1.2 Inference Rules, Deductions, The Proof Systems $\mathcal{N}_m^{\Rightarrow}$ and $\mathcal{NG}_m^{\Rightarrow}$

In order to define the notion of proof rigorously, we would have to define a formal language in which to express statements very precisely and we would have to set up a proof system in terms of axioms and proof rules (also called inference rules).

We will not go into this; this would take too much time and besides, this belongs to a logic course, which is not what CIS160 is!

Instead, we will content ourselves with an intuitive idea of what a statement is and focus on stating as precisely as possible the rules of logic that are used in constructing proofs.

In mathematics, we **prove statements.**

Statements may be *atomic* or *compound*, that is, built up from simpler statements using *logical connectives*, such as, *implication* (if–then), *conjunction* (and), *disjunction* (or), *negation* (not) and (existential or universal) *quantifiers*.

As examples of atomic statements, we have:

1. “a student is eager to learn”.
2. “a students wants an A”.
3. “an odd integer is never 0”
4. “the product of two odd integers is odd”

Atomic statements may also contain “variables” (standing for arbitrary objects). For example

1. human(x): “x is a human”
2. needs-to-drink(x): “x” needs to drink

An example of a compound statement is

$$\text{human}(x) \Rightarrow \text{needs-to-drink}(x).$$

In the above statement, $\Rightarrow$ is the symbol used for logical implication.

If we want to assert that every human needs to drink, we can write

$$\forall x(\text{human}(x) \Rightarrow \text{needs-to-drink}(x));$$

This is read: "for every x, if x is a human then x needs to drink".

If we want to assert that some human needs to drink we write

$$\exists x(\text{human}(x) \Rightarrow \text{needs-to-drink}(x));$$

This is read: "there is some x such that, if x is a human then x needs to drink".

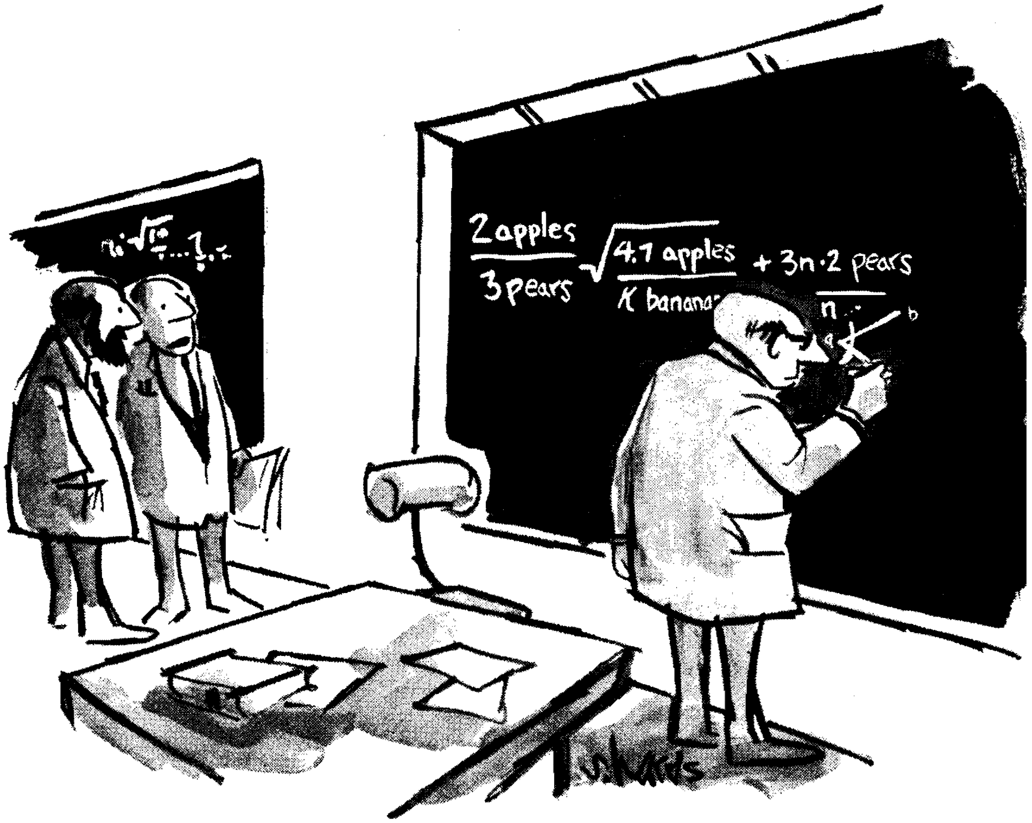
We often denote statements (also called *propositions* or *(logical) formulae*) using letters, such as A, B, P, Q, *etc.*, typically upper-case letters (but sometimes greek letters, φ, ψ, *etc.*).

If P and Q are statements, then their *conjunction* is denoted $P \wedge Q$ (say: P and Q),
their *disjunction* denoted $P \vee Q$ (say: P or Q),
their *implication* denoted $P \Rightarrow Q$ (or $P \supset Q$);
say: if P then Q.

We also have the atomic statements $\perp$ (*falsity*), which corresponds to **false** (think of it as the statement which is false no matter what), and the atomic statement $\top$ (*truth*), which corresponds to **true** (think of it as the statement which is always true).

The constant $\perp$ is also called *falsum* or *absurdum*.

It is a formalization of the notion of *absurdity* (a state in which contradictory facts hold).



"IF ONLY HE COULD THINK IN ABSTRACT TERMS."

Reproduced by special permission of *Playboy* Mag
Copyright © January 1970 by *Playboy.*

Figure 1.9: The power of abstraction

Then, it is convenient to define the *negation* of P as $P \Rightarrow \perp$ and to abbreviate it as $\neg P$ (or sometimes $\sim P$).

Thus, $\neg P$ (say: not P) is just a shorthand for $P \Rightarrow \perp$.

This interpretation of negation may be confusing at first.

The intuitive idea is that $\neg P = (P \Rightarrow \perp)$ is true if and only if P is not true because if both P and $P \Rightarrow \perp$ were true then we could conclude that $\perp$ is true, an absurdity, and if both P and $P \Rightarrow \perp$ were false then P would have to be both true and false, again, an absurdity.

Actually, since we don't know what truth is, it is "safer" (and more constructive) to say that $\neg P$ is provable iff for every proof of P we can derive a contradiction (namely, $\perp$ is provable). In particular, P should not be provable.

For example, $\neg(Q \wedge \neg Q)$ is provable (as we will see later, because any proof of $Q \wedge \neg Q$ yields a proof of $\perp$).

However, the fact that a proposition, P, is **not** provable does not imply that $\neg P$ **is** provable!

There are plenty of propositions such that both P and $\neg P$ are not provable, such as $Q \Rightarrow R$, where Q and R are two unrelated propositions (with no common symbols)!

Whenever necessary to avoid ambiguities, we add matching parentheses: $(P \wedge Q)$, $(P \vee Q)$, $(P \Rightarrow Q)$. For example, $P \vee Q \wedge R$ is ambigous; it means either $(P \vee (Q \wedge R))$ or $((P \vee Q) \wedge R)$.

An implication $P \Rightarrow Q$ should be understood as an *if–then statement*, that is, if P is true then Q is also true.

A better interpretation is that *any proof of $P \Rightarrow Q$ can be used to construct a proof of Q given any proof of P*.

As a consequence of this interpretation, we will see later that if $\neg P$ is provable, then $P \Rightarrow Q$ is also provable (instantly!) whether or not Q is provable.

In such a situation, we often say that $P \Rightarrow Q$ is *vacuously provable*.

For example, $(P \wedge \neg P) \Rightarrow Q$ is provable for any arbitrary Q (because if we assume that $P \wedge \neg P$ is provable, then we derive a contradiction, and then, another rule of logic tells us that any proposition whatsoever is provable. However, we will have to wait until Section 1.3 to see this).

Of course, there are problems with the above paragraph.

What does truth have to do with all this?

What do we mean when we say "P is true"?

What is the relationship between truth and provability?

Figure 1.10: Boole orders lunch

These are actually deep (and tricky!) questions whose answers are not so obvious.

One of the major roles of logic is to clarify the notion of truth and its relationship to provability. We will avoid these fundamental issues by dealing exclusively with the notion of proof.

So, the big question is: *What is a proof?*

Typically, the statements that we prove depend on some set of *hypotheses*, also called *premises* (or *assumptions*).

As we shall see shortly, this amounts to proving implications of the form

$$(P_1 \land P_2 \land \cdots \land P_n) \Rightarrow Q.$$

However, there are certain advantages in defining the notion of *proof* (or *deduction*) of a proposition from a set of premises.

Sets of premises are usually denoted using upper-case greek letters such as Γ or Δ.

Roughly speaking, a *deduction* of a proposition Q from a set of premises Γ is a finite labeled tree whose root is labeled with Q (the *conclusion*), whose leaves are labeled with premises from Γ (possibly with multiple occurrences), and such that every interior node corresponds to a given set of *proof rules* (or *inference rules*).

Certain simple deduction trees are declared as obvious proofs, also called *axioms*.

Figure 1.11: David Hilbert, 1862-1943 (left and middle), Gerhard Gentzen, 1909-1945 (middle right) and Dag-Prawitz, 1936- (right)

There are many kinds of proofs systems: Hilbert-style systems, Natural-deduction systems, Gentzen sequents systems, *etc.*

We describe a so-called *natural-deduction system* invented by G. Gentzen in the early 1930's (and thoroughly investigated by D. Prawitz in the mid 1960's).

The major advantage of this system is that it captures quite nicely the "natural" rules of reasoning that one uses when proving mathematical statements.

This does not mean that it is easy to find proofs in such a system or that this system is indeed very intuitive!

We begin with the inference rules for implication and first consider the following question:

How do proceed to prove an implication, $A \Rightarrow B$?

The rule, called *$\Rightarrow$-intro*, is:

Assume that A has already been proven and then prove B, making as many uses of A as needed.

Let us give a simple example. The *odd numbers* are the numbers

$$1,\ 3,\ 5,\ 7,\ \ 9,\ 11,\ 13,\ldots.$$

Equivalently, a whole number, n, is odd iff it is of the form $2k+1$, where $k = 0, 1, 2, 3, 4, 5, 6, \ldots$.

Let us denote the fact that a number n is odd by $\mathrm{odd}(n)$.

We would like to prove the implication

$$\mathrm{odd}(n) \Rightarrow \mathrm{odd}(n+2).$$

Following the rule $\Rightarrow$-intro, we assume odd(n) (which means that we take as proven the fact that n is odd) and we try to conclude that $n+2$ must be odd.

However, to say that n is odd is to say that $n = 2k+1$ for some whole number, k. Now,

$$n + 2 = 2k + 1 + 2 = 2(k+1) + 1,$$

which means that $n+2$ is odd. (Here, $n = 2h+1$, with $h = k+1$, and $k+1$ is whole number since k is.)

