VERSION: May 5, 2015

Recursive Functions

1. Recursive functions

Recursive functions play an important role in the proof of the incompleteness theorems, as well as in various other areas of mathematics (e.g., descriptive set theory) and of course in computer science. Specifically, an important point in the proof of the incompleteness theorem is that recursive functions are "representable" within a certain weak theory F of arithmetic (to be defined later). Here, we first introduce and study them for their own sake.

First, a few metamathematical comments. In this section, we work in a sufficiently strong background metatheory in which we can speak of the natural numbers, or even subsets of natural numbers, and related notions. For example, we could take ZFC as the background metatheory (though this is far more than we need). When we speak of "the natural numbers" we mean the uniquely defined structure as defined from this metatheory (e.g., the definition of the natural numbers within ZFC). If we view the following discussion as taking place in a background model of the metatheory axioms, then the notion of "natural numbers" depends on this background model, that is, $\mathbb{N}$ is only unique up to choice of background model of the metatheory. In this following discussion, we will not explicitly formalize this metatheory, but implicitly assume it suffices to define the objects we discuss. In §2 we will more carefully introduce an axiomatization for the natural numbers and establish connections between recursive functions and "representability" in this system. This will be important for the proof of the incompleteness theorem.

Definition 1.1. A *total* function f from ω^n to ω is just a function $f\colon \omega^n \to \omega$, that is, with domain ω^n. A *partial* function f from $\omega^n \to \omega$ is a function $f\colon D \to \omega$ where $D \subseteq \omega^n$ is the domain of the function.

The distinction between total and partial functions is important in the subject, and we must be careful to specify what we are talking about if it is not clear from the context.

Intuitively, a (total or partial) recursive function $f\colon \omega^n \to \omega$ is a function which is machine computable. The collection of algorithms corresponds to the collection of partial recursive recursive functions (as not every algorithm computes a total function). One approach to the subject is to formalize this notion of a "machine computation." There are several simple machine models which can be taken as the definition of machine computations such as Turing machines, register machines, etc. This gives a natural and intuitive approach, however, it is somewhat cumbersome to verify that all of the needed functions are computable in this manner.

On the other hand, one could take an approach which is even more removed from the intuitive notions of computability, but which perhaps results in a yet more concise and elegant presentation. Namely, one could define the recursive and semi-recursive sets (we will define these in our approach below) as the the sets which are Δ_1 and Σ_1 respectively over V_ω (the collection of hereditarily finite sets; again we will define these notions below). Our approach is more axiomatic, but still closely related to the basic intuition of computability. Along these lines, the reader will

note that clause 3 (primitive recursion) is closely related to the programming notion of a **for** loop, while clause 4 (minimalization) is closely related to the programming notion of a **while** loop (these two programming notions would be used in practice to implement these respective two clauses).

Although perhaps somewhat less intuitive than the approach involving machine computability, our approach results in a more compact presentation, and also has other advantages such as identifying the class of primitive recursive functions along the way. Of course, it can be shown that all the various approaches define precisely the same class of functions.

The fact that this class of functions (which ever approach one takes to defining it) is the "right" notion of "computable function" is a philosophical statement which is referred to as *Church's thesis*. This is considered accepted orthodoxy by current mainstream mathematics, but it is not inconceivable that this could change in the future if more exotic physical computation methods are discovered. We emphasize, though, that Church's thesis plays no role in our mathematical presentation. Definitions 1.2 and 1.3 below are precise and unambiguous, regardless of one's philosophical beliefs regarding Church's thesis.

Definition 1.2. The collection of total recursive functions $f\colon \omega^n \to \omega$ (for some n) is the smallest collection of functions satisfying the following:

(1) (simple functions) For any $k \in \omega$, the constant function $f(\vec{x}) = k$ is recursive. The projection function $f(x_1, \ldots, x_n) = x_j$ is recursive, and the successor function $f(n) = n + 1$ is recursive.

(2) (composition) The class is closed under composition, that is, if $f(x_1, \ldots, x_n)$ is recursive and $g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)$ are recursive then so is $h(x_1, \ldots, x_m) = f(g_1(\vec{x}), \ldots g_n(\vec{x}))$.

(3) (primitive recursion) The class is closed under *primitive recursion*. That is, if $g(\vec{x})$ is recursive, and $h(y, z, \vec{x})$ is recursive, then so is f defined recursively by

$$f(n, \vec{x}) = \begin{cases} g(\vec{x}) & \text{if } n = 0 \\ h(f(n-1, \vec{x}), n-1, \vec{x}) & \text{if } n > 0 \end{cases}$$

(4) (restricted minimalization) The class is closed under minimalization. That is, if $g(\vec{x}, n)$ is recursive and for all $\vec{x}$ there is an n such that $g(\vec{x}, n) = 0$, then the function f defined by $f(\vec{x}) = \mu n\ (g(\vec{x}, n) = 0)$ is recursive. Here "μn" denotes "the least n."

the call of functions that can be defined using just clauses (1)-(3) is called the class of *primitive recursive functions*.

Note that all primitive recursive functions are total, that is, clauses (1)-(3) do not lead out of the class of total functions.

Clause (4), if applied to a g that does not necessarily satisfy the hypothesis of (4), may lead to a partial function. This suggests the following definition.

Definition 1.3. The collection of *partial recursive functions* is the smallest class of partial function from ω^n (for some n) to ω satisfying (1)-(3) above and
(4′) (unrestricted minimalization) if $g(\vec{x}, n)$ is partial recursive, then the partial function f defined by $f(\vec{x}) = \mu n\ (g(\vec{x}, n) = 0)$ is partial recursive. Here, $f(\vec{x})$ is defined and equal to n if for all $m < n$, $g(\vec{x}, m)$ is defined and not equal to 0, and $g(\vec{x}, n)$ is defined and equal to 0.

Remark 1.4. In applying clauses 2 and 3 in Definition 1.3, the natural conventions concerning the domains are used. In clause 2 (composition), $h(\vec{x})$ is defined iff all of $g_1(\vec{x}), \ldots, g_n(\vec{x})$ are defined, and also $f(g_1(\vec{x}), \ldots, g_n(\vec{x}))$ is defined. Similarly, in clause 3 (primitive recursion), $f(n, \vec{x})$ is defined iff $f(0, \vec{x}) = g(\vec{x})$ is defined, $f(1, \vec{x}) = h(f(0, \vec{x}), 0, \vec{x})$ is defined, $\ldots$, $f(n, \vec{x}) = h(f(n-1, \vec{x}), n-1, \vec{x})$ is defined.

Remark 1.5. It is true, but not immediate from the definitions, that a partial recursive function which is total is actually a total recursive function. We will see this below.

For f a partial function we use the notation $f(\vec{x}) \downarrow$ to mean $f(\vec{x})$ is defined.

It is natural to consider not just functions, but also relations. We thus make the following definition.

Definition 1.6. A relation $R \subseteq \omega^n$ is recursive iff the characteristic function $\chi_R \colon \omega^n \to \{0, 1\}$ is recursive. Likewise, we say R is primitive recursive if χ_R is primitive recursive.

We begin building a catalog of recursive functions.

Lemma 1.7. *Addition and multiplication are (primitive) recursive.*

Proof. The addition function $f(n, m) = n + m$ can be defined by a primitive recursion on m: $f(n, 0) = n$, and for $m > 0$, $f(n, m) = f(n, m-1) + 1$. Likewise, the multiplication function $g(n, m) = n \cdot m$ can be defined by: $g(n, 0) = 0$ and $g(n, m) = g(n, m-1) + m$ (using that $+$ is primitive recursive by the first sentence). □

Lemma 1.8. *The sign function* $sg(n) = \begin{cases} 1 & \text{if } n > 0 \\ 0 & \text{if } n = 0 \end{cases}$ *is (primitive) recursive.*

Proof. Use a primitive recursion, $\mathrm{sg}(0) = 0$, and (for $m > 0$) $\mathrm{sg}(m) = h(\mathrm{sg}(m-1), m-1)$ where h is the constant 0 function. □

Lemma 1.9. *The predecessor function $p(0) = 0$, $p(n) = n-1$ for $n > 0$ is primitive recursive.*

Proof. The definition given shows it is primitive recursive (we are allowed to use $n - 1$ as an argument in the second case). □

Lemma 1.10. *The non-negative subtraction function* $a \dot{-} b = \begin{cases} a - b & \text{if } a \geqslant b \\ 0 & \text{otherwise} \end{cases}$ *is (primitive) recursive.*

Proof. By a primitive recursion on b. $a \dot{-} 0 = a$ and $a \dot{-} b = p(a \dot{-} (b-1))$ for $b > 0$. □

Lemma 1.11. *The relations $R_=(m, n) \leftrightarrow (m = n)$, $R_<(m, n) \leftrightarrow (m < n)$, and $R_>(m, n) \leftrightarrow (m > n)$ are all (primitive) recursive.*

Proof. $\chi_{R_=}(m, n) = 1 \dot{-} ((m \dot{-} n) + (n \dot{-} m))$. Also, $\chi_{R_<}(m, n) = \mathrm{sg}(n \dot{-} m)$ and similarly for $R_>$. □

Lemma 1.12. *The class of (primitive) recursive relations is closed under the boolean operations $\wedge$, $\vee$, $\neg$.*

Proof. Let R, S be (primitive) recursive (for simplicity of notation, we assume R, S are unary relations). Then $\chi_{R \wedge S}(n) = \chi_R(n) \cdot \chi_S(n)$. Also, $\chi_{R \vee S}(n) = \mathrm{sg}(\chi_R(n) + \chi_S(n))$. Finally, $\chi_{\neg R}(n) = 1 \dot{-} \chi_R(n)$. □

Note that the relations $m \leqslant n$ and $m \geqslant n$ are also therefore (primitive) recursive.

Lemma 1.13. *A function defined by cases using recursive case conditions and recursive functions is also recursive. Likewise for primitive recursive cases and functions. More precisely, If $R_1, \ldots, R_k$ are recursive (or primitive recursive) relations, and $f_1, \ldots, f_k$ are recursive (or primitive recursive) functions, then the function*

$$f(n) = \begin{cases} f_1(n) & \text{if } R_1(n) \\ f_2(n) & \text{if } R_2(n) \\ & \vdots \\ f_k(n) & \text{if } R_k(n) \\ f_{k+1}(n) & \text{otherwise} \end{cases}$$

is also recursive (primitive recursive). Here, in defining $f(n)$, we use the first case that applies.

Proof.

$$\begin{aligned} \chi_f(n) = {} & f_1(n) \cdot \chi_{R_1}(n) + f_2(n) \cdot (\chi_{R_2}(n) \dot{-} \chi_{R_1}(n)) + \cdots \\ & + f_{k+1}(n) \cdot ((1 \dot{-} \chi_{R_1}(n)) \cdots \dot{-} \chi_{R_k}(n)). \end{aligned}$$

□

Lemma 1.14. *Recursive relations are closed under substitution of recursive functions. That is, if R is a recursive relation and f is a total recursive function, then $R'(n) \leftrightarrow R(f(n))$ is also recursive. The same is true for primitive recursive.*

Proof. $\chi_{R'}(n) = \chi_R(f(n))$ is a composition of two recursive (or primitive recursive) functions. □

Recall a relation R is recursive iff its characteristic function χ_R is recursive. We can also go from functions back to relations according to the following lemma.

Lemma 1.15. *Let $f \colon \omega^n \to \omega$ be a (total) function. Then f is recursive iff its graph $G_f = \{(\vec{n}, m) \colon f(\vec{n}) = m\}$ is.*

Proof. Suppose f is total recursive. then the graph G_f is a recursive relation since $\chi_{G_f}(\vec{n}, m) = \chi_=(f(\vec{n}), m)$ is a composition of recursive functions.

Suppose next that f is total and G_f is a recursive relation, that is, χ_{G_f} is recursive. Then $f(\vec{n}) = \mu m \ (1 \dot{-} \chi_{G_f}(\vec{n}, m) = 0)$. Note that χ_{G_f} is total and $\forall \vec{n} \ \exists m \ (1 \dot{-} \chi_{G_f}(\vec{n}, m) = 0$. This shows that f is total recursive. □

Remark 1.16. Lemma 1.15 does not hold in its entirety for partial recursive functions. If f is a partial recursive function, then its graph G_f need not be recursive (i.e., Δ^0_1) but only semirecursive (i.e., Σ^0_1). We will define these notions below. However, the other direction of Lemma 1.15 does still hold. That is, is f is a partial function and G_f is recursive, then the proof of Lemma 1.15 still shows that f is a partial recursive function (the minimalization operation in the proof is now no longer always defined).

We next show that the recursive relations are closed under *bounded number quantification*, which we define next.

Definition 1.17 (bounded number quantification)**.** Suppose $R(n_1, \ldots, n_k, m)$ is a recursive $k+1$-ary relation. If $S \subseteq \omega^k$ is given by $S(n_1, \ldots, n_k) \leftrightarrow \exists m \leqslant n_i \; R(n_1, \ldots, n_k, m)$ (for some fixed i), then we say S is obtained by a (single) bounded existential quantification from R. Likewise, if we have $S(n_1, \ldots, n_k) \leftrightarrow \forall m \leqslant n_i \; R(n_1, \ldots, n_k, m)$ then we say S is obtained by a (single) bounded universal quantification from R. In both cases we say S is obtained by a (single) bounded quantification from R. We say S is obtained by bounded quantification from R (R now $k+\ell$-ary) is S is obtained from R by ℓ applications of these bounded number quantifications.

For example, we might have

$$R(n, m) \leftrightarrow \exists a \leqslant n \; \forall b \leqslant a \; \exists c \leqslant m \; S(n, m, a, b, c).$$

This R is obtained by applying three bounded number quantifiers to S.

Lemma 1.18. *If S is recursive and R is obtained from S by bounded number quantification, then R is recursive. Likewise for primitive recursive relations.*

Proof. It is enough to assume R is obtained from S by a single bounded number quantification. It is also enough to consider the bounded existential quantifier as $\forall m \leqslant n \; S$ is equivalent to $\neg \exists m \leqslant n \; \neg R$ (a direct proof for $\forall m \leqslant n$ is also easy to give). So assume $R(n_1, \ldots, n_k) \leftrightarrow \exists m \leqslant n_i \; S(n_1, \ldots, n_k, m)$, where S is recursive. Then χ_R is given by a primitive recursion over n_i (to ease notation, assume $i = 1$):

$$\begin{aligned} \chi_R(0, n_2, \ldots, n_k) &= \chi_S(0, n_2, \ldots, n_k, 0) \\ \chi_R(n_1, n_2, \ldots, n_k) &= \mathrm{sg}(\chi_R(n_1 - 1, n_2, \ldots, n_k) + \chi_S(n_1, n_2, \ldots, n_k, n_1)) \end{aligned}$$

□

A related fact is the following.

Lemma 1.19. *Suppose R is recursive. Let f be total recursive. Then the function g defined by*

$$g(m, k) = \begin{cases} \mu n \; [(m < n \leqslant f(m)) \wedge R(n, k)] & \text{if such an } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

is recursive. The same holds for R, f, g being primitive recursive.

Proof. When R, f are recursive the result follows easily from the closure of the recursive functions under restricted minimalization. We must give a slightly different argument for the primitive recursive case (which also works for the recursive case).

Note that $g(m) = h(m, m+1, f(m))$ where

$$h(m, a, b) = \begin{cases} \mu n \; [(a \leqslant n \leqslant b) \wedge R(n, k)] & \text{if such an } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

so it suffices to show that h is primitive recursive. We define h by a primitive recursion on b as follows: $h(m,a,0) = 0$ and for $b > 0$ we have

$$h(m,a,b) = \begin{cases} 0 & \text{if } b < a \\ 0 & \text{if } (b = a) \wedge \neg R(a) \\ a & \text{if } (b = a) \wedge R(a) \\ h(m,a,b-1) & \text{if } (b > a) \wedge h(m,a,b-1) \neq 0 \\ 0 & \text{if } (b > a) \wedge h(m,a,b-1) = 0 \wedge (a = 0) \wedge R(0) \\ b & \text{if } (b > a) \wedge h(m,a,b-1) = 0 \wedge \neg(a = 0 \wedge R(0)) \wedge R(b) \\ 0 & \text{otherwise} \end{cases}$$

Form Lemma 1.13 it follows that h is primitive recursive. □

The following lemma summarizes much of this discussion.

Lemma 1.20. *The class of recursive relations contains $=$, $<$, $>$, and is closed under complements, finite unions and intersections, bounded number quantification, and substitution of recursive functions. Similarly the class of primitive recursive relations is closed under these operations. Also, a function is recursive iff its graph is recursive.*

Continuing with our catalog of recursive functions and relations, we now show that various coding and decoding functions and related notions are all recursive (in fact, primitive recursive).

We let the *exponentiation* function $E(m,n)$, which we usually denote by m^n, be defined in the usual way, with the provision that $E(0,0) = 1$. This function is primitive recursive as it can be given by the following primitive recursion on n: $E(m,0) = 1$, and for $n > 0$, $E(m,n) = E(m,n-1) \cdot m$.

Let $p(0) = 2$, $p(1) = 3$, $p(2) = 5, \ldots$, and in general $p(n) =$ the next prime after $p(n-1)$ (we refer to $p(i)$ as the "i^{th} prime").

Definition 1.21. For $(a_0, \ldots, a_k) \in \omega^{<\omega}$ let $\langle a_0, \ldots, a_k \rangle = p_0^{a_0+1} p_1^{a_1+1} \cdots p_k^{a_k+1}$. Let $\text{Seq} = \{\langle \vec{a} \rangle \colon \vec{a} \in \omega^{<\omega}\}$ be the set of all codes of finite sequences. For $n = \langle a_0, \ldots, a_k \rangle \in \text{Seq}$, let $\text{lh}(n) = k+1$ be the length of the sequence coded by n, and for $n \notin \text{Seq}$, let $\text{lh}(n) = 0$. Define the binary decoding function $(n,i) \to (n)_i$ by $(n)_i = a_i$ if $n = \langle a_0, \ldots, a_k \rangle$ codes a sequence of length $> i$, and $(n)_i = 0$ otherwise.

Clearly the map $(\vec{a}) \to \langle \vec{a} \rangle$ is one-to-one on $\omega^{<\omega}$.

Lemma 1.22. *The function $n \mapsto p(n)$ and the set Seq are primitive recursive. For any fixed $k \in \omega$, the function $(a_0, \ldots, a_k) \to \langle a_0, \ldots, a_k \rangle$ is primitive recursive. The function lh and the decoding function $(n,i) \to (n)_i$ are primitive recursive.*

Proof. First note that set of primes P is (primitive) recursive. This follows from Lemma 1.20 as

$$P(n) \leftrightarrow (n > 1) \wedge \neg(\exists a < n \; \exists b < n \; (n = a \cdot b) \wedge (a > 1 \wedge b > 1)).$$

The next prime function $i \mapsto t(i)$ =least prime greater than i is also recursive as

$$t(i) = \mu n \; [(P(n) \wedge (n > i)].$$

Note that the minimalization operator here is always obtained, since there are infinitely many primes.

The prime function $n \mapsto p(n)$ is now recursive as it is given by a primitive recursion: $p(0) = 2$ and for $n > 0$, $p(n) = t(p(n-1))$.

To see the next prime function t and the prime function p are actually primitive recursive we argue as follows. First, the function $n \mapsto n!$ is easily primitive recursive (we define, as usual, $0! = 1$). We then have

$$t(m) = \begin{cases} \mu n\ (m < n \leqslant m! + 1) \wedge P(n) & \text{if such an } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

We use here the fact that the next prime greater than m is always $\leqslant m! + 1$ (since all of the prime factors of $m! + 1$ are relatively prime to $m!$, and hence greater than m). From Lemma 1.19 it follows that the t function is primitive recursive. [We note that it is actually a theorem of number theory ("Bertrand's postulate") that there is always a prime between m and $2m$ for any m, but the trivial bound $m! + 1$ suffices for the above argument.] The prime function $p(m)$ is now given by a primitive recursion: $p(0) = 2$, and for $m > 0$, $p(m) = t(p(m-1))$. Thus both the next prime function, and the nth prime function are primitive recursive.

Note that $n \in \text{Seq} \leftrightarrow \forall p \leqslant n\ \forall q \leqslant n\ [(p, q \text{ are prime } \wedge p < q \wedge q|n) \rightarrow p|n]$. Since the dividing relation is clearly primitive recursive (using Lemma 1.20), this shows Seq is also. For any fixed k, the function $(a_0, \ldots, a_k) \rightarrow \langle a_0, \ldots, a_k \rangle$ is clearly primitive recursive. We have

$$\text{lh}(n) = \mu k \leqslant n\ [(n \notin \text{Seq} \wedge k = 0) \vee (n \in \text{Seq} \wedge p(k) \nmid n].$$

which shows the lh function is primitive recursive. Finally,

$$\begin{aligned}(n)_i = \mu k \leqslant n\ [&(n \notin \text{Seq} \wedge k = 0) \vee (n \in \text{Seq} \wedge i \geqslant \text{lh}(n) \wedge k = 0) \\ &\vee (n \in \text{Seq} \wedge i < \text{lh}(n) \wedge p(i)^{k+1} \mid n \wedge p(i)^{k+2} \nmid n)].\end{aligned}$$

which shows the function $(n, i) \mapsto (n)_i$ is primitive recursive. □

Exercise 1. Suppose g and h are primitive recursive and f is defined from them by the following *total recursion*:

$$\begin{aligned} f(0, \vec{a}) &= g(\vec{a}) \\ f(n+1, \vec{a}) &= h(\langle f(\vec{a}, 0), \ldots, f(\vec{a}, n) \rangle, \vec{a}, n). \end{aligned}$$

Show that f is primitive recursive. [hint: show that the function $f'(n, \vec{a}) = \langle f(0, \vec{a}), \ldots, f(n, \vec{a}) \rangle$ is primitive recursive.]

1.1. **Recursive sets, functions, and definability.** In this section we introduce a definability hierarchy for sets of integers, and place the recursive sets in this hierarchy. This hierarchy will involve definability over the structure of the natural numbers. We continue to work in a sufficiently strong background metatheory so that all of our various notions (e.g., $\mathbb{N}$, make sense).

Let us consider the first-order language $\mathcal{L} = (\cdot, +, E, S, <, 0)$ with logical symbols whose intended meaning is multiplication, addition, exponentiation, the successor function (i.e., $S(n) = n + 1$), the usual ordering on the natural numbers, and a constant symbol for the 0 element. We call this the *language of arithmetic*.

We introduce a hierarchy of formulas and sets.

Definition 1.23. We say a formula $\phi(x_1, \ldots, x_n)$ is Δ_0 if it is built-up through the following:

(1) All atomic formulas (in the language of number theory) are Δ_0.

