Anwendung der Logik

Peter Ladkin

ladkin@techfak.uni-bielefeld.de
http://www.techfak.uni-bielefeld.de/~ladkin

[begin **Administrativa**]

Ein Compendium-Beispiel (nicht Thema-Beispiel) für die Seminar-Arbeit steht unter

`http://www.techfak.uni-bielefeld.de/~ladkin`

nämlich

Computer-Related Incidents and Accidents with Commercial Airplanes

Es ist ein Kompendium der schriftlichen Resourcen vom WWW über dieses Thema

Die Bedürfnisse;

- Ein Thema auswählen

- relevante Resourcen im WWW und Bib suchen;

- Seminar-Vortrag/Vorschlag halten, um einen Kommentar von den anderen Teilnehmen zu bekommen;

- eine Zusammenfassung für das WWW: kleine Einführung oder 'Compendium' schreiben.

Für die, die nichts über das WWW wissen, dieser Seminar könnte zusammen mit meinem WWW-Design Seminar (Fr 1200-1400) gebunden werden (4 WS im diesen Semester + nochmal 2WS $\rightarrow$ Prüfung)

[end Administrativa]

Mögliche Arbeitsthemen:

- Verschiedene Arten
  von logischen Systemen

- Ein System und seine Anwendungen

- Logik in der Spezifikation

- Logik in der Verifikation

- Horn-Clause Logik - Logik-Programmierung

- Konstruktive Logik
- Lineare Logik
- Lambek Kalkül
- Modale Logik
- Dynamische Logik
- Automated Theorem Provers (ATPs)
- Die Logik eines ATP

Syntaktische Systeme der Logik

- Hilbertsche Systeme
- Natürliches Schließen
- Sequent-Kalkül
- Resolution
- Algebraische Methoden
  (Shostak, Nelson-Oppen,
  Knuth-Bendix-Rewriting-Systeme)
- Kombinatorische Logik

Semantische Systeme der Logik

- Klassische Systeme

- Nicht-Klassische Systeme

Nicht-Klassische Systeme der Logik

- Modale Logik
- Konstruktive Logik
- Inheritance-Systeme
- Type-Systeme
- Non-Monoton-Systeme
- Relevance Logik
- Lineare Logik
- Lambek-Kalkül

Modale Logik

- Temporale Logik (Spezifikation, Verifikation, Handlungsplanung)
- Situation Calculus (Handlungsplanung)
- Belief/Knowledge Logik
- Montague Grammatik

Konstruktive Logik

- Intuitionistische Logik
- .... von höherer Ordnung
- Manna-Waldinger Logik
- NuPRL
- Lineare Logik

Syntax of Logic

A logical system is based on a *language* which may be *formal* or *natural*

Examples:	(formal)	Propositional Logic
		First-Order Logic
		Higher-Order Logic
		Modal Logic
	(natural)	Deutsch
		English

There are two aspects to the syntax of logic (good old data-structure stuff):

- Defining objects (*well-formed formulas*)

- Defining operations on objects (*inference*)

These are both normally defined as built by *recursive functions* from a *recursive set* (let's just say *finite set* for the moment) of *atoms*

Atoms for wff's are *symbols*

Atoms for inference are *axioms*

The **Semantics** give the meaning of wff's.

Semantics is often *compositional*
that is, the meaning of the whole (formula) is determined by the meaning of the parts (subformulas)

We have a structure $\langle M, < \rangle$ where

- M is a set (of wff's)
- $<$ is a *well-founded partial order* on M

Then, for $f \in M$:

$$\textit{Meaning}(f) \triangleq F(\{\textit{Meaning}(g) | g < f\})$$

where F is some function
(let's call it the *semantic function*)

Examples of compositional semantics:

- Classical Propositional Logic
- Classical Predicate Logic
- Modal Logic
- Higher-Order Logic
- Sequential Programs (Floyd-Hoare logic)

Examples of non-compositional semantics:

- Brouwer's (Heyting's) Intuitionistic Logic

  (many semantics, including the *realisability* semantics of Kleene/Friedman)

- Concurrent Programs

  (Program 1 communicates with Program 2: how it functions is influenced by its *environment*, which includes Program 2, and not merely by the text of Program 1)

- Natural Language

  The reference of *indexicals* in a sentence (*he*, *it*, *them*) depends often on the context of a sentence.

