Gödel's Second Incompleteness Theorem.

Let $S_{\mathrm{ar}'} := S_{\mathrm{ar}} \cup \{?\}$, and $\Phi'_{\mathrm{PA}} := \Phi_{\mathrm{PA}} \cup \Delta$, where $\Delta :=?$ is an extension by definitions.

1. **Encoding Pairs over $\mathbb{N}$.** The mapping $\pi : \mathbb{N}^2 \to \mathbb{N}$,

$$\pi(m,n) := \frac{1}{2}(m+n)(m+n+1)+m$$

is bijective. Notice that for $m, n \in \mathbb{N}$,

$$\begin{array}{rcl} m & \leq & \pi(m,n), \text{ and} \\ n & \leq & \pi(m,n). \end{array}$$

2. **Encoding Finite Sets over $\mathbb{N}$.** (Due to Hinman) For the nonempty set $\{a_0, \ldots, a_r\}$, take the number

$$\sum_{i=0}^{r} 2^{a_i}.$$

Take the number 0 for $\emptyset$. This is a bijective mapping from finite sets over $\mathbb{N}$ to $\mathbb{N}$.

3. **Encoding Nonempty Finite Sequences over $\mathbb{N}$.** For the nonempty sequence $\langle a_0, \ldots, a_r \rangle$, take the number

$$\left(\prod_{i=0}^{r-1} p_i^{a_i}\right) \cdot p_r^{a_r+1} - 2.$$

It is easy to verify that there is a bijective mapping from $\mathbb{N}$ to finite nonempty sequences over $\mathbb{N}$. (In this context, we shall assume that sequences are nonempty.)

4. **A Bijective Gödel Numbering of S_{ar}-Terms.** The mapping $G_T : T^{S_{\mathrm{ar}}} \to \mathbb{N}$,

$$\begin{array}{lcl} G_T(0) & := & 0; \\ G_T(1) & := & 1; \\ G_T(v_n) & := & 3n+2; \\ G_T(t_1+t_2) & := & 3\pi(G_T(t_1), G_T(t_2)) + 3; \\ G_T(t_1 \cdot t_2) & := & 3\pi(G_T(t_1), G_T(t_2)) + 4 \end{array}$$

is bijective.

5. **A Bijective Gödel Numbering of S_{ar}-Formulas.** The mapping $G_F : L^{S_{\mathrm{ar}}} \to \mathbb{N}$,

$$\begin{array}{lcl} G_F(t_1 \equiv t_2) & := & 4\pi(G_T(t_1), G_T(t_2)); \\ G_F(\neg\varphi) & := & 4G_F(\varphi) + 1; \\ G_F(\varphi \vee \psi) & := & 4\pi(G_F(\varphi), G_F(\psi)) + 2; \\ G_F(\exists v_n \varphi) & := & 4\pi(n, G_F(\varphi)) + 3 \end{array}$$

is bijective.

6. **Encoding Sequents and Derivations.** We shall regard a derivation as a nonempty finite sequence $\langle \sigma_0, \ldots, \sigma_n \rangle$ in which σ_i is the $(i+1)$st sequent, $0 \le i \le n$. Each $\sigma_i = (a_i, s_i)$ consists of an antecedent a_i (a possibly empty *set* of formulas) and a succedent s_i (a formula).

   If we encode formulas by means of a Gödel numbering, then naturally sets of formulas, sequents, and derivations can be encoded by natural numbers.

7. **Lemma.** *Let*

$$\varphi(x) := (\psi \wedge \chi(x)) \vee (\neg\psi \wedge \delta(x)),$$

   be an S_{ar}-formula in which

$$\begin{array}{rcl} \psi & \vdash & \exists^{=1} x \chi(x), \\ \neg\psi & \vdash & \exists^{=1} x \delta(x), \end{array}$$

   and x does not occur free in ψ. Then $\vdash \exists^{=1} x \varphi(x)$.

   Proof. It suffices to show $\psi \vdash \exists^{=1} x \varphi(x)$ and $\neg\psi \vdash \exists^{=1} x \varphi(x)$. We shall give a derivation for $\psi \vdash \exists^{=1} x \varphi(x)$ below; the case $\neg\psi \vdash \exists^{=1} x \varphi(x)$ is symmetrical.

1.	$\psi\ \exists^{=1} x \chi(x)$	premise
2.	$\psi\ \psi$	(Assm)
3.	$\psi\ \neg\neg\psi$	IV.3.6(a1) applied to 2.
4.	$\psi\ (\neg\neg\psi \vee \neg\delta(y))$	($\vee$S) applied to 4. with $y \notin \mathrm{free}(()\varphi(x))$
5.	$\psi\ (\neg\neg\psi \vee \neg\delta(z))$	($\vee$S) applied to 4. with $y \neq z \notin \mathrm{free}(()\varphi(x$
6.	$\psi\ \varphi(y)\ \varphi(y)$	(Assm)
7.	$\psi\ \varphi(y)\ (\psi \wedge \chi(y))$	IV.3.5 applied to 6. and 4.
8.	$\psi\ \varphi(y)\ \chi(y)$	IV.3.6(d2) applied to 7.
9.	$\psi\ \varphi(z)\ \varphi(z)$	(Assm)
10.	$\psi\ \varphi(z)\ (\psi \wedge \chi(z))$	IV.3.5 applied to 9. and 5.
11.	$\psi\ \varphi(z)\ \chi(z)$	IV.3.6(d2) applied to 10.
12.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))$	(Assm), $u \notin \mathrm{free}(()\varphi(x)) \cup \{y, z\}$
13.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(u)$	IV.3.6(d1) applied to 12.
14.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \psi$	(Assm)
15.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \psi \wedge \chi(u)$	IV.3.6(b) applied to 14. and 13.
16.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv y))\ \varphi(u)$	($\vee$S) applied to 15.
17.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \exists x \varphi(x)$	($\exists$S) applied to 16.
18.	$\psi\ \exists^{=1} x \chi(x)\ \exists x \varphi(x)$	($\exists$A) applied to 17.
19.	$\psi\ \exists x \varphi(x)$	(Ch) applied to 1. and 18.
20.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \forall v(\chi(v) \to v \equiv u)$	IV.3.6(d2) applied to 12.
21.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ (\chi(y) \to y \equiv u)$	IV.5.5(a1) applied to 20.
22.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ (\chi(z) \to z \equiv u)$	IV.5.5(a1) applied to 20.
23.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ (\chi(y) \to y \equiv u)$	(Ant) applied to 21.
24.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(z)\ (\chi(z) \to z \equiv u)$	(Ant) applied to 22.
25.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(y)$	(Assm)

26.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(z)\ \chi(z)$	(Assm)
27.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ y \equiv u$	IV.3.5 applied to 23. and 25.
28.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(z)\ z \equiv u$	IV.3.5 applied to 24. and 26.
29.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(z)\ y \equiv u$	(Ant) applied to 27.
30.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(z)\ z \equiv u$	(Ant) applied to 28.
31.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(z)\ u \equiv y$	IV.5.3(a) applied to 29.
32.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(z)\ u \equiv y\ z \equiv y$	(Sub) applied to 30.
33.	$\psi\ (\chi(u) \wedge \forall v(\chi(v) \to v \equiv u))\ \chi(y)\ \chi(z)\ z \equiv y$	(Ch) applied to 31. and 32.
34.	$\psi\ \exists^{=1} x \chi(x)\ \chi(y)\ \chi(z)\ z \equiv y$	($\exists$A) applied to 33.
35.	$\psi\ \chi(y)\ \chi(z)\ \exists^{=1} x \chi(x)$	(Ant) applied to 1.
36.	$\psi\ \chi(y)\ \chi(z)\ \exists^{=1} x \chi(x)\ z \equiv y$	(Ant) applied to 34.
37.	$\psi\ \chi(y)\ \chi(z)\ z \equiv y$	(Ch) applied to 35. and 36.
38.	$\psi\ \varphi(y)\ \chi(y)\ \chi(z)\ z \equiv y$	(Ant) applied to 37.
39.	$\psi\ \varphi(y)\ \chi(y)\ (\chi(z) \to z \equiv y)$	IV.3.6(c) applied to 38.
40.	$\psi\ \varphi(y)\ (\chi(z) \to z \equiv y)$	(Ch) applied to 8. and 39.
41.	$\psi\ \varphi(y)\ \varphi(z)\ \chi(z)$	(Ant) applied to 11.
42.	$\psi\ \varphi(y)\ \varphi(z)\ (\chi(z) \to z \equiv y)$	(Ant) applied to 40.
43.	$\psi\ \varphi(y)\ \varphi(z)\ z \equiv y$	IV.3.5 applied to 42. and 41.
44.	$\psi\ \varphi(y)\ (\varphi(z) \to z \equiv y)$	IV.3.6(c) applied to 43.
45.	$\psi\ \varphi(y)\ \forall z(\varphi(z) \to z \equiv y)$	IV.5.5(b4) applied to 44.
46.	$\psi\ \varphi(y)\ (\varphi(y) \wedge \forall z(\varphi(z) \to z \equiv y))$	IV.3.6(b) applied to 6. and 45.
47.	$\psi\ \varphi(y)\ \exists^{=1} x \varphi(x)$	($\exists$S) applied to 46.
48.	$\psi\ \exists x \varphi(x)\ \exists^{=1} x \varphi(x)$	($\exists$A) applied to 47.
49.	$\psi\ \exists^{=1} x \varphi(x)$	(Ch) applied to 19. and 48.

