Logika intuicjonistyczna

Zeimer

6, 13 marca 2018

Kto i po co wymyśla logiki

- Filozofowie — "A może poszli do lasu?" — potrzebna jest logika modalna, która rozstrzygnie, czy poszli, czy może jest konieczne, że jednak nie.
- Lingwiści — "Polacy mordowali żydów." — potrzebna jest jakaś logika, w której będzie można formalizować znaczenie zdań języka naturalnego.
- Informatycy — "U mnie działa." — potrzebna jest jakaś logika, która pozwoli chwycić programy za mordę i sprawi, że będą działały u wszystkich.
- Matematycy — wymyślają jakieś głupoty z nudów, żeby brać na nie granty

Jak powstaje konkretna logika — teoria

- Problem — ktoś ma jakiś problem i uważa, że można go rozwiązać za pomocą logiki.
- Intuicje — twórca logiki ma pewien zestaw intuicji, pozwalający mu nieformalnie rozumować na temat problemu.
- Składnia — intuicyjne myślenie o problemie wyraża się w pewnym języku nieformalnym. Żeby wyrazić formalne myślenie o problemie, trzeba skonstruować do tego celu język formalny.
- Semantyka — próba uchwycenia ulotnych i niewyraźnych intuicji za pomocą precyzyjnego języka matematyki.
- System(y) dowodzenia — próba zastąpienia dowodów intuicyjnych (niepewne) i opartych na semantyce (trudne w automatyzacji) przez formalne manipulacje na symbolach.

Jak powstaje logika — praktyka

W praktyce nie jest tak kolorowo jak na powyższym slajdzie.

- Logiki często nie powstają, by rozwiązać jakiś problem, ale dlatego, że ich autor nie lubi jakiejś innej logiki i postanowił zrobić swoją (np. Brouwer, prekursor logiki intuicjonistycznej).
- Intuicji często brak, jeżeli logika wiążę się głównie z dziwnymi zabawami matematyków (np. wyrzućmy coś z jakiejś logiki i zobaczmy, jakie twierdzenia da się udowodnić).
- Składnia zazwyczaj zostaje ukradziona z logiki klasycznej lub jest jej lekką modyfikacją.
- Dobrej semantyki często brak. Jest tak w przypadku logiki intuicjonistycznej (choć nie do końca) oraz logiki liniowej (tutaj sytuacja jest beznadziejna).

Cele rozwoju logiki

Rozwijanie konkretnej logiki ma różne cele:

- Formalny: celem rozwoju logiki rozumianej tutaj jako pary (semantyka, system dowodzenia) jest udowodnienie:
  - Twierdzenia o poprawności (ang. soundness), które mówi, że możemy dowieść tylko zdań prawdziwych.
  - Twierdzenia o pełności (ang. completeness), które mówi, że każde zdanie prawdziwe ma dowód.

  Pierwsze z nich jest absolutnie konieczne. Drugie jest miłe, ale czasem nieosiągalne.
- Filozoficzny: wymyślanie nowych semantyk w celu pogłębienia wcześniejszych intuicji.
- Inżynierski: wymyślanie nowych systemów dowodzenia, aby łatwiej było dowodzić.
- Praktyczny: rozwiązywanie problemów, do których stworzono logikę.

Jak powstała logika intuicjonistyczna

- Zaczęło się od tego, że niejaki L. E. J. Brouwer z różnych filozoficznych powodów nie lubił logiki klasycznej. W swoich pracach potępiał on prawo wyłączonego środka. Tak powstała intuicja.
- Jego uczeń Arend Heyting ukradł składnię z logiki klasycznej i wymyślił algebry Heytinga. Tak powstała składnia i pierwsza semantyka.
- Gerhard Gentzen wymyślił dedukcję naturalną i rachunek sekwentów. Tak powstały systemy dowodzenia.
- Kripke wymyślił semantykę Kripkego. Tak powstała kolejna semantyka.
- Curry i Howard zauważyli, że dowody w logice intuicjonistycznej odpowiadają termom rachunku lambda z typami prostymi i że można wykorzystać to do komputerowej formalizacji dowodów. Tak powstał problem, który logika intuicjonistyczna rozwiązywała.

