METODY DOWODZENIA TWIERDZEŃ I AUTOMATYZACJA ROZUMOWAŃ

WYKŁAD 2: PRELIMINARIA LOGICZNE

III rok kognitywistyki UAM, 2016–2017

1 Plan na dziś

Wprowadzimy kilka pojęć, które będą istotnie wykorzystywane w wielu dalszych wykładach:

1. Wprowadzimy pojęcie *zbioru Hintikki*.
2. Udowodnimy Lemat Hintikki (dla KRZ).
3. Wprowadzimy pojęcie *własności niesprzeczności*.
4. Udowodnimy twierdzenie o istnieniu modelu (dla KRZ).
5. Udowodnimy twierdzenie o zwartości (dla KRZ).

Uwagi historyczne dotyczące metod dowodowych będą podawane podczas poszczególnych wykładów. Na końcu dzisiejszego wykładu podamy krótką listę ważnych osiągnięć w logice, głównie w XX wieku.

2 Drobiazgi formalne

Potrzebne będą pewne proste pojęcia pomocnicze. Niektóre z nich są zapewne znane z kursu *Wprowadzenia do logiki*.

2.1 Stopnie i rangi formuł

Funkcja stopnia dg zdefiniowana jest indukcyjnie:

1. Stopień formuł atomowych (zmiennych oraz $\bot$ i $\top$) jest równy 0.
2. $dg(\neg\psi) = dg(\psi) + 1$

3. $dg((\varphi \circ \psi)) = dg(\varphi) + dg(\psi) + 1$, gdzie $\circ$ jest funktorem dwuargumentowym.

Funkcja rangi rk zdefiniowana jest indukcyjnie:

1. $rk(p) = rk(\neg p) = 0$ dla zmiennych zdaniowych p. $rk(\bot) = rk(\top) = 0$.
2. $rk(\neg\neg\psi) = rk(\psi) + 1$
3. $rk(\alpha) = rk(\alpha_1) + rk(\alpha_2) + 1$
4. $rk(\beta) = rk(\beta_1) + rk(\beta_2) + 1$

Zdefiniowane wyżej funkcje charakteryzują złożoność składniową formuł. Są przydatne w dowodach twierdzeń.

2.2 Notacja

Formuły są liniowymi ciągami symboli. W notacji *infiksowej* symbol funktora dwuargumentowego piszemy między symbolami jego argumentów. Musimy korzystać z nawiasów, dla zaznaczenia struktury składniowej formuł. W notacji *prefiksowej* (notacji Łukasiewicza, *polskiej*) symbol funktora poprzedza swoje argumenty. W tej notacji nie potrzebujemy nawiasów. Oczywiście przyjąć trzeba ustalone symbole dla funktorów (różne od symboli dla zmiennych), np.:

1. N – negacja
2. A – alternatywa
3. K – koniunkcja
4. C – implikacja
5. E – równoważność.

PRZYKŁAD. Prawo *modus tollendo tollens*:

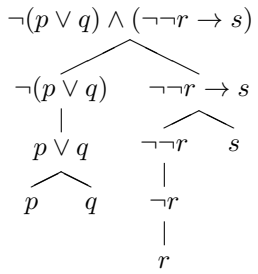
1. W notacji infiksowej: $((p \to q) \wedge \neg q) \to \neg p$
2. W notacji prefiksowej: $CKCpqNqNp$

2.3 Reprezentacja budowy składniowej formuł

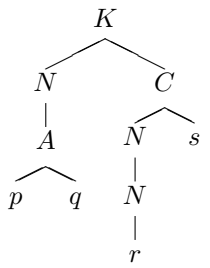
Pamiętamy indukcyjną definicję zbioru formuł języka KRZ. Przypomnijmy też, że budowę składniową formuł reprezentować możemy przez *drzewa składniowe* (w postaci pełnej lub skróconej). Ograniczymy się do przykładu, ilustrującego tę konstrukcję.

