

COMPLETE PROOFS OF GÖDEL'S INCOMPLETENESS THEOREMS

LECTURES BY B. KIM

Step 0: Preliminary Remarks

We define recursive and recursively enumerable functions and relations, enumerate several of their properties, prove Gödel's β -Function Lemma, and demonstrate its first applications to coding techniques.

Definition. For $R \subset \omega^n$ a relation, $\chi_R : \omega^n \rightarrow \omega$, the *characteristic function* on R , is given by

$$\chi_R(\bar{a}) = \begin{cases} 1 & \text{if } \neg R(\bar{a}), \\ 0 & \text{if } R(\bar{a}). \end{cases}$$

Definition. A function from ω^m to ω ($m \geq 0$) is called **recursive** (or **computable**) if it is obtained by finitely many applications of the following rules:

- R1.
 - $I_i^n : \omega^n \rightarrow \omega$, $1 \leq i \leq n$, defined by $(x_1, \dots, x_n) \mapsto x_i$ is *recursive*;
 - $+$: $\omega \times \omega \rightarrow \omega$ and \cdot : $\omega \times \omega \rightarrow \omega$ are *recursive*;
 - $\chi_{<} : \omega \times \omega \rightarrow \omega$ is *recursive*.
- R2. (Composition) For recursive functions G, H_1, \dots, H_k such that $H_i : \omega^n \rightarrow \omega$ and $G : \omega^k \rightarrow \omega$, $F : \omega^n \rightarrow \omega$, defined by

$$F(\bar{a}) = G(H_1(\bar{a}), \dots, H_k(\bar{a})).$$

is *recursive*.

- R3. (Minimization) For $G : \omega^{n+1} \rightarrow \omega$ recursive, such that for all $\bar{a} \in \omega^n$ there exists some $x \in \omega$ such that $G(\bar{a}, x) = 0$, $F : \omega^n \rightarrow \omega$, defined by

$$F(\bar{a}) = \mu x (G(\bar{a}, x) = 0)$$

is *recursive*. (Recall that $\mu x P(x)$ for a relation P is the minimal $x \in \omega$ such that $x \in P$ obtains.)

Definition. $R(\subseteq \omega^k)$ is called **recursive**, or **computable** (R is a recursive relation) if χ_R is a recursive function.

Proofs in this note are adaptation of those in [Sh] into the deduction system described in [E]. Many thanks to Peter Ahumada and Michael Brewer who wrote up this note.

Properties of Recursive Functions and Relations:

P0. Assume $\sigma : \{1, \dots, k\} \rightarrow \{1, \dots, n\}$ is given. If $G : \omega^k \rightarrow \omega$ is recursive, then $F : \omega^n \rightarrow \omega$ defined by, for $\bar{a} = (a_1, \dots, a_n)$,

$$F(\bar{a}) = G(a_{\sigma(1)}, \dots, a_{\sigma(k)}) = G(I_{\sigma(1)}^n(\bar{a}), \dots, I_{\sigma(k)}^n(\bar{a})),$$

is recursive. Similarly, if $P(x_1, \dots, x_k)$ is recursive, then so is

$$R(x_1, \dots, x_n) \equiv P(x_{\sigma(1)}, \dots, x_{\sigma(k)}).$$

P1. For $Q \subset \omega^k$ a recursive relation, and $H_1, \dots, H_k : \omega^n \rightarrow \omega$ recursive functions,

$$P = \{\bar{a} \in \omega^n \mid Q(H_1(\bar{a}), \dots, H_k(\bar{a}))\}$$

is a recursive relation.

Proof. $\chi_P(\bar{a}) = \chi_Q(H_1(\bar{a}), \dots, H_k(\bar{a}))$ is a recursive function by R2.

P2. For $P \subset \omega^{n+1}$, a recursive relation such that for all $\bar{a} \in \omega^n$ there exists some $x \in \omega$ such that $P(\bar{a}, x)$, then $F : \omega^n \rightarrow \omega$, defined by

$$F(\bar{a}) = \mu x P(\bar{a}, x)$$

is recursive.

Proof. $F(\bar{a}) = \mu x (\chi_P(\bar{a}, x) = 0)$, so we may apply R3.

P3. Constant functions, $C_{n,k} : \omega^n \rightarrow \omega$ such that $C_{n,k}(\bar{a}) = k$, are recursive. (Hence for recursive $F : \omega^{m+n} \rightarrow \omega$ or $P \subseteq \omega^{m+n}$, and $\bar{b} \in \omega^n$, both the map $(x_1, \dots, x_m) \mapsto F(x_1, \dots, x_m; \bar{b})$ and $P(x_1, \dots, x_m; \bar{b}) \subseteq \omega^m$ are recursive.)

Proof. By induction:

$$C_{n,0}(\bar{a}) = \mu x (I_{n+1}^{n+1}(\bar{a}, x) = 0)$$

$$C_{n,k+1}(\bar{a}) = \mu x (C_{n,k}(\bar{a}) < x)$$

are recursive by R3 and P2, respectively.

P4. For $Q, P \subset \omega^n$, recursive relations, $\neg P$, $P \vee Q$, and $P \wedge Q$ are recursive.

Proof. We have that

$$\chi_{\neg P}(\bar{a}) = \chi_{<}(0, \chi_P(\bar{a})),$$

$$\chi_{P \vee Q}(\bar{a}) = \chi_P(\bar{a}) \cdot \chi_Q(\bar{a}),$$

$$P \wedge Q = \neg(\neg P \vee \neg Q).$$

P5. The predicates $=$, \leq , $>$, and \geq are recursive. (Hence each finite set is recursive.)

Proof. For $a, b \in \omega$,

$$a = b \text{ iff } \neg(a < b) \wedge \neg(b < a),$$

$$a \geq b \text{ iff } \neg(a < b),$$

$$a > b \text{ iff } (a \geq b) \wedge \neg(a = b), \text{ and}$$

$$a \leq b \text{ iff } \neg(a > b),$$

hence these are recursive by P4.

Notation. We write, for $\bar{a} \in \omega^n$, $f : \omega^n \rightarrow \omega$ a function and $P \subset \omega^{m+1}$ a relation,

$$\mu x < f(\bar{a}) P(x, \bar{b}) \equiv \mu x (P(x, \bar{b}) \vee x = f(\bar{a})).$$

In particular, $\mu x < f(\bar{a}) P(x, \bar{b})$ is the smallest integer less than $f(\bar{a})$ which satisfies P , if such exists, or $f(\bar{a})$, otherwise.

We also write

$$\exists x < f(\bar{a}) P(x) \equiv (\mu x < f(\bar{a}) P(x)) < f(\bar{a}), \text{ and}$$

$$\forall x < f(\bar{a}) P(x) \equiv \neg(\exists x < f(\bar{a}) (\neg P(x))).$$

The first is clearly satisfied if some $x < f(\bar{a})$ satisfies $P(x)$, while the second is satisfied if all $x < f(\bar{a})$ satisfy $P(x)$.

P6. For $P \subset \omega^{n+1}$ a recursive relation, $F : \omega^{n+1} \rightarrow \omega$, defined by

$$F(a, \bar{b}) = \mu x < a P(x, \bar{b}),$$

is recursive.

Proof. $F(a, \bar{b}) = \mu x (P(x, \bar{b}) \vee x = a)$, and thus F is recursive by P2, since for all \bar{b} , a satisfies $P(x, \bar{b}) \vee x = a$.

P7. For $R \subset \omega^{n+1}$ a recursive relation, $P, Q \subset \omega^{n+1}$ such that

$$P(a, \bar{b}) \equiv \exists x < a R(x, \bar{b}); \quad Q(a, \bar{b}) \equiv \forall x < a R(x, \bar{b})$$

are recursive. (Hence, with P1, it follows both

$$\text{Div}(y, z) (\equiv y|z) = \exists x < z + 1 (z = x \cdot y),$$

and PN, the set of all prime numbers, are recursive.)

Proof. Note that P is defined by composition of recursive functions and predicates, hence recursive by P1, and Q is defined by composition of recursive functions, recursive predicates, and negation, hence recursive by P1 and P4.

P8. $\dot{-} : \omega \times \omega \rightarrow \omega$, defined by

$$a \dot{-} b = \begin{cases} a - b & \text{if } a \geq b, \\ 0 & \text{otherwise,} \end{cases}$$

is recursive.

Proof. Note that

$$a \dot{-} b = \mu x (b + x = a \vee a < b).$$

P9. If $G_1, \dots, G_k : \omega^n \rightarrow \omega$ are recursive functions, and $R_1, \dots, R_k \subset \omega^n$ are recursive relations partitioning ω^n (i.e., for each $\bar{a} \in \omega^n$, there exists a unique i such that $R_i(\bar{a})$), then $F : \omega^n \rightarrow \omega$, defined by

$$F(\bar{a}) = \begin{cases} G_1(\bar{a}) & \text{if } R_1(\bar{a}), \\ G_2(\bar{a}) & \text{if } R_2(\bar{a}), \\ \vdots & \vdots \\ G_k(\bar{a}) & \text{if } R_k(\bar{a}), \end{cases}$$

is recursive.

Proof. Note that

$$F = G_1\chi_{\neg R_1} + \dots + G_k\chi_{\neg R_k}.$$

P10. If $Q_1, \dots, Q_k \subset \omega^n$ are recursive relations, and $R_1, \dots, R_k \subset \omega^n$ are recursive relations partitioning ω^n , then $P \subset \omega^n$, defined by

$$P(\bar{a}) \text{ iff } \begin{cases} Q_1(\bar{a}) & \text{if } R_1(\bar{a}), \\ \vdots & \vdots \\ Q_k(\bar{a}) & \text{if } R_k(\bar{a}), \end{cases}$$

is recursive.

