

# Gödel's First Incompleteness Theorem

Will Troiani

February 24, 2025

## Contents

1	Introduction	1
2	General Recursive Functions and Relations	4
3	The general recursive functions and the general recursive relations are representable	6
3.1	The $\beta$ -function	7
3.2	Representability	10
4	Gödel Numbering	15
5	Towards the Gödel sentence	15
5.1	Diagonalisation	16
5.2	“Proof of”	16
6	Gödel's Sentence	17
7	Is the use of general recursive functions problematic?	18

## 1 Introduction

Gödel's First Incompleteness Theorem holds in a very broad setting, indeed, observe the following vague statement.

**Proposition 1.0.1.** *[Gödel's First Incompleteness Theorem (vague)] Let  $L$  be any formal system of arithmetic (at least strong enough to describe the basic statements about addition and multiplication) whose set of axioms and set of deduction rules are both computable. Then  $L$  is necessarily either incomplete, or inconsistent.*

We progressively make this statement more precise. To begin, we define the first order language which we will be working with (see [6] for Definitions of a *first order language* and a *first order theory*).

**Definition 1.0.2.** The first order language  $Q$  consists of the following.

- A single sort  $A$ .
- Four function symbols:

$$\begin{aligned}0 &: A \\ S &: A \longrightarrow A \\ + &: A \times A \longrightarrow A \\ \times &: A \times A \longrightarrow A\end{aligned}$$

- No relation symbols.

The first order theory  $Q$  consists of the following axioms.

$$\forall x, \neg(x = S(x)), \quad (1)$$

$$\forall x, \neg(S(x) = 0) \quad (2)$$

$$\forall x \forall y, S(x) = S(y) \implies x = y \quad (3)$$

$$\forall x, \neg(x = 0) \implies \exists y, x = S(y) \quad (4)$$

$$\forall x, x + 0 = x \quad (5)$$

$$\forall x \forall y, x + S(y) = S(x + y) \quad (6)$$

$$\forall x, x \times 0 = 0 \quad (7)$$

$$\forall x \forall y, x \times S(y) = (x \times y) + x \quad (8)$$

**Remark 1.0.3.** The first order theory  $Q$  is the familiar first order theory of Peano arithmetic but with the axiom schema corresponding to induction omitted. This theory  $Q$  is often called **Robinson arithmetic** in literature.

Since  $Q$  does not admit the inductive axiom, it is hardly surprising that  $Q$  is incomplete, indeed, one can prove rather simply that  $Q$  cannot prove nor disprove the statement

$$\forall x, 0 + x = x \quad (9)$$

see [5, §8.4] for a proof. The more interesting question is whether  $Q$  can be *consistently completed*, a notion we now make precise.

**Definition 1.0.4.** Let  $L$  be a consistent first order theory (see [3] for the basic definitions, complete, consistent, etc). The system  $L$  is **consistently completable** if there exists a first order theory  $L'$  satisfying the following.

- Every axiom of  $L$  is provable in  $L'$ .
- $L'$  is consistent and complete.

A common miss-understanding of Gödel's First Incompleteness Theorem is that  $Q$  (and hence the first order theory of Peano arithmetic) is not consistently completable. This is not true, as the following Example demonstrates.

**Example 1.0.5.** Given a consistent first order theory  $L$ , it was shown in [3, Theorem 1] how to construct a new first order theory  $L^*$  satisfying the following.

- Every axiom of  $L$  is provable in  $L^*$ ,
- $L^*$  is consistent and complete (and saturated, which won't be used here).

Applying this to  $Q$  and we obtain  $Q^*$ , which contains  $Q$ , is consistent, and complete. Hence,  $Q$  is consistently completable (assuming it is consistent).

Indeed, the phrase "...whose set of axioms and set of deduction rules are both computable" in Proposition 1.0.1 cannot be ignored. We make this phrase precise by working with *general recursive functions* and *relations*. We define "general recursive" in Definition 2.0.1. Indeed, the general recursive functions and relations play an important role in the theory of computation more broadly, but this is not necessary to understand Gödel's Theorem. For the current purposes, the role of general recursive functions and relations will be to carve out a subset of formulas which satisfy a representability criteria (Proposition 1.0.6 below).

In the following lemma, we denote the formula in  $Q$  corresponding to a natural number  $n$  by  $\underline{n}$ , for example,  $\underline{2}$  denotes  $S(S(0))$ .

**Proposition 1.0.6.** *Let  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  be a general recursive function. Then there exists a relation  $F$  with free variables  $x_1, \dots, x_m, y$  satisfying:*

$$\text{If } f(n_1, \dots, n_m) = k \text{ then } Q \vdash \forall y, F[x_i := \underline{n_i}]_{i=1}^m \iff y = \underline{k} \quad (10)$$

where  $F[x_i := \underline{n_i}]_{i=1}^m$  denotes the formula  $F$  with  $\underline{n_i}$  substituted for all free occurrences of  $x_i$  for  $i = 1, \dots, m$ .

Moreover, if a relation  $r \subseteq \mathbb{N}^m$  is general recursive, then there exists a formula  $R$  in  $Q$  with free variables  $x_1, \dots, x_n$  satisfying the following.

$$\begin{aligned} \text{If } (n_1, \dots, n_m) \in r \text{ then } Q \vdash R[x_i := \underline{n_i}]_{i=1}^m \\ \text{If } (n_1, \dots, n_m) \notin r \text{ then } Q \vdash \neg R[x_i := \underline{n_i}]_{i=1}^m \end{aligned}$$

Proposition 1.0.6 is in fact the core of the argument for Gödel's First Incompleteness Theorem. It is proved and discussed further in Section 2. This is where the class of general recursive relations is paramount, a similar statement to Proposition 1.0.6 but without the hypothesis that  $R$  is general recursive is *false*.

We are now cornered into making a very precise definition of “computable sets”, as if all sets are defined to be computable, then Gödel's First Incompleteness Theorem does not hold.

A set will be *computable* if there exists a general recursive function which in some way “recognises” the elements. General recursive functions have the natural numbers as their domains though, so we need to encode the elements of the set into natural numbers first, but not any encoding will do as what if this encoding itself is non-computable?

Thus we will fix a particular encoding of first order formulas into natural numbers. This is done using Gödel numbers, defined in the following way.

**Definition 1.0.7.** Given a term or formula  $\varphi$  of  $Q$ , we associate a natural number  $\ulcorner \varphi \urcorner \in \mathbb{N}$  in the following way.

- To each letter in the alphabet associated to  $Q$  we associate an integer according to the following table.

$\gamma(0) = 1$	$\gamma(S) = 3$	$\gamma(+)= 5$	$\gamma(\times) = 7$
$\gamma(() = 9$	$\gamma()) = 11$	$\gamma(\neg) = 13$	$\gamma(\wedge) = 15$
$\gamma(\vee) = 17$	$\gamma(\implies) = 19$	$\gamma(\forall) = 21$	$\gamma(\exists) = 23$
$\gamma(=) = 25$	$\gamma(x_1) = 2$	$\gamma(x_2) = 4$	$\dots$

To each term or formula  $\varphi$  is an associated sequence of symbols  $s_1 \dots s_n$  which spell out  $\varphi$ , that is, as words  $\varphi = s_1 \dots s_n$ . Denoting the  $i^{\text{th}}$  (in magnitude) prime number by  $p_i$ , we define:

$$\ulcorner \varphi \urcorner = p_1^{\gamma(s_1)} \dots p_n^{\gamma(s_n)} \quad (11)$$

**Example 1.0.8.** We calculate the Gödel number associated to the formula  $S(0) = 0 + 1$ .

$$\begin{aligned} \ulcorner S(0) = 0 + 1 \urcorner &= \ulcorner S(0) = 0 + S(0) \urcorner \\ &= 2^{\gamma(S)} 3^{\gamma(()} 5^{\gamma(0)} 7^{\gamma())} 11^{\gamma(=)} 13^{\gamma(0)} 17^{\gamma(+)} 19^{\gamma(S)} 23^{\gamma(()} 29^{\gamma(0)} 31^{\gamma())} \\ &= 2^3 3^9 5^{17} 11^{23} 13^1 17^5 19^3 23^9 29^1 31^{11} \\ &= 191352835104285876966611134901860756135433453873754327850773507007732920 \end{aligned}$$

**Definition 1.0.9.** Let  $X$  be a set, and for each  $x \in X$  assume there is some integer  $\underline{x}$  uniquely associated to  $x$ . The **characteristic function** of  $X$  is the function  $\chi_X : \mathbb{N} \rightarrow \mathbb{N}$  which for every  $x \in X$  is such that  $\chi_X(\underline{x}) = 0$  and for all other  $x \in \mathbb{N}$  is such that  $\chi_X(x) = 1$ .