  Meanings of sentences themselves often depend on the entire *discourse*

Nevertheless, one attempts to devise an equivalent system with a compositional semantics:

- Transformational grammar

  (Chomsky and many others)

- Montague grammar

  (Montague, then Partee and Dowty)

  It's a higher-order modal logic

Syntactical Styles

David Hilbert: Hilbert-style systems:
logical axioms + simple inference rule

Gerhard Gentzen: Natural Deduction:
no axioms; inference rules for each connective
Untersuchungen über das logische Schliessen,
Mathematische Zeitschrift 39, 1934, 176-210.

Sequent Calculus (also due to Gentzen):
similar to a metatheory of ND.
Axioms are $A \vdash A$, where

$$A_1, A_2, ..., A_m \vdash B_1, B_2, ..., B_n$$

is to be read as: *if all of the A's are true, then one of the B's is true*.

I shall use the formulation of Dag Prawitz
in his book *Natural Deduction*,
Almqvist and Wiksell, Stockholm 1965.

First, **Well-Formed Formulas**

First ingredient: a *set* of *symbols*

Symbols will usually include
$(\, , \,) \, , \wedge \, , \vee \, , \Rightarrow \, , \neg$
and symbols called *propositional variables*

One defines a set of meaningful strings,
i.e., strings to which one assigns meaning:
the *well-formed formulae* (wff's)

$(A \wedge B)$ is well-formed
$AB \wedge (($ is not
neither is $(\wedge AB)$

Usually, one uses parentheses around
infix expressions, because they can have
two different semantic interpretations
c.f., $A \wedge B \vee C$ – do I mean
$(A \wedge B) \vee C$ or $A \wedge (B \vee C)$?
But often one leaves them out

In fact, if one uses prefix notation –

$\wedge AB$, $\vee AB$, $\Rightarrow AB$, $\neg A$

one doesn't need to use parentheses.
There's a unique reading of the formula

This is called Polish notation.
Here's Reverse Polish:

$AB\wedge$, $AB\vee$, $AB \Rightarrow$, $\neg A$

And here's Cambridge Polish (aka Lisp)

$(\wedge AB)$, $(\vee AB)$, $(\Rightarrow AB)$, $(\neg A)$

(why? because one mixes up symbols and their meanings, whereas in pure propositional logic the symbols have a precise sort – they're variables or logical constants or punctuation)

A recursive definition of wff —

Every propositional variable is a wff
(there's an infinite fixed set of them)

If A is a wff then so is $(\neg A)$
If A and B are wffs then so is $(A \vee B)$
If A and B are wffs then so is $(A \wedge B)$
If A and B are wffs then so is $(A \Rightarrow B)$
If A and B are wffs then so is $(A \equiv B)$

Why do we want a recursive definition?
How do recursive definitions work?

Recall that

$$\mathit{Meaning}(f) \triangleq F(\{\mathit{Meaning}(g) | g < f\})$$

So if we want a compositional semantics, to find the meaning of a wff f, we can calculate the meaning of g for all $g < f$
And so on.

But we must be assured we can stop.

We thus need the notion of a
well-founded order $<$

An order $<$ is *well-founded* iff
given any set S of things in the order,
and any element $y \in S$,
there is no *infinite descending chain in* S.

