej formule φ, zastąpmy każdą podformułę postaci $\psi \wedge \vartheta$ formułą $\neg(\psi \to \neg\vartheta)$ oraz każdą podformułę postaci $\psi \vee \vartheta$ formułą $\neg\psi \to \vartheta$. Aksjomaty (B1)–(B4) mówią, że zastąpione formuły są równoważne. Tak więc łatwo dostajemy $\vdash_{H^+} \varphi \to \tilde{\varphi}$ oraz $\vdash_{H^+} \tilde{\varphi} \to \varphi$. Szczegóły dowodu pozostawimy Czytelnikowi. ∎

5.2 System naturalnej dedukcji

System naturalnej dedukcji (wprowadzony przez S. Jaśkowskiego i G. Gentzena) operuje wyrażeniami zwanymi *sekwentami*. Są to wyrażenia postaci $\Delta \vdash \varphi$, gdzie Δ jest pewnym skończonym zbiorem formuł, a φ jest formułą. W odróżnieniu od systemu hilbertowskiego, w naturalnej dedukcji istotne są reguły dowodzenia, a aksjomat jest bardzo prosty. Charakterystyczną cechą naturalnej dedukcji jest to, że reguły dowodzenia (za wyjątkiem reguły (PS) „przez sprzeczność") są podzielone na grupy, po jednej dla każdego spójnika. W ramach jednej takiej grupy mamy dwa rodzaje reguł. *Reguły wprowadzania* mówią o tym w jakiej sytuacji można wprowadzić dany spójnik na prawo od znaku $\vdash$ (tj. wywnioskować formułę danego kształtu). *Reguły eliminacji* mówią o tym w jakiej sytuacji można ten spójnik wyeliminować, tzn. jak można użyć formuły zbudowanej z jego pomocą do wyprowadzenia innej formuły. Regułę dowodzenia „przez sprzeczność" można traktować jako „silną" regułę eliminacji $\bot$. Pamiętajmy, że $\neg\varphi$ oznacza formułę $\varphi \to \bot$.

Poniżej będziemy stosować następującą konwencję: Napis $\Delta, \varphi_1, \ldots, \varphi_n$ oznacza zbiór $\Delta \cup \{\varphi_1, \ldots, \varphi_n\}$, przy czym nie zakładamy tu, że $\varphi_i \notin \Delta$.

Aksjomat

(A0) $\Delta, \varphi \vdash \varphi$

Reguły dowodzenia

$$(\to\text{-intro}) \ \frac{\Delta, \varphi \vdash \psi}{\Delta \vdash \varphi \to \psi} \qquad (\to\text{-elim}) \ \frac{\Delta \vdash \varphi \to \psi \qquad \Delta \vdash \varphi}{\Delta \vdash \psi}$$

$$(\wedge\text{-intro}) \ \frac{\Delta \vdash \varphi \qquad \Delta \vdash \psi}{\Delta \vdash \varphi \wedge \psi} \qquad (\wedge\text{-elim}) \ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \varphi} \qquad (\wedge\text{-elim}) \ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \psi}$$

$$(\vee\text{-intro}) \ \frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi} \qquad (\vee\text{-intro}) \ \frac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}$$

$$(\vee\text{-elim}) \ \frac{\Delta \vdash \varphi \vee \psi \qquad \Delta, \varphi \vdash \vartheta \qquad \Delta, \psi \vdash \vartheta}{\Delta \vdash \vartheta}$$

$$(\text{PS}) \ \frac{\Delta, \neg\varphi \vdash \bot}{\Delta \vdash \varphi}$$

Zauważmy, że szczególnym przypadkiem reguły ($\to$-intro) jest następująca reguła, można ją traktować jak regułę wprowadzenia negacji.

$$\frac{\Delta, \varphi \vdash \bot}{\Delta \vdash \neg\varphi}$$

Zauważmy też, że szczególnym przypadkiem reguły ($\to$-elim) jest następująca reguła, można ją traktować jak regułę eliminacji negacji.

$$\frac{\Delta \vdash \neg\varphi \quad \Delta \vdash \varphi}{\Delta \vdash \bot}$$

O ile dowody w systemi hilbertowskim są tradycyjnie definiowane jako ciągi, a więc struktury liniowe, to w systemie naturalnej dedukcji dowody są drzewami. Pozwala to znacznie lepiej wizualizować zależności pomiędzy przesłankami i konkluzją stosowanych reguł. *Dowodem* sekwentu $\Delta \vdash \varphi$ w systemie naturalnej dedukcji nazwiemy drzewo etykietowane sekwentami tak, że korzeń ma etykietę $\Delta \vdash \varphi$, liście są etykietowane wystąpieniami aksjomatu oraz każdy wewnętrzny wierzchołek jest etykietowany sekwentem otrzymanym z etykiet potomków tego wierzchołka przy zastosowaniu jednej z reguł. Piszemy $\Delta \vdash_N \varphi$, gdy sekwent $\Delta \vdash \varphi$ ma dowód w systemie naturalnej dedukcji. Gdy $\Delta = \emptyset$, to mówimy też, że φ jest *twierdzeniem* systemu naturalnej dedukcji i zapisujemy to przez $\vdash_N \varphi$. Jeśli Δ jest zbiorem nieskończonym, to $\Delta \vdash_N \varphi$ oznacza, że istnieje dowód sekwentu $\Delta_0 \vdash \varphi$, dla pewnego skończonego $\Delta_0 \subseteq \Delta$.

Poniżej podajemy kilka przykładów dowodów w systemie naturalnej dedukcji.

Przykład 5.7

- Pokażemy $\vdash_N p \to p$.

$$\frac{p \vdash p}{\vdash p \to p}\ (\to\text{-intro})$$

- Pokażemy $\vdash_N p \to (q \to p)$.

$$\frac{\dfrac{p, q \vdash p}{p \vdash q \to p}\ (\to\text{-intro})}{\vdash p \to (q \to p)}\ (\to\text{-intro})$$

- Pokażemy $\vdash_N \neg\neg p \to p$.

$$\frac{\dfrac{\dfrac{\neg\neg p, \neg p \vdash \neg\neg p \qquad \neg\neg p, \neg p \vdash \neg p}{\neg\neg p, \neg p \vdash p}\ (\to\text{-elim})}{\neg\neg p \vdash p}\ (\text{PS})}{\vdash \neg\neg p \to p}\ (\to\text{-intro})$$

Twierdzenie 5.8 *Dla dowolnego sekwentu $\Delta \vdash \varphi$ mamy następującą równoważność:*

$$\Delta \vdash_N \varphi \quad \textit{wtedy i tylko wtedy, gdy} \quad \Delta \vdash_{H^+} \varphi.$$

Dowód: Aby pokazać, że każdy dowód w $\vdash_N$ daje się przerobić na dowód w $\vdash_{H^+}$ wystarczy sprawdzić, że każda z reguł systemu naturalnej dedukcji jest *dopuszczalna* w H^+. Tzn. wystarczy sprawdzić, że jeśli mamy dowody przesłanek w $\vdash_{H^+}$, to możemy udowodnić konkluzję. Zauważmy, że wyprowadzalność reguły(→-intro) jest konsekwencją twierdzenia o dedukcji, natomiast reguła (→-elim) jest regułą (MP). Przykładowo pokażemy wyprowadzenie (∨-elim) oraz (PS) w H^+, pozostawiając Czytelnikowi wyprowadzenie pozostałych reguł.

Załóżmy, że mamy w H^+ dowody następujących sekwentów: $\Delta \vdash \varphi \vee \psi$, $\Delta, \varphi \vdash \vartheta$ oraz $\Delta, \psi \vdash \vartheta$. Wówczas, stosując aksjomat (B2) i regułę (MP) mamy $\Delta \vdash_{H^+} \neg\varphi \to \psi$. Zatem $\Delta, \neg\varphi \vdash_{H^+} \psi$ i ponieważ $\Delta \vdash_{H^+} \psi \to \vartheta$ to również $\Delta, \neg\varphi \vdash_{H^+} \psi \to \vartheta$. Stąd $\Delta, \neg\varphi \vdash_{H^+} \vartheta$. Stosując twierdzenie o dedukcji dostajemy $\Delta \vdash_{H^+} \neg\varphi \to \vartheta$. Skoro mamy również $\delta \vdash_{H^+} \varphi \to \vartheta$, to na mocy Lematu 5.4(3) otrzymujemy $\Delta \vdash_{H^+} \vartheta$.

Dla wyprowadzenia (PS) załóżmy, że $\Delta, \neg\varphi \vdash_{H^+} \bot$. Z twierdzenia o dedukcji dostajemy $\Delta \vdash_{H^+} \neg\neg\varphi$. Tak więc z (A3) i (MP) dostajemy $\Delta \vdash_{H^+} \varphi$.

Dla pokazania implikacji odwrotnej wystarczy pokazać, że wszystkie aksjomaty systemu H^+ są twierdzeniami systemu naturalnej dedukcji. Wyprowadzenia (A1) i (A3) w ND zostały podane w Przykładzie 5.7. Przykładowo pokażemy wyprowadzenia (A2) i (B1). Zaczniemy od wyprowadzenia (A2). Niech $\Delta = \{\varphi \to (\psi \to \vartheta),\ \varphi \to \psi,\ \varphi\}$. Mamy następujący dowód:

$$\frac{\dfrac{\Delta \vdash \varphi \to (\psi \to \vartheta) \qquad \Delta \vdash \varphi}{\Delta \vdash \psi \to \vartheta}\ (\to\text{-elim}) \qquad \dfrac{\Delta \vdash \varphi \to \psi \qquad \Delta \vdash \varphi}{\Delta \vdash \psi}\ (\to\text{-elim})}{\Delta \vdash \vartheta}\ (\to\text{-elim})$$

Stosując trzy razy ($\rightarrow$ -intro) do sekwentu $\Delta \vdash \vartheta$ dostajemy wyprowadzenie aksjomatu (A2).

Następnie pokażemy dowód (B1) w ND. Zaczniemy od wyprowadzenia $\neg(\varphi \rightarrow \neg\psi) \vdash \varphi$, gdzie $\Delta = \{\neg(\varphi \rightarrow \neg\psi), \neg\varphi\}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta, \varphi, \psi \vdash \neg\varphi \qquad \Delta, \varphi, \psi \vdash \varphi}{\Delta, \varphi, \psi \vdash \bot}\,(\rightarrow\text{-elim})}{\Delta, \varphi \vdash \neg\psi}\,(\rightarrow\text{-intro})}{\Delta \vdash \varphi \rightarrow \neg\psi}\,(\rightarrow\text{-intro}) \qquad \Delta \vdash \neg(\varphi \rightarrow \neg\psi)}{\dfrac{\Delta \vdash \bot}{\neg(\varphi \rightarrow \neg\psi) \vdash \varphi}\,(\mathrm{PS})}\,(\rightarrow\text{-elim})$$

Następnie wyprowadzimy sekwent $\neg(\varphi \rightarrow \neg\psi) \vdash \psi$. Niech $\Delta = \{\neg(\varphi \rightarrow \neg\psi), \neg\psi\}$

$$\dfrac{\dfrac{\dfrac{\Delta, \varphi \vdash \neg\psi}{\Delta \vdash \varphi \rightarrow \neg\psi}\,(\rightarrow\text{-intro}) \qquad \Delta \vdash \neg(\varphi \rightarrow \neg\psi)}{\Delta \vdash \bot}\,(\rightarrow\text{-elim})}{\neg(\varphi \rightarrow \neg\psi) \vdash \psi}\,(\mathrm{PS})$$

Mając wyprowadzone sekwenty $\neg(\varphi \rightarrow \neg\psi) \vdash \varphi$ oraz $\neg(\varphi \rightarrow \neg\psi) \vdash \psi$ możemy zakończyć dowód (B1).

$$\dfrac{\dfrac{\neg(\varphi \rightarrow \neg\psi) \vdash \varphi \qquad \neg(\varphi \rightarrow \neg\psi) \vdash \psi}{\neg(\varphi \rightarrow \neg\psi) \vdash \varphi \wedge \psi}\,(\wedge\text{-intro})}{\vdash \neg(\varphi \rightarrow \neg\psi) \rightarrow (\varphi \wedge \psi)}\,(\rightarrow\text{-intro})$$

∎

5.3 Rachunek sekwentów

Dla przedstawienia rachunku sekwentów rozszerzymy nieco pojęcie sekwentu. Przez *sekwent* będziemy teraz rozumieć napis $\Delta \vdash \Gamma$, gdzie Δ oraz Γ są skończonymi zbiorami formuł. Intuicyjnie, wyprowadzalność sekwentu $\Delta \vdash \Gamma$ w rachunku sekwentów będzie oznaczać, że alternatywa formuł z Γ wynika z hipotez Δ.

Podobnie jak w poprzedniej części, rozważamy formuły, zbudowane w oparciu o spójniki $\rightarrow, \vee, \wedge$ oraz stałą zdaniową $\bot$. Negację $\neg$ traktujemy jako spójnik zdefiniowany przez $\rightarrow$ i $\bot$.

Charakterystyczną cechą rachunku sekwentów jest specyficzna postać reguł. Reguły w tym systemie naturalnie dzielą się na dwie grupy: jedna grupa reguł opisuje sytuacje kiedy możemy wprowadzić dany spójnik na lewo od znaku $\vdash$, a druga grupa jest odpowiedzialna za wprowadzanie spójnika na prawo od $\vdash$. Dla każdego spójnika mamy odpowiadającą parę reguł. Aksjomat (A$\bot$) można traktować jako regułę (bez przesłanek) wprowadzenia $\bot$ z lewej strony znaku $\vdash$.

Przypomnijmy, że napis $\Delta, \varphi_1, \ldots, \varphi_n$ oznacza zbiór $\Delta \cup \{\varphi_1, \ldots, \varphi_n\}$.

Aksjomaty

(A00) $\Delta, \varphi \vdash \Gamma, \varphi$

(A$\bot$) $\Delta, \bot \vdash \Gamma$

Reguły dowodzenia

$$(\to\text{-lewa})\ \frac{\Delta \vdash \Gamma, \varphi \qquad \Delta, \psi \vdash \Gamma}{\Delta, \varphi \to \psi \vdash \Gamma} \qquad (\to\text{-prawa})\ \frac{\Delta, \varphi \vdash \Gamma, \psi}{\Delta \vdash \Gamma, \varphi \to \psi}$$

$$(\wedge\text{-lewa})\ \frac{\Delta, \varphi, \psi \vdash \Gamma}{\Delta, \varphi \wedge \psi \vdash \Gamma} \qquad (\wedge\text{-prawa})\ \frac{\Delta \vdash \Gamma, \varphi \qquad \Delta \vdash \Gamma, \psi}{\Delta \vdash \Gamma, \varphi \wedge \psi}$$

$$(\vee\text{-lewa})\ \frac{\Delta, \varphi \vdash \Gamma \qquad \Delta, \psi \vdash \Gamma}{\Delta, \varphi \vee \psi \vdash \Gamma} \qquad (\vee\text{-prawa})\ \frac{\Delta \vdash \Gamma, \varphi, \psi}{\Delta \vdash \Gamma, \varphi \vee \psi}$$

Dowodem sekwentu $\Delta \vdash \Gamma$, tak jak poprzednio, nazywamy drzewo etykietowane sekwentami tak, że korzeń jest etykietowany przez $\Delta \vdash \Gamma$, liście są etykietowane aksjomatami oraz wierzchołki wewnętrzne są etykietowane sekwentami otrzymanymi poprawnie przez zastosowanie reguł dowodzenia. Jeśli istnieje dowód sekwentu $\Delta \vdash \Gamma$ w rachunku sekwentów to zapisujemy to tak: $\Delta \vdash_G \Gamma$. (Litera G pochodzi od nazwiska twórcy tego systemu, G. Gentzena.) Piszemy też $\Delta \vdash_G \varphi$, gdy Δ jest nieskończony, ale $\Delta \vdash_G \varphi$ dla pewnego skończonego $\Delta_0 \subseteq \Delta$.

Zauważmy, że jeśli mamy sekwent $\Delta \vdash \Gamma, \varphi$ to stosując aksjomat (A$\bot$), a następnie ($\to$-lewa) dostajemy sekwent $\Delta, \neg\varphi \vdash \Gamma$. Zatem natępująca reguła jest *dopuszczalna* w systemie $\vdash_G$ (tj. jeśli dodamy ją do systemu, to zbiór wyprowadzalnych sekwentów nie ulegnie zmianie):

$$(\neg\text{-lewa})\ \frac{\Delta \vdash \Gamma, \varphi}{\Delta, \neg\varphi \vdash \Gamma}$$

Ponadto zauważmy, że jeśli mamy dowód sekwentu $\Delta \vdash \Gamma$, to dla każdej formuły φ możemy ją dodać do prawej strony każdego sekwentu w tym dowodzie i otrzymamy dowód sekwentu $\Delta \vdash \Gamma, \varphi$. Łatwy dowód indukcyjny pozostawiamy Czytelnikowi (Ćwiczenie 12). W szczególności, jeśli mamy udowodniony sekwent $\Delta, \varphi \vdash \Gamma$, to możemy też udowodnić sekwent $\Delta, \varphi \vdash \Gamma, \bot$. Stosując do niego regułę ($\to$-prawa) otrzymujemy sekwent $\Delta \vdash \Gamma, \neg\varphi$. Tym samym pokazaliśmy, że następująca reguła jest dopuszczalna w systemie $\vdash_G$:

$$(\neg\text{-prawa})\ \frac{\Delta, \varphi \vdash \Gamma}{\Delta \vdash \Gamma, \neg\varphi}$$

Twierdzenie 5.9 *Dla każdych Δ i φ mamy następującą równoważność*

$$\Delta \vdash_G \varphi \quad \textit{wtedy i tylko wtedy, gdy} \quad \Delta \vdash_{H^+} \varphi.$$

Powyższe twierdzenie pozostawimy bez dowodu. Łatwo jest „przetłumaczyć" każde wyprowadzenie w systemie $\vdash_G$ na dowód w stylu Hilberta. Dla dowodu implikacji odwrotnej rozszerza się system $\vdash_G$ przez dodanie nowej reguły zwanej *cięciem*.

$$(\text{cięcie})\ \frac{\Delta, \varphi \vdash \Gamma \qquad \Delta \vdash \varphi, \Gamma}{\Delta \vdash \Gamma}$$

Niech $\vdash_{GC}$ oznacza system gentzenowski z cięciem. Bez trudu można pokazać, że reguła odrywania jest dopuszczalna w $\vdash_{GC}$. Zatem, korzystając z twierdzenia o pełności dla systemu hilbertowskiego, łatwo pokazujemy, że każda tautologia jest twierdzeniem systemu $\vdash_{GC}$. Główna trudność w dowodzie Twierdzenia 5.9 polega na udowodnieniu następującego twierdzenia *o eliminacji cięcia*. Twierdzenie to podajemy bez dowodu.

Twierdzenie 5.10 (o eliminacji cięcia) *Jeśli* $\Delta \vdash_{GC} \Gamma$*, to* $\Delta \vdash_{G} \Gamma$.

Główna zaleta dowodów w rachunku sekwentów (bez cięcia) wynika z następującej *własności podformuł:* wszystkie formuły występujące w przesłance dowolnej reguły są podformułami formuł występujących w konkluzji. Zatem np. w dowodzie sekwentu $\vdash \varphi$ mamy do czynienia tylko z podformułami formuły φ. Dla danej formuły φ, łatwiej więc znaleźć dowód w sensie Gentzena niż np. dowód w sensie Hilberta. Dlatego systemy zbliżone do rachunku sekwentów znajdują zastosowanie w automatycznym dowodzeniu twierdzeń. Pokażemy to na przykładzie.

Przykład 5.11

1. Poszukamy dowodu sekwentu $\vdash \neg\neg\varphi \to \varphi$ w $\vdash_G$. Ponieważ najbardziej zewnętrznym spójnikiem w rozważanej formule jest $\to$, to ostatnią regułą w poszukiwanym dowodzie musiała być reguła ($\to$-prawa). Zatem wystarczy znaleźć dowód sekwentu $\neg\neg\varphi \vdash \varphi$. Najbardziej zewnętrznym spójnikiem formuły po lewej stronie jest $\neg$, a zatem na mocy reguły ($\neg$-lewa) wystarczy udowodnić sekwent $\vdash \varphi, \neg\varphi$. Podobnie, na mocy reguły ($\neg$-prawa), wystarczy udowodnić sekwent $\varphi \vdash \varphi$, a on przecież jest aksjomatem.

2. Jeśli zastosujemy powyższą procedurę do formuły, która nie jest tautologią, to dostaniemy wskazówkę na to gdzie należy szukać wartościowania falsyfikującego tę formułę. (Wartościowanie falsyfikujące sekwent $\Delta \vdash \Gamma$ to takie, które spełnia wszystkie formuły z Δ oraz falsyfikuje wszystkie formuły z Γ.) Dla zilustrowania tej tezy weźmy bardzo prosty sekwent $\vdash p \to q$. Postępując podobnie jak porzednio dochodzimy do sekwentu $p \vdash q$, który nie jest aksjomatem, i którego nie możemy już dalej rozłożyć. Jako wartościowanie falsyfikujące wystarczy wziąć wartościowanie spełniające p i falsyfikujące q.

Z własności podformuł wynika też własność *konserwatywności* systemu nad swoimi fragmentami: jeśli formuła, w której nie występuje jakiś spójnik jest tautologią, to jej wyprowadzenie nie wymaga reguł związanych z tym spójnikiem.

Ćwiczenia

1. Niech $\vdash_{H_1}$ oznacza system dowodzenia otrzymany z systemu $\vdash_H$ przez zamianę aksjomatu (A3) na następujący aksjomat:
   (A3') $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$.
   Dowieść, że obydwa systemy są równoważne, tzn., że dla dowolnego sekwentu $\Delta \vdash \varphi$, zachodzi $\Delta \vdash_H \varphi$ wtedy i tylko wtedy, gdy $\Delta \vdash_{H_1} \varphi$.

2. Niech $\vdash_{H_2}$ oznacza system dowodzenia otrzymany z systemu $\vdash_H$ przez zamianę aksjomatu (A3) na następujący aksjomat:

   (A3") $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$.

   Dowieść, że obydwa systemy są równoważne, tzn., że dla dowolnego sekwentu $\Delta \vdash \varphi$, zachodzi $\Delta \vdash_H \varphi$ wtedy i tylko wtedy, gdy $\Delta \vdash_{H_2} \varphi$.

3. Dowieść, że aksjomatu (A3) nie da się wyprowadzić z aksjomatów (A0–2) przy pomocy reguły odrywania.

4. Dowieść $\vdash_H \neg p \to (p \to q)$ używając twierdzenia o dedukcji oraz bez użycia tego twierdzenia.

5. Pokazać, że w systemie $\vdash_H$ dopuszczalna jest następująca reguła:

$$\frac{\varphi \to \psi \qquad \neg\psi}{\neg\varphi}$$

   tzn. pokazać, że jeśli $\Delta \vdash_H \varphi \to \psi$ oraz $\Delta \vdash_H \neg\psi$, to również mamy $\Delta \vdash_H \neg\varphi$.

6. Dowieść, że dla każdej formuły φ, nie będącej tautologią, istnieje maksymalny zbiór formuł Δ (nad daną sygnaturą) o tej własności, że $\Delta \nvdash_H \varphi$.

7. Każdy z poniższych sekwentów wyprowadzić w systemie $\vdash_{H^+}$, $\vdash_N$, $\vdash_G$.

   (a) $\vdash \bot \to p$;

   (b) $p \to q, q \to r \vdash p \to r$;

   (c) $\vdash (\neg p \to p) \to p$;

   (d) $p, \neg p \vdash q$;

   (e) $p \to (q \to r) \vdash q \to (p \to r)$;

   (f) $\vdash (\neg p \to \neg q) \to (q \to p)$;

   (g) $\vdash \neg(p \wedge q) \to (\neg p \vee \neg q)$.

8. Dowieść, że jeśli $\Delta \vdash_N \varphi$, to dla dowolnej formuły ψ zachodzi $\Delta, \psi \vdash_N \varphi$.

9. Dowieść, że jeśli $\Delta \vdash_N \bot$, to dla dowolnej formuły φ zachodzi $\Delta \vdash_N \varphi$.

10. Dla każdego z sytemów $\vdash_{H^+}$, $\vdash_N$, $\vdash_G$ dowieść, że jeśli sekwent $\Delta \vdash \varphi$ jest wyprowadzalny w tym systemie oraz S jest podstawieniem formuł na zmienne zdaniowe, to sekwent $S(\Delta) \vdash S(\varphi)$ powstający w wyniku podstawienia jest też wyprowadzalny w tym systemie.

11. Udowodnić, że w rachunku sekwentów zamiana reguły ($\vee$-prawa) na dwie reguły:

$$\frac{\Delta \vdash \Gamma, \varphi}{\Delta \vdash \Gamma, \varphi \vee \psi} \qquad\qquad \frac{\Delta \vdash \Gamma, \psi}{\Delta \vdash \Gamma, \varphi \vee \psi}$$

    daje w wyniku równoważny system dowodzenia (wyprowadzalne są te same sekwenty).

12. Udowodnić, że następujące reguły *osłabiania* są dopuszczalne w rachunku sekwentów:

$$\frac{\Delta \vdash \Gamma}{\Delta, \varphi \vdash \Gamma} \qquad\qquad \frac{\Delta \vdash \Gamma}{\Delta \vdash \Gamma, \varphi}$$

13. Wyprowadzić w rachunku sekwentów:

    (a) $\vdash p \vee \neg p$;

    (b) $\vdash ((p \to q) \to p) \to p$.

    Czy można to zrobić używając tylko sekwentów postaci $\Delta \vdash \varphi$ (z jedną formułą po prawej)?

6 Pełność rachunku zdań

Zagadnienie pełności systemów formalnych jest jednym z centralnych problemów logiki. O ile poprawność systemu formalnego (zwana też *adekwatnością*) oznacza, że wszystkie twierdzenia systemu są prawdziwe względem przyjętej semantyki, to *pełność* jest własnością mówiącą o tym, że każda formuła prawdziwa daje się udowodnić w systemie. Jest wiele różnych dowodów twierdzenia o pełności dla rachunku zdań. My podamy elegancki dowód pochodzący od L. Kalmára. Dla udowodnienia nieco silniejszej wersji twierdzenia o pełności (Twierdzenie 6.7) wykorzystamy silne i bardzo pożyteczne Twierdzenie 6.5 zwane twierdzeniem o zwartości.

Lemat 6.1 (Kalmár) *Niech φ będzie formułą zbudowaną przy użyciu $\to$ oraz $\bot$, o zmiennych zawartych w zbiorze $\{q_1, \dots q_n\}$ i niech $\varrho : ZZ \to \{0,1\}$ będzie dowolnym wartościowaniem. Dla $i = 1, \dots, n$ definiujemy formuły:*

$$q_i' = \begin{cases} q_i & \text{jeśli } \varrho(q_i) = 1, \\ \neg q_i & \text{jeśli } \varrho(q_i) = 0. \end{cases}$$

Niech φ' będzie formułą identyczną z φ, jeśli $\models \varphi[\varrho]$, w przeciwnym razie niech φ' oznacza formułę $\neg\varphi$. Wówczas

$$\{q_1', \dots, q_n'\} \vdash_H \varphi'.$$

Dowód: Dowód jest prowadzony przez indukcję ze względu na budowę formuły φ. Jeśli φ jest zmienną q_i to $\varphi' = q_i'$. Zatem trywialnie zachodzi $\{q_1', \dots, q_n'\} \vdash \varphi'$.

Jeśli φ jest stałą $\bot$, to $\varphi' = \neg\bot$ i oczywiście dla dowolnego wyboru $q_1', \dots, q_n'$ zachodzi

$$\{q_1', \dots, q_n'\} \vdash_H \neg\bot.$$

Załóżmy teraz, że φ jest postaci $\psi \to \vartheta$ i rozważmy następujące przypadki.