PRZYKŁAD. Formuła $\neg(p \vee q) \wedge (\neg\neg r \to s)$ przekształcona do postaci prefiksowej wygląda następująco: $KNApqCNNrs$.

Pełne drzewo składniowe tej formuły (w notacji infiksowej) wygląda następująco:



Skrócone drzewo składniowe tej formuły (w notacji prefiksowej) wygląda następująco:



Pełne i skrócone drzewa składniowe można oczywiście budować dla każdej z wymienionych notacji.

3 Lemat Hintikki

Zbiór **H** formuł języka KRZ nazywamy *zdaniowym zbiorem Hintikki*, jeśli:

1. Dla dowolnej zmiennej zdaniowej p, zachodzi co najmniej jedno z dwojga: $p \notin \mathbf{H}$ lub $\neg p \notin \mathbf{H}$
2. $\bot \notin \mathbf{H}$ oraz $\neg\top \notin \mathbf{H}$;

3. Jeśli $\neg\neg\psi \in \mathbf{H}$, to $\psi \in \mathbf{H}$;

4. Jeśli $\alpha \in \mathbf{H}$, to $\alpha_1 \in \mathbf{H}$ oraz $\alpha_2 \in \mathbf{H}$;

5. Jeśli $\beta \in \mathbf{H}$, to $\beta_1 \in \mathbf{H}$ lub $\beta_2 \in \mathbf{H}$.

Zbiory Hintikki nazywa się także zbiorami *nasyconymi w dół* (*downward saturated*). Może trafniej byłoby mówić: *nasycone w głąb*? Cantor mówił podobno, że wyobraża sobie zbiory jako *przepaście*.

Lemat Hintikki. Każdy zdaniowy zbiór Hintikki jest spełnialny.

Dowód. Niech $\mathbf{H}$ będzie zbiorem Hintikki. Zbudujemy wartościowanie v, przy którym każdy element zbioru $\mathbf{H}$ przyjmie wartość 1.

- Jeśli $p \in \mathbf{H}$, to niech $v(p) = 1$. Jeśli $\neg p \in \mathbf{H}$, to niech $v(p) = 0$. Jeśli ani p ani $\neg p$ nie należą do $\mathbf{H}$, to niech $v(p) = 0$. Wreszcie, niech $v(\bot) = v(\neg\top) = 0$.

- Jak pamiętamy z semantyki KRZ, wartościowanie v można jednoznacznie rozszerzyć do odwzorowania v^* wszystkich formuł zdaniowych w zbiór $\{0, 1\}$.

- Wtedy $v^*(\psi) = 1$ dla wszystkich $\psi \in \mathbf{H}$, czego dowodzimy np. przez indukcję po randze formuł.

- Dla zmiennych zdaniowych mamy $v^*(p) = 1$ wtedy i tylko wtedy, gdy $p \in \mathbf{H}$. Dalej, $v^*(\bot) = v^*(\neg\top) = 0$ na mocy definicji v. Tak więc, $v^*(\psi) = 1$ dla wszystkich formuł o randze 0 należących do $\mathbf{H}$.

- Załóżmy, że dla wszystkich formuł $\psi \in \mathbf{H}$ rangi mniejszej od $n > 0$ zachodzi $v^*(\psi) = 1$.

- Jeśli α ma rangę n, to α_1 oraz α_2 są elementami $\mathbf{H}$ oraz mają rangę mniejszą od n. Z założenia indukcyjnego $v^*(\alpha_1) = 1 = v^*(\alpha_2)$. Wtedy $v^*(\alpha) = 1$.

- Jeśli β ma rangę n, to albo $\beta_1 \in \mathbf{H}$ albo $\beta_2 \in \mathbf{H}$. Nadto, β_1 oraz β_2 mają rangę mniejszą od n. Z założenia indukcyjnego: albo $v^*(\beta_1) = 1$ albo $v^*(\beta_2) = 1$. A zatem $v^*(\beta) = 1$.