A set of first order formulas  $X$  is **general recursive** if the characteristic function of the set of Gödel numbers of the formulas of  $X$  is general recursive.

**Definition 1.0.10.** A first order theory  $\mathbb{T}$  is **effectively, consistently, completable** if there exists a first order theory  $\mathbb{T}'$  satisfying the following.

- The set of axioms in  $\mathbb{T}'$  is general recursive.
- The set of deduction rules in  $\mathbb{T}'$  is general recursive.
- Every axiom rule of  $\mathbb{T}$  is provable in  $\mathbb{T}'$ .
- $\mathbb{T}'$  is consistent and complete.

Before stating our version of Gödel's First Incompleteness Theorem, we make a historical remark. Proposition 1.0.1 stated that  $L$  is either incomplete or inconsistent, but in fact this is *not* what was first proved by Gödel. The original paper [1] instead proves the weaker claim where the word “inconsistent” is replaced by “ $\omega$ -inconsistent”, which we define precisely in Definition 6.0.2. It was Rosser who in [4] relinquished Gödel's Theorem of the assumption of  $\omega$ -consistency. The important fact for now is that  $\omega$ -consistency implies consistency, but the converse does not hold, so Rosser's result is strictly stronger than what Gödel original wrote.

We can now state our version of Gödel's First Incompleteness Theorem precisely.

**Theorem 1.0.11** (Gödel's First Incompleteness Theorem (precise)). *If  $Q$  is  $\omega$ -consistent, then  $Q$  is not effectively, consistently completable.*

The argument will proceed by first defining a particular first order sentence, the Gödel sentence  $G_Q$ . This sentence will have the following properties.

$$\text{If } Q \text{ is consistent, then } Q \not\vdash G_Q \quad (12)$$

$$\text{If } Q \text{ is } \omega\text{-consistent, then } Q \not\vdash \neg G_Q \quad (13)$$

That such a sentence exists is remarkable. It is not simple to write  $G_Q$  down. We discuss this sentence and its construction more carefully in Section 6.

## 2 General Recursive Functions and Relations

First we define which functions constitute the “computable” ones. These will be the *general recursive* functions.

**Definition 2.0.1.** The set  $\Psi$  of **general recursive functions** is defined inductively.

- First, the base cases.
  - The constantly 0 function  $\mathbf{z} : \mathbb{N} \rightarrow \mathbb{N}$ ,  $\mathbf{z}(n) = 0$  is in  $\Psi$ .
  - The successor function  $\mathbf{s} : \mathbb{N} \rightarrow \mathbb{N}$ ,  $\mathbf{s}(n) = n + 1$  is in  $\Psi$ .
  - For any natural number  $n$  let  $m \leq n$  and denote by  $\pi_m^n : \mathbb{N}^n \rightarrow \mathbb{N}$  the projection onto the  $m^{\text{th}}$  component. For each such pair  $(n, m)$  the function  $\pi_m^n$  is in  $\Psi$ .
- Now the inductive cases.
  - If  $g : \mathbb{N}^m \rightarrow \mathbb{N}^r$  and  $h_1, \dots, h_m : \mathbb{N}^t \rightarrow \mathbb{N}$  are in  $\Psi$ , then the composite  $g \circ (h_1, \dots, h_m)$  is in  $\Psi$ .
  - Say  $f : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$  is a function for which there exists  $g, h \in \Psi$  are such that

$$f(0, n_1, \dots, n_m) = h(n_1, \dots, n_m) \quad (14)$$

$$f(k+1, n_1, \dots, n_m) = g(k, f(k, n_1, \dots, n_m), n_1, \dots, n_m) \quad (15)$$

then  $f$  is in  $\Psi$ .

A function  $f$  for which there exists functions  $g, h \in \Psi$  adhering to conditions (14) and (15) is said to be defined by **primitive recursion** via  $g, h$ . A function defined inductively by the axioms thus given along with the following extra axiom is **general recursive**.

- Let  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  be a function in  $\Psi$  such that for all  $(n_2, \dots, n_m) \in \mathbb{N}^{m-1}$  there exists  $n_1 \in \mathbb{N}$  such that  $f(n_1, \dots, n_m) = 0$ . Consider the function denoted  $\mu f : \mathbb{N}^{m-1} \rightarrow \mathbb{N}$  which maps  $(n_2, \dots, n_m)$  to the least  $n \in \mathbb{N}$  such that  $f(n, n_2, \dots, n_m) = 0$ . All such  $\mu f$  are in  $\Psi$ .

A **general recursive relation**  $R \subseteq \mathbb{N}^m$  is a relation for which there exists a general recursive function  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  satisfying:

$$f(n_1, \dots, n_m) = \begin{cases} 0, & (n_1, \dots, n_m) \in R \\ 1, & (n_1, \dots, n_m) \notin R \end{cases} \quad (16)$$

**Remark 2.0.2.** Notice the slight oddity that  $f$  in (16) maps to 0 if  $(n_1, \dots, n_m)$  is an element of  $R$ , and maps to 1 if  $(n_1, \dots, n_m)$  is *not* an element of  $R$ .

**Remark 2.0.3.** Note, in the penultimate clause of Definition 2.0.1, we allow for the case that  $m = 0$ . In this situation, this clause becomes the following.

- Say  $f : \mathbb{N} \rightarrow \mathbb{N}$  is a function for which there exists  $g \in \Psi$  and  $h \in \mathbb{N}$  such that

$$f(0) = h \quad (17)$$

$$f(k+1) = g(k, f(k)) \quad (18)$$

This allows for definitions of general recursive functions of the following form. These two examples will be used later.

$$\begin{array}{ll} \text{sg}(0) = 0 & \overline{\text{sg}}(0) = 1 \\ \text{sg}(k+1) = 1 & \overline{\text{sg}}(k+1) = 0 \end{array}$$

Note: one may wonder if the case when  $m = 1$  is allowed in the final clause of Definition 2.0.1, but this just states again that the zero function is general recursive.

**Example 2.0.4.** The **predecessor function** is general recursive.

$$\begin{array}{l} P(0) = 0 \\ P(k+1) = k \end{array}$$

Here, the constant function  $n \mapsto k$  is general recursive because it is the composite of  $k$  copies of the successor function composed with the zero function.

The **cut-off subtraction function** is general recursive.

$$\begin{array}{l} -(0, x) = x \\ -(k+1, x) = P(-(k, x)) \end{array}$$

We will write  $x - y$  for  $-(y, x)$ .

The **distance function** is general recursive.

$$\begin{array}{l} d(0, x) = x \\ d(y, x) = (x - y) + (y - x) \end{array}$$

Note the distance function is not the zero function (read carefully!)

We establish some general methods for constructing general recursive functions/relations.

**Lemma 2.0.5.** *If  $f : \mathbb{N} \longrightarrow \mathbb{N}$  is a general recursive function, then the relation  $R$  defined by*

$$(n, m) \in R \text{ iff } f(n) = m \quad (19)$$

*is a general recursive relation.*

*Proof.* The characteristic function  $\chi_R$  of  $R$  is given by the following.

$$\chi_R(n, m) = \text{sg}(d(f(n), m)) \quad (20)$$

□

**Example 2.0.6.** The formulas  $n = m$  and  $n < m$  are general recursive. They respectively have characteristic functions given  $\text{sg}(d(n, m))$  and  $\text{sg}(m - n)$ .

**Lemma 2.0.7.** *If  $R, S \subseteq \mathbb{N}$  are general recursive relations, then so are  $R^c$  and  $R \cup S$ .*

*Proof.* Let  $\chi_R, \chi_S$  be the characteristic functions of  $R, S$  respectively. The characteristic function of  $R^c$  is equal to  $\overline{\text{sg}}(\chi_R)$ . The characteristic function of  $R \cup S$  is equal to the product  $\chi_R \times \chi_S$ , and it can be shown that multiplication is a general recursive function. □

**Remark 2.0.8.** A helpful way to think about Lemma 2.0.7 is in the special case where  $R, S$  are defined by *properties*  $P, Q$ . Lemma 2.0.7 in this case says that if  $R, S$  are general recursive, then so are the relations defined by the properties “not  $P$ ”, “ $P$  and  $Q$ ”, “ $P$  or  $Q$ ”, “ $P$  implies  $Q$ ”.