(2) Δ_0 is closed under the boolean connectives.
(3) (closure under bounded quantification) If $\psi(x_1, \ldots, x_{n+1}) \in \Delta_0$, then so is $\phi = \exists x_{n+1} \leqslant x_j \ \psi(x_1, \ldots, x_n, x_j)$ (where $1 \leqslant j \leqslant n$) and so is $\phi = \forall x_{n+1} \leqslant x_j \ \psi(x_1, \ldots, x_n, x_j)$.

Thus, Δ_0 formulas are the formulas which contain only bounded number quantification. The following lemma is a useful normal form for Δ_0 formulas.

Lemma 1.24. *Every Δ_0 formula φ is logically equivalent to a Δ_0 formula ψ of the form $\psi(x_1, \ldots, x_k) = \exists y_1 \leqslant z_1 \ \cdots \forall y_\ell \leqslant z_\ell \ \sigma(x_1, \ldots, x_k, y_1, \ldots, y_\ell)$ where σ is quantifier-free., That is, ψ has the form a string of bounded number quantifiers followed by a quantifier-free formula. Here $z_1 \in \{x_1, \ldots, x_k\}$, $z_2 \in \{x_1, \ldots, x_k, y_1\}$, etc.*

Proof. It is enough to show that if ψ_1 and ψ_2 are in the normal form, then $\psi_1 \vee \psi_2$ is logically equivalent to a ψ is the normal form. Say $\psi_1(\vec{x}) = \exists y_1 \leqslant x_1 \ \psi_1'(\vec{x}, y_1)$, and $\psi_2(\vec{x}) = \forall z_1 \leqslant x_1 \ \psi_2'(\vec{x}, z_1)$, where ψ_1', ψ_2' are in the normal form and have smaller length that ψ_1, ψ_2 respectively. By changing the quantified variable (alphabetic variant) we may assume that $z_1 \neq y_1$. But then $\psi_1 \vee \psi_2$ is logically equivalent to

$$\exists y_1 \leqslant x_1 \ \forall z_1 \leqslant x_1 \ [\psi_1'(\vec{x}, y_1) \vee \psi_2'(\vec{x}, z_1)]$$

By induction, $\psi_1' \vee \psi_2'$ is logically equivalent to a Δ_0 formula in normal form, and we are done. □

The higher level formulas are defined inductively as follows.

Definition 1.25. For $n \geqslant 1$, we say $\phi \in \Sigma_n$ if it is of the form $\phi = \exists x_1 \ \ldots \exists x_n \ \psi$, where $\psi \in \Pi_{n-1}$, and $\phi \in \Pi_n$ if it is of the form $\phi = \forall x_1 \ \ldots \forall x_n \ \psi$ where $\psi \in \Sigma_{n-1}$ (we interpret Σ_0, Π_0 as being Δ_0).

Note that the negation of a Σ_n (or Π_n) formulas is logically equivalent to a Π_n (or Σ_n) formulas.

Exercise 2. Show that if φ, ψ are Σ_n formulas, then $\varphi \wedge \psi$ and $\varphi \vee \psi$ are logically equivalent to Σ_n formulas. Likewise for Π_n. [hint: follow the proof of Lemma 1.24.]

The above definitions of formula classes are purely syntactic. We now use them to introduce complexity classes for sets of integers.

Definition 1.26. We say a set $A \subseteq \omega$ is Δ_0^0 if there is a Δ_0 formula φ which defines it, that is, for all $n \in \omega$, $n \in A \leftrightarrow \mathbb{N} \models \phi(n)$. We say A is Σ_n^0 (or Π_n^0) if there is a Σ_n (resp. Π_n) formula ϕ which defines it. We say A is Δ_n^0 if it is both Σ_n^0 and Π_n^0. We say a set $A \subseteq \omega$ is *arithmetic* if A is Σ_n^0 for some n.

We now turn to the connection between the notion of recursive and definability in the arithmetic hierarchy.

Lemma 1.27. *Every Δ_0^0 set $A \subseteq \omega$ is primitive recursive.*

Proof. Since the function $\cdot, +, E, S$ and the relation $<$ are all primitive recursive, this follows immediately from Lemma 1.20. □

Consider again the functions and relations pertaining to our coding and decoding operations. The relations P (set of primes) and Seq are easily Δ_0^0. The next prime function t easily has a Δ_0^0 graph. For the other functions, it is helpful to have the following technical definition.

Definition 1.28. An $m \in \omega$ is *good* if it is of the form $m = 2^1 \cdot 3^2 \cdot \cdots p_i^{i+1}$ for some $i \in \omega$.

Lemma 1.29. *The G of good integers in Δ_0^0.*

Proof. We have

$$m \in G \leftrightarrow 2|m \wedge 4 \nmid m \wedge \forall p, q, a < m\ [(P(p) \wedge P(q) \wedge (p < q) \wedge (q|m) \\ \wedge \forall p < r < q\ \neg P(r)) \rightarrow (p^a|m \leftrightarrow q^{a+1}|m)]$$

□

The graph G_p of the function $i \mapsto p(i) = i$th prime can be written as

$$G_p(i, p) \leftrightarrow \exists m \leqslant 2^{(i+1)^3}\ [G(m) \wedge P(p) \wedge p^{i+1}|m \wedge p^{i+2} \nmid m]$$

We use the fact that $2^1 \cdot 3^2 \cdot \cdots \cdot p(i)^{i+1} \leqslant 2^{(i+1)^3}$ as $p(i) \leqslant 2^{i+1}$. Let us denote this function as $b(i) = 2^{(i+1)^3}$ as it will appear several times. Note that the expression inside the brackets is Δ_0. The graph of the length function can be similarly expressed.

$$(\mathrm{lh}(n) = i) \leftrightarrow \exists m \leqslant b(i)\ [(n \notin \mathrm{Seq} \wedge i = 0) \vee G(m) \\ \wedge \exists p, q < m\ (P(p) \wedge P(q) \wedge p^i \mid m \wedge p^{i+1} \nmid m \wedge p \mid n \wedge \\ q^{i+1} \mid m \wedge q^{i+2} \nmid m \wedge q \nmid n)]$$

Again, the expression inside the square brackets is Δ_0. Finally, we have

$$((n)_i = k) \leftrightarrow \exists m \leqslant b(i)\ [(n \notin \mathrm{Seq} \wedge k = 0) \vee G(m) \\ \wedge \exists p < m\ (P(p) \wedge p^{i+1} \mid m \wedge p^{i+2} \nmid m \wedge p^{k+1} \mid n \wedge p^{k+2} \nmid n)] \\ \vee \forall m < n^{n+2}\ [G(m) \rightarrow \neg \exists p < m\ (P(p) \wedge p^{i+1} \mid m)\} \wedge (i = 0)]$$

We will show that the recursive subsets of ω^k are precisely the Δ_1^0 subsets.

Lemma 1.30. *Every Δ_1^0 subset of ω is recursive.*

Proof. Let $A \subseteq \omega$ be Δ_1^0, and let φ, ψ be Σ_1 formulas in the language of number theory such that for all $n \in \omega$, $n \in a \leftrightarrow \varphi^{\mathbb{N}}(n) \leftrightarrow \neg\psi^{\mathbb{N}}(n)$. Say $\varphi(m) \leftrightarrow \exists n\ \varphi'(m, n)$, $\psi(m) \leftrightarrow \exists n\ \psi'(m, n)$ where φ', ψ' are Δ_0 formulas. From Lemma 1.27, the relation $R(m, n)$, $S(m, n)$ are primitive recursive, where $R(m, n) \leftrightarrow \varphi'^{\mathbb{N}}(m, n)$ and likewise for S and ψ'.

Let $f(m) = \mu n\ [R(m, n) \vee S(m, n)]$. For any m, note that there is always an n such that $R(m, n)$ or $S(m, n)$ holds as either $\varphi^{\mathbb{N}}(m)$ or $\psi^{\mathbb{N}}(m)$. Thus, f is a total recursive function. We then have

$$\chi_A(m) = \chi_R(m, f(m))$$

which shows that A is recursive. □

To show the other containment of Lemma 1.30, and for other arguments, we need the notion of a *code* of a partial recursive function, and a computation witness. Suppose f is a total or partial recursive function. For simplicity we assume f is unary. We first define the notion of a code for a recursive function. Following is an inductive definition of the set $C \subseteq \omega$ of codes for the partial recursive functions, along with as assignment map $e \mapsto f_e$ for $e \in C$ which assigns the partial recursive function f_e to e.

Definition 1.31. The set $C \subseteq \omega$ of codes for the partial recursive functions and the assignment map $e \mapsto f_e$ are defined inductively through the following cases (note that the second component $(e)_1$ of the sequence is declaring the arity of the function).

(1) $e = \langle 0, 1\rangle \in C$, and f_e is the unary successor function, $f_e(a) = a + 1$.
(2) $e = \langle 1, k, m\rangle \in C$ and $f_e$is the k-ary constant function m.
(3) $e = \langle 2, k, \ell\rangle \in C$ if $\ell \leqslant k$. f_e is the k-ary projection onto the ℓth coordinate, that is $f_e(a_1, \ldots, a_k) = a_\ell$.
(4) $e = \langle 3, k, \ell, p\rangle \in C$ where $\ell \in C$, $p \in \mathrm{Seq}$, $\forall i < \mathrm{lh}(p)\ ((p)_i \in C \wedge ((p)_i)_1 = k)$, and $\mathrm{lh}(p) = (\ell)_1$. f_e is the function defined by composition from $f = f_\ell$ and $g_1 = f_{(p)_0}, \ldots, g_n = f_{(p)_{n-1}}$ where $n = \mathrm{lh}(p)$.
(5) $e = \langle 4, k, \ell, p\rangle \in C$ where $\ell, p \in C$, $(\ell)_1 = k - 1$, $(p)_1 = k + 1$. f_e is the function defined by primitive recursion from $g = f_\ell$ and $h = f_p$.
(6) $e = \langle 5, k, \ell\rangle$ where $(\ell)_1 = k+1$. f_e is the function defined by minimalization from the function $g = f_\ell$.

An immediate induction on the inductive definition of partial recursive function shows that for any partial recursive function f, there is an $e \in C$ such that $f_e = f$ (that is, f_e and f have the same domains, and are equal on their domains).

Lemma 1.32. *The set C of codes of partial recursive functions is recursive, in fact, primitive recursive.*

Proof. The idea is to witness e is in C by an integer f coding a sequence of length $e+1$. Each component $(f)_i$ will be 0 or 1. $(f)_i = 1$ will stand for the assertion that $i \in C$. Whenever $(f)_i = 1$, then either $i \in C$ by virtue of clauses 0, 1, or 2 above, or i has the form of clauses 3, 4, or 5, and the integers smaller than i which need to be in C are given value 1 by f. Note that if f codes a sequence of length $e + 1$, with each element of the sequence in $\{0, 1\}$, then $f \leqslant 2^{2(e+1)^2} < 2^{(e+1)^3} = b(e)$.

More formally,

$$\begin{aligned} e \in C \leftrightarrow \exists f \leqslant b(e)\ [&f \in \mathrm{Seq} \wedge \mathrm{lh}(f) = e + 1 \wedge \forall i \leqslant e\ ((f)_i \leqslant 1) \wedge (f)_e = 1 \\ &\wedge \forall i \leqslant e\ (f)_i = 1 \rightarrow \\ &\quad i = \langle 0, 1\rangle \\ &\quad \vee \exists k, m \leqslant i\ (i = \langle 1, k, m\rangle) \\ &\quad \vee \exists k, \ell \leqslant i\ ((\ell \leqslant k) \wedge i = \langle 2, k, \ell\rangle) \\ &\quad \vee \exists k, \ell, p \leqslant i\ (i = \langle 3, k, \ell, p\rangle \wedge p \in \mathrm{Seq} \wedge (f)_\ell = 1 \wedge \forall i < \mathrm{lh}(p) \\ &\qquad ((f)_{(p)_i} = 1 \wedge ((p)_i)_1 = k \wedge \mathrm{lh}(p) = (\ell)_1 \\ &\quad \vee \text{[similarly for clauses 5 and 6]}. \end{aligned}$$

From the closure properties of the primitive recursive relations it follows that C is primitive recursive. In fact, from the previous computations, we see that this may be written in the form

$$e \in C \leftrightarrow \exists u \leqslant b(e)\ [u = 2^{(i+1)^3} \wedge \psi(e, u)]$$

where ψ is Δ_0, as all of the quantifiers in ψ are bounded by u. □

Lemma 1.33. *If $A \subseteq \omega$ is recursive, then $A \in \Delta^0_1$.*

Proof. Since $\omega - A$ is also recursive, it suffices to show that $A \in \Sigma^0_1$. Let $f = \chi_A$, so f is total recursive and takes values in $\{0, 1\}$. The proof is similar to that of Lemma 1.32 in that we must "unravel" the inductive definition of f. Thus, we will write

$$m \in A \leftrightarrow \exists u \, [\mathrm{Seq}(u) \wedge \text{“}u \text{ codes a computation witness that } f(m) = 1\text{”}]$$

We will write the formal definition of a computation witness below. More generally, we define a relation $W(e, m, n, u)$ which says that u is a computation witness that $f_e(\vec{m}) = n$. Here we use this notation: let m' denote the value 0 if $m \notin \mathrm{Seq}$, and if $m \in \mathrm{Seq}$ then $m' = \langle (m)_1, \ldots, (m)_{\mathrm{lh}(m)-1} \rangle$. That is, we drop the first element $(m)_0$ from the sequence coded by m, and then recode. Thus, if m codes an input sequence $(n, \vec{x})$, then m' will code $\vec{x}$.

Exercise 3. Show that $m' < m$ and the relation $R(m, k) \leftrightarrow (k = m')$ is Δ^0_0.

The idea is that the computation witness must contain all of the integers needed to verify that the correct value has been computed. For example, if the function f is computed by a primitive recursion from g and h (as in Definition 1.3), then the integer u will witness $f(a, \vec{x}) = b$ if u contains witnesses for $f(0, \vec{x}) = g(\vec{x})$, $f(1, \vec{x}) = h(f(0, \vec{x}), 0, \vec{x})$, up through $f(a, \vec{x}) = h(f(a - 1, \vec{x}), a - 1, \vec{x})$. The computation witness u will be a sequence with $(u)_j = \langle e, m, n \rangle$ for all $j < \mathrm{lh}(u)$. The sequence $\langle e, m, n \rangle$ will "witness" that $f_e(\vec{m}) = n$. Being a correct witness will require, inductively, that certain other witnesses are present.

We now precisely define the relation $W(\bar{e}, \bar{m}, \bar{n}, u)$ which gives the set of $(\bar{e}, \bar{m}, \bar{n}, u)$ for which $\bar{e} \in C$, $\bar{m} \in \mathrm{Seq}$, and u is a computation witness that $f_{\bar{e}}(\vec{m}) = \bar{n}$.

We have:

$$\begin{aligned}
W(\bar{e}, \bar{m}, \bar{n}, u) \leftrightarrow\ & (\bar{e} \in C) \wedge \mathrm{Seq}(\bar{m}) \wedge \mathrm{Seq}(u) \wedge \exists \bar{j} < u \ ((u)_{\bar{j}} = \langle \bar{e}, \bar{m}, \bar{n} \rangle) \wedge \\
& (\forall e, m, n \leqslant u \ \forall j < \mathrm{lh}(u) \ \{(u)_j = \langle e, m, n \rangle \rightarrow \\
& [e = \langle 0, 1 \rangle \wedge \mathrm{lh}(m) = 1 \wedge (n = (m)_0 + 1)] \\
& \vee [\exists p, q \leqslant u \ e = \langle 1, p, q \rangle \wedge \mathrm{lh}(m) = p \wedge n = q] \\
& \vee [\exists p, q \leqslant u \ e = \langle 2, p, q \rangle \wedge \mathrm{lh}(m) = p \wedge n = (m)_q] \\
& \vee [\exists p, q, r \leqslant u \ e = \langle 3, p, q, r \rangle \wedge \mathrm{lh}(m) = p \wedge \exists t \leqslant u \\
& \quad (\mathrm{Seq}(t) \wedge \mathrm{lh}(t) = \mathrm{lh}(r) \wedge \forall i < \mathrm{lh}(t) \ \exists j < \mathrm{lh}(u) \\
& \quad\quad ((u)_j = \langle (r)_i, m, (t)_i \rangle) \wedge \exists j < \mathrm{lh}(u) \ ((u)_j = \langle q, t, n \rangle))] \\
& \vee [\exists p, q, r \leqslant u \ e = \langle 4, p, q, r \rangle \wedge \mathrm{lh}(m) = p \wedge \exists t \leqslant u \ (\mathrm{Seq}(t) \\
& \quad \wedge \mathrm{lh}(t) = (m)_0 + 1 \wedge \exists j < \mathrm{lh}(u) \ ((u)_j = \langle q, m', (t)_0 \rangle) \wedge \forall i \leqslant (m)_0 \\
& \quad \exists j < \mathrm{lh}(u) \ \ ((u)_j = \langle r, \langle (t)_{i-1}, i - 1, m' \rangle, (t)_i \rangle) \wedge n = (t)_{(m)_0})] \\
& \vee [\exists p, q \leqslant u \ e = \langle 5, p, q \rangle \wedge \mathrm{lh}(m) = p \\
& \quad \wedge \exists t \leqslant b(u) \ (\mathrm{Seq}(t) \wedge \mathrm{lh}(t) = n + 1 \wedge \exists j < \mathrm{lh}(u) \ ((u)_j = \langle q, \langle \vec{m}, n \rangle, 0 \rangle) \\
& \quad \wedge \forall r < n \ \exists j < \mathrm{lh}(u) \ ((u)_j = \langle q, \langle \vec{m}, r \rangle, (t)_j \rangle \wedge (t)_j \neq 0))]\})
\end{aligned}$$

□

Using again the fact that good sequences of length $i + 1$ are bounded by $b(i) = 2^{(i+1)^3}$, (the best bound here is not important), our computation of the set C of

codes, the computations of the coding and decoding operations, and the above computation of W, we see that W can be expressed in the form

$$W(\bar{e}, \bar{m}, \bar{n}, u) \leftrightarrow \exists v \leqslant b(u)\ (v = b(u) \wedge \psi(\bar{e}, \bar{m}, \bar{n}, u, v))$$

where ψ is Δ_0. For example, "$\mathrm{lh}(m) = p$" in the above formula for W is replaced by $\exists b \leqslant v\ (b = u(m) \wedge \exists \ell < b\ [\cdots])$, where $[\cdots]$ is as the previous computation of the lh function.

If $A \subseteq \omega$ is recursive, then we have $\chi_A = f_e$ for some e. We then have

$$\begin{aligned} m \in A &\leftrightarrow \exists u\ W(e, m, 1, u) \\ &\leftrightarrow \exists u\ \exists v \leqslant b(u)\ [v = b(u) \wedge \psi(e, m, 1, u, v)] \\ &\leftrightarrow \exists v\ \exists u \leqslant v\ [v = b(u) \wedge \psi(e, m, 1, u, v)] \end{aligned}$$

where ψ is Δ_0. Thus $A \in \Sigma^0_1$, and likewise $\omega - A \in \Sigma^0_1$, so $A \in \Delta^0_1$.

We thus have:

Theorem 1.34. *Every Δ^0_0 set is primitive recursive, and the recursive subsets of ω are exactly the Δ^0_1 subsets.*

The Σ^0_1 sets occur frequently enough to warrant their own terminology.

Definition 1.35. A set $A \subseteq \omega$ is called *semi-recursive* or *recursively enumerable* or *computably enumerable* if it is Σ^0_1.

It follows immediately from Theorem 1.34 that a set is recursive iff both A and its complement $\omega - A$ are computably enumerable. The term "computably enumerable" derives from (2) of the following characterization.

Lemma 1.36. *The following are equivalent for a non-empty $A \subseteq \omega$:*

(1) *A is Σ^0_1.*
(2) *A is the range of a total recursive function.*
(3) *A is the domain of a partial recursive function.*

Proof. Suppose A is the range of the total recursive function $f = f_e \colon \omega \to \omega$. Then

$$n \in A \leftrightarrow \exists m\ \exists u\ W(e, m, n, u)$$

which shows $A \in \Sigma^0_1$. similarly, if $A = \mathrm{dom}(f_e)$ (where f_e is partial recursive), then

$$m \in A \leftrightarrow \exists n\ \exists u\ W(e, m, n, u)$$

which shows $A \in \Sigma^0_1$.

Suppose next that $A \in \Sigma^0_1$. Say $n \in A \leftrightarrow \exists m\ \psi^{\mathbb{N}}(n, m)$ where ψ is Δ_0. Let $R(n, m)$ be the (primitive) recursive relation defined by ψ. Fix $n_0 \in A$. Let

$$f(k) = \begin{cases} (k)_0 & \text{if } R((k)_0, (k)_1) \\ n_0 & \text{otherwise} \end{cases}$$

The f is total recursive and $A = \mathrm{ran}(f)$. Also, if we define

$$g(n) = \mu m\ R(n, m)$$

then g is partial recursive and $A = \mathrm{dom}(g)$. □

The above analysis also yields the following Kleene normal form theorem for recursive functions.

Theorem 1.37. *Let f be a partial recursive function. Then there are primitive recursive functions h, g such that*

$$f(m) = h(\mu k\ g(m,k) = 0)$$

Proof. Let $f = f_e$. Let $g(m,k) = \begin{cases} 0 & \text{if } W(e,m,(k)_0,(k)_1) \\ 1 & \text{otherwise} \end{cases}$. Let $h(k) = (k)_0$. Then the desired equation holds. □

As an immediate corollary we have.

Corollary 1.38. *If f is a partial recursive function (according to Definition 1.3) which is a total function, then f is total recursive (according to Definition 1.2).*

We also record the following fact, which say that there is a universal Σ^0_1 set.

Theorem 1.39. *There is a Σ^0_1 set $U \subseteq \omega \times \omega$ such that for every Σ^0_1 set $A \subseteq \omega$ there is an $e \in \omega$ with $A = U_e = \{m \colon U(e,m)\}$.*

Proof. Define

$$U(e,m) \leftrightarrow \exists k\ W(e,m,(k)_0,(k)_1).$$

Clearly $U \in \Sigma^0_1$ and from (3) of Lemma 1.36 we have that U is universal. □

Finally in this section we mention some of the properties of the arithmetical pointclasses.

Theorem 1.40. *For $n \geqslant 1$ the Σ^0_n sets are closed under finite unions and intersections, existential number quantification, bounded universal number quantification (i.e., $\forall n \leqslant m$), and recursive substitution (i.e., if f is total recursive and $R \in \Sigma^0_n$, then so is $R'(n) \leftrightarrow R(f(n))$).*

Similarly, the Π^0_n sets are closed under finite unions and intersections, universal number quantification, existential number quantification, and recursive substitution.