Therefore, we proved that *if we assume* odd(n)*, then we can conclude* odd$(n+2)$, and according to our rule for proving implications, we have indeed proved the proposition

$$\mathrm{odd}(n) \Rightarrow \mathrm{odd}(n+2).$$

Note that the effect of rule $\Rightarrow$-intro is to *introduce* the premise, $\mathrm{odd}(n)$, which was temporarily assumed, into the left-hand side (we also say *antecedent*) of the proposition $\mathrm{odd}(n) \Rightarrow \mathrm{odd}(n+2)$.

This is why this rule is called *implication introduction*.

It should be noted that the above proof of the proposition $\mathrm{odd}(n) \Rightarrow \mathrm{odd}(n+2)$ *does not depend* on any premises (other than the implicit fact that we are assuming that n is a whole number).

In particular, this proof does not depend on the premise, $\mathrm{odd}(n)$, which was assumed (became "active") during our subproof step.

Thus, after having applied the rule $\Rightarrow$-intro, we should really make sure that the premise $\mathrm{odd}(n)$ which was made temporarily active is deactivated, or as we say, *discharged*.

When we write informal proofs, we rarely (if ever) explicitly discharge premises when we apply the rule $\Rightarrow$-intro but if we want to be rigorous we really should.

Also observe that if n is even, then the proposition $\mathrm{odd}(n) \Rightarrow \mathrm{odd}(n+2)$ *is still provable* (true), but it yields no information since the premise, $\mathrm{odd}(n)$, is not provable.

For a second example, we wish to prove the proposition $P \Rightarrow (Q \Rightarrow P)$.

According to our rule, we assume P as a premise and we try to prove $Q \Rightarrow P$ assuming P.

In order to prove $Q \Rightarrow P$, we assume Q as a new premise so the set of premises becomes $\{P, Q\}$, and then we try to prove P from P and Q.

This time, it should be obvious that P is provable since we assumed both P and Q.

Indeed, the rule that P is always provable from any set of assumptions including P itself is one of the basic *axioms* of our logic (which means that it is a rule that requires no justification whatsover).

So, we have obtained a proof of $P \Rightarrow (Q \Rightarrow P)$.

What is not entirely satisfactory about the above "proof" of $P \Rightarrow (Q \Rightarrow P)$ is that when the proof ends, the premises P and Q are still hanging around as "open" assumptions.

However, a proof should not depend on any "open" assumptions and to rectify this problem we introduce a mechanism of "discharging" or "closing" premises, as we already suggested in our previous example.

What this means is that certain rules of our logic are required to discard (the usual terminology is "discharge") certain occurrences of premises so that the resulting proof does not depend on these premises.

Technically, there are various ways of implementing the discharging mechanism but they all involve some form of tagging (with "new" variable).

For example, the rule formalizing the process that we have just described to prove an implication, $A \Rightarrow B$, known as *$\Rightarrow$-introduction*, uses a tagging mechanism described precisely in Definition 1.2.1.

Now, the rule that we have just described is not sufficient to prove certain propositions that should be considered provable under the "standard" intuitive meaning of implication.

For example, after a moment of thought, I think most people would want the proposition
$P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$ to be provable.

If we follow the procedure that we have advocated, we assume both P and $P \Rightarrow Q$ and we try to prove Q. For this, we need a new rule, namely:

If P and $P \Rightarrow Q$ are both provable, then Q is provable.

The above rule is known as the *$\Rightarrow$-elimination rule* (or *modus ponens*) and it is formalized in tree-form in Definition 1.2.1.

We now formalize our proof system.

We begin by defining a proof system in natural deduction style (a la Prawitz) for propositions built up from an "official set of atomic propositions", or set of *propositional symbols*,

$$\mathbf{PS} = \{\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3, \cdots\},$$

using only *implication*, ⇒, as a logical connective.

If P and Q are two propositions already built up, then

$$P \Rightarrow Q$$

is also a proposition. We use parentheses freely in order to disambiguate, so we may write $(P \Rightarrow Q)$ instead of $P \Rightarrow Q$. For example, $P \Rightarrow Q \Rightarrow R$ is ambiguous; it can be read as $(P \Rightarrow Q) \Rightarrow R$ or as $P \Rightarrow (Q \Rightarrow R)$.

Examples: $\mathbf{P}_1 \Rightarrow \mathbf{P}_2$ and $\mathbf{P}_1 \Rightarrow (\mathbf{P}_2 \Rightarrow \mathbf{P}_1)$.

Typically, we will use upper-case letters such as P, Q, R, S, A, B, C, etc., to denote arbitrary propositions formed using atoms from $\mathbf{PS}$.

We represent proofs and deductions as certain kinds of trees and view the logical rules (inference rules) as tree-building rules.

In the definition below, the expression Γ, P stands for the union of the multiset Γ and P. So, P may already belong to Γ. A picture such as

$$\begin{array}{c} \Delta \\ \mathcal{D} \\ P \end{array}$$

represents a deduction tree, $\mathcal{D}$, whose root is labeled with P and whose leaves are labeled with propositions from the *multiset* Δ (possibly with multiples occurrences of its members).

Some of the propositions in Δ may be tagged by variables.

The list of untagged propositions in Δ is the list of *premises* of the deduction tree. We often use an abbreviated version of the above notation where we omit the deduction, $\mathcal{D}$, and simply write

$$\begin{matrix}\Delta \\ P\end{matrix}$$

For example, in the deduction tree below,

$$\dfrac{\dfrac{P \Rightarrow (R \Rightarrow S) \qquad P}{R \Rightarrow S} \qquad \dfrac{Q \Rightarrow R \qquad \dfrac{P \Rightarrow Q \qquad P}{Q}}{R}}{S}$$

no leaf is tagged, so the premises form the multiset

$$\Delta = \{P \Rightarrow (R \Rightarrow S), P, Q \Rightarrow R, P \Rightarrow Q, P\},$$

with two occurrences of P, and the conclusion is S.

Definition 1.2.1 The *axioms, inference rules and deduction trees* for *implicational logic* are defined as follows:

Axioms:

(i) Every one-node tree labeled with a single proposition, P, is a deduction tree for P with set of premises, $\{P\}$.

(ii) The tree

$$\frac{\Gamma, P}{P}$$

is a deduction tree for P with multiset set of premises, $\Gamma \cup \{P\}$.

The above is a concise way of denoting a two-node tree with its leaf labeled with the multiset consisting of P and the propositions in Γ, each of these proposition (including P) having possibly multiple occurrences but at least one, and whose root is labeled with P.

A more explicit form is

$$\frac{\overbrace{P_1, \cdots, P_1}^{k_1}, \cdots, \overbrace{P_i, \cdots, P_i}^{k_i}, \cdots, \overbrace{P_n, \cdots, P_n}^{k_n}}{P_i}$$

where $k_1, \ldots, k_n \geq 1$ and $n \geq 1$.

This axiom says that we always have a deduction of P_i from any set of premises including P_i.

The $\Rightarrow$*-introduction rule*:

If $\mathcal{D}$ is a deduction tree for Q from the premises in $\Gamma \cup \{P\}$, then

$$\frac{\begin{array}{c}\Gamma, P^x\\ \mathcal{D}\\ Q\end{array}}{P \Rightarrow Q}\; x$$

is a deduction tree for $P \Rightarrow Q$ from Γ.

Note that this inference rule has the additional effect of discharging some occurrences of the premise, P.

These occurrences are tagged with a new variable, x, and the tag x is also placed immediately to the right of the inference bar.

This is a reminder that the deduction tree whose conclusion is $P \Rightarrow Q$ no longer has the occurrences of P labeled with x as premises.

The $\Rightarrow$-*elimination rule*:

If $\mathcal{D}_1$ is a deduction tree for $P \Rightarrow Q$ from the premises, Γ, and $\mathcal{D}_2$ is a deduction for P from the premises, Δ, then

$$\frac{\begin{array}{cc} \Gamma & \Delta \\ \mathcal{D}_1 & \mathcal{D}_2 \\ P \Rightarrow Q & P \end{array}}{Q}$$

is a deduction tree for Q from the premises in $\Gamma \cup \Delta$. This rule is also known as *modus ponens*.

In the above axioms and rules, Γ or Δ may be empty, P, Q denote arbitrary propositions built up from the atoms in **PS** and $\mathcal{D}$, $\mathcal{D}_1$ and $\mathcal{D}_2$ denote deductions, possibly a one-node tree.

A *deduction tree* is either a one node tree labeled with a single proposition or a tree constructed using the above axioms and rules.

A *proof tree* is a deduction tree such that *all its premises are discharged*.

The above proof system is denoted $\mathcal{N}_m^{\Rightarrow}$ (here, the subscript m stands for *minimal*, referring to the fact that this a bare-bone logical system).

In words, the $\Rightarrow$-introduction rule says that in order to prove an implication $P \Rightarrow Q$ from a set of premises Γ, we assume that P has already been proved, add P to the premises in Γ and then prove Q from Γ and P.

Once this is done, the premise P is deleted. This rule formalizes the kind of reasoning that we all perform whenever we prove an implication statement.

In that sense, it is a natural and familiar rule, except that we perhaps never stopped to think about what we are really doing.

However, the business about discharging the premise P when we are through with our argument is a bit puzzling.

Most people probably never carry out this "discharge step" consciously, but such a process does take place implicitly.

It might help to view the action of proving an implication $P \Rightarrow Q$ as the construction of a program that converts a proof of P into a proof of Q.

Then, if we supply a proof of P as input to this program (the proof of $P \Rightarrow Q$), it will output a proof of Q.

So, if we don't give the right kind of input to this program, for example, a "wrong proof" of P, we should not expect that the program return a proof of Q.

However, this does not say that the program is incorrect; the program was designed to do the right thing only if it is given the right kind of input.

☡

1. Only the leaves of a deduction tree may be discharged. Interior nodes, including the root, are *never* discharged.
2. Once a set of leaves labeled with some premise P marked with the label x has been discharged, none of these leaves can be discharged again. So, each label (say x) can only be used once. This corresponds to the fact that some leaves of our deduction trees get "killed off" (discharged).

3. A proof is a deduction tree whose leaves are *all discharged* (Γ is empty). This corresponds to the philosophy that if a proposition has been proved, then the validity of the proof should not depend on any assumptions that are still active.

   We may think of a deduction tree as an unfinished proof tree.

4. When constructing a proof tree, we have to be careful not to include (accidently) extra premises that end up not beeing discharged. If this happens, we probably made a mistake and the redundant premises should be deleted.

   On the other hand, if we have a proof tree, we can always add extra premises to the leaves and create a new proof tree from the previous one by discharging all the new premises.

5. Beware, when we deduce that an implication $P \Rightarrow Q$ is provable, we **do not** prove that P **and** Q are provable; we only prove that **if** P is provable **then** Q is provable.

