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, $\chi_R : \omega^n \to \omega$, the *characteristic function* on R, is given by

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

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.
- $I_i^n : \omega^n \to \omega$, $1 \leq i \leq n$, defined by $(x_1, \ldots, x_n) \mapsto x_i$ is *recursive*;
- $+ : \omega \times \omega \to \omega$ and $\cdot : \omega \times \omega \to \omega$ are *recursive*;
- $\chi_< : \omega \times \omega \to \omega$ is *recursive*.

R2. (Composition) For recursive functions $G, H_1, \ldots, H_k$ such that $H_i : \omega^n \to \omega$ and $G : \omega^k \to \omega$, $F : \omega^n \to \omega$, defined by

$$F(\overline{a}) = G(H_1(\overline{a}), \ldots, H_k(\overline{a})).$$

is *recursive*.

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

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

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

$$F(\overline{a}) = G(a_{\sigma(1)},...,a_{\sigma(k)}) = G(I^n_{\sigma(1)}(\overline{a}),...,I^n_{\sigma(k)}(\overline{a})),$$

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

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

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

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

is a recursive relation.

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

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

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

is recursive.

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

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

Proof. By induction:

$$C_{n,0}(\overline{a}) = \mu x(I^{n+1}_{n+1}(\overline{a},x) = 0)$$
$$C_{n,k+1}(\overline{a}) = \mu x(C_{n,k}(\overline{a}) < x)$$

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

$$\chi_{\neg P}(\overline{a}) = \chi_<(0,\chi_P(\overline{a})),$$
$$\chi_{P \vee Q}(\overline{a}) = \chi_P(\overline{a}) \cdot \chi_Q(\overline{a}),$$
$$P \wedge Q = \neg(\neg P \vee \neg Q).$$

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 $\overline{a} \in \omega^n$, $f : \omega^n \to \omega$ a function and $P \subset \omega^{m+1}$ a relation,

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

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

We also write

$$\exists x < f(\overline{a})\, P(x) \equiv (\mu x < f(\overline{a})\, P(x)) < f(\overline{a}), \text{ and}$$
$$\forall x < f(\overline{a})\, P(x) \equiv \neg(\exists x < f(\overline{a})\, (\neg P(x))).$$

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

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

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

is recursive.

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

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

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

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

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

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

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

is recursive.

Proof. Note that

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

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

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

is recursive.

Proof. Note that

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

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

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

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

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 $\overline{a} \in \omega^n$, $R(\overline{a})$ iff $\exists x Q(\overline{a}, x)$ and $\neg R(\overline{a})$ iff $\exists x P(\overline{a}, x)$.

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

$$F(\overline{a}) = \mu x(Q(\overline{a}, x) \lor P(\overline{a}, x)),$$

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

We show that

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

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

The β-Function Lemma.

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

Remark 1. Let $A = \{a_1, ...a_n\} \subseteq \omega \smallsetminus \{0, 1\}$ $(n \geq 2)$ be a set such that any two distinct elements of A are realtively 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 $p \not| 1 + jz$. 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. $J : \omega^2 \to \omega$, 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

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

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

Given $a_1, \ldots, a_{n-1} \in \omega$, 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 $j < c$,

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

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) $\mathrm{Div}(1 + (J(a_i, i) + 1) \cdot z, y)$;
    From $(*)$.

(iii) For all $x < a_i$, $1 + (J(x,i)+1)z \not| y$;
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 $a_1, \ldots, a_n$, is given by

$$<a_1, \ldots, a_n> = \mu x(\beta(x,0) = n \wedge \beta(x,1) = a_1 \wedge \cdots \wedge \beta(x,n) = a_n).$$

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

$$<a_1, \ldots, a_n> = <b_1, \ldots, b_m>$$

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

$$<> = \mu x(\beta(x,0) = 0) = 0.$$

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 $()_i : \omega \to \omega$, 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 $(<a_1 \ldots a_n>)_i = a_i$ and $lh(<a_1 \ldots a_n>) = n$.
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, $a = <(a)_1, \ldots, (a)_{lh(a)}>$). 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 $Init : \omega^2 \to \omega$ 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 $1 \leq i \leq n$,

$$Init(<a_1, \ldots, a_n>, i) = <a_1, \ldots, a_i>,$$

as intended.