8. **Corollary.** *If*

$$\vdash \varphi(x) \leftrightarrow ((\psi_0 \wedge \chi_0(x)) \vee \ldots \vee (\psi_{n+1} \wedge \chi_{n+1}(x))),$$

and for $0 \leq p < q \leq n+1$,

$$\vdash \neg\psi_p \vee \neg\psi_q,$$

and if

$$\vdash \bigvee_{k=0}^{n+1} \psi_k,$$

then

$$\vdash \exists^{=1} x \varphi(x).$$

9. **Corollary.** *Let*

$$\varphi(x_0, \ldots, x_{n-1}, x) := (\psi \wedge \chi(x_0, \ldots, x_{n-1}, x)) \vee (\neg\psi \wedge \delta(x_0, \ldots, x_{n-1}, x)),$$

be an S_{ar}*-formula in which*

$$\begin{array}{rcl} \psi & \vdash & \exists^{=1} x \chi(x_0, \ldots, x_{n-1}, x), \\ \neg\psi & \vdash & \exists^{=1} x \delta(x_0, \ldots, x_{n-1}, x), \end{array}$$

and x *does not occur free in* ψ. *Then* $\vdash \forall x_0 \ldots \forall x_{n-1} \exists^{=1} x \varphi(x_0, \ldots, x_{n-1}, x)$.

10. **Lemma.** (Course-of-Values Induction) *Let* φ *be an* S_{ar}*-formula. Then*

$$\Phi_{\mathrm{PA}} \vdash \forall x((\forall y < x)\varphi\frac{y}{x} \to \varphi) \to \forall x\varphi.$$

11. **Lemma.** *Let* φ *be an* S_{ar}*-formula, then*

$$\Phi_{\mathrm{PA}} \cup \{\exists x\varphi\} \vdash \exists x(\varphi \wedge \forall(y < x)\neg\varphi\frac{y}{x}).$$

Furthermore we have

$$\Phi_{\mathrm{PA}} \cup \{\exists x\varphi\} \vdash \exists^{=1} x(\varphi \wedge \forall(y < x)\neg\varphi\frac{y}{x}).$$

Proof. Since

$$\Phi_{\mathrm{PA}} \vdash \forall x((\forall y < x)\neg\varphi\frac{y}{x} \to \neg\varphi) \to \forall x\neg\varphi.$$

12. **Definition.** A function $f : \mathbb{N}^n \to \mathbb{N}$ is Σ_1-*definable* if there is a Σ_1-formula $\varphi(v_0, \ldots, v_{n-1}, v_n)$ such that

(1) For all $a_0, \ldots, a_{n-1} \in \mathbb{N}$, $\Phi_{\mathrm{PA}} \vdash \varphi(\boldsymbol{a_0}, \ldots, \boldsymbol{a_{n-1}}, \boldsymbol{f(a_0, \ldots, a_{n-1})})$;

(2) $\Phi_{\mathrm{PA}} \vdash \forall v_0 \ldots \forall v_{n-1} \exists^{=1} v_n \varphi(v_0, \ldots, v_{n-1}, v_n)$.

13. **Lemma.** β*-function is* Σ_1*-definable.*
Proof. Since

$$\chi(u, q, j, a) \vdash (a < q) \wedge \chi(u, q, j, a)$$

and thus

$$\chi(u, q, j, a) \vdash (\exists e < q)\chi(u, q, j, e),$$

it follows that $\varphi_\beta(u, q, j, a)$ is equivalent to

$$((\exists e < q)\chi(u, q, j, e) \wedge \chi(u, q, j, a) \wedge (\forall e < a)\neg\chi(u, q, j, e)) \vee ((\forall e < a)\neg\chi(u, q, j, e) \wedge a \equiv 0).$$

Moreover,

$$(\exists e < q)\chi(u, q, j, e) \vdash \exists^{=1} x(\chi(u, q, j, x) \wedge (\forall e < x)\neg\chi(u, q, j, x))$$

and

$$(\forall e < q)\neg\chi(u, q, j, e) \vdash \exists^{=1} x\ x \equiv 0.$$

From **Lemma 1** we have that

$$\vdash \exists^{=1} x\varphi_\beta(u, q, j, x)$$

and further that

$$\vdash \forall v_0 \forall v_1 \forall v_2 \exists^{=1} v\varphi_\beta(v_0, v_1, v_2, v).$$

Finally, notice that $\varphi_\beta \in \Delta_0$, so φ_β represents the β-function. The proof is complete.

14. **Lemma.** *If $f : \mathbb{N} \to \mathbb{N}$ is Σ_1-definable by an S_{ar}-formula $\varphi_f(v_0, v_1)$, then*

$$\Phi_{\mathrm{PA}} \vdash \forall n \exists t (\exists p < t)(\forall i \leq n) \varphi_f(i, \beta(t, p, i)).$$

Proof. (INCOMPLETE.)

15. **Definition.** Let R be an $(n+1)$-ary relation over $\mathbb{N}$, then we say the $(n+1)$-ary function

$$F(a_0, \dots, a_n) := \begin{cases} 0 & \text{if } Ra_0 \dots a_n \text{ holds} \\ 1 & \text{otherwise} \end{cases}$$

is the characteristic function of R.

16. **Lemma.** *Let $\exists x_0 \dots \exists x_n \varphi$ be a Σ_1-formula in which φ is Δ_0. Then there is a Δ_0-formula ψ such that $\exists x \psi$ is equivalent to $\exists x_0 \dots \exists x_n \varphi$, in which x does not occur.*

Proof. Choose

$$\psi := (\exists x_0 < x) \dots (\exists x_n < x) \varphi.$$ ∎

17. **Lemma.** *Let φ and ψ be Σ_1-formulas, then the following are all equivalent to some Σ_1-formulas:*

(a) $(\varphi \vee \psi)$,

(b) $(\varphi \wedge \psi)$,

(c) $(\exists x < t)\varphi$,

(d) $(\forall x < t)\varphi$,

where in the above $x \notin \mathrm{var}(t)$.

Proof. If φ and ψ are both Δ_0-formulas, then all the assertions are trivial. If both φ and ψ are not Δ_0-formulas, then we may assume without loss of generality that

$$\begin{aligned} \varphi &= \exists u \varphi_0, \text{ and} \\ \psi &= \exists v \psi_0, \end{aligned}$$

where according to the above lemma φ_0 and ψ_0 are Δ_0-formulas and furthermore, $u \neq v$, u does not occur in ψ_0 and v does not occur in φ. The assertions immediately follow:

(a) $(\varphi \vee \psi)$ is equivalent to

$$\exists w (\exists u < w)(\exists v < w)(\varphi_0 \vee \psi_0),$$

where w does not occur in φ or ψ.

(b) Similar to (a).

(c) $(\exists x < t)\varphi$ is equivalent to

$$\exists w (\exists x < t)(\exists u < w)\varphi_0,$$

where w does not occur in $(\exists x < t)\varphi$.

(d) Similar to (c).

As for the other two cases, the proof is similar. $\square$

18. **Lemma.** *Let the n-ary function f be represented by*

$$t \equiv v_n,$$

where t is a term with $\mathrm{var}(t) \subset \{v_0, \ldots, v_{n-1}\}$*. Then f is Σ_1-definable.*

19. **Lemma.** (Composition) *Let $g_1, \ldots, g_m$ be a list of n-ary functions, and h an m-ary function. Also, pick $f : \mathbb{N}^n \to \mathbb{N}$ with*

$$f(a_1, \ldots, a_n) = h(g_1(a_1, \ldots, a_n), \ldots, g_m(a_1, \ldots, a_n)),$$

for $a_1, \ldots, a_n \in \mathbb{N}$.
If $g_1, \ldots, g_m$ and h are all Σ_1-definable, then so is f.

20. **Lemma.** (Primitive Recursion) *Let g and h be n- and $(n+2)$-ary functions, respectively. Also, pick $f : \mathbb{N}^{n+1} \to \mathbb{N}$ with*

$$\begin{aligned} &f(a_1, \ldots, a_n, 0) = g(a_1, \ldots, a_n); \\ &f(a_1, \ldots, a_n, a_{n+1} + 1) = h(a_1, \ldots, a_{n+1}, f(a_1, \ldots, a_n, a_{n+1})), \end{aligned}$$

for $a_1, \ldots, a_{n+1} \in \mathbb{N}$.
If g and h are both Σ_1-definable, then so is f.

21. The characteristic function $F_=$ of the binary relation $m = n$ is Σ_1-defined by the formula

$$F_=(v_0, v_1) \equiv v_2 := (v_0 \equiv v_1 \wedge v_2 \equiv 0) \wedge (\neg v_0 \equiv v_1 \wedge v_2 \equiv 1).$$

22. The characteristic function $F_<$ of the binary relation $m < n$ is Σ_1-defined by the formula

$$F_<(v_0, v_1) \equiv v_2 := (v_0 < v_1 \wedge v_2 \equiv 0) \vee (v_0 \geq v_1 \wedge v_2 \equiv 1).$$

23. The unary relation $R_{Odd}n$ states that n is an odd number:

$$R_{Odd}n \quad \text{iff} \quad \text{there is } m < n \text{ such that } n = 2m + 1.$$

Its characteristic function F_{Odd} is Σ_1-defined by the formula

$$\begin{aligned} F_{Odd}(v_0) \equiv v_1 \quad := \quad &((\exists v_2 < v_0) v_0 \equiv 2 \cdot v_2 + 1 \wedge v_1 \equiv 1) \vee \\ &((\forall v_2 < v_0) \neg v_0 \equiv 2 \cdot v_2 + 1 \wedge v_1 \equiv 0). \end{aligned}$$

24. The binary function $m \dot{-} n$ (cut-off subtraction) returns m minus n if $m \geq n$, otherwise it returns 0:

$$m \dot{-} n := \begin{cases} m - n & \text{if } m \geq n \\ 0 & \text{otherwise.} \end{cases}$$

Since $\Phi_{\mathrm{PA}} \cup \{v_0 \geq v_1\} \vdash \exists^{=1} v_2\, v_1 + v_2 \equiv v_0$, it is Σ_1-defined by

$$v_0 \dot{-} v_1 \equiv v_2 := (v_0 \geq v_1 \wedge v_1 + v_2 \equiv v_0) \vee (v_0 < v_1 \wedge v_2 \equiv 0).$$

25. The unary relation $R_{Div}mn$ states that m divides n:

$$R_{Div}mn \quad \text{iff} \quad \text{there is } k \leq n \text{ such that } m \cdot k = n.$$