Proof. Note that

$$\chi_P(\bar{a}) = \begin{cases} \chi_{Q_1}(\bar{a}) & \text{if } R_1(\bar{a}), \\ \vdots & \vdots \\ \chi_{Q_k}(\bar{a}) & \text{if } R_k(\bar{a}), \end{cases}$$

is recursive by P9.

Definition. A relation $P \subset \omega^n$ is **recursively enumerable (r.e.)** if there exists some recursive relation $Q \subset \omega^{n+1}$ such that

$$P(\bar{a}) \text{ iff } \exists x Q(\bar{a}, x).$$

Remark If a relation $R \subset \omega^n$ is recursive, then it is recursively enumerable, since $R(\bar{a}) \text{ iff } \exists x (R(\bar{a}) \wedge x = x)$.

Negation Theorem. A relation $R \subset \omega^n$ is recursive if and only if R and $\neg R$ are recursively enumerable.

Proof. If R is recursive, then $\neg R$ is recursive. Hence by above remark, both are r.e.

Now, let P and Q be recursive relations such that for $\bar{a} \in \omega^n$, $R(\bar{a}) \text{ iff } \exists x Q(\bar{a}, x)$ and $\neg R(\bar{a}) \text{ iff } \exists x P(\bar{a}, x)$.

Define $F : \omega^n \rightarrow \omega$ by

$$F(\bar{a}) = \mu x (Q(\bar{a}, x) \vee P(\bar{a}, x)),$$

recursive by P2, since either $R(\bar{a})$ or $\neg R(\bar{a})$ must hold.

We show that

$$R(\bar{a}) \text{ iff } Q(\bar{a}, F(\bar{a})).$$

In particular, $Q(\bar{a}, F(\bar{a}))$ implies there exists x (namely, $F(\bar{a})$) such that $Q(\bar{a}, x)$, thus $R(\bar{a})$ holds. Further, if $\neg Q(\bar{a}, F(\bar{a}))$, then $P(\bar{a}, F(\bar{a}))$, since $F(\bar{a})$ satisfies $Q(\bar{a}, x) \vee P(\bar{a}, x)$. Thus $\neg R(\bar{a})$ holds.

The β -Function Lemma.

β -Function Lemma (Gödel). *There is a recursive function $\beta : \omega^2 \rightarrow \omega$ such that $\beta(a, i) \leq a-1$ for all $a, i \in \omega$, and for any $a_0, a_1, \dots, a_{n-1} \in \omega$, there is an $a \in \omega$ such that $\beta(a, i) = a_i$ for all $i < n$.*

Remark 1. Let $A = \{a_1, \dots, a_n\} \subseteq \omega \setminus \{0, 1\}$ ($n \geq 2$) be a set such that any two distinct elements of A are relatively prime. Then given non-empty subset B of A , there is $y \in \omega$ such that for any $a \in A$, $a|y$ iff $a \in B$. (y is a product of elements in B .)

Lemma 2. If $k|z$ for $z \neq 0$, then $(1 + (j + k)z, 1 + jz)$ are relatively prime for any $j \in \omega$.

Proof. Note that for p prime, $p|z$ implies that $p \nmid 1 + jz$. But if $p|1 + (j + k)z$ and $p|1 + jz$, then $p|kz$, implying $p|k|z$ or $p|z$, and thus $p|z$, a contradiction.

Lemma 3. $J : \omega^2 \rightarrow \omega$, defined by $J(a, b) = (a + b)^2 + (a + 1)$, is one-to-one.

Proof. If $a + b < a' + b'$, then

$$J(a, b) = (a + b)^2 + a + 1 \leq (a + b)^2 + 2(a + b) + 1 = (a + b + 1)^2 \leq (a' + b')^2 < J(a', b').$$

Thus if $J(a, b) = J(a', b')$, then $a + b = a' + b'$, and

$$0 = J(a', b') - J(a, b) = a' - a,$$

implying that $a = a'$ and $b = b'$, as desired.

Proof of β -Function Lemma. Define

$$\beta(a, i) = \mu x < a-1 (\exists y < a (\exists z < a (a = J(y, z) \wedge \text{Div}(1 + (J(x, i) + 1) \cdot z, y))))),$$

It is clear that β is recursive, and that $\beta(a, i) \leq a-1$.

Given $a_1, \dots, a_{n-1} \in \omega$, we want to find $a \in \omega$ such that $\beta(a, i) = a_i$ for all $i < n$. Let

$$c = \max_{i < n} \{J(a_i, i) + 1\},$$

and choose $z \in \omega$, nonzero, such that for all $j < c$ nonzero, $j|z$.

By Lemma 2, for all j, l such that $1 \leq j < l \leq c$, $(1 + jz, 1 + lz)$ are relatively prime, since $0 < l - j < c$ implies that $(l - j)|z$. By Remark 1, there exists $y \in \omega$ such that for all $j < c$,

$$1 + (j + 1)z | y \text{ iff } j = J(a_i, i) \text{ for some } i < n. \quad (*)$$

Let $a = J(y, z)$.

We note the following, for each a_i :

(i) $a_i < y < a$ and $z < a$;

In particular, $y, z < a$ by the definition of J , and that $a_i < y$ by (*).

(ii) $\text{Div}(1 + (J(a_i, i) + 1) \cdot z, y)$;

From (*).

(iii) For all $x < a_i$, $1 + (J(x, i) + 1)z \not\parallel y$;

Since J is one-to-one, $x < a_i$ implies $J(x, i) \neq J(a_i, i)$, and for $j \neq i$, $J(x, i) \neq J(a_j, j)$. Thus, by (*), x does not satisfy the required predicate for y and z as chosen above.

Since for any other y' and z' , $a = J(y, z) \neq J(y', z')$, we have that a_i is in fact the minimal integer satisfying the predicate defining β , and thus $\beta(a, i) = a_i$, as desired.

The β -function will be the basis for various systems of coding. Our first use will be in encoding sequences of numbers:

Definition. The **sequence number** of a sequence of natural numbers a_1, \dots, a_n , is given by

$$\langle a_1, \dots, a_n \rangle = \mu x (\beta(x, 0) = n \wedge \beta(x, 1) = a_1 \wedge \dots \wedge \beta(x, n) = a_n).$$

Note that the map $\langle \rangle$ is defined on all sequences due to the properties of β proved above. Further, since β is recursive, $\langle \rangle$ is recursive, and $\langle \rangle$ is one-to-one, since

$$\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_m \rangle$$

implies that $n = m$ and $a_i = b_i$ for each i . Note, too, that the sequence number of the empty sequence is

$$\langle \rangle = \mu x (\beta(x, 0) = 0) = 0.$$

An important feature of our coding is that we can recover a given sequence from its sequence number:

Definition. For each $i \in \omega$, we have a function $()_i : \omega \rightarrow \omega$, given by

$$(a)_i = \beta(a, i).$$

Clearly $()_i$ is recursive for each i . $()_0$ will be called the **length** and denoted lh .

As intended, it follows from these definitions that $(\langle a_1 \dots a_n \rangle)_i = a_i$ and $lh(\langle a_1 \dots a_n \rangle) = n$.

Note also that whenever $a > 0$, we have $lh(a) < a$ and $(a)_i < a$.

Definition. The relation $Seq \subset \omega$ is given by

$$Seq(a) \text{ iff } \forall x < a (lh(x) \neq lh(a) \vee \exists i < lh(a) ((x)_{i+1} \neq (a)_{i+1})).$$

That Seq is recursive is evident from properties enumerated above. From our definition, it is clear that $Seq(a)$ if and only if a is the sequence number for some sequence (in particular, $a = \langle (a)_1, \dots, (a)_{lh(a)} \rangle$). Note that

$$\neg Seq(a) \text{ iff } \exists x < a (lh(x) = lh(a) \wedge \forall i < lh(a) ((x)_{i+1} = (a)_{i+1})).$$

Definition. The **initial sequence** function $Init : \omega^2 \rightarrow \omega$ is given by

$$Init(a, i) = \mu x (lh(x) = i \wedge \forall j < i ((x)_{j+1} = (a)_{j+1})).$$

Again, $Init$ is evidently recursive. Note that for $1 \leq i \leq n$,

$$Init(\langle a_1, \dots, a_n \rangle, i) = \langle a_1, \dots, a_i \rangle,$$

as intended.

Definition. The **concatenation** function $*$: $\omega^2 \rightarrow \omega$ is given by

$$a * b = \mu x (lh(x) = lh(a) + lh(b) \\ \wedge \forall i < lh(a) ((x)_{i+1} = (a)_{i+1}) \wedge \forall j < lh(b) ((x)_{lh(a)+j+1} = (b)_{j+1}).$$

Note that $*$ is recursive, and that

$$\langle a_1 \dots a_n \rangle * \langle b_1 \dots b_m \rangle = \langle a_1 \dots a_n, b_1 \dots b_m \rangle,$$

as desired.

Definition. For $F : \omega \times \omega^k \rightarrow \omega$, we define $\bar{F} : \omega \times \omega^k \rightarrow \omega$ by

$$\bar{F}(a, \bar{b}) = \langle F(0, \bar{b}), \dots, F(a-1, \bar{b}) \rangle,$$

or, equivalently,

$$\mu x (lh(x) = a \wedge \forall i < a ((x)_{i+1} = F(i, \bar{b}))).$$

Note that $F(a, \bar{b}) = (\bar{F}(a+1, \bar{b}))_{a+1}$, thus we have that \bar{F} is recursive if and only if F is recursive. Because $\bar{F}(a, \bar{b})$ is defined in terms of values $F(x, \bar{b})$, for x strictly smaller than a , this construction will enable us to define F inductively.

Properties of Recursive Functions and Relations (continued):

P11. For $G : \omega \times \omega \times \omega^n \rightarrow \omega$ a recursive function, the function $F : \omega \times \omega^n \rightarrow \omega$, given by

$$F(a, \bar{b}) = G(\bar{F}(a, \bar{b}), a, \bar{b}),$$

is recursive.

