Basic Proof Theory
Propositional Logic

(See the book by Troelstra and Schwichtenberg)

Proof rules and proof systems

Proof systems are defined by (proof or inference) rules of the form

$$\frac{T_1 \quad \dots \quad T_n}{T} \text{ rule-name}$$

where $T_1, \dots T_n$ (premises) and T (conclusion) are syntactic objects (eg formulas).

Intuitive reading: If $T_1, \dots, T_n$ are provable, then T is provable.

Degenerate case: If $n = 0$ the rule is called an axiom and the horizontal line is sometimes omitted.

If some U is provable, we write $\vdash U$.

Proof trees

Proofs (also: derivations) are drawn as trees of nested proof rules. Example:

$$\dfrac{\dfrac{\dfrac{}{T_1} \quad \dfrac{\dfrac{}{U}}{T_2}}{S_1} \qquad \dfrac{\dfrac{}{T_3}}{S_2}}{R}$$

We sometimes omit the names of proof rules in a proof tree if they are obvious or for space reasons. *You* should always show them!

Every fragment

$$\dfrac{T_1 \quad \dots \quad T_n}{T}$$

of a proof tree must be (an instance of) a proof rule.
All proofs must start with axioms.

The depth of a proof tree is the number of rules on the longest branch of the tree. Thus ≥ 1

Abbreviations

Until further notice:

$\bot$, $\neg$, $\wedge$, $\vee$, $\rightarrow$ are primitives.

$\top$ abbreviates $\neg\bot$

A possible simplification:

$\neg F$ abbreviates $F \rightarrow \bot$

We now consider three important proof systems:

- Sequent Calculus
- Natural Deduction
- Hilbert Systems

Sequent Calculus
Propositional Logic

Sequent Calculus

Invented by Gerhard Gentzen in 1935. Birth of proof theory.

Proof rules

$$\frac{S_1 \quad \dots \quad S_n}{S}$$

where $S_1, \dots S_n$ and S are sequents: expressions of the form

$$\Gamma \Rightarrow \Delta$$

with Γ and Δ finite multisets of formulas.

Multiset = set with possibly repeated elements; using sets possible but less elegant.

Notice: $\Rightarrow$ is just a—suggestive—separator

Intention of the calculus:

$\Gamma \Rightarrow \Delta$ is provable (derivable)

iff

$\bigwedge \Gamma \models \bigvee \Delta \quad (\bigwedge \Gamma \rightarrow \bigvee \Delta$ valid)

Sequents: Notation

- We use set notation for multisets, e.g. $\{A, B \to C, A\}$
- Drop $\{\}$: $F_1, \ldots, F_m \Rightarrow G_1, \ldots G_n$
- F, Γ abbreviates $\{F\} \cup \Gamma$ (similarly for Δ)
- Γ_1, Γ_2 abbreviates $\Gamma_1 \cup \Gamma_2$ (similarly for Δ)

Sequent Calculus rules

$$\frac{}{\bot, \Gamma \Rightarrow \Delta} \; \bot L \qquad \frac{}{A, \Gamma \Rightarrow A, \Delta} \; Ax$$

$$\frac{\Gamma \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta} \; \neg L \qquad \frac{F, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \neg F, \Delta} \; \neg R$$

$$\frac{F, G, \Gamma \Rightarrow \Delta}{F \wedge G, \Gamma \Rightarrow \Delta} \; \wedge L \qquad \frac{\Gamma \Rightarrow F, \Delta \quad \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \wedge G, \Delta} \; \wedge R$$

$$\frac{F, \Gamma \Rightarrow \Delta \quad G, \Gamma \Rightarrow \Delta}{F \vee G, \Gamma \Rightarrow \Delta} \; \vee L \qquad \frac{\Gamma \Rightarrow F, G, \Delta}{\Gamma \Rightarrow F \vee G, \Delta} \; \vee R$$

$$\frac{\Gamma \Rightarrow F, \Delta \quad G, \Gamma \Rightarrow \Delta}{F \rightarrow G, \Gamma \Rightarrow \Delta} \; \rightarrow L \qquad \frac{F, \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \rightarrow G, \Delta} \; \rightarrow R$$