Definition. The **concatenation** function $* : \omega^2 \to \omega$ 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

$$< a_1 \dots a_n > * < b_1 \dots b_m > = < a_1 \dots a_n, b_1 \dots b_m >,$$

as desired.

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

$$\overline{F}(a, \overline{b}) = < F(0, \overline{b}), \dots, F(a-1, \overline{b}) >,$$

or, equivalently,

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

Note that $F(a, \overline{b}) = (\overline{F}(a+1, \overline{b}))_{a+1}$, thus we have that $\overline{F}$ is recursive if and only if F is recursive.

Properties of Recursive Functions and Relations (continued):

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

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

is recursive. Because $\overline{F}(a, \overline{b})$ is defined in terms of values $F(x, \overline{b})$, for x strictly smaller than a, this inductive definition of F makes sense.

Proof. Note that

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

where

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

According to this definition, $F(0, \overline{b}) = G(<>, 0, \overline{b}) = G(0, 0, \overline{b})$,

$$F(1, \overline{b}) = G(< G(0, 0, \overline{b}) >, 1, \overline{b}),$$

and

$$F(2, \overline{b}) = G(< G(0, 0, \overline{b}), G(< G(0, 0, \overline{b}) >, 1, \overline{b}) >, 2, \overline{b}),$$

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

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

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

is recursive.

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

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

with recursive $G'(x, y, \overline{z}) = \beta(x, G(y, \overline{z}) + 1)$. 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 $G:\omega^n \to \omega$ and $H:\omega^2\times\omega^n\to\omega$, $F:\omega\times\omega^n\to\omega$ 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

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

are all recursive.)

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

P14. Given recursive relations $Q\subset\omega^{n+1}$ and $R\subset\omega^{n+1}$ and recursive $H:\omega\times\omega^n\to\omega$ 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 $H':\omega\times\omega^n\to\omega$ 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 $F : \omega^2 \to \omega$ 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 $bd : \omega \to \omega$ is given by

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

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

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

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. $\forall x \forall y \; Sx = Sy \to x = y$.
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. $\forall x \forall y \; x < Sy \longleftrightarrow x < y \vee x = y$.
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

$$(\varphi^x_0 \wedge \forall x(\varphi \to \varphi^x_{Sx})) \to \varphi,$$

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,

$$\underline{n} \equiv \underbrace{SS \ldots S}_{n} 0.$$

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

$$Q \vdash \forall y(\varphi(\underline{k_1}, \ldots, \underline{k_n}, y) \longleftrightarrow y = \underline{f(k_1, \ldots, k_n)})$$

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

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

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

and

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

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, $Q \vdash \underline{m-1} \neq \underline{n} \to \underline{m} \neq \underline{n+1}$. 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 and Rule T, 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 $Q \vdash \neg(\underline{m} = \underline{n})$. Again applying Q8 and 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

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

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

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

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

is a tautology, we have $Q \vdash y = 0 \longleftrightarrow \psi(\underline{k_1}, \dots, \underline{k_n}, y)$, 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

$$\vdash \neg\varphi(\underline{k_1}, \dots, \underline{k_n}) \to (y = \underline{1} \longleftrightarrow \psi(\underline{k_1}, \dots, \underline{k_n}, y),$$

we obtain that $Q \vdash y = \underline{1} \longleftrightarrow \psi(\underline{k_1}, \dots, \underline{k_n}, y)$, as required. Thus, $\psi(\overline{x}, y)$ represents χ_P.

