Modal Logic
Part I

Elaine Pimentel
OPLSS Summer School
Oregon, USA

UCL, UK
June 23 – 26, 2026

Motivation I – What is a proof?

Theorem 1. There exist $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Motivation I – What is a proof?

Theorem 1. There exist $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof. Consider $a = \sqrt{2}^{\sqrt{2}}$.
If $a \in \mathbb{Q}$, then take $x = y = \sqrt{2}$.
If $a \notin \mathbb{Q}$, then take $x = a$ and $y = \sqrt{2}$. Then

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

□

Motivation I – What is a proof?

Theorem 1. There exist $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof. Consider $a = \sqrt{2}^{\sqrt{2}}$.
If $a \in \mathbb{Q}$, then take $x = y = \sqrt{2}$.
If $a \notin \mathbb{Q}$, then take $x = a$ and $y = \sqrt{2}$. Then

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

$\square$

Classical mathematician: cool!!! 😎

Theorem 1. There exist $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof. Consider $a = \sqrt{2}^{\sqrt{2}}$.
If $a \in \mathbb{Q}$, then take $x = y = \sqrt{2}$.
If $a \notin \mathbb{Q}$, then take $x = a$ and $y = \sqrt{2}$. Then

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

□

Classical mathematician: cool!!! 😎

Intuitionistic mathematician: but $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$??? 😕

Motivation I – What is a proof?

CHAPTER **10**

THE GELFOND-SCHNEIDER THEOREM

1. Hilbert's seventh problem. In 1900 David Hilbert announced a list of twenty-three outstanding unsolved problems. The seventh problem was settled by the publication of the following result in 1934 by A. O. Gelfond, which was followed by an independent proof by Th. Schneider in 1935.

THEOREM 10.1. *If α and β are algebraic numbers with $\alpha \neq 0$, $\alpha \neq 1$, and if β is not a real rational number, then any value of α^β is transcendental.*

Remarks. The hypothesis that "β is not a real rational number" is usually stated in the form "β is irrational." Our wording is an attempt to avoid the suggestion that β must be a real number. Such a number as $\beta = 2 + 3i$, sometimes called a "complex rational number," satisfies the hypotheses of the theorem. Thus the theorem establishes the transcendence of such numbers as 2^i and $2^{\sqrt{2}}$. In general, $\alpha^\beta = \exp\{\beta \log \alpha\}$ is multiple-valued, and this is the reason for the phrase "any value of" in the statement of Theorem 10.1. One value of $i^{-2i} = \exp\{-2i \log i\}$ is e^π, and so this is transcendental according to the theorem.

Before proceeding to the proof of Theorem 10.1, we state an alternative form of the result.

134

Font: Irrational numbers, Ivan Niven.

Motivation I – What is a proof?

136 THE GELFOND-SCHNEIDER THEOREM Ch. 10

Schneider theorem, and they will be given with proofs in the next section.

LEMMA 10.3. *Consider a determinant with the non-zero element ρ_j^a in the j-th row and $1 + a$-th column, with $j = 1, 2, \cdots, t$ and $a = 0, 1, \cdots, t - 1$. This is called a Vandermonde determinant, and it vanishes if and only if $\rho_j = \rho_k$ for some distinct pair of subscripts j, k.*

This can be found in J. V. Uspensky, *Theory of Equations*, McGraw-Hill, p. 214. The next four lemmas are in Harry Pollard, *The Theory of Algebraic Numbers*, John Wiley, p. 53, p. 60, pp. 63–66, p. 72.

LEMMA 10.4. *Let α and β be algebraic numbers in a field K of degree h over the rationals. If the conjugates of α for K are $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_h$ and for β are $\beta = \beta_1, \beta_2, \cdots, \beta_h$, then the conjugates of $\alpha\beta$ and $\alpha + \beta$ are $\alpha_1\beta_1, \cdots, \alpha_h\beta_h$ and $\alpha_1 + \beta_1, \cdots, \alpha_h + \beta_h$.*

LEMMA 10.5. *If α is an algebraic number, then there is a positive rational integer r such that $r\alpha$ is an algebraic integer.*

LEMMA 10.6. *If K is an algebraic number field of degree h over the rationals, then there exist integers $\beta_1, \beta_2, \cdots, \beta_h$ in K such that every integer in K is expressible uniquely as a linear combination $g_1\beta_1 + \cdots + g_h\beta_h$ with rational integral coefficients. The numbers β_j are called an integral basis for K, and the discriminant of such a basis is a non-zero rational integer.*

LEMMA 10.7. *If α is an algebraic number in a field K of degree h over the rationals, then the norm $N(\alpha)$, defined as the product of α and its conjugates, satisfies the relation $N(\alpha\beta) = N(\alpha)\cdot N(\beta)$. Also $N(\alpha) = 0$ if and only if $\alpha = 0$. If α is an algebraic integer, then $N(\alpha)$ is a rational integer. If α is rational, then $N(\alpha) = \alpha^h$.*

Font: Irrational numbers, Ivan Niven.

Motivation I – What is a proof?

Finally, from complex variable theory we need the concept of entire function, i.e., a function that is analytic in the whole complex plane, and Cauchy's residue theorem. These ideas can be found, for example, in K. Knopp's *Theory of Functions*, vol. I, Dover, p. 112ff. and p. 130.

3. Two lemmas. LEMMA 10.8. *Consider the m equations in n unknowns*

(10.1)

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = 0, \qquad k = 1, 2, \cdots, m,$$

with rational integral coefficients a_{ij}, and with $0 < m < n$. Let the positive integer A be an upper bound of the absolute values of all coefficients; thus $A \geqq |a_{ij}|$ for all i and j. Then there is a non-trivial solution $x_1, x_2, \cdots, x_n$ in rational integers of equations (10.1) *such that*

$$|x_j| < 1 + (nA)^{m/(n-m)}, \qquad j = 1, 2, \cdots, n.$$

Proof. Write y_k for $a_{k1}x_1 + \cdots + a_{kn}x_n$ so that to each point $x = (x_1, x_2, \cdots, x_n)$ there corresponds a point $y = (y_1, y_2, \cdots, y_m)$. A point such as x is said to be a *lattice point* if its coordinates x_j are rational integers. If x is a lattice point, then the corresponding point y is also a lattice point because the a_{ij} are rational integers. Let q be any positive integer. Let x range over the $(2q+1)^n$ lattice points inside or on the n-dimensional cube defined by $|x_j| \leqq q$ for all subscripts j. Then the corresponding values of y_k satisfy

$$|y_k| = \left|\sum_{j=1}^{n} a_{kj}x_j\right| \leqq \sum_{j=1}^{n} |a_{kj}| \cdot |x_j| \leqq \sum_{j=1}^{n} Aq = nAq.$$

Thus, as x ranges over the $(2q+1)^n$ lattice points as indicated, the corresponding lattice points y have coordinates y_k which are integers among the $2nAq + 1$

Font: Irrational numbers, Ivan Niven.

Motivation I – What is a proof?

Sec. 3 TWO LEMMAS 139

LEMMA 10.9. *Consider the p equations in q unknowns*

(10.4)

$$\alpha_{k1}\xi_1 + \alpha_{k2}\xi_2 + \cdots + \alpha_{kq}\xi_q = 0, \qquad k = 1, 2, \cdots, p,$$

with coefficients α_{ij} which are integers in an algebraic number field K of finite degree. Assume that $0 < p < q$. Let $A \geqq 1$ be an upper bound for the absolute values of the coefficients and their conjugates for K, thus $A \geqq \| \alpha_{ij} \|$ for all i and j. Then there exists a positive constant c depending on the field K but independent of α_{ij}, p, and q, such that the equations (10.4) have a non-trivial solution $\xi_1, \xi_2, \cdots, \xi_q$ in integers of the field K satisfying

$$\| \xi_k \| < c + c(cqA)^{p/(q-p)}, \qquad k = 1, 2, \cdots, p.$$

Proof. Let h be the degree of K over the field of rational numbers, and let $\beta_1, \beta_2, \cdots, \beta_h$ be an integral basis for the field. If α is any integer of K, then by Lemma 10 6 we can express α uniquely as a linear combination of the integral basis,

$$\alpha = g_1\beta_1 + g_2\beta_2 + \cdots + g_h\beta_h,$$

with rational integral coefficients g_j. Denote the conjugates of α for K by $\alpha = \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(h)}$, and similarly for the β_j. Taking conjugates in the last equation, by Lemma 10.4 we get

$$\alpha^{(i)} = g_1\beta_1^{(i)} + g_2\beta_2^{(i)} + \cdots + g_h\beta_h^{(i)}, \qquad i = 1, 2, \cdots, h.$$

The determinant $|\beta_j^{(i)}|$ is the discriminant of the basis, and it is not zero by Lemma 10.6. Hence we can solve these equations for the g_j as linear combinations of the $\alpha^{(i)}$, with coefficients dependent only on the basis. Taking absolute values throughout these solutions, we can write

(10.5) $$|g_j| < c_1 \| \alpha \|, \qquad j = 1, 2, \cdots, h,$$

Font: Irrational numbers, Ivan Niven.

Motivation I – What is a proof?

$$
\begin{aligned}
|\zeta| &< |\log \alpha|^{-p} \cdot \frac{p}{q} \cdot c_8^p p^{p(3-m)/2} \cdot \frac{2q}{p} \\
&< \{2c_8 |\log \alpha|^{-1}\}^p p^{p(3-m)/2} \\
&= c_9^p p^{p(3-m)/2}.
\end{aligned}
$$

With this estimate for $|\zeta|$, and that of Lemma 10.12 for its conjugates, we write, by (10.10),

$$|N(\zeta)| < c_9^p p^{p(3-m)2}(c^p p^p)^{h-1} = (c_9 c^{h-1})^p p^{-p} = c_0^p p^{-p},$$

where $c_0 = c_9 c^{h-1}$. This and Lemma 10.11 imply that

$$c_0^p p^{-p} > C^{-p}, \qquad Cc_0 > p,$$

for some positive constants independent of n and p. But this is a contradiction, because $p \geqq n$, and we can choose n arbitrarily large.