Intuicje — potęgowanie liczb niewymiernych

Theorem

Istnieją takie liczby niewymierne a, b, że a^b jest wymierne.

Dowód.

Rozważmy przypadki:

1. Jeżeli $\sqrt{2}^{\sqrt{2}}$ jest wymierne, niech $a = b = \sqrt{2}$. Wtedy $a^b = \sqrt{2}^{\sqrt{2}}$ jest wymierne na mocy założenia.

2. Jeżeli nie, to niech $a = \sqrt{2}^{\sqrt{2}}$, b $= \sqrt{2}$. Wtedy $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$ jest wymierne. $\square$

Intuicje — potęgowanie liczb niewymiernych

Zagadka: podaj takie liczby niewymierne a, b, że a^b jest wymierne. Rozwiązanie zagadki: mimo że na poprzednim slajdzie udowodniliśmy, że takie liczby istnieją, to nie wiemy, co to za liczby. Wynika to z faktu, że posłużyliśmy się zasadą wyłączonego środka (ang. law of excluded middle, w skrócie LEM), głoszącą, że $P \vee \neg P$. Jest ona niekonstruktywna, tzn. pozwala udowodnić istnienie obiektów bez konstruowania ich wprost.

Intuicje — paradoks pijoka

Theorem

W każdym niepustym barze istnieje taka osoba (nazwijmy ją pijokiem), że jeżeli ona pije, to wszyscy piją.

Dowód.

Rozważmy przypadki:
1. Jeżeli wszyscy piją, to pozamiatane (bar jest niepusty, więc na pijoka weźmy kogokolwiek).
2. Jeżeli ktoś nie pije, to niech on zostanie pijokiem. Załóżmy, że pijok pije. Ponieważ jednak wiemy, że pijok nie pije, to dostajemy sprzeczność i wobec tego wszyscy piją. $\square$

Intuicje — paradoks pijoka

Zagadka: wejdź do swojego ulubionego baru i wskaż pijoka. Rozwiązanie zagadki: mamy tutaj ten sam problem, co poprzednio. Mimo iż udowodniliśmy istnienie pijoka, to nie wiemy, kto konkretnie nim jest. Zasada wyłączonego środka i niekonstruktywizm po raz kolejny weszły nam w paradę.

Intuicje — prawo wyłączonego środka

Problemy z LEM staną się jaśniejsze, gdy naszą logikę będziemy rozważać w bardziej obliczeniowy sposób, mianowicie gdy dowód P będziemy rozumieć jako program, który jest "certyfikatem" prawdziwości P. W takim układzie dowód $P \vee \neg P$ to program rozstrzygający prawdziwość zdania P. W takiej interpretacji LEM pozwala nam rozstrzygnąć wszystkie problemy nierozstrzygalne.

Intuicje — prawo wyłączonego środka

- 1. Problem stopu. Na mocy LEM każda maszyna Turinga kończy pracę albo i nie, ale nie potrafimy sprawdzić, która z tych dwóch opcji zachodzi.
- 2. Równość liczb rzeczywistych. LEM mówi nam, że dwie liczby rzeczywisty albo są równe, albo nie. Tego również nie potrafimy sprawdzić (jeżeli faktycznie są równe i mają nieskończone rozwinięcia dziesiętne, to porównywanie ich cyfra po cyfrze nigdy się nie skończy).