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

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

$$Q \vdash \psi(\underline{k_1}, \dots, \underline{k_n}, y) \longleftrightarrow y = 0.$$

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

$$Q \vdash \psi(\underline{k_1} \dots \underline{k_n}, y) \longleftrightarrow y = \underline{1},$$

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 $\mathcal{L}_\mathbb{N}$,

$$Q \vdash \varphi^x_0 \to \cdots \to (\varphi^x_{\underline{k-1}} \to (x < \underline{k} \to \varphi))$$

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

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

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

$$Q \vdash \varphi^x_0 \to \dots \to (\varphi^x_{\underline{k-1}} \to (x < \underline{k} \to \varphi)).$$

We must show that

$$Q \vdash \varphi^x_0 \to \cdots \to (\varphi^x_{\underline{k}} \to (x < \underline{k+1} \to \varphi)).$$

Equivalently, we want to show that $\Gamma \vdash \varphi$ where $\Gamma = Q \cup \{\varphi^x_0, ..., \varphi^x_{\underline{k}}, x < \underline{k+1}\}$. By Q8, $\Gamma \vdash x < \underline{k} \lor x = \underline{k}$. In the first case, the inductive hypothesis implies that $\Gamma \vdash \varphi$, while in the latter case, $\models x = \underline{k} \to (\varphi^x_{\underline{k}} \longleftrightarrow \varphi)$, and hence $\Gamma \vdash \varphi$. By either route, Γ proves φ.

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

$$Q \vdash (\varphi \land \forall z(z < x \to \neg\varphi^x_z)) \longleftrightarrow x = \underline{n}.$$

Proof. We define

$$\psi \equiv (\varphi \land \forall z(z < x \to \neg\varphi^x_z)).$$

Now, we obtain

$$\models x = \underline{n} \to (\psi \longleftrightarrow (\varphi^x_{\underline{n}} \land \forall z(z < \underline{n} \to \neg\varphi^x_z))). \qquad (*)$$

By (a) and Lemma 6, we get

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

and, applying substitution and generalization, we obtain

$$Q \vdash \forall z(z < \underline{n} \to \neg\varphi^x_z).$$

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

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

For the reverse implication, we note that

$$\models \forall z(z < x \to \neg\varphi^x_z) \to (\underline{n} < x \to \neg\varphi^x_{\underline{n}}),$$

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

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^n_i, $+$, $\cdot$, 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^n_i is representable by $\varphi(x_1, \ldots, x_n, y) \equiv x_i = y$. In particular, for any $k_1, \ldots, k_n \in \omega$, $I^n_i(k_1, \ldots, k_n) = k_i$, and hence

$$Q \vdash \varphi(\underline{k_1}, \ldots, \underline{k_n}, y) \longleftrightarrow y = \underline{k_i} \longleftrightarrow y = \underline{I^n_i(k_1, \ldots, k_n)},$$

by our choice of φ. Generalization completes the result.

R2. $F(\overline{a}) = G(H_1(\overline{a}), \ldots, H_k(\overline{a}))$, 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

$$\alpha(\overline{x}, y) \equiv \exists z_1, \ldots, z_k(\psi_1(\overline{x}, z_1) \wedge \cdots \wedge \psi_k(\overline{x}, z_k) \wedge \varphi(z_1, \ldots, z_k, y)).$$

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

$$Q \vdash \alpha(\underline{a_1}, \ldots, \underline{a_n}, y) \longleftrightarrow y = \underline{G(H_1(\overline{a}), \ldots, H_k(\overline{a}))} \qquad (\dagger)$$

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

Now, for $\Gamma = Q \cup \{\alpha(\underline{a_1}, \ldots, \underline{a_n}, y)\}$, since the ψ_i represent H_i, we have that $\Gamma \vdash \exists z_1, \ldots, z_k(z_1 = \underline{H_1(\overline{a})} \wedge \cdots \wedge z_k = \underline{H_k(\overline{a})} \wedge \varphi(z_1, \ldots, z_k, y))$. Hence we have

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

and since the z_i do not appear,

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

Since φ represents G, we have

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

as required.