Notes on Chapter 10

The special case of Theorem 10.1 for any imaginary quadratic irrational β was established by A. O. Gelfond, *Compt. Rend. Acad. Sci. Paris*, **189** (1929), 1224–1226. The original papers establishing Theorem 10.1 are: A. O. Gelfond, *Doklady Akad. Nauk S.S.S.R.*, **2** (1934), 1–6; Th. Schneider, *J. reine angew. Math.*, **172** (1935), 65–69. The American Mathematical Society has provided an English translation (Translation Number 65) of an advanced expository paper by A. O. Gelfond, *The approximation of algebraic numbers by algebraic numbers and the theory of transcendental numbers, Uspehi Mat. Nauk* (*N.S.*), **4**, no. 4 (32), 19–49 (1949). There is an exposition of Gelfond's proof by E. Hille, *Amer. Math. Monthly*, **49** (1942), 654–661.

The proof of Theorem 10.1 given here is based on a simplification of Gelfond's proof by C. L. Siegel, *Transcendental Numbers*, Princeton, pp. 80–83.

Although the methods of Chapters 9 and 10 establish the transcendence of wide classes of numbers, there are many unsolved prob-

Font: Irrational numbers, Ivan Niven.

Motivation I – What is a proof?

Theorem 1. There exist $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof. Consider $a = \sqrt{2}^{\sqrt{2}}$.
If $a \in \mathbb{Q}$, then take $x = y = \sqrt{2}$.
If $a \notin \mathbb{Q}$, then take $x = a$ and $y = \sqrt{2}$. Then

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

□

Classical mathematician: cool!!! 😎

Intuitionistic mathematician: but $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$??? 😕

Dexter Kozen showed me this constructive example: $\sqrt{2}^{log_2 9}$

😱

Thank you, Dexter!

Motivation II – What are modalities?

modality noun

mo·dal·i·ty   mō-ˈda-lə-tē

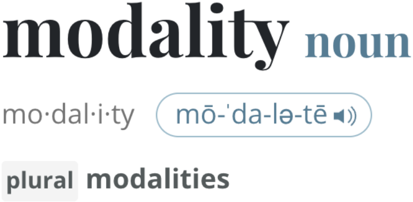
plural modalities

modality noun

mo·dal·i·ty mō-ˈda-lə-tē

plural **modalities**

According to the Merrian-Webster:



According to the Merrian-Webster:

1. the quality or state of being modal.

modality noun

mo·dal·i·ty mō-ˈda-lə-tē

plural **modalities**

According to the Merrian-Webster:

1. the quality or state of being modal.
2. the classification of logical propositions according to their asserting or denying the possibility, impossibility, contingency, or necessity of their content.

Motivation II – What are modalities?

modality noun

mo·dal·i·ty mō-ˈda-lə-tē

plural **modalities**

According to the Merrian-Webster:

1. the quality or state of being modal.
2. the classification of logical propositions according to their asserting or denying the possibility, impossibility, contingency, or necessity of their content.

But we can give a better answer ☺

> *A modal is an expression that is used to qualify the truth of a judgement (SEP).*

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"
  "it is permitted to access this file"

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"
  "it is permitted to access this file"
  "after every request, it is possible to recover"

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"
  "it is permitted to access this file"
  "after every request, it is possible to recover"

- Classical logic tells us what is true at a point.

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"
  "it is permitted to access this file"
  "after every request, it is possible to recover"

- Classical logic tells us what is true at a point.
- Modal logic lets us talk about truth relative to possibility, time, knowledge, obligation, or state transitions for example.

Motivation III – Why modalities?

- Classical logic can express:

  "the server is running"

- But often we want to express things like:

  "the server must eventually respond"
  "the agent knows that the password is valid"
  "it is permitted to access this file"
  "after every request, it is possible to recover"

- Classical logic tells us what is true at a point.
- Modal logic lets us talk about truth relative to possibility, time, knowledge, obligation, or state transitions for example.
- Modal logic is powerful because the same proof-theoretic and semantic machinery can be reused across many notions of qualified truth.

Motivation IV – Modalities and CS

- Verification of programs and protocols

"something bad never happens"

"a request can always eventually be served"

Motivation IV – Modalities and CS

- Verification of programs and protocols

  "something bad never happens"

  "a request can always eventually be served"

- Reasoning about distributed systems / multi-agent systems

  "what agents know, believe, or can infer"

Motivation IV – Modalities and CS

- Verification of programs and protocols

"something bad never happens"

"a request can always eventually be served"

- Reasoning about distributed systems / multi-agent systems

"what agents know, believe, or can infer"

- Security and access control

"permissions, obligations, capabilities"

Motivation IV – Modalities and CS

- Verification of programs and protocols

“something bad never happens”

“a request can always eventually be served”

- Reasoning about distributed systems / multi-agent systems

“what agents know, believe, or can infer”

- Security and access control

“permissions, obligations, capabilities”

- Specification languages

“temporal and dynamic logics for describing system behaviour”

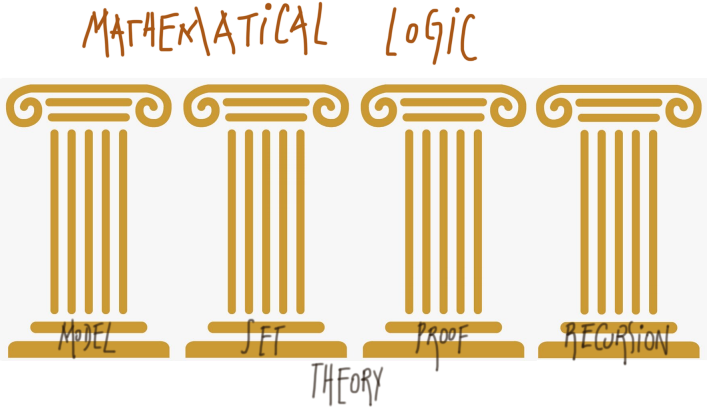
In this tutorial: Modal logics!!

- Proof theory
- Semantics: Kripke, Truth-table, Games
- Applications

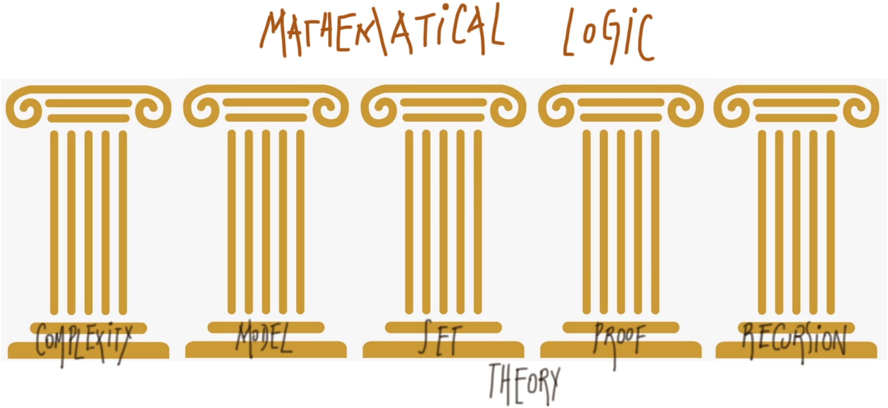
Outline

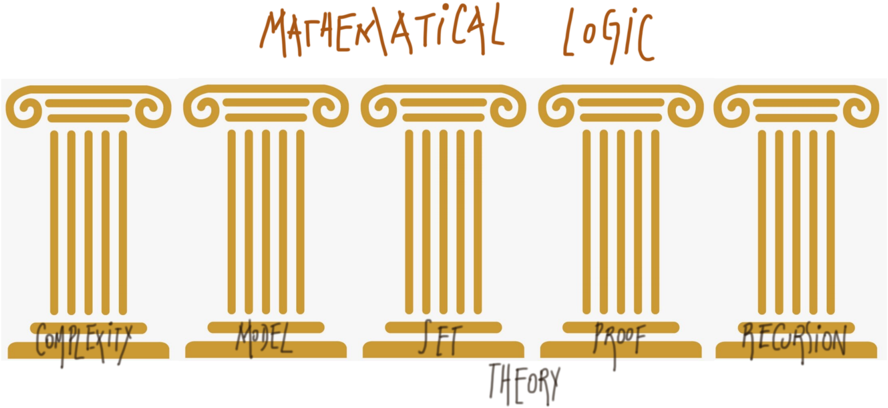
Outline

What is Proof Theory?



What is Proof Theory?





discipline	mathematical objects	(some) tools
set theory	sets	functions
model theory	models & theories	definable & type-definable sets
complexity theory	algorithms	time & memory
recursion theory	computable functions	algorithms
proof theory	proofs	formalisms

What is Proof Theory?

Proof theory according to Sonia Marin

It is all about proofs:

- are they equal? (by the way, what is equal??)
- can we transform one proof into another?
- can we identify patterns?

Proof theory according to Sonia Marin

It is all about proofs:

- are they equal? (by the way, what is equal??)
- can we transform one proof into another?
- can we identify patterns?
- for answering all this: formalisation of proofs in a purely mathematical language;
- discipline: proof theory;

Proof theory according to Sonia Marin

It is all about proofs:

- are they equal? (by the way, what is equal??)
- can we transform one proof into another?
- can we identify patterns?
- for answering all this: formalisation of proofs in a purely mathematical language;
- discipline: proof theory;
- Applications: automatic theorem provers/checkers; extract algorithms from a proof; extract counter-examples from failed proof-search (proof mining); extract proof systems from counter-examples; determine which axioms are required to prove which theorems (reverse mathematics); determine sizes of the proofs (proof complexity).

Outline

Proof Theory

Hilbert systems

Natural deduction

Sequent calculus

Negation

Introduction to modal logic

Semantics

Hilbert calculus

- Syntax:
  - countable set of propositional variables $p_1, p_2, \ldots$;
  - logical connectives $\rightarrow, \wedge, \vee, \perp$;
  - formulas $A, B ::= p \mid A \rightarrow B \mid A \wedge B \mid A \vee B \mid \perp$.

