

Logika dla informatyków

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. zimowy 2025/26

inf.ug.edu.pl/~amb

Andrzej M. Borzyszkowski (Instytut Informatyki) Logika dla informatyków sem. zimowy 2025/26 1 / 33

Logika Organizacja

Założenia

- wstęp do matematyki
 - zbiory i operacje na nich – suma, przecięcie, różnica, iloczyn kartezjański, ...
 - relacje i operacje na nich
 - funkcje (również częściowe) jako szczególne relacje
- środowisko programisty + wstęp do programowania
 - Linux, w tym umiejętność korzystania z terminala
 - podstawowa umiejętność programowania

Andrzej M. Borzyszkowski (Instytut Informatyki) Logika dla informatyków sem. zimowy 2025/26 3 / 33

Logika Organizacja

Organizacja

- literatura:
 - M. Huth, M. Ryan, *Logic in Computer Science*, Cambridge, 2004
 - D. Jackson, *Software Abstractions – Logic, Language and Analysis*, Revised edition, MIT Press, 2012
 - G. J. Holzmann, *The SPIN Model Checker: Primer and Reference Manual*, Addison-Wesley, 2004
 - i wiele innych rozproszonych materiałów
- materiały są/będą dostępne inf.ug.edu.pl/~amb
- obecność na wykładzie (oczywiście) nieobowiązkowa
- znajomość wykładu (oczywiście) obowiązkowa
- już na ćwiczeniach
- egzamin na zakończenie

Andrzej M. Borzyszkowski (Instytut Informatyki) Logika dla informatyków sem. zimowy 2025/26 2 / 33

Logika Przegląd

Logika

- stwierdzenia deklaratywne – wyrażenia o wartości logicznej: „pada deszcz” ale nie: „czy pada deszcz?”, „deszczu, deszczu przestań padać”, „co za pogoda!”, ...
- stwierdzenia możemy łączyć spójnikami logicznymi
 - negacja: „nieprawda, że pada”,
 - koniunkcja: „pada deszcz i świeci słońce”
 - dyzjunkcja (alternatywa): „pada deszcz lub świeci słońce”
uwaga: występuje też alternatywa rozłączna „albo...albo”;
przyjmujemy nierozłączną
 - implikacja: „jeśli teraz pada, to będą grzyby”
- bardziej skomplikowane są stwierdzenia z kwantyfikatorami
 - dla każdego x
 - istnieje x taki, że

Andrzej M. Borzyszkowski (Instytut Informatyki) Logika dla informatyków sem. zimowy 2025/26 4 / 33

Problemy

- wartości nieznane: „każda liczba parzysta ≥ 2 jest sumą dwóch liczb pierwszych” (hipoteza Goldbacha)
- *jeszcze* niekreślone: „jutro będzie padać”
- dokładniejszy opis rzeczy zmiennych: „zawsze jest tak, że jeśli pada deszcz, to później będzie słońce”
- implikacja materialna: „jeśli na księżycu pada deszcz, to...”
- „albo jest pogoda, albo jest słońce” – czy to prawda?
- „aby udowodnić twierdzenie, udowodnimy lemat” – skąd pomysł na taki lemat?

Historia logiki w 10 liniach

- 1 Arystoteles – zdanie, prawdziwe lub nie
- 2 Leibniz (XVII w.) – spójniki logiczne, obliczenia symboliczne
- 3 Boole (XIX w.) – logika jak algebra, bit = 0 lub 1
- 4 Frege (XX w.) – kwantyfikatory, logika jako podstawa
- 5 Russell – paradoksy: „teraz kłamię”, remedium: teoria typów
- 6 Hilbert – wiara w system aksjomatów opisujących całą matematykę
- 7 Gödel – tak się nie da: odpowiednio bogaty system musi być niezupełny, pojęcie obliczalności
- 8 Tarski – pojęcie modelu
- 9 Church – rachunek lambda jako wzór obliczeń (programowanie funkcyjne – Lisp, Haskell)
- 10 Turing – maszyna Turinga jako model obliczeń, implementacja elektrotechniczna

Czym zajmuje się logika

- język (składnia) – jak budowane są sensowne napisy
- semantyka – co one znaczą
- wnioskowanie – zakładamy prawdziwość pewnych zdań, jak zbudować inne, też prawdziwe
- własności systemów logicznych:
 - niesprzeczność – nie da się wywieść nieprawdy z prawdziwych założeń
 - zupełność – każde zdanie prawdziwe można udowodnić

... do informatyki

- obliczalność $\mapsto$ komputery
- teorie typów $\mapsto$ języki programowania
- rachunek lambda $\mapsto$ języki funkcyjne
- teoria modeli $\mapsto$ języki specyfikacji i prototypowania
- pojęcie spełniania $\mapsto$ weryfikacja modelowa
- reguły wnioskowania $\mapsto$ semantyka operacyjna
- logiki modalne $\mapsto$ opis zachowania programów (co jest możliwe, co konieczne, co prawdopodobne)
- logiki temporalne $\mapsto$ opis zachowania programów w czasie (co może się zdarzyć w przyszłości, co musi się zdarzyć, ...)

