1.8 Adding Quantifiers; The Proof Systems $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\forall,\exists,\bot}$, $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\forall,\exists,\bot}$

As we mentioned at the begining, atomic propositions may contain variables. The intention is that such variables correspond to arbitrary objects. An example is

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

Now, in mathematics, we usually prove universal statements, that is statement that hold for all possible "objects", or existential statement, that is, statement asserting the existence of some object satisfying a given property.

As we saw earlier, we assert that every human needs to drink by writing the proposition

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

Observe that once the quantifier $\forall$ (pronounced "for all" or "for every") is applied to the variable x, the variable x becomes a place-holder and replacing x by y or any other variable does not change anything.

What matters is the locations to which the outer x points to in the inner proposition. We say that x is a *bound variable* (sometimes a "dummy variable").

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

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

Again, once the quantifier $\exists$ (pronounced "there exists") is applied to the variable x, the variable x becomes a place-holder.

However, the intended meaning of the second proposition is very different and weaker than the first. It only asserts the existence of some object satisfying the statement

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

Statements may contain variables that are not bound by quantifiers. For example, in

$$\forall y\, \mathrm{parent}(x, y)$$

the variable y is bound but the variable x is not.

Here, the intended meaning of $\mathrm{parent}(x, y)$ is that x is a parent of y.

Variables that are not bound are called *free*. The proposition

$$\forall y \exists x\, \mathrm{parent}(x, y),$$

which contains only bound variables in meant to assert that every y has some parent x.

Typically, in mathematics, we only prove statements without free variables. However, statements with free variables may occur during intermediate stages of a proof.

The intuitive meaning of the statement $\forall x P$ is that P holds for all possible objects x and the intuitive meaning of the statement $\exists x P$ is that P holds for some object x.

Thus, we see that it would be useful to use symbols to denote various objects.

For example, if we want to assert some facts about the "parent" predicate, we may want to introduce some *constant symbols* (for short, constants) such as "Jean", "Mia", etc. and write

$$\text{parent}(\text{Jean}, \text{Mia})$$

to assert that Jean is a parent of Mia.

Often, we also have to use *function symbols* (or *operators, constructors*), for instance, to write statement about numbers: $+$, $*$, etc. Using constant symbols, function symbols and variables, we can form *terms*, such as

$$(x * x + 1) * (3 * y + 2).$$

In addition to function symbols, we also use *predicate symbols*, which are names for atomic properties. We have already seen several examples of predicate symbols: "human", "parent".

So, in general, when we try to prove properties of certain classes of objects (people, numbers, strings, graphs, etc.), we assume that we have a certain *alphabet* consisting of constant symbols, function symbols and predicate symbols.

Using these symbols and an infinite supply of variables (assumed distinct from the variables which we use to label premises) we can form *terms and predicate terms*.

We say that we have a *(logical) language*. Using this language, we can write compound statements.

Let us be a little more precise. In a *first-order language*, $\mathbf{L}$, in addition to the logical connectives, $\Rightarrow, \wedge, \vee, \neg, \bot, \forall$ and $\exists$, we have a set, $\mathbf{L}$, of *nonlogical symbols* consisting of

(i) A set **CS** of constant symbols, $c_1, c_2, \ldots,$.

(ii) A set **FS** of function symbols, $f_1, f_2, \ldots,$. Each function symbol, f, has a *rank*, $n_f \geq 1$, which is the number of arguments of f.

(iii) A set **PS** of predicate symbols, $P_1, P_2, \ldots,$. Each predicate symbol, P, has a *rank*, $n_P \geq 0$, which is the number of arguments of P. Predicate symbols of rank 0 are propositional letters, as in earlier sections.

(iv) The equality predicate, $=$, is added to our language when we want to deal with equations.

(v) First-order variables, $t_1, t_2, \ldots,$ used to form quantified formulae.

The difference between function symbols and predicate symbols is that function symbols are interpreted as functions defined on a structure (for example, addition, $+$, on $\mathbb{N}$), whereas predicate symbols are interpreted as properties of objects, that is, they take the value **true** or **false**.

An example is the language of *Peano arithmetic*, $\mathbf{L} = \{0, S, +, *, =\}$. Here, the intended structure is $\mathbb{N}$, 0 is of course zero, S is interpreted as the function $S(n) = n+1$, the symbol $+$ is addition, $*$ is multiplication and $=$ is equality.

Using a first-order language, $\mathbf{L}$, we can form terms, predicate terms and formulae. The *terms over* $\mathbf{L}$ are the following expressions:

(i) Every variable, t, is a term;

(ii) Every constant symbol, $c \in \mathbf{CS}$, is a term;

(iii) If $f \in \mathbf{FS}$ is a function symbol taking n arguments and $\tau_1, \ldots, \tau_n$ are terms already constructed, then $f(\tau_1, \ldots, \tau_n)$ is a term.

