METODY DOWODZENIA TWIERDZEŃ I AUTOMATYZACJA ROZUMOWAŃ

WYKŁAD 3: METODA AKSJOMATYCZNA

III rok kognitywistyki UAM, 2016–2017

Plan na dziś:

1. Przypomnimy, na czym polega aksjomatyczna metoda dowodzenia twierdzeń.
2. Udowodnimy twierdzenie o dedukcji (KRZ).
3. Udowodnimy twierdzenia o trafności oraz pełności metody aksjomatycznej (KRZ).

Dla tęskniących za logiką pierwszego rzędu: chińskie przysłowie mówi, że *cierpliwy dostaje wszystko na czas*.

1 Metoda aksjomatyczna w KRZ

1.1 Uwagi historyczne

Metoda aksjomatyczna w matematyce znana jest od czasów *Elementów* Euklidesa, gdzie była metodą uzyskiwania twierdzeń geometrii. Od XIX wieku metoda aksjomatyczna zaczyna być stosowana we wszystkich działach matematyki.

W logice matematycznej najwcześniej stosowaną metodą dowodową była metoda aksjomatyczna. Stosunkowo wcześnie rozwijana były też takie metody, jak dedukcja naturalna oraz rachunki sekwentów. Do najbardziej popularnych metod dowodowych dołączyły: metoda rezolucji oraz metoda tablic analitycznych.

Zaletą metody aksjomatycznej jest łatwość dowodów twierdzeń metalogicznych. Natomiast z praktycznego (ludzkiego oraz maszynowego) punktu widzenia metoda aksjomatyczna ustępuje innym metodom, takim jak dedukcja naturalna, rezolucja, rachunki sekwentów. Metody dowodowe rozwijane współcześnie mają wiele wspólnego z zagadnieniem automatyzacji rozumowań. Trwają intensywne badania nad możliwościami powierzenia programom komputerowym zadania przeprowadzania dowodów. Zadania te podlegają pewnym ograniczeniom, o czym powiemy więcej nieco później.

Kilka faktów historycznych związanych z metodą aksjomatyczną:

1. Gottlob Frege: *Begriffsschrift* (1879)
2. Alfred N. Whitehead, Bertrand Russell: *Principia Mathematica* (1910–1913)
3. David Hilbert, Wilhelm Ackermann: *Grundzüge der Theoretischen Logik* (1928)
4. David Hilbert, Paul Bernays: *Grundlagen der Mathematik* (1934, 1939)
5. David Hilbert: *Grundlagen der Geometrie* (1899)
6. Polscy logicy (Stanisław Leśniewski, Adolf Lindenbaum, Jan Łukasiewicz, Alfred Tarski)

1.2 Metoda aksjomatyczna: pojęcie dowodu

Przypomnimy, jak wygląda stosowanie metody aksjomatycznej w dowodzeniu twierdzeń logicznych.

1. W ustalonym języku wybieramy:
   (a) zestaw aksjomatów (przyjmowanych bez dowodu)
   (b) zestaw (pierwotnych) reguł wnioskowania.
2. Oba te zbiory muszą być podane w sposób efektywny.

Dowodem w systemie aksjomatycznym $\mathbb{A}$ jest dowolny skończony ciąg formuł $(\psi_1, \psi_2, \ldots, \psi_n)$ taki, że każda formuła ψ_i jest bądź aksjomatem, bądź wnioskiem reguły wnioskowania o przesłankach występujących wcześniej w tym ciągu.

Wyprowadzeniem ze zbioru formuł S w systemie aksjomatycznym $\mathbb{A}$ jest dowolny skończony ciąg formuł $(\psi_1, \psi_2, \ldots, \psi_n)$ taki, że każda formuła ψ_i jest bądź aksjomatem, bądź elementem zbioru S, bądź wnioskiem reguły wnioskowania o przesłankach występujących wcześniej w tym ciągu.

Tezą systemu aksjomatycznego $\mathbb{A}$ jest każda formuła ψ, która jest ostatnim elementem jakiegoś dowodu. Piszemy wtedy: $\vdash_{\mathbb{A}} \psi$.

