Gödel's Second Incompleteness Theorem

Abbreviation. We use $\mu x[\varphi(x)]$ to abbreviate

$$\varphi(x) \wedge (\forall x' < x)\neg\varphi(x').$$

Proposition (That Has Been Proven). *The following are derivable from* Φ_{PA}*:*

(a) $\neg \boldsymbol{m} \equiv \boldsymbol{n}$, *for* $m, n \in \mathbb{N}$ *and* $m \neq n$.

(b) $\forall x(0 + x \equiv x)$.

(c) $\forall x \forall y((x + 1) + y \equiv x + (y + 1))$.

(d) $\forall x \forall y(x + y \equiv x \rightarrow y \equiv 0)$.

(e) $\forall x(x < \boldsymbol{n+1} \rightarrow \neg x \equiv \boldsymbol{n+1})$, *for* $n \in \mathbb{N}$.

(f) $(\forall x < \boldsymbol{n+1}) \bigvee_{i=0}^{n} x \equiv \boldsymbol{i}$, *for* $n \in \mathbb{N}$.

(g) $\forall x(\neg x \equiv 0 \rightarrow \exists y\ x \equiv y + 1)$.

(h) $\forall x(1 + x \equiv x + 1)$.

(i) $\forall x(x \equiv 0 \vee 0 < x)$.

(j) $\forall x \forall y(\neg x \equiv y \rightarrow (x < y \vee y < x))$.

(k) $\boldsymbol{m} + \boldsymbol{n} \equiv \boldsymbol{(m+n)}$, *for* $m, n \in \mathbb{N}$.

(l) $\boldsymbol{m} \cdot \boldsymbol{n} \equiv \boldsymbol{(m \cdot n)}$, *for* $m, n \in \mathbb{N}$.

(m) $\forall x(\neg x \equiv \boldsymbol{n} \rightarrow (x < \boldsymbol{n} \vee \boldsymbol{n} < x))$, *for* $n \in \mathbb{N}$.

(n) $\forall x \forall y(x < y \rightarrow \neg(x \equiv y \vee y < x))$.

(o) $\forall x \forall y \forall z(x + z \equiv y + z \rightarrow x \equiv y)$.

Propositions (That Has Not Yet Been Proven). *The following are derivable from* Φ_{PA}*:*

(1) $0 \le x$

(2) $(x < y \wedge y < z) \rightarrow x < z$

(3) $\neg x < x$

(4) $(x \le y \wedge y \le x) \rightarrow x \equiv y$

(5) $x < y \rightarrow x + 1 < y + 1$

(6) $x < y \leftrightarrow x + 1 \le y$

(7) $x < y \vee x \equiv y \vee y < x$

(8) $x + y \equiv y + x$

(9) $x + (y + z) \equiv (x + y) + z$

(10) $x \cdot y \equiv y \cdot x$

(11) $x \cdot (y \cdot z) \equiv (x \cdot y) \cdot z$

(12) $x \cdot (y + z) \equiv (x \cdot y) + (x \cdot z)$

(13) $x < y \rightarrow x + z < y + z$

(14) $x + z < y + z \rightarrow x < y$

(15) $0 < z \rightarrow x + 1 \le x + z$

(16) $(0 < z \wedge x < y) \rightarrow x \cdot z < y \cdot z$

(17) $(0 < z \wedge x \cdot z \equiv y \cdot z) \rightarrow x \equiv y$

(18) $(x < y \wedge z < w) \rightarrow x + z < y + w$

(19) $(x < y \wedge z < w) \rightarrow x \cdot z < y \cdot w$

Proposition.

(1) $\Phi_{\mathrm{PA}} \vdash \underline{m} + \underline{n} \equiv \underline{m + n}$

(2) $\Phi_{\mathrm{PA}} \vdash \underline{m \cdot n} \equiv \underline{m} \cdot \underline{n}$

Proof. (INCOMPLETE) We use induction on n in both cases.

For (1), the base case $n = 0$ is trivial since $\forall x\ x + 0 \equiv x \in \Phi_{\mathrm{PA}}$. For the inductive case $n = k+1$, the terms $\underline{m}+\underline{k+1}, (\underline{m}+\underline{k})+1, (\underline{m+k})+1 = \underline{(m+k)+1} = \underline{m+(k+1)}$ are provably equivalent in Φ_{PA}, using (9) in the above proposition and induction hypothesis.