On the other hand, for $\Sigma = Q \cup \{y = \underline{G(H_1(\overline{a}), \ldots, H_k(\overline{a}))}\}$,

$\Sigma \vdash \varphi(\underline{H_1(\overline{a})}, \ldots, \underline{H_k(\overline{a})}, y)$
$\Sigma \vdash \exists z_1, \ldots, z_k(z_1 = \underline{H_1(\overline{a})} \wedge \cdots z_k = \underline{H_k(\overline{a})} \wedge \varphi(z_1, \ldots, z_k, y))$
$\Sigma \vdash \exists z_1, \ldots, z_k(\psi_1(\overline{a}, z_i) \wedge \cdots \psi_k(\overline{a}, z_k) \wedge \varphi(z_1, \ldots, z_k, y))$
$\Sigma \vdash \alpha(\underline{a_1}, \ldots, \underline{a_n}, y)$

Thus (†) is established.

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

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

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

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

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

thus

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

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

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

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

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

Hence, by Lemma 7,

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

and thus,

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

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:

- $h : \mathcal{L} \cup \{\neg, \to, \forall\} \cup \mathcal{V} \to \omega$ 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.
- $\mathrm{AR} : \omega \to \omega \setminus \{0\}$ recursive such that $\mathrm{AR}(h(f)) = n$ and $\mathrm{AR}(h(P)) = n$ 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 $\ulcorner\urcorner : \{\mathcal{L}\text{-terms and } \mathcal{L}\text{-formulas}\} \to \omega$ inductively, by

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

- For $\mathcal{L}$-terms $u_1, \ldots, u_n$ and n-ary $f \in \mathcal{F}$,
$$\ulcorner f u_1 u_2 \ldots u_n \urcorner = \,<h(f), \ulcorner u_1 \urcorner, \ulcorner u_2 \urcorner, \ldots, \ulcorner u_n \urcorner>.$$
- For $\mathcal{L}$-terms $t_1, \ldots, t_n$ and $P \in \mathcal{P}$,
$$\ulcorner P t_1 t_2 \ldots t_n \urcorner = \,<h(P), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_n \urcorner>.$$
- For $\mathcal{L}$-formulas φ and ψ,
$$\begin{aligned} \ulcorner \varphi \to \psi \urcorner &= \,<h(\to), \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner>, \\ \ulcorner \neg \varphi \urcorner &= \,<h(\neg), \ulcorner \varphi \urcorner>, \\ \ulcorner \forall x \varphi \urcorner &= \,<h(\forall), \ulcorner x \urcorner, \ulcorner \varphi \urcorner>. \end{aligned}$$

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

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

(1) $\mathit{Vble} = \{\ulcorner v \urcorner \mid v \in \mathcal{V}\} \subset \omega$ and $\mathit{Const} = \{\ulcorner c \urcorner \mid c \in \mathcal{C}\} \subset \omega$.

Proof. Note
$$\begin{aligned} \mathit{Vble}(x) &\text{ iff } x = \,<(x)_1>\, \wedge \underline{\mathcal{V}}((x)_1), \\ \mathit{Const}(x) &\text{ iff } x = \,<(x)_1>\, \wedge \underline{\mathcal{C}}((x)_1). \end{aligned}$$

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

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

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

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

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

Proof. Note
$$\mathit{Form}(a) \text{ iff } \begin{cases} \mathit{Form}((a)_2) & \text{if } a = \,<h(\neg), (a)_2>, \\ \mathit{Form}((a)_2) \wedge \mathit{Form}((a)_3) & \text{if } a = \,<h(\to), (a)_2, (a)_3>, \\ \mathit{Vble}((a)_2) \wedge \mathit{Form}((a)_3) & \text{if } a = \,<h(\forall), (a)_2, (a)_3>, \\ \mathit{AtF}(a) & \text{otherwise.} \end{cases}$$