The Δ^0_n (for $n \geqslant 1$) classes are closed under finite unions and intersections, complements, bounded number quantification, and substitution by total recursive functions.

All of the Σ^0_n, Π^0_n classes have universal sets.

Proof. We consider the case Σ^0_n. Closure under existential number quantification is obvious. Consider a bounded universal number quantification, say $B(n) \leftrightarrow \forall m \leqslant n\ A(n,m)$ where $A \in \Sigma^0_n$. Thus, $B(n) \leftrightarrow \forall m \leqslant n\ \exists k\ C(n,m,k)$, where $C \in \Pi^0_{n-1}$ (recursive if $n = 1$). Using our coding functions we can then write $B(n) \leftrightarrow \exists l\ \forall m \leqslant n\ C(n,m,(l)_k)$. By induction this shows B is Σ^0_n. The finite union and intersection cases are easy (as in Exercise 2). Closure under recursive substitution follows from the fact that a recursive substitution into a recursive relation results in a recursive relation (from the closure properties of recursive relations), and the fact that a recursive relation is Δ^0_1. The closure properties for Δ^0_n follow from those for Σ^0_n and Π^0_n. □

Exercise 4. Show that the classes Δ^0_n cannot have universal sets. [hint: if $U \subseteq \omega \times \omega$ were Δ^0_n and universal for the Δ^0_n subsets of ω, then "diagonalize" out of the class of Δ^0_n sets by defining $n \in A \leftrightarrow (n,n) \notin U$].

Exercise 5. Show that a universal Σ^0_n or Π^0_n set cannot be Δ^0_n [hint: follow the diagonal argument of the previous exercise. If the universal set U were Δ^0_n, show that the set A above would be in Δ^0_n, but not a section of U.]

2. Representability in arithmetic

There is a close relationship between recursive sets and functions and simply definable sets in models of arithmetic. This connection is important for the proof of the incompleteness theorem, and we now make it precise. First, though, we need to clarify what we mean when we speak of "the natural numbers" or "a model of arithmetic." The reader will no doubt see that we should have (in principle) addressed this point earlier, since we have been referring to the natural numbers repeatedly in our discussion of recursive functions.

Up to this point (and for a while longer), we have implicitly been working in an unspecified metatheory, that is, background axiom system which axiomatizes the rules for the objects (e.g., the natural numbers) with which we have been dealing. We have taken for granted that this metatheory suffices to establish the basic properties of the natural numbers (e.g., unique factorization into primes) that we have used. This background metatheory could be taken to bell of ZFC set theory, but we will argue later that a much weaker theory (a fragment of Peano Arithmetic) suffices. We will continue to work informally in this background metatheory for now, but we will be discussing formal axiom systems for arithmetic and formal proofs from these axioms. In particular, we will introduce below a finite set of axioms F and discuss proofs from F. Thus, within the background metatheory we are discussing formal proofs from F of certain sentences in the first-order logic of the language of number theory. We will take the formal language of number theory as the language $\mathcal{L} = (\cdot, +, E, S, <, \mathbf{0})$ with logical symbols for multiplication, addition, exponentiation, the successor function (i.e., $S(n) = n + 1$), the usual ordering on the natural numbers, and a constant symbol for the 0 element (the least element in the ordering). Note that we must be careful to separate the formal statements we are discussing from objects and statements in the metatheory. For example, 0 will denote the least element of the natural numbers (whose properties are given by the axioms in the metatheory) while $\mathbf{0}$ will denote the constant term in the formal language of number theory. To illustrate, we might make the statement "for every $n > 0$, there is a proof from F of the sentence $S^n(\mathbf{0}) \not\approx \mathbf{0}$." Here the "for every $n > 0$" is a statement in the metatheory, while "$S^n(\mathbf{0}) \not\approx \mathbf{0}$" is a formal sentence in $\mathcal{L}$. We will use $0, =$ for statements in the metatheory, and $\mathbf{0}, \approx$ in the formal theory. Both the metatheory and the formal sentences in $\mathcal{L}$ will have quantifiers, variables, and the symbols $+, \cdot$, but this should be enough to avoid confusion between the metatheory and the formal theory (we could, if desired, further the notational distinction by using different symbols for addition in the metatheory and the addition symbol in the formal language). For most purposes it is not extremely important to identify the optimal set of axioms A for the background metatheory (though we will do so later).

We now introduce a formal theory for the natural numbers. One standard axiomatization for the natural numbers is the so-called *Peano axiom* scheme, which we denote PA. This is a first-order theory in the language $\mathcal{L}$ above. It will actually suffice to establish all of the properties of the natural numbers in the metatheory that we will need as well. We will for now, however, continue to work informally in the (unspecified) metatheory and view this axiom system (and its fragment F) as a form system which are studying within the metatheory. It may help the reader to temporarily take the background metatheory as ZFC, to avoid confusion with the formal theory.

The following axiom scheme PA is the Peano axioms for the natural numbers. It consists of a finite set of axioms F (sometimes called the Frege subsystem) together with an infinite schema of induction axioms. We present the axiom scheme in the language $\mathcal{L} = \{+, \cdot, E, S, <, \mathbf{0}\}$ mentioned above, but note that the language consisting of just $+$ and $\cdot$ would suffice (the other functions, relations, and $\mathbf{0}$ can be defined from $+$ and $\cdot$ within the version of the Peano axiom scheme mentioning only the axioms for these two function). It simplifies things a little to have these extra symbols in the language, however.

Definition 2.1. The Peano axiom scheme is the following set of sentences in the language of number theory.
(Successor Axioms)
$\forall x\ \neg(S(x) \approx \mathbf{0})$.
$\forall x\ \forall y\ (S(x) \approx S(y) \to x \approx y)$
(Order axioms)
$\forall x\ \neg(x < \mathbf{0})$
$\forall x\ \forall y(x < y \vee x \approx y \vee y < x)$.
$\forall x\ \forall y\ (x < S(y) \leftrightarrow x \leqslant y)$
(Addition axioms)
$\forall x\ (x + \mathbf{0} \approx x)$
$\forall x\ \forall y\ x + S(y) \approx S(x + y)$.
(Multiplication axioms)
$\forall x\ x \cdot \mathbf{0} \approx \mathbf{0}$.
$\forall x\ \forall y\ x \cdot S(y) \approx x \cdot y + x$
(Exponentiation axioms)
$\forall x\ xE\mathbf{0} \approx S(\mathbf{0})$
$\forall x\ \forall y\ xES(y) \approx (xEy) \cdot x$
(Induction axioms)
For every formula $\phi(x)$ the axiom $[\phi(\mathbf{0}) \wedge \forall x\ (\phi(x) \to \phi(x+1))] \to \forall x\ \phi(x)$

We let PA denote the Peano axioms scheme, and let F denote PA minus the induction axioms. Thus, F is a finite set of axioms. Note that F just says that the various functions and relations are correctly computed at $S(y)$ from their values at y. As we said above, we could get by, in defining the Peano axioms, with just the addition and multiplication axioms for F.

Exercise 6. Let F' be the version of PA in the language $\mathcal{L}' = \{+, \cdot\, \mathbf{0}\}$ consisting of the addition, multiplication, and zero axioms together with the induction axioms. Define $<$ by $x < y$ iff $\exists z\ (z \neq \mathbf{0} \wedge y \approx x + z)$. Show from F' that $<$ satisfies the order axioms.

Exercise 7. Show that PA proves the following stronger induction axiom: let $\phi(x_1, \ldots, x_n)$ be a formula. Then

$$\forall x_1\ \cdots \forall x_{n-1}\ [\phi(x_1, \ldots, x_{n-1}, \mathbf{0}) \wedge \forall x_n\ (\phi(x_1, \ldots, x_n) \to \phi(x_1, \ldots, x_{n-1}, x_n + 1)] \to \forall x_n\ \phi(x_1, \ldots, x_n)].$$

The following notions of representability is important for the proof of the incompleteness theorem.

Definition 2.2. Let $R \subseteq \omega^k$. We say R is *representable* in F if there is a formula $\varphi(x_1, \ldots, x_k)$ in the language of number theory such that for all $a_1, \ldots, a_k \in \omega$ we have

(1) If $R(a_1, \ldots, a_k)$ then $F \vdash \varphi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}))$.
(2) If $\neg R(a_1, \ldots, a_k)$ then $F \vdash \neg\varphi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}))$.

We make a similar definition for functions.

Definition 2.3. Let $f\colon \omega^k \to \omega$. We say f is *representable* in F if its graph is representable. That is, there is a formula $\varphi(x_1, \ldots, x_k, y)$ in the language of number theory such that for all $a_1, \ldots, a_k \in \omega$ we have

(1) If $f(a_1, \ldots, a_k) = b$ then $F \vdash \varphi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}), S^b(\mathbf{0}))$.
(2) If $f(a_1, \ldots, a_k) \neq b$ then $F \vdash \neg\varphi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}), S^b(\mathbf{0}))$.

Our first goal is to show that all recursive relations and (total) recursive functions are representable in F.

Exercise 8. Show that every representable relation or function is recursive.

An important technical point is that representability of functions coincides with a seemingly stronger concept which we now define.

Definition 2.4. A (total) function $f\colon \omega^k \to \omega$ is *strongly representable* if there is a formula $\phi(x_1, \ldots, x_k, y)$ such that for all $a_1, \ldots, a_k$,

(1) $\mathrm{F} \vdash \phi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}), S^{f(\vec{a})}(\mathbf{0}))$ and also
(2) $\mathrm{F} \vdash [\forall z\ (\phi(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}), z) \to z \approx S^{f(\vec{a})}(\mathbf{0}))]$.

Clearly strong representability implies representability. We show that the converse holds, but first a simple technical lemma.

Lemma 2.5. *For any $n \in \omega$, $F \vdash \forall z\ (z \leqslant S^n(\mathbf{0}) \to z \approx \mathbf{0} \vee z \approx S(\mathbf{0}) \vee \cdots \vee z \approx S^n(\mathbf{0}))$.*

Proof. By induction on n. The result holds for $n = 0$ since $\mathrm{F} \vdash (z \leqslant \mathbf{0} \to z \approx \mathbf{0})$ as $\mathrm{F} \vdash \forall z\ \neg(z < \mathbf{0})$. Assume the result holds for n and assume $z \leqslant S^{n+1}(\mathbf{0})$. If $z < S^{n+1}(\mathbf{0}) = S(S^n(\mathbf{0}))$, then F proves that $z \leqslant S^n(\mathbf{0})$, in which case by induction F proves $z \approx \mathbf{0} \vee \cdots \vee z \approx S^n(\mathbf{0})$. Thus, $\mathrm{F} \vdash z \approx \mathbf{0} \vee \cdots \vee z \approx S^{n+1}(\mathbf{0})$. □

Lemma 2.6. *If f is representable, then it is strongly representable.*

Proof. Suppose $\phi(x, y)$ represents $f\colon \omega \to \omega$. Define

$$\psi(x, y) = [\phi(x, y) \wedge \forall w < y\ \neg\phi(x, w)].$$

We claim that ψ strongly represents f. Fix $n \in \omega$, and let $m = f(n)$. By assumption, $\mathrm{F} \vdash \phi(S^n(\mathbf{0}), S^m(\mathbf{0}))$. We must show that $\mathrm{F} \vdash \forall w < S^m(\mathbf{0})\ \neg\phi(S^n(\mathbf{0}), w)$. Work within F, and assume $w < S^m(\mathbf{0})$. From lemma 2.5 we can deduce $(w \approx \mathbf{0} \vee w \approx S(\mathbf{0}) \vee \cdots \vee w \approx S^{m-1}(\mathbf{0}))$. Since ϕ represents f we have that $\mathrm{F} \vdash \neg\phi(S^n(\mathbf{0}), \mathbf{0}), \ldots, \mathrm{F} \vdash \neg\phi(S^n(\mathbf{0}), S^{m-1}(\mathbf{0}))$. From these two statements it follows that $\mathrm{F} \vdash \forall w < S^m(\mathbf{0})\ \neg\phi(S^n(\mathbf{0}), w)$. Thus, $\mathrm{F} \vdash \psi(S^n(\mathbf{0}), S^m(\mathbf{0}))$.

Working within F, assume now $\psi(S^n(\mathbf{0}), z)$, so $\forall w < z\ \neg\phi(S^n(\mathbf{0}), w)$. Since $\mathrm{F} \vdash \phi(S^n(\mathbf{0}), S^m(\mathbf{0}))$, we may deduce that $z \leqslant S^m(\mathbf{0})$ (we use that fact that $\mathrm{F} \vdash (z < S^m(\mathbf{0}) \vee z \approx S^n(\mathbf{0}) \vee z > S^m(\mathbf{0}))$). So we may deduce $z \approx \mathbf{0} \vee \cdots \vee z \approx S^m(\mathbf{0})$. Since $\mathrm{F} \vdash \neg\phi(S^n(\mathbf{0}), \mathbf{0}), \ldots, \mathrm{F} \vdash \neg\phi(S^n(\mathbf{0}), S^{m-1}(\mathbf{0}))$, we may deduce $z \approx S^m(\mathbf{0})$. □

The main result in this section is that the representable relations and functions are exactly the recursive ones.

Lemma 2.7. *Let t be a* closed term*, that is, a term containing no free variables. Then there is an $n \in \omega$ such that $F \vdash t \approx S^n(\mathbf{0})$.*

Proof. By induction on the term t. If $t = \mathbf{0}$ this is trivial. If $t = S(u)$ this is also trivial as $\mathrm{F} \vdash u \approx S^n(\mathbf{0})$ for some n by induction, and $S(S^n(\mathbf{0})) = S^{n+1}(\mathbf{0})$. If $t = u+v$, then by induction it suffices to show that $\mathrm{F} \vdash S^n(\mathbf{0})+S^m(\mathbf{0}) \approx S^{n+m}(\mathbf{0})$. This, in turn, is proved by induction on n, say, with the inductive step given by $\mathrm{F} \vdash S(S^{n-1}(\mathbf{0}))+S^m(\mathbf{0}) \approx S(S^{n-1}(\mathbf{0})+S^m(\mathbf{0})) \approx S(S^{n+m-1}(\mathbf{0})) = S^{n+m}(\mathbf{0})$. The result for terms of the form $t = u \cdot v$ follows similarly from $\mathrm{F} \vdash S^n(\mathbf{0}) \cdot S^m(\mathbf{0}) \approx S^{n \cdot m}(\mathbf{0})$ which is proved by induction, using the result for addition. The inductive step is given by

$$\mathrm{F} \vdash (S^n(\mathbf{0}) \cdot S(S^{m-1}(\mathbf{0}))) \approx S^n(\mathbf{0}) \cdot S^{m-1}(\mathbf{0}) + S^n(\mathbf{0}) \approx S^{nm-n}(\mathbf{0}) + S^n(\mathbf{0}) \approx S^{nm}(\mathbf{0}).$$

The result for exponentiation is similar. □

Lemma 2.8. *If φ is quantifier free then the relation R defined by φ is representable in F, in fact, it is represented by the same formula φ.*

Proof. First consider the case φ is atomic. For this it suffices to show that if t, u are closed terms then $\mathrm{F} \vdash t < u$ iff $t^{\mathbb{N}} < u^{\mathbb{N}}$ and and likewise $\mathrm{F} \vdash (t \approx u)$ iff $t^{\mathbb{N}} = u^{\mathbb{N}}$. We consider first the the $\approx$ case. By Lemma 2.7 there are $n, m \in \omega$ such that $\mathrm{F} \vdash t \approx S^n(\mathbf{0})$ and $\mathrm{F} \vdash u \approx S^m(\mathbf{0})$. It suffices to show that if $n = m$ then $\mathrm{F} \vdash S^n(\mathbf{0}) \approx S^m(\mathbf{0})$ and if $n \neq m$ then $\mathrm{F} \vdash \neg(S^n(\mathbf{0}) \approx S^m(\mathbf{0}))$. The first is trivial. For the second, we prove by induction on $\min\{n, m\}$ that if $n \neq m$ then $\mathrm{F} \vdash \neg(S^n(\mathbf{0}) \approx S^m(\mathbf{0}))$. If $\min\{n, m\} = 0$, this follows from the first successor axiom. Otherwise, by induction $\mathrm{F} \vdash \neg(S^{n-1}(\mathbf{0}) \approx S^{m-1}(\mathbf{0}))$. The second successor axiom then gives that $\mathrm{F} \vdash \neg(S^n(\mathbf{0}) \approx S^m(\mathbf{0}))$.

We now consider the $<$ case. Again by Lemma 2.7 there are $n, m \in \omega$ such that $\mathrm{F} \vdash t \approx S^n(\mathbf{0})$ and $\mathrm{F} \vdash S^m(\mathbf{0})$. It suffices to know that if $n < m$ then $\mathrm{F} \vdash S^n(\mathbf{0}) < S^m(\mathbf{0})$ and otherwise $\mathrm{F} \vdash \neg(S^n(\mathbf{0}) < S^m(\mathbf{0}))$. First we show by induction on $m > n$ that $\mathrm{F} \vdash S^n(\mathbf{0}) < S^m(\mathbf{0})$. For $m = n + 1$, $\mathrm{F} \vdash S^n(\mathbf{0}) < S^{n+1}(\mathbf{0}) = S(S^n(\mathbf{0}))$ follows from the axiom of F $\forall x\ \forall y\ (x < S(y) \leftrightarrow x \leqslant y)$ which implies $\forall x\ (x < S(x))$. Assuming the result is true for m, that is $\mathrm{F} \vdash (S^n(\mathbf{0}) < S^m(\mathbf{0}))$, the same axiom then shows that $\mathrm{F} \vdash (S^n(\mathbf{0}) < S(S^m(\mathbf{0})) = S^{m+1}(\mathbf{0}))$. Assume now that $n \geqslant m$. Working in F, assume towards a contradiction that $S^n(\mathbf{0}) < S^m(\mathbf{0})$. From lemma 2.5 we have $\mathrm{F} \vdash S^n(\mathbf{0}) \approx \mathbf{0} \vee \cdots \vee S^n(\mathbf{0}) \approx S^{m-1}(\mathbf{0})$. However, from the equality case we know that $\mathrm{F} \vdash \neg(S^n(\mathbf{0}) \approx \mathbf{0}), \ldots, \mathrm{F} \vdash \neg(S^n(\mathbf{0}) \approx S^{m-1}(\mathbf{0}))$. This is a contradiction.

If R is representable by φ, and S is representable by ψ, then it is easy to see that $R \wedge S$ is representable by $\varphi \wedge \psi$, and likewise for $R \vee S$ and $\neg R$.

□

Lemma 2.9. *If $\varphi \in \Delta_0$ then the relation R defined by φ is representable in F, in fact it is represented by the same formula φ.*

Proof. It suffices to show that if $R(x, y)$ is representable by $\varphi(x, y)$, then $S(n) \leftrightarrow \exists m \leqslant n\ R(n, m)$ is representable by $\psi(x) = \exists y\ (y \leqslant x \wedge \varphi(x, y))$. Let $n \in \omega$, and first suppose $S(n)$. Thus there is an $m \leqslant n$ such that $R(n, m)$. Thus, $\mathrm{F} \vdash \varphi(S^n(\mathbf{0}), S^m(\mathbf{0}))$. From lemma 2.8, $\mathrm{F} \vdash S^m(\mathbf{0}) \leqslant S^n(\mathbf{0})$. Hence, $\mathrm{F} \vdash \exists y\ (y \leqslant S^n(\mathbf{0}) \wedge \varphi(S^n(\mathbf{0}), y)$, that is, $\mathrm{F} \vdash \psi(S^n(\mathbf{0}))$.

Assume now that $n \in \omega$ and $\neg S(n)$, hence for all $m \leqslant n$ we have $\neg R(n, m)$. From lemma 2.5, $\mathrm{F} \vdash \forall y\ (y \leqslant S^n(\mathbf{0}) \to y \approx \mathbf{0} \vee \cdots \vee y \approx S^n(\mathbf{0}))$. Since ϕ

represents R we also have $\mathrm{F} \vdash \neg\varphi(S^n(\mathbf{0}), \mathbf{0}), \ldots, \mathrm{F} \vdash \neg\varphi(S^n(\mathbf{0}), S^n(\mathbf{0}))$. These two statements logically imply $\forall y\ (y \leqslant S^n(\mathbf{0}) \to \neg(\varphi(S^n(\mathbf{0}), y)$. Thus, $\mathrm{F} \vdash \neg\exists y \leqslant S^n(\mathbf{0})\ (\varphi(S^n(\mathbf{0}), y))$, that is, $\mathrm{F} \vdash \neg\psi(S^n(\mathbf{0}))$ and we are done. □

The next theorem is the result we need on the representability of recursive functions.

Theorem 2.10. *Every recursive relation and every total recursive function is representable in F.*

Proof. Let $R \subseteq \omega$ be recursive (we assume R is unary for convenience). From Theorem 1.34 we have Σ_1 formulas φ, ψ such that $n \in R \leftrightarrow \varphi^{\mathbb{N}}(n) \leftrightarrow \neg\psi^{\mathbb{N}}(n)$. Say $\varphi(x) = \exists y\ \varphi'(x, y)$, $\psi(x) = \exists y\ \psi'(x, y)$ where φ', ψ' are Δ_0.

Let $\rho(x)$ be the Σ_1 formula:

$$\begin{aligned}\rho(x) &= \exists y\ [\varphi'(x, y) \wedge \forall z < y\ (\neg\varphi'(x, y) \wedge \neg\psi'(x, y))] \\ &= \exists y\ \chi(x, y)\end{aligned}$$

We show that ρ represents R. From Lemma 2.9, the relations R', S' defined by φ' and ψ' are representable, in fact by φ' and ψ' themselves (though this last fact is not important). Likewise, χ represents the relation it defines over $\mathbb{N}$.

Suppose first that $n \in R$, so $\varphi^{\mathbb{N}}(n)$ and $\neg\psi^{\mathbb{N}}(n)$. Let m be least such that ${\varphi'}^{\mathbb{N}}(n, m)$. Then for all $m' < m$ we have $\neg{\varphi'}^{\mathbb{N}}(n, m')$, and of course also $\neg\psi^{\mathbb{N}}(n, m')$. By the representability of the relations defined by φ' and ψ' we have that for all $m' < m$ that $\mathrm{F} \vdash \neg\varphi'(S^n(\mathbf{0}), S^{m'}(\mathbf{0}))$ and $\mathrm{F} \vdash \neg\psi'(S^n(\mathbf{0}), S^{m'}(\mathbf{0}))$. Also, from Lemma 2.5, $\mathrm{F} \vdash \forall z\ (z < S^m(\mathbf{0}) \to (z \approx \mathbf{0} \vee \cdots \vee z \approx S^{m-1}(\mathbf{0}))$. It follows that $\mathrm{F} \vdash \forall z < S^m(\mathbf{0})\ (\neg\varphi'(S^n(\mathbf{0}), z) \wedge \neg\psi(S^n(\mathbf{0}), z))$. Since we also have $\mathrm{F} \vdash \varphi'(S^n(\mathbf{0}), S^m(\mathbf{0}))$ we have that $\mathrm{F} \vdash \chi(S^n(\mathbf{0}), S^m(\mathbf{0}))$. This statement logically implies the statement $\exists z\ \chi(S^n(\mathbf{0}), z) = \rho(S^n(\mathbf{0}))$, so $\mathrm{F} \vdash \rho(S^n(\mathbf{0}))$.

