# Formal Proof Systems for First-Order Logic

Assaf Kfoury

First created: September 3, 1974
Last modified: July 10, 2018

## Contents

# 1 Preamble

I wrote the bulk of these notes for a one-semester seminar in Fall 1974, which I taught when I was a postdoc at MIT shortly after I completed my PhD. I initially typed them using an IBM Selectric typewriter at a time when electronic typesetting hardly existed. In the mid-1980's, I re-typed them using LaTeX (which was only developed in the early 1980's). Over the years, I periodically referred to them in courses I taught at different institutions, typically in various courses related to formal methods in computer science. I also made slight adjustments, in particular in relation to books that did not exist in the mid-1970's and books that were later re-printed by new publishers (because their original publishers had gone out of business). I used the notes again for a one-semester course on mathematical logic in Fall 1995, in the Mathematics Dept at Boston University.

Certain concepts and results of mathematical logic have been viewed and used differently over the years. Some have gained in importance, others have lost much of their centrality. The perspective in these notes is very much from the 1970's and 1980's, which I learned from my own teachers in graduate school. I did not try to change that pespective whenever I went back and re-read my notes, partly because I wanted to avoid the effort of recasting the whole document and partly because I thought there is a value in showing how the field has shifted since the 1970's and 1980's – this will be clear from a careful comparison with current presentations of formal proof systems for first-order logic. At the end, even though the presentation in these notes may be obsolete or 'old-fashioned' in places, I believe much of the contents will remain part of the canon of mathematical logic.

I give a few examples of that shift in perspective:

1. Which comes first, *compactness* or *completeness*?

Many now view that *compactness* comes first, which is also my view. It used to be the other way around. Additional comments on this reversal between *compactness* or *completeness* are in my notes *Compactness and Completeness of Propositional Logic and First-Order Logic* (click here to download).

2. What else is there to do of practical significance after the *NP-completeness* of propositional satisfiability?

It turns there is plenty to do. Witness the explosion in research related to what are called *SAT Solvers* and *SMT Solvers* in the last two or three decades. This is research that spans from the very theoretical to the very practical.

3. Is it possible to do good research in *mathematical logic* without knowing anything about *computer science* – and vice-versa, good research in *computer science* without knowing anything about *mathematical logic*?

The two fields were always recognized as being somehow related, if only because most of the pioneers of computer science in the 1950's and 1960's, and their precursors in the 1930's and 1940's when there was no separate discipline called 'computer science', were trained as mathematical logicians. But the relationship seemed similar to that between mathematics and engineering, say, in that the

former simply provided the formulas and formalisms to do the latter. One can be an excellent engineer without contributing anyting new to mathematics, and vice-versa. However, what has gradually emerged in recent decades is that, in many core areas of computer science, good research is in fact good research *in* mathematical logic. The integration between the two fields – at least in such areas as foundations of programming languages, model checking, automated proof assistants, and many others – is such that it is not possible to dissociate between the two. It is no longer an external relationship, as it is between mathematics and engineering, but an increasingly organic and mutually beneficial interaction. Additional comments on the deepening integration between mathematical logic and computer sicence are in my article *Mathematical Logic in Computer Science* (click here to download).

## 2 Hilbert-Style Proof Systems

A deductive calculus such as the one given in Enderton's book, Section 2.4, is often called a *Hilbert-style proof* (or *axiomatic*) *system* — or more simply, a *Hilbert system*. But there are many variations of Hilbert systems, each defined by a collection of *axiom schemes* and a collection of *inference rules*. It is a matter of taste and convenience how we choose axiom schemes and inference rules (so that the resulting system is both sound and complete).

The system in Enderton's book, as well as all the systems for first-order logic except for one (System F) which we list below, include among the logical axioms "all generalizations of tautologies" or "all closed tautologies" or "all tautologies". A *tautology* means a substitution instance of a propositional (or sentential) tautology, just as it is defined in Enderton's, page 106. Propositional tautologies in Enderton's are defined semantically, page 34. But it is also possible to set up a Hilbert system for propositional logic, which derives exactly all the propositional tautologies, i.e. so that the resulting proof system is "sound" and "complete". Enderton does not present any deductive calculus for propositional logic and, therefore, he does not need to prove any soundness and completeness result for it; he restricts his presentation of propositional logic to its semantics.

### A Hilbert system for propositional logic

$\alpha$, $\beta$ and $\gamma$ denote arbitrary propositional wff's.

- *Axiom schemes*
  - $(\alpha \to (\beta \to \alpha))$ ;
  - $((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$ ;
  - $(\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta)$ .
- *Inference rules*
  - Modus Ponens: $\dfrac{\alpha \qquad \alpha \to \beta}{\beta}$ .

The preceding proof system for propositional logic can be found in many texts, for example in [12]. It is not the only Hilbert system for propositional logic; others are given in Sections 1.10, 1.14, and 1.15 in [2], and in Section 19 in [9].[1]

We next list a few alternative formulations of Hilbert-style proof systems for first-order logic. We start with a system which is very close to the system in Enderton's book.

### System A

Use the following convention: $\varphi(x)$ denotes any wff which has no free variable other than $x$, and $\varphi(c)$ denotes the result of substituting the constant symbol $c$ for every free occurrence of $x$ in $\varphi(x)$. $\alpha$, $\psi$ and $\theta$ denote arbitrary wff's (satisfying whatever restrictions are added).

[1] Although the Hilbert system for propostional logic in [9] has relatively many axiom schemes, a total of ten, it has the advantage that by omitting just one of them (corresponding to the law of "excluded middle") the result is a Hilbert system for intuitionistic propositional logic – more on this in later sections.

- *Axiom schemes*

  A1 All closed tautologies;

  A2 $(\forall x\ \varphi(x)) \to \varphi(c)$ ;

  A3 $\varphi(c) \to (\exists x\ \varphi(x))$ ;

  A4 All generalizations of $x \approx x$ ;

  A5 All generalizations of $x \approx y \to (\alpha \to \alpha')$, where $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing zero or more occurrences of $x$ by $y$.

- *Inference rules*

  A6 Modus Ponens: $\dfrac{\psi \qquad \psi \to \theta}{\theta}$ ;

  A7 Generalization: $\dfrac{\psi \to \varphi(c)}{\psi \to (\forall x\ \varphi(x))}$ provided constant $c$ does not occur in $\varphi(x)$ nor in $\psi$;

  A8 Generalization: $\dfrac{\varphi(c) \to \psi}{(\exists x\ \varphi(x)) \to \psi}$ provided constant $c$ does not occur in $\varphi$ nor in $\psi$.

Note that the axiom scheme A2 above is more restrictive than the one on page 104 of Enderton's book, which is:

$$(\forall x\ \alpha) \to \alpha^x_t \text{ provided } t \text{ is substitutable for } x \text{ in } \alpha$$

where $t$ is not restricted to a constant symbol and, therefore, one has to worry about capture of free variables in $t$ after substituting it for $x$ in $\alpha$. Moreover, Enderton allows $\alpha$ to have free variables other than $x$.

## System B

System B is a variation on System A, but simpler, with the same notational conventions.

- *Axiom schemes*

  B1 All closed tautologies;

  B2 $(\forall x\ \varphi(x)) \to \varphi(c)$ ;

  B3 All generalizations of $x \approx x$ ;

  B4 All generalizations of $x \approx y \to (\alpha \to \alpha')$, where $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing zero or more occurrences of $x$ by $y$.

- *Inference rules*

  B5 Modus Ponens: $\dfrac{\psi \qquad \psi \to \theta}{\theta}$ ;

  B6 Generalization: $\dfrac{\varphi(c) \to \psi}{(\exists x\ \varphi(x)) \to \psi}$ provided $c$ does not occur in $\varphi$ nor in $\psi$ .

## System C

System C is a variation on System B, exhibiting a useful symmetry for some arguments, with the same notational conventions as before.

- *Axiom schemes*

  C1 All closed tautologies;

  C2 All generalizations of $x \approx x$ ;

  C3 All generalizations of $x \approx y \to (\alpha \to \alpha')$, where $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing zero or more occurrences of $x$ by $y$.

- *Inference rules*

  C4 Modus Ponens: $\dfrac{\psi \qquad \psi \to \theta}{\theta}$ ;

  C5 Generalization: $\dfrac{\varphi(c) \to \psi}{(\forall x\ \varphi(x)) \to \psi}$ ;

  C6 Generalization: $\dfrac{\varphi(c) \to \psi}{(\exists x\ \varphi(x)) \to \psi}$ provided $c$ does not occur in $\varphi$ nor in $\psi$ .

## System D

System D is a variation on System C, with the same notational conventions. But note that System D does *not* include Modus Ponens as one of its inference rules.

- *Axiom schemes*

  D1 All closed tautologies;

  D2 All generalizations of $x \approx x$ ;

  D3 All generalizations of $x \approx y \to (\alpha \to \alpha')$, where $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing zero or more occurrences of $x$ by $y$.

- *Inference rules*

  D4 Generalization: $\dfrac{((\forall x\ \varphi(x)) \to \varphi(c)) \to \psi}{\psi}$ ;

  D5 Generalization: $\dfrac{((\exists x\ \varphi(x)) \to \varphi(c)) \to \psi}{\psi}$ provided $c$ does not occur in $\varphi$ nor in $\psi$.

**Reference**: Without the axiom schemes for the equality symbol $\approx$, Systems A, B, C, and D are basically the systems given in Chapter VIII of [15]. In [15], all the logical connectives $\{\neg, \vee, \wedge, \to\}$ and both quantifiers $\{\exists, \forall\}$ are included as primitive symbols in the syntax of wff's, in contrast to Enderton who includes only $\{\neg, \to, \forall\}$ as primitives, leaving the other symbols $\{\vee, \wedge, \exists\}$ as abbreviations.

**Exercise 1**: Show that (i) the proof system in Enderton's book, in Section 2.4, is equivalent to System A, (ii) System A is equivalent to System B, (iii) System B is equivalent to System C, and (iv) System C is equivalent to System D. Thus, all of these 5 formal proof systems are equivalent, i.e. everything deducible in one is deducible in the other and vice-versa.

## System E

System E is again very close to the system in Enderton's book. $\varphi$ and $\psi$ are arbitrary wff's, $x$ and $y$ arbitrary variables, and $t$ an arbitrary term.