Formuła ψ jest $\mathbb{A}$-konsekwencją zbioru formuł S, gdy ψ jest ostatnim elementem jakiegoś wyprowadzenia z S. Piszemy wtedy: $S \vdash_{\mathbb{A}} \psi$.

Za aksjomaty przyjmujemy formuły bądź schematy formuł. W pierwszym przypadku wśród reguł wnioskowania uwzględniamy regułę podstawiania RP: $\frac{\varphi}{\varphi[p_i/\psi]}$ (formuły ψ za zmienną p_i w formule φ).

W razie potrzeby, korzysta się z reguły zastępowania definicyjnego.

Aksjomaty charakteryzują znaczenie stałych logicznych.

Wzbogacamy środki inferencyjne systemu poprzez pokazanie, że pewne reguły są w nim wyprowadzalne (wtórne).

1.3 Dla uciechy

Kurs *Logika I* wykorzystywał zapewne aksjomatykę KRZ następującego rodzaju (aksjomatyka w stylu Hilberta-Bernaysa):

Reguły wnioskowania:

1. MP $\frac{\varphi \quad \varphi \to \psi}{\psi}$, reguła odrywania, *modus ponens*
2. RP $\frac{\varphi}{\varphi[p_i/\psi]}$, reguła podstawiania.

Aksjomaty:

1. $p_1 \to (p_2 \to p_1)$
2. $(p_1 \to (p_2 \to p_3)) \to ((p_1 \to p_2) \to (p_1 \to p_3))$
3. $(p_1 \to p_2) \to (\neg p_2 \to \neg p_1)$
4. $\neg\neg p_1 \to p_1$
5. $p_1 \to \neg\neg p_1$
6. $(p_1 \wedge p_2) \to p_1$
7. $(p_1 \wedge p_2) \to p_2$
8. $(p_1 \to p_2) \to ((p_1 \to p_3) \to (p_1 \to (p_2 \wedge p_3)))$
9. $p_1 \to (p_1 \vee p_2)$
10. $p_2 \to (p_1 \vee p_2)$
11. $(p_1 \to p_2) \to ((p_3 \to p_2) \to ((p_1 \vee p_3) \to p_2))$
12. $(p_1 \equiv p_2) \to (p_1 \to p_2)$
13. $(p_1 \equiv p_2) \to (p_2 \to p_1)$
14. $(p_1 \to p_2) \to ((p_2 \to p_1) \to (p_1 \equiv p_2))$

Znanych jest bardzo wiele aksjomatyk dla klasycznego rachunku zdań. Przytoczymy jedynie dwa przykłady.

Aksjomatyka Jana Łukasiewicza (implikacyjno-negacyjna)

1. $(\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))$

2. $(\neg\varphi \to \varphi) \to \varphi$

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

Reguła wnioskowania MP: $\frac{\varphi \quad \varphi\to\psi}{\psi}$
Aksjomatyka Adama Wiegnera (pierwotne: $\wedge$ oraz $\neg$)

1. $p \to (p \wedge p)$

2. $(p \wedge q) \to p$

3. $(p \uparrow q) \to (q \uparrow p)$

4. $(p \to q) \to ((q \uparrow r) \to (p \uparrow r))$

Reguły wnioskowania: MP, RP, zastępowanie definicyjne

2 Aksjomatyka KRZ w Fitting 1990

W zalecanej dla tego kursu monografii Fitting 1990 proponuje się aksjomatykę KRZ, wykorzystującą notację Smullyana.

2.1 Aksjomaty

Schematy aksjomatów:

1. $\varphi \to (\psi \to \varphi)$

2. $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

3. $\bot\!\to \varphi$

4. $\varphi \to \top$

5. $\neg\neg\varphi \to \varphi$

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

7. $\alpha \to \alpha_1$

8. $\alpha \to \alpha_2$

9. $(\beta_1 \to \varphi) \to ((\beta_2 \to \varphi) \to (\beta \to \varphi))$

Reguła wnioskowania: $\frac{\varphi \quad \varphi\to\psi}{\psi}$ (*modus ponens*, reguła odrywania, MP)

2.2 Przykład dowodu

Prawo tożsamości: $p \to p$

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ Ax.2
2. $p \to ((p \to p) \to p)$ Ax.1
3. $(p \to (p \to p)) \to (p \to p)$ MP: 1,2
4. $p \to (p \to p)$ Ax. 1
5. $p \to p$ MP: 3,4

Słuchacze mogą spróbować przedstawić ten dowód w postaci drzewa (zob. pierwszy wykład).

