



Sequent Calculus

Definition: Validity of sequents

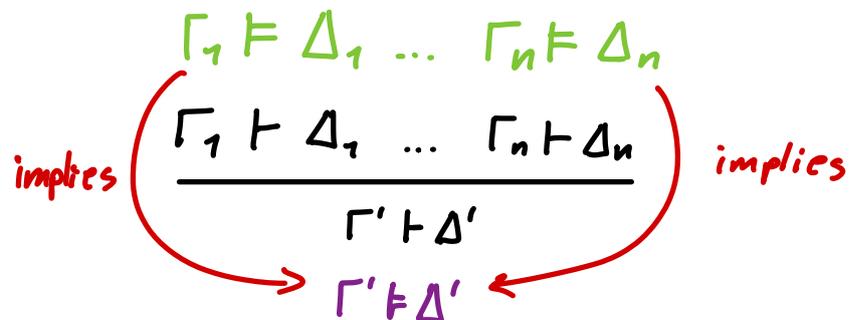
A sequent $F_1, \dots, F_n \vdash G_1, \dots, G_m$ is valid

iff $F_1, \dots, F_n \vDash G_1, \dots, G_m$, that is every model satisfying all of F_1, \dots, F_n satisfies at least one of G_1, \dots, G_m

Practically this means in an arbitrary interpretation v either one of F_1, \dots, F_n evaluates to false or one of G_1, \dots, G_m evaluates to true.

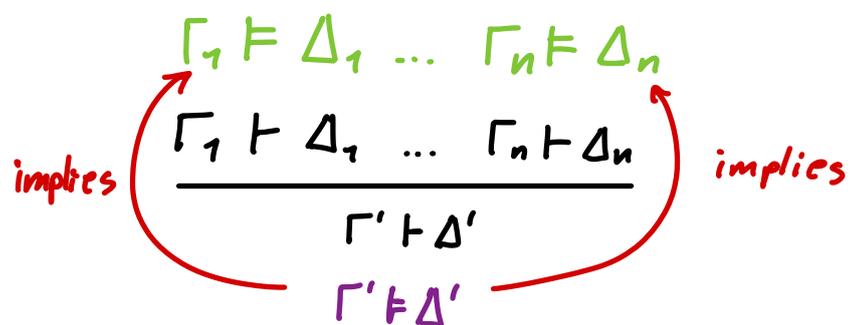
Definition: Soundness of rules

A rule is sound iff whenever all premises are valid, then so is its conclusion.



Definition: Invertibility

A rule is invertible iff whenever its conclusion is valid, then so are all its premises.



Model Theory

Definition: Equality and Congruence Axioms

- 1) $\forall x (x \sim x)$
- 2) $\forall xy (x \sim y \rightarrow y \sim x)$
- 3) $\forall xyz (x \sim y \wedge y \sim z \rightarrow x \sim z)$
- 4) for each n -ary function symbols f :
 $\forall \bar{x} \bar{y} (\bar{x} \sim \bar{y} \rightarrow f(\bar{x}) \sim f(\bar{y}))$ with $\bar{x} = x_1 \dots x_n$, $\bar{y} = y_1 \dots y_n$
- 5) for each n -ary predicate symbol P :
 $\forall \bar{x} \bar{y} (\bar{x} \sim \bar{y} \rightarrow (P(\bar{x}) \rightarrow P(\bar{y})))$

Proposition:

Let P be a formula with equality:

" P sat in model with equality"

is equivalent to

" $P \wedge (1) \wedge (2) \wedge (3) \wedge (4) \wedge (5)$ sat"

Model Theory

Definition: Forcing $\geq n$ elements in the domain

$$\exists^{\geq n} := \exists x_1 \dots \exists x_n \bigwedge_{i \neq j} \neg (x_i \sim x_j)$$

$$(A, \xi) \models \exists^{\geq n} \text{ iff } |D_A| \geq n$$

Definition: Forcing $\leq n$ Elements

$$\exists^{\leq n} := \neg \underbrace{(\exists^{\geq n+1})}_{|D_A| < n+1 \text{ i.e. } |D_A| \leq n}$$

Corollary: Infinite Satisfiability

$$\forall x P(x, f(x)) \wedge \forall y \neg P(y, y) \wedge \forall u, v, w ((P(u, v) \wedge P(v, w)) \rightarrow P(u, w))$$

is satisfiable only in Models with infinite domain

Model Theory

Definition: Isomorphic interpretations

Let \mathcal{L} be a FO-language and $(A, \mathcal{I}^A), (A', \mathcal{I}^{A'})$ be two \mathcal{L} -structures. They are isomorphic if there exists bijective $g: D_A \rightarrow D_{A'}$ s.t.

