Metody Dowodzenia Twierdzeń
I Automatyzacja Rozumowań

III rok kognitywistyki UAM, 2016–2017

1 Cele wykładu

Wykład ma trzy zasadnicze cele:

1. Przedstawienie wybranych metod dowodowych, stosowanych w logice. Omówimy: metodę aksjomatyczną, tablice analityczne, rezolucję, dedukcję naturalną oraz rachunki sekwentów.
2. Ukazanie możliwości podania matematycznej reprezentacji intuicyjnego pojęcia *obliczalności*. Wybieramy formalizm *funkcji rekurencyjnych*.
3. Przedstawienie wybranych faktów metalogicznych, które uznaje się za najważniejsze osiągnięcia w logice matematycznej XX wieku.

2 Uwagi organizacyjne

1. Wykład prowadzi Jerzy Pogonowski. Strona internetowa wykładu:

   http://logic.amu.edu.pl/index.php/Mdtiar

   Na tej stronie zamieszczono syllabus przedmiotu.
2. Konwersatoria prowadzi w tym roku akademickim Pani dr Dorota Leszczyńska-Jasion.
3. Zajęcia w pracowni komputerowej prowadzi w tym roku akademickim Pani dr Mirosława Kołowska-Gawiejnowicz.
4. Tematy wykładów pokrywają się z tematami wykładów z roku akademickiego 2015–2016 (wtedy było to 15 spotkań po 90 minut). Ponieważ jednak mamy do dyspozycji jedynie 15 spotkań po 45 minut, więc zmuszeni jesteśmy do ograniczenia przekazywanych treści.
5. Materiały dydaktyczne do wykładu 2015–2016 są dostępne na wyżej wymienionej stronie. Materiały do tegorocznego wykładu będą na niej zamieszczane na bieżąco.

6. Korzystać będziemy z wiadomości przekazanych na kursach: *Wprowadzenie do logiki*, *Logika I*, *Matematyczne podstawy kognitywistyki*.

7. Kurs kończy się egzaminem pisemnym. Przykładowe pytania egzaminacyjne zostaną podane przed rozpoczęciem sesji zimowej. Na ostatnim wykładzie zrobimy powtórkę materiału, przygotowującą do egzaminu.

8. Zasady zaliczenia konwersatorium oraz zajęć w pracowni komputerowej zostaną podane przez prowadzących te zajęcia.

3 Literatura

3.1 Literatura podstawowa

1. Fitting, M. 1996. *First-Order Logic and Automated Theorem Proving*. Springer, Berlin.

2. Ławrow, I.A., Maksimowa, Ł.L. 2004. *Zadania z teorii mnogości, logiki matematycznej i teorii algorytmów*. Wydawnictwo Naukowe PWN, Warszawa.

3. Pogorzelski, W.A. 1992. *Elementarny słownik logiki formalnej*. Wydawnictwo Filii Uniwersytetu Warszawskiego, Białystok.

4. *Stanford Encyclopedia of Philosophy*: http://plato.stanford.edu/ (artykuły poświęcone teorii dowodu oraz automatyzacji rozumowań: *The development of proof theory*, *Automated reasoning*).

3.2 Literatura dodatkowa

1. D'Agostino, M., Gabbay, D., Hähnle, R., Posega, J. (Eds.) 1999. *Handbook of Tableaux Methods*. Kluwer Academic Publishers, Dordrecht Boston London.

2. Gallier, J. 2003. *Logic for Computer Science. Foundations of Automated Theorem Proving*. Dover Publications, Mineola, New York.

3. Kaye, R. 2007. *The Mathematics of Logic. A guide to completeness theorems and their applications*. Cambridge University Press, Cambridge.

4. Ligonniére, R. 1992. *Prehistoria i historia komputerów*. Ossolineum, Wrocław-Warszawa-Kraków.

5. Marciszewski, W., Murawski, R. 1995. *Mechanization of reasoning in a historical perspective*. Rodopi, Amsterdam-Atlanta.

