we have $\mathcal{F}[rem(x, y)]$, that is,

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

(Note that we have renamed the bound variable x of the induction hypothesis to x', to avoid capturing the free occurrence of x in $rem(x, y)$.) In particular (taking x' to be y), we obtain

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

which is the statement $(*)$ we were trying to establish.

Because we have established the desired result in both cases, we have completed the proof. ▟

Note that the proof of the inductive step for the case in which $y = 0$ was completed without appealing to the induction hypothesis. This corresponds to the base case in a stepwise induction proof.

Remark (why not stepwise induction?). The above proof would be awkward to carry out by stepwise induction rather than complete induction. In the inductive step we attempted to prove our desired conclusion $\mathcal{F}[y]$, which is of the form

$$(\forall\ integer\ x)\mathcal{G}[x,\ y],$$

where

$$\mathcal{G}[x,\ y]: \quad \begin{array}{l} gcd(x,\ y) \preceq_{div} x \\ \quad and \\ gcd(x,\ y) \preceq_{div} y. \end{array}$$

For an arbitrary nonnegative integer x, we found (in the case in which *not* $(y = 0)$) that to establish $\mathcal{G}[x, y]$ it suffices to establish the corresponding condition $(*)$,

$$\mathcal{G}[y,\ rem(x,\ y)].$$

We were then able to apply our induction hypothesis,

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

to establish (renaming x to x' and taking y' to be $rem(x, y)$, since $rem(x, y) < y$) that

$$(\forall\ integer\ x')\mathcal{G}[x',\ rem(x,\ y)].$$

This gives the desired condition $(*)$, taking x' to be y.

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

$$(\forall\ integer\ x)\mathcal{G}[x,\ y-1].$$

This does not necessarily give us the condition $(*)$, that is, $\mathcal{G}[y,\ rem(x,\ y)]$, because $rem(x,\ y)$ can be any nonnegative integer less than y. A successful stepwise-induction proof (whether by the *decomposition* version or the original version) requires a more complex inductive sentence. ┘

The proof of the *common-divisor* proposition illustrates some of the strategic aspects of performing a proof by induction.

Remark (generalization). The proof of the *common-divisor* proposition did not require us to generalize the sentence to be proved, but it can be used to illustrate the need for generalization. Suppose, instead of being given the sentence

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

to prove, we had been given only the left conjunct,

$$(\forall\ integer\ x,\ y)\big[gcd(x,\ y) \preceq_{div} x\big].$$

Although this is a weaker sentence, we would not be able to establish it by imitating the above proof. We can see this as follows:

Suppose we reverse the quantifiers and attempt to prove

$$(\forall\ integer\ y,\ x)\big[gcd(x,\ y) \preceq_{div} x\big]$$

by complete induction on y, taking the inductive sentence to be

$$\mathcal{F}[y]:\quad (\forall\ integer\ x)\big[gcd(x,\ y) \preceq_{div} x\big].$$

The desired conclusion of the inductive step would also be

$$(\forall\ integer\ x)\big[gcd(x,\ y) \preceq_{div} x\big].$$

For an arbitrary nonnegative integer x, we would succeed in showing (in the case in which *not* $(y=0)$) that, to establish the subsentence

$$gcd(x,\ y) \preceq_{div} x,$$

it suffices to establish the sentence $(*)$,

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

as in our original proof.

However, because we are attempting to show a weaker sentence, our induction hypothesis is the correspondingly weaker sentence

$$(\forall\ integer\ y')\begin{bmatrix} if\ \ y' < y \\ then\ \ (\forall\ integer\ x)\big[gcd(x,\ y') \preceq_{div} x\big] \end{bmatrix}.$$

Our weaker induction hypothesis would allow us to show (taking y' to be $rem(x, y)$ and x to be y, because $rem(x, y) < y$) that

$$gcd(y, rem(x, y)) \preceq_{div} y,$$

which is the first conjunct of the sentence (*) we need to establish. We could not easily show the second conjunct, that

$$gcd(y, rem(x, y)) \preceq_{div} rem(x, y).$$

In fact, if initially we were only given the single condition

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

to prove, we would have had to discover the second condition ourselves and prove the more general, stronger statement consisting of the conjunction of the two conditions together, as we did in the proposition. This generalization process may require some ingenuity. ┘

The proposition we have just established states that, for all nonnegative integers x and y, the nonnegative integer $gcd(x, y)$ is indeed a common divisor of x and y, i.e., it exhibits the common-divisor relationship

$$gcd(x, y) \preceq_{div} x \quad \textit{and} \quad gcd(x, y) \preceq_{div} y.$$

It can also be shown that $gcd(x, y)$ is the "greatest" common divisor of x and y, where "greatest" means greatest with respect to the divides relation $\preceq_{div}$. In other words, for every nonnegative integer z, if z is a common divisor of x and y, that is, if

$$z \preceq_{div} x \textit{ and } z \preceq_{div} y,$$

then $gcd(x, y)$ is "greater" than z, that is,

$$z \preceq_{div} gcd(x, y).$$

In short,

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

The proof of this property is left as an exercise (**Problem 8.12**).

We have defined the greatest-common-divisor function $gcd(x, y)$ in terms of the rather unnatural looking *zero* and *remainder* axioms; we can then establish that $gcd(x, y)$ is indeed a greatest common divisor of x and y. In an alternative augmentation of the theory, we can define the function by axioms that express the desired property, that $gcd(x, y)$ is a greatest common divisor of x and y. In other words, we take the *common-divisor* and *greatest* properties to be the axioms for *gcd*, and then prove the original *zero* and *remainder* axioms as properties. These alternative axioms, however, do not suggest a method for computing the *gcd* function.

8.10 THE LEAST-NUMBER PRINCIPLE

In this section, we establish a basic property of the nonnegative integers, which turns out to be equivalent to the *complete induction* principle.

Proposition (least-number principle)

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

$$\begin{array}{l} \textit{if} \ \ (\exists \ \textit{integer} \ x)\mathcal{G}[x] \\ \textit{then} \ \ (\exists \ \textit{integer} \ x) \begin{bmatrix} \mathcal{G}[x] \\ \quad \textit{and} \\ (\forall \ \textit{integer} \ x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \textit{not} \ \mathcal{G}[x'] \end{bmatrix} \end{bmatrix} \end{array} \qquad (\textit{least number})$$

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

In other words, if a statement $\mathcal{G}[x]$ is true for some nonnegative integer x, there must be a least nonnegative integer x' for which it is true.

Proof. Consider an arbitrary sentence $\mathcal{G}[x]$, where x' is not free in $\mathcal{G}[x]$.

Recall that the *complete induction* principle asserted that, for each sentence $\mathcal{F}[x]$, the universal closure of the sentence

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

is valid, where x' is not free in $\mathcal{F}[x]$. If we take $\mathcal{F}[x]$ to be *not* $\mathcal{G}[x]$, we obtain

$$\begin{array}{l} \textit{if} \ \ (\forall \ \textit{integer} \ x) \begin{bmatrix} \textit{if} \ \ (\forall \ \textit{integer} \ x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \textit{not} \ \mathcal{G}[x'] \end{bmatrix} \\ \textit{then} \ \ \textit{not} \ \mathcal{G}[x] \end{bmatrix} \\ \textit{then} \ \ (\forall \ \textit{integer} \ x)\big[\textit{not} \ \mathcal{G}[x]\big]. \end{array}$$

Using the propositional-logic equivalence

$$\begin{bmatrix} \textit{if} \ \ \mathcal{H}_1 \\ \textit{then} \ \ \textit{not} \ \mathcal{H}_2 \end{bmatrix} \ \equiv \ \textit{not} \ \big[\mathcal{H}_1 \ \textit{and} \ \mathcal{H}_2\big],$$

we obtain the equivalent sentence

$$\begin{array}{l} \textit{if} \ \ (\forall \ \textit{integer} \ x) \ \textit{not} \begin{bmatrix} (\forall \ \textit{integer} \ x') \begin{bmatrix} \textit{if} \ \ x' < x \\ \textit{then} \ \ \textit{not} \ \mathcal{G}[x'] \end{bmatrix} \\ \quad \textit{and} \\ \mathcal{G}[x] \end{bmatrix} \\ \textit{then} \ \ (\forall \ \textit{integer} \ x)\big[\textit{not} \ \mathcal{G}[x]\big]. \end{array}$$

By the duality between the universal and existential quantifiers, this is equivalent to

$$\begin{array}{l} \mathit{if}\ \ \mathit{not}\ (\exists\ \mathit{integer}\ x) \begin{bmatrix} (\forall\ \mathit{integer}\ x') \begin{bmatrix} \mathit{if}\ \ x' < x \\ \mathit{then}\ \ \mathit{not}\ \mathcal{G}[x'] \end{bmatrix} \\ \quad \mathit{and} \\ \mathcal{G}[x] \end{bmatrix} \\ \mathit{then}\ \ \mathit{not}\ (\exists\ \mathit{integer}\ x)\mathcal{G}[x]. \end{array}$$