•) for n -ary function symbols f :

$$g(f^A(b_1, \dots, b_n)) = f^{A'}(g(b_1), \dots, g(b_n))$$

•) for n -ary predicate symbols P :

$$P^A(b_1, \dots, b_n) \iff P^{A'}(g(b_1), \dots, g(b_n))$$

Lemma: Isomorphism Lemma

If A and A' in the same language \mathcal{L} are isomorphic, then for any WFF P :

$$A \models P \text{ iff } A' \models P$$

Intuitionistic Logic

Definition: Relation Properties

A relation R is called:

• reflexive: $\forall x [xRx]$

• transitive: $\forall x, y, z [(xRy \wedge yRz) \rightarrow (xRz)]$

• serial: $\forall x \exists y [xRy]$

• euclidean: $\forall x, y, z [(xRy \wedge xRz) \rightarrow yRz]$

Definition: Kripke Model for Intuitionistic Logic

A Kripke Model $\mathcal{M} = (W, R, V)$ is called intuitionistic if

• R is transitive and reflexive

• for every propositional variable p it holds that:
 $w \in V(p)$ and wRv implies $v \in V(p)$

this is called monotonicity

Semantically, formulas of intuitionistic logic are evaluated at worlds of intuitionistic Kripke models as in the usual semantics for modal logics, except:

• $\mathcal{M}, w \Vdash A \rightarrow B \iff$ if wRv and $\mathcal{M}, v \Vdash A$ then $\mathcal{M}, v \Vdash B$

this reads as: for all $v \in W, wRv$:

$\mathcal{M}, v \Vdash A$ implies $\mathcal{M}, v \Vdash B$

• $\mathcal{M}, w \Vdash \neg A \iff \mathcal{M}, w \Vdash A \rightarrow \perp$

this can be read as: for all $v \in W, wRv$: $\mathcal{M}, v \not\Vdash A$

• $\mathcal{M}, w \not\Vdash \perp$

no world satisfies falsum

Modal Logic

Definition: Normal Modal Logic

Is a set of modal formulas s.t. it contains

•) all propositional tautologies

•) all instances of Kripke schema: $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$

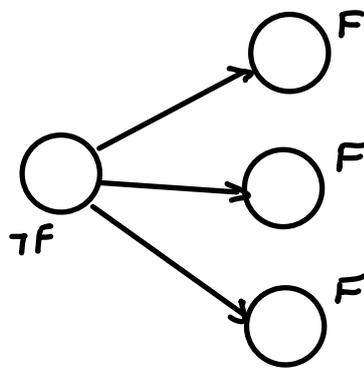
and is closed under

•) Modus Ponens: $\frac{A \rightarrow B \quad A}{B}$

•) Necessitation: $\frac{F}{\Box F}$

Corollary: Even though validity of F implies validity of $\Box F$
The formula $F \rightarrow \Box F$ is not valid

Take the following Model:



Modal Logic

Definition: Common Modal Axiom Schemas

Name	Axiom	Frame Condition
K:	$\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$	holds in all Frames
T:	$\Box A \rightarrow A$	reflexive: wRw
Q:	$\Box\Box A \rightarrow \Box A$	dense: $wRv \Rightarrow \exists u (wRu \wedge vRu)$
4:	$\Box A \rightarrow \Box\Box A$	transitive: $wRv \wedge vRu \Rightarrow wRu$
D:	$\Box A \rightarrow \Diamond A$ or $\Diamond \top \rightarrow \neg \Box \perp$	serial: $\forall w \exists v (wRv)$
B:	$A \rightarrow \Box\Diamond A$ or $\Diamond\Box \rightarrow A$	symmetric: $wRv \Rightarrow vRw$
S:	$\Diamond A \rightarrow \Box\Diamond A$	eudidean: $wRu \wedge wRv \Rightarrow vRu$
GL:	$\Box(\Box A \rightarrow A) \rightarrow \Box A$	R transitive, R^{-1} well-founded
Gr2:	$\Box(\Box(A \rightarrow \Box A) \rightarrow A) \rightarrow A$	R refl. + trans, R^{-1} -Id wf
H:	$\Box(\Box A \rightarrow B) \vee \Box(\Box B \rightarrow A)$	$wRu \wedge wRv \Rightarrow vRu \vee vRw$
M:	$\Box\Diamond A \rightarrow \Diamond\Box A$	
G:	$\Diamond\Box A \rightarrow \Box\Diamond A$	convergent: $wRu \wedge wRv \Rightarrow \exists x (vRx \wedge uRx)$
-:	$A \rightarrow \Box A$	discrete: $wRv \Rightarrow w=v$
-:	$\Diamond A \rightarrow \Box A$	partial function: $wRu \wedge wRv \Rightarrow u=v$
-:	$\Diamond A \leftrightarrow \Box A$	function: $\forall w \exists! v: wRv$
-:	$\Box A$ or $\Box \perp$	empty: $\forall w \forall v \neg (wRv)$

Modal Logic

Definition: Common Modal Systems

Name	Axioms	Frame condition
K	—	all frames
T	T	reflexive
K4	4	transitive
S4	T, 4	preorder
S5	T, 5 or D, B, 4	equivalence relation
S4.3	T, 4, H	total preorder
S4.1	T, 4, M	preorder and $\forall w \exists u (w R u \wedge \forall v (u R v \Rightarrow u = v))$
S4.2	T, 4, G	directed preorder
GL, K4W	GL or 4, GL	finite strict partial order
Grz, S4Grz	Grz or T, 4, Grz	finite partial order
D	D	serial
D45	D, 4, 5	transitive, serial, and Euclidean

Lambda Calculus

Definition: Numerals

$$\begin{aligned}
0 &:= \lambda f x. x \\
1 &:= \lambda f x. f x \\
2 &:= \lambda f x. f (f x) \\
3 &:= \lambda f x. f (f (f x)) \\
&\vdots \\
n &:= \lambda f x. \underbrace{f (f \dots (f x) \dots)}_{n \text{ times}}
\end{aligned}$$

Definition: Successor

$$SUCC := \lambda n f x. f (n f x)$$

Definition: Addition

$$\begin{aligned}
PLUS &:= \lambda m n f x. m (n f x) \\
&= \lambda m n. m SUCC n
\end{aligned}$$

Definition: Multiplication

$$\begin{aligned}
MULT &:= \lambda m n f. m (n f) \\
&= \lambda m n. m (PLUS n) 0
\end{aligned}$$

Definition: Predecessor

Defined by two equations:

$$PRED 0 = 0 \text{ and } PRED (SUCC n) = n$$

Let $\langle M, N \rangle := PAIR := \lambda z. z M N$ and

$\pi_0 := \lambda xy. x$ $\pi_1 := \lambda xy. y$ be projections

and $h := \lambda p. PAIR (\pi_1 p) (SUCC (\pi_1 p))$

then $PRED := \lambda n. \pi_0 (n h (PAIR 0 0))$

Definition: Exponentiation

$$\begin{aligned}
POW &:= \lambda b n. n b \\
&= \lambda b n. n (MULT b) 1
\end{aligned}$$

Definition: Boolean Values

$$\begin{aligned}
TRUE &:= \lambda xy. x \\
FALSE &:= \lambda xy. y
\end{aligned}$$

Definition: Boolean Operators

$$\begin{aligned}
OR &:= \lambda p q. p p q \\
AND &:= \lambda p q. p q p \\
NOT &:= \lambda p. p FALSE TRUE \\
ITE &:= \lambda p a b. p a b
\end{aligned}$$