Examples of proof trees.

(a)

$$\dfrac{\dfrac{P^x}{P}}{P \Rightarrow P}\; x$$

So, $P \Rightarrow P$ is provable; this is the least we should expect from our proof system!

(b)

$$\dfrac{\dfrac{\dfrac{\dfrac{(Q \Rightarrow R)^y \qquad \dfrac{(P \Rightarrow Q)^z \quad P^x}{Q}}{R}}{P \Rightarrow R}\; x}{(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)}\; y}{(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))}\; z$$

In order to better appreciate the difference between a deduction tree and a proof tree, consider the following two examples:

1. The tree below is a deduction tree, since two its leaves are labeled with the premises $P \Rightarrow Q$ and $Q \Rightarrow R$, that have not been discharged yet.

So, this tree represents a deduction of $P \Rightarrow R$ from the set of premises $\Gamma = \{P \Rightarrow Q, Q \Rightarrow R\}$ but it is *not a proof tree* since $\Gamma \neq \emptyset$. However, observe that the original premise, P, labeled x, has been discharged.

$$\dfrac{\dfrac{Q \Rightarrow R \qquad \dfrac{P \Rightarrow Q \qquad P^x}{Q}}{R}}{P \Rightarrow R}\; x$$

2. The next tree was obtained from the previous one by applying the $\Rightarrow$-introduction rule which triggered the discharge of the premise $Q \Rightarrow R$ labeled y, which is no longer active.

However, the premise $P \Rightarrow Q$ is still active (has not been discharged, yet), so the tree below is a deduction tree of $(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$ from the set of premises $\Gamma = \{P \Rightarrow Q\}$. It is not yet a proof tree since $\Gamma \neq \emptyset$.

$$\dfrac{\dfrac{\dfrac{(Q \Rightarrow R)^y \qquad \dfrac{P \Rightarrow Q \qquad P^x}{Q}}{R}}{P \Rightarrow R}\; x}{(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)}\; y$$

Finally, one more application of the $\Rightarrow$-introduction rule will discharged the premise $P \Rightarrow Q$, at last, yielding the proof tree in (b).

(c) This example illustrates the fact that different proof trees may arise from the same set of premises, $\{P, Q\}$: For example,

$$\cfrac{\cfrac{\cfrac{P^x, Q^y}{P}}{P \Rightarrow P}\; x}{Q \Rightarrow (P \Rightarrow P)}\; y$$

and

$$\cfrac{\cfrac{\cfrac{P^x, Q^y}{P}}{Q \Rightarrow P}\; y}{P \Rightarrow (Q \Rightarrow P)}\; x$$

Similarly, there are six proof trees with a conclusion of the form

$$A \Rightarrow (B \Rightarrow (C \Rightarrow P))$$

begining with the deduction

$$\frac{P^x, Q^y, R^z}{P}$$

corresponding to the six permutations of the premises, P, Q, R.

Note that we would not have been able to construct the above proofs if Axiom (ii),

$$\frac{\Gamma, P}{P}$$

was not available. We need a mechanism to "stuff" more premises into the leaves of our deduction trees in order to be able to discharge them later on.

We may also view Axiom (ii) as a *weakening rule* whose purpose is to weaken a set of assumptions.

Even though we are assuming all of the proposition in Γ and P, we only retain the assumption P.

The necessity of allowing multisets of premises is illustrated by the following proof of the proposition $P \Rightarrow (P \Rightarrow (Q \Rightarrow (Q \Rightarrow (P \Rightarrow P))))$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P^u, P^v, P^y, Q^w, Q^x}{P}}{P \Rightarrow P}\; y}{Q \Rightarrow (P \Rightarrow P)}\; x}{Q \Rightarrow (Q \Rightarrow (P \Rightarrow P))}\; w}{P \Rightarrow (Q \Rightarrow (Q \Rightarrow (P \Rightarrow P)))}\; v}{P \Rightarrow (P \Rightarrow (Q \Rightarrow (Q \Rightarrow (P \Rightarrow P))))}\; u$$

(d) In the next example, the two occurrences of A labeled x are discharged simultaneously.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{(A \Rightarrow (B \Rightarrow C))^z \quad A^x}{B \Rightarrow C} \qquad \cfrac{(A \Rightarrow B)^y \quad A^x}{B}}{C}}{A \Rightarrow C}\; x}{(A \Rightarrow B) \Rightarrow (A \Rightarrow C)}\; y}{\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)}\; z$$

(e) In contrast to Example (d), in the proof tree below the two occurrences of A are discharged separately. To this effect, they are labeled differently.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(A \Rightarrow (B \Rightarrow C))^z \qquad A^x}{B \Rightarrow C} \qquad \dfrac{(A \Rightarrow B)^y \qquad A^t}{B}}{C}}{A \Rightarrow C}\; x}{(A \Rightarrow B) \Rightarrow (A \Rightarrow C)}\; y}{\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)}\; z}{A \Rightarrow \Big(\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)\Big)}\; t$$

The process of discharging premises when constructing a deduction is admittedly a bit confusing.

Part of the problem is that a deduction tree really represents the last of a sequence of stages (corresponding to the application of inference rules) during which the current set of "active" premises, that is, those premises that have not yet been discharged (closed, cancelled) evolves (in fact, shrinks).

Some mechanism is needed to keep track of which premises are no longer active and this is what this business of labeling premises with variables achieves.

Historically, this is the first mechanism that was invented. However, Gentzen (in the 1930's) came up with an alternative solution which is mathematically easier to handle.

Moreover, it turns out that this notation is also better suited to computer implementations, if one wishes to implement an automated theorem prover.

The point is to keep a record of all undischarged assumptions at every stage of the deduction.

Thus, a deduction is now a tree whose nodes are labeled with expressions of the form $\Gamma \rightarrow P$, called *sequents*, where P is a proposition, and Γ is a record of all undischarged assumptions at the stage of the deduction associated with this node.

During the construction of a deduction tree, it is necessary to discharge packets of assumptions consisting of one or more occurrences of the same proposition.

To this effect, it is convenient to tag packets of assumptions with labels, in order to discharge the propositions in these packets in a single step.

We use variables for the labels, and a packet labeled with x consisting of occurrences of the proposition P is written as $x\colon P$.

Thus, in a sequent $\Gamma \rightarrow P$, the expression Γ is any finite set of the form

$$x_1\colon P_1, \ldots, x_m\colon P_m,$$

where the x_i are pairwise distinct (but the P_i need not be distinct).

Given $\Gamma = x_1\colon P_1, \ldots, x_m\colon P_m$, the notation $\Gamma, x\colon P$ is only well defined when $x \neq x_i$ for all i, $1 \leq i \leq m$, in which case it denotes the set

$$x_1\colon P_1, \ldots, x_m\colon P_m, x\colon P.$$

Using sequents, the axioms and rules of Definition 1.2.2 are now expressed as follows:

Definition 1.2.2 The *axioms and inference rules* of the system $\mathcal{NG}_m^{\Rightarrow}$ (*implicational logic, Gentzen-sequent style (the $\mathcal{G}$ in $\mathcal{NG}$ stands for Gentzen)*) are listed below:

$$\Gamma, x \colon P \to P \quad \text{(Axioms)}$$

$$\frac{\Gamma, x \colon P \to Q}{\Gamma \to P \Rightarrow Q} \quad (\Rightarrow\text{-}\mathit{intro})$$

$$\frac{\Gamma \to P \Rightarrow Q \quad \Gamma \to P}{\Gamma \to Q} \quad (\Rightarrow\text{-}\mathit{elim})$$

In an application of the rule ($\Rightarrow$-*intro*), observe that in the lower sequent, the proposition P (labeled x) is deleted from the list of premises occurring on the left-hand side of the arrow in the upper sequent.

We say that the proposition P which appears as a hypothesis of the deduction is *discharged* (or *closed*).

A *deduction tree* is either a one-node tree labeled with an axiom or a tree constructed using the above inference rules.

A *proof tree* is a deduction tree whose conclusion is a sequent with an empty set of premises (a sequent of the form $\emptyset \to P$).

It is important to note that the ability to label packets consisting of occurrences of the same proposition with different labels is essential, in order to be able to have control over which groups of packets of assumptions are discharged simultaneously.

Equivalently, we could avoid tagging packets of assumptions with variables if we assumed that in a sequent $\Gamma \to C$, the expression Γ, also called a *context*, is a *multiset* of propositions.

Let us display the proof tree for the second proof tree in Example (c) in our new Gentzen-sequent system. The orginal proof tree is

$$\cfrac{\cfrac{\cfrac{P^x, Q^y}{P}}{Q \Rightarrow P}\quad y}{P \Rightarrow (Q \Rightarrow P)}\quad x$$

and the corresponding proof tree in our new system is

$$\dfrac{\dfrac{x\colon P, y\colon Q \to P}{x\colon P \to Q \Rightarrow P}}{\to P \Rightarrow (Q \Rightarrow P)}$$

Observe how the set of premises on the lefthand side of every sequent in the tree (the Γ in $\Gamma \to P$) keeps track of the multiset of "active" premises.

Here is a proof of the third example given above in our new system. Let

$$\Gamma = x\colon A \Rightarrow (B \Rightarrow C), y\colon A \Rightarrow B, z\colon A.$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \to A \Rightarrow (B \Rightarrow C) \quad \Gamma \to A}{\Gamma \to B \Rightarrow C} \quad \dfrac{\Gamma \to A \Rightarrow B \quad \Gamma \to A}{\Gamma \to B}}{x\colon A \Rightarrow (B \Rightarrow C), y\colon A \Rightarrow B, z\colon A \to C}}{x\colon A \Rightarrow (B \Rightarrow C), y\colon A \Rightarrow B \to A \Rightarrow C}}{x\colon A \Rightarrow (B \Rightarrow C) \to (A \Rightarrow B) \Rightarrow (A \Rightarrow C)}}{\to \big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)}$$

Remark: An attentive reader will have surely noticed that the second version of the ⇒-elimination rule,

$$\frac{\Gamma \to P \Rightarrow Q \quad \Gamma \to P}{\Gamma \to Q} \quad (\Rightarrow\textit{-elim}),$$

differs slightly from the first version given in Definition 1.2.1.

Indeed, in Prawitz's style, the rule that matches exactly the ⇒-elim rule above is

$$\frac{\begin{array}{c}\Gamma \\ \mathcal{D}_1 \\ P \Rightarrow Q\end{array} \quad \begin{array}{c}\Gamma \\ \mathcal{D}_2 \\ P\end{array}}{Q}$$

where the deductions of $P \Rightarrow Q$ and P have the *same* set of premises, Γ.

Equivalently, the rule in sequent-format that corresponds to the ⇒-elimination rule of Definition 1.2.1 is

$$\frac{\Gamma \to P \Rightarrow Q \quad \Delta \to P}{\Gamma, \Delta \to Q} \quad (\Rightarrow\textit{-elim'}),$$

where Γ, Δ must be interpreted as the union of Γ and Δ.