The *predicate terms over* $\mathbf{L}$ are the following expressions:

(i) If $P \in \mathbf{PS}$ is a predicate symbol taking n arguments and $\tau_1, \ldots, \tau_n$ are terms already constructed, then $P(\tau_1, \ldots, \tau_n)$ is a predicate term. When $n = 0$, the predicate symbol, P, is a predicate term called a propositional letter.

(ii) When we allow the equality predicate, for any two terms τ_1 and τ_2, the expression $\tau_1 = \tau_2$ is a predicate term. It is usually called an *equation*.

The *(first-order) formulae over* $\mathbf{L}$ are the following expressions:

(i) Every predicate term, $P(\tau_1, \ldots, \tau_n)$, is an atomic formula. This includes all propositional letters. We also view $\bot$ (and sometimes $\top$) as an atomic formula.

(ii) When we allow the equality predicate, every equation, $\tau_1 = \tau_2$, is an atomic formula.

(iii) If P and Q are formulae already constructed, then $P \Rightarrow Q$, $P \wedge Q$, $P \vee Q$, $\neg P$ are compound formulae. We treat $P \equiv Q$ as an abbreviation for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, as before.

(iv) If P is a formula already constructed and t is any variable, then $\forall t P$ and $\exists t P$ are compound formulae.

Unlike the rules for $\Rightarrow, \vee, \wedge$ and $\bot$, which are rather straightforward, the rules for quantifiers are more subtle due the presence of variables (occurring in terms and predicates).

We have to be careful to forbid inferences that would yield "wrong" results and for this we have to be very precise about the way we use free variables.

More specifically, we have to exercise care when we make *substitutions* of terms for variables in propositions.

For example, say we have the predicate "odd", intended to express that a number is odd. Now, we can substitute the term $(2y+1)^2$ for x in $\mathrm{odd}(x)$ and obtain

$$\mathrm{odd}((2y+1)^2).$$

More generally, if $P(t_1, t_2, \ldots, t_n)$ is a statement containing the free variables $t_1, \ldots, t_n$ and if $\tau_1, \ldots, \tau_n$ are terms, we can form the new statement

$$P[\tau_1/t_1, \ldots, \tau_n/t_n]$$

obtained by substituting the term τ_i for all free occurrences of the variable t_i, for $i = 1, \ldots, n$.

By the way, we denote terms by the greek letter τ because we use the letter t for a variable and using t for both variables and terms would be confusing; sorry!

However, if $P(t_1, t_2, \ldots, t_n)$ contains quantifiers, some bad things can happen, namely, some of the variables occurring in some term τ_i may become quantified when τ_i is substituted for t_i.

For example, consider

$$\forall x \exists y\, P(x, y, z)$$

which contains the free variable z and substitute the term $x + y$ for z: we get

$$\forall x \exists y\, P(x, y, x + y).$$

We see that the variables x and y occurring in the term $x + y$ become bound variables after substitution. We say that there is a "capture of variables".

This is not what we intended to happen! To fix this problem, we recall that bound variables are really place holders, so they can be renamed without changing anything.

Therefore, we can rename the bound variables x and y in $\forall x \exists y\, P(x, y, z)$ to u and v, getting the statement $\forall u \exists v\, P(u, v, z)$ and now, the result of the substitution is

$$\forall u \exists v\, P(u, v, x + y).$$

Finally, here are the inference rules for the quantifiers, first stated in a natural deduction style and then in sequent style.

It is assumed that we use two disjoint sets of variables for labeling premises $(x, y, \cdots)$ and free variables $(t, u, v, \cdots)$.

As we will see, the $\forall$-introduction rule and the $\exists$-elimination rule involve a crucial restriction on the occurrences of certain variables. Remember, *variables are terms*!

Definition 1.8.1 The *inference rules for the quantifiers* are

$\forall$-introduction:

If $\mathcal{D}$ is a deduction tree for $P[u/t]$ from the premises, Γ, then

$$\frac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ P[u/t]\end{array}}{\forall t P}$$

is a deduction tree for $\forall t P$ from the premises, Γ.

Here, u must be a variable that does not occur free in any of the propositions in Γ or in $\forall t P$. The notation $P[u/t]$ stands for the result of substituting u for all free occurrences of t in P.

Recall that Γ denotes the set of premises of the deduction tree, $\mathcal{D}$, so if $\mathcal{D}$ only has one node, then $\Gamma = \{P[u/t]\}$ and t should not occur in P.