**Lemma 2.0.9.** *Let  $R \subseteq \mathbb{N}$  be a general recursive relation and  $f : \mathbb{N} \longrightarrow \mathbb{N}$  a general recursive function. The following two relations are general recursive.*

$$\begin{aligned} E &\subseteq \mathbb{N}, \text{ where } n \in E \text{ iff there exists } x \in \mathbb{N}, x \leq f(n) \text{ such that } x \in R \\ F &\subseteq \mathbb{N}, \text{ where } n \in F \text{ iff for all } x \in \mathbb{N} \text{ such that } x \leq f(n) \text{ we have } x \in R \end{aligned}$$

*Proof.* It can easily be shown that the factorial function  $n \longmapsto n!$  is general recursive. Let  $\chi_R$  denote the characteristic function of  $R$ . We first define the following general recursive function.

$$\begin{aligned} \hat{\chi}_E(0) &= \chi_R(f(0)) \times \chi_R(f(0) - 1) \times \dots \times \chi_R(0) \\ \hat{\chi}_E(j+1) &= \chi_R(j+1) \times \hat{\chi}_E(j) \end{aligned}$$

The characteristic function of  $E$  is then equal to the general recursive function  $\hat{\chi}(f(\_))$  which maps  $n \longmapsto \hat{\chi}(f(n))$ .

For  $F$ , we first define the following general recursive function.

$$\begin{aligned} \hat{\chi}_F(0) &= \chi_R(0) \\ \hat{\chi}_F(j+1) &= \chi_R(j+1) + \hat{\chi}_F(j) \end{aligned}$$

The characteristic function of  $F$  is then equal to the general recursive function  $\text{sg}(\hat{\chi}_F(f(\_)))$  which maps  $n \longmapsto \text{sg}(\hat{\chi}_F(f(n)))$ . □

### 3 The general recursive functions and the general recursive relations are representable

**Definition 3.0.1.** A  $f : \mathbb{N}^m \longrightarrow \mathbb{N}$  is **representable** if there exists a formula  $F(x_1, \dots, x_m, y)$  in  $Q$  with free variables  $x_1, \dots, x_m, y$  such that  $F$  satisfies the following.

$$\text{If } f(n_1, \dots, n_m) = k \text{ then } Q \vdash \forall y, F(\underline{n_1}, \dots, \underline{n_m}, y) \iff y = \underline{k} \quad (21)$$

We say that  $f$  is **strongly represented** by  $F$ .

A relation  $r \subseteq \mathbb{N}^m$  is **representable** if there exists a formula  $R(x_1, \dots, x_m)$  in  $\mathcal{Q}$  with free variables  $x_1, \dots, x_m$  such that  $R$  satisfies the following.

$$\begin{aligned} \text{If } (n_1, \dots, n_m) \in r \text{ then } Q \vdash R(\underline{n_1}, \dots, \underline{n_m}) \\ \text{If } (n_1, \dots, n_m) \notin r \text{ then } Q \vdash \neg R(\underline{n_1}, \dots, \underline{n_m}) \end{aligned}$$

We say that  $r$  is strongly represented by  $R$ .

The main result of this Section is the following.

**Lemma 3.0.2.** *The general recursive functions and the general recursive relations are representable.*

Our method of proof will be to focus on the general recursive functions, and then prove the statement about general recursive relations as a Corollary. We begin with a general recursive function  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  and mimic the construction of  $f$  to construct the required formula  $F$ . However, we wish to avoid proving directly that if  $f$  is defined by primitive recursion via  $g, h$ , that such an  $F$  exists, as this turns out to be difficult. So, we begin with a new classification of the general recursive functions.

### 3.1 The $\beta$ -function

**Definition 3.1.1.** Let  $\Phi$  denote the set constructed inductively from the following.

- First, the base cases.
  - The constantly 0 function  $\mathbf{z} : \mathbb{N} \rightarrow \mathbb{N}$  is in  $\Phi$ .
  - The successor function  $\mathbf{s} : \mathbb{N} \rightarrow \mathbb{N}, \mathbf{s}(n) = n + 1$  is in  $\Phi$ .
  - For any natural number  $n$  let  $m \leq n$  and denote by  $\pi_m^n : \mathbb{N}^n \rightarrow \mathbb{N}$  the projection onto the  $m^{\text{th}}$  component. For each such pair  $(n, m)$  the function  $\pi_m^n$  is in  $\Phi$ .
  - The addition function  $\mathbf{a} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \mathbf{a}(n, m) = n + m$ .
  - The multiplication function  $\mathbf{m} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \mathbf{m}(n, m) = nm$  is in  $\Phi$ .
  - The characteristic function  $\chi_\Delta$  of the diagonal relation  $\Delta \subseteq \mathbb{N} \times \mathbb{N}$  defined by

$$(n, m) \in \Delta \text{ if and only if } n = m \tag{22}$$

is in  $\Phi$ .

- Now the inductive cases.
  - If  $g : \mathbb{N}^m \rightarrow \mathbb{N}$  and  $h_1, \dots, h_m : \mathbb{N}^r \rightarrow \mathbb{N}$  are in  $\Phi$ , then the composite  $g(h_1, \dots, h_r)$  is in  $\Phi$ .
  - Let  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  be a function in  $\Psi$  such that for all  $(n_2, \dots, n_m) \in \mathbb{N}^{m-1}$  there exists  $n_1 \in \mathbb{N}$  such that  $f(n_1, \dots, n_m) = 0$ . Consider the function denoted  $\mu f : \mathbb{N}^{m-1} \rightarrow \mathbb{N}$  which maps  $(n_2, \dots, n_m)$  to the least  $n \in \mathbb{N}$  such that  $f(n, n_2, \dots, n_m) = 0$ , we denote this natural number  $n$  by  $\mu n.f(n, n_2, \dots, n_m)$ . All such  $\mu f$  are in  $\Phi$ .

**Lemma 3.1.2.** *In the notation of Definitions 2.0.1, 3.1.1 we have that  $\Psi = \Phi$ . In other words, the inductive definition of the set  $\Phi$  gives an alternate definition of the general recursive functions.*

It is relatively straight forward to prove that the extra base cases of Definition 3.1.1 are general recursive, the real work in proving Lemma 3.1.2 will come from showing that the inductive clauses are sufficient for describing a general recursive function  $f : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$  which is defined from primitive recursion via  $g, h$ . We

sketch the argument now: for every natural number  $k \in \mathbb{N}$  and every sequence  $(n_1, \dots, n_m) \in \mathbb{N}^m$  of natural numbers, there is a finite sequence associated to  $h(k, (n_1, \dots, n_m))$ :

$$(f(0, \underline{n}), f(1, (n_1, \dots, n_m)), \dots, f(k, (n_1, \dots, n_m))) \quad (23)$$

Next, we develop a family of functions  $\{\alpha_k : \mathbb{N}^k \rightarrow \mathbb{N}\}_{k=1}^\infty$  and another function  $\beta : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  subject to the following: if  $(y_0, \dots, y_m)$  is a sequence of natural numbers, then for all  $i = 0, \dots, m$  we have:

$$\beta(\alpha_{m+1}(y_0, \dots, y_m), i) = y_i \quad (24)$$

Hence, if  $d \in \mathbb{N}$  encodes sequence (23), then the function  $\beta$  can be used to describe  $h$ :

$$h(k, (n_1, \dots, n_m)) = \beta(d, k + 1) \quad (25)$$

It then will remain to show that  $\beta \in \Phi$ . In fact, many such  $\beta$  exist, we present a particular choice in Definition 3.1.10, while Definition 3.1.3 defines the general class of suitable functions.

**Definition 3.1.3.** Let  $A := \{\alpha_k : \mathbb{N}^k \rightarrow \mathbb{N}\}_{k=1}^\infty$  be a family of functions. A  **$\beta$ -function** corresponding to  $A$  is a function  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  satisfying the following properties.

1. For every length  $m + 1$  sequence  $(y_0, \dots, y_m)$  of natural numbers we have  $\beta(\alpha_{m+1}(y_0, \dots, y_m), i) = y_i$ .
2. In the notation of Lemma 3.1.2, we have  $\beta \in \Phi$ .

**Remark 3.1.4.** Notice that we do not ask that the  $\alpha_k$  are in  $\Phi$ . Hence, a  $\beta$ -function should be thought of as a *computable decoder*, even in the presence of *non-computable encoders*  $\alpha_k$ .

Also, we do not have any requirement in Definition 3.1.3 on the behaviour  $\beta$  when applied to elements  $(d, i)$  where  $d$  is not in the image of any  $\alpha_k$ .

We begin with a particular construction of the family  $\{\alpha_k\}_{k=1}^\infty$ . Since we wish to describe a sequence of natural numbers via a single natural number, the Chinese Remainder Theorem is a natural place to begin.

**Theorem 3.1.5** (Chinese Remainder Theorem). *Let  $x_0, \dots, x_m$  be a sequence of coprime natural numbers. Denote by  $x$  the product  $x_0 \dots x_m$ . The following is an isomorphism, where we write  $[l]_k$  for the integer  $l$  modulo  $k$ .*

$$c : \mathbb{Z}/x\mathbb{Z} \rightarrow \mathbb{Z}/x_0\mathbb{Z} \times \dots \times \mathbb{Z}/x_m\mathbb{Z} \quad (26)$$

$$[m]_x \mapsto ([m]_{x_0}, \dots, [m]_{x_m}) \quad (27)$$

We will have to calculate a suitable choice for  $x_0, \dots, x_m$  before the Chinese Remainder Theorem can be used. The following Lemma tells us our choice.