Its characteristic function F_{Div} is Σ_1-defined by the formula

$$\begin{array}{rcl} F_{Div}(v_0, v_1) \equiv v_2 & := & ((\exists v_3 \leq v_1) v_0 \cdot v_3 \equiv v_1 \wedge v_2 \equiv 0) \vee \\ & & ((\forall v_3 \leq v_1) \neg v_0 \cdot v_3 \equiv v_1 \wedge v_2 \equiv 1). \end{array}$$

26. **Lemma.** *If the characteristic function F_R of the $(n+1)$-ary relation R is Σ_1-definable, then so is that of its complement.*

Proof. Let $F_{\neg R}$ be the characteristic function, then

$$F_{\neg R}(a_0, \ldots, a_n) = 1 \dot{-} F_R(a_0, \ldots, a_n).$$

∎

27. **Lemma.** *Let P and Q be n-ary and m-ary relations over $\mathbb{N}$, and without loss of generality assume that $n \geq m$. If the charateristic functions of them are both Σ_1-definable, then so are those of the n-ary relations $P \cup Q$ and $P \cap Q$.*

Proof. Let F_P, F_Q, $F_{P\cup Q}$ and $F_{P\cap Q}$ be the characteristic functions of P, Q, $P \cup Q$ and $P \cap Q$, respectively. Then

$$\begin{array}{rcl} F_{P\cup Q}(a_1, \ldots, a_n) & = & F_P(a_1, \ldots, a_n) \cdot F_Q(a_1, \ldots, a_m), \text{ and} \\ F_{P\cap Q}(a_1, \ldots, a_n) & = & 1 \dot{-} (1 \dot{-} F_P(a_1, \ldots, a_n)) \cdot (1 \dot{-} F_Q(a_1, \ldots, a_m)). \end{array}$$

Clearly if F_P and F_Q are both Σ_1-definable, then so are $F_{P\cup Q}$ and $F_{P\cap Q}$. ∎

28. If f is a Σ_1-definable unary function, then the unary function

$$\prod_{m=0}^{n} f(m) := \begin{cases} f(0) & \text{if } n = 0 \\ f(n) \cdot \left(\displaystyle\prod_{m=0}^{n \dot{-} 1} f(m) \right) & \text{otherwise} \end{cases}$$

which takes n as the argument is also Σ_1-definable because

$$\begin{array}{rcl} \displaystyle\prod_{m=0}^{0} f(m) & = & f(0), \text{ and} \\ \displaystyle\prod_{m=0}^{n+1} f(m) & = & f(n+1) \cdot \left(\displaystyle\prod_{m=0}^{n} f(m) \right). \end{array}$$

29. The function n factorial

$$n! := \prod_{m=0}^{n} m$$

is Σ_1-definable.

30. **Lemma.** *If the characteristic function of the* $(n+1)$*-ary relation* R *is* Σ_1*-definable, then so is that of the* $(n+1)$*-ary relation*

"there is some $b \leq a_n$ *such that* $R(a_0, \ldots, a_{n-1}, b)$*".*

Proof. Let F and $F_\exists$ be the characteristic functions of R and of

"there is some $b \leq a_n$ such that $R(a_0, \ldots, a_{n-1}, b)$",

respectively, then

$$F_\exists(a_0, \ldots, a_n) = \prod_{m=0}^{a_n} F(a_0, \ldots, m).$$

Clearly if F is Σ_1-definable, then so is $F_\exists$. ∎

31. **Corollary.** *If the characteristic function of the* $(n+1)$*-ary relation* R *is* Σ_1*-definable, then so is that of the* $(n+1)$*-ary relation*

"for all $b \leq a_n$*,* $R(a_0, \ldots, a_{n-1}, b)$*".*

Proof. Let F and $F_\forall$ be the characteristic functions of R and of

"for all $b \leq a_n$, $R(a_0, \ldots, a_{n-1}, b)$",

respectively, then

$$F_\forall(a_0, \ldots, a_n) = 1 \dot{-} \prod_{m=0}^{a_n} (1 \dot{-} F(a_0, \ldots, m)).$$

Clearly if F is Σ_1-definable, then so is $F_\forall$. ∎

32. **Corollary.** *If the characteristic function of the* $(n+1)$*-ary relation* R *is* Σ_1*-definable, then so is that of the* $(n+1)$*-ary relation*

"there is some $b < a_n$ *such that* $R(a_0, \ldots, a_{n-1}, b)$*".*

Proof. Let F' and F be the characteristic functions of

"there is some $b \leq a_n$ such that $R(a_0, \ldots, a_{n-1}, b)$"

and of

"there is some $b < a_n$ such that $R(a_0, \ldots, a_{n-1}, b)$", respectively, then

$$F(a_0,\dots,a_n) = (1 \dot{-} F_=(0,a_n)) + F_=(0,a_n)\cdot F'(a_0,\dots,a_n \dot{-} 1).$$

Since the characteristic function of R is Σ_1-definable, F' and hence F are Σ_1-definable as well. $\square$

33. **Corollary.** *If the characteristic function of the $(n+1)$-ary relation R is Σ_1-definable, then so is that of the $(n+1)$-ary relation*

"for all $b < a_n$, $R(a_0,\dots,a_{n-1},b)$".

Proof. Let F' and F be the characteristic functions of

"for all $b \le a_n$, $R(a_0,\dots,a_{n-1},b)$"

and of

"for all $b < a_n$, $R(a_0,\dots,a_{n-1},b)$",

respectively, then

$$F(a_0,\dots,a_n) = F_=(0,a_n)\cdot F'(a_0,\dots,a_n \dot{-} 1).$$

Since the characteristic function of R is Σ_1-definable, F' and hence F are Σ_1-definable as well. $\square$

34. **Lemma.** (Bounded Minimalization) *Let f be a Σ_1-definable $(n+1)$-ary function, then the $(n+1)$-ary function*

$$\begin{aligned} &(\mu q < a_n)[f(a_0,\dots,a_{n-1},q)=0] \\ :=\ &\begin{cases} \text{the least } q < a_n \text{ such that } f(a_0,\dots,a_{n-1},q)=0 & \text{if such a } q \text{ exists} \\ a_n & \text{otherwise,} \end{cases} \end{aligned}$$

which takes arguments $a_0,\dots,a_n$, is Σ_1-definable as well.

Proof. Suppose f is Σ_1-definable, then the characteristic function F of the $(n+1)$-ary relation

"there is $q < a_n$ such that $f(a_0,\dots,a_{n-1},q)=0$"

is also Σ_1-definable, and so is the $(n+2)$-ary function

$$g(a_0,\dots,a_n,b) := \begin{cases} b & \text{if } F(a_0,\dots,a_n)=0 \\ a_n & \text{otherwise} \end{cases}$$

since

$$g(a_0,\dots,a_n,b) = (1 \dot{-} F(a_0,\dots,a_n))\cdot b + F(a_0,\dots,a_n)\cdot a_n.$$

It turns out that $\mu q < a_n[f(a_0, \ldots, a_{n-1}, q) = 0]$ is thus Σ_1-definable, because

$$\begin{array}{lcl} (\mu q < 0)[f(a_0, \ldots, a_{n-1}, q) = 0] & = & 0, \text{ and} \\ (\mu q < a_n + 1)[f(a_0, \ldots, a_{n-1}, q) = 0] & = & g(a_0, \ldots, a_n + 1, (\mu q < a_n)[f(a_0, \ldots, a_{n-1}, q) = 0]). \end{array}$$

$\square$

35. **Corollary.** (Enhanced Bounded Minimalization) *Let f and g be Σ_1-definable m-ary and n-ary functions, respectively. Choose $k := \max\{m-1, n\}$, then the k-ary function*

$$\begin{array}{ll} & (\mu q < g(a_1, \ldots, a_n))[f(a_1, \ldots, a_{m-1}, q) = 0] \\ := & \begin{cases} \text{the least } q < g(a_1, \ldots, a_n) \text{ such that } f(a_1, \ldots, a_{m-1}, q) = 0 & \text{if such a } q \text{ exists} \\ g(a_1, \ldots, a_n) & \text{otherwise,} \end{cases} \end{array}$$

which takes $a_1, \ldots, a_k$ as the arguments, is Σ_1-definable.

Proof. Since f is Σ_1-definable, the m-ary function

$$h(a_1, \ldots, a_{m-1}, b) := (\mu q < b)[f(a_1, \ldots, a_{m-1}, q) = 0]$$

is also Σ_1-definable. It follows that the k-ary function

$$(\mu q < g(a_1, \ldots, a_n))[f(a_1, \ldots, a_{m-1}, q) = 0] = h(a_1, \ldots, a_{m-1}, g(a_1, \ldots, a_n))$$

is Σ_1-definable as well. $\square$

36. The function $m \div n$ returns the quotient of m divided by n if $n \neq 0$, otherwise it returns $m+1$:

$$m \div n := \begin{cases} m+1 & \text{if } n = 0; \\ m \dot{-} (\mu k < m+1)[n \cdot (m \dot{-} k) \dot{-} m = 0] & \text{otherwise.} \end{cases}$$

It is Σ_1-definable because

$$m \div n = (1 \dot{-} n) \cdot (m+1) + n \cdot (m \dot{-} (\mu k < m+1)[n \cdot (m \dot{-} k) \dot{-} m = 0])$$

for $m, n \in \mathbb{N}$.