Składnia

$$\phi, \psi ::= \top | \bot | p | \neg\phi | \phi \vee \psi | \phi \wedge \psi | \phi \to \psi | \phi \iff \psi$$

- Składnia logiki intuicjonistycznej jest taka sama jak składnia logiki klasycznej (p oznacza tutaj jedną z przeliczalnie wielu zmiennych zdaniowych).
- Żeby zmniejszyć rozmiar składni, czynimy następujące uproszczenia:
  - Wyrzucamy $\neg\phi$ i definiujemy $\neg\phi = \phi \to \bot$
  - Wyrzucamy $\phi \iff \psi$ i definiujemy $\phi \iff \psi = \phi \to \psi \wedge \psi \to \phi$
- Są jeszcze inne możliwości uproszczenia składni, których jednak nie poczynimy:
  - Moglibyśmy wyrzucić $\top$ i zdefiniować $\top = \bot \to \bot$

Semantyka formalna, nieformalna i intuicje

Oprócz intuicji oraz semantyki formalnej jest też trzeci byt, który możemy nazwać semantyką nieformalną. Intuicja jest nieformalna i przedskładniowa, zaś semantyka formalna jest formalna i poskładniowa. Semantyka nieformalna jest nieformalna i poskładniowa.

W przypadku logiki intuicjonistycznej pochodzi ona od rodziny systemów dowodzenia zwanych zbiorczo dedukcją naturalną. Dzieje się tak w myśl maksymy Wittgensteina "meaning is use", czyli "znaczenie to użycie" - nieformalna semantyka logiki intuicjonistycznej pochodzi od reguł wnioskowania rządzących dedukcją naturalną, z którą zapoznamy się później.

Algebry Heytinga - definicja

$(H, \leqslant, \top, \bot, \wedge, \vee, \to)$ jest algebrą Heytinga, gdy $(H, \leqslant)$ jest częściowym porządkiem z elementem najmniejszym $\bot$ i największym $\top$, zaś $\wedge$, $\vee$ i $\to$ to działania binarne i dla dowolnych $x, y, z \in H$ zachodzi:

- $x \leqslant \top$
- $x \wedge y \leqslant x$
- $x \wedge y \leqslant y$
- $z \leqslant x$ i $z \leqslant y$ implikuje $z \leqslant x \wedge y$
- $\bot \leqslant x$
- $x \leqslant x \vee y$
- $y \leqslant x \vee y$
- $x \leqslant z$ i $y \leqslant z$ implikuje $x \vee y \leqslant z$
- $z \leqslant (x \to y)$ wtedy i tylko wtedy, gdy $z \wedge x \leqslant y$

Algebry Heytinga - waluacje

Niech H będzie algebrą Heytinga.

Waluacja to funkcja $v : \mathrm{Var} \to H$, gdzie Var oznacza zbiór zmiennych zdaniowych naszej logiki.

Waluację możemy rozszerzyć do funkcji $\tilde{v} : \mathrm{Frm} \to H$, gdzie Frm to zbiór zdań naszej logiki, za pomocą następującej definicji:

$$\begin{aligned}
\tilde{v}(\top) &= \top \\
\tilde{v}(\bot) &= \bot \\
\tilde{v}(P \land Q) &= \tilde{v}(P) \land \tilde{v}(Q) \\
\tilde{v}(P \lor Q) &= \tilde{v}(P) \lor \tilde{v}(Q) \\
\tilde{v}(P \to Q) &= \tilde{v}(P) \to \tilde{v}(Q)
\end{aligned}$$

Zauważmy, że symbole $\top, \bot, \land, \lor, \to$ po lewej oznaczają spójniki logiczne, a po prawej - operacje w algebrze Heytinga H.

Algebry Heytinga - spełnianie

Niech $\Gamma = \{\phi_1, \ldots, \phi_n\}$ będzie skończonym zbiorem zdań.
Niech $\bigwedge \Gamma$ oznacza $\phi_1 \wedge \cdots \wedge \phi_n$.
Niech ψ będzie zdaniem naszej logiki.

ψ jest H-konsekwencją zbioru zdań Γ, co zapisujemy $\Gamma \models_H \psi$, gdy dla każdej waluacji $v : \mathrm{Var} \to H$ zachodzi $\tilde{v}(\bigwedge \Gamma) \leqslant \tilde{v}(\psi)$.

Jako specjalny przypadek powyższej definicji możemy powiedzieć, że ψ jest spełnione w H (ang. H-valid), co zapisujemy $\models_H \psi$, gdy dla każdej waluacji $v : \mathrm{Var} \to H$ mamy $\tilde{v}(\psi) = \top$.