(A) $\not\models \psi[\varrho]$.
Wówczas $\varphi' = \varphi$ oraz $\psi' = \neg\psi$. Z założenia indukcyjnego mamy $\{q_1', \dots, q_n'\} \vdash_H \neg\psi$. Zatem $\{q_1', \dots, q_n'\}, \psi \vdash_H \bot$. Z Lematu 5.4(2) mamy $\{q_1', \dots, q_n'\}, \psi \vdash_H \bot \to \vartheta$. Zatem, stosując (MP) dostajemy $\{q_1', \dots, q_n'\}, \psi \vdash_H \vartheta$ i z twierdzenia o dedukcji

$$\{q_1', \dots, q_n'\} \vdash_H \psi \to \vartheta.$$

(B) $\models \vartheta[\varrho]$.
Wówczas $\varphi' = \varphi$, oraz $\vartheta' = \vartheta$. Z założenia indukcyjnego mamy $\{q_1', \dots, q_n'\} \vdash_H \vartheta$. Zatem $\{q_1', \dots, q_n'\}, \psi \vdash_H \vartheta$ i z twierdzenia o dedukcji dostajemy

$$\{q_1', \dots, q_n'\} \vdash_H \psi \to \vartheta.$$

(C) $\models \psi[\varrho]$ oraz $\not\models \vartheta[\varrho]$.
Wówczas $\varphi' = \neg\varphi$. $\psi' = \psi$ oraz $\vartheta' = \neg\vartheta$. Z założenia indukcyjnego mamy

$$\{q_1', \dots, q_n'\} \vdash_H \psi \text{ oraz } \{q_1', \dots, q_n'\} \vdash_H \neg\vartheta.$$

Z Lematu 5.4(1) mamy

$$\{q'_1, \ldots, q'_n\} \vdash_H \psi \to (\neg\vartheta \to \neg(\psi \to \vartheta)).$$

Stosując teraz dwukrotnie (MP) dostajemy

$$\{q'_1, \ldots, q'_n\} \vdash_H \neg(\psi \to \vartheta).$$

To kończy dowód lematu. ∎

Lemat 6.2 *Dla dowolnego zbioru formuł Δ i dla dowolnych formuł φ i ψ, jeśli $\Delta, \varphi \vdash_H \psi$ oraz $\Delta, \neg\varphi \vdash_H \psi$, to $\Delta \vdash_H \psi$.*

Dowód: Jeśli $\Delta, \varphi \vdash_H \psi$ to na mocy twierdzenia o dedukcji mamy $\Delta \vdash_H \varphi \to \psi$. Podobnie dostajemy $\Delta \vdash_H \neg\varphi \to \psi$. Stosując Lemat 5.4(3), oraz dwukrotnie regułę odrywania dostajemy $\Delta \vdash_H \psi$. ∎

Lemat Kalmára odgrywa kluczową rolę w dowodzie poniższego twierdzenia o pełności.

Twierdzenie 6.3 (o pełności dla $\vdash_H$) *Jeśli φ jest tautologią zbudowaną przy użyciu $\to$ oraz $\bot$, to $\vdash_H \varphi$.*

Dowód: Załóżmy, że φ jest tautologią. Niech $\{q_1, \ldots, q_n\}$ będą wszystkimi zmiennymi występującymi w φ. Dla dowolnej liczby $0 \leq m \leq n$ nazwiemy *m-zbiorem* każdy zbiór formuł $\{q'_1, \ldots, q'_m\}$, gdzie q'_i jest albo q_i lub $\neg q_i$. Zauważmy, że 0-zbiór jest pusty.

Udowodnimy następującą własność: dla każdego m spełniającego $0 \leq m \leq n$,

$$\text{jeśli } \Delta \text{ jest } m\text{-zbiorem, to } \Delta \vdash_H \varphi. \tag{2}$$

Zauważmy, że biorąc $m = 0$ w (2) dostajemy tezę twierdzenia. Dowód (2) przeprowadzimy przez indukcję ze względu na m w zbiorze $\{0, \ldots, n\}$ uporządkowanym relacją $\leq^{-1}$. Dla $m = n$ własność (2) wynika z Lematu 6.1 oraz z faktu, że φ jest tautologią. Załóżmy, że (2) zachodzi dla pewnego $0 < m < n$ i niech Δ będzie dowolnym $(m-1)$-zbiorem. Z założenia indukcyjnego dostajemy

$$\Delta, q_m \vdash_H \varphi$$

oraz

$$\Delta, \neg q_m \vdash_H \varphi.$$

Zatem na mocy Lematu 6.2 dostajemy

$$\Delta \vdash_H \varphi.$$

To kończy dowód (2) i tym samym dowód twierdzenia o pełności. ∎

Korzystając z Lematu 5.6 natychmiast dostajemy twierdzenie o pełności dla systemu $\vdash_{H^+}$ ze wszystkimi spójnikami zdaniowymi.

Twierdzenie 6.4 (o pełności dla $\vdash_{H^+}$) *Jeśli φ jest tautologią, to $\vdash_{H^+} \varphi$.*

Dowód: Ponieważ $\vdash_{H^+} \varphi \to \tilde{\varphi}$, więc z twierdzenia o poprawności wynika, że $\models \varphi \to \tilde{\varphi}$. A zatem $\tilde{\varphi}$ jest tautologią. Z twierdzenia o pełności dla systemu $\vdash_H$ dostajemy $\vdash_H \tilde{\varphi}$. Stąd $\vdash_{H^+} \tilde{\varphi}$ i ponieważ $\vdash_{H^+} \tilde{\varphi} \to \varphi$ (por. Lemat 5.6) więc stosując (MP) dostajemy $\vdash_{H^+} \tilde{\varphi}$ ∎

6.1 Elementy teorii modeli

Powiemy, że zbiór formuł Δ jest *spełnialny* gdy istnieje wartościowanie $\varrho : \mathrm{ZZ} \to \{0,1\}$ spełniające wszystkie formuły ze zbioru Δ.

Twierdzenie 6.5 (o zwartości) *Zbiór formuł Δ jest spełnialny wtedy i tylko wtedy, gdy każdy skończony podzbiór zbioru Δ jest spełnialny.*

Dowód: Powiemy, że zbiór Δ jest *skończenie spełnialny*, gdy każdy skończony podzbiór zbioru Δ jest spełnialny.

Szkic dowodu twierdzenia o zwartości wygląda następująco. Bez zmniejszenia ogólności możemy przyjąć, że wszystkie rozważane formuły są zbudowane przy użyciu jedynie spójników $\to$ oraz $\bot$. Używając lematu Kuratowskiego-Zorna pokazujemy najpierw, że istnieje maksymalny skończenie spełnialny zbiór formuł Γ zawierający Δ. Oczywiście mamy

$$\bot \notin \Gamma. \tag{3}$$

Ponadto, dla dowolnej formuły φ mamy

$$\text{jeśli } \varphi \notin \Gamma, \text{ to } \neg\varphi \in \Gamma. \tag{4}$$

Istotnie, jeśli φ oraz $\neg\varphi$ nie należą do Γ, to istnieją skończone zbiory $X, Y \subseteq \Gamma$, takie że $X \cup \{\varphi\}$ oraz $Y \cup \{\neg\varphi\}$ nie są spełnialne. Wynika stąd, że zbiory wartościowań spełniających X oraz Y są rozłączne. Tak więc $X \cup Y$ nie jest spełnialny, a otrzymana sprzeczność dowodzi (4).

Zatem dla dowolnych formuł φ, ψ,

$$(\varphi \to \psi) \in \Gamma \quad \text{wtedy i tylko wtedy, gdy} \quad \varphi \notin \Gamma \text{ lub } \psi \in \Gamma. \tag{5}$$

Rzeczywiście, jeśli $(\varphi \to \psi)$ i φ należą do Γ oraz $\psi \notin \Gamma$, to $\neg\psi \in \Gamma$ na mocy (4). Wówczas niespełnialny zbiór $\{(\varphi \to \psi), \varphi, \neg\psi\}$ jest podzbiorem Γ, co dowodzi implikacji z lewej do prawej w (5). Na odwrót, jeśli $(\varphi \to \psi) \notin \Gamma$, to na mocy (4) mamy $\neg(\varphi \to \psi) \in \Gamma$. Jeśli teraz $\psi \in \Gamma$, to niespełnialny zbiór $\{\neg(\varphi \to \psi), \psi\}$ jest podzbiorem Γ. Podobnie, jeśli $\varphi \notin \Gamma$, to $\neg\varphi \in \Gamma$, więc $\{\neg(\varphi \to \psi), \psi\} \subseteq \Gamma$, co kończy dowód (5).

Teraz możemy zdefiniować wartościowanie $\varrho : \mathrm{ZZ} \to \{0,1\}$ tak, że dla dowolnej zmiennej $p \in \mathrm{ZZ}$ warunki $\varrho(p) = 1$ i $p \in \Gamma$ są równoważne. Z następującej własności wynika, że ϱ spełnia wszystkie formuły ze zbioru Γ, a zatem Δ jest zbiorem spełnialnym.

Dla dowolnej formuły φ,

$$\models \varphi[\varrho] \qquad \text{wtedy i tylko wtedy, gdy} \qquad \varphi \in \Gamma. \tag{6}$$

Dowód (6) przeprowadzamy przez indukcję ze względu na budowę formuły φ. Własności (3) używamy w przypadku gdy φ jest $\bot$, a własności (5) w przypadku, gdy zewnętrznym spójnikiem φ jest $\rightarrow$. ∎

Przykład 6.6 Podamy przykład zastosowania twierdzenia o zwartości. Pokażemy, że jeśli nieskończonej mapy (o przeliczalnej liczbie krajów) nie da się pokolorować przy pomocy k kolorów, to istnieje skończony fragment tej mapy, którego też nie da się pokolorować przy pomocy k kolorów. Niech I będzie zbiorem krajów tej mapy. Rozważmy zmienne zdaniowe $p_{i,j}$, gdzie $i \in I$ oraz $j < k$. Wartościowania będą odpowiadać kolorowaniom mapy. Intencją jest to aby wartościowanie przypisywało zmiennej $p_{i,j}$ wartość 1 wtedy i tylko wtedy, gdy kraj i ma na mapie kolor j. Poniższe formuły przedstawiają podstawowe warunki dotyczące kolorowania.

Każdy kraj ma jakiś kolor: dla każdego $i \in I$ wyraża to formuła

$$p_{i,0} \vee p_{i,1} \vee \ldots \vee p_{i,k-1}.$$

Każdy kraj ma co najwyżej jeden kolor: dla każdego $i \in I$, oraz każdych $i, j < k$, jeśli $j \neq j'$ to mamy formułę

$$\neg(p_{i,j} \wedge p_{i,j'}).$$

Każde dwa sąsiadujące kraje mają różne kolory: dla $i, i' \in I$ takich, że i oraz i' sąsiadują oraz dla każdego $j < k$ rozważmy formułę

$$\neg(p_{i,j} \wedge p_{i',j}).$$

Niech Δ będzie zbiorem wszystkich formuł przedstawionych wyżej. Łatwo jest zauważyć, że Δ jest spełnialny wtedy i tylko wtedy, gdy mapę da się pokolorować k kolorami. Zatem jeśli mapy nie da się pokolorować k kolorami to Δ nie jest spełnialny i z twierdzenia o zwartości wynika, że istnieje skończony podzbiór Δ_0, który nie jest spełnialny. Wówczas fragmentu mapy zawierającego kraje wymienione w indeksach zmiennych występujących w formułach z Δ_0 nie da się pokolorować przy pomocy k kolorów.

Jako wniosek z twierdzenia o zwartości otrzymujemy następujące wzmocnienie twierdzenia o pełności (por. Twierdzenie 6.4).

Twierdzenie 6.7 („Silne" twierdzenie o pełności) *Dla dowolnego zbioru formuł Δ oraz dowolnej formuły φ, jeśli φ jest semantyczną konsekwencją zbioru Δ, to $\Delta \vdash_{H^+} \varphi$.*

Dowód: Jeśli $\Delta \models \varphi$ to zbiór $\Delta \cup \{\neg\varphi\}$ nie jest spełnialny. Na mocy twierdzenia o zwartości istnieje skończony podzbiór $\Delta_0 \subseteq \Delta$ taki, że $\Delta_0 \cup \{\neg\varphi\}$ nie jest spełnialny. Zatem $\Delta_0 \models \varphi$.

Tak więc jeśli $\Delta_0 = \{\psi_1, \ldots, \psi_n\}$ to oczywiście formuła $\psi_1 \to (\psi_2 \to \cdots \to (\psi_n \to \varphi)\cdots)$ jest tautologią. Z twierdzenia o pełności wnioskujemy, że $\vdash_{H^+} \psi_1 \to (\psi_2 \to \cdots \to (\psi_n \to \varphi)\cdots)$. Stosując n razy (MP) do powyższej formuły dostajemy

$$\Delta_0 \vdash_{H^+} \varphi.$$

Tak więc $\Delta \vdash_{H^+} \varphi$, co kończy dowód twierdzenia. ∎

Powiemy, że zbiór formuł Δ jest *sprzeczny*, gdy $\Delta \vdash_H \bot$. Zbiór, który nie jest sprzeczny nazwiemy *niesprzecznym*. Oto nieco inne sformułowanie „silnego" twierdzenia o pełności:

Twierdzenie 6.8 *Zbiór formuł jest spełnialny wtedy i tylko wtedy, gdy jest niesprzeczny.*

Dowód: Zauważmy, że zbiór Δ jest spełnialny wtedy i tylko wtedy, gdy $\Delta \not\models \bot$. A zatem teza wynika z Twierdzeń 5.5 i 6.7, jeśli przyjmiemy $\varphi = \bot$. ∎

A oto twierdzenie o pełności dla rachunku sekwentów i naturalnej dedukcji.

Wniosek 6.9 *Jeśli* $\Delta \models \varphi$ *to* $\Delta \vdash_G \varphi$ *oraz* $\Delta \vdash_N \varphi$.

Dowód: Natychmiast z Twierdzeń 5.8, 5.9 i 6.7. ∎

Ćwiczenia

1. Dowieść, że „silne" twierdzenie o pełności (Twierdzenie 6.7) pociąga twierdzenie o zwartości.
2. Udowodnić, że jeśli w systemie $\vdash_{H^+}$ zamienimy aksjomaty (B1–B4) na aksjomaty

   (D1) $\varphi \to \varphi \vee \psi$;
   (D2) $\psi \to \varphi \vee \psi$;
   (D3) $(\varphi \to \vartheta) \wedge (\psi \to \vartheta) \to (\varphi \vee \psi \to \vartheta)$;
   (C1) $\varphi \wedge \psi \to \varphi$;
   (C2) $\varphi \wedge \psi \to \psi$;
   (C3) $(\vartheta \to \varphi) \wedge (\vartheta \to \psi) \to (\vartheta \to \varphi \wedge \psi)$.

   to twierdzenie o pełności pozostanie prawdziwe.
3. Dany jest nieskończony zbiór chłopców, z których każdy ma skończoną liczbę narzeczonych. Ponadto dla każdego $k \in N$, dowolnych k chłopców ma co najmniej k narzeczonych. Dowieść, że każdy chłopiec może się ożenić z jedną ze swoich narzeczonych bez popełnienia bigamii.

7 Pełność rachunku predykatów

7.1 Hilbertowski system dowodzenia

Poniższy system dowodzenia dotyczy formuł pierwszego rzędu nad ustaloną sygnaturą Σ, zbudowanych w oparciu o spójniki $\to$, $\bot$ oraz kwantyfikator $\forall$. Przypomnijmy, że $\neg\varphi$ oznacza formułę $\varphi \to \bot$.

Przez *generalizację* formuły φ będziemy rozumieć dowolną formułę postaci $\forall x_1 \ldots \forall x_n \varphi$, gdzie $x_1, \ldots x_n$ są dowolnymi zmiennymi.

Aksjomaty

Dowolne generalizacje formuł postaci:

(A1) $\varphi \to (\psi \to \varphi)$;
(A2) $(\varphi \to (\psi \to \vartheta)) \to ((\varphi \to \psi) \to (\varphi \to \vartheta))$;
(A3) $\neg\neg\varphi \to \varphi$;
(A4) $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$;
(A5) $\varphi \to \forall x\varphi$, o ile $x \notin FV(\varphi)$;
(A6) $\forall x\varphi \to \varphi(\sigma/x)$, o ile σ jest dopuszczalny dla x w φ;
(A7) $x = x$;
(A8) $x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \cdots)$, dla $f \in \Sigma_n^F,\ n \geq 0$;
(A9) $x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to (r(x_1, \ldots, x_n) \to r(y_1, \ldots, y_n))) \cdots)$, dla $r \in \Sigma_n^R,\ n \geq 1$.

Reguły dowodzenia

$$\text{(MP)} \qquad \frac{\varphi \qquad \varphi \to \psi}{\psi}$$

Pojęcie dowodu formalnego w powyższym systemie definiuje się dokładnie tak samo jak w przypadku rachunku zdań (por. Rozdział 5). Piszemy też $\Delta \vdash_H \varphi$, gdy istnieje dowód formuły φ ze zbioru hipotez Δ. Sam system, podobnie jak w przypadku rachunku zdań, będziemy oznaczać przez $\vdash_H$. Nie powinno prowadzić to do niejednoznaczności. Zwróćmy uwagę, że system $\vdash_H$ zależy od sygnatury Σ. Tak więc mamy różne systemy dla różnych sygnatur. Pojęcie niesprzecznego zbioru formuł definiuje się tak samo jak w rachunku zdań.

Przykład 7.1 Pokażemy główne kroki dowodu formuły $(x = y \to y = x)$.

1. $\forall x_1 \forall x_2 \forall y_1 \forall y_2 (x_1 = y_1 \to (x_2 = y_2 \to (x_1 = x_2 \to y_1 = y_2)))$ (A9)
2. $x = y \to (x = x \to (x = x \to y = x))$ na mocy (A6) oraz (MP)
3. $x = x \to (x = y \to (x = x \to y = x))$ z (2), jest to instancja tautologii zdaniowej
4. $x = x$ (A7)

5. $x = y \to (x = x \to y = x)$ (MP(4,3))

6. $x = x \to (x = y \to y = x)$ z (5), jest to instancja tautologii zdaniowej

7. $x = x$ (A7)

8. $x = y \to y = x$ (MP(7,6))

Twierdzenie 7.2 (o dedukcji) *Dla dowolnego zbioru formuł Δ oraz dowolnych formuł φ, ψ, jeśli $\Delta, \varphi \vdash_H \psi$, to $\Delta \vdash_H \varphi \to \psi$.*

Dowód: Dowód tego twierdzenia jest dokładnie taki sam jak analogicznego twierdzenia dla rachunku zdań (por. Twierdzenie 5.2). ∎

Natępujące twierdzenie mówi, że wybór nazwy zmiennej związanej nie ma wpływu na dowodliwość formuły. Jest to tzw. własność *α-konwersji*.

Twierdzenie 7.3 (o α-konwersji) *Jeśli $\Delta \vdash_H \forall x\, \psi$ oraz zmienna $y \notin FV(\forall x\, \psi)$ jest dopuszczalna dla x w ψ, to $\Delta \vdash_H \forall y\, \psi(y/x)$.*

Dowód: Ponieważ $y \notin FV(\forall x\, \psi)$, to na mocy (A5) mamy

$$\Delta \vdash_H \forall x\, \psi \to \forall y \forall x\, \psi. \tag{7}$$

Z drugiej strony mamy następującą wersję aksjomatu (A6)

$$\Delta \vdash_H \forall y\, (\forall x\, \psi \to \psi(y/x)),$$

co łącznie z aksjomatem (A4) daje

$$\Delta \vdash_H \forall y \forall x\, \psi \to \forall y\, \psi(y/x). \tag{8}$$

Tak więc, zakładając $\Delta \vdash_H \forall x\, \psi$ i stosując (MP) do (7), a następnie do (8) dostajemy

$$\Delta \vdash_H \forall y\, \psi(y/x),$$

co kończy dowód. ∎

Podamy jeszcze jedno użyteczne twierdzenie. Mówi ono, że tzw. *reguła generalizacji* jest dopuszczalna w systemie $\vdash_H$. Niech

$$FV(\Delta) = \bigcup \{FV(\varphi) \mid \varphi \in \Delta\}.$$

Twierdzenie 7.4 (o generalizacji) *Jeśli zachodzi $\Delta \vdash_H \varphi$, to dla dowolnej zmiennej x, takiej że $x \notin FV(\Delta)$, mamy $\Delta \vdash_H \forall x\, \varphi$.*

Dowód: Dowodzimy twierdzenie przez indukcję ze względu na liczbę kroków w dowodzie formuły φ ze zbioru hipotez Δ. Jeśli φ jest jednym z aksjomatów (A1–9), to dowolna generalizacja tej formuły jest też aksjomatem, więc teza zachodzi. Aby pokazać $\Delta \vdash_H \forall x\, \varphi$, dla formuły $\varphi \in \Delta$ używamy aksjomatu (A5) i reguły (MP).

Jeśli ostatnim krokiem w dowodzie było zastosowanie (MP), to dla pewnej formuły ψ mamy $\Delta \vdash_H \psi \to \varphi$ oraz $\Delta \vdash_H \psi$ w mniejszej liczbie kroków. Z założenia indukcyjnego otrzymujemy $\Delta \vdash_H \forall x\, (\psi \to \varphi)$ oraz $\Delta \vdash_H \forall x\, \psi$. Zatem stosując (MP) do $\forall x\, (\psi \to \varphi)$ oraz do instancji $\forall x(\psi \to \varphi) \to (\forall x\psi \to \forall x\varphi)$ aksjomatu (A4) otrzymujemy $\forall x\psi \to \forall x\varphi$. Ponowne zastosowanie (MP) do tej formuły oraz do $\forall x\, \psi$ daje nam $\forall x\, \varphi$. ∎

Powiemy, że formuła φ jest *konsekwencją semantyczną* zbioru formuł Δ (i napiszemy $\Delta \models \varphi$), gdy dla każdej struktury $\mathfrak{A}$ i dla każdego wartościowania ϱ w $\mathfrak{A}$ spełniającego wszystkie formuły ze zbioru Δ, mamy $(\mathfrak{A}, \varrho) \models \varphi$. Zwróćmy uwagę, że jeśli Δ jest zbiorem zdań, to powyższa definicja jest równoważna następującej własności: każdy model dla Δ jest modelem dla φ. W ogólnym przypadku, gdy formuły z Δ mogą zawierać zmienne wolne, powyższe dwie definicje nie są równoważne. Na przykład, jeśli f jest symbolem operacji jednoargumentowej, to $x = y \not\models f(z) = z$, ale każdy model dla $x = y$ (czyli jednoelementowy) jest modelem dla $f(z) = z$.

Twierdzenie 7.5 (o poprawności)
Dla dowolnego zbioru formuł Δ i formuły φ, jeśli $\Delta \vdash_H \varphi$, to $\Delta \models \varphi$.

Dowód: Dowód przeprowadzamy przez indukcję ze względu na liczbę kroków w dowodzie formuły φ ze zbioru hipotez Δ. Jeśli $\varphi \in \Delta$, to oczywiście mamy $\Delta \models \varphi$. Sprawdzamy, że jeśli φ jest dowolną generalizacją jednego z aksjomatów (A1–9), to zachodzi $\models \varphi$. Oczywiście reguła (MP) zachowuje relację semantycznej konsekwencji, tzn. jeśli $\Delta \models \varphi$ i $\Delta \models \varphi \to \psi$, to $\Delta \models \psi$. ∎

Twierdzenie o poprawności może być użyte do pokazania, że pewne wynikania nie dają się wyprowadzić w systemie $\vdash_H$. Przykładowo, zobaczmy, że $x = y \not\vdash_H \forall x\, (x = y)$. Istotnie, biorąc dwuelementową strukturę $\mathfrak{A}$ oraz wartościowanie, które „skleja" wartości zmiennych x oraz y, dostajemy $x = y \not\models \forall x\, (x = y)$. Zatem z twierdzenia o poprawności wnioskujemy, że $x = y \not\vdash_H \forall x\, (x = y)$. Jest to również przykład na to, że system $\vdash_H$ nie jest zamknięty ze względu na dowolne generalizacje, tzn. założenie $x \notin FV(\Delta)$ w twierdzeniu o generalizacji jest istotne.

Zachodzi również odwrotne twierdzenie do Twierdzenia 7.5. Dowód tego twierdzenia jest celem niniejszego rozdziału.

System formalny dla formuł zawierających pozostałe spójniki: $\wedge$, $\vee$ i kwantyfikator egzystencjalny otrzymuje się z $\vdash_H$ przez dodanie aksjomatów charakteryzujących te symbole:

(B1) $\varphi \wedge \psi \to \neg(\varphi \to \neg\psi)$
(B2) $\neg(\varphi \to \neg\psi) \to \varphi \wedge \psi$
(B3) $\varphi \vee \psi \to (\neg\varphi \to \psi)$
(B4) $(\neg\varphi \to \psi) \to \varphi \vee \psi$

(B5) $\exists x\, \varphi \to \neg\forall x\, \neg\varphi$
(B6) $\neg\forall x\, \neg\varphi \to \exists x\, \varphi$

Głównym narzędziem w dowodzie „silnego" twierdzenia o pełności będzie tzw. *twierdzenie o istnieniu modelu*. Metoda dowodu tego twierdzenia polega na budowaniu modelu ze stałych. Zaproponował ją L. Henkin.

Najpierw wprowadzimy następującą definicję. Niech Γ będzie zbiorem zdań pierwszego rzędu nad sygnaturą Σ oraz niech $C \subseteq \Sigma_0$ będzie pewnym zbiorem stałych. Powiemy, że Γ jest zbiorem *C-nasyconym*, gdy Γ jest zbiorem niesprzecznym oraz dla dowolnej formuły $\varphi(x)$ o co najwyżej jednej zmiennej wolnej x, jeśli $\Gamma \nvdash_H \forall x\, \varphi(x)$, to istnieje stała $c \in C$, taka że $\Gamma \vdash_H \neg\varphi(c/x)$.

Niech Γ będzie C-nasycony. Zauważmy, że jeśli $\Gamma \vdash_H \neg\forall x\, \varphi(x)$ oraz jeśli φ jest postaci $\neg\psi$, to wówczas $\Gamma \vdash_H \neg\forall x\ \varphi(x)$ jest równoważne $\Gamma \vdash_H \exists x\ \psi(x)$. Ponadto z warunku C-nasycenia Γ wynika istnienie stałej $c \in C$ takiej, że $\Gamma \vdash_H \neg\varphi(c/x)$. To ostatnie jest równoważne (na mocy prawa podwójnego przeczenia) temu, że $\Gamma \vdash_H \psi(c/x)$. Tak więc w tym przypadku c jest „świadkiem" zachodzenia własności $\Gamma \vdash_H \exists x\ \psi(x)$.

Mocą sygnatury Σ nazwiemy moc zbioru $(\bigcup_{n=0}^{\infty} \Sigma_n^F) \cup (\bigcup_{n=1}^{\infty} \Sigma_n^R)$. Moc sygnatury Σ będziemy oznaczać przez $|\Sigma|$.

Dopuścimy możliwość rozszerzenia sygnatury o stałe. Dla dowolnego zbioru C rozłącznego z sygnaturą Σ, przez $\Sigma(C)$ będziemy oznaczać sygnaturę powstałą z Σ przez dodanie symboli stałych ze zbioru C.

Lemat 7.6 (o nasyceniu) *Niech C będzie nieskończonym zbiorem, rozłącznym z sygnaturą Σ oraz takim, że $|\Sigma| \leq |C|$. Niech Δ będzie niesprzecznym zbiorem zdań nad Σ. Istnieje zbiór zdań Γ nad sygnaturą $\Sigma(C)$ taki, że $\Delta \subseteq \Gamma$ oraz Γ jest C-nasycony.*

Dowód: Bez zmniejszenia ogólności możemy przyjąć, że istnieje zmienna z nie występująca wolno w żadnej formule ze zbioru Δ (w przeciwnym przypadku możemy tak przenumerować zmienne, aby ten warunek był spełniony). Przedstawimy dowód dla przypadku kiedy Σ i C są zbiorami przeliczalnymi. Dowód ogólnego przypadku pozostawimy Czytelnikowi jako ćwiczenie (należy zastosować indukcję pozaskończoną). Ustawmy zbiór wszystkich formuł nad $\Sigma(C)$ o jednej zmiennej wolnej x w ciąg $\varphi_0, \varphi_1, \ldots$ Zdefiniujemy ciąg zbiorów $\{\Gamma_n \mid n \in \mathbb{N}\}$ oraz ciąg stałych $\{c_n \mid n \in \mathbb{N}\} \subseteq C$ o następujących własnościach:

- Γ_n zawiera skończenie wiele stałych z C.
- $\Delta \subseteq \Gamma_n$ jest niesprzecznym zbiorem zdań nad $\Sigma(C)$.
- Jeśli $\Gamma_n \nvdash_H \forall x\, \varphi_n(x)$, to $\Gamma_{n+1} = \Gamma_n \cup \{\neg\varphi_n(c_n/x)\}$.

Ustalmy dowolną stałą $c_* \in C$. Przyjmujemy $\Gamma_0 = \Delta$. Jeśli $\Gamma_n \vdash_H \forall x\, \varphi_n(x)$, to definiujemy $\Gamma_{n+1} = \Gamma_n$ oraz $c_n = c_*$. Jeśli natomiast $\Gamma_n \nvdash_H \forall x\, \varphi_n(x)$ to niech $c_n \in C$ będzie stałą nie

występującą w Γ_n ani w φ_n. Musimy pokazać, że $\Gamma_{n+1} = \Gamma_n \cup \{\neg\varphi_n(c_n/x)\}$ jest zbiorem niesprzecznym. Załóżmy przeciwnie, że

$$\Gamma_{n+1} \vdash_H \bot.$$

Zatem $\Gamma_n \vdash_H \neg\neg\varphi_n(c_n/x)$ i z (A3) dostajemy $\Gamma_n \vdash_H \varphi_n(c_n/x)$. Ponieważ c_n nie występuje w Γ_n ani w φ_n to możemy w dowodzie powyższego sekwentu zamienić wszystkie wystąpienia c_n przez nową zmienną z, która się w tym dowodzie nie pojawiła oraz nie występuje wolno w formułach z Γ_n. Tak więc otrzymujemy $\Gamma_n \vdash_H \varphi_n(z/x)$ oraz $z \notin FV(\Gamma_n)$. Na mocy Twierdzenia 7.4 o generalizacji dostajemy $\Gamma_n \vdash_H \forall z\, \varphi_n(z/x)$. Ponieważ x jest dopuszczalna dla z w $\varphi_n(z/x)$ oraz $\varphi_n(z/x)(x/z) = \varphi_n(x)$, to stosując α-konwersję (Twierdzenie 7.3) dostajemy $\Gamma_n \vdash_H \forall x\, \varphi_n(x)$, wbrew założeniu. W ten sposób udowodniliśmy niesprzeczność zbioru Γ_{n+1}. To kończy konstrukcję zbiorów Γ_n oraz stałych c_n.