Definition: Is Zero

$$ISZERO := \lambda n. n (\lambda x. FALSE) TRUE$$

Definition: Less than Equal

$$LEQ := \lambda n m. ISZERO (SUB m n)$$

Definition: Pairs

$$\begin{aligned}
PAIR &:= \lambda xy f. f x y \\
FIRST &:= \lambda p. p (\lambda xy. x) \\
SECOND &:= \lambda p. p (\lambda xy. y)
\end{aligned}$$

Definition: Linked List

$$NIL := \lambda f. TRUE$$

the rest is just $PAIR x (PAIR y (PAIR \dots))$

$$NULL := \lambda p. p (\lambda xy. FALSE)$$

checks if p is empty list

Definition: Fixed Points

$$\begin{aligned}
Y &:= \lambda g. (\lambda x. g (x x)) (\lambda x. g (x x)) \\
\Theta &:= (\lambda xy. y (x x y)) (\lambda xy. y (x x y))
\end{aligned}$$

Primitive Recursive Functions

Definition: Basic Functions

$$\text{zero}^n: \mathbb{N}^n \rightarrow \mathbb{N}, \\ \bar{x} \mapsto 0$$

$$s: \mathbb{N} \rightarrow \mathbb{N} \\ x \mapsto x+1$$

$$\text{proj}_i^n: \mathbb{N}^n \rightarrow \mathbb{N} \\ \bar{x} \mapsto x_i$$

... are all prim. rec.

Definition: Composition

Let $h: \mathbb{N}^m \rightarrow \mathbb{N}$, $g: \mathbb{N}^k \rightarrow \mathbb{N}$

then $h \circ g: \mathbb{N}^k \rightarrow \mathbb{N}$ with

$$h \circ (g_1, \dots, g_m) := \\ h(g_1(x_1, \dots, x_k), \dots, g_m(x_1, \dots, x_k))$$

Definition: Addition

$$0 + y = y \\ s(x) + y = s(x + y)$$

so for $\rho(g, h)$

$$g := \text{proj}_1^1 \quad \text{Add}(0, y) = y \\ h := s \circ \text{proj}_2^3 \quad \text{Add}(s(x), y) = s(\text{Add}(x, y))$$

Definition: Truncated Subtraction

Runs over second argument so use auxiliary RSUB with x, y flipped:

$$\text{RSUB} := \rho(\text{proj}_1^1, \text{PRED} \circ \text{proj}_2^3)$$

$$\text{then SUB} := \text{RSUB} \circ (\text{proj}_2^2, \text{proj}_1^2)$$

Definition: μ -recursion f partial

$$g(x) = \mu y (f(x, y) = 0) = \min y \text{ s.t. :}$$

$$f(x, y) = 0 \text{ and } (f(x, z) \downarrow \text{ and } f(x, z) = 0 \forall z \leq y) \\ \uparrow \text{ otherwise}$$

Definition: Primitive recursion

Given $g: \mathbb{N}^k \rightarrow \mathbb{N}$ and $h: \mathbb{N}^{k+2} \rightarrow \mathbb{N}$
i.e. $g(x_1, \dots, x_k)$ and $h(y, z, x_1, \dots, x_k)$

then the primitive recursion operator ρ is defined as:

$$\rho(g, h) := f: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$$

with

$$f(y, x_1, \dots, x_k) = \begin{cases} g(x_1, \dots, x_k) & \text{if } y = 0 \\ h(y', f(y', x_1, \dots, x_k), x_1, \dots, x_k) & \text{if } y = s(y') \\ & \text{for some } y' \in \mathbb{N} \end{cases}$$

Definition:

Primitive recursive functions are closed under ρ and \circ

Definition: Multiplication

$$\text{Mul} = \rho(\text{zero}^1, \text{Add} \circ (\text{proj}_2^3, \text{proj}_3^3))$$