Because any sentence is equivalent to its contrapositive, that is,

$$\begin{bmatrix} \mathit{if}\ \ \mathit{not}\ \mathcal{H}_1 \\ \mathit{then}\ \ \mathit{not}\ \mathcal{H}_2 \end{bmatrix} \equiv \begin{bmatrix} \mathit{if}\ \ \mathcal{H}_2 \\ \mathit{then}\ \ \mathcal{H}_1 \end{bmatrix}$$

is valid in propositional logic, we obtain

$$\begin{array}{l} \mathit{if}\ \ (\exists\ \mathit{integer}\ x)\mathcal{G}[x] \\ \mathit{then}\ \ (\exists\ \mathit{integer}\ x) \begin{bmatrix} (\forall\ \mathit{integer}\ x') \begin{bmatrix} \mathit{if}\ \ x' < x \\ \mathit{then}\ \ \mathit{not}\ \mathcal{G}[x'] \end{bmatrix} \\ \quad \mathit{and} \\ \mathcal{G}[x] \end{bmatrix} \end{array}$$

or equivalently, reversing the conjuncts,

$$\begin{array}{l} \mathit{if}\ \ (\exists\ \mathit{integer}\ x)\mathcal{G}[x] \\ \mathit{then}\ \ (\exists\ \mathit{integer}\ x) \begin{bmatrix} \mathcal{G}[x] \\ \quad \mathit{and} \\ (\forall\ \mathit{integer}\ x') \begin{bmatrix} \mathit{if}\ \ x' < x \\ \mathit{then}\ \ \mathit{not}\ \mathcal{G}[x'] \end{bmatrix} \end{bmatrix}. \end{array}$$

This is precisely the *least-number* principle for the sentence $\mathcal{G}[x]$. ┘

Note that the proof of the validity of the *least-number* principle required only the *complete induction* principle and properties of propositional and predicate logic; it made no mention of other properties of the less-than relation $<$ or of the nonnegative integers. One can actually establish that the *least-number* principle and the *complete induction* principle are equivalent in predicate logic.

PROBLEMS

As usual, you may use in your proofs any property that is stated in the text earlier than the page reference for the problem, even if that property is given without proof; and you may use the results of any previous problem, even if you haven't solved that problem yourself.

Problem 8.1 (addition) page 384, 392

Establish the validity of the following sentences in the theory of the nonnegative integers, augmented by the axioms for addition:

(a) *Sort*

$$(\forall\ \mathit{integer}\ x,\ y)\big[\mathit{integer}(x+y)\big]$$

(b) *Associativity*

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

(c) *Left cancellation*

$$(\forall\ \mathit{integer}\ x,\ y,\ z)\begin{bmatrix}\mathit{if}\ \ z+x=z+y\\ \mathit{then}\ \ x=y\end{bmatrix}$$

(d) *Right cancellation*

$$(\forall\ \mathit{integer}\ x,\ y,\ z)\begin{bmatrix}\mathit{if}\ \ x+z=y+z\\ \mathit{then}\ \ x=y\end{bmatrix}$$

(e) *Annihilation*

$$(\forall\ \mathit{integer}\ x,\ y)\begin{bmatrix}\mathit{if}\ \ x+y=0\\ \mathit{then}\ \ x=0\ \ \mathit{and}\ \ y=0\end{bmatrix}.$$

Problem 8.2 (multiplication) page 393

Establish the validity of the following sentences in the theory of the nonnegative integers, augmented by the axioms for addition and multiplication:

(a) *Sort*

$$(\forall\ \mathit{integer}\ x,\ y)\big[\mathit{integer}(x\cdot y)\big]$$

(b) *Right one*

$$(\forall\ \mathit{integer}\ x)\big[x\cdot 1\ =\ x\big]$$

(c) *Left zero*

$$(\forall\ \mathit{integer}\ x)\big[0\cdot x\ =\ 0\big]$$

(d) *Left successor*

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

(e) *Left one*

$$(\forall\ \mathit{integer}\ x)\big[1\cdot x\ =\ x\big]$$

(f) *Right distributivity*

$$(\forall\ \mathit{integer}\ x,\ y,\ z)\big[x\cdot(y+z)\ =\ x\cdot y+x\cdot z\big]$$

(g) *Associativity*

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

(h) *Commutativity*

$$(\forall\ integer\ x,\ y)\big[x \cdot y \ = \ y \cdot x\big]$$

(i) *Left distributivity*

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

Problem 8.3 (exponentiation) page 394

(a) Use the axioms for the exponentiation function to determine the value of 3^2.

Establish the validity of the following sentences in the theory of the nonnegative integers, augmented by the axioms for addition, multiplication, and exponentiation:

(b) *Sort*

$$(\forall\ integer\ x,\ y)\big[integer(x^y)\big]$$

(c) *Exp one*

$$(\forall\ integer\ x)\big[x^1 \ = \ x\big]$$

(d) *Zero exp*

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

(e) *One exp*

$$(\forall\ integer\ y)\big[1^y \ = \ 1\big]$$

(f) *Exp plus*

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

(g) *Exp times*

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

Problem 8.4 (factorial) page 398

Suppose we augment our theory of the nonnegative integers by formulating two axioms that define a unary function symbol $x!$, denoting the *factorial* function under the intended model for the nonnegative integers. The axioms are

$$0! \ = \ 1 \qquad (zero)$$

$$(\forall\ integer\ x)\big[(x+1)! \ = \ (x+1) \cdot (x!)\big] \qquad (successor)$$

For example,

$$3! = 3 \cdot (2!) = 3 \cdot 2 \cdot (1!) = 3 \cdot 2 \cdot 1 \cdot (0!) = 3 \cdot 2 \cdot 1 \cdot 1 = 6.$$

Let us introduce an alternative definition of the factorial function by formulating two additional axioms that define a binary function symbol $fact2(x, y)$, as follows:

$$(\forall\ integer\ y)\big[fact2(0, y) = y\big] \qquad (zero)$$

$$(\forall\ integer\ x, y)\begin{bmatrix} fact2(x+1,\ y) \\ = \\ fact2\big(x,\ (x+1)\cdot y\big)\end{bmatrix} \qquad (successor)$$

Prove that the sentence

$$(\forall\ integer\ x)\big[fact2(x, 1) = x!\big] \qquad (alternative\ definition)$$

is valid.

Hint: Prove a more general property.

Problem 8.5 (predecessor and subtraction) page 399, 401

Establish the validity of the following sentences in the theory of the nonnegative integers augmented by the axioms for the addition, predecessor, and subtraction functions and the *positive* relation:

(a) *Decomposition*

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

(b) *Right one*

$$(\forall\ positive\ x)[x - 1 = x^-]$$

(c) *Addition*

$$(\forall\ integer\ x, y)\big[(x + y) - y = x\big]$$

(d) *Negative*

$$(\forall\ integer\ x, y)\big[x - (y + x) = 0 - y\big].$$

Problem 8.6 (subtraction axiom) page 401

(a) Show that the sentence

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

is not valid in the augmented theory of the nonnegative integers.

(b) If we add $\mathcal{F}$ to the theory as a new axiom, is the resulting theory consistent? Justify your answer.

Problem 8.7 (weak less-than) page 403

In the augmented theory of the nonnegative integers, establish the validity of the *left-addition* property for the weak less-than relation, that is,

$$(\forall\ integer\ x,\ y)\begin{bmatrix} x \le y \\ \equiv \\ (\exists\ integer\ z)\big[x + z = y\big] \end{bmatrix}.$$

Problem 8.8 (max and min) page 405

In the augmented theory of the nonnegative integers, establish the validity of the following properties of the maximum and minimum functions:

(a) *Greater-than*

$$(\forall\ integer\ x,\ y)\begin{bmatrix} max(x,\ y) \ge x \\ and \\ max(x,\ y) \ge y \end{bmatrix}$$

(b) *Minimax*

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

Problem 8.9 (quotient-remainder) page 409, 414

In the augmented theory of the nonnegative integers, establish the validity of the following properties of the quotient and remainder functions:

(a) *Sort (for quotient)*

$$\begin{matrix}(\forall\ integer\ x) \\ (\forall\ positive\ y)\end{matrix}\ \big[integer\big(quot(x,\ y)\big)\big]$$

(b) *Sort (for remainder)*

$$\begin{matrix}(\forall\ integer\ x) \\ (\forall\ positive\ y)\end{matrix}\ \big[integer\big(rem(x,\ y)\big)\big]$$

(c) *Uniqueness*

$$(\forall\ integer\ x,\ y,\ u,\ v)\left[\text{if } \begin{bmatrix} x = y \cdot u + v \\ and \\ v < y \end{bmatrix} \text{ then } \begin{bmatrix} u = quot(x,\ y) \\ and \\ v = rem(x,\ y) \end{bmatrix}\right].$$

Problem 8.10 (quotient-remainder by stepwise induction) page 417

Prove the *quotient-remainder* proposition by stepwise induction, without using complete induction. More precisely, do the following:

(a) Suggest an inductive sentence $\mathcal{F}$ for the stepwise induction proof.

(b) Give the stepwise induction proof of your inductive sentence.

(c) Use the validity of $\mathcal{F}$ to establish the *quotient-remainder* proposition.

