COMPUTABILITY II
& GÖDEL'S INCOMPLETENESS THEOREMS

ARISTOTELIS PANAGIOTOPOULOS

Contents

Intro

In the beginning of the 20th century various paradoxes (Russell, Skolem, Fraenkel,..) resulted to a crisis in the foundations of mathematics. Hilbert put forward a new proposal for the foundation of mathematics which has come to be known as *Hilbert's Program*. In 1899 Hilbert had already published *Grundlagen der Geometrie* where he provided the first axiomatization of elementary geometry that was sufficient to prove all statements in Euclid's *Elements*, without any hidden assumptions. Hilbert's program wanted a similar formalization of all of mathematics in axiomatic form, together with a proof that this axiomatization of mathematics is consistent. During the second half of 1920s there was hope in some mathematical circles (see, International Congress of Mathematicians in Bologna, 1928) that they were really close in finding a complete and consistent axiomatizations for classical mathematical theories such as real analysis and arithmetic. By 1931 and due to Gödel we knew already that these beliefs were rooted in false optimism.

Consider for example the universe $\mathcal{N} = (\mathbb{N}, 0, \leq, +, *)$ of all natural numbers together with structure enough to allow us express (in first order logic) basic arithmetic properties, such as the fact that there are infinitely many prime numbers:

$$\forall x \exists p \forall a, b \; (x \leq p) \wedge \big((a * b = p) \implies ((a = p) \vee (b = p))\big)$$

To resolve successfully Hilbert's program for arithmetic one would need to find a collection $\mathcal{A}$ of statements (axioms) which are consistent and suffice in proving all statements which are true in $\mathcal{N}$. Gödel's 1st incompleteness theorem says that there is no "computable" such collection $\mathcal{A}$. It is usually stated as follows:

Theorem 1. *Let $\mathcal{A}$ be a collection of arithmetic statements so that*

(1) $\mathcal{A}$ is recursive;
(2) $\mathcal{A}$ is consistent, i.e., does not prove $\neg(0 = 0)$;
(3) $\mathcal{A}$ proves enough elementary arithmetic statements, e.g., all Robinson's axioms.

Then there is an arithmetic statement which can neither be proved nor disproved from $\mathcal{A}$.

This statement is actually a slight strengthening of the original Gödel's incompleteness theorem due to Rosser. The original weak statement replaces (2) by the following stronger assumption (to be explained later on)

(2') $\mathcal{A}$ is *ω-consistent.*

The even weaker statement which replaces both and (2) and (3) by the following is due to Tarski:

(4) $\mathcal{A}$ is *correct*, i.e., all statements provable from $\mathcal{A}$ are true in $(\mathbb{N}, 0, \leq, +, *)$.

It will be instructive to start by providing a short proof of Tarski's theorem. Later, after we develop more recursion-theoretic machinery we will prove Theorem 1 and provide more applications.

1. Incompleteness in a nutshell

Let $\mathbb{M}$ be some machine which prints out one after the other various expressions in the alphabet:

$$\neg \; P \; N \; (\;)$$

By an **expression** we mean any finite non empty string such as $(()PN)$. Any expression that is eventually going to be printed out of $\mathbb{M}$ we call it **printable**. Let X be some expression. The **norm** of X is the expression $X(X)$. For example, the norm of $((N$ is $((N(((N)$. A **sentence** is any expression of the following four forms

$$P(X), \quad PN(X), \quad \neg P(X), \quad \neg PN(X),$$

where X is any expression. We assign a truth value to all sentences. We say that $P(X)$ is true if X is printable. We say that $\neg P(X)$ is true if X is not printable. We say that $PN(X)$ is true if the norm of X is printable and we say that $\neg PN(X)$ is true if the norm of X is not printable.

Definition 2. We say that $\mathbb{M}$ is **correct** if every printable sentence is true. We say that $\mathbb{M}$ is **complete** if for every true sentence is printable.

Theorem 3. *There is no machine $\mathbb{M}$ that is both complete and correct.*

Proof. The idea is to find a sentence which asserts its own non-printability. For example consider the sentence $\neg PN(\neg PN)$...

□

Tarski's theorem

Here we derive a weak form of Gödel's incompletness theorem after establishing Tarski's "undefinability of truth" result. The syntax we are going to use in non-standard and is not going to be used anywhere else (except in HW1). The reason we use it is that it simplifies significantly some technical details and allows for a quick proof of Tarski's theorem. As in Section 1 we will define an alphabet and among the various expressions we are going to distinguish certain "well formed" ones which we are going to call sentences. We will then assign a truth-value to these sentences by interpreting them as statements about the natural numbers.

2. Alphabet

We will use an alphabet consisting of the following 13 symbols

$$0 \;\; ' \;\; (\;\;) \;\; p \;\; \oplus \;\; v \;\; \neg \;\; \Rightarrow \;\; \forall \;\; = \;\; \leq \;\; |$$

We are now going to introduce some abbreviations for certain expressions in the above alphabet. Of course, when working formally, all abbreviations should be replaced with the original expressions.

$0, 0', 0'', \ldots$ will be called **numerals** and we will abbreviate them by $\hat{0}, \hat{1}, \hat{2}, \ldots$.

$p, p_{\oplus}, p_{\oplus\oplus}$ will be abbreviated by $+, *, \mathrm{E}$

$(v_{\oplus}), (v_{\oplus\oplus}), (v_{\oplus\oplus\oplus}), \ldots$ will be called **variables** and will be abbreviated by $v_1, v_2, v_3, \ldots$

The last symbol | will be used only in the HW.

3. Terms and formulas

By a **term** we mean any expression that is included in the smallest collection of expressions which

(1) contains all numerals and variables;
(2) contains any expressions of the form $(t + s)$, $(t * s)$, (tEs), t' where s, t are themselves terms.

An **atomic formula** is any expression of the form $t = s$ or $t \leq s$, where s, t are any terms. By a **formula** we mean any expression that is included in the smallest collection of expressions which contains

(1) all atomic formulas;
(2) any expression of the form $\neg\varphi$ where φ is a formula;
(3) any expression of the form $(\varphi \implies \psi)$, where φ, ψ are formulas;
(4) any expression of the form $\forall v_n \varphi$, where v_n is a variable and φ is a formula.

4. Sentences

For any term t we can generate its syntactic tree in the obvious way. Leaves of this tree are either numerals or variables. Any leaf of the syntactic tree of t that is labeled by v_n is an **occurrence** of v_n in t. All occurrences of v_n in t are **free occurrences**. Similarly all occurrences of v_n in atomic formulas are free occurrences. Inductively the free occurrences of v_n in $(\varphi \implies \psi)$ are the free occurrences of v_n in φ and the free occurrences of v_n in ψ; the free occurrences of v_n in $\neg\varphi$ are the free occurrences of v_n in φ; v_n does not occur freely in $\forall v_n \varphi$; and free occurrences of v_n in $\forall v_m \varphi$ are those of φ, if $n \neq m$.

A **sentence** σ is any formula in which no variable occurs freely.

5. Assigning truth-values

So far everything took place on the syntactic level. Now we can use the natural numbers and the actual operations of successor, addition, multiplication, and exponentiation to give meaning to the well formed expressions.

A term t is called **closed** if no variable occurs free in t. To each closed term we **assign** a unique natural number as follows: to the numerals $\hat{0}, \hat{1}, \hat{2}, \ldots$ we assign the actual numbers $0, 1, 2, \ldots$; if n has been assigned to t and m has been assigned to s then we assign $n+1, n+m, n*m, n^m$ to the terms $t', (t+s), (t*s), (tEs)$ respectively.

Example. the term $((0'''p0')p_{\oplus}0'')'$ is assigned the number 9.

Let formula φ be a formula $\hat{m}$ is a numeral, we denote by $\varphi(\hat{m} \rightsquigarrow v_n)$ the formula attained by φ after we replace all free occurrences of v_n in φ by the numeral $\hat{m}$.

We define a sentence to be **true** inductively:

(1) $t = s$ is true if and only if t, s are closed the number assigned to t equals to the one assigned to s;
(2) $t \leq s$ is true if and only if t, s are closed the number assigned to t is less than or equal to the one assigned to s;

(3) $\neg\sigma$ is true if and only if σ is not true;
(4) $(\sigma \Rightarrow \tau)$ is true if and only if either σ is not true or both σ, τ are true;
(5) $\forall v_n \varphi$ is true if and only if for all numerals $\hat{m}$, we have that $\varphi(\hat{m} \rightsquigarrow v_n)$ is true.

6. Definable relations of numbers

Let R be a subset of $\mathbb{N}^k$ and φ be a formula whose free variables are $v_{n_1}, \ldots, v_{n_k}$. We say that φ **defines** R if for all $(m_1, \ldots, m_k) \in \mathbb{N}^k$ we have that

$$\varphi(\hat{m}_1 \rightsquigarrow v_{n_1}, \ldots, \hat{m}_k \rightsquigarrow v_{n_k}) \text{ is true} \iff (m_1, \ldots, m_k) \in R$$

The set of even numbers is definable for example by the formula

$$\neg\forall v_2 \neg(v_1 = 0'' p_{\oplus} v_2)$$

Later in this class we will study more the relationship between definable relations and recursive/recursively enumerable relations. We will see for example that if we dropped $p_{\oplus\oplus}$ from the alphabet, restricting this way our ability to refer directly to exponentiation, the definable sets would be the same. A function $f\colon \mathbb{N}^k \to \mathbb{N}$ is **definable** if its graph is definable as a relation.

7. Concatenation in base b

For every $b \geq 2$ we define a function $(m, n) \mapsto m \star_b n$ from $\mathbb{N}^2$ to $\mathbb{N}$ as follows: let $l_b(n)$ be the number of digits one needs to express n in base b notation and set

$$m \star_b n := m * b^{l_b(n)} + n$$

Informally $m \star_b n$ is the number whose base b expression is attained by concatenating the base b expression of m on the left of the base b expression of m.

Besides the usual base 10 we will also consider the $b = 13$ case. We will use the following primitive digits for expressing numbers in base 13 notation:

$$0 \;\; 1 \;\; 2 \;\; 3 \;\; 4 \;\; 5 \;\; 6 \;\; 7 \;\; 8 \;\; 9 \;\; \alpha \;\; \beta \;\; \gamma$$

Lemma 4. *The relation $x \star_b y = z$ is definable for every $b \geq 2$.*

Proof. Notice that $b^{l_b(n)}$ is simply the smallest power of b that is greater or equal to n. We will show that the relation consisting of all points of the form $(n, b^{l_b(n)})$ is definable.

The set of all numbers which are powers of b is definable by the formula $\mathrm{Pow}_b(x) = \exists y(x = (\hat{b}Ey))$, or more formally,... (left to the reader)

The collection of all pairs (x, y) with the property that y is the smallest power of b greater or equal to x is definable by the formula

$$s(x, y) = \mathrm{Pow}_b(y) \wedge (x \leq y) \wedge (\forall y((z < y) \wedge \mathrm{Pow}_b(z)) \Rightarrow (z < x)),$$

or more formally... But then $x \star_b y = z$ is definable by the formula

$$\exists a s(y, a) \wedge (z = ((x * a) + y)$$

□

Notice that if m, n, k are positive natural numbers then $(m \star_b n) \star_b k = m \star_b (n \star_b k)$. The same fails however when n is 0, e.g. $(3 \star_{10} 0) \star_{10} 1 = 310 \neq 31 = 3 \star_{10} (0 \star_{10} 1)$. Whenever we write $m \star_b n \star_b k$ from now on, it will be implicit that the parenthesis is on the left pair (this way we do not lose information).

Lemma 5. *The $(k+1)$-ary relation $x_1 \star_b x_2 \star_b \ldots \star_b x_k = y$ is definable.*

Proof. Exercise. □

8. Gödel-Quine numbering

Under the interpretation of our language on $\mathbb{N}$ we can can use formulas and sentences to talk about properties of numbers. Gödel's idea was to "coordinatize" the syntax using natural numbers and turn, this way, our language to implicitly talk about syntactic properties of the language as well as metamathematical properties of the interpretation we fixed. The setup we chose will allow us to chose a different "coordinatization" than Gödel's original one which will significantly simplify our proofs. This "coordinatization" is due to Quine.

To each expression E in the above fixed language we are going to assign a number. Since our alphabet has 13 symbols it will be convenient to express numbers in base $b = 13$ to simplify the coding. We will denote $m \star_{13} n$ simply by $m \star n$. Every symbol in out alphabet is assigned a number according to the following table.

0	$'$	(	)	p	$\oplus$	v	$\neg$	$\Rightarrow$	$\forall$	$=$	$\leq$	$\mid$
1	0	2	3	4	5	6	7	8	9	α	β	γ

Let $\mathcal{E}^-$ be the collection of all expressions which on the left do not end with $'$ then to each E in $\mathcal{E}^-$ we can assign the number whose representation in base 13 is the one attained by E if we replace every symbol with the corresponding digit in the above table. For example the expression $))0'|$ is assigned the number 3310γ (in base 13). We denote by E_n the expression that corresponds to the number n in the above coding.

Remark 6. We have:

(1) the map $n \mapsto E_n$ defines a bijection between $\mathbb{N}$ and $\mathcal{E}^-$;
(2) the numeral $\hat{m}$ is assigned the number 13^m (here we used base 10).
(3) If E_z is the expression we get if we concatenate E_x to the left of E_y, i.e., $E_z = E_x E_y$ then $z = x \star y$.

The only properties we will use about this coordinatization are summarized in the next corollary.

Corollary 7. *The following two relations are definable:*

(1) $\mathrm{Conc}(z, x, y) \subseteq \mathbb{N}^3$ *which states that z is the Gödel-Quine number of the expression $E_x E_y$.*

(2) $\mathrm{Numeral}(x, y)$ *which states that* E_y *is the numeral* $\hat{x}$.

Our task now is to see whether various syntactic and metamathematical properties generate definable relations under the Gödel-Quine coding. In particular consider consider the following subsets of $\mathbb{N}$:

(1) all natural numbers which correspond to sentences;
(2) all natural numbers which correspond to true sentences;
(3) all natural numbers which correspond to provable sentences.

So far we haven't defined what the last set is. This will be done in HW1. There you will prove that the first and last set is indeed definable. Regarding the second set we will see now that this is not the case.

9. Tarski's Theorem

Let $\#_{\mathcal{T}}$ be the collection of all natural numbers n for which the expression E_n is a true sentence. Assume moreover that we have established a proof system for arithmetic and we denote by $\#_{\mathcal{P}}$ the collection of all natural numbers n for which the expression E_n is a provable sentence. In this subsection we will prove the following Theorem due to Tarski.

Theorem 8 (Tarski)**.** *The set* $\#_{\mathcal{T}}$ *is not definable.*

Before we proceed to the proof of Tarski's theorem we point out that it immediately implies the following incompleteness theorem. We will later see that every recursive set is definable in the sense of this section.

Corollary 9 (Gödel-Tarski)**.** *If the proof system is correct and* $\#_{\mathcal{P}}$ *is definable then there exists a true but non-provable sentence.*

Non-constructive proof. For a constructive argument we the end of this section.

Correctness implies that $\#_{\mathcal{P}} \subseteq \#_{\mathcal{T}}$. But we also have $\#_{\mathcal{P}} \neq \#_{\mathcal{T}}$ since $\#_{\mathcal{P}}$ was assumed to be definable and $\#_{\mathcal{T}}$ is not. Hence we have $\#_{\mathcal{P}} \subsetneq \#_{\mathcal{T}}$ and therefore there is a sentence true but not provable. □

Let A be a subset of $\mathbb{N}$. A **Gödel sentence** σ for A is sentence with the property that

$$\sigma \text{ is true} \iff \mathrm{GQ}_{\#}(\sigma) \in A.$$

where $\mathrm{GQ}_{\#}(\sigma)$ stands for the Gödel-Quine number of σ. In other words σ can be thought as if it is stating $\mathrm{GQ}_{\#}(\sigma) \in A$. Most incompleteness arguments rely on cooking up some appropriate Gödel sentence. Gödel's method for constructing such sentences depended in showing that there is definable map $\mathrm{sub}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the property that if n is the Gödel number of a formula φ having v_1 as its only free variable then $\mathrm{sub}(m, n)$ is the Gödel number of the formula $\varphi(\hat{m} \rightsquigarrow v_1)$. Using a trick due to Tarski we can simplify Gödel original method in the context of the Gödel-Quine numbering.

Two formulas φ, ψ which have the exact same collection of free variables $v_{n_1}, \dots, v_{n_k}$ are called **equivalent** if for all numerals $\hat{m}_1, \dots \hat{m}_k$ we have that the sentence $\varphi(\hat{m}_1 \rightsquigarrow v_{n_1}, \dots, \hat{m}_k \rightsquigarrow v_{n_k})$ is true if and only if $\psi(\hat{m}_1 \rightsquigarrow v_{n_1}, \dots, \hat{m}_k \rightsquigarrow v_{n_k})$ is true. In particular, two sentences σ, τ are **equivalent** if σ is true if and only if τ is true. Let E now be an expression and let m be a natural number. We define a new expression, which we denote by $E[\hat{m}]$, by setting

$$E[\hat{m}] := \forall v_1(v_1 = \hat{m} \Rightarrow E)$$

Lemma 10. *If φ is a formula having v_1 as its only free variable then for every $m \in \mathbb{N}$ we have that $\varphi(\hat{m} \rightsquigarrow v_1)$ and $\varphi[\hat{m}]$ are equivalent.*

Proof. $\varphi[\hat{m}]$ is true iff
for every $n \in \mathbb{N}$ we have that $\hat{n} = \hat{m} \Rightarrow \varphi(\hat{n} \rightsquigarrow v_1))$ is true iff
for every $n \in \mathbb{N}$ we have that either $\neg \hat{n} = \hat{m}$ is true or $\varphi(\hat{n} \rightsquigarrow v_1))$ is true iff
$\varphi(\hat{m} \rightsquigarrow v_1))$ is true. □

Let now $\mathrm{sub}_{\mathrm{T}} \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the map that sends the pair (m, n) to the Gödel-Quine number of the expression $E_n[\hat{m}]$.

Lemma 11. *The map $\mathrm{sub}_{\mathrm{T}}$ is definable.*

Proof. We compute the Gödel-Quine number of $E_n[\hat{m}]$. Recall the correspondence (in base $b = 13$):

$\forall$	(	v	$\oplus$	)	(	(	v	$\oplus$	)	=		$\Rightarrow$		)
											$\hat{m}$		E_n	
9	2	6	5	3	2	2	6	5	3	α	$\mathrm{GQ}_{\#}(\hat{m})$	8	$\mathrm{GQ}_{\#}(E_n)$	3

But $\mathrm{GQ}_{\#}(E_n) = n$ and $\mathrm{GQ}_{\#}(\hat{m})$ is simply 13^m in base $b = 10$. Let c be the natural number which in base 13 its expression is 9265322653α and notice that

$$\mathrm{sub}_{\mathrm{T}}(m, n) = k \iff$$

$$\exists x(x = 13^m \wedge k = c \star_{13} x \star_{13} 8 \star_{13} n \star_{13} 3)$$

By Lemma 5 it is easy to see now that the relation $\mathrm{sub}_{\mathrm{T}}(m, n) = k$ is definable by turning the above to the corresponding formula (replace $\exists$ with $\neg\forall\neg$, replace m, n and k with variables v_1, v_2 and v_3, etc.) □

Let now $d \colon \mathbb{N} \to \mathbb{N}$ be the diagonal of $\mathrm{sub}_{\mathrm{T}}$. That is

$$d(n) = \mathrm{sub}_{\mathrm{T}}(n, n) = \mathrm{GQ}_{\#}(E_n[\hat{n}])$$

is the Gödel-Quine number of the expression $E_n[\hat{n}]$. For every $A \subseteq \mathbb{N}$ we set

$$d^{-1}(A) := \{m \in \mathbb{N} \colon d(m) \in A\}.$$

Lemma 12. *If the set $A \subseteq \mathbb{N}$ is definable then $d^{-1}(A)$ is definable.*

Proof. Notice that

$$m \in d^{-1}(A) \iff \exists y(d(m) = y \wedge y \in A).$$

□

Lemma 13. *If A is definable then there is a Gödel sentence for A.*

Proof. Let φ be a formula whose only free variable is v_1 and which defines $d^{-1}(A)$. Let n_φ be the Gödel-Quine number of φ. Consider the sentence $\varphi[\hat{n}_\varphi]$. We claim that this is a Gödel sentence for A. To see this notice that

$$\varphi[\hat{n}_\varphi] \text{ is true } \iff n_\varphi \in d^{-1}(A) \iff d(n_\varphi) \in A$$

But $d(n_\varphi)$ is the Gödel-Quine number of $\varphi[\hat{n}_\varphi]$. □

We can now finish the proof of Tarski's theorem.

Proof of Theorem 8. If the set $\#_{\mathcal{T}}$ of all Gödel-Quine numbers of true sentences was definable then the set $\#_{\mathcal{F}}$ of all Gödel-Quine numbers of false sentences, being the complement of $\#_{\mathcal{T}}$, would be definable as well. But then by the previous lemma we would have a Gödel sentence σ for $\#_{\mathcal{F}}$ which gives a contradiction because then

$$\sigma \text{ is true } \iff \mathrm{GQ}_{\#}(\sigma) \in \#_{\mathcal{F}} \iff \sigma \text{ is false}$$

where the first equivalence is because σ is the Gödel sentence of $\#_{\mathcal{F}}$, and the second equivalence is because of the definition of $\#_{\mathcal{F}}$. □

Using Lemma 12 we can provide a "constructive" proof of Corollary 9.

