

Capítulo udf

Representability in $\mathbf{Q}$

-NoValue-

req.1 Introduction

inc:req:int:
sec The incompleteness theorems apply to theories in which basic facts about computable functions can be expressed and proved. We will describe a very minimal such theory called “ $\mathbf{Q}$ ” (or, sometimes, “Robinson’s Q ,” after Raphael Robinson). We will say what it means for a function to be *representable* in $\mathbf{Q}$, and then we will prove the following:

A function is representable in $\mathbf{Q}$ if and only if it is computable.

For one thing, this provides us with another model of computability. But we will also use it to show that the set $\{\varphi : \mathbf{Q} \vdash \varphi\}$ is not decidable, by reducing the halting problem to it. By the time we are done, we will have proved much stronger things than this.

The language of $\mathbf{Q}$ is the language of arithmetic; $\mathbf{Q}$ consists of the following axioms (to be used in conjunction with the other axioms and rules of first-order logic with *predicado de identidad*):

$$\forall x \forall y (x' = y' \rightarrow x = y) \quad (Q_1)$$

$$\forall x \ 0 \neq x' \quad (Q_2)$$

$$\forall x (x = 0 \vee \exists y x = y') \quad (Q_3)$$

$$\forall x (x + 0) = x \quad (Q_4)$$

$$\forall x \forall y (x + y') = (x + y)' \quad (Q_5)$$

$$\forall x (x \times 0) = 0 \quad (Q_6)$$

$$\forall x \forall y (x \times y') = ((x \times y) + x) \quad (Q_7)$$

$$\forall x \forall y (x < y \leftrightarrow \exists z (z' + x) = y) \quad (Q_8)$$

For each natural number n , define the numeral $\bar{n}$ to be the term $0''\dots'$ where there are n tick marks in all. So, $\bar{0}$ is the *símbolo de constante* 0 by itself, $\bar{1}$ is $0'$, $\bar{2}$ is $0''$, etc.

As a theory of arithmetic, $\mathbf{Q}$ is *extremely* weak; for example, you can't even prove very simple facts like $\forall x x \neq x'$ or $\forall x \forall y (x + y) = (y + x)$. But we will see that much of the reason that $\mathbf{Q}$ is so interesting is *because* it is so weak. In fact, it is just barely strong enough for the incompleteness theorem to hold. Another reason $\mathbf{Q}$ is interesting is because it has a *finite* set of axioms.

A stronger theory than $\mathbf{Q}$ (called *Peano arithmetic* $\mathbf{PA}$) is obtained by adding a schema of induction to $\mathbf{Q}$:

$$(\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(x'))) \rightarrow \forall x \varphi(x)$$

where $\varphi(x)$ is any formula. If $\varphi(x)$ contains free **variáveis** other than x , we add universal quantifiers to the front to bind all of them (so that the corresponding instance of the induction schema is a **sentença**). For instance, if $\varphi(x, y)$ also contains the **variável** y free, the corresponding instance is

$$\forall y ((\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(x'))) \rightarrow \forall x \varphi(x))$$

Using instances of the induction schema, one can prove much more from the axioms of $\mathbf{PA}$ than from those of $\mathbf{Q}$. In fact, it takes a good deal of work to find “natural” statements about the natural numbers that can't be proved in Peano arithmetic!

Definição req.1. A function $f(x_0, \dots, x_k)$ from the natural numbers to the natural numbers is said to be *representable in $\mathbf{Q}$* if there is a formula $\varphi_f(x_0, \dots, x_k, y)$ such that whenever $f(n_0, \dots, n_k) = m$, $\mathbf{Q}$ proves

1. $\varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m})$
2. $\forall y (\varphi_f(\overline{n_0}, \dots, \overline{n_k}, y) \rightarrow \overline{m} = y).$

There are other ways of stating the definition; for example, we could equivalently require that $\mathbf{Q}$ proves $\forall y (\varphi_f(\overline{n_0}, \dots, \overline{n_k}, y) \leftrightarrow y = \overline{m})$.

Teorema req.2. A function is representable in $\mathbf{Q}$ if and only if it is computable.

There are two directions to proving the theorem. The left-to-right direction is fairly straightforward once arithmetization of syntax is in place. The other direction requires more work. Here is the basic idea: we pick “general recursive” as a way of making “computable” precise, and show that every general recursive function is representable in $\mathbf{Q}$. Recall that a function is general recursive if it can be defined from zero, the successor function succ , and the projection functions P_i^n , using composition, primitive recursion, and regular minimization. So one way of showing that every general recursive function is representable in $\mathbf{Q}$ is to show that the basic functions are representable, and whenever some functions are representable, then so are the functions defined from them using composition, primitive recursion, and regular minimization. In other words, we might show that the basic functions are representable, and

that the representable functions are “closed under” composition, primitive recursion, and regular minimization. This guarantees that every general recursive function is representable.

It turns out that the step where we would show that representable functions are closed under primitive recursion is hard. In order to avoid this step, we show first that in fact we can do without primitive recursion. That is, we show that every general recursive function can be defined from basic functions using composition and regular minimization alone. To do this, we show that primitive recursion can actually be done by a specific regular minimization. However, for this to work, we have to add some additional basic functions: addition, multiplication, and the characteristic function of the identity relation $\chi_{=}$. Then, we can prove the theorem by showing that all of *these* basic functions are representable in $\mathbf{Q}$, and the representable functions are closed under composition and regular minimization.

-NoValue-

req.2 Functions Representable in $\mathbf{Q}$ are Computable

inc:req:rpc: sec We'll prove that every function that is representable in $\mathbf{Q}$ is computable. We first have to establish a lemma about functions representable in $\mathbf{Q}$.

inc:req:rpc: lem:rep-q **Lema req.3.** *If $f(x_0, \dots, x_k)$ is representable in $\mathbf{Q}$, there is a fórmula $\varphi(x_0, \dots, x_k, y)$ such that*

$$\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m}) \quad \text{iff} \quad m = f(n_0, \dots, n_k).$$

Prova. The “if” part is **Definição req.1(1)**. The “only if” part is seen as follows: Suppose $\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m})$ but $m \neq f(n_0, \dots, n_k)$. Let $l = f(n_0, \dots, n_k)$. By **Definição req.1(1)**, $\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{l})$. By **Definição req.1(2)**, $\forall y (\varphi_f(\overline{n_0}, \dots, \overline{n_k}, y) \rightarrow \overline{l} = y)$. Using logic and the assumption that $\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m})$, we get that $\mathbf{Q} \vdash \overline{l} = \overline{m}$. On the other hand, by **Lema req.14**, $\mathbf{Q} \vdash \overline{l} \neq \overline{m}$. So $\mathbf{Q}$ is inconsistent. But that is impossible, since $\mathbf{Q}$ is satisfied by the standard model (see ??), $\mathfrak{N} \models \mathbf{Q}$, and satisfiable theories are always consistent by the Soundness Theorem (????????????). $\square$

Lema req.4. *Every function that is representable in $\mathbf{Q}$ is computable.*

Prova. Let's first give the intuitive idea for why this is true. To compute f , we do the following. List all the possible **derivações** δ in the language of arithmetic. This is possible to do mechanically. For each one, check if it is a **derivação** of a fórmula of the form $\varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m})$ (the fórmula representing f in $\mathbf{Q}$ from **Lema req.3**). If it is, $m = f(n_0, \dots, n_k)$ by **Lema req.3**, and we've found the value of f . The search terminates because $\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{f(n_0, \dots, n_k)})$, so eventually we find a δ of the right sort.