Algebry Heytinga - fakty

Theorem

Semantyka algebro-Heytingowa jest poprawna i pełna (ang. sound and complete), tzn. zdanie ϕ jest dowodliwe w systemie dedukcji naturalnej z kontekstami wtedy i tylko wtedy, gdy jest spełnione w każdej algebrze Heytinga H.

Theorem

Zdanie ϕ jest dowodliwe w systemie dedukcji naturalnej z kontekstami wtedy i tylko wtedy, gdy jest spełnione w każdej ***skończonej*** *algebrze Heytinga H.*

Spostrzeżenie filozoficzne

Zauważmy, że powyższe twierdzenia głoszą, że semantyka jest poprawna i pełna względem jakiegoś systemu dowodzenia, nie zaś na odwrót, jak teoretycznie powinno być. Jest to znamienne, gdyż w logice intuicjonistycznej dominuje wspomniana już semantyka nieformalna, pochodząca z systemu dedukcji naturalnej.

Semantyka Kripkego

Ramka Kripkego to para (W, R), gdzie W jest zbiorem, zaś R relacją binarną na W. Elementy W będziemy nazywać światami, zaś R będziemy nazywać relacją dostępności.

Modelem Kripkego będziemy nazywać trójkę $(W, \leqslant, \Vdash)$, gdzie $(W, \leqslant)$ jest ramką Kripkego, w której $\leqslant$ jest preporządkiem, zaś $\Vdash$ jest relacją między światami a zdaniami naszej logiki, która dla dowolnej zmiennej zdaniowej p oraz zdań ϕ i ψ spełnia następujące warunki:

$$w \Vdash \top$$
$$w \leqslant u \text{ i } w \Vdash p \text{ implikuje } u \Vdash p$$
$$w \Vdash \phi \wedge \psi \text{ wtw } w \Vdash \phi \text{ i } w \Vdash \psi$$
$$w \Vdash \phi \vee \psi \text{ wtw } w \Vdash \phi \text{ lub } w \Vdash \psi$$
$$w \Vdash \phi \to \psi \text{ wtw dla każdego } u \geqslant w \text{ jeżeli } u \Vdash \phi \text{ to } u \Vdash \psi$$
$$w \Vdash \bot \text{ nie zachodzi}$$

Semantyka Kripkego - intuicje

Semantyka Kripkego tłumaczy prawdziwość zdań w logice intuicjonistycznej w sposób temporalno-epistemiczny, tj. mówi jak matematycy zdobywają wiedzę w czasie:

- Światy możemy utożsamiać ze stanami wiedzy.
- Zapis $w \Vdash \phi$ możemy odczytywać tak, że ϕ jest prawdziwe w świecie w.
- Zapis $w \leqslant u$ możemy odczytywać tak, że u jest światem większej wiedzy niż w.

Semantyka Kripkego - fakty

Theorem

Semantyka Kripkego jest poprawna i pełna (ang. sound and complete), tzn. zdanie ϕ jest dowodliwe w systemie dedukcji naturalnej z kontekstami wtedy i tylko wtedy, gdy ϕ zachodzi w każdym świecie każdego modelu Kripkego.

Język i metajęzyk

Należy rozróżnić pojęcia języka i metajęzyka. Przez język należy rozumieć logikę, którą się zajmujemy (w naszym przypadku jest to logika intuicjonistyczna), zaś metajęzyk to język, w którym przedstawiamy naszą logikę (w naszym wypadku jest to język polski).

Rozróżnienie to jest ważne, gdyż istnienie zdań mówiących coś o samych sobie może prowadzić do sprzeczności, a tego nie chcemy. Żeby się przed tym bronić, o zdaniach języka będziemy zawsze mówić w metajęzyku.

To rozróżnienie pomoże nam też zrozumieć, jak działają systemy dowodzenia.

Osąd

Osąd (ang. judgement) - zdanie w metajęzyku mówiące coś o zdaniach języka. Przykładem osądu może być stwierdzenie "zdanie $P \wedge Q$ jest prawdziwe" - jest to polskie zdanie mówiące coś o zdaniu $P \wedge Q$, będące zdaniem naszej logiki intuicjonistycznej.