37. The unary relation $R_{Prime}n$ states that n is a prime:

$$R_{Prime}n \quad \text{iff} \quad n > 1 \text{ and for all } m \leq n \dot{-} 1, \text{ if } m \text{ divides } n \text{ then } m = 1.$$

Its characteristic function F_{Prime} is Σ_1-definable because

$$F_{Prime}(n) = 1 \dot{-} (1 \dot{-} F_{<}(1, n)) \cdot \left(\prod_{m=0}^{n \dot{-} 1} (1 \dot{-} (1 \dot{-} F_{Div}(m, n)) \cdot F_{=}(1, m)) \right).$$

38. The unary function $Prime(n)$ returns the $(n+1)$st prime. It is Σ_1-definable because

$$\begin{array}{lcl} Prime(0) & = & 2 \\ Prime(n+1) & = & (\mu m < Prime(n)! + 2)[1 \dot{-} (1 \dot{-} F_{Prime}(m)) \cdot (1 \dot{-} F_<(Prime(n), m)) = 0]. \end{array}$$

39. The exponential function m^n returns the nth power of m:

$$m^n := \begin{cases} 1 & \text{if } n = 0 \\ m \cdot m^{n-1} & \text{otherwise.} \end{cases}$$

It is Σ_1-definable because

$$\begin{array}{lcl} m^0 & = & 1; \\ m^{n+1} & = & m \cdot m^n. \end{array}$$

40. The pairing function $\pi(m, n)$ returns the number encoding the pair (m, n):

$$\pi(m, n) := (((m + n) \cdot (m + n + 1)) \div 2) + m,$$

is Σ_1-definable.

41. The first-component function $\pi_1(n)$ returns the first component of the pair encoded by n:

$$\pi_1(n) := (\mu m < n + 1) \left[\prod_{k=0}^{n} F_=(\pi(m, k), n) = 0 \right],$$

is Σ_1-definable.

42. The second-component function $\pi_2(n)$ returns the second component of the pair encoded by n:

$$\pi_2(n) := (\mu m < n + 1) \left[\prod_{k=0}^{n} F_=(\pi(k, m), n) = 0 \right],$$

is Σ_1-definable.

43. The function $Length(n)$ returns the length of the sequence encoded by n:

$$Length(n) := (n + 3) \dot{-} (\mu m < n + 2)[F_{Div}(Prime(n + 2 \dot{-} m), n + 2) = 0],$$

is Σ_1-definable.

(The least $m < n + 2$ such that $F_{Div}(Prime(n + 2 \dot{-} m), n + 2) = 0$ equals $n + 2 \dot{-} k$, where $F_{Div}(Prime(k), n + 2) = 0$ and for all $k' > k$, $F_{Div}(Prime(k'), n + 2) = 1$.)

44. The function $n[k]$ returns the $(k+1)$st component of the sequence encoded by n:

$$n[k] := \begin{cases} \text{the least } m < n+2 \text{ with } P(m,n,k) & \text{if } k < Length(n) - 1 \\ \text{one less than the least } m < n+2 \text{ with } P(m,n,k) & \text{if } k = Length(n) - 1 \\ n+1 & \text{otherwise,} \end{cases}$$

where the ternary relation $P(m,n,k)$ states that the mth power of the $(k+1)$st prime divides $n+2$ but the $(m+1)$st power does not.

Since the characteristic function

$$F_P(m,n,k) = 1 \dot{-} (1 \dot{-} F_{Div}(Prime(k)^m, n+2)) \cdot F_{Div}(Prime(k)^{m+1}, n+2)$$

of $P(m,n,k)$ is Σ_1-definable, we have

$$\begin{aligned} n[k] = \quad & (1 \dot{-} F_<(k, Length(n) \dot{-} 1)) \cdot (\mu m < n+2)[F_P(m,n,k) = 0] \\ & +(1 \dot{-} F_=(k, Length(n) \dot{-} 1)) \cdot ((\mu m < n+2)[F_P(m,n,k) = 0] \dot{-} 1) \\ & +(1 \dot{-} F_<(Length(n) \dot{-} 1, k)) \cdot (n+1) \end{aligned}$$

is Σ_1-definable as well.

45. The function $m * n$ attaches the sequence encoded by n to the sequence encoded by m:

$$\begin{aligned} m * n \quad := \quad & \Big((m+2) \div Prime(Length(m) \dot{-} 1)\Big) \\ \cdot \quad & \left(\prod_{k=0}^{Length(n) \dot{-} 1} Prime(Length(m) + k)^{n[k]} \right) \\ \cdot \quad & Prime(Length(m) + Length(n) \dot{-} 1) \\ \dot{-} \quad & 2 \end{aligned}$$

is Σ_1-definable.

46. **Lemma.** *The following are derivable:*

(a) $\forall v_0 \forall v_1 Length(v_0 * v_1) \equiv Length(v_0) + Length(v_1)$;

(b) $\forall v_0 \forall v_1 (((v_0 + 2) \div Prime(Length(v_0) \dot{-} 1)) \cdot Prime(Length(v_0))^{v_1+1}) \dot{-} 2 \equiv v_0 * Prime(0)^{v_1+1}$;

(c) $(\forall i < Length(v_0))(v_0 * v_1)[i] \equiv v_0[i]$;

(d) $\forall i (Length(v_0) \leq i \to (v_0 * v_1)[i] \equiv v_1[i \dot{-} Length(v_0)])$.

47.

48. The function $Last(n)$ returns the last component of the sequence encoded by n:

$$Last(n) := n[Length(n) \dot{-} 1]$$

is Σ_1-definable.

49. The binary relation $R_{\in}(m,n)$ states that m is a member of the set encoded by n. Its characteristic function $F_{\in}$ is Σ_1-definable because

$$F_{\in}(m,n) = F_{Odd}(n \div 2^m).$$

50. The function $Max(n)$ returns the maximum element of the set encoded by n if that set is nonempty, otherwise it returns 0:

$$Max(n) := \begin{cases} \text{the maximum } m \text{ with } R_{\in}(m,n) & \text{if } n \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

It is Σ_1-definable because

$$Max(n) = n \dot{-} (\mu k < n+1)[F_{\in}(n \dot{-} k, n) = 0].$$

51. The binary relation $R_{\subset}(m,n)$ states that the set encoded by m is a subset of the set encoded by n:

$$R_{\subset}(m,n) \quad \text{iff} \quad \text{for all } k < m, \text{ if } R_{\in}(k,m) \text{ then } R_{\in}(k,n).$$

Clearly its characteristic function $F_{\subset}$ is Σ_1-definable.

52. The function $m \cup n$ (cf. Fundamentals of Mathematical Logic, Hinman) returns the union of the two sets encoded by m and n:

$$m \cup n := (\mu k < m+n+1)[1 \dot{-} (1 \dot{-} F_{\subset}(m,k)) \cdot (1 \dot{-} F_{\subset}(n,k)) = 0],$$

is Σ_1-definable.

53. The function $m \dot{\setminus} n$ removes the element n from the set encoded by m if n is a member of that set, otherwise it leaves m unchanged:

$$m \dot{\setminus} n := \begin{cases} m \dot{-} 2^n & \text{if } R_{\in}(n,m) \\ m & \text{otherwise.} \end{cases}$$

It is Σ_1-definable because

$$m \dot{\setminus} n = (1 \dot{-} F_{\in}(n,m)) \cdot (m \dot{-} 2^n) + F_{\in}(n,m) \cdot m.$$

54. **Lemma.** (Course-of-Values Recursion)

55. The operation $t\frac{t'}{v_n}$ (simple term substitution) is defined inductively below:

$$\begin{array}{lcl} 0\frac{t}{v_n} & := & 0; \\ 1\frac{t}{v_n} & := & 1; \\ v_m\frac{t}{v_n} & := & \begin{cases} t & \text{if } m = n; \\ v_m & \text{otherwise;} \end{cases} \\ (t_1 + t_2)\frac{t}{v_n} & := & t_1\frac{t}{v_n} + t_2\frac{t}{v_n}; \\ (t_1 \cdot t_2)\frac{t}{v_n} & := & t_1\frac{t}{v_n} \cdot t_2\frac{t}{v_n}. \end{array}$$

The corresponding ternary function $TSbst(m,n,k)$ returns the number encoding $t\frac{t'}{v_n}$, where t and t' have Gödel numbers m and k, respectively. It is defined by

$$\begin{array}{lcl}
TSbst(0,n,k) & := & 0; \\
TSbst(1,n,k) & := & 1; \\
TSbst(3m+2,n,k) & := & \begin{cases} k & \text{if } m = n; \\ 3m+2 & \text{otherwise;} \end{cases} \\
TSbst(3m+3,n,k) & := & 3 \cdot \pi(TSbst(\pi_1(m),n,k), TSbst(\pi_2(m),n,k)) + 3; \\
TSbst(3m+4,n,k) & := & 3 \cdot \pi(TSbst(\pi_1(m),n,k), TSbst(\pi_2(m),n,k)) + 4.
\end{array}$$

It is Σ_1-definable.

56. The operation $\mathrm{var}(t)$ returning the set of all variables occurring in t is defined inductively below:

$$\begin{array}{lcl}
\mathrm{var}(0) & := & \emptyset; \\
\mathrm{var}(1) & := & \emptyset; \\
\mathrm{var}(v_n) & := & \{v_n\}; \\
\mathrm{var}(t_1 + t_2) & := & \mathrm{var}(t_1) \cup \mathrm{var}(t_2); \\
\mathrm{var}(t_1 \cdot t_2) & := & \mathrm{var}(t_1) \cup \mathrm{var}(t_2).
\end{array}$$

The corresponding unary function $TVar(n)$ returns the number encoding $\mathrm{var}(t)$ where t has Gödel number n. It is defined by

$$\begin{array}{lcl}
TVar(0) & := & 0; \\
TVar(1) & := & 0; \\
TVar(3n+2) & := & 2^n; \\
TVar(3n+3) & := & TVar(\pi_1(n)) \cup TVar(\pi_2(n)); \\
TVar(3n+4) & := & TVar(\pi_1(n)) \cup TVar(\pi_2(n)).
\end{array}$$

It is Σ_1-definable.

