System hilbertowski

Wykład 2

Plan wykładu

- ► Definicja systemu hilbertowskiego
- ► Reguły pochodne
- ► Twierdzenia dla innych operatorów
- ► Weryfikator dowodów
- ► Przykład
- ► Porównanie z systemem gentzenowskim

Definicja systemu hilbertowskiego

System $\mathcal{H}$ jest systemem dowodzenia złożonym z trzech schematów aksjomatów oraz jednej reguły dowodzenia.

Dla dowolnych formuł A, B, C następujące formuły są aksjomatami:

Aksjomat 1 $\vdash (A \to (B \to A))$

Aksjomat 2 $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

Aksjomat 3 $\vdash (\neg B \to \neg A) \to (A \to B))$

Reguła dowodzenia jest nazywana regułą modus ponens (MP). Dla dowolnych formuł A i B:

$$\frac{\vdash A \qquad \vdash A \to B}{\vdash B}$$

Podstawowe twierdzenie systemu hilbertowskiego

$\vdash (A \to A)$

Dowód:

Aksjomat 2 $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

A A → A A

$\vdash (A \to (A \to A \to C)) \to ((A \to A \to A) \to (A \to C))$

$\vdash (A \to (A \to A \to A)) \to ((A \to A \to A) \to (A \to A))$

Podstawowe twierdzenie systemu hilbertowskiego

$\vdash (A \to A)$

Dowód:

A2 $\vdash (A \to (A \to A \to A)) \to ((A \to A \to A) \to (A \to A))$

Aksjomat 1 $\vdash (A \to (B \to A))$

A A → A

$\vdash (A \to (A \to A \to A))$

Podstawowe twierdzenie systemu hilbertowskiego

$\vdash (A \to A)$

Dowód:

A2 $\vdash (A \to (A \to A \to A)) \to ((A \to A \to A) \to (A \to A))$

A1 $\vdash (A \to (A \to A \to A))$

Modus ponens $((A \to A \to A) \to (A \to A))$

Podstawowe twierdzenie systemu hilbertowskiego

$|- (A \to A)$

Dowód:

A2 $|- (A \to (A \to A \to A)) \to ((A \to A \to A) \to (A \to A))$

A1 $|- (A \to (A \to A \to A))$

MP $|- ((A \to A \to A) \to (A \to A))$

Aksjomat 1 $|- (A \to (A \to A))$

Podstawowe twierdzenie systemu hilbertowskiego

$|- (A \to A)$

Dowód:

A2 $|- (A \to (A \to A \to A)) \to ((A \to A \to A) \to (A \to A))$

A1 $|- (A \to (A \to A \to A))$

MP $|- ((A \to A \to A) \to (A \to A))$

A1 $|- (A \to (A \to A))$

Modus ponens $(A \to A)$

Definicja założenia

Niech U będzie zbiorem formuł, A zaś formułą.

U |– A oznacza, że formuły ze zbioru U są założeniami w dowodzie formuły A.

Jeśli $A_i \in U$, to dowód U |– A może zawierać element postaci U |– A_i.

Reguła dedukcji

- Reguła dedukcji

$$\frac{U \cup \{A\} \ |- B}{U \ |- \ A \to B}$$

Twierdzenie o dedukcji

Reguła dedukcji jest poprawną regułą dowodową.

Dowód

Indukcja ze względu na długość dowodu

$$U \cup \{A\} \ |- B$$

Dowód twierdzenia o dedukcji

n=1

Formułę B udowodniono w jednym kroku, czyli:

- $B \in U \cup \{A\}$

lub

- B jest elementem zbioru aksjomatów $\mathcal{H}$

Dowód twierdzenia o dedukcji

n=1

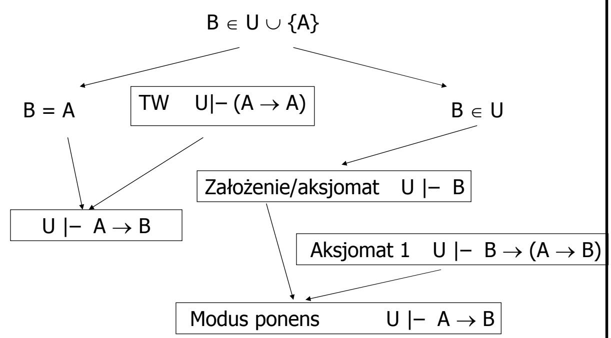
Formułę B udowodniono w jednym kroku, czyli:

► $B \in U \cup \{A\}$

lub

► B jest elementem zbioru aksjomatów $\mathcal{H}$

Dowód twierdzenia o dedukcji



Dowód twierdzenia o dedukcji

n > 1

Ostatni krok dowodu jest:

► jednokrokowym wyprowadzeniem formuły czyli sprowadza się do przypadku n=1

albo

► wyprowadzeniem B z zastosowaniem MP

Dowód twierdzenia o dedukcji

wyprowadzenie B z zastosowaniem MP

zatem istnieje formuła C taka, że dla i, j < n zachodzi:

i-ty element dowodu jest postaci $U \cup \{A\} \mid\!- C$

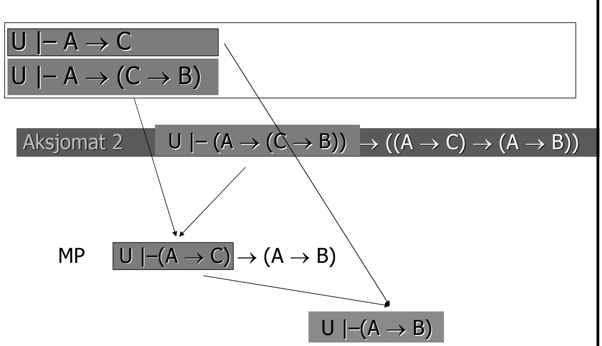
j-ty element dowodu jest postaci $U \cup \{A\} \mid\!- C \to B$

Z założenia indukcyjnego mamy:

$U \mid\!- A \to C$

$U \mid\!- A \to (C \to B)$

Dowód twierdzenia o dedukcji



Reguły pochodne systemu $\mathcal{H}$

► Reguła kontrapozycji

$$\frac{U \mid\!- \neg B \to \neg A}{U \mid\!- A \to B}$$

Reguły pochodne systemu $\mathcal{H}$

- Reguła przechodniości

$$\frac{U \vdash A \to B \qquad U \vdash B \to C}{U \vdash A \to C}$$

Reguły pochodne systemu $\mathcal{H}$

- Reguła wymiany poprzednika

$$\frac{U \vdash A \to (B \to C)}{U \vdash B \to (A \to C)}$$

Reguły pochodne systemu $\mathcal{H}$

- Reguła podwójnego zaprzeczenia

$$\frac{U \vdash \neg\neg A}{U \vdash A}$$

Reguły pochodne systemu $\mathcal{H}$

- Reductio ad absurdum

$$\frac{U \vdash \neg A \to \mathit{fałsz}}{U \vdash A}$$

Twierdzenia dla innych operatorów logicznych

Osłabianie

$\vdash A \to A \vee B$

$\vdash B \to A \vee B$

$\vdash (A \to B) \to (C \vee A) \to (C \vee B)$

Twierdzenia dla innych operatorów logicznych

Przemienność

$\vdash A \vee B \leftrightarrow B \vee A$

Twierdzenia dla innych operatorów logicznych

Łączność

$|- A \vee (B \vee C) \leftrightarrow (A \vee B) \vee C$

Poprawność i pełność systemu $\mathcal{H}$

1. System hilbertowski $\mathcal{H}$ jest systemem poprawnym, czyli jeśli $|- A$ to $|= A$.
2. System hilbertowski $\mathcal{H}$ jest systemem pełnym, czyli jeśli $|= A$ to $|- A$.

Niesprzeczność

Zbiór formuł nazywamy sprzecznym wtw gdy dla pewnej formuły A zachodzi: $U|- A$ oraz $U|- \neg A$. Zbiór U jest niesprzeczny wtw, gdy nie jest sprzeczny.