- *Axiom schemes*

  E1 All tautologies;

  E2 $(\forall x\ (\varphi \to \psi)) \to (\varphi \to (\forall x\ \psi))$ provided variable $x$ is not free in $\varphi$ ;

  E3 $(\forall x\ \varphi) \to \varphi_t^x$ provided $t$ is substitutable for $x$ in $\varphi$ ;

  E4 $x \approx x$ ;

  E5 $x \approx y \to (t \approx t')$, where $t'$ is obtained from $t$ by replacing one occurrence of $x$ by $y$ ;

  E6 $x \approx y \to (\varphi \to \varphi')$, where $\varphi$ is atomic and $\varphi'$ is obtained from $\varphi$ by replacing one occurrence of $x$ by $y$ ;

- *Inference rules*

  E7 Modus Ponens: $\dfrac{\varphi \qquad \varphi \to \psi}{\psi}$ ;

  E8 Generalization: $\dfrac{\varphi}{(\forall x\ \varphi)}$ .

**Reference**: System E is the system in Chapter 1 of [3]. The primitive symbols in [3] are $\{\neg, \wedge, \forall\}$, so that $(\varphi \to \psi)$ (in the axiom schemes and inference rules) is the usual abbreviation for $\neg(\varphi \wedge \neg\psi)$.

**Exercise 2**: Show the proof system in Enderton's book, in Section 2.4, is equivalent to System E.

### System F

By comparison to the preceding systems, System F has fewer axiom schemes but more inference rules. Its single propositional axiom scheme and its many inference rules make it very different from the preceding Hilbert systems, and in fact quite close to a Gentzen system (more on this in Section 4).

- *Axiom schemes*

  F1 $\neg\alpha \vee \alpha$ ;

  F2 $\alpha_t^x \to (\exists x\ \alpha)$, provided $t$ is substitutable for $x$ in $\alpha$;

  F3 $x \approx x$

  F4 $(x_1 \approx y_1 \to (\cdots \to (x_n \approx y_n \to fx_1 \cdots x_n \approx fy_1 \cdots y_n) \cdots))$ , where $f$ is any function symbol of arity $n \geq 1$ ;

  F5 $(x_1 \approx y_1 \to (\cdots \to (x_n \approx y_n \to (Px_1 \cdots x_n \to Py_1 \cdots y_n)) \cdots))$ , where $P$ is any predicate symbol of arity $n \geq 1$ .

- *Inference rules*

  F6 Expansion: $\dfrac{\alpha}{\beta \vee \alpha}$ ;

  F7 Contraction: $\dfrac{\alpha \vee \alpha}{\alpha}$ ;

  F8 Associativity: $\dfrac{\alpha \vee (\beta \vee \gamma)}{(\alpha \vee \beta) \vee \gamma}$ ;

  F9 Cut Rule: $\dfrac{\alpha \vee \beta \qquad \neg\alpha \vee \gamma}{\beta \vee \gamma}$ ;

  F10 $\exists$-Introduction Rule: $\dfrac{\alpha \to \beta}{(\exists x\ \alpha) \to \beta}$ provided $x$ does not occur free in $\beta$.

**Reference**: System F is basically the system in Chapter 2 of [14]. The primitive symbols in [14] are $\{\neg, \vee, \exists\}$, so that $(\alpha \to \beta)$ is the usual abbreviation for $(\neg\alpha \vee \beta)$.

**Exercise 3**: Show the proof system in Enderton's book, in Section 2.4, is equivalent to System F.

## 3 Tableaux Systems, Gentzen Systems, Natural Deduction

There are formal proof systems other than Hilbert-style for classical logic, whether propositional, first-order, or higher-order. Among these alternatives are *tableaux*, *Gentzen*, and *natural deduction* systems. None of these are discussed in Enderton's book.

In a Hilbert system, finding a derivation for a wff may be a tricky business, as one has to guess which axiom and which inference rule to use without systematic reliance on the syntax of the given wff. In tableaux, Gentzen, and natural deduction systems, there is less of this kind of guesswork, and derivations (or refutations) are largely syntax-directed. In particular, these alternative systems are more suitable for automatic theorem-proving[2] and allow for elegant presentations of intuitionistic logic[3]. One distinctive feature of these systems, not shared by Hilbert systems, is that they systematically and more efficiently produce a formal proof for a given wff — if it is indeed a valid wff, and if it is not, these systems will sometimes (but not always!) produce a counterexample to its validity. (Of course, we can also use a Hilbert system to produce a formal proof for a valid wff, typically by some exhaustive listing of all possible derivations, but this is not efficient at all!) Actually, in some variants of these alternative proof systems, it becomes very clear that a formal proof is basically a record of "an unsuccessful attempt to produce a counterexample". This is a simple idea, but it seems to be an insight of considerable importance in many applications.[4]

Not to give the wrong impression, there have been attempts to do automatic theorem-proving as well as presentations of intuitionistic logic based on Hilbert systems (of one form or another), but these are generally ill-suited for a computational task and often seem to obscure it by syntactic details. Of course, there are also subjective considerations (e.g. personal taste, familiarity, etc.) in choosing an appropriate proof system to work with. Moreover, although Hilbert systems are "inefficient and barbarously unintuitive",[5] they have advantages. First, the simplicity of their relatively few inference rules makes them suitable for encoding into arithmetic.[6] Second, it is relatively easy to tamper with the axiom schemes of Hilbert systems in order to adapt them to non-classical logics.[7]

Concerning tableaux systems, Smullyan gives a particularly lucid presentation in [15] (where tableaux are called "analytic tableaux") for classical logic, both propositional and first-order. Bell and Machover in [2], and then more recently Nerode and Shore in [12], also give presentations of classical logic and intuitionistic logic, both propositional and first-order, based on tableaux.

I will not say anything more about tableaux systems, in part because they are really duals of Gentzen systems: Whereas a Gentzen system systematically searches for a formal *proof* in *tree* form, a tableaux system systematically searches for a *refutation* in upside-down tree form. A node in a Gentzen proof tree corresponds to a branch in a tableau (more or less), and the Elimination Theorem for tableaux corresponds to Gentzen's Hauptsatz — for a definition of all these concepts, see the forementioned references (in relation to tableaux sysems) and the references in Section 4 (in relation to Gentzen systems). One of the best expositions of the relationship between tableaux

[2] Automatic theorem-proving is a very active research area in computer science, where the "resolution" methods are essentially based on Gentzen systems or tableaux systems. For further reading on this, see [6] or [13] or [4].

[3] Intuitionistic logic is important in several foundational areas of computer science, notably in relation to typed $\lambda$-calculi and programming language theory.

[4] Further elaboration on this last point can be found in Chapter 14 of [13].

[5] Direct quote from [8], page 32.

[6] Without arithmetization of syntax we cannot reach Gödel's Incompleteness Theorem. See Ch. 3 in Enderton's.

[7] One such logic is intuitionism, for which we nevertheless prefer to use a proof system based on natural deduction.

and Gentzen systems can be found in [15]. The view that tableaux are just a variant of Gentzen systems is discussed in some detail in [16].

Section 4 and Section 5 present a Gentzen system and a natural-deduction system, respectively, for classical logic.

Section 6 will be devoted to intuitionistic logic. Formal proof systems for intuitionism can be of the Hilbert, or tableaux, or Gentzen, or natural-deduction variety. However, as already indicated, Hilbert systems are the least capable of revealing the computational aspects of the logic and its connections with typed $\lambda$-calculi.[8] By the "computational" aspects we mean this: When confronted with a sentence $\sigma$, instead of asking "when is $\sigma$ true?" or "when is $\sigma$ derivable?", we ask "what is a *proof* of $\sigma$?". While tableaux and Gentzen systems are better adapted to the task than Hilbert systems, the simplest way to consider this computational content of intuitionism is to use natural deduction. In particular, using natural deduction, it is easy to exhibit the so-called *Curry-Howard isomorphism* between intuitionistic logics and typed $\lambda$-calculi ("wff's and types are the same, proofs and $\lambda$-terms are the same"). More can be found in the early chapters of [7] on the beneficial effects of natural deduction.

The proof system in Section 6 will therefore be the natural-deduction system in Section 5 appropriately restricted to intuitionistic logic, both propositional and first-order.

[8] A presentation of Hilbert systems for intuitionism can be found in Sections 9.8 and 9.9 of [2], or in Sections 19 and 23 of [9]. One advantage of the presentation in [9] is that it is extendable to a Hilbert system for classical logic by adding just one axiom scheme, namely $(\neg\neg\alpha \to \alpha)$ or $(\neg\alpha \vee \alpha)$, the law of "excluded middle" – see Section 6.

# 4 Gentzen Systems

We need some preliminary definitions. A *sequent* is a pair of finite (possibly empty) sequences of wff's, say $\Gamma = \gamma_1, \ldots, \gamma_\ell$ and $\Delta = \delta_1, \ldots, \delta_m$, which we write as $\Gamma|\Delta$ or as $\gamma_1, \ldots, \gamma_\ell|\delta_1, \ldots, \delta_m$. The first part $\Gamma$ is the *antecedent* of the sequent, and the second part $\Delta$ the *succedent*. If $\Gamma$ is empty, we write $|\Delta$ for the sequent; if $\Delta$ is empty, we write $\Gamma|$; and if both are empty, we write $|$.

For an intuitive understanding of the axiom scheme and inference rules below, keep in mind the following: If $\ell, m \geqslant 1$, the sequent $\gamma_1, \ldots, \gamma_\ell|\delta_1, \ldots, \delta_m$ will have the same meaning as the wff $\gamma_1 \wedge \cdots \wedge \gamma_\ell \to \delta_1 \vee \ldots \vee \delta_m$. More precisely, given an interpretation $(\mathfrak{A}, s)$, i.e. a structure $\mathfrak{A}$ together with a valuation of the variables $s : V \to |\mathfrak{A}|$, $(\mathfrak{A}, s)$ satisfies the sequent $\gamma_1, \ldots, \gamma_\ell|\delta_1, \ldots, \delta_m$ iff

$$(\mathfrak{A}, s) \models \gamma_1 \wedge \cdots \wedge \gamma_\ell \to \delta_1 \vee \ldots \vee \delta_m$$

This extends to the case when $\ell = 0$ or $m = 0$: If $\ell = 0$, the conjunction $\gamma_1 \wedge \cdots \wedge \gamma_\ell$ is viewed as "true" and the sequent is equivalent to $\delta_1 \vee \ldots \vee \delta_m$; if $m = 0$, the disjunction $\delta_1 \vee \ldots \vee \delta_m$ is viewed as "false" and the sequent is equivalent to $\neg(\gamma_1 \wedge \cdots \wedge \gamma_\ell)$ or $\neg\gamma_1 \vee \cdots \vee \neg\gamma_\ell$; if $\ell = m = 0$, the sequent $|$ is unsatisfiable.