Hilbert calculus

- Syntax:
  - countable set of propositional variables $p_1, p_2, \ldots$;
  - logical connectives $\rightarrow, \wedge, \vee, \bot$;
  - formulas $A, B ::= p \mid A \rightarrow B \mid A \wedge B \mid A \vee B \mid \bot$.
- Axiom schemata (schematic variable $\mathcal{A}, \mathcal{B}, \mathcal{C}$ stand for formulas):

$$\begin{array}{ll} K & \mathcal{A} \rightarrow \mathcal{B} \rightarrow \mathcal{A} \\ S & (\mathcal{A} \rightarrow \mathcal{B} \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow \mathcal{B}) \rightarrow \mathcal{A} \rightarrow \mathcal{C} \end{array}$$

  plus a single rule modus ponens (MP):

$$\frac{\mathcal{A} \rightarrow \mathcal{B} \quad \mathcal{A}}{\mathcal{B}} \; MP$$

Hilbert calculus

- Syntax:
  - countable set of propositional variables $p_1, p_2, \ldots$;
  - logical connectives $\to, \wedge, \vee, \bot$;
  - formulas $A, B ::= p \mid A \to B \mid A \wedge B \mid A \vee B \mid \bot$.
- Axiom schemata (schematic variable $\mathcal{A}, \mathcal{B}, \mathcal{C}$ stand for formulas):

$$\begin{array}{ll} K & \mathcal{A} \to \mathcal{B} \to \mathcal{A} \\ S & (\mathcal{A} \to \mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{B}) \to \mathcal{A} \to \mathcal{C} \end{array}$$

  plus a single rule modus ponens (MP):

$$\frac{\mathcal{A} \to \mathcal{B} \quad \mathcal{A}}{\mathcal{B}}\ MP$$

- Derivation: finite sequence of formulas where each element is an axiom instance or follows from two earlier elements by modus ponens.

Trying to prove $A \to A$ (with help of Revantha and Björn)

$$
\begin{array}{ll}
K & \mathcal{A} \to \mathcal{B} \to \mathcal{A} \\
S & (\mathcal{A} \to \mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{B}) \to \mathcal{A} \to \mathcal{C}
\end{array}
$$

$$
\begin{array}{lll}
1. & (A \to (B \to A) \to A) \to (A \to (B \to A)) \to A \to A & (S) \\
2. & A \to (B \to A) \to A & (K) \\
3. & (A \to (B \to A)) \to A \to A & (MP1, 2) \\
4. & A \to (B \to A) & (K) \\
5. & A \to A & (MP3, 4)
\end{array}
$$

Trying to prove $A \to A$ (with help of Revantha and Björn)

K	$\mathcal{A} \to \mathcal{B} \to \mathcal{A}$
S	$(\mathcal{A} \to \mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{B}) \to \mathcal{A} \to \mathcal{C}$

1.	$(A \to (B \to A) \to A) \to (A \to (B \to A)) \to A \to A$	(S)
2.	$A \to (B \to A) \to A$	(K)
3.	$(A \to (B \to A)) \to A \to A$	$(MP1, 2)$
4.	$A \to B \to A$	(K)
5.	$A \to A$	$(MP3, 4)$

Trying to prove $A \to A$ (with help of Revantha and Björn)

$$
\begin{array}{ll}
K & \mathcal{A} \to \mathcal{B} \to \mathcal{A} \\
S & (\mathcal{A} \to \mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{B}) \to \mathcal{A} \to \mathcal{C}
\end{array}
$$

$$
\begin{array}{lll}
1. & (A \to (B \to A) \to A) \to (A \to (B \to A)) \to A \to A & (S) \\
2. & A \to (B \to A) \to A & (K) \\
3. & (A \to (B \to A)) \to A \to A & (MP1, 2) \\
4. & A \to (B \to A) & (K) \\
5. & A \to A & (MP3, 4)
\end{array}
$$

- how could we construct its derivation (algorithm)?
- complexity?
- structural relationship between $A \to A$ and its derivation?
- why on earth we have to start with that instance of S?
- difficulty of finding the instances of axioms to start with.

Outline

Usual way of making inferences in mathematics.

Usual way of making inferences in mathematics.

BHK (Brouwer-Heyting-Kolmogorov) conditions:

- H1 A proof of $A \wedge B$ is given by presenting a proof of A and a proof of B.
- H2 A proof of $A \vee B$ is given by presenting either a proof of A or a proof of B.
- H3 A proof of $A \to B$ is a construction which permits us to transform any proof of A into a proof of B.
- H4 Absurdity $\perp$ (contradiction) has no proof.

Reasoning about Brouwer-Heyting-Kolmogorov conditions

H1 A proof of $A \wedge B$ is given by presenting a proof of A and a proof of B.

$$\frac{A \quad B}{A \wedge B} \; \wedge I$$

H1 A proof of $A \wedge B$ is given by presenting a proof of A and a proof of B.

$$\frac{A \quad B}{A \wedge B} \wedge I$$

H2 A proof of $A \vee B$ is given by presenting either a proof of A or a proof of B.

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2$$

Reasoning about Brouwer-Heyting-Kolmogorov conditions

H1 A proof of $A \wedge B$ is given by presenting a proof of A and a proof of B.

$$\frac{A \quad B}{A \wedge B}\ \wedge I$$

H2 A proof of $A \vee B$ is given by presenting either a proof of A or a proof of B.

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2$$

H3 A proof of $A \to B$ is a construction which permits us to transform any proof of A into a proof of B.

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$: the 'direct grounds' are a derivation of A and a derivation of B. If C follows when A and B are assumed, through the inversion principle, the elimination rule is:

$$\frac{A \wedge B \qquad \begin{array}{c}[A, B] \\ \vdots \\ C\end{array}}{C} \wedge E$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$: the 'direct grounds' are a derivation of A and a derivation of B. If C follows when A and B are assumed, through the inversion principle, the elimination rule is:

$$\frac{A \wedge B \qquad \begin{array}{c}[A, B] \\ \vdots \\ C\end{array}}{C} \wedge E$$

If, in particular, $C = A$, then

$$\frac{A \wedge B}{A} \wedge E_1$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$: the 'direct grounds' are a derivation of A and a derivation of B. If C follows when A and B are assumed, through the inversion principle, the elimination rule is:

$$\frac{A \wedge B \qquad \begin{matrix}[A, B] \\ \vdots \\ C\end{matrix}}{C} \wedge E$$

The same with $C = B$, thus

$$\frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

Reasoning about Brouwer-Heyting-Kolmogorov conditions

Elimination rules – inversion principle:
"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$

$$\frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

- $A \vee B$: either it has been derived from A and C is derivable from assumption A, or it has been derived from B and C is derivable from assumption B:

$$\frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$

$$\frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

- $A \vee B$

$$\frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

- $A \rightarrow B$: 'direct ground' existence of a hypothetical derivation of B from the assumption A.

  C can be derived from the existence of such a derivation:

  If C follows from B, then it already follows from A.

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$

$$\frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

- $A \vee B$

$$\frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \vee E$$

- $A \rightarrow B$: 'direct ground' existence of a hypothetical derivation of B from the assumption A.

  C can be derived from the existence of such a derivation:

  If C follows from B, then it already follows from A.

$$\frac{A \rightarrow B \quad A \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \rightarrow E$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$

$$\frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

- $A \vee B$

$$\frac{A \vee B \quad \begin{array}{c}[A] \\ \vdots \\ C\end{array} \quad \begin{array}{c}[B] \\ \vdots \\ C\end{array}}{C}\ \vee E$$

- $A \rightarrow B$

$$\frac{A \rightarrow B \quad A \quad \begin{array}{c}[B] \\ \vdots \\ C\end{array}}{C}\ \rightarrow E$$

If, in particular, $C = B$, then

$$\frac{A \rightarrow B \quad A}{B}\ \rightarrow E$$

Elimination rules – inversion principle:

"Whatever follows from the direct grounds for deriving a proposition, must follow from that proposition."

- $A \wedge B$

$$\frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

- $A \vee B$

$$\frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

- $A \to B$

$$\frac{A \to B \quad A}{B} \to E$$

- $\bot$: 'direct grounds' for deriving $\bot$ are empty:

$$\frac{\bot}{C} \bot E$$

Reasoning about Brouwer-Heyting-Kolmogorov conditions

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

- $A \vee B$

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

- $A \to B$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I \qquad \frac{A \to B \quad A}{B} \to E$$

- $\bot$

$$\frac{\bot}{C} \bot E$$

Reasoning about Brouwer-Heyting-Kolmogorov conditions

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

- $A \vee B$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \vee E$$

- $A \rightarrow B$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \rightarrow B}\ \rightarrow I \qquad \frac{A \rightarrow B \quad A}{B}\ \rightarrow E$$

- $\bot$

$$\frac{\bot}{C}\ \bot E$$

Derivation: tree with vertices labelled by formulas.
Example:

$$\frac{[A]}{A \rightarrow A}\ \rightarrow I$$

Reasoning about Brouwer-Heyting-Kolmogorov conditions

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B}\wedge I \qquad \frac{A \wedge B}{A}\wedge E_1 \qquad \frac{A \wedge B}{B}\wedge E_2$$

- $A \vee B$

$$\frac{A}{A \vee B}\vee I_1 \qquad \frac{B}{A \vee B}\vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\vee E$$

- $A \rightarrow B$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B}\rightarrow I \qquad \frac{A \rightarrow B \quad A}{B}\rightarrow E$$

- $\perp$

$$\frac{\perp}{C}\perp E$$

Derivation: tree with vertices labelled by formulas.

A problem: prove analyticity! (called normalisation)

Reasoning about Brouwer-Heyting-Kolmogorov conditions

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

- $A \vee B$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee E$$

- $A \rightarrow B$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B} \rightarrow I \qquad \frac{A \rightarrow B \quad A}{B} \rightarrow E$$

- $\perp$

$$\frac{\perp}{C}\ \perp E$$

Derivation: tree with vertices labelled by formulas.

A problem: prove analyticity! (called normalisation)

Another problems: harmony, pure systems, etc...