Niech

$$\Gamma = \bigcup_{n\in N} \Gamma_n.$$

Pokażemy, że Γ jest zbiorem C-nasyconym. Oczywiście Γ jako suma łańcucha zbiorów niesprzecznych jest również zbiorem niesprzecznym. Niech $\varphi(x)$ będzie dowolną formułą nad $\Sigma(C)$ o jednej zmiennej wolnej i załóżmy, że $\Gamma \nvdash_H \forall x\, \varphi(x)$. Niech $\varphi(x) = \varphi_n(x)$, dla pewnego n. Oczywiście mamy $\Gamma_n \nvdash_H \forall x\, \varphi_n(x)$ i z konstrukcji zbiorów Γ_n wynika, że $\Gamma_{n+1} \vdash_H \neg\varphi_n(c_n/x)$. Zatem $\Gamma \vdash_H \neg\varphi_n(c_n/x)$, co dowodzi C-nasycenia zbioru Γ. ∎

7.2 Konstrukcja modelu ze stałych

Niech $C \subseteq \Sigma_0$ będzie dowolnym zbiorem stałych i niech Γ będzie dowolnym C-nasyconym zbiorem zdań nad Σ. W zbiorze C definiujemy relację równoważności $\sim$:

$$c_1 \sim c_2 \qquad \text{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H c_1 = c_2.$$

Zdefiniujemy strukturę $\mathfrak{A}_\Gamma$. Nośnikiem tej struktury jest zbiór ilorazowy $C/\sim$. Musimy określić interpretację symboli operacji i relacji z Σ. Dla przykładu załóżmy, że $f \in \Sigma_2^F$ jest symbolem operacji dwuargumentowej. Funkcję $f^{\mathfrak{A}_\Gamma} : (C/\sim)^2 \to C/\sim$ definiujemy warunkiem

$$f^{\mathfrak{A}_\Gamma}([c_1]_\sim, [c_2]_\sim) = [d]_\sim \qquad \text{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H f(c_1, c_2) = d.$$

Dla pokazania, że $f^{\mathfrak{A}_\Gamma}$ jest dobrze określoną funkcją musimy sprawdzić, że:

$$\text{Dla dowolnych } c_1, c_2 \in C \text{ istnieje } d \in C \text{ takie, że } \Gamma \vdash_H f(c_1, c_2) = d \tag{9}$$

$$\text{Jeśli } c_1 \sim c_1',\ c_2 \sim c_2' \text{ oraz } \Gamma \vdash_H f(c_1, c_2) = d \text{ i } \Gamma \vdash_H f(c_1', c_2') = d',\ \text{to } d \sim d'. \tag{10}$$

Własność (9) wynika z faktu, że zbiór Γ jest C-nasycony. Zauważmy najpierw, że $\Gamma \vdash_H \neg\forall x\, \neg f(c_1, c_2) = x$. Istotnie, załóżmy $\forall x\, \neg f(c_1, c_2) = x$. Wówczas z aksjomatu (A6) dostajemy $\neg f(c_1, c_2) = f(c_1, c_2)$. Z drugiej strony, z aksjomatu (A7) i (A6) dostajemy $f(c_1, c_2) = f(c_1, c_2)$. Tak więc otrzymujemy $\bot$, a więc $\Gamma \vdash_H \neg\forall x\, \neg f(c_1, c_2) = x$. Zatem z C-nasycenia Γ wynika istnienie stałej $d \in C$ takiej, że $\Gamma \vdash_H \neg\neg f(c_1, c_2) = d$. Korzystając teraz z (A3) dostajemy $\Gamma \vdash_H f(c_1, c_2) = d$.

Własność (10) wynika natychmiast z następującej postaci aksjomatu (A8) (postać tę otrzymujemy z (A8) z pomocą aksjomatu (A6))

$$c_1 = c_1' \to (c_2 = c_2' \to f(c_1, c_2) = f(c_1', c_2')).$$

Interpretacja symboli relacji w $\mathfrak{A}_\Gamma$ wygląda podobnie. Dla przykładu zdefiniujemy relację $r^{\mathfrak{A}_\Gamma}$ dla symbolu $r \in \Sigma_2^R$.

$$([c_1]_\sim, [c_2]_\sim) \in r^{\mathfrak{A}_\Gamma} \qquad \text{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H r(c_1, c_2).$$

W tym przypadku również musimy dowieść poprawności definicji (tzn. niezależności od wyboru reprezentantów). Czyli musimy pokazać, że jeśli $c_1 \sim c_1'$ oraz $c_2 \sim c_2'$, to

$$\Gamma \vdash_H r(c_1, c_2) \qquad \text{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H r(c_1', c_2').$$

Wynika to natychmiast z aksjomatów (A9) i (A6).

Teraz możemy przejść do twierdzenia o istnieniu modelu.

Twierdzenie 7.7 (o istnieniu modelu) *Każdy niesprzeczny zbiór zdań nad dowolną sygnaturą Σ ma model, którego moc nie przekracza* $\max\{\aleph_0, |\Sigma|\}$*.Dokładniej, dla struktury $\mathfrak{A}_\Gamma$ zbudowanej powyżej oraz dowolnej formuły φ takiej, że $FV(\varphi) \subseteq \{x_1, \ldots, x_n\}$ i dla dowolnego wartościowania ϱ takiego, że $\varrho(x_i) = [c_i]_\sim$, dla $i = 1, \ldots, n$ mamy*

$$(\mathfrak{A}_\Gamma, \varrho) \models \varphi \qquad \textit{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H \varphi(c_1/x_1, \ldots, c_n/x_n). \tag{11}$$

Dowód: Załóżmy, że Δ jest niesprzecznym zbiorem zdań. Niech C będzie dowolnym nieskończonym zbiorem rozłącznym z Σ i takim, że $|C| \geq |\Sigma|$. Z Lematu 7.6 o nasyceniu wiemy, że istnieje zbiór zdań $\Gamma \subseteq \Delta$ nad sygnaturą $\Sigma(C)$, który jest C-nasycony. Stosując lemat Kuratowskiego-Zorna dowodzimy, że istnieje maksymalny zbiór Γ o powyższych własnościach. Niech Γ będzie takim zbiorem. Dalsza część dowodu będzie przebiegała w odniesieniu do ustalonego zbioru Γ.

Najpierw zanotujmy następującą ważną własność zbioru Γ. Dla dowolnego zdania φ,

$$\text{jeśli } \Gamma \nvdash_H \varphi, \text{ to } \Gamma \cup \{\varphi\} \text{ jest zbiorem sprzecznym.} \tag{12}$$

Dla dowodu (12) zauważmy, że jeśli $\Gamma \cup \{\varphi\}$ jest zbiorem niesprzecznym, to jest on C-nasycony. Istotnie, jeśli $\Gamma \cup \{\varphi\} \nvdash_H \forall x\, \psi(x)$, dla pewnej formuły ψ o jednej zmiennej wolnej, to mamy również $\Gamma \nvdash_H \forall x\, \psi(x)$. Zatem dla pewnej stałej $c \in C$ zachodzi $\Gamma \vdash_H \neg\psi(c/x)$, więc oczywiście również $\Gamma \cup \{\varphi\} \vdash_H \neg\psi(c/x)$. Tak więc z maksymalności zbioru Γ wynika, że $\Gamma \cup \{\varphi\}$ musi być zbiorem sprzecznym. To dowodzi (12).

Zauważmy, że z własności (11) wynika pierwsza część twierdzenia, bowiem mamy wówczas $\mathfrak{A}_\Gamma \models \Gamma$. Własność (11) dowodzimy przez indukcję ze względu na budowę formuły φ. Dla formuł atomowych musimy dowieść następującą pomocniczą własność. Dla dowolnego termu t i stałej $d \in C$ mamy

$$[\![t]\!]_\varrho^{\mathfrak{A}_\Gamma} = [d]_\sim \qquad \text{wtedy i tylko wtedy, gdy} \qquad \Gamma \vdash_H t(c_1/x_1, \ldots, c_n/x_n) = d, \tag{13}$$

gdzie $FV(t) \subseteq \{x_1, \ldots, x_n\}$ oraz $v(x_i) = [c_i]_\sim$, dla $i = 1, \ldots, n$. Dowód (13) przeprowadzamy przez rutynową indukcję ze względu na budowę termu t. Szczegóły pozostawiamy Czytelnikowi.

Powracamy do dowodu (11). Jeśli φ jest formułą $t_1 = t_2$, to $[\![t_1]\!]_\varrho^{\mathfrak{A}_\Gamma} = [\![t_2]\!]_\varrho^{\mathfrak{A}_\Gamma}$ wtedy i tylko wtedy, gdy dla pewnego $d \in C$ zachodzi $[\![t_1]\!]_\varrho^{\mathfrak{A}_\Gamma} = [d]_\sim$ oraz $[\![t_2]\!]_\varrho^{\mathfrak{A}_\Gamma} = [d]_\sim$. Na mocy (13) jest to równoważne temu, że dla pewnego $d \in C$ zachodzi $\Gamma \vdash_H t_1(c_1/x_1, \ldots, c_n/x_n) = d$ oraz $\Gamma \vdash_H t_2(c_1/x_1, \ldots, c_n/x_n) = d$. Ostatnia własność jest równoważna (na mocy C-nasycenia zbioru Γ) własności $\Gamma \vdash_H t_1(c_1/x_1, \ldots, c_n/x_n) = t_2(c_1/x_1, \ldots, c_n/x_n)$.

Załóżmy teraz, że φ jest formułą postaci $\psi \to \vartheta$. Niech ψ^* oznacza formułę $\psi(c_1/x_1, \ldots, c_n/x_n)$ oraz niech ϑ^* oznacza formułę $\vartheta(c_1/x_1, \ldots, c_n/x_n)$. Załóżmy, że $(\mathfrak{A}_\Gamma, \varrho) \models \varphi$ i rozważmy dwa przypadki. Jeśli $\Gamma \vdash_H \psi^*$, to na mocy założenia indukcyjnego mamy $(\mathfrak{A}_\Gamma, \varrho) \models \psi$. Zatem $(\mathfrak{A}_\Gamma, \varrho) \models \vartheta$ i korzystając ponownie z założenia indukcyjnego otrzymujemy $\Gamma \vdash_H \vartheta^*$. Dalej na mocy aksjomatu (A1) i reguły (MP) otrzymujemy $\Gamma \vdash_H \psi^* \to \vartheta^*$. Jeśli natomiast $\Gamma \nvdash_H \psi^*$, to jak wynika z (12) zbiór $\Gamma \cup \{\psi^*\}$ jest sprzeczny. Stąd $\Gamma \cup \{\psi^*\} \vdash_H \vartheta^*$ i z twierdzenia o dedukcji (Twierdzenie 7.2) dostajemy ponownie $\Gamma \vdash_H \psi^* \to \vartheta^*$. Dowód implikacji odwrotnej, tzn., że $\Gamma \vdash_H \psi^* \to \vartheta^*$ pociąga $(\mathfrak{A}_\Gamma, \varrho) \models \varphi$ pozostawiamy Czytelnikowi do uzupełnienia.

Na koniec rozważmy przypadek gdy φ jest postaci $\forall y\, \psi(y)$. Załóżmy, że $(\mathfrak{A}_\Gamma, \varrho) \models \varphi$. Niech ψ^* oznacza formułę $\psi(c_1/x_1, \ldots, c_n/x_n)$. Formuła ψ^* ma co najwyżej jedną zmienną wolną y. Jeśli $\Gamma \nvdash_H \forall y\, \psi^*$, to z C-nasycenia Γ istnieje taka stała $d \in C$, że $\Gamma \vdash_H \neg\psi^*(d/y)$. Zatem na mocy założenia indukcyjnego otrzymujemy $(\mathfrak{A}_\Gamma, \varrho_y^{[d]_\sim}) \not\models \psi$, co daje sprzeczność z naszym założeniem $(\mathfrak{A}_\Gamma, \varrho) \models \varphi$. Tak więc musi być $\Gamma \vdash_H \forall y\, \psi^*$. Na odwrót, załóżmy, że $\Gamma \vdash_H \forall y\, \psi^*$ i niech $d \in C$ będzie dowolną stałą. Z aksjomatu (A6) dostajemy $\Gamma \vdash_H \psi^*(d/y)$ i na mocy założenia indukcyjnego dostajemy $(\mathfrak{A}_\Gamma, \varrho_y^{[d]_\sim}) \models \psi$. Ponieważ d jest dowolne, to powyższe spełnianie dowodzi $(\mathfrak{A}_\Gamma, \varrho) \models \varphi$. Tym samym dowód twierdzenia jest zakończony. ∎

Na zakończenie udowodnimy zapowiedziane wcześniej „silne" twierdzenie o pełności dla systemu $\vdash_H$. Jest ono prostym wnioskiem z twierdzenia o istnieniu modelu.

Twierdzenie 7.8 („Silne" twierdzenie o pełności) *Dla dowolnego zbioru formuł Δ i dla dowolnej formuły φ, jeśli $\Delta \models \varphi$, to $\Delta \vdash_H \varphi$. W szczególności, jeśli φ jest tautologią języka pierwszego rzędu, to $\vdash_H \varphi$.*

Dowód: Załóżmy, że $\Delta \nvdash \varphi$. Niech $C = \{c_0, c_1, \ldots\}$ będzie nieskończonym przeliczalnym zbiorem stałych, rozłącznym z sygnaturą Σ. Ustawmy zmienne indywiduowe w ciąg $x_0, x_1, \ldots$ Dla dowolnej formuły ψ nad sygnaturą Σ niech ψ^* oznacza zdanie nad sygnaturą $\Sigma(C)$ otrzymane z ψ przez zastąpienie każdej zmiennej x_n wolno występującej w ψ stałą c_n. Niech $\Delta^* = \{\psi^* \mid \psi \in \Delta\}$.

Twierdzimy, że zbiór zdań $\Delta^* \cup \{\neg\varphi^*\}$ jest zbiorem niesprzecznym. Załóżmy przeciwnie, że

$$\Delta^* \cup \{\neg\varphi^*\} \vdash \bot.$$

Wówczas dla pewnego skończonego podzbioru $\Delta_0 \subseteq \Delta$ mamy $\Delta_0^* \cup \{\neg\varphi^*\} \vdash \bot$. Z twierdzenia o dedukcji dostajemy $\Delta_0^* \vdash \neg\neg\varphi^*$ i na mocy aksjomatu (A3) mamy $\Delta_0^* \vdash \varphi^*$ Przyjmijmy, że

$\Delta_0 = \{\psi_1, \ldots, \psi_n\}$. Stosując n razy twierdzenie o dedukcji, dostajemy

$$\vdash \psi_1^* \to (\cdots \to (\psi_n^* \to \varphi^*) \cdots).$$

Zastępując w powyższym dowodzie stałe c_i nowymi, nigdzie w tym dowodzie nie pojawiającymi się zmiennymi z_i, następnie generalizując (por. Twierdzenie 7.4) i podstawiając na miejsce zmiennych związanych z_i (por. aksjomat (A6)) zmienne x_i dostajemy[12]

$$\vdash \psi_1 \to (\cdots \to (\psi_n \to \varphi) \cdots),$$

czyli $\Delta_0 \vdash \varphi$, a co za tym idzie również $\Delta \vdash \varphi$, wbrew założeniu. Tak więc zbiór $\Delta^* \cup \{\neg\varphi^*\}$ jest niesprzeczny.

Z twierdzenia o istnieniu modelu wynika, że $\Delta^* \cup \{\neg\varphi^*\}$ ma model. Istnieje więc $\Sigma(C)$-struktura $\mathfrak{A}$ taka, że $\mathfrak{A} \models \Delta^*$ oraz $\mathfrak{A} \not\models \varphi^*$. Niech $\varrho : X \to A$ będzie wartościowaniem, które każdej zmiennej x_i przypisuje wartość $c_i^{\mathfrak{A}}$. Na mocy Twierdzenia 7.7 mamy wówczas $(\mathfrak{A}, \varrho) \models \psi$, dla każdej formuły $\psi \in \Delta$ oraz $(\mathfrak{A}, \varrho) \not\models \varphi$. Dowodzi to $\Delta \not\models \varphi$. ∎

Ćwiczenia

1. Rozpatrzmy system $\vdash_h$, którego aksjomatami są formuły postaci (A1–A9), a nie dowolne generalizacje takich formuł. Regułami wnioskowania w $\vdash_h$ niech będą (MP) oraz *reguła generalizacji:*

$$\frac{\varphi}{\forall x\, \varphi}$$

   Udowodnić, że twierdzenia systemów $\vdash_h$ i $\vdash_H$ są takie same, ale z $\Gamma \vdash_h \varphi$ nie wynika $\Gamma \models \varphi$.

2. Udowodnić twierdzenie o pełności dla nieprzeliczalnych sygnatur.

3. System naturalnej dedukcji dla logiki pierwszego rzędu można otrzymać przez dodanie do systemu $\vdash_N$ nastepujących reguł:

$$\frac{\Gamma \vdash \varphi(y/x)}{\Gamma \vdash \forall x \varphi}\ (\forall\text{-intro}) \qquad \frac{\Gamma \vdash \forall x \varphi}{\Gamma \vdash \varphi(t/x)}\ (\forall\text{-elim})$$

$$\frac{\Gamma \vdash \varphi(t/x)}{\Gamma \vdash \exists x \varphi}\ (\exists\text{-intro}) \qquad \frac{\Gamma \vdash \exists x \varphi \quad \Gamma, \varphi(y/x) \vdash \psi}{\Gamma \vdash \psi}\ (\exists\text{-elim})$$

   przy czym regułę (∀-intro) wolno stosować tylko wtedy gdy $y \notin FV(\forall x \varphi)$ oraz y nie jest wolne w żadnej z formuł ze zbioru Γ. Natomiast reguła (∃-intro) używana jest przy zastrzeżeniu $y \notin FV(\Gamma \cup \{\exists x \varphi\} \cup \{\psi\})$. Udowodnić twierdzenie o pełności dla tego systemu.

4. Zaproponować reguły rachunku sekwentów dla logiki pierwszego rzędu.

[12] Zauważmy, że zmienna x_i jest dopuszczalna dla z_i w stosownej formule.

8 Teoria modeli

W tym rozdziale poznamy podstawowe fakty z teorii modeli. Większość z nich to wnioski z twierdzenia o pełności.

Zaczniemy od twierdzenia o zwartości.

Twierdzenie 8.1 (o zwartości)

1. *Dla dowolnego zbioru formuł Δ i dowolnej formuły φ, jeśli $\Delta \models \varphi$, to istnieje skończony podzbiór $\Delta_0 \subseteq \Delta$ taki, że $\Delta_0 \models \varphi$.*
2. *Dla dowolnego zbioru formuł Δ, jeśli każdy skończony podzbiór $\Delta_0 \subseteq \Delta$ jest spełnialny, to Δ też jest spełnialny.*

Dowód: W części pierwszej, jeśli $\Delta \models \varphi$, to z twierdzenia o pełności wynika, że $\Delta \vdash_H \varphi$. W dowodzie występuje tylko skończenie wiele formuł z Δ. Jeśli Δ_0 jest zbiorem wszystkich tych formuł, to oczywiście $\Delta_0 \vdash_H \varphi$. Z twierdzenia o poprawności wynika, że $\Delta_0 \models \varphi$.

Część druga wynika z części pierwszej, gdy przyjmiemy $\varphi = \bot$. Niespełnialność zbioru Δ to bowiem to samo, co $\Delta \models \bot$. ∎

Pierwszym ważnym przykładem zastosowania twierdzenia o zwartości jest dowód innego ważnego twierdzenia teorii modeli.

Twierdzenie 8.2 (Skolem, Löwenheim, Tarski) *Jeśli zbiór formuł Δ nad Σ ma model nieskończony, to ma także model każdej mocy $\mathfrak{m} \geq \max\{\aleph_0, |\Sigma|\}$, gdzie $|\Sigma|$ to moc sygnatury Σ.*

Dowód: Niech C będzie zbiorem nowych symboli stałych, dotychczas nie występujących w Σ, którego moc wynosi $\mathfrak{m}$. Niech $\bar{\Delta} = \Delta \cup \{c \neq d \mid c, d \in \Sigma \text{oraz } c \text{ różne od } d\}$.

Ten nowy zbiór formuł nad nową sygnaturą $\Sigma(C)$ jest spełnialny. Aby się o tym przekonać, weźmy dowolny skończony podzbiór $\bar{\Delta}_0 \subseteq \bar{\Delta}$ oraz nieskończony model $\mathfrak{A}$ zbioru Δ (o którego istnieniu wiemy z założeń). Zinterpretujmy w $\mathfrak{A}$ skończenie wiele symboli z C, które występują w $\bar{\Delta}_0$, jako dowolnie wybrane, różne elementy. Jest oczywiste, że określony w ten sposób model $\bar{\mathfrak{A}}_0$ spełnia $\bar{\Delta}_0$. Zatem na mocy twierdzenia o zwartości, $\bar{\Delta}$ istotnie też ma model.

Wynika stąd, że $\bar{\Delta}$ jest zbiorem niesprzecznym. Stosując do niego twierdzenie o istnieniu modelu, otrzymujemy model $\bar{\mathfrak{B}}$ o mocy nie przekraczającej mocy zbioru wszystkich formuł logiki pierwszego rzędu nad $\Sigma(C)$, która wynosi $\mathfrak{m}$, ale jednocześnie nie mniejszej niż $|C| = \mathfrak{m}$, bo wszystkie stałe z C muszą być w nim zinterpretowane jako różne elementy.

Jeśli teraz w modelu $\bar{\mathfrak{B}}$ zignorujemy interpretację stałych z C to otrzymamy Σ-strukturę $\mathfrak{B}$ mocy $\mathfrak{m}$, która jest modelem zbioru Δ ∎

Wniosek 8.3 *Żadna struktura nieskończona nie daje się opisać zbiorem zdań logiki pierwszego rzędu z dokładnością do izomorfizmu. Dokładniej, nie istnieje zbiór Δ zdań logiki pierwszego rzędu który ma model nieskończony $\mathfrak{A}$ i zarazem dla każdej struktury $\mathfrak{B}$ spełniającej Δ zachodzi $\mathfrak{B} \cong \mathfrak{A}$.*

Historycznie rzecz biorąc, twierdzenie Skolema-Löwenheima-Tarskiego jest następcą dwóch słabszych i starszych twierdzeń, które zresztą nadal są przywoływane. Zatem dla pełności informacji formułujemy je poniżej.

Twierdzenie 8.4 (Dolne twierdzenie Skolema-Löwenheima) *Każdy spełnialny zbiór zdań nad Σ ma model o mocy nie większej niż moc zbioru formuł logiki pierwszego rzędu nad Σ.*

Twierdzenie 8.5 (Górne twierdzenie Skolema-Löwenheima) *Jeśli zbiór zdań nad Σ ma model nieskończony, to dla każdego $\mathfrak{m}$ ma model o mocy nie mniejszej niż $\mathfrak{m}$.*

Najstarszym protoplastą tej grupy twierdzeń było po prostu

Twierdzenie 8.6 (Skolema-Löwenheima) *Każda nieskończona struktura $\mathfrak{A}$ nad co najwyżej przeliczalną sygnaturą zawiera co najwyżej przeliczalną podstrukturę, elementarnie równoważną z $\mathfrak{A}$.*

W tym sformułowaniu twierdzenie to daje się udowodnić bez odwołania do twierdzeń o pełności ani o istnieniu modelu i było znane wcześniej od nich.

Wywołało ono kiedyś potężny ferment w dziedzinie logiki: jak to jest możliwe, że teoria mnogości ma przeliczalny model, gdy skądinąd musi on zawierać zbiory nieprzeliczalne, jak np. $\mathbf{P}(\mathbb{N})$? Oczywiście nikt wolał głośno nie wypowiadać drugiej ewentualności: że teoria mnogości nie ma żadnego modelu i jest po prostu sprzeczna. Nic więc dziwnego, że to twierdzenie było znane początkowo jako Paradoks Skolema. Na szczęście staranna analiza wskazuje, że nie mamy tu jednak do czynienia z antynomią. Otóż jeśli mamy przeliczalny model teorii mnogości, to wszystkie zbiory do niego należące oglądane *z zewnątrz* są przeliczalne. Jednak dla niektórych z nich, np. dla interpretacji $\mathbf{P}(\mathbb{N})$, żadna funkcja z interpretacji $\mathbb{N}$ zbioru liczb naturalnych na interpretację $\mathbf{P}(\mathbb{N})$ sama nie jest elementem *tego modelu*. To już wystarcza, aby spełniał on zdanie mówiące, że $\mathbf{P}(\mathbb{N})$ jest nieprzeliczalny.

Tradycyjnie o wszystkich twierdzeniach z powyższej grupy mówi się „twierdzenie Skolema-Löwenheima".

Twierdzenia o zwartości i twierdzeń Skolema-Löwenheima często używa się do tego, by wykazać istnienie różnych nietypowych modeli. Jeśli przypomnimy sobie elementarną równoważność $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$, wyprowadzoną jako wniosek z Twierdzenia 4.13, to rozpoznamy w niej również potencjalny efekt zastosowania (dolnego) twierdzenia Skolema-Löwenheima.

Klasycznym przykładem zastosowania twierdzenia o zwartości jest poniższy fakt:

Twierdzenie 8.7 *Jeśli zbiór zdań Δ ma modele skończone dowolnie dużej mocy, to ma też model nieskończony.*

Dowód: Przypuśćmy, że Δ ma modele skończone dowolnie dużej mocy.

Niech $\bar{\Delta} = \Delta \cup \{(\exists x_1 \ldots \exists x_n \bigwedge_{i<j} x_i \neq x_j) \mid n \in \mathbb{N}\}$. Oczywiście $\bigwedge_{i<j} x_i \neq x_j$ oznacza koniunkcję wszystkich $n(n-1)$ formuł postaci $x_i \neq x_j$, w których $i < j$.

Zbiór $\bar{\Delta}$ jest spełnialny, bo każdy jego skończony podzbiór $\bar{\Delta}_0 \subseteq \bar{\Delta}$ jest spełnialny. Istotnie, modelem $\bar{\Delta}_0$ jest każdy model Δ mocy co najmniej $\max\{n \mid (\exists x_1 \ldots \exists x_n \bigwedge_{i<j} x_i \neq x_j) \in \bar{\Delta}_0\}$. Na mocy twierdzenia o zwartości $\bar{\Delta}$ jest też spełnialny. Ma on wyłącznie modele nieskończone, a każdy jego model jest też modelem dla Δ. ∎

Twierdzenie o zwartości może też służyć do dowodzenia niewyrażalności pewnych pojęć w logice pierwszego rzędu. Posłużymy się tu następującym przykładem.

Twierdzenie 8.8 *Pojęcie dobrego porządku nie jest wyrażalne w logice pierwszego rzędu. Dokładniej, dla każdego zbioru Δ formuł pierwszego rzędu nad sygnaturą $=, \leq$ takiego, że każdy dobry porządek jest modelem Δ, istnieje też taka struktura $\mathfrak{A}$ nie będąca dobrym porządkiem, że $\mathfrak{A} \models \Delta$.*

Dowód: Niech zbiór zdań Δ ma tę właściwość, że każdy dobry porządek jest jego modelem. Bez utraty ogólności możemy założyć, że Δ zawiera już zwykłe aksjomaty liniowych porządków. Niech $C = \{c_0, c_1, \ldots\}$ będzie zbiorem nowych stałych.

Niech $\bar{\Delta} = \Delta \cup \{c_i < c_j \mid j < i\}$. Każdy skończony podzbiór $\bar{\Delta}_0 \subseteq \bar{\Delta}$ jest spełnialny, np. w zbiorze $\mathbb{N}$, w którym każda stała c_i występująca w $\bar{\Delta}_0$ jest interpretowana jako $2|\bar{\Delta}_0| - i$, zaś pozostałe stałe jako 0.