Proof. Note that

$$F(a, \bar{b}) = G(H(a, \bar{b}), a, \bar{b})$$

where

$$H(a, \bar{b}) = \mu x (Seq(x) \wedge lh(x) = a \wedge \forall i < a ((x)_{i+1} = G(Init(x, i), i, \bar{b}))).$$

According to this definition, $F(0, \bar{b}) = G(\langle \rangle, 0, \bar{b}) = G(0, 0, \bar{b})$,

$$F(1, \bar{b}) = G(\langle G(0, 0, \bar{b}) \rangle, 1, \bar{b}),$$

and

$$F(2, \bar{b}) = G(\langle G(0, 0, \bar{b}), G(\langle G(0, 0, \bar{b}) \rangle, 1, \bar{b}) \rangle, 2, \bar{b}),$$

showing that computation is cumbersome, but possible, for any particular value a .

P12. For $G : \omega \times \omega^n \rightarrow \omega$ and $H : \omega \times \omega^n \rightarrow \omega$ recursive functions, $F : \omega \times \omega^n \rightarrow \omega$ defined by

$$F(a, \bar{b}) = \begin{cases} F(G(a, \bar{b}), \bar{b}) & \text{if } G(a, \bar{b}) < a, \text{ and} \\ H(a, \bar{b}) & \text{otherwise,} \end{cases}$$

is recursive.

Proof. Note that when $G(a, \bar{b}) < a$, we have

$$F(G(a, \bar{b}), \bar{b}) = (\bar{F}(a, \bar{b}))_{G(a, \bar{b})+1} = \beta(\bar{F}(a, \bar{b}), G(a, \bar{b}) + 1) = G'(\bar{F}(a, \bar{b}), a, \bar{b})$$

with recursive $G'(x, y, \bar{z}) = \beta(x, G(y, \bar{z}) + 1)$. Thus F is recursive by P11.

For most purposes, when we define a function F inductively by cases, we must satisfy two requirements to guarantee that our function is well-defined. First, if $F(x, \bar{b})$ appears in a defining case involving a , we must show that $x < a$ whenever this case is true. Second, we must show that our base case is not defined in terms of F . In particular, this means that we cannot use F in a defining case which is used to compute $F(0, \beta)$.

P13. Given recursive $G : \omega^n \rightarrow \omega$ and $H : \omega^2 \times \omega^n \rightarrow \omega$, $F : \omega \times \omega^n \rightarrow \omega$ given by

$$F(a, \bar{b}) = \begin{cases} H(F(a-1, \bar{b}), a-1, \bar{b}) & \text{if } a > 0, \text{ and} \\ G(\bar{b}) & \text{otherwise,} \end{cases}$$

is recursive. (For example, the maps

$$n \mapsto n! = \begin{cases} (n-1)! \cdot n & \text{if } n > 0 \\ 1 & n = 0, \end{cases}$$

$$(n, m) \mapsto m^n = \begin{cases} m^{(n-1)} \cdot m & \text{if } n > 0, \\ 1 & n = 0, \end{cases}$$

and

$$n \mapsto (n+1)^{\text{th}} \text{ prime} = \begin{cases} \mu x (x > n^{\text{th}} \text{ prime} \wedge \text{PN}(x)) & \text{if } n > 0 \\ 2 & n = 0 \end{cases}$$

are all recursive.)

Proof. Note that $H(F(a-1, \bar{b}), a-1, \bar{b}) = H(\beta(\bar{F}(a, \bar{b}), a), a-1, \bar{b})$ has the form of P11.

P14. Given recursive relations $Q \subset \omega^{n+1}$ and $R \subset \omega^{n+1}$ and recursive $H : \omega \times \omega^n \rightarrow \omega$ such that $H(a, \bar{b}) < a$ whenever $Q(a, \bar{b})$ holds, the relation $P \subset \omega^{n+1}$, given by

$$P(a, \bar{b}) \text{ iff } \begin{cases} P(H(a, \bar{b}), \bar{b}) & \text{if } Q(a, \bar{b}), \\ R(a, \bar{b}) & \text{otherwise,} \end{cases}$$

is recursive.

Proof. Define $H' : \omega \times \omega^n \rightarrow \omega$ by

$$H'(a, \bar{b}) = \begin{cases} H(a, \bar{b}) & \text{if } Q(a, \bar{b}), \text{ and} \\ a & \text{otherwise.} \end{cases}$$

H' is clearly recursive. Note

$$\chi_P(a, \bar{b}) = \begin{cases} \chi_P(H'(a, \bar{b}), \bar{b}) & \text{if } H'(a, \bar{b}) < a, \text{ and} \\ \chi_R(a, \bar{b}) & \text{otherwise.} \end{cases}$$

The following example will prove useful:

Definition. Let $A \subset \omega^2$ be given by

$$A(a, c) \text{ iff } Seq(c) \wedge lh(c) = a \wedge \forall i < a ((c)_{i+1} = 0 \vee (c)_{i+1} = 1),$$

and let $F : \omega^2 \rightarrow \omega$ be given by

$$F(a, i) = \begin{cases} \mu x(A(a, x)) & \text{if } i = 0, \\ \mu x(F(a, i-1) < x \wedge A(a, x)) & \text{if } 0 < i < 2^a, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Then the function $bd : \omega \rightarrow \omega$ is given by

$$bd(n) = F(n, 2^n - 1).$$

Evidently, A , F , and bd are all recursive. In fact,

$$bd(n) = \max\{ \langle c_1 c_2 \dots c_n \rangle \mid c_i = 0 \text{ or } 1 \}.$$

Step 1: Representability of Recursive Functions in Q

We define Q , a subtheory of the natural numbers, and prove the Representability Theorem, stating that all recursive functions are representable in this subtheory.

Consider the language of natural numbers $\mathcal{L}_{\mathcal{N}} = \{+, \cdot, S, <, 0\}$. We specify the theory Q with the following axioms.

- Q1. $\forall x \ Sx \neq 0$.
- Q2. $\forall x \forall y \ Sx = Sy \rightarrow x = y$.
- Q3. $\forall x \ x + 0 = x$.
- Q4. $\forall x \forall y \ x + Sy = S(x + y)$.
- Q5. $\forall x \ x \cdot 0 = 0$.
- Q6. $\forall x \forall y \ x \cdot Sy = x \cdot y + x$.
- Q7. $\forall x \ \neg(x < 0)$.
- Q8. $\forall x \forall y \ x < Sy \leftrightarrow x < y \vee x = y$.
- Q9. $\forall x \forall y \ x < y \vee x = y \vee y < x$.

Note that the natural numbers, \mathcal{N} , are a model of the theory Q . If we add to this theory the set of all generalizations of formulas of the form

$$(\varphi_0^x \wedge \forall x(\varphi \rightarrow \varphi_{Sx}^x)) \rightarrow \varphi,$$

providing the capability for induction, we call this theory Peano Arithmetic, or PA . Thus $Q \subset PA$, and $PA \vdash Q$.

Notation. We define, for a natural number n ,

$$\underline{n} \equiv \underbrace{SS \dots S}_n 0.$$

Definition. A function $f : \omega^n \rightarrow \omega$ is **representable** in Q if there exists an $\mathcal{L}_{\mathcal{N}}$ -formula $\varphi(x_1, \dots, x_n, y)$ such that

$$Q \vdash \forall y(\varphi(\underline{k}_1, \dots, \underline{k}_n, y) \leftrightarrow y = \underline{f(k_1, \dots, k_n)})$$

for all $k_1, \dots, k_n \in \omega$. We say φ represents f in Q .

Definition. A relation $P \subset \omega^n$ is **representable** in Q if there exists an \mathcal{L}_N -formula $\varphi(x_1, \dots, x_n)$ such that for all $k_1, \dots, k_n \in \omega$,

$$P(k_1, \dots, k_n) \rightarrow Q \vdash \varphi(\underline{k_1}, \dots, \underline{k_n})$$

and

$$\neg P(k_1, \dots, k_n) \rightarrow Q \vdash \neg \varphi(\underline{k_1}, \dots, \underline{k_n}).$$

Again, we say that φ represents P in Q .

To prove the Representability Theorem, we will require the following:

Lemma 1. If $m = n$, then $Q \vdash \underline{m} = \underline{n}$, and if $m \neq n$, then $Q \vdash \neg(\underline{m} = \underline{n})$.

Proof. It is enough to demonstrate this for $m > n$. For $n = 0$, our result follows from axiom Q1. Assume, then, that the result holds for $k = n$ and all $l > k$. Then we have that, for a given $m > n + 1$, $Q \vdash \underline{m-1} \neq \underline{n}$. By axiom Q2 we have, $Q \vdash \underline{m-1} \neq \underline{n} \rightarrow \underline{m} \neq \underline{n+1}$. Hence we conclude that $Q \vdash \underline{m} \neq \underline{n+1}$, and the result holds for $k = n + 1$, as required.

Lemma 2. $Q \vdash \underline{m} + \underline{n} = \underline{m+n}$.

Proof. For $n = 0$, our result follows from axiom Q3. Assume, then, that the result holds for $k = n$. We must show it holds for $k = n + 1$ as well. But $Q \vdash \underline{m} + \underline{n} = \underline{m+n}$, and we obtain $Q \vdash \underline{m} + \underline{n+1} = \underline{m+n+1}$ by Q4.

Lemma 3. $Q \vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$

Proof. For $n = 0$, our result follows from axiom Q5. Assume, then, that the result holds for $k = n$. Then $Q \vdash \underline{m} \cdot \underline{n} = \underline{mn}$. Applying Q6, we have that $Q \vdash \underline{m} \cdot \underline{n+1} = \underline{mn} + \underline{m}$, and applying the previous lemma, we have the result for $k = n + 1$, as required.