Sequent Calculus rules

Intuition: read backwards as proof search rules

$$\frac{}{\bot, \Gamma \Rightarrow \Delta}\ \bot L \qquad \frac{}{A, \Gamma \Rightarrow A, \Delta}\ Ax$$

$$\frac{\Gamma \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta}\ \neg L \qquad \frac{F, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \neg F, \Delta}\ \neg R$$

$$\frac{F, G, \Gamma \Rightarrow \Delta}{F \wedge G, \Gamma \Rightarrow \Delta}\ \wedge L \qquad \frac{\Gamma \Rightarrow F, \Delta \quad \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \wedge G, \Delta}\ \wedge R$$

$$\frac{F, \Gamma \Rightarrow \Delta \quad G, \Gamma \Rightarrow \Delta}{F \vee G, \Gamma \Rightarrow \Delta}\ \vee L \qquad \frac{\Gamma \Rightarrow F, G, \Delta}{\Gamma \Rightarrow F \vee G, \Delta}\ \vee R$$

$$\frac{\Gamma \Rightarrow F, \Delta \quad G, \Gamma \Rightarrow \Delta}{F \rightarrow G, \Gamma \Rightarrow \Delta}\ \rightarrow L \qquad \frac{F, \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \rightarrow G, \Delta}\ \rightarrow R$$

Every rule decomposes its principal formula

$$\overline{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}$$

$$\dfrac{}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q} \rightarrow R$$

$$\dfrac{F, \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \rightarrow G, \Delta} \quad \rightarrow R$$

$$\dfrac{\dfrac{}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q} \rightarrow R$$

$$\dfrac{F, \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \rightarrow G, \Delta} \quad \rightarrow R$$

$$\dfrac{\dfrac{}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}\ \wedge L}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q}\ \rightarrow R$$

$$\dfrac{F, G, \Gamma \Rightarrow \Delta}{F \wedge G, \Gamma \Rightarrow \Delta} \quad \wedge L$$

$$\dfrac{\dfrac{\overline{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q} \wedge L}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q} \rightarrow R$$

$$\dfrac{F, G, \Gamma \Rightarrow \Delta}{F \wedge G, \Gamma \Rightarrow \Delta} \quad \wedge L$$

$$\dfrac{\dfrac{\dfrac{}{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}\ \lor R}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\ \land L}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\ \to R$$

$$\dfrac{\Gamma \Rightarrow F, G, \Delta}{\Gamma \Rightarrow F \lor G, \Delta} \quad \lor R$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \lor R, Q \lor \neg R \Rightarrow P, Q}}{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}\ \lor R}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\ \land L}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\ \to R$$

$$\dfrac{\Gamma \Rightarrow F, G, \Delta}{\Gamma \Rightarrow F \lor G, \Delta} \quad \lor R$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overline{P \vee R, Q \vee \neg R \Rightarrow P, Q}\;\vee L}{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}\;\vee R}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}\;\wedge L}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q}\;\rightarrow R}{}
$$

$$
\dfrac{F, \Gamma \Rightarrow \Delta \quad G, \Gamma \Rightarrow \Delta}{F \vee G, \Gamma \Rightarrow \Delta} \quad \vee L
$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{P, Q \lor \neg R \Rightarrow P, Q} \qquad \overline{R, Q \lor \neg R \Rightarrow P, Q}}{P \lor R, Q \lor \neg R \Rightarrow P, Q}\ \lor L}{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}\ \lor R}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\ \land L}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\ \to R$$

$$\dfrac{F, \Gamma \Rightarrow \Delta \quad G, \Gamma \Rightarrow \Delta}{F \lor G, \Gamma \Rightarrow \Delta} \qquad \lor L$$

$$\dfrac{\dfrac{\overline{P, Q \vee \neg R \Rightarrow P, Q}\ Ax \qquad \overline{R, Q \vee \neg R \Rightarrow P, Q}}{P \vee R, Q \vee \neg R \Rightarrow P, Q}\ \vee L}{\dfrac{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}{\dfrac{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \to P \vee Q}\ \to R}\ \wedge L}\ \vee R$$

$$\overline{A, \Gamma \Rightarrow A, \Delta} \quad Ax$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P, Q \lor \neg R \Rightarrow P, Q}\ Ax \qquad \dfrac{}{R, Q \lor \neg R \Rightarrow P, Q}\ \lor L}{P \lor R, Q \lor \neg R \Rightarrow P, Q}\ \lor L}{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}\ \lor R}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\ \land L}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\ \to R}{}$$