**Lemma 3.1.6.** *Let  $y_0, \dots, y_m$  be a sequence of natural numbers. Denote by  $j$  the following natural number.*

$$j = \max(m, y_0, \dots, y_m) + 1 \quad (28)$$

and for  $i = 0, \dots, m$  define the following:

$$x_i = 1 + (i + 1)j! \quad (29)$$

Then the following properties are satisfied.

- The  $x_0, \dots, x_m$  are relatively prime.
- For each  $i = 0, \dots, m$  we have  $y_i < x_i$ .



*Proof.* Let  $i \neq k$  and consider the difference  $x_i - x_k$ :

$$(1 + i)j! - (1 + k)j! = (i - k)j! \quad (30)$$

Say  $p$  divides  $(i - k)j!$ . Notice that  $i - k$  is at most  $n$  and we have chosen  $j > n$ , so if  $p$  divides  $i - k$  then  $p$  divides  $j!$ . Thus it suffices to assume  $p$  divides  $j!$ . We thus have that division of  $1 + (i + 1)j!$  by  $p$  is 1, so in particular  $p$  does *not* divide  $1 + (i + 1)j! = x_i$  for any  $i \neq k$ .

We have shown that if  $p$  divides  $x_k$  and  $x_i - x_k$  then  $p$  does not divide  $x_i$ , a contradiction.

The second clause is easy, we notice that  $y_i < j < j! < x_i$ . □

We now outline our method for representing a sequence  $(y_0, \dots, y_m)$  of natural numbers via a single natural number  $d$ . First we construct a  $(x_0, \dots, x_m)$  as given in (29), then we calculate  $c^{-1}([y_0]_{x_0}, \dots, [y_m]_{x_m})$ , where  $c^{-1}$  is the inverse of the isomorphism given by the Chinese Remainder Theorem 3.1.5. Notice that  $c^{-1}([y_0]_{x_0}, \dots, [y_m]_{x_m})$  is an element of  $\mathbb{Z}/x\mathbb{Z}$  (where  $x = x_0 \dots x_m$ ), we let  $d$  denote the least, positive representative of the equivalence class  $c^{-1}([y_0]_{x_0}, \dots, [y_m]_{x_m})$ . Hence, we have described a family of functions:

$$\alpha_{k+1} : \mathbb{N}^{k+1} \longrightarrow \mathbb{N} \quad (31)$$

$$(y_0, \dots, y_m) \longmapsto d \quad (32)$$

Now we show the existence of a corresponding  $\beta$ -function, we sketch the general idea here. Let  $(y_0, \dots, y_m)$  be a sequence of natural numbers and let  $y$  denote  $\alpha_{m+1}(y_0, \dots, y_m)$ . We require a function  $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$  so that for all such sequences we have  $\beta(y, i) = y_i$ . By the discussion above, we can recover  $y_i$  from  $y$  by constructing  $x_0, \dots, x_m$  and then  $y_i = [y]_{x_i}$ . Now a subtlety arises, the integer  $x_i$  is defined as  $1 + (i + 1)j!$  where  $j$  is defined as  $\max(m, y_0, \dots, y_m) + 1$ , hence, if we were to construct  $y_i$  from  $y$  alone we would need a way to construct  $y_0, \dots, y_m$ , so this is a circular approach!

However, if we already had access to the integer  $j!$  then this problem would go away. So, we can define a function  $\beta^* : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$  subject to  $\beta^*(y, j!, i) = y_i$ . Then it is simply a matter of finding a way to encode the pair  $(y, j!)$  as a single integer, in other words, we need to define an injective function  $J : \mathbb{N} \times \mathbb{N} \hookrightarrow \mathbb{N}$  such that  $J \in \Phi$ . We do this in Definition 3.1.7.

**Definition 3.1.7.** Define the following functions.

$$J : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad (33)$$

$$(x, y) \longmapsto \frac{1}{2}(x + y)(x + y + 1) + x \quad (34)$$

$$K : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad (35)$$

$$(x, y) \longmapsto \min x' \leq y, \exists y' \leq x, x = J(x', y') \quad (36)$$

$$L : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad (37)$$

$$(x, y) \longmapsto \min y' \leq y, \exists y' \leq x, x = J(x', y') \quad (38)$$

**Lemma 3.1.8.** In the notation of Definition 3.1.7, the function  $J$  is injective, and for all  $(x, y) \in \mathbb{N} \times \mathbb{N}$  we have:

$$K(J(x, y), J(x, y)) = x \quad (39)$$

$$L(J(x, y), J(x, y)) = y \quad (40)$$

**Remark 3.1.9.** The exact definition of the functions  $J, K, L$  are not important, we just need them to be functions in  $\Phi$  (see Definition 3.1.1) and equations (39), (40) to hold.

Also, one might wonder why we didn't define  $K(x, y) = \mu x'. \exists y' \leq x, x = J(x', y')$ , this is because if we did, then  $K$  would be in  $\Phi$  only if  $J$  is surjective, which we wish not to check.

We can now define our  $\beta$ -function.

**Definition 3.1.10.** Define the following.

$$\beta^* : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad \beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad (41)$$

$$(l, y, i) \longmapsto \text{rem}(1 + (i + 1)l!, y) \qquad (y, i) \longmapsto \beta^*(K(y), L(y), i) \quad (42)$$

**Lemma 3.1.11.** Let  $(y_0, \dots, y_m)$  be a sequence of natural numbers,  $j = \max(m, y_0, \dots, y_m) + 1$ ,  $y = \alpha_m(y_0, \dots, y_m)$ ,  $d = J(j, y)$   $\beta : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$  be as given in Definition 3.1.10. Then for all  $i = 0, \dots, m$  we have:

$$\beta(d, i) = y_i \quad (43)$$

*Proof.* This is a simple calculation.

$$\begin{aligned} \beta(d, i) &= \beta^*(K(d), J(d), i) \\ &= \beta^*(j, y, i) \\ &= \text{rem}(1 + (i + 1)j!, y) \\ &= y_i \end{aligned}$$

□

We now use the function  $\beta$  to prove Lemma 3.1.2.

*Proof of Lemma 3.1.2.* We leave as an exercise the fact that the functions defined in the base case are elements of  $\Psi$ . We prove here that if  $f : \mathbb{N}^{m+1} \longrightarrow \mathbb{N}$  is a function defined by primitive recursion via  $g, h$  then  $f \in \Phi$ .

First define the relation  $R \subseteq \mathbb{N}^{m+2}$  where  $(d, y, n_1, \dots, n_m) \in R$  if and only if the following holds.

$$\beta(d, 0) = f(n_1, \dots, n_m) \text{ and for all } k < y, \beta(d, k + 1) = g(k, \beta(d, k), n_1, \dots, n_m) \quad (44)$$

We observe that the relation  $R$  is general recursive, and let  $\chi_R : \mathbb{N}^{m+2} \longrightarrow \mathbb{N}$  denote its characteristic function and define the following.

$$\hat{h} : \mathbb{N}^{m+1} \longrightarrow \mathbb{N} \quad (45)$$

$$(y, n_1, \dots, n_m) \longrightarrow \mu d. \chi_R(d, y, n_1, \dots, n_m) \quad (46)$$

We then have:

$$h(y, n_1, \dots, n_m) = \beta(\hat{h}(y, n_1, \dots, n_m), y) \quad (47)$$

□

## 3.2 Representability

Now we can prove that the general recursive functions are representable in  $Q$ .

**Lemma 3.2.1.** In the notation of Definition 3.1.1, the functions  $\mathbf{z}, \mathbf{s}, \pi_m^n, \mathbf{a}, \mathbf{m}, \chi_\Delta$  are all representable in  $Q$ .

*Proof.* First, consider the function  $\mathbf{z} : \mathbb{N} \longrightarrow \mathbb{N}$ . We claim this is represented by the formula  $\varphi_{\mathbf{z}}$  given by  $y = 0$ . We must show that for any  $n \in \mathbb{N}$  we have  $Q \vdash \varphi_{\mathbf{z}}(\underline{n}, y) \iff y = 0$ . We have taken  $\varphi_{\mathbf{z}}$  to be  $y = 0$ , so in fact we must show  $Q \vdash y = 0 \iff y = 0$ . We consider the following proof tree.

$$\frac{\frac{[y = 0]^1}{y = 0 \implies y = 0} (\implies I)^1 \quad \frac{[y = 0]^2}{y = 0 \implies y = 0} (\implies I)^2}{y = 0 \implies y = 0 \wedge y = 0 \implies y = 0} \wedge I$$

$$\frac{\varphi_{\mathbf{z}}(\underline{n}, y) \iff y = 0}{\forall y, \varphi_{\mathbf{z}}(\underline{n}, y) \iff y = 0} (\forall I)$$

It is similarly trivial to show the following.