4 Własności niesprzeczności

Niech $\mathcal{C}$ będzie rodziną zbiorów formuł języka KRZ. Mówimy, że $\mathcal{C}$ jest *zdaniową własnością niesprzeczności* (*propositional consistency property*), jeśli dla każdego zbioru $S \in \mathcal{C}$:

1. Dla każdej zmiennej zdaniowej p: albo $p \notin S$ albo $\neg p \notin S$
2. $\bot \notin S$ oraz $\neg \top \notin S$
3. Jeśli $\neg\neg\psi \in S$, to $S \cup \{\psi\} \in S$
4. Jeśli $\alpha \in S$, to $S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$
5. Jeśli $\beta \in S$, to $S \cup \{\beta_1\} \in \mathcal{C}$ lub $S \cup \{\beta_2\} \in \mathcal{C}$.

- Tak więc, każda własność niesprzeczności jest rodziną zbiorów, spełniającą pewne warunki domknięcia.
- Jeśli $S \in \mathcal{C}$, to mówimy, że S jest *$\mathcal{C}$-niesprzeczny*.

PRZYKŁADY:

- Rodzina wszystkich zbiorów niesprzecznych jest zdaniową własnością niesprzeczności.
- Rodzina wszystkich zbiorów spełnialnych jest zdaniową własnością niesprzeczności.
- Rodzina wszystkich zbiorów, których każdy skończony podzbiór jest spełnialny, jest zdaniową własnością niesprzeczności.
- Nazwiemy zbiór formuł S *tablicowo niesprzecznym*, gdy nie istnieje zamknięta tablica analityczna dla S. Rodzina wszystkich zbiorów tablicowo niesprzecznych jest zdaniową własnością niesprzeczności.

Pojęcie *własności niesprzeczności* można określić także dla logiki pierwszego rzędu (zrobimy to później). Pojęcie *własności niesprzeczności* można określić dla różnych metod dowodowych. Szczególnie interesują nas własności niesprzeczności, które spełniają pewne dalsze warunki domknięcia:

- Własność niesprzeczności $\mathcal{C}$ jest *domknięta na podzbiory*, gdy dla każdego $S \in \mathcal{C}$ oraz wszystkich $T \subseteq S$: $T \in \mathcal{C}$.
- Własność niesprzeczności $\mathcal{C}$ jest *charakteru skończonego*, gdy: $S \in \mathcal{C}$ wtedy i tylko wtedy, gdy każdy skończony podzbiór zbioru S należy do $\mathcal{C}$.

Zachodzą następujące fakty:

1. Każda własność niesprzeczności może zostać rozszerzona do własności niesprzeczności domkniętej na podzbiory.

2. Każda własność niesprzeczności charakteru skończonego jest domknięta na podzbiory.

3. Każda własność niesprzeczności domknięta na podzbiory może zostać rozszerzona do własności niesprzeczności charakteru skończonego.

Jako ewentualne ćwiczenie na konwersatorium zaproponować można udowodnienie powyższych punktów 1–3. Dodajmy, że dowody znaleźć można na stronie wykładu z roku akademickiego 2015–2016.

PRZERYWNIK MUZYCZNY: LOGIC RAP.

Profesor:
Bierzemy ciąg niesprzecznych zbiorów, wstępujący ściśle.
To jaka jest ich suma, niech ja tylko pomyślę.
Ona też jest niesprzeczna, mój młody kolego.
Ty pytasz: panie psorze, ach, dlaczego, dlaczego?
Dowód podam nie wprost, jak w kościele na tacę.
Przypuśćmy, drodzy goście, że byłoby inaczej.
Gdyby była sprzeczna, no to nie ma siły:
Sprzeczność już na którymś piętrze by się pojawiła.
Co przeczy założeniu oraz kończy dowód.
Studenci:
I wszystkim nam dostarcza doskonały powód,
By zakończyć ten wykład i żywo na piwo!