This is not quite precise because our procedure operates on **derivações** and **fórmulas** instead of just on numbers, and we haven't explained exactly why “listing all possible **derivações**” is mechanically possible. But as we've seen, it

is possible to code terms, **fórmulas**, and **derivações** by Gödel numbers. We've also introduced a precise model of computation, the general recursive functions. And we've seen that the relation $\text{Prf}_{\mathbf{Q}}(d, y)$, which holds iff d is the Gödel number of a **derivação** of the **fórmula** with Gödel number y from the axioms of $\mathbf{Q}$, is (primitive) recursive. Other primitive recursive functions we'll need are $\text{num}(\text{??})$ and $\text{Subst}(\text{??})$. From these, it is possible to define f by minimization; thus, f is recursive.

First, define

$$A(n_0, \dots, n_k, m) = \text{Subst}(\text{Subst}(\dots \text{Subst}(\text{?}\varphi_f\text{?}, \text{num}(n_0), \text{?}x_0\text{?}), \dots), \text{num}(n_k), \text{?}x_k\text{?}), \text{num}(m), \text{?}y\text{?})$$

This looks complicated, but it's just the function $A(n_0, \dots, n_k, m) = \text{?}\varphi_f(\overline{n_0}, \dots, \overline{n_k}, \overline{m})\text{?}$.

Now, consider the relation $R(n_0, \dots, n_k, s)$ which holds if $(s)_0$ is the Gödel number of a **derivação** from $\mathbf{Q}$ of $\varphi_f(\overline{n_0}, \dots, \overline{n_k}, (s)_1)$:

$$R(n_0, \dots, n_k, s) \text{ iff } \text{Prf}_{\mathbf{Q}}((s)_0, A(n_0, \dots, n_k, (s)_1))$$

If we can find an s such that $R(n_0, \dots, n_k, s)$ holds, we have found a pair of numbers— $(s)_0$ and $(s)_1$ —such that $(s)_0$ is the Gödel number of a **derivação** of $A_f(\overline{n_0}, \dots, \overline{n_k}, (s)_1)$. So looking for s is like looking for the pair d and m in the informal proof. And a computable function that “looks for” such an s can be defined by regular minimization. Note that R is regular: for every $n_0, \dots, n_k$, there is a **derivação** δ of $\mathbf{Q} \vdash \varphi_f(\overline{n_0}, \dots, \overline{n_k}, f(n_0, \dots, n_k))$, so $R(n_0, \dots, n_k, s)$ holds for $s = \langle \text{?}\delta\text{?}, f(n_0, \dots, n_k) \rangle$. So, we can write f as

$$f(n_0, \dots, n_k) = (\mu s R(n_0, \dots, n_k, s))_1. \quad \square$$

-NoValue-

req.3 The Beta Function Lemma

In order to show that we can carry out primitive recursion if addition, multiplication, and $\chi_{=}$ are available, we need to develop functions that handle sequences. (If we had exponentiation as well, our task would be easier.) When we had primitive recursion, we could define things like the “ n -th prime,” and pick a fairly straightforward coding. But here we do not have primitive recursion—in fact we want to show that we can do primitive recursion using minimization—so we need to be more clever.

inc:req:bet:
sec

Lema req.5. *There is a function $\beta(d, i)$ such that for every sequence $a_0, \dots, a_n$ there is a number d , such that for every $i \leq n$, $\beta(d, i) = a_i$. Moreover, β can be defined from the basic functions using just composition and regular minimization.*

inc:req:bet:
lem:beta

Think of d as coding the sequence $\langle a_0, \dots, a_n \rangle$, and $\beta(d, i)$ returning the i -th element. (Note that this “coding” does *not* use the power-of-primes coding we’re already familiar with!). The lemma is fairly minimal; it doesn’t say we can concatenate sequences or append elements, or even that we can *compute* d from $a_0, \dots, a_n$ using functions definable by composition and regular minimization. All it says is that there is a “decoding” function such that every sequence is “coded.”

The use of the notation β is Gödel’s. To repeat, the hard part of proving the lemma is defining a suitable β using the seemingly restricted resources, O.s., using just composition and minimization—however, we’re allowed to use addition, multiplication, and $\chi_=_$. There are various ways to prove this lemma, but one of the cleanest is still Gödel’s original method, which used a number-theoretic fact called Sunzi’s Theorem (traditionally, the “Chinese Remainder Theorem”).

Definição req.6. Two natural numbers a and b are *relatively prime* iff their greatest common divisor is 1; in other words, they have no other divisors in common.

Definição req.7. Natural numbers a and b are *congruent modulo c* , $a \equiv b \pmod{c}$, iff $c \mid (a - b)$, O.s., a and b have the same remainder when divided by c .

Here is Sunzi’s Theorem:

Teorema req.8. Suppose $x_0, \dots, x_n$ are (pairwise) relatively prime. Let $y_0, \dots, y_n$ be any numbers. Then there is a number z such that

$$\begin{aligned} z &\equiv y_0 \pmod{x_0} \\ z &\equiv y_1 \pmod{x_1} \\ &\vdots \\ z &\equiv y_n \pmod{x_n}. \end{aligned}$$

Here is how we will use Sunzi’s Theorem: if $x_0, \dots, x_n$ are bigger than $y_0, \dots, y_n$ respectively, then we can take z to code the sequence $\langle y_0, \dots, y_n \rangle$. To recover y_i , we need only divide z by x_i and take the remainder. To use this coding, we will need to find suitable values for $x_0, \dots, x_n$.

A couple of observations will help us in this regard. Given $y_0, \dots, y_n$, let

$$\begin{aligned} j &= \max(n, y_0 + 1, \dots, y_n + 1), \\ m &= \text{lcm}(1, \dots, j), \end{aligned}$$

and let

$$\begin{aligned} x_0 &= 1 + m \\ x_1 &= 1 + 2 \cdot m \\ x_2 &= 1 + 3 \cdot m \\ &\vdots \\ x_n &= 1 + (n + 1) \cdot m \end{aligned}$$

Then two things are true:

1. $x_0, \dots, x_n$ are relatively prime.
2. For each i , $y_i < x_i$.

inc:req:bet:
rel-prime
inc:req:bet:
less

To see that (1) is true, note that if p is a prime number and $p \mid x_i$ and $p \mid x_k$, then $p \mid 1 + (i + 1)m$ and $p \mid 1 + (k + 1)m$. But then p divides their difference,

$$(1 + (i + 1)m) - (1 + (k + 1)m) = (i - k)m.$$

Since p divides $1 + (i + 1)m$, it can't divide m as well (otherwise, the first division would leave a remainder of 1). So p divides $i - k$, since p divides $(i - k)m$. But $|i - k|$ is at most n , and we have chosen $j \geq n$, so this implies that $p \mid m$, again a contradiction. So there is no prime number dividing both x_i and x_k . Clause (2) is easy: we have $y_i < j \leq m < x_i$.

Now let us prove the β function lemma. Remember that we can use 0, successor, plus, times, $\chi_=$, projections, and any function defined from them using composition and minimization applied to regular functions. We can also use a relation if its characteristic function is so definable. As before we can show that these relations are closed under Boolean combinations and bounded quantification; for example:

$$\begin{aligned} \text{not}(x) &= \chi_=(x, 0) \\ (\min x \leq z) R(x, y) &= \mu x (R(x, y) \vee x = z) \\ (\exists x \leq z) R(x, y) &\Leftrightarrow R((\min x \leq z) R(x, y), y) \end{aligned}$$

We can then show that all of the following are also definable without primitive recursion:

1. The pairing function, $J(x, y) = \frac{1}{2}[(x + y)(x + y + 1)] + x$;
2. the projection functions

$$\begin{aligned} K(z) &= (\min x \leq z) (\exists y \leq z) z = J(x, y), \\ L(z) &= (\min y \leq z) (\exists x \leq z) z = J(x, y); \end{aligned}$$

3. the less-than relation $x < y$;

4. the divisibility relation $x \mid y$;
5. the function $\text{rem}(x, y)$ which returns the remainder when y is divided by x .