### About notation

In Kleene's presentation [9], on which this section is based, as well as in many other presentations of Gentzen systems (e.g. see [6] or [15]), a sequent is written as $\Gamma \rightarrow \Delta$ (with a boldface arrow) and our arrow "$\to$" (not boldface) is the same as their "$\supset$". To avoid confusion with our "$\to$", we use "$|$" (boldface bar) instead of "$\rightarrow$" in sequents. The notation is this section is similar (but not quite identical) to Dummett's [5], which uses another symbol yet, namely ":", to separate the two parts of a sequent. (We cannot use ":" as the sequent separator because we will need it for another purpose when we consider intuitionistism and its connection to typed $\lambda$-calculi.)

In recent years, some people have started to use "$\vdash$" to separate the two parts of a sequent (e.g. see Chapter 5 in [7]). This has been a common practice, for example, when a type-inference system is set up for a typed $\lambda$-calculus, where an expression of the form "$A \vdash M : \tau$" can be viewed as a sequent. This is perhaps unfortunate — or, in any case, it goes against the traditional practice of reserving "$\vdash$", a symbol outside the syntax of formal expressions, to assert that a formal expression can be derived using axioms and inference rules. What is a convenient shorthand to say that a "sequent with antecedent $\Gamma$ and succedent $\Delta$ is derivable"? In our notation, we write $\vdash \Gamma|\Delta$ , and in Kleene's $\vdash \Gamma \rightarrow \Delta$ . But it is clearly confusing to write $\vdash \Gamma \vdash \Delta$ , where the two occurrences of $\vdash$ mean two different things.

The symbol "$|$" is not in the syntax of wff's, but in the syntax of sequents. The rules of the Gentzen system below transform formal expressions that are sequents into other such formal expressions.

It is easier to see the organization of a Gentzen system by first considering the simpler case of propositional logic. We later point out how to extend the system for the case of first-order logic.

### Propositional logic

$\Gamma$, $\Delta$, $\Theta$, and $\Lambda$ range over finite sequences of zero or more wff's. $\alpha$, $\beta$, $\gamma$ and $\delta$ range over the set of wff's. There is only one axiom scheme, and many inference rules. The latter are divided into

*logical* and *structural*. All logical rules are "introduction" rules, in the sense that they introduce one of the logical connectives $\to, \wedge, \vee, \neg$, on the left or on the right of a sequent, and they are thus given the suggestive names $(\to|)$, $(\wedge|)$, $(\vee|)$, $(\neg|)$ (introduction on the left) and $(|\to)$, $(|\wedge)$, $(|\vee)$, $(|\neg)$ (introduction on the right).

- *Axiom scheme* $\alpha \mid \alpha$
- *Logical inference rules*
  - introduction of $\to$

$$\frac{\Delta \mid \Lambda, \alpha \qquad \beta, \Gamma \mid \Theta}{\alpha \to \beta, \Delta, \Gamma \mid \Lambda, \Theta} \ (\to|) \qquad\qquad \frac{\alpha, \Gamma \mid \Theta, \beta}{\Gamma \mid \Theta, \alpha \to \beta} \ (|\to)$$

  - introduction of $\wedge$

$$\frac{\alpha, \Gamma \mid \Theta}{\alpha \wedge \beta, \Gamma \mid \Theta} \ (\wedge|) \qquad \frac{\beta, \Gamma \mid \Theta}{\alpha \wedge \beta, \Gamma \mid \Theta} \ (\wedge|) \qquad \frac{\Gamma \mid \Theta, \alpha \qquad \Gamma \mid \Theta, \beta}{\Gamma \mid \Theta, \alpha \wedge \beta} \ (|\wedge)$$

  - introduction of $\vee$

$$\frac{\alpha, \Gamma \mid \Theta \qquad \beta, \Gamma \mid \Theta}{\alpha \vee \beta, \Gamma \mid \Theta} \ (\vee|) \qquad \frac{\Gamma \mid \Theta, \alpha}{\Gamma \mid \Theta, \alpha \vee \beta} \ (|\vee) \qquad \frac{\Gamma \mid \Theta, \beta}{\Gamma \mid \Theta, \alpha \vee \beta} \ (|\vee)$$

  - introduction of $\neg$

$$\frac{\Gamma \mid \Theta, \alpha}{\neg\alpha, \Gamma \mid \Theta} \ (\neg|) \qquad\qquad \frac{\alpha, \Gamma \mid \Theta}{\Gamma \mid \Theta, \neg\alpha} \ (|\neg)$$

- *Structural inference rules*
  - weakening

$$\frac{\Gamma \mid \Theta}{\gamma, \Gamma \mid \Theta} \ (\mathtt{W}|) \qquad\qquad \frac{\Gamma \mid \Theta}{\Gamma \mid \Theta, \gamma} \ (|\mathtt{W})$$

  - contraction

$$\frac{\gamma, \gamma, \Gamma \mid \Theta}{\gamma, \Gamma \mid \Theta} \ (\mathtt{C}|) \qquad\qquad \frac{\Gamma \mid \Theta, \gamma, \gamma}{\Gamma \mid \Theta, \gamma} \ (|\mathtt{C})$$

– exchange

$$\frac{\Delta, \delta, \gamma, \Gamma \mid \Theta}{\Delta, \gamma, \delta, \Gamma \mid \Theta}\ (\mathtt{E}|) \qquad\qquad \frac{\Gamma \mid \Lambda, \gamma, \delta, \Theta}{\Gamma \mid \Lambda, \delta, \gamma, \Theta}\ (|\mathtt{E})$$

– cut

$$\frac{\Delta \mid \Lambda, \gamma \qquad \gamma, \Gamma \mid \Theta}{\Delta, \Gamma \mid \Lambda, \Theta}\ (\mathtt{Cut})$$

Let $G_0$ denote the Gentzen system described above for propositional logic. In the examples to follow, a double line in a derivation (with the citation of a rule) stands for zero or more applications of the weakening, contraction, and exchange rules (following the application of the cited rule).

**Example 1.** For arbitrary wff's $\alpha$ and $\beta$, the following is a valid derivation in $G_0$:

$$\dfrac{\dfrac{\dfrac{\alpha \mid \alpha}{\alpha, \neg\alpha \mid \beta}\ (\neg|)}{\neg\alpha \mid \alpha \to \beta}\ (|\to)}{\mid \neg\alpha \to (\alpha \to \beta)}\ (|\to)$$

**Example 2.** For an arbitrary wff $\alpha$, the following are valid derivations in $G_0$:

$$\dfrac{\dfrac{\alpha \mid \alpha}{\mid \alpha, \neg\alpha}\ (|\neg)}{\mid \alpha \vee \neg\alpha}\ (|\vee) \qquad\qquad \dfrac{\dfrac{\dfrac{\alpha \mid \alpha}{\mid \alpha, \neg\alpha}\ (|\neg)}{\neg\neg\alpha \mid \alpha}\ (\neg|)}{\mid \neg\neg\alpha \to \alpha}\ (|\to)$$

## First-order logic

The system for propositional logic is extended by adding rules for the quantifiers and, if an equality symbol $\approx$ is included in the syntax of wff's, axiom schemes and/or rules for equality. The simplest here, for purposes of comparison with the systems in Section 2 and Section 5, is to have only axiom schemes for equality.[9] As in Section 2 and Enderton's book (page 105), $\alpha_t^x$ is the wff obtained from wff $\alpha$ by substituting every free occurrence of $x$ by the term $t$, provided the substitution is legal (i.e. no free variable in $t$ is captured by a quantifier in $\alpha$). Note the proviso "$y$ not free in $\Gamma$ and $\Theta$" in the $(|\forall)$ and $(\exists|)$ rules.

[9] In [9] the equality symbol in not included in the syntax of wff's. The axiom schemes we choose for equality here are basically those in [6], Section 6.3.

- *Inference rules for quantifiers*
  - introduction of $\forall$

$$\frac{\alpha_t^x, \Gamma \mid \Theta}{(\forall x\, \alpha), \Gamma \mid \Theta}\ (\forall|) \qquad \frac{\Gamma \mid \Theta, \alpha_y^x}{\Gamma \mid \Theta, (\forall x\, \alpha)}\ (|\forall)$$

($y$ not free in $\Gamma$ and $\Theta$)

  - introduction of $\exists$

$$\frac{\alpha_y^x, \Gamma \mid \Theta}{(\exists x\, \alpha), \Gamma \mid \Theta}\ (\exists|) \qquad \frac{\Gamma \mid \Theta, \alpha_t^x}{\Gamma \mid \Theta, (\exists x\, \alpha)}\ (|\exists)$$

($y$ not free in $\Gamma$ and $\Theta$)

- *Axiom schemes for equality*
  - $\mid\ x \approx x$
  - $x_1 \approx y_1,\ \ldots\ ,\ x_n \approx y_n\ \mid\ fx_1 \cdots x_n \approx fy_1 \cdots y_n$
    (for every function symbol $f$ of arity $n \geq 1$)
  - $x_1 \approx y_1,\ \ldots\ ,\ x_n \approx y_n,\ Px_1 \cdots x_n\ \mid\ Py_1 \cdots y_n$
    (for every predicate symbol $P$ of arity $n \geq 1$)

Let $G$ denote the Gentzen system described above for first-order logic.

**Exercise 1.** Show that without the proviso "$y$ not free in $\Gamma$ and $\Theta$" in $(|\forall)$ and $(\exists|)$ the system is inconsistent, i.e. there is a derivation in $G$ for the unsatisfiable sequent $\mid$ .

**Example 3.** For an arbitrary wff $\alpha$, the following is a valid derivation in $G$:

$$\dfrac{\dfrac{\dfrac{\alpha^x_y \mid \alpha^x_y}{\alpha^x_y \mid (\exists x\ \alpha)}\ (\mid\exists) \qquad \dfrac{(\exists x\ \alpha) \mid (\exists x\ \alpha)}{(\exists x\ \alpha), \neg(\exists x\ \alpha) \mid}\ (\neg\mid)}{\dfrac{\alpha^x_y, \neg(\exists x\ \alpha) \mid}{\neg(\exists x\ \alpha) \mid \neg\alpha^x_y}\ (\mid\neg)}\ (\texttt{Cut})}{\dfrac{\neg(\exists x\ \alpha) \mid (\forall x\ \neg\alpha)}{\mid \neg(\exists x\ \alpha) \to (\forall x\ \neg\alpha)}\ (\mid\forall)}\ (\mid\to)$$

In the next theorem, the symbol "$\vdash_H$" is for derivability relative to one of the Hilbert systems in Section 2 (which all derive precisely the same set of wff's), and "$\vdash_G$" is for derivability relative to $G$. $\Gamma$ is an arbitrary finite (possibly empty) sequence of wff's and $\alpha$ an arbitrary wff.