Lemma 4. If $m < n$, then $Q \vdash \underline{m} < \underline{n}$. Further, if $m \geq n$, we have $Q \vdash \neg(\underline{m} < \underline{n})$.

Proof. For $n = 0$, the result follows from Q7. Assume, then, that the results hold for $k = n$. We show both claims hold for $k = n + 1$ as well.

First, suppose $m < n + 1$. Either $m < n$, and $Q \vdash \underline{m} < \underline{n}$ by the induction hypothesis, or $m = n$, and $Q \vdash \underline{m} = \underline{n}$ by Lemma 1. In either case, by Q8, we have that $Q \vdash \underline{m} < \underline{n+1}$.

Second, suppose $m \geq n + 1$. Then $m > n$ and by the induction hypothesis, $Q \vdash \neg(\underline{m} < \underline{n})$. By Lemma 1, we also have $Q \vdash \neg(\underline{m} = \underline{n})$. Applying Q8 and Rule T, we have $Q \vdash \underline{m} > \underline{n}$. Again applying Rule T, we have that $Q \vdash \neg(\underline{m} < \underline{n+1})$, as desired.

Lemma 5. For any relation $P \subset \omega^n$, P is representable in Q if and only if χ_P is representable.

Proof. Assume P is representable and that $\varphi(x_1 \dots x_n)$ represents P . Let

$$\psi(\bar{x}, y) \equiv (\varphi(\bar{x}) \wedge y = 0) \vee (\neg \varphi(\bar{x}) \wedge y = \underline{1}).$$

We claim $\psi(\bar{x}, y)$ represents χ_P :

Suppose $P(k_1, \dots, k_n)$ holds. Then $Q \vdash \varphi(\underline{k_1}, \dots, \underline{k_n})$. Now since

$$\varphi(\underline{k_1}, \dots, \underline{k_n}) \rightarrow (y = 0 \leftrightarrow \psi(\underline{k_1}, \dots, \underline{k_n}, y))$$

is a tautology, we have $Q \vdash y = 0 \iff \psi(\underline{k}_1, \dots, \underline{k}_n, y)$, as required. Similarly, if $\neg P(k_1, \dots, k_n)$ holds, then $Q \vdash \neg\varphi(\underline{k}_1, \dots, \underline{k}_n)$, and since

$$\vdash \neg\varphi(\underline{k}_1, \dots, \underline{k}_n) \rightarrow (y = \underline{1} \iff \psi(\underline{k}_1, \dots, \underline{k}_n, y)),$$

we obtain that $Q \vdash y = \underline{1} \iff \psi(\underline{k}_1, \dots, \underline{k}_n, y)$, as required. Thus, $\psi(\bar{x}, y)$ represents χ_P .

Assume now that $\psi(\bar{x}, y)$ represents χ_P . Then $\psi(\bar{x}, 0)$ represents P .

In particular, when $P(k_1, \dots, k_n)$ holds, we have

$$Q \vdash \psi(\underline{k}_1, \dots, \underline{k}_n, y) \iff y = 0.$$

Substitution of y by 0 yields $Q \vdash \psi(\underline{k}_1, \dots, \underline{k}_n, 0)$, as desired. Similarly, when $\neg P(k_1, \dots, k_n)$ holds, we have

$$Q \vdash \psi(\underline{k}_1 \dots \underline{k}_n, y) \iff y = \underline{1},$$

and because $Q \vdash \neg(0 = \underline{1})$ we may conclude $Q \vdash \neg\psi(\underline{k}_1 \dots \underline{k}_n, 0)$, as needed. Thus is P representable.

Lemma 6. For a formula φ in $\mathcal{L}_{\mathcal{N}}$,

$$Q \vdash \varphi_0^x \rightarrow \dots \rightarrow (\varphi_{\underline{k}-1}^x \rightarrow (x < \underline{k} \rightarrow \varphi))$$

Proof. The proof is by induction on k . When k is 0, we have

$$Q \vdash (x < 0 \rightarrow \varphi).$$

This is (vacuously) true by axiom Q7. Now, assume that

$$Q \vdash \varphi_0^x \rightarrow \dots \rightarrow (\varphi_{\underline{k}-1}^x \rightarrow (x < \underline{k} \rightarrow \varphi)).$$

We must show that

$$Q \vdash \varphi_0^x \rightarrow \dots \rightarrow (\varphi_{\underline{k}}^x \rightarrow (x < \underline{k} + \underline{1} \rightarrow \varphi)).$$

Equivalently, we want to show that $\Gamma \vdash \varphi$ where $\Gamma = Q \cup \{\varphi_0^x, \dots, \varphi_{\underline{k}}^x, x < \underline{k} + \underline{1}\}$. By Q8, $\Gamma \vdash x < \underline{k} \vee x = \underline{k}$. In the first case, the inductive hypothesis implies that $\Gamma \vdash \varphi$, while in the latter case, $\models x = \underline{k} \rightarrow (\varphi_{\underline{k}}^x \iff \varphi)$, and hence $\Gamma \vdash \varphi$. By either route, Γ proves φ .

Lemma 7. If (a) $Q \vdash \neg\varphi_{\underline{k}}^x$ for each $k < n$, and (b) $Q \vdash \varphi_{\underline{n}}^x$, then for $z \neq x$ not appearing in φ ,

$$Q \vdash (\varphi \wedge \forall z(z < x \rightarrow \neg\varphi_z^x)) \iff x = \underline{n}.$$

Proof. We define

$$\psi \equiv (\varphi \wedge \forall z(z < x \rightarrow \neg\varphi_z^x)).$$

Now, we obtain

$$\models x = \underline{n} \rightarrow (\psi \iff (\varphi_{\underline{n}}^x \wedge \forall z(z < \underline{n} \rightarrow \neg\varphi_z^x))). \quad (*)$$

By (a) and Lemma 6, we get

$$Q \vdash x < \underline{n} \rightarrow \neg\varphi, \quad (**)$$

and, applying substitution and generalization, we obtain

$$Q \vdash \forall z(z < \underline{n} \rightarrow \neg\varphi_z^x).$$

Combining this with (b) and (*), we conclude

$$Q \vdash x = \underline{n} \rightarrow \psi.$$

For the reverse implication, we note that

$$\models \forall z(z < x \rightarrow \neg\varphi_z^x) \rightarrow (\underline{n} < x \rightarrow \neg\varphi_{\underline{n}}^x),$$

and thus (b) implies $Q \vdash \psi \rightarrow \neg(\underline{n} < x)$. Now $Q \cup \{\psi, x < \underline{n}\} \vdash \varphi \wedge \neg\varphi$ by (**) and the definition of ψ . Therefore $Q \vdash \psi \rightarrow \neg(x < \underline{n})$ and by Axiom Q9 we conclude $Q \vdash \psi \rightarrow x = \underline{n}$.

Representability Theorem. *Every recursive function or relation is representable in Q .*

Proof. It suffices to prove representability of functions having the forms enumerated in the definition of recursiveness:

R1. I_i^n , $+$, \cdot , and $\chi_{<}$.

The latter three are representable by Lemmas 2, 3, and 4. In particular, for $+$, say, we have that $\varphi(x_1, x_2, y) \equiv y = x_1 + x_2$ represents $+$ in Q , since for any $m, n \in \omega$,

$$\begin{aligned} Q \vdash \underline{m} + \underline{n} &= \underline{m+n}, \\ Q \vdash y = \underline{m} + \underline{n} &\longleftrightarrow y = \underline{m+n}, \\ Q \vdash \varphi(\underline{m}, \underline{n}, y) &\longleftrightarrow y = \underline{m+n}, \text{ and hence} \\ Q \vdash \forall y(\varphi(\underline{m}, \underline{n}, y) &\longleftrightarrow y = \underline{m+n}), \end{aligned}$$

as required. \cdot and $\chi_{<}$ are similar (with $\chi_{<}$ making additional use of Lemma 5).

I_i^n is representable by $\varphi(x_1, \dots, x_n, y) \equiv x_i = y$. In particular, for any $k_1, \dots, k_n \in \omega$, $I_i^n(k_1, \dots, k_n) = k_i$, and hence

$$Q \vdash \varphi(\underline{k}_1, \dots, \underline{k}_n, y) \longleftrightarrow y = \underline{k}_i \longleftrightarrow y = \underline{I_i^n(k_1, \dots, k_n)},$$

by our choice of φ . Generalization completes the result.

R2. $F(\bar{a}) = G(H_1(\bar{a}), \dots, H_k(\bar{a}))$, where G and each of the H_i are representable.

Assume that G is represented in Q by φ and the H_i are represented in Q by ψ_i , respectively. We show that F is represented by

$$\alpha(\bar{x}, y) \equiv \exists z_1, \dots, z_k(\psi_1(\bar{x}, z_1) \wedge \dots \wedge \psi_k(\bar{x}, z_k) \wedge \varphi(z_1, \dots, z_k, y)).$$

In other word we want to show, for any $a_1, \dots, a_n \in \omega$,

$$Q \vdash \alpha(\underline{a}_1, \dots, \underline{a}_n, y) \longleftrightarrow y = \underline{G(H_1(\bar{a}), \dots, H_k(\bar{a}))} \quad (\dagger)$$

where $\bar{a} = (a_1 \dots a_n)$.