57. The operation $\mathrm{fvar}(\varphi)$ returning the set of all variables (free or bound) occuring in the formula φ is defined inductively below:

$$\begin{array}{lcl}
\mathrm{fvar}(t_1 \equiv t_2) & := & \mathrm{var}(t_1) \cup \mathrm{var}(t_2); \\
\mathrm{fvar}(\neg\varphi) & := & \mathrm{fvar}(\varphi); \\
\mathrm{fvar}(\varphi \vee \psi) & := & \mathrm{fvar}(\varphi) \cup \mathrm{fvar}(\psi); \\
\mathrm{fvar}(\exists v_n \varphi) & := & \{v_n\} \cup \mathrm{fvar}(\varphi)\,.
\end{array}$$

The corresponding unary function $FVar(n)$ returns the number encoding $\mathrm{fvar}(\varphi)$ where φ has Gödel number n. It is defined by

$$\begin{array}{lcl}
FVar(4n) & := & TVar(\pi_1(n)) \cup TVar(\pi_2(n)); \\
FVar(4n+1) & := & FVar(n); \\
FVar(4n+2) & := & FVar(\pi_1(n)) \cup FVar(\pi_2(n)); \\
FVar(4n+3) & := & 2^{\pi_1(n)} \cup FVar(\pi_2(n)).
\end{array}$$

It is Σ_1-definable.

58. The operation free(φ) returning the set of all free variables of the formula φ is defined inductively below:

$$\begin{array}{lcl} \mathrm{free}(t_1 \equiv t_2) & := & \mathrm{var}(t_1) \cup \mathrm{var}(t_2); \\ \mathrm{free}(\neg\varphi) & := & \mathrm{free}(\varphi); \\ \mathrm{free}(\varphi \vee \psi) & := & \mathrm{free}(\varphi) \cup \mathrm{free}(\psi); \\ \mathrm{free}(\exists v_n \varphi) & := & \mathrm{free}(\varphi) \setminus \{v_n\}. \end{array}$$

The corresponding unary function $Free(n)$ returns the number encoding free(φ) where φ has Gödel number n. It is defined by

$$\begin{array}{lcl} Free(4n) & := & TVar(\pi_1(n)) \cup TVar(\pi_2(n)); \\ Free(4n+1) & := & Free(n); \\ Free(4n+2) & := & Free(\pi_1(n)) \cup Free(\pi_2(n)); \\ Free(4n+3) & := & Free(\pi_2(n)) \mathbin{\dot{\setminus}} \pi_1(n). \end{array}$$

It is Σ_1-definable.

59. The operation rpl(φ, v_n, t) replaces in φ all occurrences of v_n (free or bound, if any) by those of the term t if $t = v_m$, otherwise it only replaces all *free* occurrences of v_n (if any) by those of the term t. For example,

$$\mathrm{rpl}(\exists v_0\ v_0 \equiv v_1, v_0, v_1) = \exists v_1\ v_1 \equiv v_1,$$

and

$$\mathrm{rpl}(v_1 \equiv 0 \vee \exists v_1\ v_2 \equiv v_1, v_1, 0) = 0 \equiv 0 \vee \exists v_1\ v_2 \equiv v_1.$$

More precisely, it is defined inductively by

$$\begin{array}{lcl} \mathrm{rpl}(t_1 \equiv t_2, v_n, t) & := & t_1 \frac{t}{v_n} \equiv t_2 \frac{t}{v_n}; \\ \mathrm{rpl}(\neg\varphi, v_n, t) & := & \neg\, \mathrm{rpl}(\varphi, v_n, t); \\ \mathrm{rpl}(\varphi \vee \psi, v_n, t) & := & \mathrm{rpl}(\varphi, v_n, t) \vee \mathrm{rpl}(\psi, v_n, t); \\ \mathrm{rpl}(\exists v_m \varphi, v_n, 0) & := & \begin{cases} \exists v_m \varphi & \text{if } m = n; \\ \exists v_m\, \mathrm{rpl}(\varphi, v_n, 0) & \text{otherwise;} \end{cases} \\ \mathrm{rpl}(\exists v_m \varphi, v_n, 1) & := & \begin{cases} \exists v_m \varphi & \text{if } m = n; \\ \exists v_m\, \mathrm{rpl}(\varphi, v_n, 1) & \text{otherwise;} \end{cases} \\ \mathrm{rpl}(\exists v_m \varphi, v_n, v_p) & := & \begin{cases} \exists v_p\, \mathrm{rpl}(\varphi, v_n, v_p) & \text{if } m = n; \\ \exists v_m\, \mathrm{rpl}(\varphi, v_n, v_p) & \text{otherwise;} \end{cases} \\ \mathrm{rpl}(\exists v_m \varphi, v_n, t_1 + t_2) & := & \begin{cases} \exists v_m \varphi & \text{if } m = n; \\ \exists v_m\, \mathrm{rpl}(\varphi, v_n, t_1 + t_2) & \text{otherwise;} \end{cases} \\ \mathrm{rpl}(\exists v_m \varphi, v_n, t_1 \cdot t_2) & := & \begin{cases} \exists v_m \varphi & \text{if } m = n; \\ \exists v_m\, \mathrm{rpl}(\varphi, v_n, t_1 \cdot t_2) & \text{otherwise.} \end{cases} \end{array}$$

The corresponding ternary function $Rpl(m, n, k)$ returns the number encoding rpl(φ, v_n, t) where φ has Gödel number m and t has Gödel number k. It is defined by

$$
\begin{array}{lcl}
Rpl(4m,n,k) & := & 4\cdot\pi(TSbst(\pi_1(m),n,k),TSbst(\pi_2(m),n,k));\\
Rpl(4m+1,n,k) & := & 4\cdot Rpl(m,n,k)+1;\\
Rpl(4m+2,n,k) & := & 4\cdot\pi(Rpl(\pi_1(m),n,k),Rpl(\pi_2(m),n,k))+2;\\
Rpl(4m+3,n,3k) & := & \begin{cases} 4m+3 & \text{if } \pi_1(m)=n;\\ 4\cdot\pi(\pi_1(m),Rpl(\pi_2(m),n,3k))+3 & \text{otherwise;}\end{cases}\\
Rpl(4m+3,n,3k+1) & := & \begin{cases} 4m+3 & \text{if } \pi_1(m)=n;\\ 4\cdot\pi(\pi_1(m),Rpl(\pi_2(m),n,3k+1))+3 & \text{otherwise;}\end{cases}\\
Rpl(4m+3,n,3k+2) & := & \begin{cases} 4\cdot\pi(k,Rpl(\pi_2(m),n,3k+2))+3 & \text{if } \pi_1(m)=n;\\ 4\cdot\pi(\pi_1(m),Rpl(\pi_2(m),n,3k+2))+3 & \text{otherwise.}\end{cases}
\end{array}
$$

It is Σ_1-definable.

60. The operation $\mathrm{sft}(\varphi, M)$ shifts in φ all indices of bound variables v_n by M, i.e. all bound occurrences of every variable v_n are replaced by those of v_{n+M}. For example,

$$\mathrm{sft}(\exists v_2(v_0 \equiv v_2 \vee \exists v_0\ v_0 \equiv v_1), 3) = \exists v_5(v_0 \equiv v_5 \vee \exists v_3\ v_3 \equiv v_1).$$

More precisely, it is defined inductively by

$$
\begin{array}{lcl}
\mathrm{sft}(t_1 \equiv t_2, M) & := & t_1 \equiv t_2;\\
\mathrm{sft}(\neg\varphi, M) & := & \neg\,\mathrm{sft}(\varphi, M);\\
\mathrm{sft}(\varphi \vee \psi, M) & := & \mathrm{sft}(\varphi, M) \vee \mathrm{sft}(\psi, M);\\
\mathrm{sft}(\exists v_n \varphi, M) & := & \exists v_{n+M}\,\mathrm{rpl}(\mathrm{sft}(\varphi, M), v_n, v_{n+M}).
\end{array}
$$

Notice that in any resulting formula after applying sft, all occurrences of each variable (if any) are either all free or all bound.

The corresponding binary function $Sft(m,n)$ returns the number encoding $\mathrm{sft}(\varphi, n)$ where φ has Gödel number m. It is defined by

$$
\begin{array}{lcl}
Sft(4m,n) & := & 4m;\\
Sft(4m+1,n) & := & 4Sft(m,n)+1;\\
Sft(4m+2,n) & := & 4\pi(Sft(\pi_1(m),n),Sft(\pi_2(m),n))+2;\\
Sft(4m+3,n) & := & 4\pi(\pi_1(m)+n,Rpl(Sft(\pi_2(m),n),\pi_1(m),\pi_1(m)+n))+3.
\end{array}
$$

It is Σ_1-definable.

61. The operation $\varphi\frac{t}{v_n}$ (simple formula substitution) is defined inductively be-

low:[1]

$$\begin{array}{lcll}
(t_1 \equiv t_2)\dfrac{t}{v_n} & := & \left(t_1\dfrac{t}{v_n}\right) \equiv \left(t_2\dfrac{t}{v_n}\right); & \\
(\neg\varphi)\dfrac{t}{v_n} & := & \neg\left(\varphi\dfrac{t}{v_n}\right); & \\
(\varphi \vee \psi)\dfrac{t}{v_n} & := & \left(\varphi\dfrac{t}{v_n}\right) \vee \left(\psi\dfrac{t}{v_n}\right); & \\
(\exists v_m\varphi)\dfrac{t}{v_n} & := & \begin{cases} \exists v_m\varphi & \text{if } t = v_n \text{ or } v_n \notin \mathrm{free}(\exists v_m\varphi); \\ \exists v_m\left(\varphi\dfrac{t}{v_n}\right) & \text{if } t \neq v_n,\ v_n \in \mathrm{free}(\exists v_m\varphi), \text{ and } v_m \notin \mathrm{var}(t); \\ \mathrm{rpl}(\mathrm{sft}(\exists v_m\varphi, M), v_n, t) & \text{otherwise,} \end{cases} &
\end{array}$$

where M is one more than the maximum of indices of all variables occurring in $\exists v_m\varphi$ or t.