$$\frac{F, \Gamma \Rightarrow \Delta \quad G, \Gamma \Rightarrow \Delta}{F \lor G, \Gamma \Rightarrow \Delta} \quad \lor L$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P, Q \lor \neg R \Rightarrow P, Q}\,Ax \qquad \dfrac{\dfrac{}{R, Q \Rightarrow P, Q} \qquad \dfrac{}{R, \neg R \Rightarrow P, Q}}{R, Q \lor \neg R \Rightarrow P, Q}\,\lor L}{P \lor R, Q \lor \neg R \Rightarrow P, Q}\,\lor L}{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}\,\lor R}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\,\land L}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\,\to R$$

$$\dfrac{F, \Gamma \Rightarrow \Delta \qquad G, \Gamma \Rightarrow \Delta}{F \lor G, \Gamma \Rightarrow \Delta} \qquad \lor L$$

$$
\dfrac{\dfrac{}{P, Q \vee \neg R \Rightarrow P, Q}\;Ax \qquad \dfrac{\dfrac{}{R, Q \Rightarrow P, Q}\;Ax \quad \dfrac{}{R, \neg R \Rightarrow P, Q}}{R, Q \vee \neg R \Rightarrow P, Q}\;\vee L}{\dfrac{\dfrac{\dfrac{P \vee R, Q \vee \neg R \Rightarrow P, Q}{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}\;\vee R}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}\;\wedge L}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \to P \vee Q}\;\to R}\;\vee L
$$

$$
\dfrac{}{A, \Gamma \Rightarrow A, \Delta}\quad Ax
$$

$$
\dfrac{\dfrac{}{P, Q \vee \neg R \Rightarrow P, Q}\ Ax \qquad \dfrac{\dfrac{}{R, Q \Rightarrow P, Q}\ Ax \quad \dfrac{}{R, \neg R \Rightarrow P, Q}\ \neg L}{R, Q \vee \neg R \Rightarrow P, Q}\ \vee L}{\dfrac{P \vee R, Q \vee \neg R \Rightarrow P, Q}{\dfrac{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}{\dfrac{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \rightarrow P \vee Q}\ \rightarrow R}\ \wedge L}\ \vee R}\ \vee L
$$

$$
\frac{\Gamma \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta} \quad \neg L
$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{}{P, Q \lor \neg R \Rightarrow P, Q}\,Ax
      \qquad
      \dfrac{
        \dfrac{}{R, Q \Rightarrow P, Q}\,Ax
        \qquad
        \dfrac{\dfrac{}{R \Rightarrow R, P, Q}}{R, \neg R \Rightarrow P, Q}\,\neg L
      }{R, Q \lor \neg R \Rightarrow P, Q}\,\lor L
    }{P \lor R, Q \lor \neg R \Rightarrow P, Q}\,\lor L
  }{
    \dfrac{P \lor R, Q \lor \neg R \Rightarrow P \lor Q}{(P \lor R) \land (Q \lor \neg R) \Rightarrow P \lor Q}\,\land L
  }\,\lor R
}{\Rightarrow (P \lor R) \land (Q \lor \neg R) \to P \lor Q}\,\to R
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P, Q \vee \neg R \Rightarrow P, Q}\,Ax \qquad \dfrac{\dfrac{}{R, Q \Rightarrow P, Q}\,Ax \qquad \dfrac{\dfrac{}{\color{red}{R} \Rightarrow \color{red}{R}, P, Q}\,Ax}{R, \neg R \Rightarrow P, Q}\,\neg L}{R, Q \vee \neg R \Rightarrow P, Q}\,\vee L}{P \vee R, Q \vee \neg R \Rightarrow P, Q}\,\vee L}{P \vee R, Q \vee \neg R \Rightarrow P \vee Q}\,\vee R}{(P \vee R) \wedge (Q \vee \neg R) \Rightarrow P \vee Q}\,\wedge L}{\Rightarrow (P \vee R) \wedge (Q \vee \neg R) \to P \vee Q}\,\to R
$$

$$
\dfrac{}{A, \Gamma \Rightarrow A, \Delta} \quad \color{magenta}{Ax}
$$

Proof search properties

- For every logical operator ($\neg$ etc)
  there is one left and one right rule
- Every formula in the premise of a rule
  is a subformula of the conclusion of the rule.