Another proof of Corollary 9. Since $\#_{\mathcal{P}}$ is definable then the set $(\#_{\mathcal{P}})^c$ of all Gödel-Quine numbers of sentences which are not provable is definable. By Lemma 12 we can find be a formula φ whose only free variable is v_1 and which defines $d^{-1}((\#_{\mathcal{P}})^c)$. Let n_φ be the Gödel-Quine number of φ. Consider the sentence $\varphi[\hat{n}_\varphi]$. We claim that $\varphi[\hat{n}_\varphi]$ is true but not provable. We have that

$$\varphi[\hat{n}] \text{ is true } \iff \varphi(\hat{n} \rightsquigarrow v_1) \text{ is true}$$

and since φ defines $d^{-1}((\#_{\mathcal{P}})^c)$ the latter is equivalent to $d(n_\varphi) \in (\#_{\mathcal{P}})^c$ which by the definition of d it is equivalent to $\varphi[\hat{n}]$ being not provable. To summarize, we just showed that

$$\varphi[\hat{n}] \text{ is true } \iff \varphi[\hat{n}] \text{ is not provable}$$

We now have to show that it is both true and not provable. But it this is not the case then $\varphi[\hat{n}]$ would be both not-true and provable which contradicts the fact that the proof system was assumed to be correct.

□

10. An abstract form of the argument

The previous argument is applicable in any setup where we can isolate the following structure:

(1) $\mathcal{E}$ is an enumerable set which we call *expressions*;
(2) $\mathcal{S} \subseteq \mathcal{E}$ which we call *sentences*;
(3) $\mathcal{P} \subseteq \mathcal{S}$ which we call *provable sentences*;
(4) $\Phi \subseteq \mathcal{E}$ which we call *formulas in one free variable*;

(5) a function $\mathcal{E} \times \mathbb{N} \to \mathcal{E}$ denoted by $(E, n) \mapsto E[n]$ so that $\varphi[n] \in \mathcal{S}$ whenever $\varphi \in \Phi$;
(6) $\mathcal{T} \subseteq \mathcal{S}$ which we call *true sentences*;

Notice that every

Let $A \subseteq \mathbb{N}$ and $\varphi \in \Phi$. We say that φ *defines* A if

$$n \in A \iff \varphi[n] \in \mathcal{T}.$$

Let $g\colon \mathcal{E} \to \mathbb{N}$ be an $1-1$ enumeration of the expressions and write E_n for the unique expression with $g(E_n) = n$. Let $d\colon \mathbb{N} \to \mathbb{N}$ be the map with $d(n) = g(E_n[n])$.

Theorem 14 (Abstract form of Gödel-Tarski)**.** *If $d^{-1}\big(g(\mathcal{S} \setminus \mathcal{P})\big)$ is definable and $\mathcal{P} \subseteq \mathcal{T}$ then $\mathcal{P} \neq \mathcal{T}$.*

Proof. Exercise. □

11. Discussion

We used the structure $(\mathbb{N}, 0, \leq, S, +, *, \mathrm{E})$

However, given $(\mathbb{N}, +, *)$ we can define $(\mathbb{N}, 0, S, +, *, \leq)$.

In fact we have enough strength to define E as well.

What about $(\mathbb{N}, 0, 1, +)$?

It is known as Presburger arithmetic and it admits complete and recursive axiomatization (no self-reference is possible).

Some more recursion theory

12. Oracles

Recall that the collection $\mathcal{R}$ of all recursive functions is the smallest collection of partial maps $f\colon \mathbb{N}^k \to \mathbb{N}, k \geq 0$ which contains

(1) the constant maps $c_0\colon \mathbb{N}^n \to \mathbb{N}$ with $(x_1, \ldots, x_n) \mapsto 0$;
(2) the successor map $S\colon \mathbb{N} \to \mathbb{N}$ with $x \mapsto x + 1$;
(3) the projections $\pi_j\colon \mathbb{N}^n \to \mathbb{N}$ with $(x_1, \ldots, x_n) \mapsto x_j$, where $j \leq n$;

and which is closed under the operations

(i) of composition: given $g\colon \mathbb{N}^n \to \mathbb{N}$ and $h_1, \ldots, h_n\colon \mathbb{N}^l \to \mathbb{N}$ in $\mathcal{R}$ then the map $f\colon \mathbb{N}^l \to \mathbb{N}$ is in $\mathcal{R}$, where

$$f(x_1, \ldots, x_l) = g(h_1(x_1, \ldots, x_l), \ldots, h_n(x_1, \ldots, x_l))$$

(ii) of primitive recursion: given $g\colon \mathbb{N}^n \to \mathbb{N}$ and $h\colon \mathbb{N}^{n+2} \to \mathbb{N}$ in $\mathcal{R}$, the map $f\colon : \mathbb{N}^{n+1} \to \mathbb{N}$ is in $\mathcal{R}$, where

$$f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n), \text{ and}$$

$$f(n+1, x_1, \ldots, x_n) = h(n, f(n, x_1, \ldots, x_n), x_1, \ldots, x_n).$$

(iii) of minimalization: given $g\colon \mathbb{N}^{n+1} \to \mathbb{N}$ in $\mathcal{R}$ then the map $f\colon \mathbb{N}^n \to \mathbb{N}$ is in $\mathcal{R}$, where

$$f(\bar{x}) = \mu y[g(y, \bar{x}) = 0],$$

where $f(\bar{x}) \downarrow$ iff there is y so that $g(y, \bar{x}) = 0$ and for all $z < y$ we have that $g(z, \bar{x}) \downarrow$.

Definition 15. An **oracle** is any total map $\alpha\colon \mathbb{N} \to \mathbb{N}$.

Let $F_1, \ldots, F_n$ be any total functions with $F_i\colon \mathbb{N}^{n_i} \to \mathbb{N}$. We say that a partial map f is **recursive in** $F_1, \ldots, F_n$ and we write $f \in \mathcal{R}(F_1, \ldots, F_n)$ if f is in the smallest collection defined as $\mathcal{R}$ is defined above but which together with the maps in (1),(2), (3) it additionally contains $F_1, \ldots, F_n$. The interesting case is of course when $F_i \notin \mathcal{R}$.

Lemma 16. *For any $F_1, \ldots, F_n$ as above there is some unary $\alpha\colon \mathbb{N} \to \mathbb{N}$ so that*

$$\mathcal{R}(F_1, \ldots, F_n) = \mathcal{R}(\alpha).$$

Reminder. We have a primitive recursive $\langle \_ \rangle\colon \bigcup_{n \geq 0} \mathbb{N}^n \to \mathbb{N}$ which codes all finite sequences with natural numbers $\langle \emptyset \rangle = 0$, and if p_i is the i-th prime (with $p_0 = 2$) we have

$$\langle (n_0, \ldots, n_k) \rangle = \Pi_{i=0}^{k} p_i^{n_0+1}.$$

Recall that the subset $\mathrm{Seq}(s)$ of $\mathbb{N}$ consisting of all numbers numbers s which are in the range of $\langle \_ \rangle$ is primitive recursive. We have a primitive recursive decoding function $(s)_i$ where if $\mathrm{Seq}(s)$ and n_i+1 is the exponent of p_i in the above factorization then $(s)_i = n_i$ and in all other cases $(s)_i = 0$.

If we want to code/decode $\mathbb{N}^k$ with $\mathbb{N}$, for a fixed k, there are "direct" and bijective primitive recursive ways of doing so.

Proof of Lemma 16. We can assume without loss of generality that every $F = F_i$ is unary by replacing $F\colon \mathbb{N}^k \to \mathbb{N}$ with $\overline{F}\colon \mathbb{N} \to \mathbb{N}$ with

$$\overline{F}(s) = F((s)_0, \ldots, (s)_{k-1})$$

Given now unary $\overline{F}_1, \ldots \overline{F}_n$, we can code them in one map $\alpha\colon \mathbb{N} \to \mathbb{N}$ with

$$\alpha(n) = \langle \overline{F}_1(n), \ldots \overline{F}_n(n) \rangle$$

□

Given $\alpha\colon \mathbb{N} \to \mathbb{N}$ we denote by $\overline{\alpha}$ the map $\mathbb{N} \to \mathbb{N}$ given by

$$\overline{\alpha}(n) = \langle \alpha(0), \ldots, \alpha(n-1) \rangle.$$

Notice that $\overline{\alpha}(n)$ is primitive recursive $\overline{\alpha}(n+1) = \langle \overline{\alpha}(n) * \langle \alpha(n) \rangle \rangle$ where recall that

$$s * t = \langle n_0, \ldots, n_k, m_0, \ldots, m_l \rangle, \quad \text{if } s = \langle n_0, \ldots, n_k \rangle, t = \langle m_0, \ldots, m_l \rangle,$$

and $s * t = 0$ otherwise.

Lemma 17. *A partial k-ary map f is recursive in α if and only if there is a primitive recursive relation $P \subseteq \mathbb{N}^{k+2}$ so that:*

$$f(\bar{x}) = y \iff \exists n P(\bar{x}, y, \overline{\alpha}(n)).$$

Proof. $\Leftarrow$ Assume that f is a partial k-ary map whose graph is defined by some primitive recursive P as above. Then

$$f(\bar{x}) = \big(\mu s[P\big(\bar{x}, (s)_0, \overline{\alpha}((s)_1)\big)]\big)_0$$

$\Rightarrow$

Notice that we can recover n and $\alpha(n)$ from $\overline{\alpha}(n)$ using primitive recursive functions:

(i) $n = \text{length}(\overline{\alpha}(n))$

(ii) $\alpha(n) = y$ iff $\exists z \leq \overline{\alpha}(n)$ $(\text{length}(\overline{\alpha}(z)) = n + 1 \ \wedge \ y = (\overline{\alpha}(z))_n)$.

Step 1. Check that all maps $(1), (2), (3)$ are of this form.

Step 2. To check composition we can assume for simplicity that $f(x) = g(h(x))$. Inductively we assume that $h(x) = y \iff \exists n P(x, y, \overline{\alpha}(n))$ and $g(y) = z \iff \exists m P'(y, z, \overline{\alpha}(m))$ but then

$$\begin{aligned} f(x) = z &\iff \exists y\big(h(x) = y \wedge g(y) = z\big) \iff \\ &\iff \exists y\big(\exists n P(x, y, \overline{\alpha}(n)) \wedge \exists m P'(y, z, \overline{\alpha}(m))\big) \\ &\iff \exists y \exists n \exists m\big(P(x, y, \overline{\alpha}(n)) \wedge P'(y, z, \overline{\alpha}(m))\big) \\ \iff \exists s(s = \langle y, n, m\rangle)&\big(P(x, (s)_0, \overline{\alpha}((s)_1)) \wedge P'((s)_0, z, \overline{\alpha}((s)_2))\big) \end{aligned}$$

It is not difficult to see that the last expression can be brought in the form $\exists s \, Q(x, z, \overline{\alpha}(s))$ where Q is a primitive recursive relation. For example one has to find a primitive recursive function $p\colon \mathbb{N} \to \mathbb{N}$ with the property that $p(\overline{\alpha}(s)) = \overline{\alpha}((s)_2)$. for every function $\alpha\colon \mathbb{N} \to \mathbb{N}$. For that use (i), (ii) above.

Step 3. Primitive recursion left as exercise.

Step 4. To check minimalization we can assume again without loss of generality that $f(x) = \mu t[g(x, t) = 0]$ and that $g(x, t) = y \iff \exists n P(x, t, y, \overline{\alpha}(n))$ with P primitive recursive. But then

$$\begin{aligned} f(x) = y &\iff \big(g(x, y) = 0 \wedge (\forall z < y \ g(x, z) > 0)\big) \\ &\iff \exists n P(x, y, 0, \overline{\alpha}(n)) \wedge \big(\forall z < y \exists w(w > 0 \wedge \exists m \ P(x, y, w, \overline{\alpha}(m)))\big) \\ \iff \exists n P(x, y, 0, \overline{\alpha}(n)) &\wedge \exists w \exists m\big(\forall z < y((w)_z > 0 \wedge \ P(x, y, (w)_z, \overline{\alpha}((m)_z)))\big) \\ &\iff \exists l = \langle n, w, m\rangle (\text{Primitive Recursive Stuff}) \end{aligned}$$

□

Recall that if $A \subseteq \mathbb{N}^n$ then we can "identify" A with its characteristic function χ_A. Recall also that the convention is that $\chi_A(\overline{x}) = 0$ if and only if $\overline{x} \in A$.

Theorem 18 (Kleene's normal form relative to α)**.** *There is a total, primitive recursive function $U\colon \mathbb{N}\to\mathbb{N}$ and a primitive recursive relation $T\subseteq\mathbb{N}^3$ so that that for each total unary function α, every k-ary partial recursive function with respect to α has the form*

$$U\big(\mu n\left[T(e,\langle x_1,\dots,x_k\rangle,\overline{\alpha}(n))\right]\big),\quad \textit{for some } e.$$

Proof. Recall that there exists a primitive recursive relation $\widehat{T}\subseteq\mathbb{N}$ so that the relation

$$\exists m\widehat{T}(e,\langle x_1,\dots,x_k\rangle,m)$$

is universal for recursively enumerable relations, i.e., for every recursively enumerable $R(x_1,\dots,x_k)$ there is e so that R equals the above relation for this fixed e.

Let now $f\colon\mathbb{N}^k\to\mathbb{N}$ be partial recursive with respect to α. By the previous lemma we have primitive recursive relation P so that:

$$f(\bar{x})=y \iff \exists n P(\bar{x},y,\overline{\alpha}(n)).$$

Hence for some e we have that

$$\begin{aligned} f(\bar{x})=y &\iff \exists n\exists m\widehat{T}(e,\langle x_1,\dots,x_k,y,\overline{\alpha}(n)\rangle,m)\\ &\iff \exists l\ \widehat{T}(e,\big\langle x_1,\dots,x_k,y,\overline{\alpha}((l)_0)\big\rangle,(l)_1)\\ &\iff \exists l\ \widetilde{T}(e,\big\langle x_1,\dots,x_k,y,\overline{\alpha}(l)\big\rangle), \end{aligned}$$

where $\widetilde{T}(e,\big\langle x_1,\dots,x_k,y,u\big\rangle):=\widehat{T}(e,\big\langle x_1,\dots,x_k,y,p(u)\big\rangle,q(u))$, and p,q are the obvious primitive recursive functions. Thus

$$\begin{aligned} f(x_1,\dots,x_k)&=\big(\mu\, n\,[\widetilde{T}(e,\big\langle x_1,\dots,x_k,(n)_0,\overline{\alpha}((n)_1)\big\rangle)]\big)_0=\\ &=U\big(\mu\, n\,[T(e,\big\langle x_1,\dots,x_k,\overline{\alpha}(n)\big\rangle)]\big), \end{aligned}$$

where $U(z)=(z)_0$ and $T(e,\big\langle x_1,\dots,x_k,z\big\rangle)=\widetilde{T}(e,\big\langle x_1,\dots,x_k,r(z),s(z)\big\rangle)$, for the obvious primitive recursive maps r,s. □

Corollary 19 (Kleene's enumeration theorem.)**.** *For every α, the class $\mathcal{R}(\alpha)$ of partial recursive maps with respect to α has the enumeration property.*

Proof. By Kleene's Theorem the map $\varphi_k^\alpha\colon\mathbb{N}^{k+1}\to\mathbb{N}$ with $\varphi_k^\alpha(e,x_1,\dots,x_k)=U\big(\mu n\left[T(e,\langle x_1,\dots,x_k\rangle,\overline{\alpha}(n))\right]\big)$ is in $\mathcal{R}_{k+1}(\alpha)$ and it is universal for $\mathcal{R}_k(\alpha)$. □

A relation $R(\bar{x})$ is **recursive in** α if its characteristic function is. It is **recursively enumerable in** α if there is some recursive in α relation $P(n,\bar{x})$ so that $R(\bar{x})=\exists n\, P(n,\bar{x})$.

Everything that was proved in Math117a about recursively enumerable relations has a relative to α version. In particular:

Theorem 20. *There is a primitive recursive relation $T(e,x,u)$ so that for all α and all $P \subseteq \mathbb{N}$ we have that P is recursively enumerable in α if and only if there is $e \in \mathbb{N}$ so that*

$$P(x) \iff \exists n T(e,x,\overline{\alpha}(n)).$$

13. Turing degrees

For $\alpha, \beta \colon \mathbb{N} \to \mathbb{N}$ total maps we say that $\alpha \leq_T \beta$ if and only if α is recursive in β, i.e. $\{\text{rec in } \alpha\} \subseteq \{\text{rec in } \beta\}$

Think that β is a stronger oracle (knows more) than α.

$\alpha \leq_T \alpha$

$\alpha \leq_T \beta$ and $\beta \leq_T \gamma$ implies $\alpha \leq_T \gamma$.

$\alpha \equiv_T \beta$ iff $\alpha \leq_T \beta$ and $\beta \leq_T \alpha$

The equivalence class $[\alpha]_T = \{\beta \colon \alpha \equiv_T \beta\}$ of α under $\equiv_T$ is the **Turing degree** of α.

The collection $\mathcal{D} = \{[\alpha]_T \colon \alpha \in \mathbb{N}^{\mathbb{N}}\}$ of all Turing degrees forms a partial ordering under $\leq_T$.

We will now provide an alternative description of $\leq_T$. We first need to fix some notation.

$\mathbb{N}^{<\mathbb{N}} = \{s \colon \mathbb{N} \to \mathbb{N} \mid \mathrm{dom}(s) = \{0, \ldots, n-1\}, n \in \mathbb{N}\}$. We write $s = (s_0, \ldots, s_{n-1})$ for any element $s \in \mathbb{N}^{<\mathbb{N}}$, so that $s_i \in \mathbb{N}$. We also denote by $|s|$ the length of s which in the above case is n. We write $s \subseteq t$ if $t = (t_0, \ldots, t_{n-1})$ **extends** $s = (s_0, \ldots, s_{m-1})$, i.e., if $t_i = s_i$ for all $i \leq m-1$. If $k \leq |s|$ then we write $s|k$ for $(s_0, \ldots, s_{k-1})$. We extend this notation to elements α of $\mathbb{N}^{\mathbb{N}}$, in the obvious way, so that $\alpha|k \in \mathbb{N}^k$. Notice that $\mathbb{N}^{<\mathbb{N}} = \bigcup_n \mathbb{N}^n$ has a natural tree structure under $\subseteq$ where each $\mathbb{N}^n$ is a "horizontal level."

Definition 21. A (total) map $\varphi \colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ is called monotone if

$$s \subseteq t \implies \varphi(s) \subseteq \varphi(t).$$

Given any such monotone map, we define a partial map $\varphi^* \colon \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ by

$$\varphi^*(\alpha) = \bigcup_n \varphi(\alpha|n),$$

whenever the length $|\varphi(\alpha|n)|$ grows to infinity. Write $\varphi^*(\alpha) \downarrow$ if and only if $\forall m \exists n |\varphi(\alpha|n)| > m$.

Definition 22. We say that φ is computable if $\overline{\varphi} \colon \langle s \rangle \mapsto \langle \varphi(s) \rangle$ is computable.

Theorem 23. *Let α, β be two oracles. Then $\alpha \leq_T \beta$ if and only if there is a computable monotone $\varphi \colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ so that $\varphi^*(\beta) = \alpha$.*

Proof. ($\Leftarrow$). Let $\varphi \colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ be computable so that $\varphi^*(\beta) = \alpha$. We have that

$$\alpha(k) = \varphi(\beta|l)\big)(k), \quad \text{where} \quad l = \mu\, n[|\varphi(\beta|n)| > k]$$

In other words, recalling the notation $\overline{\beta}(n) = \langle \beta | n \rangle = \langle \beta(0), \beta(1), \dots, \beta(n-1) \rangle$, we have that

$$\alpha(k) = \left(\overline{\varphi}\big(\overline{\beta}(\,\mu\, n \big[\text{lenght}(\overline{\varphi}(\overline{\beta}(n))) > k \big]\,)\big) \right)_k$$

($\Rightarrow$). Assume that $\alpha \leq_T \beta$. Then by Theorem 18 there are primitive recursive U, R so that for some fixed e we have

$$\alpha(k) = U(\mu n \big[R(e, k, \overline{\beta}(n)) \big]).$$

We will find now some $\varphi = \varphi_e$ so that $\varphi^*(\beta) = \alpha$.

To compute $\varphi(s)$ the rough idea is to plug $\langle s | n \rangle \in \mathcal{N}^{<\mathbb{N}}$ in the place of $\overline{\beta}(n)$. Of course even when $k << |s|$ there is no guarantee that there is some $n > 0$ so that $R(e, k, \langle s | n \rangle) = 0$. To accommodate for this problem in a way that will not ruin monotonicity or $\varphi^*(\beta) = \alpha$ we will modify things as follows. First given s we will predetermine the length of $|\varphi(s)|$ by defining the following function:

$$\text{length}^{\varphi}(s) = \mu\, l \left[(l < |s|) \wedge \big(\forall k \leq l \, \exists n < |s| \, R(e, k, \langle s | n \rangle) = 0 \big) \right]$$

We will now send s to a sequence $\varphi(s)$ with $|\varphi(s)| = \text{length}^{\varphi}(s)$ so that for all $k < \text{length}^{\varphi}(s)$ we have

$$\varphi(s)(k) = U(\mu n \leq |s| \big[R(e, k, \langle s | n \rangle) \big]).$$

It is left to the reader to confirm that φ is monotone computable and $\varphi^*(\beta) = \alpha$. $\square$

A consequence of the above proof is that we have a sequence $\varphi_0, \dots, \varphi_e, \dots$ of recursive monotone maps so that

$$\alpha \leq_T \beta \iff \exists e (\varphi_e^*(\beta) = \alpha)$$

In fact it is not difficult to see that this is a "uniformly recursive" family, i.e., the map $\varphi(e, s) = \varphi_e(s)$ is recursive!

Theorem 24. *$(\mathcal{D}, \leq_T)$ is not a total order, i.e., there are α, β so that neither $\alpha \leq_T \beta$, nor $\beta \leq_T \alpha$.*

Proof. We will construct α, β as the limits of the respective sequences $s^n, t^n \in \mathbb{N}^{<\mathbb{N}}$. For every n we will make sure that $|s^n| = |t^n| = l_n$ with l_n strictly increasing and so that $s^n \subseteq s^{n+1}, t^n \subseteq t^{n+1}$. At the end we set $\alpha = \bigcup_n s^n$ and $\beta = \bigcup_n t^n$.

At the n-th stage we will make sure that s^n, t^n are selected so that if $n = 2e + 1$ then any extension of s^n to some α is not in the image of any extension β of t^n under φ_e^*. If $n = 2e$ we will make sure that any extension of t^n to some β is not in the image of any extension α of s_n under φ_e^*.