Problem 8.11 (divides relation) page 419

In the theory of the nonnegative integers augmented by the definition of the divides relation, establish the validity of the following sentences:

(a) *Right zero*

$$(\forall\ integer\ x)[x \preceq_{div} 0]$$

(b) *Left zero*

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

(c) *Greater than*

$$\begin{array}{l}(\forall\ integer\ x)\\(\forall\ positive\ y)\end{array}\begin{bmatrix}if\ \ x > y\\ then\ \ not\ (x \preceq_{div} y)\end{bmatrix}$$

(d) *Subtraction*

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

Show also that these properties constitute an alternative definition for the divides relation. In other words, in the theory of the nonnegative integers augmented by the above four properties, establish the validity of the original definition of $\preceq_{div}$:

(e) *Divides*

$$(\forall\ integer\ x,\ y)\begin{bmatrix}x \preceq_{div} y\\ \equiv \\ (\exists\ integer\ z)[x \cdot z = y]\end{bmatrix}.$$

Problem 8.12 (greatest common divisor) page 426

Establish that the greatest common divisor $gcd(x,\ y)$ is indeed the "greatest" of the common divisors of x and y, with respect to the divides relation $\preceq_{div}$; in other words, in the augmented theory of the nonnegative integers, establish the validity of the sentence

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

Problem 8.13 (fallacious induction principle) page 379

One would expect that, for each sentence $\mathcal{F}[x]$ in the theory of the nonnegative integers, the universal closure of the following sentence would be valid:

$$\begin{array}{l} \mathit{if} \begin{bmatrix} \mathcal{F}[0] \\ \quad \mathit{and} \\ (\forall\ \mathit{integer}\ y) \begin{bmatrix} \mathit{if}\ \ \mathcal{F}[y] \\ \mathit{then}\ \ \mathcal{F}[y^+] \end{bmatrix} \end{bmatrix} \\ \mathit{then}\ \ (\forall\ \mathit{integer}\ x)\mathcal{F}[x]. \end{array}$$

After all, the above sentence is obtained from the original *induction* principle by "renaming" the bound variable x of the inductive step to y.

In fact, if y occurs free in $\mathcal{F}[x]$, the sentence is not always true. Find a sentence $\mathcal{F}[x]$ in the theory for which the universal closure of the above implication is not valid.

Problem 8.14 (decomposition property) page 382

Consider a theory defined by the axioms of the unaugmented theory of the nonnegative integers without the *induction* principle. Show that the *decomposition* property is not valid in this theory. That is, present an interpretation under which all the axioms (other than the *induction* principle) are true but the *decomposition* property is false.

Problem 8.15 (decomposition induction principle) page 402

Establish the *decomposition induction* principle, that is, show that for each sentence $\mathcal{F}[x]$, the universal closure of the sentence

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

is valid.

Problem 8.16 (no induction principle) page 406

Consider a theory defined by the two generation axioms and the two uniqueness axioms for the nonnegative integers and the two axioms for addition. Note that this theory does not have an induction principle.

Show that the valid sentences of this theory are not the same as the valid sentences of the augmented theory of the nonnegative integers, by exhibiting a model $\mathcal{I}$ for the six axioms of this theory such that the sentence

$$(\forall\ \mathit{integer}\ x,\ y)(\exists\ \mathit{integer}\ z)\big[x + z = y\ \ \mathit{or}\ \ y + z = x\big]$$

is false. Intuitively speaking, this sentence says that for all integers x and y, either $x \leq y$ or $y \leq x$.

11

Deductive Tableaux

We have introduced a deductive-tableau system to prove the validity of sentences in predicate logic and in finite theories, with or without equality. In this chapter, we adapt the system to prove validity in more complex theories, theories with induction.

We have seen how we can add axioms as assertions into tableaux in predicate logic (with or without equality) to establish the validity of sentences in particular finite theories. The various forms of the principle of mathematical induction, however, are all axiom schemata, each corresponding to an infinite set of axioms. We have devised no method for dealing with axiom schemata within the tableau framework. We cannot introduce an infinite set of assertions into a tableau. Instead, for each theory, we represent the induction principle as a new deduction rule.

11.1 NONNEGATIVE INTEGERS

We begin by reviewing a typical theory with stepwise induction, that of the nonnegative integers. In this theory, we shall use k, ℓ, and m, with or without subscripts, as additional constant symbols.

AXIOMS

The nonnegative integers have been defined by a set of generation and uniqueness axioms and by the induction principle. Let us consider first the axioms.

In the theory of nonnegative integers we have the generation axioms

$integer(0)$	$(zero)$
$(\forall\, integer\ x)\big[integer(x+1)\big]$	$(successor)$

and the uniqueness axioms

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

A tableau over the nonnegative integers is a tableau with equality with the *zero* and *successor* generation axioms and the *zero* and *successor* uniqueness axioms as initial assertions.

The relativized-quantifier notation ($\forall\, integer\ \ldots$) requires special attention here. Without using this notation, the *successor* generation axiom, for example, is actually

$$(\forall x)\begin{bmatrix} if\ \ integer(x) \\ then\ \ integer(x+1) \end{bmatrix}.$$

Thus the corresponding assertion should be (applying outermost skolemization)

assertions	goals
$if\ \ integer(x)$ $then\ \ integer(x+1)$ $\qquad (successor)$	

Similarly for the uniqueness axioms:

$if\ \ integer(x)$ $then\ \ not\ (x+1=0)$ $\qquad (zero)$	
$if\ \ integer(x)\ \ and\ \ integer(y)$ $then\ \ if\ \ x+1=y+1$ $\qquad then\ \ x=y$ $\qquad (successor)$	

The axioms that define new functions (e.g., multiplication) or new relations (e.g., less than) are included as assertions, as before. Once we have proved a property over the nonnegative integers, we may add it as an assertion to all subsequent tableaux over the nonnegative integers.

Because the tableau is with equality, we include the *reflexivity* axiom $(x = x)$ among our assertions, and we may also use the *equality* rule.

INDUCTION RULE

In addition to the generation and uniqueness axioms, the nonnegative integers were also defined in terms of the (stepwise) induction principle:

> For each sentence $\mathcal{F}[x]$ in the theory,
> the universal closure of the sentence
>
> $$\begin{array}{ll} \mathit{if} & \begin{bmatrix} \mathcal{F}[0] \\ \quad \mathit{and} \\ (\forall\, \mathit{integer}\ x) \begin{bmatrix} \mathit{if}\ \ \mathcal{F}[x] \\ \mathit{then}\ \ \mathcal{F}[x+1] \end{bmatrix} \end{bmatrix} \\ \mathit{then} & (\forall\, \mathit{integer}\ x)\mathcal{F}[x] \end{array} \qquad (\mathit{induction})$$
>
> is an axiom.

We would like to incorporate this axiom schema, which was used for informal proofs, into our deductive-tableau framework as a deduction rule. We therefore include in a tableau over the nonnegative integers a new deduction rule for mathematical induction. This induction rule allows us to establish a goal of form

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

by proving the conjunction of a base case and an inductive step.

Rule (stepwise induction)

For a closed sentence

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

we have

assertions	goals
	$(\forall\, \mathit{integer}\ x)\mathcal{F}[x]$
	$\begin{array}{l} \mathcal{F}[0] \\ \quad \mathit{and} \\ \begin{bmatrix} \mathit{if}\ \ \mathit{integer}(m) \\ \mathit{then}\ \ \mathit{if}\ \ \mathcal{F}[m] \\ \qquad\quad \mathit{then}\ \ \mathcal{F}[m+1] \end{bmatrix} \end{array}$

where m is a new constant. ⌟

Here the conjunct

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

corresponds to the base case, and the conjunct

$$\begin{array}{l} \textit{if } \ \textit{integer}(m) \\ \textit{then } \ \textit{if } \ \mathcal{F}[m] \\ \qquad \textit{then } \ \mathcal{F}[m+1] \end{array}$$

corresponds to the inductive step of an informal stepwise-induction proof.

Remark (closed sentence). We are permitted to apply the *stepwise induction* rule only if the goal is a closed sentence. Otherwise, if the goal

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

contains a free variable y, it actually stands for the existentially quantified goal

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

We cannot apply the *induction* principle to prove an existentially quantified sentence. ⌟

We give an informal justification of the rule.

Justification (stepwise induction). The induction rule preserves validity, not equivalence. Let us show that, if the required goal

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

appears in the tableau, then we may add the generated rows without affecting the validity of the tableau.

By the *stepwise induction* principle, we know that, to show the truth of a closed sentence

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

it suffices to establish the conjunction

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

(We need not consider the universal closure of the sentence since by our assumption it contains no free variables.)

Thus (by the *implied-row* property) we may add to our tableau the new goal

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

that is,

	$\mathcal{F}[0]$ *and* $(\forall\, x)^{\forall}\begin{bmatrix} \mathit{if}\ \ \mathit{integer}(x) \\ \mathit{then}\ \ \mathit{if}\ \ \mathcal{F}[x] \\ \qquad\quad \mathit{then}\ \ \mathcal{F}[x+1] \end{bmatrix}$

Because the quantifier $(\forall\, x)$ of this goal is of universal force, we may drop the quantifier (by the $\forall$-*elimination* rule), replacing the variable x with the new skolem constant m (because the goal has no free variables), to obtain

	$\mathcal{F}[0]$ *and* $\begin{bmatrix} \mathit{if}\ \ \mathit{integer}(m) \\ \mathit{then}\ \ \mathit{if}\ \ \mathcal{F}[m] \\ \qquad\quad \mathit{then}\ \ \mathcal{F}[m+1] \end{bmatrix}$

This is precisely the goal derived by the rule. By the *intermediate-tableau* property (Section 5.1), we do not need to include the intermediate goal. ▪

EXAMPLES

We illustrate the proof of some properties in the theory of nonnegative integers. The reader may observe that there is a close correspondence between these deductive-tableau proofs and informal proofs of the same properties in Section 8.2.