Spis treści całości

- rachunek zdań: dedukcja naturalna, język formalny, semantyka, własności rachunku: niesprzeczność i zupełność, postacie normalne, SAT solvers
- rachunek predykatów: język formalny, dedukcja naturalna, semantyka, modelowanie z użyciem rachunku relacyjnego
- program Alloy pozwalający budować prowizoryczne modele systemów
- logiki temporalne: pozwalające wyrażać „zmiennosc”, logiki LTL i CTL – składnia i semantyka
- weryfikacja modelowa (model checking): weryfikator modelowy SPIN, algorytmy weryfikacji modelowej dla LTL i CTL

Język rachunku zdań

- gramatyka (w postaci Backusa-Naura)

$$\varphi ::= p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi)$$

gdzie p oznacza zdanie atomowe

- każda formuła ma jednoznaczne drzewo rozbioru gramatycznego, a poddrzewa wyznaczają podformuły
- można zrezygnować z nawiasów zewnętrznych
- można przyjąć siłę wiązań: $\neg$, potem $\wedge$ i $\vee$, a najslabiej $\rightarrow$
- można przyjąć kierunek wiązań
 - do lewej: $\varphi \wedge \psi \wedge \chi$ zamiast $(\varphi \wedge \psi) \wedge \chi$
 - do prawej: $\varphi \rightarrow \psi \rightarrow \chi$ zamiast $\varphi \rightarrow (\psi \rightarrow \chi)$

Rachunek zdań

Język, c.d.

- *uwaga*: $(\varphi \wedge \psi) \wedge \chi$ nie jest równe $\varphi \wedge (\psi \wedge \chi)$
- ani $\varphi \wedge \psi$ nie jest równe $\psi \wedge \varphi$
- ani φ nie jest równe $\varphi \wedge \varphi$, itd., itp.
- formuły mogą być semantycznie równoważne (dalsze wykłady)
- mogą być równoważne w sensie dowodowym (bliższe wykłady)
- formuła składa się nawiasów, spójników logicznych i formuł atomowych (oznaczanych literami np. p, q, p_1, q'' itp.)
- litery greckie oznaczają formuły
- np. $(p \wedge \neg q'') \wedge \chi$ podaje fragment rozbioru gramatycznego pewnej formuły; nie jest ona jednak w pełni znana

Dedukcja naturalna

Reguły dedukcji naturalnej

- wprowadzanie koniunkcji: $\frac{\varphi \quad \psi}{\varphi \wedge \psi} (\wedge i)$
- ta reguła ma dwie przesłanki (kolejność jest ważna)
- jest to już (krótki dowód) sekwentu $\varphi, \psi \vdash \varphi \wedge \psi$
- eliminacja koniunkcji:

$$\frac{\varphi \wedge \psi}{\varphi} (\wedge e1) \quad \frac{\varphi \wedge \psi}{\psi} (\wedge e2)$$

- dwie reguły, każda o jednej przesłance

Dedukcja naturalna

- dane są przesłanki,
... stosujemy reguły dowodzenia,
... i dochodzimy do wniosków
- jeśli pada i nie mam parasola, to zmoknę, nie zmokłem, padało,
wniosek: miałem parasol
 - aby dojść do tego wniosku, trzeba zastosować jakieś reguły
- $p \wedge \neg q \rightarrow r, \neg r, p \vdash q$
- sekwent: $\varphi_1, \varphi_2, \dots \vdash \psi$
zbiór przesłanek (kolejność nie gra roli, może być pusty) i jeden wniosek
- znaczy: „istnieje dowód wniosku na podstawie przesłanek”
- wcale nie twierdzimy, że przesłanki zachodzą