1. W dowodzie korzystano tylko z dwóch pierwszych aksjomatów.
2. Tak samo dowodzimy schematu prawa tożsamości: $\psi \to \psi$.
3. Ten prosty dowód ukazuje dwie trudności metody aksjomatycznej:
   (a) Jak zacząć dowód aksjomatyczny?
   (b) W dowodzie występują formuły bardziej złożone od dowodzonej tezy.

Rozważmy jeszcze jeden przykład: $(\neg\varphi \to \varphi) \to \varphi$ (*consequentia mirabilis*, prawo Claviusa).

1. Za β-formułę w schemacie aksjomatów 9 weźmy formułę: $\neg\varphi \to \varphi$.
2. Wtedy β_1 jest formułą $\neg\neg\varphi$, a β_2 formułą φ. Otrzymujemy więc:
3. $(\neg\neg\varphi \to \varphi) \to ((\varphi \to \varphi) \to ((\neg\varphi \to \varphi) \to \varphi))$.
4. $\neg\neg\varphi \to \varphi$ podpada pod schemat aksjomatów 5.
5. $\varphi \to \varphi$ jest tezą (jak już pokazaliśmy), czyli dołączyć można w tym miejscu kroki dowodu $\varphi \to \varphi$.
6. Dwukrotne zastosowanie reguły odrywania daje $(\neg\varphi \to \varphi) \to \varphi$.

Oczywiście powyższą argumentację można przekształcić do postaci formalnego dowodu.

3 Twierdzenie o dedukcji

Budowanie dowodów aksjomatycznych ułatwia następujący fakt, dotyczący metody aksjomatycznej.

3.1 Twierdzenie

Oznaczenia: niech $\vdash_{ph}$ będzie relacją konsekwencji wyznaczoną przez podany wyżej zestaw aksjomatów i regułę odrywania.
TWIERDZENIE O DEDUKCJI.
$S \cup \{\varphi\} \vdash_{ph} \psi$ wtedy i tylko wtedy, gdy $S \vdash_{ph} (\varphi \to \psi)$.
UWAGI.

1. Implikacja odwrotna wynika z monotoniczności $\vdash_{ph}$ (Fitting pisze: jest trywialna).

2. W dowodzie implikacji prostej wykorzystamy pierwsze dwa aksjomaty systemu (oraz regułę odrywania).

3. Twierdzenie o dedukcji udowodnili (niezależnie od siebie) Herbrand i Tarski.

3.2 Dowód twierdzenia o dedukcji

1. Załóżmy, że $S \cup \{\varphi\} \vdash_{ph} \psi$.

2. Niech $\chi_1, \chi_2, \ldots, \chi_n$ będzie wyprowadzeniem ψ z $S \cup \{\varphi\}$.

3. Wtedy χ_n jest identyczna z ψ.

4. Każdy element ciągu $(\chi_1, \chi_2, \ldots, \chi_n)$ jest bądź aksjomatem, bądź elementem S, bądź wnioskiem reguły odrywania o przesłankach będących wcześniejszymi elementami tego ciągu.

5. Tworzymy ciąg formuł $(*)$: $(\varphi \to \chi_1, \varphi \to \chi_2, \ldots, \varphi \to \chi_n)$.

6. Ostatnim jego elementem jest zatem $\varphi \to \psi$.

7. Ciąg ten nie musi być wyprowadzeniem, ale:

8. Rozszerzymy ten ciąg do ciągu, który będzie wyprowadzeniem $\varphi \to \psi$ z S, co zakończy dowód twierdzenia o dedukcji.

   (a) χ_i jest aksjomatem lub elementem S. Wtedy przed formułą $\varphi \to \chi_i$ wstawiamy do ciągu $(*)$ formuły: χ_i oraz $\chi_i \to (\varphi \to \chi_i)$.