Now define

$$\begin{aligned}\beta^*(d_0, d_1, i) &= \text{rem}(1 + (i + 1)d_1, d_0) \text{ and} \\ \beta(d, i) &= \beta^*(K(d), L(d), i).\end{aligned}$$

This is the function we want. Given $a_0, \dots, a_n$ as above, let

$$j = \max(n, a_0 + 1, \dots, a_n + 1),$$

and let $d_1 = \text{lcm}(1, \dots, j)$. By (1) above, we know that $1 + d_1, 1 + 2d_1, \dots, 1 + (n+1)d_1$ are relatively prime, and by (2) that all are greater than $a_0, \dots, a_n$. By Sunzi's Theorem there is a value d_0 such that for each i ,

$$d_0 \equiv a_i \pmod{(1 + (i + 1)d_1)}$$

and so (because d_1 is greater than a_i),

$$a_i = \text{rem}(1 + (i + 1)d_1, d_0).$$

Let $d = J(d_0, d_1)$. Then for each $i \leq n$, we have

$$\begin{aligned}\beta(d, i) &= \beta^*(d_0, d_1, i) \\ &= \text{rem}(1 + (i + 1)d_1, d_0) \\ &= a_i\end{aligned}$$

which is what we need. This completes the proof of the β -function lemma.

Problema req.1. Show that the relations $x < y$, $x \mid y$, and the function $\text{rem}(x, y)$ can be defined without primitive recursion. You may use 0, successor, plus, times, $\chi_=$, projections, and bounded minimization and quantification.

-NoValue-

req.4 Simulating Primitive Recursion

inc:req:pri:
sec Now we can show that definition by primitive recursion can be “simulated” by regular minimization using the beta function. Suppose we have $f(\vec{x})$ and $g(\vec{x}, y, z)$. Then the function $h(x, \vec{z})$ defined from f and g by primitive recursion is

$$\begin{aligned}h(\vec{x}, 0) &= f(\vec{x}) \\ h(\vec{x}, y + 1) &= g(\vec{x}, y, h(\vec{x}, y)).\end{aligned}$$

We need to show that h can be defined from f and g using just composition and regular minimization, using the basic functions and functions defined from them using composition and regular minimization (such as β).

Lema req.9. *If h can be defined from f and g using primitive recursion, it can be defined from f , g , the functions zero, succ, P_i^n , add, mult, $\chi_=$, using composition and regular minimization.* inc:req:pri:
lem:prim-rec

Prova. First, define an auxiliary function $\hat{h}(\vec{x}, y)$ which returns the least number d such that d codes a sequence which satisfies

1. $(d)_0 = f(\vec{x})$, and
2. for each $i < y$, $(d)_{i+1} = g(\vec{x}, i, (d)_i)$,

where now $(d)_i$ is short for $\beta(d, i)$. In other words, $\hat{h}$ returns the sequence $\langle h(\vec{x}, 0), h(\vec{x}, 1), \dots, h(\vec{x}, y) \rangle$. We can write $\hat{h}$ as

$$\hat{h}(\vec{x}, y) = \mu d (\beta(d, 0) = f(\vec{x}) \wedge (\forall i < y) \beta(d, i+1) = g(\vec{x}, i, \beta(d, i))).$$

Note: no primitive recursion is needed here, just minimization. The function we minimize is regular because of the beta function lemma **Lema req.5**.

But now we have

$$h(\vec{x}, y) = \beta(\hat{h}(\vec{x}, y), y),$$

so h can be defined from the basic functions using just composition and regular minimization. □

-NoValue-

req.5 Basic Functions are Representable in Q

First we have to show that all the basic functions are representable in **Q**. In the end, we need to show how to assign to each k -ary basic function $f(x_0, \dots, x_{k-1})$ a fórmula $\varphi_f(x_0, \dots, x_{k-1}, y)$ that represents it. inc:req:bre:
sec

We will be able to represent zero, successor, plus, times, the characteristic function for equality, and projections. In each case, the appropriate representing function is entirely straightforward; for example, zero is represented by the formula $y = 0$, successor is represented by the fórmula $x'_0 = y$, and addition is represented by the fórmula $(x_0 + x_1) = y$. The work involves showing that **Q** can prove the relevant sentenças; for example, saying that addition is represented by the fórmula above involves showing that for every pair of natural numbers m and n , **Q** proves

$$\begin{aligned} \overline{n} + \overline{m} &= \overline{n + m} \text{ and} \\ \forall y ((\overline{n} + \overline{m}) = y &\rightarrow y = \overline{n + m}). \end{aligned}$$

Proposição req.10. *The zero function $\text{zero}(x) = 0$ is represented in **Q** by $\varphi_{\text{zero}}(x, y) \equiv y = 0$.* inc:req:bre:
prop:rep-zero

Proposição req.11. *The successor function $\text{succ}(x) = x + 1$ is represented in **Q** by $\varphi_{\text{succ}}(x, y) \equiv y = x'$.* inc:req:bre:
prop:rep-succ

inc:req:bre: **Proposição req.12.** *prop:rep-proj* The projection function $P_i^n(x_0, \dots, x_{n-1}) = x_i$ is represented in $\mathbf{Q}$ by

$$\varphi_{P_i^n}(x_0, \dots, x_{n-1}, y) \equiv y = x_i.$$

Problema req.2. Prove that $y = 0$, $y = x'$, and $y = x_i$ represent zero, succ, and P_i^n , respectively.

inc:req:bre: **Proposição req.13.** *prop:rep-id* The characteristic function of $=$,

$$\chi_=(x_0, x_1) = \begin{cases} 1 & \text{if } x_0 = x_1 \\ 0 & \text{otherwise} \end{cases}$$

is represented in $\mathbf{Q}$ by

$$\varphi_{\chi_=(x_0, x_1, y)} \equiv (x_0 = x_1 \wedge y = \bar{1}) \vee (x_0 \neq x_1 \wedge y = \bar{0}).$$

The proof requires the following lemma.

inc:req:bre: **Lema req.14.** *lem:q-proves-neq* Given natural numbers n and m , if $n \neq m$, then $\mathbf{Q} \vdash \bar{n} \neq \bar{m}$.

Prova. Use induction on n to show that for every m , if $n \neq m$, then $\mathbf{Q} \vdash \bar{n} \neq \bar{m}$.

In the base case, $n = 0$. If m is not equal to 0, then $m = k + 1$ for some natural number k . We have an axiom that says $\forall x \, 0 \neq x'$. By a quantifier axiom, replacing x by $\bar{k}$, we can conclude $0 \neq \bar{k}'$. But $\bar{k}'$ is just $\bar{m}$.

In the induction step, we can assume the claim is true for n , and consider $n + 1$. Let m be any natural number. There are two possibilities: either $m = 0$ or for some k we have $m = k + 1$. The first case is handled as above. In the second case, suppose $n + 1 \neq k + 1$. Then $n \neq k$. By the induction hypothesis for n we have $\mathbf{Q} \vdash \bar{n} \neq \bar{k}$. We have an axiom that says $\forall x \, \forall y \, x' = y' \rightarrow x = y$. Using a quantifier axiom, we have $\bar{n}' = \bar{k}' \rightarrow \bar{n} = \bar{k}$. Using propositional logic, we can conclude, in $\mathbf{Q}$, $\bar{n} \neq \bar{k} \rightarrow \bar{n}' \neq \bar{k}'$. Using modus ponens, we can conclude $\bar{n}' \neq \bar{k}'$, which is what we want, since $\bar{k}'$ is $\bar{m}$. $\square$

Note that the lemma does not say much: in essence it says that $\mathbf{Q}$ can prove that different numerals denote different objects. For example, $\mathbf{Q}$ proves $0'' \neq 0'''$. But showing that this holds in general requires some care. Note also that although we are using induction, it is induction *outside* of $\mathbf{Q}$.