Drzewo dowodu

- drzewo dowodu ma wniosek jako korzeń,
w każdym węźle uzasadnienie formuły
 - albo odwołanie się do reguły ze wskazaniem przesłanek
 - albo stwierdzenie, że formuła jest przesłanką
 - jeszcze inna możliwość za chwilę
- dowód można zapisywać linearnie, od przesłanek do wniosku, np.
udowodnimy że $p \wedge q, r \vdash q \wedge r$

	formuła	uzasadnienie	c.d. uzasadnienia
1	$p \wedge q$	przesłanka	
2	r	przesłanka	
3	q	$(\wedge e2)$	1
4	$q \wedge r$	$(\wedge i)$	3, 2 (w tej kolejności)

Drzewo i reprezentacja

- dane drzewo można na wiele sposobów zapisać w numerowanej tabelce
- istnieje potencjalnie wiele drzew dowodów o tych samych przesłankach i tym samym wniosku
- w reprezentacji nie musi to być drzewo w sensie dosłownym z dwóch powodów
 - niektóre przesłanki mogą być w ogóle nieużyte
 - a niektóre mogą być użyte więcej niż jeden raz
- np. udowodnimy $\varphi, \psi \vdash \varphi \wedge \varphi$

$\frac{\varphi}{\varphi \wedge \varphi}(\wedge i)$	1	φ	przesłanka	
	2	ψ	przesłanka	
	3	$\varphi \wedge \varphi$	$(\wedge i)$	1, 1

Podwójna negacja i modus tollens

- podwójna negacja: $\frac{\neg\neg\varphi}{\varphi}(\neg\neg e)$ oraz $\frac{\varphi}{\neg\neg\varphi}(\neg\neg i)$
- modus tollens: $\frac{\varphi \rightarrow \psi \quad \neg\psi}{\neg\varphi}(MT)$
- przykłady:
 - $p \rightarrow q \rightarrow r, p, \neg r \vdash \neg q$
 - $\neg p \rightarrow q, \neg q \vdash p$
 - $p \rightarrow \neg q, q \vdash \neg p$

Uwaga: logika intuicjonistyczna odrzuca regułę $\neg\neg e$

Reguła odrywania (modus ponens)

$$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi}(\rightarrow e)$$

- klasyczna reguła rozumowania rozpatrywana w starożytności
- jest to reguła eliminacji spójnika $\rightarrow$
- analogia z pojęciem funkcji i aplikacji funkcji do argumentu: „jeśli procedura zwraca liczbę całkowitą mając na wejściu napis i jeśli na wejściu jest napis, to na wyjściu będzie liczba całkowita”
- można sformalizować logikę używając *tylko* tej reguły (i dużej liczby aksjomatów)
- dedukcja naturalna idzie w przeciwnym kierunku

Wprowadzanie implikacji

$$\frac{\boxed{\begin{array}{c} \varphi \\ \dots \\ \psi \end{array}}}{\varphi \rightarrow \psi}(\rightarrow i)$$

- potrafimy przeprowadzić dowód formuły ψ przyjmując założenie φ (i korzystając z innych przesłanek)
- co wyrażone jest formułą $\varphi \rightarrow \psi$
- analogia do funkcji: jeśli funkcja, mając na wejściu napis, zwraca liczbę całkowitą, to znaczy, że jest typu napis $\rightarrow$ integer

Wprowadzanie implikacji – przykłady

- $p \rightarrow q \vdash \neg q \rightarrow \neg p$

- dowód:

1 $p \rightarrow q$ przesłanka

2 $\neg q$ założenie

3 $\neg p$ MT 1,2

4 $\neg q \rightarrow \neg p \rightarrow i$ 2-3

- $\neg q \rightarrow \neg p \vdash p \rightarrow q$

- dowód:

1 $\neg q \rightarrow \neg p$ przesłanka

2 p założenie

3 $\neg \neg p \neg \neg i$ 2

4 $\neg \neg q$ MT 1,3

5 $q \neg \neg e$ 4

6 $p \rightarrow q \rightarrow i$ 2-5

Reguła kopiowania

- $\vdash p \rightarrow q \rightarrow p$

- dowód:

1 p założenie

2 q założenie

3 $p \checkmark$ 1

4 $q \rightarrow p \rightarrow i$ 2-3

5 $p \rightarrow q \rightarrow p \rightarrow i$ 1-4

- dwa wystąpienia p są różne, raz jako założenie, raz jako wniosek z założeń
reguła wprowadzania implikacji wymaga p na końcu pudełka, stąd konieczność kopiowania