Set $s^{-1} = t^{-1} = \emptyset$ and $l_{-1} = 0$. Assume now that for $n \geq 0$ we have defined $s^{n-1}, t^{n-1}, l_{n-1}$. We define s^n, t^n, l_n.

Case $n = 2e$. We will make sure that $\varphi_e^*(\alpha) \neq \beta$.

Subcase 1. If for every s that extends s^{n-1} we have that $\varphi_e(s)$ does not strictly extend t^{n-1}, then let s^n and t^n be any strict extensions of s^{n-1} and t^{n-1} of equal

length and set $l_n = |s^n|$. Any α, β extending s^n, t^n will have the property that $\varphi_e^*(\alpha)|l_n \neq t^n = \beta|l_n$.

Subcase 2. If there is some s extends s^{n-1} so that $\varphi_e(s)$ also strictly extends t^{n-1} then set $s^n = s$, $l_n = |s^n|$ and pick t^n be any extension of t^{n-1} with $|t^n| = l_n$ so that $t^n_{l_{n-1}} \neq \big(\varphi_e(s^n)\big)_{l_{n-1}}$. Again this guarantees that any α, β extending s^n, t^n will have the property that $\varphi_e^*(\alpha)|l_n \neq t^n = \beta|l_n$.

Case $n = 2e + 1$. We do the same thing with the roles of α and β exchanged so that $\varphi_e^*(\beta) \neq \alpha$, for any α, β extending s^n, t^n. □

Here are some properties of the poset $(\mathcal{D}, \leq_T)$.

- There is a smallest element which we denote by $\underset{\sim}{0}$ and which consists of all recursive oracles.
- For every $\underset{\sim}{a}, \underset{\sim}{b}$ there is a least upper bound $\underset{\sim}{a} \vee \underset{\sim}{b}$ which we attain by picking representatives α, β with $[\alpha]_T = \underset{\sim}{a}, [\beta]_T = \underset{\sim}{b}$ and setting
$$\underset{\sim}{a} \vee \underset{\sim}{b} = [n \mapsto \langle \alpha(n), \beta(n) \rangle].$$
- For every $\underset{\sim}{a}$ there are only countably many $\underset{\sim}{b}$ with $\underset{\sim}{b} \leq_T \underset{\sim}{a}$. To see this notice that we have countably many reductions (e.g. $(\varphi_e)_e$ in previous Theorem).
- As a consequence the set $\{\underset{\sim}{b} \colon \underset{\sim}{b} \geq_T \underset{\sim}{a}\}$, known as the cone above $\underset{\sim}{a}$, is uncountable for every $\underset{\sim}{a}$.
- If $(\underset{\sim}{a}_n)$ is any sequence of Turing degrees then there is some $\underset{\sim}{a}$ above all of them. Simply let α_n with $[\alpha_n]_T = \underset{\sim}{a}_n$ and set $\underset{\sim}{a} = [\alpha]_T$, where $\alpha(\langle n, m \rangle) = \alpha_n(m)$.
- For every $\underset{\sim}{a}$ there is a $A \subseteq \mathbb{N}$ so that $\underset{\sim}{a} = [\chi_A]_T$.

This last property allows us to think of oracles as subsets of $\mathbb{N}$, or equivalently, points in the Cantor space $2^{\mathbb{N}}$. Given this we have a somewhat canonical Turing degree above $\underset{\sim}{0}$: the degree corresponding to the set $H \subseteq \mathbb{N}$ coding the halting problem
$$H(e) \iff \exists n T(e, e, n).$$
The denote $[\chi_H]$ by $\underset{\sim}{0}'$ and we call it the **Turing jump** of $\underset{\sim}{0}$. In fact $\underset{\sim}{a} \mapsto \underset{\sim}{a}'$ is a well defined operation uniformly on $(\mathcal{D}, \leq_T)$.

14. Reductions and Turing jump

Let $A, B \subseteq \mathbb{N}$. We say that that A is **reducible** to B if there is a computable and total map $f \colon \mathbb{N} \to \mathbb{N}$ so that
$$n \in A \iff f(n) \in B.$$
In other words, $f^{-1}(B) = A$, equivalently $\chi_A = \chi_B \circ f$. We write $A \leq_R B$. Such reductions are often called **many to one reductions** since we do not demand injectivity of f. It is immediate that $\leq_R$ refines $\leq_T$ in that:
$$A \leq_R B \implies A \leq_T B.$$

The converse is false since, for example the complement $H^c \subseteq \mathbb{N}$ of the halting problem H does not reduce to H since this would make H^c recursively enumerable and this would imply that H is recursive.

Let $\mathcal{C}$ be a collection of subsets of $\mathbb{N}$ and $B \subseteq \mathbb{N}$. Say that B is **$\mathcal{C}$-complete** if:

(1) $B \in \mathcal{C}$;
(2) for every $A \in \mathcal{C}$ we have that $A \leq_R B$.

Theorem 25. *For every $\alpha \in \mathbb{N}^{\mathbb{N}}$ and let $\mathcal{RE}(\alpha)$ be the collection of all subsets of $\mathbb{N}$ which are recursively enumerable with respect to α. Then there is some $\mathcal{RE}(\alpha)$-complete set.*

Proof. Let $T(e, x, u)$ be the primitive recursive set from Theorem 20 with the property that A is recursively enumerable in α if and only if there is $e \in \mathbb{N}$ so that

$$x \in A \iff \exists l \, T(e, x, \overline{\alpha}(l)),$$

and set

$$B = \{\langle m, n\rangle \mid \exists l \, T(m, n, \overline{\alpha}(l))\}$$

If $A \in \mathcal{C}$ then there is e_A so that $A = \{n \mid \langle e_A, n\rangle \in B\}$, and therefore the map $n \mapsto \langle e_A, n\rangle$ is the desired reduction. □

Definition 26. For every $\underset{\sim}{a}$ we define the **Turing jump** $\underset{\sim}{a}'$ to be the degree $[A]_T$ where A is any $\mathcal{RE}(\alpha)$-complete set, for some $\alpha \in \underset{\sim}{a}$.

Notice that:

- the definition does not depend on the choice of A since for every two $\mathcal{RE}(\alpha)$-complete sets A, A' we have that $A \leq_R A'$ and $A' \leq_R A$;
- $\underset{\sim}{a}'$ is strictly above $\underset{\sim}{a}$ since otherwise $H^c_\alpha(n) = \neg\exists l \, T(n, n, \overline{\alpha}(l))$ would be in $\mathcal{R}(\alpha)$ (since it is closed under complements) in particular, by the universality of T there would be e so that $H^c_\alpha(n) = \exists l \, T(e, n, \overline{\alpha}(l))$ for all n. But for $n = e$ this gives a contradiction.

We have:

$$\underset{\sim}{a} < \underset{\sim}{a}' < \underset{\sim}{a}'' < \dots$$

Let $[\underset{\sim}{0} < \underset{\sim}{0}']$ stand for the subposet of $(\mathcal{D}, \leq_T)$ consisting of all degrees which are between $\underset{\sim}{0}$ and $\underset{\sim}{0}'$. How complicated this is?

By a famous result there are incomparable Turing degrees $[\chi_A]_T, [\chi_B]_T$ so that both sets A, B are recursively enumerable. In fact the unique countable atomless Boolean algebra embeds in the r.e. part of this interval.

15. The arithmetic hierarchy

Set

$$\begin{aligned}\text{Recursively enumerable sets} &\iff \Sigma^0_1\\ \text{co-Recursively enumerable sets} &\iff \Pi^0_1\\ \text{Recursive sets} &\iff \Sigma^0_1 \cap \Pi^0_1 \iff \Delta^0_1\end{aligned}$$

Notice that the Σ class above is closed under $\exists$-quantification, Π is closed under $\forall$-quantification and Δ is closed under complement. Next:

$$\begin{aligned}\Sigma^0_2 &= \{\exists n P(\bar{x}, n) \mid P \in \Pi^0_1\}\\ \Pi^0_2 &= \{P^c \mid P \in \Sigma^0_2\}\\ \Delta^0_2 &= \Pi^0_2 \cap \Sigma^0_2\end{aligned}$$

Of course we can keep on going by setting:

$$\begin{aligned}\Sigma^0_{n+1} &= \exists \Pi^0_n\\ \Pi^0_{n+1} &= \neg \Sigma^0_{n+1}\\ \Delta^0_2 &= \Pi^0_{n+1} \cap \Sigma^0_{n+1}\end{aligned}$$

Remark. An easy induction shows that:

$$\Pi^0_n \cup \Sigma^0_n \subseteq \Delta^0_{n+1} = \Pi^0_{n+1} \cap \Sigma^0_{n+1},$$

(for the inductive step show separately that $\Sigma^0_n \subseteq \Sigma^0_{n+1}$ and $\Pi^0_n \subseteq \Sigma^0_{n+1}$)

Before we connect this notions with the Turing degree complexity we point out that definable relation from Section 1 check out to be the same as

$$\bigcup_n \Sigma^0_n = \bigcup_n \Pi^0_n = \bigcup \Delta^0_n,$$

where the equality of these three follows from the previous remark. We will develop this point of view in the next few weeks, replacing the word "definable " from now on with the standard term "**arithmetic**".

Proposition 27. *Here are some more properties:*

1. *Σ^0_n is closed under $\wedge, \vee$, bounded quantification, substitution by total recursive functions, and by $\exists$-quantification;*
2. *Π^0_n is closed under $\wedge, \vee$, bounded quantification, substitution by total recursive functions, and by $\forall$-quantification;*
3. *Δ^0_n is closed under $\neg\wedge, \vee$, bounded quantification, and substitution by total recursive functions*

Proof. Run induction on n. For $n = 1$ we have established all these properties in math117a. Assume we have these properties for n we show them for $n+1$. In fact it suffice to show (1) since the rest follow easily by it. This is easy. For example assume that

$$R_1(\bar{x}) = \exists n P_1(n, \bar{x}), \quad R_2(\bar{x}) = \exists m P_2(m, \bar{x}),$$

where $P_1, P_2 \in \Pi^0_n$. Then by inductive assumption $P(m, n, \bar{x}) = P_1(n, \bar{x}) \wedge P_2(m, \bar{x}) \in \Pi^0_n$ and therefore $R_1 \wedge R_2 \in \Sigma^0_{n+1}$ since

$$(R_1 \wedge R_2)(\bar{x}) = \exists w P((w)_0, (w)_1), \bar{x})$$

The rest follow similarly and are left to the reader. □

Proposition 28. *Σ^0_n and Π^0_n have the enumeration property while Δ^0_n does not.*

Proof. For Σ^0_n and Π^0_n use again induction. We know it for $n = 1$. Consider Σ^0_{n+1}. For every k we want to find

$$W^{k+1}(e, x_1, \ldots, x_k) \in \Sigma^0_{n+1}$$

that is universal for k-ary Σ^0_{n+1} relations. By inductive assumption find in Π^0_n is a universal relation $U^{k+2}(e, y, x_1, \ldots, x_k)$ for Π^0_n relations and set

$$W^{k+1}(e, x_1, \ldots, x_k) := \exists y U^{k+2}(e, y, x_1, \ldots, x_k).$$

Then W^{k+1} is clearly Σ^0_{n+1} and universal since if $R \in \Sigma^0_{n+1}$ is k-ary then

$$R(\bar{x}) \iff \exists y Q(y, \bar{x}) \iff \exists y U^{k+2}(e, y, x_1, \ldots, x_k), \text{ for some } e.$$

The Δ^0_n-case is an exercise. □

Corollary 29. *(Exercise) We have that:*

- *Σ^0_n and Π^0_n are not closed under complements;*
- *Σ^0_n is not closed under $\forall$-quantification;*
- *Π^0_n in not closed under $\exists$-quantification;*
- *$\Pi^0_n \cup \Sigma^0_n \subsetneq \Delta^0_{n+1}$, $\Delta^0_{n+1} \subsetneq \Sigma^0_{n+1}$, and $\Delta^0_{n+1} \subsetneq \Pi^0_{n+1}$.*

Example 30. Let $\{\varphi_e\}$ be an effective and acceptable enumeration of recursive functions. Let $C = \{e \mid \varphi_e \text{ is total}\}$. What is the complexity of C?

By effectiveness we have that $C = \{e \mid \forall x \exists y \, \varphi(e, x) = y\}$. So it is at most Π^0_2. Could it be below that? The answer is NO. It cannot be Σ^0_2. In fact it is Π^0_2-complete. To see this let A be an arbitrary Π^0_2 subset of $\mathbb{N}$ and show that $A \leq_R C$:

$$x \in A \iff \forall y B(x, y) \iff \forall y f(x, y) \downarrow$$

for some $B \in \Sigma^0_1$ or equivalently for some partial recursive f. Therefore there exists e so that

$$x \in A \iff \forall y(\varphi(e, x, y) \downarrow) \iff \forall y\big(\varphi(S(e, x), y) \downarrow\big)$$

As a consequence we have that $x \mapsto S(e, x)$ is a reduction from A to C.

16. Post's Theorem

Post's theorem provides a bridge between the arithmetic hierarchy and the Turing jump operation $\underset{\sim}{a} \mapsto \underset{\sim}{a}'$ when $\underset{\sim}{a}$ is of the form

$$\underset{\sim}{0}^{(n)} := \underset{\sim}{0}^{'\cdots'} \quad n\text{-many times}$$

Theorem 31 (Post's theorem)**.** *Let C_n be any Σ^0_n-complete set. We have that:*

(1) $R \subseteq \mathbb{N}^k$ is recursively enumerable in C_n if and only if $R \in \Sigma^0_{n+1}$;
(2) $R \subseteq \mathbb{N}^k$ is recursive in C_n if and only if $R \in \Delta^0_{n+1}$;

Proof. Part (2) follows from part (1) since R being recursive relative to some C is the same as both R and R^c being recursively enumerable with respect to C.

Assume now that $R \in \Sigma^0_{n+1}$ then $R(\bar{x}) = \exists y P(y, \bar{x})$ with $P \in \Pi^0_n$. But then $P^c \leq_R C_n$, where P^c is viewed as a subset of $\mathbb{N}$ via $\bar{x} \mapsto \langle \bar{x} \rangle$. But then $P^c \leq_T C_n$ which implies $P \leq_T C_n$.

Conversely if R is in $\mathcal{RE}(C_n)$ then let α be the characteristic function of C_n and by Kleene's normal form we have for some e and some primitive recursive T that:

$$R(\bar{x}) \iff \exists m\, T(e, \bar{x}, \overline{\alpha}(m)) \iff \exists n \big(\mathrm{Seq}(n) \wedge \forall i < \mathrm{length}(n)((n)_i = \alpha(i) \wedge T(e, \bar{x}, n))\big)$$

Notice that the part after $\exists$ is just a conjunction of Σ^0_n and Π^0_n and therefore it is Σ^0_{n+1}. Since Σ^0_{n+1} is closed under $\exists$ we are done. □

Corollary 32. *With the notation above we have $[C_n]_T = \underset{\sim}{0}^{(n)}$.*

Proof. For $n = 1$ it follows by definition of $\underset{\sim}{0}'$. Assume that $[C_n]_T = \underset{\sim}{0}^{(n)}$ and let C_{n+1} be a Σ^0_{n+1}-complete set. By Post's theorem this is a complete $\mathcal{RE}(C_n)$-set and therefore $[C_{n+1}]_T = [C_n]'_T$ which by inductive hypothesis is $(\underset{\sim}{0}^{(n)})' = \underset{\sim}{0}^{(n+1)}$. □

Structures and definability

The definitions we gave in Section 1 were specific for that very concrete context. In this section we develop some basic first order logic in the right formalism and in great generality. The reader should treat this section entirely independently form Section 1 and avoid fusing the common mix the terminology.

17. Syntax of first order logic

We would like to have a general framework to deal with issues of definability and provability which can for various mathematical structures and theories.

Examples. Here are some structures we would like to study.

- The usual arithmetic structure of natural numbers: $\mathcal{N} = (\mathbb{N}, 0, S, +, *, <)$, where $S(n) = n + 1$.
- The structure of our favorite group $\mathcal{G} = (G, e, \cdot)$.
- The structure of a linear or more generaly partial order $\mathcal{P} = (P, \leq)$.

A **formal language** consists of an alphabet together with a set of rules which form the syntactically correct expressions. Our alphabet will always contain the following **logical symbols**:

- infinitely many variables: $x_1 \;\; x_2 \;\; x_3 \;\; \ldots$
- negation, conjunction, existential quantifier: $\neg \;\; \wedge \;\; \exists$
- equality: $=$
- a comma and the two parenthesis symbols: , ( )

The **non-logical symbols** specified each time by providing a collection:

$$\mathcal{L} = \{R_i\}_{i\in I} \bigsqcup \{f_j\}_{j\in J} \bigsqcup \{c_k\}_{k\in K}$$

- each R_i is a relation symbol of some arity $n_i \geq 1$;
- each f_j is a function symbol of some arity $m_j \geq 1$;
- each c_k is a constant symbol.

Terms will be used to represent elements (points) in the structure. At this point however they are just syntactical objects defined inductively:

- a single variable symbol or a single constant symbol is a term;
- if $t_1, \ldots, t_n$ are terms and f is n-ary function symbol then the expression $f(t_1, \ldots, t_n)$ is a term.

Formulas will be used in formulating statements between tuples of elements in the structure. At this point however they are just syntactical objects defined inductively:

- if $t_1, \ldots, t_n, t, s$ are terms and R is n-ary function symbol then the expressions $R(t_1, \ldots, t_n)$ and $=(s, t)$ (which we will most often write as $s = t$) are both formulas which are more specifically called **atomic formulas**;
- if φ, χ are formulas and x some variable then the expressions $\neg\varphi$, $(\varphi \wedge \chi)$, and $\exists x\varphi$ are formulas.

In what follows we are going to be using certain abbreviations. Here are some:

- We write $(\varphi \vee \chi)$ for the formula $\neg(\varphi \wedge \chi)$
- We write $(\varphi \Rightarrow \chi)$ for the formula $(\neg\varphi \vee \chi)$
- We write $(\varphi \Leftrightarrow \chi)$ for the formula $\big((\varphi \Rightarrow \chi) \wedge (\chi \Rightarrow \varphi)\big)$
- We write $\forall x_i\varphi$ for the formula $\neg\exists\neg x_i\varphi$

Example. For arithmetic the language $\mathcal{L}$ is $\mathcal{L}_{ar} = \{0, S, +, *, \leq\}$. Terms include $0, x_i, x_j, S(0), S(S(0)), *(S(S(0)), x_1)$, etc. However we will introduce abbreviations/conventions:

- We write $\underline{1}, \underline{2}, \underline{3}, \ldots$ for $S(0), S(S(0)), S(S(S(0))), \ldots$;
- For expressions like $*(x_i, \underline{3})$ and $*(x_i, \underline{2})$ we simply write $x_i * \underline{3}$ and $x_i + \underline{2}$

An example of a formula in arithmetic is: $\forall x(0 < x \Rightarrow \exists y(S(y) = x))$

Definition 33. The **scope** of $\exists x_i\varphi$ is φ. An occurrence of a variable x_i in the formula χ is is called **bound** if it occurs in a quantifier $\exists x_i$ or if it occurs in the scope of some *subformula* $\exists x_i\varphi$ of χ, (where what is a subformula is defined by induction on the complexity of the formula χ). A **sentence** is any formula φ which has no free variables.

We will be using the notation $\varphi(x_1, \dots, x_n)$ whenever the collection of all free variables of φ is a subset (some times strict subset) of $x_1, \dots, x_n$.

18. Semantics of first order logic

Let $\mathcal{L} = \{R_i\} \bigsqcup \{f_j\} \bigsqcup \{c_k\}$ of arities n_i, m_j, and 0 respectively. A **structure** for $\mathcal{L}$ is any tuple

$$\mathcal{A} = (A, \{R_i^{\mathcal{A}}\}, \{f_j^{\mathcal{A}}\}, \{c_k^{\mathcal{A}}\}), \quad \text{where:}$$

- A is a non-empty set;
- $R_i^{\mathcal{A}}$ is a subset of A^{n_i};
- $f_i^{\mathcal{A}} \colon A^{m_i} \to A$ is a function;
- $c_i^{\mathcal{A}}$ is any point of A.

The moment we interpret our language $\mathcal{L}$ by attaching it on $\mathcal{A}$, terms, formulas, and sentences inherit meaning.

A term $t(x_1, \dots, x_n)$, whose free variables are among $x_1, \dots x_n$, becomes a function $t^{\mathcal{A}} \colon A^n \to A$ defined by induction in the obvious way (think of polynomials):

- if $t(x_1, \dots, x_n)$ is x_2 then $t^{\mathcal{A}}(a_1, \dots, a_n) = a_2$ (is the projection in the second coordinate);
- if $t(x_1, \dots, x_n)$ is c then $t^{\mathcal{A}}(a_1, \dots, a_n) = c^{\mathcal{A}}$ is the constant map;
- $t(\bar{x})$ is $f(t_1(\bar{x}), \dots, t_m(\bar{x}))$ then $t^{\mathcal{A}}(\bar{a}) = f^{\mathcal{A}}(t_1^{\mathcal{A}}(\bar{a}), \dots, t_m^{\mathcal{A}}(\bar{a}))$.

Given now a formula $\varphi(x_1, \dots, x_n)$ together with an assignment $x_i \mapsto a_i \in M$ we define inductively what does it mean for φ **to hold of** $\mathcal{A}, \bar{a}$, notationally, $\mathcal{A}, \bar{a} \models \varphi$:

- If φ is $R(t_1, \dots, t_m)$ then $\mathcal{A}, \bar{a} \models \varphi$ if and only if $(t_1^{\mathcal{A}}(\bar{a}), \dots, t_m^{\mathcal{A}}(\bar{a})) \in R^{\mathcal{A}}$;
- If φ is $(t_1 = t_2)$ then $\mathcal{A}, \bar{a} \models \varphi$ if and only if $t_1^{\mathcal{A}}(\bar{a}) = t_2^{\mathcal{A}}(\bar{a})$ as points in M;
- $\mathcal{A}, \bar{a} \models \neg\varphi$ if and only if it is not the case that $\mathcal{A}, \bar{a} \models \varphi$;
- $\mathcal{A}, \bar{a} \models \varphi \wedge \chi$ if and only if both $\mathcal{A}, \bar{a} \models \varphi$ and $\mathcal{A}, \bar{a} \models \chi$;
- if φ is $\exists x_i \chi$ then $\mathcal{A}, \bar{a} \models \varphi$ if and only if there is some $b_i \in M$ so that the assignment $(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots x_n) \mapsto (a_1, \dots, a_{i-1}, b_i, a_{i+1}, \dots a_n)$ we have that $\mathcal{A}, (a_1, \dots, a_{i-1}, b_i, a_{i+1}, \dots a_n) \models \chi$

We will use the alternative notation $\mathcal{A} \models \varphi(\bar{a})$ for the statement $\mathcal{A}, \bar{a} \models \varphi(\bar{x})$.