$\forall$-elimination:

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

$$\begin{array}{c} \Gamma \\ \mathcal{D} \\ \forall t P \\ \hline P[\tau/t] \end{array}$$

is a deduction tree for $P[\tau/t]$ from the premises, Γ.

Here τ is an arbitrary term and it is assumed that bound variables in P have been renamed so that none of the variables in τ are captured after substitution.

$\exists$-introduction:

If $\mathcal{D}$ is a deduction tree for $P[\tau/t]$ from the premises, Γ, then

$$\dfrac{\begin{array}{c}\Gamma\\ \mathcal{D}\\ P[\tau/t]\end{array}}{\exists t P}$$

is a deduction tree for $\exists t P$ from the premises, Γ.

As in $\forall$-elimination, τ is an arbitrary term and the same proviso on bound variables in P applies.

$\exists$-elimination:

If $\mathcal{D}_1$ is a deduction tree for $\exists t P$ from the premises, Γ, and if $\mathcal{D}_2$ is a deduction tree for C from the premises in $\Delta \cup \{P[u/t]\}$, then

$$\dfrac{\begin{array}{cc}\Gamma & \Delta, P[u/t]^x \\ \mathcal{D}_1 & \mathcal{D}_2 \\ \exists t P & C\end{array}}{C}\ x$$

is a deduction tree of C from the set of premises in $\Gamma \cup \Delta$.

Here, u must be a variable that does not occur free in any of the propositions in Δ, $\exists t P$, or C, and all premises $P[u/t]$ labeled x are discharged.

In the $\forall$-introduction and the $\exists$-elimination rules, the variable u is called the *eigenvariable* of the inference.

In the above rules, Γ or Δ may be empty, P, C denote arbitrary propositions constructed from a first-order language, $\mathbf{L}$, $\mathcal{D}, \mathcal{D}_1, \mathcal{D}_2$ are deductions, possibly a one-node tree, and t is *any* variable.

The system of *first-order classical logic*, $\mathcal{N}_c^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ is obtained by adding the above rules to the system of propositional classical logic $\mathcal{N}_c^{\Rightarrow,\vee,\wedge,\bot}$.

The system of *first-order intuitionistic logic*, $\mathcal{N}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ is obtained by adding the above rules to the system of propositional intuitionistic logic $\mathcal{N}_i^{\Rightarrow,\vee,\wedge,\bot}$.

Using sequents, the quantifier rules in first-order logic are expressed as follows:

Definition 1.8.2 The *inference rules for the quantifiers in Gentzen-sequent style* are

$$\frac{\Gamma \to P[u/t]}{\Gamma \to \forall t P} \quad (\forall\text{-}intro) \qquad \frac{\Gamma \to \forall t P}{\Gamma \to P[\tau/t]} \quad (\forall\text{-}elim)$$

where in ($\forall$-*intro*), u does not occur free in Γ or $\forall t P$;

$$\frac{\Gamma \to P[\tau/t]}{\Gamma \to \exists t P} \quad (\exists\text{-}intro)$$

$$\frac{\Gamma \to \exists t P \quad z\colon P[u/t], \Gamma \to C}{\Gamma \to C} \quad (\exists\text{-}elim)$$

where in ($\exists$-*elim*), u does not occur free in Γ, $\exists t P$, or C. Again, t is *any* variable.

The variable u is called the *eigenvariable* of the inference. The systems $\mathcal{NG}_c^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ and $\mathcal{NG}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ are defined from the systems $\mathcal{NG}_c^{\Rightarrow,\vee,\wedge,\bot}$ and $\mathcal{NG}_i^{\Rightarrow,\vee,\wedge,\bot}$, respectively, by adding the above rules.

The equivalence of the proof systems $\mathcal{N}_c^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ and $\mathcal{NG}_c^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ (and the proof systems $\mathcal{N}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ and $\mathcal{NG}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$) is not hard but somewhat laborious to prove.

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 $\mathcal{N}_c^{\Rightarrow,\wedge,\vee,\bot,\forall,\exists}$ or $\mathcal{NG}_c^{\Rightarrow,\wedge,\vee,\bot,\forall,\exists}$.

Therefore, as in propositional logic, when we use the word "provable" unqualified, we mean provable in *classical logic*. Otherwise, we say *intuitionistically provable* .

A first look at the above rules shows that universal formulae, $\forall tP$, behave somewhat like infinite conjunctions and that existential formulae, $\exists tP$, behave somewhat like infinite disjunctions.

The $\forall$-introduction rule looks a little strange but the idea behind it is actually very simple:

Since u is totally unconstrained, if $P[u/t]$ is provable (from Γ), then intuitively $P[u/t]$ holds of any arbitrary object, and so, the statement $\forall t P$ should also be provable (from Γ).