Zatem na mocy twierdzenia o zwartości $\bar{\Delta}$ jest również spełnialny. Niech $\mathfrak{A}$ będzie modelem $\bar{\Delta}$. Relacja $\leq^{\mathfrak{A}}$ jest porządkiem liniowym, spełnia Δ, ale nie jest porządkiem dobrym, bo zawiera nieskończony ciąg zstępujący $c_0^{\mathfrak{A}} > c_1^{\mathfrak{A}} > c_2^{\mathfrak{A}} > \ldots$ ∎

Interesujące jest porównanie powyższego dowodu z alternatywnym dowodem za pomocą metody Fraïssé, sugerowanym w Ćwiczeniu 1 do Rozdziału 4.

Ćwiczenia

1. Wskazać przykład takiego zbioru Δ zdań logiki pierwszego rzędu, że każde dwa jego *przeliczalne* modele są izomorficzne, ale istnieją dwa *nieprzeliczalne*, nieizomorficzne ze soba modele zbioru Δ.
2. Udowodnić, że dla każdej struktury skończonej $\mathfrak{A}$ nad skończoną sygnaturą istnieje taki zbiór Δ zdań pierwszego rzędu, że $\mathfrak{A} \models \Delta$ i dla każdej struktury $\mathfrak{B} \models \Delta$ zachodzi $\mathfrak{B} \cong \mathfrak{A}$.
3. Niech Σ będzie skończoną sygnaturą. Udowodnić, że dla każdego zbioru zdań Δ nad Σ, następujące dwa warunki są równoważne
   - Δ ma wyłącznie skończone modele.
   - Δ ma z dokładnością do izomorfizmu skończenie wiele modeli.

4. Udowodnić, że klasa wszystkich struktur izomorficznych ze strukturą postaci $\mathfrak{A} = \langle \mathcal{P}(A), \cup, \cap, \subseteq \rangle$, gdzie $\cup, \cap$ oraz $\subseteq$ są odpowiednio sumą, przecięciem i zawieraniem zbiorów, nie jest aksjomatyzowalna żadnym zbiorem zdań pierwszego rzędu.

5. Pokazać, że jeśli klasa $\mathcal{A}$ struktur nad sygnaturą Σ jest aksjomatyzowalna pewnym zbiorem zdań logiki pierwszego rzędu, oraz jej dopełnienie składające się ze struktur sygnatury Σ, ktore nie należą do $\mathcal{A}$ też jest aksjomatyzowalne, to każda z tych klas jest w istocie aksjomatyzowalna *jednym* zdaniem pierwszego rzędu.

   Wskazówka: Założyć, że pierwsza klasa jest aksjomatyzowalna przez Δ, a druga przez Δ', ale żaden skończony podzbiór Δ nie jest aksjomatyzacją $\mathcal{A}$. Pokazać, że $\Delta \cup \Delta'$ spełnia założenia twierdzenia o zwartości.

6. Pokazać następujące twierdzenie Robinsona: Jeśli Δ, Δ' są spełnialnymi zbiorami zdań nad pewną sygnaturą Σ, zaś $\Delta \cup \Delta'$ nie jest spełnialny, to istnieje takie zdanie φ, że $\Delta \models \varphi$ oraz $\Delta' \models \neg\varphi$.

   Wskazówka: Pokazać, że jeśli teza nie zachodzi, to $\Delta \cup \Delta'$ spełnia założenia twierdzenia o zwartości.

7. Niech $Spec(\varphi)$ oznacza zbiór mocy wszystkich skończonych modeli formuły φ. Pokazać, że jeśli Δ jest takim zbiorem zdań, iż dla każdego $\varphi \in \Delta$ zbiór $Spec(\neg\varphi)$ jest skończony, oraz jeśli $\Delta \models \psi$, to także $Spec(\neg\psi)$ jest skończony.

9 Arytmetyka pierwszego rzędu

Słowo *arytmetyka* używane jest w odniesieniu do różnych teorii dotyczących liczb naturalnych. Nasza sygnatura dla arytmetyki pierwszego rzędu składa się z dwuargumentowych symboli funkcyjnych $+$ i $\cdot$, oznaczających dodawanie i mnożenie, symbolu następnika $\boldsymbol{s}$, oraz stałej 0.

Skoro przedmiotem arytmetyki są liczby naturalne, więc strukturę $\mathfrak{N} = \langle \mathbb{N}, +, \cdot, 0, \boldsymbol{s} \rangle$, ze „zwykłymi" operacjami arytmetycznymi nazwiemy *standardowym modelem arytmetyki*. Zbiór $\mathbf{Th}(\mathfrak{N})$ złożony ze wszystkich zdań prawdziwych w modelu $\mathfrak{N}$ nazywiemy zaś *arytmetyką zupełną*. Niestety, arytmetyka zupełna nie wyznacza modelu standardowego jednoznacznie.

Fakt 9.1 *Dla dowolnej mocy* $\mathfrak{m} \geq \aleph_0$ *istnieje* niestandardowy model arytmetyki *mocy* $\mathfrak{m}$*, tj. struktura mocy* $\mathfrak{m}$

$$\mathfrak{M} = \langle \mathbb{M}, \oplus, \otimes, \mathbf{0}, \mathbf{S} \rangle,$$

która jest elementarnie równoważna $\mathfrak{N}$ *ale nieizomorficzna z* $\mathfrak{N}$*.*

Dowód: Niech Δ składa się ze wszystkich formuł postaci $x \neq \boldsymbol{s}(\boldsymbol{s}(\ldots \boldsymbol{s}(\mathbf{0}) \ldots))$. Nietrudno pokazać, że każdy skończony podzbiór zbioru $\mathbf{Th}(\mathfrak{N}) \cup \Delta$ jest spełnialny w modelu $\mathfrak{N}$ przez dostatecznie dużą wartość x. Na mocy twierdzenia o zwartości (Twierdzenie 8.1), całość jest spełnialna w pewnym modelu $\mathfrak{M}$ przez pewne wartościowanie ϱ. Wtedy $\mathfrak{M}$ spełnia te same zdania co $\mathfrak{N}$, ale element $\varrho(x)$ nie ma odpowiednika w modelu $\mathfrak{N}$, bo każdy element $\mathfrak{N}$ można otrzymać z zera za pomocą nastepnika. Z Twierdzenia 8.2 wynika, że model $\mathfrak{M}$ może być żądanej mocy. ∎

Powyższy fakt to kolejny przykład wskazujący na ograniczenia siły wyrazu logiki pierwszego rzędu. Pora więc na pewne obserwacje o charakterze pozytywnym. Język arytmetyki jest tak elastyczny, że można w nim zdefiniować każdą funkcję obliczalną.

Twierdzenie 9.2 (Gödel) *Dla dowolnej częściowej funkcji obliczalnej* $f : \mathbb{N}^k \multimap \mathbb{N}$ *istnieje taka formuła* φ*, że* $FV(\varphi) \subseteq \{x_1, \ldots, x_k, y\}$ *oraz dla* $\varrho(x_1) = n_1, \ldots, \varrho(x_k) = n_k, \varrho(y) = m$ *zachodzi równoważność*

$$(\mathfrak{N}, \varrho) \models \varphi \quad \textit{wtedy i tylko wtedy, gdy} \quad f(n_1, \ldots, n_k) = m.$$

Dowód Twierdzenia 9.2 opuszczamy. Istotnym problemem technicznym w tym dowodzie jest konieczność kodowania ciągów liczb o nieznanej z góry długości. Używa się w tym celu tzw. chińskiego twierdzenia o resztach.

Wniosek 9.3 *Teoria* $\mathbf{Th}(\mathfrak{N})$ *jest nierozstrzygalna. Co więcej, ani zbiór* $\mathbf{Th}(\mathfrak{N})$*, ani jego dopełnienie nie są nawet rekurencyjnie przeliczalne.*

Dowód: Z Twierdzenia 9.2 wynika w szczególności, że dla dowolnego zbioru rekurencyjnie przeliczalnego $A \subseteq \mathbb{N}$ istnieje formuła $\varphi(x)$, o jednej zmiennej wolnej x, dla której

$$(\mathfrak{N}, x : n) \models \varphi \quad \text{wtedy i tylko wtedy, gdy} \quad n \in A.$$

Korzystając z Lematu 2.10, możemy napisać to tak:

$$\varphi(\underline{n}) \in \mathbf{Th}(\mathfrak{N}) \quad \text{wtedy i tylko wtedy, gdy} \quad n \in A,$$

gdzie symbol $\underline{n}$ oznacza term $\boldsymbol{s}^n(\mathbf{0})$. A więc rozstrzygalność $\mathbf{Th}(\mathfrak{N})$ implikowałaby rozstrzygalność problemu stopu.

Aby udowodnić drugą część twierdzenia, przypomnijmy, że problem decyzyjny

Czy dana maszyna Turinga zatrzymuje się dla każdego słowa wejściowego?

nie jest częściowo rozstrzygalny, i że to samo dotyczy jego dopełnienia. Jeśli zakodujemy nasz problem w postaci zbioru $A \subseteq \mathbb{N}$, to zbiór ten będzie można zdefiniować formułą arytmetyki z dwoma kwantyfikatorami, wyrażającą własność

Dla każdego *(kodu) słowa w* istnieje *kod obliczenia akceptującego to słowo.*

Zbiór A jest więc też definiowalny formułą arytmetyki i byłby rekurencyjnie przeliczalny, gdyby taka była teoria $\mathbf{Th}(\mathfrak{N})$. ∎

9.1 Twierdzenie Gödla o niezupełności

Skoro nie można zdefiniować jednoznacznie modelu standardowego (Fakt 9.1), może można chociaż, za pomocą odpowiednich aksjomatów, scharakteryzować zdania które są w nim prawdziwe? Przez PA (od „Peano Arithmetics") oznaczymy teorię o aksjomatach:

- $\forall x \forall y\, (\boldsymbol{s}(x) = \boldsymbol{s}(y) \to x = y)$;
- $\forall x \neg(\boldsymbol{s}(x) = 0)$
- $\forall x\, (x + 0 = x)$;
- $\forall x \forall y\, (x + \boldsymbol{s}(y) = \boldsymbol{s}(x + y))$;
- $\forall x\, (x \cdot 0 = 0)$;
- $\forall x \forall y\, (x \cdot \boldsymbol{s}(y) = (x \cdot y) + x)$;
- $\forall x\, (\varphi(x) \to \varphi(\boldsymbol{s}(x))) \to (\varphi(0) \to \forall x\, \varphi(x))$,

gdzie $\varphi(x)$ może być dowolną formułą. Pierwsze dwa aksjomaty mówią, że operacja następnika jest różnowartościowa, a zero nie jest następnikiem żadnej liczby (to gwarantuje nieskończoność każdego modelu). Kolejne dwa aksjomaty stanowią indukcyjną definicję dodawania, a następne dwa — indukcyjną definicję mnożenia. Na końcu zamiast pojedynczego aksjomatu, mamy schemat aksjomatu, nazywany schematem *indukcji*. Zatem zbiór aksjomatów Peano jest w istocie nieskończony. Ale zbiór ten jest rekurencyjny: można efektywnie ustalić co jest aksjomatem a co nie jest.

Oczywiście standardowy model arytmetyki jest modelem arytmetyki Peano:

$$\mathfrak{N} \models \mathrm{PA}.$$

Inaczej mówiąc, wszystkie konsekwencje aksjomatów Peano (twierdzenia teorii PA) są prawdziwe w standardowym modelu. A na odwrót? Kiedyś przypuszczano, że PA jest *teorią zupełną* (por. Definicja 4.14), tj. że każde zdanie prawdziwe w $\mathfrak{N}$ jest twierdzeniem arytmetyki Peano.

Przypuszczenie to okazało sie fałszywe dzieki odkryciu dokonanemu przez Gödla, a mianowicie dzięki metodzie *arytmetyzacji* (numeracji Gödla), która pozwoliła na wyrażanie w języku arytmetyki faktów odnoszących się do samej arytmetyki, w szczególności istnienia lub nieistnienia dowodu dla danej formuły.

Twierdzenie 9.4 (Gödla o niezupełności) *Istnieje takie zdanie Z w języku arytmetyki, że* $\mathrm{PA} \nvdash_H Z$ *i* $\mathrm{PA} \nvdash_H \neg Z$.

Dowód: Skoro zbiór aksjomatów PA jest rekurencyjny, więc zbiór wszystkich twierdzeń teorii PA (formuł, które można wyprowadzić z tych aksjomatów) jest rekurencyjnie przeliczalny. Aby bowiem stwierdzić, że dana formuła jest twierdzeniem PA, wystarczy systematycznie generować wszystkie możliwe dowody, aż wreszcie otrzymamy ten właściwy.

Gdyby PA była teorią zupełną, to dla dowolnego zdania φ, prędzej czy później znaleźlibyśmy albo dowód formuły φ albo formuły $\neg\varphi$. A więc w takim przypadku PA byłaby po prostu rozstrzygalna.

Ale z drugiej strony, teoria zupełna jest identyczna z teorią każdego swojego modelu, więc PA byłaby identyczna z $\mathbf{Th}(\mathfrak{N})$. Wówczas jednak teoria $\mathbf{Th}(\mathfrak{N})$ musiałaby być rozstrzygalna, co przeczy Wnioskowi 9.3. ∎

Istota twierdzenia Gödla polega nie na tym, że akurat PA jest niezupełna. Jeśli zbiór aksjomatów PA rozszerzymy do innego (rekurencyjnie przeliczalnego) zbioru aksjomatów prawdziwych w $\mathfrak{N}$ to nadal będzie istniało zdanie niezależne od tych aksjomatów. Dowód pozostanie prawie bez zmian. A więc nie tylko PA, ale w ogóle każda efektywnie zadana teoria musi być niezupełna, jeśli tylko jest dostatecznie silna na to, aby dało sie w niej zinterpretować pojęcia arytmetyczne.

Przytoczony powyżej „współczesny" dowód twierdzenia Gödla wykorzystuje numerację gödlowską pośrednio, poprzez odwołanie się do pojęcia rozstrzygalnego problemu decyzyjnego. (Mówiąc o algorytmach generujących dowody, w istocie mamy na myśli pewne obliczenia na kodach takich dowodów, itd.) Oryginalny dowód Gödla posługiwał się numeracją bezpośrednio i przebiegał mniej więcej tak jak niżej. Na początek numerujemy wszystkie symbole języka arytmetyki:

Symbol:	0	$\boldsymbol{s}$	$+$	$\cdot$	$\bot$	$\rightarrow$	$=$	$\forall$	$($	$)$	x_0	x_1	$\ldots$
Numer:	1	2	3	4	5	6	7	8	9	10	11	12	$\ldots$

Każdemu ciągowi znaków, w tym każdej formule, dowodowi itp., można teraz przypisać kod liczbowy. Jeśli przez $\#a$ oznaczymy numer znaku a, to kodem napisu „$a_1a_2\ldots a_n$" jest liczba

$$Kod(a_1a_2\ldots a_n) = 2^{\#a_1}3^{\#a_2}5^{\#a_3}7^{\#a_4}\cdots p_n^{\#a_n},$$

gdzie p_n oznacza n-tą liczbę pierwszą. Odkrycie Gödla oparte jest na obserwacji, że własności formuł arytmetyki mogą być wyrażane w języku samej arytmetyki jako teorioliczbowe własności kodów. Zamiast np. mówić o własnościach formuły $\forall x_0((x_1 + x_0 = 0) \to \bot)$, można mówić o własnościach jej kodu, tj. liczby

$$Kod(\forall x_0((x_1 + x_0 = 0) \to \bot)) = 2^8 3^{11} 5^9 7^9 11^{12} 13^3 17^{11} 19^7 23^1 29^{10} 31^6 37^5 41^{10}.$$

Przypomnijmy, że symbol $\underline{n}$ oznacza term $\boldsymbol{s}^n(\mathbf{0})$. Oczywiście znaczeniem termu $\underline{n}$ w $\mathfrak{N}$ jest liczba n. Można teraz np. napisać taką formułę $\varphi(x)$ o jednej zmiennej wolnej x, że dla dowolnego $n \in \mathbb{N}$ spełnianie $\mathfrak{N} \models \varphi(\underline{n})$ ma miejsce wtedy i tylko wtedy, gdy

- n jest numerem pewnej formuły o co najwyżej jednej zmiennej wolnej.

Oczywiście wiele rozmaitych własności syntaktycznych możemy wyrazić w podobny sposób. Przydatna jest np. formuła $\sigma(x, y)$ o takiej własności:

$\mathfrak{N} \models \sigma(\underline{n}, \underline{m})$, wtedy i tylko wtedy, gdy

- m jest numerem pewnej formuły $\alpha(x)$ o jednej zmiennej wolnej,
- n jest numerem zdania $\alpha(\underline{m})$.

W skrócie zapiszemy to tak:

$$\mathfrak{N} \models \sigma(\underline{n}, \underline{m}), \text{ wtedy i tylko wtedy, gdy } n \text{ jest numerem zdania } \alpha_m(\underline{m}).$$

Nie każda własność formuł może jednak być wyrażona w języku arytmetyki.

Twierdzenie 9.5 (Tarskiego o niewyrażalności prawdy) *Nie istnieje formuła wyrażająca prawdziwość formuł w standardowym modelu, tj. taka formuła $\pi(x)$, że*

$$\mathfrak{N} \models \pi(\underline{n}) \textit{ wtedy i tylko wtedy, gdy } n \textit{ jest numerem zdania prawdziwego w } \mathfrak{N}.$$

Dowód: Dowód twierdzenia polega na wyrażeniu znanego *paradoksu kłamcy*[13] w języku arytmetyki. Rozpatrzmy nastepującą formułę

$$\tau(x) \equiv \exists y\, (\sigma(y, x) \wedge \neg\pi(y)).$$

Wówczas $\mathfrak{N} \models \tau(\underline{n})$ wtedy i tylko wtedy, gdy

- n jest numerem pewnej formuły $\alpha(x)$ o jednej zmiennej wolnej,
- zdanie $\alpha(\underline{n})$ jest fałszywe w $\mathfrak{N}$.

Mniej ściśle, ale prościej:

$$\mathfrak{N} \models \tau(\underline{n}) \text{ wtedy i tylko wtedy, gdy } \mathfrak{N} \models \neg\alpha_n(\underline{n}).$$

[13] Stwierdzenie *„To zdanie jest fałszywe"* nie może być ani prawdziwe ani fałszywe.

Formuła $\tau(x)$ też ma numer, powiedzmy, że $\tau(x) = \alpha_k(x)$. A zatem możemy napisać

$$\mathfrak{N} \models \tau(\underline{k}) \text{ wtedy i tylko wtedy, gdy } \mathfrak{N} \models \neg\alpha_k(\underline{k}).$$

Możemy to napisać z czystym sumieniem, bo warunek

- k jest numerem pewnej formuły $\alpha(x)$ o jednej zmiennej wolnej,

jest oczywiście spełniony. Ale przecież $\alpha_k(\underline{k})$ to właśnie formuła $\tau(\underline{k})$. A zatem:

$$\mathfrak{N} \models \tau(\underline{k}) \text{ wtedy i tylko wtedy, gdy } \mathfrak{N} \models \neg\tau(\underline{k}).$$

No jasne: zdanie $\tau(\underline{k})$ stwierdza *„Ja jestem fałszywe!"* Ze znanym skutkiem ... ∎

Uwaga: Twierdzenie Tarskiego podpowiada rozstrzygnięcie paradoksu kłamcy: Problem leży w niewyrażalności pojęcia „zdania prawdziwego", także w języku polskim. A skoro pytamy o własność, której nie umiemy zdefiniować, to nie dziwmy się, że nie ma odpowiedzi.

Twierdzenie Gödla o niezupełności arytmetyki otrzymamy po nieznacznej modyfikacji powyższego rozumowania. Zamiast niemożliwego do zdefiniowania pojęcia prawdy, użyjemy wyrażalnej własności „mieć dowód w arytmetyce Peano". Otrzymamy w ten sposób zdanie Z, które mówi: „*Ja nie mam dowodu!*".

Inny dowód Twierdzenia 9.4: Postępujemy jak w poprzednim dowodzie, używając formuły $\pi'(x)$ o własności

$\mathfrak{N} \models \pi'(\underline{n})$ wtedy i tylko wtedy, gdy n jest numerem zdania, które ma dowód w PA.

Otrzymamy w końcu taką konkluzję: $\mathfrak{N} \models \tau(\underline{k})$ wtedy i tylko wtedy, gdy $\mathrm{PA} \nvdash_H \tau(\underline{k})$.

Przyjmując $Z = \tau(\underline{k})$, wnioskujemy, że ani Z ani $\neg Z$ nie może mieć dowodu w PA. Założenie $PA \vdash_H Z$ prowadzi do sprzeczności, bo jeśli $PA \vdash_H Z$ to $\mathfrak{N} \models Z$. Ale założenie $PA \vdash_H \neg Z$ też prowadzi do sprzeczności, bo mielibyśmy z jednej strony $\mathfrak{N} \models \neg Z$, a z drugiej $\mathfrak{N} \models Z$. Uwaga: nietrudno zauważyć, że $\mathfrak{N} \models Z$. ∎

Rozumowanie Gödla prowadzi do jeszcze jednego ważnego wniosku, nazywanego *drugim twierdzeniem o niezupełności*. Niech m będzie numerem zdania „$0 = \boldsymbol{s}(0)$" i niech **Con** oznacza zdanie $\neg\pi'(\underline{m})$. Zdanie to wyraża niesprzeczność arytmetyki Peano. Rozumowanie podobne do użytego w dowodzie Twierdzenia 9.4 można... sformalizować w języku arytmetyki. Otrzymamy konkluzję:

$$\mathrm{PA} \vdash_H \mathbf{Con} \to Z,$$

gdzie Z jest zdaniem z Twierdzenia 9.4. W konsekwencji otrzymujemy:

Wniosek 9.6 $\mathrm{PA} \nvdash_H \mathbf{Con}$.

Niesprzeczności arytmetyki Peano nie można udowodnić na gruncie samej arytmetyki Peano (chyba, że PA jest sprzeczna). Ta sama konkluzja dotyczy każdej dostatecznie silnej teorii.

Na zakończenie powiedzmy jeszcze, że teoria PA jest nierozstrzygalna. Dowód tego faktu wymaga pewnego udoskonalenia Twierdzenia 9.2. Zamiast równoważności

$$(\mathfrak{N}, \varrho) \models \varphi \quad \text{wtedy i tylko wtedy, gdy} \quad f(n_1, \ldots, n_k) = m,$$

można mianowicie pokazać równoważność postaci

$$\mathrm{PA} \vdash_H \varphi(\underline{n}_1, \ldots, \underline{n}_k, \underline{m}) \quad \text{wtedy i tylko wtedy, gdy} \quad f(n_1, \ldots, n_k) = m.$$

Nierozstrzygalność PA można udowodnić metodą podobną do użytej w dowodzie Wniosku 9.3.

Ćwiczenia

1. Udowodnić, że istnieje niestandardowy, przeliczalny model $Th(\mathfrak{N})$, a w nim liczba, mająca nieskończenie wiele dzielników pierwszych.
2. Pokazać, że następujące zdania są twierdzeniami arytmetyki Peano:
   (a) $\underline{2} \cdot \underline{2} = \underline{4}$;
   (b) $\forall x(\neg(x = 0) \to \exists y(x = \boldsymbol{s}(y)))$;
   (c) $\forall x \forall y \forall z((x + y) + z = x + (y + z))$;
   (d) $\forall x \forall y(x + y = y + x)$;
3. Jaka jest różnica pomiędzy następującymi zdaniami?
   - *Dwa razy dwa jest cztery.*
   - *Zdanie „Dwa razy dwa jest cztery" jest prawdziwe.*

   Wskazówka: Pierwsze zdanie mówi o pewnej własności liczb. Żeby się z nim zgodzić, wystarczy wiedzieć ile jest dwa razy dwa. Co trzeba wiedzieć, aby zrozumieć drugie zdanie?

10 Zdaniowa logika dynamiczna

Zdaniowa logika dynamiczna (PDL, od angielskiej nazwy *Propositional Dynamic Logic*) została zaproponowana przez V. Pratta w 1976 r. Jest ona eleganckim i zwięzłym formalizmem pozwalającym badać rozumowania dotyczące programów iteracyjnych. Formalizm ten rozszerza logikę modalną poprzez wprowadzenie modalności dla każdego programu z osobna. W tej części pokażemy jedynie dwie podstawowe własności PDL: własność małego modelu oraz pełność aksjomatyzacji. Z własności małego modelu natychmiast wynika rozstrzygalność problemu spełnialności dla PDL. System o podobnym charakterze, o nazwie *Logika Algorytmiczna*, został zaproponowany w roku 1970 przez A. Salwickiego.

10.1 Składnia i semantyka PDL

Syntaktycznie PDL jest mieszaniną trzech klasycznych składników: logiki zdaniowej, logiki modalnej oraz algebry wyrażeń regularnych. Język PDL zawiera wyrażenia dwóch rodzajów: *zdania* (lub formuły) $\varphi, \psi, \ldots$ oraz *programy* $\alpha, \beta, \gamma, \ldots$. Zakładamy, że mamy do dyspozycji przeliczalnie wiele atomowych symboli każdego rodzaju. *Programy atomowe* są oznaczane przez $a, b, c, \ldots$, a zbiór wszystkich atomowych programów oznaczamy przez Π_0.

Programy są budowane z programów atomowych przy użyciu operacji *złożenia* (;), *niedeterministycznego wyboru* ($\cup$) oraz *iteracji* (*). Intuicyjnie wykonanie programu $\alpha;\beta$ oznacza wykonanie α, a następnie wykonanie na danych wyprodukowanych przez α programu β. Wykonanie programu $\alpha \cup \beta$ oznacza niedeterministyczny wybór wykonania α lub β. Natomiast wykonanie programu α^* oznacza wykonanie α pewną liczbę razy, być może zero. Ponadto mamy operację *testowania* tworzącą z każdej formuły φ nowy program $\varphi?$. Wykonanie programu $\varphi?$ jest możliwe tylko wtedy, gdy warunek φ zachodzi. Z drugiej strony, formuły mogą odwoływać się do dowolnego programu α poprzez *modalność konieczności* $[\alpha]$: dla dowolnego zdania φ, napis

$$[\alpha]\varphi$$

czytamy „po (każdym) wykonaniu programu α koniecznie musi zajść φ".

Definicja 10.1 Definicja formuł i programów jest wzajemnie rekurencyjna. Definiujemy zbiór programów Π oraz zbiór formuł Φ jako najmniejsze zbiory spełniające następujące warunki

- ZZ $\subseteq \Phi$
- $\Pi_0 \subseteq \Pi$
- jeśli $\varphi, \psi \in \Phi$, to $\varphi \to \psi \in \Phi$ oraz $\bot \in \Phi$
- jeśli $\alpha, \beta \in \Pi$, to $(\alpha;\beta)$, $(\alpha \cup \beta)$, oraz $\alpha^* \in \Pi$
- jeśli $\alpha \in \Pi$ oraz $\varphi \in \Phi$, to $[\alpha]\varphi \in \Phi$
- jeśli $\varphi \in \Phi$, to $\varphi? \in \Pi$.

Aby uniknąć pisania zbyt wielu nawiasów stosujemy następujące priorytety:

- Jednoargumentowe operatory (wliczając $[\alpha]$) wiążą silniej niż dwuargumentowe.
- Operator ; wiąże silniej niż $\cup$.
- Spójniki logiczne mają takie same priorytety jak zdefiniowano wcześniej.

Tak więc wyrażenie

$$[\alpha; \beta^* \cup \gamma^*]\varphi \vee \psi$$

odpowiada następującemu wyrażeniu z nawiasami

$$([(\alpha; \beta^*) \cup \gamma^*]\varphi) \vee \psi.$$

Ponieważ operatory ; oraz $\cup$ okażą się być łączne, więc zwyczajowo będziemy opuszczać nawiasy w wyrażeniach typu $\alpha; \beta; \gamma$ lub $\alpha \cup \beta \cup \gamma$.

Przypomnijmy, że negacja $\neg\varphi$ jest skrótem formuły $\varphi \to \bot$. Dualnie do $[]$ definiujemy *modalność możliwości*

$$<\alpha>\varphi \quad := \quad \neg[\alpha]\neg\varphi.$$

Zdanie $<\alpha>\varphi$ czytamy „istnieje obliczenie programu α, które zatrzymuje się w stanie spełniającym formułę φ". Istotną różnicą pomiędzy modalnościami $[]$ i $<>$ jest to, że $<\alpha>\varphi$ implikuje iż program α się zatrzymuje, podczas gdy $[\alpha]\varphi$ nie gwarantuje zatrzymania się programu α. W szczególności formuła $[\alpha]\bot$ wyraża własność mówiącą, że żadne obliczenie programu α nie zatrzymuje się. Natomiast formuła $<\alpha>\bot$ jest zawsze fałszywa.

Przejdziemy teraz do zdefiniowania semantyki. Podstawową strukturą semantyczną dla PDL jest tzw. struktura Kripkego.