Suppose next that $n \notin R$, and let m be least so that $\psi^{\mathbb{N}}(m)$. Exactly as in the previous paragraph we have $\mathrm{F} \vdash \psi'(S^n(\mathbf{0}), S^m(\mathbf{0}))$ and

$$\mathrm{F} \vdash \forall z < S^m(\mathbf{0})\ (\neg\varphi'(S^n(\mathbf{0}), z) \wedge \neg\psi'(S^n(\mathbf{0}), z)).$$

We must show that $\mathrm{F} \vdash \neg\rho(S^n(\mathbf{0}))$. It suffices to derive a contradiction from F and $\rho(S^n(\mathbf{0})) = \exists y\ \chi(S^n(\mathbf{0}), y)$. So, assume F and $\chi(S^n(\mathbf{0}), y)$. From $\chi(S^n(\mathbf{0}), y)$ it follows that $\forall z < y\ [\neg\psi'(S^n(\mathbf{0}), z)]$. Since $\mathrm{F} \vdash \psi'(S^n(\mathbf{0}), S^m(\mathbf{0}))$, it follows that $y \leqslant S^m(\mathbf{0})$ (we use here the fact that F proves that $<$ is a linear order). From Lemma 2.5 it follows that $\mathrm{F} \vdash (y \approx \mathbf{0} \vee \cdots \vee y \approx S^m(\mathbf{0}))$. But by representability of the relation defined by φ' we have $\mathrm{F} \vdash \neg\varphi'(S^n(\mathbf{0}), \mathbf{0}), \ldots, \mathrm{F} \vdash \neg\varphi'(S^n(\mathbf{0}), S^m(\mathbf{0}))$. From these facts it follows that $\mathrm{F} \vdash \neg\varphi'(S^n(\mathbf{0}), y)$, and so $\mathrm{F} \vdash \neg\chi(S^n(\mathbf{0}), y)$, a contradiction.

□

3. Incompleteness

In this section we prove several versions of the Gödel incompleteness theorem. First we define a coding of the formulas of number theory into the integers. Fix a bijection π between the finitely many symbols of the language (including the logical symbols) excluding the (infinitely many) variable symbols and the set $\{0, 1, \ldots, n_0 - 1\}$. Extend π to the variables by $\pi(x_k) = n_0 + k$. Then π is a bijection between the logical symbols and the integers, and the relation $R(a, b) \leftrightarrow \pi(x_a) = b$ is clearly recursive.

Definition 3.1. If $\phi = s_0 s_1, \ldots, s_k$ is a string of symbols in the language of number theory, then the *Gödel code* of ϕ is defined by $\#(\phi) = \langle \pi(s_0), \ldots, \pi(s_k) \rangle \in \omega$.

We will use in the following arguments the fact that certain relations and (total) functions on the integers are recursive. In fact, all of the relations and functions we need are primitive recursive. These facts can be easily checked from the closure properties of recursive functions of §1.

The next result is the key technical lemma for the incompleteness results. It says, in effect, that we may construct self-referential formulas. The formulas attempt to refer to themselves by referring to the Gödel codes of themselves.

Lemma 3.2. *Let $\theta(x)$ be a formula in the language of number theory with one free variable x. Then there is a sentence σ (in the language of number theory) such that $F \vdash (\sigma \leftrightarrow \theta(S^{\#\sigma}(\mathbf{0})))$.*

Proof. Let $f\colon \omega \to \omega$ be the primitive recursive function defined as follows. If n is the code of a formula ψ with one free variable, then $f(n)$ is the code of the sentence $\psi(S^{\#\psi}(\mathbf{0}))$. Otherwise, let $f(n) = 0$. Let $\rho(x, y)$ strongly represent f in F. Let τ be the formula

$$\tau = \exists x_1 \ (\rho(x_0, x_1) \wedge \theta(x_1)).$$

Note that τ has one free variable, x_0. Let $n = \#\tau$. Let $\sigma = \tau(S^{\#\tau}(\mathbf{0}))$. Let $m = f(n)$, which is the code for $\tau(S^{\#\tau}(\mathbf{0})) = \sigma$. We show that σ works. Working within F, first assume σ. Thus, $\exists x_1 \ (\rho(S^{\#\tau}(\mathbf{0}), x_1) \wedge \theta(x_1))$. By strong representability, $\mathrm{F} \vdash \forall x_1 \ (\rho(S^{\#\tau}(\mathbf{0}), x_1) \to x_1 \approx S^m(\mathbf{0}))$. These two sentences logically imply $\theta(S^m(\mathbf{0}))$, that is, $\theta(S^{\#\sigma}(\mathbf{0}))$.

Assume next $\theta(S^{\#\sigma}(\mathbf{0}))$, that is, $\theta(S^m(\mathbf{0}))$. Since $\mathrm{F} \vdash \rho(S^n(\mathbf{0}), S^m(\mathbf{0}))$ by representability, we may deduce $\exists x_1 \ (\rho(S^n(\mathbf{0}), x_1) \wedge \theta(x_1))$. Thus, we may deduce $\tau(S^n(\mathbf{0}))$, that is, σ. □

We now state the first version of the incompleteness theorem. We call a set of sentences T recursive if $\{\#\phi\colon \phi \in T\}$ is recursive. The reader will note that the sentence σ constructed in the following proof is a formalization of the statement "this sentence is not provable."

Theorem 3.3. *Let T be a consistent, recursive set of sentences in the language of number theory which contains F. Then T is incomplete, that is, there is a sentence σ such that $T \nvdash \sigma$ and $T \nvdash \neg\sigma$.*

Proof. Towards a contradiction assume that T is complete. Let $R = \{\#\phi\colon T \vdash \phi\}$. We claim that R is recursive. This is because we may check if $n \in R$ by enumerating all possible deductions from T and checking at each step if it is a deduction from T of either ϕ (the formula with code n) or a deduction of $\neg\phi$. We output a 1 if for the least such deduction we encounter it is a deduction of ϕ. Checking if an integer codes a valid deduction from T is recursive, using the assumption that T is recursive. This algorithm will always terminate by our completeness assumption. The answer will be correct as T is consistent.

Let θ represent $\neg R$ in F. Let σ be the sentence of lemma 3.2 applied to θ. Thus, F, and hence T proves the statement

$$\sigma \leftrightarrow \theta(S^{\#\sigma}(\mathbf{0})).$$

Let $n = \#\sigma$. If $R(n)$, then $\mathrm{F} \vdash \neg\theta(S^n(\mathbf{0}))$, and so $T \vdash \neg\sigma$. Thus, $\neg R(n)$, a contradiction. If $\neg R(n)$, then $\mathrm{F} \vdash \theta(S^n(\mathbf{0}))$, and so $T \vdash \sigma$. Hence $R(n)$, a contradiction. □

Theorem 3.3 was proved by contradiction, and thus does not actually produce a concrete sentence σ which is independent of T. With a little extra argument we can do this. First we give the argument due to Gödel which shows this under a slightly stronger hypothesis.

Definition 3.4. We say T is ω-consistent if there is no formula $\phi(x)$ such that for all $n \in \omega$, $T \vdash \neg\phi(S^n(\mathbf{0}))$ but $T \vdash \exists x\ \phi(x)$.

Of course, an ω-consistent theory is consistent, but the converse is not true. An ω-inconsistent theory is one that has no standard model.

For T a recursive set of sentences in the language of number theory, let R_T be the relation defined by $R_T(a, b)$ iff b is the code of a deduction from T of the formula with code a. R_T is clearly recursive. Let $\rho(x, y)$ strongly represent R in F. Let $\theta(x) = \neg\exists y\ \rho(x, y)$, and let $\sigma_1 = \sigma_1(T)$ be the sentence such that $\mathrm{F} \vdash \sigma_1 \leftrightarrow \theta(S^{\#\sigma_1}(\mathbf{0}))$ from lemma 3.2.

Theorem 3.5. *Let T be an ω-consistent, recursive set of sentences in the language of number theory which contains F. Then $T \nvdash \sigma_1$ and $T \nvdash \neg\sigma_1$.*

Proof. The proof is similar to theorem 3.3. Assume first that $T \vdash \sigma_1$. Let $n = \#\sigma_1$. Let m code a deduction of σ_1 from T. Thus, $T \vdash \rho(S^n(\mathbf{0}), S^m(\mathbf{0}))$ (in the notation above). This logically implies $\neg\theta(S^n(\mathbf{0}))$, and thus $T \vdash \neg\sigma_1$. This contradicts the assumption that T is consistent (note: this case only used the consistency of T).

Assume next that $T \vdash \neg\sigma_1$. Thus, $T \vdash \neg\theta(S^n(\mathbf{0}))$, and so $T \vdash \exists y\ \rho(S^n(\mathbf{0}), y)$. Since $T \nvdash \sigma_1$ from the previous paragraph, we know that for all $m \in \omega$ that $\neg R_T(n, m)$, and hence $T \vdash \neg\rho(S^n(\mathbf{0}), S^m(\mathbf{0}))$. This contradicts the ω-consistency of T. □

The extra hypothesis of ω-consistency, though minor, is slightly annoying. An improvement of theorem 3.5, due to Rosser, shows that it is actually unnecessary. Let $R_T(a, b)$ and $\rho(x, y)$ be as above. Let $g\colon \omega \to \omega$ be a recursive function such that if a is the code of ϕ, then $g(a)$ is the code of $\neg\phi$. Let $\eta(x, y)$ strongly represent g. Let $\tau(x)$ be the formula

$$\tau = \forall y\ (\rho(x, y) \to \exists z < y\ \exists w\ (\eta(x, w) \wedge \rho(w, z)))$$

Let $\sigma_2 = \sigma_2(T)$ be the sentence from lemma 3.2 for this τ.

Theorem 3.6. *Let T be a consistent, recursive set of sentences in the language of number theory which contains F. Then $T \nvdash \sigma_2$ and $T \nvdash \neg\sigma_2$.*

Proof. Let $n = \#\sigma_2$. Assume first $T \vdash \sigma_2$. Let m code a deduction of σ_2 from T. So, $T \vdash \rho(S^n(\mathbf{0}), S^m(\mathbf{0}))$. Also, $T \vdash \forall y\ (\rho(S^n(\mathbf{0}), y) \to \exists z < y\ \exists w\ (\eta(S^n(\mathbf{0}), w) \wedge \rho(w, z)))$. These statements logically imply $\exists z < S^m(\mathbf{0})\ \exists w\ (\eta(S^n(\mathbf{0}), w) \wedge \rho(w, z))$. We violate the consistency of T by showing $T \vdash \forall z < S^m(\mathbf{0})\ \forall w\ (\eta(S^n(\mathbf{0}), w) \to \neg\rho(w, z))$. From lemma 2.5 it is enough to fix $k < m$ and show that $T \vdash \forall w\ (\eta(S^n(\mathbf{0}), w) \to \neg\rho(w, S^k(\mathbf{0})))$. By strong representability of η, it is enough to show that $T \vdash \neg\rho(S^{n'}(\mathbf{0}), S^k(\mathbf{0}))$, where n' is the code for $\neg\sigma_2$. Since T is consistent and $T \vdash \sigma_2$ by assumption, $T \nvdash \neg\sigma_2$, and so $\neg R(n', k)$. By representability, $T \vdash \neg\rho(S^{n'}(\mathbf{0}), S^k(\mathbf{0}))$ and we are done.

Assume next that $T \vdash \neg\sigma_2$. Let again $n' = \#\neg\sigma_2$, and let now m code a deduction from T of $\neg\sigma_2$. So, $T \vdash \rho(S^{n'}(\mathbf{0}), S^m(\mathbf{0}))$. Since $T \vdash \neg\sigma_2$ we also have $T \vdash \exists y\ (\rho(S^n(\mathbf{0}), y) \wedge \forall z < y\ \forall w\ (\eta(S^n(\mathbf{0}), w) \to \neg\rho(w, z)))$. To violate the consistency of T it is enough to show that $T' = T \cup \{\alpha\}$ is inconsistent, where $\alpha(y) = (\rho(S^n(\mathbf{0}), y) \wedge \forall z < y\ \forall w\ (\eta(S^n(\mathbf{0}), w) \to \neg\rho(w, z)))$. Since $T \vdash \eta(S^n(\mathbf{0}), S^{n'}(\mathbf{0}))$, it follows that $T' \vdash y \leqslant S^m(\mathbf{0})$ (we use here the order axiom of F which gives $y \leqslant S^m(\mathbf{0})$ or $y > S^m(\mathbf{0})$). From lemma 2.5 it is enough to show that each $k \leqslant S^m(\mathbf{0})$ that $T'' = T \cup \{(\rho(S^n(\mathbf{0}), S^k(\mathbf{0})) \wedge \forall z < S^k(\mathbf{0})\ \forall w\ (\eta(S^n(\mathbf{0}), w) \to \neg\rho(w, z)))\}$ is inconsistent. This is clearly the case, however, since for all such k we have $T \vdash \neg\rho(S^n(\mathbf{0}), S^k(\mathbf{0}))$ since by consistency $R(n, k)$ holds (recall we are assuming $T \vdash \neg\sigma_2$). □

Note that the sentences σ_1, σ_2 of the Gödel theorems are Π_1 sentences in the language of number theory [For σ_2 we must replace the $\exists w$ quantifier by a bounded quantifier. This can easily be done as there is a simple primitive recursive bound for the function g, in the notation just before Theorem 3.6].

Thus, incompleteness arises for sentences having only one unbounded number quantifier.

The incompleteness theorems as we stated them apply to theories in the language of number theory, however it is not difficult to see that they consequently apply to theories in which we can "interpret" the theory F. To make this precise, let $\mathcal{L}$ denote the language of number theory, and $\mathcal{L}'$ a first-order language (e.g., the language of set theory). Suppose we have formulas $\alpha_{\mathbb{N}}$, α_+, $\alpha_\cdot$, α_E, $\alpha_<$, α_S, $\alpha_{\mathbf{0}}$ of $\mathcal{L}'$. $\alpha_{\mathbb{N}}$ is intending to define a "copy" of $\mathbb{N}$, and the other formulas, α_+ for example, are intending to define the corresponding function, relation, or constant symbol on this copy. Let T' be a theory (set of sentences) in $\mathcal{L}'$, for example T' might be the axioms of ZFC. Suppose T' proves that $\exists x\ \alpha_{\mathbb{N}}(x)$ (i.e., the copy of $\mathbb{N}$ is non-empty) and also for each of the axioms ψ of F, $T' \vdash \psi'$ where ψ' is the interpretation of ψ into $\mathcal{L}'$ using the α formula in a natural way. For example, an atomic formula of the form $x + (y \cdot z) \approx w$ is replaced by $\exists z_1 \exists z_2\ \ (\alpha_{\mathbb{N}}(z_1) \wedge \alpha_{\mathbb{N}}(z_2) \wedge \alpha_\cdot(y, z, z_1) \wedge \alpha_+(x, z_1, z_2) \wedge z_2 \approx w)$. In this way, each formula ψ of number theory is replaced by a formula ψ' of $\mathcal{L}'$ such that if $\mathrm{F} \vdash \psi$ then $T' \vdash \psi'$. Of course, T' may prove more about its copy of $\mathbb{N}$ than does F, for example, if $\mathcal{L}'$ is the language of set theory and $\alpha_{\mathbb{N}} =$"$x \in \omega$," (and the other α are defined in the usual way these functions etc. are defined in set theory), then ZFC proves much more about $\mathbb{N}$ than F does, in particular ZFC proves that all of the Peano axioms hold in $\mathbb{N}$.

At any rate, if T' proves all of the ψ' for $\psi \in$ F, then all of the proofs of the incompleteness results given above for $\mathcal{L}$ may be carried over immediately for theories extending T'. Since F is finite, it follows that there is a finite T' which suffices to prove all of the ψ'.

For example, let ZFC$'$ denote the finite subset of ZFC which suffices to prove all of the ψ' for $\psi \in$ F. We then have:

Theorem 3.7. *Let T be a recursive, consistent theory in the language of set theory which extends the finite fragment ZFC$'$. Then T is incomplete. Moreover, there is a Π_1 sentence $\sigma_2 = \sigma_2(T)$ such that $T \nvdash \sigma_2$ and $T \nvdash \neg\sigma_2$.*

Proof. Define $R(a, b)$ and $\rho(x, y)$ as in theorem 3.6. Let $\rho'(x, y)$ be the interpretation of ρ into the language of set theory. Thus, if $R(a, b)$ then $\mathrm{F} \vdash \rho(S^a(\mathbf{0}), S^b(\mathbf{0}))$ and so $T \vdash \rho'_{a,b}$ and likewise for $\neg R(a, b)$, where $\rho'_{a,b}$ denotes the interpretation of

$\rho(S^a(\mathbf{0}), S^b(\mathbf{0}))$. The proof is now essentially identical to theorem 3.6 using ρ' in place of ρ. □

Lastly, we discuss the second Gödel incompleteness theorem. We now consider theories T which may be in the language of number theory, or set theory, etc., for which we have an interpretation of $\mathbb{N}$ as above. Let $R(b)$ iff b codes a deduction from T of a logical contradiction, say $\exists x\ (x \not\approx x)$. Let $\rho(x)$ represent R in F, and let CON_T be the sentence $\neg\exists x\ \rho$. If T is in set theory, say, then we let CON_T be the interpretation of this sentence into the language of set theory. The second version of the incompleteness theorem say that if T is recursive, consistent, and sufficiently strong (but we need more that T contains F now), then $T \nvdash \mathrm{CON}_T$. It is enough to have T contain PA (even a smaller fragment of it, say Π_1-induction), but we state the result now for theories extending ZFC.

Theorem 3.8. *Let T be a recursive, consistent theory in the language of set theory extending ZFC. Then $T \nvdash CON_T$.*

Proof. Let σ_1 be the sentence from the first version of the Gödel incompleteness theorem, so $T \nvdash \sigma_1$ (recall this direction only used the consistency of T). The proof of this (theorem 3.5) was presented in the metatheory. That is, in the metatheory we showed that if T is consistent, then $T \nvdash \sigma_1$. Closer examination of the proof reveals that the only properties of the integers used in the proof are theorems of PA. Certainly, however, they are all theorems of ZFC. Thus, this argument in the metatheory, when formalized, becomes the statement that $\mathrm{ZFC} \vdash (\mathrm{CON}_T \to \phi)$, where ϕ is the formalization of the statement "there does not exist a proof of σ_1 from T." However, this formalization is just the statement $\tau(S^{\#\sigma_1}(\mathbf{0}))$ (using the notation of theorem 3.5), and this is T provably equivalent to σ_1 (more precisely, the interpretations of these statements into the language of set theory). Thus, $\mathrm{ZFC} \vdash (\mathrm{CON}_T \to \sigma_1)$. It follows that $\mathrm{ZFC} \nvdash \mathrm{CON}_T$ from theorem 3.5. □

4. Hilbert's 10th Problem

We let $\mathbb{Z}_+$ denote the set of positive integers. Our goal in this section is to show that there is a 4th degree polynomial

$$p(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$$

such that the statement "$\exists a_1, \ldots a_k \in \mathbb{Z}_+\ p(a_1, \ldots, a_k) = 0$" is independent of ZFC. This displays a conection between logic, set theory and number theory, and has deep implications for Diophantine analysis.

By "polynomial" we will henceforth mean an element $p \in \mathbb{Z}[x_1, \ldots, x_k]$ for some $k \geqslant 0$, that is, our polynomials have integer coefficients (i.e., they may be negative).

Definition 4.1. A relation $R \subseteq \mathbb{Z}_+^k$ is *Diophantine* if there is a polynomial

$$p(x_1, \ldots, x_k, y_1, \ldots, y_\ell)$$

such that for all $a_1, \ldots, a_k \in \mathbb{Z}_+^k$ we have

$$(a_1, \ldots, a_k) \in R \leftrightarrow \exists b_1, \ldots, b_\ell \in \mathbb{Z}_+\ p(a_1, \ldots, a_k, b_1, \ldots, b_\ell) = 0.$$

That is, $\vec{a} \in R$ iff $p(\vec{a}, \vec{y}) \in \mathbb{Z}[y_1, \ldots, y_\ell]$ has a positive integer root.

Since the formula $p(x_1, \ldots, x_k) = 0$ is clearly Δ_0 (moving the negative terms to the other side of the equation this becomes an atomic formula), it is immediate that every Diphantine set is Σ_1^0. Our main theorem will be that the converse holds.

Specifically, our main theorem is the following.

Theorem 4.2. *Every Σ_1^0 relation $S \subseteq (\mathbb{Z}_+)^n$ is Diophantine.*

Moreover, the proof will be constructive in the sense that it will give us a procedure for transforming a Σ_1 formula φ in the language of number theory into a polynomial p_φ such that the Σ_1^0 set defined by φ has a diophantine representation given by p_φ. This will allow us to make a connection with the Gödel incompleteness theorem and produce a specific polynomial such that statement that is has a root is independent of ZFC. By an algebra trick (credited to Skolem) we are able to reduce any diophantine problem down to a 4th degree one, which will give the final theorem.

Theorem 4.2 was proved in 1970 by Matiyasevic, and built upon earlier work of sereral people including Davis, Putnam, and J. Robinson. Our presentation will largely follow the 1973 paper of Davis [**?**].

We first note, according to the following lemma, that the requirement that the roots of the polynomial be positive, instead of just arbitrary integers, is for convenience and doesn't change the diophantine sets.