1. Pierwsze założenie za mocne, ale ratuje rym.

2. Były jeszcze dwie (obsceniczne) linijki, które tu opuszczamy.

Twierdzenie. Załóżmy, że $\mathcal{C}$ jest własnością niesprzeczności charakteru skończonego oraz że S_1, S_2, S_3, ... jest łańcuchem wstępującym (ze względu na inkluzję) elementów rodziny $\mathcal{C}$. Wtedy $\bigcup_n S_n \in \mathcal{C}$.

Dowód. Ponieważ $\mathcal{C}$ jest własnością niesprzeczności charakteru skończonego, więc wystarczy udowodnić, że każdy skończony podzbiór zbioru $\bigcup_n S_n$ należy do $\mathcal{C}$.

Przypuśćmy, że $\{\psi_1, \ldots, \psi_k\} \subseteq \bigcup_n S_n$. Pokażemy, że $\{\psi_1, \ldots, \psi_k\} \in \mathcal{C}$.

Dla każdego $1 \leqslant i \leqslant k$ istnieje najmniejszy indeks n_i taki, że $\psi_i \in S_{n_i}$. Niech $m = \max\{n_1, \ldots, n_k\}$. Wtedy $\psi_i \in S_m$ dla wszystkich $1 \leqslant i \leqslant k$.

Ponieważ $S_m \in \mathcal{C}$ oraz $\mathcal{C}$ jest domknięta na podzbiory, więc $\{\psi_1, \ldots, \psi_k\} \in \mathcal{C}$.

5 Twierdzenie o istnieniu modelu

Twierdzenie o Istnieniu Modelu (dla KRZ). Jeśli $\mathcal{C}$ jest zdaniową własnością niesprzeczności oraz $S \in \mathcal{C}$, to S jest spełnialny.

- Twierdzenie to będzie wielokrotnie wykorzystane w dowodach pełności rozważanych metod dowodowych.
- Dowód tego twierdzenia istotnie korzysta z Lematu Hintikki.
- Zasadniczy pomysł polega na tym, że każdy zbiór S z rozważanej własności niesprzeczności $\mathcal{C}$ można rozszerzyć do pewnego zbioru Hintikki $\mathbf{H}_S$, również należącego do $\mathcal{C}$. Skoro $S \subseteq \mathbf{H}_S$, a $\mathbf{H}_S$ jest spełnialny (Lemat Hintikki!), to również S jest spełnialny.

5.1 Dowód twierdzenia o istnieniu modelu

- Załóżmy, że $S \in \mathcal{C}$.
- Na mocy poprzednich ustaleń możemy założyć, że $\mathcal{C}$ jest charakteru skończonego.
- Ustawiamy wszystkie formuły języka KRZ w ciąg przeliczalny: $\psi_1, \psi_2, \psi_3, \ldots$ (w porządku leksykograficznym).
- Definiujemy ciąg S_1, S_2, S_3,... elementów $\mathcal{C}$ w sposób następujący:
  1. $S_1 = S$
  2. $S_{n+1} = S_n \cup \{\psi_n\}$, o ile $S_n \cup \{\psi_n\} \in \mathcal{C}$, natomiast $S_{n+1} = S_n$ w przeciwnym przypadku.
- Wszystkie elementy tego ciągu należą do $\mathcal{C}$ i tworzą łańcuch wstępujący. Niech $\mathbf{H}_S = \bigcup_n S_n$. Wtedy $S \subseteq \mathbf{H}_S$.
- Ponieważ $\mathcal{C}$ jest charakteru skończonego i jest domknięta na sumy łańcuchów, więc $\mathbf{H}_S \in \mathcal{C}$.

$\mathbf{H}_S$ jest elementem maksymalnym w $\mathcal{C}$: Przypuśćmy, że istnieje $K \in \mathcal{C}$ taki, że: $\mathbf{H}_S \subseteq K$ oraz $\mathbf{H}_S \neq K$. Wtedy istnieje $\psi_n \in K - \mathbf{H}_S$. Oznacza to, że $\psi_n \notin S_{n+1}$, a zatem $S_n \cup \{\psi_n\} \notin \mathcal{C}$.