**Theorem 1.** $\Gamma \vdash_H \alpha$ *if and only if* $\vdash_G \Gamma \mid \alpha$

*Proof.* Both directions are straightforward, if somewhat tedious, inductions on derivations. The details are in Section 77 of Kleene's book [9]. Kleene uses a specific Hilbert system, page 82 in [9], which is not the same as any of the systems in Section 2, but which is readily shown to be equivalent to System E in Section 2 (and therefore equivalent to all the systems in Section 2). □

**Theorem 1.** $\Gamma \vdash_H \alpha$ *if and only if* $\vdash_G \Gamma \mid \alpha$ .

**Proof:** Both directions are straightforward, if somewhat tedious, inductions on derivations. The details are in Section 77 of Kleene's book [9]. Kleene uses a specific Hilbert system, page 82 in [9], which is not the same as any of the systems in Section 2, but which is readily shown to be equivalent to System E in Section 2 (and therefore equivalent to all the systems in Section 2). ■

If $\Gamma$ in Theorem 1 is a finite sequence of wff's $\gamma_1, \ldots, \gamma_n$ then, by repeated use of the Deduction Theorem (Enderton's, page 111), $\Gamma \vdash_H \alpha$ iff $\vdash_H \gamma_1 \to \cdots \to \gamma_n \to \alpha$. By repeated use of $(\texttt{E}\mid)$ and $(\mid\to)$, we also have that $\vdash_G \Gamma\mid\alpha$ iff $\vdash_G \mid \gamma_1 \to \cdots \to \gamma_n \to \alpha$. Hence, in this case,

$$\vdash_H \gamma_1 \to \cdots \to \gamma_n \to \alpha \qquad \text{iff} \qquad \vdash_G \mid \gamma_1 \to \cdots \to \gamma_n \to \alpha\ ,$$

which makes the symbol "$\mid$" appear redundant, and justifies the practice of some people to discard the symbol "$\vdash_G$" altogether (as asserting derivability) and use "$\vdash_G$" instead of "$\mid$" (as sequent separator) for complete notational symmetry between the Hilbert and Gentzen systems.

It is clear that every derivation $\mathcal{D}$ in $G$ can be organized in the form of a tree, with a sequent inserted at every node of the tree. The *root sequent*, i.e. the one inserted at the root of the derivation tree, is the sequent derived by $\mathcal{D}$. Let us say that two derivations $\mathcal{D}_\infty$ and $\mathcal{D}_\in$ in $G$ are *equivalent* if $\mathcal{D}_\infty$ and $\mathcal{D}_\in$ have the same root sequent. Let $G^-$ denote the system obtained from $G$ by omitting the rule $(\texttt{Cut})$.

**Theorem 2** (Gentzen's Hauptsatz[10])**.** *Every derivation in $G$ can be effectively transformed into an equivalent derivation in $G^-$*

[10] Nothing mysterious about this name: Hauptsatz means "main theorem" in German.

*Proof.* When there is no equality symbol $\approx$ in the language and no axiom schemes for equality, a proof can be found in [9], Section 78, or in [15], Chapter XII. In the presence of $\approx$, a proof is given in [6], Chapter 6.[11] □

**Theorem 2** (Gentzen's Hauptsatz[12], or cut-elimination theorem). *Every derivation in $G$ can be effectively transformed into an equivalent derivation in $G^-$ .*

**Proof:** When there is no equality symbol $\approx$ in the language and no axiom schemes for equality, a proof can be found in [9], Section 78, or in [15], Chapter XII. In the presence of $\approx$, a proof is given in [6], Chapter 6.[13] ■

**Example 4.** The following is a derivation in $G^-$, which is also equivalent to the derivation in $G$ of Example 3:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha^x_y \mid \alpha^x_y}{\alpha^x_y \mid (\exists x\ \alpha)}\,(\mid\exists)}{\alpha^x_y, \neg(\exists x\ \alpha) \mid}\,(\neg\mid)}{\neg(\exists x\ \alpha) \mid \neg\alpha^x_y}\,(\mid\neg)}{\neg(\exists x\ \alpha) \mid (\forall x\ \neg\alpha)}\,(\mid\forall)}{\mid \neg(\exists x\ \alpha) \to (\forall x\ \neg\alpha)}\,(\mid\to)$$

There are several important applications of Gentzen's Hauptsatz in first-order logic, none discussed in Enderton's book. For example, it can be used to establish Craig's Interpolation Theorem, which in turn is used to establish Beth's Definability Theorem and Robinson's Joint Consistency Theorem (for statements of these theorems and proofs based on cut-elimination, see [6], Chapter 6, or [15], Chapter XV, or [2], Section 9.12). It is worth noting that these three theorems can be established just as elegantly using model-theoretic techniques, without recourse to the syntactic transformation of Gentzen's Hauptsatz (see [3], Section 2.2, or [11], Chapter 22). But more important is the use of Gentzen's Hauptsatz in investigations of consistency results — more on this below.

## Restrictions for intuitionism

A Gentzen system for intuitionistic propositional logic (resp. first-order logic) is obtained by omitting just two rules from $G_0$ (resp. $G$): $(\mid\neg)$ and $(\mid\mathtt{W})$.

[11] *Warning*: There are several variants of Gentzen systems in [9], [15] and [6], sometimes with minor differences introduced for reasons of efficiency and/or clarity of exposition. What we here call $G$ is exactly the system $G1$ in [9], and essentially (but not exactly) the system $\mathcal{G}^*$ in [15], in both cases without any of the parts related to $\approx$. In [6] there is no less than a dozen systems, and among these, $LK_e$ is exactly our $G$.

[12] Nothing mysterious about this name: Hauptsatz means "main theorem" in German.

[13] *Warning*: There are several variants of Gentzen systems in [9], [15] and [6], sometimes with minor differences introduced for reasons of efficiency and/or clarity of exposition. What we here call $G$ is exactly the system $G1$ in [9], and essentially (but not exactly) the system $\mathcal{G}^*$ in [15], in both cases without any of the parts related to $\approx$. In [6] there is no less than a dozen systems, and among these, $LK_e$ is exactly our $G$.

**Example 5.** The derivation in Example 1 is acceptable intuitionistically, but none of the derivations in Examples 2, 3 and 4, is, because each of the latter uses rule $(\vert\neg)$.

An equivalent restriction of $G$ for intuitionism is given in the next exercise.

**Exercise 2.** Show that omitting $(\vert\neg)$ and $(\vert\mathtt{W})$ from $G$ is equivalent to requiring that the succedent of every sequent has *at most* one wff, i.e. every sequent is restricted to be of the form $\Gamma\vert$ or the form $\Gamma\vert\beta$. (*Hint*: Consider the easier case of $G_0$ first. Show by induction that if $\vdash \Gamma\vert\beta_1, \ldots, \beta_m$ without $(\vert\neg)$ and $(\vert\mathtt{W})$, as well as without $(\neg\vert)$, then $m = 1$ — and if without just $(\vert\neg)$ and $(\vert\mathtt{W})$, then $m \leqslant 1$. For the opposite implication, show by induction on derivations that every use of $(\vert\neg)$ or $(\vert\mathtt{W})$ can be eliminated.)

Let $G_I$ denote the system obtained from $G$ by omitting the two rules $(\vert\neg)$ and $(\vert\mathtt{W})$, and let $G_I^-$ denote the system obtained from $G_I$ by omitting in addition the rule $(\mathtt{Cut})$.

**Theorem 3** (Gentzen's Hauptsatz for intuitionistic logic). *Every derivation in $G_I$ can be effectively transformed into an equivalent derivation in $G_I^-$ .*

**Proof:** When there is no equality symbol $\approx$ in the language and no axiom schemes for equality, a proof can be found in [9], Section 78. ∎

## Gentzen's Hauptsatz and consistency results

For Gentzen, the Hauptsatz was a tool he used to establish the consistency of a particular axiomatization of number theory, commonly called *Peano arithmetic*. Moreover, Gentzen wanted to establish this consistency by proof-theoretic means, without appeal to semantic considerations.

Let $P$ denote Peano arithmetic. The axioms of $P$ are the finitely many axioms of $A_M$ (in Section 3.7 of Enderton's book) in addition to the following *induction axiom scheme*:

$$\varphi(\mathbf{0}) \;\rightarrow\; (\; \forall \boldsymbol{v}_1\; (\varphi(\boldsymbol{v}_1) \;\rightarrow\; \varphi(\boldsymbol{S}\boldsymbol{v}_1))\;) \;\rightarrow\; (\; \forall \boldsymbol{v}_1\; \varphi(\boldsymbol{v}_1)\;)$$

representing infinitely many axioms, one for each wff $\varphi$ with no free variable other than $\boldsymbol{v}_1$, in the language of the standard model of arithmetic $\mathfrak{N}$. An instance of the induction axiom scheme is an *induction axiom*.[14]

Recall that a set $\Gamma$ of wff's is consistent if $\Gamma$ does not derive any contradiction, i.e. if for every wff $\alpha$ it is the case that $\Gamma \nvdash (\alpha \wedge \neg\alpha)$. Typically, it is not easy to verify such a condition by proof-theoretic means. It is often easier to check the satisfiability of $\Gamma$ instead which, by soundness and completeness, is equivalent to its consistency.

For example, the finite set $A_M$ is consistent because we recognize that the standard model $\mathfrak{N}$ satisfies every axiom in $A_M$, thus avoiding the hard work of proving directly that $A_M$ does not derive a contradiction. The same can be said of $P$, by our understanding of induction over the natural numbers. In fact, based on our common knowledge of the underlying operations and relations of $\mathfrak{N}$, i.e. $<$, $+$, $\cdot$, etc., we are willing to declare the axioms of $A_M$ are "obviously true" in $\mathfrak{N}$. If

[14] Peano arithmetic is not discussed in Enderton's book. It is listed in the Index with a reference to page 183, but "Peano arithmetic" is nowhere mentioned on page 183! The induction axiom scheme is mentioned in Exercise 3.1.1 of Enderton's, page 183, but it is restricted to the language of the reduct $\mathfrak{N}_S$, and we do not make such a restriction here.

taken to task, we can of course be more rigorous by applying the methods of Section 2.2 to check that $\mathfrak{N} \models A_M$, and with a little extra work we can also check that $\mathfrak{N} \models P$, but again this uses unformalized set-theoretic reasoning.