[explanation](#)

Prova de Proposição req.13. If $n = m$, then $\bar{n}$ and $\bar{m}$ are the same term, and $\chi_=(n, m) = 1$. But $\mathbf{Q} \vdash (\bar{n} = \bar{m} \wedge \bar{1} = \bar{1})$, so it proves $\varphi_=(\bar{n}, \bar{m}, \bar{1})$. If $n \neq m$, then $\chi_=(n, m) = 0$. By **Lema req.14**, $\mathbf{Q} \vdash \bar{n} \neq \bar{m}$ and so also $(\bar{n} \neq \bar{m} \wedge 0 = 0)$. Thus $\mathbf{Q} \vdash \varphi_=(\bar{n}, \bar{m}, \bar{0})$.

For the second part, we also have two cases. If $n = m$, we have to show that $\mathbf{Q} \vdash \forall y (\varphi_=(\bar{n}, \bar{m}, y) \rightarrow y = \bar{1})$. Arguing informally, suppose $\varphi_=(\bar{n}, \bar{m}, y)$, O.s.,

$$(\bar{n} = \bar{n} \wedge y = \bar{1}) \vee (\bar{n} \neq \bar{n} \wedge y = \bar{0})$$

The left disjunct implies $y = \bar{1}$ by logic; the right contradicts $\bar{n} = \bar{n}$ which is provable by logic.

Suppose, on the other hand, that $n \neq m$. Then $\varphi_{=}(n, m, y)$ is

$$(\bar{n} = \bar{m} \wedge y = \bar{1}) \vee (\bar{n} \neq \bar{m} \wedge y = \bar{0})$$

Here, the left disjunct contradicts $\bar{n} \neq \bar{m}$, which is provable in $\mathbf{Q}$ by [Lema req.14](#); the right disjunct entails $y = \bar{0}$. $\square$

Proposição req.15. *The addition function $\text{add}(x_0, x_1) = x_0 + x_1$ is represented in $\mathbf{Q}$ by*

*inc:req:brc:
prop:rep-add*

$$\varphi_{\text{add}}(x_0, x_1, y) \equiv y = (x_0 + x_1).$$

Lema req.16. $\mathbf{Q} \vdash (\bar{n} + \bar{m}) = \overline{n + m}$

*inc:req:brc:
lem:q-proves-add*

Prova. We prove this by induction on m . If $m = 0$, the claim is that $\mathbf{Q} \vdash (\bar{n} + 0) = \bar{n}$. This follows by axiom Q_4 . Now suppose the claim for m ; let's prove the claim for $m + 1$, O.s., prove that $\mathbf{Q} \vdash (\bar{n} + \overline{m + 1}) = \overline{n + m + 1}$. Note that $\overline{m + 1}$ is just $\bar{m}'$, and $\overline{n + m + 1}$ is just $\overline{n + m'}$. By axiom Q_5 , $\mathbf{Q} \vdash (\bar{n} + \bar{m}') = (\bar{n} + \bar{m})'$. By induction hypothesis, $\mathbf{Q} \vdash (\bar{n} + \bar{m}) = \overline{n + m}$. So $\mathbf{Q} \vdash (\bar{n} + \bar{m}') = \overline{n + m'}$. $\square$

Prova de Proposição req.15. The fórmula $\varphi_{\text{add}}(x_0, x_1, y)$ representing add is $y = (x_0 + x_1)$. First we show that if $\text{add}(n, m) = k$, then $\mathbf{Q} \vdash \varphi_{\text{add}}(\bar{n}, \bar{m}, \bar{k})$, O.s., $\mathbf{Q} \vdash \bar{k} = (\bar{n} + \bar{m})$. But since $k = n + m$, $\bar{k}$ just is $\overline{n + m}$, and we've shown in [Lema req.16](#) that $\mathbf{Q} \vdash (\bar{n} + \bar{m}) = \overline{n + m}$.

We also have to show that if $\text{add}(n, m) = k$, then

$$\mathbf{Q} \vdash \forall y (\varphi_{\text{add}}(\bar{n}, \bar{m}, y) \rightarrow y = \bar{k}).$$

Suppose we have $(\bar{n} + \bar{m}) = y$. Since

$$\mathbf{Q} \vdash (\bar{n} + \bar{m}) = \overline{n + m},$$

we can replace the left side with $\overline{n + m}$ and get $\overline{n + m} = y$, for arbitrary y . $\square$

Proposição req.17. *The multiplication function $\text{mult}(x_0, x_1) = x_0 \cdot x_1$ is represented in $\mathbf{Q}$ by*

*inc:req:brc:
prop:rep-mult*

$$\varphi_{\text{mult}}(x_0, x_1, y) \equiv y = (x_0 \times x_1).$$

Prova. Exercise. $\square$

Lema req.18. $\mathbf{Q} \vdash (\bar{n} \times \bar{m}) = \overline{n \cdot m}$

*inc:req:brc:
lem:q-proves-mult*

Prova. Exercise. $\square$

Problema req.3. Prove [Lema req.18](#).

Problema req.4. Use [Lema req.18](#) to prove [Proposição req.17](#).

Recall that we use $\times$ for the function symbol of the language of arithmetic, and $\cdot$ for the ordinary multiplication operation on numbers. So $\cdot$ can appear between expressions for numbers (such as in $m \cdot n$) while $\times$ appears only between terms of the language of arithmetic (such as in $(\overline{m} \times \overline{n})$). Even more confusingly, $+$ is used for both the [símbolo de função](#) and the addition operation. When it appears between terms—p.ex., in $(\overline{n} + \overline{m})$ —it is the 2-place [símbolo de função](#) of the language of arithmetic, and when it appears between numbers—p.ex., in $n + m$ —it is the addition operation. This includes the case $\overline{n + m}$: this is the standard numeral corresponding to the number $n + m$.

-NoValue-

req.6 Composition is Representable in Q

[inc:req:cmp:](#) Suppose h is defined by
[sec](#)

$$h(x_0, \dots, x_{l-1}) = f(g_0(x_0, \dots, x_{l-1}), \dots, g_{k-1}(x_0, \dots, x_{l-1})).$$

where we have already found [fórmulas](#) $\varphi_f, \varphi_{g_0}, \dots, \varphi_{g_{k-1}}$ representing the functions f , and $g_0, \dots, g_{k-1}$, respectively. We have to find [a fórmula](#) φ_h representing h .

Let's start with a simple case, where all functions are 1-place, O.s., consider $h(x) = f(g(x))$. If $\varphi_f(y, z)$ represents f , and $\varphi_g(x, y)$ represents g , we need [a fórmula](#) $\varphi_h(x, z)$ that represents h . Note that $h(x) = z$ iff there is a y such that both $z = f(y)$ and $y = g(x)$. (If $h(x) = z$, then $g(x)$ is such a y ; if such a y exists, then since $y = g(x)$ and $z = f(y)$, $z = f(g(x))$.) This suggests that $\exists y (\varphi_g(x, y) \wedge \varphi_f(y, z))$ is a good candidate for $\varphi_h(x, z)$. We just have to verify that **Q** proves the relevant [fórmulas](#).