(5) $\mathit{Sub} : \omega^3 \to \omega$, such that $\mathit{Sub}(\ulcorner t \urcorner, \ulcorner x \urcorner, \ulcorner u \urcorner) = \ulcorner t^x_u \urcorner$ and $\mathit{Sub}(\ulcorner \varphi \urcorner, \ulcorner x \urcorner, \ulcorner u \urcorner) = \ulcorner \varphi^x_u \urcorner$ for terms t and u, variable x, and formula φ.

Proof. Define

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

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, $Free(\ulcorner\varphi\urcorner, \ulcorner x\urcorner)$ if and only if x occurs free in φ, and $Free(\ulcorner\tau\urcorner, \ulcorner x\urcorner)$ if and only if x occurs in τ

Proof. Define

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

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

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

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, $Subst(\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner)$ if and only if t is substitutable for x in φ.

Proof. Define

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

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

(9) We define

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

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 $\forall x\varphi$),

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

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

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

$$\overline{v}(\varphi) = \text{F} \quad \text{iff} \quad \overline{v_b}(\varphi) = \text{F} \quad \text{iff} \quad False(\ulcorner\varphi\urcorner, b).$$

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

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

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

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

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

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

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

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

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

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

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

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

$$\underline{\mathrm{AG4}}(a) \text{ iff } \exists x, y < a\,(\mathit{Vble}(x) \wedge \mathit{Form}(y) \\ \wedge \neg \mathit{Free}(y, x) \wedge a = <h(\to), y,\ <h(\forall), x, y>>)$$

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

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

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

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

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

$$\underline{\mathrm{AG6}}(a) \text{ iff } \exists x, y, b, c < a\,(\mathit{Vble}(x) \wedge \mathit{Vble}(y) \wedge \mathit{AtF}(b) \wedge \mathit{AtF}(c) \\ \wedge\ \mathit{lh}(b) = \mathit{lh}(c) \wedge \forall j < \mathit{lh}(b) + 1((c)_j = (b)_j \vee ((c)_j = y \wedge (b)_j = x)) \\ \wedge\ a = <h(\to),\ <h(=), x, y>,\ <h(\to), b, c>>)$$

(16) $\mathit{Gen}(a, b) \subset \omega^2$, such that $\mathit{Gen}(\ulcorner\varphi\urcorner, \ulcorner\psi\urcorner)$ if and only if φ is a generalization of ψ (i.e., $\varphi = \forall x_1 \ldots \forall x_n \psi$ for some finite $\{x_i\} \subset \mathcal{V}$).

Proof. Note that

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

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

Proof. Note that

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

We have, to this point, defined three codings: $<>$ on sequences of natural numbers, h on the language and logical symbols, and $\ulcorner\urcorner$ on the terms and formulas. We presently define a fourth coding, of sequences of formulas:

$$[\![\,]\!] : \{\text{sequences of } \mathcal{L}\text{-formulas}\} \to \omega,$$

given by

$$[\![\varphi_1, \ldots, \varphi_n]\!] = <\ulcorner\varphi_1\urcorner, \ldots, \ulcorner\varphi_n\urcorner> .$$

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 $\llbracket\ \rrbracket$, 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

$$\underline{T} = \{\ulcorner\sigma\urcorner \mid \sigma \in T\}.$$

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

We shall make use of the following relations:

- $\mathit{Ded}_T = \{\llbracket\varphi_1, \ldots, \varphi_n\rrbracket \mid \varphi_1, \ldots, \varphi_n$ is a deduction from $T\} \subset \omega$.
  Note that

$$\mathit{Ded}_T(a) \text{ iff } \mathit{Seq}(a) \wedge \mathit{lh}(a) \neq 0$$
$$\wedge \forall j < \mathit{lh}(a)\, (\underline{\Lambda}((a)_{j+1}) \vee \underline{T}((a)_{j+1}) \vee \exists i, k < j+1\, ((a)_{k+1} = < h(\to), (a)_{i+1}, (a)_{j+1} >))$$