This is a common situation: Semantic methods involve a certain amount of set-theoretic as well as intuitive reasoning outside formal proof systems. As a consequence, in relation to questions of consistency, it is sometimes argued that semantic methods are uninformative, or in any case do not provide the right kind of information, or are too precarious to serve as a basis for consistency proofs. It is even argued that, short of a formal proof-theoretic verification, the consistency of a set of wff's should be taken as an explicit unproved assumption.[15]

My own bias is to accept the consistency of $P$ (or any other set of axioms) based on semantic, i.e. unformalized set-theoretic and intuitive reasoning. There are criteria of rigor for such reasoning and there is no need to formalize them. But this does not mean that establishing the consistency of $P$ by formal proof-theoretic means is without value, because additional information about $P$ beyond its consistency is also obtained in this way. And perhaps this is the real value of Gentzen's demonstration of the consistency of $P$.

It is towards this goal that Gentzen developed the sequent calculus and then proved the Hauptsatz. After Gentzen's formal proof of the consistency of $P$, there were other formal proofs following the same general ideas. Gödel's Second Incompleteness Theorem (in Enderton's book, Section 3.6) can be adapted to say: *If $P$ is consistent, then no wff asserting the consistency of $P$ (by some appropriate encoding) is derivable from $P$.* By Gödel's result, starting from $P$ as non-logical axioms, the rules of $G$ (or any formal system equivalent to $G$) are not strong enough to formally prove the consistency of $P$. Thus, in one way or another, the proof system has to be extended to a more powerful deductive calculus, for example by including inference rules with infinitely many premises or by allowing transfinite induction. However extended, the Hauptsatz remains the key technical result in establishing the consistency of $P$. Further discussion of these issues can be found in [9], Section 79, and in the Appendix of [10].

[15] Shoenfield says that "the main trouble with [a consistency proof for $P$ by means of the standard model] is that it is so uninformative. ... It does not increase our understanding, since nothing goes into it which we did not put into it in the first place" [14], page 214.

Mendelson says that, by using semantic methods, "we have not proved in a rigorous way that the axioms of $P$ are true under the standard interpretation, but have taken it as intuitively obvious" [10], page 107.

Kleene says that "giving a model for the axioms [of $P$] in intuitive arithmetical terms does not establish beyond all doubt that no contradiction can arise in the theory deduced from the axioms, unless it can also be demonstrated that the reasonings in the theory can be translated into intuitive arithmetical reasonings in terms of the objects used in the model" [9], page 475. The proviso in the excerpt from Kleene applies to $A_M$, and therefore the consistency of $A_M$ using a restricted form of semantic reasoning, i.e. using what is called "finitary set-theoretic methods", is acceptable to Kleene, but the proviso does not apply to $P$ because showing the satisfiability of any induction axiom in the standard model requires "non-finitary set-theoretic methods". A discussion of "finitary" vs. "non-finitary" methods is also found in Shoenfield's book [14], page 214.

# 5 Natural Deduction

The "feeling" of natural deduction is very different from that of Hilbert-style proof systems. It is closer to Gentzen-style systems, but there are several differences too. (Natural deduction was also first formulated by Gentzen. So, it isn't entirely proper to reserve the name "Gentzen" only for the sequent calculi of Section 4.) In particular, in natural deduction there are *no* axiom schemes and *only* inference rules. To compensate for the lack of axioms, natural deduction allows the introduction of wff's as hypotheses at any stage of a derivation. Moreover, while a Gentzen system has only *introduction* rules, natural deduction uses both *introduction* and *elimination* rules.

The presentation in this section is based on [18]. We can restrict the rules of the system to the logical connectives of a functionally complete set, say $\{\rightarrow, \bot\}$, leaving the other connectives $\{\vee, \wedge, \neg, \leftrightarrow\}$ to be defined in terms of the first two. (The symbol $\bot$ stands for *false*.) However, we prefer to include rules for all the connectives, with the understanding that we can always revert to a system restricted to rules for only $\{\rightarrow, \bot\}$ to simplify an argument (typically an induction on the length of derivations). The inclusion of rules for all the logical connectives not only makes the system more user-friendly, but gives more situations to illustrate the dual mechanism of introducing and cancelling hypotheses. Moreover, when we restrict the system for intuitionism, it will not be possible to define all the connectives in terms of only $\{\rightarrow, \bot\}$.

We start with the simpler case of propositional logic, and later add the necessary rules for first-order logic. For propositional logic, there are introduction and elimination rules for each of the 5 connectives: $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neg$, but not for $\bot$.

## Propositional logic

$\varphi$, $\psi$ and $\sigma$ range over the set of all wff's. By including rules for all of the 6 connectives, we get a total of 15 (one of them, $\to$E, can be recognized as Modus Ponens).

1. One introduction rule, called $\wedge$I, and two elimination rules, both called $\wedge$E, for "$\wedge$":

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\ \wedge\mathtt{I} \qquad\qquad \frac{\varphi \wedge \psi}{\varphi}\ \wedge\mathtt{E} \qquad\qquad \frac{\varphi \wedge \psi}{\psi}\ \wedge\mathtt{E}$$

2. Two introduction rules, both called $\vee$I, and one elimination rule, called $\vee$E, for "$\vee$":

$$\frac{\varphi}{\varphi \vee \psi}\ \vee\mathtt{I} \qquad\qquad \frac{\psi}{\varphi \vee \psi}\ \vee\mathtt{I} \qquad\qquad \frac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]\\ \vdots\\ \sigma\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots\\ \sigma\end{array}}{\sigma}\ \vee\mathtt{E}$$

3. One introduction rule, called $\to$I, and one elimination rule, called $\to$E, for "$\to$":

$$\frac{\begin{array}{c}[\varphi]\\ \vdots\\ \psi\end{array}}{\varphi \to \psi}\ \to\mathtt{I} \qquad\qquad \frac{\varphi \qquad \varphi \to \psi}{\psi}\ \to\mathtt{E}$$

4. One introduction rule, called $\leftrightarrow$I, and two elimination rules, both called $\leftrightarrow$E, for "$\leftrightarrow$":

$$\frac{\begin{array}{cc}[\varphi] & [\psi]\\ \vdots & \vdots\\ \psi & \varphi\end{array}}{\varphi \leftrightarrow \psi}\ \leftrightarrow\mathtt{I} \qquad\qquad \frac{\varphi \qquad \varphi \leftrightarrow \psi}{\psi}\ \leftrightarrow\mathtt{E} \qquad\qquad \frac{\psi \qquad \varphi \leftrightarrow \psi}{\varphi}\ \leftrightarrow\mathtt{E}$$

5. One introduction rule, called $\neg$I, and one elimination rule, called $\neg$E, for "$\neg$":

$$\frac{\begin{array}{c}[\varphi]\\ \vdots\\ \bot\end{array}}{\neg\varphi}\ \neg\mathtt{I} \qquad\qquad \frac{\varphi \qquad \neg\varphi}{\bot}\ \neg\mathtt{E}$$

6. Two rules for "$\bot$", the first called $\bot$ and the second `RAA`:

$$\frac{\bot}{\varphi}\ \bot \qquad\qquad \frac{\begin{array}{c}[\neg\varphi]\\ \vdots\\ \bot\end{array}}{\varphi}\ \texttt{RAA}$$

   Note that the rules for "$\bot$" are the only rules not exhibiting a symmetry between "introduction" and "elimination".

Several of the rules above allow for a hypothesis $\varphi$ to be *cancelled* (or *discharged*) which is indicated by enclosing $\varphi$ between square brackets, i.e. by writing "$[\varphi]$". `RAA` stands for *reductio ad absurdum*, which formalizes the principle of a "proof by contradiction": If we can derive a contradiction, i.e. $\bot$, from $\neg\varphi$ then we can derive $\varphi$ (without the hypothesis $\neg\varphi$). A few examples will make precise these notions.

Let $N_0$ denote the above system of rules for propositional logic.

**Example 1.** A derivation according to the rules of $N_0$:

$$\dfrac{\dfrac{\dfrac{[\varphi\wedge\psi]^1}{\psi}\ \wedge\texttt{E} \qquad \dfrac{[\varphi\wedge\psi]^1}{\varphi}\ \wedge\texttt{E}}{\psi\wedge\varphi}\ \wedge\texttt{I}}{(\varphi\wedge\psi)\ \rightarrow\ (\psi\wedge\varphi)}\ \rightarrow\texttt{I}_1$$

Note how we pair off the hypothesis $\varphi\wedge\psi$ with the rule $\rightarrow\texttt{I}$ that cancels it, by attaching the same index "1" to both the cancellation brackets and the corresponding rule, i.e. by writing $[\ ]^1$ and $\rightarrow\texttt{I}_1$. ∎

**Example 2.** Another derivation in $N_0$:

$$\dfrac{\dfrac{\dfrac{[\varphi]^2 \qquad [\varphi\rightarrow\bot]^1}{\bot}\ \rightarrow\texttt{E}}{(\varphi\rightarrow\bot)\rightarrow\bot}\ \rightarrow\texttt{I}_1}{\varphi\rightarrow((\varphi\rightarrow\bot)\rightarrow\bot)}\ \rightarrow\texttt{I}_2$$

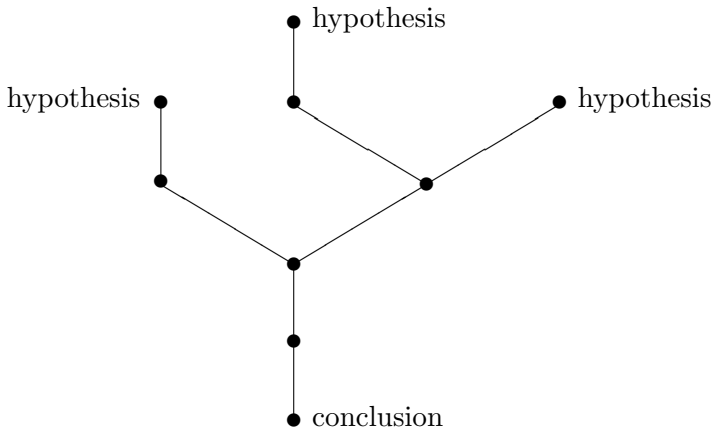
There are two cancellations in this example, for two different hypotheses, thus the two indexes, "1" and "2". ∎

**Example 3.** A more interesting derivation in $N_0$:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\psi}\,\wedge\mathtt{E} \qquad \dfrac{\dfrac{[\varphi \wedge \psi]^1}{\varphi}\,\wedge\mathtt{E} \qquad [\varphi \to (\psi \to \sigma)]^2}{\psi \to \sigma}\,\to\mathtt{E}}{\sigma}\,\to\mathtt{E}}{(\varphi \wedge \psi) \to \sigma}\,\to\mathtt{I}_1}{(\varphi \to (\psi \to \sigma)) \to ((\varphi \wedge \psi) \to \sigma)}\,\to\mathtt{I}_2$$

There are two cancelled hypotheses in this example, with two occurrences of the first and one occurrence of the second. ∎

It should be clear that any derivation using the rules of natural deduction can be organized in the form of a tree, with one wff attached to every node of the tree. The wff's at the leaf nodes are the *hypotheses* used in the derivation (some or all of them cancelled), and the single wff at the root node is the *conclusion* of the derivation. For the derivation in Example 3 the resulting tree is:




Given a set $\Gamma$ of wff's and a wff $\varphi$, we write $\Gamma \vdash \varphi$ iff there is a derivation of the conclusion $\varphi$ from uncancelled hypotheses that are all in $\Gamma$. Thus, for the derivations shown in Examples 1, 2, and 3, we have:

$$\vdash (\varphi \wedge \psi) \to (\psi \wedge \varphi)\ , \qquad \vdash \varphi \to ((\varphi \to \bot) \to \bot)\ , \qquad \vdash (\varphi \to (\psi \to \sigma)) \to ((\varphi \wedge \psi) \to \sigma)\ ,$$

respectively, and in all three cases we take $\Gamma = \varnothing$. Although not shown in these examples, we do not require that $\Gamma$ be exactly the set of all uncancelled hypotheses: $\Gamma$ may contain many (even infinitely many) wff's that do not appear at all in the derivation.