  This is called the subformula property.
  $\Rightarrow$ no need to guess anything when applying a rule backward
- Backward rule application terminates
  because one operator is removed in each step.

Instances of rules

Definition

An instance of a rule is the result of replacing Γ and Δ by multisets of concrete formulas and F and G by concrete formulas.

Example

$$\frac{\Rightarrow P \wedge Q, A, B}{\neg(P \wedge Q) \Rightarrow A, B}$$

is an instance of

$$\frac{\Gamma \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta}$$

setting $F := P \wedge Q$, $\Gamma := \emptyset$, $\Delta := \{A, B\}$

Proof trees

Definition (Proof tree)

A proof tree is a tree whose nodes are sequents and where each parent-children fragment

$$\frac{S_1 \quad \dots \quad S_n}{S}$$

is an instance of a proof rule.

($\Rightarrow$ all leaves must be instances of axioms)

A sequent S is provable (or derivable) if there is a proof tree with root S.
We write $\vdash_G S$ to denote that S is derivable.

Proof trees

An alternative inductive definition of proof trees:

Definition (Proof tree)

If

$$\frac{S_1 \quad \ldots \quad S_n}{S}$$

is an instance of a proof rule and
there are proof trees $T_1, \ldots T_n$ with roots $S_1, \ldots, S_n$

then

$$\frac{T_1 \quad \ldots \quad T_n}{S}$$

is a proof tree (with root S).

What does $\Gamma \Rightarrow \Delta$ "mean"?

Definition

$$|\Gamma \Rightarrow \Delta| \;=\; \left(\bigwedge \Gamma \to \bigvee \Delta\right)$$

Example: $|\{A, B\} \Rightarrow \{P, Q\}| = (A \wedge B \to P \vee Q)$

Remember: $\bigwedge \emptyset = \top$ and $\bigvee \emptyset = \bot$

We aim to prove: $\vdash_G S$ iff $\models |S|$

Lemma (Rule Equivalence)

For every rule $\dfrac{S_1 \quad \ldots \quad S_n}{S}$

- $|S| \equiv |S_1| \wedge \ldots \wedge |S_n|$
- $|S|$ *is a tautology iff all* $|S_i|$ *are tautologies*

Theorem (Soundness of $\vdash_G$)

If $\vdash_G S$ *then* $\models |S|$.

Proof by induction on the height of the proof tree for $\vdash_G S$.
Tree must end in rule instance

$$\frac{S_1 \quad \dots \quad S_n}{S}$$

If $n = 0$ then we vacuously have $\models |S_i|$ for all i.
If $n > 0$ then by IH we also have $\models |S_i|$ for all i.
So $\models |S_i|$ for all i, hence $\models |S|$ by the previous lemma.

Proof Search and Completeness

Proof search = growing a proof tree from the root

- Start from an initial sequent S_0
- At each stage we have some potentially *partial* proof tree with unproved leaves
- In each step, pick some unproved leaf S and some rule instance

  $$\frac{S_1 \quad \ldots \quad S_n}{S}$$

  and extend the tree with that rule instance
  (creating new unproved leaves $S_1, \ldots, S_n$)

Proof search terminates if . . .

- there are no more unproved leaves — success
- there is some unproved leaf where no rule applies — failure
  By the rules, that leaf is of the form

$$P_1, \ldots, P_k \Rightarrow Q_1, \ldots, Q_l$$

where all P_i and Q_j are atoms, no $P_i = Q_j$, and no $P_i = \bot$.

Example (failed proof)

$$\dfrac{\dfrac{\dfrac{}{P \Rightarrow P}\,Ax \quad Q \Rightarrow P}{P \vee Q \Rightarrow P}\,\vee L \quad \dfrac{P \Rightarrow Q \quad \dfrac{}{Q \Rightarrow Q}\,Ax}{P \vee Q \Rightarrow Q}\,\vee L}{P \vee Q \Rightarrow P \wedge Q}\,\wedge R$$

Falsifying assignments?