Definicja 10.2 *Struktura Kripkego* jest uporządkowaną parą $\mathfrak{K} = \langle K, \mathfrak{m}_{\mathfrak{K}} \rangle$, gdzie K jest zbiorem elementów $u, v, w, \ldots$ zwanych *stanami*, a $\mathfrak{m}_{\mathfrak{K}}$ jest funkcją przyporządkowującą każdemu atomowemu zdaniu $p \in \mathrm{ZZ}$, podzbiór $\mathfrak{m}_{\mathfrak{K}}(p) \subseteq K$ oraz każdemu atomowemu programowi $a \in \Pi_0$, relację binarną $\mathfrak{m}_{\mathfrak{K}}(a) \subseteq K \times K$.

Poniżej funkcję $\mathfrak{m}_{\mathfrak{K}}$ rozszerzymy do dowolnych formuł i dowolnych programów. Intuicyjnie dla formuły φ, zbiór stanów $\mathfrak{m}_{\mathfrak{K}}(\varphi)$ jest zbiorem wszystkich stanów struktury $\mathfrak{K}$, w których φ jest spełniona. Natomiast dla programu α, relacja $\mathfrak{m}_{\mathfrak{K}}(\alpha)$ jest tzw. relacją wejścia-wyjścia programu α w strukturze $\mathfrak{K}$.

Definicja 10.3

$$\begin{aligned}
\mathfrak{m}_{\mathfrak{K}}(\varphi \to \psi) &:= (K - \mathfrak{m}_{\mathfrak{K}}(\varphi)) \cup \mathfrak{m}_{\mathfrak{K}}(\psi) \\
\mathfrak{m}_{\mathfrak{K}}(\bot) &:= \emptyset \\
\mathfrak{m}_{\mathfrak{K}}([\alpha]\varphi) &:= \{u \mid \forall v \in K(\langle u, v\rangle \in \mathfrak{m}_{\mathfrak{K}}(\alpha) \Rightarrow v \in \mathfrak{m}_{\mathfrak{K}}(\varphi))\} \\
\mathfrak{m}_{\mathfrak{K}}(\alpha;\beta) &:= \{\langle u, v\rangle \mid \exists w \in K(\langle u, w\rangle \in \mathfrak{m}_{\mathfrak{K}}(\alpha) \wedge \langle w, v\rangle \in \mathfrak{m}_{\mathfrak{K}}(\beta))\} \\
\mathfrak{m}_{\mathfrak{K}}(\alpha \cup \beta) &:= \mathfrak{m}_{\mathfrak{K}}(\alpha) \cup \mathfrak{m}_{\mathfrak{K}}(\beta) \\
\mathfrak{m}_{\mathfrak{K}}(\alpha^*) &:= \bigcup_{n \geq 0} \mathfrak{m}_{\mathfrak{K}}(\alpha)^n \\
\mathfrak{m}_{\mathfrak{K}}(\varphi?) &:= \{\langle u, u\rangle \mid u \in \mathfrak{m}_{\mathfrak{K}}(\varphi)\}.
\end{aligned}$$

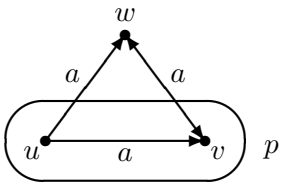
Definicja 10.4 Powiemy, że formuła φ jest *spełniona* w stanie u struktury $\mathfrak{K}$, gdy $u \in \mathfrak{m}_{\mathfrak{K}}(\varphi)$. Podobnie jak w logice pierwszego rzędu spełnianie zapisujemy następująco $(\mathfrak{K}, u) \models \varphi$. Gdy z kontekstu wynika o jaką strukturę chodzi, to możemy po prostu pisać $u \models \varphi$.

Powiemy, że formuła φ jest *prawdziwa* w strukturze $\mathfrak{K}$, gdy jest spełniona w każdym stanie tej struktury. Zapisujemy to $\mathfrak{K} \models \varphi$. Formuła φ jest *tautologią* PDL, gdy jest ona prawdziwa w każdej strukturze Kripkego. Wreszcie powiemy, że formuła φ jest *spełnialna*, gdy istnieje struktura Kripkego $\mathfrak{K}$, taka że φ jest spełniona w przynajmniej jednym stanie $\mathfrak{K}$.

Przykład 10.5 Niech p będzie zmienną zdaniową oraz niech a będzie atomowym programem. Niech $\mathfrak{K} = (K,\ \mathfrak{m}_{\mathfrak{K}})$ będzie taką strukturą Kripkego, że

$$\begin{aligned}
K &= \{u, v, w\} \\
\mathfrak{m}_{\mathfrak{K}}(p) &= \{u, v\} \\
\mathfrak{m}_{\mathfrak{K}}(a) &= \{\langle u, v\rangle, \langle u, w\rangle, \langle v, w\rangle, \langle w, v\rangle\}.
\end{aligned}$$

Nastepujący diagram ilustruje $\mathfrak{K}$.



W tej strukturze mamy $u \models \texttt{<}a\texttt{>}\neg p \wedge \texttt{<}a\texttt{>}p$, ale $v \models \texttt{[}a\texttt{]}\neg p$ oraz $w \models \texttt{[}a\texttt{]}p$. Ponadto każdy stan struktury $\mathfrak{K}$ spełnia następującą formułę

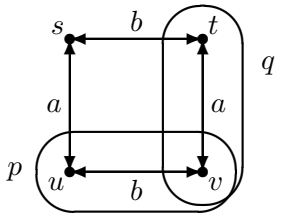
$$\texttt{<}a^*\texttt{>[}(aa)^*\texttt{]}p \wedge \texttt{<}a^*\texttt{>[}(aa)^*\texttt{]}\neg p.$$

Przykład 10.6 Niech p, q będą zmiennymi zdaniowymi i niech a, b będą atomowymi progra-

mami. Ponadto niech $\mathfrak{K} = (K, \mathfrak{m}_{\mathfrak{K}})$ będzie strukturą Kripkego zdefiniowaną następująco

$$\begin{aligned} K &= \{s,t,u,v\} \\ \mathfrak{m}_{\mathfrak{K}}(p) &= \{u,v\} \\ \mathfrak{m}_{\mathfrak{K}}(q) &= \{t,v\} \\ \mathfrak{m}_{\mathfrak{K}}(a) &= \{\langle t,v\rangle, \langle v,t\rangle, \langle s,u\rangle, \langle u,s\rangle\} \\ \mathfrak{m}_{\mathfrak{K}}(b) &= \{\langle u,v\rangle, \langle v,u\rangle, \langle s,t\rangle, \langle t,s\rangle\}. \end{aligned}$$

Następujący rysunek ilustruje $\mathfrak{K}$.



Następujące formuły są prawdziwe w $\mathfrak{K}$.

$$\begin{aligned} p &\leftrightarrow [(ab^*a)^*]p \\ q &\leftrightarrow [(ba^*b)^*]q. \end{aligned}$$

Ponadto niech α będzie programem

$$\alpha = (aa \cup bb \cup (ab \cup ba)(aa \cup bb)^*(ab \cup ba))^*. \tag{14}$$

Program α traktowany jako wyrażenie regularne, generuje wszystkie słowa nad alfabetem $\{a,b\}$ o parzystej liczbie wystąpień a oraz b. Można pokazać, że dla dowolnego zdania φ, formuła $\varphi \leftrightarrow [\alpha]\varphi$ jest prawdziwa w $\mathfrak{K}$.

Zauważmy, że operator * jest z natury infinitarny. Z definicji domknięcie zwrotne i przechodnie relacji jest nieskończoną sumą. Z tego względu twierdzenie o zwartości nie zachodzi dla PDL. Istotnie, zbiór

$$\{\langle\alpha^*\rangle\varphi\} \cup \{\neg\varphi,\ \neg\langle\alpha\rangle\varphi,\ \neg\langle\alpha^2\rangle\varphi,\ \ldots\}$$

jest skończenie spełnialny (tzn. każdy skończony podzbiór jest spełnialny), ale cały zbiór nie jest spełnialny.

10.2 Przykłady tautologii PDL

W tej części przedstawimy przykłady tautologii PDL. Wszystkie dowody, jako łatwe pozostawimy Czytelnikowi. Pierwsza grupa tautologii to schematy znane z logiki modalnej.

Twierdzenie 10.7 *Następujące formuły są tautologiami* PDL.

(i) $\langle\alpha\rangle(\varphi \vee \psi) \quad \leftrightarrow \quad \langle\alpha\rangle\varphi \vee \langle\alpha\rangle\psi$

(ii) $[\alpha](\varphi \wedge \psi) \quad \leftrightarrow \quad [\alpha]\varphi \wedge [\alpha]\psi$

(iii) $[\alpha](\varphi \to \psi) \quad \to \quad ([\alpha]\varphi \to [\alpha]\psi)$

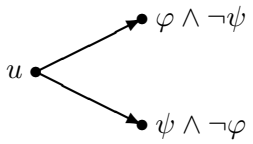
(iv) $\langle\alpha\rangle(\varphi \wedge \psi) \quad \to \quad \langle\alpha\rangle\varphi \wedge \langle\alpha\rangle\psi$

(v) $[\alpha]\varphi \vee [\alpha]\psi \quad \to \quad [\alpha](\varphi \vee \psi)$

(vi) $\langle\alpha\rangle\bot \quad \leftrightarrow \quad \bot$

(vii) $[\alpha]\varphi \quad \leftrightarrow \quad \neg\langle\alpha\rangle\neg\varphi.$

Implikacje odwrotne w Twierdzeniu 10.7(iii)–(v) nie zachodzą. Przykładowo implikacja odwrotna do (iv) nie jest spełniona w stanie u następującej struktury Kripkego.



Następna grupa tautologii, specyficzna dla PDL, dotyczy spójników programotwórczych ; i $\cup$ oraz testu ?.

Twierdzenie 10.8 *Następujące formuły są tautologiami* PDL.

(i) $\langle\alpha \cup \beta\rangle\varphi \quad \leftrightarrow \quad \langle\alpha\rangle\varphi \vee \langle\beta\rangle\varphi$

(ii) $[\alpha \cup \beta]\varphi \quad \leftrightarrow \quad [\alpha]\varphi \wedge [\beta]\varphi$

(iii) $\langle\alpha\,;\,\beta\rangle\varphi \quad \leftrightarrow \quad \langle\alpha\rangle\langle\beta\rangle\varphi$

(iv) $[\alpha\,;\,\beta]\varphi \quad \leftrightarrow \quad [\alpha][\beta]\varphi$

(v) $\langle\varphi?\rangle\psi \quad \leftrightarrow \quad (\varphi \wedge \psi)$

(vi) $[\varphi?]\psi \quad \leftrightarrow \quad (\varphi \to \psi).$

Ostatnia grupa tautologii dotyczy operatora iteracji *.

Twierdzenie 10.9 *Nastepujące formuły są tautologiami* PDL.

(i) $[\alpha^*]\varphi \quad \to \quad \varphi$

(ii) $\varphi \quad \to \quad \langle\alpha^*\rangle\varphi$

(iii) $[\alpha^*]\varphi \quad \rightarrow \quad [\alpha]\varphi$

(iv) $\langle\alpha\rangle\varphi \quad \rightarrow \quad \langle\alpha^*\rangle\varphi$

(v) $[\alpha^*]\varphi \quad \leftrightarrow \quad [\alpha^*\alpha^*]\varphi$

(vi) $\langle\alpha^*\rangle\varphi \quad \leftrightarrow \quad \langle\alpha^*\alpha^*\rangle\varphi$

(vii) $[\alpha^*]\varphi \quad \leftrightarrow \quad [\alpha^{**}]\varphi$

(viii) $\langle\alpha^*\rangle\varphi \quad \leftrightarrow \quad \langle\alpha^{**}\rangle\varphi$

(ix) $[\alpha^*]\varphi \quad \leftrightarrow \quad \varphi \wedge [\alpha][\alpha^*]\varphi$

(x) $\langle\alpha^*\rangle\varphi \quad \leftrightarrow \quad \varphi \vee \langle\alpha\rangle\langle\alpha^*\rangle\varphi$

(xi) $[\alpha^*]\varphi \quad \leftrightarrow \quad \varphi \wedge [\alpha^*](\varphi \rightarrow [\alpha]\varphi)$

(xii) $\langle\alpha^*\rangle\varphi \quad \leftrightarrow \quad \varphi \vee \langle\alpha^*\rangle(\neg\varphi \wedge \langle\alpha\rangle\varphi)$.

Własność (ii) mówi, że α^* jest semantycznie relacją zwrotną. Przechodniość relacji α^* jest wyrażona w (vi). Natomiast fakt, ze α^* zawiera relację α jest wyrażony w (iv). Implikacja $\leftarrow$ w (xi) wyraża zasadę indukcji. Bazą jest założenie, że własność φ jest spełniona w pewnym stanie u. Warunek indukcyjny mówi, że w każdym stanie osiągalnym z u poprzez skończoną liczbę iteracji programu α, kolejne wykonanie α zachowuje własność φ. Teza stwierdza, że wówczas φ jest spełnione we wszystkich stanach osiągalnych w skończonej liczbie iteracji α.

10.3 Własność małego modelu

W tej części udowodnimy własność małego modelu dla PDL. Własność ta mówi, że jeśli φ jest spełnialna to jest spełniona w pewnej skończonej strukturze Kripkego. Co więcej, jak będzie wynikało z dowodu, struktura ta ma co najwyżej $2^{|\varphi|}$ stanów, gdzie $|\varphi|$ oznacza rozmiar formuły φ. Wynika stąd natychmiast rozstrzygalność problemu spełnialności dla PDL. Technika zastosowana w dowodzie twierdzenia o małym modelu nosi nazwę *filtracji* i jest od dawna stosowana w logikach modalnych. W przypadku PDL sytuację komplikuje fakt, że definicja formuł i programów jest wzajemnie rekurencyjna, co powoduje że indukcyjne rozumowania są nieco bardziej delikatne. Własność małego modelu dla PDL została udowodniona w 1977 r. przez M. Fischera i R. Ladnera.

Zaczniemy od definicji domknięcia Fischera-Ladnera. Zdefiniujemy dwie funkcje

$$\begin{aligned} FL &: \Phi \rightarrow 2^\Phi \\ FL^\Box &: \{[\alpha]\varphi \mid \alpha \in \Psi,\ \varphi \in \Phi\} \rightarrow 2^\Phi \end{aligned}$$

przez wzajemną indukcję

(a) $FL(p) := \{p\}$, gdy p jest zmienną zdaniową

(b) $FL(\varphi \rightarrow \psi) := \{\varphi \rightarrow \psi\} \cup FL(\varphi) \cup FL(\psi)$

(c) $FL(\bot) \;:=\; \{\bot\}$

(d) $FL(\texttt{[}\alpha\texttt{]}\varphi) \;:=\; FL^{\Box}(\texttt{[}\alpha\texttt{]}\varphi) \cup FL(\varphi)$

(e) $FL^{\Box}(\texttt{[}a\texttt{]}\varphi) \;:=\; \{\texttt{[}a\texttt{]}\varphi\}$, gdy a jest atomowym programem

(f) $FL^{\Box}(\texttt{[}\alpha \cup \beta\texttt{]}\varphi) \;:=\; \{\texttt{[}\alpha \cup \beta\texttt{]}\varphi\} \cup FL^{\Box}(\texttt{[}\alpha\texttt{]}\varphi) \cup FL^{\Box}(\texttt{[}\beta\texttt{]}\varphi)$

(g) $FL^{\Box}(\texttt{[}\alpha\,;\,\beta\texttt{]}\varphi) \;:=\; \{\texttt{[}\alpha\,;\,\beta\texttt{]}\varphi\} \cup FL^{\Box}(\texttt{[}\alpha\texttt{]}\,\texttt{[}\beta\texttt{]}\varphi) \cup FL^{\Box}(\texttt{[}\beta\texttt{]}\varphi)$

(h) $FL^{\Box}(\texttt{[}\alpha^*\texttt{]}\varphi) \;:=\; \{\texttt{[}\alpha^*\texttt{]}\varphi\} \cup FL^{\Box}(\texttt{[}\alpha\texttt{]}\,\texttt{[}\alpha^*\texttt{]}\varphi)$

(i) $FL^{\Box}(\texttt{[}\psi?\texttt{]}\varphi) \;:=\; \{\texttt{[}\psi?\texttt{]}\varphi\} \cup FL(\psi)$.

Zbiór $FL(\varphi)$ jest nazywany *domknięciem Fischera-Ladnera*. Zauważmy, że definicja $FL(\varphi)$ jest indukcyjna ze względu na budowę formuły φ, natomiast pomocnicza funkcja $FL^{\Box}$ jest określona jedynie na formułach postaci $\texttt{[}\alpha\texttt{]}\varphi$ i jej definicja jest indukcyjna ze względu na budowę programu α. Tak więc chociaż w warunku (h) formuła po prawej stronie definicji jest dłuższa niż po lewej, to program α w zewnętrznej modalności jest prostszy niż α^* i dlatego definicja ta jest dobrze ufundowana.

Niech $|\alpha|$ oraz $|\varphi|$ oznaczają długość programu α i formuły φ rozumianą jako liczbę wystąpień symboli nie licząc nawiasów. Następujący lemat podaje ograniczenie górne na moc domknięcia Fischera-Ladnera.

Lemat 10.10

(i) *Dla dowolnej formuły* φ *mamy* $|FL(\varphi)| \;\leq\; |\varphi|$.

(ii) *Dla dowolnej formuły* $\texttt{[}\alpha\texttt{]}\varphi$ *mamy* $|FL^{\Box}(\texttt{[}\alpha\texttt{]}\varphi)| \;\leq\; |\alpha|$.

Dowód: Dowód jest przez jednoczesną indukcję ze względu na schemat definiujący FL oraz $FL^{\Box}$. Pozostawimy go Czytelnikowi jako ćwiczenie. ∎

Następny lemat ma charakter techniczny. Będzie wykorzystany w dowodzie lematu o filtracji.

Lemat 10.11

(i) *Jeśli* $\sigma \in FL(\varphi)$, *to* $FL(\sigma) \;\subseteq\; FL(\varphi)$.

(ii) *Jeśli* $\sigma \in FL^{\Box}(\texttt{[}\alpha\texttt{]}\varphi)$, *to* $FL(\sigma) \;\subseteq\; FL^{\Box}(\texttt{[}\alpha\texttt{]}\varphi) \cup FL(\varphi)$.

Dowód: Dowodzimy (i) oraz (ii) przez jednoczesną indukcję. Szczegóły pozostawiamy Czytelnikowi jako ćwiczenie. ∎

Następujące własości FL są bezpośrednią konsekwencją Lematu 10.11.

Lemat 10.12

(i) *Jeśli* $[\alpha]\psi \in FL(\varphi)$, *to* $\psi \in FL(\varphi)$.

(ii) *Jeśli* $[\rho?]\psi \in FL(\varphi)$, *to* $\rho \in FL(\varphi)$.

(iii) *Jeśli* $[\alpha \cup \beta]\psi \in FL(\varphi)$, *to* $[\alpha]\psi \in FL(\varphi)$ *oraz* $[\beta]\psi \in FL(\varphi)$.

(iv) *Jeśli* $[\alpha\,;\,\beta]\psi \in FL(\varphi)$, *to* $[\alpha]\,[\beta]\psi \in FL(\varphi)$ *and* $[\beta]\psi \in FL(\varphi)$.

(v) *Jeśli* $[\alpha^*]\psi \in FL(\varphi)$, *to* $[\alpha]\,[\alpha^*]\psi \in FL(\varphi)$.

Dla danej formuły φ oraz struktury Kripkego $\mathfrak{K} = (K,\ \mathfrak{m}_{\mathfrak{K}})$ definiujemy nową strukturę $\mathfrak{K}/FL(\varphi) = \langle K/FL(\varphi),\ \mathfrak{m}_{\mathfrak{K}/FL(\varphi)}\rangle$, zwaną *filtracją struktury* $\mathfrak{K}$ *przez* $FL(\varphi)$. Najpierw definiujemy binarną relację $\equiv$ w zbiorze stanów $\mathfrak{K}$.

$$u \equiv v \quad \text{wtedy i tylko wtedy, gdy} \quad \forall \psi \in FL(\varphi)\ (u \in \mathfrak{m}_{\mathfrak{K}}(\psi) \iff v \in \mathfrak{m}_{\mathfrak{K}}(\psi)).$$

Innymi słowy utożsamiamy stany u oraz v jeśli są one nierozróżnialne przez żadną formułę ze zbioru $FL(\varphi)$. Filtracja struktury jest zwykłą konstrukcją ilorazową. Niech

$$\begin{aligned}
[u] &:= \{v \mid v \equiv u\} \\
K/FL(\varphi) &:= \{[u] \mid u \in K\} \\
\mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(p) &:= \{[u] \mid u \in \mathfrak{m}_{\mathfrak{K}}(p)\}, \quad \text{gdy } p \text{ jest zmienną zdaniową} \\
\mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(a) &:= \{\langle [u],[v]\rangle \mid \langle u,v\rangle \in \mathfrak{m}_{\mathfrak{K}}(a)\}, \quad \text{gdy } a \text{ jest atomowym programem.}
\end{aligned}$$

Przekształcenie $\mathfrak{m}_{\mathfrak{K}/FL(\varphi)}$ rozszerza się w zwykły sposób na wszystkie formuły i programy.

Następujący lemat pokazuje związek pomiędzy strukturami $\mathfrak{K}$ oraz $\mathfrak{K}/FL(\varphi)$. Główna trudność techniczna polega tu sformułowaniu poprawnego założenia indukcyjnego. Sam dowód (jednoczesna indukcja) jest zupełnie rutynowy i dlatego pozostawimy go Czytelnikowi jako ćwiczenie.

Lemat 10.13 (o filtracji) *Niech* u, v *będą stanami w strukturze Kripkego* $\mathfrak{K}$.

(i) *Dla dowolnej formuły* $\psi \in FL(\varphi)$, *mamy* $u \in \mathfrak{m}_{\mathfrak{K}}(\psi) \iff [u] \in \mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(\psi)$.

(ii) *Dla dowolnej formuły* $[\alpha]\psi \in FL(\varphi)$ *zachodzi*

(a) *jeśli* $\langle u,v\rangle \in \mathfrak{m}_{\mathfrak{K}}(\alpha)$, *to* $\langle [u],[v]\rangle \in \mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(\alpha)$;

(b) *jeśli* $\langle [u],[v]\rangle \in \mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(\alpha)$ *oraz* $u \in \mathfrak{m}_{\mathfrak{K}}([\alpha]\psi)$, *to* $v \in \mathfrak{m}_{\mathfrak{K}}(\psi)$.

Z lematu o filtracji natychmiast dostajemy twierdzenie o małym modelu.

Twierdzenie 10.14 (Własność małego modelu) *Niech* φ *będzie spełnialną formułą* PDL. *Wówczas* φ *jest spełniona w strukturze Kripkego mającej co najwyżej* $2^{|\varphi|}$ *stanów.*

Dowód: Jeśli φ jest spełnialna, to istnieje struktura Kripkego $\mathfrak{K}$ oraz stan $u \in \mathfrak{K}$, taki że $u \in \mathfrak{m}_{\mathfrak{K}}(\varphi)$. Niech $FL(\varphi)$ będzie domknięciem Fischera-Ladnera formuły φ. Na mocy Lematu 10.13 o filtracji mamy $[u] \in \mathfrak{m}_{\mathfrak{K}/FL(\varphi)}(\varphi)$. Ponadto $\mathfrak{K}/FL(\varphi)$ ma nie więcej stanów niż liczba wartościowań przypisujących wartości logiczne formułom z $FL(\varphi)$. Tych ostatnich jest, na mocy Lematu 10.10(i), co najwyżej $2^{|\varphi|}$. ∎

Z powyższego twierdzenia natychmiast wynika rozstrzygalność problemu spełnialności dla formuł PDL. Naiwny algorytm polegający na przeszukiwaniu wszystkich struktur Kripkego o co najwyżej $2^{|\varphi|}$ stanach ma złożoność podwójnie wykładniczą względem długości formuły. Używając nieco sprytniejszej metody można rozstrzygnąć problem spełnialności w czasie pojedynczo wykładniczym. Złożoność ta jest najlepsza możliwa, można bowiem pokazać, że problem spełnialności dla PDL jest zupełny w deterministycznym czasie wykładniczym.

10.4 Aksjomatyzacja PDL

Podamy teraz system formalny dla PDL i naszkicujemy dowód jego pełności. Jest to system w stylu Hilberta.

Aksjomaty

(P0) Aksjomaty logiki zdaniowej

(P1) $[\alpha](\varphi \to \psi) \quad \to \quad ([\alpha]\varphi \to [\alpha]\psi)$

(P2) $[\alpha](\varphi \wedge \psi) \quad \leftrightarrow \quad [\alpha]\varphi \wedge [\alpha]\psi$

(P3) $[\alpha \cup \beta]\varphi \quad \leftrightarrow \quad [\alpha]\varphi \wedge [\beta]\varphi$

(P4) $[\alpha\,;\,\beta]\varphi \quad \leftrightarrow \quad [\alpha][\beta]\varphi$

(P5) $[\psi?]\varphi \quad \leftrightarrow \quad (\psi \to \varphi)$

(P6) $\varphi \wedge [\alpha][\alpha^*]\varphi \quad \leftrightarrow \quad [\alpha^*]\varphi$

(P7) $\varphi \wedge [\alpha^*](\varphi \to [\alpha]\varphi) \quad \to \quad [\alpha^*]\varphi$ (aksjomat indukcji)

Reguły dowodzenia

(MP) $\dfrac{\varphi \quad \varphi \to \psi}{\psi}$

(GEN) $\dfrac{\varphi}{[\alpha]\varphi}$

Reguła (GEN) nazywana jest regułą *modalnej generalizacji*. Jeśli φ daje się wyprowadzić w powyższym systemie poszerzonym o dodanie nowych aksjomatów ze zbioru Σ, to będziemy to zapisywać przez $\Sigma \vdash \varphi$. Jak zwykle piszemy $\vdash \varphi$, gdy Σ jest zbiorem pustym.

Fakt, że wszystkie aksjomaty są tautologiami PDL wynika z Sekcji 10.2. Pozostawimy Czytelnikowi sprawdzenie, że powyższe reguły zachowują własność bycia tautologią. Tak

więc każde twierdzenie powyższego systemu jest tautologią. Naszkicujemy dowód twierdzenia odwrotnego, czyli tzw. twierdzenia o pełności dla PDL. Przypomnijmy, że zbiór formuł Σ jest *sprzeczny*, gdy $\Sigma \vdash \bot$. W przeciwnym przypadku mówimy, że Σ jest niesprzeczny. W poniższym lemacie zebrane są podstawowe własności zbiorów niesprzecznych potrzebne do dowodu twierdzenia o pełności.

Lemat 10.15 *Niech Σ będzie zbiorem formuł* PDL. *Wówczas*

(i) *Σ jest niesprzeczny wtedy i tylko wtedy, gdy $\Sigma \cup \{\varphi\}$ jest niesprzeczny lub $\Sigma \cup \{\neg\varphi\}$ jest niesprzeczny;*

(ii) *jeśli Σ jest niesprzeczny, to Σ jest zawarty w maksymalnym niesprzecznym zbiorze formuł.*

Ponadto, jeśli Σ jest maksymalnym niesprzecznym zbiorem formuł, to

(iii) *Σ zawiera wszystkie twierdzenia* PDL*;*

(iv) *jeśli $\varphi \in \Sigma$ oraz $\varphi \to \psi \in \Sigma$, to $\psi \in \Sigma$;*

(v) *$\varphi \vee \psi \in \Sigma$ wtedy i tylko wtedy, gdy $\varphi \in \Sigma$ lub $\psi \in \Sigma$;*

(vi) *$\varphi \wedge \psi \in \Sigma$ wtedy i tylko wtedy, gdy $\varphi \in \Sigma$ oraz $\psi \in \Sigma$;*

(vii) *$\varphi \in \Sigma$ wtedy i tylko wtedy, gdy $\neg\varphi \notin \Sigma$;*

(viii) *$\bot \notin \Sigma$.*

Z powyższego lematu natychmiast dostajemy następującą własność.

Lemat 10.16 *Niech Σ oraz Γ będą maksymalnymi niesprzecznymi zbiorami formuł oraz niech α będzie dowolnym programem. Następujące dwa warunki są równoważne:*

(a) *Dla dowolnej formuły ψ, jeśli $\psi \in \Gamma$, to $\langle\alpha\rangle\psi \in \Sigma$.*

(b) *Dla dowolnej formuły ψ, jeśli $[\alpha]\psi \in \Sigma$, to $\psi \in \Gamma$.*

Struktura, którą za chwilę zbudujemy przy użyciu maksymalnych niesprzecznych zbiorów formuł nie będzie strukturą Kripkego z tego względu, że znaczeniem programu α^* nie będzie musiało być domknięcie przechodnie i zwrotne relacji wyznaczonej przez α. Spełnione będą nieco słabsze własności, wystarczające jednak do przeprowadzenia dowodu twierdzenia o pełności.