- The function  $\mathbf{s}$  is represented by  $\varphi_{\mathbf{s}}(x, y)$  defined as  $y = x + 1$ .
- The function  $\pi_n^m$  is represented by  $\varphi_{\pi_n^m}(x_1, \dots, x_n, y)$  defined as  $y = x_m$ .
- The function  $\mathbf{a}$  is represented by  $\varphi_{\mathbf{a}}(x_1, x_2, y)$  defined as  $x_1 + x_2 = y$ .
- The function  $\mathbf{m}$  is represented by  $\varphi_{\mathbf{m}}(x_1, x_2, y)$  defined as  $x_1 \times x_2 = y$ .

It is also simple to prove that  $\chi_\Delta$  is representable, but it requires an intermediate step. First we show that if  $n \neq m$  then  $Q \vdash \neg(\underline{n} = \underline{m})$ .

To this end, say  $n \neq m$  and assume further that  $n > m$ . We construct a proof with premise  $\underline{n} = \underline{m}$  and then use finitely many applications of the axiom  $\forall x \forall y, S(x) = S(y) \implies x = y$  to deduce that  $Q \vdash S(\dots S(0)) = 0$ . Using  $(\exists I)$  we can thus infer that  $Q \vdash \exists x, S(x) = 0$  which contradicts the axiom  $\forall x, \neg(S(x) = 0)$ . This establishes the claim.

It is now straight forward to show that  $\chi_\Delta$  is represented by  $\varphi_{\chi_\Delta}(x_1, x_2, y)$  defined as  $(x_1 = x_2 \wedge y = 0) \vee (\neg(x_1 = x_2) \wedge y = 1)$ .  $\square$

**Lemma 3.2.2.** *If  $g, h : \mathbb{N} \longrightarrow \mathbb{N}$  are represented by  $G(x, y)$  and  $H(x, y)$  respectively, then the composite  $gh$  is represented in  $Q$  by the following term which we denote by  $F(x, y)$ .*

$$\exists z, H(x, z) \wedge G(z, y) \quad (48)$$

*Proof.* Say  $n, m \in \mathbb{N}$  are such that  $gh(n) = m$ . Let  $k \in \mathbb{N}$  be such that  $h(n) = k$ . Then by assumption, we have the following.

$$Q \vdash \forall y, H(\underline{n}, y) \iff y = \underline{k} \quad (49)$$

$$Q \vdash \forall y, G(\underline{k}, y) \iff y = \underline{m} \quad (50)$$

We then have the following prooftree.

[illegible]

We have shown:

$$\text{If } gh(n) = m \text{ then } Q \vdash \forall y, F(\underline{n}, y) \iff y = \underline{m} \quad (51)$$

as required.

**Lemma 3.2.3.** *Let  $g : \mathbb{N}^m \rightarrow \mathbb{N}^r$  and  $h_1, \dots, h_m : \mathbb{N} \rightarrow \mathbb{N}^r$  be representable functions. Then the composite  $g(h_1, \dots, h_m)$  is representable.*

*Proof.* Similar to the proof of Lemma 3.2.2 and is left as an exercise.  $\square$

In what follows, we write  $w < n + 1$  for  $\exists w', w' + w = n + 1$ .

**Lemma 3.2.4.** *Let  $f : \mathbb{N}^m \rightarrow \mathbb{N}$  be a representable function, represented by  $F(x_1, \dots, x_m, y)$  say. The function  $\mu^f$  is represented by the following formula which we denote by  $G$ .*

$$G(x_2, \dots, x_m, y) := F(y, x_2, \dots, x_m, 0) \wedge \forall w, w < y \implies \neg F(w, x_2, \dots, x_m, 0) \quad (52)$$

Before proving Lemma 3.2.4, we prove some preliminary lemmas.

**Lemma 3.2.5.** For all  $n > 0$  we have that  $Q \vdash \forall w, w < \underline{n+1} \implies w = 0 \vee \dots \vee w = \underline{n}$ .

*Proof.* We proceed by induction on  $n$ . First consider the case where  $n = 0$ . We need to show that  $Q \vdash \forall w, w < S(0) \implies w = 0$ . Throughout, if a proof  $\pi$  has assumptions  $p_1, \dots, p_n$  we will write  $\pi(p_1, \dots, p_n)$ . First we consider the following prooftree which we denote by  $\zeta(\neg(x = 0), \forall w, w < S(0))$ .

$$\frac{\neg(x = 0) \quad \frac{\forall x, \neg(x = 0) \implies \exists y, S(y) = x}{\neg(x = 0) \implies \exists y, S(y) = x} (\forall E) \quad \frac{[S(y') = x] \quad \exists w', x + S(w') = S(0)}{\exists w', S(y') + S(w') = S(0)} (= E)}{\frac{\exists y, S(y) = x}{\exists y'' \exists w', S(y'') + S(w') = S(0)} (\exists E)} (\exists I)$$

We can now construct the following, which we denote  $\xi(\neg(x = 0), \forall w, w < S(0))$ .

$$\frac{\zeta(\neg(x = 0), x < S(0)) \quad \frac{\frac{\frac{\forall x \forall y, y + S(x) = S(y + x)}{\forall y, y + S(w') = S(y + w')} (\forall E)}{[S(y'') + S(w') = S(0)] \quad \frac{S(y'') + S(w') = S(y'') + S(w')} (\forall E)}{S(y'') + S(w') = S(0)} (= E)}{\frac{\exists w', S(y'') + S(w') = S(0)}{\exists y'' \exists w', S(y'') + S(w') = S(0)} (\exists I)} (\exists E)$$

From  $\xi(\neg(x = 0), x < S(0))$  we can construct a proof of  $\exists y'' \exists w', w' + y'' = 0$  with assumption  $\neg(x = 0)$  in the following way, we label this proof  $\nu(\neg(x = 0), \forall w, w < S(0))$ .

$$\frac{\xi(\neg(x = 0), x < S(0)) \quad \frac{\frac{\frac{\forall x \forall y, S(x) = S(y) \implies x = y}{\forall y, S(y'') + S(w') = S(y) \implies y'' + S(w') = y} (\forall E)}{[S(y'') + S(w') = S(0)] \quad \frac{S(y'') + S(w') = S(0) \implies y'' + S(w') = 0} (\implies E)}{y'' + S(w') = 0} (\exists E)}{\frac{\exists w', y'' + S(w') = 0}{\exists y'' \exists w', y'' + S(w') = 0} (\exists I)} (\exists E)$$

From this, a contradiction can be drawn, and hence we end up at the following prooftree.

$$\frac{\nu([\neg(x = 0)]^1, [x < S(0)]^2) \quad \frac{\frac{\frac{\forall x \forall y, x + S(y) = S(x + y)}{\forall y, y'' + S(y) = S(y'') + y} (\forall E)}{y'' + S(w') = 0} (\forall E)}{\frac{S(y'') + w' = 0}{\exists z, S(z) = 0} (\exists I)} (= E)}{\frac{\exists w', y'' + S(w') = 0}{\exists z, S(z) = 0} (\exists E)} (\exists I)$$

For the inductive step, we assume that  $Q \vdash \forall w, w < \underline{n+1} \implies w = 0 \wedge \dots \wedge w = \underline{n}$  and show that  $Q \vdash \forall w, w < \underline{n+2} \implies w = 0 \wedge \dots \wedge w = \underline{n+1}$ . First we introduce some derived rules.

$$\frac{\exists y, x + S(y) = z}{\exists y, S(x + y) = z} (\exists S) \quad \frac{\exists y, S(x + y) = S(z)}{\exists y, x + y = z} (SE)_{\exists} \quad \frac{\exists x, t \quad \exists y, u = v}{\exists x \exists y, t[u := v]} (= E)_{\exists}$$

This first rule comes from the following prooftree.

$$\frac{\frac{\frac{\forall x \forall y, x + S(y) = S(x + y)}{\forall y, x + S(y) = S(x + y)} (\forall E)}{[x + S(y') = z] \quad \frac{x + S(y') = S(x + y')}{S(x + y') = z} (= E)}{\frac{S(x + y') = z}{\exists y, S(x + y) = z} (\exists I)} (\exists E)$$

The second rule comes from the following.

