The rules of constructive reasoning

Rosalie Iemhoff

Utrecht University

Intuitionistic logic

Constructive theories

Intermediate logics   Intuitionistic logic   Modal logics

Substructural logics

Theorems versus proofs

A is derivable from Γ using the axioms and rules of the formal system L:

$$\Gamma \vdash_{\mathsf{L}} A.$$

Rules

Dfn. A *rule* is an expression of the form Γ/A or

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

where A is a formula and Γ a finite set of formulas. It is an *axiom* if Γ is empty.

Dfn. A *formal system* L is a set of rules.

Dfn. $\Gamma \vdash_{\mathsf{L}} A$ iff there are formulas $A_1, \ldots, A_n = A$ such that every A_i either belongs to Γ or there is a rule Π/B in L such that for some substitution σ: $\sigma B = A_i$ and $\sigma\Pi \subseteq \{A_1, \ldots, A_{i-1}\}$.

Rules

Ex. Hilbert-style systems. Universal quantification:

$$\frac{A(x)}{\forall x A(x)} \, .$$

Ex. Sequent calculi. Cut:

$$\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \, .$$

Ex. Resolution. Rule:

$$\frac{X \cup \{p\} \quad \{\neg p\} \cup Y}{X \cup Y} \, .$$

Ex. Cutting planes. Sum:

$$\frac{\sum a_i p_i \geq c \quad \sum b_i p_i \geq d}{\sum (a_i + b_i) p_i \geq c + d} \, .$$

Ex. Natural deduction, type theory.

Disjunction properties

Ex. If $\vdash_{\mathsf{IQC}} A \vee B$ then $\vdash_{\mathsf{IQC}} A$ or $\vdash_{\mathsf{IQC}} B$.

Ex. If $\vdash_{\mathsf{KT}} A \rightarrow \Box A$ then $\vdash_{\mathsf{KT}} A$ or $\vdash_{\mathsf{KT}} \neg A$ (Williamson '92).

Dfn. A *multi-conclusion consequence relation* (m.c.r.) $\vdash$ is a relation on finite sets of formulas that is

reflexive	$A \vdash A$;
monotone	$\Gamma \vdash \Delta$ implies $\Gamma, \Pi \vdash \Delta, \Sigma$;
transitive	$\Gamma \vdash A, \Delta$ and $\Pi, A \vdash \Sigma$ implies $\Gamma, \Pi \vdash \Delta, \Sigma$;
structural	$\Gamma \vdash \Delta$ implies $\sigma\Gamma \vdash \sigma\Delta$ for all substitutions σ.

It is *single-conclusion* (s.c.r.) if $|\Delta \cup \Sigma| \leq 1$.

Note: For all s.c.r. $\vdash$ there is a formal system L such that $\vdash = \vdash_{\mathsf{L}}$.

For all formal systems L, $\vdash_{\mathsf{L}}$ is a s.c.r.

Derivable and admissible in s.c.r.

Dfn. $Th(\vdash) \equiv \{A \mid \ \vdash A \text{ holds } \}$.

Γ/A is *derivable* iff $\Gamma \vdash_{\mathsf{L}} A$.

Γ/A is *strongly derivable* iff $\vdash_{\mathsf{L}} \bigwedge \Gamma \rightarrow A$.

$R = \Gamma/A$ is *admissible* ($\Gamma \mathrel{|\!\sim}_{\mathsf{L}} A$) iff $Th(\vdash_{\mathsf{L}}) = Th(\vdash_{\mathsf{L},R})$.

Note: The minimal s.c.r. $\vdash$ for which $Th(\vdash_{\mathsf{L}}) = Th(\vdash)$ is

$$\{\Gamma \vdash A \mid \ \vdash_{\mathsf{L}} A \text{ or } A \in \Gamma \ \}.$$

The maximal one is $\mathrel{|\!\sim}_{\mathsf{L}}$.

Dfn. Γ/Δ is *derivable* if $\Gamma \vdash_{\mathsf{L}} A$ for some $A \in \Delta$.

$\Gamma \mathrel{|\!\sim}_{\mathsf{L}} \Delta$ iff for all σ: $\vdash_{\mathsf{L}} \bigwedge \sigma\Gamma$ implies $\vdash_{\mathsf{L}} \sigma A$ for some $A \in \Delta$.

Ex. $\bot/A$ is admissible in any consistent logic.

Ex. Cut is admissible in $\mathsf{LK} - \{\mathsf{Cut}\}$.