Example (left-zero). The addition function $+$ is defined by the two axioms

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

We would like to show that 0 is a left identity for addition, that is,

$$(\forall\, integer\ x)\big[0 + x \;=\; x\big] \qquad (left\ zero)$$

We begin with the goal

assertions	goals
	G1. $(\forall\, integer\ x)\big[0 + x \;=\; x\big]$

in a tableau over the nonnegative integers.

The tableau contains among its assertions the generation and uniqueness axioms for the nonnegative integers, the *reflexivity* axiom for equality, and the two axioms for addition,

if $integer(x)$ *then* $x + 0 \;=\; x$ *(right zero)*	
if $integer(x)$ *and* $integer(y)$ *then* $x + (y+1) \;=\; (x+y)+1$ *(right successor)*	

Applying the *stepwise induction* rule to goal G1, we obtain the goal

	G2. $\boxed{0 + 0 \;=\; 0}^{+}$ *and* $\left[\begin{array}{l} \textit{if } integer(m) \\ \textit{then if } 0 + m \;=\; m \\ \qquad \textit{then } 0 + (m+1) \;=\; m+1 \end{array}\right]$

The first conjunct corresponds to the base case and the second to the inductive step of an informal stepwise-induction proof.

Recall the *right-zero* axiom for addition,

if $integer(x)$ *then* $\boxed{x + 0 \;=\; x}^{-}$	

By the *resolution* rule, applied to the axiom and goal G2, with $\{x \leftarrow 0\}$, the first conjunct of goal G2 may be dropped, leaving

	G3. $\boxed{integer(0)}^{+}$ *and* $\left[\begin{array}{l} \textit{if } integer(m) \\ \textit{then if } 0+m = m \\ \qquad \textit{then } 0+(m+1) = m+1 \end{array}\right]$

Recall the *zero* generation axiom

$\boxed{integer(0)}^{-}$	

By the *resolution* rule, applied to the axiom and goal G3, the first conjunct of the goal may be dropped, leaving

	G4. *if* $integer(m)$ *then if* $0+m = m$ *then* $0+(m+1) = m+1$

We have thus proved the base case of the induction; it remains to show the inductive step, i.e., goal G4.

By two applications of the *if-split* rule, we may break down goal G4 into

A5. $integer(m)$	
A6. $0+m = m$	
	G7. $\boxed{0+(m+1)} = m+1$

Assertion A6 corresponds to the induction hypothesis, and goal G7 to the desired conclusion, of the inductive step of an informal induction proof. Assertion A5 corresponds to the phrase "Consider an arbitrary nonnegative integer m. ..."

Recall the *right-successor* axiom for addition,

if $integer(x)$ *and* $integer(y)$ *then* $\left[\boxed{x+(y+1)} = (x+y)+1\right]^{-}$	

By the *equality* rule, with $\{x \leftarrow 0,\ y \leftarrow m\}$, we obtain

	G8. $\boxed{integer(0)}^{+}$ *and* $\boxed{integer(m)}^{+}$ *and* $(0+m)+1 \;=\; m+1$

Recall the *zero* generation axiom,

$\boxed{integer(0)}^{-}$	

and the assertion A5,

$\boxed{integer(m)}^{-}$	

By two applications of the *resolution* rule, to these assertions and the goal G8, we obtain

	G9. $\boxed{0+m}+1 = m+1$

By the *equality* rule again, using the induction hypothesis (assertion A6),

$\left[\boxed{0+m} \;=\; m\right]^{-}$	

we may reduce goal G9 to

	G10. $\boxed{m+1 \;=\; m+1}^{+}$

Finally, by the reflexivity of equality, we obtain the goal

	G11. *true*

This completes the proof of the *left-zero* property

$$(\forall\, integer\ x)\big[0+x \;=\; x\big].$$

We may now include this property as an assertion in future tableaux over the nonnegative integers. ▄

Note that the base case and the inductive step of an informal proof by induction correspond to a single proof in the deductive-tableau system.

Remark (beware of hasty skolemization). In a pure predicate-logic tableau proof, there is little harm in applying the skolemization rules to eliminate all quantifiers, at least those of strict force. On the other hand, in a tableau proof over the nonnegative integers, we must exercise some discretion in removing quantifiers. If we remove the outermost universal quantifier $(\forall\, integer\ x)$ of a goal, we cannot apply induction on x to the resulting goal. $\lrcorner$

Remark (removal of sort conditions). Many of the steps in the above proof had the effect of removing sort conditions, such as $integer(0)$ or $integer(m)$, by resolution with an assertion. Removal of sort conditions is often a routine and monotonous part of a proof; in such cases, we shall omit the details and justify the step with the annotation "removal of sort conditions."

Sometimes it is necessary to apply more than one resolution step to remove a sort condition. For instance, to remove a sort condition $integer(m+1)$ in a goal, we may apply the *resolution* rule to the *successor* generation axiom and the goal, obtaining the new condition $integer(m)$. The new condition can then be removed by resolution with an assertion. In the following proof, one such step will be spelled out in detail; subsequent steps of this kind will be omitted and justified by the annotation "removal of sort conditions." $\lrcorner$

Example (left successor). Suppose we would like to show the *left-successor* property of addition, that is,

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

In the theory of the nonnegative integers, we begin with the goal

assertions	goals
	G1. $(\forall\, integer\ x, y)\big[(x+1)+y \;=\; (x+y)+1\big]$

We have several options in applying skolemization and induction on x and y. Following the informal proof (Section 8.2), we prefer to skolemize x first and then to apply induction on y.

Abandoning the relativized-quantifier notation in $(\forall\ integer\ x)$, we can express goal G1 as

	G1$'$. $(\forall x)^{\forall}\begin{bmatrix} if\ \ integer(x) \\ then\ \ (\forall\ integer\ y)\begin{bmatrix}(x+1)+y\ = \\ (x+y)+1\end{bmatrix}\end{bmatrix}$

By application of the $\forall$-*elimination* rule, we may drop the outermost quantifier of goal G1$'$, replacing the variable x with the skolem constant k, to obtain

	G2. $\mathit{if}\ \mathit{integer}(k)$ $\mathit{then}\ (\forall\ \mathit{integer}\ y)\big[(k+1)+y = (k+y)+1\big]$

Henceforth we shall abandon the relativized-quantifier notation implicitly as part of the process of eliminating a relativized quantifier, without mentioning it as a separate step.

By the *if-split* rule, goal G2 may be decomposed into

A3. $\mathit{integer}(k)$	
	G4. $(\forall\ \mathit{integer}\ y)\big[(k+1)+y = (k+y)+1\big]$

By the *stepwise induction* rule applied to goal G4, we obtain

	G5. $\boxed{(k+1)+0} = (k+0)+1$ and $\left[\begin{array}{l} \mathit{if}\ \mathit{integer}(m) \\ \mathit{then}\ \mathit{if}\ (k+1)+m = (k+m)+1 \\ \qquad \mathit{then} \begin{bmatrix}(k+1)+(m+1) = \\ (k+(m+1))+1\end{bmatrix}\end{array}\right]$

Here the first conjunct corresponds to the base case and the second to the inductive step of an informal proof. We first establish the base case.

Base Case

Recall the *right-zero* axiom for addition,

$\mathit{if}\ \mathit{integer}(x)$ $\mathit{then}\ \left[\boxed{x+0} = x\right]^{-}$	

By the *equality* rule, applied to the axiom and goal G5, with $\{x \leftarrow k+1\}$, the goal is transformed to

	G6. $\boxed{\mathit{integer}(k+1)}^{+}$ and $k+1 = (k+0)+1$ and $[\ \ldots\ ]$

We do not write the last conjunct, the inductive step, because it plays no role in this portion of the proof.

For this step, we spell out the details of how to remove the sort condition *integer*$(k+1)$. Recall the *successor* generation axiom

if *integer*(x) *then* $\boxed{integer(x+1)}^{-}$	

By the *resolution* rule, applied to the axiom and goal G6, with $\{x \leftarrow k\}$, we obtain

	G7. $\boxed{integer(k)}^{+}$ *and* $k+1 \;=\; (k+0)+1$ *and* [. . .]

Recall the assertion A3

$\boxed{integer(k)}^{-}$	

By the *resolution* rule, applied to assertion A3 and goal G7, we drop the remaining sort condition, leaving

	G8. $k+1 \;=\; \boxed{k+0}+1$ *and* [. . .]

Subsequently, all such patterns of reasoning will be justified by the phrase "removal of sort conditions."