A *chain in* S is a totally-ordered
subset of S. That is,
a $C = \{x_1, x_2, ..., x_n, ...\} \subseteq S$
such that $\forall x, y \in C : x \leq y \vee y \leq x$
that is, one can arrange them somehow
in an ordered line

$$... < x_n < x_k < x_s < ......$$

This is equivalent to saying that any
descending chain C in S has a lower bound
in C.

A *lower bound* x of a chain C in S is an element
below all elements of C, i.e.,

$$x \in S \wedge \forall y \in C : x \leq y$$

Consider the natural numbers $\langle \mathcal{N}, < \rangle$
where $\mathcal{N} = \{0, 1, 2, 3, 4, ...\}$
$<$ is well-founded (look at it)

Consider the integers $\langle \mathcal{I}, < \rangle$
where $\mathcal{I} = \{...., -2, -1, 0, 1, 2, 3, ...\}$
$<$ is *not* well-founded (look at it)

Induction is the rule

$$\frac{\begin{array}{l}\mathcal{P}(0) \\ \forall\, n \in \mathcal{N} \;:\; (\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1))\end{array}}{\forall\, n \in \mathcal{N} \;:\; \mathcal{P}(n)}$$

Why is it true within $\langle \mathcal{N}, < \rangle$?

Suppose the conclusion is false
but the first premiss true

So $S = \{ n \mid \neg\mathcal{P}(n) \} \neq \emptyset$
Pick m_0, its minimal element (exists by wf-ness)

$m_0 \neq 0$ (first premiss)
so $m_0 - 1$ exists
Now $\neg\mathcal{P}(m_0)$
but $\mathcal{P}(m_0 - 1)$ since $m_0 - 1 \notin S$
which renders the second premiss false
with $n = m_0 - 1$

So if both Premise 1 and Conclusion are true
then Premise 2 is false

Hence if both Premises are true
then Conclusion is true

Hence the well-foundedness of $<$ is used to show that induction is valid.

Induction is true also for any wf order $<$ in a more general form.

$$\frac{\begin{array}{l}\forall\, z \in \mathcal{S} \,:\, \textit{minimal}_{\mathcal{S}}(z) \Rightarrow \mathcal{P}(z) \\ \forall\, x \in \mathcal{S} \,:\, (\forall\, y \in \mathcal{S} \,:\, y < x \Rightarrow \mathcal{P}(y)) \Rightarrow \mathcal{P}(x)\end{array}}{\forall\, x \in \mathcal{S} \,:\, \mathcal{P}(x)}$$

Here, $\textit{minimal}_{\mathcal{S}}(z)$ is a predicate stating z is a minimal element of $\mathcal{S}$

Induction justifies recursive definitions in particular for us, a recursive definition of semantics based on the construction of wff's

Thus a compositional semantics with $<$ interpreted as *subformula of*

We started with the *objects* - wff's

Wff's are sequences of symbols

Now we consider sequences of wff's
and distinguish certain of them as proofs

Inference, the Hilbert way

One starts off with a set of axioms Ax
that is, wffs such as $X \Rightarrow (Y \Rightarrow X)$
where X, Y are propositional variables

... and three inference rules:

- **Axiom (AX)**: $\dfrac{}{A}$ where $A \in$ **AX**

- **Modus (Ponendo) Ponens (MP)**:
$$\frac{\begin{array}{l} A \\ A \Rightarrow B \end{array}}{B}$$

- **Substitution (SUB)**: $\dfrac{A}{A[X/B]}$
  where $A[X/B]$ denotes the formula obtained by replacing every occurrence of the propositional variable X in A by the wff B.