Now, for $\Gamma = Q \cup \{\alpha(\underline{a}_1, \dots, \underline{a}_n, y)\}$, since the ψ_i represent H_i , we have that $\Gamma \vdash \exists z_1, \dots, z_k(z_1 = \underline{H_1(\bar{a})} \wedge \dots \wedge z_k = \underline{H_k(\bar{a})} \wedge \varphi(z_1, \dots, z_k, y))$. Hence we have

$$\Gamma \models \exists z_1, \dots, z_k(\varphi(\underline{H_1(\bar{a})}, \dots, \underline{H_k(\bar{a})}, y)),$$

and since the z_i do not appear,

$$\Gamma \models \varphi(\underline{H_1(\bar{a})}, \dots, \underline{H_k(\bar{a})}, y).$$

Since φ represents G , we have

$$\Gamma \models y = \underline{G(H_1(\bar{a}), \dots, H_k(\bar{a}))},$$

as required.

$$\begin{aligned}
& \text{On the other hand, for } \Sigma = Q \cup \{y = \underline{G(H_1(\bar{a}), \dots, H_k(\bar{a}))}\}, \\
& \Sigma \vdash \varphi(\underline{H_1(\bar{a})}, \dots, \underline{H_k(\bar{a})}, y) \\
& \Sigma \vdash \exists z_1, \dots, z_k (z_1 = \underline{H_1(\bar{a})} \wedge \dots \wedge z_k = \underline{H_k(\bar{a})} \wedge \varphi(z_1, \dots, z_k, y)) \\
& \Sigma \vdash \exists z_1, \dots, z_k (\psi_1(\bar{a}, z_1) \wedge \dots \wedge \psi_k(\bar{a}, z_k) \wedge \varphi(z_1, \dots, z_k, y)) \\
& \Sigma \vdash \alpha(\underline{a_1}, \dots, \underline{a_n}, y)
\end{aligned}$$

Thus (\dagger) is established.

R3. $F(\bar{a}) = \mu x (G(\bar{a}, x) = 0)$, where G is representable in Q and for all \bar{a} there exists x such that $G(\bar{a}, x) = 0$, is representable in Q .

Assume G is represented in Q by $\varphi(x_1, \dots, x_n, x, y)$. Let

$$\psi(x_1, \dots, x_n, x) \equiv \varphi_0^y \wedge \forall z (z < x \rightarrow \neg \varphi_{0z}^{yx}).$$

Let $F(\bar{a}) = b$ and $k_i = G(\bar{a}, i)$ for $i \in \omega$. Then

$$Q \vdash \varphi(\underline{a_1}, \dots, \underline{a_n}, \underline{i}, y) \longleftrightarrow y = \underline{k_i},$$

thus

$$Q \vdash \varphi(\underline{a_1}, \dots, \underline{a_n}, \underline{i}, 0) \longleftrightarrow 0 = \underline{k_i},$$

. Hence now if $j < b$, so that $k_j \neq 0$, then

$$Q \vdash \neg \varphi(\underline{a_1}, \dots, \underline{a_n}, \underline{j}, 0).$$

On the other hand, $k_b = 0$, so

$$Q \vdash \varphi(\underline{a_1}, \dots, \underline{a_n}, \underline{b}, 0).$$

Hence, by Lemma 7,

$$Q \vdash (\varphi(\bar{a}, x, y)_0^y \wedge \forall z (z < x \rightarrow \neg \varphi(\bar{a}, x, y)_{0z}^{yx})) \longleftrightarrow x = \underline{b},$$

and thus,

$$Q \vdash \psi(\bar{a}, x) \longleftrightarrow x = \underline{b}.$$

By generalization, we have that ψ represents F in Q , as desired.

Step 2: Axiomatizable Complete Theories are Decidable

We begin by showing that we may encode terms and formulas of a reasonable language in such a way that important classes of formulas, e.g., the logical axioms, are mapped to recursive subsets of the natural numbers. We use this to derive the main result.

Definition. Let \mathcal{L} be a countable language with subsets \mathcal{C} , \mathcal{F} , and \mathcal{P} of constant, function, and predicate symbols, respectively ($= \in \mathcal{P}$). Let \mathcal{V} be a set of variables for \mathcal{L} . \mathcal{L} is called reasonable if the following two functions exist:

- $h : \mathcal{L} \cup \{\neg, \rightarrow, \forall\} \cup \mathcal{V} \rightarrow \omega$ injective such that $\underline{\mathcal{V}} = h(\mathcal{V})$, $\underline{\mathcal{C}} = h(\mathcal{C})$, $\underline{\mathcal{F}} = h(\mathcal{F})$, and $\underline{\mathcal{P}} = h(\mathcal{P})$ are all recursive.
- $\text{AR} : \omega \rightarrow \omega \setminus \{0\}$ recursive such that $\text{AR}(h(f)) = n$ and $\text{AR}(h(P)) = n$ for n -ary function and predicate symbols f and P .

For the rest of this note, the language \mathcal{L} is countable and reasonable.

Now we define a coding $\lceil \cdot \rceil : \{\mathcal{L}\text{-terms and } \mathcal{L}\text{-formulas}\} \rightarrow \omega$ inductively, by

- For $x \in \mathcal{V} \cup \mathcal{C}$, $\lceil x \rceil = \langle h(x) \rangle$.

- For \mathcal{L} -terms u_1, \dots, u_n and n -ary $f \in \mathcal{F}$,

$$[fu_1u_2 \dots u_n] = \langle h(f), [u_1], [u_2], \dots, [u_n] \rangle .$$
- For \mathcal{L} -terms t_1, \dots, t_n and $P \in \mathcal{P}$,

$$[Pt_1t_2 \dots t_n] = \langle h(P), [t_1], \dots, [t_n] \rangle .$$
- For \mathcal{L} -formulas φ and ψ ,

$$\begin{aligned} [\varphi \rightarrow \psi] &= \langle h(\rightarrow), [\varphi], [\psi] \rangle, \\ [\neg\varphi] &= \langle h(\neg), [\varphi] \rangle, \\ [\forall x\varphi] &= \langle h(\forall), [x], [\varphi] \rangle . \end{aligned}$$

Note that our definition of $[\]$ is one-to-one. Given a term or formula σ , we call $[\sigma]$ the Gödel number of σ .

We show the following predicates and functions are recursive (We follow definitions for syntax in [E].):

- (1) $Vble = \{[v] \mid v \in \mathcal{V}\} \subset \omega$ and $Const = \{[c] \mid c \in \mathcal{C}\} \subset \omega$.

Proof. Note

$$\begin{aligned} Vble(x) &\text{ iff } x = \langle (x)_1 \rangle \wedge \underline{\mathcal{V}}((x)_1), \\ Const(x) &\text{ iff } x = \langle (x)_1 \rangle \wedge \underline{\mathcal{C}}((x)_1). \end{aligned}$$

- (2) $Term = \{[t] \mid t \text{ an } \mathcal{L}\text{-term}\} \subset \omega$.

Proof. Note

$$Term(a) \text{ iff } \begin{cases} \forall j < (lh(a) \dot{-} 1) \ Term((a)_{j+2}) & \text{if } Seq(a) \wedge \underline{\mathcal{F}}((a)_1) \\ & \wedge AR((a)_1) = lh(a) \dot{-} 1, \\ Vble(a) \vee Const(a) & \text{otherwise.} \end{cases}$$

- (3) $AtF = \{[\sigma] \mid \sigma \text{ an atomic } \mathcal{L}\text{-formula}\} \subset \omega$.

Proof. Note

$$\begin{aligned} AtF(a) &\text{ iff } Seq(a) \wedge \underline{\mathcal{P}}((a)_1) \wedge (AR((a)_1) = lh(a) \dot{-} 1) \\ &\quad \wedge \forall j < (lh(a) \dot{-} 1) (Term((a)_{j+2})). \end{aligned}$$

- (4) $Form = \{[\varphi] \mid \varphi \text{ an } \mathcal{L}\text{-formula}\} \subset \omega$.

Proof. Note

$$Form(a) \text{ iff } \begin{cases} Form((a)_2) & \text{if } a = \langle h(\neg), (a)_2 \rangle, \\ Form((a)_2) \wedge Form((a)_3) & \text{if } a = \langle h(\rightarrow), (a)_2, (a)_3 \rangle, \\ Vble((a)_2) \wedge Form((a)_3) & \text{if } a = \langle h(\forall), (a)_2, (a)_3 \rangle, \\ AtF(a) & \text{otherwise.} \end{cases}$$

- (5) $Sub : \omega^3 \rightarrow \omega$, such that $Sub([t], [x], [u]) = [t_u^x]$ and $Sub([\varphi], [x], [u]) = [\varphi_u^x]$ for terms t and u , variable x , and formula φ .

Proof. Define

$$Sub(a, b, c) = \begin{cases} c & \text{if } Vble(a) \wedge a = b, \\ \langle (a)_1, Sub((a)_2, b, c), \dots \\ \quad \dots, Sub((a)_{lh(a)}, b, c) \rangle & \text{if } lh(a) > 1 \wedge (a)_1 \neq h(\forall) \\ \quad \wedge Seq(a), \\ \langle (a)_1, (a)_2, Sub((a)_3, b, c) \rangle & \text{if } a = \langle h(\forall), (a)_2, (a)_3 \rangle, \\ \quad \wedge (a)_2 \neq b \\ a & \text{otherwise.} \end{cases}$$

Note that, if well-defined, the function has the properties desired above.

We show Sub is well-defined by induction on a : $a = 0$ falls into the first or last category since $lh(0) = 0$, hence $Sub(0, b, c)$ is well-defined for all $b, c \in \omega$. If $a \neq 0$, then $(a)_i < a$ for all $i \leq lh(a)$, and thus we may assume the values $Sub((a)_i, b, c)$ are well-defined, showing $Sub(a, b, c)$ to be well-defined in all cases.

- (6) $Free \subset \omega^2$, such that for formula φ , term τ , and variable x , $Free(\lceil \varphi \rceil, \lceil x \rceil)$ if and only if x occurs free in φ , and $Free(\lceil \tau \rceil, \lceil x \rceil)$ if and only if x occurs in τ

Proof. Define

$$Free(a, b) \text{ iff } \begin{cases} \exists j < (lh(a) - 1) (Free((a)_{j+2}, b)) & \text{if } lh(a) > 1 \wedge (a)_1 \neq h(\forall), \\ Free((a)_3, b) \wedge (a)_2 \neq b & \text{if } lh(a) > 1 \wedge (a)_1 = h(\forall), \\ a = b & \text{otherwise.} \end{cases}$$

$Free$ clearly has the desired property, and that it is well-defined follows by essentially the same induction on a as above.

