8

Nonnegative Integers

The most important axiomatic theories for us will be those defined by the *principle of mathematical induction.* This principle is represented here as an axiom schema, an infinite set of axioms, like the functional- and predicate-substitutivity axioms for equality. Theories with induction include those of the nonnegative integers, tuples, trees, and other fundamental structures. We begin with the nonnegative integers, which are the most familiar and the most important.

8.1 BASIC PROPERTIES

In the theory of the nonnegative integers, we define

- A constant symbol 0, denoting the integer *zero*
- A unary function symbol x^+, denoting the *successor* function
- A unary predicate symbol $integer(x)$.

The reader should understand that 0 is an informal notation for a constant symbol (such as a or b) and is not to be confused with the actual integer zero, which is a domain element. Under the intended model for the theory, the symbol 0 will be assigned the integer zero as its value.

Also the symbol x^+ is an informal notation for a unary function symbol (such as $f(x)$ or $g(x)$). Under the intended model for the theory, the function symbol x^+ will be assigned the successor function, i.e., the function that maps the integer d into the integer $d + 1$.

The terms of the theory include

$$0, \quad 0^+, \quad (0^+)^+, \quad ((0^+)^+)^+, \quad \ldots .$$

Conventionally, 0^+ is abbreviated as 1, $(0^+)^+$ as 2, $((0^+)^+)^+$ as 3, and so forth. The symbols 1, 2, 3, ... are merely informal abbreviations for these terms; they are not notations for constant symbols. Under the intended model they denote the actual domain elements one, two, three, ...

The predicate symbol *integer*(x) is intended to be true if x is assigned a nonnegative integer, and false otherwise. In the simplest models for the theory, all the domain elements will be nonnegative integers, and hence *integer*(x) will always be true. Later, however, we shall introduce elements into our domain that are not nonnegative integers; the predicate symbol *integer*(x) will then be used to distinguish between the nonnegative integers and the other domain elements.

The theory of the nonnegative integers is a theory with equality defined by the following axioms:

- The *generation* axioms

$integer(0)$	(*zero*)
$(\forall\ integer\ x)[integer(x^+)]$	(*successor*)

- The *uniqueness* axioms

$(\forall\ integer\ x)[not\ (x^+ = 0)]$	(*zero*)
$(\forall\ integer\ x, y)\begin{bmatrix} if\ \ x^+ = y^+ \\ then\ \ x = y \end{bmatrix}$	(*successor*)

- The *induction* principle

For each sentence $\mathcal{F}[x]$ in the theory, the universal closure of the sentence

$$if \begin{bmatrix} \mathcal{F}[0] \\ \quad and \\ (\forall\ integer\ x)\begin{bmatrix} if\ \ \mathcal{F}[x] \\ then\ \ \mathcal{F}[x^+] \end{bmatrix} \end{bmatrix} \qquad (induction)$$

$$then\ \ (\forall\ integer\ x)\mathcal{F}[x]$$

is an axiom.

The two generation axioms have the intuitive meaning that any element that can be constructed from the zero element 0 and the successor function x^+ is a nonnegative integer. Thus 0, 0^+, $(0^+)^+$, ... all denote nonnegative integers.

The two uniqueness axioms have the intuitive meaning that each nonnegative integer can be constructed in at most one way from the zero element 0 and the successor function x^+. Thus 0, 0^+, $(0^+)^+$, ... denote distinct nonnegative integers.

Note that the axioms for the theory include two *zero* axioms and two *successor* axioms. In referring to them later we shall always discriminate between them by speaking of the *zero* generation axiom or the *zero* uniqueness axiom and of the *successor* generation axiom or the *successor* uniqueness axiom.

The *induction* principle is actually an axiom schema, because it represents an infinite set of axioms, one for each sentence $\mathcal{F}[x]$ in the theory. The sentence $\mathcal{F}[x]$ is called the *inductive sentence.* The subsentence

$$\mathcal{F}[0]$$

is called the *base case* of the induction. The subsentence

$$(\forall \textit{ integer } x) \begin{bmatrix} \textit{if } \mathcal{F}[x] \\ \textit{then } \mathcal{F}[x^+] \end{bmatrix}$$

is called the *inductive step*; the subsentences $\mathcal{F}[x]$ and $\mathcal{F}[x^+]$ of the inductive step are called the *induction hypothesis* and the *desired conclusion*, respectively. The variable x is called the *inductive variable.*

The inductive sentence $\mathcal{F}[x]$ may have free variables other than x. The *induction* principle asserts that the universal closure of the implication is valid, i.e., true under every model of the theory. This implies that the implication itself is true under every model.

The *induction* principle may be paraphrased intuitively as follows:

> To show that a sentence $\mathcal{F}[x]$ is true for every nonnegative integer x (under a given interpretation), it suffices to show the base case
>
> $\mathcal{F}[0]$ is true
>
> and the inductive step
>
> for an arbitrary nonnegative integer x,
> if $\mathcal{F}[x]$ is true,
> then $\mathcal{F}[x+1]$ is also true.

The *induction* principle states that, to show that a sentence is true for all the nonnegative integers, it suffices to show that the sentence is true for 0 and that, whenever it is true for a nonnegative integer x, it is also true for the successor x^+. Therefore it is true for 0^+ (by one application of the inductive step), for $(0^+)^+$ (by another application of the inductive step), and so forth.

In **Problem 8.13**, the reader is requested to show that a schema obtained by renaming a bound variable in the *induction* principle, which is therefore apparently equivalent to the *induction* principle, is actually not valid. (This exercise

is included as one of the last problems in this chapter because of its theoretical nature.)

Since the theory of the nonnegative integers is a theory with equality, we include the equality axioms. In particular, we have the appropriate instances of the *substitutivity* axiom schemata,

$$(\forall x, y)\begin{bmatrix} \textit{if} \;\; x = y \\ \textit{then} \;\; x^+ = y^+ \end{bmatrix} \qquad (\textit{functional substitutivity for } x^+)$$

$$(\forall x, y)\begin{bmatrix} \textit{if} \;\; x = y \\ \textit{then} \;\; \textit{integer}(x) \;\equiv\; \textit{integer}(y) \end{bmatrix}$$

$$(\textit{predicate substitutivity for integer})$$

In the intended model for the theory, the domain consists of the ordinary nonnegative integers $0, 1, 2, \ldots$ and the function symbol x^+ is assigned the successor function over the nonnegative integers. The reader will see (in Chapter 14) that there are actually some quite different "nonstandard" models for this theory.

In this chapter, when we speak about the validity of a sentence, we shall always mean validity in the theory of the nonnegative integers. Let us show the validity of a sentence in this theory.

Proposition (decomposition)

The sentence

$$(\forall \textit{ integer } x)\begin{bmatrix} \textit{if} \;\; \textit{not } (x = 0) \\ \textit{then} \;\; (\exists \textit{ integer } y)[x = y^+] \end{bmatrix} \qquad (\textit{decomposition})$$

is valid (in the theory of the nonnegative integers). ∎

Proof. The proof employs the instance of the *induction* principle in which the inductive sentence is taken to be

$$\mathcal{F}[x]: \quad \begin{array}{l} \textit{if} \;\; \textit{not } (x = 0) \\ \textit{then} \;\; (\exists \textit{ integer } y)[x = y^+] \end{array}.$$

To show

$$(\forall \textit{ integer } x)\mathcal{F}[x]$$

(under an interpretation), it suffices, by the *induction* principle and propositional logic, to establish the base case,

$$\mathcal{F}[0],$$

and the inductive step,

$$(\forall \textit{ integer } x)\begin{bmatrix} \textit{if} \;\; \mathcal{F}[x] \\ \textit{then} \;\; \mathcal{F}[x^+] \end{bmatrix}.$$

We show the base case and the inductive step separately.

Base Case

We want to show

$$\mathcal{F}[0]: \quad \begin{array}{l} \textit{if not } (0 = 0) \\ \textit{then } (\exists \textit{ integer } y)[0 = y^+] \end{array}.$$

Because (by the *reflexivity* axiom for equality) $0 = 0$, the antecedent

$$\textit{not } (0 = 0)$$

of this implication is false and therefore the entire sentence is true.

Inductive Step

We want to show

$$(\forall \textit{ integer } x) \begin{bmatrix} \textit{if } \mathcal{F}[x] \\ \textit{then } \mathcal{F}[x^+] \end{bmatrix},$$

that is,

$$(\forall \textit{ integer } x) \begin{bmatrix} \textit{if } \begin{bmatrix} \textit{if not } (x = 0) \\ \textit{then } (\exists \textit{ integer } y)[x = y^+] \end{bmatrix} \\ \textit{then } \begin{bmatrix} \textit{if not } (x^+ = 0) \\ \textit{then } (\exists \textit{ integer } y)[x^+ = y^+] \end{bmatrix} \end{bmatrix}.$$

Consider an arbitrary nonnegative integer x, that is, an element x such that

$$\textit{integer}(x).$$

We assume the induction hypothesis

$$\mathcal{F}[x]: \quad \begin{array}{l} \textit{if not } (x = 0) \\ \textit{then } (\exists \textit{ integer } y)[x = y^+] \end{array}$$

and would like to show the desired conclusion

$$\mathcal{F}[x^+]: \quad \begin{array}{l} \textit{if not } (x^+ = 0) \\ \textit{then } (\exists \textit{ integer } y)[x^+ = y^+] \end{array}.$$

It suffices to show the consequent,

$$(\exists \textit{ integer } y)[x^+ = y^+],$$

of the desired conclusion $\mathcal{F}[x^+]$.

Because we have supposed $\textit{integer}(x)$ and we know (by the *reflexivity* axiom for equality) that $x^+ = x^+$, we have

$$\begin{array}{c} \textit{integer}(x) \\ \textit{and} \\ x^+ = x^+. \end{array}$$

Therefore (by the *existential quantifier-instantiation* proposition, taking y to be x) we have

$$(\exists y) \begin{bmatrix} \textit{integer}(y) \\ \textit{and} \\ x^+ = y^+ \end{bmatrix}$$

or, in terms of our relative quantifier notation,

$$(\exists \textit{ integer } y)[x^+ = y^+],$$

as we wanted to show.

Since we have established both the base case and the inductive step, the proof is complete. ▟

The above proof has the unusual feature that it requires the *induction* principle but makes no use of the induction hypothesis in the inductive step. Nevertheless, the principle is essential in this proof. If the principle were deleted from the theory of the nonnegative integers, there would be models for the resulting theory under which the *decomposition* property would not be true. The reader is requested to show this in **Problem 8.14**. (This problem, like Problem 8.13, is placed late in the list because of its theoretical nature.)

8.2 THE ADDITION FUNCTION

Suppose we augment our theory of the nonnegative integers by formulating two axioms that define a binary function symbol $x + y$, denoting, under the intended model, the *addition* (*plus*) function over the nonnegative integers. As usual, $x + y$ is merely a conventional notation for a standard binary function symbol of predicate logic, such as $f_{97}(x, y)$.

The axioms for addition are as follows:

$(\forall \textit{ integer } x)[x + 0 = x]$	(*right zero*)
$(\forall \textit{ integer } x, y)[x + y^+ = (x + y)^+]$	(*right successor*)

As usual, when we introduce a new function symbol into a theory with equality, we automatically provide the corresponding instances of the *functional-substitutivity* axiom schema for addition, that is,

$$(\forall x, y, z)\begin{bmatrix} \textit{if } & x = y \\ \textit{then } & x + z = y + z \end{bmatrix} \qquad (\textit{left functional substitutivity})$$

and

$$(\forall x, y, z)\begin{bmatrix} \textit{if } & x = y \\ \textit{then } & z + x = z + y \end{bmatrix} \qquad (\textit{right functional substitutivity})$$

We also provide those instances of the *induction* principle for which the inductive sentence $\mathcal{F}[x]$ contains occurrences of the new symbol $x + y$.

The *right-zero* and *right-successor* axioms for addition are in the form of a typical "recursive" definition for the function. The *right-zero* axiom defines

the function for the case in which its second argument is 0. The *right-successor* axiom defines the function for the case in which its second argument is of form y^+; the value of $x + y^+$ is defined in terms of the value of $x + y$. Because (by the *decomposition* proposition) the second argument must either be 0 or of the form y^+, the two axioms cover all possibilities. These axioms suggest a method for computing the addition function, as we shall see in a subsequent remark.