[inc:req:cmp:](#) **Proposição req.19.** If $h(n) = m$, then $\mathbf{Q} \vdash \varphi_h(\overline{n}, \overline{m})$.
[prop:rep1](#)

Prova. Suppose $h(n) = m$, O.s., $f(g(n)) = m$. Let $k = g(n)$. Then

$$\mathbf{Q} \vdash \varphi_g(\overline{n}, \overline{k})$$

since φ_g represents g , and

$$\mathbf{Q} \vdash \varphi_f(\overline{k}, \overline{m})$$

since φ_f represents f . Thus,

$$\mathbf{Q} \vdash \varphi_g(\overline{n}, \overline{k}) \wedge \varphi_f(\overline{k}, \overline{m})$$

and consequently also

$$\mathbf{Q} \vdash \exists y (\varphi_g(\overline{n}, y) \wedge \varphi_f(y, \overline{m})),$$

O.s., $\mathbf{Q} \vdash \varphi_h(\overline{n}, \overline{m})$. □

Proposição req.20. If $h(n) = m$, then $\mathbf{Q} \vdash \forall z (\varphi_h(\bar{n}, z) \rightarrow z = \bar{m})$.

*inc:req:cmp:
prop:rep2*

Prova. Suppose $h(n) = m$, O.s., $f(g(n)) = m$. Let $k = g(n)$. Then

$$\mathbf{Q} \vdash \forall y (\varphi_g(\bar{n}, y) \rightarrow y = \bar{k})$$

since φ_g represents g , and

$$\mathbf{Q} \vdash \forall z (\varphi_f(\bar{k}, z) \rightarrow z = \bar{m})$$

since φ_f represents f . Using just a little bit of logic, we can show that also

$$\mathbf{Q} \vdash \forall z (\exists y (\varphi_g(\bar{n}, y) \wedge \varphi_f(y, z)) \rightarrow z = \bar{m}).$$

O.s., $\mathbf{Q} \vdash \forall y (\varphi_h(\bar{n}, y) \rightarrow y = \bar{m})$. □

The same idea works in the more complex case where f and g_i have arity greater than 1.

Proposição req.21. If $\varphi_f(y_0, \dots, y_{k-1}, z)$ represents $f(y_0, \dots, y_{k-1})$ in $\mathbf{Q}$, and $\varphi_{g_i}(x_0, \dots, x_{l-1}, y)$ represents $g_i(x_0, \dots, x_{l-1})$ in $\mathbf{Q}$, then

*inc:req:cmp:
prop:rep-composition*

$$\begin{aligned} \exists y_0 \dots \exists y_{k-1} (\varphi_{g_0}(x_0, \dots, x_{l-1}, y_0) \wedge \dots \wedge \\ \varphi_{g_{k-1}}(x_0, \dots, x_{l-1}, y_{k-1}) \wedge \varphi_f(y_0, \dots, y_{k-1}, z)) \end{aligned}$$

represents

$$h(x_0, \dots, x_{l-1}) = f(g_0(x_0, \dots, x_{l-1}), \dots, g_{k-1}(x_0, \dots, x_{l-1})).$$

Prova. Exercise. □

Problema req.5. Using the proofs of **Proposição req.20** and **Proposição req.21** as a guide, carry out the proof of **Proposição req.21** in detail.

-NoValue-

req.7 Regular Minimization is Representable in $\mathbf{Q}$

Let's consider unbounded search. Suppose $g(x, z)$ is regular and representable in $\mathbf{Q}$, say by the formula $\varphi_g(x, z, y)$. Let f be defined by $f(z) = \mu x [g(x, z) = 0]$. We would like to find a formula $\varphi_f(z, y)$ representing f . The value of $f(z)$ is that number x which (a) satisfies $g(x, z) = 0$ and (b) is the least such, O.s., for any $w < x$, $g(w, z) \neq 0$. So the following is a natural choice:

*inc:req:min:
sec*

$$\varphi_f(z, y) \equiv \varphi_g(y, z, 0) \wedge \forall w (w < y \rightarrow \neg \varphi_g(w, z, 0)).$$

In the general case, of course, we would have to replace z with $z_0, \dots, z_k$.

The proof, again, will involve some lemmas about things $\mathbf{Q}$ is strong enough to prove.

inc:req:min: **Lema req.22.** For every *símbolo de constante* a and every natural number n ,
lem:succ

$$\mathbf{Q} \vdash (a' + \bar{n}) = (a + \bar{n})'.$$

Prova. The proof is, as usual, by induction on n . In the base case, $n = 0$, we need to show that $\mathbf{Q}$ proves $(a' + 0) = (a + 0)'$. But we have:

$$\mathbf{Q} \vdash (a' + 0) = a' \quad \text{by axiom } Q_4 \quad (\text{req.1})$$

$$\mathbf{Q} \vdash (a + 0) = a \quad \text{by axiom } Q_4 \quad (\text{req.2})$$

$$\mathbf{Q} \vdash (a + 0)' = a' \quad \text{by Eq. (req.2)} \quad (\text{req.3})$$

$$\mathbf{Q} \vdash (a' + 0) = (a + 0)' \quad \text{by Eq. (req.1) and Eq. (req.3)}$$

In the induction step, we can assume that we have shown that $\mathbf{Q} \vdash (a' + \bar{n}) = (a + \bar{n})'$. Since $\overline{n+1}$ is $\bar{n}'$, we need to show that $\mathbf{Q}$ proves $(a' + \bar{n}') = (a + \bar{n}')'$. We have:

$$\mathbf{Q} \vdash (a' + \bar{n}') = (a' + \bar{n})' \quad \text{by axiom } Q_5 \quad (\text{req.4})$$

$$\mathbf{Q} \vdash (a' + \bar{n}') = (a + \bar{n}')' \quad \text{inductive hypothesis} \quad (\text{req.5})$$

$$\mathbf{Q} \vdash (a' + \bar{n}') = (a + \bar{n}')' \quad \text{by Eq. (req.4) and Eq. (req.5).} \quad \square$$

It is again worth mentioning that this is weaker than saying that $\mathbf{Q}$ proves $\forall x \forall y (x' + y) = (x + y)'$. Although this *sentença* is true in $\mathfrak{N}$, $\mathbf{Q}$ does not prove it.

inc:req:min: **Lema req.23.** $\mathbf{Q} \vdash \forall x \neg x < 0$.
lem:less-zero

Prova. We give the proof informally (O.s., only giving hints as to how to construct the formal *derivação*).

We have to prove $\neg a < 0$ for an arbitrary a . By the definition of $<$, we need to prove $\neg \exists y (y' + a) = 0$ in $\mathbf{Q}$. We'll assume $\exists y (y' + a) = 0$ and prove a contradiction. Suppose $(b' + a) = 0$. Using Q_3 , we have that $a = 0 \vee \exists y a = y'$. We distinguish cases.

Case 1: $a = 0$ holds. From $(b' + a) = 0$, we have $(b' + 0) = 0$. By axiom Q_4 of $\mathbf{Q}$, we have $(b' + 0) = b'$, and hence $b' = 0$. But by axiom Q_2 we also have $b' \neq 0$, a contradiction.

Case 2: For some c , $a = c'$. But then we have $(b' + c') = 0$. By axiom Q_5 , we have $(b' + c)' = 0$, again contradicting axiom Q_2 . $\square$

inc:req:min: **Lema req.24.** For every natural number n ,
lem:less-nsucc

$$\mathbf{Q} \vdash \forall x (x < \overline{n+1} \rightarrow (x = 0 \vee \dots \vee x = \bar{n})).$$

Prova. We use induction on n . Let us consider the base case, when $n = 0$. In that case, we need to show $a < \bar{1} \rightarrow a = 0$, for arbitrary a . Suppose $a < \bar{1}$. Then by the defining axiom for $<$, we have $\exists y (y' + a) = 0'$ (since $\bar{1} \equiv 0'$).