- (7) $Sent = \{\lceil \varphi \rceil \mid \varphi \text{ is an } \mathcal{L}\text{-sentence}\} \subset \omega$.

Proof. Note

$$Sent(a) \text{ iff } Form(a) \wedge \forall b < a (\neg Vble(b) \vee \neg Free(a, b)).$$

- (8) $Subst(a, b, c) \subset \omega^3$ such that for a given formula φ , variable x , and term t , $Subst(\lceil \varphi \rceil, \lceil x \rceil, \lceil t \rceil)$ if and only if t is substitutable for x in φ .

Proof. Define

$$Subst(a, b, c) \text{ iff } \begin{cases} Subst((a)_2, b, c) & \text{if } a = \langle h(\neg), (a)_2 \rangle, \\ Subst((a)_2, b, c) \wedge Subst((a)_3, b, c) & \text{if } a = \langle h(\rightarrow), (a)_2, (a)_3 \rangle, \\ \neg Free(a, b) \vee (\neg Free(c, (a)_2) \\ \quad \wedge Subst((a)_3, b, c)) & \text{if } a = \langle h(\forall), (a)_2, (a)_3 \rangle, \\ 0 = 0 & \text{otherwise.} \end{cases}$$

Note that $Subst$ has the desired property, and is well-defined by essentially the same induction used above.

(9) We define

$$False(a, b) \text{ iff } \begin{cases} \neg False((a)_2, b) \wedge False((a)_3, b) & \text{if } a = \langle h(\rightarrow), (a)_2, (a)_3 \rangle \\ \quad \quad \quad \wedge Form((a)_2) \wedge Form((a)_3), & \\ \neg False((a)_2, b) & \text{if } a = \langle h(\neg), (a)_2 \rangle \wedge Form((a)_2), \\ Form(a) \wedge (b)_a = 0 & \text{otherwise.} \end{cases}$$

False is recursive by the same induction as applied above. We note the significance of *False* presently.

To each $b \in \omega$, we may associate a truth assignment v_b such that for a prime formula ψ (atomic or of the form $\forall x\varphi$),

$$v_b(\psi) = F \text{ iff } (b)_{[\psi]} = 0.$$

Further, for any truth assignment $v : A \rightarrow \{T, F\}$, where A is a finite set of prime formulas, there exists a b such that $v = v_b$: we may write $A = \{\varphi_1, \dots, \varphi_n\}$ such that $[\varphi_1] < [\varphi_2] < \dots < [\varphi_n]$. For $1 \leq j \leq [\varphi_n]$ define $c_j = 0$ when $j = [\varphi_i]$ for some $i \leq n$ and $v(\varphi_i) = F$, and $c_j = 1$ otherwise. Then $b = \langle c_1, \dots, c_{[\varphi_n]} \rangle$ satisfies $v_b = v$ on A .

Then moreover, for any formula φ built up from A ,

$$\bar{v}(\varphi) = F \text{ iff } \bar{v}_b(\varphi) = F \text{ iff } False([\varphi], b).$$

(10) Define $Taut = \{[\sigma] \mid \sigma \text{ is a tautology}\} \subset \omega$.

Proof. Recall $bd : \omega \rightarrow \omega$ such that $bd(a) = \max\{\langle c_1, \dots, c_a \rangle \mid c_i \in \{0, 1\}\}$, recursive, has been previously defined. Define

$$Taut(a) \text{ iff } Form(a) \wedge \forall b < (bd(a) + 1) (\neg False(a, b)).$$

(11) $\underline{AG2} = \{[\varphi] \mid \varphi \text{ is in axiom group 2}\} \subset \omega$.

Proof. Recall axiom group 2 contains formulas of the form $\forall x\psi \rightarrow \psi_t^x$, with term t substitutable for x in ψ . Thus

$$\begin{aligned} \underline{AG2}(a) \text{ iff } \exists x, y, z < a (Vble(x) \wedge Form(y) \wedge Term(z) \wedge Subst(y, x, z) \\ \wedge a = \langle h(\rightarrow), \langle h(\forall), x, y \rangle, Sub(y, x, z) \rangle), \end{aligned}$$

where $\exists x, y, z < a P(x, y, z)$ abbreviates what one would expect.

(12) $\underline{AG3} = \{[\varphi] \mid \varphi \text{ is in axiom group 3}\} \subset \omega$.

Proof. Recall we take axiom group 3 to be the formulas having the following form: $\forall x(\psi \rightarrow \psi') \rightarrow (\forall x\psi \rightarrow \forall x\psi')$. Thus

$$\begin{aligned} \underline{AG3}(a) \text{ iff } \exists x, y, z < a (Vble(x) \wedge Form(y) \wedge Form(z) \\ \wedge a = \langle h(\rightarrow), \langle h(\forall), x, \langle h(\rightarrow), y, z \rangle \rangle, \\ \langle h(\rightarrow), \langle h(\forall), x, y \rangle, \langle h(\forall), x, z \rangle \rangle \rangle) \end{aligned}$$

(13) $\underline{AG4} = \{[\varphi] \mid \varphi \text{ is in axiom group 4}\} \subset \omega$.

Proof. Recall axiom group 4 contains formulas of the form $\psi \rightarrow \forall x\psi$, where x does not occur free in ψ . Thus

$$\begin{aligned} \underline{\text{AG4}}(a) \text{ iff } \exists x, y < a (Vble(x) \wedge Form(y) \\ \wedge \neg Free(y, x) \wedge a = \langle h(\rightarrow), y, \langle h(\forall), x, y \rangle \rangle) \end{aligned}$$

$$(14) \underline{\text{AG5}} = \{[\varphi] \mid \varphi \text{ is in axiom group 5}\} \subset \omega.$$

Proof. Recall axiom group 5 contains formulas of the form $x = x$, for a variable x , hence

$$\underline{\text{AG5}}(a) \text{ iff } \exists x < a (Vble(x) \wedge a = \langle h(=), x, x \rangle).$$

$$(15) \underline{\text{AG6}} = \{[\varphi] \mid \varphi \text{ is in axiom group 6}\} \subset \omega.$$

Proof. Recall formulas of axiom group 6 have the form $x = y \rightarrow (\psi \rightarrow \psi')$, where ψ is an atomic formula and ψ' is obtained by from ψ by replacing one or more occurrences of x with y . Thus

$$\begin{aligned} \underline{\text{AG6}}(a) \text{ iff } \exists x, y, b, c < a (Vble(x) \wedge Vble(y) \wedge AtF(b) \wedge AtF(c) \\ \wedge lh(b) = lh(c) \wedge \forall j < lh(b) + 1 ((c)_j = (b)_j \vee ((c)_j = y \wedge (b)_j = x)) \\ \wedge a = \langle h(\rightarrow), \langle h(=), x, y \rangle, \langle h(\rightarrow), b, c \rangle \rangle) \end{aligned}$$

$$(16) \text{Gen}(a, b) \subset \omega^2, \text{ such that } \text{Gen}([\varphi], [\psi]) \text{ if and only if } \varphi \text{ is a generalization of } \psi \text{ (i.e., } \varphi = \forall x_1 \dots \forall x_n \psi \text{ for some finite } \{x_i\} \subset \mathcal{V}\text{)}.$$

Proof. Note that

$$\text{Gen}(a, b) \text{ iff } \begin{cases} a = \langle h(\forall), (a)_2, (a)_3 \rangle \wedge Vble((a)_2) \wedge \text{Gen}((a)_3, b) & \text{if } a > b, \\ 0 = 0 & \text{if } a = b, \\ 0 = 1 & \text{if } a < b. \end{cases}$$

$$(17) \underline{\Lambda} = \{[\sigma] \mid \sigma \in \Lambda\} \subset \omega, \text{ where } \Lambda \text{ is the set of logical axioms.}$$

Proof. Note that

$$\begin{aligned} \underline{\Lambda}(a) \text{ iff } \exists b < a + 1 (Form(a) \wedge \text{Gen}(a, b) \\ \wedge (Taut(b) \vee \underline{\text{AG2}}(b) \vee \underline{\text{AG3}}(b) \vee \underline{\text{AG4}}(b) \vee \underline{\text{AG5}}(b) \vee \underline{\text{AG6}}(b))) \end{aligned}$$

We have, to this point, defined three codings: $\langle \rangle$ on sequences of natural numbers, h on the language and logical symbols, and $[\]$ on the terms and formulas. We presently define a fourth coding, of sequences of formulas:

$$\llbracket \] : \{\text{sequences of } \mathcal{L}\text{-formulas}\} \rightarrow \omega,$$

given by

$$\llbracket \varphi_1, \dots, \varphi_n \rrbracket = \langle [\varphi_1], \dots, [\varphi_n] \rangle.$$

This map is one-to-one, as it is derived from the established (injective) codings, and in particular, we can determine, for a given number, if it lies in the image of $\llbracket \cdot \rrbracket$, and, if so, recover the associated sequence of formulas.

Definition. Given \mathcal{L} , let T be a theory (a collection of sentences) in \mathcal{L} . Define

$$\underline{T} = \{ \lceil \sigma \rceil \mid \sigma \in T \}.$$

We say that T is **axiomatizable** if there exists a theory S , axiomatizing T (that is, such that $\text{Cn } S = \text{Cn } T$), such that \underline{S} is recursive. We say that T is **decidable** if $\underline{\text{Cn } T}$ is recursive.