The corresponding ternary function $FSbst(m,n,k)$ returns the number encoding $\varphi\frac{t}{v_n}$ where φ has Gödel number m and t has Gödel number k. It is defined by

$$\begin{array}{lcl}
FSbst(4m,n,k) & := & 4\pi(TSbst(\pi_1(m),n,k), TSbst(\pi_2(m),n,k)); \\
FSbst(4m+1,n,k) & := & 4FSbst(m,n,k)+1; \\
FSbst(4m+2,n,k) & := & 4\pi(FSbst(\pi_1(m),n,k), FSbst(\pi_2(m),n,k))+2; \\
FSbst(4m+3,n,k) & := & \begin{cases} 4m+3 \\ \quad \text{if } k = 3n+2 \text{ or not } R_\in(n, Free(4m+3)); \\ 4\pi(\pi_1(m), FSbst(\pi_2(m),n,k))+3 \\ \quad \text{if } k \neq 3n+2 \text{ and } R_\in(n, Free(4m+3)) \text{ and} \\ \quad \text{not } R_\in(\pi_1(m), TVar(k)); \\ Rpl(Sft(4m+3, Max(FVar(4m+3) \cup TVar(k))+1), n, k) \\ \quad \text{otherwise.} \end{cases}
\end{array}$$

It is Σ_1-definable.

62. The operation $\mathrm{tbnd}(t, v_n)$ replaces in t all occurrences of constants and of variables by those of v_n. For example,

$$\mathrm{tbnd}(1 + (v_0 \cdot 0), v_2) = v_2 + (v_2 \cdot v_2).$$

More precisely, it is defined inductively

$$\begin{array}{lcl}
\mathrm{tbnd}(0, v_n) & := & v_n; \\
\mathrm{tbnd}(1, v_n) & := & v_n; \\
\mathrm{tbnd}(v_m, v_n) & := & v_n; \\
\mathrm{tbnd}(t_1 + t_2, v_n) & := & \mathrm{tbnd}(t_1, v_n) + \mathrm{tbnd}(t_2, v_n); \\
\mathrm{tbnd}(t_1 \cdot t_2, v_n) & := & \mathrm{tbnd}(t_1, v_n) \cdot \mathrm{tbnd}(t_2, v_n).
\end{array}$$

[1] The defintion of formula substitution stated here is slightly different from that given in textbook; for example, for the definition here we have $(\exists v_0 \exists v_1\ v_0 + v_1 \equiv v_2)\frac{v_1}{v_2} = \exists v_0 \exists v_4\ v_0 + v_4 \equiv v_1$, and for that given in text we have $(\exists v_0 \exists v_1\ v_0 + v_1 \equiv v_2)\frac{v_1}{v_2} = \exists v_0 \exists v_3\ v_0 + v_3 \equiv v_1$.

The corresponding function $TBnd(m,n)$ returns the number encoding $\mathrm{tbnd}(t,v_n)$ where t has Gödel number m. It is defined by

$$
\begin{array}{lcl}
TBnd(0,n) & := & 3n+2; \\
TBnd(1,n) & := & 3n+2; \\
TBnd(3m+2,n) & := & 3n+2; \\
TBnd(3m+3,n) & := & 3\pi(TBnd(\pi_1(m),n), TBnd(\pi_2(m),n))+3; \\
TBnd(3m+4,n) & := & 3\pi(TBnd(\pi_1(m),n), TBnd(\pi_2(m),n))+4.
\end{array}
$$

It is Σ_1-definable.

63. The operation $\mathrm{fbnd}(\varphi,n)$ replaces in φ all occurrences of constants and of variables (free or bound) by those of v_n. For example,

$$\mathrm{fbnd}(\exists v_2 \neg(v_0+v_1 \equiv 1\cdot v_1), v_3) = \exists v_3 \neg(v_3+v_3 \equiv v_3 \cdot v_3).$$

It is defined inductively by

$$
\begin{array}{lcl}
\mathrm{fbnd}(t_1 \equiv t_2, v_n) & := & \mathrm{tbnd}(t_1,v_n) \equiv \mathrm{tbnd}(t_2,v_n); \\
\mathrm{fbnd}(\neg\varphi, v_n) & := & \neg\,\mathrm{fbnd}(\varphi,v_n); \\
\mathrm{fbnd}(\varphi\vee\psi, v_n) & := & \mathrm{fbnd}(\varphi,v_n) \vee \mathrm{fbnd}(\psi,v_n); \\
\mathrm{fbnd}(\exists v_m\varphi, v_n) & := & \exists v_n\,\mathrm{fbnd}(\varphi,v_n).
\end{array}
$$

The corresponding function $FBnd(m,n)$ returns the number encoding $\mathrm{fbnd}(\varphi,v_n)$ where φ has Gödel number m. It is defined by

$$
\begin{array}{lcl}
FBnd(4m,n) & := & 4\pi(TBnd(\pi_1(m),n), TBnd(\pi_2(m),n)); \\
FBnd(4m+1,n) & := & 4FBnd(m,n)+1; \\
FBnd(4m+2,n) & := & 4\pi(FBnd(\pi_1(m),n), FBnd(\pi_2(m),n))+2; \\
FBnd(4m+3,n) & := & 4\pi(n, FBnd(\pi_2(m),n))+3.
\end{array}
$$

It is Σ_1-definable.

64. The unary relation $R_{(\mathrm{Assm})}(n)$ states that the sequent encoded by n results from applying the rule (Assm):

$$R_{(\mathrm{Assm})}n \quad \text{iff} \quad R_{\in}(\pi_2(n),\pi_1(n)).$$

Its characteristic function $F_{(\mathrm{Assm})}(n)$ is Σ_1-definable because

$$F_{(\mathrm{Assm})}(n) = F_{\in}(\pi_2(n),\pi_1(n)).$$

65. The unary relation $R_{(\equiv)}(n)$ states that the sequent encoded by n results from applying the rule $(\equiv)$:

$$R_{(\equiv)}(n) \quad \text{iff} \quad R_{=}(\pi_1(n),0) \text{ and } P(n),$$

where $P(n)$ states that there is some $m < \pi_2(n)$ such that

$$R_{=}(\pi_2(n), 4 \cdot \pi(m, m)),$$

of which the characteristic function F_P is Σ_1-definable. The characteristic function $F_{(\equiv)}(n)$ is Σ_1-definable because

$$F_{(\equiv)}(n) = 1 \dot{-} (1 \dot{-} F_{=}(\pi_1(n), 0)) \cdot (1 \dot{-} F_P(n)).$$

66. The binary relation $R_{(\mathrm{Ant})}(m, n)$ states that the sequent encoded by m results from applying the rule (Ant) to the sequent encoded by n:

$$R_{(\mathrm{Ant})}(m, n) \quad \text{iff} \quad R_{\subset}(\pi_1(n), \pi_1(m)) \text{ and } \pi_2(m) = \pi_2(n).$$

Its characteristic function $F_{(\mathrm{Ant})}(m, n)$ is Σ_1-definable because

$$F_{(\mathrm{Ant})}(m, n) = 1 \dot{-} (1 \dot{-} F_{\subset}(\pi_1(n), \pi_1(m))) \cdot (1 \dot{-} F_{=}(\pi_2(m), \pi_2(n))).$$

67. The ternary relation $R_{(\mathrm{PC})}(m, n, k)$ states that the sequent encoded by m results from applying the rule (PC) to the sequents encoded by n and k, respectively:

$$R_{(\mathrm{PC})}(m, n, k) \quad \text{iff} \quad P(m, n, k, p),\ \pi_2(m) = \pi_2(n) \text{ and } \pi_2(n) = \pi_2(k),$$

where $P(m, n, k, p)$ states that there is some $p < \pi_1(n)$ such that

$$\pi_1(n) = \pi_1(m) + 2^p \quad \text{and} \quad \pi_1(k) = \pi_1(m) + 2^{4 \cdot p + 1}$$

(p encodes ψ), of which the characteristic function F_P is Σ_1-definable. The characteristic function $F_{(\mathrm{PC})}$ is Σ_1-definable because

$$\begin{aligned} F(m, n, k) \quad = \quad & 1 \dot{-} (1 \dot{-} F_P(m, n, k, p)) \\ & \cdot (1 \cdot F_{=}(\pi_2(m), \pi_2(n))) \\ & \cdot (1 \dot{-} F_{=}(\pi_2(n), \pi_2(k))). \end{aligned}$$

68. The ternary relation $R_{(\mathrm{Ctr})}(m, n, k)$ states that the sequent encoded by m results from applying the rule (Ctr) to the sequents encoded by n and k, respecitvely:

$$\begin{aligned} R_{(\mathrm{Ctr})}(m, n, k) \quad \text{iff} \quad & \pi_1(n) = \pi_1(m) + 2^{4 \cdot \pi_2(m) + 1}, \\ & \pi_1(k) = \pi_1(n) \text{ and} \\ & \pi_2(k) = 4 \cdot \pi_2(n) + 1. \end{aligned}$$

Its characteristic function $F_{(\mathrm{Ctr})}$ is Σ_1-definable because

$$\begin{aligned} F_{(\mathrm{Ctr})}(m, n, k) \quad = \quad & 1 \dot{-} (1 \dot{-} F_{=}(\pi_1(n), \pi_1(m) + 2^{4\pi_2(m)+1})) \\ & \cdot (1 \dot{-} F_{=}(\pi_1(k), \pi_1(n))) \\ & \cdot (1 \dot{-} F_{=}(\pi_2(k), 4\pi_2(n) + 1)). \end{aligned}$$

69. The ternary relation $R_{(\vee\mathrm{A})}(m,n,k)$ states that the sequent encoded by m results from applying the rule $(\vee\mathrm{A})$ to the sequents encoded by n and k, respectively:

$$R_{(\vee\mathrm{A})}(m,n,k) \quad \text{iff} \quad P(m,n,k),\ \pi_2(m)=\pi_2(n) \text{ and } \pi_2(n)=\pi_2(k),$$

where $P(m,n,k)$ states that there are some $p,q<\pi_1(n)$ and some $r<\pi_1(k)$ such that

$$\pi_1(n)=p+2^q,\quad \pi_1(k)=p+2^r \quad \text{and} \quad \pi_1(m)=p\cup 2^{4\cdot\pi(q,r)+2}$$