Examples

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I \qquad \frac{A \to B \quad A}{B} \to E$$

$$\frac{\bot}{C} \bot E$$

1. Prove $B \wedge C$ from $A \wedge B$ and C

Examples

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots\\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots\\ C\end{array}}{C}\ \vee E$$

$$\frac{\begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A \to B}\ \to I \qquad \frac{A \to B \quad A}{B}\ \to E$$

$$\frac{\bot}{C}\ \bot E$$

1. Prove $B \wedge C$ from $A \wedge B$ and C

$$\frac{\dfrac{A \wedge B}{B}\ (\wedge E_2) \qquad C}{B \wedge C}\ (\wedge I)$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	`\not`, `\neg`
∧	/\	`\and`
∨	\/	`\or`
→	->	`\to`, `\r`, `\imp`
↔	<->	`\iff`, `\lr`
∀	forall	`\all`
∃	exists	`\ex`
λ	fun	`\lam`, `\fun`
≠	~=	`\ne`

$$\dfrac{\dfrac{A \wedge B}{B}\ (\wedge E_2) \qquad C}{B \wedge C}\ (\wedge I)$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	`\not`, `\neg`
∧	/\	`\and`
∨	\/	`\or`
→	->	`\to`, `\r`, `\imp`
↔	<->	`\iff`, `\lr`
∀	forall	`\all`
∃	exists	`\ex`
λ	fun	`\lam`, `\fun`
≠	~=	`\ne`

```
section
variable (A B C : Prop)

theorem example_1 : (A ∧ B)  → C → B ∧ C := by
  rintro h1 : (A ∧ B)
  rintro h2 : C
  apply And.intro
  . exact And.right h1
  . exact h2

```

$$\dfrac{\dfrac{A \wedge B}{B}\;(\wedge E_2) \qquad C}{B \wedge C}\;(\wedge I)$$

Examples

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C}\ \vee E$$

$$\frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}\ \to I \qquad \frac{A \to B \quad A}{B}\ \to E$$

$$\frac{\bot}{C}\ \bot E$$

2. Prove $B \wedge A$ from $A \wedge B$

Examples

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I \qquad \frac{A \to B \quad A}{B} \to E$$

$$\frac{\bot}{C} \bot E$$

2. Prove $B \wedge A$ from $A \wedge B$

$$\frac{\dfrac{A \wedge B}{B} (\wedge E_2) \quad \dfrac{A \wedge B}{A} (\wedge E_1)}{B \wedge A} (\wedge I)$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	`\not`, `\neg`
∧	/\	`\and`
∨	\/	`\or`
→	->	`\to`, `\r`, `\imp`
↔	<->	`\iff`, `\lr`
∀	forall	`\all`
∃	exists	`\ex`
λ	fun	`\lam`, `\fun`
≠	~=	`\ne`

```
theorem example_2 : A ∧ B → B ∧ A := by
  sorry
```

$$\dfrac{\dfrac{A \land B}{B}\,(\land E_2) \qquad \dfrac{A \land B}{A}\,(\land E_1)}{B \land A}\,(\land I)$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	`\not`, `\neg`
∧	/\	`\and`
∨	\/	`\or`
→	->	`\to`, `\r`, `\imp`
↔	<->	`\iff`, `\lr`
∀	forall	`\all`
∃	exists	`\ex`
λ	fun	`\lam`, `\fun`
≠	~=	`\ne`

```
theorem example_2 : A ∧ B → B ∧ A := by
  rintro h : A ∧ B
  apply And.intro
  . exact And.right h
  . exact And.left h
```

$$\dfrac{\dfrac{A \wedge B}{B}\ (\wedge E_2) \qquad \dfrac{A \wedge B}{A}\ (\wedge E_1)}{B \wedge A}\ (\wedge I)$$

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \rightarrow B} \rightarrow I \qquad \frac{A \rightarrow B \quad A}{B} \rightarrow E$$

$$\frac{\bot}{C} \bot E$$

3. Prove $A \vee B$ from $B \vee A$

Examples

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee E$$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \to B}\ \to I \qquad \frac{A \to B \quad A}{B}\ \to E$$

$$\frac{\bot}{C}\ \bot E$$

3. Prove $A \vee B$ from $B \vee A$

$$\frac{B \vee A \quad \dfrac{[B]}{A \vee B}\ \vee I_2 \quad \dfrac{[A]}{A \vee B}\ \vee I_1}{A \vee B}\ \vee E$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	\not, \neg
∧	/\	\and
∨	\/	\or
→	->	\to, \r, \imp
↔	<->	\iff, \lr
∀	forall	\all
∃	exists	\ex
λ	fun	\lam, \fun
≠	~=	\ne

```
theorem example_3 : B ∨ A → A ∨ B := by
  rintro h : B ∨ A
  apply Or.elim h
  . intro b; right; exact b
  . sorry
```

$$\dfrac{B \lor A \qquad \dfrac{[B]}{A \lor B}\,\lor I_2 \qquad \dfrac{[A]}{A \lor B}\,\lor I_1}{A \lor B}\,\lor E$$

Examples

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	\not, \neg
∧	/\	\and
∨	\/	\or
→	->	\to, \r, \imp
↔	<->	\iff, \lr
∀	forall	\all
∃	exists	\ex
λ	fun	\lam, \fun
≠	~=	\ne

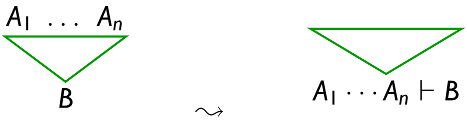
```
theorem example_3 : B ∨ A → A ∨ B := by
  rintro h : B ∨ A
  apply Or.elim h
  . intro b; right; exact b
  . intro a; left; exact a
```

$$\dfrac{B \vee A \qquad \dfrac{[B]}{A \vee B}\,\vee I_2 \qquad \dfrac{[A]}{A \vee B}\,\vee I_1}{A \vee B}\,\vee E$$

Outline

Gentzen: sequent calculus

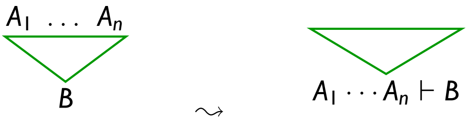
Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

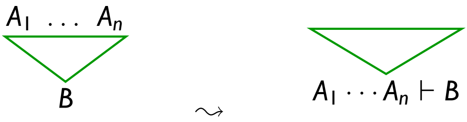
Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.
Rules: right = introduction rules; left = re-reading elimination rules.

Some locality: sequents keep track of open assumptions



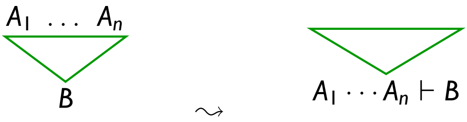
where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B}\ \wedge I \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



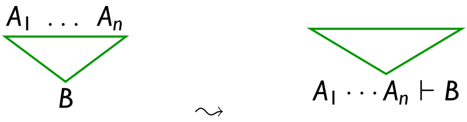
where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{A \quad B}{A \wedge B}\ \wedge I \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R$$

$$\frac{A \wedge B}{A}\ \wedge E_1 \quad \frac{A \wedge B}{B}\ \wedge E_2 \quad \rightsquigarrow \quad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \quad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

Some locality: sequents keep track of open assumptions



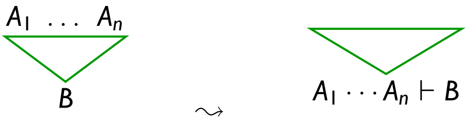
where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

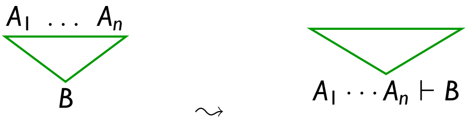
- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

- $A \vee B$

$$\frac{A}{A \vee B} \vee I_1 \quad \frac{B}{A \vee B} \vee I_2 \quad \rightsquigarrow \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2$$

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

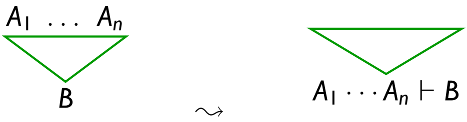
- $A \vee B$

$$\frac{A}{A \vee B} \vee I_1 \quad \frac{B}{A \vee B} \vee I_2 \quad \rightsquigarrow \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2$$

$$\frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C} \vee E \quad \rightsquigarrow \quad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee L$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \dots, A_n$ is the context.

- $A \wedge B$

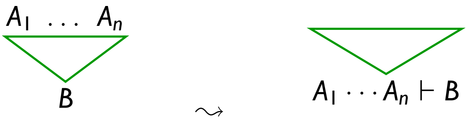
$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

- $A \vee B$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

- $A \vee B$

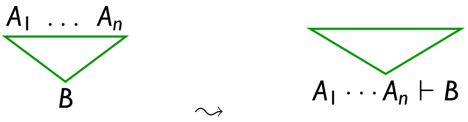
$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

- $A \to B$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I \rightsquigarrow \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \to R \qquad \frac{A \to B \quad A}{B} \to L \rightsquigarrow \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C} \to L$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

- $A \vee B$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

- $A \rightarrow B$

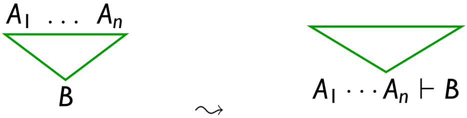
$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}\ \rightarrow R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C}\ \rightarrow L$$

- $\bot$

$$\frac{\bot}{C}\ \bot E \quad \rightsquigarrow \quad \frac{}{\Gamma, \bot \vdash C}\ \bot L$$

Gentzen: sequent calculus

Some locality: sequents keep track of open assumptions



where $\Gamma = A_1, \ldots, A_n$ is the context.

- $A \wedge B$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

- $A \vee B$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

- $A \rightarrow B$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C} \rightarrow L$$

- $\perp$

$$\frac{}{\Gamma, \perp \vdash C}\ \perp L$$

- Initial rule:

$$\frac{}{\Gamma, A \vdash A}$$

Gentzen: sequent calculus

- Initial rule:

$$\overline{\Gamma, A \vdash A}$$

- Derivation: tree with vertices labelled by sequents.

Gentzen: sequent calculus

- Initial rule:

$$\overline{\Gamma, A \vdash A}$$

- Derivation: tree with vertices labelled by sequents.

$$\dfrac{\overline{A \vdash A}\ \text{init}}{\vdash A \to A} \to R$$

Gentzen: sequent calculus

- Initial rule:

$$\overline{\Gamma, A \vdash A}$$

- Derivation: tree with vertices labelled by sequents.