$$\frac{\frac{\frac{\frac{\forall x \forall y, S(x) = S(y) \implies x = y}{\forall y, S(x + y') = S(y) \implies x + y' = y} (\forall E)}{[S(x + y') = S(z)] \quad S(x + y') = S(z) \implies x + y' = z} (\implies E)}{\frac{x + y' = z}{\exists y, x + y = z} (\exists I)} \quad \frac{\exists y, S(x + y) = S(z)}{\exists y, x + y = z} (\exists E)$$

The third rule:

$$\frac{\frac{\frac{[(u = v)[y := y']]}{t[x := x'] [u[y := y'] := v[y := y']] (\exists I)}{\exists y, t[x := x'] [u := v]} (\exists I)}{\frac{\exists y, u = v \quad \exists x \exists y, t[u := v]}{\exists x \exists y, t[u := v]} (\exists E)} \quad \frac{\exists x, t \quad \exists y, t[u := v]}{\exists x \exists y, t[u := v]} (\exists E)$$

We will also make use of the following derived rule, for which we add commutativity as an axiom to  $Q$ . That is, we assume now that  $Q$  also admits the axiom  $\forall x \forall y, x + y = y + x$ .

$$\frac{\exists x \exists y, S(x) + y = t}{\exists x \exists y, y + S(x) = t} (C)_{\exists}$$

We first consider the following prooftree which we denote by  $\pi$ .

$$\frac{\frac{\frac{\forall w \exists w', w + S(w') = \underline{n+2}}{\exists w', w + S(w') = \underline{n+2}} (\forall E)}{\exists w', S(w + w') = \underline{n+2}} (\exists S)}{\exists w', w + w' = \underline{n+1}} (SE)_{\exists} \quad \frac{\frac{\forall x \neg(x = 0) \implies \exists w'', x = S(w'')}{\neg(w = 0) \implies \exists w'', w = S(w'')} (\forall E)}{\exists w'', w = S(w'')} (\implies E)}{\frac{\exists w' \exists w'', S(w'') + w' = \underline{n+1}}{\exists w' \exists w'', w' + S(w'') = \underline{n+1}} (= E)_{\exists}} (C)_{\exists}$$

We can now make use of the inductive hypothesis to prove  $\exists w', (w + S(w') = \underline{n+2}) \wedge (w' = 0 \vee \dots \vee w' = \underline{n})$ . From this we can prove  $\forall w, w = 1 \vee \dots \vee w = \underline{n+1}$ , as the proof has an assumption  $\neg(w = 0)$ . The result then follows.  $\square$

The familiar trichotomy axiom, that for all natural numbers  $n$  we have  $n = 0 \vee n > 0$  is also proveable by  $Q$ . This is the content of the next Lemma and indeed this will be used in the proof of Lemma 3.2.4.

**Lemma 3.2.6.** *The trichotomy axiom is provable in  $Q$ , that is, for all  $n \in \mathbb{N}$  we have  $Q \vdash \forall x, x < \underline{n} \vee x = \underline{n} \vee \underline{n} < x$ .*

Now we sketch a proof of Lemma 3.2.4.

*Proof of Lemma 3.2.4.* Assume that  $\mu f(n_2, \dots, n_m) = k$ , we first show that  $Q \vdash \forall y, y = \underline{k} \implies G(\underline{n_2}, \dots, \underline{n_m}, y)$ .

Notice that by the following proof tree it is sufficient to show  $Q \vdash G(\underline{n_2}, \dots, \underline{n_m}, \underline{k})$ .

$$\frac{\frac{\frac{[y = \underline{k}]^1}{G(\underline{n_2}, \dots, \underline{n_m}, y)} (= E)}{y = \underline{k} \implies G(\underline{n_2}, \dots, \underline{n_m}, y)} (\implies E)^1}{\forall y, y = \underline{k} \implies G(\underline{n_2}, \dots, \underline{n_m}, y)} (\forall I)$$

To show  $Q \vdash \forall y, G(\underline{n}_2, \dots, \underline{n}_m, \underline{k})$  it suffices by  $(\wedge I)$  to show the following.

$$Q \vdash F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0), \quad Q \vdash \forall w, w < \underline{k} \implies \neg F(w, \underline{n}_2, \dots, \underline{n}_m, 0) \quad (53)$$

The first of these is easy because it follows directly from the fact that  $f(k, n_2, \dots, n_m) = 0$ . For the second of these, it suffices by Lemma 3.2.5 to prove the following for all  $n < k$ :

$$Q \vdash \neg F(\underline{n}, \underline{n}_2, \dots, \underline{n}_m, 0) \quad (54)$$

Since  $\mu f(n_2, \dots, n_m) = k$  we have for all  $n < k$  that there exists  $l_n > 0$  satisfying  $f(n, n_2, \dots, n_m) = l_n$ . Since  $f$  is represented by  $F$  we have  $Q \vdash \forall y, F(\underline{n}, \underline{n}_2, \dots, \underline{n}_m, y) \iff y = \underline{l}_n$  and hence  $Q \vdash F(\underline{n}, \underline{n}_2, \dots, \underline{n}_m, 0) \iff 0 = \underline{l}_n$ . Hence,  $Q, F(\underline{n}, \underline{n}_2, \dots, \underline{n}_m, 0) \vdash 0 = \underline{l}_n$  leads to a contradiction as  $l_n > 0$ .

Now we need to show  $Q \vdash \forall y, G(\underline{n}_2, \dots, \underline{n}_m, y) \implies y = \underline{k}$ . We do this by showing  $Q, G(\underline{n}_2, \dots, \underline{n}_m, y) \vdash \neg(\underline{k} < y) \wedge \neg(y < \underline{k})$  which by Lemma 3.2.6 then implies that  $Q, G(\underline{n}_2, \dots, \underline{n}_m, y) \vdash y = \underline{k}$ . It then follows from  $(\implies I)$  and  $(\forall I)$  that  $Q \vdash \forall y, G(\underline{n}_2, \dots, \underline{n}_m, y) \implies y = \underline{k}$ .

Hence, the proof has been reduced to considering the following two prooftrees. We have seen in (53) already that  $Q \vdash F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0)$ , let  $\pi$  be any proof of  $F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0)$ .

$$\frac{\begin{array}{c} \pi \\ \vdots \\ F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0) \end{array} \quad \frac{[\underline{k} < y]^1 \quad \frac{\frac{G(\underline{n}_2, \dots, \underline{n}_m, y)}{\forall w, w < y \implies \neg F(w, \underline{n}_2, \dots, \underline{n}_m, 0)} (\wedge E)}{\underline{k} < y \implies \neg F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0)} (\forall E)}{\neg F(\underline{k}, \underline{n}_2, \dots, \underline{n}_m, 0)} (\implies E)}{\frac{\perp}{\neg(\underline{k} < y)}} (\neg I)^1 \quad (\neg E)$$

In the following prooftree, we use the fact that  $Q \vdash \forall w, w < \underline{k} \implies \neg F(w, \underline{n}_2, \dots, \underline{n}_m, 0)$  as shown earlier in this proof, let  $\zeta$  be any proof of  $\forall w, w < \underline{k} \implies \neg F(w, \underline{n}_2, \dots, \underline{n}_m, 0)$ .

$$\frac{\frac{\frac{G(\underline{n}_2, \dots, \underline{n}_m, y)}{F(y, \underline{n}_2, \dots, \underline{n}_m, 0)} (\wedge E) \quad \frac{[\underline{y} < \underline{k}]^1 \quad \frac{\frac{\zeta}{\forall w, w < \underline{k} \implies \neg F(y, \underline{n}_2, \dots, \underline{n}_m, 0)}{y < \underline{k} \implies \neg F(y, \underline{n}_2, \dots, \underline{n}_m, 0)} (\forall E)}{\neg F(y, \underline{n}_2, \dots, \underline{n}_m, 0)} (\implies E)}{\neg F(y, \underline{n}_2, \dots, \underline{n}_m, 0)} (\neg E)}{\frac{\perp}{\neg(\underline{y} < \underline{k})}} (\neg I)^1$$

□

**Proposition 3.2.7.** *Every general recursive function is representable.*

*Proof.* By Lemma 3.1.2 it suffices to prove the result by induction on the structure of  $\Phi$  as given in Definition 3.1.1. The result then follows from Lemmas 3.2.1, 3.2.2, 3.2.3, 3.2.4. □

**Corollary 3.2.8.** *Every general recursive relation is representable.*

*Proof.* Let  $r \subseteq \mathbb{N}^m$  be a general recursive relation. By definition the characteristic function  $\chi_r$  of  $r$  is general recursive, where  $\chi_r$  is defined as follows.

$$\chi_r(n_1, \dots, n_m) = \begin{cases} 0, & (n_1, \dots, n_m) \in r \\ 1, & (n_1, \dots, n_m) \notin r \end{cases} \quad (55)$$