Słoń morski jest ssakiem.
Foka jest ssakiem.
Rekin jest ssakiem.
....
Kaszalot jest ssakiem.
Kaszalot nie jest ssakiem.
....

?

Kaszalot (*Physeter macrocephalus*)

Domena	eukarioty
Królestwo	zwierzęta
Typ	strunowce
Podtyp	kręgowce
Gromada	ssaki
Podgromada	ssaki żyworodne
Szczep	łożyskowce
Rząd	walenie
Podrząd	zębowce
Rodzina	kaszalotowate
Gatunek	kaszalot

Niesprzeczność

Zbiór formuł nazywamy sprzecznym wtw gdy dla pewnej formuły A zachodzi: $U|- A$ oraz $U|- \neg A$. Zbiór U jest niesprzeczny wtw, gdy nie jest sprzeczny.

Słoń morski jest ssakiem.
Foka jest ssakiem.
Rekin jest ssakiem.
....
Kaszalot jest ssakiem.
Kaszalot nie jest ssakiem.
....

Teoria sprzeczna jest bezużyteczna.

Paragraf 22 (Joseph Heller)

There was only one catch and that was Catch-22, which specified that a concern for one's safety in the face of dangers that were real and immediate was the process of a rational mind. Orr was crazy and could be grounded. All he had to do was ask; and as soon as he did, he would no longer be crazy and would have to fly more missions. Orr would be crazy to fly more missions and sane if he didn't, but if he was sane he had to fly them. If he flew them he was crazy and didn't have to; but if he didn't want to he was sane and had to. Yossarian was moved very deeply by the absolute simplicity of this clause of Catch-22 and let out a respectful whistle.

Niesprzeczność

Zbiór formuł nazywamy sprzecznym wtw gdy dla pewnej formuły A zachodzi: U|– A oraz U|– $\neg$A. Zbiór U jest niesprzeczny wtw, gdy nie jest sprzeczny.

Zbiór formuł jest sprzeczny wtw gdy U|– A dla dowolnej formuły A.

Zbiór formuł jest niesprzeczny wtw gdy U$|\not-$ A dla pewnej formuły A.

Weryfikator dowodów

Aksjomaty reprezentujemy jako fakty

```
aksjomat(A imp (_ A), 1).
aksjomat((A imp (B imp C)) imp ((A imp B) imp (A imp C)), 2).
aksjomat(((neg B) imp (neg A)) imp (A imp B), 3).
```

Dowód reprezentujemy jako listę elementów postaci: `wypr(A, F)`, gdzie `A` jest listą formuł tworzącą bieżący zbiór założeń, a `F` jest udowodnioną formułą.

Pomocnicza procedura `dowód`:

```
dowód(Lista) :- dowód(Lista, 0, [])
```

Numer wiersza używany przy wypisywaniu

Lista dotychczas udowodnionych formuł

Weryfikator dowodów

Sprawdzenie, czy A jest aksjomatem

```
dowód([], _, _).
dowód([Form|Reszta], NrW, Udow):-
      NrW1 is NrW + 1,
      Form = wypr(_, A),
      aksjomat(A,N).
      wypisz_wiersz(NrW1, Form ['Aksjomat', N]),
      dowód(Reszta, NrW1, [Form|Udow]).
```

Sprawdzenie, czy A jest założeniem

```
dowód([], _, _).
dowód([Form|Reszta], NrW, Udow):-
      NrW1 is NrW + 1,
      Form = wypr(Założenia, A),
      member(A, Założenia).
      wypisz_wiersz(NrW1, Form ['Założenie']),
      dowód(Reszta, NrW1, [Form|Udow]).
```

Weryfikator dowodów

Sprawdzenie, czy formuła A powstała w wyniku MP

```
dowód([Form|Reszta], NrW, Udow):-
     NrW1 is NrW + 1,
     Form = wypr(_, A),
     nth1(L1, Udow, wypr(_,B imp A)),
     nth1(L2, Udow, wypr(_,B)),
     MP1 is NrW1 - L1,
     MP2 is NrW1 - L2,
     wypisz_wiersz(NrW1, Form, ['MP ', MP1, ',', MP2]),
     dowód(Reszta, NrW1 [Form | Udow]).
```