A moment of reflexion will reveal that the resulting proofs systems are equivalent (that is, every proof in one system can converted to a proof in the other system).

The version of the ⇒-elimination rule in Definition 1.2.1 may be considered preferable because it gives us the ability to make the sets of premises labeling leaves smaller.

On the other hand, after experimenting with the construction of proofs, one gets the feeling that every proof can be simplified to a "unique minimal" proof, if we define "minimal" in a suitable sense, namely, that a minimal proof never contains an elimination rule immediately following an introduction rule.

Then, it turns out that to define the notion of uniqueness of proofs, the second version is preferable.

However, it is important to realize that in general, a proposition may possess distinct minimal proofs!

In principle, it does not matter which of the two systems $\mathcal{N}_m^{\Rightarrow}$ or $\mathcal{NG}_m^{\Rightarrow}$ we use to construct deductions; it is a matter of taste. My experience is that I make fewer mistakes with the Gentzen-sequent style system $\mathcal{NG}_m^{\Rightarrow}$.

$K_{v}+\sqrt[3]{\frac{N}{4}}\cdot\sum(\frac{2}{5})\frac{\pi}{9-C^2}$
$3.6^{\pi}_{b}\hat{\Delta}\frac{R}{c\,8}\rightarrow 7.3^{K}(Z\frac{n_i}{\tau})^{R}$
$\chi^3_{6N}\leq B+\sqrt{5e}=2.6^{R^3}_{\pi^4}$

© 1973 *The New Yorker* Magazine, Inc.

Figure 1.12: Math jokes

1.3 Adding $\wedge$, $\vee$, $\perp$; The Proof Systems $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ and $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$

In order to deal with negation, we introduce the symbol, $\perp$, which corresponds to falsity (the atomic statement always false).

The symbol $\perp$ is also called *absurdity* or *falsum*.

We define $\neg P$ (the *negation* of P) as the implication $P \Rightarrow \perp$.

Our propositions are now built up from the propositional symbols in **PS** using the logical connectives, $\Rightarrow$, $\wedge$, $\vee$ and $\neg$ (using $\perp$). Thus, if P and Q are propositions, so are

1. $P \Rightarrow Q$
2. $P \wedge Q$
3. $P \vee Q$
4. $\perp$, and
5. $\neg P$.

Definition 1.3.1 The *axioms, inference rules and deduction trees* for *(propositional) classical logic* are:

Axioms:

(i) Every one-node tree labeled with a single proposition, P, is a deduction tree for P with set of premises, $\{P\}$.

(ii) The tree

$$\frac{\Gamma, P}{P}$$

is a deduction tree for P with multiset of premises, $\Gamma \cup \{P\}$.

The *⇒-introduction rule*:

If $\mathcal{D}$ is a deduction of Q from the premises in $\Gamma \cup \{P\}$, then

$$\dfrac{\begin{array}{c}\Gamma, P^x\\ \mathcal{D}\\ Q\end{array}}{P \Rightarrow Q}\ x$$

is a deduction tree for $P \Rightarrow Q$ from Γ. All premises, P, labeled x are discharged.

The *⇒-elimination rule (or modus ponens)*:

If $\mathcal{D}_1$ is a deduction tree for $P \Rightarrow Q$ from the premises, Γ, and $\mathcal{D}_2$ is a deduction for P from the premises, Δ, then

$$\dfrac{\begin{array}{cc}\Gamma & \Delta\\ \mathcal{D}_1 & \mathcal{D}_2\\ P \Rightarrow Q & P\end{array}}{Q}$$

is a deduction tree for Q from the premises in $\Gamma \cup \Delta$.

The $\land$-*introduction rule*:

If $\mathcal{D}_1$ is a deduction tree for P from the premises, Γ, and $\mathcal{D}_2$ is a deduction for Q from the premises, Δ, then

$$\frac{\begin{matrix}\Gamma & \Delta \\ \mathcal{D}_1 & \mathcal{D}_2 \\ P & Q\end{matrix}}{P \land Q}$$

is a deduction tree for $P \land Q$ from the premises in $\Gamma \cup \Delta$.

The $\land$-*elimination rule*:

If $\mathcal{D}$ is a deduction tree for $P \land Q$ from the premises, Γ, then

$$\frac{\begin{matrix}\Gamma \\ \mathcal{D} \\ P \land Q\end{matrix}}{P} \qquad\qquad \frac{\begin{matrix}\Gamma \\ \mathcal{D} \\ P \land Q\end{matrix}}{Q}$$

are deduction trees for P and Q from the premises, Γ.

The $\vee$-*introduction rule*:

If $\mathcal{D}$ is a deduction tree for P or for Q from the premises, Γ, then

$$\frac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ P\end{array}}{P \vee Q} \qquad\qquad \frac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ Q\end{array}}{P \vee Q}$$

are deduction trees for $P \vee Q$ from the premises in Γ.

The $\vee$-*elimination rule*:

If $\mathcal{D}_1$ is a deduction tree for $P \vee Q$ from the premises, Γ, $\mathcal{D}_2$ is a deduction for R from the premises in $\Delta \cup \{P\}$ and $\mathcal{D}_3$ is a deduction for R from the premises in $\Lambda \cup \{Q\}$, then

$$\frac{\begin{array}{ccc}\Gamma & \Delta, P^x & \Lambda, Q^y\\ \mathcal{D}_1 & \mathcal{D}_2 & \mathcal{D}_3\\ P \vee Q & R & R\end{array}}{R}\;{\scriptstyle x,y}$$

is a deduction tree for R from the premises in $\Gamma \cup \Delta \cup \Lambda$.

All premises, P, labeled x and all premises, Q, labeled y are discharged.

The $\perp$-*elimination rule*:

If $\mathcal{D}$ is a deduction tree for $\perp$ from the premises, Γ, then

$$\begin{array}{c} \Gamma \\ \mathcal{D} \\ \dfrac{\perp}{P} \end{array}$$

is a deduction tree for P from the premises, Γ, for *any* proposition, P.

The *proof-by-contradiction rule* (also known as *reductio ad absurdum rule*, for short *RAA*):

If $\mathcal{D}$ is a deduction tree for $\perp$ from the premises in $\Gamma \cup \{\neg P\}$, then

$$\dfrac{\begin{array}{c}\Gamma, \neg P^x \\ \mathcal{D} \\ \perp\end{array}}{P}\, x$$

is a deduction tree for P from the premises, Γ. All premises, $\neg P$, labeled x are discharged.

Since $\neg P$ is an abbreviation for $P \Rightarrow \perp$, the $\neg$-introduction rule is a special case of the $\Rightarrow$-introduction rule (with $Q = \perp$). However, it is worth stating it explicitly:

The *$\neg$-introduction rule*:

If $\mathcal{D}$ is a deduction tree for $\perp$ from the premises in $\Gamma \cup \{P\}$, then

$$\cfrac{\begin{array}{c}\Gamma, P^x \\ \mathcal{D} \\ \perp\end{array}}{\neg P}\; x$$

is a deduction tree for $\neg P$ from the premises, Γ. All premises, P, labeled x are discharged.

The above rule can be viewed as a proof-by-contradiction principle applied to negated propositions.

Similarly, the $\neg$-elimination rule is a special case of $\Rightarrow$-elimination applied to $\neg P$ ($= P \Rightarrow \perp$) and P:

The *$\neg$-elimination rule*:

If $\mathcal{D}_1$ is a deduction tree for $\neg P$ from the premises, Γ, and $\mathcal{D}_2$ is a deduction for P from the premises, Δ, then

$$\frac{\begin{array}{cc} \Gamma & \Delta \\ \mathcal{D}_1 & \mathcal{D}_2 \\ \neg P & P \end{array}}{\perp}$$

is a deduction tree for $\perp$ from the premises in $\Gamma \cup \Delta$.

In the above axioms and rules, Γ, Δ or Λ may be empty, P, Q, R denote arbitrary propositions built up from the atoms in **PS**, $\mathcal{D}$, $\mathcal{D}_1$, $\mathcal{D}_2$ denote deductions, possibly a one-node tree, and all the premises labeled x or y are discharged.

A *deduction tree* is either a one-node tree labeled with a single proposition or a tree constructed using the above axioms and inference rules.

A *proof tree* is a deduction tree such that *all its premises* are discharged. The above proof system is denoted $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (here, the subscript c stands for *classical*).

The system obtained by removing the proof-by-contradiction (RAA) rule is called *(propositional) intuitionistic logic* and is denoted $\mathcal{N}_i^{\Rightarrow,\wedge,\vee,\perp}$.

The system obtained by deleting both the $\perp$-elimination rule and the proof-by-contradiction rule is called *(propositional) minimal logic* and is denoted $\mathcal{N}_m^{\Rightarrow,\wedge,\vee,\perp}$.

The version of $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ in terms of Gentzen sequents is the following:

Definition 1.3.2 The *axioms and inference rules* of the system $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$ (of *propositional classical logic, Gentzen-sequent style*) are listed below:

$$\Gamma, x \colon P \to P \quad \text{(Axioms)}$$

$$\frac{\Gamma, x \colon P \to Q}{\Gamma \to P \Rightarrow Q} \quad (\Rightarrow\textit{-intro})$$

$$\frac{\Gamma \to P \Rightarrow Q \quad \Gamma \to P}{\Gamma \to Q} \quad (\Rightarrow\textit{-elim})$$

$$\frac{\Gamma \to P \quad \Gamma \to Q}{\Gamma \to P \wedge Q} \quad (\wedge\textit{-intro})$$

$$\frac{\Gamma \to P \wedge Q}{\Gamma \to P} \quad (\wedge\textit{-elim}) \qquad \frac{\Gamma \to P \wedge Q}{\Gamma \to Q} \quad (\wedge\textit{-elim})$$

$$\frac{\Gamma \to P}{\Gamma \to P \vee Q} \quad (\vee\textit{-intro}) \qquad \frac{\Gamma \to Q}{\Gamma \to P \vee Q} \quad (\vee\textit{-intro})$$

$$\frac{\Gamma \to P \vee Q \quad \Gamma, x \colon P \to R \quad \Gamma, y \colon Q \to R}{\Gamma \to R} \quad (\vee\textit{-elim})$$

$$\frac{\Gamma \to \perp}{\Gamma \to P} \quad (\perp\textit{-elim})$$

$$\frac{\Gamma, x \colon \neg P \to \perp}{\Gamma \to P} \quad (\textit{by-contra})$$

$$\frac{\Gamma, x\colon P \to \perp}{\Gamma \to \neg P} \quad (\neg\text{-introduction})$$

$$\frac{\Gamma \to \neg P \quad \Gamma \to P}{\Gamma \to \perp} \quad (\neg\text{-elimination})$$

Since the rule ($\perp$-*elim*) is trivial (does nothing) when $P = \perp$, from now on, we will assume that $P \neq \perp$.