Note that the tree

$$\frac{P[u/t]}{\forall t P}$$

is generally an *illegal deduction* because the deduction tree above $\forall t P$ is a one-node tree consisting of the single premise, $P[u/t]$, and u occurs in $P[u/t]$ unless t does not occur in P.

The meaning of the $\forall$-elimination is that if $\forall tP$ is provable (from Γ), then P holds for all objects and so, in particular for the object denoted by the term τ, i.e., $P[\tau/t]$ should be provable (from Γ).

The $\exists$-introduction rule is dual to the $\forall$-elimination rule.

If $P[\tau/t]$ is provable (from Γ), this means that the object denoted by τ satisfies P, so $\exists tP$ should be provable (this latter formula asserts the existence of some object satisfying P, and τ is such an object).

The $\exists$-elimination rule is reminiscent of the $\vee$-elimination rule and is a little more tricky.

It goes as follows: Suppose that we proved $\exists t P$ (from Γ). Moreover, suppose that for every possible case, $P[u/t]$, we were able to prove C (from Γ).

Then, as we have "exhausted" all possible cases and as we know from the provability of $\exists t P$ that some case must hold, we can conclude that C is provable (from Γ) without using $P[u/t]$ as a premise.

Like the $\vee$-elimination rule, the $\exists$-elimination rule is not very constructive. It allows making a conclusion (C) by considering alternatives without knowing which one actually occurs.

Anagolously to disjunction, in (first-order) intuitionistic logic, if an existential statement $\exists t P$ is provable, then from any proof of $\exists t P$, some term, τ, can be extracted so that $P[\tau/t]$ is provable.

Such a term, τ, is called a *witness*. The witness property is not easy to prove. It follows from the fact that intuitionistic proofs have a normal form.

However, no such property holds in classical logic (for instance, see the a^b rational with a, b irrational example revisited below).

Here is an example of a proof in the system $\mathcal{N}_c^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$ (actually, in $\mathcal{N}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$) of the formula
$\forall t(P \wedge Q) \Rightarrow \forall t P \wedge \forall t Q$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall t(P \wedge Q)^x}{P[u/t] \wedge Q[u/t]}}{P[u/t]}}{\forall t P} \qquad \dfrac{\dfrac{\dfrac{\forall t(P \wedge Q)^x}{P[u/t] \wedge Q[u/t]}}{Q[u/t]}}{\forall t Q}}{\dfrac{\forall t P \wedge \forall t Q}{\forall t(P \wedge Q) \Rightarrow \forall t P \wedge \forall t Q}\, x}$$

In the above proof, u is a new variable, i.e., a variable that does not occur free in P or Q.

We also have used some basic properties of substitutions such as:

$$\begin{aligned}
(P \wedge Q)[\tau/t] &= P[\tau/t] \wedge Q[\tau/t] \\
(P \vee Q)[\tau/t] &= P[\tau/t] \vee Q[\tau/t] \\
(P \Rightarrow Q)[\tau/t] &= P[\tau/t] \Rightarrow Q[\tau/t] \\
(\neg P)[\tau/t] &= \neg P[\tau/t] \\
(\forall s P)[\tau/t] &= \forall s P[\tau/t] \\
(\exists s P)[\tau/t] &= \exists s P[\tau/t],
\end{aligned}$$

for any term, τ, such that no variable in τ is captured during the substitution (in particular, in the last two cases, the variable s does not occur in τ).

The reader should show that $\forall t P \wedge \forall t Q \Rightarrow \forall t(P \wedge Q)$ is also provable in $\mathcal{N}_i^{\Rightarrow,\vee,\wedge,\bot,\forall,\exists}$.

However, in general, one can't just replace $\forall$ by $\exists$ (or $\wedge$ by $\vee$) and still obtain provable statements. For example, $\exists t P \wedge \exists t Q \Rightarrow \exists t(P \wedge Q)$ is not provable at all!

Here are some useful equivalences involving quantifiers. The first two are analogous to the de Morgan laws for $\wedge$ and $\vee$.

Proposition 1.8.3 *The following equivalences are provable in classical first-order logic:*

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

In fact, the last three and $\exists t \neg P \Rightarrow \neg\forall t P$ are provable intuitionistically. Moreover, the propositions $\exists t(P \wedge Q) \Rightarrow \exists t P \wedge \exists t Q$ and $\forall t P \vee \forall t Q \Rightarrow \forall t(P \vee Q)$ are provable in intuitionistic first-order logic (and thus, also in classical first-order logic).

Remark: We can illustrate, again, the fact that classical logic allows for non-constructive proofs by reexamining the example at the end of Section 1.3.

There, we proved that if $\sqrt{2}^{\sqrt{2}}$ is rational, then $a = \sqrt{2}$ and $b = \sqrt{2}$ are both irrational numbers such that a^b is rational and if $\sqrt{2}^{\sqrt{2}}$ is irrational then $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ are both irrational numbers such that a^b is rational.