Suppose b has that property, O.s., we have $(b' + a) = 0'$. We need to show $a = 0$. By axiom Q_3 , we have either $a = 0$ or that there is a c such that $a = c'$.

In the former case, there is nothing to show. So suppose $a = c'$. Then we have $(b' + c') = o'$. By axiom Q_5 of $\mathbf{Q}$, we have $(b' + c)' = o'$. By axiom Q_1 , we have $(b' + c) = o$. But this means, by axiom Q_8 , that $c < o$, contradicting [Lema req.23](#).

Now for the inductive step. We prove the case for $n + 1$, assuming the case for n . So suppose $a < \overline{n + 2}$. Again using Q_3 we can distinguish two cases: $a = o$ and for some b , $a = b'$. In the first case, $a = o \vee \dots \vee a = \overline{n + 1}$ follows trivially. In the second case, we have $b' < \overline{n + 2}$, O.s., $b' < \overline{n + 1}'$. By axiom Q_8 , for some c , $(c' + b') = \overline{n + 1}'$. By axiom Q_5 , $(c' + b)' = \overline{n + 1}'$. By axiom Q_1 , $(c' + b) = \overline{n + 1}$, and so $b < \overline{n + 1}$ by axiom Q_8 . By inductive hypothesis, $b = o \vee \dots \vee b = \overline{n}$. From this, we get $b' = o' \vee \dots \vee b' = \overline{n}'$ by logic, and so $a = \overline{1} \vee \dots \vee a = \overline{n + 1}$ since $a = b'$. $\square$

Lema req.25. For every natural number m ,

inc:req:min:
lem:trichotomy

$$\mathbf{Q} \vdash \forall y ((y < \overline{m} \vee \overline{m} < y) \vee y = \overline{m}).$$

Prova. By induction on m . First, consider the case $m = 0$. $\mathbf{Q} \vdash \forall y (y = o \vee \exists z y = z')$ by Q_3 . Let a be arbitrary. Then either $a = o$ or for some b , $a = b'$. In the former case, we also have $(a < o \vee o < a) \vee a = o$. But if $a = b'$, then $(b' + o) = (a + o)$ by the logic of $=$. By Q_4 , $(a + o) = a$, so we have $(b' + o) = a$, and hence $\exists z (z' + o) = a$. By the definition of $<$ in Q_8 , $o < a$. If $o < a$, then also $(o < a \vee a < o) \vee a = o$.

Now suppose we have

$$\mathbf{Q} \vdash \forall y ((y < \overline{m} \vee \overline{m} < y) \vee y = \overline{m})$$

and we want to show

$$\mathbf{Q} \vdash \forall y ((y < \overline{m + 1} \vee \overline{m + 1} < y) \vee y = \overline{m + 1})$$

Let a be arbitrary. By Q_3 , either $a = o$ or for some b , $a = b'$. In the first case, we have $\overline{m}' + a = \overline{m + 1}$ by Q_4 , and so $a < \overline{m + 1}$ by Q_8 .

Now consider the second case, $a = b'$. By the induction hypothesis, $(b < \overline{m} \vee \overline{m} < b) \vee b = \overline{m}$.

The first disjunct $b < \overline{m}$ is equivalent (by Q_8) to $\exists z (z' + b) = \overline{m}$. Suppose c has this property. If $(c' + b) = \overline{m}$, then also $(c' + b)' = \overline{m}'$. By Q_5 , $(c' + b)' = (c' + b')$. Hence, $(c' + b') = \overline{m}'$. We get $\exists u (u' + b') = \overline{m + 1}$ by existentially generalizing on c' and keeping in mind that $\overline{m}' \equiv \overline{m + 1}$. Hence, if $b < \overline{m}$ then $b' < \overline{m + 1}$ and so $a < \overline{m + 1}$.

Now suppose $\overline{m} < b$, O.s., $\exists z (z' + \overline{m}) = b$. Suppose c is such a z , O.s., $(c' + \overline{m}) = b$. By logic, $(c' + \overline{m})' = b'$. By Q_5 , $(c' + \overline{m}') = b'$. Since $a = b'$ and $\overline{m}' \equiv \overline{m + 1}$, $(c' + \overline{m + 1}) = a$. By Q_8 , $\overline{m + 1} < a$.

Finally, assume $b = \overline{m}$. Then, by logic, $b' = \overline{m}'$, and so $a = \overline{m + 1}$.

Hence, from each disjunct of the case for m and b , we can obtain the corresponding disjunct for $m + 1$ and a . $\square$

inc:req:min:
prop:rep-minimization

Proposição req.26. If $\varphi_g(x, z, y)$ represents $g(x, z)$ in $\mathbf{Q}$, then

$$\varphi_f(z, y) \equiv \varphi_g(y, z, 0) \wedge \forall w (w < y \rightarrow \neg \varphi_g(w, z, 0))$$

represents $f(z) = \mu x [g(x, z) = 0]$.

Prova. First we show that if $f(n) = m$, then $\mathbf{Q} \vdash \varphi_f(\bar{n}, \bar{m})$, O.s.,

$$\mathbf{Q} \vdash \varphi_g(\bar{m}, \bar{n}, 0) \wedge \forall w (w < \bar{m} \rightarrow \neg \varphi_g(w, \bar{n}, 0)).$$

Since $\varphi_g(x, z, y)$ represents $g(x, z)$ and $g(m, n) = 0$ if $f(n) = m$, we have

$$\mathbf{Q} \vdash \varphi_g(\bar{m}, \bar{n}, 0).$$

If $f(n) = m$, then for every $k < m$, $g(k, n) \neq 0$. So

$$\mathbf{Q} \vdash \neg \varphi_g(\bar{k}, \bar{n}, 0).$$

We get that

inc:req:min:
rep-less

$$\mathbf{Q} \vdash \forall w (w < \bar{m} \rightarrow \neg \varphi_g(w, \bar{n}, 0)). \quad (\text{req.6})$$

by **Lema req.23** in case $m = 0$ and by **Lema req.24** otherwise.

Now let's show that if $f(n) = m$, then $\mathbf{Q} \vdash \forall y (\varphi_f(\bar{n}, y) \rightarrow y = \bar{m})$. We again sketch the argument informally, leaving the formalization to the reader.

Suppose $\varphi_f(\bar{n}, b)$. From this we get (a) $\varphi_g(b, \bar{n}, 0)$ and (b) $\forall w (w < b \rightarrow \neg \varphi_g(w, \bar{n}, 0))$. By **Lema req.25**, $(b < \bar{m} \vee \bar{m} < b) \vee b = \bar{m}$. We'll show that both $b < \bar{m}$ and $\bar{m} < b$ leads to a contradiction.

If $\bar{m} < b$, then $\neg \varphi_g(\bar{m}, \bar{n}, 0)$ from (b). But $m = f(n)$, so $g(m, n) = 0$, and so $\mathbf{Q} \vdash \varphi_g(\bar{m}, \bar{n}, 0)$ since φ_g represents g . So we have a contradiction.

Now suppose $b < \bar{m}$. Then since $\mathbf{Q} \vdash \forall w (w < \bar{m} \rightarrow \neg \varphi_g(w, \bar{n}, 0))$ by **Eq. (req.6)**, we get $\neg \varphi_g(b, \bar{n}, 0)$. This again contradicts (a). $\square$

-NoValue-

req.8 Computable Functions are Representable in $\mathbf{Q}$

inc:req:crq:
sec

Teorema req.27. Every computable function is representable in $\mathbf{Q}$.