For (2), the base case $n = 0$ is trivial since $\forall x\ x \cdot 0 \equiv 0 \in \Phi_{\mathrm{PA}}$. For the inductive case $n = k + 1$, the terms $\underline{m} \cdot \underline{k+1}, (\underline{m} \cdot \underline{k}) + \underline{m}, \underline{m \cdot k} + \underline{m}, \underline{(m \cdot k) + m} = \underline{m \cdot (k+1)}$ are provably equivalent in Φ_{PA}, using the fact that $\forall x \forall y\ x \cdot (y+1) \equiv x \cdot y + x \in \Phi_{\mathrm{PA}}$, induction hypothesis and the result obtained in (1). $\square$

Proposition. *Let t be a variable-free S_{ar}-term, i.e. an S_{ar}-term in which no variable occurs; we write $t^{\mathfrak{N}}$ for the evaluation of t in $\mathfrak{N}$ (e.g. $(1+1)^{\mathfrak{N}} = 2$). Then*

$$\Phi_{\mathrm{PA}} \vdash t \equiv \underline{t^{\mathfrak{N}}}.$$

Proof. The claim is proven by induction on t: It is clear for $t = 0$ or $t = 1$; for $t = t_1 + t_2$ or $t = t_1 \cdot t_2$, the claim follows by induction hypothesis and the above proposition. $\square$

Lemma on Primitive Recursive Functions. *Every primitive recursive function is Σ_1-definable. Moreover, if f is defined by primitive recursion on g and h, then the recursion equations are provable.*

Lemma on Course-of-Values Induction. *For any formula φ, the following is derivable in Φ_{PA}:*

$$\forall x((\forall y < x)\varphi\tfrac{y}{x} \to \varphi) \to \forall x\varphi.$$

Lemma on the Least Principle. *For any formula φ, the following is derivable in Φ_{PA}:*

$$\exists x\varphi \to \exists x(\varphi \wedge (\forall y < x)\neg\varphi\tfrac{y}{x}).$$

Proof. (INCOMPLETE) Immediately follows from the above lemma. $\square$

Proposition.
$$\Phi_{\mathrm{PA}} \vdash \exists z(x \equiv y + z \vee x < y).$$

Thus, it is valid to introduce the following function:

Definition. The binary function $sub(m, n)$ returns the value $m - n$ if $m \geq n$ and 0 otherwise; it is the least d such that ($m = n + d$ or $m < n$).

It is represented by $sub(x, y) \equiv z$:
$$\mu z[x \equiv y + z \vee x < y].$$

Proposition. *The following are derivable from Φ_{PA}:*

(a) $x < y \to sub(x, y) \equiv 0$

(b) $x \geq y \to x \equiv y + sub(x, y)$

(c) $z \cdot sub(x, y) \equiv sub(z \cdot x, z \cdot y)$

Proposition.
$$\Phi_{\mathrm{PA}} \vdash \exists u \exists z \; x \equiv y \cdot z + u.$$

This proposition triggers the following definition:

Definition. The binary function $rem(m, n)$ returns the remainder of m divided by n if $n > 0$ and m otherwise; it is the least r such that there is a q with $m = n \cdot q + r$.

It is represented by $rem(x, y) \equiv z$:
$$\mu z[\exists u \; x \equiv y \cdot u + z].$$

Definition. The binary function $div(m, n)$ returns the quotient of m divided by n if $n > 0$ and 0 otherwise; it is the least q such that $m = n \cdot q + rem(m, n)$.

It is represented by $div(x, y) \equiv z$:
$$\mu z[x \equiv y \cdot z + rem(x, y)].$$

Abbreviation. The formula $\varphi_{div}(x, y)$ states that x divides y:

$$rem(x, y) \equiv 0.$$

Proposition.

$$\Phi_{\text{PA}} \vdash \varphi_{div}(y, cut(x, rem(x, y))).$$

Proposition.

$$\Phi_{\text{PA}} \vdash \varphi_{div}(x, y) \to \exists z\ x \cdot z \equiv x.$$

Proposition.

$$\Phi_{\text{PA}} \vdash (0 < x \wedge \varphi_{div}(y, x)) \to y \leq x.$$

Definition. The unary function $exp(m, n)$ returns the nth power m^n of m (where $m^0 := 1$ for any m).