Lemma 4.3. *A relation $R \subseteq \mathbb{Z}_+^k$ is Diophantine according to Definition 4.1 iff there is a polynomial p' such that for all $\vec{a} \in \mathbb{Z}_+^k$ we have $\vec{a} \in R \leftrightarrow \exists \vec{b} \in \mathbb{Z}^\ell \ p'(\vec{a}, \vec{b}) = 0$.*

Proof. Suppose first that $R \subseteq \mathbb{Z}_+^k$ is Diophantine according to Definition 4.1, that is, for some ℓ and some $p \in \mathbb{Z}[x_1, \dots, x_k, y_1, \dots, y_\ell]$ we have $\vec{a} \in R$ iff $\exists \vec{b} \in \mathbb{Z}_+ \ p(\vec{a}, \vec{b}) = 0$. for each variable y_j we introduce 4 variables $w_1^j, \dots, w_4^j$ and let

$$p'(x_1, \dots, x_k, y_1, \dots, y_\ell, \dots, w_1^j, w_2^j, w_3^j, w_4^j, \dots)$$

be the $k + \ell + 4\ell$-ary polynomial given by

$$\begin{aligned} p' = &(1 + (w_1^1)^2 + (w_2^1)^2 + (w_3^1)^2 + (w_4^1)^2 - y_1)^2 + \cdots \\ &+ (1 + (w_1^\ell)^2 + (w_2^\ell)^2 + (w_3^\ell)^2 + (w_4^\ell)^2 - y_\ell)^2 + (p(x_1, \dots, x_k, y_1, \dots, y_\ell))^2 \end{aligned}$$

Using Lagrange's theorem that an integer n is $\geqslant 0$ iff it can be written as the sum of 4 squares of integers, we see that for any $\vec{a}$ that $p(\vec{a}, \vec{y})$ has a root in $\mathbb{Z}_+^\ell$ iff $p'(\vec{a}, \vec{y}, \vec{w})$ has a root in $\mathbb{Z}^{5\ell}$.

Suppose next that $R \subseteq \mathbb{Z}_+^k$ is represented in the $\mathbb{Z}$-sense, that is, there is a polynomial $p'(x_1, \dots, x_k, y_1, \dots, y_\ell)$ such that for all $\vec{a} \in \mathbb{Z}_+^k$ we have $\vec{a} \in R$ iff $\exists \vec{b} \in \mathbb{Z}^\ell \ p'(\vec{a}, \vec{b}) = 0$. For each variable y_j we introduce two variables z_j, w_j and let $p(x_1 \dots, x_k, z_1, \dots, z_\ell, w_1, \dots, w_\ell)$ be the polynomial

$$p = (z_1 - w_1)^2 + \cdots + (z_\ell - w_\ell)^2 + (p'(x_1, \dots, x_k, z_1 - w_1, \dots, z_\ell - w_\ell))^2.$$

Since every integer is a difference of two positive integers, $p(\vec{a}, \vec{y}, \vec{z})$ has a root in the positive integers iff $p'(\vec{a}, \vec{y})$ has a root in the integers. □

We now begin the process of showing Σ_1^0 relaions are Diophantine.

Lemma 4.4. *The class of Diophantine relations is closed under $\cap$, $\cup$, $\exists^{\mathbb{Z}_+}$.*

Proof. Suppose $R \subseteq \mathbb{Z}_+^r$, $S \subseteq \mathbb{Z}_+^s$ are Diophantine and represented by the polynomials $p(x_1, \dots, x_r, y_1, \dots, y_\ell)$, $q(x_1, \dots, x_s, z_1, \dots, z_m)$. Then $R \cap S$ is represented by the polynomial $t = p^2 + q^2$ and $R \cup S$ is represented by $u = p \cdot q$. The relation $T \subseteq \mathbb{Z}_+^{r-1}$ given by $T(x_1, \dots, \hat{x_j}, \dots x_r) \leftrightarrow \exists x_j \ R(x_1, \dots, x_r)$ is represented by

$$p'(x_1, \dots, \hat{x_j}, \dots, x_r, z_1, y_1, \dots, y_\ell) = p(x_1, \dots, z_1, \dots, x_r, y_1, \dots, y_\ell),$$

where the variable z_1 is substituted for x_j in p.

□

We can rephrase Lemma 4.4 as saying that the collection of formulas φ in the language of number theory which define (over $\mathbb{Z}_+$) Diophantine relations is closed under $\wedge$, $\vee$ and $\exists x_j$.

Lemma 4.5. *For any polynomials $p(\vec{x})$, $q(\vec{x})$, the relations defined by the formulas $p(\vec{x}) \approx q(\vec{x})$ and $p(\vec{x}) < q(\vec{x})$ are Diophantine.*

Proof. The relation $R \subseteq \mathbb{Z}_+^k$ defined by $p(\vec{x}) \approx q(\vec{x})$ is represented by the polynomial $p(\vec{x}) - q(\vec{x})$. The relation S defined by $p(\vec{x}) < q(\vec{x})$ is represented by the formula $q(\vec{x}) - p(\vec{x}) - y$. □

From Lemmas 4.4 and 4.5 it follows that the relations defined by the formulas $p(\vec{x}) \leqslant q(\vec{x})$, $p(\vec{x}) \not\approx q(\vec{x})$ are also Diophantine. It further follows that the collection of relations on $\mathbb{Z}_+$ defined over $\mathbb{N}$ by quantifier-free formulas in the language $\mathcal{L}' = (+, \cdot, <, S, \mathbf{0})$ (note: we have omitted exponentiation) are Diophantine. That is, if $\varphi(x_1, \ldots, x_k)$ is a quantifier-free formula in $\mathcal{L}'$ the set

$$R = \{(a_1, \ldots, a_k) \in \mathbb{Z}_+^k : \varphi^{\mathbb{N}}(S^{a_1}(\mathbf{0}), \ldots, S^{a_k}(\mathbf{0}))\}$$

is Diophantine.

Definition 4.6. We say a function $f : \mathbb{Z}_+^k \to \mathbb{Z}_+$ is Diophantine iff its graph $G_f \subseteq \mathbb{Z}_+^{k+1}$ is Diophantine. More generally, we say a function $f : \mathbb{Z}_+^k \to \mathbb{Z}$ is Diophantine if $G_f \cap \mathbb{Z}_+^{k+1}$ is Diophantine.

Lemma 4.7. *The collection of Diophantine relations is closed under substitution by Diophantine functions.*

Proof. Let $R \subseteq \mathbb{Z}_+^k$ be Diophantine and $f_1(z_1, \ldots, z_\ell), \ldots, f_k(z_1, \ldots, z_\ell)$ are Diophantine functions, where for notational convenience we have assumed all the f_j have the same arity and use the same variables (the general case is similar). Let $S(z_1, \ldots, z_\ell)$ iff $R(f_1(\vec{z}), \ldots, f_k(\vec{z}))$. Say $f, \ldots, f_k$ are represented by $p_1, \ldots, p_k$. Then S is defined by the formula

$$\varphi(z_1, \ldots, z_\ell) = \exists w_1, \ldots w_k \, [(f_1(\vec{z}) = w_1) \wedge \cdots \wedge (f_k(\vec{z}) = w_k) \wedge R(w_1, \ldots, w_k)]$$

From Definition 4.6 and Lemma 4.4 it follows that S is Diophantine. □

It is immediate that all polynomials are Diophantine functions.

To complete the proof that every Σ_1^0 relation is Diophantine it suffices to show two things: (1) The exponentiation finction $nEm = n^m$ is Diophantine, and (2) The class of formulas defining Diophantine relations is closed under bounded existential and universal quantification.

The bounded existential quantification case follows from the above lemmas as $\varphi(x_1, \ldots, x_k) = \exists y \leqslant x_j \, \psi(x_1, \ldots, x_k, y)$ is equivalent to $\exists y \, [(y \leqslant x_j) \wedge \psi(x_1, \ldots, x_k, y)]$, and the result follows by Lemma 4.4.

The exponentiation and bounded universal quantification cases, however, require much more work. The first main step is to reduce bounded universal quantification down to showing some specific functions are Diophantine, an argument to Davis and Putnam. This uses the Chinese remainder theorem (CRT), and is similar to arguments used by Gödel in his pairing functions.

Definition 4.8. We let $f_1(n, m) = \binom{n}{m}$, $f_2(n) = n!$, and $f_3(a, b, n) = \prod_{i=1}^{n}(a + ib)$.

The following lemma reduces the problem of showing Σ_1^0 sets are Diophantine to showing the specific function of Definition 4.8 are Diophantine.

Lemma 4.9. *Assume the functions of Definition 4.8 are Diophantine. Then the collection of Diophantine relations is closed under bounded universal quantification.*

Proof. Let $R(y, x_1, \ldots, x_n) \leftrightarrow \forall k \leqslant y\ S(y, k, x_1, \ldots, x_n)$ where S is Diophantine. So, for some polynomial P we have:

(1)
$$R(y, x_1, \ldots, x_n) \leftrightarrow \forall k \leqslant y\ S(y, k, x_1, \ldots, x_n)$$

(2)
$$\leftrightarrow \forall k \leqslant y\ \exists y_1, \ldots, y_m\ [P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$

(3)
$$\leftrightarrow \exists u\ \forall k \leqslant y\ \exists y_1, \ldots, y_m \leqslant u\ [P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$

We first get a polynomial $b(y, u, x_1, \ldots, x_n)$ bounding $|P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)|$ whenever $k \leqslant y$ and $y_1, \ldots, y_m \leqslant u$. Namely, if $P = \sum t$ is sum of monomials of the form $t = cy^a k^b x_1^{r_1} \cdots x_n^{r_n} y_1^{s_1} \cdots y_m^{s_m}$, then let $b = y+u+\sum |c| y^{a+b} u^{s_1+\cdots+s_m} x_1^{r_1} \cdots x_n^{r_n}$. Note that $b(y, u, \vec{x}) > y, b(y, u, \vec{x}) > u$ as well.

Suppose first that for some y, $x_1, \ldots, x_n$ and u that

$$\forall k \leqslant y\ \exists y_1, \ldots, y_m \leqslant u\ P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

For each $k \leqslant y$, let $y_1^{(k)}, \ldots, y_m^{(k)} \leqslant u$ be such that

$$P(y, k, \vec{x}, y_1^{(k)}, \ldots, y_m^{(k)}) = 0.$$

Let $t = b(y, u, \vec{x})!$. Consider the y numbers $(1 + t)$, $(1 + 2t), \ldots, (1 + yt)$. These are pairwise relatively prime since any prime divisor of $(1+it)$ and $(1+jt)$ would divide $(j-i)t$ where $(j-i) \leqslant y \leqslant b(y, u, \vec{x})$ and so would divide t, and thus divide 1, a contradiction. By the CRT, let $a_1, \ldots a_m$ be such that $a_i \equiv y_i^{(k)} \mod (1 + kt)$ for each $i = 1, \ldots, m$, and each $k = 1, \ldots, y$. Note that if we define c by $\prod_{k=1}^{y}(1+kt) = 1+ct$, then $c \equiv k \mod (1+kt)$ for all $k = 1, \ldots, y$. This is because $(1+ct) \equiv 0 \equiv (1+kt) \mod (1 + kt)$, and so $ct \equiv kt \mod (1 + kt)$. Since $(t, 1 + kt) = 1$, this gives $c \equiv k \mod (1 + kt)$. We thus have $P(y, c, \vec{x}, a_1, \ldots, a_m) \equiv P(y, k, \vec{x}, y_1^{(k)}, \ldots, y_m^{(k)}) = 0 \mod (1+kt)$ for each $k = 1, \ldots, y$, and thus $P(y, c, \vec{x}, a_1, \ldots, a_m) \equiv 0 \mod (1+ct)$.

Also, for each a_i and each $k = 1, \ldots, y$ we have $a_i \equiv y_i^{(k)} \leqslant u \mod (1 + kt)$ and thus $\prod_{j=1}^{u}(a_i - j) \equiv 0 \mod (1+kt)$. Thus, $\prod_{j=1}^{u}(a_i - j) \equiv 0 \mod (1+ct)$. Thus, we have shown one direction of the following claim.

Claim. For any $y, u, \vec{x}$ we have

$$\forall k \leqslant y\ \exists y_1, \ldots, y_m \leqslant u\ [P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$
$$\leftrightarrow \exists c, t, a_1, \ldots, a_m [t = b(y, u, \vec{x})! \wedge 1 + ct = \prod_{k=1}^{y}(1 + kt) \wedge (1 + ct) | \prod_{j=1}^{u}(a_1 - j)$$
$$\wedge \cdots \wedge (1 + ct) | \prod_{j=1}^{u}(a_m - j) \wedge (1 + ct) | P(y, c, \vec{x}, a_1, \ldots, a_m)]$$

For the other direction, fix $y, u, \vec{x}$, and suppose $c, t, a_1, \ldots, a_m$ witness the right-hand side of the above claim. As above, the $(1 + kt)$, for $1 \leqslant k \leqslant y$, are pairwise reatively prime, and $c \equiv k \mod (1+kt)$ for all these k. Since $(1+ct) | \prod_{j=1}^{u}(a_i - j)$ for each $1 \leqslant i \leqslant m$, we have that for each $1 \leqslant k \leqslant y$ and each prime factor

of $1 + kt$ that there is a $j \leqslant u$ such that $a_i \equiv j \mod p$. Since p must be relatively prime to t, and $t = b(y, u, \vec{x})!$, this gives that $p > b(y, u, \vec{x})$. Let $y_i^{(k)}$ denote such a j. Since also $c \equiv k \mod (1 + kt)$, we have $c \equiv k \mod p$. Thus, $P(y, k, \vec{x}, y_1^{(k)}, \ldots, y_m^{(k)}) \equiv 0 \mod p$. But, $P(y, k, \vec{x}, y_1^{(k)}, \ldots, y_m^{(k)}) < b(y, u\vec{x}) < p$, and so $P(y, k, \vec{x}, y_1^{(k)}, \ldots, y_m^{(k)}) = 0$.

From this the lemma follows, since $\prod_{k=1}^{y}(1 + kt) = f_3(1, t, y)$, and for $a > u + 1$ that $\prod_{j=1}^{u}(a - j) = f_3(a - u - 1, 1, u)$. □

Our next task is to show that the functions of Definition 4.8 are Diophantine given that the exponential function $(n, m) \mapsto n^m$ is Diophantine. We first show that $f_1(n, m) = \binom{n}{m}$ is Diophantine, from which the other two will follow.

Lemma 4.10. *Assume the exponential function is Diophantine. Then the function $f_1(n, m) = \binom{n}{m}$ is Diophantine.*

Proof. We show that for all $m \leqslant n$ and all $u > 2^n$ that

$$\binom{n}{m} \equiv \lfloor \frac{(u+1)^n}{u^m} \rfloor \mod u$$

Fix such $m \leqslant n$ and $u > 2^n$. Then

$$\frac{(u+1)^n}{u^m} = \binom{n}{m} + u\Big(\sum_{i=m+1}^{n} \binom{n}{i} u^{i-m-1}\Big) + \sum_{i=0}^{m-1} \binom{n}{i} u^{i-m}.$$

It suffices to show that $\sum_{i=0}^{m-1} \binom{n}{i} u^{i-m} < 1$. Since $\sum_{i=0}^{n} \binom{n}{i} = (1+1)^n = 2^n$, we have $\sum_{i=0}^{m-1} \binom{n}{i} u^{i-m} < \frac{1}{u} \sum_{i=0}^{m-1} \binom{n}{i} \leqslant \frac{2^n}{u} < 1$.

This shows that f_1 is Diophantine since we now have

$$k = \binom{n}{m} \leftrightarrow \exists u, v, w \, [v = 2^n \wedge u > v \wedge w = \lfloor \frac{(u+1)^n}{u^m} \rfloor \wedge (k < u) \wedge k \equiv w \mod u]$$

Note that $w = \lfloor \frac{(u+1)^n}{u^m} \rfloor$ iff $wu^m \leqslant (u+1)^n < (w+1)u^m$. Since the function $n \mapsto 2^n$ is Diophantine by assumption, this show that f_1 is also. □

Lemma 4.11. *Assume the exponential function is Diophantine. Then the function $f_2(n) = n!$ is Diophantine.*

Proof. We claim that if $u > (2n)^{n+1}$, then $n! = \lfloor \frac{u^n}{\binom{u}{n}} \rfloor$. To see this, note that

$$\frac{u^n}{\binom{u}{n}} = u^n \frac{n!}{u(u-1)\cdots(u-n+1)} = n! \, [(1 - \frac{1}{u})(1 - \frac{2}{u}) \cdots (1 - \frac{n-1}{u})]^{-1} \geqslant n!.$$

On the other hand,

$$n! \, [(1 - \frac{1}{u})(1 - \frac{2}{u}) \cdots (1 - \frac{n-1}{u})]^{-1} \leqslant n! \, [(1 - \frac{n}{u})^{-1}]^n \leqslant n! \, (1 + \frac{2n}{u})^n$$
$$= n! \, [1 + \sum_{i=1}^{n} \binom{n}{i} \left(\frac{2n}{u}\right)^i]^n \leqslant n! \, [1 + \frac{2n}{u} \sum_{i=1}^{n} \binom{n}{i}] \leqslant n! + \frac{2n}{u} 2^n n!$$
$$\leqslant n! + \frac{2n}{u} 2^n n^n < n! + 1.$$

This shows the claim, and from this the lemma follows by a straightforward computation as at the end of Lemma 4.10, using now that Lemma 4.10 gives that f_1 is Dipohantine. □

Lemma 4.12. *Assume the exponential function is Diophantine. Then the function* $f_3(a,b,n) = \prod_{i=1}^{n}(a+ib)$ *is Diophantine.*

Proof. Let $M = b(a+nb)^n+1$, so $M > f_3(a,b,n)$ and $(b,M) = 1$. Since $(b,M) = 1$, there is a $q < M$ such that $qb \equiv a \mod M$. Then,

$$\begin{aligned} f_3(a,b,n) = \prod_{i=1}^{n}(a+ib) &\equiv \prod_{i=1}^{n}(qb+ib) \mod M \\ &= b^n(q+1)(q+2)\cdots(q+n) = b^n n! \binom{q+n}{q} \mod M \end{aligned}$$

So, $f_3(a,b,n)$ is the unique integer less than M which is congruent to $b^n n!\binom{q+n}{q}$ mod M.

This again easily shows that f_3 is Diophantine, namely,

$$\begin{aligned} k = f_3(a,b,n) \leftrightarrow \exists u,v,w,M,q\ [&M = b(a+nb)^n + 1 \wedge M|(qb-a) \wedge u = n! \\ &\wedge v = \binom{q+n}{n} \wedge w = b^n \wedge (k < M) \wedge M|(k - wuv)]. \end{aligned}$$

□

To summarize, from Lemmas 4.9, 4.10, 4.11, and 4.12 we have shown the following theorem.

Theorem 4.13. *Assume the exponential function is Diophantine. Then every* Σ_1^0 *set* $S \subseteq (\mathbb{Z}_+)^n$ *is Diophantine.*

5. The exponential function

To complete the proof of Theorem 4.2 it suffuces to show the following theorem.

Theorem 5.1. *The exponential function* $nEm = n^m$ *on* $\mathbb{Z}_+^2$ *is Diophantine.*

The proof of theorem 5.1 is difficult and will occupy the rest of this section. This theorem was proved by Matiyasevic in 1970, and gave the solution to Hilbert's 10th problem. To show the exponential function is Diophantine, as we will see, it suffices to show that something with exponential-like growth is Diophantine. Matiyasevic originally used the Fibonacci sequence, but here we will use the set of solutions to Pell's equations which somewhat simplifies the arguments, though the main ideas are the same.

Readers may note that some of the arguments we give concerning the solutions to Pell's equations are actually special instances of much more general results in algebraic number theory. However, we give elementary arguments here to keep the arguments self-contained.

Definition 5.2. For a positive integer d, the corresponding Pell equation is

$$x^2 - dy^2 = 1$$

where we regard $x, y \in \mathbb{N}$.

Of course, it make little difference whether we regard x, y and as ranging over $\mathbb{N}$ or $\mathbb{Z}$, as the solutions over $\mathbb{Z}$ are just those obtained from the solutions over $\mathbb{N}$ by possibly changing the signs of x and/or y.

Note that one solution is just $(x, y) = (1, 0)$. If we let $d = a^2 - 1$ for some integer $a > 1$, then we also have the solution $(x, y) = (a, 1)$. We will henceforth take d of this form, that is, $d = a^2 - 1$.

We first characterize the set of solutions to Pell's equations. Note that if we consider $\mathbb{Q}(\sqrt{d})$, then (x, y) is a solution to Pell's equation iff the element $x + y\sqrt{d}$ has norm 1, where $N(x+y\sqrt{d}) = (x+\sqrt{d})(x-\sqrt{d}) = x^2 - dy^2$. It is a general fact, true in any number field, that the norm is a multiplicitive function (the norm of z, in general, is the product $\pi_1(z)\pi_2(z)\cdots\pi_n(z)$ where the π_i are the automorphisms of the field over $\mathbb{Q}$). In our case, we see can see by a direct elementary computation that this is the case, namely:

$$(x^2 - dy^2)(u^2 - dv^2) = (xu + dyv)^2 - d(xv + yu)^2.$$

Thus, if (x, y) and (u, v) are solutions to Pell's equation, then so is $(xu+dyv, xv+yu)$. Replacing y by $-y$ we see that $(xu - dyv, xv - yu)$ is also a solution.

Since $a + \sqrt{d}$ is a solution, it follows that if we let $(a + \sqrt{d})^n = x_n + y_n\sqrt{d}$, then (x_n, y_n) is a solution. We show next that these are all of the non-negative solutions to the equation.

Let (x, y) be a solution with $x, y \geqslant 0$. Clearly $x + y\sqrt{d} \geqslant 1$. Let n be such that $(a + \sqrt{d})^n \leqslant x + y\sqrt{d} < (a + \sqrt{d})^{n+1}$. Multiplying through by $(a - \sqrt{d})^n$ we get $1 \leqslant x' + y'\sqrt{d} < a + \sqrt{d}$ where (x', y') is a solution. Taking reciprocals we get $1 \geqslant x' - y'\sqrt{d} > a - \sqrt{d}$, or $-1 \leqslant -x' + y'\sqrt{d} < -a + \sqrt{d}$. Adding these equations gives $0 \leqslant 2y'\sqrt{d} < 2\sqrt{d}$ or $0 \leqslant y' < 1$, so $y' = 0$. So, $x' = 1$, and $x' + y'\sqrt{d} = 1$ and so $x + y\sqrt{d} = (a + \sqrt{d})^n$.

We summarize this analysis into the following lemma.