Definicja 10.17 *Niestandardową strukturą Kripkego* nazwiemy każdą strukturę $\mathfrak{N} = (N, \mathfrak{m}_{\mathfrak{N}})$ spełniającą wszystkie warunki struktury Kripkego podane w definicjach 10.2 oraz 10.3 za wyjątkiem warunku (14). Zamiast tego warunku żądamy, aby $\mathfrak{m}_{\mathfrak{N}}(\alpha^*)$ było relacją zwrotną

i przechodnią, zawierało relację $\mathfrak{m}_{\mathfrak{N}}(\alpha)$ oraz spełniało aksjomaty (P6) i (P7). Tzn. zamiast warunku

$$\mathfrak{m}_{\mathfrak{N}}(\alpha^*) \;:=\; \bigcup_{n\geq 0} \mathfrak{m}_{\mathfrak{N}}(\alpha)^n, \tag{15}$$

żądamy, aby dla każdego programu α, relacja $\mathfrak{m}_{\mathfrak{N}}(\alpha^*)$ była zwrotna, przechodnia, zawierała $\mathfrak{m}_{\mathfrak{N}}(\alpha)$ oraz spełniała następujące dwa warunki dla dowolnej formuły φ

$$\mathfrak{m}_{\mathfrak{N}}(\texttt{[}\alpha^*\texttt{]}\varphi) \;=\; \mathfrak{m}_{\mathfrak{N}}(\varphi \wedge \texttt{[}\alpha\,;\,\alpha^*\texttt{]}\varphi) \tag{16}$$

$$\mathfrak{m}_{\mathfrak{N}}(\texttt{[}\alpha^*\texttt{]}\varphi) \;=\; \mathfrak{m}_{\mathfrak{N}}(\varphi \wedge \texttt{[}\alpha^*\texttt{]}(\varphi \rightarrow \texttt{[}\alpha\texttt{]}\varphi)). \tag{17}$$

Wracamy teraz do konstrukcji struktury z maksymalnych niesprzecznych zbiorów formuł. Zdefiniujemy niestandardową strukturę Kripkego $\mathfrak{N} = (N,\ \mathfrak{m}_{\mathfrak{N}})$ następująco: Elementami zbioru N są maksymalne niesprzeczne zbiory formuł PDL. Dalej:

$$\begin{aligned}
\mathfrak{m}_{\mathfrak{N}}(\varphi) \;&:=\; \{s \mid \varphi \in s\} \\
\mathfrak{m}_{\mathfrak{N}}(\alpha) \;&:=\; \{\langle s,t\rangle \mid \text{dla wszystkich } \varphi, \text{ jeśli } \varphi \in t, \text{ to } \texttt{<}\alpha\texttt{>}\varphi \in s\} \\
&=\; \{\langle s,t\rangle \mid \text{dla wszystkich } \varphi, \text{ jeśli } \texttt{[}\alpha\texttt{]}\varphi \in s, \text{ to } \varphi \in t\}.
\end{aligned}$$

Z Lematu 10.16 wynika, że obydwie definicje $\mathfrak{m}_{\mathfrak{N}}(\alpha)$ są równoważne. Dowód nastepującego twierdzenia pozostawimy Czytelnikowi.

Twierdzenie 10.18 *Struktura $\mathfrak{N}$ jest niestandardową strukturą Kripkego.*

Dowód: Fakt, że $\mathfrak{N}$ spełnia własności (16) oraz (17) wynika natychmiast z Lematu 10.15(iii) oraz z aksjomatów (P6) i (P7). Sprawdzenie pozostałych warunków pozostawimy Czytelnikowi jako ćwiczenie. ∎

Istotną cechą niestandardowych struktur Kripkego jest to, że daje się przenieść na nie lemat o filtracji (Lemat 10.13).

Lemat 10.19 (o filtracji dla niestandardowych struktur Kripkego)
Niech $\mathfrak{N}$ będzie niestandardową strukturą Kripkego i niech u, v będą stanami w $\mathfrak{N}$.

(i) *Dla dowolnej formuły $\psi \in FL(\varphi)$, mamy $u \in \mathfrak{m}_{\mathfrak{N}}(\psi) \iff [u] \in \mathfrak{m}_{\mathfrak{N}/FL(\varphi)}(\psi)$.*

(ii) *Dla dowolnej formuły $\texttt{[}\alpha\texttt{]}\psi \in FL(\varphi)$ zachodzi*

  (a) *jeśli $\langle u,v\rangle \in \mathfrak{m}_{\mathfrak{N}}(\alpha)$,to $\langle [u],[v]\rangle \in \mathfrak{m}_{\mathfrak{N}/FL(\varphi)}(\alpha)$;*
  (b) *jeśli $\langle [u],[v]\rangle \in \mathfrak{m}_{\mathfrak{N}/FL(\varphi)}(\alpha)$ oraz $u \in \mathfrak{m}_{\mathfrak{N}}(\texttt{[}\alpha\texttt{]}\psi)$, to $v \in \mathfrak{m}_{\mathfrak{N}}(\psi)$.*

Dowód: Szczegóły dowodu tego lematu pomijamy, zachęcając jednocześnie Czytelnika do spróbowania własnych sił. Różnica w dowodzie tego lematu w stosunku do dowodu Lematu 10.13 polega na tym, że w dowodze kroku indukcyjnego dla części (ii) dla przypadku, gdy α jest programem postaci β^* wykorzystujemy jedynie własności (16) oraz (17), zamiast (15). ∎

Możemy już teraz zakończyć dowód twierdzenia o pełności.

Twierdzenie 10.20 (Pełność dla PDL)
Każda tautologia PDL jest twierdzeniem systemu: dla dowolnej formuły φ, jeśli $\models \varphi$, to $\vdash \varphi$.

Dowód: Rozumujemy przez sprzeczność. Jeśli $\nvdash \varphi$, to $\{\neg\varphi\}$ jest zbiorem niesprzecznym. Zatem, na mocy Lematu 10.15(ii) istnieje maksymalny nesprzeczny zbiór u formuł PDL zawierający $\neg\varphi$. Na mocy lematu o filtracji dla niestandardowych struktur Kripkego (Lemat 10.19) stwierdzamy, że $\neg\varphi$ jest spełniona w stanie $[u]$ skończonej struktury $\mathfrak{N}/FL(\varphi)$. Łatwo jest zauważyć, że skończona niestandardowa struktura Kripkego jest zwykłą strukturą Kripkego (tzn. taką, w której zachodzi (15)). Tak więc φ nie jest tautologią. To kończy dowód twierdzenia o pełności. ∎

Ćwiczenia

1. Uzupełnić brakujące dowody w tej części.
2. Pokazać, że dla PDL nie zachodzi twierdzenie o dedukcji.
3. Rozszerzmy zbiór programów poprzez dodanie spójnika programotwórczego $\cap$, interpretowanego w strukturach Kripkego jako przecięcie teoriomnogościowe relacji. Niech $\mathrm{PDL}_\cap$ oznacza logikę zdaniową dla tak poszerzonych programów. Pokazać, że $\mathrm{PDL}_\cap$ nie ma własności małego modelu, tzn. że istnieje spełnialna formuła, która nie jest spełniona w żadnej skończonej strukturze Kripkego.
4. Udowodnić, że spełnialność formuł logiki $\mathrm{PDL}_\cap$ jest nierozstrzygalna. *Wskazówka:* Zakodować problem „domina” (pokrycia płaszczyzny płytkami).

11 Logika intuicjonistyczna

Logika klasyczna oparta jest na pojęciu *wartości logicznej* zdania. Poprawnie zbudowane i jednoznaczne stwierdzenie jest w tej logice klasyfikowane jako „prawdziwe" lub „fałszywe". Wartość logiczna zdania złożonego (np. implikacji) jest zaś ustalana na podstawie wartości jego składowych (niezależnie od ich faktycznej treści). W większości przypadków takie postępowanie jest naturalne i wygodne. Ale nie zawsze. Przypomnijmy na przykład, że klasyczna materialna implikacja nie zawsze odpowiada jakiejkolwiek faktycznej zależności pomiędzy przesłanką i konkluzją (Rozdział 3.1). Inną konsekwencją dwuwartościowości logiki klasycznej jest prawo wyłączonego środka. Akceptujemy alternatywę $p \vee \neg p$, niezależnie od tego czy zdanie p jest faktycznie prawdziwe czy fałszywe, a nawet nie wiedząc, co dokładnie to zdanie wyraża. Zilustrujmy to na przykładzie:

Fakt 11.1 *Istnieją takie liczby niewymierne x i y, że x^y jest liczbą wymierną.*

Dowód: Jeśli $\sqrt{2}^{\sqrt{2}}$ jest wymierne, to można przyjąć $x = y = \sqrt{2}$, w przeciwnym przypadku niech $x = \sqrt{2}^{\sqrt{2}}$ i $y = \sqrt{2}$. ∎

Powyższy dowód, przy całej swojej prostocie i elegancji, ma pewną oczywistą wadę: nadal nie wiemy, *jakie* liczby naprawdę spełniają żądany warunek. A oto inny dowód Faktu 11.1.

Dowód 2: Dla $x = \sqrt{2}$ oraz $y = 2\log_2 3$ mamy $x^y = 3$. ∎

Mówimy, że drugi dowód, w odróżnieniu od pierwszego, jest *konstruktywny*. Oczywiście, konstruktywny dowód zawiera w sobie więcej przydatnej informacji niż niekonstruktywny, ale z punktu widzenia logiki klasycznej, oba te dowody są tak samo poprawne.

Logika, dopuszczająca tylko wnioskowania o charakterze konstruktywnym, znana jest pod tradycyjną, nieco mylącą, nazwą logiki *intuicjonistycznej*. W tej logice nie przypisujemy zdaniom wartości logicznych. Nieformalne objaśnienie zasad logiki intuicjonistycznej posługuje się pojęciem *konstrukcji*. Zdanie jest uważane za prawdziwe, gdy można podać jego konstrukcję, tworzoną według następujących zasad (od nazwisk Brouwera, Heytinga i Kołmogorowa zwanych *interpretacją BHK*):

- *Konstrukcja dla $\varphi \wedge \psi$ polega na podaniu konstrukcji dla φ i konstrukcji dla ψ;*
- *Konstrukcja dla $\varphi \vee \psi$ polega na wskazaniu jednego ze składników φ, ψ i podaniu konstrukcji dla tego składnika.*
- *Konstrukcja dla implikacji $\varphi \to \psi$ to metoda (funkcja) przekształcająca każdą konstrukcję przesłanki φ w konstrukcję dla konkluzji ψ.*
- *Nie ma konstrukcji dla fałszu $\bot$.*
- *Konstrukcja dla $\forall x\, \varphi(x)$ to metoda, która każdej potencjalnej wartości a zmiennej x przypisuje konstrukcję dla $\varphi(a)$.*

- *Konstrukcja dla $\exists x\,\varphi(x)$ polega na wskazaniu pewnej wartości a zmiennej x, oraz konstrukcji dla $\varphi(a)$.*

Negacja intuicjonistyczna $\neg\varphi$ utożsamiana jest z implikacją $\varphi \to \bot$. A zatem

- *Konstrukcja dla $\neg\varphi$ to metoda obracająca każdą ewentualną konstrukcję φ w absurd („rzecz, której nie ma").*

Nie od rzeczy jest tu nastepująca uwaga: o konstrukcji dla $\varphi \to \psi$ można myśleć jak o funkcji *typu* $\varphi \to \psi$, bo przecież konstrukcjom dla φ (obiektom „typu φ") przypisuje ona konstrukcje dla ψ, czyli obiekty „typu ψ". Za chwilę wrócimy do tej analogii.

Przykład 11.2 Konstrukcję dla formuły $p \to \neg\neg p$ możemy zapisać tak:

> *Przypuśćmy, że dana jest konstrukcja C dla przesłanki p. Wtedy konstrukcja dla konkluzji $\neg\neg p$ (czyli dla $(p \to \bot) \to \bot$) jest następująca: daną konstrukcję dla formuły $p \to \bot$ należy zastosować do C.*

Próba podania konstrukcji dla implikacji odwrotnej $\neg\neg p \to p$ natrafia jednak na nieprzezwyciężalną trudność. Aby wykorzystać daną konstrukcję dla $(p \to \bot) \to \bot$, musielibyśmy mieć konstrukcję dla $p \to \bot$, a skoro jej nie mamy, to założenie jest bezużyteczne.

Niemożliwe jest też wskazanie konstrukcji dla schematu $p \vee \neg p$, nie znając p nie możemy bowiem wskazać żadnego z członów alternatywy.

Podobnie będzie na przykład z implikacją $\forall x(q \vee p(x)) \to q \vee \forall x\, p(x)$. Konstrukcja przesłanki dla każdej wartości a zmiennej x generuje albo konstrukcję dla q albo konstrukcję dla $p(a)$. Ale skorzystać z niej można tylko dla konkretnych wartości a. Tymczasem, aby podać konstrukcję dla konkluzji, musielibyśmy umieć podjąć krytyczną decyzję „w ciemno".

Proponujemy teraz Czytelnikowi wykonanie Ćwiczenia 2, a nastepnie próbę znalezienia konstrukcji dla formuł z Ćwiczenia 5.

11.1 Intuicjonistyczny rachunek zdań

Objaśnienia odwołujące się do pojęcia konstrukcji są tylko nieformalne. Ścisłą definicję logiki intuicjonistycznej może stanowić system wnioskowania, na przykład w stylu naturalnej dedukcji. Dla uproszczenia ograniczymy się tutaj do intuicjonistycznego rachunku zdań. System naturalnej dedukcji dla takiego rachunku, przedstawiony poniżej można uważać za uściślenie interpretacji BHK. Otrzymujemy go z systemu klasycznego (Sekcja 5.2) przez odrzucenie reguły PS.[14]

[14] Robimy to, zauważając z pewną satysfakcją, że właśnie ta reguła „nie pasuje" do pozostałych, bo odbiega swoją formą od zasady wprowadzania i eliminacji spójników.

$$(\to\text{-intro})\ \frac{\Delta, \varphi \vdash \psi}{\Delta \vdash \varphi \to \psi} \qquad (\to\text{-elim})\ \frac{\Delta \vdash \varphi \to \psi \qquad \Delta \vdash \varphi}{\Delta \vdash \psi}$$

$$(\wedge\text{-intro})\ \frac{\Delta \vdash \varphi \qquad \Delta \vdash \psi}{\Delta \vdash \varphi \wedge \psi} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \varphi} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \psi}$$

$$(\vee\text{-intro})\ \frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi} \qquad (\vee\text{-intro})\ \frac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}$$

$$(\vee\text{-elim})\ \frac{\Delta \vdash \varphi \vee \psi \qquad \Delta, \varphi \vdash \vartheta \qquad \Delta, \psi \vdash \vartheta}{\Delta \vdash \vartheta}$$

Ciekawy jest sposób w jaki z klasycznego rachunku sekwentów (Sekcja 5.3) można otrzymać system dla logiki intuicjonistycznej. Otóż należy w tym celu ograniczyć liczbę formuł występujących po prawej stronie sekwentów do (co najwyżej) jednej, przy czym sekwent $\Gamma \vdash$ z pustą prawą stroną można utożsamiać z sekwentem $\Gamma \vdash \bot$. Reguła ($\vee$-prawa) traci wtedy sens i trzeba ją zastąpić przez dwie reguły podobne do tych z Ćwiczenia 11 w Rozdziale 5. Pozostałe reguły pozostają w zasadzie bez zmian.

$$(\to\text{-lewa})\ \frac{\Delta \vdash \varphi \qquad \Delta, \psi \vdash \vartheta}{\Delta, \varphi \to \psi \vdash \vartheta} \qquad (\to\text{-prawa})\ \frac{\Delta, \varphi \vdash \psi}{\Delta \vdash \varphi \to \psi}$$

$$(\wedge\text{-lewa})\ \frac{\Delta, \varphi, \psi \vdash \vartheta}{\Delta, \varphi \wedge \psi \vdash \vartheta} \qquad (\wedge\text{-prawa})\ \frac{\Delta \vdash \varphi \qquad \Delta \vdash \psi}{\Delta \vdash \varphi \wedge \psi}$$

$$(\vee\text{-lewa})\ \frac{\Delta, \varphi \vdash \vartheta \qquad \Delta, \psi \vdash \vartheta}{\Delta, \varphi \vee \psi \vdash \vartheta} \qquad \frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi}\ (\vee\text{-prawa})\ \frac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}$$

Intuicjonistyczny system dowodzenia w stylu Hilberta dla logiki zdaniowej, w której występuje tylko implikacja i fałsz, a negacja $\neg\varphi$ jest zdefiniowana jako $\varphi \to \bot$, otrzymamy bardzo łatwo: wystarczy usunąć aksjomat $\neg\neg\varphi \to \varphi$ z systemu klasycznego i dodać jeden nowy:

(A3i) $\bot \to \varphi$.

Ale aksjomaty (B1)–(B4) z Rozdziału 5 do logiki intuicjonistycznej nie pasują, bo nie zgadzają się z interpretacją BHK. Trzeba więc przyjąć aksjomaty z Ćwiczenia 2 do Rozdziału 6, które zamiast definiować koniunkcję i alternatywę, wyrażają ich najważniejsze własności.

(D1) $\varphi \to \varphi \vee \psi$;

(D2) $\psi \to \varphi \vee \psi$;

(D3) $(\varphi \to \vartheta) \wedge (\psi \to \vartheta) \to (\varphi \vee \psi \to \vartheta)$;

(C1) $\varphi \wedge \psi \to \varphi$;

(C2) $\varphi \wedge \psi \to \psi$;

(C3) $(\vartheta \to \varphi) \wedge (\vartheta \to \psi) \to (\vartheta \to \varphi \wedge \psi)$.

Fakt 11.3 *Opisane powyżej intuicjonistyczne systemy dowodzenia (naturalna dedukcja, rachunek sekwentów oraz system Hilberta) są sobie równoważne: formuła φ jest twierdzeniem dowolnego z tych systemów wtedy i tylko wtedy, gdy jest twierdzeniem każdego z pozostałych.*

Dowód: Ćwiczenie. ∎

Semantyka topologiczna

Jak już powiedzieliśmy, logika intuicjonistyczna różni się od klasycznej tym, że nie odwołuje się do pojęcia wartości logicznej, a formalna definicja jest syntaktyczna (przez system dowodzenia) a nie semantyczna. Okazuje się jednak, że intuicjonistyczny rachunek zdań ma ciekawą semantykę topologiczną. Stanowi ona uogólnienie semantyki klasycznego rachunku zdań z Ćwiczenia 7 do Rozdziału 1. Różnica polega na tym, że znaczeniami formuł mogą być jedynie zbiory otwarte.

Definicja 11.4 Niech $\mathcal{O}$ będzie rodziną wszystkich podzbiorów otwartych zbioru liczb rzeczywistych $\mathbb{R}$. Dla $A \subseteq \mathbb{R}$, przez $\mathrm{Int}(A)$ oznaczymy *wnętrze* zbioru A, tj. największy zbiór otwarty zawarty w A. *Wartościowaniem* w zbiorze $\mathcal{O}$ nazwiemy dowolną funkcję $\varrho : \mathrm{ZZ} \to \mathcal{O}$. Dla danego ϱ, możemy każdej formule zdaniowej przypisać wartość w $\mathcal{O}$:

- $[\![\bot]\!]_\varrho = \emptyset$ oraz $[\![\top]\!]_\varrho = \mathbb{R}$;
- $[\![p]\!]_\varrho = \varrho(p)$, gdy p jest symbolem zdaniowym;
- $[\![\neg\varphi]\!]_\varrho = \mathrm{Int}(\mathbb{R} - [\![\varphi]\!]_\varrho)$;
- $[\![\varphi \vee \psi]\!]_\varrho = [\![\varphi]\!]_\varrho \cup [\![\psi]\!]_\varrho$;
- $[\![\varphi \wedge \psi]\!]_\varrho = [\![\varphi]\!]_\varrho \cap [\![\psi]\!]_\varrho$;
- $[\![\varphi \to \psi]\!]_\varrho = \mathrm{Int}((\mathbb{R} - [\![\varphi]\!]_\varrho) \cup [\![\psi]\!]_\varrho)$.

Powiemy, że formuła φ jest *prawdziwa* w $\mathbb{R}$, gdy jej wartością jest cały zbiór $\mathbb{R}$.

Twierdzenie 11.5 *Formuła rachunku zdań jest intuicjonistycznym twierdzeniem, wtedy i tylko wtedy, gdy jest prawdziwa w $\mathbb{R}$.*

Uwaga: Implikacja „tylko wtedy" w Twierdzeniu 11.5 zachodzi nie tylko dla liczb rzeczywistych, ale także dla dowolnej przestrzeni topologicznej.

Przykład 11.6 Aby się przekonać, że prawo wyłączonego środka nie jest twierdzeniem logiki intuicjonistycznej, przypuśćmy, że $\varrho(p) = (0, \infty)$. Wtedy $[\![p \vee \neg p]\!]_\varrho = \mathbb{R} - \{0\} \neq \mathbb{R}$.

Jeśli zaś $\varrho(p) = \mathbb{R} - \{1\}$ to także $[\![\neg\neg p \to p]\!]_\varrho = \mathbb{R} - \{1\}$, więc i formuła $\neg\neg p \to p$ nie jest intuicjonistycznym twierdzeniem.

Normalizacja dowodów

Wróćmy teraz do systemu naturalnej dedukcji dla intuicjonistycznego rachunku zdań. Dla uproszczenia ograniczmy się na razie do tzw. minimimalnej logiki implikacyjnej, tj. do formuł zbudowanych z pomocą samej implikacji. Przypuśćmy, że mamy taki dowód:

$$\dfrac{\begin{array}{cc} (1) & \begin{array}{c}(2)\\ \vdots \\ \Gamma, \varphi \vdash \psi\end{array} \\ \vdots & \dfrac{}{\Gamma \vdash \varphi \to \psi}\,(\to\mathrm{I}) \\ \Gamma \vdash \varphi & \end{array}}{\Gamma \vdash \psi}\,(\to\mathrm{E})$$

W tym dowodzie najpierw wprowadzamy implikację, a zaraz potem ją eliminujemy. Można jednak zrobić inaczej. Tam gdzie w części (2) dowodu używane jest założenie φ można po prostu wstawić całą część (1). Chociaż rozmiary nowego dowodu mogą być większe (założenie φ mogło być używane kilkakrotnie) to jednak jego struktura będzie prostsza. Docelowo możemy uzyskać dowód, w którym takie sytuacje jak na rysunku w ogóle nie występują. Taki dowód nazwiemy dowodem *normalnym*. Proces normalizacji dowodu jest podobny do procesu eliminacji cięcia, a dowody normalne mają podobne zalety jak dowody bez cięcia. W szczególności, wyszukiwanie dowodu dla danej formuły staje się łatwiejsze, jeśli można się ograniczyć do dowodów normalnych.

11.2 Lambda-termy z typami

Normalizacja dowodów ma bliski związek z rachunkiem lambda. Przypomnijmy tu podstawowe definicje.

Definicja 11.7 Przyjmijmy, że mamy pewien przeliczalny nieskończony zbiór *zmiennych przedmiotowych*. Termy rachunku lambda (*lambda-termy*) określamy przez indukcję:

- Zmienne przedmiotowe są termami.
- Jeśli M i N są termami, to (MN) też.
- Jeśli M jest termem i x jest zmienną, to $(\lambda x M)$ jest termem.

Wyrażenie postaci (MN) nazywamy *aplikacją*, a wyrażenie postaci $(\lambda x M)$ to λ-*abstrakcja*. Stosujemy nastepujące konwencje notacyjne:

– opuszczamy zewnętrzne nawiasy;
– aplikacja wiąże w lewo, tj. MNP oznacza $(MN)P$;
– piszemy $\lambda x_1 \ldots x_n.M$ zamiast $\lambda x_1(\ldots(\lambda x_n M)\cdots)$.

Uwaga: kropka w wyrażeniu $\lambda x_1 \ldots x_n.M$ zastępuje lewy nawias, którego zasięg rozciąga się do końca wyrażenia M. Zwyczajowo używa się też notacji $\lambda x.M$.

Operator lambda-abstrakcji λ, podobnie jak kwantyfikator, wiąże zmienne, tj. wszystkie wystąpienia x w wyrażeniu λxM uważa się za *związane*. Zazwyczaj lambda-termy rozważa się z dokładnością do alfa-konwersji, tj. utożsamia się termy różniące się tylko zmiennymi związanymi.

Pominiemy tu ścisłą definicję podstawienia $M[N/x]$, która jest podobna do definicji stosowanej dla formuł z kwantyfikatorami.

Definicja 11.8 Relacja *beta-redukcji* to najmniejsza relacja w zbiorze lambda-termów, spełniająca warunki:

– $(\lambda xP)Q \to_\beta P[Q/x]$;

– jeśli $M \to_\beta M'$, to $MN \to_\beta M'N$, $NM \to_\beta NM'$ oraz $\lambda xM \to_\beta \lambda xM'$.

Inaczej mówiąc, $M \to_\beta M'$ zachodzi gdy podterm termu M postaci $(\lambda xP)Q$, czyli *redeks*, zostaje zastąpiony w M' przez wynik podstawienia $P[Q/x]$. Znakiem $\twoheadrightarrow_\beta$ oznaczamy domknięcie przechodnio-zwrotne relacji $\to_\beta$. Mówimy, że term jest *w postaci normalnej*, gdy nie zawiera żadnego redeksu, tj. nie *redukuje się*.

Zauważmy tu analogię pomiędzy redukcją $(\lambda xP)Q \to_\beta P[Q/x]$ i wywołaniem procedury P, przy którym na miejsce parametru formalnego x podstawiony zostaje parametr aktualny Q.

Definicja 11.9 Przyjmijmy pewien zbiór *typów atomowych*, który oznaczymy przez ZZ (zbieżność oznaczeń jest nieprzypadkowa). Powiemy teraz, że

- Typy atomowe są typami;
- Jeśli σ i τ są typami, to $\sigma \to \tau$ jest typem.

A zatem nasze typy to po prostu formuły zdaniowe zbudowane przy pomocy samej implikacji. Stosujemy taką konwencję, że strzałka jest łączna w prawo, tj. napis $\sigma \to \tau \to \rho$ oznacza $\sigma \to (\tau \to \rho)$.

Przez *otoczenie typowe* rozumiemy zbiór deklaracji postaci $(x : \tau)$, gdzie x jest zmienną (przedmiotową) a τ jest typem. Żądamy przy tym, aby otoczenie było funkcją, tj. aby jedna zmienna nie była deklarowana dwa razy. Przez $\Gamma(x{:}\sigma)$ oznaczamy otoczenie określone tak:

$$\Gamma(x{:}\sigma)(y) = \begin{cases} \Gamma(y), & \text{jeśli } y \neq x; \\ \sigma, & \text{w przeciwnym przypadku.} \end{cases}$$

Lambda-termom można teraz przypisywać typy. Napis $M : \tau$ stwierdza, że M jest termem typu τ. Interpretacja operatora $\to$ jest taka: Term typu $\tau \to \sigma$ zaaplikowany do argumentu typu τ daje wynik typu σ. Ponieważ typ termu może zależeć od typów jego zmiennych wolnych, więc nasz system przypisania typów wyprowadza asercje postaci $\Gamma \vdash M : \tau$, gdzie Γ jest otoczeniem typowym.

Aksjomat: $\Gamma(x : \sigma) \vdash x : \sigma$

Reguły:

$$\frac{\Gamma(x{:}\sigma) \vdash M : \tau}{\Gamma \vdash (\lambda x\, M) : \sigma \to \tau}\ (\text{Abs}) \qquad \frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{(MN) : \tau}\ (\text{App})$$

Ważne, że takie przypisanie typu zachowuje się przy beta-redukcji.

Fakt 11.10 *Jeśli* $\Gamma \vdash M : \tau$ *oraz* $M \to_\beta N$, *to* $\Gamma \vdash N : \tau$.

11.3 Izomorfizm Curry'ego-Howarda (formuły-typy)

Uderzające podobieństwo pomiędzy regułami przypisania typów i regułami dowodzenia w naturalnej dedukcji bywa nazywane *izomorfizmem Curry'ego-Howarda*. Lambda-termy z typami prostymi, to w istocie to samo co dowody w logice minimalnej. Bez wchodzenia w szczegóły sformułujmy tu najważniejszą konsekwencję tego izomorfizmu.

Fakt 11.11 *Formuła implikacyjna* φ *jest twierdzeniem intuicjonistycznym wtedy i tylko wtedy, gdy istnieje zamknięty (tj. bez zmiennych wolnych) lambda-term typu* φ.

Związek pomiędzy dowodami i lambda-termami staje się jeszcze bardziej interesujący, gdy zauważymy podobieństwo dowodu ze strony 84 do beta-redeksu postaci $(\lambda x P)Q$:

$$\dfrac{\begin{array}{cc} \begin{array}{c}(1)\\ \vdots\\ \Gamma \vdash Q : \varphi\end{array} & \dfrac{\begin{array}{c}(2)\\ \vdots\\ \Gamma, x{:}\varphi \vdash P : \psi\end{array}}{\Gamma \vdash \lambda x\, P : \varphi \to \psi}\ (\text{Abs}) \end{array}}{\Gamma \vdash (\lambda x\, P)Q : \psi}\ (\text{App})$$

Normalizacja tamtego dowodu daje w wyniku dowód, którego odpowiednikiem jest term $P[Q/x]$. Ewaluacja lambda-termów (beta-redukcja) ściśle więc reprezentuje zjawisko normalizacji dowodów. W szczególności okazuje się, że dowodom normalnym odpowiadają termy w postaci normalnej. Ma to niebagatelne znaczenie w związku z następującym twierdzeniem, którego (nietrywialny) dowód pomijamy.