Since  $\chi_r$  is general recursive, it follows from Proposition 3.2.7 that there exists a relation  $R(x_1, \dots, x_m, y)$  subject to:

$$Q \vdash \forall y, R(\underline{n}_1, \dots, \underline{n}_m, y) \iff y = 0 \quad (56)$$

We now consider the formula  $R(x_1, \dots, x_m, 0)$  which we denote  $\hat{R}(x_1, \dots, x_m)$ . We claim that  $\hat{R}(x_1, \dots, x_m)$  represents  $r$ . Let  $(n_1, \dots, n_m)$  be such that  $(n_1, \dots, n_m) \in r$ . Then  $Q \vdash \forall y, R(\underline{n_1}, \dots, \underline{n_m}, y) \iff y = 0$ . Observe now the following prooftree.

$$\frac{\frac{0 = 0 \text{ rflx}}{\frac{\frac{\frac{\forall y, R(\underline{n_1}, \dots, \underline{n_m}, y) \iff y = 0}{\forall y, y = 0 \implies R(\underline{n_1}, \dots, \underline{n_m}, y)} (\wedge E)}{0 = 0 \implies R(\underline{n_1}, \dots, \underline{n_m}, 0)} (\forall E)}{R(\underline{n_1}, \dots, \underline{n_m}, 0)} (\implies E)}$$

We have shown:

$$\text{If } (n_1, \dots, n_m) \in r, \text{ then } Q \vdash \hat{R}(\underline{n_1}, \dots, \underline{n_m}) \quad (57)$$

Now, say  $(n_1, \dots, n_m) \notin r$ . We thus have  $Q \vdash \hat{R}(\underline{n_1}, \dots, \underline{n_m}, y) \iff y = \underline{1}$ . We then have the following prooftree.

$$\frac{\begin{array}{c} \vdots \\ \neg(0 = S(0)) \end{array} \quad \frac{[R(\underline{n_1}, \dots, \underline{n_m}, 0)]^1}{\frac{\frac{\frac{\forall y, R(\underline{n_1}, \dots, \underline{n_m}, y) \iff y = \underline{1}}{\forall y, R(\underline{n_1}, \dots, \underline{n_m}, y) \implies y = \underline{1}} (\wedge E)}{R(\underline{n_1}, \dots, \underline{n_m}, 0) \implies 0 = \underline{1}} (\forall E)}{0 = \underline{1}} (\implies E)}{\frac{\perp}{\neg(R(\underline{n_1}, \dots, \underline{n_m}, 0))} (\neg I)^1} \quad \neg(0 = S(0))$$

We have shown:

$$\text{If } (n_1, \dots, n_m) \notin r, \text{ then } Q \vdash \neg(\hat{R}(\underline{n_1}, \dots, \underline{n_m})) \quad (58)$$

Completing the proof.  $\square$

## 4 Gödel Numbering

Due to the advancement and modern presence of computer machines, it is not surprising that the natural numbers are capable of encoding and expressing complex sentences. For instance, one could map every character inside this document to its associated ASCII integer, concatenate all these integers, and then read the result as a natural number  $n$ . This natural number has “more” inside it than the raw number  $n$ , but if read in the correct way, in fact expresses an exposition on Gödel’s First Incompleteness Theorem.

That integers can *encode* data is a key part of Gödel’s argument. Ultimately, Gödel’s argument comes down to defining a formula (the Gödel sentence  $G_Q$ ) whose provability infers a relationship of natural numbers which expresses (when interpreted in the correct way) a paradox.

The particular choice of encoding taken here is largely arbitrary, many other codings could be (and have been) used and still result in a correct argument. See Definition 1.0.7 for the encoding.

**Remark 4.0.1.** Later, we will need to be able to extract the term/formula  $\varphi$  from the integer  $\ulcorner \varphi \urcorner$  in the situation where we know that  $\ulcorner \varphi \urcorner$  is the Gödel number for some formula, hence we require that the mapping  $\varphi \mapsto \ulcorner \varphi \urcorner$  is injective. This is why we the definition of  $\ulcorner \varphi \urcorner$  involves the exponents of prime numbers.

## 5 Towards the Gödel sentence

In Section 2 we constructed many examples of general recursive functions, relations, and formulas. In this Section, we construct more elaborate general recursive relations, which will be crucial in defining the Gödel sentence,  $G_Q$ .

## 5.1 Diagonalisation

**Notation 5.1.1.** In the following, if a formula  $\varphi$  of  $Q$  admits one free variable  $y$ , then we will write  $\varphi(y)$ .

**Definition 5.1.2.** The **diagonalisation** of a formula  $\varphi(y)$  of  $Q$  is the following formula which we denote by  $\Delta(\varphi(y))$ :

$$\exists y, y = \ulcorner \varphi(y) \urcorner \wedge \varphi(y) \quad (59)$$

We next construct a function  $\text{diag} : \mathbb{N} \longrightarrow \mathbb{N}$  which given maps a number  $n$  which is the Gödel number of a formula  $\varphi(y)$  to  $\text{diag}(n) = \ulcorner \Delta(\varphi(y)) \urcorner$ .

**Lemma 5.1.3.** *The function*

$$\begin{aligned} \text{num} : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto \ulcorner n \urcorner \end{aligned}$$

*is general recursive.*

*Proof.* We can define this as follows.

$$\begin{aligned} \text{num}(0) &= 2^{\gamma(0)} = 2^1 = 2 \\ \text{num}(j+1) &= 2^{\gamma(S)} \times \text{num}(j) = 2^3 \times \text{num}(j) = 8 \times \text{num}(j) \end{aligned}$$

□

**Definition 5.1.4.** The **concatination** of two Gödel numbers  $n, m$ , denoted  $n * m$  is given as follows. First write  $n = p_1^{\ulcorner s_1 \urcorner} \dots p_n^{\ulcorner s_n \urcorner}$  and  $m = p_1^{\ulcorner t_1 \urcorner} \dots p_m^{\ulcorner t_m \urcorner}$ . Then  $n * m$  is the integer  $p_1^{\ulcorner t_1 \urcorner} \dots p_n^{\ulcorner s_n \urcorner} p_{n+1}^{\ulcorner t_1 \urcorner} \dots p_{n+m}^{\ulcorner t_m \urcorner}$ .

A fact we will not prove is the following.

**Fact 5.1.5.** *The function*

$$\begin{aligned} \text{diag} : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto \ulcorner \exists y, y = \urcorner * \text{num}(n) * \ulcorner \wedge \urcorner * n \end{aligned}$$

*is general recursive.*

**Remark 5.1.6.** Notice that in the special case where  $n$  is the Gödel number of some formula  $\varphi(y)$ , ie,  $n = \ulcorner \varphi(y) \urcorner$  then  $\text{diag}(n) = \ulcorner \Delta(\varphi(y)) \urcorner$ .

## 5.2 “Proof of”

We have shown how to represent any formula  $\varphi$  by an integer, its corresponding Gödel number  $\ulcorner \varphi \urcorner$ . Now we want to represent entire proofs with integers. This will be done by first constructing a “linear” representation of a proof tree. This is simply done by stacking a tree into a single trunk following the convention of putting the right branch at every binary deduction rule underneath the left branch. We given an example.

$$\frac{\frac{\overline{\varphi} \text{ ax}}{\psi \vee \varphi} (\vee I)_L \quad \frac{\overline{\gamma} \text{ ax}}{\gamma \vee \delta} (\vee I)_R}{(\psi \vee \varphi) \wedge (\gamma \vee \delta)} \wedge I \rightsquigarrow \frac{\frac{\overline{\varphi} \text{ ax}}{\psi \vee \varphi} (\vee I)_L \quad \frac{\overline{\gamma} \text{ ax}}{\gamma \vee \delta} (\vee I)_R}{(\psi \vee \varphi) \wedge (\gamma \vee \delta)} \wedge I$$

In the situation where there are more than one binary connective in the proof tree, we methodically work from the top of the tree (nearest the leaves) down to the root. Hence, a proof tree can be identified with a sequence of formulas, reading the truncated tree from top to bottom. It is to this sequence of formulas, we associated a *super Gödel number*.



**Definition 5.2.1.** Let  $\varphi_1, \dots, \varphi_n$  be a sequence of formulas. The **super Gödel number** of this sequence is given by the following.

$$p_1^{\ulcorner \varphi_1 \urcorner} \dots p_n^{\ulcorner \varphi_n \urcorner} \quad (60)$$

There is now the following crucial fact, we will leave unproven.

**Fact 5.2.2.** *There is a relation  $\text{proof} \subseteq \mathbb{N} \times \mathbb{N}$  which on a pair of natural numbers  $(n, m)$  where  $n$  is the super Gödel number of a proof of a formula  $\varphi$ , and  $m = \ulcorner \varphi \urcorner$ . This relation is general recursive.*

The proof of Fact 5.2.2 is where the bulk of the busy work of Gödel's Theorem lies. We leave references of work which goes through the proof of this part in more detail: [2], [1], [5], however we note that these resources use simpler proof systems, the author knows of no detailed account of the proof of Fact 5.2.2 (as stated with respect to Gentzen's Natural Deduction).