By $\exists$-introduction, we deduce that if $\sqrt{2}^{\sqrt{2}}$ is rational then there exist some irrational numbers a, b so that a^b is rational and if $\sqrt{2}^{\sqrt{2}}$ is irrational then there exist some irrational numbers a, b so that a^b is rational.

In classical logic, as $P \vee \neg P$ is provable, by $\vee$-elimination, we just proved that there exist some irrational numbers a and b so that a^b is rational.

However, this argument does not give us explicitly numbers a and b with the required properties! It only tells us that such numbers must exist.

Now, it turns out that $\sqrt{2}^{\sqrt{2}}$ is indeed irrational (this follows from the Gel'fond-Schneider Theorem, a hard theorem in number theory).

Furthermore, there are also simpler explicit solutions such as $a = \sqrt{2}$ and $b = \log_2 9$, as the reader should check!

We conclude this section by giving an example of a "wrong proof".

Here is an example in which the $\forall$-introduction rule is applied illegally, and thus, yields a statement which is actually false (not provable).

In the incorrect "proof" below, P is an atomic predicate symbol taking two arguments (for example, "parent") and 0 is a constant denoting zero:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(t,0)^{x}}{\forall t P(t,0)}\ \text{illegal step!}}{P(t,0) \Rightarrow \forall t P(t,0)}\,x}{\forall t(P(t,0) \Rightarrow \forall t P(t,0))}}{P(0,0) \Rightarrow \forall t P(t,0)}$$

The problem is that the variable t occurs free in the premise $P[t/t, 0] = P(t, 0)$ and therefore, the application of the $\forall$-introduction rule in the first step is illegal.

However, note that this premise is discharged in the second step and so, the application of the $\forall$-introduction rule in the third step is legal.

The (false) conclusion of this faulty proof is that $P(0,0) \Rightarrow \forall t P(t,0)$ is provable. Indeed, there are plenty of properties such that the fact that the single instance, $P(0,0)$, holds does not imply that $P(t,0)$ holds for all t.

Remark: The above example shows why it is desirable to have premises that are universally quantified. A premise of the form $\forall t P$ can be instantiated to $P[u/t]$, using $\forall$-elimination, where u is a brand new variable.

Later on, it may be possible to use $\forall$-introduction without running into trouble with free occurrences of u in the premises. But we still have to be very careful when we use $\forall$-introduction or $\exists$-elimination.

Before concluding this section, let us give a few more examples of proofs using the rules for the quantifiers. First, let us prove that

$$\forall t P \equiv \forall u P[u/t],$$

where u is any variable not free in $\forall t P$ and such that u is not captured during the substitution.

This rule allows us to rename bound variables (under very mild conditions). We have the proofs

$$\dfrac{\dfrac{\dfrac{(\forall t P)^{\alpha}}{P[u/t]}}{\forall u P[u/t]}}{\forall t P \Rightarrow \forall u P[u/t]}\ \alpha$$

and

$$\dfrac{\dfrac{\dfrac{(\forall u P[u/t])^{\alpha}}{P[u/t]}}{\forall t P}}{\forall u P[u/t] \Rightarrow \forall t P}\ \alpha$$

Now, we give a proof (intuitionistic) of

$$\exists t(P \Rightarrow Q) \Rightarrow (\forall tP \Rightarrow Q),$$

where t does not occur (free or bound) in Q.

$$\dfrac{\dfrac{(\exists t(P \Rightarrow Q))^z \qquad \dfrac{\dfrac{(P[u/t] \Rightarrow Q)^x \qquad \dfrac{(\forall tP)^y}{P[u/t]}}{Q}}{Q}\, x}{\forall tP \Rightarrow Q}\, y}{\exists t(P \Rightarrow Q) \Rightarrow (\forall tP \Rightarrow Q)}\, z$$

In the above proof, u is a new variable that does not occur in Q, $\forall tP$, or $\exists t(P \Rightarrow Q)$. Since t does not occur in Q, we have

$$(P \Rightarrow Q)[u/t] = P[u/t] \Rightarrow Q.$$

The converse requires (RAA) and is a bit more complicated.