As before, whenever we add new axioms to a theory, we run the risk of making it inconsistent. Usually we disregard this issue and assume that the axioms we provide do not introduce inconsistencies. One can show that the axioms for addition, and in general other sets of axioms of the same (recursive) form, preserve the consistency of the theory.

It may not be obvious that the *right-zero* and *right-successor* axioms actually define the addition function we are familiar with in everyday life. We cannot state or prove this within the theory, but we can try to convince ourselves that it is so by showing that the function defined by the axioms satisfies the properties we expect the addition function to have.

In our augmented theory we can establish the validity of the following properties of addition:

$$(\forall\ \textit{integer}\ x,\ y)\big[\textit{integer}(x + y)\big] \qquad (\textit{sort})$$

$$(\forall\ \textit{integer}\ x)\big[x + 1 \ = \ x^+\big] \qquad (\textit{right one})$$

$$(\forall\ \textit{integer}\ x)\big[0 + x \ = \ x\big] \qquad (\textit{left zero})$$

$$(\forall\ \textit{integer}\ x,\ y)\big[(x + 1) + y = (x + y) + 1\big] \qquad (\textit{left successor})$$

$$(\forall\ \textit{integer}\ x,\ y)\big[x + y = y + x\big] \qquad (\textit{commutativity})$$

The *sort* property establishes that the result $x+y$ of adding two nonnegative integers is also a nonnegative integer.

Recall that, in the *right-one* property, 1 is merely an abbreviation for 0^+, the binary function symbol $+$ in the term $x+1$ denotes the addition function, and the unary function symbol $^+$ in the term x^+ denotes the successor function. Once we have established the *right-one* property, we can use the more conventional expression $t + 1$, rather than t^+, to denote the successor of t, for any term t that denotes a nonnegative integer. For example, in the *left-successor* property, we write $x+1$ and $(x+y)+1$, in terms of the addition function, rather than x^+ and $(x + y)^+$, in terms of the successor function.

The order in which the properties are presented is significant; some of their proofs make use of earlier properties on the list. We will give proofs for the last

four of these properties, illustrating various features of mathematical proofs; the proof for the first one is routine and is left as an exercise (**Problem 8.1(a)**).

PROOF WITHOUT INDUCTION

We begin with the *right-one* property; its proof does not require the *induction* principle.

Proposition (right one)

The sentence

$$(\forall\ \textit{integer}\ x)\big[x + 1 \ = \ x^+\big]$$

is valid. ▟

Proof. Consider an arbitrary nonnegative integer x, that is, an element x such that

$$\textit{integer}(x).$$

We would like to prove that

$$x + 1 \ = \ x^+.$$

Because 1 is an abbreviation for 0^+, we actually want to show

$$x + 0^+ \ = \ x^+.$$

Because $\textit{integer}(x)$ and (by the *zero* generation axiom) $\textit{integer}(0)$, we have (by the *right-successor* axiom for addition)

$$(\dagger) \qquad x + 0^+ \ = \ (x + 0)^+.$$

Because $\textit{integer}(x)$, we have (by the *right-zero* axiom for addition)

$$x + 0 \ = \ x.$$

Therefore, by the *functional-substitutivity* equality axiom for the successor function,

$$(\ddagger) \qquad (x + 0)^+ \ = \ x^+.$$

Finally, by (†), (‡), and the *transitivity* axiom for equality, we obtain

$$x + 0^+ \ = \ x^+,$$

as we wanted to show. ▟

As usual, in the above proof we have invoked basic properties of predicate logic without mentioning them. For example, when we applied the *functional-substitutivity* axiom to derive (‡), we appealed implicitly to the *universal* part of the *quantifier-instantiation* proposition. Let us now discuss some other features of the above proof.

Remark (sort conditions). In the above proof, before we could apply the *right-successor* axiom for addition to conclude (†), that

$$x + 0^+ = (x + 0)^+,$$

it was necessary to establish the "sort conditions" that x and 0 are both nonnegative integers, that is,

$$\mathit{integer}(x) \quad \text{and} \quad \mathit{integer}(0).$$

This is because the axiom reads (after renaming the bound variables to avoid confusion)

$$(\forall\ \mathit{integer}\ u,\ v)\big[u + v^+ = (u + v)^+\big]$$

or, abandoning the relative quantifier notation,

$$(\forall\, u, v)\begin{bmatrix} \mathit{if}\ \ \mathit{integer}(u)\ \ \mathit{and}\ \ \mathit{integer}(v) \\ \mathit{then}\ \ u + v^+ = (u + v)^+ \end{bmatrix}.$$

In other words, the axiom applies only if u and v are nonnegative integers. In particular, taking u to be x and v to be 0, we have

$$\begin{aligned} &\mathit{if}\ \ \mathit{integer}(x)\ \ \mathit{and}\ \ \mathit{integer}(0) \\ &\mathit{then}\ \ x + 0^+ = (x + 0)^+. \end{aligned}$$

Then, because $\mathit{integer}(x)$ and $\mathit{integer}(0)$, we can conclude that

$$x + 0^+ = (x + 0)^+,$$

as we did in the proof.

For the same reason, before we could apply the *right-zero* axiom for addition, to conclude that

$$x + 0 = x,$$

it was necessary to establish that x is a nonnegative integer, that is,

$$\mathit{integer}(x).$$

In future proofs we shall not always bother to establish such sort conditions, i.e., that the terms we construct denote nonnegative integers, since these aspects of a proof tend to be repetitive and straightforward. Sort conditions may be assumed without proof in all the exercises, unless otherwise requested. ▟

Remark (equality). We shall assume henceforth that the reader is so familiar with the theory of equality that we do not need to mention its properties explicitly during a proof.

Thus we may abbreviate the above argument, showing that $x + 0^+ = x^+$, as follows:

for an arbitrary nonnegative integer x,

$$x + 0^+ = (x + 0)^+$$

(by the *right-successor* axiom for addition)

$$= x^+$$

(by the *right-zero* axiom for addition).

Here we have not mentioned the *functional-substitutivity* and *transitivity* axioms for equality. ▟

We have established the *right-one* property, i.e., that

$$(\forall \textit{ integer } x)\big[x + 1 = x^+\big].$$

In particular, for any term t, we may conclude (by the *universal quantifier-instantiation* proposition) that

if integer(t)
then $t + 1 = t^+$.

Hence (by the substitutivity of equality) if t stands for a nonnegative integer, any sentence $\mathcal{F}\langle t^+\rangle$ containing the term t^+ is equivalent to the corresponding sentence $\mathcal{F}\langle t+1\rangle$ containing instead the term $t+1$. Therefore as we have remarked earlier, we may now use the conventional notation $t + 1$ freely in place of our original notation t^+, to denote the successor of t.

Remark (computation of addition). The axioms for the addition function can be used to prove properties of the function, such as the above *right-one* property. Furthermore, the axioms actually suggest a way to compute the function, in terms of the constant 0 and the successor function x^+. In other words, the axioms can be regarded as a "program" for performing addition. This is illustrated by the following example.

Suppose we would like to compute $3+2$, that is, $((0^+)^+)^+ + (0^+)^+$. In other words, we would like to find a term equal to $((0^+)^+)^+ + (0^+)^+$ expressed solely in terms of the constant 0 and the successor function x^+, not the addition function $x + y$. We have

$$\begin{aligned}
((0^+)^+)^+ + (0^+)^+ &= (((0^+)^+)^+ + 0^+)^+ \\
&\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition)} \\
&= ((((0^+)^+)^+ + 0)^+)^+ \\
&\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition)} \\
&= ((((0^+)^+)^+)^+)^+ \\
&\qquad \text{(by the } \textit{right-zero} \text{ axiom for addition).}
\end{aligned}$$

In short,

$$((0^+)^+)^+ + (0^+)^+ = ((((0^+)^+)^+)^+)^+,$$

that is,

$$3 + 2 = 5.$$

In the computation we have applied properties of equality without mentioning them explicitly. We have also disregarded the *sort* conditions, e.g., that *integer*(0) and *integer*(0^+) are true. ▟

A SIMPLE INDUCTION PROOF

The proof of the *right-one* property did not require induction. The proof of the *decomposition* property did use induction, but the inductive step did not use the induction hypothesis. Now let us consider a proof that makes use of the *induction* principle in a more conventional way.

Proposition (left zero)

The sentence

$$(\forall\ \textit{integer}\ x)\big[0 + x\ =\ x\big]$$

is valid. ∎

Proof. The proof employs the instance of the *induction* principle in which the inductive sentence is taken to be

$$\mathcal{F}[x]:\quad 0 + x\ =\ x.$$

To prove

$$(\forall\ \textit{integer}\ x)\mathcal{F}[x],$$

it suffices, by the *induction* principle, to establish the base case,

$$\mathcal{F}[0],$$

and the inductive step,

$$(\forall\ \textit{integer}\ x)\begin{bmatrix}\textit{if}\ \ \mathcal{F}[x] \\ \textit{then}\ \ \mathcal{F}[x+1]\end{bmatrix}.$$

(Note that here we use the more familiar notation $x + 1$ rather than x^+.)

We establish the base case and the inductive step separately.

Base Case

We want to prove

$$\mathcal{F}[0]:\quad 0 + 0\ =\ 0.$$

But this is an instance of the *right-zero* axiom for addition,

$$(\forall\ \textit{integer}\ x)[x + 0\ =\ x].$$

Inductive Step

We want to prove

$$(\forall\ \textit{integer}\ x)\begin{bmatrix}\textit{if}\ \ \mathcal{F}[x] \\ \textit{then}\ \ \mathcal{F}[x+1]\end{bmatrix}.$$

For an arbitrary nonnegative integer x, we assume the induction hypothesis

$$\mathcal{F}[x]:\quad 0 + x\ =\ x$$

and attempt to establish the desired conclusion

$$\mathcal{F}[x+1]: \quad 0+(x+1) = x+1.$$

But we have

$$\begin{aligned} 0+(x+1) &= (0+x)+1 \\ &\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition)} \\ &= x+1 \\ &\qquad \text{(by our induction hypothesis).} \end{aligned}$$

CHOICE OF VARIABLES

The principle of mathematical induction states that

for all sentences $\mathcal{F}[x]$ in the theory of the nonnegative integers, the universal closure of

$$\textit{if} \begin{bmatrix} \mathcal{F}[0] \\ \quad \textit{and} \\ (\forall \textit{ integer } x) \begin{bmatrix} \textit{if } \mathcal{F}[x] \\ \textit{then } \mathcal{F}[x+1] \end{bmatrix} \end{bmatrix}$$

$$\textit{then } (\forall \textit{ integer } x)\mathcal{F}[x]$$

is an axiom.

Note that x can be taken to be any variable; thus we can apply the principle to prove sentences $(\forall \textit{ integer } x)\mathcal{F}[x]$ by "induction on x," $(\forall \textit{ integer } y)\mathcal{F}[y]$ by "induction on y," or $(\forall \textit{ integer } z)\mathcal{F}[z]$ by "induction on z," and so forth.

The following proposition illustrates a proof by induction on y.

Proposition (left successor)

The sentence

$$(\forall \textit{ integer } x, y)\big[(x+1)+y = (x+y)+1\big]$$

is valid. ∎

Proof. Consider an arbitrary nonnegative integer x; we attempt to prove

$$(\forall \textit{ integer } y)\big[(x+1)+y = (x+y)+1\big].$$

The proof is by induction on y; we take the inductive sentence to be

$$\mathcal{F}[y]: \quad (x+1)+y = (x+y)+1.$$

To prove

$$(\forall \textit{ integer } y)\mathcal{F}[y],$$

it suffices, by the *induction* principle, to establish the base case,

$$\mathcal{F}[0],$$

and the inductive step,

$$(\forall \textit{ integer } y)\begin{bmatrix}\textit{if } \mathcal{F}[y] \\ \textit{then } \mathcal{F}[y+1]\end{bmatrix}.$$

We establish the base case and the inductive step separately.