Osąd "zdanie jest prawdziwe" jest chyba najczęściej badanym, ale mogą być też inne: "zdanie jest fałszywe", "zdanie jest poprawnie zbudowane" etc. Bardzo ważnym osądem jest osąd hipotetyczny (ang. hypothetical judgement), który ma postać "ze zdania P wynika zdanie Q".

Zauważmy, że osądy mogą być prawdziwe i fałszywe. Przykładem fałszywego osądu może być osąd "zdanie $\perp$ jest prawdziwe" (chyba, że logika którą formalizujemy jest sprzeczna).

Reguła wnioskowania

Reguła wnioskowania (ang. rule of inference) - w najogólniejszym rozumieniu jest to pewna operacja zdefiniowana w metajęzyku, za pomocą której można przekształcać kolekcje osądów w inne kolekcje osądów.

Niech osąd P true oznacza "zdanie P jest prawdziwe". Przykładem reguły wnioskowania może być reguła wprowadzania koniunkcji, którą możemy zapisać

$$\frac{P \text{ true} \qquad Q \text{ true}}{P \land Q \text{ true}}$$

Reguła, mimo że zapisana za pomocą symboli, jest zdaniem języka polskiego, które głosi, że jeżeli zdanie P jest prawdziwe i zdanie Q jest prawdziwe, to zdanie $P \land Q$ jest prawdziwe.

Reguły wnioskowania - konwencje

Wygodną konwencją dotyczącą zapisu reguł wnioskowania jest to, że jeżeli w danym systemie dowodzenia występuje tylko jeden rodzaj osądów, to zamiast osądu będziemy pisać zdanie, którego on dotyczy, np. zamiast osądu P true będziemy pisać samo P. W tej konwencji regułę z poprzedniego slajdu możemy przedstawić tak:

$$\frac{P \quad Q}{P \wedge Q}$$

Konwencję tę można stosować też, gdy jest więcej niż jeden rodzaj osądów, ale nie istnieje ryzyko pomyłki.

Aksjomat

Aksjomat to osąd, który uznajemy za prawdziwy bez dowodu. Przykładem aksjomatu może być np. osąd $P \vee \neg P$ true, który głosi, że "zdanie $P \vee \neg P$ jest prawdziwe".

Aksjomaty a reguły

Aksjomat z poprzedniego slajdu może nieco przypominać regułę wnioskowania

$$\frac{}{P \vee \neg P \text{ true}}$$

która głosi, że z nicości możemy wywnioskować prawdziwość zdania $P \vee \neg P$. Różnica między aksjomatami i regułami staje się istotna, gdy próbujemy nadać naszej logice interpretację obliczeniową. Te konstrukty, które mają taką interpretację, zostają wtedy regułami wnioskowania, aksjomaty służą zaś do wyrażania osądów niemających interpretacji obliczeniowej.

System dowodzenia

System dowodzenia (ang. proof system) dla logiki (rozumianej tutaj jako czysta składnia, lub też po prostu zbiór zdań Frm) to kolekcja osądów, reguł wnioskowania i aksjomatów. Regułom i aksjomatom nadajemy zazwyczaj jakieś nazwy, żeby można było łatwo się do nich odnosić. System może też wprowadzać jakieś nowe rodzaje bytów (np. konteksty), jeżeli są potrzebne do wydawania osądów.

O ile wszystkie systemy dowodzenia opierają się na osądach, o tyle reguły wnioskowania i aksjomaty mogą występować w różnych proporcjach.

System Hilberta dla logiki intuicjonistycznej

Osąd: P true - "zdanie P jest prawdziwe" (zapisywany wg naszej konwencji po prostu jako P).