To conclude, we give a proof (intuitionistic) of

$$(\forall t P \vee Q) \Rightarrow \forall t (P \vee Q),$$

where t does not occur (free or bound) in Q.

$$\dfrac{\dfrac{(\forall t P \vee Q)^z \qquad \dfrac{\dfrac{\dfrac{(\forall t P)^x}{P[u/t]}}{P[u/t] \vee Q}}{\forall t (P \vee Q)} \qquad \dfrac{\dfrac{Q^y}{P[u/t] \vee Q}}{\forall t (P \vee Q)}}{\forall t (P \vee Q)}\ {\scriptstyle x,y}}{(\forall t P \vee Q) \Rightarrow \forall t (P \vee Q)}\ {\scriptstyle z}$$

In the above proof, u is a new variable that does not occur in $\forall t P$ or Q. Since t does not occur in Q, we have

$$(P \vee Q)[u/t] = P[u/t] \vee Q.$$

The converse requires (RAA).

Obviously, every first-order formula that is provable intuitionistically is also provable classically and we know that there are formulae that are provable classically but *not* provable intuitionistically.

Therefore, it appears that classical logic is more general than intuitionistic logic.

However, this not not quite so because there is a way of interpreting classical logic into intuitionistic logic.

To be more precise, every classical formula, A, can be translated into a formula, A^*, where A^* is classically equivalent to A and A is provable classically iff A^* is provable intuitionistically.

Various translations are known, all based on a "trick" involving double-negation (This is because $\neg\neg\neg A$ and $\neg A$ are intuitionistically equivalent).

Translations were given Kolmogorov (1925), Gödel (1933) and Gentzen (1933). For example, Gödel used the following translation:

$$\begin{aligned}
A^* &= \neg\neg A, \quad \text{if } A \text{ is atomic,} \\
(\neg A)^* &= \neg A^*, \\
(A \wedge B)^* &= (A^* \wedge B^*), \\
(A \Rightarrow B)^* &= \neg(A^* \wedge \neg B^*), \\
(A \vee B)^* &= \neg(\neg A^* \wedge \neg B^*), \\
(\forall x A)^* &= \forall x A^*, \\
(\exists x A)^* &= \neg\forall x \neg A^*.
\end{aligned}$$

Actually, if we restrict our attention to propositions (that is, formulae without quantifiers), a theorem of Glivenko (1929) states that if a proposition, A, is provable classically, then $\neg\neg A$ is provable intuitionistically.

In view of these results, the proponents of intuitionistic logic claim that classical logic is really a special case of intuitionistic logic!

However, the above translations have some undesirable properties, as noticed by Girard. For more details on all this, see Gallier [5].

1.9 First-Order Theories

Nonempty sets of premises, Γ, are crucially needed if we want to develop theories about various kinds of structures and objects, such as the natural numbers, groups, rings, fields, trees, graphs, sets, *etc.*

Indeed, we need to make definitions about the objects we want to study and we need to state some axioms asserting the main properties of these objects.

We do this by putting these definitions and axioms in Γ.

Actually, we have to allow Γ to be infinite but we still require that our deduction trees are finite; they can only use finitely many of the formulae in Γ.

We are then interested in all formulae, P, such that $\Delta \to P$ is provable, where Δ is any finite subset of Γ; the set of all such P's is called a *theory* (or *first-order theory*).

Of course we have the usual problem of consistency: If we are not careful, our theory may be inconsistent, *i.e.*, it may consist of all formulae.

Let us give two examples of theories.

Our first example is the *theory of equality*.

Given a language, $\mathbf{L}$, with a given supply of constant, function and predicate symbols, the theory of equality consists of the following formulae taken as axioms:

$$\forall x(x = x)$$
$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n$$
$$[(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)]$$
$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n$$
$$[(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \wedge P(x_1, \ldots, x_n) \Rightarrow P(y_1, \ldots, y_n)],$$

for all function symbols (of n arguments) and all predicate symbols (of n arguments), including the equality predicate, $=$, itself.

It is not immediately clear from the above axioms that $=$ is symmetric and transitive but this can be shown easily.

Our second example is the first-order theory of the natural numbers known as *Peano's arithmetic* (for short, *PA*).

Here, we have the constant 0 (zero), the unary function symbol S (for successor function; the intended meaning is $S(n) = n + 1$) and the binary function symbols $+$ (for addition) and $*$ (for multiplication).

In addition to the axioms for the theory of equality we have the following axioms:

$$\forall x \neg(S(x) = 0)$$
$$\forall x \forall y(S(x) = S(y) \Rightarrow x = y)$$
$$\forall x \forall y(x + 0 = x)$$
$$\forall x \forall y(x + S(y) = S(x + y))$$
$$\forall x \forall y(x * 0 = 0)$$
$$\forall x \forall y(x * S(y) = x * y + x)$$
$$[A(0) \wedge \forall x(A(x) \Rightarrow A(S(x)))] \Rightarrow \forall n A(n),$$

where A is any first-order formula with one free variable.

This last axiom is the *induction axiom*. Observe how $+$ and $*$ are defined recursively in terms of 0 and S and that there are infinitely many induction axioms (countably many).