By the *equality* rule, applied once more to the *right-zero* axiom and goal G8, with $\{x \leftarrow k\}$, the goal is transformed further (removing a sort condition) to

	G9. $\boxed{k+1 \;=\; k+1}^{+}$ *and* [. . .]

By the reflexivity of equality, the first conjunct of goal G9 may now be dropped altogether, leaving the goal

	G10. *if integer*(m) *then if* $(k+1)+m \ = \ (k+m)+1$ *then* $(k+1)+(m+1) \ = \ (k+(m+1))+1$

The remaining goal corresponds to the inductive step of an informal stepwise-induction proof.

Inductive Step

By two applications of the *if-split* rule, we may break down goal G10 into

A11. *integer*(m)	
A12. $\left[\begin{array}{c}\boxed{(k+1)+m} \\ = \\ (k+m)+1\end{array}\right]^-$	
	G13. $\begin{array}{c}\boxed{(k+1)+(m+1)} \\ = \\ \boxed{k+(m+1)} \ +1\end{array}$

Assertion A12 corresponds to the induction hypothesis and goal G13 to the desired conclusion of the inductive step. Assertion A11 corresponds to the phrase "Consider an arbitrary nonnegative integer m ... ."

Recall the *right-successor* axiom for addition,

if integer(x) *and integer*(y) *then* $\left[\boxed{x+(y+1)} \ = \ (x+y)+1\right]^-$	

By the *equality* rule, applied twice to the axiom and goal G13, first with the most-general unifier $\{x \leftarrow k+1, \ y \leftarrow m\}$ and then with $\{x \leftarrow k, \ y \leftarrow m\}$, we may transform the goal (removing sort conditions) into

	G14. $\begin{array}{c}\boxed{(k+1)+m} \ +1 \\ = \\ ((k+m)+1)+1\end{array}$

Applying the *equality* rule to the induction hypothesis (assertion A12) and goal G14, we may transform the goal into

	G15. $\boxed{\begin{array}{c}\big((k+m)+1\big)+1\\ =\\ \big((k+m)+1\big)+1\end{array}}$	+

Finally, by the reflexivity of equality, we obtain the final goal

	G16. *true*

The proof in the following example uses each of the previous two properties as assertions. It shows that it may be necessary to prove some properties before proving others.

Example (commutativity). Suppose we would like to show that addition is commutative, i.e., that

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

It turns out to be convenient to first prove the slightly different property

$$(\forall\, integer\ x)\Big[(\forall\, integer\ y)[x+y=y+x]\Big] \qquad (alternative)$$

The two properties are equivalent but not identical because of the way the relativized quantifier is defined (Section 6.9). The *commutativity* property is an abbreviation of

$$(\forall\, x,\ y)\begin{bmatrix} if\ integer(x)\ \ and\ \ integer(y)\\ then\ x+y=y+x \end{bmatrix}.$$

The *alternative* property, on the other hand, is an abbreviation of

$$(\forall\, x)\begin{bmatrix} if\ integer(x)\\ then\ (\forall\, y)\begin{bmatrix} if\ integer(y)\\ then\ x+y=y+x\end{bmatrix}\end{bmatrix}.$$

The latter will be easier to prove. Then we will be able to use it as an assertion in a simple proof of the original *commutativity* property.

- *Proof of the Alternative Property*

To prove the *alternative* property, we begin with the initial goal

assertions	goals
	G1. $(\forall\, integer\ x)\Big[(\forall\, integer\ y)[x+y=y+x]\Big]$

Again, we have some freedom in applying skolemization and induction on x and y. In this proof, we prefer to skolemize x first and to apply induction on y later.

By application of the $\forall$-*elimination* rule, we may drop the quantifier $(\forall\, x)$ of goal G1, replacing the variable x with the skolem constant ℓ, and then apply the *if-split* rule, to obtain

A2. $integer(\ell)$	
	G3. $(\forall\ integer\ y)\big[\ell + y \;=\; y + \ell\big]$

Applying stepwise induction on y to goal G3, we obtain

	G4. $\ell + 0 \;=\; \boxed{0 + \ell}$ *and* $\left[\begin{array}{l} \textit{if } integer(m) \\ \textit{then if } \ell + m \;=\; m + \ell \\ \qquad \textit{then } \ell + (m+1) \;=\; (m+1) + \ell \end{array}\right]$

Base Case

In an earlier example, we proved the *left-zero* property for addition, which we may therefore include in our tableau as an assertion,

if $integer(x)$ *then* $\left[\boxed{0 + x} \;=\; x\right]^{-}$	

By the *equality* rule, applied to the property and goal G4, with $\{x \leftarrow \ell\}$, removing a sort condition, the goal is reduced to

	G5. $\boxed{\ell + 0 \;=\; \ell}^{+}$ *and* $\left[\begin{array}{l} \textit{if } integer(m) \\ \textit{then if } \ell + m \;=\; m + \ell \\ \qquad \textit{then } \ell + (m+1) \;=\; (m+1) + \ell \end{array}\right]$

Recall the *right-zero* axiom for addition,

if $integer(x)$ *then* $\boxed{x + 0 = x}^{-}$	

By the *resolution* rule, applied to the axiom and goal G5, with $\{x \leftarrow \ell\}$, removing a sort condition, the first conjunct of the goal may now be dropped, leaving

	G6. *if* $integer(m)$ *then if* $\ell + m = m + \ell$ *then* $\ell + (m+1) = (m+1) + \ell$

We have thus disposed of the base case; it remains to complete the inductive step.

Inductive Step

By two applications of the *if-split* rule, we may break down goal G6 into the assertions

A7. $integer(m)$	
A8. $\left[\ell + m = \boxed{m + \ell}\right]^{-}$	

and the goal

	G9. $\ell + (m+1) = \boxed{(m+1) + \ell}$

Assertion A8 corresponds to the induction hypothesis, and goal G9 to the desired conclusion, of the inductive step. Assertion A7 corresponds to the phrase "Consider an arbitrary nonnegative integer m. ..."

Recall the *left-successor* property for addition (which we proved in the preceding example),

if $integer(x)$ *and* $integer(y)$ *then* $\left[\boxed{(x+1) + y} = (x+y) + 1\right]^{-}$	

By the *equality* rule, applied to the property and goal G9, with $\{x \leftarrow m,\ y \leftarrow \ell\}$, removing sort conditions, we may transform the goal into

	G10. $\ell + (m+1) = \boxed{m + \ell} + 1$

By the *equality* rule (right-to-left), applied to the induction hypothesis (assertion A8) and goal G10, we may transform the goal into

	G11. $\boxed{\ell + (m+1) \;=\; (\ell + m) + 1}^{+}$

Recall the *right-successor* axiom for addition,

if $integer(x)$ *and* $integer(y)$ *then* $\boxed{x + (y+1) \;=\; (x+y) + 1}^{-}$	

By the *resolution* rule, applied to the axiom and goal G11, with $\{x \leftarrow \ell,\ y \leftarrow m\}$, removing sort conditions, we obtain the final goal

	G12. *true*

We have remarked that the preceding proof of the *alternative* property used both the *left-zero* and *left-successor* properties as assertions. Had we attempted to prove the *alternative* property without having proved the other two properties first, it would have been difficult to complete the proof.

Now that we have completed the proof of the *alternative* property

$$(\forall\ integer\ x)\Big[(\forall\ integer\ y)[x + y = y + x]\Big],$$

we may use it as an assertion in the proof of the original *commutativity* property

$$(\forall\ integer\ x,\ y)[x + y = y + x].$$

- *Proof of the Commutativity Property*

We begin with a tableau in which the (unabbreviated) *alternative* property is given as an assertion

assertions	goals
if $integer(x)$ *then if* $integer(y)$ *then* $\boxed{x + y = y + x}^{-}$	

and the initial goal is the *commutativity* property

	G1. $(\forall\ integer\ x,\ y)[x + y = y + x]$

By the $\forall$-elimination rule, we may drop the quantifiers of goal G1, and apply the *if-split* and *and-split* rules, leaving

A2. $integer(\ell)$	
A3. $integer(m)$	
	G4. $\boxed{\ell + m = m + \ell}^{+}$

Here the bound variables x and y of the goal G1 have been replaced by the skolem constants ℓ and m, respectively.

By the *resolution* rule, applied to the *alternative* property and the goal G4, with $\{x \leftarrow \ell,\ y \leftarrow m\}$, removing sort conditions, we obtain the final goal

	G5. *true*

This concludes the proof of the original *commutativity* property

$$(\forall\ integer\ x,\ y)[x + y = y + x]\,. \quad ■$$

In the above sequence, we had the foresight to prove the *alternative* property before attempting to prove the original *commutativity* property. In practice, if in the course of a proof we discover we need an instance of some other property, we may interrupt the main proof and attempt to prove the required property as a subsidiary proposition, or *lemma*, in a separate tableau. Once we have completed the proof of the lemma, we can add it as an assertion in the tableau of the interrupted main proof, and continue the main proof.

The proofs of some properties of the multiplication, exponentiation, and factorial functions are requested in **Problems 11.1**, **11.2**, and **11.3**, respectively. The *fibonacci* function is introduced in **Problem 11.4**. A relation that distinguishes between even and odd nonnegative integers is presented in **Problem 11.5**.