A *deduction tree* is a tree whose interior nodes correspond to inference rules and whose leaves are axioms and a *proof tree* is a deduction tree whose conclusion is a sequent with an empty set of premises (a sequent of the form $\emptyset \to P$).

Propositional minimal logic, denoted $\mathcal{N}\mathcal{G}_m^{\Rightarrow,\wedge,\vee,\perp}$, is obtained by dropping the ($\perp$-*elim*) and (*by-contra*) rules.

Propositional intuitionistic logic, denoted $\mathcal{N}\mathcal{G}_i^{\Rightarrow,\wedge,\vee,\perp}$, is obtained by dropping the (*by-contra*) rule.

When we say that a proposition, P, is *provable from* Γ, we mean that we can construct a proof tree whose conclusion is P and whose set of premises is Γ, in one of the systems $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$.

Therefore, when we use the word "provable" unqualified, we mean provable in *classical logic*.

If P is provable from Γ in one of the intuitionistic systems $\mathcal{N}_i^{\Rightarrow,\wedge,\vee,\perp}$ or $\mathcal{NG}_i^{\Rightarrow,\wedge,\vee,\perp}$, then we say *intuitionistically provable* (and similarly, if P is provable from Γ in one of the systems $\mathcal{N}_m^{\Rightarrow,\wedge,\vee,\perp}$ or $\mathcal{NG}_m^{\Rightarrow,\wedge,\vee,\perp}$, then we say *provable in minimal logic*).

When P is provable from Γ, most people write $\Gamma \vdash P$, or $\vdash \Gamma \rightarrow P$, sometimes with the name of the corresponding proof system tagged as a subscript on the sign $\vdash$ if necessary to avoid ambiguities.

When Γ is empty, we just say P is provable (provable in intuitionistic logic, etc.) and write $\vdash P$.

We treat *logical equivalence* as a derived connective, that is, we view $P \equiv Q$ as an abbreviation for
$(P \Rightarrow Q) \land (Q \Rightarrow P)$.

In view of the inference rules for $\land$, we see that to prove a logical equivalence $P \equiv Q$, we just have to prove both implications $P \Rightarrow Q$ and $Q \Rightarrow P$.

In view of the $\neg$-elimination rule, we may be tempted to interpret the provability of a negation, $\neg P$, is as "P is not provable".

Indeed, if $\neg P$ and P were both provable, then $\perp$ would be provable. So, P should not be provable if $\neg P$ is.

However, if P is not provable, then $\neg P$ is **not** provable in general! There are plenty of propositions such that neither P nor $\neg P$ is provable (for instance, P, with P an atomic proposition).

Thus, the fact that P is not provable is not equivalent to the provability of $\neg P$ and we should not interpret $\neg P$ as "P is not provable".

Let us now make some (much-needed) comments about the above inference rules. There is no need to repeat our comments regarding the $\Rightarrow$-rules.

The $\wedge$-introduction rule says that in order to prove a conjunction $P \wedge Q$ from some premises Γ, all we have to do is to prove *both* that P is provable from Γ *and* that Q is provable from Γ.

The $\wedge$-elimination rule says that once we have proved $P \wedge Q$ from Γ, then P (and Q) is also provable from Γ. This makes sense intuitively as $P \wedge Q$ is “stronger” than P and Q separately ($P \wedge Q$ is true iff both P and Q are true).

The $\vee$-introduction rule says that if P (or Q) has been proved from Γ, then $P \vee Q$ is also provable from Γ. Again, this makes sense intuitively as $P \vee Q$ is “weaker” than P and Q.

The $\vee$-elimination rule formalizes the *proof-by-cases* method. It is a more subtle rule.

The idea is that if we know that in the case where P is already assumed to be provable and similarly in the case where Q is already assumed to be provable that we can prove R (also using premises in Γ), then if $P \vee Q$ is also provable from Γ, as we have “covered both cases”, it should be possible to prove R from Γ only (i.e., the premises P and Q are discarded).

The $\perp$-elimination rule formalizes the principle that once a false statement has been established, then anything should be provable.

The proof-by-contradiction rule formalizes the method of proof by contradiction!

That is, in order to prove that P can be deduced from some premises Γ, one may assume the negation, $\neg P$, of P (intuitively, assume that P is false) and then derive a contradiction from Γ and $\neg P$ (i.e., derive falsity). Then, P actually follows from Γ *without using $\neg P$ as a premise*, i.e., $\neg P$ is discharged.

Most people, I believe, will be comfortable with the rules of minimal logic and will agree that they constitute a “reasonable” formalization of the rules of reasoning involving $\Rightarrow$, $\wedge$ and $\vee$.

Indeed, these rules seem to express the intuitive meaning of the connectives $\Rightarrow$, $\wedge$ and $\vee$.

However, some may question the two rules $\perp$-elimination and proof-by-contradiction.

Indeed, their meaning is not as clear and, certainly, the proof-by-contradiction rule introduces a form of indirect reasoning that is somewhat worrisome.

The problem has to do with the meaning of disjunction and negation and more generally, with the notion of *constructivity* in mathematics.

In fact, in the early 1900's, some mathematicians, especially L. Brouwer (1881-1966), questioned the validity of the proof-by-contradiction rule, among other principles.

Two specific cases illustrate the problem, namely, the propositions

$$P \vee \neg P \quad \text{and} \quad \neg\neg P \Rightarrow P.$$

As we will see shortly, the above propositions are both provable in classical logic.

Now, Brouwer and some mathematicians belonging to his school of thoughts (the so-called "intuitionsists" or "constructivists") advocate that in order to prove a disjunction, $P \vee Q$ (from some premises Γ) one has to either exhibit a proof of P or a proof or Q (from Γ).

However, it can be shown that this fails for $P \vee \neg P$. The fact that $P \vee \neg P$ is provable (in classical logic) **does not** imply (in general) that either P is provable or that $\neg P$ is provable!

That $P \vee \neg P$ is provable is sometimes called the *principle of the excluded middle*!

In intuitionistic logic, $P \vee \neg P$ is **not** provable (in general). Of course, if one gives up the proof-by-contradiction rule, then fewer propositions become provable.

On the other hand, one may claim that the propositions that remain provable have more constructive proofs and thus, feels on safer grounds.

A similar controversy arises with $\neg\neg P \Rightarrow P$. If we give up the proof-by-contradiction rule, then this formula is no longer provable, i.e., $\neg\neg P$ is no longer equivalent to P.

However, note that one can still prove $P \Rightarrow \neg\neg P$ in minimal logic (try doing it!).

Even stranger, $\neg\neg\neg P \Rightarrow \neg P$ is provable in intuitionistic (and minimal) logic, so $\neg\neg\neg P$ and $\neg P$ are equivalent intuitionistically!

Remark: Suppose we have a deduction

$$\begin{array}{c}\Gamma, \neg P\\ \mathcal{D}\\ \perp\end{array}$$

as in the proof by contradiction rule.

Then, by $\neg$-introduction, we get a deduction of $\neg\neg P$ from Γ:

$$\dfrac{\begin{array}{c}\Gamma, \neg P^x\\ \mathcal{D}\\ \perp\end{array}}{\neg\neg P}\ x$$

So, if we knew that $\neg\neg P$ was equivalent to P (actually, if we knew that $\neg\neg P \Rightarrow P$ is provable) then the proof by contradiction rule would be justified as a valid rule (it follows from modus ponens).

We can view the proof by contradiction rule as a sort of act of faith that consists in saying that if we can derive an inconsistency (i.e., chaos) by assuming the falsity of a statement P, then P has to hold in the first place.

It not so clear that such an act of faith is justified and the intuitionists refuse to take it!

In the rest of this section, we make further useful remarks about (classical) logic and give some explicit examples of proofs illustrating the inference rules of classical logic. We begin by proving that $P \lor \neg P$ is provable in classical logic.

Proposition 1.3.3 *The proposition $P \lor \neg P$ is provable in classical logic.*

Proof. We prove that $P \lor (P \Rightarrow \bot)$ is provable by using the proof-by-contradiction rule as shown below:

$$\dfrac{\dfrac{((P \lor (P \Rightarrow \bot)) \Rightarrow \bot)^y \qquad \dfrac{\dfrac{\dfrac{((P \lor (P \Rightarrow \bot)) \Rightarrow \bot)^y \qquad \dfrac{P^x}{P \lor (P \Rightarrow \bot)}}{\bot}}{P \Rightarrow \bot}\; x}{P \lor (P \Rightarrow \bot)}}{\bot}}{P \lor (P \Rightarrow \bot)}\; y \text{ (by-contra)}$$

□

Next, we consider the equivalence of P and $\neg\neg P$.

Proposition 1.3.4 *The proposition $P \Rightarrow \neg\neg P$ is provable in minimal logic. The proposition $\neg\neg P \Rightarrow P$ is provable in classical logic. Therefore, in classical logic, P is equivalent to $\neg\neg P$.*

Proof. We leave that $P \Rightarrow \neg\neg P$ is provable in minimal logic as an exercise. Below is a proof of $\neg\neg P \Rightarrow P$ using the proof-by-contradiction rule:

$$\dfrac{\dfrac{\dfrac{((P \Rightarrow \bot) \Rightarrow \bot)^y \quad (P \Rightarrow \bot)^x}{\bot}}{P}\; x \ \text{(by-contra)}}{((P \Rightarrow \bot) \Rightarrow \bot) \Rightarrow P}\; y$$

□

The next proposition shows why $\bot$ can be viewed as the "ultimate" contradiction.

Proposition 1.3.5 *In intuitionistic logic, the propositions $\bot$ and $P \land \neg P$ are equivalent for all P. Thus, $\bot$ and $P \land \neg P$ are also equivalent in classical propositional logic*

Proof. We need to show that both $\bot \Rightarrow (P \land \neg P)$ and $(P \land \neg P) \Rightarrow \bot$ are provable in intuitionistic logic.

The provability of $\bot \Rightarrow (P \wedge \neg P)$ is an immediate consequence or $\bot$-elimination, with $\Gamma = \emptyset$. For $(P \wedge \neg P) \Rightarrow \bot$, we have the following proof:

$$\dfrac{\dfrac{\dfrac{(P \wedge \neg P)^x}{\neg P} \qquad \dfrac{(P \wedge \neg P)^x}{P}}{\bot}}{(P \wedge \neg P) \Rightarrow \bot}\; x$$

□

So, in intuitionistic logic (and also in classical logic), $\bot$ is equivalent to $P \wedge \neg P$ for all P.

This means that $\bot$ is the "ultimate" contradiction, it corresponds to total inconsistency.

1.4 Clearing Up Differences Between ¬-introduction, ⊥-elimination and RAA

The differences between the rules, ¬-introduction, ⊥-elimination and the proof by contradiction rule (RAA) are often unclear to the uninitiated reader and this tends to cause confusion.