Base Case

We would like to prove

$$\mathcal{F}[0]: \quad (x+1)+0 = (x+0)+1.$$

But we have

$$\begin{aligned}(x+1)+0 &= x+1 \\ &\qquad \text{(by the } \textit{right-zero} \text{ axiom for addition)} \\ &= (x+0)+1 \\ &\qquad \text{(by the } \textit{right-zero} \text{ axiom for addition again).}\end{aligned}$$

Inductive Step

For an arbitrary nonnegative integer y, we assume the induction hypothesis

$$\mathcal{F}[y]: \quad (x+1)+y = (x+y)+1$$

and attempt to prove the desired conclusion

$$\mathcal{F}[y+1]: \quad (x+1)+(y+1) = \big(x+(y+1)\big)+1.$$

But we have

$$\begin{aligned}(x+1)+(y+1) &= \big((x+1)+y\big)+1 \\ &\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition)} \\ &= \big((x+y)+1\big)+1 \\ &\qquad \text{(by our induction hypothesis)} \\ &= \big(x+(y+1)\big)+1 \\ &\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition again).}\end{aligned}$$

∎

Note that in the above proof the inductive sentence $\mathcal{F}[y]$, that is,

$$(x+1)+y = (x+y)+1,$$

contained free occurrences of x as well as y.

Remark (choice of variables). The proof illustrates some of the strategic aspects of the use of the *induction* principle. It might seem more straightforward to attempt the proof by induction on x, taking the inductive sentence to be

$$\mathcal{F}[x]: \quad (\forall \textit{ integer } y)\big[(x+1)+y = (x+y)+1\big].$$

In such a proof, we would first attempt to establish the base case

$$\mathcal{F}[0]: \quad (\forall \textit{ integer } y)\big[(0+1)+y \;=\; (0+y)+1\big].$$

Considering an arbitrary nonnegative integer y, we would try to prove

$$(0+1)+y \;=\; (0+y)+1$$

or, equivalently (by two applications of the *left-zero* property of addition),

$$1+y \;=\; y+1.$$

For this purpose, we would have to prove that

$$(\forall \textit{ integer } y)[1+y \;=\; y+1],$$

requiring an additional application of the *induction* principle, on y. An attempt to establish the inductive step of such a proof would lead to similar obstructions.

In other words, a decision to use induction on x, rather than on y, in proving the *left-successor* property of addition would lead to a needlessly complicated proof. In general, part of the strategic aspect of using the *induction* principle is deciding on which variable to do induction. This decision depends on the axioms and properties we have available. Sometimes an unsuccessful proof attempt will suggest a variable on which to do induction. ▟

USE OF EARLIER RESULTS

Once we have established the validity of a sentence in the theory of the nonnegative integers, we can use it in the proofs of other sentences, just as we would use an axiom. The proof of the following *commutativity* property relies on the validity of the *left-zero* property,

$$(\forall \textit{ integer } x)\big[0+x \;=\; x\big],$$

and the *left-successor* property,

$$(\forall \textit{ integer } x,\, y)\big[(x+1)+y \;=\; (x+y)+1\big],$$

which we established in the preceding sections.

Proposition (commutativity)

The sentence

$$(\forall \textit{ integer } x,\, y)\big[x+y \;=\; y+x\big]$$

is valid. ▟

Proof. Consider an arbitrary nonnegative integer x; we would like to prove

$$(\forall \textit{ integer } y)\big[x+y \;=\; y+x\big].$$

The proof is by induction on y; we take the inductive sentence to be

$$\mathcal{F}[y]: \quad x + y = y + x.$$

To prove

$$(\forall \textit{ integer } y)\mathcal{F}[y],$$

it suffices, by the *induction* principle, to establish the base case,

$$\mathcal{F}[0],$$

and the inductive step,

$$(\forall \textit{ integer } y) \begin{bmatrix} \textit{if } \mathcal{F}[y] \\ \textit{then } \mathcal{F}[y+1] \end{bmatrix}.$$

Base Case

We would like to prove

$$\mathcal{F}[0]: \quad x + 0 = 0 + x.$$

But we have

$$\begin{aligned} x + 0 &= x \\ &\qquad \text{(by the } \textit{right-zero} \text{ axiom for addition)} \\ &= 0 + x \\ &\qquad \text{(by the } \textit{left-zero} \text{ property of addition).} \end{aligned}$$

Inductive Step

For an arbitrary nonnegative integer y, we assume the induction hypothesis

$$\mathcal{F}[y]: \quad x + y = y + x$$

and attempt to establish the desired conclusion

$$\mathcal{F}[y+1]: \quad x + (y+1) = (y+1) + x.$$

But we have

$$\begin{aligned} x + (y+1) &= (x+y) + 1 \\ &\qquad \text{(by the } \textit{right-successor} \text{ axiom for addition)} \\ &= (y+x) + 1 \\ &\qquad \text{(by our induction hypothesis)} \\ &= (y+1) + x \\ &\qquad \text{(by the } \textit{left-successor} \text{ property of addition).} \end{aligned}$$

The proof of the *commutativity* proposition for addition above made use of the *left-zero* and the *left-successor* properties of addition, whose validity we established earlier. Had we attempted to prove the *commutativity* proposition without having proved the other two properties first, we would have had to include the proof of the two required properties within the proof of the proposition, making the combined proof rather unwieldy.

We can also establish the validity of the following properties of the addition function:

$$(\forall \textit{ integer } x, y, z)\big[(x+y)+z = x+(y+z)\big] \qquad (\textit{associativity})$$

$$(\forall \textit{ integer } x, y, z)\begin{bmatrix}\textit{if } \; z+x = z+y \\ \textit{then } \; x = y\end{bmatrix} \qquad (\textit{left cancellation})$$

$$(\forall \textit{ integer } x, y, z)\begin{bmatrix}\textit{if } \; x+z = y+z \\ \textit{then } \; x = y\end{bmatrix} \qquad (\textit{right cancellation})$$

$$(\forall \textit{ integer } x, y)\begin{bmatrix}\textit{if } \; x+y = 0 \\ \textit{then } \; x = 0 \;\; \textit{and} \;\; y = 0\end{bmatrix} \qquad (\textit{annihilation})$$

The proofs are left as an exercise (**Problem 8.1(b)-(e)**).

Note that once we have established the *associativity* property of addition we can freely use the conventional notation $r + s + t$, rather than $(r + s) + t$ or $r + (s + t)$, because both terms have the same value under every model.

8.3 MULTIPLICATION AND EXPONENTIATION

In this section we extend the theory by defining two new functions. We shall also illustrate some of the strategic aspects of using the *induction* principle.

MULTIPLICATION

Let us further augment our theory of the nonnegative integers by introducing axioms that define a binary function symbol $x \cdot y$, denoting, under the intended model, the *multiplication* (*times*) function over the nonnegative integers.

The axioms for multiplication are as follows:

$$\boxed{\begin{array}{ll} (\forall \textit{ integer } x)\big[x \cdot 0 \;=\; 0\big] & (\textit{right zero}) \\[2ex] (\forall \textit{ integer } x, y)\big[x \cdot (y+1) \;=\; x \cdot y + x\big] & (\textit{right successor}) \end{array}}$$

We write $x \cdot y + x$ as an abbreviation of $(x \cdot y) + x$.

As before, we introduce the corresponding instances of the *functional-substitutivity* equality axiom schema for multiplication automatically:

$$(\forall x, y, z)\begin{bmatrix} \textit{if } x = y \\ \textit{then } x \cdot z = y \cdot z \end{bmatrix} \qquad (\textit{left functional substitutivity})$$

$$(\forall x, y, z)\begin{bmatrix} \textit{if } x = y \\ \textit{then } z \cdot x = z \cdot y \end{bmatrix} \qquad (\textit{right functional substitutivity})$$

We also introduce automatically those instances of the *induction* principle for which the inductive sentence contains occurrences of the new function symbol $x \cdot y$. Henceforth we shall not mention these additional axioms.

Note also that we retain the axioms that define the addition function.

In our augmented theory we can establish the validity of the following properties of multiplication:

$$(\forall \textit{ integer } x, y)[\textit{integer}(x \cdot y)] \qquad (\textit{sort})$$

$$(\forall \textit{ integer } x)[x \cdot 1 = x] \qquad (\textit{right one})$$

$$(\forall \textit{ integer } x)[0 \cdot x = 0] \qquad (\textit{left zero})$$

$$(\forall \textit{ integer } x, y)[(x + 1) \cdot y = x \cdot y + y] \qquad (\textit{left successor})$$

$$(\forall \textit{ integer } x)[1 \cdot x = x] \qquad (\textit{left one})$$

From these properties we can establish the associativity, commutativity, and distributivity of multiplication:

$$(\forall \textit{ integer } x, y, z)[x \cdot (y + z) = x \cdot y + x \cdot z] \qquad (\textit{right distributivity})$$

$$(\forall \textit{ integer } x, y, z)[(x \cdot y) \cdot z = x \cdot (y \cdot z)] \qquad (\textit{associativity})$$

$$(\forall \textit{ integer } x, y)[x \cdot y = y \cdot x] \qquad (\textit{commutativity})$$

$$(\forall \textit{ integer } x, y, z)[(x + y) \cdot z = x \cdot z + y \cdot z] \qquad (\textit{left distributivity})$$

The proofs of all these properties are left as an exercise (**Problem 8.2**). As usual, the order in which the properties are presented is significant; some of their proofs make use of earlier properties on the list.

EXPONENTIATION

Let us augment our theory of the nonnegative integers further by introducing two axioms that define a binary function symbol x^y, denoting, under the intended model, the *exponentiation* function over the nonnegative integers.

The axioms for exponentiation are as follows:

$$\boxed{\begin{array}{ll} (\forall\ \textit{integer}\ x)\left[x^0 = 1\right] & (\textit{exp zero}) \\ (\forall\ \textit{integer}\ x,\ y)\left[x^{y+1} = x^y \cdot x\right] & (\textit{successor}) \end{array}}$$

(Note that, under these axioms, 0^0 is taken to be 1, not 0.)

From these axioms we can establish the validity of the following properties of exponentiation:

$$(\forall\ \textit{integer}\ x,\ y)\left[\textit{integer}(x^y)\right] \qquad (\textit{sort})$$

$$(\forall\ \textit{integer}\ x)\left[x^1 = x\right] \qquad (\textit{exp one})$$

$$(\forall\ \textit{integer}\ y)\begin{bmatrix}\textit{if}\ \ \textit{not}\ (y = 0) \\ \textit{then}\ \ 0^y = 0\end{bmatrix} \qquad (\textit{zero exp})$$

$$(\forall\ \textit{integer}\ y)\left[1^y = 1\right] \qquad (\textit{one exp})$$

$$(\forall\ \textit{integer}\ x,\ y,\ z)\left[x^{y+z} = (x^y)\cdot(x^z)\right] \qquad (\textit{exp plus})$$

$$(\forall\ \textit{integer}\ x,\ y,\ z)\left[x^{y\cdot z} = (x^y)^z\right] \qquad (\textit{exp times})$$

The proofs of these properties are left as an exercise (**Problem 8.3**).

THE NEED FOR GENERALIZATION

In proving a property by mathematical induction, it is frequently necessary to prove a stronger, more general property instead. This phenomenon is illustrated in the proof of the following proposition.

Proposition (alternative exponentiation)

Suppose we define a new ternary function, denoted by *exp*3, by the following two axioms:

$$\boxed{\begin{array}{ll} (\forall\ \textit{integer}\ x,\ z)\big[exp3(x,\ 0,\ z)\ =\ z\big] & (\textit{zero}) \\[2ex] (\forall\ \textit{integer}\ x,\ y,\ z)\big[exp3(x,\ y+1,\ z)\ =\ exp3(x,\ y,\ x\cdot z)\big] & (\textit{successor}) \end{array}}$$

Then the sentence

$$(\forall\ \textit{integer}\ x,\ y)\big[exp3(x,\ y,\ 1)\ =\ x^y\big] \qquad (\textit{special exp3})$$

is valid. ∎

Before we prove the proposition, let us explain the $exp3$ function. For any nonnegative integers x, y, and z, the function is defined in such a way that

$$exp3(x,\ y,\ z)\ =\ x^y \cdot z.$$

Following the axioms, to compute $exp3(x,\ y,\ z)$ we multiply z by x precisely y times.