A-FORM OF INDUCTION RULE

The *stepwise induction* rule applies to goals. There is a dual assertion version that applies to assertions.

Rule (stepwise induction, A-form)

For a closed sentence

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

we have

assertions	goals
$(\exists\ integer\ x)\mathcal{F}[x]$	
$\mathcal{F}[0]$ *or* $\begin{bmatrix} integer(m)\ \ and \\ (not\ \mathcal{F}[m])\ \ and \\ \mathcal{F}[m+1] \end{bmatrix}$	

where m is a new constant. ▟

We seldom use this version. Roughly, it says that if $\mathcal{F}[x]$ is true for some integer x, either it is true for 0 or there is some point at which it becomes true. Its justification is requested in **Problem 11.6**.

We do not introduce a tableau form of the *complete induction* principle described in Section 8.6. Complete induction will be seen to be a special case of well-founded induction, which is discussed in the following two chapters.

11.2 TUPLES

In the same way that we introduced the *stepwise induction* rule over the nonnegative integers as a new deduction rule, we can incorporate the *stepwise induction* rules for other theories with induction, including tuples and trees. We consider first the theory of tuples. In this theory, we shall use r, s, and t, with or without subscripts, as additional constant symbols.

AXIOMS AND INDUCTION RULE

A tableau over the tuples is a tableau with equality with the generation axioms

assertions	goals
$tuple(\langle\ \rangle)$ *(empty)*	
if $atom(u)$ *and* $tuple(x)$ *then* $tuple(u \diamond x)$ *(insertion)*	

and the uniqueness axioms

if $atom(u)$ *and* $tuple(x)$ *then* *not* $(u \diamond x = \langle\ \rangle)$ (*empty*)	
if $atom(u)$ *and* $atom(v)$ *and* $tuple(x)$ *and* $tuple(y)$ *then* *if* $u \diamond x = v \diamond y$ (*insertion*) *then* $u = v$ *and* $x = y$	

The axioms that define any new constructs (e.g., append of tuples) are also included as assertions. As usual, any previously proved properties may be incorporated as assertions.

Because the tableau is with equality, we also include the *reflexivity* axiom $(x = x)$ among our assertions, and we may use the *equality* rule in conducting any proof.

In addition, we include in a tableau over the tuples a new deduction rule for stepwise induction. The *stepwise induction* rule for tuples allows us to establish a goal of form $(\forall\, tuple\ x)\mathcal{F}[x]$ by proving the conjunction of a base case and an inductive step.

Rule (stepwise induction)

For a closed sentence

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

we have

assertions	goals
	$(\forall\, tuple\ x)\mathcal{F}[x]$
	$\mathcal{F}[\langle\ \rangle]$ *and* $\begin{bmatrix} \textit{if}\ \ atom(a)\ \textit{and}\ tuple(r) \\ \textit{then}\ \ \textit{if}\ \ \mathcal{F}[r] \\ \qquad \textit{then}\ \ \mathcal{F}[a \diamond r] \end{bmatrix}$

where a and r are new constants. ┘

Here the conjunct

$$\mathcal{F}[\langle\ \rangle]$$

corresponds to the base case, and the conjunct

$$\begin{aligned}&\textit{if } \ atom(a) \ \textit{ and } \ tuple(r)\\&\textit{then } \ \textit{if } \ \mathcal{F}[r]\\&\qquad \textit{then } \ \mathcal{F}[a \diamond r]\end{aligned}$$

corresponds to the inductive step of an informal induction proof. Note that, as in the theory of the nonnegative integers, we are permitted to apply the *stepwise induction* rule only if the goal is a closed sentence.

The justification for the rule is analogous to that for the *stepwise induction* rule over the nonnegative integers (**Problem 11.7(a)**). The reader is requested to formulate and justify an A-form of this rule, which applies to assertions (**Problem 11.7(b)**).

EXAMPLE

In the following example, we illustrate the proof of a property in the theory of tuples. Again, the reader can observe the close similarity between this proof and the corresponding informal proof in Section 9.3.

The example illustrates some of the strategic aspects of the use of the induction principle: the treatment of generalization in a tableau setting and the importance of the order in which skolemization and induction are applied.

Example (alternative reverse). The *reverse* function, which reverses the elements in a tuple, is defined by the following two axioms:

$reverse(\langle\ \rangle) = \langle\ \rangle$	(*empty*)
$\begin{matrix}(\forall\, atom\ u)\\(\forall\, tuple\ x)\end{matrix}\left[reverse(u \diamond x) = reverse(x) \diamond \langle u \rangle\right]$	(*insertion*)

The append function $\diamond$, used in the *insertion* axiom for *reverse*, is defined by the following two axioms:

$(\forall\, tuple\ y)\left[\langle\ \rangle \diamond y = y\right]$	(*left empty*)
$\begin{matrix}(\forall\, atom\ u)\\(\forall\, tuple\ x,\ y)\end{matrix}\left[(u \diamond x) \diamond y = u \diamond (x \diamond y)\right]$	(*left insertion*)

From these axioms, let us assume that we have previously proved within the deductive-tableau system the following properties of append:

$$\begin{array}{l}(\forall\, \textit{atom } u)\\(\forall\, \textit{tuple } y)\end{array}\Big[\langle u\rangle \diamond y \;=\; u \circ y\Big] \qquad (\textit{singleton})$$

$$(\forall\, \textit{tuple } x)\big[x \diamond \langle\,\rangle \;=\; x\big] \qquad (\textit{right empty})$$

$$(\forall\, \textit{tuple } x,\, y,\, z)\big[(x \diamond y) \diamond z \;=\; x \diamond (y \diamond z)\big] \qquad (\textit{associativity})$$

Therefore we are permitted to include these properties as assertions in subsequent initial tableaux.

Suppose we define a function $rev2(x,\, y)$, which reverses the tuple x and appends the result with the tuple y, by the following two axioms:

$$\boxed{\begin{array}{ll}(\forall\, \textit{tuple } y)[rev2(\langle\,\rangle,\, y) \;=\; y] & (\textit{left empty})\\[2ex] \begin{array}{l}(\forall\, \textit{atom } u)\\(\forall\, \textit{tuple } x,\, y)\end{array}\Big[rev2(u \circ x,\, y) \;=\; rev2(x,\, u \circ y)\Big] & (\textit{left insertion})\end{array}}$$

The property we would like to show in this example is that the function $rev2$ gives us an alternative definition of the *reverse* function, that is,

$$(\forall\, \textit{tuple } x)\big[reverse(x) \;=\; rev2(x,\, \langle\,\rangle)\big] \qquad (\textit{special})$$

We must first prove the more general property

$$(\forall\, \textit{tuple } x,\, y)\big[rev2(x,\, y) \;=\; reverse(x) \diamond y\big] \qquad (\textit{general})$$

Then we will be able to use the *general* property as an assertion in the proof of the desired *special* property.

- *Proof of the General Property*

To prove the *general* property, we begin with the goal

assertions	goals
	G1. $(\forall\, \textit{tuple } x, y)\big[rev2(x,\, y) \;=\; reverse(x) \diamond y\big]$

As in the informal proof (Section 9.3) we have a choice among applying skolemization and induction on x and y. In this case we prefer to apply induction on x first, eliminating the quantifier for y later. This order is essential, as we shall explain afterwards.

By the *stepwise induction* rule applied to goal G1, it suffices to prove the conjunction of a base case and an inductive step,

	G2. $(\forall\ tuple\ y)^{\forall}\left[rev2(\langle\,\rangle,\ y) = reverse(\langle\,\rangle) \diamond y\right]$ *and* $\left[\begin{array}{l} if\ \ atom(a)\ \ and\ \ tuple(r) \\ then\ \ if\ \ (\forall\ tuple\ y')\left[\begin{array}{l} rev2(r,\ y') \ = \\ reverse(r) \diamond y' \end{array}\right] \\ \qquad then\ \ (\forall\ tuple\ y'')\left[\begin{array}{l} rev2(a \diamond r,\ y'') \ = \\ reverse(a \diamond r) \diamond y'' \end{array}\right] \end{array}\right]$

The quantified variable y was renamed to clarify the exposition in the following steps.

By the $\forall$-*elimination* rule, we may drop the $(\forall\ tuple\ y)$ quantifier of goal G2, leaving

	G3. $\left[\begin{array}{l} if\ \ tuple(t) \\ then\ \boxed{rev2(\langle\,\rangle,\ t)} \ = \ \boxed{reverse(\langle\,\rangle)} \diamond t \end{array}\right]$ *and* $\left[\begin{array}{l} if\ \ atom(a)\ \ and\ \ tuple(r) \\ then\ \ if\ \ (\forall\ tuple\ y')\left[\begin{array}{l} rev2(r,\ y') \ = \\ reverse(r) \diamond y' \end{array}\right] \\ \qquad then\ \ (\forall\ tuple\ y'')\left[\begin{array}{l} rev2(a \diamond r,\ y'') \ = \\ reverse(a \diamond r) \diamond y'' \end{array}\right] \end{array}\right]$

Note that the bound variable y of goal G2 has been replaced in goal G3 by the skolem constant t.