For example in arithmetic $\mathcal{N} = (\mathbb{N}, 0, S, +, *, \leq)$ we know that

$$\mathcal{N} \models \text{ there infinitely many primes}$$
$$\mathcal{N} \models \forall x \exists y (x < y \wedge \text{Prime}(y))$$
$$\mathcal{N} \models \forall x \exists y (x < y \wedge \underline{1} < y \wedge \forall z (\exists w (w * z = y) \Rightarrow (z = \underline{1}) \vee (z = y))))$$

Again in the language of arithmetic $\mathcal{L}_{ar} = \{0, S, +, *, <\}$ consider the usual structure $\mathcal{N}$ as well as the structure $\mathcal{A} = (\mathbb{R}, 0, e^{(\cdot)}, +, *, <)$. If σ is $\forall x \forall y (x + S(y) = S(x + y))$ then $\mathcal{N} \models \sigma$ while $\mathcal{A} \not\models \sigma$, i.e., $\mathcal{A} \models \neg\sigma$.

Definition 34. Let $\mathcal{A}$ be a structure in $\mathcal{L}$ and Σ be a collection of sentences in $\mathcal{L}$. We say that $\mathcal{A}$ is a **model of the theory** Σ, notationally $\mathcal{A} \models \Sigma$, if for all $\sigma \in \Sigma$ we have $\mathcal{A} \models \sigma$.

Example. Consider the language $\mathcal{L} = \{e, *\}$ where e is a constant and $*$ is binary function symbol and let Σ consist of the following sentences:

- $\forall x \forall y \forall z (x * (y * z) = (x * y) * z)$
- $\forall x (x * e = x \wedge e * x = x)$
- $\forall x \exists y (x * y = e \wedge y * x = e)$

Then every $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \models \Sigma$, is a group and conversely if $\mathcal{A}$ is a group with identity $e^{\mathcal{A}}$ and multiplication given by $*^{\mathcal{A}}$ then $\mathcal{A} \models \Sigma$. In other words Σ is the theory of groups.

Let Σ be a collection of sentences and σ be some sentence. We say that Σ **logically implies** σ, and we write $\Sigma \models \sigma$, if for every structure $\mathcal{A}$ with $\mathcal{A} \models \Sigma$, we have that $\mathcal{A} \models \sigma$. Notice that while this is a relation between syntactic objects (Σ and σ) it is defined by "reflecting" on the realm of structures. It is therefore a "semantic" relation between Σ and σ. Later we will define a purely syntactic relation between Σ and σ denoted by $\Sigma \vdash \sigma$. For example, if Σ is the above theory of groups then:

$$\Sigma \models \forall a \forall y \exists x \; a * x = y$$

A **tautology** is any sentence σ that is logically implied from $\Sigma = \emptyset$. Moreover, if σ, τ are such, so that $\sigma \Leftrightarrow \tau$ is a tautology, then we say that σ and τ are **logically equivalent**. Here are two examples of tautologies (where c_k is a constant in $\mathcal{L}$):

$$c_k = c_k, \quad \forall x \forall y \; \varphi(x, y) \Leftrightarrow \forall y \forall x \; \varphi(x, y).$$

Similarly we can say that a formula $\varphi(x_1, \ldots, x_n)$ is a **tautology** and that $\varphi(x_1, \ldots, x_n)$, $\psi(x_1, \ldots, x_n)$ are **logically equivalent** if and only if $\forall x_1 \cdots \forall x_n \varphi$ is a tautology and $\forall x_1 \cdots \forall x_n (\varphi \Leftrightarrow \psi)$ is a tautology, respectively.

We can now show that every formula is logically equivalent to one that is of a very specific form, known as *prenex normal form*. A formula χ is **quantifier free** if $\exists$ does not appear in it (and therefore neither $\forall := \neg \exists \neg$ appears in it). A formula φ is in **prenex normal form** if it is of the form:

$$Q_1 y_1 \ldots Q_n y_n \; \chi$$

where $Q_i \in \{\exists, \forall\}$, $y_i \neq y_j$, and χ is quantifier free.

For example, the formula $\forall x_4 \exists x_1 \exists x_2 ((R(x_3, x_2) \wedge x_1 = x_4) \vee \neg P(x_5, x_4))$ is in prenex normal form, while $\exists x_1 \exists x_2 ((R(x_3, x_2) \wedge x_1 = x_2) \vee \forall x_4 \neg P(x_5, x_4))$ is not.

Theorem 35. *Every formula is logically equivalent to a formula that is in prenex normal form.*

Proof. We briefly sketch the idea behind the algorithm. Let φ be the formula under consideration.

Step 1. List all subformulas of the form $Qy\psi(y, \bar{x})$ and replace y in Qy as well as all free occurrences of y within $\psi(y, \bar{x})$ with an entirely new variable which

doesn't appear anywhere in φ or in any other application of Step 1 to some different subformula.

Step 2. Apply the following operations inducting on the construction of φ:

$$\begin{aligned}
\neg\exists\psi &\longrightarrow \forall\neg\psi \\
\neg\forall\psi &\longrightarrow \exists\neg\psi \\
(\psi_1 \wedge \exists\psi_2) &\longrightarrow \exists(\psi_1 \wedge \psi_2) \\
(\exists\psi_1 \wedge \psi_2) &\longrightarrow \exists(\psi_1 \wedge \psi_2) \\
(\psi_1 \wedge \forall\psi_2) &\longrightarrow \forall(\psi_1 \wedge \psi_2) \\
(\forall\psi_1 \wedge \psi_2) &\longrightarrow \forall(\psi_1 \wedge \psi_2)
\end{aligned}$$

Notice that each time this operation is applied it lifts the position of the associated quantifier in the inductive construction of φ one layer above without introducing new quantifiers (therefore successive application will eventually terminate).

□

Example.

$$\begin{aligned}
&(\exists x R(x,z) \wedge \neg\exists z S(z,w)) \wedge \exists x P(x,u)) \\
&(\exists x' R(x',z) \wedge \neg\exists z' S(z',w)) \wedge \exists x'' P(x'',u)) \\
&\exists x''(\exists x' R(x',z) \wedge \neg\exists z' S(z',w)) \wedge P(x'',u)) \\
&\exists x''(\exists x' R(x',z) \wedge \forall z' \neg S(z',w)) \wedge P(x'',u)) \\
&\exists x''\big(\forall z'(\exists x' R(x',z) \wedge \neg S(z',w))\big) \wedge P(x'',u)) \\
&\exists x''\forall z'\big((\exists x' R(x',z) \wedge \neg S(z',w)) \wedge P(x'',u)\big) \\
&\exists x''\forall z'\big(\exists x'(R(x',z) \wedge \neg S(z',w)) \wedge P(x'',u)\big) \\
&\exists x''\forall z'\exists x'\big((R(x',z) \wedge \neg S(z',w)) \wedge P(x'',u)\big)
\end{aligned}$$

If φ is in prenex normal form then we treat all consecutive existential quantifiers as one block and all consecutive universal quantifiers as one block. We say that φ **is** $\exists_n$ if $\varphi = \exists x_1^{(1)} \dots \exists x_{k_1}^{(1)}\ \forall x_1^{(2)} \dots \forall x_{k_2}^{(2)}\ \dots \chi$ with n many blocks of quantifiers. Similarly if φ starts with $\forall$ contains n-many blocks of quantifiers we say that φ **is** $\forall_n$. In the above example, the last formula is $\forall_3$. More generally if φ is an arbitrary formula then we say that φ is φ **is** $\exists_n$ orφ **is** $\forall_n$ if it is logically equivalent to a formula ψ which is in prenex normal form and it is $\exists_n$ or $\forall_n$, respectively.

Finding the least n so that φ is either $\exists_n$ or $\forall_n$, gives as a handy measure of complexity for the formula.

19. Definability

Fix a language $\mathcal{L}$ and an $\mathcal{L}$-structure $\mathcal{A} = (A, \{R_i^{\mathcal{A}}\}, \{R_j^{\mathcal{A}}\}, \{c_k^{\mathcal{A}}\})$.

A subset P of A^n is **definable** if there is a formula $\varphi(x_1, \ldots, x_n)$ so that

$$(a_1, \ldots, a_n) \in P \iff \mathcal{A} \models \varphi(a_1, \ldots, a_n),$$

for all $\bar{a} \in A^n$. We say that P is **definable with parameters** if there is a formula $\varphi(x_1, \ldots, x_n, y_1, \ldots, y_k)$ and a tuple $(b_1, \ldots, b_k) \in A^k$ so that

$$(a_1, \ldots, a_n) \in P \iff \mathcal{A} \models \varphi(a_1, \ldots, a_n, b_1, \ldots, b_k),$$

for all $\bar{a} \in A^n$. Notice that if each b_i in the parameters is definable, i.e., if $\{b_i\}$ is definable then P is (simply) definable. A function $f\colon A^n \to A$ is definable, or definable with parameters, if its graph is so.

Examples.

(1) If $\mathcal{G} = (G, e^{\mathcal{G}}, *^{\mathcal{G}})$ is a group (see previous example) then one can define inversion $g \mapsto g^{-1}$ by the formula $\varphi(x, y) := (x * y = e)$. The axioms of the group imply that for every x there is a unique such y.

(2) Let $\mathcal{L} = \emptyset$ and let $\mathcal{A} = (A)$ be any $\mathcal{L}$-structure. With a little bit of work one can see that the only definable subsets of A are $\emptyset$ and A. Similarly the only definable with parameters subsets of A are the finite sets and the co-finite sets.

(3) Consider the structure $\mathcal{R} = (\mathbb{R}, 0^{\mathcal{R}}, +^{\mathcal{R}}, *^{\mathcal{R}})$ to be the usual real numbers with the usual operations. Notice that $x < y$ is definable by $\exists z(z \neq 0 \wedge x + z^2 = y)$. So order is definable. Similarly we can define the successor $x \mapsto x + 1$. It is a theorem of model theory that $\mathcal{A}$ satisfies quantifier elimination, i.e., for every formula $\varphi(\bar{x})$ there is a quantifier free formula $\psi(\bar{x})$ defining the same set of R^n as φ. From that it follows that the only subsets of $\mathbb{R}$ definable with parameters in $\mathcal{A}$ are the ones included in the Boolean algebra which contains all intervals (a, b) with $a, b \in \mathbb{R} \cup \{+\infty, -\infty\}$ and all finite sets. A consequence of this is that we can find a "complete and recursive" collection of sentences which axiomatize the theory of $\mathcal{R}$.

Examples like $\mathcal{A}, \mathcal{R}$ above are *tame* in that the definable sets in them are very simple and we can understand the behavior of formulas via geometric means. The situation with $\mathcal{G}$ (for certain groups) above and of $\mathcal{N} = (\mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, *^{\mathbb{N}}, <^{\mathbb{N}})$ is very different. These are *wild* structure where "geometry" steps back and recursion theory enters the picture. In the next few weeks we will study definability in $\mathcal{N}$. Something that may seem paradoxical is that while $\mathcal{R}$ contains $\mathcal{N}$ as a "substructure" (up to definitional expansion, see example (3) above), $\mathcal{R}$ is *tame* while $\mathcal{N}$ is *wild*. However notice that by the quantifier elimination result mentioned above $\mathbb{N}$ is not definable in $\mathcal{R}$. Therefore we cannot explicitly or implicitly ask questions in $\mathcal{R}$ about $\mathcal{N}$. Moreover, notice how easier is to answer in $\mathcal{R}$ questions which are fairly hard to be answered in $\mathcal{N}$ such as:

$$\exists x \exists y \exists z(x * y * x > 0 \wedge x^n + y^n = z^n),$$

where x^n stands for $x * \cdots * x$ (n-many times) for any fixed $n > 2$.

20. A coarse study of definability in arithmetic

Consider the usual structure $\mathcal{N} = (\mathbb{N}, 0, S, +, *, <)$ of arithmetic (for simplicity we write $0, S, \ldots$ for $0^{\mathcal{N}}, S^{\mathcal{N}}, \ldots$) as well as the structure $\mathcal{N}_{pr} = (\mathbb{N}, +)$ known as Presburger arithmetic. In terms of the discussion in Section 19 $\mathcal{N}$ is on the *wild* side while $\mathcal{N}_{pr}$ is on the *tame* side. Before we prove the former we elaborate a bit on the later.

The usual way method for proving that a structure $\mathcal{A}$ is on the *tame* side goes through quantifier elimination. That is, if one shows that every formula $\varphi(\bar{x})$ is logically equivalent in $\mathcal{A}$ with some quantifier free formula $\chi(\bar{x})$ then the task of understanding the definable sets is much easier (since quantifier free formulas are "finitary statements." Here logically equivalent with respect to $\mathcal{A}$ means that

$$\mathcal{A} \models \forall x_1 \ldots \forall x_n \, \varphi(\bar{x}) \iff \chi(\bar{x}).$$

so does $\mathcal{N}_{pr}$ have quantifier elimination? Well first notice that $0, <, S$ are definable in $\mathcal{N}_{pr}$ so we can expand $\mathcal{N}_{pr}$ to the structure $\mathcal{N}_{pr}^{+} = (\mathbb{N}, 0, S, +, <)$ without changing the definable sets. Even in this definitional expansion $\mathcal{N}_{pr}^{+}$ has no quantifier elimination because on can show that for every $k \geq 2$ the formula

$$\phi_k(x) \quad \equiv \quad \exists y \, (y = \overbrace{x + \ldots + x}^{k-\text{times}})$$

is not equivalent to a quantifier free formula. However that's all! One can prove that the structure $\mathcal{N}_{pr}^{++} = (\mathbb{N}, 0, S, +, <, 2\mathbb{N}, \ldots, k\mathbb{N}, \ldots)$ has quantifier elimination. From that it follows that the definable subsets of $\mathbb{N}$ in $\mathcal{N}_{pr}^{++}$ are precisely all sets A which are eventually periodic (with possible period $k = 0$),i.e., there is some $l > 0$ and a $k \geq 0$ so that for $n \geq l$ we have that $n \in A$ if and only if $n = l + mk$ for some $m \geq 0$. As a consequence, $*$ is not definable in $\mathcal{N}_{pr}^{++}$ (and therefore neither in $\mathcal{N}_{pr}$) since the set $\{n^2 \colon n \in \mathbb{N}\}$ is not eventually periodic.

Exercise. Show that in $\mathcal{N}' = (\mathbb{N}, S, *)$, where $*$ is the usual multiplication and S is the successor, the usual addition operation $+$ is definable.

The following theorem and its corollary illustrates the gap between tame and wild. It also justifies as to why we called the collection of all sets in $\bigcup_n \Sigma_n^0$ arithmetical.

Theorem 36 (Gödel)**.** *Every (partial) recursive function is definable in $\mathcal{N}$. Every recursively enumerable set is also definable in $\mathcal{N}$.*

Corollary 37. *A set $A \subseteq \mathbb{N}^k$ is definable in $\mathcal{N}$ if and only if $A \in \bigcup_n \Sigma_n^0$*

Proof of Corollary. One direction is by the above theorem. The other direction is from prenex normal form and the fact that quantifier free formulas of arithmetic define recursive (in fact primitive recursive) subsets of $\mathbb{N}^k$ in $\mathcal{N}$. □

We proceed now to the proof of Theorem 36.

Proof of Theorem 36. It suffice to show the first since every r.e. set is the domain of some recursive f and the domain of f is always definable from the graph by the formula $\varphi(x) \equiv \exists y\, f(x) = y$.

This is done by induction. We show that simple maps are definable and that the collection of definable functions is closed under composition, minimalization, primitive recursion.

Simple maps. All $\mathrm{proj}_i^n \colon \mathbb{N}^n \to \mathbb{N}, c_0 \colon \mathbb{N} \to \mathbb{N}$, and $S \colon \mathbb{N} \to \mathbb{N}$ have definable graphs given, respectively, by the formulas:

$$\varphi(x_1, \ldots, x_n, y) \;\equiv\; y = x_i, \quad \varphi(x, y) \;\equiv\; y = 0, \quad \varphi(x, y) \;\equiv\; y = S(x),$$

Composition. Let $f(n_1, \ldots, n_k) = h(g_1(\bar{n}), \ldots, g_m(\bar{n}))$ and assume that $\psi(y_1, \ldots, y_m, z)$ defines (the graph of) h and $\psi_i(x_1, \ldots, x_k, y)$ defines the graph of g_i, $i = 1, \ldots, m$. Then the definition of f is given by the following formula $\varphi(x_1, \ldots, x_k, z) \equiv$

$$\exists y_1 \ldots \exists y_m \big(\psi_1(x_1, \ldots, x_k, y_1) \wedge \ldots \wedge \psi_m(x_1, \ldots, x_k, y_m) \wedge \psi(y_1, \ldots, y_m, z)\big).$$

Minimalization. Let $f(n_1, \ldots, n_k) = \mu n\, [g(n_1, \ldots, n_k, n) = 0]$ and assume that g is defined by $\psi(x_1, \ldots, x_k, x, y)$ then f is defined by $\varphi(x_1, \ldots, x_k, z) \equiv$

$$\exists x \psi(x_1, \ldots, x_k, x, 0) \wedge \forall x' \bigg((x' < x) \implies \exists y \big(\neg(y = 0) \wedge \psi(x_1, \ldots, x_k, x', y)\big) \bigg).$$

Primitive Recursion. Assume now that f is the unique function given by

$$f(0, \bar{n}) = g(\bar{n}), \quad f(i + 1, \bar{n}) = h(f(i, \bar{n}), i, \bar{n}),$$

where g is defined by $\psi(\bar{x}, x)$ and h is defined by $\chi(z, w, \bar{x}, y)$. Then we have that f is "defined" by $\varphi(w, x_1, \ldots, x_k, z) \equiv$

$$(w = 0 \wedge \psi(\bar{x}, z)) \vee$$

$$\vee \bigg(w > 0 \wedge \overbrace{\exists l_0 \ldots \exists l_w}^{w-\text{many}} \big(\psi(\bar{x}, l_0) \wedge \chi(l_0, 1, \bar{x}, l_1) \wedge \ldots \wedge \chi(l_{w-1}, w, \bar{x}, l_w) \wedge (l_w = z)\big) \bigg),$$

where the i-th term in the above conjunction is just $\chi(l_{i-1}, i, \bar{x}, l_i)$.

Of course this is not an actual formula since the number of existential quantifiers depends on w. What Gödel did is to find a way to definably code any sequence $l_0, \ldots l_m$ of natural numbers. We need a definable function $\gamma(l, i)$ so that

$$\forall m > 0 \forall l_0, \ldots, l_{m-1} \exists l \big(\gamma(l, i) = l_i, \forall i < m\big)$$

We will actually find a definable function $\beta(a, b, i)$ so that

$$\forall m < 0\; \forall \bar{l}\; \exists a\; \exists b\; \big(\beta(a, b, i) = l_i, \forall i < m\big)$$

So granted from the following lemmas such a function the proof is complete. □

Definition 38. By the Gödel's β-function we mean the map

$$\beta(a, b, i) = \mathrm{rmd}(a, 1 + (i + 1)b),$$

i.e., the remainder of the division of $1 + (i + 1)b$ with a.

First observe that β is clearly definable by $\varphi(x,y,w,z) \equiv$

$$\exists q\big(x = q * (S(0) + (w + S(0)) * y) + z \ \wedge \ z < (S(0) + (w + S(0)) * y)\big)$$

Lemma 39. $\forall m < 0 \ \forall\, l_0, \ldots, l_{m-1} \ \exists a \ \exists b \ \big(\beta(a,b,i) = l_i, \forall i < m\big)$

Proof. We will make use of the Chinese remainder theorem:

Claim (Chinese remainder theorem)**.** *If $b_0, \ldots, b_{m-1}$ are pairwise relatively prime then for every $l_0, \ldots, l_{m-1}$ with $l_i < d_i$ there is some l so that for all $i < m$ we have that $l_i = \mathrm{rmd}(l, b_i)$.*

Proof of Claim. Consider the map $r\colon \mathbb{N} \to \mathbb{N}^m$ with $r(n) = (n_0, \ldots, n_{m-1})$, where $n_i = \mathrm{rmd}(l, b_i)$. Notice that there are at most $b = b_0 * \ldots * b_{m-1}$ possible $r(n)$'s. It is enough to show that r is $1-1$ on $\{0, \ldots, b-1\}$. Otherwise there would be some $m < m' < b$ with $r(m) = r(m')$. So $b_i | (m' - m)$ for all i. But since b_i's are relatively prime we have that $b_0 * \ldots * b_{m-1} | m' - m$, a contradiction. □

We can now finish the proof of the lemma. We will set $b = n!$ with n large enough so that if we set $b_i = 1 + (1+i)b$ for every $i < m$, we will have that:

(1) $l_i < b_i$ for all i

(2) b_i and b_j are relatively prime when $i \neq j$.

The first task is clearly achievable by picking large n. For the second task notice that if for some prime p we have that $p | b_i$ and $p | b_j$, with $i < j$ say, then $p | (j - i)b$. Having picked n large enough implies that $p | b$ and therefore combining this with the assumption $p | b_i$ we get $p | 1$, a contradiction. □

A finer study of definability and Hilbert's 10th problem

This section is motivated by the following two problems.