We shall make use of the following relations:

- $Ded_T = \{ \llbracket \varphi_1, \dots, \varphi_n \rrbracket \mid \varphi_1, \dots, \varphi_n \text{ is a deduction from } T \} \subset \omega$.
Note that

$$Ded_T(a) \text{ iff } Seq(a) \wedge lh(a) \neq 0$$

$$\wedge \forall j < lh(a) (\underline{\Delta}((a)_{j+1}) \vee \underline{T}((a)_{j+1}) \vee \exists i, k < j+1 ((a)_{k+1} = \langle h(\rightarrow), (a)_{i+1}, (a)_{j+1} \rangle))$$

- $Prf_T \subset \omega^2$, given by $Prf_T(a, b)$ iff $Ded_T(b) \wedge a = (b)_{lh(b)}$.
- $Pf_T \subset \omega$, given by $Pf_T(a)$ iff $Sent(a) \wedge \exists x Prf_T(a, x)$.

Note that we may read $Prf_T(a, b)$ as “ b is a proof of a from T ,” and $Pf_T(a)$ as “ a is a sentence provable from T .” In particular

$$Pf_T = \underline{\text{Cn } T} = \{ \lceil \sigma \rceil \mid T \vdash \sigma \}.$$

We use this fact to prove the following:

Theorem. *If T is axiomatizable, then $Pf_T = \underline{\text{Cn } T}$ is recursively enumerable.*

Proof. Let S axiomatize T , where S is recursive. From the above definitions, we see that Ded_S and Prf_S are recursive relations, hence Pf_S is an r.e. relation. But $Pf_S = Pf_T$, since $\text{Cn } S = \text{Cn } T$.

Theorem. *If T is axiomatizable and complete in \mathcal{L} , then T is decidable.*

Proof. By the negation theorem, it suffices to show that $\neg Pf_T$ is recursively enumerable. Note that since T is complete, for any sentence σ , $T \not\vdash \sigma$ if and only if $T \vdash \neg\sigma$. Hence

$$\begin{aligned} \neg Pf_T(a) &\text{ iff } \neg Sent(a) \vee \exists m Prf_T(\langle h(\neg), a \rangle, m) \\ &\text{ iff } \exists m (\neg Sent(a) \vee Prf_T(\langle h(\neg), a \rangle, m)). \end{aligned}$$

Thus $\neg Pf_T$ is recursively enumerable, and Pf_T is recursive.

We can see that if we say T is axiomatizable in wider sense when S axiomatizing T is recursively enumerable, then the above two theorems still hold with this seemingly weaker notion. In fact, two notions are equivalent, which is known as Craig’s Theorem.

Step 3: The Incompleteness Theorems and Other Results

We return now to the language of natural numbers, \mathcal{L}_N . Recall that we define, for a natural number n ,

$$\underline{n} \equiv \underbrace{SS \dots S}_n 0.$$

Definition. The **diagonalization** of an $\mathcal{L}_{\mathcal{N}}$ formula φ is a new formula

$$d(\varphi) \equiv \exists v_0(v_0 = \ulcorner \varphi \urcorner \wedge \varphi),$$

where \exists and \wedge provide the usual abbreviations in $\mathcal{L}_{\mathcal{N}}$.

In particular, we note $d(\varphi)$ is satisfiable precisely when φ is satisfiable by some truth assignment taking v_0 to the Gödel number of φ , and $\mathcal{L}_{\mathcal{N}} \models d(\varphi)$ precisely when φ is satisfied by *every* truth assignment taking v_0 to $\ulcorner \varphi \urcorner$.

Lemma. There exists a recursive function $dg : \omega \rightarrow \omega$ such that for any $\mathcal{L}_{\mathcal{N}}$ formula, $dg(\ulcorner \varphi \urcorner) = \ulcorner d(\varphi) \urcorner$.

Proof. Define $num : \omega \rightarrow \omega$ by $num(0) = \langle 0 \rangle$ and, for $n \in \omega$

$$num(n+1) = \langle h(S), num(n) \rangle.$$

In particular, note that $num(n) = \ulcorner \underline{n} \urcorner$.

Define

$$dg(a) = \langle h(\neg), \langle h(\forall), \ulcorner v_0 \urcorner, \langle h(\neg), \langle h(\neg), \langle h(\rightarrow), \langle h(=), \ulcorner v_0 \urcorner, num(a) \rangle, \langle h(\neg), a \rangle \rangle \rangle \rangle \rangle \rangle$$

Then

$$\begin{aligned} dg(\ulcorner \varphi \urcorner) &= \langle h(\neg), \langle h(\forall), \ulcorner v_0 \urcorner, \langle h(\neg), \langle h(\neg), \langle h(\rightarrow), \langle h(=), \ulcorner v_0 \urcorner, num(\ulcorner \varphi \urcorner) \rangle, \langle h(\neg), \ulcorner \varphi \urcorner \rangle \rangle \rangle \rangle \rangle, \\ &= \langle h(\neg), \langle h(\forall), \ulcorner v_0 \urcorner, \langle h(\neg), \langle h(\neg), \langle h(\rightarrow), \langle h(=), \ulcorner v_0 \urcorner, \ulcorner \ulcorner \varphi \urcorner \urcorner \rangle, \langle h(\neg), \ulcorner \varphi \urcorner \rangle \rangle \rangle \rangle \rangle. \end{aligned}$$

However, writing out what formula this encodes and introducing our usual abbreviations, we have

$$\begin{aligned} dg(\ulcorner \varphi \urcorner) &= \ulcorner \neg \forall v_0 \neg (\neg (v_0 = \ulcorner \varphi \urcorner) \rightarrow \neg \varphi) \urcorner \\ &= \ulcorner \exists v_0 (v_0 = \ulcorner \varphi \urcorner \wedge \varphi) \urcorner \\ &= \ulcorner d(\varphi) \urcorner, \end{aligned}$$

as desired.

Fixed Point Theorem (Gödel). *For any $\mathcal{L}_{\mathcal{N}}$ -formula $\varphi(x)$ (i.e., either a sentence or a formula having x as the only free variable), there is some $\mathcal{L}_{\mathcal{N}}$ -sentence σ such that*

$$Q \vdash \sigma \longleftrightarrow \varphi(\ulcorner \sigma \urcorner).$$

Proof. Since dg is recursive, it is representable in Q by Step 1, say by $\psi(x, y)$. Then

$$Q \vdash \forall y (\psi(\underline{n}, y) \longleftrightarrow y = dg(n)).$$

Let $\delta(v_0) \equiv \exists y (\psi(v_0, y) \wedge \varphi(y))$, and let $n = \ulcorner \delta(v_0) \urcorner$. Define

$$\sigma \equiv d(\delta(v_0)) \equiv \exists v_0 (v_0 = \underline{n} \wedge \delta(v_0)).$$

Then if we let $k = dg(n) = \ulcorner \sigma \urcorner$, we have

$$\models \sigma \longleftrightarrow \delta(\underline{n}) \longleftrightarrow \exists y (\psi(\underline{n}, y) \wedge \varphi(y)).$$

But

$$Q \vdash \psi(\underline{n}, y) \longleftrightarrow y = \underline{k},$$

and therefore

$$Q \vdash \sigma \iff \exists y(y = \underline{k} \wedge \varphi(y)) \iff \varphi(\underline{k}) \iff \varphi([\sigma]),$$

as required.

Tarski Undefinability Theorem. $\text{Th}\mathcal{N} = \{[\sigma] \mid \mathcal{N} \models \sigma\}$ is not definable.

Proof. Suppose $\text{Th}\mathcal{N}$ were definable by $\beta(x)$. Then by the fixed point lemma, with $\varphi = \neg\beta$, there exists a sentence σ such that

$$\mathcal{N} \models \sigma \iff \neg\beta([\sigma]).$$

Then $\mathcal{N} \models \sigma$ implies that $\mathcal{N} \not\models \beta([\sigma])$, implying $\mathcal{N} \not\models \sigma$, or $\mathcal{N} \models \neg\sigma$, since $\text{Th}\mathcal{N}$ is complete. On the other hand, $\mathcal{N} \not\models \sigma$ implies $\mathcal{N} \models \neg\sigma$, and thus that $\mathcal{N} \models \beta([\sigma])$, implying $\mathcal{N} \models \sigma$. The contradictions together imply that β cannot represent $\text{Th}\mathcal{N}$.

Strong Undecidability of Q. Let T be a theory in $\mathcal{L} \supset \mathcal{L}_{\mathcal{N}}$. If $T \cup Q$ is consistent in \mathcal{L} , then T is not decidable in \mathcal{L} ($\text{Cn}T$ is not recursive).

Proof. Assume that $\text{Cn}T$ is recursive. We first show that this implies recursiveness of $\text{Cn}T \cup Q$. Since Q is finite, it suffices to show that for any sentence τ in the language, $\text{Cn}T \cup \{\tau\}$ is recursive.

In particular, note that if $\alpha \in \text{Cn}T \cup \{\tau\}$, then $\tau \rightarrow \alpha \in \text{Cn}T$. Thus

$$a \in \text{Cn}T \cup \{\tau\} \text{ iff } \text{Sent}(a) \wedge \langle h(\rightarrow), [\tau], a \rangle \in \text{Cn}T.$$

Hence $\text{Cn}T \cup \{\tau\}$ is recursive, as desired.

To prove the theorem, then, it suffices to show that $\text{Cn}T \cup Q$ is not recursive. If this were the case, then it would be representable, say by $\beta(x)$, in Q . By the fixed point lemma, there exists an $\mathcal{L}_{\mathcal{N}}$ sentence σ such that

$$Q \vdash \sigma \iff \neg\beta([\sigma]).$$

If $T \cup Q \vdash \sigma$, then

$$Q \vdash \beta([\sigma]),$$

by the representability of $\text{Cn}T \cup Q$ by $\beta(x)$ in Q . In particular,

$$Q \vdash \neg\sigma,$$

a contradiction. On the other hand, if $T \cup Q \not\vdash \sigma$, then by representability,

$$Q \vdash \neg\beta([\sigma]),$$

and hence

$$Q \vdash \sigma,$$

a contradiction, implying that $\text{Cn}T \cup Q$ is not representable, and hence not recursive.