Lemma 5.3. *Let $a > 0$ and $d = a^2 - 1$. The non-negative (i.e., $x, y \geqslant 0$) solutions to Pell's equation $x^2 - dy^2 = 1$ are exactly the pairs of the form (x_n, y_n) where $x_n + y_n\sqrt{d} = (a + \sqrt{d})^n$ for some $n \geqslant 0$. The general solutions are of the form $(\pm x_n, \pm y_n)$. Furthermore*

$$x_{m\pm n} = x_m x_n \pm d y_m y_n \tag{4}$$

$$y_{m\pm n} = \pm x_m y_n + y_m x_n \tag{5}$$

In, particular, taking $n = 1$ and $n = -1$, we have the following forward and backward recurrence formulas for the x_m, y_m:

$$x_{m+1} = a x_m + d y_m, \qquad y_{m+1} = x_m + a y_m. \tag{6}$$

$$x_{m-1} = a x_m - d y_m, \qquad y_{m-1} = -x_m + a y_m. \tag{7}$$

We also have the following second-order recurrence equations for the x_m and y_m separately:

$$x_{m+1} = 2a x_m - x_{m-1} \tag{8}$$

$$y_{m+1} = 2a y_m - y_{m-1} \tag{9}$$

Proof. Equation 4 follows from

$$x_{m+n} + y_{m+n}\sqrt{d} = (a+\sqrt{d})^{m+n} = (a+\sqrt{d})^m (a+\sqrt{d})^n = (x_m + \sqrt{d}y_m)(x_n + \sqrt{d}y_n).$$

Equation 5 similarly follows from $(a+\sqrt{d})^{m-n}(a+\sqrt{d})^n = (a+\sqrt{d})^m$, which gives $x_{m-n}+y_{m-n}\sqrt{d} = (a+\sqrt{d})^{m-n} = (a+\sqrt{d})^m(a-\sqrt{d})^n = (x_m+\sqrt{d}y_m)(x_n-\sqrt{d}y_n)$.

To see equations 8, 9, note that these holds for $m = 1$, as the first three solutions are $(1,0)$, $(a,1)$, and $(a^2+d, 2a) = (2a^2-1, 2a)$, which satisfy these equations, and inductively we then have:

$$\begin{aligned} x_{m+2} - 2ax_{m+1} + x_m &= (ax_{m+1} + dy_{m+1}) - 2a(ax_m + dy_m) + (ax_{m-1} + dy_{m-1}) \\ &= a(x_{m+1} - 2ax_m + x_{m-1}) + d(y_{m+1} - 2ay_m + y_{m-1}) \\ &= 0 \end{aligned}$$

with similar equations holding for the y_m (note, as the above equations show, that once a linear recurrence relations such as 8, 9 hold for the first three terms, they must automatically hold for all the terms in view of equations 6). □

Note that we may phrase the first-order recurrence relations for the x_m, y_m in matrix form as

$$\begin{pmatrix} x_{m+1} \\ y_{m+1} \end{pmatrix} = \begin{pmatrix} a & d \\ 1 & a \end{pmatrix} \begin{pmatrix} x_m \\ y_m \end{pmatrix}$$

An immediate consequence of the first-order recurrence relations is the following.

Lemma 5.4. *For all m we have:*

(1) $x_m \geqslant a^m$.
(2) $y_m \geqslant m$, *and for* $m \geqslant 1$, $y_m \geqslant a^{m-1}$.

Proof. These follow immediately by induction from the first-order recurrence relations. □

An immediate consequence of the second-order recurrence relations is the following.

Lemma 5.5. *For all m we have:*

(1) $y_m \equiv m \mod (a-1)$.
(2) $y_m \equiv m \mod 2$.

Proof. Proceding inductively, and noting that $a \equiv 1 \mod (a-1)$, we have $y_m = 2ay_{m-1} - y_{m-2} \equiv 2(m-1) - (m-2) = m \mod (a-1)$. Likese, the recurrence realtion shows $y_m \equiv y_{m-2} \mod 2$, and the second result follows. □

We now investigate the number theoretic properties of the solutions. We will see that the x_n and the y_n terms each satisfy certain delicate properties.

Lemma 5.6. *The non-negative solutions (x_n, y_n) of Pell's equation satisfy the following.*

(1) *For all n, $(x_n, y_n) = 1$.*
(2) *For all m, n we have $y_m \mid y_n$ iff $m \mid n$.*

Proof. If $p \mid x_n$, $p \mid y_n$, then $p \mid (x_n^2 - dy_n^2) = 1$, a contradiction, so $(x_n, y_n) = 1$. This result also follows from the backward recurrence equation 7, since if $p \mid x_n$, $p \mid y_n$, then equation 7 shows that $p \mid x_{n-1}$ and $p \mid y_{n-1}$, so we inductively conclude that $p \mid y_1 = 1$, a contradiction.

Fix m, and we show by induction on k that $y_m \mid y_{km}$. The case $k = 1$ is trivial, and we have $y_{(k+1)m} = x_{km}y_m + x_m y_{km}$ so since $y_m \mid y_{km}$ by induction we see that $y_m \mid y_{(k+1)m}$.

Finally, suppose $m \nmid n$, say $n = km + r$ where $0 < r < m$. Then $y_n = x_{km}y_r + x_r y_{km}$. If $y_m \mid y_n$, then since $y_m \mid y_{km}$ we see that $y_m \mid (x_{km}y_r)$. Since $(x_{km}, y_{km}) = 1$, and so $(x_{km}, y_m) = 1$, we have that $y_m \mid y_r$. This a contradiction as $y_m > y_r$ (clearly from equation 6, the x_n and y_n are strictly increasing sequences). □

Lemma 5.6 says that $y_m \mid y_t$ iff $m \mid t$. The next lemma tells us when $y_m^2 \mid y_t$.

Lemma 5.7. *For all m, t we have that $y_m^2 \mid y_t$ iff $my_m \mid t$.*

Proof. We have

$$(x_{mk} + y_{mk}\sqrt{d}) = (a + \sqrt{d})^{mk} = (x_m + y_m\sqrt{d})^k = \sum_{i=0}^{k} \binom{k}{i} x_m^{k-i} y_m^i (\sqrt{d})^i$$

So,

$$y_{mk} = \sum_{\substack{i=1 \\ i \text{ odd}}}^{k} \binom{k}{i} x_m^{k-1} y_m^i d^{(i-1)/2} \equiv k x_m^{k-1} y_m \mod y_m^3.$$

So, setting $k = y_m$ we have $y_{my_m} \equiv 0 \mod y_m^2$. It follows from Lemma 5.6 that if $my_m \mid t$ then $y_m^2 \mid y_t$.

Suppose next that $y_m^2 \mid y_t$. From Lemma 5.6 we have that $m \mid t$, say $t = mk$. The above equation gives that $y_t = y_{mk} \equiv k x_m^{k-1} y_m \mod y_m^3$. so, $y_m \mid k x_m^{k-1}$. Since $(x_m, y_m) = 1$, we have $y_m \mid k$, so $my_m \mid t$. □

We now establish some properties of the x_m.

Lemma 5.8. $x_{2km \pm j} \equiv (-1)^k x_j \mod x_m$.

Proof. For $k = 1$ we have

$$\begin{aligned} x_{2m \pm j} &= x_m x_{m \pm j} + d y_m y_{m \pm j} \\ &\equiv d y_m (\pm x_m y_j + y_m x_j) \mod x_m \\ &\equiv d y_m^2 x_j \mod x_m \\ &= (x_m^2 - 1) x_j \mod x_m \\ &\equiv -x_j \mod x_m \end{aligned}$$

Proceeding inductively we now have:

$$\begin{aligned} x_{2(k+1)m \pm j} &= x_{2m} x_{2km \pm j} + d y_{2m} y_{2km \pm j} \\ &\equiv (-1) x_0 (-1^k) x_j + d y_{2m} y_{2km \pm j} \mod x_m \\ &= (-1)^{k+1} x_j + d(y_m x_m + x_m y_m) y_{2km \pm j} \\ &\equiv (-1)^{k+1} x_j \mod x_m \end{aligned}$$

□

For given x_m and $i \leqslant m$, we now investigate when $x_j \equiv x_i \mod x_m$. We first show that the representatives $\mod x_m$ of $x_0, \ldots x_{2m}$ are all distinct, except in one rather trivial exceptional case.

Lemma 5.9. *Suppose $i \leqslant j \leqslant 2m$ and $x_i \equiv x_j \mod x_m$ ($m > 0$). Then $i = j$ unless $a = 2$, $m = 1$, $i = 0$, $j = 2$ (in which case $x_0 = 1$, $x_1 = 2$, and $x_2 = 7$).*

Proof. Consider $x_0, \ldots, x_{m-1}$, and note that $x_{m-1} \leqslant \frac{1}{2}x_m$ since $x_m = ax_{m-1} + dy_{m-1}$. Unless $a = 2$ and $y_{m-1} = 0$ (i.e., $m = 1$), we must have strict inequality. Since $x_{m+j} = x_{2m-(m-j)} \equiv -x_{m-j} \mod x_m$, we have that $x_{m+1}, \ldots, x_{2m}$ are equivalent to $-x_{m-1}, \ldots, -x_1 \mod x_m$. If strict inequality holds then then these two sets of values are disjoint, and the result follows. For x_{m-1} to equal $\frac{1}{2}x_m$ we must have that x_m is even, $a = 2$, $m = 1$, and we must have $i = m - 1 = 0$, $j = m + 1 = 2$. □

Lemma 5.10. *Let $i \leqslant m$, and suppose $x_j \equiv x_i \mod x_m$. Then $j \equiv \pm i \mod 4m$ unless $a = 2$, $m = 1$ and $i = 0$.*

Proof. Suppose $x_j \equiv x_i \mod x_m$, where $i \leqslant m$. Let $j' = j \mod 4m$. Then $x_j \equiv x_{j'} \mod x_m$ by Lemma 5.9 and so $x_{j'} \equiv x_i \mod x_m$. If $j' \leqslant 2m$, then by Lemma 5.9 we have $j' = i$ (or else we are in the exceptional case). Otherwise, $j' = 4m - k$ where $k < 2m$. Then $x_{j'} \equiv x_k \mod x_m$ and $x_k \equiv x_i \mod x_m$. From Lemma 5.9 we have $k = i$ (or else the exceptional case) and so $j \equiv j' \equiv -i \mod 4m$. □

The above lemmas give properties of the x_m, y_m for a particular value of a (recall $d = a^2 - 1$). We need also a simple lemma relating the solutions for different values of a.

Lemma 5.11. *If $a \equiv b \mod k$ then $x_m(a) \equiv x_m(b) \mod k$ and $y_m(a) \equiv y_m(b) \mod k$.*

Proof. This is true for $m = 0, 1$ as $x_1(a) = a$, and then follows immediately for $m > 1$ from the second-order recurrence relations. □

Finally, a technical lemma relating $x_n(a)$, $y_n(a)$ and the the exponential function y^n. We will use this the exponential function is Diophantine from the fact (which we will establish first) that the functions $(a, m) \mapsto x_m(a), y_m(a)$ are Diophantine.

Lemma 5.12. $x_n(a) - y_n(a)(a - y) \equiv y^n \mod 2ay - y^2 - 1$.

Proof. $x_0(a) - y_0(a)(a - y) = x_0(a) = 1$, and $x_1(a) - y_1(a)(a - y) = a - (a - y) = y$. Also

$$\begin{aligned} x_{m+1}(a) - y_{m+1}(a)(a - y) &= 2a(x_m(a) - y_m(a)(a - y)) - (x_{m-1}(a) - (a - y)y_{m-1}) \\ &\equiv 2ay^m - y^{m-1} = y^{m-1}(2ay - 1) \\ &\equiv y^{m-1}y^2 = y^{m+1} \mod 2ay - y^2 - 1. \end{aligned}$$

□

Theorem 5.13. *The function $f(a, k) = x_k(a)$ is Diophantine.*

Proof. For fixed a and k, consider three solutions (x, y), (z, w), (u, v) to the Pell's equations:

$$x^2 - (a^2 - 1)y^2 = 1 \tag{10}$$

$$z^2 - (b^2 - 1)w^2 = 1 \tag{11}$$

$$u^2 - (a^2 - 1)v^2 = 1 \tag{12}$$

where we require that $b \equiv 1 \mod 4y$, and $b > 1$ (we will require more on b below). That is, we require

$$b = 1 + 4ky \tag{13}$$

Say $(x, y) = (x_i(a), y_i(a))$, $(z, w) = (x_j(a), y_j(a))$, and $(u, v) = (x_n(a), y_n(a))$.

The idea is to make b a sufficiently large base, require $y_j(b)$ to be congruent to $k \bmod b - 1$, and so $\bmod 4y$, (so $j \equiv k \mod 4y$), and then try to require that j be equal to i as best we can. Specifically, we will require that j be congruent to $i \bmod 4y$ (more or less) so that $i \equiv k \mod 4y$. We will require that $k \leqslant y$ and this will give $i = k$.

So, let us require that $k \leqslant y$:

$$y = k + e - 1 \tag{14}$$

and $w \equiv k \mod 4y$:

$$w = k + 4(d - 1)y \tag{15}$$

Since $w \equiv j \mod b - 1$ (and so $\mod 4y$), this says that $j \equiv k \mod 4y$. Let us also suppose that $b \equiv a \mod x_n(a)$, that is,

$$b = a + qu \tag{16}$$

This gives $x_j(b) \equiv x_j(a) \mod x_n(a)$. Let us then add the requirement that $x_j(b) \equiv x_i(a) \mod x_n(a)$, that is:

$$z = x + cu \tag{17}$$

This then gives that $x_j(a) \equiv x_i(a) \mod x_n(a)$. We will have $i \leqslant n$ shortly, and so by Lemma 5.10 we have $j \equiv \pm i \mod 4n$ (note that $k \leqslant y$ so $i \neq 0$, so we are not in the exceptional case of Lemma 5.10). We add the requirement that $(y_i(a))^2 \mid y_n(a)$:

$$v = \ell y^2 \tag{18}$$

From Lemma 5.7 this gives $y_i(a) \mid n$ (and so $i \leqslant n$). Hence, $j \equiv \pm i \mod 4y_i(a)$. Since $j \equiv k \mod 4y$, this gives $i \equiv k \mod 4y$. Since $i, k \leqslant y$ (recall $i \leqslant y_i(a)$), this says $i = k$, and so $x = x_k(a)$.

Summarizing, we have shown that for any a, k that if there is a solution exists to the equations (10)–(18), then $x = x_k(a)$.

For the other direction, consider $(x_k(a), y_k(a))$, that is, take $i = k$ in the above notation. Let $(x, y) = (x_k(a), y_k(a))$. So, (10) is satisfied. Let $n = 2ky$ and let $(u, v) = (x_n(a), y_n(a))$, so $y^2 \mid v$. So, (12) and (18) are satisfied. By the CRT let $b > 1, a$ be such that $b \equiv 1 \mod 4y$ and $b \equiv a \mod u$. Note here that if a prime p divides y then $p \mid v$ and so $p \nmid u$ (as $(u, v) = 1$). Also, since n ie even, $y_n(a) = v$ is even, so u is odd. So, $(4y, u) = 1$ so we may apply the CRT to get b. This satisfies (13) and (16). Let $(z, w) = (x_k(b), y_k(b))$, so (11) is satisfied. We have $k \leqslant y = y_k(a)$, so (14) holds. Also, $w = y_k(b) \equiv k \mod (b - 1)$ and so $w \equiv k \mod 4y$ and so (15) holds. Finally, $z = x_k(b) \equiv x_k(a) = x \mod u$ since $b \equiv a \mod u$. Thus, (17) holds.

This completes the proof of Theorem 5.13.

□

Theorem 5.14. *The exponential function $f(n,k) = n^k$ is Diophantine.*

Proof. We must show that the relation $m = n^k$ is Diophantine. The idea is to use Lemma 5.12 to relate the exponential function n^k to the solution $(x_k(a), y_k(a))$ for a large enough base a. Fix for the moment n, k, and consider $(x_k(a), y_k(a))$ (we will specify a momentarily). From lemma 5.12 we have that $n^k \equiv x_k(a) - (a-n)y_k(a) \mod 2an - n^2 - 1$. Thus, to equations (10)–(18) we add the equation

$$(x - (a-n)y - m)^2 = (f-1)^2(2an - n^2 - 1)^2 \tag{19}$$

which says that $m \equiv n^k \mod 2an - n^2 - 1$ (we will have momentarily that $a > 1$; also we square both sides since we may have $x - (a-n)y - m = \pm\ell(2an - n^2 - 1)$ for some $\ell \in \mathbb{N}$). We consider a $w > n, k$, so we add the equation

$$w = n + h = k + \ell \tag{20}$$

Suppose now that a is itself of the form $a = x_j(w)$ and the corresponding $y_j(w)$ is divisible by $w - 1$. That is, we add the equation

$$a^2 - (w^2 - 1)(w-1)^2 z^2 = 1 \tag{21}$$

This requires a to be $x_j(w)$ and $(w-1) \mid y_j(w)$. Thus, from Lemma 5.5 we have $j \equiv y_j(w) \equiv 0 \mod w - 1$, so $(w-1) \mid j$ and thus $j \geqslant w - 1$. Hence $a = x_j(w) \geqslant w^j \geqslant w^{w-1} > n^k$. We require that $m < 2an - n^2 - 1$ by adding the equation

$$m + g = 2an - n^2 - 1 \tag{22}$$

So, we now have $m \equiv n^k \mod 2an - n^2 - 1$ and $m < 2an - n^2 - 1$. To conclude $m = n^k$ it suffices to show that $n^k < 2an - n^2 - 1$ as well. Since $a > n^k$ we have $2an - n^2 - 1 > n^k$. To see this, note that if $n = 1$ then $a > n^k = 1$, so $2an - n^2 - 1 \geqslant 4 - 1 - 1 = 2 > 1 = n^k$. So assume $n > 1$. Then $2an - n^2 - 1 > n^{k+1} + (n^{k+1} - n^2 - 1) \geqslant (n^k + 1) + (n^{k+1} - n^2 - 1) \geqslant n^k + (n^{k+1} - n^2) \geqslant n^k$.

We have shown so far that if m, n, k are such that there is a solution to the equations (10)–(22), then $m = n^k$.

For the other direction, suppose $m = n^k$. Let $w > n, k$ and let $a = x_{w-1}(w)$, and note that $y_{w-1}(w) \equiv w - 1 \equiv 0 \mod w - 1$. Then $a > 1$ and $(w-1) \mid y_{w-1}(w)$ so we have $y_{w-1}(w) = (w-1)z$ which satisfies equation (21). Since $w > n, k$ we can satisfy (20). We again have that $a \geqslant w^{w-1} > n^k$ and so $2an - n^2 - 1 > n^k$ and so we can satisfy (22). Set $x = x_k(a)$, $y = y_k(a)$. Then from Lemma 5.12 we have that (19) can be satisfied. Since $x = x_k(a)$ and $y = y_k(a)$, we can satisfy equations (10)–(18). □

This completes the proof of Theorem 4.2.

6. Independence and Undecidability

We now connect Theorem 4.2 with independence and the Gödel incompleteness theorem, and with the notion of undecidability. The phrase "decidable" refers to there being an algorithm (a "decision process") for computing whether the property holds. Of course, this is just the notion of the set in question (when coded as a set of natural numbers) being recursive, that is Δ^0_1.

In Exercise 5 it was shown that the universal Σ^0_1 set is not Δ^0_1 (and a similar statement holds for all the Σ^0_n, Π^0_n). Let us expand this discussion a bit. Let $U \subseteq \omega \times \omega$ be the universal Σ^0_1 of Theorem 1.39. So, $U \in \Sigma^0_1$ and for every Σ^0_1 set $A \subseteq \omega$ we have $A = U_e = \{n \colon U(e,n)\}$ for some e.

Lemma 6.1. *$U \notin \Delta^0_1$.*

Proof. Suppose $U \in \Delta^0_1$. Let $A = \{e \colon \neg U(e,e)\}$. Since Δ^0_1 is closed under complements and substitution by recursive functions (the function $e \mapsto (e,e)$ is recursive), we have that $A \in \Delta^0_1$. Since U is universal, this gives that $A = U_{e_0}$ for some e_0. But then $e_0 \in A$ iff $\neg U(e_0, e_0)$ (definition of A) iff $\neg e_0 \in A$ (since $A = U_{e_0}$), a contradiction. □

The following theorem gives the "undecidability" version of Hilbert's 10th problem.

Theorem 6.2. *There is no algorithm which takes as input a polynomial $p \in \bigcup_k \mathbb{Z}[x_1, \ldots, x_n]$ and decides if $p(\vec{x})$ has a root in $\mathbb{Z}^k$. In fact, there is one particular polynomial $p_0(x, y, z_1, \ldots, z_k)$ such that there is no algorithm which takes as input $(a,b) \in \mathbb{Z}^2$ and decides if $p_0(a, b, \vec{z})$ has an integer root for the $\vec{z}$.*

Proof. Let $U \subseteq \omega \times \omega$ be the universal Σ^0_1 set. From Theorem 4.2 there is a polynomial $p(x, y, z_1, \ldots, z_k)$ such that for all $(a,b) \in \mathbb{Z}^2$ we have $U(a,b)$ iff $\exists z_1, \ldots, z_k \; p(a, b, \vec{z}) = 0$. Since $U \notin \Delta^0_1$ (i.e., is not recursive), there is no algorithm for computing membership in u, and thus there can be no algorithm for deciding if $p(a, b, \vec{z})$ has an integer root. □

By combining Theorem 4.2 with the Gödel incompleteness theorem we may present the Hilbert's 10th problem result as an independence result.

Theorem 6.3. *There is a polynomial $p \in \mathbb{Z}[z_1, \ldots, z_k]$ (for some k) such that the statement $\exists z_1, \ldots, z_k \in \mathbb{Z} \; p(\vec{z}) = 0$ is independent of ZFC. That is, it is not provable in ZFC whether or not this polynomial has an integer root.*

Proof. Let $U \subseteq \omega \times \omega$ again be the universal Σ^0_1 set. Let φ be the statement $\neg$CON(ZFC), which is a Σ_1 statement in the language of arithmetic. Let $A = \{n \in \omega \colon \varphi\}$. Note that since φ is a sentence, A is either $\varnothing$ or ω, but we cannot prove in ZFC which case holds. However, A is the Σ^0_1 set defined by φ. The proofs of the closure properties of Δ^0_1 and the definition of U show that there is an e_0 such that $A(n) \leftrightarrow U(e_0, n)$, and this equivalence is provable in ZFC (in fact, in PA). If we let p be the polynomial representing U again, then we have $A(n)$ iff $p(e_0, n, \vec{z})$ has an integer root, so

$$\text{ZFC} \vdash (\varphi \leftrightarrow \exists y \; \exists \vec{z} \; p(e_0, y, \vec{z}) = 0).$$

Since φ is independent of ZFC (assuming the consistency of ZFC) we have that the statement $\exists y \; \exists \vec{z} \; p(e_0, y, \vec{z}) = 0$ is also independent of ZFC. □

Theorem 6.3 produces a polynomial p (with integer coefficients) of some degree and some dimension (number of variables) such that it is independent of ZFC whether p has an integer root. A natural question is how small can we make the degree and/or the dimension of the polynomial. The following general result shows that every Diophantine problem is equivalent to a 4th degree one. This result is attributed to Skolem.