(p encodes Γ, q encodes φ, r encodes ψ), of which the characteristic function F_P is Σ_1-definable. The characteristic function $F_{(\vee\mathrm{A})}$ is Σ_1-definable because

$$\begin{aligned} F_{(\vee\mathrm{A})}(m,n,k) &= 1 \mathbin{\dot-} (1 \mathbin{\dot-} F_P(m,n,k)) \\ &\qquad \cdot (1 \mathbin{\dot-} F_=(\pi_2(m),\pi_2(n))) \\ &\qquad \cdot (1 \mathbin{\dot-} F_=(\pi_2(n),\pi_2(k))). \end{aligned}$$

70. The binary relation $R_{(\vee\mathrm{S})}(m,n)$ states that the sequent encoded by m results from applying the rule $(\vee\mathrm{S})$ to the sequent encoded by n:

$$R_{(\vee\mathrm{S})}(m,n) \quad \text{iff} \quad \pi_1(m)=\pi_1(n) \text{ and } P(m,n),$$

where $P(m,n)$ states that there is some $k<\pi_2(m)$ such that

$$\pi_2(m)=4\cdot\pi(k,\pi_2(n))+2 \quad \text{or} \quad \pi_2(m)=4\cdot\pi(\pi_2(n),k)+2$$

(k encodes ψ), of which the characteristic function F_P is Σ_1-definable. The characteristic function $F_{(\vee\mathrm{S})}$ is Σ_1-definable because

$$F_{(\vee\mathrm{S})}(m,n)=1 \mathbin{\dot-} (1 \mathbin{\dot-} F_=(\pi_1(m),\pi_1(n)))\cdot(1 \mathbin{\dot-} F_P(m,n)).$$

71. The binary relation $R_{(\exists\mathrm{A})}(m,n)$ states that the sequent encoded by m results from applying the rule $(\exists\mathrm{A})$ to the sequent n:

$$R_{(\exists\mathrm{A})}(m,n) \quad \text{iff} \quad P(m,n) \text{ and } \pi_2(m)=\pi_2(n),$$

where $P(m,n)$ states that there are some $k,p<\pi_1(n)$ and some $q<\pi_1(m)$ such that

(i) $\pi_1(m)=k\cup 2^{4\cdot q+3}$,
(ii) $\pi_1(n)=k+2^{FSbst(\pi_2(q),\pi_1(q),3\cdot p+2)}$,
(iii) for all $r<\pi_1(m)$, if $R_\in(r,\pi_1(m))$ then not $R_\in(p,Free(r))$, and
(iv) not $R_\in(p,Free(\pi_2(m)))$

(k encodes Γ, p is the index of y and $4q+3$ encodes $\exists x\varphi$), of which the characteristic function F_P is Σ_1-definable. The characteristic function $F_{(\exists\mathrm{A})}$ is Σ_1-definable because

$$F_{(\exists\mathrm{A})}(m,n) = 1 \dot{-} (1 \dot{-} F_P(m,n)) \cdot (1 \dot{-} F_{=}(\pi_2(m), \pi_2(n))).$$

72. The binary relation $R_{(\exists\mathrm{S})}(m,n)$ states that the sequent encoded by m results from applying the rule ($\exists$S) to the sequent encoded by n:

$$R_{(\exists\mathrm{S})}(m,n) \quad \text{iff} \quad \pi_1(m) = \pi_1(n),\ R_{Div}(4, \pi_2(m)+1) \text{ and } P(m,n),$$

where $P(m,n)$ states that there is some $k < \pi_2(n)$ such that

$$\pi_2(n) = FSbst(\pi_2((\pi_2(m) \dot{-} 3) \div 4), \pi_1((\pi_2(m) \dot{-} 3) \div 4), k)$$

(k encodes t), of which the characteristic function $F_P(m,n)$ is Σ_1-definable. The characteristic function $F_{(\exists\mathrm{S})}$ is Σ_1-definable because

$$\begin{aligned} F_{(\exists\mathrm{S})}(m,n) \quad = \quad & 1 \dot{-} (1 \dot{-} F_{=}(\pi_1(m), \pi_1(n))) \\ & \cdot (1 \dot{-} F_{Div}(4, \pi_2(m)+1)) \\ & \cdot (1 \dot{-} F_P(m,n)). \end{aligned}$$

73. The binary relation $R_{(\mathrm{Sub})}(m,n)$ states that the sequent encoded by m results from applying the rule (Sub) to the sequent encoded by n:

$$\begin{array}{lll} R_{(\mathrm{Sub})}(m,n) & \text{iff} & \text{there are some } k < \pi_1(m), \\ & & \text{some } p < FBnd(\pi_2(m), Max(FVar(\pi_2(m)))+1) \text{ and} \\ & & \text{some } q < Max(Free(p))+1 \text{ such that} \\ & & \quad \text{(i)} \quad R_{\in}(q, Free(p)), \\ & & \quad \text{(ii)} \quad \pi_1(m) = \pi_1(n) \cup 2^{4\cdot k}, \\ & & \quad \text{(iii)} \quad \pi_2(m) = FSbst(p,q,\pi_2(4\cdot k)), \text{ and} \\ & & \quad \text{(iv)} \quad \pi_2(n) = FSbst(p,q,\pi_1(4\cdot k)) \end{array}$$

($4k$ encodes $t \equiv t'$, p encodes φ and q is the index of x). Its characteristic function $F_{(\mathrm{Sub})}$ is Σ_1-definable.

74. The binary relation $R_{\in LA}(m,n)$ intuitively states that m is a member of the last antecedent of n:

$$R_{\in LA}(m,n) \quad \text{:iff} \quad R_{\in}(m, \pi_1(Last(n))).$$

Its characteristic function is Σ_1-definable because

$$F_{\in LA}(m,n) = F_{\in}(m, \pi_1(n[Last])).$$

75. We use $\varphi_{Dvn}(v_0)$ as an abbreviation for

$$\begin{array}{l}
(\varphi_{(\mathrm{Assm})}(v_0[0]) \vee \varphi_{(\equiv)}(v_0[0]))\wedge \\
(1 < Length(v_0) \to (\varphi_{(\mathrm{Assm})}(v_0[1])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\mathrm{Ant})}(v_0[1], v_0[0])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\vee\mathrm{A})}(v_0[1], v_0[0], v_0[0])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\vee\mathrm{S})}(v_0[1], v_0[0])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\exists\mathrm{A})}(v_0[1], v_0[0])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\exists\mathrm{S})}(v_0[1], v_0[0])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\equiv)}(v_0[1])\vee \\
\qquad\qquad\qquad\qquad \varphi_{(\mathrm{Sub})}(v_0[1], v_0[0])))\wedge \\
(\forall k < Length(v_0)) \\
(2 \leq k \to (\varphi_{(\mathrm{Assm})}(v_0[k])\vee \\
\qquad\qquad \varphi_{(\equiv)}(v_0[k])\vee \\
\qquad\qquad (\exists j < k)\varphi_{(\mathrm{Ant})}(v_0[k], v_0[j])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\mathrm{PC})}(v_0[k], v_0[i], v_0[j])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\mathrm{PC})}(v_0[k], v_0[j], v_0[i])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\mathrm{Ctr})}(v_0[k], v_0[i], v_0[j])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\mathrm{Ctr})}(v_0[k], v_0[j], v_0[i])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\vee\mathrm{A})}(v_0[k], v_0[i], v_0[j])\vee \\
\qquad\qquad (\exists j < k)(\exists i < j)\varphi_{(\vee\mathrm{A})}(v_0[k], v_0[j], v_0[i])\vee \\
\qquad\qquad (\exists j < k)\varphi_{(\vee\mathrm{S})}(v_0[k], v_0[j])\vee \\
\qquad\qquad (\exists j < k)\varphi_{(\exists\mathrm{A})}(v_0[k], v_0[j])\vee \\
\qquad\qquad (\exists j < k)\varphi_{(\exists\mathrm{S})}(v_0[k], v_0[j])\vee \\
\qquad\qquad (\exists j < k)\varphi_{(\mathrm{Sub})}(v_0[k], v_0[j]))),
\end{array}$$

which intuitively states that v_0 encodes a derivation.

76. **Lemma.** *The following sentence is derivable from* Φ_{PA}*:*

$$\forall v_0 \forall v_1((\varphi_{Dvn}(v_0) \wedge \varphi_{Dvn}(v_1)) \to \varphi_{Dvn}(v_0 * v_1)).$$

77. Since Φ is decidable, the unary relation $R_\Phi(n)$ which states that the formula φ with Gödel number n is a member of Φ is decidable as well and is represented in Φ_{PA} by a Σ_1-formula $\varphi_0(x)$; also, the complement of this relation is decidable and is represented by a Σ_1-formula $\varphi_1(x)$.

We choose

$$\varphi_H(x, y) := (\varphi_{Dvn}(y) \wedge (\forall i < y)(\varphi_{\notin LA}(i, y) \vee \varphi_0(i))\wedge) \vee ().$$

there is a Σ_1-formula $\varphi_0(x)$ that represents in Φ_{PA} the unary relation ; the complement of this relation is also

Let $\delta_0(x)$ be a Σ_1-formula that is equivalent to

$$\varphi_{Dvn}(x) \wedge (\forall i < \pi_1(x[Last]))(R_\in(i, \pi_1(x[Last])) \to \varphi_0(i)).$$

78. The Predicate $\varphi_H(v_0, v_1)$ states that v_1 encodes a derivation for the formula encoded by v_0. (For $m \in \mathbb{N}$, if m does not encode a derivation from Φ, then let it encode a derivation for the trivial theorem $0 \equiv 0$, which has Gödel number 0). It is defined as

$$\begin{aligned}\exists u((&F_{Drvn}(v_1) \equiv \pi_1(\pi_1(u)) + 1\wedge\\ &F_{Der\Phi}(v_1) \equiv \pi_1(\pi_2(u)) + 1\wedge\\ &v_0 \equiv \pi_2(Last(v_1)))\vee\\ &((F_{Drvn}(v_1) \equiv 0 \vee F_{Der\Phi}(v_1) \equiv 0) \wedge v_0 \equiv 0)),\end{aligned}$$

where $F_{Drvn}(n)$ is the characteristic function of the unary relation stating that n encodes a derivation and $F_{Der\Phi}(n)$ is the characteristic function of the unary relation stating that the antecedent of the last sequent of the derivation encoded by n consists of axioms from Φ.