A **proof** is a sequence of wff's
such that each one is either an axiom
or follows from earlier wff's in the
sequence by application of MP or SUB

This is (almost) a recursive definition
if phrased right

An example of SUB:

$$(X \Rightarrow (Y \Rightarrow X)[X/(X \vee Y), Y/(Z \Rightarrow X)]$$

is defined to be

$$(X \vee Y) \Rightarrow ((Z \Rightarrow X) \Rightarrow (X \vee Y))$$

leading to the proof

$$\frac{(X \Rightarrow (Y \Rightarrow X)}{(X \vee Y) \Rightarrow ((Z \Rightarrow X) \Rightarrow (X \vee Y))}$$

An example of MP:

$$\frac{\begin{array}{l}(X \Rightarrow (Y \Rightarrow X)) \\ (X \Rightarrow (Y \Rightarrow X)) \Rightarrow (Y \Rightarrow (X \Rightarrow (Y \Rightarrow X)))\end{array}}{(Y \Rightarrow (X \Rightarrow (Y \Rightarrow X)))}$$

A **theorem** is the last wff in a proof

There's another way to characterise the proofs and the theorems

- Anything one can write down using the three rules is a proof (sufficiency).

- The only proofs are those sequences which can be obtained by doing this (necessity).

Here's a restricted way to get the theorems (I interpret the rules as applying to a *sequence* of wffs to form a supersequence)

Let $Inst$ be the transitive closure of Ax under SUB. It is easy to show $Inst = \{\langle D \rangle | \exists\, B \in \mathsf{wff}, X \in \mathsf{PV}, A \in \mathsf{Ax} : D = A[X/B]\}$

Let Pf be the transitive closure of $Inst$ under MP, and End(P) $\triangleq$ $P[Len(P)]$

Then $Thms = \{A \mid \exists\, P \in Pf : A = \mathsf{End}(P)\}$

Exercise: Show

Theorem: $Thms$ is the set of theorems of propositional logic

Exercise: Let Mp be the transitive closure of Ax under MP and AX. (Mp is a set of sequences.) Let Sub be the transitive closure of Mp under SUB and AX.
Show $Sub \neq Thms$.

This is an instance of a general phenomenon, that sets characterised one way can be shown to be buildable by using other operations or the same operations in another order

Another example: *Birkhoff's Theorem* which establishes the basis for equational logic and universal algebra

So, wff's and proofs may be considered as the transitive closure of a set under certain operations

When the operations are *constructors* that is, they retain the arguments somehow in the value (wff's contain argument wff's as subformulae; proofs contain the argument as initial segment) then induction over the constructors is valid for all objects in the transitive closure

For example, the formula-building function

$$A, B \mapsto (A \vee B)$$

is a constructor, since the arguments A and B form a part of the value $(A \vee B)$

A binary truth function is not a constructor
Why not? (Proof?)

What axiom systems are there for propositional logic?

A common set is

1: $p \Rightarrow (q \Rightarrow p)$
2: $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
3: $\neg\neg p \Rightarrow p$

Church, *Introduction to Mathematical Logic*, Princeton UP, 1956 uses this in the form

C.3: $((p \Rightarrow \bot) \Rightarrow \bot) \Rightarrow p$

because he defines $\neg p$ to be $(p \Rightarrow \bot)$ where $\bot$ is the logical constant whose value is always $False$

Lukasiewicz 1930 uses **1**, **2** and
L.3: $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$

Also, he suggests the set

L.II.1: $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
L.II.2: $(\neg p \Rightarrow p) \Rightarrow p$
L.II.3: $p \Rightarrow (\neg p \Rightarrow q)$

A famous set comes from
Whitehead and Russell,
Principia Mathematica, vol. 1
Cambridge UP, 1910.