- $\mathit{Prf}_T \subset \omega^2$, given by $\mathit{Prf}_T(a, b)$ iff $\mathit{Ded}_T(b) \wedge a = (b)_{\mathit{lh}(b)}$.
- $\mathit{Pf}_T \subset \omega$, given by $\mathit{Pf}_T(a)$ iff $\mathit{Sent}(a) \wedge \exists x \mathit{Prf}_T(a, x)$.

Note that we may read $\mathit{Prf}_T(a, b)$ as "b is a proof of a from T," and $\mathit{Pf}_T(a)$ as "a is a sentence provable from T." In particular

$$\mathit{Pf}_T = \underline{\mathrm{Cn}\, T} = \{\ulcorner\sigma\urcorner \mid T \vdash \sigma\}.$$

We use this fact to prove the following:

Theorem. *If T is axiomatizable, then $\mathit{Pf}_T = \underline{\mathrm{Cn}\, T}$ 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 $\mathit{Pf}_S = \mathit{Pf}_T$, since $\mathrm{Cn}\, S = \mathrm{Cn}\, T$.

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

Proof. By the negation theorem, it suffices to show that $\neg \mathit{Pf}_T$ is recursively enumerable. Note that since T is complete, for any sentence σ, $T \nvdash \sigma$ if and only if $T \vdash \neg\sigma$. Hence

$$\begin{aligned}\neg \mathit{Pf}_T(a) &\text{ iff } \neg \mathit{Sent}(a) \vee \exists m \mathit{Prf}_T(< h(\neg), a >, m)\\ &\text{ iff } \exists m(\neg \mathit{Sent}(a) \vee \mathit{Prf}_T(< h(\neg), a >, m)).\end{aligned}$$

Thus $\neg \mathit{Pf}_T$ 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, $\mathcal{L}_{\mathbb{N}}$. Recall that we define, for a natural number n,

$$\underline{n} \equiv \underbrace{SS \ldots S}_{n} 0.$$

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

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

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 $dg : \omega \to \omega$ such that for any $\mathcal{L}_{\mathcal{N}}$ formula, $dg(\ulcorner \varphi \urcorner) = \ulcorner d(\varphi) \urcorner$.

Proof. Define $num : \omega \to \omega$ by $num(0) = <0>$ and, for $n \in \omega$

$$num(n+1) = <h(S), num(n)> .$$

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

Define

$$\begin{aligned} dg(a) = {} & <h(\neg),\ <h(\forall), \ulcorner v_0 \urcorner,\ <h(\neg), \\ & \qquad <h(\neg),\ <h(\to),\ <h(=), \ulcorner v_0 \urcorner, num(a)>,\ <h(\neg), a>>>>>> \end{aligned}$$

Then

$$\begin{aligned} dg(\ulcorner \varphi \urcorner) &= <h(\neg),\ <h(\forall), \ulcorner v_0 \urcorner,\ <h(\neg), \\ & \qquad <h(\neg),\ <h(\to),\ <h(=), \ulcorner v_0 \urcorner, num(\ulcorner \varphi \urcorner)>,\ <h(\neg), \ulcorner \varphi \urcorner>>>>>>, \\ &= <h(\neg),\ <h(\forall), \ulcorner v_0 \urcorner,\ <h(\neg), \\ & \qquad <h(\neg),\ <h(\to),\ <h(=), \ulcorner v_0 \urcorner, \ulcorner \underline{\ulcorner \varphi \urcorner} \urcorner>,\ <h(\neg), \ulcorner \varphi \urcorner>>>>>> . \end{aligned}$$

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

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

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*

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

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

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

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

$$Q \vdash \sigma \longleftrightarrow \exists y(y = \underline{k} \wedge \varphi(y)) \longleftrightarrow \varphi(\underline{k}) \longleftrightarrow \varphi(\underline{\ulcorner\sigma\urcorner}),$$

as required.