Reguła wnioskowania: $\dfrac{\phi \to \psi \qquad \phi}{\psi}$ (modus ponens)

Aksjomaty:

- THEN-1: $\phi \to (\chi \to \phi)$
- THEN-2: $(\phi \to (\chi \to \psi)) \to ((\phi \to \chi) \to (\phi \to \psi))$
- AND-1: $\phi \land \chi \to \phi$
- AND-2: $\phi \land \chi \to \chi$
- AND-3: $\phi \to (\chi \to (\phi \land \chi))$
- OR-1: $\phi \to \phi \lor \chi$
- OR-2: $\chi \to \phi \lor \chi$
- OR-3: $(\phi \to \psi) \to ((\chi \to \psi) \to (\phi \lor \chi \to \psi))$
- FALSE: $\bot \to \phi$
- TRUE: $\top$

Systemy Hilberta

Przedstawiony powyżej system Hilberta jest dość minimalistyczny - ma jeden osąd, jedną regułę wnioskowania i 10 aksjomatów. Jest nieporęczny zarówno dla ludzi (trudno dowodzić w nim ręcznie, gdyż różni się od nieformalnego sposobu dowodzenia w matematyce) jak i dla komputerów (nieprzydatny w automatycznym dowodzeniu).

Zauważmy, że nie jest to jedyny system Hilberta, jaki można skonstruować - jest ich nieskończenie wiele, w zależności od wybranego zestawu aksjomatów.

Rachunek sekwentów (dla logiki klasycznej)

Rachunek sekwentów to system, w którym występuje jeden osąd, zwany sekwentem. Zapisujemy go $\Gamma \vdash \Delta$, a czytamy "z koniunkcji zdań ze zbioru Γ wynika alternatywa zdań ze zbioru Δ".

Reguły wnioskowania występują w dwóch seriach, nazywanych lewą i prawą. "Lewe" reguły mówią, jak operować na zdaniach, które w sekwencie są po lewej stronie, a "prawe" jak operować na zdaniach, które w sekwencie są po prawej.

Charakterystyczne dla tego systemu jest, że reguł wnioskowania jest dużo, nie ma zaś aksjomatów.

Klasyczny rachunek sekwentów - spójniki

- $\dfrac{\Gamma, A \wedge B \vdash \Delta}{\Gamma, A, B \vdash \Delta}(L\wedge)$
- $\dfrac{\Gamma \vdash \Delta, A \wedge B}{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}(R\wedge)$
- $\dfrac{\Gamma, A \vee B \vdash \Delta}{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}(L\vee)$
- $\dfrac{\Gamma \vdash \Delta, A \vee B}{\Gamma \vdash \Delta, A, B}(R\vee)$
- $\dfrac{\Gamma, \neg A \vdash \Delta}{\Gamma \vdash \Delta, A}(L\neg)$
- $\dfrac{\Gamma \vdash \Delta, \neg A}{\Gamma, A \vdash \Delta}(R\neg)$
- $\dfrac{\Gamma, A \rightarrow B \vdash \Delta}{\Gamma \vdash \Delta, A \qquad \Gamma, B \vdash \Delta}(L \rightarrow)$
- $\dfrac{\Gamma \vdash \Delta, A \rightarrow B}{\Gamma, A \vdash \Delta, B}(R \rightarrow)$

Interpretacja reguł dla spójników

Regułę postaci

$$\frac{\mathcal{J}_1 \ldots \mathcal{J}_n}{\mathcal{J}'_1 \ldots \mathcal{J}'_n}$$

można interpretować (czytając z góry na dół): "żeby dowieść osądów $\mathcal{J}_1, \ldots, \mathcal{J}_n$, wystarczy dowieść osądów $\mathcal{J}'_1, \ldots, \mathcal{J}'_n$.

Zauważmy, że reguły dla negacji możemy otrzymać z reguł dla implikacji, zaś reguły dla implikacji z reguł dla negacji i dysjunkcji.

Klasyczny rachunek sekwentów - reguły strukturalne

- $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}$ (WL)
- $\dfrac{\Gamma \vdash A, \Delta}{\Gamma \vdash \Delta}$ (WR)
- $\dfrac{\Gamma, A \vdash \Delta}{\Gamma, A, A \vdash \Delta}$ (CL)
- $\dfrac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, A, \Delta}$ (CR)
- $\dfrac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}$ (PL)
- $\dfrac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_1}$ (PR)

Interpretacja reguł strukturalnych

Reguły WL i WR mówią, że możemy usuwać założenia i cele; CL i CR mówią, że możemy je kopiować; PL i PR mówią, że możemy zamieniać ich kolejność.