WR.1: $(p \vee p) \Rightarrow p$
WR.2: $q \Rightarrow (p \vee q)$
WR.3: $(q \vee p) \Rightarrow (p \vee q)$
WR.4: $(q \Rightarrow r) \Rightarrow ((p \vee q) \Rightarrow (p \vee r))$

however, it's not complete

One must add to Whitehead and Russell's axioms the following six, which introduce the other connectives

WR.5: $(\neg p \vee q) \Rightarrow (p \Rightarrow q)$
WR.6: $(p \Rightarrow q) \Rightarrow (\neg p \vee q)$
WR.7: $(\neg p \vee \neg q) \Rightarrow \neg(p \wedge q)$
WR.8: $\neg(p \wedge q) \Rightarrow (\neg p \vee \neg q)$
WR.9: $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$
WR.10: $(p \equiv q) \Rightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$

Hilbert and Bernays,
Grundlagen der Mathematik I, Zweite Auflage
Springer 1968, p64 (1. Aufl. was 1934)

The king himself:
Frege, *Begriffschrift*, 1879

1, **2**, plus
F.3: $(p \Rightarrow (q \Rightarrow r)) \Rightarrow (q \Rightarrow (p \Rightarrow r))$
F.4: $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
F.5: $p \Rightarrow \neg\neg p$
F.6: $\neg\neg p \Rightarrow p$

A single axiom suffices!
S. Lesniewski, *Grundzüge eines neuen Systems der Grundlagen der Mathematik*, Fundamenta Mathematica 14 (1929)

Also with the Sheffer stroke, with rule $\dfrac{A \quad A|(B|C)}{C}$

(Nicod, *A reduction in the number of primitive propositions of logic*, Proc. Camb. Phil. Soc. 19, 1917)

Hilbert, *Grundlagen der Geometrie*, 1900
(also in Hilbert-Bernays, p69)

H.I. Implication **1.** $p \Rightarrow (q \Rightarrow p)$
2. $(p \Rightarrow (p \Rightarrow q)) \Rightarrow (p \Rightarrow q)$
3. $(p \Rightarrow q) \Rightarrow$
$((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$

H.II. Conjunction **1.** $p \wedge q \Rightarrow p)$
2. $p \wedge q \Rightarrow q$
3. $(p \Rightarrow q) \Rightarrow$
$((p \Rightarrow r) \Rightarrow (p \Rightarrow (q \wedge r)))$

H.III. Disjunction **1.** $p \Rightarrow (p \vee q)$
2. $q \Rightarrow (p \vee q)$
3. $(p \Rightarrow r) \Rightarrow$
$((q \Rightarrow r) \Rightarrow (p \vee r \Rightarrow r))$

H.IV. Equivalence **1.** $(p \equiv q) \Rightarrow (p \Rightarrow q)$
2. $(p \equiv q) \Rightarrow (q \Rightarrow p)$
3. $(p \Rightarrow q) \Rightarrow$
$((q \Rightarrow p) \Rightarrow (p \equiv q)$

Note I.3 is identical to 4

Hilbert's axioms (cont'd)

V. Negation **1.** $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$

2. $p \Rightarrow \neg\neg p$

3. $\neg\neg p \Rightarrow p$

Kleene, *Introduction to Metamathematics*
North-Holland 1971 (6th reprint of
1952 edition) gives

K.1.a: $p \Rightarrow (q \Rightarrow p)$
K.1.b: $(p \Rightarrow q) \Rightarrow ((p \Rightarrow (q \Rightarrow r)) \Rightarrow (p \Rightarrow r))$
K.2: MP (it's a rule!)
K.3: $p \Rightarrow (q \Rightarrow (p \wedge q))$
K.4.a: $p \wedge q \Rightarrow p$
K.4.b: $p \wedge q \Rightarrow q$
K.5.a: $p \Rightarrow p \vee q$
K.5.b: $q \Rightarrow p \vee q$
K.6: $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r))$
K.7: $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$
K.8: $\neg\neg p \Rightarrow p$

Note that many of these have occurred before

If K.8 is replaced by
K.9: $\neg p \Rightarrow (p \Rightarrow q)$
then the system corresponds to
intuitionistic propositional logic

Also, one can translate the axioms of Boolean Algebra into logic: there are two binary operations $\wedge$, $\vee$ and a unary $\neg$.