Prova. For definiteness, and using the Church–Turing Thesis, let's say that a function is computable iff it is general recursive. The general recursive functions are those which can be defined from the zero function zero, the successor function succ, and the projection function P_i^n using composition, primitive recursion, and regular minimization. By **Lema req.9**, any function h that can be defined from f and g can also be defined using composition and regular minimization from f , g , and zero, succ, P_i^n , add, mult, $\chi_{=}$. Consequently, a

function is general recursive iff it can be defined from zero, succ, P_i^n , add, mult, $\chi_=_$ using composition and regular minimization.

We've furthermore shown that the basic functions in question are representable in **Q** (Proposições req.10 a req.13, req.15 e req.17), and that any function defined from representable functions by composition or regular minimization (Proposição req.21, Proposição req.26) is also representable. Thus every general recursive function is representable in **Q**. $\square$

explanation

We have shown that the set of computable functions can be characterized as the set of functions representable in **Q**. In fact, the proof is more general. From the definition of representability, it is not hard to see that any theory extending **Q** (or in which one can interpret **Q**) can represent the computable functions. But, conversely, in any *derivação* system in which the notion of *derivação* is computable, every representable function is computable. So, for example, the set of computable functions can be characterized as the set of functions representable in Peano arithmetic, or even Zermelo–Fraenkel set theory. As Gödel noted, this is somewhat surprising. We will see that when it comes to provability, questions are very sensitive to which theory you consider; roughly, the stronger the axioms, the more you can prove. But across a wide range of axiomatic theories, the representable functions are exactly the computable ones; stronger theories do not represent more functions as long as they are axiomatizable.

-NoValue-

req.9 Representing Relations

Let us say what it means for a *relation* to be representable.

inc:req:rel:
sec

Definição req.28. A relation $R(x_0, \dots, x_k)$ on the natural numbers is *representable in Q* if there is a formula $\varphi_R(x_0, \dots, x_k)$ such that whenever $R(n_0, \dots, n_k)$ is true, **Q** proves $\varphi_R(\overline{n_0}, \dots, \overline{n_k})$, and whenever $R(n_0, \dots, n_k)$ is false, **Q** proves $\neg\varphi_R(\overline{n_0}, \dots, \overline{n_k})$.

inc:req:rel:
defn:representing-relations

Teorema req.29. A relation is representable in **Q** if and only if it is computable.

inc:req:rel:
thm:representing-rels

Prova. For the forwards direction, suppose $R(x_0, \dots, x_k)$ is represented by the formula $\varphi_R(x_0, \dots, x_k)$. Here is an algorithm for computing R : on input $n_0, \dots, n_k$, simultaneously search for a proof of $\varphi_R(\overline{n_0}, \dots, \overline{n_k})$ and a proof of $\neg\varphi_R(\overline{n_0}, \dots, \overline{n_k})$. By our hypothesis, the search is bound to find one or the other; if it is the first, report “yes,” and otherwise, report “no.”

In the other direction, suppose $R(x_0, \dots, x_k)$ is computable. By definition, this means that the function $\chi_R(x_0, \dots, x_k)$ is computable. By Teorema req.2, χ_R is represented by a formula, say $\varphi_{\chi_R}(x_0, \dots, x_k, y)$. Let $\varphi_R(x_0, \dots, x_k)$ be the formula $\varphi_{\chi_R}(x_0, \dots, x_k, \overline{1})$. Then for any $n_0, \dots, n_k$, if $R(n_0, \dots, n_k)$ is true, then $\chi_R(n_0, \dots, n_k) = 1$, in which case **Q** proves $\varphi_{\chi_R}(\overline{n_0}, \dots, \overline{n_k}, \overline{1})$, and

so $\mathbf{Q}$ proves $\varphi_R(\overline{n_0}, \dots, \overline{n_k})$. On the other hand, if $R(n_0, \dots, n_k)$ is false, then $\chi_R(n_0, \dots, n_k) = 0$. This means that $\mathbf{Q}$ proves

$$\forall y (\varphi_{\chi_R}(\overline{n_0}, \dots, \overline{n_k}, y) \rightarrow y = \overline{0}).$$

Since $\mathbf{Q}$ proves $\overline{0} \neq \overline{1}$, $\mathbf{Q}$ proves $\neg \varphi_{\chi_R}(\overline{n_0}, \dots, \overline{n_k}, \overline{1})$, and so it proves $\neg \varphi_R(\overline{n_0}, \dots, \overline{n_k})$. $\square$

Problema req.6. Show that if R is representable in $\mathbf{Q}$, so is χ_R .

-NoValue-

req.10 Undecidability

inc:req:und:
sec

We call a theory $\mathbf{T}$ *undecidable* if there is no computational procedure which, after finitely many steps and unfailingly, provides a correct answer to the question “does $\mathbf{T}$ prove φ ?” for any sentence φ in the language of $\mathbf{T}$. So $\mathbf{Q}$ would be decidable iff there were a computational procedure which decides, given a sentence φ in the language of arithmetic, whether $\mathbf{Q} \vdash \varphi$ or not. We can make this more precise by asking: Is the relation $\text{Prov}_{\mathbf{Q}}(y)$, which holds of y iff y is the Gödel number of a sentence provable in $\mathbf{Q}$, recursive? The answer is: no.

Teorema req.30. $\mathbf{Q}$ is undecidable, O.s., the relation

$$\text{Prov}_{\mathbf{Q}}(y) \Leftrightarrow \text{Sent}(y) \wedge \exists x \text{Prf}_{\mathbf{Q}}(x, y)$$

is not recursive.

Prova. Suppose it were. Then we could solve the halting problem as follows: Given e and n , we know that $\varphi_e(n) \downarrow$ iff there is an s such that $T(e, n, s)$, where T is Kleene’s predicate from ???. Since T is primitive recursive it is representable in $\mathbf{Q}$ by a formula ψ_T , that is, $\mathbf{Q} \vdash \psi_T(\overline{e}, \overline{n}, \overline{s})$ iff $T(e, n, s)$. If $\mathbf{Q} \vdash \psi_T(\overline{e}, \overline{n}, \overline{s})$ then also $\mathbf{Q} \vdash \exists y \psi_T(\overline{e}, \overline{n}, y)$. If no such s exists, then $\mathbf{Q} \vdash \neg \psi_T(\overline{e}, \overline{n}, \overline{s})$ for every s . But $\mathbf{Q}$ is ω -consistent, O.s., if $\mathbf{Q} \vdash \neg \varphi(\overline{n})$ for every $n \in \mathbb{N}$, then $\mathbf{Q} \not\vdash \exists y \varphi(y)$. We know this because the axioms of $\mathbf{Q}$ are true in the standard model $\mathfrak{N}$. So, $\mathbf{Q} \not\vdash \exists y \psi_T(\overline{e}, \overline{n}, y)$. In other words, $\mathbf{Q} \vdash \exists y \psi_T(\overline{e}, \overline{n}, y)$ iff there is an s such that $T(e, n, s)$, O.s., iff $\varphi_e(n) \downarrow$. From e and n we can compute $\# \exists y \psi_T(\overline{e}, \overline{n}, y)^\#$, let $g(e, n)$ be the primitive recursive function which does that. So

$$h(e, n) = \begin{cases} 1 & \text{if } \text{Prov}_{\mathbf{Q}}(g(e, n)) \\ 0 & \text{otherwise.} \end{cases}$$

This would show that h is recursive if $\text{Prov}_{\mathbf{Q}}$ is. But h is not recursive, by ??, so $\text{Prov}_{\mathbf{Q}}$ cannot be either. $\square$

Corolário req.31. First-order logic is undecidable.