Ex. L has the disjunction property iff $A \vee B \mathrel{|\!\sim}_{\mathsf{L}} \{A, B\}$.

Ex. $\{A, \neg A \vee B\}/B$ is admissible in Belnap's relevance logic.

Not sound for IQC:

$$\dfrac{\begin{matrix}[\neg A] \\ \vdots \\ \bot\end{matrix}}{A}$$

Tautology problem

Thm. (Statman '79)
The TAUT problem of IPC is PSPACE-complete.

The TAUT problem of $\text{IPC}_{\rightarrow}$ is PSPACE-complete.

Thm. (Ladner '77)
The TAUT problem of S4 is PSPACE-complete.

Decidability

Thm. (Tarski '51)
The first order theory of $(\mathbb{R}, 0, 1, +, \cdot, =, \leq)$ is decidable.

Thm. (Gabbay '73)
The constructive f.o. theory of $(\mathbb{R}, 0, 1, +, \cdot, =, \leq)$ is undecidable.

DP and EP

Given a proof of $A \vee B$, how hard is it to find one of A or of B?

Thm. (Buss & Mints '99)
In IQC the complexity of DP and EP is superexponential.

In IPC the complexity of DP is polynomial.

The study of substitutions σ such that $\vdash_{\mathsf{L}} \sigma A$.

The study of the structure of theorems.

Note: If A is satisfiable, it is unifiable (using only $\top$ and $\bot$).

Thm. (Prucnal '73)
$\mathsf{IPC}_{\to,\wedge}$ is *structurally complete* (admissible = strongly derivable).

Prf. For $\sigma(r) = A \to r$, for all B: $\vdash \sigma B \leftrightarrow (A \to B)$ and $\vdash A \to \big(B \leftrightarrow \sigma(B)\big)$. $A \mathrel{|\!\sim} B$ implies $\vdash \sigma B$, which implies $\vdash A \to B$.

Unifiers

Dfn. σ is a *unifier* of A iff $\vdash \sigma A$.

$\tau \leqslant \sigma$ iff for some τ' for all atoms r: $\vdash \tau(r) \leftrightarrow \tau'\sigma(r)$.

σ is a *maximal* unifier of A if among the unifiers of A it is maximal.

A unifier σ of A is a *mgu* if $\tau \leqslant \sigma$ for all unifiers τ of A.

A unifier σ of A is *projective* if for all atoms r: $A \vdash r \leftrightarrow \sigma(r)$.

A formula A is *projective* if it has a projective unifier (pu).

Note: Projective unifiers are mgus: $\vdash \tau A$ implies $\vdash \tau(r) \leftrightarrow \tau\sigma(r)$.

Dfn. A logic has unification type

unitary if every unifiable formula has a mgu,

finitary if every unifiable formula has finitely many mus.

Thm. Classical logic is unitary and structurally complete.

Prf. Given a valuation v define

$$\sigma_v(r) = \begin{cases} A \wedge r & \text{if } v(r) = 0 \\ A \to r & \text{if } v(r) = 1. \end{cases}$$

If $v(A) = 1$, then $\vdash_{\mathsf{CPC}} \sigma_v A$.

Lem. If A is projective, then

$$A \mathrel{|\!\!\sim} B \;\Leftrightarrow\; A \vdash B.$$

Lem. L has finitary unification if for every A there is a finite set of projective formulas Π_A such that

$$\bigvee \Pi_A \mathrel{|\!\!\sim} A \mathrel{|\!\!\sim} \bigvee \Pi_A.$$

Prf. If $\vdash \sigma A$ then $\vdash \sigma B$ for some $B \in \Pi_A$ with pu σ_B. So $\sigma \leq \sigma_B$.

Note: Π provides a $\mathrel{|\!\!\sim}$-normal form: $\bigvee \Pi_A \mathrel{\sim\!\!|\!\!|\!\!\sim} A$.

Dfn. $\mathcal{R}$ is a *basis* for the admissible rules of L iff the rules in $\mathcal{R}$ are admissible in L and $\mathcal{R}$ derives all admissible rules of L.

Lem. If for every A there is a finite set of projective formulas Π_A and a set of admissible rules $\mathcal{R}$ such that

$$\bigvee \Pi_A \mathrel{|\!\!\sim} A \vdash_{\mathcal{R}} \bigvee \Pi_A,$$

then

- $\mathcal{R}$ is a basis for the admissible rules of L,
- L has finitary unification,
- $\bigvee \Pi$ is a $\mathrel{|\!\!\sim}$-normal form of A.