The 5 rules that allow cancellation of hypotheses are: $\vee$E, $\rightarrow$I, $\leftrightarrow$I, $\neg$I, and RAA, which are called accordingly *cancellation rules*. These require some care, as they can be used in a more liberal fashion than suggested by the notation. When we use one of these rules:

- *A wff enclosed in* [ ]*, in the statement of the rule, does not mean that this wff has to actually appear as a hypothesis in the derivation.*

Hence, in particular, when we use $\rightarrow$I, $\neg$I and RAA (but not $\vee$E and $\leftrightarrow$I) which introduce in their conclusion a wff $\varphi$ (or $\neg\varphi$) not mentioned among their premises, it is even possible that this $\varphi$ (or $\neg\varphi$) appears nowhere in the derivation. This is illustrated in the next example.

**Example 4.**

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\psi}\,\wedge\mathtt{E} \qquad \dfrac{[\varphi \wedge \psi]^1}{\varphi}\,\wedge\mathtt{E}}{\psi \wedge \varphi}\,\wedge\mathtt{I}}{(\varphi \wedge \psi) \;\rightarrow\; (\psi \wedge \varphi)}\,\rightarrow\mathtt{I}_1}{\sigma \;\rightarrow\; (\varphi \wedge \psi) \;\rightarrow\; (\psi \wedge \varphi)}\,\rightarrow\mathtt{I}_2$$

The last use of $\rightarrow$I, with index "2", does not cancel any hypothesis occurrence and, moreover, introduces a fresh wff $\sigma$ into the derivation. ∎

Moreover, when we use one of the cancellation rules:

- *Even if a wff enclosed in* [ ] *actually appears as a hypothesis in the derivation, not all of its occurrences have to be cancelled.*

This is justified as there is no harm in adding redundant hypotheses in a derivation. For example, we can cancel only one of the two occurrences of $\varphi \wedge \psi$ in Example 4, resulting in:

$$\varphi \wedge \psi \;\vdash\; \sigma \;\rightarrow\; ((\varphi \wedge \psi) \;\rightarrow\; (\psi \wedge \varphi))$$

or we can cancel neither of the two occurrences, resulting again in:

$$\varphi \wedge \psi \;\vdash\; \sigma \;\rightarrow\; ((\varphi \wedge \psi) \;\rightarrow\; (\psi \wedge \varphi))$$

or we can cancel the two occurrences separately (by using the rule $\rightarrow$I twice), resulting in:

$$\vdash\; \sigma \;\rightarrow\; ((\varphi \wedge \psi) \;\rightarrow\; ((\varphi \wedge \psi) \;\rightarrow\; (\psi \wedge \varphi)))$$

We define one more book-keeping device, before turning to first-order logic. Let $\mathcal{D}$ be a derivation viewed as a tree. Consider a node in $\mathcal{D}$, more precisely the wff $\varphi$ attached to this node in $\mathcal{D}$, which is obtained by the use of a cancellation rule. For definiteness, let this rule be $\to\mathtt{I}$ and its use instance be $\to\mathtt{I}_n$ (an index $n$ gets attached to it when used in a derivation) so that, in particular, $\varphi$ must be of the form $\sigma \to \tau$. We use the term *parcel*, or *parcel of hypotheses*, to refer to all occurrences of $\sigma$ enclosed in $[\ ]^n$. If we need to be more specific, we may say the "parcel with index $n$" or "parcel $n$". A parcel consists therefore of finitely many (possibly none) occurrences of the same hypothesis that are discharged together by one of the rules in $\{\vee\mathtt{E}, \to\mathtt{I}, \leftrightarrow\mathtt{I}, \neg\mathtt{I}, \mathtt{RAA}\}$. Our convention, already used in the preceding examples, is to uniquely identify a parcel of hypotheses by an index $n \in \mathbb{N}$.

**Example 5.**

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi\wedge\psi]^1}{\varphi}\wedge\mathtt{E}}{\varphi\vee\sigma}\vee\mathtt{I} \qquad \dfrac{[\sigma]^2}{\varphi\vee\sigma}\vee\mathtt{I}}{\varphi\vee\sigma}\vee\mathtt{E}_{1,2} \qquad \dfrac{\dfrac{\dfrac{[\varphi\wedge\psi]^3}{\psi}\wedge\mathtt{E}}{\psi\vee\sigma}\vee\mathtt{I} \qquad \dfrac{[\sigma]^4}{\psi\vee\sigma}\vee\mathtt{I}}{\psi\vee\sigma}\vee\mathtt{E}_{3,4}}{(\varphi\vee\sigma)\wedge(\psi\vee\sigma)}\wedge\mathtt{I}}{(\varphi\wedge\psi)\vee\sigma \ \to\ (\varphi\vee\sigma)\wedge(\psi\vee\sigma)}\to\mathtt{I}_5$$

In this derivation there are 5 parcels. Each use of $\vee\mathtt{E}$ cancels two distinct parcels (parcels 1 and 2, parcels 3 and 4), whereas the use of $\to\mathtt{I}$ cancels only one parcel (parcel 5). ∎

### First-order logic

The system for propositional logic, $N_0$, is extended by adding rules for the quantifiers and, if an equality symbol $\approx$ is included in the syntax of wff's, by adding rules for equality too. $\varphi$ and $\psi$ range over the set of wff's, $x$, $y$ and $z$ over variables, and $t$ over terms. Call $N$ the resulting system.

1. One introduction rule, called $\forall\mathtt{I}$, and one elimination rule, called $\forall\mathtt{E}$, for "$\forall$":

$$\frac{\varphi(x)}{\forall x\ \varphi(x)}\ \forall\mathtt{I} \qquad\qquad \frac{\forall x\ \varphi(x)}{\varphi(t)}\ \forall\mathtt{E}$$

   where in $\forall\mathtt{I}$ the variable $x$ does not occur free in any hypothesis on which $\varphi(x)$ depends, i.e. in any uncancelled hypothesis in the derivation of $\varphi(x)$, and in $\forall\mathtt{E}$ the substitution of $t$ for $x$ is legal, i.e. no free variable in $t$ is captured by a quantifier in $\varphi$.

2. One introduction rule, called $\exists\mathtt{I}$, and one elimination rule, called $\exists\mathtt{E}$, for "$\exists$":

$$\frac{\varphi(t)}{\exists x\ \varphi(x)}\ \exists\mathtt{I} \qquad\qquad \frac{\exists x\ \varphi(x) \qquad \begin{array}{c}[\varphi(x)]\\ \vdots\\ \psi\end{array}}{\psi}\ \exists\mathtt{E}$$

   where in $\exists\mathtt{I}$ the substitution of $t$ for $x$ is legal, i.e. no free variable in $t$ is captured by a quantifier in $\varphi$, and in $\exists\mathtt{E}$ the variable $x$ does not occur free in $\psi$ nor in any uncancelled hypothesis (other than $\varphi(x)$) on which $\varphi(x)$ depends, i.e. in any uncancelled hypothesis in the subderivation with conclusion $\psi$.

3. The rules for equality simulate the axioms for equality, used in Hilbert systems (Section 2) or in Gentzen systems (Section 4). There is no symmetry here between "introduction" and "elimination" rules, in contrast to rules for the logical connectives and the quantifiers. In $\mathtt{EQ4}$, $f$ is an arbitrary function symbol of arity $n \geqslant 0$, and in $\mathtt{EQ5}$, $P$ is an arbitrary predicate symbol of arity $n \geqslant 0$.

$$\frac{}{x \approx x}\ \mathtt{EQ1} \qquad \frac{x \approx y}{y \approx x}\ \mathtt{EQ2} \qquad \frac{x \approx y \qquad y \approx z}{x \approx z}\ \mathtt{EQ3}$$

$$\frac{x_1 \approx y_1 \quad \cdots \quad x_n \approx y_n}{fx_1 \cdots x_n \approx fy_1 \cdots y_n}\ \mathtt{EQ4} \qquad\qquad \frac{x_1 \approx y_1 \quad \cdots \quad x_n \approx y_n \quad Px_1 \cdots x_n}{Py_1 \cdots y_n}\ \mathtt{EQ5}$$

**Example 6.** A derivation in $N$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x\ (\varphi(x) \wedge \psi(x))]^1}{\varphi(x) \wedge \psi(x)}\ \forall \mathtt{E}}{\varphi(x)}\ \wedge \mathtt{E}}{\forall x\ \varphi(x)}\ \forall \mathtt{I} \qquad \dfrac{\dfrac{\dfrac{[\forall x\ (\varphi(x) \wedge \psi(x))]^1}{\varphi(x) \wedge \psi(x)}\ \forall \mathtt{E}}{\psi(x)}\ \wedge \mathtt{E}}{\forall x\ \psi(x)}\ \forall \mathtt{I}}{(\forall x\ \varphi(x)) \wedge (\forall x\ \psi(x))}\ \wedge \mathtt{I}}{\forall x\ (\varphi(x) \wedge \psi(x))\ \rightarrow\ (\forall x\ \varphi(x)) \wedge (\forall x\ \psi(x))}\ \rightarrow \mathtt{I}_1$$

**Example 7.** Another derivation in $N$:

$$\dfrac{\dfrac{[\exists x\ (\varphi(x) \vee \psi(x))]^4 \qquad \dfrac{[\varphi(x) \vee \psi(x)]^3 \qquad \dfrac{\dfrac{[\varphi(x)]^1}{\exists x\ \varphi(x)}\ \exists \mathtt{I}}{(\exists x\ \varphi(x)) \vee (\exists x\ \psi(x))}\ \vee \mathtt{I} \qquad \dfrac{\dfrac{[\psi(x)]^2}{\exists x\ \psi(x)}\ \exists \mathtt{I}}{(\exists x\ \varphi(x)) \vee (\exists x\ \psi(x))}\ \vee \mathtt{I}}{(\exists x\ \varphi(x)) \vee (\exists x\ \psi(x))}\ \vee \mathtt{E}_{1,2}}{(\exists x\ \varphi(x)) \vee (\exists x\ \psi(x))}\ \exists \mathtt{E}_3}{\exists x\ (\varphi(x) \vee \psi(x))\ \rightarrow\ (\exists x\ \varphi(x)) \vee (\exists x\ \psi(x))}\ \rightarrow \mathtt{I}_4$$

The symbol "$\vdash_H$" is for derivability relative to one of the Hilbert systems in Section 2 (which all derive precisely the same set of wff's), and "$\vdash_N$" is for derivability relative to the rules of natural deduction. For comparisons with systems in previous sections, take $\bot$ as an abbreviation for $\alpha \wedge \neg\alpha$, for some fixed but otherwise arbitrary wff $\alpha$.