15, 16 $\wedge$, $\vee$ are associative
17, 18 $\wedge$, $\vee$ are commutative
19, 20 $\wedge$, $\vee$ distribute over each other
21, 22: $(p \vee q) \wedge p = p, (p \wedge q) \vee p = p$
23, 24: $(p \vee p) = p, (p \wedge p) = p$
25, 26: $p \vee \neg p = 1, p \wedge \neg p = 0$
27-30: $p \wedge 1 = p, p \vee 1 = 1, p \vee 0 = p, p \wedge 0 = 0$
31, 32: $\neg(p \wedge q) = (\neg p \vee \neg q), \neg(p \vee q) = (\neg p \wedge \neg q)$

One translates $X = Y$ into $(X \Rightarrow Y) \wedge (Y \Rightarrow X)$
Either $\top$, $\perp$ are logical constants,
or add $\perp$ and define $\top$ as $\neg\perp$
or define $\perp$ as $p \wedge \neg p$
(read this as a bootstrap)

Semantics

The semantics for classical propositional logic bases itself on *truth values* (Wittgenstein, *Logisch-Philosophische Abhandlungen*)

Propositions (wff's) can be either True or False (T or F; 1 or 0; $\top$ or $\bot$)

Semantics is compositional
the relation *subformula of* is well-founded
so we may use a recursive definition starting with the minimal subformulas, i.e., the propositional variables

One assigns truth values to the propositional variables and a recursive definition of truth value assigns each wff a truth value

That is, for each clause of the recursive definition of formula, one says how the result is true or false, given the possible values of its arguments

Operations: $$\begin{array}{lll} A, B & \mapsto & (A \vee B) \\ A, B & \mapsto & (A \wedge B) \\ A, B & \mapsto & (A \Rightarrow B) \\ A & \mapsto & (\neg A) \end{array}$$

So, A, B must be given their possible values ($\top$, $\bot$) and we must say what value $(A\ op\ B)$ has

This specifies $(A\ op\ B)$ as a binary function of these arguments

The arguments are truth-values as are the results

Hence these are *truth functions* and we have a *truth-functional semantics*

Tautologies are wff's which are always true no matter what values the variables take, e.g.,

A	$\Rightarrow$	(	B	$\Rightarrow$	A)
T	T		T	T	T
T	T		F	T	T
F	T		T	F	F
F	T		F	T	F

I got this table by considering all the possible combinations of T and F for A and B, and combining them using the basic Truth Tables for the connectives

Here are the truth tables for two connectives

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	$\neg A$
F	T
T	F

These are tables giving all possible values
of the function for all possible arguments

This is possible because the functions only have
finitely many argument combinations
and therefore only finitely many values

But I only gave the truth tables for one unary and one binary truth function

Why? Because they form a *complete set* of truth functions

That is, all binary truth functions may be obtained by composition from these two.

That says that all possible truth tables may be obtained by combining these two

Can you prove this statement above?

How many such functions are there?

OK, OK, here are the truth tables for the other two connectives

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

In fact, here's an even better exercise

Prove that you can obtain all unary and binary truth functions from the single

A	B	$A \mid B$
T	T	F
T	F	F
F	T	F
F	F	T

This is called Joint Denial or Sheffer Stroke, Sheffer's only notable contribution to logic, used by both Wittgenstein and Russell

Semantics: what it means, what you're trying to calculate by doing inference

All the axioms of Hilbert-style propositional logic are tautologies

and the rules MP, SUB preserve tautologies, that is,

(MP) if A is a tautology and
$A \Rightarrow B$ is a tautology then
so is B

(SUB) if A is a tautology, then
so is $A[X/B]$

Check this.

Thus, all theorems of Hilbert-style logic
are tautologies

But are all tautologies also theorems
of Hilbert-style logic?

Yes. This is called the Completeness Theorem
for Hilbert-style propositional logic

You could perhaps prove it?