Example (computation of exp3). We have

$$\begin{aligned} exp3(3,\ 2,\ 4)\ &=\ exp3\big(3,\ (0+1)+1,\ 4\big) \\ &\qquad \text{(because 2 is an abbreviation for } (0+1)+1) \\ &=\ exp3(3,\ 0+1,\ 3\cdot 4) \\ &\qquad \text{(by the } \textit{successor} \text{ axiom for } exp3) \\ &=\ exp3(3,\ 0,\ 3\cdot 3\cdot 4) \\ &\qquad \text{(by the } \textit{successor} \text{ axiom for } exp3 \text{ again)} \\ &=\ 3\cdot 3\cdot 4 \\ &\qquad \text{(by the } \textit{zero} \text{ axiom for } exp3). \end{aligned}$$

In other words

$$exp3(3,\ 2,\ 4)\ =\ 3\cdot 3\cdot 4\ =\ 3^2\cdot 4.$$ ∎

The proposition suggests that we can use the axioms for $exp3(x,\ y,\ z)$ as an alternative method for computing x^y, simply by taking z to be 1 and computing $exp3(x,\ y,\ 1)$.

Let us prove the proposition.

Proof (alternative exponentiation). Rather than proving the original *special exp3* property,

$$(\forall\ \textit{integer}\ x,\ y)\big[exp3(x,\ y,\ 1)\ =\ x^y\big],$$

we prove instead the stronger, more general property

$$(\forall\ \textit{integer}\ x,\ y,\ z)\big[exp3(x,\ y,\ z)\ =\ x^y\cdot z\big] \qquad (\textit{general exp3})$$

which fully characterizes the $exp3$ function.

Once we have proved the *general exp3* property, we can infer the desired *special exp3* property easily. For consider arbitrary nonnegative integers x and y; we have

$$exp3(x,\ y,\ 1) \ = \ x^y \cdot 1$$
(by the more general sentence)

$$= \ x^y$$
(by the *right-one* property of multiplication).

To prove the *general exp3* property, consider an arbitrary nonnegative integer x; we would like to show

$$(\forall\ integer\ y, z)\big[exp3(x,\ y,\ z) \ = \ x^y \cdot z\big].$$

The proof is by induction on y, taking the inductive sentence to be

$$\mathcal{F}[y]: \quad (\forall\ integer\ z)\big[exp3(x,\ y,\ z) \ = \ x^y \cdot z\big].$$

Base Case

We would like to prove

$$\mathcal{F}[0]: \quad (\forall\ integer\ z)\big[exp3(x,\ 0,\ z) \ = \ x^0 \cdot z\big].$$

For an arbitrary nonnegative integer z, we have

$$exp3(x,\ 0,\ z) \ = \ z$$
(by the *zero* axiom for $exp3$).

But on the other hand, we have

$$x^0 \cdot z \ = \ 1 \cdot z$$
(by the *exp-zero* axiom for exponentiation)

$$= \ z$$
(by the *left-one* property of multiplication).

Inductive Step

For an arbitrary nonnegative integer y, we assume the induction hypothesis

$$\mathcal{F}[y]: \quad (\forall\ integer\ z)\big[exp3(x,\ y,\ z) \ = \ x^y \cdot z\big]$$

and attempt to show the desired conclusion

$$\mathcal{F}[y+1]: \quad (\forall\ integer\ z')\big[exp3(x,\ y+1,\ z') \ = \ (x^{y+1}) \cdot z'\big].$$

(Here we have renamed the bound variable z of the desired conclusion to z', to avoid confusion with the variable z in the induction hypothesis.)

For an arbitrary nonnegative integer z', we have

$$exp3(x,\ y+1,\ z') \ = \ exp3(x,\ y,\ x \cdot z')$$
(by the *successor* axiom for $exp3$).

But on the other hand, we have

$$(x^{y+1}) \cdot z' \ = \ (x^y \cdot x) \cdot z'$$
(by the *successor* axiom for exponentiation)

$$= x^y \cdot (x \cdot z')$$
(by the *associativity* property of multiplication)

$$= exp3(x,\ y,\ x \cdot z')$$
(by the induction hypothesis, taking z to be $x \cdot z'$).

In short, we have established that

$$exp3(x,\ y+1,\ z') \ = \ (x^{y+1}) \cdot z',$$

as we wanted to show. ▟

The proof of the above proposition illustrates some of the strategic aspects of discovering a proof by induction.

Remark (generalization). We proved the original *special exp3* property

$$(\forall \textit{ integer } x,\ y)\big[exp3(x,\ y,\ 1) \ = \ x^y\big]$$

by establishing the *general exp3* property

$$(\forall \textit{ integer } x,\ y,\ z)\big[exp3(x,\ y,\ z) \ = \ x^y \cdot z\big].$$

Had we attempted to prove the *special exp3* property without first generalizing, the above proof would not have worked. It would be difficult to establish the original property directly, because in establishing the inductive step in the proof, we would assume the induction hypothesis,

$$\mathcal{F}'[y]: \quad exp3(x,\ y,\ 1) \ = \ x^y,$$

and attempt to prove the desired conclusion,

$$\mathcal{F}'[y+1]: \quad exp3(x,\ y+1,\ 1) \ = \ x^{y+1}.$$

It suffices to show (by the *successor* axioms for $exp3$ and exponentiation) that

$$exp3(x,\ y,\ x \cdot 1) \ = \ x^y \cdot x.$$

The desired conclusion is concerned with $exp3(x,\ y,\ x \cdot 1)$, that is, $exp3(x,\ y,\ x)$, while the induction hypothesis gives us information only about $exp3(x,\ y,\ 1)$.

Thus in attempting to prove the original weaker property, we have a correspondingly weaker induction hypothesis, one that is no longer strong enough to prove the desired conclusion. By proving the more general property, we have the advantage of the correspondingly more general induction hypothesis. For the *alternative-exponentiation* proposition, it is paradoxically easier to prove the more general, stronger property than it is to prove the weaker special case.

In proving a property by induction, it often requires ingenuity to discover a generalization that enables the proof to go through. Sometimes an unsuccessful attempt to prove the original property will suggest an appropriate generalization. ▟

Generalization is also required to solve **Problem 8.4**, which is concerned with the *factorial* function $x!$.

Remark (treatment of quantifiers). In proving the property

$$(\forall\ \textit{integer}\ x,\ y,\ z)\big[exp3(x,\ y,\ z)\ =\ x^y \cdot z\big],$$

we treated each of the quantifiers differently:

- To dispose of the quantifier ($\forall$ *integer* x), we considered an arbitrary nonnegative integer at the beginning of the proof.
- To dispose of ($\forall$ *integer* y), we performed induction on y.
- To dispose of ($\forall$ *integer* z), we allowed the quantifier to remain in the inductive sentence $\mathcal{F}[y]$ and considered arbitrary nonnegative integers z both in the base case and in the inductive step.

The success of a proof may depend on how we treat quantifiers. To see this, the reader may attempt to prove the property differently, e.g., by induction on x, taking the inductive sentence to be

$$(\forall\ \textit{integer}\ y,\ z)\big[exp3(x,\ y,\ z) = x^y \cdot z\big].$$

The proof will be considerably more complex.

Had we originally been given the quantifiers in a different order, say,

$$(\forall\ \textit{integer}\ z,\ x,\ y)\big[exp3(x,\ y,\ z)\ =\ x^y \cdot z\big],$$

we would have needed to reorder them. If we had chosen arbitrary nonnegative integers x and z before performing induction on y, the inductive sentence would have had no quantifiers and both the induction hypothesis and the desired conclusion would contain the same variable z. The step in the above proof in which we took z to be $x \cdot z'$, where z and z' are the bound variables of the induction hypothesis and the desired conclusion, respectively, would have been impossible.

The decision about how to treat each quantifier depends on the form of the axioms and properties we have for our function and predicate symbols. ▟

8.4 PREDECESSOR AND SUBTRACTION

Before we define the predecessor and subtraction functions, let us introduce a useful unary predicate symbol.

POSITIVE

We augment our theory by defining a unary predicate symbol *positive*(x), denoting, under the intended model, the relation that is true for positive integers and false for zero. It is defined by the axiom

$$(\forall x)\begin{bmatrix} positive(x) \\ \equiv \\ integer(x) \;\; and \;\; not\ (x = 0) \end{bmatrix} \qquad (positive)$$

Using this predicate symbol in relativized quantifiers enables us to abbreviate many properties. For example, we can express the *decomposition* property for the nonnegative integers, that is,

$$(\forall\ integer\ x)\begin{bmatrix} if\ \ not\ (x = 0) \\ then\ \ (\exists\ integer\ y)[x = y + 1] \end{bmatrix},$$

as

$$(\forall\ positive\ x)(\exists\ integer\ y)\big[x = y + 1\big].$$

From the *zero* uniqueness axiom, it follows that

$$(\forall\ integer\ x)\big[positive(x + 1)\big] \qquad (sort)$$

PREDECESSOR

Suppose we augment our theory by introducing axioms to define a unary function symbol x^-, denoting, under the intended model, the *predecessor* function over the nonnegative integers, i.e., the function that maps the positive integer d into the integer $d - 1$. The axiom for the predecessor function is

$$(\forall\ integer\ x)\big[(x + 1)^- = x\big] \qquad (predecessor)$$

Remark (the value of 0^-). Note that the above axiom does not specify the value of the term 0^-. Although this term is legal in the language, the axioms do not force it to have any particular value.

For example, we might have many different models for the augmented theory over the nonnegative integers, each assigning a different value to the term 0^-. This vagueness is intentional; we do not care what the value of 0^- is under a model for the augmented theory. ▟

In the augmented theory, we can prove the following properties of the predecessor function:

$$(\forall\ positive\ x)\big[integer(x^-)\big] \qquad (sort)$$

$$(\forall\ positive\ x)\big[x\ =\ x^- + 1\big] \qquad (decomposition)$$

The proof of the *sort* property is omitted; the proof of the *decomposition* property is left as an exercise (**Problem 8.5(a)**). Our earlier *decomposition* property

$$(\forall\ positive\ x)(\exists\ integer\ y)\big[x = y + 1\big]$$

follows immediately from this one by the *existential quantifier-instantiation* proposition.

SUBTRACTION

Suppose we augment our theory further by formulating axioms that define a binary function symbol $x - y$, denoting the *subtraction* (*minus*) function under the intended model for the nonnegative integers.

The axioms for the subtraction function are as follows:

$(\forall \textit{ integer } x)[x - 0 = x]$	(*right zero*)
$(\forall \textit{ integer } x, y)[(x+1) - (y+1) = x - y]$	(*successor*)

Example (computation of minus). To illustrate the axioms, we show the computation of the value of $3 - 2$. We have

$$\begin{aligned} 3 - 2 &= \big(((0+1)+1)+1\big) - \big((0+1)+1\big) \\ &= \big((0+1)+1\big) - (0+1) \\ &\qquad \text{(by the } \textit{successor} \text{ axiom)} \\ &= (0+1) - 0 \\ &\qquad \text{(by the } \textit{successor} \text{ axiom again)} \\ &= 0 + 1 \\ &\qquad \text{(by the } \textit{right-zero} \text{ axiom)} \\ &= 1. \end{aligned}$$

In short,

$$3 - 2 = 1.$$ ▟

Remark (unspecified values). Note that these axioms do not specify the value of terms of the form $s - t$, where the value of s is less than the value of t. Although such terms are legal in the language, the axioms do not force them to have any particular value.

For example, we might have many different models for the extended theory, each assigning a different domain element to the term $2 - 3$, that is,

$$\big((0+1)+1\big) - \big(((0+1)+1)+1\big).$$

However, according to the *successor* axiom, the value assigned to the term

$$\big((0+1)+1\big) - \big(((0+1)+1)+1\big)$$

must be the same as the value assigned to

$$(0+1) - \big((0+1)+1\big),$$

whatever that is. ▟

In the augmented theory, we can prove the following properties of subtraction:

$$(\forall \textit{ positive } x)[x - 1 \;=\; x^-] \qquad (\textit{right one})$$

$$(\forall \textit{ integer } x,\, y)\big[(x + y) - y \;=\; x\big] \qquad (\textit{addition})$$

The proofs of these properties, and an additional one, are left as an exercise (**Problem 8.5(b)-(d)**).