**Theorem 1.** *For an arbitrary set of wff's* $\Gamma$ *and an arbitrary wff* $\varphi$, $\Gamma \vdash_H \varphi$ *if and only if* $\Gamma \vdash_N \varphi$.

**Proof:** A proof can be found in [16], pp 148-159. A sketch of a proof, with useful comments, is also in [8], pp 26-32. Another proof is to first show: $\Gamma \vdash_N \varphi$ iff $\vdash_G \Gamma | \varphi$ (with the restriction that $\Gamma$ is finite), and then invoke Theorem 1 of Section 4. For the equivalence between natural deduction and a Gentzen system (when both are restricted to the intuitionistic case), there are proofs in [16], pp 168-186, and in [7], Ch. 5. ∎

## Restrictions for intuitionism

A natural-deduction system for intuitionistic propositional logic (resp. first-order logic) is obtained by omitting just one rule from $N_0$ (resp. $N$): `RAA`.

All the derivations so far, in Examples 1 to 7, are acceptable intuitionistically, because none uses the rule `RAA`.

**Example 8.** Here is a derivation which is not allowed intuitionistically:

$$\dfrac{\dfrac{[\neg\varphi]^1 \quad [\neg\varphi \to \bot]^2}{\bot}\ \to\mathtt{E}}{\dfrac{\varphi}{(\neg\varphi \to \bot) \to \varphi}\ \to\mathtt{I}_2}\ \mathtt{RAA}_1$$

If we take $\neg\varphi$ as an abbreviation for $\varphi \to \bot$, then we have here:

$$\vdash\ \neg\neg\varphi\ \to\ \varphi$$

which is certainly accepted classically. A subtle point: With the forementioned abbreviation, the derivation in Example 2 shows that

$$\vdash\ \varphi\ \to\ \neg\neg\varphi$$

which *is* acceptable intuitionistically. There is no contradiction here: Intuitionism does not take $\varphi$ and $\neg\neg\varphi$ as equivalent wff's. ∎

## Normalization

A fundamental result has to do with the elimination of superfluous parts in derivations. The motivation is best given by examples.

**Example 9.**

$$\dfrac{\dfrac{\dfrac{\sigma \qquad \sigma \to \varphi}{\varphi}\ \to\mathtt{E} \qquad [\psi]^1}{\varphi \wedge \psi}\ \wedge\mathtt{I}}{\dfrac{\varphi}{\psi \to \varphi}\ \to\mathtt{I}_1}\ \wedge\mathtt{E}$$

The conjunction $\varphi \wedge \psi$ is introduced only to be immediately eliminated. It is clearly more efficient to write instead:

$$\dfrac{\dfrac{\sigma \qquad \sigma \to \varphi}{\varphi}\ \to\mathtt{E}}{\psi \to \varphi}\ \to\mathtt{I}_1$$

The consecutive uses of $\wedge\mathtt{I}$ and $\wedge\mathtt{E}$ are now removed. ∎

**Example 10.** The following is a more interesting derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\sigma \wedge \varphi]^3}{\varphi}\,\wedge\mathtt{E} \qquad [\varphi \to \psi]^2}{\psi}\,\to\mathtt{E} \qquad \dfrac{\dfrac{[\sigma \wedge \varphi]^3}{\sigma}\,\wedge\mathtt{E}}{\psi \to \sigma}\,\to\mathtt{I}_1}{\sigma}\,\to\mathtt{E}}{(\varphi \to \psi) \to \sigma}\,\to\mathtt{I}_2}{(\sigma \wedge \varphi) \to ((\varphi \to \psi) \to \sigma)}\,\to\mathtt{I}_3$$

More efficiently, we can write the following derivation:

$$\dfrac{\dfrac{\dfrac{[\sigma \wedge \varphi]^3}{\sigma}\,\wedge\mathtt{E}}{(\varphi \to \psi) \to \sigma}\,\to\mathtt{I}_2}{(\sigma \wedge \varphi) \to ((\varphi \to \psi) \to \sigma)}\,\to\mathtt{I}_3$$

We have cut out the consecutive uses of $\to\mathtt{I}$ (with index 1) and $\to\mathtt{E}$. ∎

A derivation in which an introduction is never followed by an elimination is called *normal*.

**Theorem 2** (Normal Form Theorem). *Every derivation $\mathcal{D}$ is equivalent to a normal derivation $\mathcal{D}'$, i.e. if $\mathcal{D}$ is a derivation of $\varphi$ from $\Gamma$ then there is a* normal *derivation $\mathcal{D}'$ of $\varphi$ from $\Gamma$.*

A *reduction step* consists in the removal of a superfluous introduction followed by an elimination. Theorem 3 says that the process of going from $\mathcal{D}$ to $\mathcal{D}'$ in Theorem 2 can be carried out effectively.

**Theorem 3** (Normalization Theorem). *For every derivation $\mathcal{D}$ there is a finite sequence of reduction steps that reduces $\mathcal{D}$ into a normal derivation $\mathcal{D}'$ equivalent to $\mathcal{D}$.*

An even stronger result than the preceding two is the *strong normalization theorem*.

**Theorem 4** (Strong Normalization Theorem). *Every sequence of reduction steps applied to a derivation $\mathcal{D}$ terminates in a normal derivation $\mathcal{D}'$ equivalent to $\mathcal{D}$.*

# 6 Additional Remarks on Intuitionism

A distinctive feature of intuitionism is that it will not accept proofs that are not *constructive*. What is a constructive proof? The best answer is given by examples: Below are three *non*-constructive proofs of well-known results. After the proofs, we point out what makes them non-constructive. These examples are often used when intuitionism is first introduced.

**Theorem 1** *There are solutions of $x^y = z$ with $x$ and $y$ irrational numbers and $z$ rational.*

*Proof.* We know $\sqrt{2}$ is irrational. Moreover, $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If it is rational, let $x = \sqrt{2}$ and $y = \sqrt{2}$, making $z = x^y$ a rational number. If $\sqrt{2}^{\sqrt{2}}$ is irrational, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, so that $z = x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$, which is again a rational number. ■ □

**Theorem 2** (König's Lemma) *Every infinite, finitely branching, tree $\mathcal{T}$ has an infinite path.*

*Proof.* Using induction, we define an infinite sequence of nodes $x_0, x_1, \ldots$, forming an infinite path in $\mathcal{T}$. At stage 0 of the induction, let $x_0$ be the root of $\mathcal{T}$, which has infinitely many successors by the hypothesis that $\mathcal{T}$ is infinite. At stage $n \geq 1$, assume we have already selected nodes $x_0, x_1, \ldots, x_{n-1}$ so far, forming a path of length $n-1$, such that $x_{n-1}$ has infinitely many successors. By hypothesis, $\mathcal{T}$ is finitely branching, which implies $x_{n-1}$ has only finitely many immediate successors. Hence, one of the immediate successors of $x_{n-1}$, say $y$, must have infinitely many successors. Define $x_n$ to be $y$, which has infinitely many successors in $\mathcal{T}$, and proceed to stage $n+1$ of the induction. ■ □

Another way of stating König's Lemma (KL) is to say: *If a finitely branching tree has arbitrarily long finite paths, then it has an infinite path.* Stated this way, it evokes some connection with the compactness theorem in classical logic: If a set $\Gamma$ of wff's is finitely satisfiable, then $\Gamma$ is satisfiable. This is indeed the case, as it can be shown that KL and the compactness theorem basically assert the same thing.[16]

Another connection with the compactness theorem in logic is the Bolzano-Weierstrass (BW) theorem in real analysis. There are different formulations of this theorem. We give one which makes plain the non-constructive nature of the proof. (Another formulation is given in Exercise 5, page 173, in Enderton's book.)

[16] To see the connection in the case of propositional logic, consider the collection of all truth assignments to the propositional variables $A_1, A_2, \ldots, A_n, \ldots$, organized as a single infinite full binary tree, call it $\mathcal{T}$, i.e. at the $n$-th level of $\mathcal{T}$ a left (resp. right) branch corresponds to assigning $T$ (resp. $F$) to variable $A_n$. Given a set $\Sigma$ of propositional wff's, we define another binary tree $\mathcal{T}^{\pm}$ from $\mathcal{T}$: Given infinite path $\pi = t_1 t_2 \cdots t_n \cdots$ in $\mathcal{T}$, where each $t_n$ is $T$ or $F$, let $k$ be the smallest integer (if any) such that the truth assignment corresponding to $\pi$ does *not* satisfy some wff in $\Sigma$; if such a $k$ exists, delete from $\mathcal{T}$ all paths extending the finite path $t_1 t_2 \cdots t_k$. The resulting $\mathcal{T}^{\pm}$ contains some finite paths (possibly none) and some infinite paths (possibly none). Now, $\Sigma$ is finitely satisfiable iff $\mathcal{T}^{\pm}$ has arbitrarily long finite paths (equivalently, which is easier to see, there is an unsatisfiable finite subset of $\Sigma$ iff there is a finite bound on the length of all paths in $\mathcal{T}^{\pm}$) and $\Sigma$ is satisfiable iff $\mathcal{T}^{\pm}$ has an infinite path.