- Analyticity = cut-admissibility.

$$\frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C}\ \text{cut}$$

- Initial rule:

$$\overline{\Gamma, A \vdash A}$$

- Derivation: tree with vertices labelled by sequents.
- Analyticity = cut-admissibility.

$$\frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C}\ \text{cut}$$

- Analyticity $\rightsquigarrow$ sub-formula property: induces a structure on the proofs (in terms of the end formula).

Gentzen: sequent calculus

- Initial rule:

$$\overline{\Gamma, A \vdash A}$$

- Derivation: tree with vertices labelled by sequents.
- Analyticity = cut-admissibility.

$$\frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C}\ \text{cut}$$

- Analyticity $\rightsquigarrow$ sub-formula property: induces a structure on the proofs (in terms of the end formula).
- Thus, proof structure can be exploited to formalise reasoning, investigate meta-logical properties of the logic e.g. consistency, decidability, complexity and interpolation, and develop automated deduction procedures.

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \to R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C} \to L$$

$$\frac{}{\Gamma, \bot \vdash C} \bot L \qquad \frac{}{\Gamma, A \vdash A} \text{init}$$

1. Prove $B \wedge C$ from $A \wedge B$ and C

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \to R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C} \to L$$

$$\frac{}{\Gamma, \bot \vdash C} \bot L \qquad \frac{}{\Gamma, A \vdash A} \text{init}$$

1. Prove $B \wedge C$ from $A \wedge B$ and C

$$\frac{\dfrac{\dfrac{}{B, C \vdash B}\text{init}}{A \wedge B, C \vdash B}(\wedge L_2) \qquad \dfrac{}{A \wedge B, C \vdash C}\text{init}}{A \wedge B, C \vdash B \wedge C}(\wedge R)$$

Interactive sequent prover

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C} \rightarrow L$$

$$\frac{}{\Gamma, \bot \vdash C} \bot L \qquad \frac{}{\Gamma, A \vdash A} \text{init}$$

2. Prove $B \wedge A$ from $A \wedge B$

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \to R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C} \to L$$

$$\frac{}{\Gamma, \bot \vdash C} \bot L \qquad \frac{}{\Gamma, A \vdash A} \text{init}$$

2. Prove $B \wedge A$ from $A \wedge B$

$$\dfrac{\dfrac{\dfrac{}{B \vdash B}\,\text{init}}{A \wedge B \vdash B}\,(\wedge L_2) \quad \dfrac{\dfrac{}{A \vdash A}\,\text{init}}{A \wedge B \vdash A}\,(\wedge L_1)}{A \wedge B \vdash B \wedge A}\,(\wedge R)$$

Interactive sequent prover

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}\ \to L$$

$$\frac{}{\Gamma, \bot \vdash C}\ \bot L \qquad \frac{}{\Gamma, A \vdash A}\ \text{init}$$

3. Prove $A \vee B$ from $B \vee A$

Examples

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to R \qquad \frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}\ \to L$$

$$\frac{}{\Gamma, \bot \vdash C}\ \bot L \qquad \frac{}{\Gamma, A \vdash A}\ \text{init}$$

3. Prove $A \vee B$ from $B \vee A$

$$\dfrac{\dfrac{\dfrac{}{B \vdash B}\ \text{init}}{B \vdash A \vee B}\ \vee R_2 \qquad \dfrac{\dfrac{}{A \vdash A}\ \text{init}}{A \vdash A \vee B}\ \vee R_1}{B \vee A \vdash A \vee B}\ \vee L$$

Interactive sequent prover

Outline

Adding negation

Negation $\neg A$ is defined as $A \to \bot$.

Adding negation

Negation $\neg A$ is defined as $A \to \bot$.
Hence:

$$\dfrac{\begin{array}{c}[A]\\ \vdots \\ \bot\end{array}}{\neg A}\ (\neg I) \qquad \dfrac{\neg A \quad A}{\bot}\ (\neg E)$$

In sequent calculus:

$$\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ (\neg R) \qquad \dfrac{\Gamma \vdash A}{\Gamma, \neg A \vdash C}\ (\neg L)$$

Is there something missing?

Let's try to prove $A \vee \neg A$:

Is there something missing?

Let's try to prove $A \vee \neg A$:

In natural deduction:

$$\dfrac{\begin{matrix} ? \\ A \end{matrix}}{A \vee \neg A} \ \vee I_1$$

Is there something missing?

Let's try to prove $A \lor \neg A$:

In natural deduction:

$$\dfrac{\dfrac{\begin{array}{c}?\\ \bot\end{array}}{\neg A}\ \neg I}{A \lor \neg A}\ \lor I_2$$

Is there something missing?

Let's try to prove $A \vee \neg A$:

In natural deduction:

Is there something missing?

Let's try to prove $A \vee \neg A$:

In natural deduction:

In sequent calculus:

$$\dfrac{\overset{?}{\vdash A}}{\vdash A \vee \neg A}\ \vee R_1$$

Is there something missing?

Let's try to prove $A \vee \neg A$:

In natural deduction:

In sequent calculus:

$$\dfrac{\dfrac{\overset{?}{A \vdash \bot}}{\vdash \neg A}\,\neg R}{\vdash A \vee \neg A}\,\vee R_2$$

Is there something missing?

Let's try to prove $A \vee \neg A$:

In natural deduction:

In sequent calculus:

Double negation!

Is there something missing?

Double negation!

Is there something missing?

The answer is: it depends!

Double negation!

Is there something missing?

The answer is: it depends!

If you are in the intuitionistic (constructive) setting, you are completely fine!

Double negation!

Is there something missing?

The answer is: it depends!

If you are in the intuitionistic (constructive) setting, you are completely fine!

If you are in the classical setting, you are not at all fine!

Double negation!

Is there something missing?

The answer is: it depends!

If you are in the intuitionistic (constructive) setting, you are completely fine!

If you are in the classical setting, you are not at all fine!

In natural deduction: double negation rule

$$\dfrac{\begin{array}{c}[\neg A] \\ \vdots \\ \bot\end{array}}{A}\ DN$$

Double negation!

Is there something missing?

The answer is: it depends!

If you are in the intuitionistic (constructive) setting, you are completely fine!

If you are in the classical setting, you are not at all fine!

In natural deduction: double negation rule

$$\dfrac{\begin{array}{c}[\neg A]\\ \vdots\\ \bot\end{array}}{A}\ DN$$

In sequent calculus: multiple conclusion sequents

$$\dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ C\ R$$

Double negation!

Is there something missing?

The answer is: it depends!

If you are in the intuitionistic (constructive) setting, you are completely fine!

If you are in the classical setting, you are not at all fine!

In natural deduction: double negation rule

$$\dfrac{\begin{array}{c}[\neg A] \\ \vdots \\ \bot\end{array}}{A}\ DN$$

In sequent calculus: multiple conclusion sequents

$$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ C\ R$$

Consequence: the following rule is admissible

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee R$$

Natural deduction rules for (propositional) classical logic

$$\frac{A \quad B}{A \wedge B} \wedge I \qquad \frac{A \wedge B}{A} \wedge E_1 \qquad \frac{A \wedge B}{B} \wedge E_2$$

$$\frac{A}{A \vee B} \vee I_1 \qquad \frac{B}{A \vee B} \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C} \vee E$$

$$\frac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B} \to I \qquad \frac{A \to B \quad A}{B} \to E$$

$$\frac{\bot}{C} \bot E \qquad \frac{\begin{matrix}[\neg A] \\ \vdots \\ \bot\end{matrix}}{A} DN \qquad \frac{\begin{matrix}[A] \\ \vdots \\ \bot\end{matrix}}{\neg A} (\neg I) \qquad \frac{\neg A \quad A}{\bot} (\neg E)$$

Natural deduction rules for (propositional) classical logic

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \vee E$$

$$\frac{\bot}{C}\ \bot E \qquad \frac{\begin{matrix}[\neg A] \\ \vdots \\ \bot\end{matrix}}{A}\ DN \qquad \frac{\begin{matrix}[A] \\ \vdots \\ \bot\end{matrix}}{\neg A}\ (\neg I) \qquad \frac{\neg A \quad A}{\bot}\ (\neg E)$$

4. Prove $A \vee \neg A$.

Natural deduction rules for (propositional) classical logic

$$\frac{A}{A \lor B}\ \lor I_1 \qquad \frac{B}{A \lor B}\ \lor I_2 \qquad \frac{A \lor B \quad \begin{array}{c}[A]\\ \vdots\\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots\\ C\end{array}}{C}\ \lor E$$

$$\frac{\bot}{C}\ \bot E \qquad \frac{\begin{array}{c}[\neg A]\\ \vdots\\ \bot\end{array}}{A}\ DN \qquad \frac{\begin{array}{c}[A]\\ \vdots\\ \bot\end{array}}{\neg A}\ (\neg I) \qquad \frac{\neg A \quad A}{\bot}\ (\neg E)$$

4. Prove $A \lor \neg A$.

$$\dfrac{\dfrac{[\neg(A \lor \neg A)] \qquad \dfrac{\dfrac{\dfrac{[\neg(A \lor \neg A)] \quad \dfrac{[A]}{A \lor \neg A}\ \lor_1 I}{\bot}\ \neg E}{\neg A}\ \neg I}{A \lor \neg A}\ \lor_2 I}{\bot}\ \neg E}{A \lor \neg A}\ DN$$

Natural deduction rules for (propositional) classical logic

Lean

Unicode	Ascii	Lean input
	true	
	false	
¬	not	\not, \neg
∧	/\	\and
∨	\/	\or
→	->	\to, \r, \imp
↔	<->	\iff, \lr
∀	forall	\all
∃	exists	\ex
λ	fun	\lam, \fun
≠	~=	\ne

```
open Classical

theorem example_4 : A ∨ ¬ A := by
  apply byContradiction
  intro (h1 : ¬ (A ∨ ¬ A))
  have h2 : ¬ A := by
    intro (h3 : A)
    have h4 : A ∨ ¬ A := Or.inl h3
    show False
    exact h1 h4
  have h5 : A ∨ ¬ A := Or.inr h2
  show False
  exact h1 h5

end
```

$$\dfrac{\dfrac{[\neg(A \lor \neg A)] \qquad \dfrac{\dfrac{\dfrac{[\neg(A \lor \neg A)] \quad \dfrac{[A]}{A \lor \neg A}\,\lor_1 I}{\bot}\,\neg E}{\neg A}\,\neg I}{A \lor \neg A}\,\lor_2 I}{\bot}\,\neg E}{A \lor \neg A}\,DN$$