Note that in the *right-one* property the function symbol $-$ in $x - 1$ denotes the binary subtraction function, while the function symbol $^-$ in the term x^- denotes the unary predecessor function. Once we have established this property, we may use the more conventional notation $t - 1$, in place of t^-, to denote the predecessor of t, if we know that t is positive.

Problem 8.6 introduces a new axiom for the subtraction function.

DECOMPOSITION INDUCTION

Using the definition of the predecessor function, we can prove an alternative version of the *induction* principle.

Proposition (decomposition induction)

For each sentence $\mathcal{F}[x]$, the universal closure of the sentence

$$\textit{if} \begin{bmatrix} \mathcal{F}[0] \\ \quad \textit{and} \\ (\forall \textit{ positive } x) \begin{bmatrix} \textit{if } \mathcal{F}[x-1] \\ \textit{then } \mathcal{F}[x] \end{bmatrix} \end{bmatrix}$$

$$\textit{then } (\forall \textit{ integer } x)\mathcal{F}[x] \qquad (\textit{decomposition induction})$$

is valid. ▟

The decomposition version of the *induction* principle may be paraphrased informally as follows:

> To show that a sentence $\mathcal{F}[x]$ is true for every nonnegative integer x (under a given interpretation), it suffices to show the base case
>
> $\mathcal{F}[0]$ is true
>
> and the inductive step
>
> for an arbitrary positive integer x,
> if $\mathcal{F}[x-1]$ is true
> then $\mathcal{F}[x]$ is also true.

The only difference between the decomposition version of the *induction* principle and the original version is that in the decomposition version we infer $\mathcal{F}[x]$

from $\mathcal{F}[x-1]$, where x is positive, while in the original version we infer $\mathcal{F}[x+1]$ from $\mathcal{F}[x]$, where x is nonnegative.

The proof of the *decomposition-induction* proposition is requested in **Problem 8.15**. (This problem, like Problem 8.13 and 8.14, is placed at the end because of its theoretical nature.)

Because the *decomposition induction* principle is valid in the theory of the nonnegative integers, we can use either the original or the decomposition version of the *induction* principle in establishing the validity of a sentence in the theory. Which version is more convenient to use in a proof depends on how we choose to formulate our axioms and properties. If these tend to refer to the successor $x+1$, the original version will be more convenient; if they refer to the predecessor $x-1$, the decomposition version will be more convenient. In this book we typically use the successor function; therefore the original version is usually easier to use.

8.5 THE LESS-THAN RELATION

In this section, we introduce two versions of the less-than relation, which turn out to be weak and strict partial relations, respectively.

THE WEAK LESS-THAN RELATION

Suppose we augment our theory further by formulating two axioms that define a binary predicate symbol $x \leq y$, denoting the *weak less-than relation* under the intended model for the nonnegative integers.

The axioms for the weak less-than relation are as follows:

$$(\forall \textit{ integer } x) \begin{bmatrix} x \leq 0 \\ \equiv \\ x = 0 \end{bmatrix} \qquad (\textit{right zero})$$

$$(\forall \textit{ integer } x, y) \begin{bmatrix} x \leq y+1 \\ \equiv \\ x = y+1 \;\; \textit{or} \;\; x \leq y \end{bmatrix} \qquad (\textit{right successor})$$

Example (computation of $\leq$). Let us use the axioms to compute the truth-value of $0 \leq 1$, that is, $0 \leq 0+1$. We have

$$0 \leq 0+1$$

if and only if (by the *right-successor* axiom)

$$0 = 0 + 1 \quad or \quad 0 \leq 0$$

if and only if (because, by the *zero* uniqueness axiom, *not* $(0 = 0 + 1)$)

$$0 \leq 0$$

if and only if (by the *right-zero* axiom)

$$0 = 0,$$

which is true. ∎

In **Problem 8.7**, we request the reader to prove the following basic property of the weak less-than relation:

$$(\forall \textit{ integer } x, y) \begin{bmatrix} x \leq y \\ \equiv \\ (\exists \textit{ integer } z)[x + z = y] \end{bmatrix} \qquad (\textit{left addition})$$

The weak less-than relation we have defined can be shown to be a weak partial ordering; in other words, we can establish the validity in the theory of the nonnegative integers of the three weak partial-ordering axioms for $\leq$:

$$(\forall \textit{ integer } x, y, z) \begin{bmatrix} \textit{if } x \leq y \textit{ and } y \leq z \\ \textit{then } x \leq z \end{bmatrix} \qquad (\textit{transitivity})$$

$$(\forall \textit{ integer } x, y) \begin{bmatrix} \textit{if } x \leq y \textit{ and } y \leq x \\ \textit{then } x = y \end{bmatrix} \qquad (\textit{antisymmetry})$$

$$(\forall \textit{ integer } x)[x \leq x] \qquad (\textit{reflexivity})$$

We can also establish the following properties of the weak less-than relation:

$$(\forall \textit{ integer } x)[0 \leq x] \qquad (\textit{left zero})$$

$$(\forall \textit{ integer } x, y)[x \leq x + y] \qquad (\textit{right addition})$$

$$(\forall \textit{ integer } x, y)[x \leq y \textit{ or } y \leq x] \qquad (\textit{totality})$$

The predicate symbol $\geq$ denotes the *weak greater-than relation*, which is the inverse of the weak less-than relation $\leq$. It is defined by the following axiom:

$$\boxed{(\forall \textit{ integer } x, y)[x \geq y \equiv y \leq x] \qquad (\textit{weak greater-than})}$$

EXPRESSING PROPERTIES OF FUNCTIONS

We can now express the properties of several other functions in terms of the weak less-than relation. For the subtraction function, we can establish the following

properties:

$$(\forall\ integer\ x,\ y)\begin{bmatrix} if\ \ x \le y \\ then\ \ integer(y-x) \end{bmatrix} \qquad (sort)$$

$$(\forall\ integer\ x,\ y)\begin{bmatrix} if\ \ x \le y \\ then\ \ x+(y-x)\ =\ y \end{bmatrix} \qquad (decomposition)$$

$$(\forall\ integer\ x,\ y,\ z)\begin{bmatrix} if\ \ x \le y \\ then\ \begin{bmatrix} x+z=y \\ \equiv \\ z=y-x \end{bmatrix} \end{bmatrix} \qquad (cancellation)$$

We can augment our theory further by introducing two binary function symbols $max(x, y)$ and $min(x, y)$, denoting the *maximum* and *minimum*, respectively, of the nonnegative integers x and y. The axioms that define these functions are as follows:

$$(\forall\ integer\ x,\ y)\left[max(x,\ y) = \begin{Bmatrix} if\ \ x \le y \\ then\ \ y \\ else\ \ x \end{Bmatrix}\right] \qquad (maximum)$$

$$(\forall\ integer\ x,\ y)\left[min(x,\ y) = \begin{Bmatrix} if\ \ x \le y \\ then\ \ x \\ else\ \ y \end{Bmatrix}\right] \qquad (minimum)$$

From these axioms we can establish the following properties of the maximum and minimum functions:

$$(\forall\ integer\ x,\ y)\begin{bmatrix} max(x,\ y) \ge x \\ and \\ max(x,\ y) \ge y \end{bmatrix} \qquad (greater\text{-}than)$$

$$(\forall\ integer\ x,\ y)\begin{bmatrix} min(x,\ y) \le x \\ and \\ min(x,\ y) \le y \end{bmatrix} \qquad (less\text{-}than)$$

$$(\forall\ integer\ x,\ y,\ z)\begin{bmatrix} min\big(x,\ max(y,\ z)\big) \\ = \\ max\big(min(x,\ y),\ min(x,\ z)\big) \end{bmatrix} \qquad (minimax)$$

$$(\forall\ integer\ x,\ y,\ z)\begin{bmatrix} max\big(x,\ min(y,\ z)\big) \\ = \\ min\big(max(x,\ y),\ max(x,\ z)\big) \end{bmatrix} \qquad (maximin)$$

The reader is requested to establish the *greater-than* and *minimax* properties in **Problem 8.8.**

THE STRICT LESS-THAN RELATION

We have already remarked that the weak less-than relation $\leq$ is a weak partial ordering. Let us augment the theory further to define a new binary predicate symbol $<$, denoting the (*strict*) *less-than relation,* by the following axiom:

$$\boxed{(\forall \textit{ integer } x,\, y) \begin{bmatrix} x < y \\ \equiv \\ x \leq y \textit{ and not } (x = y) \end{bmatrix} \qquad (\textit{less-than})}$$

In other words, $<$ denotes the irreflexive restriction of the weak less-than relation $\leq$. Thus we know (by the *irreflexive-restriction* proposition of the theory of the weak partial ordering $\leq$) that $<$ is a strict partial ordering in the augmented theory of the nonnegative integers; i.e., the sentences

$$(\forall \textit{ integer } x,\, y,\, z) \begin{bmatrix} \textit{if } x < y \textit{ and } y < z \\ \textit{then } x < z \end{bmatrix} \qquad (\textit{transitivity})$$

$$(\forall \textit{ integer } x)\big[\textit{not } (x < x)\big] \qquad (\textit{irreflexivity})$$

are valid. Therefore any property we can prove in the theory of the strict partial ordering $<$ is valid in our augmented theory of the nonnegative integers. For example, the *asymmetry* property

$$(\forall \textit{ integer } x,\, y) \begin{bmatrix} \textit{if } x < y \\ \textit{then not } (y < x) \end{bmatrix} \qquad (\textit{asymmetry})$$

is valid.

We have defined the strict less-than predicate symbol $<$ to denote the irreflexive restriction of the weak less-than relation $\leq$. We can also show that the weak less-than predicate symbol $\leq$ denotes the reflexive closure of $<$, that is,

$$(\forall \textit{ integer } x,\, y) \begin{bmatrix} x \leq y \\ \equiv \\ x < y \textit{ or } x = y \end{bmatrix} \qquad (\textit{reflexive closure})$$

The less-than relation $<$ can be shown to be total, that is,

$$(\forall \textit{ integer } x,\, y)\big[x < y \textit{ or } y < x \textit{ or } x = y\big] \qquad (\textit{totality})$$

It follows (because $<$ is asymmetric and $\leq$ is its reflexive closure) that

$$(\forall \textit{ integer } x,\, y) \begin{bmatrix} \textit{not } (x < y) \\ \equiv \\ y \leq x \end{bmatrix} \qquad (\textit{total asymmetry})$$

The predicate symbol $>$, denoting the corresponding (*strict*) *greater-than relation*, is defined by the axiom

$$\boxed{(\forall \textit{ integer } x, y)[x > y \equiv y < x] \qquad (\textit{greater-than})}$$

We can also establish the following properties of the strict less-than relation:

$$(\forall \textit{ integer } x, y)\begin{bmatrix} x < y \\ \equiv \\ (\exists \textit{ positive } z)[x + z = y] \end{bmatrix} \qquad (\textit{left addition})$$

$$(\forall \textit{ positive } x)[0 < x] \qquad (\textit{left zero})$$

$$(\forall \textit{ integer } x)[\textit{not } (x < 0)] \qquad (\textit{right zero})$$

$$(\forall \textit{ integer } x)[x < x + 1] \qquad (\textit{adjacent})$$

$$(\forall \textit{ integer } x)(\forall \textit{ positive } y)[x < x + y] \qquad (\textit{right addition})$$

$$(\forall \textit{ integer } x, y)\begin{bmatrix} x < y + 1 \\ \equiv \\ x \leq y \end{bmatrix} \qquad (\textit{right successor})$$

$$(\forall \textit{ integer } x, y)\begin{bmatrix} x < y \\ \equiv \\ x + 1 \leq y \end{bmatrix} \qquad (\textit{left successor})$$

In **Problem 8.16**, the reader is asked to consider a version of the theory of the nonnegative integers without the induction principle. (Again, this problem is placed at the end of the list because of its theoretical nature.)

8.6 THE COMPLETE INDUCTION PRINCIPLE

Using the less-than relation $<$, we can state and prove an alternative version of the *induction* principle, which is often much more convenient to use.