Proof search = Counterexample search

Can view sequent calculus as a search for a falsifying assignment for $|\Gamma \Rightarrow \Delta|$:

Make Γ true and Δ false

Some examples:

$$\frac{F, G, \Gamma \Rightarrow \Delta}{F \wedge G, \Gamma \Rightarrow \Delta} \quad \wedge L$$

To make $F \wedge G$ true, make both F and G true

$$\frac{\Gamma \Rightarrow F, \Delta \quad \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \wedge G, \Delta} \quad \wedge R$$

To make $F \wedge G$ false, make F or G false

Lemma (Search Equivalence)

At each stage of the search process,
if $S_1, \ldots, S_k$ *are the unproved leaves, then* $|S_0| \equiv |S_1| \wedge \ldots \wedge |S_k|$

Proof by induction on the number of search steps.
Initially trivially true (base case).
When applying a rule instance

$$\frac{U_1 \quad \ldots \quad U_n}{S_i}$$

we have

$$\begin{aligned} |S_0| \equiv & |S_1| \wedge \ldots \wedge |S_i| \wedge \ldots \wedge |S_k| \\ & \text{(by IH)} \\ \equiv & |S_1| \wedge \cdots \wedge |S_{i-1}| \wedge |U_1| \wedge \cdots \wedge |U_n| \wedge |S_{i+1}| \wedge \ldots \wedge |S_k| \\ & \text{(by Lemma Rule Equivalence)} \end{aligned}$$

Lemma

If proof search fails, $|S_0|$ is not a tautology.

Proof If proof search fails, there is some unproved leaf

$$S = \qquad P_1, \ldots, P_k \Rightarrow Q_1, \ldots, Q_l$$

where all P_i, Q_j atoms, no $P_i = Q_j$ and no $P_i = \bot$.
Any assignment $\mathcal{A}$ with $\mathcal{A}(P_i) = 1$ (for all i)
and $\mathcal{A}(Q_j) = 0$ (for all j) satisfies $\mathcal{A}(|S|) = 0$.
Thus $\mathcal{A}(|S_0|) = 0$ by Lemma Search Equivalence. □

Because of soundness of $\vdash_G$:

Corollary

Starting with some fixed S_0, proof search cannot both fail (for some choices) and succeed (for other choices).

$\Rightarrow$ no need for backtracking upon failure!

Theorem (Completeness)

If $\models |S|$ *then* $\vdash_G S$.

Proof by contraposition: if not $\vdash_G S$ then proof search must fail.
Therefore $\not\models |S|$.
Additionally we have:

Lemma

Proof search terminates.

Proof In every step, one logical operator is removed.
$\Rightarrow$ Size of sequent decreases by 1
$\Rightarrow$ Depth of proof tree is bounded by size of S_0
$\Rightarrow$ Construction of proof tree terminates. □
Observe: Breadth only bounded by $2^{\text{size of } S_0}$.

Corollary

Proof search is a decision procedure: it always terminates and it succeeds iff $\models S$.

Multisets versus sets

Termination only because of multisets.
With sets, the principal formula may get duplicated:

$$\frac{\Gamma \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta}\ \neg L \quad \overset{\Gamma := \{\neg F\}}{\rightsquigarrow} \quad \frac{\neg F \Rightarrow F, \Delta}{\neg F \Rightarrow \Delta}$$

An alternative formulation of the set version:

$$\frac{\Gamma \backslash \{\neg F\} \Rightarrow F, \Delta}{\neg F, \Gamma \Rightarrow \Delta}$$

Gentzen used sequences (hence "sequent calculus")

Admissible Rules and Cut Elimination

Admissible rules

Definition

A rule

$$\frac{S_1 \quad \dots \quad S_n}{S}$$

is admissible if $\vdash_G S_1, \dots, \vdash_G S_n$ together imply $\vdash_G S$.

$\Rightarrow$ Admissible rules can be used in proofs like normal rules

Admissibility of

$$\frac{S_1 \quad \dots \quad S_n}{S}$$

can be shown semantically (using $\vdash_G$ iff $\models$)
by proving that $\models |S_1|, \dots, \models |S_n|$ together imply $\models |S|$.

Proof theory is interested in syntactic proofs that show how to eliminate admissible rules.