Definition: Predecessor

$$\text{PRED} := \rho(\text{zero}^0, \text{proj}_1^2)$$

Definition: Is zero

$$\text{ISZERO} := \rho(s \circ \text{zero}^0, \text{zero}^2)$$

Definition: less or equal

$$\text{LEQ} := \text{ISZERO} \circ \text{SUB}$$

Definition: greater or equal

$$\text{GEQ} := \text{LEQ} \circ (\text{proj}_2^2, \text{proj}_1^2)$$

Definition: If

$$\text{ITE} := \rho(\text{proj}_2^2, \text{proj}_3^4)$$

Definition: And, Or, Not, equal

$$\text{AND} := \text{ITE} \circ (\text{proj}_1^2, \text{proj}_2^2, \text{zero}^2)$$

$$\text{OR} := \text{ITE} \circ (\text{proj}_1^2, s \circ \text{zero}^2, \text{proj}_2^2)$$

$$\text{NOT} := \text{ITE} \circ (\text{proj}_1^2, \text{zero}^2, s \circ \text{zero}^2)$$

$$\text{EQ} := \text{AND} \circ (\text{LEQ}, \text{GEQ})$$

Well Formed Formulas WFF

Formally,

Definition

Is the minimal set X s.t.

- ▶ $\perp, A, B, \dots \in X$
- ▶ If $P \in X$ then $(\neg P) \in X$
- ▶ If $P, Q \in X$ then $(P * Q) \in X$, where $*$ $\in \{\wedge, \vee, \rightarrow\}$

Priority to avoid parenthesis: $\neg > \wedge > \vee > \rightarrow$

Definition: Subformula of a WFF Q is Q and every WFF P which appears in Q .

Semantics

$v : WFF \rightarrow \{0, 1\}$ is an interpretation if:

- ▶ $\perp : v(\perp) = 0$
- ▶ $\neg P : v(\neg P) = 1$ iff $v(P) = 0$
- ▶ $P \wedge Q : v(P \wedge Q) = \min\{v(P), v(Q)\}$
- ▶ $P \vee Q : v(P \vee Q) = \max\{v(P), v(Q)\}$

P	Q	$P \wedge Q$	$P \vee Q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

- ▶ $P \rightarrow Q : v(P \rightarrow Q) = 0$ iff $v(P) = 1$ and $v(Q) = 0$

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

Definition. If $v(P) = 1$ we say that P is **satisfied** by v , or that v is a **model** for P .

Structural Induction

Proposition

Let \mathcal{A} be a property. If

- ▶ \mathcal{A} holds for \perp, A, B, \dots
- ▶ For all WFF P if $\mathcal{A}(P)$ then $\mathcal{A}(\neg P)$
- ▶ For all WFFs P, Q if $\mathcal{A}(P)$ and $\mathcal{A}(Q)$, then $\mathcal{A}(P * Q)$, where $*$ $\in \{\wedge, \vee, \rightarrow\}$

then \mathcal{A} holds for all WFFs.

Proof: Let $Y = \{P \in WFF \mid \mathcal{A}(P)\}$. Y satisfies the properties of the definition of WFF. Hence $WFF \subseteq Y$, hence \mathcal{A} holds for all WFFs.

Semantics

- ▶ P is **satisfiable** if it has at least a model. P is **unsatisfiable** otherwise.

- ▶ A set of WFF Γ is **satisfiable** if there is at least a model which satisfies *all* its formulas

- ▶ P is a **tautology** (or **valid**) if every interpretation v is a model for P (denoted by $\models P$).

- ▶ P and Q are **equivalent** ($P \equiv Q$) if $v(P) = v(Q)$ for all v .

Theorem

P is a tautology iff $\neg P$ is unsatisfiable.

Formalizing arguments

Semantical Consequence

Let Γ be a set of WFF and Q be a formula. Q is a (**semantical**) **consequence** of Γ iff for each interpretation v

((for all $P_i \in \Gamma, v(P_i) = 1$) $\implies v(Q) = 1$) (denoted by $\Gamma \models Q$).

- ▶ **central notion:** an argument is true if the conclusion is true whenever the premises are true (independently on whether the premises are actually always true)

Formalizing arguments II

Theorem $\Gamma \models Q$ iff $\Gamma \cup \{\neg Q\}$ is unsatisfiable.

Proof

$\Gamma \models Q$ iff, for every interpretation v ,

(($\forall P_i \in \Gamma, v(P_i) = 1$) $\implies v(Q) = 1$). I.e. for every v either there exists a $P_i \in \Gamma$ such that $v(P_i) = 0$ or $v(Q) = 1$. Therefore, for every v there exist at least one formula $F \in \Gamma \cup \{\neg Q\}$ for which $v(F) = 0$.