Problem 1. We saw in previous section that a set $A \subseteq \mathbb{N}^n$ is definable in $\mathcal{N}$ if and only if it is arithmetical. However, both definable sets and arithmetical sets are layered in natural hierarchies.

$$\text{Definable:} \quad \Delta^0_1, \Sigma^0_1, \Pi^0_1, \quad \Delta^0_2, \Sigma^0_2, \Pi^0_2, \ldots$$

$$\text{Arithmetical:} \quad \exists_0, \forall_0, \quad \exists_1, \forall_1, \quad \exists_2, \forall_2, \ldots$$

By definition we have that $\exists_0 = \forall_0$. Moreover, it is easy to see that for any $A \in \exists_0$ there is a polynomial time algorithm which decides whether a given $\bar{x} \in \mathbb{N}^n$ is in A. As a consequence $\exists_0$ is a strict subset of the collection Δ^0_1, of all recursive sets.

It follows that for every n we have that $\exists_n$ is a subset of Σ^0_n and that $\forall_n$ is a subset of Π^0_n. It is not clear however whether these inclusions are strict. In particular, is it the case that $\exists_1 = \Sigma^0_1$ or $\exists_1 \subseteq \Sigma^0_n$?

Problem 2. In the proceedings of the Second International Congress in Paris on August 8, 1900 Hilbert announced the 23 problems which, in his opinion, would shape mathematics for the next century. The 10th problem in this list was the following:

"Is there an algorithm that decides if any given Diophantine equation
$F(\bar{x}) = 0$ has an integer solution?"

By a **Diophantine equation** we mean a polynomial $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ with coefficients from $\mathbb{Z}$. By an integer solution we mean a vector $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ so that $F(k_1, \ldots, k_n) = 0$.

Both problems are addressed by Matiyasevich's celebrated theorem:

Theorem 40 (Matiyasevich (1970))**.** *Let $A \subseteq \mathbb{N}^n$ is Σ_1^0 then there exists a polynomial $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ with integer coefficients so that for every $\bar{a} \in \mathbb{N}^n$:*

$$(a_1, \ldots, a_n) \in A \quad \Longleftrightarrow \quad \exists y_1 \in \mathbb{N} \ldots \exists y_m \in \mathbb{N}\, F(a_1, \ldots, a_n, y_1, \ldots, y_m).$$

Of course notice that by we can always pass terms of F having negative coefficients on the other side so that $F(\bar{x}, \bar{y}) = 0$ is equivalent with $H(\bar{x}, \bar{y}) = G(\bar{x}, \bar{y})$, and H, G have coefficients from $\mathbb{N}$.

Given Matiyasevich's "representation" theorem we can solve both problems above.

Solution to Problem 1: $\exists_1 = \Sigma_1^0$. In fact notice that the above theorem says something seemingly stronger, i.e., the quantifier free formula we are using in the $\exists_1$ representation of A is just a polynomial no $\neg$ is used (or $\wedge, \vee$, but the later two can be easily coded using polynomials). Therefore $\exists_n = \Sigma_n^0$ and $\forall_n = \Pi_n^0$ for all n.

Solution to Problem 2: No! First notice that having an algorithm determining whether every diophantine equation has *integer* solutions is the same as having an algorithm determining whether every diophantine equation has *positive integer* solutions:

- $F(x_1, \ldots, x_n) = 0$ has solutions in $\mathbb{Z}$ if and only if $F'(x_1, \ldots, x_n) = 0$ has solutions in $\mathbb{N}$ where
$$F'(x_1, \ldots, x_n) = \Pi_{\text{all combinations of } \pm}\, F(\pm x_1, \ldots, \pm x_n)$$
- $F(x_1, \ldots, x_n) = 0$ has solutions in $\mathbb{N}$ if and only if $F'(\bar{x}, \bar{y}, \bar{z}, \bar{w}) = 0$ has solutions in $\mathbb{Z}$ where
$$F'(\bar{x}, \bar{y}, \bar{z}, \bar{w}) = F(x_1^2 + y_1^2 + z_1^2 + w_1^2, \ldots, x_n^2 + y_n^2 + z_n^2 + w_n^2)$$

For the later we use Lagrange theorem that every positive integer is the sum of four squares. Let now $A \in \Sigma_1^0 \setminus \Delta_1^0$. Then by Matiyasevich's theorem A is of the form

$$\exists y_1 \ldots \exists y_m\, F(a_1, \ldots, a_n, y_1, \ldots, y_m),$$

and therefore, if there was an algorithm deciding when every Diophantine equation has solutions in $\mathbb{N}$, then we could use it to show that A is recursive, contradicting that $A \notin \Delta_1^0$.

Another interesting corollary of the above theorem is the following:

Corollary 41. *If $A \subseteq \mathbb{N}$ is recursively enumerable then there exists a polynomial $F(\bar{x}) \in \mathbb{Z}(\bar{x})$ so that:*

$$A = \{F(\bar{x}) | x_1, \ldots, x_n \geq 0\} \cap \mathbb{N}$$

In particular, various sets such as the collection of prime numbers are presicely the positive range of the positive domain of some polynomial.

Proof. Exercise. □

The proof of Matiyasevich theorem is long and it would take 2-3 weeks to give complete details. Here we will provide just a sketch which illustrates the main ideas and the various tricks involved in the proof.

21. Reduction to exponential Diophantine

Definition 42. A set $A \subseteq \mathbb{N}^n$ is **Diophantine** if there exists a polynomial $F(\bar{x}, \bar{y})$ with integer coefficients so that for $\bar{a} \in \mathbb{N}^n$ we have that

$$\bar{a} \in A \quad \iff \quad \exists \bar{y}\ F(\bar{a}, \bar{y}) = 0$$

A partial map $f\colon \mathbb{N}^n \to \mathbb{N}$ is Diophantine if its graph is, as a subset of $\mathbb{N}^{n+1}$.

If A is Σ^0_1 then the partial map f whose domain is A and $f(\bar{a}) = 0$ is recursive so it will be enough to prove (sketch the proof) of the following theorem

Theorem 43 (Reformulation of Matiyasevich Theorem)**.** *Every partial recursive function $f\colon \mathbb{N}^n \to \mathbb{N}$ is Diophantine.*

Let's run the usual proof by induction on the complexity of the definition of f to see what closure properties we need to establish for the class of all Diophantine functions.

Step 1 $c_0, \mathrm{proj}^n_i, S$ are all Diophantine by using a dummy variable:

$$\exists z(y = 0), \quad \exists z(y = x_i), \quad \exists z(x + 1 - y = 0),$$

Step 2 $f(\bar{x}) = g(h_1(\bar{x}), \ldots, h_m(\bar{x}))$, then $f(\bar{x}) = y$ if and only if

$$\exists \bar{y}(\wedge_{i \le m} h_i(\bar{x}) = y_i \ \wedge\ g(\bar{y}) = y)$$

Need. Closure under $\exists$ and $\wedge$.

Step 3 $f(\bar{x}) = \mu y[g(\bar{x}, y) = 0]$ then $f(\bar{x}) = y$ if and only if

$$g(\bar{x}, y) = 0 \ \wedge\ \forall z < y\ \exists w\big((g(\bar{x}, z) = w) \wedge (w > 0)\big)$$

Need. $w > 0$ is Diophantine and closure under bounded quantifiers $\forall x < y$.

Step 4 $f(0, \bar{x}) = g(\bar{x})$ and $f(i + 1, \bar{x}) = h(f(i, \bar{x}), i, \bar{x})$ then $f(i, \bar{x}) = y$ iff

$$(i = 0 \wedge y = g(\bar{x})) \vee$$

$$\left(i > 0 \wedge \exists a \exists b\big((g(\bar{x}) = \beta(a, b, 0)) \wedge (y = \beta(a, b, i)) \wedge \forall j < ij + 1 = h(\beta(a, b, j), j, \bar{x})\big)\right)$$

Need. β is Diophantine, and closure under $\vee$ and under substitution by Diophantine functions.

So the theorem will be proved once we prove (sketch the proof of) the following lemma.

Lemma 44. *The collection of Diophantine sets contains the relations $x < y$, $x \equiv y \bmod z$, and Gödel's function β, and it is closed under $\vee, \wedge, \exists, \forall x < y$ and under substitution by Diophantine maps.*

Proof. Everything is easy and it is left as an exercise except $\forall x < y$ which is hard and which we are going to analyze in what follows.

For example notice that $(\exists \bar{y} F(\bar{x}, \bar{y}) = 0) \vee (\exists \bar{z} G(\bar{x}, \bar{z}) = 0)$ is simply equivalent to $\exists \bar{y} \exists \bar{z} \big(F(\bar{x}, \bar{y}) * G(\bar{x}, \bar{z}) = 0\big)$, and the product of two polynomials is a polynomial. □

The next lemma shows that we can reduce the problem of showing that $\forall x \leq y$ is Diophantine to the problem of showing that certain functions which are fusions of "exponentiation" and $n \mapsto n!$ are Diophantine. It will be convenient for purposes of indexing to work with $\forall x(1 \leq x \leq y)$ rather than $\forall x \leq y$. Since Diophantine sets are closed under $\wedge$ this is not a simplification in substance.

Lemma 45. *Let A be the set of all $(x_1, \ldots, x_n, t) \in \mathbb{N}^{n+1}$ with the property that*

$$\forall k(1 \leq k \leq t) \;\; \exists y_1, \ldots, y_m \;\; f(x_1, \ldots, x_n, k, y_1, \ldots, y_m) = 0,$$

for some polynomial f with integer coefficients. Then $(\bar{x}, t) \in A$ if and only if, for this $(\bar{x}, t)$, the following system has a solution for some value of $Y, N, K, Y_1, \ldots, Y_m$:

(1) $N > c * (x_1 * \cdots * x_n * t * Y)^d$;
(2) $1 + KN! = \Pi_{k=1}^{t}(1 + kN!)$;
(3) $f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv 0 \mod (1 + KN!)$;
(4) $\Pi_{j \leq Y}(Y_i - j) \equiv 0 \mod (1 + KN!)$, *and* $Y < Y_i$, *for all* $i \in \{1, \ldots, m\}$.

Where c, d are some fixed constants which depend only on f.

Proof. Recall Gödel's β map which was defined by the assignment $(a, b, i) \mapsto (a \mod 1 + (i+1)b)$. Because of the bounds of the index k it would be good to work with the map $\tilde{\beta}$ which sends (a, b, i) to $(a \mod 1 + ib)$

We first prove the variant of the Lemma where condition (4) is replaced with

(4') $\tilde{\beta}(Y_i, N!, k) \leq Y$ for every $i \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, t\}$.

The set $A(\bar{x}, t) = \forall k(1 \leq k \leq t) \; \exists \bar{y} \; f(\bar{x}, k, \bar{y}) = 0$ can be informally rewritten as:

$$(\star) \qquad \exists \bar{y}^{(1)} \; \cdots \; \exists \bar{y}^{(k)} \; \cdots \; \exists \bar{y}^{(t)} \;\; \bigwedge_{k=1}^{t} f(\bar{x}, k, \bar{y}^{(k)}) = 0$$

Of course this is not in Diophantine form because the number of quantifiers and the number of conjunctions is not constant but depends on t.

For each i with $1 \leq i \leq m$ we will use the variable Y_i and the $\tilde{\beta}$-map to code the vector $(y_i^{(1)}, \ldots, y_i^{(k)}, \ldots, y_i^{(t)})$ where

$$\bar{y}^{(1)} = (y_1^{(1)}, \ldots, y_i^{(1)}, \ldots, y_m^{(1)}), \quad \cdots \quad , \bar{y}^{(t)} = (y_1^{(t)}, \ldots, y_i^{(t)}, \ldots, y_m^{(t)})$$

In particular, by a careful reading of the proof of Lemma 39 notice that if $N \geq \max\{t, y_i^{(1)}, \ldots, y_i^{(t)}\}$ then we can always find arbitrary large natural numbers to set Y_i equal to, so that $y_i^{(k)} = \tilde{\beta}(Y_i, N!, k)$. In particular:

$$Y_i \equiv y_i^{(k)} \mod (1 + kN!)$$

and as a consequence for every k we have that:

$$f(\bar{x}, k, Y_1, \ldots, Y_m) \equiv f(\bar{x}, k, y_1^{(k)}, \ldots, y_m^{(k)}) \equiv 0 \mod (1 + kN!) \tag{5}$$

This deals with the first problem, i.e., the unboundedly many $\exists$ quantifiers. Next we turn the $\wedge_{k=1}^{t}$ into the single equation (3) where K is specified in (2).

Claim. *If K is the unique natural number specified by (2) then for every k we have*

$$K \equiv k \mod (1 + kN!)$$

Proof of Claim. Notice that $(1+KN!)-(1+kN!) \equiv 0 \mod (1+kN!)$ holds. Since both terms are multiples of $(1 + kN!)$. This implies the claim. □

By equation (5) we now have that $f(\bar{x}, K, Y_1, \ldots, Y_m) \equiv 0 \mod (1 + kN!)$, and since $(1 + kN!)$'s are relatively prime we have that

$$f(\bar{x}, K, Y_1, \ldots, Y_m) \equiv 0 \mod (1 + KN!)$$

So far we have shown that if $(\bar{x}, t) \in A$, i.e., if there are $\bar{y}^{(1)} \ldots \bar{y}^{(t)}$ so that together with $\bar{x}$ they satisfy $(\star)$ then there are $Y_1, \ldots, Y_m, K, N$ satisfying conditions (2) and (3). We haven't introduced Y yet but as long as it satisfies $Y > \max\{y_i^{(k)} \mid k \leq t, i \leq m\}$ then (4') clearly holds and (1) clearly works for any c, d as long as we pick N large enough (this doesn't affect the argument so far).

We need though (1), (4') to be able to prove the converse. To see this, assume that for some $(\bar{x}, t)$ there are $Y_1, \ldots, Y_m, K, N$ satisfying (2) and (3). We have $f(\bar{x}, K, \bar{Y}) \equiv 0 \mod (1 + KN!)$ and therefore $f(\bar{x}, K, \bar{Y}) \equiv 0 \mod (1 + kN!)$ which implies $f(\bar{x}, k, y_1^{(k)}, \ldots, y_m^{(k)}) \equiv 0 \mod (1 + kN!)$ where $y_i^{(k)}$ is defined to be $\tilde{\beta}(Y_i, N!, k)$. But can we remove the mod$(1 + kN!)$ part?

We would if $f(\bar{x}, k, y_1^{(k)}, \ldots, y_m^{(k)})$ was forced to be smaller than $(1 + kN!)$. Since f is a polynomial we can always find c, d so that

$$|f(\bar{x}, k, \bar{y}^{(k)})| < c(\bar{x} * t * Y)^d,$$

and conditions (1) and (4') now guarantee the required.

Exercise. Show that (1),(2),(3),(4) hold for some $Y, N, K, Y_1, \ldots, Y_m$ if and only if (1),(2),(3),(4') hold for some $Y, N, K, Y_1, \ldots, Y_m$ □

Notice that the conditions (1) and (3) are Diophantine. For (2) and (4) it suffices to show that the maps $x \mapsto x!$ and $(r, x) \mapsto \binom{r}{x}$ for $r \geq x$ are Diophantine. For example notice that (4) can be rewritten as

$$Y! \binom{Y_i - 1}{Y},$$

and a similar idea (but more complicated) reduces (2). It is time to use Matiyasevich's Lemma whose proof we are going to discuss in the next section.

Lemma 46 (Matiyasevich's Lemma)**.** *The map $(x, y) \mapsto x^y$ is Diophantine.*

Having this we can prove the following lemma.

Lemma 47. *The maps $x \mapsto x!$ and $(r,x) \mapsto \binom{r}{x}$ for $r \geq x$ are Diophantine.*

Proof. Notice that $x! = \lim_{r\to\infty} \frac{r^x}{\binom{r}{x}}$ since for fixed x and $r \geq x$ we have that:

$$\frac{r^x}{\binom{r}{x}} = \frac{r^x}{\frac{r!}{x!(r-x)!}} = x!\left(\frac{r}{r}\frac{r}{r-1}\cdots\frac{r}{r-x+1}\right)$$

So assuming we know how large r we have to pick then we can define $x! = \left\lfloor \frac{r^x}{\binom{r}{x}} \right\rfloor$, that is

$$x! = y \iff y\binom{r}{x} \leq r^x < (y+1)\binom{r}{x}.$$

So we have reduced the problem of showing that $x \mapsto x!$ is Diophantine to the problem of showing that $(r,x) \mapsto \binom{r}{x}$ is Diophantine and the problem of finding large enough r in a Diophantine way from x.

Exercise A. Show that choosing $r = (2x)^{x+1} + 1$ solves the last problem, or find some other Diophantine (modulo Matiyasevich's Lemma) function of your own preference for choosing such large r.

Exercise B. Show that $(r,x) \mapsto \binom{r}{x}$, for $r \geq x$, is Diophantine. □

Notice that we have already proven that recursively enumerable sets are the same as "exponential Diophantine." This result is due to David-Putnam-Robinson.

In fact Julia Robinson proved that if any fixed Diophantine set $A \subset \mathbb{N}^2$ has one coordinate growing faster than any power of the other but slower than x^x then all r.e. sets are Diophantine.

22. Exponential is Diophantine

We want to prove Matiyasevich's Lemma that the map $(a,n) \mapsto a^n$ is Diophantine. First we show that it suffice to find some Diophantine function that is "approximately exponential"

Lemma 48. *Assume that we have some Diophantine map $(a,n) \mapsto y(a,n)$ with the property that for every $a > 1$ we have that*

$$(2a-1)^n \leq y(a,n+1) \leq (2a)^n$$

Then the map $(a,n) \mapsto a^n$ is Diophantine.

Proof. Notice that for any $N \geq 1$ we have that

$$a^n\big(1 - \frac{1}{2Na}\big)^n = \frac{(2Na-1)^n}{(2N)^n} \leq \frac{y(Na,n+1)}{y(N,n+1)} \leq \frac{(2Na)^n}{(2N-1)^n} = a^n\big(1-\frac{1}{2N}\big)^{-n}$$

So, for very large N we have that:

$$a^n - 1 < \frac{y(Na,n+1)}{y(N,n+1)} < a^n + 1$$

So we want to be able to compute some lower bound for N, in a Diophantine way from a, n, that makes the above inequalities work. Given that we have this lower bound map $(a, n) \mapsto N(a, n)$ we can define $m = a^n$ if and only if $\exists N$ such that:

- $(m-1) * y(m, n+1) < y(Na, n+1)$ and $y(Na, n+1) < (m+1) * y(m, n+1)$;
- $a|m$ (because there may be two integers in the above interval);
- $N > N(n, a)$.

To find $N(n, a)$ just calculate for which N we have $a^n\big(1 - \frac{1}{2N}\big)^{-n} < a^n + 1$ and for which N we have $a^n - 1 < a^n\big(1 - \frac{1}{2Na})^n$. With some easy computations one can see that setting $N(n, a) = y(a + 1, n + 2)$ makes things work. □

Recall from previous time that in order to show that every R.E. set is Diophantine, it suffice to show that the function $(a, n) \mapsto a^n$ is Diophantine. In fact, by the last lemma, it suffice to find some Diophantine map $(a, n) \mapsto y(a, n)$ with the property that for every $a > 1$ we have that

$$(2a - 1)^n \leq y(a, n + 1) \leq (2a)^n$$

A general **Pell equation** is an equation of the form:

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

where d is a parameter and x, y are variables. This equation has always the trivial solution $(x, y) = (1, 0)$. When $d = \square$, i.e., $d = r^2$ for some r, then this is the only solution since $(x - ry)(x + ry) = 1$ implies that $x = 1$. Whenever $d \neq \square$ then it has a non-trivial solution but such solution is difficult to be found. In fact we know that a certain weak-fragment of arithmetic known as Bounded Arithmetic cannot prove

$$\forall d \exists x \exists y \big(d \neq \square \implies (x^2 - dy^2 = 1 \wedge x > 1) \big)$$

This will not be a problem because we are going to work with a certain family of d's where it is easy to find non-trivial solutions. First we will establish some basic results for the arbitrary d.

Notice that over the reals, the expression $x^2 - dy^2$ factors to $(x - \sqrt{d}y)(x + \sqrt{d}y)$. It will be convenient therefore to work in the integral domain $\mathbb{Z}[\sqrt{d}]$. If $\alpha = (x + \sqrt{d}y)$ then $\bar{\alpha} = (x - \sqrt{d}y)$ is known as the **conjugate** of α. The **norm** $||\alpha||$ is simply the number $\alpha\bar{\alpha}$, so the Pell equation is simply collecting all α's with $||\alpha|| = 1$.

Of course since we work with non-negative integer solutions x, y we always have that $\alpha = x + \sqrt{d}y \geq 1$. The converse is also true:

Lemma 49. *If $\alpha = x + \sqrt{d}y \geq 1$ with $||\alpha|| = 1$ then $1 \leq x$ and $0 \leq y$.*

Proof. Since $\alpha\bar{\alpha} = 1$, we have that $\bar{\alpha} = \alpha^{-1}$. Therefore $0 < \alpha^{-1} \leq 1$. The rest follows from $\alpha + \bar{\alpha} = 2x$ and $\alpha - \bar{\alpha} = 2\sqrt{d}y$. □

So the inequality $1 \leq \alpha$ together with $||\alpha|| = 1$ implies that both x, y are non-negative. Hence the collection of all such α with is discrete and linearly ordered. So if there is a non-trivial solution represented then there is one represented by the smallest possible such γ. We call such γ the **generator** of solutions because as we will see every positive integer solution will be represented by some power of γ.

Lemma 50. *If $||\alpha|| = 1$ and $||\beta|| = 1$ then $||\alpha\beta|| = 1$. So the product of two reals which* represent *a positive solution to the Pell equation also represents a positive solution.*

Proof. Check that α, β we have that $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$. As a consequence we have that

$$||\alpha\beta|| = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\beta\bar{\beta}\bar{\alpha} = \alpha\bar{\alpha} = 1$$

□

Lemma 51. *Assume that γ is the generator of the solutions of $x^2 - dy^2 = 1$ (which exists if and only if there is some non-trivial solution). Then every solution $(x, y) \in \mathbb{N}^2$ is represented by some $\beta = x + \sqrt{d}y$ with $\beta = \gamma^n$ for some n.*

Proof. By the previous lemma, since γ represents a solution, every power γ^n also represents a solution.