Cut elimination rule

Theorem (Gentzen's *Hauptsatz*)

The cut elimination rule

$$\frac{\Gamma \Rightarrow F, \Delta \quad \Gamma, F \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \quad \textit{cut}$$

is admissible.

Proof Omitted.

Proofs with cut elimination can be much shorter than proofs without!
But: applying the rule needs creativity! (find the right F)
Intuitively: Proof of Gentzen's theorem shows how to replace creativity by calculation.

Many applications.

Tableaux Calculus
Propositional Logic

A compact version of sequent calculus

The idea

What's "wrong" with sequent calculus:

Why do we have to copy(?) Γ and Δ
with every rule application?

The answer: tableaux calculus.
The idea:

Describe *backward* sequent calculus rule application
but leave Γ and Δ implicit/shared

Comparison:

Sequent	Proof is a tree labeled by sequents, trees grow upwards
Tableaux	Proof is a tree labeled by formulas, trees grow downwards

Terminology: tableau = tableaux calculus proof tree

Tableaux rules (examples)

Notation: $+F \;\approx\;$ F occurs on the right of $\Rightarrow$
 $-F \;\approx\;$ F occurs on the left of $\Rightarrow$

S.C.		*Tab.*		*Effect*
$\dfrac{F, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \neg F, \Delta}$	$\rightsquigarrow$	$\dfrac{+\neg F}{-F}$	$\rightsquigarrow$	$\begin{array}{c} +\neg F \\ \vert \\ -F \end{array}$
$\dfrac{\Gamma \Rightarrow F, G, \Delta}{\Gamma \Rightarrow F \vee G, \Delta}$	$\rightsquigarrow$	$\dfrac{+F \vee G}{\begin{array}{c} +F \\ +G \end{array}}$	$\rightsquigarrow$	$\begin{array}{c} +F \vee G \\ \vert \\ +F \\ \vert \\ +G \end{array}$
$\dfrac{\Gamma \Rightarrow F, \Delta \quad \Gamma \Rightarrow G, \Delta}{\Gamma \Rightarrow F \wedge G, \Delta}$	$\rightsquigarrow$	$\dfrac{+F \wedge G}{+F \mid +G}$	$\rightsquigarrow$	$\begin{array}{c} +F \wedge G \\ / \quad \backslash \\ +F \qquad +G \end{array}$

Interpretation of tableaux rule

$$\frac{F}{FGH}$$

if F matches the formula at some node in the tableau extend the end of some branch starting at that node according to FGH.

Example

$$- A \to B$$
$$- B \to C$$
$$- A$$
$$+ C$$

$$A \to B, B \to C, A \Rightarrow C$$

From tableau to sequents:

- Every path from the root to a leaf in a tableau represents a sequent
- The set of all such sequents represents the set of leaves of the corresponding sequent calculus proof

$\Rightarrow$

- A branch is closed (proved) if both $+F$ and $-F$ occur on it or $-\bot$ occurs on it
- The root sequent is proved if all branches are closed

Algorithm to prove $F_1, \ldots \Rightarrow G_1, \ldots$:

1. Start with the tableau $-F_1, \ldots, +G_1, \ldots$.
2. while there is an open branch do
   pick some non-atomic formula on that branch,
   extend the branch according to the matching rule

Termination

No formula needs to be used twice on the same branch.
But possibly on *different* branches:

$$+\neg A \wedge \neg B$$
$$+A \vee B$$

A formula occurrence in a tableau can be deleted
if it has been used in every unclosed branch
starting from that occurrence

Tableaux rules

$$\frac{-\neg F}{+F} \qquad \frac{+\neg F}{-F}$$

$$\frac{-F \wedge G}{\begin{array}{c}-F\\ -G\end{array}} \qquad \frac{+F \wedge G}{+F \mid +G}$$

$$\frac{-F \vee G}{-F \mid -G} \qquad \frac{+F \vee G}{\begin{array}{c}+F\\ +G\end{array}}$$

$$\frac{-F \rightarrow G}{+F \mid -G} \qquad \frac{+F \rightarrow G}{\begin{array}{c}-F\\ +G\end{array}}$$

Natural Deduction
Propositional Logic

(See the book by Troelstra and Schwichtenberg)

Natural deduction (Gentzen 1935) aims at *natural* proofs

It formalizes good mathematical practice

Resolution but also sequent calculus aim at proof search

Main principles

1. For every logical operator $\oplus$ there are two kinds of rules:

Introduction rules: How to prove $F \oplus G$

$$\frac{\dots}{F \oplus G}$$

Elimination rules What can be proved from $F \oplus G$

$$\frac{F \oplus G \quad \dots}{\dots}$$

Examples

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

Main principles

2. Proof can contain subproofs with *local/closed* assumptions

Example

If from the local assumption F we can prove G
then we can prove $F \to G$.