(b) χ_i jest formułą φ. Wtedy przed formułą $\varphi \to \chi_i$ wstawiamy do ciągu $(*)$ formuły tworzące dowód formuły $\varphi \to \varphi$.

(c) χ_i jest wnioskiem reguły odrywania o przesłankach będących wcześniejszymi elementami tego ciągu, czyli istnieją χ_j, χ_k takie, że $j, k < i$ oraz χ_k jest formułą $\chi_j \to \chi_i$ (czyli $\varphi \to \chi_k$ jest formułą $\varphi \to (\chi_j \to \chi_i)$). Wtedy przed formułą $\varphi \to \chi_i$ wstawiamy do ciągu $(*)$ formuły: $(\varphi \to (\chi_j \to \chi_i)) \to ((\varphi \to \chi_j) \to (\varphi \to \chi_i))$ (aksjomat) oraz $(\varphi \to \chi_j) \to (\varphi \to \chi_i)$. Widać, że wtedy $\varphi \to \chi_i$ jest wnioskiem reguły odrywania o przesłankach występujących wcześniej w tak rozszerzonym ciągu.

3.3 Wykorzystanie twierdzenia o dedukcji

Zauważmy, że dowód twierdzenia o dedukcji był konstruktywny: podano przepis, jak wyprowadzenie ψ z $\{\varphi\}$ przekształcić na dowód $\varphi \to \psi$.

Korzystanie z twierdzenia o dedukcji bardzo ułatwia dowodzenie w systemach aksjomatycznych. Wykorzystując twierdzenie o dedukcji, można np. pokazać (konwersatorium), że:

1. $\vdash_{ph} (\varphi \to (\psi \to \chi)) \to (\psi \to (\varphi \to \chi))$ — prawo komutacji
2. $\vdash_{ph} (\varphi \to (\psi \to \chi)) \to ((\varphi \wedge \psi) \to \chi)$ — prawo importacji
3. $\vdash_{ph} (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))$ — sylogizm hipotetyczny

3.4 Oktawa twierdzeń o dedukcji

Studenci poznali wcześniej następujące twierdzenia o dedukcji w KRZ ($\models_{krz}$ to relacja wynikania logicznego w KRZ, $\vdash_{krz}$ to konsekwencja aksjomatyczna w KRZ, której używano):

1. *Semantyczne twierdzenie o dedukcji wprost*: $S \cup \{\varphi\} \models_{krz} \psi$ wtedy i tylko wtedy, gdy $S \models_{krz} (\varphi \to \psi)$.

2. *Syntaktyczne twierdzenie o dedukcji wprost*: $S \cup \{\varphi\} \vdash_{krz} \psi$ wtedy i tylko wtedy, gdy $S \vdash_{krz} (\varphi \to \psi)$.

3. *Semantyczne twierdzenie o dedukcji nie wprost*: $S \cup \{\neg\varphi\} \models_{krz} \bot$ wtedy i tylko wtedy, gdy $S \models_{krz} \varphi$.

4. *Syntaktyczne twierdzenie o dedukcji nie wprost*: $S \vdash_{krz} \neg\varphi$ wtedy i tylko wtedy, gdy $S \cup \{\varphi\} \vdash_{krz} \bot$.

Powyżej udowodniliśmy drugie z nich dla $\vdash_{krz} = \vdash_{ph}$. W przypadku klasycznego rachunku predykatów KRP potrzebne jest dodatkowe założenie (że φ jest zdaniem) w syntaktycznych twierdzeniach o dedukcji.