(Looking it up is easier)

But I'm going to do Prawitz-style
Gentzen-style natural deduction

Prawitz has fewer axioms

In fact, he doesn't have any

But he has lots of rules —
introduction and elimination rules
for each logical constant
(operator of propositional logic)

And he has a way of marking formulae
as *assumptions* early in a proof
and *discharging* them later

In a natural deduction, one *assumes* certain formulae, and then uses the rules to prove other formulae.
One may write an already written formula or a substitution instance thereof or one may write a formula which is an instance of a conclusion of a rule of which one has already written the instances

There are ways in which assumptions may be *discharged* (eliminated)

A theorem is a formula obtained by a proof in which all assumptions have been discharged

Here's a proof of a theorem:

$$\frac{\begin{array}{c}[A]\\ A\end{array}}{A \Rightarrow A}$$

Here, $[A]$ indicates an assumption of A that has been later discharged

This proof of $A \Rightarrow A$ is an instance of the rule $\Rightarrow$-introduction:

$$\frac{\begin{array}{c}[A]\\ B\end{array}}{A \Rightarrow B}$$

This says, from A and B, write $A \Rightarrow B$ and discharge all occurences of A above

Here's a proof of the Hilbert axiom
$A \Rightarrow (B \Rightarrow A)$ using this rule:

$$\frac{\begin{array}{c}[B] \\ [A] \\ B \Rightarrow A\end{array}}{A \Rightarrow (B \Rightarrow A)}$$

(I'm messing around with parentheses
to make it more readable)

Here, B is assumed, then A.
$B \Rightarrow A$ is concluded,
discharging assumptions of B
Finally, $A \Rightarrow (B \Rightarrow A)$ is concluded,
discharging assumptions of A.

So there are no assumptions left,
and the conclusion is thus a theorem

So what (propositional) rules are there?

(&-intro) $\dfrac{A \quad B}{A \wedge B}$ (&-elim) $\dfrac{A \wedge B}{A}$ $\dfrac{A \wedge B}{B}$

($\vee$-intro) $\dfrac{A}{A \vee B}$ $\dfrac{A}{A \vee B}$

($\vee$-elim)

$$\dfrac{A \vee B \qquad \begin{matrix}[A] \\ C\end{matrix} \qquad \begin{matrix}[B] \\ C\end{matrix}}{C}$$

Note that these rules build proof *trees*, not sequences, since proof branches converge in certain rules. The root is the theorem.

(⇒-intro) $\dfrac{\begin{array}{c}[A]\\ B\end{array}}{A \Rightarrow B}$ (⇒-elim) $\dfrac{A \quad A \Rightarrow B}{B}$

$(\neg A)$ is defined to be the formula $(A \Rightarrow \bot)$

$(\bot_{\mathsf{I}})$ $\dfrac{\bot}{A}$ $(\bot_{\mathsf{C}})$ $\dfrac{\begin{array}{c}[\neg A]\\ \bot\end{array}}{A}$

A restriction on both $\bot$ rules is that
A is different from $\bot$

A restriction on $\bot_{\mathsf{C}}$ is that
A is not of the form $B \Rightarrow \bot$
This is only for convenience

Show that if A has the form $\neg B$ in $\bot_{\mathsf{C}}$
that there's another way of deriving
the conclusion

Note that $\perp_{\mathsf{C}}$ subsumes $\perp_{\mathsf{I}}$

If $\perp_{\mathsf{C}}$ is used, the theorems are those of classical propositional logic

If $\perp_{\mathsf{I}}$ is used, the theorems are those of intuitionistic propositional logic

The difference is just that of how negation is treated

Compare with Kleene's axiomatisation of propositional logic which includes
K.8: $\neg\neg p \Rightarrow p$.
If one replaces K.8 with K.9: $\neg q \Rightarrow (p \Rightarrow q)$, intuitionistic propositional logic results

Gentzen-style natural deduction is also complete. That is, the theorems are precisely the tautologies