Many properties that hold for the natural numbers (*i.e.*, are true when the symbols $0, S, +, *$ have their usual interpretation and all variables range over the natural numbers) can be proved in this theory (Peano's arithmetic), but not all!

This is another very famous result of Gödel known as *Gödel's incompleteness Theorem* (1931).

However, the topic of incompleteness is definitely outside the scope of this course, so we will not say anymore about it.

However, we feel that it should be intructive for the reader to see how simple properties of the natural numbers can be derived (in principle!) in Peano's arithmetic.

First, it will be convenient to introduce abbreviations for the terms of the form, $S^n(0)$, which represent the natural numbers.

Thus, we add a countable supply of constants, $0, 1, 2, 3, \ldots$, to denote the natural numbers and add the axioms

$$n = S^n(0),$$

for all natural numbers, n. We will also write $n + 1$ for $S(n)$.

Let us illustrate the use of the quantifiers rules involving terms ($\forall$-elimination and $\exists$-introduction) by proving some simple properties of the natural numbers, namely, being even or odd.

We will also prove a property of the natural number that we used before (in the proof that $\sqrt{2}$ is irrational), namely, that *every natural number is either even or odd*.

For this, we add the predicate symbols, "even" and "odd", to our language, and assume the following axioms defining these predicates:

$$\begin{aligned} \forall n(\text{even}(n) &\equiv \exists k(n = 2 * k)) \\ \forall n(\text{odd}(n) &\equiv \exists k(n = 2 * k + 1)). \end{aligned}$$

Consider the term, $2 * (m + 1) * (m + 2) + 1$, where m is any given natural number. We would like to prove that

$$\text{odd}(2 * (m + 1) * (m + 2) + 1)$$

is provable in Peano arithmetic.

As an auxiliary lemma, we first prove that

$$\forall x\, \mathrm{odd}(2 * x + 1),$$

is provable in Peano arithmetic.

Let p be a variable not occurring in any of the axioms of Peano arithmetic (the variable, p, stands for an arbitrary natural number).

From the axiom,

$$\forall n(\mathrm{odd}(n) \equiv \exists k(n = 2 * k + 1)),$$

by $\forall$-elimination where the term, $2 * p + 1$, is substituted for the variable, n, we get

$$\mathrm{odd}(2 * p + 1) \equiv \exists k(2 * p + 1 = 2 * k + 1). \qquad (*)$$

Now, we can think of the provable equation,

$$2 * p + 1 = 2 * p + 1,$$

as

$$(2 * p + 1 = 2 * k + 1)[p/k].$$

So, by $\exists$-introduction, we can conclude that

$$\exists k(2 * p + 1 = 2 * k + 1),$$

which, by $(*)$, implies that

$$\text{odd}(2 * p + 1).$$

But now, since p is a variable not occurring free in the axioms of Peano arithmetic, by $\forall$-introduction, we conclude that

$$\forall x \, \text{odd}(2 * x + 1).$$

Finally, if we use $\forall$-elimination where we substitute the term, $\tau = (m + 1) * (m + 2)$, for x, we get

$$\text{odd}(2 * (m + 1) * (m + 2) + 1),$$

as claimed.

Now, we wish to prove the formula:

$$\forall n(\text{even}(n) \vee \text{odd}(n)).$$

We will use the induction principle of Peano's arithmetic with

$$A(n) = \text{even}(n) \vee \text{odd}(n),$$

For the base case, $n = 0$, since $0 = 2 * 0$, (which can be proved from the Peano's axioms!), we see that even(0) holds and so even(0) $\vee$ odd(0) is proved.

For $n = 1$, since $1 = 2 * 0 + 1$ (which can be proved from the Peano's axioms!), we see that odd(1) holds and so even(1) $\vee$ odd(1) is proved.

For the induction step, we may assume that $A(n)$ has been proved and we need to prove that $A(n+1)$ holds.

So, assume that $\text{even}(n) \vee \text{odd}(n)$ holds. We do a proof by cases.

(a) If $\text{even}(n)$ holds, by definition, this means that $n = 2k$ for some k and then, $n + 1 = 2k + 1$, which again, by definition, means that $\text{odd}(n+1)$ holds and thus, $\text{even}(n+1) \vee \text{odd}(n+1)$ holds.

(b) If $\text{odd}(n)$ holds, by definition, this means that $n = 2k + 1$ for some k and then, $n + 1 = 2k + 2 = 2(k + 1)$, which again, by definition, means that $\text{even}(n+1)$ holds and thus, $\text{even}(n+1) \vee \text{odd}(n+1)$ holds.

By $\vee$-elimination, we conclude that $\text{even}(n+1) \vee \text{odd}(n+1)$ holds, establishing the induction step.