Tarski Undefinability Theorem. $\underline{\mathrm{Th}\,\mathcal{N}} = \{\ulcorner\sigma\urcorner \mid \mathcal{N} \models \sigma\}$ *is not definable.*

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

$$\mathcal{N} \models \sigma \longleftrightarrow \neg\beta(\underline{\ulcorner\sigma\urcorner}).$$

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

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 $\mathcal{L}$ ($\underline{\mathrm{Cn}\,T}$ is not recursive).*

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

In particular, note that $\alpha \in \mathrm{Cn}(T \cup \{\tau\})$ iff $\tau \to \alpha \in \mathrm{Cn}\,T$. Thus

$$a \in \underline{\mathrm{Cn}(T \cup \{\tau\})} \;\text{ iff }\; \mathit{Sent}(a) \wedge\, < h(\to), \ulcorner\tau\urcorner, a > \in \underline{\mathrm{Cn}\,T}.$$

Hence $\underline{\mathrm{Cn}(T \cup \{\tau\})}$ is recursive, as desired.

To prove the theorem, then, it suffices to show that $\underline{\mathrm{Cn}(T \cup Q)}$ 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

$$Q \vdash \sigma \longleftrightarrow \neg\beta(\underline{\ulcorner\sigma\urcorner}).$$

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

$$Q \vdash \beta(\underline{\ulcorner\sigma\urcorner}),$$

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

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

a contradiction. On the other hand, if $T \cup Q \nvdash \sigma$, then by representability,

$$Q \vdash \neg\beta(\underline{\ulcorner\sigma\urcorner}),$$

and hence

$$Q \vdash \sigma,$$

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

Corollary. $\mathrm{Th}\,\mathcal{N}$*, 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* ($\{\ulcorner \sigma \urcorner \mid \emptyset \vdash \sigma\}$) *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, $\mathrm{Th}(\mathcal{N}, +, \cdot)$ 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

$$T \vdash \sigma \Rightarrow Q \vdash Pf_T(\underline{\ulcorner \sigma \urcorner}).$$

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

$$Q \vdash \exists x Prf_T(\underline{\ulcorner \sigma \urcorner}, x),$$

or

$$Q \vdash Pf_T(\underline{\ulcorner \sigma \urcorner}).$$

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

$$T \supset Q \vdash \alpha \longleftrightarrow \neg Pf_T(\underline{\ulcorner \alpha \urcorner}). \tag{$*$}$$

If $T \vdash \alpha$, then $Q \vdash Pf_T(\underline{\ulcorner \alpha \urcorner})$, and thus $Q \vdash \neg\alpha$, and hence $T \vdash \neg\alpha$, a contradiction. Thus $T \nvdash \alpha$.

On the other hand, if T is ω-consistent (i.e., whenever $T \vdash \exists x \varphi(x)$, then for some $n \in \omega$, $T \nvdash \neg\varphi(\underline{n})$), then $T \nvdash \neg\alpha$. In particular, if $T \vdash \neg\alpha$, then

$$T \vdash Pf_T(\underline{\ulcorner \alpha \urcorner}),$$

by $(*)$. That is,

$$T \vdash \exists x Prf_T(\underline{\ulcorner \alpha \urcorner}, x).$$

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

$$T \supset Q \vdash \neg Prf_T(\underline{\ulcorner \alpha \urcorner}, m)$$

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 $T \nvdash \alpha$ and $T \nvdash \neg\alpha$, 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 $\mathcal{L} \supset \mathcal{L}_{\mathbb{N}}$.