6. Negri, S., von Plato, J. 2001. *Structural Proof Theory*. Cambridge University Press, Cambridge.

7. Nerode, A., Shore, R.A. 1997. *Logic for Applications*. Springer-Verlag, New York.

8. Orłowska, E., Golińska-Pilarek, J. 2011. *Dual Tableaux: Foundation, Methodology, Case Studies*. Springer, Dordrecht Heidelberg London New York.

9. Smullyan, R. 1968. *First-Order Logic*. Springer, Berlin.

Proponuję także lekturę zamieszczonych na stronach ZLiK materiałów dydaktycznych: Pani Dr Doroty Leszczyńskiej-Jasion, Pana Prof. Mariusza Urbańskiego oraz Pana prof. Andrzeja Wiśniewskiego.

4 Metody dowodowe

4.1 Proste przykłady

Rozważmy dwa przykłady argumentacji:

- Nasza Pani od Biologii i Nietoperze
- „Milicja, Wrocław i ja”

NASZA PANI OD BIOLOGII I NIETOPERZE

- Nasza Pani od Biologii opowiada o Nietoperzach: *Jeśli Nietoperze nie mają piór, to: są Ptakami, o ile fruwają.* Nasza Pani od Biologii wyciąga z kieszeni Nietoperza i stwierdza: *Nietoperze nie mają piór.* Nasza Pani od Biologii zagląda do podręcznika systematyki Zwierząt i stwierdza: *Ale przecież Nietoperze nie są Ptakami.* Nasza Pani od Biologii konkluduje: *A zatem Nietoperze nie fruwają.*
- p: *Nietoperze mają pióra.*
- q: *Nietoperze fruwają.*
- r: *Nietoperze są Ptakami.*
- Przesłanka: $\neg p \to (q \to r)$
- Przesłanka: $\neg p$

- Przesłanka: $\neg r$
- Wniosek: $\neg q$

Drzewo argumentacji (dowodu) ma postać następującą:

$$\dfrac{\neg r \qquad \dfrac{\neg p \rightarrow (q \rightarrow r) \qquad \neg p}{q \rightarrow r}}{\neg q}$$

W tej argumentacji posłużono się kolejno regułami:

- *modus ponens*
- *modus tollens*.

Argumentacja jest poprawna z logicznego punktu widzenia. Wniosek jest fałszywy, a zatem któraś z przesłanek jest fałszywa.
„MILICJA, WROCŁAW I JA”. Czy na podstawie uznania następujących stwierdzeń:

- *Jeśli nie udowodniono podejrzanemu popełnienia morderstwa, to: stwierdzono samobójstwo denata lub wykonano sentencję wyroku, o ile udało się zatrzymać podejrzanego.*
- *Podejrzanemu nie udowodniono popełnienia morderstwa.*
- *Nie stwierdzono samobójstwa denata.*
- *Udało się zatrzymać podejrzanego.*

gotowa jesteś uznać stwierdzenie:

- *Wykonano sentencję wyroku*?

Uwaga: musimy podjąć decyzję dotyczącą reprezentacji składniowej pierwszej przesłanki.

Zdania proste w tym tekście:

- p: *Udowodniono podejrzanemu popełnienie morderstwa.*
- q: *Stwierdzono samobójstwo denata.*
- r: *Udało się zatrzymać podejrzanego.*

- s: *Wykonano sentencję wyroku.*
- Przesłanka: $\neg p \rightarrow (q \vee (r \rightarrow s))$
- Przesłanka: $\neg p$
- Przesłanka: $\neg q$
- Przesłanka: r
- Wniosek: s

Drzewo argumentacji (dowodu):

$$\dfrac{r \qquad \dfrac{\neg q \qquad \dfrac{\neg p \qquad \neg p \rightarrow (q \vee (r \rightarrow s))}{q \vee (r \rightarrow s)}}{r \rightarrow s}}{s}$$

W tej argumentacji posłużono się kolejno regułami:

- *modus ponens* (*reguła odrywania*)
- *opuszczania alternatywy*
- *modus ponens*.

Argumentacja jest *poprawna* z logicznego punktu widzenia.