In this section, we will try to clear up some common misconceptions about these rules.

Confusion 1. Why is RAA not a special case of ¬-introduction?

$$\dfrac{\begin{array}{c}\Gamma, P^x\\ \mathcal{D}\\ \bot\end{array}}{\neg P}\ x\,(\neg\text{-intro}) \qquad\qquad \dfrac{\begin{array}{c}\Gamma, \neg P^x\\ \mathcal{D}\\ \bot\end{array}}{P}\ x\,(\text{RAA})$$

The only apparent difference between ¬-introduction (on the left) and RAA (on the right) is that in RAA, the premise P is negated but the conclusion is not, whereas in ¬-introduction the premise P is not negated but the conclusion is.

The important difference is that the conclusion of RAA is **not** negated. If we had applied ¬-introduction instead of RAA on the right, we would have obtained

$$\dfrac{\begin{array}{c}\Gamma, \neg P^x \\ \mathcal{D} \\ \perp\end{array}}{\neg\neg P}\; x\,(\neg\text{-intro})$$

where the conclusion would have been $\neg\neg P$ as opposed to P.

However, as we already said earlier, $\neg\neg P \Rightarrow P$ is **not** provable intuitionistically.

Consequenly, RAA **is not** a special case of ¬-introduction. On the other hand, one may view ¬-introduction as a "constructive" version of RAA applying to negated propositions (propositions of the form $\neg P$).

Confusion 2. Is there any difference between $\perp$-elimination and RAA?

$$\dfrac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ \perp\end{array}}{P}\ (\perp\text{-elim}) \qquad\qquad \dfrac{\begin{array}{c}\Gamma, \neg P^x\\ \mathcal{D}\\ \perp\end{array}}{P}\ x\ (\text{RAA})$$

The difference is that $\perp$-elimination does not discharge any of its premises.

In fact, RAA is a stronger rule which implies $\perp$-elimination as we now demonstate.

RAA implies $\perp$-elimination.

Suppose we have a deduction

$$\begin{array}{c}\Gamma\\ \mathcal{D}\\ \perp\end{array}$$

Then, for any proposition P, we can add the premise $\neg P$ to every leaf of the above deduction tree and we get the deduction tree

$$\begin{array}{c}\Gamma, \neg P\\ \mathcal{D}'\\ \perp\end{array}$$

We can now apply RAA to get the following deduction tree of P from Γ (since $\neg P$ is discharged), and this is just the result of $\perp$-elimination:

$$\cfrac{\begin{array}{c}\Gamma, \neg P^x\\ \mathcal{D}'\\ \perp\end{array}}{P}\quad x\ (\mathrm{RAA})$$

The above considerations also show that RAA is obtained from ¬-introduction by adding the new rule of *¬¬-elimination* or *double-negation elimination*:

$$\frac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ \neg\neg P\end{array}}{P}\quad(\neg\neg\text{-elimination})$$

Some authors prefer adding the ¬¬-elimination rule to intuitionistic logic instead of RAA in order to obtain classical logic.

As we just demonstrated, the two additions are equivalent: by adding either RAA or ¬¬-elimination to intuitionistic logic, we get classical logic.

There is another way to obtain RAA from the rules of intuitionistic logic, this time, using the propositions of the form $P \lor \neg P$. We saw in Proposition 1.3.3 that all formulae of the form $P \lor \neg P$ are provable in classical logic (using RAA).

Confusion 3. Are propositions of the form $P \vee \neg P$ provable in intuitionistic logic?

The answer is **no**, which may be disturbing to some readers. In fact, it is quite difficult to prove that propositions of the form $P \vee \neg P$ are not provable in intuitionistic logic.

One way to gauge how intuitionisic logic differs from classical logic is to ask what kind of propositions need to be added to intuitionisic logic in order to get classical logic.

It turns out that if all the propositions of the form $P \vee \neg P$ are considered to be axioms, then RAA follows from some of the rules of intuitionistic logic.

RAA holds in Intuitionistic logic + all axioms $P \vee \neg P$.

The proof involves a subtle use of the $\perp$-elimination and $\vee$-elimination rules which may be a bit puzzling.

Assume, as we do when when use the proof by contradiction rule (RAA) that we have a deduction

$$\begin{array}{c}\Gamma, \neg P\\ \mathcal{D}\\ \bot\end{array}$$

Here is the deduction tree demonstrating that RAA is a derived rule:

$$\dfrac{P \vee \neg P \qquad \dfrac{P^x}{P} \qquad \dfrac{\begin{array}{c}\Gamma, \neg P^y\\ \mathcal{D}\\ \bot\end{array}}{P}\ (\bot\text{-elim})}{P}\ {}_{x,y}\ (\vee\text{-elim})$$

At first glance, the rightmost subtree

$$\dfrac{\begin{array}{c}\Gamma, \neg P^y\\ \mathcal{D}\\ \bot\end{array}}{P}\ (\bot\text{-elim})$$

appears to use RAA and our argument looks circular!

But this is not so because the premise $\neg P$ labeled y is *not* discharged in the step that yields P as conclusion; the step that yields P is a $\perp$-elimination step.

The premise $\neg P$ labeled y is actually discharged by the $\vee$-elimination rule (and so is the premise P labeled x). So, our argument establishing RAA is not circular after all!

In conclusion, intuitionistic logic is obtained from classical logic by *taking away the proof by contradiction rule (RAA)*.

In this more restrictive proof system, we obtain more constructive proofs. In that sense, the situation is better than in classical logic.

The major drawback is that we can't think in terms of classical truth values semantics anymore.

Conversely, classical logic is obtained from intuitionistic logic in at least three ways:

1. Add the proof by contradiction rule (RAA).
2. Add the $\neg\neg$-elimination rule.
3. Add all propositions of the form $P \vee \neg P$ as axioms.

1.5 De Morgan Laws and Other Rules of Classical Logic

In classical logic, we have the de Morgan laws:

Proposition 1.5.1 *The following equivalences (de Morgan laws) are provable in classical logic:*

$$\begin{aligned}\neg(P \wedge Q) &\equiv \neg P \vee \neg Q\\ \neg(P \vee Q) &\equiv \neg P \wedge \neg Q.\end{aligned}$$

In fact, $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ *and*
$(\neg P \vee \neg Q) \Rightarrow \neg(P \wedge Q)$
are provable in intuitionistic logic.

The proposition $(P \wedge \neg Q) \Rightarrow \neg(P \Rightarrow Q)$ *is provable in intuitionistic logic and* $\neg(P \Rightarrow Q) \Rightarrow (P \wedge \neg Q)$ *is provable in classical logic.*

Therefore, $\neg(P \Rightarrow Q)$ *and* $P \wedge \neg Q$ *are equivalent in classical logic.*

Furthermore, $P \Rightarrow Q$ *and* $\neg P \vee Q$ *are equivalent in classical logic and* $(\neg P \vee Q) \Rightarrow (P \Rightarrow Q)$ *is provable in intuitionistic logic.*

Proof. Here is an intuitionistic proof of $(\neg P \vee Q) \Rightarrow (P \Rightarrow Q)$:

$$\dfrac{\dfrac{(\neg P \vee Q)^w \qquad \dfrac{\dfrac{\dfrac{\neg P^z \qquad P^x}{\perp}}{Q}}{P \Rightarrow Q}\; x \qquad \dfrac{\dfrac{P^y \qquad Q^t}{Q}}{P \Rightarrow Q}\; y}{P \Rightarrow Q}\; z,t}{(\neg P \vee Q) \Rightarrow (P \Rightarrow Q)}\; w$$

Here is a classical proof of $(P \Rightarrow Q) \Rightarrow (\neg P \vee Q)$:

$$\dfrac{\dfrac{\dfrac{(\neg(\neg P \vee Q))^y \qquad \dfrac{\dfrac{(P \Rightarrow Q)^z \qquad \dfrac{\dfrac{(\neg(\neg P \vee Q))^y \qquad \dfrac{\neg P^x}{\neg P \vee Q}}{\perp}}{P}\; x \;\; \mathrm{RAA}}{Q}}{\neg P \vee Q}}{\perp}}{\neg P \vee Q}\; y \;\; \mathrm{RAA}}{(P \Rightarrow Q) \Rightarrow (\neg P \vee Q)}\; z$$

The other proofs are left as exercises. □

Propositions 1.3.4 and 1.5.1 show a property that is very specific to classical logic, namely, that the logical connectives $\Rightarrow, \wedge, \vee, \neg$ are not independent.

For example, we have $P \wedge Q \equiv \neg(\neg P \vee \neg Q)$, which shows that $\wedge$ can be expressed in terms of $\vee$ and $\neg$.

In intuitionistic logic, $\wedge$ and $\vee$ cannot be expressed in terms of each other via negation.

The fact that the logical connectives $\Rightarrow, \wedge, \vee, \neg$ are not independent in classical logic suggests the following question:

Are there propositions, written in terms of $\Rightarrow$ only, that are provable classically but not provable intuitionistically?

The answer is yes! For instance, the proposition

$$((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$$

(known as *Peirce's law*) is provable classically (do it) but it can be shown that it is not provable intuitionistically.

In addition to the proof by cases method and the proof by contradiction method, we also have the proof by contrapositive method valid in classical logic:

Proof by contrapositive rule:

$$\frac{\begin{array}{c}\Gamma, \neg Q^{x} \\ \mathcal{D} \\ \neg P\end{array}}{P \Rightarrow Q}\; x$$

This rule says that in order to prove an implication $P \Rightarrow Q$ (from Γ), one may assume $\neg Q$ as proved, and then deduce that $\neg P$ is provable from Γ and $\neg Q$.

This inference rule is valid in classical logic because we can construct the following deduction:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\Gamma, \neg Q^x\\ \mathcal{D}\\ \neg P\end{array} \qquad P^y}{\perp}}{Q}\; {\scriptstyle x}\ \text{(by-contra)}}{P \Rightarrow Q}\; {\scriptstyle y}$$

1.6 Formal Versus Informal Proofs; Some Examples

It should be said that *it is practically impossible to write formal proofs* (*i.e.*, proofs written as proof trees using the rules of one of the systems presented earlier) of "real" statements that are not "toy propositions".

This is because it would be extremely tedious and time-consuming to write such proofs and these proofs would be huge and thus, very hard to read.

In principle, it is possible to write formalized proofs and sometimes it is desirable to do so if we want to have absolute confidence in a proof.

For example, we would like to be sure that a flight-control system is not buggy so that a plane does not accidently crash, that a program running a nuclear reactor will not malfunction or that nuclear missiles will not be fired as a result of a buggy "alarm system".

Thus, it is very important to develop tools to assist us in constructing formal proofs or checking that formal proofs are correct and such systems do exit (Examples: Isabelle, COQ, TPS, NUPRL, PVS, Twelf). However, 99.99% of us will not have the time or energy to write formal proofs. So, what do we do?