Proposition (complete induction)

For each sentence $\mathcal{F}[x]$, the universal closure of the sentence

$$\begin{array}{l} \textit{if} \ \ (\forall \textit{ integer } x) \begin{bmatrix} \textit{if} \ \ (\forall \textit{ integer } x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \mathcal{F}[x'] \end{bmatrix} \\ \textit{then} \ \ \mathcal{F}[x] \end{bmatrix} \\ \textit{then} \ \ (\forall \textit{ integer } x)\mathcal{F}[x] \end{array}$$

(*complete induction*)

where x' does not occur free in $\mathcal{F}[x]$, is valid. ▟

As usual, the sentence $\mathcal{F}[x]$ is called the *inductive sentence* and the variable x is called the *inductive variable.* The antecedent of the principle,

$$(\forall \textit{ integer } x) \begin{bmatrix} \textit{if} \ \ (\forall \textit{ integer } x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \mathcal{F}[x'] \end{bmatrix} \\ \textit{then} \ \ \mathcal{F}[x] \end{bmatrix},$$

is called the *inductive step*; the subsentences

$$(\forall \textit{ integer } x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \mathcal{F}[x'] \end{bmatrix} \qquad \text{and} \qquad \mathcal{F}[x]$$

of the inductive step are called the *induction hypothesis* and the *desired conclusion*, respectively.

The *complete induction* principle may be paraphrased informally as follows:

> To show that a sentence $\mathcal{F}[x]$ is true for every nonnegative integer x (under a given interpretation), it suffices to show the inductive step
>
> for an arbitrary nonnegative integer x,
> if $\mathcal{F}[x']$ is true for every nonnegative integer x'
> such that $x' < x$,
> then $\mathcal{F}[x]$ is also true.

In other words, to show that a sentence $\mathcal{F}[x]$ is true for every nonnegative integer x, it suffices to show that, for an arbitrary nonnegative integer x, if

$$\mathcal{F}[0], \quad \mathcal{F}[1], \quad \mathcal{F}[2], \quad \ldots, \quad \text{and} \quad \mathcal{F}[x-1]$$

are all true, then

$$\mathcal{F}[x]$$

is also true.

The reader may have wondered why we include in the *complete induction* principle the constraint that x' does not occur free in $\mathcal{F}[x]$. In fact, if this constraint is violated, the sentence may not be valid.

Counterexample (constraint is essential). In the theory of the nonnegative integers, take

$$\mathcal{F}[x]: \ x < x'.$$

Note that, contrary to the constraint, x' occurs free in $\mathcal{F}[x]$.

The *complete induction* principle in this case is

$$(\forall\ \textit{integer}\ x')\begin{bmatrix}\textit{if}\ \ (\forall\ \textit{integer}\ x)\begin{bmatrix}\textit{if}\ \ (\forall\ \textit{integer}\ x')\begin{bmatrix}\textit{if}\ \ x' < x\\ \textit{then}\ \ x' < x'\end{bmatrix}\\ \textit{then}\ \ x < x'\end{bmatrix}\\ \textit{then}\ \ (\forall\ \textit{integer}\ x)[x < x']\end{bmatrix}.$$

(The outermost quantifier $(\forall\ \textit{integer}\ x')$ was introduced in taking the universal closure.)

The subsentence

$$\begin{aligned}&\textit{if}\ \ x' < x\\ &\textit{then}\ \ x' < x'\end{aligned}$$

is equivalent (by properties of the nonnegative integers and propositional logic) to

$$\textit{not}\ (x' < x).$$

Let us make this replacement in the principle. The resulting subsentence

$$(\forall\ \textit{integer}\ x')\big[\textit{not}\ (x' < x)\big]$$

is equivalent (by properties of the nonnegative integers) to

$$x = 0.$$

Let us make this replacement. The resulting subsentence

$$(\forall\ \textit{integer}\ x)\begin{bmatrix}\textit{if}\ \ x = 0\\ \textit{then}\ \ x < x'\end{bmatrix}$$

is equivalent (by predicate logic) to

$$0 < x'.$$

Let us make this replacement. The resulting sentence is

$$(\forall\ \textit{integer}\ x')\begin{bmatrix}\textit{if}\ \ 0 < x'\\ \textit{then}\ \ (\forall\ \textit{integer}\ x)[x < x']\end{bmatrix}.$$

If we take x' to be 1 and x to be 2, we have

$$\begin{aligned}&\textit{if}\ \ 0 < 1\\ &\textit{then}\ \ 2 < 1,\end{aligned}$$

which is false. ∎

To distinguish between the induction principles, we refer to the earlier induction, including *decomposition induction*, as *stepwise induction*.

Let us postpone the proof of the *complete induction* principle until we have had a chance to illustrate its application.

8.7 QUOTIENT AND REMAINDER

Suppose we augment our theory by defining two binary function symbols, $quot(x, y)$ and $rem(x, y)$. Under the intended model for the nonnegative integers, these symbols denote the *quotient* and *remainder*, respectively, of dividing a nonnegative integer x by a positive integer y. The axioms for the quotient of dividing x by y are

$$\begin{array}{ll} \begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\begin{bmatrix} if\ \ x < y \\ then\ \ quot(x,\ y) = 0 \end{bmatrix} & (less\text{-}than) \\[2ex] \begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\big[quot(x + y,\ y)\ =\ quot(x,\ y) + 1\big] & (addition) \end{array}$$

The axioms for the remainder of dividing x by y are

$$\begin{array}{ll} \begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\begin{bmatrix} if\ \ x < y \\ then\ \ rem(x,\ y) = x \end{bmatrix} & (less\text{-}than) \\[2ex] \begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\big[rem(x + y,\ y)\ =\ rem(x,\ y)\big] & (addition) \end{array}$$

Note that the axioms for the quotient and remainder do not specify the values of terms of form $quot(s,\ 0)$ or $rem(s,\ 0)$, although such terms are legal in the language.

From these axioms, we can establish the usual *sort* properties for the quotient function,

$$\begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\big[integer\big(quot(x,\ y)\big)\big] \qquad (sort)$$

and for the remainder function,

$$\begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\big[integer\big(rem(x,\ y)\big)\big] \qquad (sort)$$

The reader is requested to prove these properties in **Problem 8.9(a)(b).**

The following proposition expresses a relationship between the quotient and remainder functions.

Proposition (quotient-remainder)

The sentence

$$\begin{matrix}(\forall\ \textit{integer}\ x)\\(\forall\ \textit{positive}\ y)\end{matrix}\begin{bmatrix}x\ =\ y\cdot quot(x,\ y)+rem(x,\ y)\\ \quad and\\ rem(x,\ y)<y\end{bmatrix}\qquad (\textit{quotient-remainder})$$

is valid. ∎

The proof illustrates the use of the *complete induction* principle.

Proof. We actually prove the equivalent sentence

$$\begin{matrix}(\forall\ \textit{positive}\ y)\\(\forall\ \textit{integer}\ x)\end{matrix}\begin{bmatrix}x\ =\ y\cdot quot(x,\ y)+rem(x,\ y)\\ \quad and\\ rem(x,\ y)<y\end{bmatrix}$$

(obtained by reversing the quantifiers).

Consider an arbitrary positive integer y. We would like to show that

$$(\forall\ \textit{integer}\ x)\begin{bmatrix}x\ =\ y\cdot quot(x,\ y)+rem(x,\ y)\\ \quad and\\ rem(x,\ y)<y\end{bmatrix}.$$

The proof is by complete induction on x; we take the inductive sentence to be

$$\mathcal{F}[x]:\quad \begin{matrix}x\ =\ y\cdot quot(x,\ y)+rem(x,\ y)\\ \quad and\\ rem(x,\ y)<y.\end{matrix}$$

To prove $(\forall\ \textit{integer}\ x)\mathcal{F}[x]$, it suffices to establish the inductive step.

Inductive Step

We would like to show

$$(\forall\ \textit{integer}\ x)\begin{bmatrix}\textit{if}\ \ (\forall\ \textit{integer}\ x')\begin{bmatrix}\textit{if}\ \ x'<x\\ \textit{then}\ \ \mathcal{F}[x']\end{bmatrix}\\ \textit{then}\ \ \mathcal{F}[x]\end{bmatrix}.$$

For an arbitrary nonnegative integer x, we assume the induction hypothesis

$$(\forall\ \textit{integer}\ x')\begin{bmatrix}\textit{if}\ \ x'<x\\ \textit{then}\ \ \mathcal{F}[x']\end{bmatrix}$$

and attempt to show the desired conclusion

$$\mathcal{F}[x],$$

that is,

$$\begin{matrix}x\ =\ y\cdot quot(x,\ y)+rem(x,\ y)\\ \quad and\\ rem(x,\ y)<y.\end{matrix}$$

Following the way the quotient and remainder are defined, we distinguish between two subcases, depending on whether or not $x<y$.

Case: $x < y$

Then (by the *less-than* axioms for the quotient and remainder, because y is positive) we have

$$quot(x,\ y) = 0 \quad and \quad rem(x,\ y) = x.$$

The desired conclusion $\mathcal{F}[x]$ then reduces to

$$\begin{aligned} x &= y \cdot 0 + x \\ &\quad and \\ x &< y. \end{aligned}$$

The first conjunct follows from the *right-zero* axiom for multiplication and the *left-zero* property of addition; the second conjunct is the assumption for this subcase.

Case: *not* $(x < y)$

Then (by the *total-asymmetry* property of the less-than relation $<$)

$$y \leq x$$

and hence (by the *decomposition* property of the weak less-than relation $\leq$)

$$y + (x - y) \;=\; x,$$

that is (by the *commutativity* property of addition),

$$x \;=\; (x - y) + y.$$

Hence (by the *addition* axioms for the quotient and remainder, because y is positive) we have

$$quot(x,\ y) \;=\; quot\big((x - y) + y,\ y\big) \;=\; quot(x - y,\ y) + 1$$

and

$$rem(x,\ y) \;=\; rem\big((x - y) + y,\ y\big) \;=\; rem(x - y,\ y).$$

We would like to show $\mathcal{F}[x]$, that is,

$$\begin{aligned} x &= y \cdot quot(x,\ y) + rem(x,\ y) \\ &\quad and \\ rem(x,\ y) &< y, \end{aligned}$$

which expands (in this case) to

$$\begin{aligned} x &= y \cdot \big(quot(x - y,\ y) + 1\big) + rem(x - y,\ y) \\ &\quad and \\ rem(x - y,\ y) &< y. \end{aligned}$$

This can be transformed (by the *right-successor* axiom for multiplication) into

$$\begin{aligned} x &= \big(y \cdot quot(x - y,\ y) + y\big) + rem(x - y,\ y) \\ &\quad and \\ rem(x - y,\ y) &< y. \end{aligned}$$

This can be transformed further (by the *commutativity* and *associativity* properties of addition) into

$$\begin{aligned} x &= \big(y \cdot quot(x-y,\ y) + rem(x-y,\ y)\big) \dot{+} y \\ &\quad and \\ &rem(x-y,\ y) < y. \end{aligned}$$

Therefore (by the *cancellation* property of subtraction, because, in this case, $y \leq x$) it suffices to establish

$$\begin{aligned} x - y &= y \cdot quot(x-y,\ y) + rem(x-y,\ y) \\ &\quad and \\ &rem(x-y,\ y) < y, \end{aligned}$$

which is precisely $\mathcal{F}[x-y]$.

We have assumed as our induction hypothesis that

$$(\forall\ integer\ x') \begin{bmatrix} if\ \ x' < x \\ then\ \ \mathcal{F}[x'] \end{bmatrix}.$$

In particular, taking x' to be $x - y$, we have

$$\begin{aligned} &if\ \ x - y < x \\ &then\ \ \mathcal{F}[x-y]. \end{aligned}$$

Because $(x - y) + y = x$ and y is positive, it follows (by the *left-addition* property of the less-than relation $<$) that

$$x - y < x,$$

and thus we have the desired result $\mathcal{F}[x-y]$.

Because we have completed the proof of the inductive step, we have established the *quotient-remainder* proposition. ∎

Remark (why not stepwise induction?). Note that the above proposition would be awkward to prove by stepwise induction rather than complete induction. In the inductive step we showed that, to prove our desired conclusion $\mathcal{F}[x]$, it suffices (in the case in which *not* $(x < y)$) to establish the condition

$$\mathcal{F}[x-y].$$

This turned out to be implied by our induction hypothesis

$$(\forall\ integer\ x') \begin{bmatrix} if\ \ x' < x \\ then\ \ \mathcal{F}[x'] \end{bmatrix},$$

taking x' to be $x - y$, since in this case $x - y < x$.