Nie są to jednak reguły, które można stosować automatycznie, gdyż moglibyśmy nieopatrznie usunąć sobie potrzebne założenie, albo wpaść w nieskończoną pętlę, na ślepo kopiując i zamieniając kolejność założeń i celów.

Klasyczny rachunek sekwentów - pozostałe reguły

$$\frac{}{A \vdash A}(\mathrm{Ass})$$

Ass to reguła, która pozwala nam skorzystać z założenia.

$$\frac{\Gamma \vdash \Delta, A \qquad A, \Sigma \vdash \Pi}{\Gamma, \Sigma \vdash \Delta, \Pi}\ (\mathrm{Cut})$$

Cut to reguła, która pozwala nam udowodnić na boku potrzebny nam lemat.

Uwaga: w powyższej prezentacji pominięto reguły dla $\top$ oraz $\perp$, gdyż są mało ciekawe.

Klasyczny rachunek sekwentów - podsumowanie

Zauważmy, że stosowanie reguł dla spójników daje w wyniku sekwenty o mniejszej złożoności. Dzięki temu możemy je stosować bez zastanowienia, co sprawia, że rachunek sekwentów świetnie sprawdza się w automatycznym dowodzeniu.

Rachunek sekwentów dla logiki intuicjonistycznej można uzyskać z tego zaprezentowanego powyżej poprzez ograniczenie zbioru formuł po prawej stronie sekwentu do singletonu.

`http://logitext.mit.edu/main` to świetne miejsce, gdzie można poćwiczyć dowodzenie w rachunku sekwentów (zarówno klasycznym, jak i intuicjonistycznym). Uwaga: zabawa jest dość bezmyślna.

Dedukcja naturalna

Dedukcja naturalna to system, który powstał, by oddać sposób, w jaki matematycy rozumują na co dzień.

Jedynym osądem jest osąd hipotetyczny, zapisywany jako $\Gamma \vdash P$, który możemy interpretować "z koniunkcji zdań ze zbioru Γ wynika zdanie P".

Podobnie jak w rachunku sekwentów mamy tu sporo reguł i żadnych aksjomatów.

Systemy dedkucji naturalnej występują w wielu wersjach: Fitch, tradycyjnym (bez kontekstów) oraz z kontekstami. Przyjrzymy się tylko ostatniemu z nich, gdyż jest on najbardziej praktyczny.

Dedukcja naturalna - reguły dla spójników

- $\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}(\wedge\text{-intro})$
- $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}(\wedge\text{-elim L})$
- $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee\text{-intro L})$
- $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}(\wedge\text{-elim R})$
- $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee\text{-intro R})$
- $\dfrac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}(\vee\text{-elim})$
- $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}(\to\text{-intro})$
- $\dfrac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}(\to\text{-elim})$

Interpretacja reguł dla spójników

Reguły wnioskowania dla spójników dzielą się na dwie grupy, mianowicie reguły wprowadzania i reguły eliminacji. Reguły wprowadzania (czytane z góry na dół) mówią, jak udowodnić zdanie zawierające dany spójnik, np. $\vee$-intro L mówi, że jeżeli z kontekstu Γ wynika zdanie A, to z Γ wynika też zdanie $A \vee B$.

Reguły eliminacji (czytane z góry na dół) mówią, co możemy wywnioskować, mając dane zdanie w kontekście jako założenie, np. reguła $\wedge$-elim$R$ mówi, że jeżeli wiemy, że z Γ wynika $A \wedge B$, to z Γ wynika także B.

Harmonia

Rozsądnym jest, żebyśmy eliminując dane zdanie za pomocą reguły eliminacji byli w stanie wywnioskować dokładnie tyle informacji, ile potrzebowaliśmy do jego udowodnienia za pomocą reguły wprowadzania.