4.2 Dowody, algorytmy, obliczenia

- Dowody (w sensie logicznym): dobrze określone obiekty syntaktyczne. To pojęcie znane jest słuchaczom z kursu logiki.
- Dowody matematyczne: argumentacje stosowane w matematyce.
- Dogmat, przyjmowany przez logików: każdy dowód matematyczny może zostać przekształcony w dowód w sensie logicznym.
- Algorytm: czysto mechaniczna procedura, pozwalająca w skończonej liczbie prostych, z góry określonych kroków uzyskać wynik (odpowiedź, rozwiązanie).
- Intuicyjne pojęcie *procedury obliczalnej* poddano formalizacji, na wiele sposobów: funkcje rekurencyjne, maszyny Turinga, systemy Posta, algorytmy Markowa, rachunek λ Churcha, itd.
- Uzyskano wyniki dotyczące *niezupełności* oraz *nierozstrzygalności* ważnych teorii matematycznych.

5 Krótka powtórka

Przypomnimy kilka pojęć, które powinny być słuchaczom znane z kursu wprowadzenia do logiki. Będą one dotyczyły semantyki KRZ (klasycznego rachunku zdań).

5.1 Funkcje prawdziwościowe

p	q	$\bot$	$\wedge$	$\nrightarrow$	p	$\nleftarrow$	q	$\not\equiv$	$\vee$	$\downarrow$	$\equiv$	$\neg q$	$\leftarrow$	$\neg p$	$\rightarrow$	$\uparrow$	$\top$
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Pierwsze dwie kolumny podają wszystkie układy wartości argumentów, kolejne kolumny podają wartość dla tego układu argumentów każdej z szesnastu dwuargumentowych funkcji prawdziwościowych. Czy widzisz jakieś *symetrie* w tej tabeli?

Lubimy odróżniać: spójnik, funktor oraz funkcję (wszystkie z określeniem: prawdziwościowy). Nie jesteśmy jednak ortodoksami i przystajemy na uproszczenia w podręcznikach (w których funktor prawdziwościowy oraz odpowiadająca mu funkcja prawdziwościowa oznaczane są tym samym symbolem).

5.2 Zależności między funkcjami prawdziwościowymi

1. Formuły φ i ψ języka KRZ są *semantycznie równoważne*, gdy dla każdego wartościowania v: $v(\varphi) = v(\psi)$.

2. Jeśli φ i ψ są semantycznie równoważne, to piszemy $\varphi \sim \psi$.

3. $\sim$ jest relacją równoważności.

4. Fakt: $\varphi \sim \psi$ wtedy i tylko wtedy, gdy $\varphi \equiv \psi$ jest tautologią KRZ.

Każda formuła języka KRZ jest semantycznie równoważna formule zawierającej jedynie:

1. koniunkcję i negację

2. alternatywę i negację

3. implikację i negację

4. implikację i falsum.

Zapewne podczas kursu wprowadzenia do logiki słuchacze wykonywali ćwiczenia, dotyczące wzajemnej definiowalności funktorów prawdziwościowych. Prawdopodobnie niektóre z tych ćwiczeń zostaną przypomniane podczas tegorocznego konwersatorium.

Funktory $\uparrow$ (NAND, kreska Sheffera) oraz $\downarrow$ (binegacja, strzałka Peirce'a, NOR) są jedynymi, za pomocą których można (w logice klasycznej) wyrazić (zdefiniować) wszystkie pozostałe funktory prawdziwościowe. Słuchacze, którzy zechcieliby udowodnić to samodzielnie zechcą zauważyć (udowodnić), że tautologiami KRZ są:

1. $p \uparrow q \;\equiv\; \neg(p \wedge q)$
2. $\neg p \;\equiv\; p \uparrow p$
3. $(p \wedge q) \;\equiv\; ((p \uparrow q) \uparrow (p \uparrow q))$
4. $(p \vee q) \;\equiv\; ((p \uparrow p) \uparrow (q \uparrow q))$
5. $(p \rightarrow q) \;\equiv\; (p \uparrow (q \uparrow q))$
6. $(p \rightarrow q) \;\equiv\; (p \uparrow (p \uparrow q))$
7. $(p \downarrow q) \;\equiv\; \neg(p \vee q)$
8. $\neg p \;\equiv\; p \downarrow p$
9. $(p \wedge q) \;\equiv\; ((p \downarrow p) \downarrow (q \downarrow q))$
10. $(p \vee q) \;\equiv\; ((p \downarrow q) \downarrow (p \downarrow q))$
11. $(p \rightarrow q) \;\equiv\; (((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q))$