Base Case

Recall the *left-empty* axiom for *rev*2 and the *empty* axiom for *reverse*,

$if\ \ tuple(y)$ $then\ \left[\boxed{rev2(\langle\,\rangle,\ y)} \ = \ y\right]^{-}$	
$\left[\boxed{reverse(\langle\,\rangle)} \ = \ \langle\,\rangle\right]^{-}$	

By the *equality* rule, applied twice in succession to the two axioms and goal G3, with $\{y \leftarrow t\}$, we obtain

assertions	goals
	G4. $\boxed{tuple(t)}^{+}$ *and* $\left[\begin{array}{l} \textit{if } \boxed{tuple(t)}^{-} \\ \textit{then } t = \langle\ \rangle \diamond t \end{array}\right]$ *and* $[\ \ldots\ ]$

We do not write the last conjunct because it plays no part in this portion of the proof.

The next step illustrates a different way to remove sort conditions, in which we apply the *resolution* rule to an earlier goal rather than an assertion, so we spell out the details here. By the *resolution* rule applied to our earlier goal G3,

assertions	goals
	$\left[\begin{array}{l} \textit{if } \boxed{tuple(t)}^{-} \\ \textit{then } rev2(\langle\ \rangle, t) = reverse(\langle\ \rangle) \diamond t \end{array}\right]$ *and* $[\ \ldots\ ]$

and to goal G4, we may reduce the goal to

assertions	goals
	G5. $t = \boxed{\langle\ \rangle \diamond t}$ *and* $[\ \ldots\ ]$

Recall the *left-empty* axiom for append,

assertions	goals
if $tuple(y)$ *then* $\left[\boxed{\langle\ \rangle \diamond y} = y\right]^{-}$	

By the *equality* rule, applied to the axiom and goal G5, with $\{y \leftarrow t\}$, we may reduce the base case of G5 further, to

assertions	goals
	G6. $\boxed{t = t}^{+}$ *and* $[\ \ldots\ ]$

(The sort condition *tuple*(t) was again removed by applying the *resolution* rule to the earlier goal G3.)

By the reflexivity of equality, we may now drop the first conjunct of goal G6, leaving only the last conjunct, the inductive step

	G7. $\textit{if}\ \textit{atom}(a)\ \textit{and}\ \textit{tuple}(r)$ $\textit{then}\ \textit{if}\ (\forall\, \textit{tuple}\ y') \begin{bmatrix} \textit{rev2}(r,\ y') \ = \\ \textit{reverse}(r) \diamond y' \end{bmatrix}$ $\textit{then}\ (\forall\, \textit{tuple}\ y'') \begin{bmatrix} \textit{rev2}(a \diamond r,\ y'') \ = \\ \textit{reverse}(a \diamond r) \diamond y'' \end{bmatrix}$

Inductive Step

By two applications of the *if-split* rule, and one application of the *and-split* rule, we have

A8. $\textit{atom}(a)$	
A9. $\textit{tuple}(r)$	
A10. $(\forall\, \textit{tuple}\ y')^{\exists} \begin{bmatrix} \textit{rev2}(r,\ y') \ = \\ \textit{reverse}(r) \diamond y' \end{bmatrix}$	

and

	G11. $(\forall\, \textit{tuple}\ y'')^{\forall} \begin{bmatrix} \textit{rev2}(a \diamond r,\ y'') \ = \\ \textit{reverse}(a \diamond r) \ \diamond y'' \end{bmatrix}$

By the $\forall$- and $\exists$-*elimination* rules, we may drop the remaining quantifiers of assertion A10 and goal G11, and then apply the *if-split* rule to the goal, leaving

A12. $\textit{if}\ \textit{tuple}(y')$ $\textit{then}\ \textit{rev2}(r,\ y') \ =$ $\textit{reverse}(r) \diamond y'$	
A13. $\textit{tuple}(s)$	
	G14. $\boxed{\textit{rev2}(a \diamond r,\ s)} \ =$ $\textit{reverse}(a \diamond r) \diamond s$

Note that the bound variable y'' of goal G11 was replaced by the skolem constant s in goal G14. Here assertion A12 corresponds to the induction hypothesis, and goal G14 to the desired conclusion of the inductive step.

Recall the *left-insertion* axiom for *rev*2,

if $atom(u)$ *and* $tuple(x)$ *and* $tuple(y)$ *then* $\left[\boxed{rev2(u \diamond x,\ y)} = rev2(x,\ u \diamond y)\right]^{-}$	

By the *equality* rule, applied to the axiom and goal G14, with $\{u \leftarrow a,\ x \leftarrow r,\ y \leftarrow s\}$, and removal of sort conditions, we obtain

	G15. $rev2(r,\ a \diamond s) = \boxed{reverse(a \diamond r)} \diamond s$

Recall the *insertion* axiom for *reverse*,

if $atom(u)$ *and* $tuple(x)$ *then* $\left[\boxed{reverse(u \diamond x)} = reverse(x) \diamond \langle u \rangle\right]^{-}$	

By the *equality* rule, applied to the axiom and goal G15, with $\{u \leftarrow a,\ x \leftarrow r\}$, and removal of sort conditions, we obtain

	G16. $rev2(r,\ a \diamond s) = \boxed{(reverse(r) \diamond \langle a \rangle) \diamond s}$

Recall the *associativity* property of append,

if $tuple(x)$ *and* $tuple(y)$ *and* $tuple(z)$ *then* $\left[\boxed{(x \diamond y) \diamond z} = x \diamond (y \diamond z)\right]^{-}$	

By the *equality* rule, applied to the property and goal G16, with $\{x \leftarrow reverse(r),\ y \leftarrow \langle a \rangle,\ z \leftarrow s\}$, and removal of sort conditions, we obtain

	G17. $rev2(r,\ a \diamond s) \ = \ reverse(r) \diamond \boxed{\langle a \rangle \diamond s}$

Recall the *singleton* property of append,

if $atom(u)$ *and* $tuple(y)$ *then* $\left[\boxed{\langle u \rangle \diamond y} \ = \ u \diamond y\right]^-$	

By the *equality* rule, applied to the axiom and goal G17, with $\{u \leftarrow a,\ y \leftarrow s\}$, and removal of sort conditions, we obtain

	G18. $\boxed{rev2(r,\ a \diamond s) \ = \ reverse(r) \diamond (a \diamond s)}^+$

Recall our induction hypothesis (assertion A12),

if $tuple(y')$ *then* $\boxed{rev2(r,\ y') \ = \ reverse(r) \diamond y'}^-$	

By the *resolution* rule, applied to the induction hypothesis and goal G18, with $\{y' \leftarrow a \diamond s\}$, we obtain the final goal

	G19. *true*

Now that we have completed the proof of the *general* property of *rev*2,

$$(\forall\, tuple\ x,\ y)\big[rev2(x,\ y) \ = \ reverse(x) \diamond y\big],$$

we may use it as an assertion in the proof of the *special* property of *rev*2,

$$(\forall\, tuple\ x)\big[reverse(x) \ = \ rev2(x,\ \langle\ \rangle)\big].$$

■ *Proof of the Special Property*

We begin with the tableau in which the *general* property of *rev*2 is given as an assertion

assertions	goals
if $tuple(x)$ *and* $tuple(y)$ *then* $\left[\boxed{rev2(x,\ y)} = reverse(x) \diamond y\right]^{-}$	

and the initial goal is the *special* property

	G1. $(\forall\ tuple\ x)^{\forall} \left[\begin{array}{l} reverse(x) = \\ rev2(x,\ \langle\ \rangle) \end{array}\right]$

By the $\forall$-*elimination* rule, we may drop the quantifier of goal G1 and apply the *if-split* rule, leaving

A2. $tuple(s)$	
	G3. $reverse(s) = \boxed{rev2(s,\ \langle\ \rangle)}$

Here the bound variable x of the goal G1 has been replaced by the skolem constant s.

By the *equality* rule, applied to the *general* property of *rev*2 and goal G3, with $\{x \leftarrow s,\ y \leftarrow \langle\ \rangle\}$, and removal of sort conditions, we obtain

	G4. $reverse(s) = \boxed{reverse(s) \diamond \langle\ \rangle}$

Recall the *right-empty* property of append,

if $tuple(x)$ *then* $\left[\boxed{x \diamond \langle\ \rangle} = x\right]^{-}$	

By the *equality* rule, applied to the property and goal G4, with $\{x \leftarrow reverse(s)\}$, and removal of sort conditions, we obtain

	G5. $\boxed{reverse(s) = reverse(s)}^{+}$

By the reflexivity of equality, we obtain the final goal

	G6. *true*

This concludes the proof of the desired *special* property

$$(\forall\, tuple\ x)\big[reverse(x) \;=\; rev2(x, \langle\ \rangle)\big].$$ ┘

Note that, in the proof of the *general* property, we did not apply the ∀-*elimination* rule to remove the second quantifier $(\forall\, tuple\ y)$ in goal G1 until after we had applied the induction principle. This was crucial: had we removed this quantifier too early, the proof would not have succeeded. As it turned out, the induction hypothesis, assertion A12, contained the variable y'. The variable y' was then replaced by the term $a \diamond s$ in resolution with goal G18. Had we removed the quantifier first, the induction hypothesis would have contained a skolem constant instead of the variable y', and this step would have been impossible.