Theorem 6.4. *Let $p(x_1, \dots, x_k)$ be a polynomial (with integer coefficients). Then there is a polynomial $q(x_1, \dots, x_k, y_1, \dots, y_\ell)$ of degree 4 such that p has an integer root iff q has an integer root.*

Proof. Let $p(x_1, \dots, x_k) = \sum s_i(\vec{x})$ where each s_i is a monomial. Consider a monomial term $s = s(s_1, \dots, x_k) = x_1^{a_1} \cdots x_k^{a_k}$. For each such s we introduce several new variables. First, for each of the variable x_i, we introduce variable $y_{i,1}, y_{i,2}, \dots, y_{i,a_i}$. Let

$$q_{s,i} = (y_{i,1} - x_i)^2 + (y_{i,2} - x_i y_{i,1})^2 + \cdots + (y_{i,a_i} - x_i y_{i,a_i - 1})^2.$$

Thus, $q_{s,i} = 1$ asserts that $y_{i,j} = x_i^j$ for $j \leqslant a_i$ (we could be more efficient here by using binary representation for a_i and just building up the powers $(x_i)^{2^m}$). We then introduce the variables $z_1, \dots, z_k$ and let

$$r_s = (z_1 - y_{1,a_1})^2 + (z_2 - z_1 y_{2,a_2})^2 + \cdots + (z_k - z_{k-1} y_{k,a_k})^2.$$

Thus, $r_s = 0$ asserts that $z_1 = x_1^{a_1}$, $z_2 = x_1^{a_1} x_2^{a_2}, \dots,$ $z_k = x_1^{a_1} \cdots x_k^{a_k} = s$.

We then let $q = \sum_{s,i} q_{s_i} + \sum_s r_s$. Note that q is of degree 4 and $p(\vec{x}) = 0$ iff $\exists \vec{y}\ \exists \vec{z}\ q(\vec{x}, \vec{y}, \vec{z}) = 0$. □

7. The Paris-Harrington theorem

We begin by recalling the Erdös-Rado partition notation. We let κ^λ denote the set of increasing functions f from λ to κ.

Definition 7.1. We write $\kappa \to (\delta)^\lambda_\rho$ to mean for every partition $F\colon \kappa^\lambda \to \rho$ there is a $H \subseteq \kappa$ with $|H| \geqslant \delta$ which is *homogeneous* for F, that is, $\exists \alpha < \rho\ \forall f \in H^\lambda\ (F(f) = \alpha$.

Note that the property $\kappa \to (\delta)^\lambda_\rho$ implies the property $\kappa \to (\delta')^{\lambda'}_{\rho'}$ for $\delta' \leqslant \delta$, $\lambda' \leqslant \lambda$, and $\rho' \leqslant \rho$.

Extending the definition slightly, we say $\kappa \to (\delta)^{<\lambda}_\rho$ if for every partition F of $\kappa^{<\lambda} = \bigcup_{\alpha<\lambda} \kappa^\alpha$ into ρ pieces, there is a set $H \subseteq \kappa$ of size δ such that for each $\alpha < \lambda$, F is constant on H^α.

The Paris-Harrington theorem states that a certain partition property in not provable in PA, though it is provable in ZFC. This partition property concens finitary partitions, and the partition property it concerns is a strengthening of the classical Ramsey theorem, which we discuss below. Although these are partition properties of the natural numbers, more general partition properties play a large role in logic and set theory in general. We therefore briefly discuss some general facts about partition properties.

First, the following theorem says that any partition property with an infinite exponent is inconsistent with choice.

Theorem 7.2 (ZFC)**.** *For all κ, $\kappa \nrightarrow (\omega)^\omega_2$.*

Proof. Consider the equivalence relation on κ^ω defined by $f \equiv g$ iff $\exists n \in \omega\ \forall m \geqslant n\ (f(m) = g(m))$. Using AC, Let $S \subseteq \kappa^\omega$ be a selector for thie relation (i.e., S contains exactly one element from each equivalence class). Consider the partition $F\colon \kappa^\omega \to 2$ given by $F(f) = 1$ iff the least n such that $\forall m \geqslant n\ f(m) = g(m)$ is odd, where $\{g\} = S \cap [f]$ is the unique element of S equivalent to f. suppose $H \subseteq \kappa$ was infinite and homogeneous for F. Let $a_0 < a_1 < \cdots$ be an infinite increasing sequence of elements from H. Let $f(n) = a_{2n}$. Let $g = S \cap [f]$. Let n be least so that $\forall m \geqslant n\ f(m) = g(m)$. But we then change f to f' by defining $f'(n) = a_{2n+1}$ to make $n + 1$ the least point of eventual agreement (this does not change the equivalence class of f and so the representative g does not change). So, H is not homogeneous. □

So, with AC we can only consider finite-exponent partition properties (or slight variations). However, without AC, much stronger partiton properties are possible, and these play an important role in determinacy theory. For example a theorem of Martin is that $\omega_1 \to (\omega_1)^{\omega_1}$ (when the subscript is omitted, it is understood to be 2).

Definition 7.3. κ has the *strong partition property* if $\kappa \to (\kappa)^\kappa$. κ has the *weak partition property* if $\kappa \to (\kappa)^{<\kappa}$.

In a model of determinacy, there are many cardinals κ with the strong partition property, but there are no such cardinals in a model of ZFC by theorem 7.2.

Definition 7.4. κ is a *Ramsey* cardinal if $\kappa \to (\kappa)^{<\omega}$. κ is *weakly compact* if κ is uncountable and $\kappa \to (\kappa)^2$.

We note that ω is not Ramsey as can be seen by consider the partition $F\colon \omega^{<\omega} \to \omega$ given by $F(n_1, \ldots, n_k) = 1$ iff $k \in \{n_1, \ldots, n_k\}$ (here we identify $f \in \omega^{<\omega}$ with a finite subset of ω, written in increasing order). Thus, every Ramsey cardinal in uncountable, and thus is weakly compact.

The next theorem shows that weakly compact cardinals are inaccessible, and thus cannot be shown to exist in ZFC.

Theorem 7.5. *Every weakly compact cardinal is strongly inaccessible. That is, κ is a regular limit cardinal (weakly inaccessible) and if $\alpha < \kappa$ then $2^\alpha < \kappa$ (a strong limit cardinal).*

Proof. To see κ is regular, suppose $\lambda = \mathrm{cof}(\kappa) < \kappa$. Let $f\colon \lambda \to \kappa$ be increasing and cofinal. Partition κ^2 by $F(\alpha, \beta) = 1$ iff $\mathrm{ran}(f) \cap (\alpha, \beta) \neq \varnothing$. There cannot be a homogeneous set $H \subseteq \kappa$ for F of size κ. for on the one hand we can always fine $\alpha < \beta$in H with $\mathrm{ran}(f) \cap (\alpha, \beta) \neq \varnothing$ by taking β sufficiently large. On the other hand, since $|H| = \kappa > \lambda$, one of the intervals $[f(\gamma), f(\gamma + 1))$ must have $> \lambda$ many points of H in it. In particular, we can find $\alpha < \beta$ in $H \cap (f(\gamma), f(\gamma + 1))$, which says $F(\alpha, \beta) = 0$.

To finish, we need to show that if $\lambda < \kappa$ then $2^\lambda < \kappa$. Suppose $2^\lambda \geqslant \kappa$. Let $\{A_\alpha\}_{\alpha<\kappa}$ be a κ sequence of distinct subseteq of λ. We consider the partition $F\colon \kappa^2 \to 2$ defined as follows. Let $\alpha < \beta < \kappa$. Let $\delta(\alpha, \beta)$ be the least ordinal less than λ such that $\delta(\alpha, \beta) \in \Delta(A_\alpha, A_\beta)$. We set $F(\alpha, \beta) = 1$ iff $\delta(\alpha, \beta) \in A_\alpha$. Let $H \subseteq \kappa$ be homogeneous for F of size κ.

Suppose first that for $\alpha < \beta$ in H we have $F(\alpha, \beta) = 0$. For each $\alpha < \kappa$, let $a(\alpha, i)$ be the ith element of A_α (this is defined for $i < \mathrm{o.t.}(A_\alpha)$). The homogeneity

of H gives that for $\alpha < \beta$ in H that $a(\alpha, 0) \geqslant a(\beta, 0)$, past the unique point, if any, where $A_\gamma = \varnothing$. Thus there is an $a(0) < \lambda$ and a $\gamma_0 < \kappa$ such that for $\alpha > \gamma_0$ in H we have $a(\alpha, 0) = a(0)$. That is, we have stabilized the first element of the sets A_α. Past the unique point, if any, in H where $A_\gamma = \{a(0)\}$ we have that for $\alpha < \beta$ in H that $a(\alpha, 1) \geqslant a(\beta, 1)$. This give a $a(1) < \lambda$ and a $\gamma_1 < \kappa$ such that for $\alpha > \gamma_1$ in H we have $a(\alpha, 1) = a(1)$, that is, we have stabilized the first two elements of A_α. In general suppose that $i < \lambda$ and for all $j < i$ we have defined $\gamma_j < \kappa$ and $a(j) < \lambda$ such that for all $\alpha > \gamma_i$ in H and we have $a(\alpha, j) = a(j)$. Since κ is regular, $\gamma = \sup_{j<i} \gamma_j < \kappa$. The above argument then produces a $\gamma_i < \kappa$, $\gamma_i > \gamma$, and an $a(i) < \lambda$ such that for all $\alpha > \gamma_i$ in H we have $a(\alpha, i) = a(i)$. If now $\alpha < \beta$ are in H and $\alpha, \beta > \sup_{i<\lambda} \gamma_i$, then $A_\alpha = A_\beta$, a contradiction.

Suppose next that on the homogeneous side we have $F(\alpha, \beta) = 1$. Then for $\alpha < \beta$ in H we have $a(\alpha, 0) \leqslant a(\beta, 0)$. Either there is a $\gamma_0 < \kappa$ such that for all $\alpha < \gamma_0$ in H we have $a(\alpha, 0) = a(\beta, 0)$ or else there is a κ size subset of H on which $a(\alpha, 0)$ is strictly increasing (using here that κ is regular). The latter case cannot occur, as this a map $\alpha \mapsto a(\alpha, 0)$ from a set of size κ to a set of size λ. So, we may assume γ_0 and $a(0)$ are defined. Continuing, as the previous case, we define γ_i, $a(i)$ for all $i < \lambda$, which is a contradiction as in the first case. □

Remark 7.6. The proof of Theorem 7.5 shows that for all κ that $2^\kappa \nrightarrow (\kappa^+)^2$.

We now turn to partition properties on the integers. We first state the "infinitary" version of Ramsey's theorem.

Theorem 7.7 (Infinite Ramsey Theorem)**.** *For all $n, k \in \omega$, $\omega \to (\omega)^n_k$.*

Proof. We proceed by induction on n. The case $n = 1$ is trivial. Assume the result for exponent $n - 1$, and let $F\colon \omega^n \to k$ be a given partition. Let $a_0 \in \omega$ and let $F_{a_0}\colon (\omega - (a_0 + 1))^{n-1} \to k$ be defined by $F_{a_0}(i_1, \ldots, i_{n-1}) = F(a, 0, i_1, \ldots, i_{n-1})$. By the $n - 1$ case, there is an $H_{a_0} \subseteq \omega - (a_0 + 1)$ which is homogeneous for F_{a_0}. Let $a_1 \in H_{a_0}$. Define $F_{a_1}\colon (H_{a_0} - (a_1 + 1))^{n-1} \to k$ by $F_{a_1}(i_1, \ldots, i_{n-1}) = F(a_1, i_1, \ldots, i_n)$. Let $H_{a_2} \subseteq H_{a_0} - (a_1 + 1)$ be homogeneous for H_{a_1}. Continuing in this manner we define $H' = a_0 < a_1 < a_2 < \cdots$ with the property that if $\vec{a}$, $\vec{b} \in H^n$ and $\min(\vec{a}) = \min(\vec{b})$, then $F(\vec{a}) = F(\vec{b})$. This defines a map g from H' to k ($g(a_i) = F(\vec{a})$ for any $\vec{a} \in H$ with $\min(\vec{a}) = a_i$). We may fix an infinite $H \subseteq H'$ which fixes that value of g. H is then clearly homogeneous for F. □

We next state the "finitary" version of Ramsey's theorem, and show that it follows from the infinite version by a compactness argument.

Theorem 7.8 (Finite Ramsey Theorem)**.** *For all n, k, m, there is an ℓ so that $\ell \to (m)^n_k$.*

Proof. Fix n, k, m, and suppose that for all ℓ the stated property fails. For each ℓ, let $F_\ell\colon \ell^n \to k$ be a partiton without a homogeneous set of size m. For $\ell' \leqslant \ell$, let $F_{\ell',\ell}$ be the restriction of F_ℓ to $(\ell')^n$. Since for any ℓ' there are only finitely many partitions of $(\ell')^n$ into k pieces, we have that for any ℓ', $\{F_{\ell',\ell}\colon l \in \omega\}$ is finite. It follows that there is a sequence $a_0 < a_1 < a_2 < \cdots$ such that for all $i < j < k$ we have $F_{a_i,a_j} = F_{a_i,a_k}$ [given $a_0 < \cdots < a_k$ and $H_k \subseteq \omega - (a_k + 1)$ such that for all $\ell_1 < \ell_2$ in H_k we have $F_{a_k,a_{\ell_1}} = F_{a_k,a_{\ell_2}}$, let $a_{k+1} \in H_k$, and then get $H_{k+1} \subseteq H_k - (a_{k+1} + 1)$ which fixes $F_{a_{k+1},\ell}$ for all $\ell \in H_{k+1}$]. Let f_k be the common value of F_{a_k,a_ℓ} for $\ell > k$. Thus, the f_k union to a partition

$f\colon \omega^n \to k$. From Theorem 7.7, let $H \subseteq \omega$ be an infinite homogeneous set for f. Let k be large enough so that $|H \cap a_k| \geqslant m$. Then $H \cap a_k$ is homogeneous for $f \restriction (a_k)^m = F_{a_{k+1}} \restriction (a_k)^m$, and so homogeneous for $F_{a_{k+1}}$. This contradicts the definition of $F_{a_{k+1}}$. □

The statement of the finite Ramsey theorem is a sentence in the language of arithmetic, but the proof given above did not take place in arithmetic (i.e., from the axiom system PA) since it passed through the infinite Ramsey theorem 7.7 which talks about $\mathcal{P}(\omega)$. The finite Ramsey theorem can be proved in PA, however, by re-working the above argument. We give this modified argument next.

Theorem 7.9. *The statement of the finite Ramsey theorem, $\forall n, k, m\ \exists \ell\ [\ell \to (m)^n_k]$ is provable in PA.*

Proof. Fix k, and let $\varphi(n)$ be the statement that $\forall m\ \exists \ell$ for all partitons $F\colon (\ell)^n \to k$, there is a homogeneous set of size m. We prove $\varphi(n)$ by induction on n. For $n = 1$ we can take $\ell = (m-1)k + 1$. So, working in PA, assume $\varphi(n)$ and we show $\varphi(n+1)$. We follow the proof of Theorem 7.7.

Let $r(a, b)$, assumed defined for $a \leqslant n$, be the least ℓ so that for all partitions $F\colon (\ell)^a \to k$ there is a homogeneous set of size b. Let r_n be the function $r_n(m) = r(n, m)$. Note that $r_n(1) = n$. Let

$$\ell = r'_n \circ r'_n \circ \cdots \circ r'_n(1)$$

where the functions r'_n are composed $mk + 1$ times, and $r'_n = r_n + 1$. That is, let $r_{n+1}(m) = {r'}_n^{(mk+1)}(1)$, where the superscript denotes composition. Let $\ell = {r'}_{n+1}(m)$, and suppose $F\colon (\ell)^{n+1} \to k$. Let $H_{-1} = \ell$, and let $a_0 = 0$ be the least element of H_{-1}. As in 7.7 we consider the partition $F_{a_0}\colon (H_{-1} - (a_0 + 1))^n \to k$ by $F_{a_0}(i_1, \ldots, i_{n-1}) = F(a_0, i_1, \ldots, i_{n-1})$. Since $\ell = r_{n+1}(1) = {r'}_n^{(mk+1)}(1) = r_n({r'}_n^{(mk)}(1)) + 1$, we get a homogeneous set H_0 for F_{a_0} of size ${r'}_n^{(mk)}(1) + 1$. Let a_1 be the least element of H_{a_0}, so $H_{a_0} - (a_1 + 1)$ has size at least ${r'}_n^{(mk)}(1)$.

Continuing, as in 7.7 we obtain $a_0 < a_1 < \cdots < a_{mk}$ which are "min homogeneous" as in 7.7. From this set we may, as in 7.7, extract a homogeneous set of size m (we now have a coloring of these $mk + 1$ points into k colors, so there must be a homogeneous set of size m). □

Thus, working in PA we have shown that the following function is well-defined.

Definition 7.10. For $1 \leqslant n \leqslant m$ and $k \geqslant 2$, let $r(n, m, k)$ be the least ℓ such that $\ell \to (m)^n_k$.

We introduce the Ackermann hierarchy of fast-growing functions.

Definition 7.11. Let $E_0(n) = n + 1$. Let $E_{k+1}(n) = E_k \circ \cdots \circ E_k(n) = E_k^{(n)}(n)$, where the superscript denotes composition n times. Let $E_\omega(n) = E_n(n)$.

We will extend the Ackermann hierarchy further into the transfinite later. Note that $E_1(n) = 2n$, $E_2(n) = n2^n \approx 2^n$, and $E_3(n) \approx 2^{2^{2^{\cdots^n}}}$, a stack of exponentials of height n. E_4 is too large to write down in exponential notation.

The proof of Theorem 7.9 gives an estimate for the diagonal Ramsey function $r(n, n, n)$ of order $E_\omega(n)$. This, however, is not a very good estimate.

We now give an improved bound for $r(n, m, k)$ due to Erdös-Rado (1952). Recall that $n \leqslant m$ always and $r(n, n, k) = n$.

Theorem 7.12 (Erdös-Rado)**.** *For $n < m$, $r(n,m,k) \leqslant k^{\binom{t-1}{n-1}}$, where $t = r(n-1, m-1, k) + 1$.*

Proof. Let $t = r(n-1, m-1, k) + 1$, and let $\ell = k^{\binom{t-1}{n-1}+1}$. Let $F\colon (\ell)^n \to k$ be given. A set $H \subseteq \ell$ is called $(n-1)$ homogeneous if for all $\vec{a}$, $\vec{b} \in (H)^n$ with $\vec{a} \restriction n-1 = \vec{b} \restriction n-1$ we have $F(\vec{a}) = F(\vec{b})$. It suffices to show that there is an $H \subseteq \ell$ which is $n-1$ homogeneous and $|H| \geqslant t$. For say $H = \{a_1, \ldots, a_t\}$, and consider $F'\colon (H - \{a_t\})^{n-1} \to k$, given by $F'(i_1, \ldots, i_{n-1}) = F(i_1, \ldots, i_{n-1}, a_t)$. There is an $H' \subseteq H$ of size $|H'| = m-1$ which is homogeneous for F'. Then $H = H' \cup \{a_t\}$ is homogeneous for F, and $|H| \geqslant m$.

We construct the elements $a_1 < a_2 < \cdots < a_t < \ell$ of an $n-1$ homogeneous set by induction. Let $\{a_1, \ldots, a_{n-1}\} = \{0, 1, \ldots, n-2\}$. There is an $H_{n-1} \subseteq \ell - (a_{n-1}+1)$ such that if $a, b \in H_{n-1}$ then $F(a_1, \ldots, a_{n-1}, a) = F(a_1, \ldots, a_{n-1}, b)$, and $|H_{n-1}| \geqslant \frac{(\ell-n+1)}{k} \geqslant \frac{\ell}{k}$.

Suppose in general that at step $i \geqslant n-1$ we have $a_1 < \cdots < a_i$ and $H_i \subseteq \ell - (a_i + 1)$ and for any $\vec{a} \in \{a_1, \ldots, a_i\}^{n-1}$ and any $p < q$ in H_i we have $F(\vec{a}, p) = F(\vec{a}, q)$. Assume also $H_{n-1} \supseteq H_n \supseteq \cdots \supseteq H_i$ and $a_j \in H_{j-1}$ for all $j \leqslant n-1$. Let $a_{i+1} = \min(H_i)$. Let S be the set of $\vec{a} \in \{a_1, \ldots, a_{i+1}\}^{n-1}$ with $\max(\vec{a}) = a_{i+1}$. For each $b \in H_i - (a_{i+1}+1)$, we have $g(b) = \langle F(\vec{a}, b)\colon \vec{a} \in S \rangle \in k^S$. So, we may get $H_{i+1} \subseteq H_i - (a_{i+1}+1)$ on which g is constant and $|H_{i+1}| \geqslant \frac{|H_i|-1}{k^{|S|}} = \frac{|H_i|-1}{k^{\binom{i}{n-2}}}$. Thus, we can define $a_1 < \cdots < a_t$ provided

$$(\cdots(((\frac{\ell-n+1}{k} - 1)\frac{1}{k^{\binom{n-1}{n-2}}} - 1)\frac{1}{k^{\binom{n}{n-2}}} - 1)\cdots)\frac{1}{k^{\binom{t-2}{n-2}}} > 0$$

that is,

$$\frac{\ell-n+1}{k^{\binom{n-2}{n-2}+\binom{n-1}{n-2}+\cdots+\binom{t-2}{n-2}}} \geqslant \frac{1}{k^{\binom{n-1}{n-2}+\binom{n-1}{n-2}+\cdots+\binom{t-2}{n-2}}} + \frac{1}{k^{\binom{n}{n-2}+\binom{n-1}{n-2}+\cdots+\binom{t-2}{n-2}}} + \cdots + \frac{1}{k^{\binom{t-2}{n-2}}},$$

which gives

$$\ell \geqslant n + k^{\binom{n-2}{n-2}} + k^{\binom{n-2}{n-2}+\binom{n-1}{n-2}} + \cdots + k^{\binom{n-2}{n-2}+\binom{n-1}{n-2}+\cdots+\binom{t-3}{n-2}}.$$

So,

$$\begin{aligned} r(n,m,k) &\leqslant n + k^{\binom{n-2}{n-2}} + k^{\binom{n-2}{n-2}+\binom{n-1}{n-2}} + \cdots + k^{\binom{n-2}{n-2}+\binom{n-1}{n-2}+\cdots+\binom{t-3}{n-2}} \\ &= n + k^{\binom{n-1}{n-1}} + k^{\binom{n}{n-1}} + \cdots + k^{\binom{t-2}{n-1}} \\ &\leqslant k^{\binom{t-1}{n-1}}. \end{aligned}$$

To see the last inequality, note that if $n = 2$ then

$$2 + k^1 + k^2 + \cdots + k^{t-2} = 1 + \frac{k^{t-1}-1}{k-1} \leqslant 1 + k^{t-1} - 1 = k^{\binom{t-1}{n-1}}.$$

If $n \geqslant 3$ then

$$n + k^{\binom{n-1}{n-1}} + k^{\binom{n}{n-1}} + \cdots + k^{\binom{t-2}{n-1}} \leqslant n + k^{\binom{t-2}{n-1}+1} \leqslant 2k^{\binom{t-2}{n-1}+1} \leqslant k^{\binom{t-2}{n-1}+2} \leqslant k^{\binom{t-1}{n-1}}.$$

Here we have used that $n \leqslant k^n \leqslant k^{\binom{t-2}{n-1}+1}$ which holds provided $t - 2 \geqslant n$, that is provided $f(n-1, m-1, k) \geqslant n+1$, which we easily have (as $n < m$). Also,

$\binom{t-1}{n-1} - \binom{t-2}{n-1} \geqslant 2$ for all $t-2 \geqslant n-1$, which we have as

$$\begin{aligned}\binom{t-1}{n-1} - \binom{t-2}{n-1} &= \frac{(t-2)\cdots(t-n+1)[(t-1)-(t-n)]}{(n-1)!} \\ &= (n-1)\frac{(t-2)(t-3)\cdots(t-n+1)}{(n-1)(n-2)\cdots 2} \geqslant n-1 \geqslant 2\end{aligned}$$

using again that $t-n+1 \geqslant 2$.