Natural deduction rules for (first-order) classical logic

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E_1 \qquad \frac{A \wedge B}{B}\ \wedge E_2$$

$$\frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2 \qquad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C}\ \vee E$$

$$\frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \rightarrow B} \rightarrow I \qquad \frac{A \rightarrow B \quad A}{B} \rightarrow E$$

$$\frac{\bot}{C}\ \bot E \qquad \frac{\begin{array}{c}[\neg A]\\ \vdots \\ \bot\end{array}}{A}\ DN \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ \bot\end{array}}{\neg A}\ (\neg I) \qquad \frac{\neg A \quad A}{\bot}\ (\neg E)$$

$$\frac{A(y)}{\forall x.A(x)}\ \forall I \qquad \frac{\forall x.A(x)}{A(t)}\ \forall E \qquad \frac{A(t)}{\exists x.A(x)}\ \exists I \qquad \frac{\exists x.A(x) \quad \begin{array}{c}[A(y)]\\ \vdots \\ C\end{array}}{C}\ \exists E$$

Sequent calculus rules for (propositional) classical logic

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge L$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee L$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta} \rightarrow L$$

$$\frac{}{\Gamma, \bot \vdash \Delta} \bot L \qquad \frac{}{\Gamma, A \vdash A, \Delta} \text{init} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} (\neg R) \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} (\neg L)$$

Sequent calculus rules for (propositional) classical logic

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge L$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee L$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta} \to R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \to L$$

$$\frac{}{\Gamma, \bot \vdash \Delta} \bot L \qquad \frac{}{\Gamma, A \vdash A, \Delta} \text{init} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} (\neg R) \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} (\neg L)$$

4. Prove $\vdash A \vee \neg A$.

Sequent calculus rules for (propositional) classical logic

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge L$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee L$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\ \to R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \to L$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot L \qquad \frac{}{\Gamma, A \vdash A, \Delta}\ \text{init} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ (\neg R) \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ (\neg L)$$

4. Prove $\vdash A \vee \neg A$.

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\ \text{init}}{\vdash A, \neg A}\ \neg R}{\vdash A \vee \neg A}\ \vee R$$

Interactive sequent prover

Sequent calculus rules for (first order) classical logic

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge L$$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee L$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta} \to R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \to L$$

$$\frac{}{\Gamma, \bot \vdash \Delta} \bot L \qquad \frac{}{\Gamma, A \vdash A, \Delta} \text{init} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} (\neg R) \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} (\neg L)$$

$$\frac{\Gamma \vdash A(y), \Delta}{\Gamma \vdash \forall x.A(x), \Delta} \forall R \quad \frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x.A(x) \vdash \Delta} \forall L \quad \frac{\Gamma \vdash \exists x.A(x), A(t), \Delta}{\Gamma \vdash \exists x.A(x), \Delta} \exists R \quad \frac{\Gamma, A(y) \vdash \Delta}{\Gamma, \exists x.A(x) \vdash \Delta}$$

Outline

What is Modal Logic?

Carlos ______________________________ handsome.

Classical logic: truth

Carlos ____*is*____ handsome.

Classical logic: truth

Carlos ______ *is not* ______ handsome.

Modal logic: qualifies truth

Carlos ___is necessarily___ handsome.

What is Modal Logic?

Modal logic: qualifies truth

Carlos ____is necessarily____ handsome.
possibly

Modal logic: qualifies truth

Carlos ~~is necessarily~~ ________ handsome.

possibly

alethic interpretation

Modal logic: qualifies truth

Carlos __is known to be__ handsome.

Modal logic: qualifies truth

Carlos is known to be handsome. (by me)

epistemic interpretation

Modal logic: qualifies truth

Carlos __is believed to be__ handsome. (by me)

↑

doxastic interpretation

What is Modal Logic?

Modal logic: qualifies truth

Carlos <u>is obliged to be</u> handsome.

What is Modal Logic?

Modal logic: qualifies truth

Carlos __is obliged to be__ handsome.

permission

prohibition

deontic interpretation

What is Modal Logic?

Modal logic: qualifies truth

Carlos ______*is now*______ handsome.

Modal logic: qualifies truth

Carlos ___is now___ handsome.

will be

temporal interpretation

Alethic interpretation

Carlos _is necessarily_ handsome.

Alethic interpretation

necessarily Carlos is ________________ handsome.

Alethic interpretation

p = Carlos is handsome

necessarily p

Alethic interpretation

p = Carlos is handsome

$$\Box p$$

Alethic interpretation

Carlos __is possibly__ handsome.

Alethic interpretation

possibly Carlos is ________________ handsome.

Modalities and propositions

Alethic interpretation

p = Carlos is handsome

possibly p

Alethic interpretation

p = Carlos is handsome

$$\Diamond p$$

Question 1

How to reason about sentences in modal logic?

Outline

Proof Theory

Hilbert systems

Natural deduction

Sequent calculus

Negation

Introduction to modal logic

Semantics

Truth table

A	B	$A \to B$
1	1	1
1	0	0
0	1	1
0	0	1

Truth table

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Truth tables

w

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Relational models

Generalizing

v

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

w

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Relational models

Adding relations

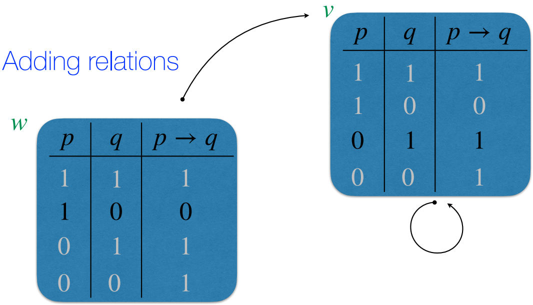
w

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

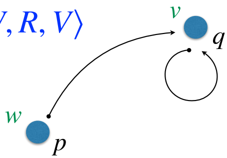
v

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

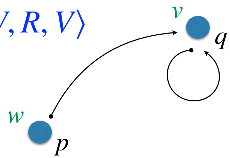
Adding relations



$\mathscr{M} = \langle W, R, V \rangle$



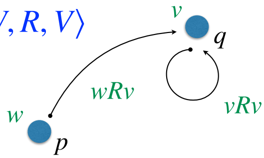
$\mathscr{M} = \langle W, R, V \rangle$



W is a non-empty set of possible worlds.

Relational models

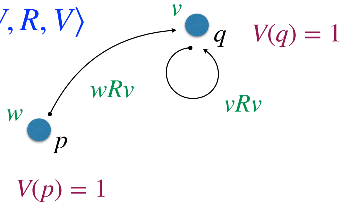
$\mathscr{M} = \langle W, R, V \rangle$



R is the relative accessibility relation:

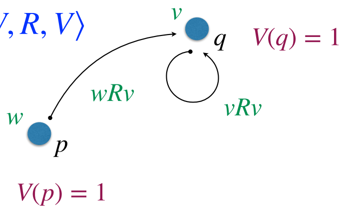
from the point of view of w, v is possible.

$\mathscr{M} = \langle W, R, V \rangle$



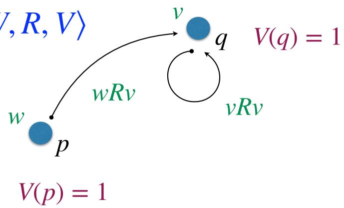
V assigns a truth value to a propositional variable at a world.

$\mathcal{M} = \langle W, R, V \rangle$



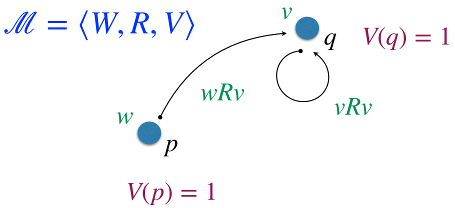
For non-atomic propositional formulas:
Just check the truth table
in each world!

$\mathcal{M} = \langle W, R, V \rangle$

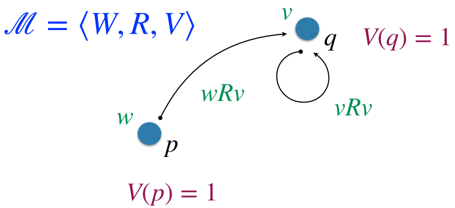


$\mathcal{M}, w \nvDash p \to q$

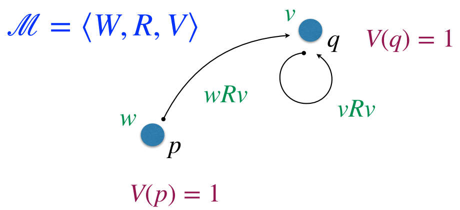
$\mathcal{M}, v \vDash p \to q$



How about modal formulas?

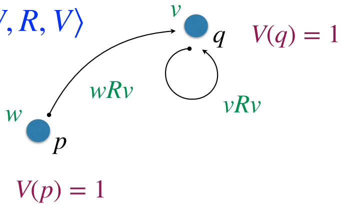


A is *necessary at a world* u provided A is true at every possible world from u.



A is *possible at a world* u provided A is true at some possible world from u.