Twierdzenie 11.12 *Każdy term z typami prostymi można zredukować do postaci normalnej.*

Wniosek z Twierdzeń 11.10–11.12 jest taki: aby ustalić czy formuła φ ma dowód, należy zbadać, czy istnieje zamknięty term typu φ w postaci normalnej. W ten sposób można np. rozstrzygnąć, które z formuł w Ćwiczeniu 6 są twierdzeniami intuicjonistycznymi.

Technika wyszukiwania dowodu danej formuły za pomocą konstrukcji odpowiedniego lambda-termu daje się uogólnić dla języków znacznie bogatszych niż zdaniowa logika implikacyjna i znajduje zastosowanie w systemach wspomagających dowodzenie, takich jak system Coq.

Przykład 11.13 W myśl interpretacji BHK, konstrukcją (dowodem) koniunkcji $\varphi \wedge \psi$ jest para konstrukcji, jedna „typu φ" a druga „typu ψ". W naturalnej dedukcji, reguła wprowadzania koniunkcji odpowiada tworzeniu takiej pary, a reguła eliminacji koniunkcji reprezentuje rzutowanie na jedną ze współrzędnych. A więc koniunkcja tak naprawdę to samo co produkt kartezjański. Jeśli rozszerzymy rachunek lambda o pary (rekordy) i rzutowania, będziemy mogli napisać takie reguły przypisania typów zawierających znak koniunkcji.

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

Ćwiczenia

1. Twierdzenie o niedefiniowalności dobrego porządku w logice pierwszego rzędu udowodniliśmy dwukrotnie. Po raz pierwszy było to Ćwiczenie 1 do Rozdziału 4, po raz drugi Twierdzenie 8.8. Który z rozważanych dowodów dostarcza więcej informacji i dlaczego?
2. Podać konstrukcje dla następujących formuł:
   (a) $\bot \to p$;
   (b) $(p \to q \to r) \to (p \to q) \to p \to r$;
   (c) $\neg\neg\neg p \to \neg p$;
   (d) $(p \to q) \to (\neg q \to \neg p)$;
   (e) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$;
   (f) $\neg\neg(p \vee \neg p)$;
   (g) $(p \to \neg q) \to (\neg p \to \neg q) \to \neg q$.
3. Udowodnić, że formuły z Ćwiczenia 2 są twierdzeniami intuicjonistycznymi.
4. Udowodnić część „tylko wtedy" Twierdzenia 11.5.
5. Udowodnić, że następujące klasyczne tautologie nie są twierdzeniami intuicjonistycznymi, odwołując się do semantyki topologicznej.
   (a) $((p \to q) \to p) \to p$;
   (b) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$;
   (c) $p \vee (p \to q)$;
   (d) $((p \leftrightarrow q) \leftrightarrow r) \leftrightarrow (p \leftrightarrow (q \leftrightarrow r))$;
   (e) $(\neg\neg p \to p) \to p \vee \neg p$;
   (f) $(p \to q) \leftrightarrow (\neg p \vee q)$;
   (g) $(p \to q) \to (\neg p \to q) \to q$.
6. Czy istnieją zamknięte lambda-termy następujących typów?
   (a) $(p \to q \to r) \to (p \to q) \to p \to r$;
   (b) $((p \to q) \to p) \to p$;
   (c) $((((p \to q) \to p) \to p) \to q) \to q$;
   (d) $((p \to q) \to r) \to (p \to r) \to r$;
   (e) $((((p \to q) \to r) \to (p \to r) \to r) \to q) \to q$.

12 Logika drugiego rzędu

Składnię logiki drugiego uzyskujemy przez rozszerzenie zbioru reguł składniowych dla logiki pierwszego rzędu o kwantyfikatory wiążące symbole relacyjne. Z przyczyn technicznych tym razem wygodnie nam będzie przyjąć, że podstawowymi spójnikami logicznymi są $\neg, \vee$ i $\exists$.

Definicja 12.1 Definicja *formuł drugiego rzędu* jest indukcyjna, podobnie jak analogiczna Definicja 2.5 dla logiki pierwszego rzędu. Jednak tym razem nie ustalamy sygnatury z góry.

- Każda formuła atomowa nad sygnaturą Σ jest formułą drugiego rzędu nad sygnaturą Σ.
- Jeśli φ, ψ są formułami drugiego rzędu nad sygnaturą Σ, to $\varphi \vee \psi$ jest też formułą drugiego rzędu nad sygnaturą Σ.
- Jeśli φ jest formułą drugiego rzędu nad sygnaturą Σ, to $\neg\varphi$ jest też formułą drugiego rzędu nad sygnaturą Σ.
- Jeśli φ jest formułą drugiego rzędu nad sygnaturą Σ a $x \in X$ jest zmienną indywiduową, to $\exists x\varphi$ jest też formułą drugiego rzędu nad sygnaturą Σ.
- jeśli φ jest formułą drugiego rzędu nad sygnaturą Σ, a R jest symbolem relacji k-argumentowej z Σ, to $\exists R\varphi$ jest formułą drugiego rzędu nad sygnaturą $\Sigma - \{R\}$.

Definicja semantyki jest też podobna jak dla logiki pierwszego rzędu.

- Znaczenie formuł atomowych jest identyczne jak w logice pierwszego rzędu.
- $(\mathfrak{A}, \varrho) \models \varphi \vee \psi$, gdy zachodzi $(\mathfrak{A}, \varrho) \models \varphi$ lub zachodzi $(\mathfrak{A}, \varrho) \models \psi$.
- $(\mathfrak{A}, \varrho) \models \neg\varphi$, gdy nie zachodzi $(\mathfrak{A}, \varrho) \models \varphi$.
- $(\mathfrak{A}, \varrho) \models \exists x\varphi$ wtedy i tylko wtedy, gdy istnieje takie $a \in A$, że zachodzi $(\mathfrak{A}, \varrho^a_x) \models \varphi$.
- Jeśli $\mathfrak{A} = \langle A, R_1, \ldots, f_1, \ldots \rangle$ jest strukturą sygnatury $\Sigma - \{R\}$ oraz ϱ jest wartościowaniem w tej strukturze, to $(\mathfrak{A}, \varrho) \models \exists R\varphi$ wtedy i tylko wtedy gdy istnieje struktura $\mathfrak{A}'$ nad sygnaturą Σ o postaci $\langle A, R, R_1, \ldots, f_1 \ldots \rangle$ spełniająca $(\mathfrak{A}, \varrho) \models \varphi$.

Dualny kwantyfikator drugiego rzędu $\forall$ wprowadzamy jako skrót notacyjny:

$$\forall R\varphi \qquad \text{oznacza} \qquad \neg\exists R\neg\varphi.$$

12.1 Nieaksjomatyzowalność logiki drugiego rzędu

Spójrzmy na następujący przykład zdania Ind nad sygnaturą arytmetyki:

$$\forall R(R(0) \wedge \forall n(R(n) \to R(s(n))) \to \forall n R(n)).$$

Orzeka ono, że każda relacja jednoargumentowa (czy podzbiór uniwersum), która zawiera 0 i jest zamknięta ze względu na na operację następnika, zawiera wszystkie elementy uniwersum. Jest to wyrażona w języku drugiego rzędu zasada indukcji matematycznej. Twierdzenie Dedekinda orzeka, że po dołożeniu tego aksjomatu do zwykłych aksjomatów arytmetyki Peano PA (z których można wtedy usunąć dotychczasowy schemat aksjomatu indukcji), otrzymujemy aksjomatyzację *kategoryczną*, czyli taką, która ma z dokładnością do izomorfizmu tylko jeden model $\mathfrak{N}$ — ten standardowy. Zauważmy przy okazji, że przykład ten wskazuje, iż dla logiki drugiego rzędu nie zachodzi górne twierdzenie Skolema-Löwenheima.

Wracając do poprzedniego przykładu, widzimy, że zbiór wszystkich zdań φ logiki pierwszego rzędu, dla których $PA \cup \{Ind\} \models \varphi$, jest tożsamy z $\mathbf{Th}(\mathfrak{N})$. Możemy teraz udowodnić, że w odróżnieniu od logiki pierwszego rzędu,

Twierdzenie 12.2 *Logika drugiego rzędu nie ma żadnego pełnego i poprawnego systemu dowodowego.*

Dowód: Zbiór konsekwencji semantycznych $\{\varphi \mid PA \cup \{Ind\} \models \varphi\} = \mathbf{Th}(\mathfrak{N})$ nie jest nawet rekurencyjnie przeliczalny, na mocy Wniosku 9.3. Tymczasem dla każdego poprawnego systemu dowodzenia X dla logiki drugiego rzędu, zbiór formuł wyprowadzalnych z rekurencyjnego zbioru $PA \cup \{Ind\}$ jest rekurencyjnie przeliczalny. ∎

Widzimy teraz jasno, że logika drugiego rzędu jest niezwykle skomplikowana w badaniu, gdyż właściwie żadne z pożytecznych twierdzeń dotyczących logiki pierwszego rzędu nie zachodzi dla logiki drugiego rzędu. Jedynym, co zostaje, to odpowiednia modyfikacja gier Ehrenfeuchta i metoda Fraïssé. Jednak ich praktyczna użyteczność jest również znikoma wobec ich złożoności. Np. w grze muszą występować rundy, w których gracze wybierają i zaznaczają całe relacje na uniwersum obu struktur. Jednak dla bardzo ograniczonych syntaktycznie fragmentów logiki drugiego rzędu możliwym staje się zapanowanie nad strategiami w odpowiadających im uproszczonych wersjach gry. Tymi właśnie metodami udowodniono kilka twierdzeń o niemożności zdefiniowania w różnych fragmentach logiki drugiego rzędu różnych konkretnych własności.

W dalszym ciągu tego rozdziału dowiemy się, jaki jest stopień trudności pytań o wyrażalność bądź niewyrażalność różnych własności w logice drugiego rzędu.

12.2 Równoważność logiki MSO i automatów skończonych

W zastosowaniach często spotyka się różne fragmenty logiki drugiego rzędu, która w całości dla wielu zastosowań jest zbyt silna. W tym rozdziale będziemy zajmowali się *monadyczną logiką drugiego rzędu*, która jest fragmentem logiki drugiego rzędu, powstałym przez ograniczenie kwantyfikacji drugiego rzędu tylko do relacji jednoargumentowych (czyli zbiorów). Na oznaczenie tej logiki powszechnie stosuje się skrót MSO (od Monadic Second Order).

MSO jest logiką bardzo często pojawiającą się w związku z informatyką. Tutaj zaprezentujemy klasyczny wynik, łączący tę logikę z teorią automatów skończonych.

Niech Σ_n będzie sygnaturą złożoną z symboli $\leq, X_1, \ldots, X_n$, w której wszystkie symbole relacyjne X_i są jednoargumentowe.

Definicja 12.3 Model sygnatury Σ_n nazwiemy *modelem-słowem* gdy jego nośnikiem jest skończony odcinek początkowy zbioru liczb naturalnych a interpretacją symbolu $\leq$ jest naturalny liniowy porządek liczb. Zbiór modeli-słów nad Σ_n będziemy oznaczać W_n.

Skorzystamy też tutaj z naturalnej wzajemnie jednoznacznej odpowiedniości pomiędzy modelami-słowami a niepustymi słowami nad alfabetem $A_n = \{0,1\}^n$: słowu $w \in A_n^+$ odpowiada model $\mathfrak{A}(w) \in W_n$ o mocy równej długości w, a jego element k należy do interpretacji relacji X_i wtedy i tylko wtedy, gdy k-ta litera słowa w jest ciągiem zerojedynkowym, który ma jedynkę na pozycji i.

Odtąd będziemy momentami umyślnie zacierali rozróżnienie pomiędzy słowami a odpowiadającymi im modelami-słowami. Zbiór $\{\mathfrak{A} \in W_n \mid \mathfrak{A} \models \varphi\}$ można więc naturalnie uważać za język słów nad A_n.

Sformułowane przez nas twierdzenie stosuje się wprost tylko do alfabetów o mocy postaci 2^n. Ponieważ jednak każdy język regularny można traktować (po odpowiednim zakodowaniu) jako język nad takim właśnie alfabetem, z którego nie wszystkie litery są wykorzystywane, ograniczenie to nie narusza ogólności naszych rozważań.

Twierdzenie 12.4 (Büchi, Elgot) *Dla każdego zdania φ monadycznej logiki drugiego rzędu zbiór $\{w \in A_n^+ \mid \mathfrak{A}(w) \models \varphi\}$ jest regularny, oraz dla każdego języka regularnego L nad A_n istnieje takie zdanie φ logiki* MSO*, że*

$$\{w \in A_n^+ \mid \mathfrak{A}(w) \models \varphi\} = L - \{\epsilon\}.$$

Czasami treść tego twierdzenia wyraża się sloganem MSO $= Reg$.

W myśl tego twierdzenia, MSO można traktować jako jeszcze jeden formalizm służący definiowaniu (niepustych) języków regularnych, oprócz powszechnie znanych wyrażeń regularnych, automatów skończonych i gramatyk regularnych.

Dowód: Zaczniemy od prostszej drugiej części twierdzenia. Niech $M = \langle Q, A_n, q_0, \Delta, F\rangle$ będzie automatem skończonym rozpoznającym L, gdzie Q to zbiór stanów, $q_0 \in Q$ to stan początkowy, $F \subseteq Q$ to zbiór stanów akceptujących a $\Delta \subseteq Q \times A_n \times Q$ to relacja przejścia. Niech $Q = \{q_1, \ldots, q_\ell\}$. Chcemy wyrazić za pomocą zdania MSO, że istnieje akceptujące obliczenie M na danym słowie.

Stanom M będą odpowiadały dodatkowe symbole relacji jednoargumentowych $X_{n+1}, \ldots, X_{n+\ell}$. Początkowo będziemy więc mieli do czynienia z modelami-słowami nad większą sygnaturą $\Sigma_{n+\ell}$. Modele te mają odpowiadać obliczeniom M na właściwym słowie wejściowym.

Formuła φ_1 postaci $\forall x(\bigwedge_{n<i\neq j\leq n+\ell} \neg(X_i(x) \wedge X_j(x)) \wedge \bigvee_{i=n+1}^{n+\ell} X_i(x))$ mówi o danym słowie, że w każdym kroku obliczenia automat był w jednym i tylko jednym stanie.

Formuła φ_2 postaci $\exists x \forall y(x \leq y \wedge X_{n+1}(x))$ mówi, że w momencie rozpoczęcia obliczenia automat był w stanie początkowym.

Formuła φ_3 postaci $\exists x \forall y (y \leq x \wedge \bigvee_{q_i \in F} X_{n+i}(x))$ mówi, że w momencie zakończenia obliczenia automat był w jednym ze stanów akceptujących.

Formuła φ_4 jest postaci $\forall x \forall y (\neg \exists z (x < z \wedge z < y) \rightarrow \bigvee_{\langle q_i, \vec{a}, q_k \rangle \in \Delta} X_{n+i}(x) \wedge \psi_{\vec{a}}(x) \wedge X_{n+k}(y))$, gdzie $\vec{a} = a_1 \dots a_n$ jest literą z A_n, zaś $\psi_{\vec{a}}(x)$ jest formułą $\bigwedge_{\{i \mid a_i = 1\}} X_i(x) \wedge \bigwedge_{\{i \mid a_i = 0\}} \neg X_i(x)$. Formuła ta mówi, że dla każdych dwóch bezpośrednio po sobie następujących pozycji w słowie, przejście pomiędy nimi odbyło się zgodnie z jedną z możliwości dostępnych w relacji przejścia automatu M.

Teraz zdanie

$$\exists X_{n+1} \dots X_{n+\ell} (\varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4)$$

orzeka, że istnieje akceptujące obliczenie automatu M na danym słowie.

Przechodzimy teraz do dowodu pierwszej części. Tym razem dla danego zdania MSO musimy skonstruować automat skończony, który akceptuje dokładnie te słowa nad A_n, w których to zdanie jest prawdziwe.

W pierwszym kroku zastąpimy MSO przez trochę inną logikę, którą nazwiemy MSO_0. Pokażemy, że jej formuły definiują wszystkie języki modeli-słów, które można zdefiniować w MSO.

Specyficzną cechą MSO_0 jest to, że nie ma w niej zmiennych indywiduowych (czyli tych, których wartościami są elementy) ani wiążących je kwantyfikatorów, a tylko symbole relacji i kwantyfikatory drugiego rzędu. Natomiast jest znacznie więcej formuł atomowych.

Oto definicja składni i jednocześnie semantyki MSO_0 – oczywiście indukcyjna. Wobec braku zmiennych pierwszego rzędu w definicji semantyki nie występuje wartościowanie.

- Formuła atomowa $X_i \subseteq X_j$ jest prawdziwa w modelu $\mathfrak{A} \in W_n$ gdy relacja X_i jest zawarta w relacji X_j.
- Formuła atomowa $Singl(X_i)$ jest prawdziwa w modelu $\mathfrak{A} \in W_n$ gdy relacja X_i jest singletonem (to właśnie kwantyfikowaniem po relacjach, które są singletonami zastąpimy kwantyfikację po elementach obecną w MSO).
- Formuła atomowa $LessEq(X_i, X_j)$ jest prawdziwa w modelu $\mathfrak{A} \in W_n$, gdy wszystkie elementy w relacji X_i są mniejsze bądź równe od wszystkich elementów w relacji X_j.
- Jeśli φ, ψ są formułami MSO_0 a X_i jest symbolem relacyjnym, to formułami są także $\varphi \vee \psi$, $\neg\varphi$ i $\exists X_i \varphi$, których semantyka jest standardowa.

Tłumaczenie danego zdania φ z MSO nad Σ_n na równoważne mu w W_n zdanie $\widetilde{\varphi}$ w MSO_0 definiuje się następująco. Po pierwsze, zamieniamy nazwy związanych zmiennych pierwszego rzędu tak, że zmienna wiązana przez każdy kwantyfikator jest inna. Bez utraty ogólności możemy założyć, że są to zmienne $x_1, \dots, x_\ell$. Teraz wszystkim zmiennym występującym w φ przypisujemy dodatkowe, nowe symbole relacji, powiedzmy, że zmiennej x_i przypisujemy X_{n+i}.

- $\widetilde{X_i(x_j)}$ to $X_{n+j} \subseteq X_i$.
- $\widetilde{(x_i = x_j)}$ to $X_{n+i} \subseteq X_{n+j} \wedge X_{n+j} \subseteq X_{n+i}$.
- $\widetilde{(x_i \leq x_j)}$ to $LessEq(X_{n+i}, X_{n+j})$.
- $\widetilde{(\varphi \vee \psi)}$ ma postać $\widetilde{\varphi} \vee \widetilde{\psi}$.
- $\widetilde{(\neg\varphi)}$ ma postać $\neg\widetilde{\varphi}$.
- Formułę $\widetilde{(\exists x_i \varphi)}$ definiujemy jako $\exists X_{n+i}(Singl(X_{n+i}) \wedge \widetilde{\varphi})$.
- Formułę $\widetilde{(\exists X_i \varphi)}$ dla $i \leq n$ definiujemy jako $\exists X_i \widetilde{\varphi}$.

Przez indukcję ze względu na budowę φ udowodnimy teraz, że

> *Dla każdego modelu-słowa $\langle A, X_1, \ldots, X_n\rangle$ i każdych $a_1, \ldots, a_\ell$ z jego nośnika, następujące warunki są równoważne:*
>
> - $(\langle A, X_1, \ldots, X_n\rangle, x_1 : a_1, \ldots, x_\ell : a_\ell) \models \varphi$
> - $\langle A, X_1, \ldots, X_n, \{a_1\}, \ldots, \{a_\ell\}\rangle \models \widetilde{\varphi}$

Wszystkie kroki indukcji sa całkowicie standardowe i pozostawiamy je Czytelnikowi.

Zatem istotnie, każdy zbiór słów-modeli, który można zdefiniować zdaniem MSO można też zdefiniować zdaniem MSO_0. Teraz dla takiego zdania pozostaje skonstruować automat skończony, który akceptuje dokładnie te słowa nad A, w których to zdanie jest prawdziwe.

Sprawa jest teraz dużo łatwiejsza niż dla oryginalnego MSO, bo każda formuła MSO_0 definiuje jakiś język nad A_{n+k}.

Sprawdzenie, że formuły atomowe definiują języki regularne, pozostawiamy Czytelnikowi jako ćwiczenie.

Język definiowany przez $\varphi \vee \psi$ jest sumą języków definiowanych przez φ i ψ, czyli jako suma języków regularnych sam jest regularny.

Język definiowany przez $\neg\varphi$ jest dopełnieniem regularnego języka definiowanego przez φ, czyli sam też jest regularny.

W wypadku formuły $\exists X_i \varphi$, o której zakładamy, że i jest najwyższym indeksem symbolu relacyjnego występującego w φ, bierzemy automat rozpoznający język nad A_i definiowany przez φ. Następnie modyfikujemy go tak, by działał nad alfabetem A_{i-1}, przy każdym przejściu niedeterministycznie zgadując, czy i-tą współrzędną litery z alfabetu A_i znajdującej się w tej komórce taśmy jest 1 czy 0. ∎

Twierdzenie Büchi ma daleko idące konsekwencje dla rozstrzygalności wielu interesujących problemów.

Wniosek 12.5 *Następujące problemy są rozstrzygalne:*

- *Czy istnieje model-słowo, w którym dane zdanie φ z MSO jest prawdziwe?*
- *Czy dane zdanie φ z MSO jest prawdziwe w każdym modelu-słowie?*

Dowód: Procedura rozstrzygająca oba problemy polega na przetworzeniu formuły φ w równoważny jej automat skończony (np. w sposób opisany w dowodzie poprzedniego twierdzenia), a następnie przeprowadzeniu testu na automacie. ∎

12.3 Informacja o tw. Fagina i Stockmeyera

Naturalne jest pytanie, czy można równie elegancko, jak to zrobił Büchi, scharakteryzować zbiory modeli definiowalnych w pełnej logice drugiego rzędu. Odpowiedź na to pytanie pojawiła się w dwóch krokach.

W pierwszej charakteryzacji występuje *egzystencjalna logika drugiego rzędu*, czasami oznaczana symbolem Σ^1_1, czyli zbiór tych formuł pełnej logiki drugiego rzędu, w których wszystkie kwantyfikatory drugiego rzędu wystepują na początku formuły, a za nimi jest już tylko zwykłe zdanie pierwszego rzędu:

$$\exists X_1 \ \ldots \exists X_n \ \underbrace{\varphi(X_1 \ldots X_n)}_{\text{zdanie pierwszego rzędu}} \quad .$$

Dla tej logiki sytuacja wygląda następująco:

Twierdzenie 12.6 (Fagin) *Dla każdego zdania φ egzystencjalnej logiki drugiego rzędu zbiór $\{w \in A_n^+ \mid \mathfrak{A}(w) \models \varphi\}$ należy do* NP*, oraz dla każdego języka $L \in$ NP istnieje zdanie φ egzystencjalnej logiki drugiego rzędu takie, że*

$$\{w \in A_n^+ \mid \mathfrak{A}(w) \models \varphi\} = L - \{\epsilon\}.$$

Podobnie jak twierdzenie Büchi i Elgota, ono też bywa reprezentowane sloganem $\Sigma^1_1 =$ NP.

Oczywiście NP to słynna klasa złożoności probelmów rozstrzyganych przez niedeterministyczne maszyny Turinga o wielomianowej złożoności czasowej.

Pełna logika drugiego rzędu, oznaczona tu przez SO, też ma analogiczną charakteryzację, która w postaci sloganu wyraża się przez SO = PH i została udowodniona przez Stockmeyera. Precyzyjna postać tego twierdzenia jest analogiczna do poprzednich, a PH to *hierarchia wielomianowa*, również doskonale znana z teorii złożoności.

Przed przejściem do następnego tematu wypada zauważyć, że twierdzenia Fagina i Stockmeyera w istocie obowiązują w zakresie szerszym niż tylko dla modeli-słów. Dotyczą one także dowolnych struktur skończonych, o ile założy się odpowiednio rozsądny sposób opisywania ich we wzajemnie jednoznaczny sposób za pomocą słów.

Po poznaniu twierdzeń Fagina i Stockmeyera lepiej rozumiemy trudności badania logiki drugiego rzędu. Jest to zadanie co najmniej równie niełatwe, jak najtrudniejsze pytania teorii złożoności, z którymi uczeni borykają się od kilkudziesięciu lat, jak dotychczas bezskutecznie. Np. dowód, że każdy zbiór słów, który jest definiowalny formułą logiki drugiego rzędu, jest też definiowalny formułą Σ_1^1, implikowałby natychmiast, że NP = PH, a zatem także NP = coNP. Zauważmy przy tym, że każdy zbiór słów, który jest definiowalny w MSO, jest też definiowalny za pomocą formuły która należy jednocześnie do MSO i Σ_1^1. Wynika to z postaci formuły definiującej zbiory regularne, która pojawia się w dowodzie twierdzenia Büchi. Zatem na poziomie kwantyfikacji wyłącznie po relacjach jednoargumentowych, pożądana równość zachodzi. Jednak przejście do relacji o dowolnej liczbie argumentów wydaje się niezmiernie trudne.

12.4 Informacja o tw. Rabina

Twierdzenie Rabina to inne, daleko idące uogólnienie twierdzenia Büchi.

Nieskończone pełne drzewo binarne to struktura $\mathfrak{T}$ nad sygnaturą $=, s_0, s_1$, w której s_0 i s_1 to symbole jednoargumentowych funkcji. Nośnik $\mathfrak{T}$ to zbiór $\{0,1\}^*$ skończonych słów zerojedynkowych, a funkcje są określone przez równości $s_0(w) = w0$ oraz $s_1(w) = w1$.

Twierdzenie 12.7 (Rabin) *Zbiór zdań logiki MSO, które są prawdziwe w $\mathfrak{T}$ jest rozstrzygalny.*

Wszystkie znane dowody twierdzenia Rabina opierają się na tym samym pomyśle, który poznaliśmy w dowodzie twierdzenia Büchi: formuły logiki MSO są tłumaczone na równoważne im automaty w taki sposób, że formuła jest prawdziwa w drzewie $\mathfrak{T}$ (poetykietowanym dodatkowymi symbolami w wierzchołkach) wtedy i tylko wtedy, gdy automat akceptuje to drzewo. Szczegóły tych dowodów są zawsze bardzo skomplikowane. Nagrodą jest za to wynik, który jest jednym z najsilniejszych znanych twierdzeń o rozstrzygalności, nie tylko zresztą w logice. Rozstrzygalność wielu innych problemów decyzyjnych wykazano po raz pierwszy przez ich odpowiednie przetłumaczenie (czyli zredukowanie) na pytanie o prawdziwość zdań MSO w nieskończonym drzewie binarnym.

Ćwiczenia

1. Napisać zdanie logiki drugiego rzędu aksjomatyzujące pojęcie porządku ciągłego i wywnioskować stąd, że dla tej logiki nie zachodzi także dolne twierdzenie Skolema-Löwenheima.
2. Pokazać, że odpowiednik twierdzenia o zwartości nie zachodzi dla logiki drugiego rzędu.
3. Napisać zdanie MSO, którego wszystkie skończone modele to dokładnie te grafy, które są 3-kolorowalne.
4. Napisać zdanie Σ_1^1, którego wszystkimi modelami są dokładnie struktury skończone.
5. Napisać zdanie MSO, które definiuje język regularny składający się z tych wszystkich słów nad $A_1 = \{0,1\}$, w których liczba jedynek jest parzysta.

13 Logika w informatyce

W tym rozdziale naszkicujemy skrótowo kilka nie wspomnianych dotychczas zagadnień logiki, które wiążą ją z informatyką. Wybór jest dość arbitralny, a opisy niezbyt wyczerpujące. Stanowią one raczej zaproszenie do dalszych, własnych poszukiwań, niż zamknięty wykład prezentowanych zagadnień.

13.1 Zdaniowe logiki trójwartościowe

Logika klasyczna, o której mowa w Wykładzie 1, jest *logiką dwuwartościową*.

Pierwsze *logiki trójwartościowe* skonstruowali niezależnie od siebie polski logik Jan Łukasiewicz i amerykański (ale urodzony w Augustowie) logik i matematyk Emil Post. Motywacje Posta były raczej kombinatoryczne, natomiast Łukasiewicz swoją konstrukcję poparł głębokim wywodem filozoficznym. Argumentował między innymi, że zdania o przyszłości, typu „ jutro pójdę do kina", nie są dzisiaj jeszcze ani prawdziwe, ani fałszywe, bo przypisanie im którejś z tych wartości zaprzeczałoby istnieniu wolnej woli. Aby logika mogła jakoś zdać sprawę ze statusu zdań o przyszłości, musi im przypisać inną, trzecią wartość logiczną.