Well, we construct "informal" proofs in which we still make use of the logical rules that we have presented but we take short-cuts and sometimes we even omit proof steps (some elimination rules, such as $\wedge$-elimination and some introduction rules, such as $\vee$-introduction) and we use a natural language (here, presumably, English!) rather than formal symbols (we say "and" for $\wedge$, "or" for $\vee$, *etc.*).

Also, we implicitly keep track of the open premises of a proof in our head rather than explicitly discharge premises when required.

This may be the biggest source of mistakes and we should make sure that when we have finished a proof, there are no “dangling premises”, that is, premises that were never used in constructing the proof.

If we are “lucky”, some of these premises are in fact unecessary and we should discard them. Otherwise, this indicates that there is something wrong with our proof and we should make sure that every premise is indeed used somewhere in the proof or else look for a counter-example.

The next question is then: How does one write “good” informal proofs?

It is very hard to answer such a question because the notion of a “good” proof is quite subjective and partly a “social” concept.

Nevertheless, people have been writing informal proofs for centuries so there are at least many examples or what to do (and what not to do!).

As for everything else, practicing a sport, playing a music intrument, knowing "good" wines, *etc.*, *the more you practice, the better you become*. Knowing the theory of swimming is fine but you have to get wet and do some actual swimming!

Similarly, knowing the proof rules is important but you have to put them to use.

Write proofs as much as you can. Find good proof writers (like good swimmers, good tennis players, *etc.*), try to figure out why they write clear and easily readable proofs and try to emulate what they do.

Don't follow bad examples (it will take you a little while to "smell" a bad proof style).

Another important point is that non-formalized proofs make heavy use of *modus ponens*.

This is because, when we search for a proof, we rarely (if ever) go back to first principles.

This would result in extremely long proofs that would be basically incomprehensible. Instead, we search in our "data base" of facts for a proposition of the form $P \Rightarrow Q$ (an *auxiliary lemma*) which is already known to be proved, and if we are smart enough (lucky enough!), we find that we can prove P and thus we deduce Q, the proposition that we really need to prove.

Generally, we have to go through several steps involving auxiliary lemmas.

This is why it is important to build up a data base of proven facts as large as possible about a mathematical field; numbers, trees, graphs, surfaces, *etc.*

This way, we increase the chance that we will be able to prove some fact about some some field of mathematics.

Let us conclude our discussion with a concrete example illustrating the usefulnes of auxiliary lemmas.

Say we wish to prove the implication

$$\neg(P \wedge Q) \Rightarrow \big((\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)\big). \quad (*)$$

It can be shown that the above proposition is not provable intuitionistically, so we will have to use the proof by contradiction method in our proof.

One will quickly realize that any proof ends up reproving basic properties of $\wedge$ and $\vee$, such as associativity, commutativity, idempotence, distributivity, *etc.*, some of the de Morgan laws, and that the complete proof is very large!

However, if we allow ourselves to use the de Morgan laws as well as various basic properties or $\wedge$ and $\vee$, such as distributivity,

$$(A \wedge B) \vee C \equiv (A \wedge C) \vee (B \wedge C),$$

commutativity of $\wedge$ and $\vee$ ($A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$), associativity of $\wedge$ and $\vee$ ($A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$, $A \vee (B \vee C) \equiv (A \vee B) \vee C$) and the idempotence of $\wedge$ and $\vee$ ($A \wedge A \equiv A$, $A \vee A \equiv A$), then we get

$$\begin{aligned}
&(\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q) \\
&\quad \equiv (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q) \\
&\quad \equiv (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge \neg Q) \\
&\quad \equiv (\neg P \wedge (\neg Q \vee Q)) \vee (\neg P \wedge \neg Q) \vee (P \wedge \neg Q) \\
&\quad \equiv \neg P \vee (\neg P \wedge \neg Q) \vee (P \wedge \neg Q) \\
&\quad \equiv \neg P \vee ((\neg P \vee P) \wedge \neg Q) \\
&\quad \equiv \neg P \vee \neg Q,
\end{aligned}$$

where we made implicit uses of commutativity and associativity, and the fact that
$R \wedge (P \vee \neg P) \equiv R$, and by de Morgan,

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q,$$

using auxiliary lemmas, we end up proving $(*)$ without too much pain.

And now, we return to some explicit examples of informal proofs.

Recall that the *set of integers* is the set

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

and that the *set of natural numbers* is the set

$$\mathbb{N} = \{0, 1, 2, \cdots\}.$$

(Some authors exclude 0 from $\mathbb{N}$. We don't like this discrimination against zero.)

An integer is *even* if it is divisible by 2, that is, if it can be written as $2k$, where $k \in \mathbb{Z}$.

An integer is *odd* if it is not divisible by 2, that is, if it can be written as $2k + 1$, where $k \in \mathbb{Z}$.

The following facts are essentially obvious:

(a) The sum of even integers is even.

(b) The sum of an even integer and of an odd integer is odd.

(c) The sum of two odd integers is even.

(d) The product of odd integers is odd.

(e) The product of an even integer with any integer is even.

Now, we can prove the following fact using the proof by cases method.

Proposition 1.6.1 *Let a, b, c be odd integers. For any integers p and q, if p and q are not both even, then*

$$ap^2 + bpq + cq^2$$

is odd.

The set of *rational numbers*, $\mathbb{Q}$, consists of all fractions p/q, where $p, q \in \mathbb{Z}$, with $q \neq 0$. The set of *real numbers* is denoted by $\mathbb{R}$.

A real number, $a \in \mathbb{R}$, is said to be *irrational* if it cannot be expressed as a number in $\mathbb{Q}$ (a fraction).

We can now use Proposition 1.6.1 and the proof by contradiction method to prove

Proposition 1.6.2 *Let a, b, c be odd integers. Then, the equation*

$$aX^2 + bX + c = 0$$

has no rational solution X.

Remark: A closer look at the proof of Proposition 1.6.2 shows that rather than using the proof by contradiction rule we really used $\neg$-introduction (a "constructive" version of RAA).

As as example of the proof by contrapositive method, we can prove that if an integer n^2 is even, then n must be even.

As it is, because the above proof uses the proof by contrapositive method, it is not constructive. Thus, the question arises, is there a constructive proof of the above fact?

Indeed there is a constructive proof if we observe that every integer, n, is either even or odd but not both.

Now, one might object that we just relied on the law of the excluded middle but there is a way to circumvent this problem by using *induction* (which we haven't officially met, yet) to prove that every integer, n, is either of the form $2k$ or of the form $2k + 1$, for some integer, k. For a rigorous proof, see Section 1.9.

Now, since *an integer is odd iff it is not even*, we may proceed to prove that *if n^2 is even, then n is not odd*, by using our constructive version of the proof by contradiction principle, namely, ¬-introduction.

Therefore, assume that n^2 is even and that n is odd. Then, $n = 2k+1$, which implies that $n^2 = 4k^2+4k+1 = 2(2k^2 + 2k) + 1$, an odd number, contradicting the fact that n^2 is asssumed to be even. □

As another illustration of the proof methods that we have just presented, let us prove that $\sqrt{2}$ is irrational, which means that $\sqrt{2}$ is *not* rational.

The reader may also want to look at the proof given by Gowers in Chapter 3 of his book [8]. Obviously, our proof is similar but we emphasize step (2) a little more.

Since we are trying to prove that $\sqrt{2}$ is not rational, let us use our constructive version of the proof by contradiction principle, namely, $\neg$-introduction.

Thus, *let us assume that $\sqrt{2}$ is rational and derive a contradiction*. Here are the steps of the proof:

1. If $\sqrt{2}$ is rational, then there exist some integers, $p, q \in \mathbb{Z}$, with $q \neq 0$, so that $\sqrt{2} = p/q$.
2. Any fraction, p/q, is equal to some fraction, r/s, where r and s are not both even.
3. By (2), we may assume that
$$\sqrt{2} = \frac{p}{q},$$
where $p, q \in \mathbb{Z}$ are *not both even* and with $q \neq 0$.
4. By (3), since $q \neq 0$, by multiplying both sides by q, we get
$$q\sqrt{2} = p.$$
5. By (4), by squaring both sides, we get
$$2q^2 = p^2.$$

6. Since $p^2 = 2q^2$, the number p^2 must be even. By a fact previously established, p *itself is even*, that is, $p = 2s$, for some $s \in \mathbb{Z}$.

7. By (6), if we substitute $2s$ for p in the equation in (5) we get $2q^2 = 4s^2$. By dividing both sides by 2, we get
$$q^2 = 2s^2.$$

8. By (7), we see that q^2 is even, from which we deduce (as above) that *q itself is even*.

9. Now, assuming that $\sqrt{2} = p/q$ where p and q are *not both even* (and $q \neq 0$), we concluded that *both p and q are even* (as shown in (6) and(8)), reaching a contradiction. Therefore, by negation introduction, we proved that $\sqrt{2}$ is *not* rational.

A closer examination of the steps of the above proof reveals that the only step that may require further justification is step (2): that any fraction, p/q, is equal to some fraction, r/s, where r and s are not both even.

This fact does require a proof and the proof uses the division algorithm, which itself requires induction (see Section 5.3, Theorem 5.3.6).

Besides this point, all the other steps only require simple arithmetic properties of the integers and are constructive.

Remark: Actually, every fraction, p/q, is equal to some fraction, r/s, where r and s have no common divisor except 1.

This follows from the fact that every pair of integers has a *greatest common divisor* (a *gcd*, see Section 5.4) and r and s are obtained by dividing p and q by their gcd.

Using this fact and Euclid's proposition (Proposition 5.4.8), we can obtain a shorter proof of the irrationality of $\sqrt{2}$.

The above argument can be easily adapted to prove that if the positive integer, n, is not a perfect square, then $\sqrt{n}$ is not rational.

Let us return briefly to the issue of constructivity in classical logic, in particular when it comes to disjunctions.

Consider the question: *are there two irrational real numbers a and b such that a^b is rational*?

Here is a way to prove that this indeed the case.

Consider the number ${\sqrt{2}}^{\sqrt{2}}$.

If this number is rational, then $a = \sqrt{2}$ and $b = \sqrt{2}$ is an answer to our question (since we already know that $\sqrt{2}$ is irrational).

Now, observe that

$$({\sqrt{2}}^{\sqrt{2}})^{\sqrt{2}} = {\sqrt{2}}^{\sqrt{2}\times\sqrt{2}} = {\sqrt{2}}^{2} = 2 \quad \text{is rational!}$$

Thus, if ${\sqrt{2}}^{\sqrt{2}}$ is irrational, then $a = {\sqrt{2}}^{\sqrt{2}}$ and $b = \sqrt{2}$ is an answer to our question.