## 6 Gödel's Sentence

In Section 5 we mentioned that the function  $\text{diag} : \mathbb{N} \rightarrow \mathbb{N}$  and the relation  $\text{proof} \subseteq \mathbb{N} \times \mathbb{N}$  are general recursive. The composition of general recursive functions remains general recursive, so the following relation is general recursive.

$$\text{gdl} \subseteq \mathbb{N} \times \mathbb{N}, \text{ where } (n, m) \in \text{gdl} \text{ iff } (n, \text{diag}(m)) \in \text{proof} \quad (61)$$

Since this is general recursive, and general recursive relations are strongly representable in  $Q$  (Lemma 3.0.2) there exists a formula GDL of  $Q$  satisfying the following.

$$\begin{aligned} (n, m) \in \text{gdl} &\text{ implies } Q \vdash \text{GDL}(\underline{n}, \underline{m}) \\ (n, m) \notin \text{gdl} &\text{ implies } Q \vdash \neg \text{GDL}(\underline{n}, \underline{m}) \end{aligned}$$

We then define  $U(y)$  to be the formula  $\forall x, \neg \text{GDL}(x, y)$ . The Gödel sentence is then the Diagonalisation of this.

$$G_Q \text{ is } \Delta(U(y)) \text{ which is } \exists y, y = \ulcorner U(y) \urcorner \wedge U(y) \quad (62)$$

We have the following proof trees.

$$\frac{\exists y, y = \ulcorner U(y) \urcorner \wedge U(y)}{U(\ulcorner U(y) \urcorner)} \exists E$$

and so  $G_Q$  can also be taken to be  $U(\ulcorner U(y) \urcorner)$ . In turn, this formula is the same as  $\forall x, \neg \text{GDL}(x, \ulcorner U(y) \urcorner)$ .

We now prove the following.

**Lemma 6.0.1.** *If  $Q$  is consistent, then  $Q \not\vdash G_Q$ .*

*Proof.* Say  $Q \vdash G_Q$  and let  $\pi$  be a proof of  $G_Q$ . We let  $m$  be the super Gödel number (Definition 5.2.1) of  $\pi$ . Since  $G_Q$  is the diagonalisation of  $U(y)$ , we hence have  $(m, \ulcorner U(y) \urcorner) \in \text{gdl}$ , which as GDL represents gdl implies that  $Q \vdash \text{GDL}(\underline{m}, \ulcorner U(y) \urcorner)$ . However, we have assumed that  $Q \vdash G_Q$ , ie,  $Q \vdash \forall x, \neg \text{GDL}(x, \ulcorner U(y) \urcorner)$ . Hence, in particular,  $Q \vdash \neg \text{GDL}(\underline{m}, \ulcorner U(y) \urcorner)$ . Hence we have contradicted our assumption that  $Q$  is consistent.  $\square$

Lastly, we wish to show that if  $Q$  is consistent, then  $Q \not\vdash \neg G_Q$ , however as mentioned in the introduction, we will only prove this in the context where  $Q$  is  $\omega$ -consistent.

**Definition 6.0.2.** The first order theory  $Q$  is  **$\omega$ -inconsistent** if there exists a formula  $\varphi(x)$  such that  $Q \vdash \exists x, \varphi(x)$  and for all integers  $m$  we have  $Q \vdash \neg \varphi(\underline{m})$ .

If  $Q$  is not  $\omega$ -inconsistent, then it is  **$\omega$ -consistent**.

**Fact 6.0.3.** *If  $Q$  is  $\omega$ -consistent, then it is consistent.*

**Lemma 6.0.4.** *If  $Q$  is  $\omega$ -consistent, then  $Q \not\vdash \neg G_Q$ .*

*Proof.* Say  $Q \vdash \neg G_Q$ . Then  $Q \vdash \exists x, \text{GDL}(x, \ulcorner U(y) \urcorner)$ . Now, since  $Q$  is  $\omega$ -consistent, it is in particular consistent, and so  $Q \vdash \neg G_Q$  implies that  $Q$  cannot prove  $G_Q$ . Hence, for every integer  $m \in \mathbb{N}$  we have that  $m$  is *not* the super Gödel number of a proof of  $G_Q$ . Hence, by strong representability, we have that  $Q \vdash \neg \text{GDL}(\underline{m}, \ulcorner U(y) \urcorner)$ , for each integer  $m \in \mathbb{N}$ . This contradicts the assumption that  $Q$  is  $\omega$ -consistent, and so we have that  $Q \not\vdash \neg G_Q$ .  $\square$

## 7 Is the use of general recursive functions problematic?

What is the role of the general recursive functions in the proof of Gödel's First Incompleteness Theorem? Essentially, they are a convenient means to describe Gödel's sentence, which is simply some formula inside the first order theory  $Q$ . Hence, the fact that these functions are general recursive is *not* their important property, but instead, the underlying representing formulas are what matter.

Notice that in order to prove Lemma 6.0.1, all we need to know is that if  $m$  is the super Gödel number of a proof of  $\pi$ , then  $Q \vdash \text{GDL}(\underline{m}, \ulcorner U(y) \urcorner)$ , hence, as long as this can be shown, the fact that  $\text{gdl}$  is a general recursive function is not important.

In fact, in order to prove Lemma 6.0.4 all we need to know is that if  $Q \not\vdash G_Q$  then for every integer  $m \in \mathbb{N}$  we have that  $Q \vdash \neg \text{GDL}(\underline{m}, \ulcorner U(y) \urcorner)$ .

Moreover, the proof of Proposition 3.2.7 that every general recursive function is representable, took the inductive structure of the definition of a general recursive function and mimicked this construction inside  $Q$  along with natural deduction to construct a representing formula.

Hence, the role of general recursive functions inside the entire proof, is essentially just a convenient way to describe the construction of the Gödel sentence, and is in fact not a crucial part of the proof.

We outline here a way to prove Gödel's First Incompleteness Theorem without making mention of general recursive functions, we will also use an abstract notion of Gödel Numbering, meaning that we do not fix a particular such translation from proofs to integers. First, fix an injective translation from formulas in  $Q$  to natural numbers, given a formula  $F$  in  $Q$  we denote by  $\underline{F}$  its translation. Also, fix an injective translation from proofs to natural numbers, for any proof  $\pi$  we let  $\underline{\pi}$  denote its translation. The next step is to prove the following Lemma.

**Lemma 7.0.1.** *There exists a formula  $F(x, y)$  with two free variables  $x, y$  subject to the following properties.*

- *Given a proof  $\pi$  of  $\forall x, F(x, y)$  we have  $Q \vdash F(\underline{\pi}, \forall x, \underline{F}(x, y))$ .*
- *If there is no proof of  $\forall x, F(x, y)$  then for each natural number  $m \in \mathbb{N}$  we have  $Q \vdash \neg F(\underline{m}, \forall x, \underline{F}(x, y))$ .*

Then Lemmas 6.0.1, 6.0.4 can easily be adapted to accomodate Lemma 7.0.1.

Hence, the introduction of general recursive functions to this argument is a detour, one could be more direct by simply working with the underlying representing formulas right from the beginning. However, this is not so simple, as what is the underlying representing formula of a function defined by primitive recursion? Recall, that we showed that these such functions are representable by making use of a  $\beta$ -function (Definition 3.1.3).

In fact, not only is the introduction of general recursive functions not necessary, it can be argued that it is indeed problematic; what *is* a general recursive function? The point of Gödel's First Incompleteness Theorem is to show a counterintuitive result concerning the theory of arithmetic. Before this is organised, how can we discuss the general recursive functions? One must accept a kind of Platonic existence of general recursive functions, but then what slips in when we do this? After all, we wish to talk about these functions, so what language do we use? A first order theory of some kind....?

It is the author's opinion that, one *ought* to present Gödel's First Incompleteness Theorem on the level of the representing formulas, in order to stay completely contained in the realm of logic and language. Only then can the philosophical implications be considered before moving onto further mathematical discourse.

# References

- [1] Kurt Gödel. On formally undecidable propositions of Principia Mathematica and related systems i. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.
- [2] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman & Hall/CRC, Boca Raton, FL, 1997.
- [3] W. Price. Soundness and completeness. Unpublished note.
- [4] B. Rosser. Extensions of some theorems of gödel and church. *Journal of Symbolic Logic*, 1936.
- [5] Peter Smith. *An Introduction to Gödel's Theorems*. Cambridge University Press, Cambridge, UK, 2007.
- [6] W. Troiani. *First Order Logic*. Unpublished note.