Trzeba tu zaznaczyć, że zupełnie inną propozycją rozwiązania tego samego problemu jest stworzona przez Brouwera logika intuicjonistyczna, którą poznaliśmy w Wykładzie 11.

Zanim przejdziemy do części trochę bardziej formalnej, rozważmy jeszcze dwa przykłady wzięte z żywej informatyki, gdzie także naturalnie pojawia się trzecia wartość logiczna.

Przykład 13.1 Rozważmy dwie deklaracje funkcji w Pascalu:

```
function f(x,y:boolean):boolean;
   begin
      ...
   end;

function g(x,y:boolean):boolean;
   begin
      ...
   end;
```

a następnie ich użycie

```
if f(x,y) and g(x,y) then ... else ...;
```

Wydaje się na pierwszy rzut oka, że to sytuacja rodem z logiki klasycznej, ale nie: przecież i `f` i `g` mogą dać w wyniku obliczenia wartości `true`, `false` lub się zapętlić, które to zdarzenie jest formą trzeciej wartości logicznej. Sposób, w jaki się z nią obejdzie funkcja `and` zależy od wyboru programisty: może on zastosować albo krótkie albo długie wyliczenie w swoim programie.

Przykład 13.2 Inna sytuacja to tabela stworzona za pomocą następującej instrukcji SQL w relacyjnej bazie danych:

```
CREATE TABLE A   (
id               INTEGER PRIMARY KEY auto_increment,
                            ...
valid            BOOLEAN,
                            ...
);
```

Przy takiej deklaracji, tabela `A` będzie mogła w kolumnie `valid` zawierać *trzy* wartości logiczne: `TRUE`, `FALSE` i `NULL`, a logika trójwartościowa objawi swoje działanie przy wykonaniu np. zapytania

```
SELECT *
FROM A AS A1, A AS A2
WHERE A1.valid and A2.valid
```

Definicja 13.3 *Zbiór formuł zdaniowej logiki trójwartościowej* to zbiór tych formuł zdaniowej logiki klasycznej (patrz Definicja 1.1), w których występują tylko spójniki $\neg, \vee$ i $\wedge$.

Wywołane w ten sposób zawężenie składni zrekompensujemy niezwłocznie po stronie semantyki.

Przez *trójwartościowanie zdaniowe* rozumiemy dowolną funkcję $\varrho : \mathrm{ZZ} \to \{0, \frac{1}{2}, 1\}$, która zmiennym zdaniowym przypisuje wartości logiczne 0, $\frac{1}{2}$ i 1.

Wartość formuły zdaniowej α przy trójwartościowaniu ϱ oznaczamy przez $[\![\alpha]\!]_\varrho$ i określamy przez indukcję:

- $[\![p]\!]_\varrho = \varrho(p)$, gdy p jest symbolem zdaniowym;
- $[\![\neg\alpha]\!]_\varrho = F_\neg([\![\alpha]\!]_\varrho)$;
- $[\![\alpha \vee \beta]\!]_\varrho = F_\wedge([\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho)$;
- $[\![\alpha \wedge \beta]\!]_\varrho = F_\vee([\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho)$;
- $[\![\neg\alpha]\!]_\varrho = F_\neg([\![\alpha]\!]_\varrho)$.

Różne wybory funkcji $F_\vee, F_\wedge : \{0, \frac{1}{2}, 1\} \times \{0, \frac{1}{2}, 1\} \to \{0, \frac{1}{2}, 1\}$ i $F_\neg : \{0, \frac{1}{2}, 1\} \to \{0, \frac{1}{2}, 1\}$ prowadzą do różnych logik trójwartościowych.

Zaczniemy od logiki najstarszej, zwanej dziś logiką Heytinga-Kleene-Łukasiewicza:

$F_\wedge(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	0	0
1	0	1	$\frac{1}{2}$
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$

$F_\vee(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	1	$\frac{1}{2}$
1	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$

$F_\neg$	
x	
0	1
1	0
$\frac{1}{2}$	$\frac{1}{2}$

Jest to logika niewątpliwie nadająca się do rozwiązania zadania, które sobie Łukasiewicz postawił. Sposób traktowania wartości logicznej $\frac{1}{2}$ jest taki, że należy ją rozumieć jako „ jeszcze nie wiadomo".

Warto zauważyć, że w przypadku tej logiki zachodzą równości

- $[\![\neg\alpha]\!]_\varrho = 1 - [\![\alpha]\!]_\varrho$,
- $[\![\alpha \vee \beta]\!]_\varrho = \max\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$,
- $[\![\alpha \wedge \beta]\!]_\varrho = \min\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$,

znane z Definicji 1.2, tak więc mozna ją traktować jako literalne uogólnienie logiki klasycznej.

Zachowanie stałych i operacji logicznych w języku SQL rządzi się właśnie prawami logiki Heytinga-Kleene-Łukasiewicza.

Zupełnie inną logikę zaproponował Bochvar:

$F_\wedge(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	0	$\frac{1}{2}$
1	0	1	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

$F_\vee(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	1	$\frac{1}{2}$
1	1	1	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

$F_\neg$	
x	
0	1
1	0
$\frac{1}{2}$	$\frac{1}{2}$

Czytelnik bez trudu rozpozna, że jest logika właściwa dla Przykładu 13.1, gdy programista wybierze długie wyliczenie wyrażeń logicznych. W sensie tej logiki stała $\frac{1}{2}$ oznacza awarię lub błąd.

Dalej mamy dość egzotycznie wyglądającą logikę Sobocińskiego:

$F_\wedge(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	0	0
1	0	1	1
$\frac{1}{2}$	0	1	$\frac{1}{2}$

$F_\vee(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	1	0
1	1	1	1
$\frac{1}{2}$	0	1	$\frac{1}{2}$

$F_\neg$	
x	
0	1
1	0
$\frac{1}{2}$	$\frac{1}{2}$

Jednak i ona ma swój poważny sens. W niej stała logiczna $\frac{1}{2}$ oznacza „nie dotyczy" lub „nieistotne". Wszyscy odruchowo wręcz stosujemy tę logikę przy okazji wypełniania różnych formularzy i kwestionariuszy. Odpowiadając na różne pytania sformułowane „tak lub nie"

w niektórych polach na odpowiedzi umieszczamy „nie dotyczy” a potem podpisujemy się pod dokumentem mimo ostrzeżenia „Świadomy/ma odpowiedzialności karnej za składanie fałszywych zeznań . . . oświadczam że wszystkie odpowiedzi w tym formularzu są zgodne ze stanem faktycznym.” Po prostu stosujemy tu logikę Sobocińskiego, w której koniunkcja kilku wyrazów o wartości 1 i kilku wyrazów o wartości $\frac{1}{2}$ daje wynik 1. Na szczęście, organy kontrolne chyba też znają ten rachunek zdań i stosują go do oceny naszych zeznań. . .

Przechodząc do logik wyglądających na pierwszy rzut oka jeszcze niezwykłej, natrafiamy na logikę z nieprzemienną koniunkcją i alternatywą, która opisuje spójniki logiczne w Pascalu, wyliczane w sposób krótki:

$F_\wedge(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	0	0
1	0	1	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

$F_\vee(x,y)$			
$x \diagdown y$	0	1	$\frac{1}{2}$
0	0	1	$\frac{1}{2}$
1	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

$F_\neg$	
x	
0	1
1	0
$\frac{1}{2}$	$\frac{1}{2}$

Dla każdego z powyższych rachunków logicznych zasadne i interesujące są pytania o to czym jest tautologia, o aksjomatyzacje i systemy dowodzenia. Tak samo jest z innymi logikami wielowartościowymi, bo Czytelnik juz zapewne zauważył, że o ile jest jedna sensowna logika dwuwartościowa i kilka, wzajemnie konkurencyjnych sensownych logik trójwartościowych, to przy wzroście liczby wartości logicznych, liczba sensownych logik też musi rosnąć. Tytułem przykładu: można sobie bez trudu wyobrazić logikę, w której chcielibyśmy mieć jednocześnie dwie różne stałe odpowiadające „nie wiadomo” i „nie dotyczy”. Taka logika miałaby więc co najmniej cztery wartości logiczne. Jak łatwo się domyślić, ogromnym obszarem zastosowań logik wielowartościowych jest sztuczna inteligencja i reprezentacja wiedzy.

Logika intucjonistyczna też może być w pewnych sytuacjach traktowana jako logika wielowartościowa. W tym przypadku potrzeba tych wartości nieskończenie wiele. Odpowiednio staranne spojrzenie na Definicję Twierdzenie 11.5 pozwala w nim dojrzeć właśnie opis zbioru tautologii zdaniowej logiki intucjonistycznej jako zbioru tautologii logiki nieskończeniewielowartościowej, w której zbiór wartości logicznych to rodzina podzbiorów otwartych $\mathbb{R}$. Trzeba jednak zaznaczyć, że podejście to zatraca pewne istotne intuicje.

13.2 Tw. Codda

Twierdzenie Codda łączy ze sobą świat logiki i świat relacyjnych baz danych. Zostanie ono sformułowane i dowiedzione w tym rozdziale. Orzeka ono, że logika pierwszego rzędu i algebra relacyjna, znana z wykładu baz danych, są wzajemnie na siebie przekładalne, przy założeniu dla logiki pierwszego rzędu tzw. semantyki dziedziny aktywnej.

Na potrzeby niniejszego rozważania zakładamy i ustalamy skończoną sygnaturę Σ, złożoną wyłącznie z symboli relacji i stałych, jak to zwykle ma miejsce w bazach danych.

Definicja 13.4 Tytułem przypomnienia (Czytelnik powinien znać algebrę relacyjną z wykładu baz danych) i dla ustalenia notacji, definiujemy *składnię algebry relacyjnej* AR nad Σ.

- Każdy symbol relacji n-argumentowej z Σ z wyjątkiem równości jest n-argumentowym wyrażeniem AR.
- Jeśli E i F są n-argumentowymi wyrażeniami AR, to $E \cup F$, $E - F$ też są n-argumentowymi wyrażeniami AR.
- Jeśli E i F są n-argumentowymi wyrażeniami AR, to $E \cup F$, $E - F$ też są n-argumentowymi wyrażeniami AR.
- Jeśli E jest n-argumentowym wyrażeniem AR oraz $i_1, \ldots, i_k$ jest ciągiem różnych ale niekoniecznie wszystkich elementów zbioru $\{1, \ldots, n\}$, to $\pi_{i_1,\ldots,i_k} E$ jest k-argumentowym wyrażeniem AR. W szczególności ciąg ten może być pusty, zaś πE jest wyrażeniem 0-argumentowym.
- Jeśli E jest n-argumentowym, zaś F jest m-argumentowym wyrażeniem AR, to $E \times F$ jest $n + m$-argumentowym wyrażeniem AR.
- Jeśli E jest n-argumentowym wyrażeniem AR oraz θ jest zbiorem równości postaci '$i = j$' lub '$i = c$', gdzie $i, j \in \{1, \ldots, n\}$ zaś c należy do zbioru symboli stałych z sygnatury Σ, to $\sigma_\theta E$ jest n-argumentowym wyrażeniem AR.

Semantyka algebry relacyjnej jest następująca: dla danej struktury $\mathfrak{A}$ nad Σ, każdemu n-argumentowemu wyrażeniu E algebry relacyjnej przypisujemy n-argumentową relację $[\![E]\!]$ w A. Definicja oczywiście przebiega indukcyjnie względem budowy E.

- Jeśli R należy do Σ, to $[\![R]\!] = R^{\mathfrak{A}}$.
- $[\![E \cup F]\!] = [\![E]\!] \cup [\![F]\!]$ oraz $[\![E - F]\!] = [\![E]\!] - [\![F]\!]$.
- $[\![\pi_{i_1,\ldots,i_k} E]\!] = \{\langle a_{i_1}, \ldots, a_{i_k}\rangle \mid \langle a_1, \ldots, a_k\rangle \in [\![E]\!]\}$.
- $[\![E \times F]\!] = [\![E]\!] \times [\![F]\!] = \{\langle a_1, \ldots, a_n, b_1 \ldots, b_m\rangle \mid \langle a_1, \ldots, a_n\rangle \in [\![E]\!] \text{ i } \langle b_1 \ldots, b_m\rangle \in [\![F]\!]\}$.
- $[\![\sigma_\theta E]\!] = \{\langle a_1, \ldots, a_n\rangle \in [\![E]\!] \mid a_i = a_j, \text{ gdy } (i = j) \in \theta \text{ oraz } a_i = c^{\mathfrak{A}}, \text{ gdy } (i = c) \in \theta\}$.

Warto zauważyć, że $[\![\pi E]\!] = \{\langle\rangle\}$, czyli jest zbiorem złożonym z ciągu pustego, gdy $[\![E]\!]$ jest niepusty, oraz jest pusty w przeciwnym wypadku. Z kolei $[\![\sigma_\emptyset E]\!] = [\![E]\!]$.

Jak wiadomo, AR jest teoretycznym modelem języka zapytań do relacyjnych baz danych. Pokażemy teraz, że algebra relacyjna jest ściśle powiązana z logiką pierwszego rzędu, a we wszystkich sytuacjach naturalnych z punktu widzenia teorii baz danych, jest jej nawet równoważna.

Dla danej formuły α logiki pierwszego rzędu takiej, że $FV(\alpha) = \{x_{i_1}, \ldots x_{i_n}\}$, oraz struktury $\mathfrak{A} = \langle A, \ldots\rangle$ określimy interpretację tej formuły w $\mathfrak{A}$, oznaczaną $[\![\alpha]\!]$, jak następuje:

$$[\![\alpha]\!] = \{\langle a_1, \ldots, a_n\rangle \in A^n \mid (\mathfrak{A}, x_{i_1} : a_1, \ldots, x_{i_n} : a_n) \models \alpha\}.$$

Intuicyjnie, $[\![\alpha]\!]$ to relacja definiowana przez formułę α w danej strukturze.

Definicja 13.5 *Aktywną dziedziną* struktury $\mathfrak{A}$ nazwiemy podzbiór $ad(\mathfrak{A}) \subseteq A$ jej uniwersum, złożony z wszystkich elementów które są wartościami stałych z sygnatury bądź występują jako współrzędna w co najmniej jednej krotce należącej do interpretacji jakiegoś symbolu relacyjnego z sygnatury.

Jak łatwo zauważyć, interpretacje wszystkich wyrażeń algebry relacyjnej obliczane w $\mathfrak{A}$ są w istocie relacjami w dziedzinie aktywnej.

Inaczej jest w logice pierwszego rzędu: użycie negacji prowadzi natychmiast do formuł, których interpretacje zawierają elementy spoza aktywnej dziedziny.

Zatem w pełnej ogólności są formuły logiki pierwszego rzędu, dla których nie istnieje wyrażenie algebry relacyjnej o tej samej interpretacji w każdej strukturze.

Jednak gdy założymy, że $A = ad(\mathfrak{A})$, to sytuacja sie zmienia. Wyrazem tego jest poniższe twierdzenie.

Twierdzenie 13.6 (Codd)

1. *Dla każdego wyrażenia E algebry relacyjnej istnieje taka formuła α_E logiki pierwszego rzędu, że dla każdej struktury $\mathfrak{A}$ spełniającej $A = ad(\mathfrak{A})$, zachodzi $[\![\alpha]\!] = [\![E]\!]$.*
2. *Dla każdej formuły α logiki pierwszego rzędu istnieje wyrażenie E_α algebry relacyjnej takie, że dla każdej struktury $\mathfrak{A}$ spełniającej $A = ad(\mathfrak{A})$, zachodzi $[\![E]\!] = [\![\alpha]\!]$.*

Dowód: Obu części twierdzenia będziemy dowodzić przez indukcję ze względu na budowę: w pierwszym punkcie wyrażenia E, a w drugim formuły α.

Przy konstrukcji α_E będziemy dbać o to, żeby $FV(\alpha_E) = \{x_1, \ldots, x_n\}$, gdzie n to liczba argumentów E.

Gdy E jest n-argumentowym symbolem relacyjnym R, to α_E ma postać $R(x_1, \ldots, x_n)$, a prawdziwość tezy jest oczywista.

$\alpha_{E \cup F}$ definiujemy jako $\alpha_E \vee \alpha_F$, zaś α_{E-F} jako $\alpha_E \wedge \neg\alpha_F$. I w tym przypadku teza jest oczywista.

Aby skonstruować $\alpha_{\pi_{i_1,\ldots,i_k}E}$ tworzymy formułę $\exists x_{j_1} \ldots \exists x_{j_{n-k}} \alpha$, gdzie $j_1, \ldots, j_{n-k}$ to wypisane w obojętnej kolejności elementy zbioru $\{1, \ldots, n\} - \{i_1, \ldots, i_k\}$. Następnie dokonujemy w niej zamiany nazw zmiennych związanych tak, by ich numery były większe niż n, a zmienne wolne przemianowujemy z x_{i_j} na y_{i_j}. Niech β będzie otrzymaną w ten sposób formułą. Wówczas $\alpha_{\pi_{i_1,\ldots,i_k}E}$ definiujemy jako $\beta(x_1/y_{i_1}, \ldots, x_k/y_{i_k})$. Widać, że ta formuła spełnia tezę.

Przy konstrukcji $\alpha_{E \times F}$ postępujemy następująco: dokonujemy zamiany nazw zmiennych związanych w formule α_F w ten sposób, by miały one numery większe niż $n + m$, zaś za zmienne wolne $x_1, \ldots, x_m$ podstawiamy kolejno $x_{n+1}, \ldots, x_{n+m}$. Niech powstała formuła nazywa się β_F. Wtedy definiujemy $\alpha_{E \times F}$ jako $\alpha_E \wedge \beta_F$. Oczyiście ta formuła spełnia tezę.

Na zakończenie tej cześci dowodu określamy formułę $\alpha_{\sigma_\theta E}$ jako

$$\alpha_E \wedge \bigwedge_{`i = j' \in \theta} x_i = x_j \wedge \bigwedge_{`i = c' \in \theta} x_i = c.$$

I tym razem sprawdzenie, że ta formuła spełnia tezę indukcyjną jest natychmiastowe.

Przystępujemy teraz do tłumaczenia formuł logiki pierwszego rzędu na algebrę relacyjną. W tym celu wygodnie jest założyć, że podstawowymi spójnikami logiki są $\vee$, $\neg$ i $\exists$, a pozostałe są zdefiniowane za ich pomocą i mają status skrótów notacyjnych.

Zaczynamy od konstrukcji jednoargumentowego wyrażenia AD takiego, że dla każdej struktury $\mathfrak{A}$, mamy $[\![AD]\!] = ad(\mathfrak{A})$.

Jest ono $\cup$-sumą wyrażeń $\pi_i R$ dla wszystkich symboli relacyjnych R w sygnaturze i wszystkich i takich, że R ma co najmniej i argumentów.

Możemy teraz przystąpić do konstrukcji. Dla każdego zadanego n nie mniejszego niż wszystkie numery zmiennych wolnych w α konstruujemy n-argumentowe wyrażenie $E_{\alpha;n}$ takie, że

$$[\![E_{\alpha;n}]\!] = \{\langle a_1, \ldots, a_n\rangle \in A^n \mid (\mathfrak{A}, x_1 : a_1, \ldots, x_n : a_n) \models \alpha\}.$$

Oznacza to, że $E_{\alpha;n}$ zawiera dodatkowe współrzędne, które pozwalają zarejestrować indeksy zmiennych wolnych występujących w α. Aby otrzymać E_α wystarczy wziąć rzut $\pi_I E_{\alpha;n}$, gdzie I to posortowany rosnąco ciąg numerów zmiennych wolnych α, co eliminuje przy okazji zbędne współrzędne.

$E_{x_i = x_j;n}$ to $\sigma_{i=j}(\underbrace{AD \times \cdots \times AD}_{n})$.

$E_{R(x_{i_1},\ldots,x_{i_k});n}$ jest zdefiniowane jako $\pi_I(R \times \underbrace{AD \times \cdots \times AD}_{n-k})$, gdzie I jest taką permutacją $\{1, \ldots, n\}$, która współrzędne R mieszcza na pozycjach o kolejnych numerach $i_1, \ldots, i_k$.

$E_{\alpha\vee\beta;n}$ jest zdefiniowane jako $E_{\alpha;n} \cup E_{\beta;n}$, natomiast $E_{\neg\alpha;n}$ to $(\underbrace{AD \times \cdots \times AD}_{n}) - E_{\alpha;n}$.

Wreszcie w wypadku $E_{\exists x_i \alpha;n}$ możemy bez utraty ogólności założyć, że $i = n + 1$. Wtedy $E_{\exists x_i \alpha;n}$ jest zdefiniowane jako $\pi_{1,\ldots,n} E_{\alpha;n+1}$.

We wszystkich przypadkach kroki dowodu indukcyjnego są oczywiste. ∎

Twierdzenie Codda jest już w pewnym stopniu częścią folkloru w teorii baz danych. Dziś wszyscy wiedzą, że algebra relacyjna to właściwie to samo, co logika pierwszego rzędu. W związku z tym, od wielu lat na konferencjach naukowych dotyczących teorii baz danych, systematycznie prezentowane są prace, których tematem jest logika pierwszego rzędu i nikt się już temu nie dziwi ani niczego nie musi uzasadniać.

W szczególności badania dotyczące gier Ehrenfeuchta oraz charakteryzacji obliczeniowych logiki pierwszego rzędu (w duchu twierdzeń Büchi i Fagina) są generalnie postrzegane jako wyniki należące do teorii baz danych.

13.3 Rozstrzygalność i nierozstrzygalność teorii

W tym rozdziale przedyskutujemy zagadnienie rozstrzygalności teorii matematycznych (rozumianych jako zbiory zdań). Przykładem teorii nierozstrzygalnej jest arytmetyka Peano (Twierdzenie 9.3). Przykład teorii rozstrzygalnej prezentujemy poniżej.

Twierdzenie 13.7 *Teoria gęstych porządków liniowych które nie mają elementów maksymalnych ani minimalnych jest rozstrzygalna.*

Dowód: Niech $\mathcal{A}$ będzie klasą wszystkich gęstych porządków liniowych które nie mają elementów maksymalnych ani minimalnych. Z Wniosku 4.15 wiemy, że $\mathbf{Th}(\mathcal{A})$ jest zupełna. Ponadto zauważmy, że $\mathbf{Th}(\mathcal{A}) = \{\alpha \mid \Delta \models \alpha\}$, gdzie Δ to następujący zbiór zdań:

$$\forall x \forall y \ (x \leq y \wedge y \leq x) \rightarrow x = y$$
$$\forall x \forall y \forall z \ (x \leq y \wedge y \leq z) \rightarrow x \leq z$$
$$\forall x \forall y \ x \leq y \vee y \leq x$$
$$\forall x \exists y \ x < y$$
$$\forall x \exists y \ y < x$$
$$\forall x \forall y \ (x < y) \rightarrow (\exists z \ x < z \wedge z < y)$$

gdzie $x < y$ jest oczywistym skrótem notacyjnym dla formuły $x \leq y \wedge x \neq y$.

Na mocy twierdzenia o pełności

$$\{\alpha \mid \Delta \models \alpha\} = \{\alpha \mid \Delta \vdash_H \alpha\}.$$

Pozostaje więc wykazać rozstrzygalność $\{\alpha \mid \Delta \vdash_H \alpha\}$.

Procedura rozstrzygająca jest następująca: Dla danej formuły α systematycznie generujemy wszystkie dowody w systemie Hilberta, poszukując wśród nich albo dowodu $\Delta \vdash_H \alpha$, albo dowodu $\Delta \vdash_H \neg\alpha$. Wobec zaobserwowanej przez nas zupełności, jeden z nich w końcu się znajdzie. Jeśli będzie to ten pierwszy, to procedura udzieli wówczas odpowiedzi: „TAK", a jeśli ten drugi, to „NIE". ∎

Przeprowadzony przez nas dowód jest całkiem prosty, ale prowadzi do algorytmu rozstrzygającego, o którego złożoności nic rozsądnego powiedzieć nie umiemy.

Istnieją bardziej zaawansowane technicznie metody dowodzenia rozstrzygalności, które pozwalają oszacować złożoność tworzonych przez nie algorytmów. Jednak można udowodnić, że żaden taki algorytm nie może mieć złożoności mniejszej niż PSPACE, o ile tylko działa poprawnie dla wszystkich formuł zawierających symbole równości.

Twierdzenie 13.8 (Stockmeyer) *Następujący problem jest* PSPACE*-trudny: czy dane zdanie logiki pierwszego rzędu nad sygnaturą zawierającą wyłącznie symbol równości jest tautologią?*

Wobec naszej wiedzy o klasach złożoności, wątpliwe jest zatem istnienie algorytmów o wielomianowej złożoności czasowej nawet dla teorii jeszcze prostszych niż ta rozpatrywana w poprzednim twierdzeniu.

Dowód: Przeprowadzamy redukcję w pamięci logarytmicznej z problemu QBF (kwantyfikowanych formuł Boolowskich) do naszego problemu.

Instancjami problemu QBF są zdania postaci $Q_1 p_1 \dots Q_n p_n \alpha$, gdzie $Q_i \in \{\exists, \forall\}$, a α jest formułą zdaniową. Pojęcie prawdziwości takiego zdania jest definiowane w naturalny sposób. Problem QBF jest znanym problemem PSPACE-zupełnym.

Redukcja określona jest jak następuje: w zdaniu powyższym każde wystąpienie p_i zastępujemy przez $x_i = y_i$. Teraz po kolei zastępujemy kwantyfikatory:

- Każdy kwantyfikator $\forall p_i$ zamieniamy na $\forall x_i \forall y_i$.
- Każdy kwantyfikator $\exists p_i$ zamieniamy na $\exists x_i \exists y_i$.

Niech formułą otrzymana po tych operacjach będzie α'. Wtedy wynikiem naszej redukcji jest formuła α''

$$\forall x \forall y (x = y \vee \alpha').$$

Jest oczywiste, że α'' daje się obliczyć z α w logarytmicznej pamięci.

Widać, że formuły atomowe $x_i = y_i$ pełnią rolę zmiennych zdaniowych p_i, przy czym w każdej strukturze o co najmniej dwóch elementach mogą przyjmować obie wartości logiczne. Kwantyfikatory $\forall x_i \forall y_i$ i $\exists x_i \exists y_i$ swoją funkcją wiernie odpowiadają kwantyfikatorom $\forall p_i$ oraz $\exists p_i$. Z kolei klauzula $\forall x \forall y (x = y)$ czyni α'' prawdziwym w strukturach jednoelementowych, niezależnie od postaci α.

Z tego wynika, że α jest prawdziwe wtedy i tylko wtedy, gdy α'' jest tautologią. ∎

Szczególnie interesujące jest następujące twierdzenie:

Twierdzenie 13.9 (Tarski) *Teoria uporządkowanego ciała liczb rzeczywistych, tj. teoria struktury* $\langle \mathbb{R}, +, *, 0, 1, \leq \rangle$ *jest rozstrzygalna.*

Jej znaczenie dla informatyki zasadza się na fakcie, że ta teoria to w istocie znana wszystkim ze szkoły *geometria analityczna*. Poważną część algorytmicznych badań w zakresie geometrii obliczeniowej można streścić jako ulepszanie algorytmu rozstrzygającego teorię $\langle \mathbb{R}, +, *, 0, 1, \leq \rangle$ dla różnych szczególnych klas formuł, pojawiających się w praktyce.

Ćwiczenia

1. Udowodnić, że logiki trójwartościowe Heytinga-Kleene-Łukasiewicza, Bochvara i Sobocińskiego spełniają prawa de Morgana.

2. Podać przykład zdania logiki pierwszego rzędu, które nie jest tautologią, ale jest prawdziwe we wszystkich strukturach $\mathfrak{A}$ takich, że $A = ad(\mathfrak{A})$.

3. Udowodnić, że zbiór tautologii logiki pierwszego rzędu nad sygnaturą składającą się tylko z równości jest rozstrzygalny.

   Wskazówka: Niech α będzie formułą o randze kwantyfikatorowej q. Udowodnić, że każde dwie struktury o mocy co najmniej q nad powyższą sygnaturą są q-elementarnie równoważne. Wywnioskować stąd, że aby sprawdzić, czy α jest tautologią wystarczyć sprawdzić to w strukturach o mocy co najwyżej q.

4. Zbadać złożoność obliczeniową algorytmu zaproponowanego powyżej i udowodnić, że zbiór tautologii logiki pierwszego rzędu nad sygnaturą składającą się tylko z równości jest PSPACE-zupełny.

5. Udowodnić, że zbiór tautologii logiki pierwszego rzędu nad sygnaturą składającą się tylko z równości i skończenie wielu symboli stałych jest rozstrzygalny.

   Wskazówka: Rozwiązać najpierw zadanie 3, a stałe zasymulować jako relacje unarne będące singletonami.

Spis treści