An exercise: as before, show that the rules preserve tautologies (um, except for the $\perp$-rules)

Gentzen-style proofs are written as a tree with the conclusion as root.
Assumptions are discharged on all branches *above* a given node (conclusion)

But one may write these trees linearly.
Here's a recursive definition (a little hidden)
One may write the conclusion first, and the premises in (arbitrary) linear order below. Below each premise, and before the next, occurs the proof of this premise

This is *Lamport's hierarchical method*

Here are the Lamport-hierarchical versions of the rules, as used in TLA proofs

$\langle 1 \rangle 1.$ $A \wedge B$

Proof:

$\langle 2 \rangle 1.$ A

$\langle 2 \rangle 2.$ B

$\langle 2 \rangle 3.$ Q.E.D.

Proof: &-intro. $\square$

$\langle 1 \rangle 1.$ A

Proof:

$\langle 2 \rangle 1.$ $A \wedge B$

$\langle 2 \rangle 2.$ Q.E.D.

Proof: &-elim-left. $\square$

$\langle 1 \rangle 1.$ B

Proof:

$\langle 2 \rangle 1.$ $A \wedge B$

$\langle 2 \rangle 2.$ Q.E.D.

Proof: &-elim-right. $\square$

$\langle 1 \rangle$1. $A \Rightarrow B$

Proof:

ASSUME A

PROVE B

$\langle 2 \rangle$1. B

Proof: (Use A freely). $\square$

$\langle 2 \rangle$2. Q.E.D.

Proof: $\Rightarrow$-intro. $\square$

$\langle 1 \rangle$1. B

Proof:

$\langle 2 \rangle$1. A

$\langle 2 \rangle$2. $A \Rightarrow B$

$\langle 2 \rangle$3. Q.E.D.

Proof: $\Rightarrow$-elim. $\square$

$\langle 1 \rangle 1.$ $A \vee B$

Proof:

$\langle 2 \rangle 1.$ A

$\langle 2 \rangle 2.$ Q.E.D.

Proof: $\vee$-intro-left. $\square$

$\langle 1 \rangle 1.$ $A \vee B$

Proof:

$\langle 2 \rangle 1.$ B

$\langle 2 \rangle 2.$ Q.E.D.

Proof: $\vee$-intro-right. $\square$

$\langle 1 \rangle 1.$ C

Proof:

$\langle 2 \rangle 1.$ $A \vee B$

$\langle 2 \rangle 2.$ $A \Rightarrow C$

$\langle 2 \rangle 3.$ $B \Rightarrow C$

$\langle 2 \rangle 4.$ Q.E.D.

Proof: $\vee$-elim. $\square$

How did I do this? Notice that from $\dfrac{\begin{matrix}[A]\\ \vdots \\ C\end{matrix}}{}$

we may simply conclude $\dfrac{}{A \Rightarrow C}$ by $\Rightarrow$-I

so that if I may prove the former, I may also prove the latter. I just added this extra step for both $\dfrac{\begin{matrix}[A]\\ \vdots \\ C\end{matrix}}{}$ and $\dfrac{\begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{}$

Here are the two $\perp$ rules

One or the other needs to be included depending on what logic you want

$\langle 1 \rangle$1. A

Proof:

$\langle 2 \rangle$1. $\perp$

$\langle 2 \rangle$2. Q.E.D.

Proof: $\perp_{\text{I}}$. $\square$

$\langle 1 \rangle$1. A

Proof:

ASSUME $A \Rightarrow \perp$

PROVE $\perp$

$\langle 2 \rangle$1. $\perp$

Proof: (Use $A \Rightarrow \perp$ freely). $\square$

$\langle 2 \rangle$2. Q.E.D.

Proof: $\perp_{\text{C}}$. $\square$

In principle, by using these rules and these rules only, you will be able to prove all the tautologies and do any propositional inference that you need to

The End