5.3 Funktory pierwszorzędne

1arg.	2 arg.	$\wedge$	$\vee$	$\rightarrow$	$\leftarrow$	$\uparrow$	$\downarrow$	$\not\rightarrow$	$\not\leftarrow$
1	1	1	1	1	1	0	0	0	0
1	0	0	1	0	1	1	0	1	0
0	1	0	1	1	0	1	0	0	1
0	0	0	0	1	1	1	1	0	0

Poszczególne kolumny tej tabeli odpowiadają: pierwszemu argumentowi, drugiemu argumentowi, koniunkcji, alternatywie, implikacji prostej, implikacji odwrotnej, kresce Sheffera, binegacji, zaprzeczeniu implikacji prostej, zaprzeczeniu implikacji odwrotnej.

Funktor $\uparrow$ jest (przez informatyków) nazywany NAND, natomiast $\downarrow$ nazywany jest (przez informatyków) NOR.

Uwaga na porządek wierszy tej tabeli! Taki podaje Fitting, my lubimy dokładnie odwrotny porządek.

5.4 Notacja Smullyana

- Od kilku dekad karierę robi notacja zaproponowana przez Raymonda Smullyana, zwana też jednolitą notacją (*uniform notation*).

- Notacja ta motywowana jest własnościami semantycznymi. Pozwala też na dość proste przeprowadzanie dowodów twierdzeń metalogicznych.

Wśród funktorów pierwszorzędnych oraz ich zaprzeczeń wyróżnimy te, które „działają” koniunkcyjnie oraz te, które „działają” alternatywnie. Formuły z tymi pierwszymi funktorami oznacza się symbolem α, te drugie zaś symbolem β. *Składniki* takich formuł są oznaczane symbolami, odpowiednio: α_1, α_2 oraz β_1, β_2. Składniki te wyznaczane są wedle następującej konwencji:

α	α_1	α_2
$\varphi \wedge \psi$	φ	ψ
$\neg(\varphi \vee \psi)$	$\neg\varphi$	$\neg\psi$
$\neg(\varphi \rightarrow \psi)$	φ	$\neg\psi$
$\neg(\varphi \leftarrow \psi)$	$\neg\varphi$	ψ
$\neg(\varphi \uparrow \psi)$	φ	ψ
$\varphi \downarrow \psi$	$\neg\varphi$	$\neg\psi$
$\varphi \nrightarrow \psi$	φ	$\neg\psi$
$\varphi \nleftarrow \psi$	$\neg\varphi$	ψ

β	β_1	β_2
$\neg(\varphi \wedge \psi)$	$\neg\varphi$	$\neg\psi$
$\varphi \vee \psi$	φ	ψ
$\varphi \rightarrow \psi$	$\neg\varphi$	ψ
$\varphi \leftarrow \psi$	φ	$\neg\psi$
$\varphi \uparrow \psi$	$\neg\varphi$	$\neg\psi$
$\neg(\varphi \downarrow \psi)$	φ	ψ
$\neg(\varphi \nrightarrow \psi)$	$\neg\varphi$	ψ
$\neg(\varphi \nleftarrow \psi)$	φ	$\neg\psi$

Później rozszerzymy jednolitą notację na język KRP (klasycznego rachunku predykatów).

6 Preliminaria matematyczne

6.1 Drzewa

Drzewem (o korzeniu x_0) nazwiemy każdy układ $\langle X, R, x_0\rangle$ taki, że:

1. $\langle X, R\rangle$ jest grafem o zbiorze *wierzchołków* X i zbiorze *krawędzi* $R \subseteq X \times X$;

2. R jest częściowym porządkiem w X;

3. x_0 jest elementem R-najmniejszym w X;

4. zbiór wszystkich R-poprzedników każdego wierzchołka jest liniowo uporządkowany przez relację R.

- *Liśćmi* drzewa D nazywamy wszystkie te jego wierzchołki, które nie mają R-następników.