Jednak $S_n \cup \{\psi_n\} \subseteq K$, ponieważ $S_n \subseteq \mathbf{H}_S \subseteq K$ oraz $\psi_n \in K$. Ponieważ $\mathcal{C}$ jest domknięta na podzbiory, więc $S_n \cup \{\psi_n\} \in \mathcal{C}$, sprzeczność.

$\mathbf{H}_S$ *jest zbiorem Hintikki:* Warunki dla zmiennych zdaniowych oraz $\bot$ i $\neg\top$ zachodzą na mocy konstrukcji zbioru $\mathbf{H}_S$ oraz definicji rodziny $\mathcal{C}$. Jeśli $\neg\neg\psi \in \mathbf{H}_S$, to $\psi \in \mathbf{H}_S$, ponieważ $\mathbf{H}_S \in \mathcal{C}$. Załóżmy, że $\alpha \in \mathbf{H}_S$. Ponieważ $\mathbf{H}_S \in \mathcal{C}$, więc $\mathbf{H}_S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$. Ponieważ $\mathbf{H}_S$ jest maksymalny, więc $\{\alpha_1, \alpha_2\} \subseteq \mathbf{H}_S$. Załóżmy, że $\beta \in \mathbf{H}_S$. Ponieważ $\mathbf{H}_S \in \mathcal{C}$, więc $\mathbf{H}_S \cup \{\beta_1\} \in \mathcal{C}\}$ lub $\mathbf{H}_S \cup \{\beta_2\} \in \mathcal{C}\}$. Ponieważ $\mathbf{H}_S$ jest maksymalny, więc $\beta_1 \in \mathbf{H}_S$ lub $\beta_2 \in \mathbf{H}_S$.

Na mocy Lematu Hintikki S jest spełnialny, ponieważ $S \subseteq \mathbf{H}_S$.

6 Twierdzenie o zwartości

Twierdzenie o Zwartości. Niech S będzie zbiorem formuł języka KRZ. Jeśli każdy skończony podzbiór zbioru S jest spełnialny, to S jest spełnialny.

Dowód. Załóżmy, że każdy skończony podzbiór zbioru S jest spełnialny. Plan dowodu jest następujący:

- Definiujemy rodzinę $\mathcal{C}$ zbiorów formuł języka KRZ jako rodzinę tych wszystkich zbiorów formuł, których każdy skończony podzbiór jest spełnialny.
- Wtedy oczywiście $S \in \mathcal{C}$.
- Trzeba będzie pokazać, że $\mathcal{C}$ jest własnością niesprzeczności.
- Następnie wystarczy skorzystać z Twierdzenia o Istnieniu Modelu.

6.1 Dowód twierdzenia o zwartości

Przypuśćmy, że $W \in \mathcal{C}$ oraz $\{p, \neg p\} \subseteq W$ dla pewnej zmiennej zdaniowej p. Zbiór $\{p, \neg p\}$ jest skończony, ale nie jest spełnialny, a więc początkowe przypuszczenie musi zostać odrzucone.

Oczywiście, jeśli $W \in \mathcal{C}$ oraz $\neg\neg\psi \in W$, to $W \cup \{\psi\} \in \mathcal{C}$.

Załóżmy, że $W \in \mathcal{C}$ oraz $\alpha \in W$. Pokażemy, że każdy skończony podzbiór zbioru $W \cup \{\alpha_1, \alpha_2\}$ jest spełnialny, czyli $W \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$. Skończony podzbiór zbioru $W \cup \{\alpha_1, \alpha_2\}$ może: nie zawierać żadnej z formuł α_1, α_2, zawierać dokładnie jedną z nich, zawierać obie. Wystarczy rozważyć ostatni przypadek, czyli $W_0 \cup \{\alpha_1, \alpha_2\}$, gdzie W_0 jest skończonym podzbiorem W. Wtedy $W_0 \cup \{\alpha\}$ też jest skończonym podzbiorem W, a więc jest spełnialny. Dowolne wartościowanie posyłające każdy element zbioru $W_0 \cup \{\alpha\}$ w 1 musi zatem posyłać w 1 zarówno α_1 jak i α_2. Oznacza to, że $W_0 \cup \{\alpha, \alpha_1, \alpha_2\}$ jest spełnialny, z zatem $W_0 \cup \{\alpha_1, \alpha_2\}$ jest spełnialny.