The formal inference rule:

$$\dfrac{\begin{matrix}[F] \\ \vdots \\ G\end{matrix}}{F \to G} \to I$$

A proof tree:

$$\dfrac{\dfrac{[P] \quad Q}{P \land Q} \land I}{P \to P \land Q} \to I$$

Form the (open) assumption Q we can prove $P \to P \land Q$.
In symbols: $Q \vdash_N P \to P \land Q$

Growing the proof tree

Upwards:

Growing the proof tree

Upwards:

$$\overline{P \to P \wedge Q}$$

Growing the proof tree

Upwards:

$$\frac{}{P \to P \wedge Q} \to I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{}{P \land Q}}{P \to P \land Q} \to I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{P \qquad Q}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q} \wedge I}{P \rightarrow P \wedge Q} \rightarrow I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q} \wedge I}{P \rightarrow P \wedge Q} \rightarrow I$$

Downwards:

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \to P \wedge Q}\ \to I$$

Downwards:

$$\dfrac{\dfrac{P \quad Q}{}}{}$$

Growing the proof tree

Upwards:

$$\cfrac{\cfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

Downwards:

$$\cfrac{\cfrac{P \quad Q}{}\ \wedge I}{}$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \to P \wedge Q}\ \to I$$

Downwards:

$$\dfrac{\dfrac{P \quad Q}{P \wedge Q}\ \wedge I}{}$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

Downwards:

$$\dfrac{\dfrac{P \quad Q}{P \wedge Q}\ \wedge I}{}\ \rightarrow I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \to P \wedge Q}\ {\to} I$$

Downwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{\quad}\ {\to} I$$

Growing the proof tree

Upwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

Downwards:

$$\dfrac{\dfrac{[P] \quad Q}{P \wedge Q}\ \wedge I}{P \rightarrow P \wedge Q}\ \rightarrow I$$

ND proof trees

The nodes of a ND proof tree are labeled by formulas.
Leaf nodes represent assumptions.
The root node is the conclusion.
Assumptions can be open or closed.
Closed assumptions are written [F].

Intuition:

- Open assumptions are used in the proof of the conclusion
- Closed assumptions are local assumptions in a subproof that have been closed (removed) by some proof rule like $\rightarrow I$.

ND proof trees are defined inductively.

- Every F is a ND proof tree (with open assumption F and conclusion F). Reading: From F we can prove F.
- New proof trees are constructed by the rules of ND.

Natural Deduction rules

$$\frac{F \quad G}{F \wedge G}\ \wedge I \qquad \frac{F \wedge G}{F}\ \wedge E_1 \quad \frac{F \wedge G}{G}\ \wedge E_2$$

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

$$\frac{F}{F \vee G}\ \vee I_1 \quad \frac{G}{F \vee G}\ \vee I_2 \qquad \frac{F \vee G \quad \begin{array}{c}[F]\\ \vdots \\ H\end{array} \quad \begin{array}{c}[G]\\ \vdots \\ H\end{array}}{H}\ \vee E$$

$$\frac{\begin{array}{c}[\neg F]\\ \vdots \\ \bot\end{array}}{F}\ \bot$$

Natural Deduction rules

Rules for $\neg$ are special cases of rules for $\rightarrow$:

$$\cfrac{\begin{matrix}[F]\\ \vdots \\ \bot\end{matrix}}{\neg F}\,\neg I \qquad \frac{\neg F \quad F}{\bot}\,\neg E$$

Natural Deduction rules

How to read a rule

$$\frac{\cdots \quad \begin{array}{c}[F] \\ \vdots \\ G\end{array} \quad \cdots}{\cdots}\ r$$

Forward:
Close all (or some) of the assumptions F in the proof of G when applying rule r

Backward:
In the subproof of G you can use the local assumption $[F]$.