- Jeśli $(x, y) \in R$ jest krawędzią w D, to x nazywamy *przodkiem* y, a y nazywamy *potomkiem* x. Jeśli $(x, y) \in R - R^2$ jest krawędzią w D, to x nazywamy *bezpośrednim przodkiem* y, zaś y nazywamy *bezpośrednim potomkiem* x.

- Każdy podzbiór zbioru wierzchołków drzewa D, który jest uporządkowany liniowo przez R nazywamy *łańcuchem* w D (czasem: *ścieżką* w D). Każdy łańcuch maksymalny (względem inkluzji) w D nazywamy *gałęzią* w D.

- Przez *długość* łańcucha P rozumiemy liczbę elementów zbioru P.

- *Rzędem* wierzchołka x nazywamy moc zbioru wszystkich bezpośrednich potomków x. *Rzędem* drzewa D jest kres górny rzędów wszystkich wierzchołków drzewa D.

- Drzewo D jest *skończone*, jeśli zbiór jego wierzchołków jest skończony; w przeciwnym przypadku jest *nieskończone*. Drzewo D jest *rzędu skończonego* (jest *skończenie generowane*), jeśli każdy jego wierzchołek ma rząd skończony.

- Przez indukcję definiujemy *poziomy* drzewa:

  1. poziom *zerowy* to zbiór jednoelementowy, złożony z korzenia drzewa;
  2. poziom $k + 1$ to zbiór wszystkich bezpośrednich następników wierzchołków poziomu k.

- W dalszym ciągu będziemy rozważać głównie drzewa skończone lub rzędu skończonego. Bliżej oswoimy się z drzewami na konwersatorium.

- *Drzewo dwójkowe* to drzewo, w którym każdy wierzchołek ma co najwyżej dwóch bezpośrednich potomków. *Pełne drzewo dwójkowe* to drzewo, w którym każdy wierzchołek ma dokładnie dwóch bezpośrednich potomków.

- Przez *drzewo znakowane* (elementami ze zbioru L) rozumiemy parę uporządkowaną (D, f), gdzie D jest drzewem, a f jest funkcją ze zbioru wierzchołków drzewa D w zbiór L. Zwykle L będzie pewnym zbiorem formuł.

- Graficzne reprezentacje drzew są rysunkami, na których wierzchołki (jakoś znakowane — punktami, liczbami, formułami, itd.) połączone są liniami, odpowiadającymi krawędziom. Przy tym, jeśli $\langle X, R, x_0 \rangle$ jest drzewem, to na rysunku zaznaczamy tylko krawędzie należące do $R - R^2$.

6.2 Lemat Königa

Lemat Königa. Jeśli drzewo $D = \langle X, R, x_0 \rangle$ rzędu skończonego jest nieskończone, to ma gałąź nieskończoną.

Dowód. Przypuśćmy, że D jest nieskończone. Zdefiniujemy gałąź nieskończoną $\{x_0, x_1, x_2, \ldots\}$ w D przez indukcję matematyczną.

Element x_0 (czyli korzeń drzewa D) jest pierwszym elementem konstruowanej gałęzi. Ponieważ D jest nieskończone, więc x_0 ma nieskończenie wiele R-następników.

Przypuśćmy, że $x_0, x_1, x_2, \ldots, x_{n-1}$ zostały zdefiniowane tak, że x_i należy do i-tego poziomu drzewa D oraz x_i ma nieskończenie wiele R-następników. Z założenia, x_{n-1} ma tylko skończenie wiele *bezpośrednich* R-następników. Ponieważ x_{n-1} ma nieskończenie wiele R-następników, więc co najmniej jeden z jego bezpośrednich R-następników także ma nieskończenie wiele R-następników. Wybieramy więc element x_n z n-tego poziomu drzewa D o tej właśnie własności. Wtedy x_n ma nieskończenie wiele R-następników. Ponieważ jest tak dla każdego n, pokazaliśmy istnienie nieskończonej gałęzi $\{x_0, x_1, x_2, \ldots\}$ w drzewie D.

Podczas dalszych wykładów będziemy wielokrotnie korzystali z różnych zasad indukcyjnych.

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