Conversely, if $||\beta|| = 1$ and $1 \leq \beta$ then there is some n with $\gamma^n \leq \beta < \gamma^{n+1}$. So, $1 \leq \beta\gamma^{-n} < \gamma$. But the previous lemma we have that $||\beta\gamma^{-n}|| = ||\beta|| \cdot ||\bar{\gamma}||^n = 1$. Since γ is the smallest non-trivial solution $\beta\gamma^{-n} = 1$ and therefore $\beta = \gamma^n$. □

For the general d it is difficult to locate the generator to the solutions of $x^2 - dy^2 = 1$. We are going to work in the special case when $d = a^2 - 1$. The Pell equation

$$(\star) \qquad x^2 - (a^2 - 1)y^2 = 1$$

has the non-trivial solution $(a, 1)$ which cannot be but the smallest such. As a consequence $\gamma = a + \sqrt{a^2 - 1}$. We define now the maps $(a, n) \mapsto x(a, n)$ and $(a, n) \mapsto y(a, n)$ where $\big(x(a, n), y(a, n)\big)$ is the n-th solution to the Pell equation $(\star)$. From the above discussion we have that:

$$x(n, a) + y(y, a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n,$$

i.e., $\big(x(0, a), y(0, a)\big) = (1, 0)$, $\big(x(1, a), y(1, a)\big) = (a, 1), \ldots$ We claim that $(a, n) \mapsto y(a, n)$ is the approximately exponential map we are looking for.

Lemma 52. *For all $n \geq 1$ we have that $(2a - 1)^n \leq y(a, n + 1) \leq (2a)^n$.*

Proof. Denote $y(a, n)$ by y_n. Notice that y_n satisfies the following recurrence relation:

$$y_{n+2} = 2ay_{n+1} - y_n.$$

This is a simple calculation. Given this, a simple induction and the initial $y_0 = 0$, $y_1 = a$, $y_2 = 2a$ give the required. □

The last thing one needs to argue is that $(a, n) \mapsto y(a, n)$ is Diophantine. We will give not details about the proof except the following crucial observation:

Lemma 53. $y(a, n) \equiv n \mod a - 1$.

Proof. Since $x(n, a) + y(y, a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n$ we have that

$$y(n, a) = \sum_{i=0,odd}^{n} a^{n-i}(a^2 - 1)^{(i-1)/2}\binom{n}{i}.$$

Notice now that all terms are zero except for when $i = 1$, for which we have that

$$na^{n-1} = \cdots = na^{n-2}(a-1) + na^{n-2} = na^{n-2}(a-1) + na^{n-3}(a-1) + \cdots + (a-1) + n,$$

which $(\mod a - 1)$ is n. □

As a consequence we can recover $y(a,n)$ in a Diophantine way from (a,n) from the perspective of the quotient (mod $a-1$). To recover it completely one needs to introduce more Diophantine restrictions. In particular one has the following theorem.

Theorem 54. *Let $n>1$ and $a>2$. Then the relation $R(y,a,n)$ with $y(a,n)=y$ holds if and only if $\exists x\ \exists X\ \exists Y\ \exists A\ \exists Z\ \exists W$ such that*

(1) $x^2+(a^2-1)y^2=1$, $y\equiv n \mod a+1$, $y>n$;
(2) $X^2+(A^2-1)Y^2=1$, $Y\equiv n \mod A+1$;
(3) $A\equiv a \mod Z$;
(4) $Y\equiv y \mod Z$;
(5) $Z^2-W^2(A^2-1)=1$;
(6) $A\equiv 1 \mod 2y$;
(7) $W\equiv 0 \mod y^2$.

Gödel's Incompleteness theorem

23. Deductive formal systems

A **deductive formal system** $\mathcal{D}$ for a formal language on alphabet $\mathcal{L}$ consists of

(1) a collection of formulas called the **axioms**;
(2) a finite set of rules $D_1,\dots,D_n$ where each D_i is a relation $D_i(\varphi_1,\dots,\varphi_{n_i},\psi)$ between formulas, called **rules of inference**.

We say that ψ is a **direct consequence** of $\varphi_1,\dots,\varphi_{n_i}$ via D_i if $D_i(\varphi_1,\dots,\varphi_{n_i},\psi)$. A **formal proof** or **deduction** in $\mathcal{D}$ is a sequence $\varphi_1,\dots,\varphi_n$ so that each φ_i is either an axiom of $\mathcal{D}$ or a direct consequence of earlier formulas in the list. A **formal theorem** in $\mathcal{D}$ is any formula φ for which there exists a formal proof $\varphi_1,\dots,\varphi_n$ with $\varphi_n=\varphi$. If φ is a formal theorem in $\mathcal{D}$ we write

$$\vdash_{\mathcal{D}} \varphi$$

Similarly we have all the above notions relativised to any fixed collection of formulas. In particular, if Σ is a collection of formulas then a formal proof from Σ is as before but we moreover allow φ_i to be from Σ. If φ is a theorem from Σ then we write

$$\Sigma \vdash_{\mathcal{D}} \varphi$$

Here are some immediate properties:

(1) If $\Sigma \subseteq \Sigma'$ and $\Sigma \vdash \varphi$then $\Sigma' \vdash \varphi$;
(2) If $\Sigma \vdash \varphi$ then there exists some finite $\Sigma_0 \subseteq \Sigma$ so that $\Sigma_0 \vdash \varphi$;
(3) if $\Sigma' \vdash \varphi$ and for all $\psi \in \Sigma'$ we have $\Sigma \vdash \psi$, then $\Sigma \vdash \varphi$.

24. A deductive formal system for first order logic

We now fixed a deductive system for first order logic. There are many other equivalent ones but this one here has the advantage that there is a single deductive rule: the modus ponens.

Recall the logical symbols for first order logic: $\neg \ \Rightarrow \ (\ )\ , \ \forall \ = \ x_1 \ x_2 \ x_3 \ldots$

Notice that we use $\Rightarrow$ instead of $\wedge$ but of course we in the standard interpretation we intend $\Rightarrow$ and $\wedge$ are definable from one another. If φ is a formula in $\mathcal{L}$ and $y_1, y_2, \ldots, y_n$ are any variables then the formula $\forall y_1 \cdots \forall y_n \varphi$ is called a **generalization** of φ.

Axioms. The logical axioms that we are going to use for the deductive formal system of first order logic are all possible generalizations of all formulas of the form:

(1) Propositional axioms.
  (a) $\varphi \Rightarrow (\psi \Rightarrow \varphi)$;
  (b) $\big(\varphi \Rightarrow (\psi \Rightarrow \chi)\big) \Rightarrow \big((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi)\big)$;
  (c) $(\neg\varphi \Rightarrow \neg\psi) \Rightarrow \big((\neg\varphi \Rightarrow \psi) \Rightarrow \varphi\big)$
(2) Quantifier axioms.
  (a) $\forall x(\phi \Rightarrow \psi) \Rightarrow (\forall x\phi \Rightarrow \forall x\psi)$
  (b) $\varphi \implies \forall x\varphi$
  (c) $\forall x\varphi \Rightarrow \varphi(t \rightsquigarrow x)$ where t is any term that is *substitutable for x in φ*, i.e., no variable z occurring in t is in the scope of a quantifier $\forall z$ in φ, e.g., if $\varphi \equiv \exists y(x \neq y)$ and $t \equiv y$ then $\forall x\varphi \not\Rightarrow \varphi(t \rightsquigarrow x)$;
(3) Equality axioms.
  (a) $x = x$, $(x = y \wedge y = z) \Rightarrow x = z$, $x = y \Rightarrow y = x$;
  (b) $(y_1 = z_1 \wedge \cdots \wedge y_n = z_n) \Rightarrow \big(R(\bar{y}) \Rightarrow R(\bar{z})\big)$ where R is a relation in $\mathcal{L}$;
  (c) $(y_1 = z_1 \wedge \cdots \wedge y_n = z_n) \Rightarrow f(\bar{y}) = f(\bar{z})$ where f is a function in $\mathcal{L}$;
  (d) $c = c$ where c is a constant in $\mathcal{L}$.

Rules of inference. We have only one rule of inference. That is

(Modus Ponens:) $\qquad\qquad D(\varphi, \varphi \Rightarrow \psi, \psi)$

It is easy to see that all logical axioms are tautologies and that for every $\mathcal{L}$-structure $\mathcal{A}$ and any tuple $\bar{a}$ of elements from A if $\mathcal{A} \models \varphi(\bar{a})$ and $\mathcal{A} \models (\varphi \Rightarrow \psi)(\bar{a})$ then $\mathcal{A} \models \psi(\bar{a})$. In other words, we have that for every formula φ, if $\models \varphi$ then $\vdash \varphi$. Gödels completeness theorem says that for complete enough deductive systems as the one we fixed, we have that the other direction is also true.

Theorem 55 (Gödel's completeness theorem)**.** *Let Σ be a collection of $\mathcal{L}$-formulas and let φ be any $\mathcal{L}$-formula. We have that*

$$\Sigma \models \varphi \implies \Sigma \vdash \varphi.$$

In particular, together with the above observation we have that $\Sigma \models \varphi \iff \Sigma \vdash \varphi$.

A corollary of this and of the property (2) at the end of the previous subsection is the compactness theorem.

Corollary 56. *If $\Sigma \models \varphi$ then there exists some finite $\Sigma_0 \subseteq \Sigma$ so that $\Sigma_0 \models \varphi$.*

The proof of Theorem 55 is given in math 6c but I am going to outline the main ideas of the proof here. First one shows that Theorem 55 follows from what is known as second form of Gödel's completeness theorem.

Definition 57. Let Σ be a collection of $\mathcal{L}$-formulas. We say that Σ is **inconsistent** if it proves some formula $\neg\varphi$ there φ is a tautology. Otherwise we say that Σ is consistent.

For example Σ is inconsistent if it proves $(x = x \wedge \neg x = x)$. In fact it is an exercise to prove that if Σ is inconsistent then it proves every formula ψ. Notice now that if for some $\mathcal{L}$-structure $\mathcal{A}$ we have that $\mathcal{A} \models \Sigma$ then, by the definition of a tautology and the symbol $\models$, we have that Σ is consistent. The second form of Gödel's completeness theorem says that the opposite is also true.

Theorem 58 (Gödel's completeness theorem 2nd form)**.** *Let Σ be a collection of $\mathcal{L}$-formulas. If Σ is consistent then there exists some $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \models \Sigma$.*

To see that the second Theorem implies the first let Σ and φ as in the first and assume that $\Sigma \models \varphi$. We will show that $\Sigma \vdash \varphi$. Notice first that $\Sigma \models \varphi$ implies that $\Sigma \cup \{\neg\varphi\}$ has no model. By the second incompleteness theorem we have that $\Sigma \cup \{\neg\varphi\}$ is inconsistent, i.e., $\Sigma \cup \{\neg\varphi\} \vdash \neg x = x$. We will now show that this implies that $\Sigma \vdash \neg\varphi \implies \neg x = x$. But $\Sigma \vdash \neg\varphi \implies x = x$ by axiom (1)(a) and (3)(a). Therefore, by axiom (1)(c) we have that $\Sigma \vdash \varphi$.

Lemma 59 (Deduction Lemma)**.** *If $\Sigma \cup \{\psi\} \vdash \chi$, then $\Sigma \vdash \psi \Rightarrow \chi$.*

Proof. This is an induction on the length of the proof $\varphi_1, \ldots, \varphi_n$ of χ out of $\Sigma \cup \{\psi\} \vdash \chi$.

It is left as an exercise.

□

As a consequence Theorem 58 implies Theorem 55. We can now sketch the proof of the later.

Proof of Theorem 58. Let Σ be a consistent collection of $\mathcal{L}$-formulas. We have to construct somehow an $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \models \Sigma$. Since the only material we have is syntactic the structure $\mathcal{A}$ will be constructed by syntactic material. This is done in steps which I will describe but not prove.

Step 1. One has to show that any consistent Σ can be extended to a Σ' that is complete, in that for every φ, either $\varphi \in \Sigma$ or $\neg\varphi \in \Sigma$. So we can assume from now on that Σ is complete.

Step 2. Then one adds witnesses to existential formulas. For every sentence σ of the form $\exists x\varphi(x)$ so that $\Sigma \vdash \sigma$, we add a new constant c_σ in the language and extend $\mathcal{L}$ and Σ to $\mathcal{L}^+, \Sigma^+$ with

$$\mathcal{L}^+ = \{c_\sigma \colon \sigma \equiv \exists x\varphi(x), \Sigma \vdash \sigma\},$$
$$\Sigma^+ = \{\varphi(c_\sigma) \colon \sigma \equiv \exists x\varphi(x), \Sigma \vdash \sigma\}.$$

We repeat this step countably many times defining $\mathcal{L}^n = (\mathcal{L}_{n-1})^+$ and $\Sigma^n = (\Sigma_{n-1})^+$ and take $\mathcal{L}^\infty$ and Σ^∞ be the union.

Step 3. The domain of $\mathcal{A}$ is defined to be the quotient of the set of all terms in $\mathcal{L}^\infty$ containing no free variables, via the equivalence relation

$$t \simeq s \iff \Sigma^\infty \vdash t = s$$

By axioms (3)(a) we have that $\simeq$ is indeed an equivalence relation. We define $R^{\mathcal{A}}$ by

$$([t_1], \dots, [t_n]) \in R^{\mathcal{A}} \iff \Sigma^\infty \vdash R(t_1, \dots, t_n)$$

By axioms (3)(b), (3)(c), (3)(d) this is well defined.

Step 4. By consistency of Σ it follows that $\mathcal{A}$ is indeed an $\mathcal{L}^\infty$ structure and that $\mathcal{A} \models \Sigma^\infty$. Forgetting all interpretation of symbols in $\mathcal{L}^\infty \setminus \mathcal{L}$ we get the reduct $\mathcal{A}\restriction\mathcal{L}$ which is an $\mathcal{L}$-structure satisfying Σ.

□

25. Coordinatization and Gödel-Tarski incompleteness

.

Draw Sent explain $\Sigma \models \sigma$ and $\Sigma \vdash \sigma$

Fix $\mathcal{L}_{\mathcal{N}}$ explain tautologies from the point of view of $\models$ and $\vdash$.

Fix $\mathcal{N}$ and draw $\mathrm{Th}(\mathcal{N})$.

Weak form of Gödel incompleteness (Gödel-Tarski): If Σ is "recursive" subset of $\mathrm{Th}(\mathcal{N})$ then there is $\sigma \in \mathrm{Th}(\mathcal{N})$ with $\Sigma \nvdash \sigma$

As in the first section we want to turn various meta-mathematical statements of arithmetic into statements about numbers. To do that we are going to "coordinatize" the formal language of arithmetic. In fact, instead of restricting our attention to $\mathcal{L}_{\mathcal{N}} = \{0, S, +, *, \leq\}$ we will show how to "coordinatize" the arbitrary countable formal language just in case we want to add more symbols later which do not appear in $\mathcal{L}_{\mathcal{N}}$.

Let $\mathcal{L} = \{R_1, R_2, \ldots\} \sqcup \{f_1, f_2, \ldots\} \sqcup \{c_1, c_2, \ldots\}$ be a countable language. Let also $\neg, \Rightarrow, \forall, (,), \mathrm{Comma}, =, x_1, x_2, x_3, \cdots$ be the logical symbols for first order logic.

Coding pure symbols. If a is any of the above symbols which is not a variable or a constant we assign to it its Gödel number $\langle a \rangle$ which is going to be equal to $\langle 0, n \rangle$ for some n (we pre-fix some informal correspondence $n \Leftrightarrow a$). For example let

$$\langle \neg \rangle := \langle 0, 0 \rangle,\ \langle \Rightarrow \rangle := \langle 0, 1 \rangle\ , \cdots, \langle = \rangle := \langle 0, 6 \rangle,$$

$$\langle R_n \rangle := \langle 0, 6 + (2n - 1) \rangle$$

$$\langle f_n \rangle := \langle 0, 6 + 2n \rangle$$

Coding terms. Let $\langle x_n \rangle := \langle 1, 2n - 1 \rangle$, $\langle c_n \rangle := \langle 1, 2n \rangle$, and the rest of the terms defined inductively by

$$\langle f(t_1, \ldots, t_m) \rangle := \langle 1, \langle f \rangle, \langle t_1 \rangle, \ldots, \langle t_m \rangle \rangle$$

Coding formulas. Similarly by induction:

$$\langle R(t_1, \ldots, t_m) \rangle := \langle 2, \langle R \rangle, \langle t_1 \rangle, \ldots, \langle t_m \rangle \rangle$$

$$\langle t = s \rangle := \langle 2, \langle = \rangle, \langle t \rangle, \langle s \rangle \rangle$$

Coding sequences of formulas. If $\varphi_0, \ldots, \varphi_n$ is a sequence of formulas then

$$\langle \varphi_0, \ldots, \varphi_n \rangle := \langle \langle \varphi_0 \rangle, \ldots, \langle \varphi_n \rangle \rangle$$

Having coordinatized all these expressions we can now collect the sets

- $\mathrm{VAR}(n) \iff n$ is the Gödel number of a variable;
- $\mathrm{TERM}(n) \iff n$ is the Gödel number of a term;
- $\mathrm{FORM}(n) \iff n$ is the Gödel number of a formula;
- $\mathrm{SENT}(n) \iff n$ is the Gödel number of a sentence;
- $\mathrm{LogicAX}(n) \iff n$ is the Gödel number of a logic axiom;
- $\mathrm{ModusPO}(k, l, m) \iff \mathrm{FORM}(k) \wedge \mathrm{FORM}(l) \wedge \mathrm{FORM}(m) \wedge$(the formula coded by m is the result of modus ponens from the formulas coded by k, l);
- $\mathrm{PROOF}(n) \iff n$ is the Gödel number of a proof.

These sets depend on the particular language we fixed, however they are always primitive recursive sets and therefore definable in $\mathcal{N}$. For example:

$$\mathrm{PROOF}(n) \iff \mathrm{Seq}(n) \wedge (\forall i < \mathrm{length}(n)\mathrm{FORM}((n)_i)) \wedge$$
$$\wedge \forall i < \mathrm{length}(n)(\mathrm{LogicAX}((n)_i) \vee \exists j, k < i \ \ \mathrm{ModusPO}((n)_j, (n)_k, (n)_i)).$$

Definition 60. Let Φ be a collection of formulas. We say that Φ is recursive if

$$\langle \Phi \rangle := \{\langle \varphi \rangle : \varphi \in \Phi\}$$

is recursive as a subset of $\mathbb{N}$.

Given any set Φ of formulas one defines $\mathrm{PROOF}_\Phi(n)$ to be the collection of all numbers which code sequences of proofs from Φ. If Φ is recursive then, as above, $\mathrm{PROOF}_\Phi(n)$ is recursive.

Definition 61. A **theory** is a collection T of sentences which is closed under implication, i.e., if $T \vdash \sigma$ then $\sigma \in T$. A theory T is **recursively axiomatizable** if there is a recursive set of sentences Σ so that $T = \mathrm{Conseq}(\Sigma)$, where

$$\mathrm{Conseq}(\Sigma) = \{\sigma \colon \sigma \text{ is a sentence with } \Sigma \vdash \sigma\}$$

A collection of sentences Σ is **complete** if for every σ we have that $\Sigma \vdash \sigma$ or $\Sigma \vdash \neg\sigma$.

Corollary 62. *If Σ is a recursive set of formulas then $\langle \mathrm{Conseq}(\Sigma) \rangle$ is recursively enumerable. If Σ is moreover complete then $\langle \mathrm{Conseq}(\Sigma) \rangle$ is recursive.*

Proof.

$$n \in \langle \mathrm{Conseq}(\Sigma) \rangle \iff \mathrm{SENT}(n) \wedge \exists m \ (\mathrm{PROOF}_\Phi(m) \wedge (m)_{\mathrm{length}(m)-1} = n),$$

which is an R.E. definition. For the second part of the statement we can assume that Σ is consistent because otherwise $\langle \mathrm{Conseq}(\Sigma) \rangle$ is just SENT. But then

$$n \in \langle \mathrm{Conseq}(\Sigma) \rangle \iff \mathrm{SENT}(n) \wedge \neg\exists m \ (\mathrm{PROOF}_\Phi(m) \wedge (m)_{\mathrm{length}(m)-1} = g(n)),$$

where $g(n)$ is the Gödel code of the negation of the sentence coded by n. □

Theorem 63 (Gödel incompleteness theorem (weak form))**.** *If Σ is a recursive collection of sentences with $\mathcal{N} \models \Sigma$ then Σ is not complete.*

Proof. If Σ is complete and $\Sigma \subseteq \mathrm{Th}(\mathcal{N})$ then $\mathrm{Conseq}(\Sigma) = \mathrm{Th}(\mathcal{N})$. So if Σ is recursive then $\langle \mathrm{Th}(\mathcal{N}) \rangle = \{\langle \sigma \rangle : \mathcal{N} \models \sigma\}$ is R.E. and therefore arithmetical (i.e., definable in $\mathcal{N}$). But by Tarksi's theorem this is not possible. □

Theorem 64 (Tarski)**.** $\langle \mathrm{Th}(\mathcal{N}) \rangle = \{\langle \sigma \rangle : \mathcal{N} \models \sigma\}$ *is not arithmetical.*

Proof. Notice that there is no binary relation U which is arithmetical and universal for arithmetical subsets of $\mathbb{N}$ (since arithmetical sets are closed under complements and primitive recursive substitution). But then if $\langle \mathrm{Th}(\mathcal{N}) \rangle$ is arithmetical, i.e., if there is a formula ψ with

$$n \in \langle \mathrm{Th}(\mathcal{N}) \rangle \iff \mathcal{N} \models \psi(n),$$

we can let $U(m,n) \iff$ "m codes a formula of the form $\varphi(x_1)$ and $\mathrm{Th}(\mathcal{N}) \models \varphi(n)$." It is clearly universal but also arithmetical since the partial map $g\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ with $(\langle\varphi(x_1)\rangle, n) \mapsto \langle\varphi(\underline{n})\rangle$ is recursive and therefore arithmetical. □

The subset $\langle\mathrm{Th}(\mathcal{N})\rangle$ of $\mathbb{N}$ is therefore not in Σ^0_n for any any n. What is its complexity? Recall that for every n we have a Σ^0_n-complete set $C_n \subseteq \mathbb{N}$. Consider the set

$$C = \oplus_n C_n := \{\langle n, m\rangle \colon m \in C_n\}.$$

It turns out that $[C]_T = [\langle\mathrm{Th}(\mathcal{N})\rangle]_T$ and this Turing degree is denoted by $\underset{\sim}{0}^{\omega}$.