$\mathscr{M} = \langle W, R, V \rangle$

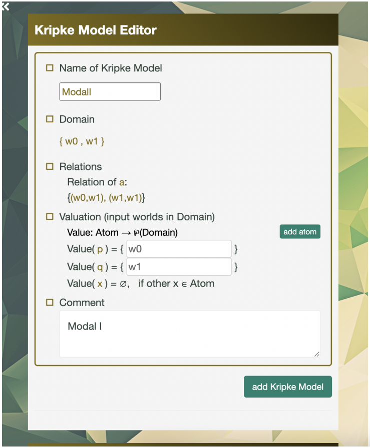


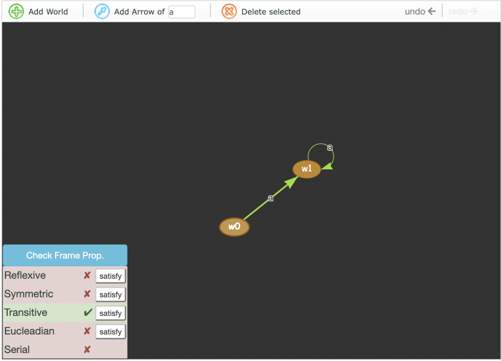
$\mathscr{M}, w \nvDash \Box p$ $\qquad$ $\mathscr{M}, v \nvDash \Box p$

$\mathscr{M}, w \vDash \Box q$ $\qquad$ $\mathscr{M}, v \vDash \Box q$

$\mathscr{M}, w \vDash \Box (p \rightarrow q)$ $\qquad$ $\mathscr{M}, v \vDash \Box (p \rightarrow q)$

Kripke models and satisfiability

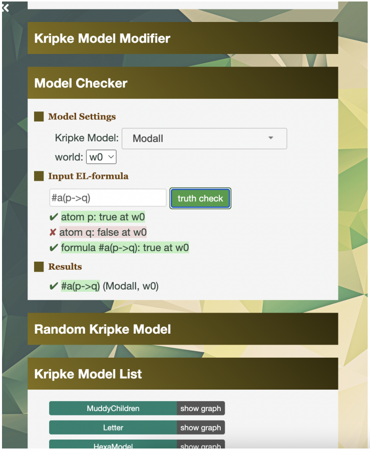


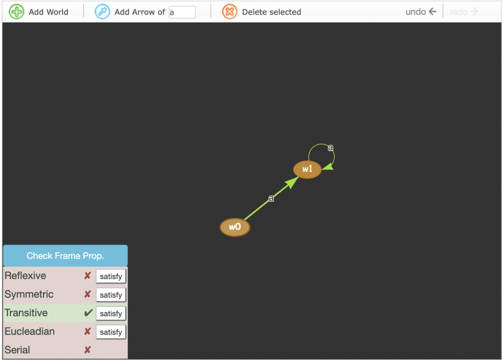


ELVis

Modal Logic Playground

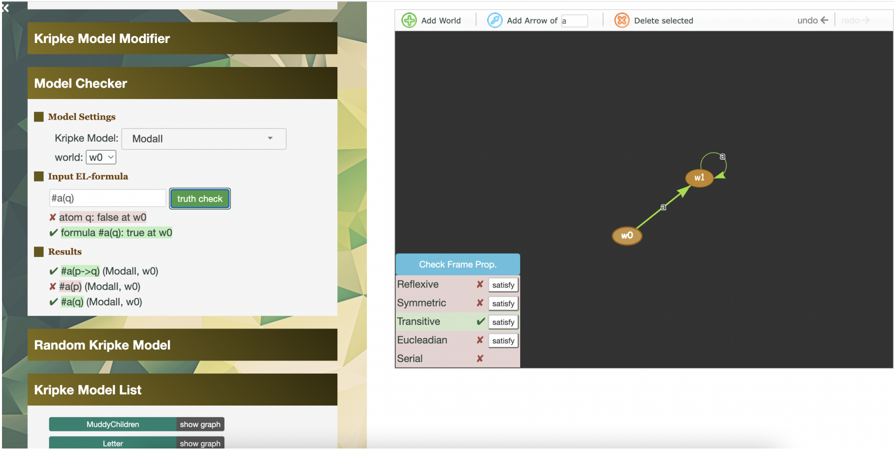
Kripke models and satisfiability





ELVis

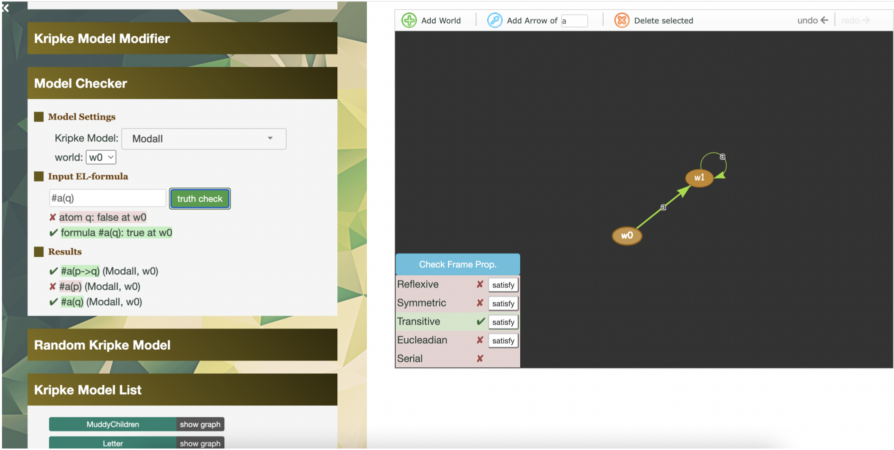
Modal Logic Playground



ELVis

Modal Logic Playground

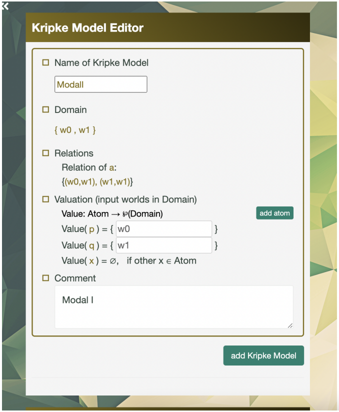
Kripke models and satisfiability

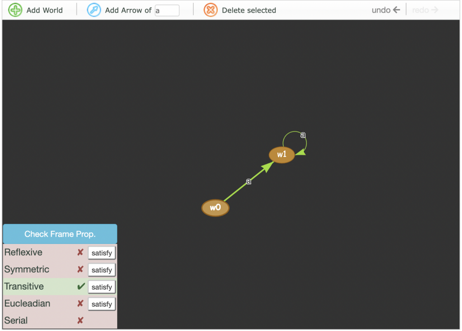


ELVis

Modal Logic Playground
Very nice page:
Accessible Theorem Provers

In the model Modal I:



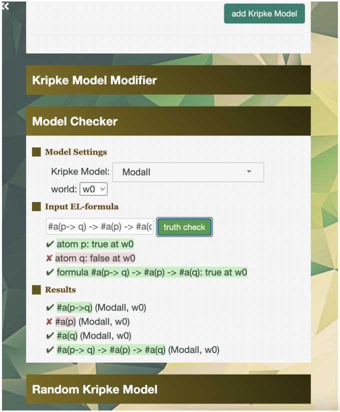


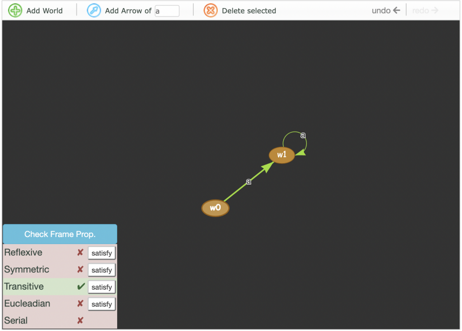
let's try to prove:

1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.

Exercises

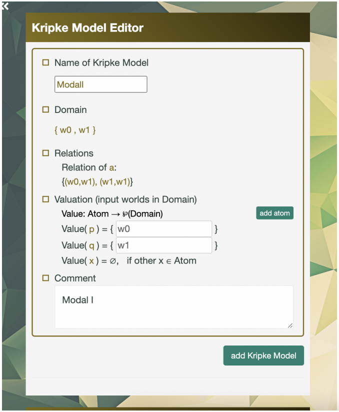
1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.

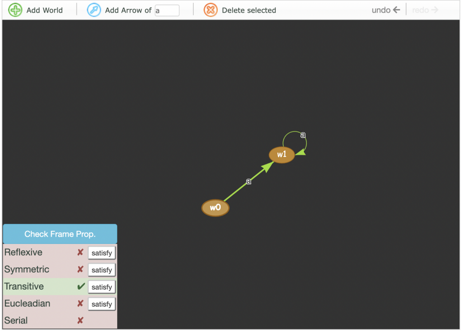




Exercises

In the model Modal I:



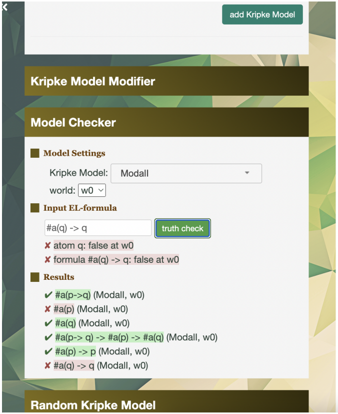


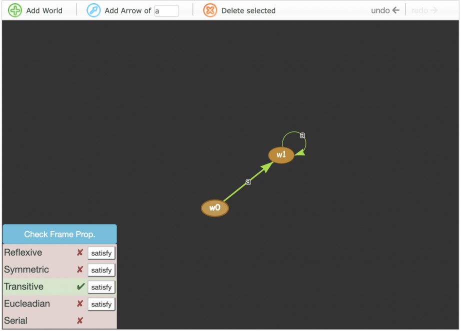
let's try to prove:

1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0.

Exercises

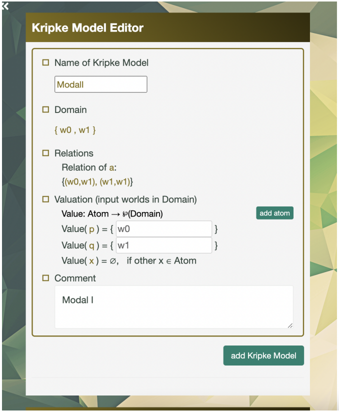
1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0.