Niedeterministyczne wyszukanie, czy formuła B imp A jest na liście

Niedeterministyczne wyszukanie, czy formuła B jest na liście

Weryfikator dowodów

Sprawdzenie, czy formuła A powstała w wyniku dedukcji

```
dowód([Form|Reszta], NrW, Udow):-
     NrW1 is NrW + 1,
     Form = wypr(Założenia, A imp B),
     nth1(L, Udow, wypr(Poprzednie, B)),
     member(A, Poprzednie),
     delete(Poprzednie, A, Założenia),
     D is NrW - L,
     wypisz_wiersz(NrW1, Form, ['Reguła dedukcji', D]),
     dowód(Reszta, NrW1 [Form | Udow]).
```

Niedeterministyczne wybranie ze zbioru Udow elementu zawierającego B

Usunięcie A z listy zawierającej założenia A imp B

elementu

Przykład

udowodnić |– $\neg A \to (A \to B)$

Aksjomat 1 |– $(A \to (B \to A))$

$\neg A$ $\neg B$

$\{\neg A\}$ |– $\neg A \to (\neg B \to \neg A)$

Przykład

udowodnić $\vdash \neg A \to (A \to B)$

$\{\neg A\} \vdash \neg A \to (\neg B \to \neg A)$ aksjomat 1

Założenie $\{\neg A\} \vdash \neg A$

Przykład

udowodnić $\vdash \neg A \to (A \to B)$

$\{\neg A\} \vdash \neg A \to (\neg B \to \neg A)$ aksjomat 1

$\{\neg A\} \vdash \neg A$ założenie

Modus ponens

$\{\neg A\} \vdash (\neg B \to \neg A)$

Przykład

udowodnić $\vdash \neg A \to (A \to B)$

$\{\neg A\} \vdash \neg A \to (\neg B \to \neg A)$	aksjomat 1
$\{\neg A\} \vdash \neg A$	założenie
$\{\neg A\} \vdash (\neg B \to \neg A)$	modus ponens

aksjomat 3 $\{\neg A\} \vdash (\neg B \to \neg A) \to (A \to B))$

Przykład

udowodnić $\vdash \neg A \to (A \to B)$

$\{\neg A\} \vdash \neg A \to (\neg B \to \neg A)$	aksjomat 1
$\{\neg A\} \vdash \neg A$	założenie
$\{\neg A\} \vdash (\neg B \to \neg A)$	modus ponens
$\{\neg A\} \vdash (\neg B \to \neg A) \to (A \to B))$	aksjomat 3

Modus ponens

$\{\neg A\} \vdash A \to B$

Przykład

udowodnić $\vdash \neg A \to (A \to B)$

$\{\neg A\} \vdash \neg A \to (\neg B \to \neg A)$	aksjomat 1
$\{\neg A\} \vdash \neg A$	założenie
$\{\neg A\} \vdash (\neg B \to \neg A)$	modus ponens
$\{\neg A\} \vdash (\neg B \to \neg A) \to (A \to B))$	aksjomat 3
$\{\neg A\} \vdash A \to B$	modus ponens

Reguła dedukcji $\dfrac{U \cup \{A\} \vdash B}{U \vdash A \to B}$

$\vdash \neg A \to (A \to B)$

Porównanie systemów

gentzenowski

- zbiory formuł
- jeden aksjomat
- wiele reguł
- własność podformuł
- powstał aby uprościć badania teoretyczne przez wprowadzenie notacji identycznej jak w tabelach semantycznych
- sekwent: $U \Rightarrow V$

hilbertowski

- pojedyncze formuły
- kilka aksjomatów
- jedna reguła
- brak własności podformuł
- tylko jedno twierdzenie udowadnia się z definicji
- w praktyce – reguły pochodne
- automatyczna weryfikacja dowodów

Zbiór formuł V jest wyprowadzalny ze zbioru U.