26. Representability

The weak form of Gödel's incompleteness was "centered" around $\mathrm{Th}(\mathcal{N})$: part of the assumption was that $\Sigma \subseteq \mathrm{Th}(\mathcal{N})$. The original theorem of Gödel is stronger in that it replaces this assumption with a weaker one. For that, we will need to abandon the notion of "definability", based on semantic notion $\mathcal{N} \models \varphi(\bar{a})$, for a syntactic notion which we will call *representability*.

We fix some $\mathcal{L} \supseteq \{0, S\}$. This way, in every $\mathcal{L}$-structure we have the term

$$\underline{n} = \overbrace{S(S(\cdots(S}^{n-\text{times}}(0))\cdots),$$

for every $n \geq 0$. Let Q be any fixed collection of sentences. A set $R \subseteq \mathbb{N}^n$ is called **representable in** Q if there is a formula $\varphi(x_1, \ldots, x_n)$ in $\mathcal{L}$ so that

$$(k_1, \ldots, k_n) \in R \implies Q \vdash \varphi(\underline{k_1}, \ldots, \underline{k_n}), \text{ and}$$

$$(k_1, \ldots, k_n) \in R^c \implies Q \vdash \neg\varphi(\underline{k_1}, \ldots, \underline{k_n}).$$

A partial function $f\colon \mathbb{N}^n \to \mathbb{N}$ is called **representable in** Q if there is a formula $\varphi(x_1, \ldots, x_n, x)$ so that

$$Q \vdash \forall x_1 \ldots \forall x_n \forall y \forall z \big(\varphi(x_1, \ldots, x_n, y) \wedge \varphi(x_1, \ldots, x_n, z) \Rightarrow y = z\big), \text{ and}$$

$$f(k_1, \ldots, k_n) = l \implies Q \vdash \varphi(\underline{k_1}, \ldots, \underline{k_n}, \underline{l}), \text{ for all } k_1, \ldots, k_n, l \in \mathbb{N}$$

Theorem 65. *Let $\mathcal{L} \supseteq \{0, S\}$ and let Q be any collection of sentences so that every recursive relation and function are Q-representable. Then $\langle \mathrm{Conseq}(Q) \rangle$ is not Q-representable.*

Proof. Same proof as Tarski's theorem. □

Question. How large does Q have to be so that all recursive relations and functions are Q-representable?

The following system due to Robinson is large enough. Notice moreover that it is finite and it does not contain any instance of an induction axiom (except perhaps the definition of $+, *$, and $<$).

Robinson System Q_0. It consists of the following axioms in $\mathcal{L} = \{0, S, +, *, <\}$:

(1) $\forall x(S(x) \neq 0)$;
(2) $\forall x\big(x \neq 0 \Rightarrow \exists y(S(y) = x)\big)$;
(3) $\forall x \forall y(S(x) = S(y) \implies x = y)$;
(4) $<$ is a linear ordering;
(5) $\forall x \forall y\big(x < S(y) \iff (x = y \vee x < y)\big)$;
(6) $\forall x(x = 0 \vee 0 < x)$;
(7) $\forall x(x + 0 = x) \wedge \forall x \forall y(x + S(y) = S(x + y))$;
(8) $\forall x(x * 0 = 0) \wedge \forall x \forall y(x * S(y) = x * y + x)$.

Exercise 66 (Wrong exercise need to assume slightly stronger axioms)**.** *Let* $\mathcal{A} = (A, 0^{\mathcal{A}}, S^{\mathcal{A}}, +^{\mathcal{A}}, *^{\mathcal{A}}, <^{\mathcal{A}})$ *be any structure with* A *countable and which satisfies the axiom system* Q_0*. Consider the "non-standard part" of* A*:*

$$\Omega = \{a \in A\colon \text{ for all } n \geq 0 \text{ we have that } \mathcal{A} \models \underline{n} < a\}.$$

When $\mathcal{A}$ *is the standard model of arithmetic* $\mathcal{N}$*, then* $\Omega = \emptyset$*. However, not every structure satisfying* Q_0 *has this property. Prove that:*

(1) the domain A *of* $\mathcal{A}$ *is the union of* Ω *and of the set* $\{0^{\mathcal{A}}, \underline{1}^{\mathcal{A}}, \underline{2}^{\mathcal{A}}, \ldots\}$*;*

(2) if $\Omega \neq \emptyset$*, then the ordering* $<^{\mathcal{A}}$ *restricted on* Ω*, i.e.* $(\Omega, <^{\mathcal{A}} \restriction \Omega \times \Omega)$*, is isomorphic to "*$(\mathbb{Q}, <)$*-many copies of* $(\mathbb{Z}, <)$*." By* $(\mathbb{Q}, <)$*-many copies of* $(\mathbb{Z}, <)$ *we mean the ordering defined on* $\mathbb{Q} \times \mathbb{Z}$ *by*

$$(p, a) < (q, b) \iff (p < q) \vee \big((p = q) \wedge a < b\big)$$

where $(\mathbb{Q}, <)$ *is the usual ordering on the rationals and* $(\mathbb{Z}, <)$ *is the usual ordering on the integers. (Hint: By a theorem of Cantor* $(\mathbb{Q}, <)$ *is the unique countable linear ordering that is dense and has no endpoints).*

Theorem 67. *Every recursive function and relation are representable in* Q_0*.*

As usual it is enough to show that all (partial) recursive functions are Q_0-representable. We will show actually that all min-recursive functions are Q_0-representable which is equivalent by HW. First we isolate in the next lemma some easy facts.

Lemma 68. *For every fixed* $m, n, p \in \mathbb{N}$ *we have that:*

(1) $Q_0 \vdash \forall x(x < \underline{n+1} \Rightarrow x = \underline{0} \vee x = \underline{1} \vee \cdots \vee \underline{n})$*;*

(2) if $m + n = p$ *then* $Q_0 \vdash \underline{m} + \underline{n} = \underline{p}$*;*

(3) if $m * n = p$ *then* $Q_0 \vdash \underline{m} * \underline{n} = \underline{p}$*;*

(4) if $m \neq n$ *then* $Q_0 \vdash \neg \underline{m} = \underline{n}$*;*

(5) if $m < n$ *then* $Q_0 \vdash \underline{m} < \underline{n}$*.*

Proof. We could of course produce an entirely syntactic proof of these facts based on the axioms of the fixed deductive system, the axioms in Q_0 and the definition of $\vdash$. However, completeness theorem Theorem 55) allows us to argue semantically. One needs to show that for every structure $\mathcal{A} = (A, 0^{\mathcal{A}}, S^{\mathcal{A}}, +^{\mathcal{A}}, *^{\mathcal{A}}, <^{\mathcal{A}})$ with $\mathcal{A} \models Q_0$ we have that $\mathcal{A} \models \sigma$, where σ is any of the statements (1)-(5). Checking that something holds for all $\mathcal{A}$ with $\mathcal{A} \models Q_0$ is often a hard task, but for simple statements like (1)-(5) things follow easily directly from the definition of $\models$.

(1) is proved by induction on n using axioms (5),(6) of Q_0. (2) is proved by induction on n using axiom (7) of Q_0. (3) is proved by induction on n using axiom (8) of Q_0. (4) is proved by induction on n using axioms (1),(2),(3) of Q_0. (5) is proved by induction on n using axiom (6) of Q_0.

For example let's do (4).

Base case ($n = 0$): if $m \neq 0$, then $\underline{m} = S(\underline{m-1})$. But then every $\mathcal{A}$ which satisfies $Q_0(1)$ is bound to satisfy $\underline{m}^{\mathcal{A}} \neq \underline{0}^{\mathcal{A}}$. So, by Gödel's completeness (Theorem

55), if $m \neq 0$ then

$$Q_0 \vdash \neg(\underline{m} = \underline{0})$$

Inductive step ($n = k + 1$): if $m = 0$ then argue as in the base case. Otherwise $m = l + 1$. So $\underline{n} = S(\underline{k})$ and $\underline{m} = S(\underline{l})$, and since $n \neq m$ we have $k \neq l$ as well. But then by inductive hypothesis $Q_0 \vdash \neg(\underline{l} = \underline{k})$ and therefore by $Q_0(3)$ we have $Q_0 \vdash \neg(\underline{m} = \underline{n})$. □

We can now proceed to the proof of Theorem 67.

Proof of Theorem 67. By HW it is enough to show that every min-recursive partial function is representable. So we need to confirm that $c_0, \mathrm{proj}_i^n, +, *, \chi_=$ are representable and that representable maps are closed under composition and under minimalization.

c_0 **is representable**. Let $\varphi(x, y) \equiv y = 0$. Then by completeness theorem

$$Q_0 \vdash \forall x \forall y \forall z \big(\varphi(x, y) \wedge \varphi(x, z) \Rightarrow y = z\big),$$

since in every $\mathcal{L}$-structure $\mathcal{A}$ in which $\mathcal{A} \models \varphi(x, y)$ and $\mathcal{A} \models \varphi(x, z)$, i.e., $\mathcal{A} \models y = 0$ and $\mathcal{A} \models z = 0$, we have that $\mathcal{A} \models y = z$ (because of the way we have tuned by definition constants and equality with $\models$).

Similarly if for some $k, l \in \mathbb{N}$ we have $c_0(k) = l$, then $l = 0$ and therefore $Q_0 \vdash \varphi(\underline{k}, \underline{l})$, i.e., $Q_0 \vdash \underline{0} = 0$, that is $Q_0 \vdash 0 = 0$, by the last logical axiom in our fixed deduction system (or using completeness again).

Representable functions are closed under μ. Assume that we have a function $g(n_1, \ldots, n_k, m) = l$ from $\mathbb{N}^{k+1}$ to $\mathbb{N}$ that is Q_0-representable by $\varphi_g(\bar{x}, y, z)$. Consider the formula

$$\varphi(\bar{x}, y) \equiv \big(\varphi_g(\bar{x}, y, 0) \wedge \forall w < y \; \exists z \; (z \neq 0 \wedge \varphi_g(\bar{x}, w, z))\big)$$

We claim that $\varphi(\bar{x}, y)$ Q_0-represents $f(n_1, \ldots, n_k) = \mu m[g(n_1, \ldots, n_k, m) = 0]$. If in some $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \models Q_0$ we had that $\mathcal{A} \models \varphi(\bar{a}, b)$ and $\mathcal{A} \models \varphi(\bar{a}, c)$, for some $\bar{a}, b, c \in A$, then by axiom $Q_0(4)$ we have $b \leq c$ of $c \leq b$ but then by formula φ they cannot be but equal, so

$$Q_0 \vdash \forall \bar{x} \forall y \forall z \big(\varphi(\bar{x}, y) \wedge \varphi(\bar{x}, z) \Rightarrow y = z\big).$$

If now $f(n_1, \ldots, n_k) = m$ then $g(n_1, \ldots, n_k, m) = 0$ but

$$g(n_1, \ldots, n_k, 0) = l_0, \; g(n_1, \ldots, n_k, 1) = l_1, \ldots, g(n_1, \ldots, n_k, m-1) = l_{m-1}.$$

with $l_0, \ldots, l_{m-1} \neq 0$. But then by Q_0-representability of g and (1) of the previous Lemma we have that $Q_0 \vdash \varphi(\underline{n_1}, \ldots, \underline{n_k}, \underline{m})$. □

27. Gödel's incompleteness theorem

A careful reading of what we have done so far shows that we have already proved the existential (i.e. non-constructive) **strong version** of Gödel's incompleteness theorem:

Theorem 69 (Gödel's 1st incompleteness theorem)**.** *Let Q be a recursive set of axioms in the language of arithmetic so that $Q_0 \subseteq Q$. If A is consistent then Q is incomplete (i.e. there is some sentence σ so that neither $Q \vdash \sigma$ nor $Q \vdash \neg\sigma$) and undecidable (i.e.* Conseq(Q) *is not recursive)*

This follows directly from Theorem 65, Corollary 62 and Theorem 67. To see this, first notice that by Corollary 62, if Q was complete then Conseq(Q) would be recursive. So it suffice to show that Conseq(Q) is not recursive. But if it was recursive then by Theorem 67 it would be representable contradicting Theorem 65. However, our task here is to produce an explicit statement σ out of Q that neither σ nor $\neg\sigma$ are provable by Q.

Before we do that we will state and prove the following useful corollary:

Corollary 70. *If T is recursively axiomatizable and consistent theory which is "at least as strong as Q_0" then T is undecidable (i.e., not recursive) and incomplete.*

Notice that we have not specified anything about the language in which we formulated the theory T. Indeed this theorem is flexible from this point of view. We need to define what "*at least as strong*" means and show how to deduce the corollary from Theorem 69

Let $\mathcal{L}^*, \mathcal{L}$ be two languages and let T be an $\mathcal{L}$-theory. By an **interpretation** $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$ of $\mathcal{L}^*$ into $(\mathcal{L}, T)$ we mean

(1) an $\mathcal{L}$ formula $\pi_U(x)$ so that $T \models \exists x \pi_U(x)$;
(2) assignments $R(\bar{x}) \mapsto \pi_R(\bar{x})$, $f(\bar{x}) \mapsto \pi_f(\bar{x}, y)$, $c \mapsto \pi_c(x)$ from the relation,function, and constant symbols of $\mathcal{L}^*$ to $\mathcal{L}$-formulas such that:
   (a) $T \models \forall \bar{x} \left(\pi_U(x_1) \wedge \ldots \wedge \pi_U(x_n) \Rightarrow \exists! y \left(\pi_U(y) \wedge \pi_f(\bar{x}, y)\right)\right.$ for every f;
   (b) $T \models \exists! x \pi_U(x) \wedge \pi_c(x)$ for every constant c.

Given an interpretation $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$ of $\mathcal{L}^*$ into $(\mathcal{L}, T)$ we have an assignment $\mathcal{A} \mapsto \mathcal{A}^*$ from $\mathcal{L}$-structures $\mathcal{A}$ which satisfy the theory T, to $\mathcal{L}^*$-structures $\mathcal{A}^*$: given $\mathcal{A}$ as above we construct $\mathcal{A}^*$ as follows

- the domain A^* of $\mathcal{A}^*$ is $\{a \in A \colon \mathcal{A} \models \pi_U(a)\}$.
- the interpretations of R, F, c's of $\mathcal{L}^*$ are given by the π_R, π_F, π_c's

Example. Let $\mathcal{L}^* = \{0, S, +, *, <\}$ be the language of arithmetic and let $\mathcal{L} = \{+, *\}$. If $T = \mathrm{Th}\big((\mathbb{Z}, +^{\mathbb{Z}}, *^{\mathbb{Z}}\big)$, then we have the interpretation $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$ given by

$$\pi_U(x) \equiv \exists x_1 \exists x_2 \exists x_3 \exists x_4 (x_1^2 + x_2^2 + x_3^2 + x_4^2 = x)$$

$$\pi_<(x_1, x_2) \equiv (x_1 \neq x_2) \wedge \exists x (\pi_U(x) \wedge x + x + 1 = x_2)$$

$$\pi_+(x_1, x_2, y) \equiv x_1 + x_2 = y, \quad \pi_*(x_1, x_2, y) \equiv x_1 * x_2 = y, \quad \pi_0(x) \equiv x + x = x.$$

Given any interpretation $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$ we can a complete one-way dictionary from $\mathcal{L}^*$-formulas φ to $\mathcal{L}$-formulas φ_π: the atomic $\mathcal{L}^*$-formulas are assigned to the obvious $\mathcal{L}$-formulas, e.g., $\varphi \equiv R(f(x), c)$ is translated to

$$\varphi_\pi \equiv \exists y \exists z (\pi_f(x, y) \wedge \wedge \pi_c(z) \wedge \pi_R(y, z)).$$

Inductively then we proceed by setting

$$(\neg\varphi)_\pi := \neg\varphi_\pi, \quad (\varphi \implies \psi)_\pi := \varphi_\pi \implies \psi_\pi, \quad (\exists x\varphi)_\pi := \exists x(\pi_U(x) \wedge \varphi_\pi).$$

By a simple induction we then have that if $\mathcal{A}^*$ is the canonical $\mathcal{L}^*$-structure constructed by $\mathcal{A}$ under $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$ then for every $\mathcal{L}^*$-formula φ and any $\bar{a}$ in A^* we have that:

$$\mathcal{A}^* \models \varphi(\bar{a}) \iff \mathcal{A} \models \varphi_\pi(\bar{a})$$

Definition 71. Let Q be a collection of sentences in $\mathcal{L}^*$ and let T be a theory in $\mathcal{L}$ By an **interpretation** $Q \curvearrowright T$ of Q into T we mean an interpretation $\mathcal{L}^* \curvearrowright (\mathcal{L}, T)$, under which $T \models \sigma_\pi$, for all $\sigma \in Q$.

Definition 72. A theory T in $\mathcal{L}$ is **at least as strong as** Q in T if and only if there exists an interpretation $Q \curvearrowright^\pi T$ of Q into T so that the assignment $\langle\sigma\rangle \mapsto \langle\sigma_\pi\rangle$ is recursive.

Notice that in order to check that $\langle\sigma\rangle \mapsto \langle\sigma_\pi\rangle$ is recursive it will suffice to check that $R, F, c \mapsto \pi_R, \pi_F, \pi_c$ is recursive which is automatically satisfied, for example, when $\mathcal{L}^*$ is finite.

We can now prove Corollary 70 from Theorem 69.

Proof of Corollary 70. It suffice to show that T is undecidable. This will imply by Corollary 62 that it is also incomplete. Assume that T was decidable and let $Q = \{\sigma \mid \sigma_\pi \in T\}$. Notice that since T is decidable so is Q (since $\langle\sigma\rangle \mapsto \langle\sigma_\pi\rangle$ is recursive) and since T is consistent so is Q. But Q also contains Q_0, contradicting Theorem 69. □

In what follows we assume throughout that $\mathcal{L} \supseteq \{0, 1\}$ and Q is a set of sentences which represents all recursive relations/functions (e.g. $Q_0 \subseteq Q$).

Lemma 73 (Gödel's fixed point lemma)**.** *For every $\mathcal{L}$-formula $\varphi(x)$ there is a sentence σ so that*

$$Q \vdash \sigma \iff \varphi(\langle\sigma\rangle)$$

Proof. Consider the map

$$\mathrm{Subs}(m, n) \begin{cases} \langle\varphi(\underline{n})\rangle & \text{if } m = \langle\varphi(x)\rangle; \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that it is recursive and therefore we can find a formula $\chi(x, y, z)$ which represents the graph of Subs. Let $\psi(x) \equiv \forall z\big(\chi(x, x, z) \Rightarrow \varphi(z)\big)$ and set $k = \langle\psi(x)\rangle$. We claim that the required sentence is $\sigma \equiv \psi(\underline{k})$. What is the code for σ? $\langle\sigma\rangle = \langle\psi(\underline{k})\rangle = \mathrm{Subs}(k, k)$. So $Q \vdash \varphi(\langle\sigma\rangle)$ is simply $Q \vdash \varphi(\underline{\mathrm{Subs}(k, k)})$. But

$$Q \vdash \varphi(\underline{\mathrm{Subs}(k, k)}) \iff \forall z\big(\chi(\underline{k}, \underline{k}, z) \Rightarrow \varphi(z)\big)$$

where the last expression is σ. □

Assume now moreover that Q is recursive. Then $\text{Proof}_Q(n,p) \iff$ "n codes a sentence σ, p codes a proof of σ from Q" is recursive and therefore Q_0-representable by a formula, say $\text{Proof}_Q(x,y)$. Consider the formula

$$\text{Prvbl}_Q(x) \equiv \exists y \text{Proof}_Q(x,y),$$

and let σ_Q be the Gödel sentence for its negation, i.e.,

$$Q \vdash \sigma_S \iff \neg\text{Prvbl}_Q(\underline{\langle\sigma_Q\rangle}).$$

Think of σ_Q as the statement "I am not provable."

Here is the original theorem due to Gödel which assumes something more than consistency, that is, ω-consistency, and we are going to define it during the proof:

Theorem 74. *We have that:*

(1) If Q is consistent then $Q \nvdash \sigma_Q$;
(2) If Q is ω-consistent then $Q \nvdash \neg\sigma_Q$;

Proof. For (1): assume that $Q \vdash \sigma_Q$. This by definition means that there is $p \in \mathbb{N}$ so that $\text{Proof}_Q(\underline{\langle\sigma_Q\rangle}, p)$. By representability of Proof_Q we have

$$Q \vdash \text{Proof}_Q(\underline{\langle\sigma_Q\rangle}, p), \text{ and therefore } Q \vdash \text{Prvbl}_Q(\underline{\langle\sigma_Q\rangle}), \text{ i.e., } Q \vdash \neg\sigma_Q,$$

which contradicts consistency. Notice that having a witness p with respect to which something is provable implies that "there exists some p" so that this thing is provable. This just follows from the axioms of the deduction system we have.

For (2): assume that $Q \vdash \neg\sigma_Q$ and we will try discover what assumption (which we will call ω-consistency) we need to add in order to get a contradiction. But $Q \vdash \neg\sigma_Q$ implies that $Q \vdash \text{Prvbl}_Q(\underline{\langle\sigma_Q\rangle})$ i.e.,

$$Q \vdash \exists y \text{Proof}_Q(\underline{\langle\sigma_Q\rangle}, y) \tag{6}$$

Assume now that from this this assumption implied that

$$\text{there is some } p \in \mathbb{N} \text{ so that } Q \vdash \text{Proof}_Q(\underline{\langle\sigma_Q\rangle}, \underline{p}) \tag{7}$$

By representability this means that p codes an actual proof of σ_Q from Q which we can now write it down and follow it ourselves in order to prove that $Q \vdash \sigma_Q$.