Therefore, using induction, we have proved that

$$\forall n(\text{even}(n) \vee \text{odd}(n)).$$

Actually, we know that even(n) and odd(n) are *mutually exclusive*, which means that

$$\forall n \neg(\text{even}(n) \wedge \text{odd}(n))$$

holds, but how do we prove it?

We can do this using induction. For $n = 0$, the statement odd(0) means that $0 = 2k + 1 = S(2k)$, for some k.

However, the first axiom of Peano's arithmetic states that $S(x) \neq 0$ for all x, so we get a contradiction.

For the induction step, assume that $\neg(\text{even}(n) \wedge \text{odd}(n))$ holds.

We need to prove that $\neg(\text{even}(n+1) \wedge \text{odd}(n+1))$ holds and we can do this by using our constructive proof-by contradiction rule.

So, assume that $\text{even}(n+1) \wedge \text{odd}(n+1)$ holds. At this stage, we realize that if we could prove that

$$\forall n(\text{even}(n+1) \Rightarrow \text{odd}(n)) \qquad (*)$$

and

$$\forall n(\text{odd}(n+1) \Rightarrow \text{even}(n)) \qquad (**)$$

then $\text{even}(n+1) \wedge \text{odd}(n+1)$ would imply $\text{even}(n) \wedge \text{odd}(n)$, contradicting the assumption $\neg(\text{even}(n) \wedge \text{odd}(n))$.

Therefore, the proof will be complete if we can prove $(*)$ and $(**)$.

Let's consider the implication $(*)$ leaving the proof of $(**)$ as an exercise.

Assume that even$(n+1)$ holds. Then, $n+1 = 2k$, for some natural number, k. We can't have $k = 0$ since otherwise we would have $n+1 = 0$, contradicting one of the Peano's axioms. But then, k is of the form $k = h+1$, for some natural number, h, so

$$n+1 = 2k = 2(h+1) = 2h+2 = (2h+1)+1.$$

By the second Peano axiom, we must have

$$n = 2h+1,$$

which proves that n is odd, as desired.

In that last proof, we made implicit use of the fact that every natural number, n, different from zero is of the form $n = m+1$, for some natural number, m, which is formalized as

$$\forall n((n \neq 0) \Rightarrow \exists m(n = m+1)).$$

This is easily proved by induction.

Having done all this work, we have finally proved $(*)$ and after proving $(**)$, we will have proved that

$$\forall n \neg(\text{even}(n) \wedge \text{odd}(n)).$$

It is also easy to prove that

$$\forall n(\text{even}(n) \vee \text{odd}(n))$$

and

$$\forall n \neg(\text{even}(n) \wedge \text{odd}(n))$$

together imply that

$$\forall n(\text{even}(n) \equiv \neg\text{odd}(n)) \quad \text{and} \quad \forall n(\text{odd}(n) \equiv \neg\text{even}(n)),$$

are provable in Peano's arithmetic, facts that we used several times in Section 1.6.

These examples of proofs in the theory of Peano's arithmetic illustrate the fact that constructing proofs in an axiomatized theory is a very laborious and tedious process.

Many small technical lemmas need to be established from the axioms, which renders these proofs very lengthy and often unintuitive.

It is therefore important to build up a database of useful basic facts if we wish to prove, with a certain amount of comfort, properties of objects whose properties are defined by an axiomatic theory (such as the natural numbers).

However, when in doubt, we can always go back to the formal theory and try to prove rigorously the facts that we are not sure about, even though this is usually a tedious and painful process.

Human provers navigate in a "*spectrum of formality*", most of the time constructing informal proofs containing quite a few (harmless!) shortcuts, sometimes making extra efforts to construct more formalized and rigorous arguments if the need arises.

Now, what if the theory of Peano's arithmetic was inconsistent! How do know that Peano's arithmetic does not imply any contradiction?

This is an important and hard question that motivated a lot of the work of Gentzen.

An easy answer is that the *standard model*, $\mathbb{N}$, of the natural numbers under addition and multiplication validates all the axioms of Peano's' arithmetic.

Therefore, if both P and $\neg P$ could be proved from the Peano axioms, then both P and $\neg P$ would be true in $\mathbb{N}$, which is absurd.

To make all this rigorous, we need to define the notion of *truth in a structure*, a notion which is explained in every logic book.

It should be noted that the constructivists will object to the above method for showing the consistency of Peano's arithmetic, because it assumes that the infinite set, $\mathbb{N}$, exists as a completed entity.

Until further notice, we will have faith in the consistency of Peano's arithmetic (so far, no inconsistency has been found).

Another very interesting theory is *set theory*. There are a number of axiomatizations of set theory and we will discuss one of them (ZF) very briefly in Section 1.10.