Had we attempted the proof by the (*decomposition* version of) stepwise induction, our induction hypothesis would have been simply

$$\mathcal{F}[x-1].$$

This does not necessarily imply $\mathcal{F}[x-y]$, because we do not know that $y = 1$. The induction hypothesis of the complete-induction proof tells us not only $\mathcal{F}[x-1]$ but the entire conjunction of

$$\mathcal{F}[0], \quad \mathcal{F}[1], \quad \ldots, \quad \mathcal{F}[x-2], \quad \text{and} \quad \mathcal{F}[x-1].$$

(A similar obstacle would have been encountered had we attempted the proof by the original version of stepwise induction.) ▟

Remark (where is the base case?). The reader may be puzzled to note that, although the earlier *stepwise induction* principle requires us to prove a base case and an inductive step, the *complete induction* principle requires only an inductive step. At first glance, it may seem as if we are getting something for nothing in using complete induction.

This appearance is misleading: In proving the inductive step for complete induction,

$$(\forall \textit{ integer } x) \begin{bmatrix} \textit{if } (\forall \textit{ integer } x') \begin{bmatrix} \textit{if } x' < x \\ \textit{then } \mathcal{F}[x'] \end{bmatrix} \\ \textit{then } \mathcal{F}[x] \end{bmatrix},$$

we must actually consider the possibility that the arbitrary nonnegative integer x is 0. In this case our induction hypothesis is

$$(\forall \textit{ integer } x') \begin{bmatrix} \textit{if } x' < 0 \\ \textit{then } \mathcal{F}[x'] \end{bmatrix}.$$

Because (by the *right-zero* property for the less-than relation $<$) there are no nonnegative integers x' such that $x' < 0$, we can never make use of the induction hypothesis in this case. Therefore we must prove the desired conclusion $\mathcal{F}[x]$, that is, $\mathcal{F}[0]$, without the help of the induction hypothesis, just as in the base case of a stepwise induction proof.

In the *quotient-remainder* proposition above, for instance, we treated separately the case in which $x < y$. Because we have taken y to be positive, this case includes the possibility that $x = 0$. The case was handled without appealing to the induction hypothesis. ▟

The proposition we have just established states that, for any nonnegative integer x and positive integer y, the quotient $quot(x, y)$ and the remainder $rem(x, y)$ exhibit the *quotient-remainder* relationship

$$\begin{aligned} x &= y \cdot quot(x, y) + rem(x, y) \\ &\textit{ and} \\ rem(x, y) &< y. \end{aligned}$$

It can actually be shown that $quot(x, y)$ and $rem(x, y)$ are unique, in the sense that, for all nonnegative integers u and v satisfying the *quotient-remainder* rela-

tionship

$$\begin{aligned} x &= y \cdot u + v \\ &\textit{and} \\ v &< y, \end{aligned}$$

we have

$$u = quot(x,\ y) \quad \textit{and} \quad v = rem(x,\ y).$$

The proof is requested in **Problem 8.9(c)**.

Remark (program correctness). The axioms for the quotient and remainder functions suggest a method for computing these functions. In other words, these axioms have computational content; we may regard them as a program for computing the quotient and remainder.

It is not immediately obvious that the functions defined by these axioms are actually the quotient and remainder functions we expect. We might have made an error in the axioms and thus defined some other functions.

The *quotient-remainder* property is a description of the intended behavior of the quotient and remainder functions. In this sense, it may be regarded as a specification for the program that computes these functions. In proving the property, we establish the correctness of the program at least with respect to this specification. In other words, we can be more confident that the program computes the functions we expect. ▟

8.8 PROOF OF COMPLETE INDUCTION

We are now ready to give the proof of the *complete induction* principle.

Proof (complete induction). For an arbitrary sentence $\mathcal{F}[x]$, suppose that

$$(*) \qquad (\forall\ \textit{integer}\ x) \begin{bmatrix} \textit{if}\ \ (\forall\ \textit{integer}\ x') \begin{bmatrix} \textit{if}\ \ x' < x \\ \textit{then}\ \ \mathcal{F}[x'] \end{bmatrix} \\ \textit{then}\ \ \mathcal{F}[x] \end{bmatrix}$$

is true, where x' is not free in $\mathcal{F}[x]$; we would like to show that then

$$(\dagger) \qquad (\forall\ \textit{integer}\ x)\mathcal{F}[x]$$

is true.

We actually prove an alternative property

$$(\ddagger) \qquad (\forall\ \textit{integer}\ y)\mathcal{F}'[y],$$

where $\mathcal{F}'[y]$ is

$$\mathcal{F}'[y]: \quad (\forall\ \textit{integer}\ x') \begin{bmatrix} \textit{if}\ \ x' < y \\ \textit{then}\ \ \mathcal{F}[x'] \end{bmatrix}$$

and y is a new variable. Intuitively speaking, $\mathcal{F}'[y]$ is the conjunction of

$$\mathcal{F}[0], \quad \mathcal{F}[1], \quad \mathcal{F}[2], \quad \ldots, \quad \text{and} \quad \mathcal{F}[y-1].$$

Proof that $(\ddagger) \Rightarrow (\dagger)$

To show that the alternative property $(\ddagger)$, that is, $(\forall\ \textit{integer}\ y)\mathcal{F}'[y]$, implies the original property $(\dagger)$, that is, $(\forall\ \textit{integer}\ x)\mathcal{F}[x]$, suppose that

$$(\forall\ \textit{integer}\ y)\mathcal{F}'[y],$$

and consider an arbitrary nonnegative integer x; we attempt to show that

$$\mathcal{F}[x]$$

is true.

From the supposition (taking y to be $x+1$) we have $\mathcal{F}'[x+1]$, that is,

$$(\forall\ \textit{integer}\ x') \begin{bmatrix} \textit{if}\ \ x' < x+1 \\ \textit{then}\ \ \mathcal{F}[x'] \end{bmatrix}.$$

In particular, taking x' to be x, we have (because x' is not free in $\mathcal{F}[x]$)

$$\begin{array}{l} \textit{if}\ \ x < x+1 \\ \textit{then}\ \ \mathcal{F}[x]. \end{array}$$

By the *adjacent* property of the less-than relation $<$, we know $x < x+1$. Therefore we conclude

$$\mathcal{F}[x],$$

as we wanted to show.

Proof that $(*) \Rightarrow (\ddagger)$

The proof of $(\ddagger)$,

$$(\forall\ \textit{integer}\ y)\mathcal{F}'[y],$$

is by the *stepwise induction* principle; we take the inductive sentence to be $\mathcal{F}'[y]$.

Base Case

We would like to show $\mathcal{F}'[0]$, that is,

$$(\forall\ \textit{integer}\ x') \begin{bmatrix} \textit{if}\ \ x' < 0 \\ \textit{then}\ \ \mathcal{F}[x'] \end{bmatrix}.$$

But, for an arbitrary nonnegative integer x', we have (by the *right-zero* property of the less-than relation $<$)

$$\textit{not}\ (x' < 0).$$

Therefore the entire implication is true.

Inductive Step

For an arbitrary nonnegative integer y, we assume the induction hypothesis (for the *stepwise induction* principle)

$$\mathcal{F}'[y]: \quad (\forall \textit{ integer } x') \begin{bmatrix} \textit{if } \ x' < y \\ \textit{then } \ \mathcal{F}[x'] \end{bmatrix}$$

and establish the desired conclusion (for the *stepwise induction* principle)

$$\mathcal{F}'[y+1]: \quad (\forall \textit{ integer } x') \begin{bmatrix} \textit{if } \ x' < y+1 \\ \textit{then } \ \mathcal{F}[x'] \end{bmatrix}.$$

Consider an arbitrary nonnegative integer x' such that

$$x' < y + 1;$$

we would like to show that

$$\mathcal{F}[x'].$$

Since $x' < y+1$, we have (by the *right-successor* property of the less-than relation $<$) that $x' \leq y$ or, equivalently (because $\leq$ is the reflexive closure of $<$),

$$x' < y \ \textit{ or } \ x' = y.$$

We treat each subcase separately.

Case: $x' < y$

By our induction hypothesis $\mathcal{F}'[y]$, we have

$$\begin{aligned} &\textit{if } \ x' < y \\ &\textit{then } \ \mathcal{F}[x']. \end{aligned}$$

Therefore, because (in this case) $x' < y$, we obtain the desired result

$$\mathcal{F}[x'].$$

Case: $x' = y$

In this case we would like to show $\mathcal{F}[y]$. From our initial supposition $(*)$ (taking x to be y) we have

$$\begin{aligned} &\textit{if } \ (\forall \textit{ integer } x') \begin{bmatrix} \textit{if } \ x' < y \\ \textit{then } \ \mathcal{F}[x'] \end{bmatrix} \\ &\textit{then } \ \mathcal{F}[y]. \end{aligned}$$

Therefore it suffices to show

$$(\forall \textit{ integer } x') \begin{bmatrix} \textit{if } \ x' < y \\ \textit{then } \ \mathcal{F}[x'] \end{bmatrix};$$

but this is precisely our induction hypothesis $\mathcal{F}'[y]$.

Because we have completed the base case and the inductive step of the stepwise induction proof, we have established the validity of the *complete induction* principle. ∎

As the proof of the above proposition illustrates, any sentence we can prove by complete induction we can also prove by stepwise induction, but the stepwise-induction proof may require a more complex inductive sentence.

In **Problem 8.10**, the reader is requested to prove the *quotient-remainder* proposition by stepwise induction, without using complete induction.

Some further applications of the *complete induction* principle are illustrated in the next section.

8.9 THE DIVIDES RELATION

In this section we introduce a new relation over the nonnegative integers and further illustrate the usefulness of the *complete induction* principle.

DIVIDES

Suppose we augment our theory by defining a new predicate symbol $x \preceq_{div} y$, denoting the *divides* relation, which holds when x divides y with no remainder. (The conventional symbol for this relation is $x|y$.)

The axiom for the divides relation is

$$\boxed{(\forall\ \textit{integer}\ x,\ y)\begin{bmatrix} x \preceq_{div} y \\ \equiv \\ (\exists\ \textit{integer}\ z)\big[x \cdot z = y\big] \end{bmatrix} \qquad (\textit{divides})}$$

Thus,

$$1 \preceq_{div} 6 \qquad 2 \preceq_{div} 6 \qquad 3 \preceq_{div} 6 \qquad 6 \preceq_{div} 6 \qquad 6 \preceq_{div} 0,$$

but not $0 \preceq_{div} 6$.

From this axiom we can establish the validity of the following properties of the divides relation:

$$(\forall\ \textit{integer}\ x)\big[x \preceq_{div} 0\big] \qquad (\textit{right zero})$$

$$(\forall\ \textit{positive}\ y)\big[\textit{not}\ (0 \preceq_{div} y)\big] \qquad (\textit{left zero})$$

$$(\forall\ \textit{integer}\ x,\ y,\ z)\begin{bmatrix} x \preceq_{div} y\ \ \textit{and}\ \ x \preceq_{div} z \\ \equiv \\ x \preceq_{div} y\ \ \textit{and}\ \ x \preceq_{div} (y+z) \end{bmatrix} \qquad (\textit{addition})$$

$$(\forall\ \textit{integer}\ x,\ y,\ z)\begin{bmatrix}\textit{if}\ \ x \preceq_{div} y\ \ \textit{or}\ \ x \preceq_{div} z \\ \textit{then}\ \ x \preceq_{div} (y \cdot z)\end{bmatrix} \qquad (\textit{multiplication})$$

$$\begin{matrix}(\forall\ \textit{positive}\ x) \\ (\forall\ \textit{integer}\ y)\end{matrix}\begin{bmatrix}x \preceq_{div} y \\ \equiv \\ rem(y,\ x) = 0\end{bmatrix} \qquad (\textit{remainder})$$

We can also show that the divides relation is a weak partial ordering; in other words, we can establish the validity in the theory of the nonnegative integers of the three weak-partial-ordering axioms for the divides relation, that is,

$$(\forall\ \textit{integer}\ x,\ y,\ z)\begin{bmatrix}\textit{if}\ \ x \preceq_{div} y\ \ \textit{and}\ \ y \preceq_{div} z \\ \textit{then}\ \ x \preceq_{div} z\end{bmatrix} \qquad (\textit{transitivity})$$

$$(\forall\ \textit{integer}\ x,\ y)\begin{bmatrix}\textit{if}\ \ x \preceq_{div} y\ \ \textit{and}\ \ y \preceq_{div} x \\ \textit{then}\ \ x = y\end{bmatrix} \qquad (\textit{antisymmetry})$$

$$(\forall\ \textit{integer}\ x)[x \preceq_{div} x] \qquad (\textit{reflexivity})$$

Note that we cannot establish the *totality* property for the divides relation; that is, the sentence

$$(\forall\ \textit{integer}\ x,\ y)[x \preceq_{div} y\ \ \textit{or}\ \ y \preceq_{div} x]$$

is not valid. For instance, neither $2 \preceq_{div} 3$ nor $3 \preceq_{div} 2$ is true.