79. (INCOMPLETE) The Predicate $\varphi_{Der\Phi}(v_0)$ states that v_0 encodes a derivation from Φ. It is defined as

$$\varphi_{Drvn}(v_0) \wedge (\forall i < \pi_1(Last(v_0)))(\varphi_{\in}(i, \pi_1(Last(v_0))) \rightarrow \varphi_{\Phi}(i))$$

80. **Theorem.** (Main) *Let* $\Phi \supset \Phi_{\mathrm{PA}}$ *be decidable. Then*

$$\Phi_{\mathrm{PA}} \vdash \forall v_0 \forall v_1((\mathrm{Der}_{\Phi}(v_0) \wedge \mathrm{Der}_{\Phi}(4\pi(4v_0 + 1, v_1) + 2)) \rightarrow \mathrm{Der}_{\Phi}(v_1)).$$

Proof. It suffices to show $\mathrm{Der}_{\Phi_{\mathrm{PA}}}(v_1)$ is derivable from

$$\Phi_{\mathrm{PA}} \cup \{\varphi_H(v_0, u_0), \varphi_{DerPA}(u_1) \wedge \pi_2(Last(u_1)) \equiv 4\pi(4v_0 + 1, v_1) + 2\}$$

since

$$(\varphi_{DerPA}(u_1)\wedge\pi_2(Last(u_1)) \equiv 4\pi(4v_0+1, v_1)+2) \leftrightarrow \varphi_H(4\pi(4v_0+1, v_1)+2, u_1)$$

is derivable from Φ_{PA}.

This can be further devided into two cases:

(1) $\varphi_{DerPA}(u_0) \wedge \pi_2(Last(u_0)) \equiv v_0$ holds;

(2) $\neg\varphi_{DerPA}(u_0) \wedge v_0 \equiv 0$ holds.

Let us first consider (1). Let v_0 and v_1 be the Gödel numbers of φ and ψ, respectively. By assumption, u_0 encodes a derivation with the last sequent

$$m.\ \Gamma_0\ \varphi$$

and u_1 encodes a derivation with the last sequent

$$n.\ \Gamma_1\ (\neg\varphi \vee \psi)$$

Then the following

$m.$	Γ_0			φ	premise
				$\vdots$	
$(m+n).$	Γ_1			$(\neg\varphi \vee \psi)$	premise
$(m+n+1).$	$\Gamma_0 \cup \Gamma_1$	$\neg\varphi$	$\neg\psi$	φ	(Ant) applied to $m.$
$(m+n+2).$	$\Gamma_0 \cup \Gamma_1$	$\neg\varphi$	$\neg\psi$	$\neg\varphi$	(Assm)
$(m+n+3).$	$\Gamma_0 \cup \Gamma_1$		$\neg\varphi$	ψ	(Ctr) applied to $(m+n+1).$ and $(m+n+$
$(m+n+4).$	$\Gamma_0 \cup \Gamma_1$		ψ	ψ	(Assm)
$(m+n+5).$	$\Gamma_0 \cup \Gamma_1$		$(\neg\varphi \vee \psi)$	ψ	($\vee$A) applied to $(m+n+3).$ and $(m+n+$
$(m+n+6).$	$\Gamma_0 \cup \Gamma_1$	$\neg(\neg\varphi \vee \psi)$	$\neg\psi$	$(\neg\varphi \vee \psi)$	(Ant) applied to $(m+n).$
$(m+n+7).$	$\Gamma_0 \cup \Gamma_1$	$\neg(\neg\varphi \vee \psi)$	$\neg\psi$	$\neg(\neg\varphi \vee \psi)$	(Assm)
$(m+n+8).$	$\Gamma_0 \cup \Gamma_1$		$\neg(\neg\varphi \vee \psi)$	ψ	(Ctr) applied to $(m+n+6).$ and $(m+n+$
$(m+n+9).$	$\Gamma_0 \cup \Gamma_1$			ψ	(PC) applied to $(m+n+5).$ and $(m+n+$

is a derivation of ψ; it is encoded by the term t_1:

$$
\begin{aligned}
&(((u_0 * u_1) + 2) \div \mathit{Prime}(A-1))\\
&\cdot \mathit{Prime}(A)^{\pi(G_0 \cup G_1 \cup 2^{4B+1} \cup 2^{4C+1}, B)}\\
&\cdot \mathit{Prime}(A+1)^{\pi(G_0 \cup G_1 \cup 2^{4B+1} \cup 2^{4C+1}, 4B+1)}\\
&\cdot \mathit{Prime}(A+2)^{\pi(G_0 \cup G_1 \cup 2^{4B+1}, C)}\\
&\cdot \mathit{Prime}(A+3)^{\pi(G_0 \cup G_1 \cup 2^{C}, C)}\\
&\cdot \mathit{Prime}(A+4)^{\pi(G_0 \cup G_1 \cup 2^{D}, C)}\\
&\cdot \mathit{Prime}(A+5)^{\pi(G_0 \cup G_1 \cup 2^{4D+1} \cup 2^{4C+1}, D)}\\
&\cdot \mathit{Prime}(A+6)^{\pi(G_0 \cup G_1 \cup 2^{4D+1} \cup 2^{4C+1}, 4D+1)}\\
&\cdot \mathit{Prime}(A+7)^{\pi(G_0 \cup G_1 \cup 2^{4D+1}, C)}\\
&\cdot \mathit{Prime}(A+8)^{\pi(G_0 \cup G_1, C)+1} - 2,
\end{aligned}
$$

where $A = \mathit{Length}(u_0 * u_1)$, $G_0 = \pi_1(\mathit{Last}(u_0))$, $G_1 = \pi_1(\mathit{Last}(u_1))$, $B = \pi_2(\mathit{Last}(u_0))$, $C = \pi_2((\pi_2(\mathit{Last}(u_1)) - 2) \div 4)$ and $D = \pi_2(\mathit{Last}(u_1))$. It can be verified that $\varphi_H(v_1, t_1)$ is true and hence derivable, thus so is $\mathrm{Der}_{\Phi_{\mathrm{PA}}}(v_1)$.

For (2), let v_1 be the Gödel number of ψ. By assumption, u_1 encodes a derivation with the last sequent

$$n.\ \Gamma_1\ (\neg 0 \equiv 0 \vee \psi)$$

Then the following

$n.$	Γ_1			$(\neg 0 \equiv 0 \vee \psi)$	premise
$(n+1).$				$0 \equiv 0$	$(\equiv)$
$(n+2).$	Γ_1	$\neg 0 \equiv 0$	$\neg\psi$	$0 \equiv 0$	(Ant) applied to $(n+1)$.
$(n+3).$	Γ_1	$\neg 0 \equiv 0$	$\neg\psi$	$\neg 0 \equiv 0$	(Assm)
$(n+4).$	Γ_1		$\neg 0 \equiv 0$	ψ	(Ctr) applied to $(n+2)$. and $(n+3)$.
$(n+5).$	Γ_1		ψ	ψ	(Assm)
$(n+6).$	Γ_1		$(\neg 0 \equiv 0 \vee \psi)$	ψ	$(\vee$A) applied to $(n+4)$. and $(n+5)$.
$(n+7).$	Γ_1	$\neg(\neg 0 \equiv 0 \vee \psi)$	$\neg\psi$	$(\neg 0 \equiv 0 \vee \psi)$	(Ant) applied to n.
$(n+8).$	Γ_1	$\neg(\neg 0 \equiv 0 \vee \psi)$	$\neg\psi$	$\neg(\neg 0 \equiv 0 \vee \psi)$	(Assm)
$(n+9).$	Γ_1		$\neg(\neg 0 \equiv 0 \vee \psi)$	ψ	(Ctr) applied to $(n+7)$. and $(n+8)$.
$(n+10).$	Γ_1			ψ	(PC) applied to $(n+6)$. and $(n+9)$.

is a derivation for ψ; it is encoded by the term t_2:

$$\begin{aligned}
&((u_1+2) \div Prime(Length(u_1)-1)) \\
&\cdot Prime(Length(u_1))^{\pi(0,0)} \\
&\cdot Prime(Length(u_1)+1)^{\pi(G_1 \cup 2^1 \cup 2^{4C+1},0)} \\
&\cdot Prime(Length(u_1)+2)^{\pi(G_1 \cup 2^1 \cup 2^{4C+1},1)} \\
&\cdot Prime(Length(u_1)+3)^{\pi(G_1 \cup 2^1,C)} \\
&\cdot Prime(Length(u_1)+4)^{\pi(G_1 \cup 2^C,C)} \\
&\cdot Prime(Length(u_1)+5)^{\pi(G_1 \cup 2^D,C)} \\
&\cdot Prime(Length(u_1)+6)^{\pi(G_1 \cup 2^{4D+1} \cup 2^{4C+1},D)} \\
&\cdot Prime(Length(u_1)+7)^{\pi(G_1 \cup 2^{4D+1} \cup 2^{4C+1},4D+1)} \\
&\cdot Prime(Length(u_1)+8)^{\pi(G_1 \cup 2^{4D+1},C)} \\
&\cdot Prime(Length(u_1)+9)^{\pi(G_1,C)+1} - 2,
\end{aligned}$$

where G_1, C and D are as above. It can be verified that $\varphi_H(v_1, t_2)$ is true and hence derivable, thus so is $\mathrm{Der}_{\Phi_{\mathrm{PA}}}(v_1)$. ▯

81. **Corollary.** (The Derivability Condition (L2)) *If $\Phi \supset \Phi_{\mathrm{PA}}$ is decidable, then*

$$\Phi \vdash (\mathrm{Der}_\Phi(\boldsymbol{n}^{\varphi}) \wedge \mathrm{Der}_\Phi(\boldsymbol{n}^{\varphi\to\psi})) \to \mathrm{Der}_\Phi(\boldsymbol{n}^{\psi}).$$