W poszukiwaniu dowodu

- chcemy udowodnić $p \wedge q \rightarrow r \vdash p \rightarrow q \rightarrow r$
- *jedynym* sposobem wyprowadzenia implikacji jest reguła ($\rightarrow i$)
- a więc dowód musi kończyć się zastosowaniem tej reguły
- w tym celu trzeba z założenia p wywieść $q \rightarrow r$
- i znowu ($\rightarrow i$)
- jak otrzymać r z przesłanki i hipotetycznych założeń p i q ?
- tu jest pole do popisu dla inwencji
- idealnie, jeśli system reguł pozwala (niemal) jednoznacznie znaleźć sposób wyprowadzenia
- ćwic.: $p \rightarrow q \rightarrow r \vdash p \wedge q \rightarrow r$

Sprzeczność i negacja

- „nieprawda, że φ ” – założenie φ prowadzi do sprzeczności
- sprzeczność – każda formuła postaci $\varphi \wedge \neg \varphi$ albo $\neg \varphi \wedge \varphi$
oznaczenie – nowa, specjalna formuła $\perp$
- eliminacja negacji poprzez wprowadzenie sprzeczności

$$\frac{\varphi \quad \neg \varphi}{\perp} (\neg e)$$

- wprowadzenie negacji jak w powyższej definicji

$$\frac{\boxed{\begin{array}{c} \varphi \\ \vdots \\ \perp \end{array}}}{\neg \varphi} (\neg i)$$

Eliminacja sprzeczności

- implikacja „formalna” – jeśli założymy rzecz nieprawdziwą, to możemy „uzasadnić” każdy wniosek

$$\frac{\perp}{\varphi}(\perp e)$$

- negacja może być uważana za skrót notacyjny, mianowicie $\neg\varphi$ jest skrótem od $\varphi \rightarrow \perp$
- reguły wprowadzania i eliminacji negacji są szczególnym przypadkiem reguł dla implikacji

$$\frac{\boxed{\begin{array}{c} \varphi \\ \dots \\ \perp \end{array}}}{\varphi \rightarrow \perp}(\rightarrow i) \quad \frac{\varphi \quad \varphi \rightarrow \perp}{\perp}(\rightarrow e)$$

Dyzjunkcja – przykład

- $p \vee q \vdash q \vee p$

- dowód:

1	$p \vee q$	przesłanka
2	p	założenie
3	$q \vee p$	$\vee i 2$
4	q	założenie
5	$q \vee p$	$\vee i 4$
6	$q \vee p$	$\vee e 1,2-3,4-5$

- ćwiczenie: przeprowadzić wywód

- $q \rightarrow r \vdash p \vee q \rightarrow p \vee r$
- $(p \vee q) \vee r \vdash p \vee (q \vee r)$ uwaga, długi i żmudny dowód
- $p \wedge (q \vee r) \vdash (p \wedge q) \vee (p \wedge r)$
- $(p \wedge q) \vee (p \wedge r) \vdash p \wedge (q \vee r)$

Dyzjunkcja

- wprowadzanie $\frac{\varphi}{\varphi \vee \psi}(\vee i1)$ oraz $\frac{\psi}{\varphi \vee \psi}(\vee i2)$

- duch intuicjonizmu: trzeba podjąć decyzję co dowodzimy
- utrudni to automatyczne dowodzenie
- eliminacja – idea rozpatrywania przypadków: nie wiemy czy φ czy ψ jest prawdą, ale w każdym przypadku dochodzimy do tej samej konkluzji

$$\frac{\varphi \vee \psi \quad \boxed{\begin{array}{c} \varphi \\ \dots \\ \chi \end{array}} \quad \boxed{\begin{array}{c} \psi \\ \dots \\ \chi \end{array}}}{\chi}(\vee e)$$

- analogia do konstrukcji programistycznej case: w każdym przypadku mamy działający program

Negacja – przykłady

- udowodnić, że $\neg p \vee q \vdash p \rightarrow q$
 - dla eliminacji dyzjunkcji, trzeba rozpatrzyć dwa przypadki
 - q kopiuje argument i nie korzysta z p
 - $\neg p$ prowadzi do sprzeczności z założeniem p , czyli dowodzi czegokolwiek, np. q
- ćwicz.: wywód $p \rightarrow \neg p \vdash \neg p$
- $p \rightarrow q, p \rightarrow \neg q \vdash \neg p$
- $p \rightarrow q \rightarrow r, p, \neg r \vdash \neg q$ (bez użycia reguły modus tollens)

Reguły pochodne

- niektóre reguły mogą być wyprowadzone za pomocą innych reguł
- przykład wyprowadzenia reguły modus tollens