□

In particular, we have the bound

Corollary 7.13.

$$r(n,m,k) \leqslant k^{r(n-1,m-1,k)^{n-1}}. \tag{23}$$

Proof. If $n = m$ this becomes $n \leqslant k^{(n-1)^{n-1}}$ which easily holds (as $k \geqslant 2$). If $n < m$ this follows from Theorem 7.12 as $\binom{r}{n-1} \leqslant r^{n-1}$.

□

From Equation 23 we see that the ramsey function grows roughly as E_3. More precisely, let $g(p) = \sup\{r(m,n,k) \colon m,n,k \leqslant p\}$.

Claim. For large enough p we have $g(p) \leqslant E_3(p+1)$.

Proof. Let $a * b$ denote a^b, $a * b * c$ denote $a * (b * c)$, etc. From Corollary 7.13 we get

$$g(p) \leqslant p * p * (p-1)p * (p-2) * p * \cdots * 3p * 2p.$$

Note that $a * b = a^b \leqslant 2^{ab} = 2 * ab$ and $c \cdot (a * b) \leqslant 2 * (c + ab) \leqslant 2 * (cab)$ provided $a, b, c \geqslant 2$.

$$\begin{aligned}g(p) &\leqslant p * p * (p-1)p * (p-2)p * \cdots * 3p * 2p \\ &\leqslant 2 * [p \cdot (p * (p-1)p * (p-2)p * \cdots * 3p * 2p)]] \\ &\leqslant 2 * 2 * p^2[(p-1)p * (p-2)p * \cdots * 3p * 2p \\ &\leqslant 2 * 2 * 2 * p^3(p-1)[(p-2)p * (p-3)p * \cdots * 3p * 2p] \\ &\leqslant 2 * 2 * 2 * 2 * p^4(p-1)(p-2)[(p-3)p * (p-4)p * \cdots * 3p * 2p] \\ &\leqslant 2 * 2 * 2 * 2 * \cdots * 2 * (p^{p-1}(p-1)(p-2)\cdots(3p)(2p))\end{aligned}$$

where the last expression has $p-1$ 2's in the tower. The final expression is bounded by $2 * 2 * p$ for large enough p. Thus, $g(p) \leqslant E_3(p+1)$.

□

We next introduce the Paris-Harrington partition property which is a strengthening of the finite Ramsey property.

Definition 7.14. The Paris-Harrington partition property for n, k, m is the statement that there is an ℓ so that for all partition $F \colon (\ell)^n \to k$ there is a homogeneous set H for F with $|H| \geqslant m$ and $|H| \geqslant \min(H)$.

We first show that the Paris-Harrington partition property is a theorem of ZFC.

Theorem 7.15. *The Paris-Harrington partition property is a theorem of ZFC.*

Proof. We use a compactness argument as the proof of Theorem 7.8. Suppose the principle fails for some n, k, m, which we fix. For all ℓ, fix a partition $F_\ell \colon (\ell)^n \to k$ for which there is no homogeneous set H as desired. Ss in the proof of Theorem 7.8, we may fix a sequence a sequence $a_0 < a_1 < \cdots$ and partitions $f_0, f_1, \ldots,$ such that for all k and all $\ell > k$ we have that $F_{a_\ell} \restriction (a_k)^n = f_k$. Let $f = \bigcup_k f_k$, so $f \colon (\omega)^n \to k$ is a partition of $(\omega)^n$. By the infinite Ramsey theorem, let $H \subseteq \omega$ be infinite and homogeneous for f. Let $i_0 \in H$ with $i_0 \geqslant m$. Fix $i_1 < \cdots < i_p$ in H with $i_1 > i_0$ and $p \geqslant i_0$. Fix k large enough so that $a_k > i_p$, and let $\ell > k$. Then $\{i_0, \ldots, i_p\}$ is homogeneous for $f_k = F_\ell \restriction (a_k)^n$, a contradiction as this set satisfies the Paris-Harrington condition. □

We now head toward showing that the Paris-Harrington partition property is not provable in PA. The approach uses the partition property to generate a sufficiently rich set of indiscernibles for a model of arithmetic.

We call $F \colon (\ell)^n \to \ell$ *regressive* if $F(a_1, \ldots, a_n) < a_0$. We call $H \subseteq \ell$ *min-homogeneous* if whenever $\vec{a}$, $\vec{b}$ are in $(H)^n$ and $\min(\vec{a}) = \min(\vec{b})$, then $F(\vec{a}) = F(\vec{b})$. We show the Paris-Harrington partition property implies the following partition property for regressive functions.

Definition 7.16 (regressive partition property)**.** The regressive partition property is the statement that for all m, n, k, s there is an ℓ such that if $F_1, \ldots, F_k \colon (\ell)^n \to \ell$ are regressive, then there is an $H \subseteq [s, \ell]$ with $|H| \geqslant m$ which is min-homogeneous for each F_i.

First we show that the Paris-Harrington partition property implies the slightly stronger version where we require that $|X| \geqslant \min(H) + n + 1$, and also we can keep $\min(H) \geqslant s$ for given s.

Lemma 7.17. *Assume the Paris-Harrington partition property (Definition 7.14). Then for any m, n, k, s there is an ℓ such that for any $F \colon (\ell)^n \to k$ there is a homogeneous $H \subseteq [s, \ell]$ with $|H| \geqslant \min(H) + n + 1$, $|H| \geqslant m$.*

Proof. Let ℓ be large enough so that for any $G \colon (\ell)^n \to k+1$ there is a homogeneous X with $|X| \geqslant \min(X)$ and $|X| \geqslant s + m + 2n + 1$. Given now $F \colon (\ell)^n \to k$, define $G(a_1, \ldots, a_n) = F(a_1 - n - 1, \ldots, a_n - n - 1)$ if all $a_i \geqslant s + n + 1$, and $G(\vec{a}) = k + 1$ otherwise. Let X be homogeneous for G with $|X| \geqslant \min(X)$ and $|X| \geqslant s+m+2n+1$. Since $|X| \geqslant s+2n+1$, there are at least n elements of X which are $\geqslant s+n+1$. So, we can find an n-tuple from X which does not have color $k+1$, and so all n-tuples from X do not have color $k+1$. That is, $\min(X) \geqslant s+n+1$. Let $H = \{a - n - 1 \colon a \in X\}$, so $H \subseteq [s, \ell]$, and $|H| = |X| \geqslant \min(X) \geqslant \min(H) + n + 1$. Also, $|H| = |X| \geqslant m$. Clearly H is homogeneous for F as X is homomogeneous for G. □

Theorem 7.18. *Work in PA. Assume the Paris-Harrington partition property (Definition 7.14). Then the regressive partition property (Definition 7.16) holds.*

Proof. Assume the Paris-Harrington partition property holds. Fix m, n, k, s as in the statement of the regressive partition property. Let ℓ be large enough so that for any $F \colon (\ell)^{n+1} \to 3^k$ there is a a $X \subseteq [s, \ell]$ with $|X| \geqslant m+n$, $|X| \geqslant \min(X)+n+1$ which is homogeneous for F.

Let now $F_1, \dots, F_k \colon (\ell)^n \to \ell$ be regressive. For each $1 \leqslant i \leqslant k$, consider the partition $G_i \colon (\ell)^{n+1} \to 3$ given by

$$G_i(a_0, a_1, \dots, a_n) = \begin{cases} 0 & \text{if } F_i(a_0, a_1, \dots, a_{n-1}) < F_i(a_0, a_2, \dots, a_{n-1}, a_n) \\ 1 & \text{if } F_i(a_0, a_1, \dots, a_{n-1}) = F_i(a_0, a_2, \dots, a_{n-1}, a_n) \\ 2 & \text{if } F_i(a_0, a_1, \dots, a_{n-1}) > F_i(a_0, a_2, \dots, a_{n-1}, a_n) \end{cases}$$

Let $G \colon (\ell)^{n+1} \to 3^k$ be the partition given by $G(a_0, a_1, \dots, a_n) = \langle F_1(\vec{a}), \dots, F_k(\vec{a}) \rangle$. Let $X \subseteq [s, \ell]$ be homogeneous for G with $|X| \geqslant m + n$ and $|X| \geqslant \min(X) + n + 1$. So, X is homogeneous for each G_i, and we claim that homogeneous color is 1 for all i. To see this, let $x_0, x_1, \dots$ enumerate X, and consider the tuples $\vec{a}_j = (x_0, x_j, x_{j+1}, \dots, x_{j+n-1})$. There are $|X| - n \geqslant \min(X) + n + 1 - n = x_0 + 1$ such tuples, and $F_i(\vec{a}_j) < x_0$ for all j. So, we must have $F_i(\vec{a}_j) = F_i(\vec{a}_{j'})$ for some $j \neq j'$ (say $j < j'$). However, we can get from $(x_0, x_j, \dots, x_{j+n-1})$ to $(x_0, x_{j'}, \dots, x_{j'+n-1})$ by a finite sequence of operations as in the definition of G_i (the first move is to delete x_j and add $x_{j'+n-1}$). But then we would have $F_i(a_j) < F(a_{j'})$ (if the homogeneous color is 0), a contradiction (and similarly if the homogeneous color is 2). So, for each i, the homogeneous color for G_i in 1.

This implies that X minus the $n-1$ largest elements $\{y_1, \dots, y_{n-1}\}$ of X is min-homogeneous for each F_i. For if $(a_0, \dots, a_{n-1}) \in X - \{y_1, \dots, y_{n-1}\}$, then

$$\begin{aligned} F_i(a_0, a_1, \dots, a_{n-1}) &= F_i(a_0, a_2, \dots, a_{n-1}, y_1) \\ &= F_i(a_0, a_3, \dots, a_{n-1}, y_1, y_2) = \cdots \\ &= F_i(a_0, y_1, \dots, y_{n-1}). \end{aligned}$$

which shows $X - \{y_1, \dots, y_{n-1}\}$ is min-homogeneous for each F_i. Clearly $|X - \{y_1, \dots, y_{n-1}\}| \geqslant m$. □

We now use the regressive partition property to obtain a strong form of indiscernibles for models of arithmentic. We note that theorem 7.18 was proved in PA and thus holds in any model of PA.

Definition 7.19. Let $\mathcal{M}$ be a model of PA, and let Γ be a finite set of formulas in the language of arithmetic. We say $I \subseteq |\mathcal{M}|$ is a set of *diagonal indiscernibles* for $\mathcal{M}$ if whenever $\varphi(u_1, \dots, u_k, v_1, \dots, v_n) \in \Gamma$, $x_0 < x_1 < \cdots < x_n$ and $x_0 < y_1 < \cdots < y_n$ are in I, and $a_1, \dots, a_k < x_0$ then

$$\mathcal{M} \models \varphi(\vec{a}, x_1, \dots, x_n) \leftrightarrow \varphi(\vec{a}, y_1, \dots, y_n).$$

Theorem 7.20. *Asssume PA and the Paris-Harrington partition property. Then for all m, n, k, k', s and formulas $\Gamma = \{\varphi_i(u_1, \dots, u_k, v_1, \dots, v_n)\}_{i \leqslant k'}$ in the language of arithmetic, there is a set I of diagonal indiscernibles for $\varphi_1, \dots, \varphi_{k'}$ with $|I| \geqslant m$, and $\min(I) \geqslant s$.*

Proof. Fix m, n, k, k', s and the set of formulas Γ of size k'. We may assume $m > 2n$. From the finite Ramsey theorem, let p be large enough so that $p \to (m + n)^{2n+1}_{k'+1}$. From the regressive Ramsey theorem, let ℓ be large enough so that if $F_1, \dots, F_k \colon (\ell)^{2n+1} \to \ell$ are regressive, then there is an $X \subseteq [s, \ell]$ with $|X| \geqslant p$ which is min-homogeneous for the F_i.

Define $F_i \colon (\ell)^{2n+1} \to \ell$ as follows. Set $F_i(x_0, x_1, \dots, x_n, x_{n+1}, \dots, x_{2n}) = 0$ if for all $\vec{a} < x_0$ we have

$$\mathcal{M} \models \varphi_j(\vec{a}, x_1, \dots, x_n) \leftrightarrow \varphi_j(\vec{a}, x_{n+1}, \dots, x_{2n}).$$

for all $j \leqslant k'$. Set also in this case $G(x_0, \ldots, x_{2n+1}) = 0$. Otherwise, let $G(x_0, \ldots, x_{2n}) \leqslant k'$ be the least such j, and let $F_i(x_0, \ldots, x_{2n}) < x_0$, for $i \leqslant k$, be the ith coordinate of the least $\vec{a}$ which violates this equation.

As the F_i are regressive, from the definition of ℓ, there is a $X \subseteq [s, \ell]$ with $|X| \geqslant p$ which is min-homogeneous for the F_i. From the definition of p we get an $H \subseteq X$ with $|H| \geqslant m + n > 3n$ on which G is constant.

Suppose first that the homogeneous value of G is $j \neq 0$. Fix $x_0 < x_1 < \cdots < x_{3n}$ in $(H)^{2n+1}$. Let $\vec{a}$ be the constant value of the $F_i(\vec{x})$ for $\vec{x} \in H$ with $\min(\vec{x}) = x_0$. Then if we let $\vec{y} = x_1, \ldots, x_n$, $\vec{z} = x_{n+1} \ldots, x_{2n}$, and $\vec{w} = x_{2n+1} \ldots, x_{3n}$ then we have

$$\mathcal{M} \models \varphi_j(\vec{a}, \vec{y}) \nleftrightarrow \varphi_j(\vec{a}, \vec{z})$$
$$\mathcal{M} \models \varphi_j(\vec{a}, \vec{y}) \nleftrightarrow \varphi_j(\vec{a}, \vec{w})$$
$$\mathcal{M} \models \varphi_j(\vec{a}, \vec{z}) \nleftrightarrow \varphi_j(\vec{a}, \vec{w})$$

which is a contradition as two of these must have the same truth value.

Suppose next that the homogeneous value for G is 0. Recall $|H| \geqslant m + n$. Let $z_1, \ldots, z_n$ be the n largest elements of H. Let $I = H - \{z_1, \ldots, z_n\}$. Then I is a set of diagonal indiscernibles for Γ of size $|I| \geqslant m$. To see they are diagonal indiscernibles, note that if $x_0 < x_1 < \cdots < x_n$ and $x_0 < y_1 < \cdots < y_n$ are in I, then for all $\vec{a} < x_0$ and all j we have

$$\mathcal{M} \models \varphi_j(\vec{a}, x_1, \cdots, x_n) \leftrightarrow \varphi_j(\vec{a}, z_1, \cdots, z_n) \leftrightarrow \varphi_j(\vec{a}, y_1, \ldots, y_n).$$

Thus I is the desired set of order indiscernibles for Γ. □

Recall that PA consists of finitely many algebraic axioms together with the induction axioms. The induction axioms are equivalent to the axioms which assert, for each formula $\varphi(x)$, that if $\exists x \varphi(x)$, then there is a least x such that $\varphi(x)$. That is, the axiom

$$\exists x \varphi(x) \to \exists x [\varphi(x) \wedge \forall y < x \, \neg \varphi(y)].$$

Note that if $\mathcal{M}$ is a model of PA, and $\mathcal{N}$ is an initial segment of $\mathcal{M}$ (i.e., $\mathcal{N} \subseteq \mathcal{M}$ and if $a \in \mathcal{N}$, $b \in \mathcal{M}$, and $b \leqslant a$, then $b \in \mathcal{M}$) then for any Δ_0 formula $\varphi(x_1, \ldots, x_n)$ and $a_1, \ldots a_n \in \mathcal{N}$,

$$\mathcal{N} \models \varphi(a_1, \ldots, a_n) \leftrightarrow \mathcal{M} \models \varphi(a_1, \ldots, a_n).$$

Lemma 7.21. *Let $\mathcal{M}$ be a model of PA and $I = x_0 < x_1 < \cdots$ be a sequence of diagonal indiscernibles (which are elements of $\mathcal{M}$) for all formulas φ in the language of number theory. Let $\mathcal{N} = \{x \in \mathcal{M} \colon \exists i \ (x \leqslant x_i)\}$. Then $\mathcal{N}$ is closed under addition, multiplication, exponentiation and is a model of PA.*

Proof. Suppose $a, b < x_i$ are elements of $\mathcal{M}$. If $a + b \geqslant x_{i+1}$ then we can get $c \leqslant b$ such that $a + c = x_{i+1}$. But then the statement $\varphi(u_1, u_2, v_1, v_2,) = u_1 + u_2 = v_2$ holds at (a, b, x_i, x_{i+1}) but not at (a, b, x_i, x_{i+2}), a contradiction. So, of $a, b < x_i$, then $a + b < x_{i+1}$. Thus, $\mathcal{N}$ is closed under addition.

If $a, b < x_i$ but $ab \geqslant x_{i+1}$, then there is a $c \leqslant b$ and an $d \leqslant a$ such that $ac + d = x_{i+1}$, where $a, c, d < x_i$. This again violates diagonal indiscernibility.

If $a, b < x_i$ and $a^b \geqslant x_{i+1}$, then there is a $c < b$ such that $a^c < x_{i+1}$ but $a^c \cdot a \geqslant x_{i+1}$. By the previous paragraph, $a^c \cdot a \leqslant x_{i+2}$. Since $a, c < x_i$, by diagonal indiscernibility we have $a^c \cdot a < x_{i+1}$, a contradiction.

So, $\mathcal{N}$ is closed under addition, multiplication, and exponentiation. Thus, $\mathcal{N}$ is a substructure of $\mathcal{M}$. As we noted above, all Δ_0 formulas are absolute between $\mathcal{N}$ and $\mathcal{M}$.

Suppose $\varphi(\vec{y}, w) = \forall z_1\ \exists z_2 \cdots \forall z_{2m-1}\ \exists z_{2m}\ \psi(\vec{y}, \vec{z})$, where ψ is Δ_0. By the diagonal indiscernibility of φ and its subformulas, we get that for all $x_{i_0} \in I$ and $\vec{a}, b < x_{i_0}$ that $\mathcal{N} \models \varphi(\vec{a}, b)$ iff

$$\forall z_1 < x_{i_1}\ \exists z_2 < x_{i_2}\ \cdots \forall z_{2m-1} < x_{i_{2m-1}}\ \exists z_{2m} < x_{i_{2m}}\ \psi(\vec{a}, b, \vec{z}) \tag{24}$$

whenever $i_0 < i_1 < \cdots < i_{2m}$. Suppose now that $\varphi(\vec{y}, w)$ is as above, $\vec{a} \in \mathcal{N}$ and $\mathcal{N} \models \exists w\ \varphi(\vec{a}, w)$. Let i_0 be such that $\vec{a}, < x_{i_0}$ and for some $b < x_{i_0}$ we have $\mathcal{N} \models \varphi(\vec{a}, b)$. Then for any $i_1 < \cdots < i_{2m}$ greater than i_0, and any $b < x_{i_0}$ we have $\mathcal{N} \models \varphi(\vec{a}, b)$ iff $\mathcal{M} \models \forall z_1 < x_{i_1} \cdots \exists z_{2m} < x_{i_{2m}}\ \psi(\vec{a}, b, \vec{z})$. since $\mathcal{M}$ satisfies PA, in $\mathcal{M}$ we can define the least $b < x_{i_0}$ such that (24) holds. That is, we have a least $b \in \mathcal{N}$ such that $\mathcal{N} \models \varphi(\vec{a}, b)$. This shows PA holds in $\mathcal{N}$. □

It now follows that the Paris-Harrington partition property is not provable in PA.

Theorem 7.22. *The Paris-Harrington partition property is not provable in PA.*

Proof. Suppose toward a contradiction that the Paris-Harrington partition property was a theorem of PA. Let $\mathcal{M}$ be a non-standard model of PA. Let $s \in \mathcal{M}$ be a non-standard element. From Theorem 7.18 in $\mathcal{M}$ with $k = m = n = s$, there is an $\ell > s$ such that $(*)$: if $F_1, \ldots, F_s$ are regressive functions on $(\ell)^s$, then there is min-homogeneous set $H \subseteq [s, \ell]$ for the F_i of size $\geqslant s$. Using PA in $\mathcal{M}$, let $\ell_0 > s$ be the least such ℓ in $\mathcal{M}$. From Theorem 7.20 in $\mathcal{M}$, there is a set $\{x_i\}_{i<s} \subseteq [s, \ell_0]$ of diagonal indiscernibles for the first s formulas $\{\varphi_j\}_{j<s}$, where $\varphi_j = \varphi_j(u_1, \ldots, u_s, v_1, \ldots, v_s)$. Since s is non-standard, $I = x_0 < x_1 < \cdots$ is an initial segment of $\{x_i\}_{i<s}$, and I is a set of diagonal indiscernibles for all the standard formulas φ. Let $\mathcal{N}$ be the initial segment of $\mathcal{M}$ determined by I. From Lemma 7.21, $\mathcal{N}$ is a model of PA. Note that $\ell_0 \notin \mathcal{M}$. However, since $\mathcal{N}$ models PA, which are are supposing proves the Paris-Harrington partition property, in $\mathcal{N}$ there is an ℓ_1 satisfying $(*)$. But $\ell_1 < \ell_0$, and ℓ_1 also satisfies $(*)$ in $\mathcal{M}$ (as $\mathcal{N}$ is closed under the coding of subsets of its integers, etc.). This contradicts the minimality of ℓ_0. □