5.3 Course of Values Recursion

5.3.1 The principle of complete induction. For every formula $\varphi[x]$, the formula of *complete induction on x for φ* is the following one:

$$\forall x\big(\forall y(y < x \to \varphi[y]) \to \varphi[x]\big) \to \forall x \varphi[x]. \tag{1}$$

It is assumed here that the variable y is different from the induction variable x and it does not occur freely in φ. The induction formula φ may contain additional variables as parameters.

5.3.2 Theorem *The principle of complete induction holds for each formula.*

Proof. The principle of complete induction 5.3.1(1) is reduced to mathematical induction as follows. Under the assumption that φ is *progressive*:

$$\forall x\big(\forall y(y < x \to \varphi[y]) \to \varphi[x]\big), \tag{$\dagger_1$}$$

we first prove, by induction on n, the auxiliary property:

$$\forall z(z < n \to \varphi[z]). \tag{$\dagger_2$}$$

In the base case there is nothing to prove. In the induction step take any $z < n + 1$ and consider two cases. If $z < n$ then we obtain $\varphi[z]$ by IH. If $z = n$ then by instantiating of ($\dagger_1$) with $x := z$ we obtain

$$\forall y(y < n \to \varphi[y]) \to \varphi[z].$$

Now we apply IH to get $\varphi[z]$.

With the auxiliary property proved we obtain that $\varphi[x]$ holds for every x by instantiating of $\forall n(\dagger_2)$ with $n := x + 1$ and $z := x$. □

5.3.3 Integer division. Consider the following course of values recursive definition on x of the integer division $x \div y$:

$$x \div 0 = 0$$
$$x \div y = 0 \leftarrow y \neq 0 \land x < y$$
$$x \div y = (x \dot{-} y) \div y + 1 \leftarrow y \neq 0 \land x \geq y.$$

We claim that

$$\vdash_{\mathrm{PA}} \; y \neq 0 \to \exists r(x = x \div y \cdot y + r \land r < y). \tag{1}$$

Verification. The property is proved by complete induction on x. Assume $y \neq 0$, take any x and consider two cases. If $x < y$ then we satisfy (1) with substitution $r := x$ since we clearly have

$$x = 0 \cdot y + x = x \div y \cdot y + x.$$

If $x \geq y$ then $x \dot{-} y < x$ and thus from IH applied to $x \dot{-} y$ there is a number r such that

$$x \dot{-} y = (x \dot{-} y) \div y \cdot y + r \land r < y. \qquad (\dagger_1)$$

Now we satisfy (1) with substitution $r := r$ because

$$\begin{aligned} x = x \dot{-} y + y &\overset{(\dagger_1)}{=} (x \dot{-} y) \div y \cdot y + y + r = \\ &= \big((x \dot{-} y) \div y + 1\big)y + r = x \div y \cdot y + r. \end{aligned}$$

□

5.3.4 Divisibility predicate. The binary divisibility predicate $x \mid y$ is introduced into PA explicitly by

$$x \mid y \leftrightarrow \exists z\, y = xz.$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} x \mid x \qquad (1)$$
$$\vdash_{\mathrm{PA}} x \mid y \rightarrow y \mid x \qquad (2)$$
$$\vdash_{\mathrm{PA}} x \mid y \land y \mid z \rightarrow x \mid z \qquad (3)$$
$$\vdash_{\mathrm{PA}} 0 \mid x \leftrightarrow x = 0 \qquad (4)$$
$$\vdash_{\mathrm{PA}} x \mid 0 \qquad (5)$$
$$\vdash_{\mathrm{PA}} 1 \mid x \qquad (6)$$
$$\vdash_{\mathrm{PA}} x \mid 1 \leftrightarrow x = 1 \qquad (7)$$
$$\vdash_{\mathrm{PA}} x \mid y \land x \mid y + 1 \rightarrow x = 1 \qquad (8)$$
$$\vdash_{\mathrm{PA}} x \mid y \land x \mid z \rightarrow x \mid y + z \qquad (9)$$
$$\vdash_{\mathrm{PA}} x \mid y \land x \mid z \rightarrow x \mid y \dot{-} z \qquad (10)$$
$$\vdash_{\mathrm{PA}} x \mid y \rightarrow x \mid yz \qquad (11)$$
$$\vdash_{\mathrm{PA}} x \mid xy \qquad (12)$$
$$\vdash_{\mathrm{PA}} x \neq 0 \land y \mid x \rightarrow y \leq x. \qquad (13)$$

5.3.5 Greatest common divisor. Consider the following recursive definition of the greatest common divisor function:

$\mathrm{gcd}(0, y) = y$
$\mathrm{gcd}(x, y) = \mathrm{gcd}(y \bmod x, x) \leftarrow x \neq 0.$

The definition of $\mathrm{gcd}(x, y)$ is by course of values recursion on x with substitution in parameter because

$$\vdash_{\mathrm{PA}} x \neq 0 \rightarrow y \bmod x < x.$$

The idea of the algorithm is based on the observation that

$$\vdash_{\mathrm{PA}} x \neq 0 \land z \mid x \to z \mid y \leftrightarrow z \mid y \bmod x. \tag{1}$$

We claim that

$$\vdash_{\mathrm{PA}} x \neq 0 \lor y \neq 0 \to \gcd(x,y) \mid x \land \gcd(x,y) \mid y \tag{2}$$

$$\vdash_{\mathrm{PA}} (x \neq 0 \lor y \neq 0) \land z \mid x \land z \mid y \to z \leq \gcd(x,y). \tag{3}$$

Verification. (2): By complete induction on x with induction formula $\forall y\,(2)$. Assume $x \neq 0 \lor y \neq 0$ and consider two cases. If $x = 0$ then $y \neq 0$ and the claim

$$y \mid 0 \land y \mid y$$

follows from 5.3.4(5)(1). If $x \neq 0$ then by IH applied to $y \bmod x < x$ we obtain

$$\gcd(y \bmod x, x) \mid y \bmod x \land \gcd(y \bmod x, x) \mid x.$$

From definition

$$\gcd(x,y) \mid y \bmod x \land \gcd(x,y) \mid x.$$

From this and (1) we finally obtain

$$\gcd(x,y) \mid x \land \gcd(x,y) \mid y.$$

Note that the induction hypothesis is applied with x in place of y.

(3): By complete induction on x with induction formulas $\forall y\,(3)$. So assume $x \neq 0 \lor y \neq 0$ holds and take any number z such that

$$z \mid x \land z \mid y. \tag{$\dagger_1$}$$

We consider two cases. If $x = 0$ then $y \neq 0$ and the claim $z \leq y$ follows from 5.3.4(13). If $x \neq 0$ then by (1) we obtain from ($\dagger_1$) that

$$z \mid y \bmod x \land z \mid x.$$

Now by IH applied to $y \bmod x < y$ we have

$$z \leq \gcd(y \bmod x, x) = \gcd(x,y).$$

Note that the induction hypothesis is applied with x in place of y. □