1	$\varphi \rightarrow \psi$	przesłanka
2	$\neg\psi$	przesłanka
3	φ	założenie
4	ψ	$\rightarrow e$ 1,3
5	$\perp$	$\neg e$ 4,2
6	$\neg\varphi$	$\neg i$ 3-5

- ćwicz.: reguła wprowadzania podwójnej negacji

Twierdzenie

system dedukcji naturalnej może obejść się bez reguł pochodnych

Prawo wyłączonego środka

- $\frac{}{\varphi \vee \neg\varphi}$ (TND) tertium not datur
- zasada używana niejawnie w konstrukcji programistycznej if then else
- wyprowadzenie z użyciem dowodu niewprost:

1	$\neg(\varphi \vee \neg\varphi)$	założenie
2	φ	założenie
3	$\varphi \vee \neg\varphi$	$\vee i$ 2
4	$\perp$	$\neg e$ 3,1
5	$\neg\varphi$	$\neg i$ 2-4
6	$\varphi \vee \neg\varphi$	$\vee i$ 2 5
7	$\perp$	$\neg e$ 6,1
8	$\varphi \vee \neg\varphi$	niewprost 1-7

Dowód niewprost

1	$\neg\varphi \rightarrow \perp$	przesłanka
2	$\neg\varphi$	założenie
3	$\perp$	$\rightarrow e$ 1,2
4	$\neg\neg\varphi$	$\neg i$ 2-3
5	φ	$\neg\neg e$ 4

- jeśli zaczniemy od założenia niewprost $\neg\varphi$, to wprowadzenie negacji da podwójne zaprzeczenie $\neg\neg\varphi$
- żeby otrzymać tezę φ trzeba skorzystać z eliminacji podwójnego zaprzeczenia
- reguła pochodna, jeśli przyjmujemy eliminację podwójnego zaprzeczenia
- jest to kolejna reguła odrzucana przez logikę intuicjonistyczną (jako niekonstruktywna)

Przykład użycia prawa wyłączonego środka (TND)

- $p \rightarrow q \vdash \neg p \vee q$
- dowód: $\neg p \vee p$ zachodzi na mocy TND
 - każdy z członów implikuje $\neg p \vee q$ (drugi pośrednio)
 - więc eliminacja dyzjunkcji daje tezę
- nie jesteśmy jednak w stanie rozstrzygnąć, czy implikacja zachodzi ponieważ prawdziwy jest następnik, czy fałszywy poprzednik
- reguła *eliminacji podwójnej negacji* i reguły pochodne: *prawo wyłączonego środka* i reguła *dowodów niewprost* to reguły **nieobecne** w logice intuicjonistycznej
- reguła modus tollens jest regułą pochodną zgodną z logiką intuicjonistyczną

Dedukcja naturalna		Reguły pochodne
Reguły dedukcji naturalnej		
	wprowadzanie	eliminacja
$\wedge$	$\frac{\varphi \quad \psi}{\varphi \wedge \psi} (\wedge i)$	$\frac{\varphi \wedge \psi}{\varphi} (\wedge e1) \quad \frac{\varphi \wedge \psi}{\psi} (\wedge e2)$
$\vee$	$\frac{\varphi}{\varphi \vee \psi} (\vee i1) \quad \frac{\psi}{\varphi \vee \psi} (\vee i2)$	$\frac{\varphi \vee \psi \quad \boxed{\begin{smallmatrix} \varphi \\ \dots \\ \chi \end{smallmatrix}} \quad \boxed{\begin{smallmatrix} \psi \\ \dots \\ \chi \end{smallmatrix}}}{\chi} (\vee e)$
$\rightarrow$	$\frac{\boxed{\begin{smallmatrix} \varphi \\ \dots \\ \psi \end{smallmatrix}}}{\varphi \rightarrow \psi} (\rightarrow i)$	$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi} (\rightarrow e)$
$\neg$	$\frac{\boxed{\begin{smallmatrix} \varphi \\ \dots \\ \perp \end{smallmatrix}}}{\neg \varphi} (\neg i)$	$\frac{\varphi \quad \neg \varphi}{\perp} (\neg e)$
$\perp$	brak	$\frac{\perp}{\varphi} (\perp e)$
$\neg\neg$	reguła pochodna	$\frac{\neg\neg\varphi}{\varphi} (\neg\neg e)$
Andrzej M. Borzyszkowski (Instytut Informaty		Logika dla informatyków sem. zimowy 2025/26 33 / 33