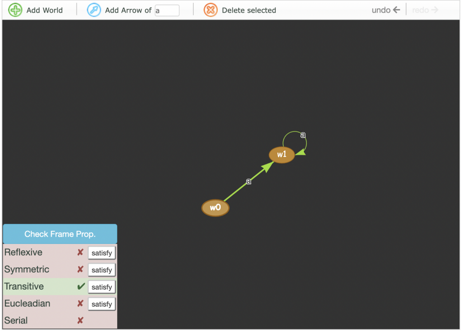




Exercises

In the model Modal I:



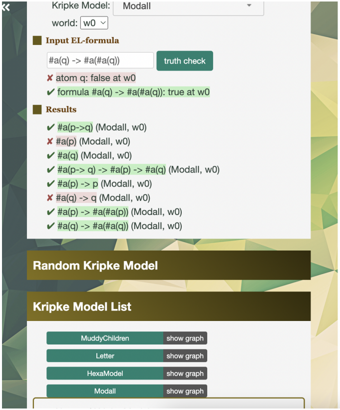


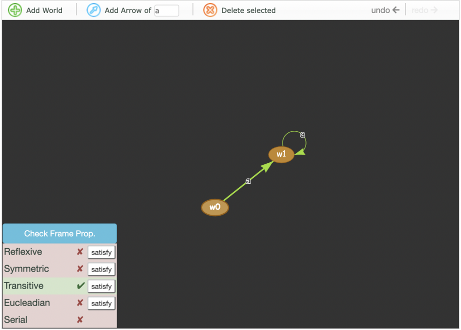
let's try to prove:

1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0.
3. $\Box p \to \Box\Box p$ and $\Box q \to \Box\Box q$ in w_0.

Exercises

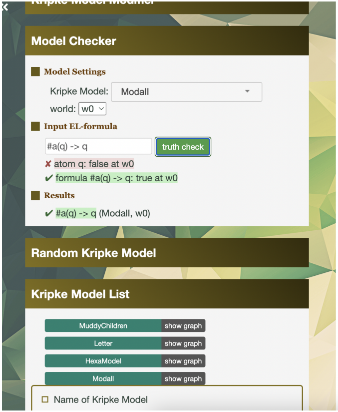
1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0. Reflexivity ✗
3. $\Box p \to \Box\Box p$ and $\Box q \to \Box\Box q$ in w_0. Transitivity ✓

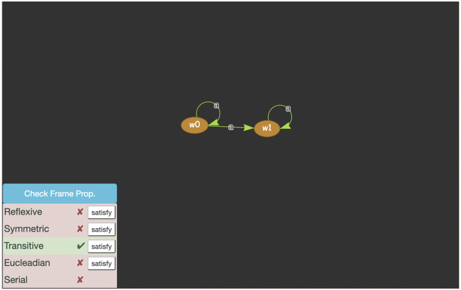




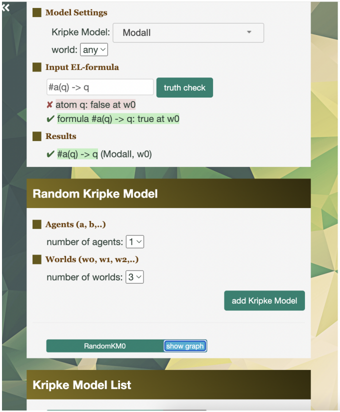
Exercises

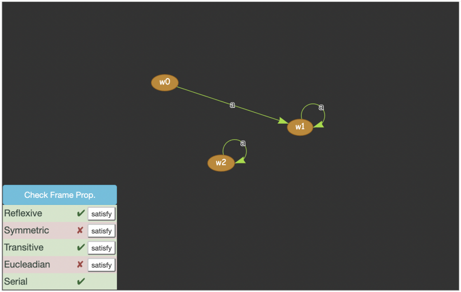
1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0. Reflexivity ✓
3. $\Box p \to \Box\Box p$ and $\Box q \to \Box\Box q$ in w_0. Transitivity ✓





1. $\Box(p \to q) \to \Box p \to \Box q$ in w_0.
2. $\Box p \to p$ and $\Box q \to q$ in w_0. Reflexivity ✓
3. $\Box p \to \Box\Box p$ and $\Box q \to \Box\Box q$ in w_0. Transitivity ✓
4. Play with random models in ELVis or the Modal Logic Playground





Relational model for modal logic (formally)

$\mathcal{M} = \langle W, R, V \rangle$, where $W \neq \emptyset, R \subseteq W \times W$ and $V : At \to \wp(W)$.

Relational model for modal logic (formally)

$\mathcal{M} = \langle W, R, V \rangle$, where $W \neq \emptyset$, $R \subseteq W \times W$ and $V : At \to \wp(W)$.

Truth at a state in a model $\mathcal{M}, w \models A$:

$\mathcal{M}, w \models p$	iff	$p \in V(w)$;
$\mathcal{M}, w \models \bot$		never holds;
$\mathcal{M}, w \models \neg A$	iff	$\mathcal{M}, w \not\models A$;
$\mathcal{M}, w \models A \wedge B$	iff	$\mathcal{M}, w \models A$ and $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \vee B$	iff	$\mathcal{M}, w \models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \to B$	iff	$\mathcal{M}, w \not\models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models \Box A$	iff	for all $v.\, wRv$ implies $\mathcal{M}, v \models A$;
$\mathcal{M}, w \models \Diamond A$	iff	there exists $v.\, wRv$ and $\mathcal{M}, v \models A$.

Relational model for modal logic (formally)

$\mathcal{M} = \langle W, R, V \rangle$, where $W \neq \emptyset, R \subseteq W \times W$ and $V : At \to \wp(W)$.

Truth at a state in a model $\mathcal{M}, w \models A$:

$\mathcal{M}, w \models p$	iff	$p \in V(w)$;
$\mathcal{M}, w \models \bot$		never holds;
$\mathcal{M}, w \models \neg A$	iff	$\mathcal{M}, w \not\models A$;
$\mathcal{M}, w \models A \wedge B$	iff	$\mathcal{M}, w \models A$ and $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \vee B$	iff	$\mathcal{M}, w \models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \to B$	iff	$\mathcal{M}, w \not\models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models \Box A$	iff	for all $v. wRv$ implies $\mathcal{M}, v \models A$;
$\mathcal{M}, w \models \Diamond A$	iff	there exists $v. wRv$ and $\mathcal{M}, v \models A$.

A formula A is satisfiable if there exists a model $\mathcal{M}$ and $w \in W$ such that $M, w \models A$.

Relational model for modal logic (formally)

$\mathcal{M} = \langle W, R, V \rangle$, where $W \neq \emptyset$, $R \subseteq W \times W$ and $V : At \to \wp(W)$.

Truth at a state in a model $\mathcal{M}, w \models A$:

$\mathcal{M}, w \models p$	iff	$p \in V(w)$;
$\mathcal{M}, w \models \bot$		never holds;
$\mathcal{M}, w \models \neg A$	iff	$\mathcal{M}, w \not\models A$;
$\mathcal{M}, w \models A \wedge B$	iff	$\mathcal{M}, w \models A$ and $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \vee B$	iff	$\mathcal{M}, w \models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \to B$	iff	$\mathcal{M}, w \not\models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models \Box A$	iff	for all v. wRv implies $\mathcal{M}, v \models A$;
$\mathcal{M}, w \models \Diamond A$	iff	there exists v. wRv and $\mathcal{M}, v \models A$.

A formula A is satisfiable if there exists a model $\mathcal{M}$ and $w \in W$ such that $M, w \models A$.

A modal formula A is valid if it is valid in every model ($\models A$).

Relational model for modal logic (formally)

$\mathcal{M} = \langle W, R, V\rangle$, where $W \neq \emptyset, R \subseteq W \times W$ and $V : At \to \wp(W)$.

Truth at a state in a model $\mathcal{M}, w \models A$:

$\mathcal{M}, w \models p$	iff	$p \in V(w)$;
$\mathcal{M}, w \models \bot$		never holds;
$\mathcal{M}, w \models \neg A$	iff	$\mathcal{M}, w \not\models A$;
$\mathcal{M}, w \models A \wedge B$	iff	$\mathcal{M}, w \models A$ and $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \vee B$	iff	$\mathcal{M}, w \models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models A \to B$	iff	$\mathcal{M}, w \not\models A$ or $\mathcal{M}, w \models B$;
$\mathcal{M}, w \models \Box A$	iff	for all $v. wRv$ implies $\mathcal{M}, v \models A$;
$\mathcal{M}, w \models \Diamond A$	iff	there exists $v. wRv$ and $\mathcal{M}, v \models A$.

A formula A is satisfiable if there exists a model $\mathcal{M}$ and $w \in W$ such that $M, w \models A$.

A modal formula A is valid if it is valid in every model ($\models A$).

The argument from a set of formulas Γ to a set of formulas Δ is valid if, for every model $\mathcal{M}$ and every world $w \in W$, if $\mathcal{M}, w \models B$ for each $B \in \Gamma$, then $\mathcal{M}, w \models A$ for some $A \in \Delta$ ($\Gamma \models \Delta$).

End of Part I

Thank you!!!

Obrigada!!!

Gracias!!!

☺

Prove the following sequents in classical logic:

1. $\neg(A \vee B) \vdash \neg A \wedge \neg B$
2. $A \vee B \vdash \neg(\neg A \wedge \neg B)$
3. $A \vee B \vdash \neg A \to B$
4. $\neg(A \wedge B) \vdash \neg A \vee \neg B$
5. $\vdash ((A \to B) \to A) \to A$ (Peirce's law)
6. $\vdash (A \to B) \vee (B \to A)$
7. $\vdash \exists x.(D(x) \to \forall y.D(y))$ (drinker's principle)

Prove the following equivalences in classical logic:

8. $\neg\neg A \equiv A$
9. $\neg A \equiv A \to \bot$

Which have constructive proofs?

10. Play the logic game!!! Lean4: game-logic

References and useful links

References:

1. B. F. Chellas, Modal Logic (Cambridge University Press, 1980)
2. Patrick Blackburn, Maarten de Rijke and Yde Venema, Modal Logic (Cambridge University Press, 2001)
3. Sara Negri and Jan von Plato, Structural Proof Theory (Cambridge University Press, 2001)

Useful links:

- Lean 4 Web: `https://live.lean-lang.org/`
- A Lean intro to Logic: `https://adam.math.hhu.de/#/g/trequetrum/lean4game-logic`
- SeqCalc: `https://seqcalc.dev/`
- ELVis: `https://nomuras.github.io/ELVis/`
- Modal Logic Playground: `https://rkirsling.github.io/modallogic/`
- Accessible theorem provers: `https://staff.cs.manchester.ac.uk/~schmidt/tools/#provers`