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. $T \vdash \sigma \Rightarrow Q \vdash Pf_T(\underline{\ulcorner\sigma\urcorner})$

II. $PA \vdash (Pf_T(\underline{\ulcorner\sigma\urcorner}) \wedge Pf_T(\underline{\ulcorner\sigma \to \delta\urcorner})) \to Pf_T(\underline{\ulcorner\delta\urcorner})$

III. $PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner\sigma\urcorner})\urcorner}\right)$

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

Lemma. If $T \vdash \sigma \to \delta$, then $PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner\delta\urcorner})$.

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

$$PA \vdash Pf_T(\underline{\ulcorner\sigma \to \delta\urcorner}),$$

and by (II),

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner\delta\urcorner}).$$

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

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

$$Q \vdash \sigma \longleftrightarrow \neg Pf_T(\underline{\ulcorner\sigma\urcorner}). \tag{†}$$

By (III), above,

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner\sigma\urcorner})\urcorner}\right). \tag{‡}$$

And further, by Lemma, we have

$$PA \vdash Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner\sigma\urcorner})\urcorner}\right) \to Pf_T(\underline{\ulcorner\neg\sigma\urcorner}).$$

Combining this result with (‡), we have

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner\neg\sigma\urcorner}).$$

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

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner\sigma \to (0 \neq 0)\urcorner}).$$

In particular,

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner\sigma\urcorner}) \wedge Pf_T(\underline{\ulcorner\sigma \to (0 \neq 0)\urcorner}),$$

hence, by (II),

$$PA \vdash Pf_T(\underline{\ulcorner\sigma\urcorner}) \to Pf_T(\underline{\ulcorner 0 \neq 0\urcorner}),$$

i.e.

$$PA \vdash Pf_T(\underline{\ulcorner \sigma \urcorner}) \to \neg Con_T.$$

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

Now, suppose that $T \vdash Con_T$. Then $T \vdash \sigma$, and hence by (I), $T \supset Q \vdash Pf_T(\underline{\ulcorner \sigma \urcorner})$. 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 $\mathcal{L} \supset \mathcal{L}_{\mathbb{N}}$, such that $\underline{T}$ recursive, and $T \vdash PA$. Then for any $\mathcal{L}$-sentence σ, if $T \vdash Pf_T(\underline{\ulcorner \sigma \urcorner}) \to \sigma$, then $T \vdash \sigma$.*

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

$$Q \vdash \delta \longleftrightarrow (Pf_T(\underline{\ulcorner \delta \urcorner}) \to \sigma).$$

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

$$PA \vdash Pf_T(\underline{\ulcorner \delta \urcorner}) \to Pf_T(\underline{\ulcorner \sigma \urcorner}).$$

In particular, by our lemma, we have

$$PA \vdash Pf_T(\underline{\ulcorner \delta \urcorner}) \to Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner \delta \urcorner}) \to \sigma \urcorner}\right),$$

and, combining this with (III) from above,

$$PA \vdash Pf_T(\underline{\ulcorner \delta \urcorner}) \to Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner \delta \urcorner}) \urcorner}\right) \wedge Pf_T\left(\underline{\ulcorner Pf_T(\underline{\ulcorner \delta \urcorner}) \to \sigma \urcorner}\right),$$

and thus, by (II),

$$PA \vdash Pf_T(\underline{\ulcorner \delta \urcorner}) \to Pf_T(\underline{\ulcorner \sigma \urcorner}),$$

as desired.

Now assume that $T \vdash Pf_T(\underline{\ulcorner \sigma \urcorner}) \to \sigma$. Then, by the above,

$$T \vdash Pf_T(\underline{\ulcorner \delta \urcorner}) \to \sigma.$$

By our choice of δ, this in turn implies that $T \vdash \delta$. By (I), we have that $Q \vdash Pf_T(\underline{\ulcorner \delta \urcorner})$, 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

$$T \vdash Pf_T(\underline{\ulcorner 0 \neq 0 \urcorner}) \to 0 \neq 0.$$

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.*