Of course if we had $\mathcal{N} \models$ in the place of $Q \vdash$, (6) and (7) would be equivalent. However the axioms in Q may force all the $\mathcal{L}$-structures which satisfy Q to have non-standard elements y (above all $\underline{n}$) which satisfy some formulas which are not satisfied by any $\underline{n}$...

ω-consistency: Q is ω-consistent if for all $\varphi(x)$, whenever $Q \vdash \exists y\varphi(y)$ then there exists some $p \in \mathbb{N}$ so that $\varphi(\underline{p})$ is not refutable, i.e., $Q \nvdash \neg\varphi(\underline{p})$. Of course, if $\varphi(y)$ represents some total relation such as Prvbl_Q then by definition of representability we have that $Q \vdash \varphi(\underline{p})$. □

Gödel wanted to get rid of this additional assumption. Rosser found a way to do it. For every Q as above consider the formula

$$\varphi(x) \equiv \forall y\big(\text{Proof}_Q(x,y) \Rightarrow \exists y' \leq y\ \text{Proof}_Q^{\neg}(x,y')\big),$$

where $\text{Proof}_Q^{\neg}(n,p) \subseteq \mathbb{N}^2$ holds if and only if p codes a proof for the negation of the sentence that is the code of n. The **Rosser sentence for** Q is the fixed point ρ_Q of the formula $\varphi(x)$.

Theorem 75 (Rosser)**.** *If Q is consistent then neither $Q \vdash \rho_Q$ nor $Q \vdash \neg\rho_Q$;*

Proof. Suppose that $Q \vdash \rho_Q$. Then

$$Q \vdash \forall y\big(\text{Proof}_Q(\underline{\langle\rho_Q\rangle}, y) \Rightarrow \exists y' \leq y\ \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, y')\big).$$

But since by assumption $Q \vdash \rho_Q$, we can find some p so that $Q \vdash \text{Proof}_Q(\underline{\langle\rho_Q\rangle}, \underline{p})$, and therefore, combining this with the previous statement

$$Q \vdash \exists y' \leq \underline{p}\ \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, y').$$

By a lemma we proved, Q_0 and therefore Q proves that everything that is $<$ than some $\underline{p}$ is of the form $\underline{r}$ (for some $r < p$). So

$$Q \vdash\ \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{0}) \vee \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{1}) \vee \ldots \vee \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{p}). \tag{8}$$

But from the other hand, by consistency we have that $Q \nvdash \neg\rho_Q$. So

$$Q \nvdash \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{0}), \ldots, Q \nvdash \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{p}).$$

So by representability of $\text{Proof}_Q^{\neg}$ we have that

$$Q \vdash \neg\text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{0}), \ldots, Q \vdash \neg\text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{p}),\ \text{and therefore}$$

$$Q \vdash \neg\big(\text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{0}) \vee \ldots \vee \text{Proof}_Q^{\neg}(\underline{\langle\rho_Q\rangle}, \underline{p})\big),$$

a contradiction with (8).

The second part of the statement we leave it as an exercise. □

This constructive proof (produces the witness σ_Q/ρ_Q to incompletenss) of the strong form of Gödel's incompleteness theorem gives us access to the second Gödel's incompleteness theorem:

Theorem 76 (Second Gödel's incompleteness theorem)**.** *Let Q as a recursive set of sentences with $Q_0 \subseteq Q$ and set $\bot \equiv \exists x(x \neq x)$. Consider the sentence*

$$\text{CON}_Q \equiv \neg\exists y\text{Proof}_Q(\langle\bot\rangle, y).$$

If Q is ω-consistent (or Q=Peano arithmetic) and Q is consistent then $Q \nvdash \text{CON}_Q$.

Proof. The actual proof is a bit technical although not difficult, see Boolos. Here we just give the main idea.

One of the things we proved in Theorem 74 is that **if Q is consistent** then Q **does not prove** σ_Q. Now because σ_Q was produced in a constructive fashion by a specific formula, one can go and rewrite formally down the proof of Theorem 74 step by step and turn it into a theorem about Q itself! In other words, one can show that

$$Q \vdash \text{CON}_Q \Rightarrow \neg\text{Prvbl}(\langle\sigma_Q\rangle)$$

But since σ_Q is a fixed point for $\neg\text{Prvbl}(x)$ we also have that

$$Q \vdash \sigma_Q \iff \neg\text{Prvbl}(\langle\sigma_Q\rangle).$$

Hence we have that

$$Q \vdash \text{CON}_Q \Rightarrow \sigma_Q$$

But then if $Q \vdash \text{CON}_Q$ this would give $Q \vdash \sigma_Q$ which is in contradiction with Theorem 74. □

28. Undecidable problems in Peano Arithmetic

We showed that Robinson arithmetic Q_0 is strong enough to produce the necessary self-referential statements which show that it is incomplete. However, it is not difficult to spot sentences which are neither provable nor disprovable from Q_0. In fact Q_0 cannot even prove whether that $+$ is commutative. Of course the point of Theorem 69 is that any attempt to "complete" Q_0 by adding a recursive collection of axioms $Q \supseteq Q_0$ on top will still be incomplete.

A theory of arithmetic that is strong enough to usually be able to prove most of the things one needs is the extension of Q_0 known as Peano arithmetic PA. For that one further includes in PA all sentences of the form:

$$\forall\bar{x}\Big(\big(\varphi(\bar{x},\underline{0}) \wedge \forall z(\varphi(\bar{x},\underline{n}) \Rightarrow \varphi(\bar{x},\underline{n+1}))\big) \Rightarrow \forall z\varphi(\bar{x},z)\Big)$$

Of course PA is still incomplete but finding explicit statements which unlike(?) σ_Q, ρ_Q have mathematical (rather than meta-mathematical) content is hard.

Usual Ramsey statement: for every $a, b, r \in \mathbb{N}$ there is $c \in \mathbb{N}$ so that

$$c \to (b)^a_r$$

Stronger Ramsey statement: for every $a, b, r \in \mathbb{N}$ there is $c \in \mathbb{N}$ so that

$$c \to^* (b)^a_r.$$

That is not only the monochromatic set A will satisfy $|A| \geq a$ but moreover the larger it is the further away away it has to start, i.e., $|A| > \min A$.

These can be turned into statements in the language of arithmetic. While the usual Ramsey statement is provable in PA the stronger one is not:

Theorem 77 (Paris-Harrington)**.**

$$PA \nvdash \forall a, b, r\ \exists c\ \big(c \to^* (b)^a_r\big).$$

Interestingly this has a fairly easy proof once we assume ZFC and we are able to rely on the existence of infinite sets.

Goodstein sequences. Take any number n, express it in sum of powers of k then express the exponents in powers of k, and the exponents of the exponents... For example when $n = 266$ and $k = 2$:

$$266 = 256 + 8 + 2 = 2^8 + 2^3 + 2^1 = 2^{2^{(2^{2^0}+2^0)}} + 2^{2^{2^0}+2^0} + 2^0$$

A Goodstein sequence starts with any number n then writes it in pure base 2 expansion as above. Then replaces all 2s with 3s and subtracts 1 at the end from the total expression. The result is the next term of the sequence... $n = G_1(n), G_2(n), \dots$ For example $n = 19$:

$$19 = 2^{2^{2^0}} + 2^{2^0} + 2^0$$
$$G_2(19) = 3^{3^{3^0}} + 3^{3^0} + 3^0 - 1 = 3^{3^{3^0}} + 3^{3^0} \sim 10^{13}$$
$$G_3(19) = 4^{4^{4^0}} + 4^{4^0} - 1 \sim 10^{154}, \quad G_4(19) \sim 10^{2000}, \qquad G_5(19) \sim 10^{3600}, \dots$$

Theorem 78 (Goodstein)**.** *For every n there exists k so that $G_k(n) = 0$.*

Theorem 79 (Paris-Kirby)**.**

$$PA \nvdash \forall n \, \exists k \, G_k(n) = 0$$

Few words about ordinal ε_0

29. Undecidable theories

We are going to present a technique due to Mostowski-Robinson-Tarski for showing that various mathematical theories are undecidable. Using this technique we are going to show that the theory of rings, groups, and graphs is undecidable. This technique uses in an essential way the fact that there is a **finitely axiomatizable** theory in the language of arithmetic (namely Q_0) which satisfies Theorem 69 and therefore Corollary 70.

Definition 80. Let $\mathcal{A}$ be an $\mathcal{L}$-structure in some language $\mathcal{L}$. We say that $\mathcal{A}$ is strongly undecidable if any theory T (i.e., any set of $\mathcal{L}$-sentences with $T = \text{Conseq}(T)$) with $\mathcal{A} \models T$ is undecidable.

This in particular means that both extreme cases, i.e., the theory $\text{Th}(\mathcal{A})$ of $\mathcal{A}$ as well as the collection of all tautologies $\text{Taut}(\mathcal{L})$ in $\mathcal{L}$ is undecidable.

Example: think expansions of $\text{Taut}(\mathcal{L}_{arithm})$ towards $\mathcal{N}$ vs towards the one point structure in the language of arithmetic.

Theorem 81. *The structure $\mathcal{N}$ of arithmetic is strongly undecidable.*

Proof. Let T be a theory with $\mathcal{N} \models T$ and assume towards contradiction that it is decidable. Let $T' = \{\sigma \colon (Q_0 \bigcup T) \vdash \sigma\}$. Then this would also be decidable since by the deduction lemma (Lemma 59) and the finiteness of Q_0 we have that:

$$\sigma \in T' \iff (Q_0 \bigcup T) \vdash \sigma \iff T \vdash \bigwedge Q_0 \Rightarrow \sigma \iff (Q_0 \Rightarrow \sigma) \in T,$$

and since $\langle \sigma \rangle \mapsto \langle (Q_0 \Rightarrow \sigma) \rangle$ is recursive. But this contradicts Theorem 69 since T' contains Q_0. □

Definition 82. Let $\mathcal{A}$ be some $\mathcal{L}_{\mathcal{A}}$-structure and let $\mathcal{B}$ be some $\mathcal{L}_{\mathcal{B}}$-structure. We say that $\mathcal{A}$ is definable in $\mathcal{B}$ if

(1) A is a subset of B that is definable, possibly with parameters, in $\mathcal{B}$, i.e., there is some formula $\varphi(x, x_1, \dots, x_k)$ and $b_1, \dots, b_k \in B$ so that
$$A = \{b \in B \colon \mathcal{B} \models \varphi(b, b_1, \dots, b_k)\};$$
(2) each $R^{\mathcal{A}}$ is similarly definable, possibly with parameters, in $\mathcal{B}$;
(3) the graph of each $f^{\mathcal{A}}$ is similarly definable, possibly with parameters, in $\mathcal{B}$.

Theorem 83. *Let $\mathcal{A}$ be some $\mathcal{L}_{\mathcal{A}}$-structure that is definable in some $\mathcal{L}_{\mathcal{B}}$-structure $\mathcal{B}$. If $\mathcal{A}$ is strongly undecidable and $\mathcal{L}_{\mathcal{A}}$ is finite then so is $\mathcal{B}$.*

Proof. First we show that we can assume without loss of generality that we can reduce the problem to the same problem but with $\mathcal{A}$ being definable without parameters in some new $\mathcal{B}_*$.

Notice that since $\mathcal{L}_{\mathcal{A}}$ is finite, we can find a finite subset P of B so that all parameters necessary for the definitions of $A, R^{\mathcal{A}}$s, $f^{\mathcal{A}}$s are included in P. Let $\mathcal{L}^*_{\mathcal{B}} = \mathcal{L}_{\mathcal{B}} \bigcup \{c_b \colon b \in P\}$ be a new language containing a constant c_b for every $b \in P$. Consider also the $\mathcal{L}^*_{\mathcal{B}}$-structure $\mathcal{B}_*$ to be $\mathcal{B}$ with c_b being interpreted in $\mathcal{B}_*$ as the corresponding $b \in P$.

Claim. If $\mathcal{B}_*$ is strongly undecidable then so is $\mathcal{B}$.

To see this let T be a theory in $\mathcal{L}_{\mathcal{B}}$ with $\mathcal{B} \models T$ and consider the $\mathcal{L}^*_{\mathcal{B}}$-theory T_* with
$$T_* = \{\sigma_* \colon T \vdash \sigma_*\} =$$
$$= \{\varphi(c_{b_1}, \dots, c_{b_k}) \colon \varphi(x_1, \dots, x_k) \text{ is a formula in } \mathcal{L}_{\mathcal{B}},\ \ T \vdash \varphi(c_{b_1}, \dots, c_{b_k})\}$$
T_* is a theory in $\mathcal{L}^*_{\mathcal{B}}$ with $\mathcal{B}_* \models T_*$ and therefore T_* is undecidable (by assumption of the claim). But notice that since the axioms in T do not contain any of the c_b constants any proof of $\varphi(c_{b_1}, \dots, c_{b_k})$ from T introduces c_b's at some point via the Deduction system axiom (2)(c). If instead of introducing c_b there we introduced some free variable and kept the proof the same we would prove $\varphi(x_1, \dots, x_k)$ from T. In other words,
$$\varphi(c_{b_1}, \dots, c_{b_k}) \in T_* \iff T \vdash \varphi(c_{b_1}, \dots, c_{b_k}) \iff T \vdash \varphi(x_1, \dots, x_k) \iff$$
$$\iff T \vdash \forall x_1 \dots \forall x_k\ \varphi(x_1, \dots, x_k) \iff \forall \bar{x} \varphi(\bar{x}) \in T$$
But then, since $\langle \varphi(\bar{c}) \rangle \mapsto \langle \forall \bar{x} \varphi(\bar{x}) \rangle$ is computable, if T was computable so would T_* be. Contradiction.

So we can assume without the loss of generality that c's where already in $\mathcal{L}_{\mathcal{B}}$, i.e., $\mathcal{A}$ was definable in $\mathcal{B}$ without parameters. But then this definition of $\mathcal{A}$ in $\mathcal{B}$ gives an interpretation $\mathcal{L}_{\mathcal{A}} \curvearrowright^{\pi} (\mathcal{L}_{\mathcal{B}}, \mathrm{Th}(\mathcal{B}))$ under which
$$\mathcal{A} \models \sigma \iff \mathcal{B} \models \sigma_\pi.$$
For example we can set $\pi_U(x)$ to be the formula given by (1) of Definition 82. Notice then that since A is non-empty we have that $\exists x \pi_U(x) \in \mathrm{Th}(\mathcal{B})$ and therefore $\mathrm{Th}(\mathcal{B}) \models \exists x \pi_U(x)$ (recall definition of interpretation)

Given now any $\mathcal{L}_{\mathcal{B}}$-theory $T_{\mathcal{B}}$ with $\mathcal{B} \models T_{\mathcal{B}}$ we can form $T_{\mathcal{A}} = \{\sigma \colon \sigma_\pi \in T_{\mathcal{B}}\}$.

Check: $T_{\mathcal{A}}$ is a theory with $\mathcal{A} \models T_{\mathcal{A}}$ and that if $T_{\mathcal{B}}$ was decidable then so would $T_{\mathcal{A}}$ be. □

Remark. In Definition 82 we were too restrictive when we demanded that in order for $\mathcal{A}$ to be definable in $\mathcal{B}$ the domain A of $\mathcal{A}$ should be an actual subset of the domain B of $\mathcal{B}$. From now on we will say that $\mathcal{A}$ is **definable** in $\mathcal{B}$ when $\mathcal{A}$ is isomorphic to some structure $\mathcal{A}'$ which is definable in $\mathcal{B}$, in the strict sense of definition 82.

Example. $(\mathbb{Z}, 0, 1, +, *)$ is strongly undecidable since $(\mathbb{N}, 0, 1, +, *)$ is trivially definable in it. As a consequence the theory of rings and the theory of integral domains is undecidable. What about fields? Maybe the extra restrictions would make the theory of fields decidable....

Theorem 84 (Robinson (her PhD thesis!))**.** $(\mathbb{Z}, 0, 1, +, *)$ *is definable in* $(\mathbb{Q}, 0, 1, +, *)$ *and therefore* $(\mathbb{Q}, 0, 1, +, *)$ *is strongly undecidable. As a consequence the theory of fields is undecidable.*

Sketch of proof. The proof uses the theory of quadratic forms in order to define $\mathbb{Z}$ as a subset of $\mathbb{Q}$. Consider the relation

$$R(a, b, k) \equiv \exists x \exists y \exists z (2 + abr^2 + bz^2 = x + ay^2).$$

Notice that $R(a, b, k)$ holds in $\mathbb{Q}$ if and only if $R(a, b, -k)$ holds. Think of a, b as parameters. Robinson shows that $\mathbb{Z}$ is the only "inductive" set with respect to all possible parameters. That is, the following formula defines $\mathbb{Z}$:

$$k \in \mathbb{Z} \iff \forall a \forall b \left[\Big(R(a,b,0) \wedge \forall n \big(R(a,b,n) \implies R(a,b,n+1) \big) \Big) \implies R(a,b,k) \right]$$

□

Theorem 85. *There exists a strongly undecidable group* $(G, \cdot, 1)$ *and therefore the theory of groups is undecidable.*

Proof. Let G be the group of all permutations of the countable set $\mathbb{Z}$ under composition. We will show that $(\mathbb{Z}, 0, 1, +, *)$ is definable (with parameters) in $(G, \cdot, e)$.

Consider the permutation $\sigma \colon \mathbb{Z} \to \mathbb{Z}$ with $\sigma(k) = k+1$ and let consider the subset $Z = \{\sigma^i \mid i \in \mathbb{Z}\}$ of G. This will be the domain of the definition of $\mathbb{Z}$ in G. We claim that $Z = \{\tau \in G \mid \tau\sigma = \sigma\tau\}$ and therefore Z is definable in G (using the parameter σ). To see this first notice that indeed, every element in Z commutes with σ. Conversely, if $\tau\sigma = \sigma\tau$, then $\tau\sigma^i = \sigma^i\tau$. Evaluating at $k = 0$ we have that $\tau(i) = i + \tau(0)$. Setting therefore $i = \tau(0)$ we get that $\tau = \sigma^j$.

Since $0, 1$ are definable by the constant e and the parameter σ in G, and since $+$ is definable simply by $\cdot$ in G we are left to show that multiplication of $\mathbb{Z}$ is definable in G. We show instead that division is definable in G and then multiplication will easily follow.

Claim. $i|j$ if and only if $\sigma^i \neq e$ for every $\tau \in G$ we have that:

$$\sigma^i\tau = \tau\sigma^i \implies \sigma^j\tau = \tau\sigma^j.$$

The $\Rightarrow$ direction is clear. For the other direction notice first that we can assume that $i \neq 0$ because then if $i = 0$ and $j \neq 0$ we can easily cook up some τ which does not commute with σ^j.

So assume that $i \neq 0$ and $\sigma^i\tau = \tau\sigma^i \implies \sigma^j\tau = \tau\sigma^j$ holds for all τ and test this on the unique τ with $\tau(k) = k + i$ if $i|k$ and $\tau(k) = k$ otherwise. Notice that τ commutes with σ^i so by assumption, $\sigma^j\tau = \tau\sigma^j$. So we have

$$\tau(k) + j = \tau(k + j)$$

But then notice that if $i \not| j$ we can plug i for k above and get $\tau(i) + j = \tau(i + j)$, i.e., $2i + j = i + j$, that is $i = 0$, a contradiction.

So we have that $(\mathbb{Z}, 0, 1, +, |)$ is definable in G. The rest follows from the exercise:

Exercise. Show that $*$ is definable in $(\mathbb{Z}, 0, 1, +, |)$. *Hint:* Notice that it suffice to show that $k \mapsto k^2$ is definable since $(i + j)^2 = i^2 + 2ij + j^2$. □

Next we show that the theory of graphs is undecidable by producing a strongly undecidable graph. By a **graph** we mean any structure $\mathcal{G} = (G, R^{\mathcal{G}})$ where $R^{\mathcal{G}}$ is any symmetric, anti-reflexive relation.

Claim 1. There is a strongly undecidable structure $\mathcal{A} = (A, S)$ where S is a quaternary relation.

Proof. Let $A = \mathbb{Z}$ and $S = \{(0, k, l, k + l) \mid k, l \in A\} \cup \{(1, k, l, k * l) \mid k, l \in A\}$. □

Claim 2. There is a strongly undecidable structure $\mathcal{B} = (B, T)$ where T is a binary relation.

Proof. Let $B = A \cup A^2 \cup \{\infty\}$ and consider the relation T defined to be the union of the sets

$$\{\big((a, b), (c, d)\big) \mid S(a, b, c, d)\},$$
$$\{\big(a, (a, b)\big) \mid a, b \in A\} \cup \{\big((a, b), b\big) \mid a, b \in A\}, \text{ and}$$
$$\{\big(\infty, a\big) \mid a \in A\} \cup \{\big((a, b), \infty\big) \mid a, b \in A\}.$$

We can now define $\mathcal{A}$ in $\mathcal{B}$ since A is definable in $\mathcal{B}$ by the formula $T(\infty, x)$ and S is definable by

$$S(x, y, z, w) \iff x, y, z, w \in A \wedge \exists p \exists q \Big(S(p, \infty) \wedge S(q, \infty) \wedge$$
$$\wedge S(x, p) \wedge S(p, y) \wedge S(z, q) \wedge S(q, w) \wedge S(p, q) \Big)$$

□

Theorem 86. *There is a strongly undecidable graph $\mathcal{G} = (G, R)$.*

Proof. Let $\mathcal{B} = (B, T)$ be strongly undecidable with T binary. For every $b \in B$ introduce three vertexes b_1, b_2, b_3 and let

$$G = \{b_1, b_2, b_3 \mid b \in B\} \cup \{s, t\}.$$

R consists of all pairs of the form: (b_1, b_2), (b_2, b_1), (b_3, b_2), (b_2, b_3), (s, b_1), (b_1, s), (t, b_2), (b_2, t), as well as all $(b_1, b_3'), (b_3', b_1)$ whenever $T(b, b')$.

Notice that B is definable in $\mathcal{G}$ (send $b \mapsto b_1$) by the formula $R(s, x)$. Similarly T is definable...

□

Mathematics Department, Caltech, 1200 E. California Blvd, Pasadena, CA 91125
E-mail address: panagio@caltech.edu
URL: http://www.its.caltech.edu/~panagio/