4 Trafność metody aksjomatycznej

TWIERDZENIE O TRAFNOŚCI. *Jeśli $S \vdash_{ph} \varphi$, to $S \models_{krz} \varphi$.*

1. Każdy aksjomat jest tautologią KRZ. Ćwiczenie: sprawdź.
2. Jeśli φ oraz $\varphi \to \psi$ są tautologiami KRZ, to ψ jest tautologią KRZ. Ćwiczenie: sprawdź. Pamiętasz *semantyczne twierdzenie o odrywaniu* w KRZ?
3. Tak więc, każdy wiersz (w szczególności: ostatni wiersz) dowolnego dowodu jest tautologią w KRZ.
4. A zatem, jeśli φ jest tezą rozważanego sytemu, to jest tautologią KRZ.
5. Fitting pisze (Fitting 1990, 74): *This argument extends easily to derivations as well; we do not give details*, co przetłumaczymy tak: *Przez indukcję po długości wyprowadzenia φ z S łatwo pokazać, że każdy jego krok wynika logicznie z S.*

5 Pełność metody aksjomatycznej

TWIERDZENIE O PEŁNOŚCI. *Jeśli $S \models_{krz} \varphi$, to $S \vdash_{ph} \varphi$.*

W dowodzie wykorzystamy: pewną zdaniową własność niesprzeczności oraz Twierdzenie o Istnieniu Modelu.

Niech φ będzie dowolną formułą. Zbiór S nazwiemy *Hilbertowsko φ-sprzecznym*, gdy $S \vdash_{ph} \varphi$. Zbiory, które nie są Hilbertowsko φ-sprzeczne nazywamy *Hilbertowsko φ-niesprzecznymi*.

LEMAT. *Dla dowolnej formuły φ, rodzina wszystkich zbiorów Hilbertowsko φ-niesprzecznych jest zdaniową własnością niesprzeczności.*

DOWÓD. Niech S będzie zbiorem Hilbertowsko φ-niesprzecznym. Oznacza to, że nie zachodzi $S \vdash_{ph} \varphi$. Trzeba pokazać, że S spełnia wszystkie warunki nakładane na elementy zdaniowej własności niesprzeczności. Proponujemy dowód nie wprost (dla każdego warunku):

1. Gdyby $\bot \in S$, to mielibyśmy $S \vdash_{ph} \bot$. Aksjomatem jest $\bot \to \varphi$, a zatem mielibyśmy $S \vdash_{ph} \varphi$, w sprzeczności z założeniem o Hilbertowskiej φ-niesprzeczności S. Tak więc, $\bot \notin S$.

2. Gdyby $\neg\top \in S$, to mielibyśmy $S \vdash_{ph} \neg\top$. Pod schemat aksjomatu 4 podpada $\neg\top \rightarrow \top$, a zatem $S \vdash_{ph} \top$. Pod schemat aksjomatu 6 podpada $\top \rightarrow (\neg\top \rightarrow \varphi)$, a zatem $S \vdash_{ph} \varphi$, w sprzeczności z założeniem o Hilbertowskiej φ-niesprzeczności S. Tak więc, $\neg\top \notin S$.

3. Przypuśćmy, że $S \cup \{\psi\}$ jest Hilbertowsko φ-sprzeczny, czyli $S \cup \{\psi\} \vdash_{ph} \varphi$. Pokażemy, że wtedy $S \cup \{\neg\neg\psi\}$ jest Hilbertowsko φ-sprzeczny. Aksjomat 5 daje: $\neg\neg\psi \rightarrow \psi$, a twierdzenie o dedukcji i poczynione przypuszczenie dają: $S \vdash_{ph} (\psi \rightarrow \varphi)$. Na mocy prawa sylogizmu hipotetycznego: $S \vdash_{ph} (\neg\neg\psi \rightarrow \varphi)$. Na mocy twierdzenia o dedukcji: $S \cup \{\neg\neg\psi\} \vdash_{ph} \varphi$, czyli $S \cup \{\neg\neg\psi\}$ jest Hilbertowsko φ-sprzeczny.

4. Przypuśćmy, że $S \cup \{\alpha_1, \alpha_2\}$ jest Hilbertowsko φ-sprzeczny, czyli: $S \cup \{\alpha_1, \alpha_2\} \vdash_{ph} \varphi$. Pokażemy, że wtedy $S \cup \{\alpha\}$ jest Hilbertowsko φ-sprzeczny, czyli że: $S \cup \{\alpha\} \vdash_{ph} \varphi$.