Note that the definition of the divides relation does not immediately suggest a method of computing the relation, i.e., of determining whether $s \preceq_{div} t$ for terms s and t denoting particular nonnegative integers. For this purpose it is necessary (according to the definition) to decide whether

$$(\exists\ \textit{integer}\ z)[s \cdot z = t].$$

But since there are infinitely many nonnegative integers z to be tested, this is impossible.

There are other properties of the divides relation that do suggest methods to compute it. For example, we can establish the validity of the following properties:

$$\begin{matrix}(\forall\ \textit{integer}\ x) \\ (\forall\ \textit{positive}\ y)\end{matrix}\begin{bmatrix}\textit{if}\ \ x > y \\ \textit{then}\ \ \textit{not}\ (x \preceq_{div} y)\end{bmatrix} \qquad (\textit{greater-than})$$

$$(\forall\ \textit{integer}\ x,\ y)\begin{bmatrix}\textit{if}\ \ x \leq y \\ \textit{then}\ \begin{bmatrix}x \preceq_{div} y \\ \equiv \\ x \preceq_{div} (y - x)\end{bmatrix}\end{bmatrix} \qquad (\textit{subtraction})$$

These two properties, together with the *right-zero* and *left-zero* properties above, suggest a method for computing the divides relation.

Example (computation of $\preceq_{div}$). Suppose we would like to determine whether 2 divides 4. We have

$$2 \preceq_{div} 4$$

if and only if (by the *subtraction* property, because $2 \leq 4$)

$$2 \preceq_{div} (4 - 2)$$

if and only if

$$2 \preceq_{div} 2$$

if and only if (by the *subtraction* property, because $2 \leq 2$)

$$2 \preceq_{div} (2 - 2)$$

if and only if

$$2 \preceq_{div} 0,$$

which is true (by the *right-zero* property). Note that we could have used the *reflexivity* property to determine that $2 \preceq_{div} 2$ is true, obtaining a shorter computation.

On the other hand, suppose we would like to determine whether 2 divides 3. We have

$$2 \preceq_{div} 3$$

if and only if (by the *subtraction* property, because $2 \leq 3$)

$$2 \preceq_{div} (3 - 2)$$

if and only if

$$2 \preceq_{div} 1,$$

which is false (by the *greater-than* property, because $2 > 1$ and 1 is positive). ■

In **Problem 8.11**, the reader is requested to show the validity of the *right-zero*, *left-zero*, *greater-than*, and *subtraction* properties of the divides relation and to show that these properties in fact constitute an alternative definition for the relation.

The *proper-divides* relation, denoted by $\prec_{div}$, is the irreflexive restriction of $\preceq_{div}$, defined by the axiom

$$\boxed{(\forall \textit{ integer } x, y) \begin{bmatrix} x \prec_{div} y \\ \equiv \\ x \preceq_{div} y \textit{ and not } (x = y) \end{bmatrix} \qquad (\textit{proper divides})}$$

Because we have established that $\preceq_{div}$ is a weak partial ordering, we know immediately (by the *irreflexive-restriction* proposition of the theory of the weak partial ordering $\preceq_{div}$) that its irreflexive restriction $\prec_{div}$ is a strict partial ordering, i.e., it is transitive and irreflexive.

The proper-divides relation $\prec_{div}$ may also be shown to satisfy the following property

$$(\forall \textit{ positive } x,\, y)\begin{bmatrix} x \prec_{div} y \\ \equiv \\ (\exists \textit{ integer } z)\begin{bmatrix} x \cdot z = y \textit{ and} \\ 1 < z \end{bmatrix} \end{bmatrix}. \qquad (\textit{multiplication})$$

GREATEST COMMON DIVISOR

Let us further augment our system by defining a binary function symbol $gcd(x, y)$ intended to denote the *greatest common divisor* of x and y. The axioms for the greatest-common-divisor function are

$$\boxed{\begin{array}{ll} (\forall \textit{ integer } x)\big[gcd(x,\, 0) = x\big] & (\textit{zero}) \\[2ex] \begin{array}{l}(\forall \textit{ integer } x)\\ (\forall \textit{ positive } y)\end{array}\big[gcd(x,\, y) \;=\; gcd\big(y,\, rem(x,\, y)\big)\big] & (\textit{remainder}) \end{array}}$$

We illustrate the use of the axioms to compute the greatest common divisor of two particular nonnegative integers.

Example (computation of gcd). Suppose we would like to determine the greatest common divisor of 6 and 9, assuming we can compute the remainder function *rem*. We have

$$\begin{aligned} gcd(6,\, 9) &= gcd\big(9,\, rem(6, 9)\big) \\ &\qquad \text{(by the } \textit{remainder} \text{ axiom, because 9 is positive)} \\ &= gcd(9,\, 6) \\ &= gcd\big(6,\, rem(9, 6)\big) \\ &\qquad \text{(by the } \textit{remainder} \text{ axiom, because 6 is positive)} \\ &= gcd(6,\, 3) \\ &= gcd\big(3,\, rem(6, 3)\big) \\ &\qquad \text{(by the } \textit{remainder} \text{ axiom, because 3 is positive)} \\ &= gcd(3,\, 0) \\ &= 3 \\ &\qquad \text{(by the } \textit{zero} \text{ axiom).} \end{aligned}$$

In short,

$$gcd(6,\, 9) \;=\; 3. \qquad \blacksquare$$

Remark (consistency). As usual when we introduce new axioms, we run the risk of making the theory inconsistent. Here the risk is greater than usual, because these axioms do not fit the same form as our previous recursive definitions. Typically, in defining a function f, we have used a *successor* axiom, which expresses the value of $f(x, y+1)$ in terms of the value of $f(x, y)$. Here the *remainder* axiom expresses the value of $gcd(x, y)$, for positive y, in terms of the value of $gcd(y, rem(x, y))$. The augmented theory is in fact consistent, as can be shown by exhibiting the model under which gcd is assigned the greatest common divisor function. ▟

It may not be clear at this point why the function defined by these axioms is called the "greatest common divisor." The following proposition establishes that $gcd(x, y)$ is a "common divisor" of x and y; later we shall observe that it is indeed the "greatest" of the common divisors.

Proposition (common divisor)

The sentence

$$(\forall \textit{ integer } x, y) \begin{bmatrix} gcd(x, y) \preceq_{div} x \\ \quad and \\ gcd(x, y) \preceq_{div} y \end{bmatrix} \qquad (\textit{common divisor})$$

is valid. ▟

In other words, $gcd(x, y)$ divides both x and y.

Proof. We actually prove (rearranging the quantifiers) the equivalent sentence

$$(\forall \textit{ integer } y, x) \begin{bmatrix} gcd(x, y) \preceq_{div} x \\ \quad and \\ gcd(x, y) \preceq_{div} y \end{bmatrix}.$$

The proof is by *complete induction* on y, taking the inductive sentence to be

$$\mathcal{F}[y]: \quad (\forall \textit{ integer } x) \begin{bmatrix} gcd(x, y) \preceq_{div} x \\ \quad and \\ gcd(x, y) \preceq_{div} y \end{bmatrix}.$$

To prove $(\forall \textit{ integer } y)\mathcal{F}[y]$, it suffices to establish the inductive step.

Inductive Step

We would like to show

$$(\forall \textit{ integer } y) \begin{bmatrix} \textit{if } (\forall \textit{ integer } y') \begin{bmatrix} \textit{if } y' < y \\ \textit{then } \mathcal{F}[y'] \end{bmatrix} \\ \textit{then } \mathcal{F}[y] \end{bmatrix}.$$

For an arbitrary nonnegative integer y, we assume the induction hypothesis

$$(\forall\ integer\ y') \begin{bmatrix} if\ \ y' < y \\ then\ \ \mathcal{F}[y'] \end{bmatrix}$$

and attempt to show the desired conclusion

$$\mathcal{F}[y],$$

that is,

$$(\forall\ integer\ x) \begin{bmatrix} gcd(x,\ y) \preceq_{div} x \\ \quad and \\ gcd(x,\ y) \preceq_{div} y \end{bmatrix}.$$

Consider an arbitrary nonnegative integer x; we would like to show that

$$\begin{array}{l} gcd(x,\ y) \preceq_{div} x \\ \quad and \\ gcd(x,\ y) \preceq_{div} y. \end{array}$$

Following the axioms for the *gcd* function, we distinguish between two subcases, depending on whether or not $y = 0$.

Case: $y = 0$

Then (by the *zero* axiom for the *gcd*) we have

$$gcd(x,\ y) \ = \ x.$$

The statement we would like to show then reduces to

$$x \preceq_{div} x \ \ and \ \ x \preceq_{div} 0.$$

The first conjunct follows from the *reflexivity* property of the divides relation, and the second from the *right-zero* property.

Case: *not* $(y = 0)$

In other words, y is positive. Then (by the *remainder* axiom for *gcd*)

$$gcd(x,\ y) \ = \ gcd\big(y,\ rem(x,\ y)\big).$$

We would like to show

$$\begin{array}{l} gcd(x,\ y) \preceq_{div} x \\ \quad and \\ gcd(x,\ y) \preceq_{div} y, \end{array}$$

which (in this case) may be expanded to

$$\begin{array}{l} gcd\big(y,\ rem(x,y)\big) \preceq_{div} x \\ \quad and \\ gcd\big(y,\ rem(x,\ y)\big) \preceq_{div} y. \end{array}$$

We know (by the *quotient-remainder* proposition, because y is positive) that

$$x = y \cdot quot(x, y) + rem(x, y).$$

Therefore the statement we would like to show may be expanded further, to

$$\begin{aligned} &gcd(y, rem(x, y)) \preceq_{div} y \cdot quot(x, y) + rem(x, y) \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} y. \end{aligned}$$

Thus (by the *addition* property of the divides relation) it suffices to establish

$$\begin{aligned} &gcd(y, rem(x, y)) \preceq_{div} y \cdot quot(x, y) \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} rem(x, y) \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} y. \end{aligned}$$

Hence (by the *multiplication* property of the divides relation) it suffices to establish

$$\begin{aligned} &\begin{bmatrix} gcd(y, rem(x, y)) \preceq_{div} y \\ \quad or \\ gcd(y, rem(x, y)) \preceq_{div} quot(x, y) \end{bmatrix} \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} rem(x, y) \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} y, \end{aligned}$$

which is equivalent (by propositional logic) to

$$(*) \qquad \begin{aligned} &gcd(y, rem(x, y)) \preceq_{div} y \\ &\quad and \\ &gcd(y, rem(x, y)) \preceq_{div} rem(x, y). \end{aligned}$$

We have assumed as our induction hypothesis that

$$(\forall\ integer\ y') \begin{bmatrix} if\ \ y' < y \\ then\ \ \mathcal{F}[y'] \end{bmatrix}.$$

In particular (taking y' to be $rem(x, y)$), we have

$$\begin{aligned} &if\ \ rem(x, y) < y \\ &then\ \ \mathcal{F}[rem(x, y)]. \end{aligned}$$

Since (by the *quotient-remainder* proposition, because y is positive in this case)

$$rem(x, y) < y,$$