Dla przykładu, żeby udowodnić $A \wedge B$ musimy udowodnić osobno A oraz B, więc mając $A \wedge B$ jako założenie możemy wywnioskować, że zachodzi nic więcej ponad A i B.

Zjawisko to nosi nazwę harmonii i jest charakterystyczne dla dedukcji naturalnej w logice intuicjonistycznej. W logice klasycznej nie jest ono obecne, gdyż tautologie takie jak $P \vee \neg P$ dają nam informacje za darmo.

Dedukcja naturalna - reszta reguł

W systemie dedukcji naturalnej mamy też reguły podobne do tych znanych z rachunku sekwentów:

- Reguły strukturalne pozwalające nam usuwać, kopiować i przestawiać założenia obecne w kontekście.
- Regułę pozwalającą nam skorzystać z założenia.
- Regułę Cut pozwalającą udowodnić na boku przydatny lemat.

Dedukcja naturalna - podsumowanie

Dedukcja naturalna jest tym systemem dowodzenia, z którego większość ludzi czerpie swoją nieformalną semantykę dla logiki intuicjonistycznej. Nadaje się ona całkiem nieźle do automatycznego dowodzenia, choć nie aż tak dobrze jak rachunek sekwentów.

Jej główną zaletą jest jednak podobieństwo do codziennego sposobu dowodzenia stosowanego przez matematyków oraz fakt, że jej dowody odpowiadają w bardzo ścisłym sensie termom rachunku λ z typami prostymi (korespondencja Curry'ego-Howarda), co czyni związane z nią intuicje podstawą rozmaitych systemów typów, funkcyjnych języków programowania oraz asystentów dowodzenia.

Więcej o dedukcji naturanej bez kontekstów można przeczytać tutaj: `http://www.cs.cmu.edu/~fp/courses/15317-f17/lectures/02-natded.pdf`

Korespondencja Curry'ego-Howarda

- Typ 1 (singleton).
- Typ $\emptyset$ (pusty).
- Termami produktu $A \times B$ są pary termów (a, b)
- Termami typu $A \to B$ są funkcje, które przekształcają term typu A w term typu B.

- Zdanie $\top$ (prawda).
- Zdanie $\perp$ (fałsz).
- Dowodami koniunkcji $P \wedge Q$ są pary dowodów (p, q).
- Dowód implikacji $P \to Q$ przekształca dowód poprzednika P w dowód następnika Q.

Korespondencja Curry'ego-Howarda

Na rozwinięcie tematu nie wystarczyło czasu. Więcej można przeczytać tutaj: `http://www.cs.cmu.edu/~fp/courses/15317-f17/lectures/03-pap.pdf`

Coq

Coq to funkcyjny język programowania z typami zależnymi oraz asystent dowodzenia (ang. proof assistant), którego działanie opiera się na ideach pochodzących ostatecznie od logiki intuicjonistycznej, dedukcji naturalnej i korespondencji Curry'ego-Howarda.

Jednym z większych sukcesów w jego zastosowaniu była formalizacja dowodu twierdzenia o czterech barwach, znanego z teorii grafów.

Jeżeli chcesz dowiedzieć się więcej na jego temat, zajrzyj na jego stronę domową `https://coq.inria.fr/` lub do mojej książki `https://zeimer.github.io/`

Zadania

- Znajdź algebrę Heytinga, w której nie zachodzi $P \vee \neg P$.
- Znajdź model Kripkego, w którym nie zachodzi $P \vee \neg P$.
- Udowodnij zdanie $\neg(P \wedge \neg P)$ w systemie Hilberta, rachunku sekwentów i dedukcji naturalnej.
- Czy dowód twierdzenia Cantora-Bernsteina jest konstruktywny?
- Sprawdź, które tautologie logiki klasycznej są tautologiami logiki intuicjonistycznej, a które nie.
- (Opcjonalne) Zainstaluj Coqa, przeczytaj `https://zeimer.github.io/R1.html` i wykonaj wszystkie ćwiczenia.