- Załóżmy, że $W \in \mathcal{C}$ oraz $\beta \in W$. Pokażemy, że: albo $W \cup \{\beta_1\} \in \mathcal{C}$ albo $W \cup \{\beta_2\} \in \mathcal{C}$. Niech W_0 będzie skończonym podzbiorem W.

- $W_0 \cup \{\beta\}$ także jest skończonym podzbiorem W, a więc jest spełnialny: istnieje wartościowanie v posyłające każdy element zbioru $W_0 \cup \{\beta\}$ w 1.
- Na mocy definicji wartościowań: albo $v(\beta_1) = 1$ albo $v(\beta_2) = 1$.
- W konsekwencji, wartościowanie v posyła w 1: albo wszystkie elementy zbioru $W_0 \cup \{\beta, \beta_1\}$ albo wszystkie elementy zbioru $W_0 \cup \{\beta, \beta_2\}$. Tak więc: albo $W_0 \cup \{\beta, \beta_1\}$ albo $W_0 \cup \{\beta, \beta_2\}$ jest spełnialny.
- Ponieważ podzbiór zbioru spełnialnego jest spełnialny, więc: albo $W_0 \cup \{\beta_1\}$ albo $W_0 \cup \{\beta_2\}$ jest spełnialny.
- Ostatecznie: albo $W \cup \{\beta_1\} \in \mathcal{C}$ albo $W \cup \{\beta_2\} \in \mathcal{C}$.

7 Uwagi historyczne

Niniejszy kurs jest zorientowany na umiejętności praktyczne: słuchacze mają poznać kilka metod dowodowych oraz możliwości ich automatyzacji. Do ogólnego wykształcenia logicznego należy też jednak rozeznanie, kto przyczynił się do rozwoju logiki.

1. Początki logiki: Arystoteles, Stoicy, logicy Średniowiecza, Leibniz.
2. Błogosławiony Rajmund Lull (*Doctor Illuminatus*, 1232–1315): logika w służbie nawracania niewiernych.
3. Gottfried Wilhelm von Leibniz (1646–1716): prekursor logiki formalnej.
4. Początki logiki matematycznej: De Morgan, Boole, Peano, Frege, Pierce, Schröder, Russell, Leśniewski, Łukasiewicz,...
5. Gottlob Frege (1848–1925): *Begriffschrift*
6. Bertrand Russell (1872–1970): *Principia Mathematica* (wspólnie z Afredem Whiteheadem (1861–1947))
7. David Hilbert (1862–1943) i jego program
8. Ernst Zermelo (1871–1953): teoria mnogości
9. Emil Post (1897–1954): algebra logiki, systemy Posta
10. Gerhard Gentzen (1909–1945): dedukcja naturalna, sekwenty
11. Alan Turing (1912–1954): teoria obliczeń

12. Jacques Herbrand (1908–1931): twierdzenie Herbranda, obliczalność
13. Thoralf Skolem (1887–1963): teoria mnogości, arytmetyka
14. Kurt Gödel (1906–1978): niezupełność PM, teoria mnogości
15. Luitzen Egbertus Jan Brouwer (1881–1966): intuicjonizm
16. Alonzo Church (1903–1995): nierozstrzygalność KRP
17. Stanisław Jaśkowski (1906–1965): dedukcja naturalna
18. Alfred Tarski (1903–1983): teoria modeli
19. Adolf Lindenbaum (1904–1941): lemat Lindenbauma

JERZY POGONOWSKI
Zakład Logiki i Kognitywistyki UAM
www.kognitywistyka.amu.edu.pl
http://logic.amu.edu.pl/index.php/Dydaktyka
pogon@amu.edu.pl