Can use labels to show which rule application closed which assumptions.

Soundness

Definition

$\Gamma \vdash_N F$ if there is a proof tree with root F and open assumptions contained in the set of formulas Γ.

Lemma (Soundness)

If $\Gamma \vdash_N F$ *then* $\Gamma \models F$

Proof by induction on the depth of the proof tree for $\Gamma \vdash_N F$.

Base case: no rule, $F \in \Gamma$

Step: Case analysis of last rule

Case $\rightarrow E$:
IH: $\Gamma \models F \rightarrow G \qquad \Gamma \models F$
To show: $\Gamma \models G$
Assume $\mathcal{A} \models \Gamma \Rightarrow^{IH} \mathcal{A}(F \rightarrow G) = 1$ and $\mathcal{A}(F) = 1 \Rightarrow \mathcal{A}(G) = 1$

Soundness

Case

$$\dfrac{\begin{array}{c}[F]\\ \vdots \\ G\end{array}}{F \to G} \to I$$

IH: $\Gamma, F \models G$
To show: $\Gamma \models F \to G$
iff for all $\mathcal{A}$, $\mathcal{A} \models \Gamma \Rightarrow \mathcal{A} \models F \to G$
iff for all $\mathcal{A}$, $\mathcal{A} \models \Gamma \Rightarrow (\mathcal{A} \models F \Rightarrow \mathcal{A} \models G)$
iff for all $\mathcal{A}$, $\mathcal{A} \models \Gamma$ and $\mathcal{A} \models F \;\Rightarrow\; \mathcal{A} \models G$
iff IH

Completeness

Towards completeness

ND can simulate truth tables

Lemma (Tertium non datur)

$\vdash_N F \lor \neg F$

Corollary (Cases)

If $F, \Gamma \vdash_N G$ *and* $\neg F, \Gamma \vdash_N G$ *then* $\Gamma \vdash_N G$*.*

Definition

$$F^{\mathcal{A}} := \begin{cases} F & \text{if } \mathcal{A}(F) = 1 \\ \neg F & \text{if } \mathcal{A}(F) = 0 \end{cases}$$

Towards completeness

Lemma (1)

If $atoms(F) \subseteq \{A_1, \dots, A_n\}$ *then* $A_1^{\mathcal{A}}, \dots, A_n^{\mathcal{A}} \vdash_N F^{\mathcal{A}}$

Proof by induction on F

Lemma (2)

If $atoms(F) = \{A_1, \dots, A_n\}$ *and* $\models F$
then $A_1^{\mathcal{A}}, \dots, A_k^{\mathcal{A}} \vdash_N F$ *for all* $k \leq n$

Proof by (downward) induction on $k = n, \dots, 0$

Completeness

Theorem (Completeness)

If $\Gamma \models F$ *then* $\Gamma \vdash_N F$

Proof

Relating
Sequent Calculs and Natural Deduction

Constructive approach to relating proof systems:

- Show how to transform proofs in one system into proofs in another system
- Implicit in inductive (meta)proof

Theorem (ND can simulate SC)

If $\vdash_G \Gamma \Rightarrow \Delta$ *then* $\Gamma, \neg\Delta \vdash_N \bot$ *(where* $\neg\{F_1, \dots\} = \{\neg F_1, \dots\}$*)*

Proof by induction on (the depth of) $\vdash_G \Gamma \Rightarrow \Delta$

Corollary (Completeness of ND)

If $\Gamma \models F$ *then* $\Gamma \vdash_N F$

Proof If $\Gamma \models F$ then $\Gamma_0 \models F$ for some finite $\Gamma_0 \subseteq \Gamma$.

Two completness proofs

- Direct
- By simulating a complete system

Theorem (SC can simulate ND)

If $\Gamma \vdash_N F$ *and* Γ *is finite then* $\vdash_G \Gamma \Rightarrow F$

Proof by induction on $\Gamma \vdash_N F$

Corollary

If $\Gamma \vdash_N F$ *then there is some finite* $\Gamma_0 \subseteq \Gamma$ *such that* $\vdash_G \Gamma_0 \Rightarrow F$