5. Skoro $S \cup \{\alpha_1, \alpha_2\} \vdash_{ph} \varphi$, to (twierdzenie o dedukcji!): $S \cup \{\alpha_1\} \vdash_{ph} (\alpha_2 \rightarrow \varphi)$ oraz $S \vdash_{ph} (\alpha_1 \rightarrow (\alpha_2 \rightarrow \varphi))$.

6. Na mocy prawa importacji (zob. ćwiczenie) oraz MP,

   $(\alpha_1 \rightarrow (\alpha_2 \rightarrow \varphi)) \rightarrow ((\alpha_1 \wedge \alpha_2) \rightarrow \varphi)$ mamy $S \vdash_{ph} ((\alpha_1 \wedge \alpha_2) \rightarrow \varphi)$

7. Na mocy aksjomatów $\alpha \rightarrow \alpha_1$ oraz $\alpha \rightarrow \alpha_2$, prawa mnożenia następników $(\alpha \rightarrow \alpha_1) \rightarrow ((\alpha \rightarrow \alpha_2) \rightarrow (\alpha \rightarrow (\alpha_1 \wedge \alpha_2)))$ oraz MP mamy $S \vdash_{ph} (\alpha \rightarrow (\alpha_1 \wedge \alpha_2))$

8. Na mocy prawa sylogizmu hipotetycznego: $S \vdash_{ph} (\alpha \rightarrow \varphi)$.

9. Twierdzenie o dedukcji daje: $S \cup \{\alpha\} \vdash_{ph} \varphi$.

10. Przypuśćmy, że $S \cup \{\beta_1\}$ oraz $S \cup \{\beta_2\}$ są Hilbertowsko φ-sprzeczne. Oznacza to, że: $S \cup \{\beta_1\} \vdash_{ph} \varphi$ oraz $S \cup \{\beta_2\} \vdash_{ph} \varphi$. Pokażemy, że wtedy $S \cup \{\beta\}$ jest Hilbertowsko φ-sprzeczny.

11. Skoro $S \cup \{\beta_1\} \vdash_{ph} \varphi$, to (twierdzenie o dedukcji!) $S \vdash_{ph} (\beta_1 \rightarrow \varphi)$.

12. Skoro $S \cup \{\beta_2\} \vdash_{ph} \varphi$, to (twierdzenie o dedukcji!) $S \vdash_{ph} (\beta_2 \rightarrow \varphi)$.

13. Przypomnijmy schemat aksjomatów 9:

    $(\beta_1 \rightarrow \varphi) \rightarrow ((\beta_2 \rightarrow \varphi) \rightarrow (\beta \rightarrow \varphi))$

14. Dwukrotne zastosowanie reguły odrywania daje: $S \vdash_{ph} (\beta \rightarrow \varphi)$.

15. Na mocy twierdzenia o dedukcji: $S \cup \{\beta\} \vdash_{ph} \varphi$, czyli $S \cup \{\beta\}$ jest Hilbertowsko φ-sprzeczny. To kończy dowód lematu.

Dowód twierdzenia o pełności:

1. Załóżmy, że $S \models_{krz} \varphi$ i przypuśćmy (dla dowodu nie wprost), że nie zachodzi $S \vdash_{ph} \varphi$.

2. Oznacza to, że S jest Hilbertowsko φ-niesprzeczny.

3. Wynika z tego, że także $S \cup \{\neg\varphi\}$ jest Hilbertowsko φ-niesprzeczny. Gdyby bowiem tak nie było, to mielibyśmy $S \cup \{\neg\varphi\} \vdash_{ph} \varphi$, a zatem także (twierdzenie o dedukcji!) $S \vdash_{ph} (\neg\varphi \rightarrow \varphi)$. Ponieważ (jak wcześniej pokazano) tezą jest $(\neg\varphi \rightarrow \varphi) \rightarrow \varphi$, to wynikałoby z tego, że $S \vdash_{ph} \varphi$, co przeczy Hilbertowskiej φ-niesprzeczności S.

4. Na mocy udowodnionego przed chwilą lematu oraz Twierdzenia o Istnieniu Modelu $S \cup \{\neg\varphi\}$ jest spełnialny.

5. W konsekwencji, nie zachodzi $S \models_{krz} \varphi$, co kończy dowód twierdzenia o pełności.

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