The formula $exp(x, y) \equiv z$ is represented by

$$\begin{aligned}
&\exists t(\exists p < t)\\
&(\beta(t, p, 0) \equiv 1 \wedge\\
&\ (\forall u < y)\beta(t, p, u + 1) \equiv \beta(t, p, u) \cdot x \wedge\\
&\ \beta(t, p, y) \equiv z).
\end{aligned}$$

Definition. The unary function $fact(n)$ returns n factorial.

The formula $fact(x) \equiv y$ is represented by

$$\begin{aligned}
&\exists t(\exists p < t)\\
&(\beta(t, p, 0) \equiv 1 \wedge\\
&\ (\forall u < x)\beta(t, p, u + 1) \equiv \beta(t, p, u) \cdot (u + 1) \wedge\\
&\ \beta(t, p, x) \equiv y).
\end{aligned}$$

Proposition.

$$\Phi_{\text{PA}} \vdash \varphi_{div}(fact(x), fact(x + y)).$$

Proof. First, it is clear that

$$\Phi_{\mathrm{PA}} \vdash \varphi_{div}(fact(x), fact(x+0))$$

since $\Phi_{\mathrm{PA}} \vdash x + 0 \equiv x$.

Next, assume

$$\Phi_{\mathrm{PA}} \vdash \varphi_{div}(fact(x), fact(x+y)).$$

Then

$$\Phi_{\mathrm{PA}} \vdash \exists z \; fact(x) \cdot z \equiv fact(x+y).$$

Since

$$\Phi_{\mathrm{PA}} \vdash fact(x+(y+1)) \equiv (x+(y+1)) \cdot fact(x+y),$$

it follows that

$$\Phi_{\mathrm{PA}} \vdash \exists u \; fact(x) \cdot u \equiv fact(x+(y+1)),$$

namely

$$\Phi_{\mathrm{PA}} \vdash \varphi_{div}(fact(x), fact(x+(y+1))).$$

The proposition holds by induction scheme. ∎

Proposition.

$$\Phi_{\mathrm{PA}} \vdash 0 < x \to (\forall y \leq x)(0 < y \to \varphi_{div}(y, fact(x))).$$

Abbreviation. Let $\varphi_{prm}(x)$ abbreviate

$$1 < x \land (\forall y \leq x)((1 < y \land \varphi_{div}(y, x)) \to y \equiv x).$$

Proposition.

$$\Phi_{\mathrm{PA}} \vdash (\varphi_{prm}(x) \land \varphi_{prm}(y) \land \varphi_{div}(y, fact(x)+1)) \to x < y.$$

Proposition.

$$\Phi_{\mathrm{PA}} \vdash 1 < x \to (\exists y \leq x)(\varphi_{prm}(y) \land \varphi_{div}(y, x)).$$

Proposition.

$$\Phi_{\text{PA}} \vdash \varphi_{prm}(x) \to (\exists y \leq fact(x)+1)(\varphi_{prm}(y) \wedge x < y).$$

Definition. Let the unary function $prime(n)$ be defined by the following primitive recursion equation:

$$\begin{array}{lcl} prime(0) & := & 2 \\ prime(n+1) & := & \mu q \leq fact(prime(n))+1[\varphi_{prm}(q) \wedge prime(n) < q]. \end{array}$$

The formula $prime(x) \equiv y$ is represented by

$$\begin{array}{l} \exists t(\exists p < t) \\ (\beta(t,p,0) \equiv 2 \wedge \\ \ (\forall u < x)\beta(t,p,u+1) \equiv f(\beta(t,p,u)) \wedge \\ \ \beta(t,p,x) \equiv y), \end{array}$$

where $f(x) \equiv y$ is represented by

$$\mu y \leq fact(x)+1[\varphi_{prm}(y) \wedge x < y].$$