**Theorem 3** (Bolzano-Weierstrass) *Every infinite subset $S$ of the closed interval $[a, b]$ of real numbers contains a convergent infinite sequence.*[17]

*Proof.* We construct an infinite nested chain of intervals $[a_n, b_n]$, each containing infinitely many elements of $S$, by induction on $n \geq 0$. First, let $a_0 = a$ and $b_0 = b$. Proceeding inductively, for arbitrary $n + 1 \geq 1$:

(1) If $[a_n, (a_n + b_n)/2]$ contains infinitely many elements, let $a_{n+1} = a_n$ and $b_{n+1} = (a_n + b_n)/2$.

(2) If $[a_n, (a_n + b_n)/2]$ contains finitely many elements, let $a_{n+1} = (a_n + b_n)/2$ and $b_{n+1} = b_n$.

This is a strict nested chain of intervals with a non-empty intersection. (It is "strict" in the sense that no two consecutive intervals are equal.) Let $x$ be an element in this intersection. The sequence $a_0, a_1, \ldots, a_n, \ldots$ or the sequence $b_0, b_1, \ldots, b_n, \ldots$ must contain infinitely many distinct elements, and both converge to $x$. ■ □

The three preceding proofs show the existence of something without providing the means to find it. In the first proof, one of two specific solutions of the equation is shown to be true, but no effective method is given to determine which.

In the proof of KL, we prove by induction that a disjunction is true, but because we do not determine which immediate successor node has infinitely many nodes below it, we do not actually have a construction for (i.e. an algorithm to generate) the infinite path we prove to exist.

The proof of BW seems to specify a construction, but because it does not provide a way of deciding whether case (1) or case (2) holds, such a construction cannot in fact be carried out.

In all three cases, what pushes the argument through to its conclusion is an appeal to the *law of excluded middle*, which says that for every assertion $A$, either $A$ is true or $\neg A$ is true, even though there may be no effective way of deciding which. This is why we say that these proofs are not *constructive*.

From an intuitionistic point of view, this invalidates the three preceding proofs as well as many other proofs in classical mathematics. It also invalidates many proofs in classical logic, such as the proofs of compactness,[18] completeness, and many other results at the foundation of classical logic. There are issues of compactness and completeness in intuitionism, to be sure, but these have to be understood differently and established differently.

Note that the notion of a constructive proof is not restricted to intuitionism and makes perfect sense in the context of classical mathematics too. The distinction between constructive and non-constructive proofs naturally arises in classical mathematics whenever we want to prove an existential statement or a disjunctive statement. A constructive proof of the same theorem, or what may be perceived as the same theorem (more on this below), is generally more informative than a non-constructive one: Not only the existence of something is established, but an effective method (an algorithm) is provided to determine it.

[17] If you had a course in analysis, you will recall this is equivalent to the property that the real numbers form a *compact space*. And, indeed, it can be shown this is the same phenomenon encountered in the compactness theorem in logic.

[18] This should be clear from the connection indicated earlier between the compactness theorem and KL and BW.

The preceding suggests that intuitionistic logic, as a system of reasoning, ought to be favored over classical logic. Indeed, if constructive proofs are more informative, why should we ever content ourselves with non-constructive proofs? The answer would be "never" if intuitionism were a clear winner in all respects — but it isn't, as something is often lost by abandoning some of the tenets of classical logic (such as the law of excluded middle and others). For one thing, intuitionism is not a single system of reasoning: There are variations within intuitionism, each advocating a different way of relaxing restrictions imposed by the rejection of the law of excluded middle. These should not preoccupy us here, as they become quite technical and result in different approaches to constructive mathematics (e.g. see [17]).

Moreover, a constructive proof of the same fact can be considerably more complicated. For example, concerning the first theorem above, there is a constructive proof for it, but which requires a deeper study of the numbers $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$. (In fact it can be shown that $\sqrt{2}^{\sqrt{2}}$ is irrational.[19])

What about constructive proofs for KL and BW? This points to another difficulty: A rejection of non-constructive proofs comes together with a different interpretation of formal statements. Both KL and BW mention an "infinite" object in their statements. In classical logic, we assume the existence (or pre-existence) of infinite sets as finished (or completed) entities. Intuitionism rejects this view and qualifies a set $X$ as "infinite" only if there is a way of effectively generating the members of $X$ without ever having to stop, and it allows operations (themselves required to be constructive) on $X$ only if they can be carried out without ever having to list (or presume the existence of) all the members of $X$. The set $\mathbb{N}$ of natural numbers can be viewed infinite in this sense, and classical logic can go along with intuitionism in this case.[20] But the infinity of the set $\mathbb{R}$ of reals has to mean two different things for classical and intuitionistic logic. What is "infinite" intuitionistically is "infinite" classically, but not necessarily the other way around.

Hence, it is not only a matter of choosing between a constructive proof and a non-constructive proof of the same theorem, but also of interpreting formal statements differently. Although the intuitionistic interpretation of a formal statement may convey more information than the classical one, it is this extra information packed into the same concept that often entails a more complicated and less transparent definition of that concept. For example, in relation to the concept of "equality between real numbers", Kleene points out the following (page 53 in [9]):

> In the intuitionistic theory of the continuum, we cannot affirm that any two real numbers $a$ and $b$ are either equal or unequal. Our knowledge about the equality or inequality of $a$ and $b$ can be more or less specific. By $a \neq b$, it is meant that $a = b$ leads to a contradiction, while $a \# b$ is a stronger kind of inequality which means that one can give an example of a rational number which separates $a$ and $b$. Of course $a \# b$ implies $a \neq b$. But there are pairs of real numbers $a$ and $b$ for which it is not known that either $a = b$ or $a \neq b$ or $a \# b$. It is clear that such complications replace the classical theory of the continuum by something less perspicuous in form.

Back to the question of whether there are constructive proofs for KL and BW: Understood constructively, both KL and BW fail. For the first counterexample below, note there are $2^{\aleph_0}$ binary trees (why?) but only $\aleph_0$ of them can be effectively generated (why?).

[19] More generally, it can be shown constructively that if $a \notin \{0, 1\}$, $a$ algebraic, and $b$ irrational algebraic, then $a^b$ is irrational. See page 8 in [17] and appropriate references therein.

[20] The effective enumerability of $\mathbb{N}$ is the starting point of recursion theory and all logicians, whether classical or intuitionistic, are comfortable with it.

**Constructive counterexample for KL:** *There is an effectively generated binary tree which contains infinite paths but none of its infinite paths can be effectively generated.*[21]

The next counterexample mentions "computable" real numbers. This is a restriction on the classical definition of real numbers that makes the notion acceptable intuitionistically. Basically, a real number $r$ is said to be *computable* (or also *recursive*) if there is an effective procedure to generate the numerals (read from left to right) in the decimal expansion of $r$.

**Constructive counterexample for BW:** *There is an effectively generated, strictly increasing sequence of rationals in the interval* $[0, 1]$ *which does not converge to any computable real number.*[22]

**Exercise 1.** For simplicity, restrict attention to binary trees. The contrapositive of KL is sometimes called the Fan Theorem (FT) which asserts: *Every well-founded binary tree is finite.*[23] Classically, KL and FT are equivalent, but not intuitionistically. In fact, FT is accepted intuitionistically, even though KL is not. What is the explanation for this apparent inconsistency? (Not every form of taking the contrapositive is rejected by intuitionism, so you have to be careful in your answer.) ∎

[21] This is a paraphrase of a more precise result in recursion theory: *There is a primitive recursive tree $R$ such that (1) for every total recursive function $f : \mathbb{N} \to \{0, 1\}$ there is $n \in \mathbb{N}$ such that $\bar{f}(n) \notin R$, and yet also (2) for every $n \in \mathbb{N}$ there is a path $t$ of length $n$ such that $t \in R$.* Take a "path" to be a binary string, a "binary tree" to be a prefix-closed set of binary strings, and $\bar{f}(n)$ to denote the string $f(0)f(1)\cdots f(n)$. A proof of this result can be found in [1], Ch. IV, Section 5. A discussion of the same is also in [17], Ch. 4, Section 7.

[22] There is a more general result asserting the existence of the so-called "Specker sequences", which implies the result here. The proof along with appropriate definitions can be found in [1], Ch. IV, Section 4, or in [17], Ch. 5, Section 4.

[23] A *well-founded* tree is one without infinite paths.

# References


[1] Michael J. Beeson. *Foundations of Constructive Mathematics*. Springer-Verlag, 1980.

[2] John Bell and Moshe Machover. *A Course in Mathematical Logic*. North-Holland, Amsterdam, 1977.

[3] Chen Chung Chang and H. Jerome Keisler. *Model Theory*. North-Holland, Amsterdam, 1973.

[4] Chin-Liang Chang and Richard Char-Tung Lee. *Symbolic Logic and Mechanical Theorem Proving*. Academic Press, New York, 1973.

[5] Michael Dummett. *Elements of Intuitionism*. Oxford University Press, 1977.

[6] Jean H. Gallier. *Logice for Computer Science, Foundations of Automatic Theorem Proving*. Harper and Row, New York, 1986.

[7] Jean-Yves Girard, Yves Lafont, and Paul Tayler. *Proofs and Types*. Cambridge University Press, Cambridge, UK, 1989.

[8] Wilfrid Hodges. Elementary predicate logic. In Dov M. Gabbay and Franz Guenthner, editors, *Handbook of Philosophical Logic, Vol. 1*, pages 1–132. Springer, Netherlands, 1983.

[9] Stephen C. Kleene. *Introduction to Metamathematics*. Van Nostrand, 1952.

[10] Elliott Mendelson. *Introduction to Mathematical Logic*. Van Nostrand, 1964.

[11] J. Donald Monk. *Mathematical Logic*. Springer-Verlag, 1976.

[12] Ani Nerode and Richard A. Shore. *Logic for Applications*. Springer-Verlag, New York, 1993.

[13] John Alan Robinson. *Logic: Form and Function, The Mechanization of Deductive Reasoning*. North Holland, New York, 1979.

[14] Joseph R. Shoenfield. *Mathematical Logic*. Addison-Wesley, 1967.

[15] Raymond M. Smullyan. *First-Order Logic*. Springer-Verlag, New York, 1968.

[16] Göran Sundholm. Systems of deductions. In Dov M. Gabbay and Franz Guenthner, editors, *Handbook of Philosophical Logic, Vol. 1*, pages 133–188. Springer, Netherlands, 1983.

[17] Anne Sjerp Troelstra and Dirk van Dalen. *Constructivism in Mathematics*. North-Holland, Amsterdam, 1988.

[18] Dirk van Dalen. *Logic and Structure, Third Edition*. Springer-Verlag, 1994.