The pu of a formula in Π_A is a composition of substitutions σ_v.

Ex. $\{p, \neg p\}$ is the projective approximation of $p \vee \neg p$.

$\{\neg p \to q, \neg p \to r\}$ is the projective approximation of $\neg p \to q \vee r$.

Thm. (Minari & Wroński '88)
In any intermediate logic L: $\neg p \to q \vee r \mathrel{|\!\!\sim}_{\mathsf{L}} (\neg p \to q) \vee (\neg p \to r)$.

Unification in intermediate logics

Thm. (Rybakov '97) Admissibility in IPC, K4, S4 ... is decidable.

Thm. (Ghilardi '99 & Rozière '95 & Iemhoff '01) IPC has finitary unification and the Visser rules are a basis for its admissible rules.

Thm. (Ghilardi '99 & Iemhoff '05) KC ($\neg A \vee \neg\neg A$) has unitary unification and the Visser rules are a basis for its admissible rules.

Thm. (Iemhoff '05) The Visser rules are a basis for the admissible rules in all intermediate logics in which they are admissible.

Thm. (Wroński '08) L has projective unification iff L $\supseteq$ LC.

$$\mathsf{LC} \quad (A \to B) \vee (B \to A)$$

Thm. (Goudsmit & Iemhoff '12) The nth Visser rule is a basis for the admissible rules in all extensions of the $(n-1)$th Gabbay-de Jongh logic in which they are admissible.

Thm. (Ghilardi '01)
K4, S4, GL and many other modal logics have finitary unification.

Thm. (Jeřábek '05)
$\mathrm{V}^\bullet$ is a basis for the admissible rules in any extension of GL in which it is admissible. Similarly for V° w.r.t. S4.

Thm. (Dzik & Wojtylak '11)
$\mathrm{L} \supseteq \mathrm{S4}$ has projective unification iff $\mathrm{L} \supseteq \mathrm{S4.3}$.

$$\mathrm{S4.3} \quad \Box(\Box A \to \Box B) \vee \Box(\Box B \to \Box A)$$

Thm. (Mints '76)
In IPC, all nonderivable admissible rules contain $\vee$ and $\rightarrow$.

Thm. (Prucnal '83)
$\mathsf{IPC}_{\rightarrow}$ is structurally complete, as is $\mathsf{IPC}_{\rightarrow,\wedge}$.

Thm. (Cintula & Metcalfe '10)
$\mathsf{IPC}_{\rightarrow,\neg}$ has finitary unification and the Wroński rules are a basis for its admissible rules.

Thm. (Olson, Raftery and van Alten '08)
Hereditary structural completeness of various substructural logics.

Thm. In many intermediate and modal logics and their fragments:

For every A there is a finite set of projective formulas Π_A and a set of admissible rules $\mathcal{R}$ such that

- $\bigvee \Pi_A \mathrel{|\!\sim} A \vdash_{\mathcal{R}} \bigvee \Pi_A$,
- there is a finite number of rewrite steps to obtain Π_A from A,
- a proof of $\sigma_B B$ is constructed for every $B \in \Pi_A$,
- the formulas in Π_A have nesting of implications/boxes ≤ 2.

Prf. Find a notion of "valuation" such that $v(A) = 1$ implies that $\Gamma_A \vdash \sigma_v(A)$ for a certain set Γ_A and $v_1, \ldots, v_n$ s.t. $\vdash \sigma_{v_n} \ldots \sigma_{v_1} \bigwedge \Gamma$.

Finally show that every formula $\mathrel{|\!\sim}$-reduces to satisfiable formulas.

Unification with parameters

Dfn. Unification with parameters: propositional variables are divided into *atoms* and *parameters*, where the parameters remain unchanged under substitutions.

Thm. There is a basis for the admissible rules of IPC of the form

$$\frac{\mathcal{S}}{S'} \quad (\mathcal{S} \text{ is a resolution refutation of } S).$$

Dfn. A *Frege system* consists of finitely many axioms and rules.

All Frege systems for CPC polynomially simulate each other.

Thm. (Mints & Kojevnikov '04)
All Frege systems for IPC polynomially simulate each other.

Thm. (Jeřábek '06)
All Frege systems for K4, S4, GL polynomially simulate each other.

Complexity

Thm. (Hrubeš '07)
The lower bound on the number of proof lines in a proof in most standard Frege systems for IPC is exponential.

Whether this holds for classical logic is not known.

(What I wish) to do

- Predicate logic;
- Nontransitive modal logics;
- Substructural logics;
- Complexity.

Finis