Corollary. $\text{Th}\mathcal{N}$, PA , and Q are all undecidable.

Proof. We need note only that each of these theories is consistent with Q .

Moreover, we have:

Undecidability of First Order Logic (Church). *For a reasonable countable language $\mathcal{L} \supset \mathcal{L}_{\mathcal{N}}$, the set of all Gödel numbers of valid sentences ($\{[\sigma] \mid \emptyset \vdash \sigma\}$) is not recursive (the set of valid sentences is not decidable).*

In fact, the above corollary is true for any countable \mathcal{L} containing a k -ary predicate or function symbol, $k \geq 2$, or at least two unary function symbols.

Gödel-Rosser First Incompleteness Theorem. *If T is a theory in a countable reasonable $\mathcal{L} \supset \mathcal{L}_{\mathcal{N}}$, with $T \cup Q$ consistent and T axiomatizable, then T is not complete.*

Proof. By Step 2, if T is complete, then T is decidable, contradicting the strong undecidability of Q .

Remarks. In $(\mathcal{N}, +)$, 0 , $<$, and S are definable. Hence the same result follows if we take $\mathcal{L}'_{\mathcal{N}} = \{+, \cdot\}$ instead of our usual $\mathcal{L}_{\mathcal{N}}$. In particular, $\text{Th}(\mathcal{N}, +, \cdot)$ is undecidable, and for any $T' \supset Q'$ (where Q' is simply Q written in the language of $\mathcal{L}'_{\mathcal{N}}$), we have that T' is, if consistent, undecidable, and, if axiomatizable, incomplete.

It is important to note that for an undecidable theory T , we may have $T \subset T'$, where T' is a decidable theory. As an example, the theory of groups is undecidable, whereas the theory of divisible torsion-free groups is decidable.

We turn our attention now to the proof of the result used in Gödel's original paper. In particular, Gödel worked in the model $(\mathcal{N}, +, \cdot, 0, <, E)$. (Note that E , exponentiation, is definable in $(\mathcal{N}, +, \cdot, 0, <)$, or, equivalently, $(\mathcal{N}, +, \cdot)$).

Let $T \supset Q$ be a consistent theory in a reasonable countable language $\mathcal{L} \supset \mathcal{L}_{\mathcal{N}}$, and presume that \underline{T} is recursive. Then

$$T \vdash \sigma \Rightarrow Q \vdash Pf_T([\sigma]).$$

In particular, $T \vdash \sigma$ implies that $Prf_T([\sigma], m)$ for some $m \in \omega$. Since Prf_T is recursive, it is representable in Q , hence $Q \vdash Prf_T([\sigma], \underline{m})$, and

$$Q \vdash \exists x Prf_T([\sigma], x),$$

or

$$Q \vdash Pf_T([\sigma]).$$

By the fixed point lemma, there exists a sentence α such that

$$T \supset Q \vdash \alpha \iff \neg Pf_T([\alpha]). \quad (*)$$

If $T \vdash \alpha$, then $Q \vdash Pf_T([\alpha])$, and thus $Q \vdash \neg\alpha$, and hence $T \vdash \neg\alpha$, a contradiction. Thus $T \not\vdash \alpha$.

On the other hand, if T is ω -consistent (i.e., whenever $T \vdash \exists x \varphi(x)$, then for some $n \in \omega$, $T \not\vdash \neg\varphi(\underline{n})$), then $T \not\vdash \neg\alpha$. In particular, if $T \vdash \neg\alpha$, then

$$T \vdash Pf_T([\alpha]),$$

by (*). That is,

$$T \vdash \exists x Prf_T([\alpha], x).$$

However, if $Prf_T([\alpha], m)$ for some $m \in \omega$, then $T \vdash \alpha$, contradicting the consistency of T . Thus we must have $\neg Prf_T([\alpha], m)$ for all $m \in \omega$. Since Q represents Prf_T ,

$$T \supset Q \vdash \neg Prf_T([\alpha], m)$$

for all $m \in \omega$, contradicting the ω -consistency of T .

Rosser generalized Gödel's proof by singling out for T a sentence α such that $T \not\vdash \alpha$ and $T \not\vdash \neg\alpha$, without the assumption of ω -consistency.

We now begin our approach to Gödel's Second Incompleteness Theorem. We fix T , a theory in a countable reasonable language $\mathcal{L} \supset \mathcal{L}_{\mathcal{N}}$.

We note the following fact from Hilbert and Bernays' *Grundlagen der Mathematik*, 1934.

Fact. If T is consistent, $T \vdash PA$, and \underline{T} is recursive, then for any sentences σ and δ in \mathcal{L} ,

- I. $T \vdash \sigma \Rightarrow Q \vdash Pf_T(\underline{[\sigma]})$
- II. $PA \vdash (Pf_T(\underline{[\sigma]}) \wedge Pf_T(\underline{[\sigma \rightarrow \delta]})) \rightarrow Pf_T(\underline{[\delta]})$
- III. $PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[Pf_T(\underline{[\sigma]})]})$

Notation. We will write $Con_T \equiv \neg Pf_T(\underline{[0 \neq 0]})$. Clearly Con_T holds if and only if T is consistent.

Lemma. If $T \vdash \sigma \rightarrow \delta$, then $PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[\delta]})$.

Proof. If $T \vdash \sigma \rightarrow \delta$, then by (I) above,

$$PA \vdash Pf_T(\underline{[\sigma \rightarrow \delta]}),$$

and by (II),

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[\delta]}).$$

Gödel's Second Incompleteness Theorem. *If T is consistent, \underline{T} is recursive, and $T \vdash PA$, then $T \not\vdash Con_T$.*

Proof. By the fixed point lemma, there exists σ such that

$$Q \vdash \sigma \iff \neg Pf_T(\underline{[\sigma]}). \quad (\dagger)$$

By (III), above,

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[Pf_T(\underline{[\sigma]})]}). \quad (\ddagger)$$

And further, by Lemma, we have

$$PA \vdash Pf_T(\underline{[Pf_T(\underline{[\sigma]})]}) \rightarrow Pf_T(\underline{[\neg\sigma]}).$$

Combining this result with (\ddagger), we have

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[\neg\sigma]}).$$

Now note that $\vdash \neg\sigma \iff (\sigma \rightarrow (0 \neq 0))$. By the lemma,

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[\sigma \rightarrow (0 \neq 0)]}).$$

In particular,

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[\sigma]}) \wedge Pf_T(\underline{[\sigma \rightarrow (0 \neq 0)]}),$$

hence, by (II),

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow Pf_T(\underline{[0 \neq 0]}),$$

i.e.

$$PA \vdash Pf_T(\underline{[\sigma]}) \rightarrow \neg Con_T.$$

Thus $PA \vdash Con_T \rightarrow \sigma$, by (†).

Now, suppose that $T \vdash Con_T$. Then $T \vdash \sigma$, and hence by (I), $T \supset Q \vdash Pf_T(\underline{[\sigma]})$. But again, by (†), this implies that $T \vdash \neg\sigma$, a contradiction, showing that T cannot prove its own consistency.

We remark that one may carry the proof through using only the assumption that \underline{T} is recursively enumerable.

Löb's Theorem. *Suppose T is a consistent theory in $\mathcal{L} \supset \mathcal{L}_N$, such that \underline{T} recursive, and $T \vdash PA$. Then for any \mathcal{L} -sentence σ , if $T \vdash Pf_T(\underline{[\sigma]}) \rightarrow \sigma$, then $T \vdash \sigma$.*

Proof. By the fixed point lemma, there exists δ such that

$$Q \vdash \delta \leftrightarrow (Pf_T(\underline{[\delta]}) \rightarrow \sigma).$$

Since $T \vdash PA \supset Q$, T proves the same result. From this we may deduce that

$$PA \vdash Pf_T(\underline{[\delta]}) \rightarrow Pf_T(\underline{[\sigma]}).$$

In particular, by our lemma, we have

$$PA \vdash Pf_T(\underline{[\delta]}) \rightarrow Pf_T(\underline{[Pf_T(\underline{[\delta]}) \rightarrow \sigma]}),$$

and, combining this with (III) from above,

$$PA \vdash Pf_T(\underline{[\delta]}) \rightarrow Pf_T(\underline{[Pf_T(\underline{[\delta]})]}) \wedge Pf_T(\underline{[Pf_T(\underline{[\delta]}) \rightarrow \sigma]}),$$

and thus, by (II),

$$PA \vdash Pf_T(\underline{[\delta]}) \rightarrow Pf_T(\underline{[\sigma]}),$$

as desired.

Now assume that $T \vdash Pf_T(\underline{[\sigma]}) \rightarrow \sigma$. Then, by the above,

$$T \vdash Pf_T(\underline{[\delta]}) \rightarrow \sigma.$$

By our choice of δ , this in turn implies that $T \vdash \delta$. By (I), we have that $Q \vdash Pf_T(\underline{[\delta]})$, and hence T proves the same result, implying that $T \vdash \sigma$, as desired.

Remark. Gödel's Second Incompleteness Theorem in fact follows from Löb's Theorem. In particular, given T as in the hypotheses of both theorems, if $T \vdash Con_T$, then

$$T \vdash Pf_T(\underline{[0 \neq 0]}) \rightarrow 0 \neq 0.$$

But by Löb's Theorem, this in turn implies that $T \vdash 0 \neq 0$, showing that such a theory, if consistent, cannot prove its own consistency.

REFERENCES

- [BJ] G. S. Boolos and R. C. Jeffrey, *Computability and logic*.
- [E] H. Enderton, *A mathematical introduction to logic*.
- [Sh] J. R. Shoenfield, *Mathematical logic*.
- [Sm] R. M. Smullyan, *Gödel's incompleteness theorems*.