In this example, we mentioned all the properties used in the proof at the beginning. Henceforth, we shall usually not mention such properties until they are used. We shall assume, nevertheless, that they are present in the initial tableau.

Remark (associativity and commutativity). In the example, we obtained goal G17 by applying the *equality* rule to the *associativity* property of append and goal G16. Henceforth we shall not include *associativity* properties explicitly as assertions in our tableaux; rather, we shall say that the new row has been obtained "by associativity" of the operator in question. For instance, we shall say that goal G17 has been obtained from goal G15 by application of the *equality* rule and "the associativity of append," without mentioning the intermediate goal G16 at all.

Similarly, when we use the *commutativity* property of an operator, we shall omit the property and say that the new row has been obtained "by commutativity" of the operator in question. ┘

Proofs of some properties of the append function are requested in **Problem 11.8**. Another property of tuples, that the *reverse* function "distributes" over the append function $\diamond$, is proposed in **Problem 11.9**. A property of a relation over tuples is set forth in **Problem 11.10**.

11.3 TREES

A tableau over the trees is a tableau with equality with the generation axioms

assertions	goals
if $atom(x)$ *then* $tree(x)$ (*atom*)	
if $tree(x)$ *and* $tree(y)$ *then* $tree(x \bullet y)$ (*construction*)	

and the uniqueness axioms

if $tree(x)$ *and* $tree(y)$ *then* *not* $\big(atom(x \bullet y)\big)$ (*atom*)	
if $tree(x_1)$ *and* $tree(x_2)$ *and* $tree(y_1)$ *and* $tree(y_2)$ *then* *if* $x_1 \bullet x_2 = y_1 \bullet y_2$ (*construction*) *then* $x_1 = y_1$ *and* $x_2 = y_2$	

In this theory, we shall use r, s, and t, with or without subscripts, as additional constant symbols.

Because the tableau is with equality, we also include the *reflexivity* axiom $(x = x)$ among our assertions, and we may use the *equality* rule in conducting any proof.

In addition, we include in a tableau over the trees a new deduction rule for stepwise induction. The *stepwise induction* rule for trees allows us to establish a goal of form $(\forall\, tree\ x)\mathcal{F}[x]$ by proving the conjunction of a base case and an inductive step.

Rule (stepwise induction)

For a closed sentence

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

we have

assertions	goals
	$(\forall\, tree\ x)\mathcal{F}[x]$
	$\begin{array}{l} if\ \ atom(a)\ \ then\ \ \mathcal{F}[a] \\ \quad and \\ \left[\begin{array}{l} if\ \ tree(r_1)\ \ and\ \ tree(r_2) \\ then\ \ if\ \ \mathcal{F}[r_1]\ \ and\ \ \mathcal{F}[r_2] \\ \qquad then\ \ \mathcal{F}[r_1 \bullet r_2] \end{array}\right] \end{array}$

where a, r_1, and r_2 are new constants. ▟

Here the conjunct

$$if\ \ atom(a)\ \ then\ \ \mathcal{F}[a]$$

corresponds to the base case, and the conjunct

$$\begin{array}{l} if\ \ tree(r_1)\ \ and\ \ tree(r_2) \\ then\ \ if\ \ \mathcal{F}[r_1]\ \ and\ \ \mathcal{F}[r_2] \\ \qquad then\ \ \mathcal{F}[r_1 \bullet r_2] \end{array}$$

corresponds to the inductive step of an informal induction proof. Note that, as in the other theories, we are permitted to apply the *stepwise induction* rule only if the goal is a closed sentence.

In **Problem 11.11**, the reader is asked to conduct a proof in a combined theory of nonnegative integers, tuples, and trees.

PROBLEMS

Proofs for the problems in this chapter should use the deductive-tableau technique. You may remove sort conditions without spelling out the details.

Many of the problems request tableau proofs of properties that appear in earlier chapters. For these proofs, you may not use properties that appear after the requested property in the earlier chapter. For example, Problem 11.1(c) requests a tableau proof of the *left-successor* property of multiplication, which appears in Chapter 8. In this proof, you may use the *right-successor* axiom for multiplication, which appears before the requested property, but not the *left-distributivity* property of multiplication, which appears afterwards.

Problem 11.1 (multiplication) page 551

Prove the following properties of multiplication in the theory of the nonnegative integers:

(a) *Right one*

$$(\forall\, integer\ x)[x \cdot 1 \ = \ x]$$

Hint: Recall that 1 is a notation for $(0+1)$.

(b) *Left zero*

$$(\forall\, integer\ x)[0 \cdot x \ = \ 0]$$

(c) *Left successor*

$$(\forall\, integer\ x,\ y)\big[(x+1)\cdot y \ = \ x \cdot y + y\big]$$

(d) *Right distributivity*

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

Problem 11.2 (exponentiation) page 551

Prove, in the theory of the nonnegative integers, that the function *exp*3 provides an alternative definition for the exponentiation function x^y, in the sense that

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

Hint: In a separate tableau, first prove a more general property. See the informal proof in Section 8.3.

Problem 11.3 (factorial) page 551

Prove, in the theory of the nonnegative integers, that the function *fact*2 does indeed provide an alternative definition for the factorial function $x!$, in the sense that

$$(\forall\, integer\ x)\big[x! \ = \ fact2(x,\ 1)\big]$$

Hint: Prove a more general property.

Problem 11.4 (fibonacci function) page 551

Suppose the *fibonacci function* $fib(x)$ is defined by the following axioms:

$$fib(0) \ = \ 0 \qquad (zero)$$

$$fib(1) \ = \ 1 \qquad (one)$$

$$(\forall\, integer\ x)\big[fib\big((x+1)+1\big) \ = \ fib(x+1) + fib(x)\big] \qquad (plus\ two)$$

The sequence of successive values $fib(0)$, $fib(1)$, $fib(2)$, $\ldots$, that is, 0, 1, 1, 2, 3, 5, 8, $\ldots$ is known as the *fibonacci sequence.*

Suppose the function $fib3(x, y, z)$ is defined by the following axioms:

$$(\forall\ integer\ y,\ z)\big[fib3(0,\ y,\ z)\ =\ y\big] \qquad (zero)$$

$$(\forall\ integer\ x,\ y,\ z)\big[fib3(x+1,\ y,\ z)\ =\ fib3(x,\ z,\ y+z)\big] \qquad (successor)$$

(a) Prove, in the theory of the nonnegative integers, that

$$(\forall\ integer\ x,\ y,\ z)\big[fib3(x+1,\ y,\ z)\ =\ y \cdot fib(x)\ +\ z \cdot fib(x+1)\big].$$

(b) Prove, in the theory of the nonnegative integers, that the function $fib3$ provides an alternative definition for the fibonacci function, in the sense that

$$(\forall\ integer\ x)\big[fib(x)\ =\ fib3(x,\ 0,\ 1)\big].$$

Problem 11.5 (even) page 551

In the theory of the nonnegative integers, suppose the relation $even(x)$ is defined by the axioms

$$even(0) \qquad (zero)$$

$$not\ even(1) \qquad (one)$$

$$(\forall\ integer\ x)\big[even((x+1)+1)\ \equiv\ even(x)\big] \qquad (plus\ two)$$

Prove that

$$(\forall\ integer\ x)[even(x)\ or\ even(x+1)].$$

Problem 11.6 (A-form) page 552

Justify the A-form of the *stepwise induction* rule for the nonnegative integers.

Problem 11.7 (tuples) page 554

(a) Justify the *stepwise induction* rule for tuples.

(b) Formulate and justify an A-form of the *stepwise induction* rule for tuples.

Problem 11.8 (append) page 562

In the theory of tuples, prove the following properties of the append function:

(a) *Right empty*

$$(\forall\ tuple\ x)[x \diamond \langle\ \rangle\ =\ x]$$

(b) *Associativity*

$$(\forall\ tuple\ x,\ y,\ z)\big[(x \diamond y) \diamond z\ =\ x \diamond (y \diamond z)\big].$$

Problem 11.9 (reverse) page 562

In the theory of tuples, prove that the *reverse* function distributes over the append function $\diamond$, that is,

$$(\forall\ tuple\ x,\ y)\big[reverse(x \diamond y)\ =\ reverse(y) \diamond reverse(x)\big]\quad (append)$$

Hint: Use the results of Problem 11.8.

Problem 11.10 (initial subtuple) page 562

In the theory of tuples, show that the initial-subtuple relation $x \preceq_{init} y$ does indeed hold if and only if x is an initial subtuple of y, that is, the sentence

$$(\forall\ tuple\ x,\ y)\begin{bmatrix} x \preceq_{init} y \\ \equiv \\ (\exists\ tuple\ z)[x \diamond z\ =\ y] \end{bmatrix}\quad (append)$$

is valid.

Hint: Prove each direction separately.

Problem 11.11 (length of flattree) page 564

Consider a combined theory of the nonnegative integers, tuples, and trees. In this theory, suppose that the function $tips(x)$, which counts the number of leaves in a tree x, is defined as in Problem 10.5. Prove that

$$(\forall\ tree\ x)\big[length\big(flattree(x)\big)\ =\ tips(x)\big].$$