So, we proved that

($\sqrt{2}$ is irrational and ${\sqrt{2}}^{\sqrt{2}}$ is rational) or
($\sqrt{2}^{\sqrt{2}}$ and $\sqrt{2}$ are irrational and $({\sqrt{2}}^{\sqrt{2}})^{\sqrt{2}}$ is rational).

However, the above proof does not tell us whether $\sqrt{2}^{\sqrt{2}}$ is rational or not!

We see one of the shortcomings of classical reasoning: certain statements (in particular, disjunctive or existential) are provable but their proof does not provide an explicit answer.

It is in that sense that classical logic is not constructive.

Actually, it turns out that another irrational number, b, can be found so that $\sqrt{2}^{b}$ is rational and the proof that b is not rational is fairly simple.

It also turns out that the exact nature of $\sqrt{2}^{\sqrt{2}}$ (rational or irrational) is known. The answers to these puzzles can be found in Section 1.8.

Many more examples of non-constructive arguments in classical logic can be given.

1.7 Truth Values Semantics for Classical Logic Soundness and Completeness

So far, even though we have deliberately focused on proof theory and ignored semantic issues, we feel that we can't postpone any longer a discussion of the truth values semantics for classical propositional logic.

We all learned early on that the logical connectives, $\Rightarrow$, $\wedge$, $\vee$ and $\neg$ can be interpreted as boolean functions, that is, functions whose arguments and whose values range over the set of *truth values*,

$$\mathbf{BOOL} = \{\mathbf{true}, \mathbf{false}\}.$$

These functions are given by the following *truth tables*:

P	Q	$P \Rightarrow Q$	$P \wedge Q$	$P \vee Q$	$\neg P$
true	**true**	**true**	**true**	**true**	**false**
true	**false**	**false**	**false**	**true**	**false**
false	**true**	**true**	**false**	**true**	**true**
false	**false**	**true**	**false**	**false**	**true**

Now, any proposition, P, built up over the set of atomic propositions, **PS**, (our propositional symbols) contains a finite set of propositional letters, say

$$\{P_1, \ldots, P_m\}.$$

If we assign some truth value (from **BOOL**) to each symbol, P_i, then we can "compute" the *truth value* of P under this assignment by using recursively the truth tables above.

For example, the proposition $\mathbf{P}_1 \Rightarrow (\mathbf{P}_1 \Rightarrow \mathbf{P}_2)$, under the truth assignment, v, given by

$$v(\mathbf{P}_1) = \mathbf{true},\ v(\mathbf{P}_2) = \mathbf{false},$$

evaluates to **false**.

Indeed, the truth value, $v(\mathbf{P}_1 \Rightarrow (\mathbf{P}_1 \Rightarrow \mathbf{P}_2))$, is computed recursively as

$$v(\mathbf{P}_1 \Rightarrow (\mathbf{P}_1 \Rightarrow \mathbf{P}_2)) = v(\mathbf{P}_1) \Rightarrow v(\mathbf{P}_1 \Rightarrow \mathbf{P}_2).$$

Now, $v(\mathbf{P}_1) = \mathbf{true}$ and $v(\mathbf{P}_1 \Rightarrow \mathbf{P}_2)$ is computed recursively as

$$v(\mathbf{P}_1 \Rightarrow \mathbf{P}_2) = v(\mathbf{P}_1) \Rightarrow v(\mathbf{P}_2).$$

Since $v(\mathbf{P}_1) = \mathbf{true}$ and $v(\mathbf{P}_2) = \mathbf{false}$, using our truth table, we get

$$v(\mathbf{P}_1 \Rightarrow \mathbf{P}_2) = \mathbf{true} \Rightarrow \mathbf{false} = \mathbf{false}.$$

Plugging this into the right-hand side of
$v(\mathbf{P}_1 \Rightarrow (\mathbf{P}_1 \Rightarrow \mathbf{P}_2))$, we finally get

$$v(\mathbf{P}_1 \Rightarrow (\mathbf{P}_1 \Rightarrow \mathbf{P}_2)) = \mathbf{true} \Rightarrow \mathbf{false} = \mathbf{false}.$$

However, under the truth assignment,

$$\mathbf{P}_1 = \mathbf{true},\ \mathbf{P}_2 = \mathbf{true},$$

our proposition evaluates to **true**.

If we now consider the proposition,

$$P = (\mathbf{P}_1 \Rightarrow (\mathbf{P}_2 \Rightarrow \mathbf{P}_1)),$$

then it is easy to see that P evaluates to **true** for all four possible truth assignments for $\mathbf{P}_1$ and $\mathbf{P}_2$.

Definition 1.7.1 We say that a proposition, P, is *satisfiable* iff it evalates to **true** for *some* truth assignment (taking values in **BOOL**) of the propositional symbols occurring in P and otherwise we say that it is *unsatisfiable*. A proposition, P, is *valid* (or a *tautology*) iff it evaluates to **true** for *all* truth assignments of the propositional symbols occurring in P.

The problem of deciding whether a proposition is satisfiable or not is called the *satisfiability problem* and is sometimes denoted by SAT.

The problem of deciding whether a proposition is valid or not is called the *validity problem*.

For example, the proposition

$$\begin{aligned} P \;=\; & (\mathbf{P}_1 \lor \neg\mathbf{P}_2 \lor \neg\mathbf{P}_3) \land (\neg\mathbf{P}_1 \lor \neg\mathbf{P}_3) \\ & \land (\mathbf{P}_1 \lor \mathbf{P}_2 \lor \mathbf{P}_4) \land (\neg\mathbf{P}_3 \lor \mathbf{P}_4) \land (\neg\mathbf{P}_1 \lor \mathbf{P}_4) \end{aligned}$$

is satisfiable since it evaluates to **true** under the truth assignment $\mathbf{P}_1 =$ **true**, $\mathbf{P}_2 =$ **false**, $\mathbf{P}_3 =$ **false** and $\mathbf{P}_4 =$ **true**.

On the other hand, the proposition

$$\begin{aligned} Q \;=\; & (\mathbf{P}_1 \lor \mathbf{P}_2 \lor \mathbf{P}_3) \land (\neg\mathbf{P}_1 \lor \mathbf{P}_2) \land (\neg\mathbf{P}_2 \lor \mathbf{P}_3) \\ & \land (\mathbf{P}_1 \lor \neg\mathbf{P}_3) \land (\neg\mathbf{P}_1 \lor \neg\mathbf{P}_2 \lor \neg\mathbf{P}_3) \end{aligned}$$

is unsatisfiable as one can verify by trying all 8 truth assignments for $\mathbf{P}_1$, $\mathbf{P}_2$, $\mathbf{P}_3$.

The reader should also verify that the proposition

$$\begin{aligned} R \;=\; & (\neg\mathbf{P}_1 \land \neg\mathbf{P}_2 \land \neg\mathbf{P}_3) \lor (\mathbf{P}_1 \land \neg\mathbf{P}_2) \lor (\mathbf{P}_2 \land \neg\mathbf{P}_3) \\ & \lor (\neg\mathbf{P}_1 \land \mathbf{P}_3) \lor (\mathbf{P}_1 \land \mathbf{P}_2 \land \mathbf{P}_3) \end{aligned}$$

is valid (observe that the proposition, R, is the negation of the proposition, Q).

The satisfiability problem is a famous problem in computer science because of its complexity. Try it, solving it is not as easy as you think!

In fact, the satisfiability problem turns out to be an *NP-complete* problem, a very important concept that you will learn about in CIS262.

The difficulty is that if a proposition, P, contains n distinct propositional letters, then there are 2^n possible truth assignments and checking all of them is practically impossible when n is large.

The validity problem is also important and it is related to SAT. Indeed, it is easy to see that a proposition, P, is valid iff $\neg P$ is unsatisfiable.

What's the relationship between validity and provability in the system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$)?

Remarkably, in classical logic, validity and provability are equivalent!

In order to prove the above claim, we need to do two things:

(1) Prove that if a proposition, P, if provable in the system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$), then it is valid. This is known as *soundness* or *consistency* (of the proof system).

(2) Prove that if a proposition, P, is valid, then it has a proof in the system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$). This is known as the *completeness* (of the proof system).

In general, it is relatively easy to prove (1) but proving (2) can be quite complicated.

In fact, some proof systems are *not* complete with respect to certain semantics.

For instance, the proof system for intuitionistic logic, $\mathcal{N}_i^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_i^{\Rightarrow,\wedge,\vee,\perp}$), is *not complete* with respect to truth values semantics!

As an example,

$$((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$$

(known as *Peirce's law*), is valid but it can be shown that it cannot be proved in intuitionistic logic.

In these notes, we will content ourselves with soundness.

Proposition 1.7.2 *(Soundness of $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ and $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$) If a proposition, P, is provable in the system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$), then it is valid (according to the truth values semantics).*

Sketch of Proof. It is enough to prove that if there is a deduction of a proposition, P, from a set of premises, Γ, then for every truth assignment for which all the propositions in Γ evaluate to **true**, then P evaluates to **true**. However, this is clear for the axioms and every inference rule preserves that property.

Now, if P is provable, a proof of P has an empty set of premises and so P evaluates to **true** for all truth assignments, which means that P is valid. $\square$

Theorem 1.7.3 *(Completeness of $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ and $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$) If a proposition, P, is valid (according to the truth values semantics), then P is provable in the system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$).*

Proofs of completeness for classical logic can be found in van Dalen [18] or Gallier [7] (but for a different proof system).

Soundness (Proposition 1.7.2) has a very useful consequence: In order to prove that a proposition, P, is *not provable*, it is enough to find a truth assignment for which P evaluates to **false**.

We say that such a truth assignment is a *counter-example* for P (or that P can be *falsified*).

For example, no propositional symbol, $\mathbf{P}_i$, is provable since it is falsified by the truth assignment $\mathbf{P}_i =$ **false**.

The soundness of the proof system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ (or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\perp}$) also has the extremely important consequence that *$\perp$ cannot be proved* in this system, which means that *contradictory statements* cannot be derived!

This is by no means obvious at first sight, but reassuring.

It is also possible to prove that the proof system $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\perp}$ is consistent (*i.e.*, $\perp$ cannot be proved) by purely proof-theoretic means involving proof normalization (See Section **??**), but this requires a lot more work.

Note that completeness amounts to the fact that every unprovable formula has a counter-example.

Remark: Truth values semantics is not the right kind of semantics for intuitionistic logic; it is too coarse.

A more subtle kind of semantics is required. Among the various semantics for intuitionistic logic, one of the most natural is the notion of *Kripke model*.

Then, again, soundness and completeness holds for intuitionistic proof systems (see van Dalen [18]).

We now add quantifiers to our language and give the corresponding inference rules.

GALILEO
JEFFERSON
BABE RUTH
"I ADMIRE THE INQUIRING MIND AND THE PRAGMATIC MIND, BUT I ALSO ADMIRE SOMEONE WHO CAN HIT."

Figure 1.13: The ability to hit