Prova. If first-order logic were decidable, provability in $\mathbf{Q}$ would be as well, since $\mathbf{Q} \vdash \varphi$ iff $\vdash \tau \rightarrow \varphi$, where τ is the conjunction of the axioms of $\mathbf{Q}$. $\square$

-NoValue-

inp.11 Σ_1 completeness

Despite the incompleteness of $\mathbf{Q}$ and its consistent, axiomatizable extensions, we have seen that $\mathbf{Q}$ does prove many basic facts about numerals. In fact, this can be extended quite considerably. To understand the scope of what can be proved in $\mathbf{Q}$, we introduce the notions of Δ_0 , Σ_1 , and Π_1 *fórmulas*. Roughly speaking, a Σ_1 *fórmula* is one of the form $\exists x \psi(x)$, where ψ is constructed using only propositional connectives and bounded quantifiers. We shall show that if φ is a Σ_1 *sentença* which is true in $\mathfrak{N}$, then $\mathbf{Q} \vdash \varphi$ (**Teorema inp.38**).

inc:inp:s1c:
sec

Definição inp.32. A *bounded existential fórmula* is one of the form $\exists x (x < t \wedge \varphi(x))$ where t is any term, which we conventionally write as $(\exists x < t) \varphi(x)$. A *bounded universal fórmula* is one of the form $\forall x (x < t \rightarrow \varphi(x))$ where t is any term, which we conventionally write as $(\forall x < t) \varphi(x)$.

inc:inp:s1c:
defn:bd-quant

Definição inp.33. A *fórmula* ψ is Δ_0 if it is built up from atomic *fórmulas* using only propositional connectives and bounded quantification. A *fórmula* φ is Σ_1 if $\varphi \equiv \exists x \psi(x)$ where ψ is Δ_0 . A *fórmula* φ is Π_1 if $\varphi \equiv \forall x \psi(x)$ where ψ is Δ_0 .

inc:inp:s1c:
defn:delta0-sigma1-pi1-frn

Lema inp.34. Suppose t is a closed term such that $\text{Val}^{\mathfrak{N}}(t) = n$. Then $\mathbf{Q} \vdash t = \bar{n}$.

inc:inp:s1c:
lem:q-proves-clterm-id

Prova. We prove this by induction on the complexity of t . For the base case, $\text{Val}^{\mathfrak{N}}(0) = 0$, and $\mathbf{Q} \vdash 0 = \bar{0}$ since $\bar{0} \equiv 0$. For the inductive case, let t_1 and t_2 be terms such that $\text{Val}^{\mathfrak{N}}(t_1) = n_1$, $\text{Val}^{\mathfrak{N}}(t_2) = n_2$, $\mathbf{Q} \vdash t_1 = \bar{n}_1$, and $\mathbf{Q} \vdash t_2 = \bar{n}_2$.

Then $\text{Val}^{\mathfrak{N}}((t'_1)) = n_1 + 1$, and we have that $\mathbf{Q} \vdash t'_1 = \bar{n}_1'$ by the first-order rules for identity applied to the induction hypothesis and the *fórmula* $\bar{n}_1' = \overline{n_1'}$, so we have $\mathbf{Q} \vdash t'_1 = \overline{n_1 + 1}$ by the definition of numerals.

For sums we have

$$\text{Val}^{\mathfrak{N}}((t_1 + t_2)) = \text{Val}^{\mathfrak{N}}(t_1) + \text{Val}^{\mathfrak{N}}(t_2) = n_1 + n_2.$$

By the induction hypothesis and the rules for identity, $\mathbf{Q} \vdash t_1 + t_2 = \bar{n}_1 + \bar{n}_2$, and then $\mathbf{Q} \vdash t_1 + t_2 = \overline{n_1 + n_2}$ by a second application of the rules for identity. By **Lema req.16**, $\mathbf{Q} \vdash \bar{n}_1 + \bar{n}_2 = \overline{n_1 + n_2}$, so $\mathbf{Q} \vdash t_1 + t_2 = \overline{n_1 + n_2}$.

Similar reasoning also works for $\times$, using **Lema req.18**. Since this exhausts the closed terms of arithmetic, we have that $\mathbf{Q} \vdash t = \bar{n}$ for all closed terms t such that $\text{Val}^{\mathfrak{N}}(t) = n$. $\square$

Problema inp.7. Prove in detail the part of **Lema inp.34** involving $\times$.

Lema inp.35. Suppose t_1 and t_2 are closed terms. Then

inc:inp:s1c:
lem:atomic-completeness

1. If $\text{Val}^{\mathfrak{N}}(t_1) = \text{Val}^{\mathfrak{N}}(t_2)$, then $\mathbf{Q} \vdash t_1 = t_2$.
2. If $\text{Val}^{\mathfrak{N}}(t_1) \neq \text{Val}^{\mathfrak{N}}(t_2)$, then $\mathbf{Q} \vdash t_1 \neq t_2$.
3. If $\text{Val}^{\mathfrak{N}}(t_1) < \text{Val}^{\mathfrak{N}}(t_2)$, then $\mathbf{Q} \vdash t_1 < t_2$.

4. If $\text{Val}^{\mathfrak{N}}(t_2) \leq \text{Val}^{\mathfrak{N}}(t_1)$, then $\mathbf{Q} \vdash \neg(t_1 < t_2)$.

Prova. Given terms t_1 and t_2 , we fix $n = \text{Val}^{\mathfrak{N}}(t_1)$ and $m = \text{Val}^{\mathfrak{N}}(t_2)$.

Suppose $\varphi \equiv t_1 = t_2$. By **Lema inp.34**, $\mathbf{Q} \vdash t_1 = \bar{n}$ and $\mathbf{Q} \vdash t_2 = \bar{n}$. If $n = m$, then $\mathbf{Q} \vdash \bar{n} = \bar{m}$ and hence $\mathbf{Q} \vdash t_1 = t_2$ by the transitivity of identity. If $n \neq m$ then $\mathbf{Q} \vdash \bar{n} \neq \bar{m}$, and by the transitivity of identity again, $\mathbf{Q} \vdash t_1 \neq t_2$.

Now let $\varphi \equiv t_1 < t_2$. For both cases, we rely on axiom Q_8 , which states that $x < y \leftrightarrow \exists z z' + x = y$ for all x, y .

Suppose $\mathfrak{N} \models t_1 < t_2$. Then there exists some $k \in \mathbb{N}$ such that $n + k + 1 = m$. By **Lema inp.34**, $\mathbf{Q} \vdash t_1 = \bar{n}$ and $\mathbf{Q} \vdash t_2 = \bar{m}$, and by the first part of this lemma, $\mathbf{Q} \vdash \bar{n} + \bar{k}' = \bar{m}$. By the transitivity of identity it follows that $\mathbf{Q} \vdash \bar{k}' + t_1 = t_2$, so $\mathbf{Q} \vdash \exists z z' + t_1 = t_2$. By the right-to-left direction of Q_8 , $\mathbf{Q} \vdash t_1 < t_2$.

Suppose instead that $\mathfrak{N} \not\models t_1 < t_2$, O.s., $m \leq n$. We work in $\mathbf{Q}$ and assume that $t_1 < t_2$. By the left-to-right direction of Q_8 , there is some z such that $z' + t_1 = t_2$. Since $\mathbf{Q} \vdash t_1 = \bar{n}$ and $\mathbf{Q} \vdash t_2 = \bar{m}$, $z' + \bar{n} = \bar{m}$. By an external induction on m using Q_5 , $z' + \bar{n} - \bar{m} = 0$. If $m = n$ then $z' \neq 0$, giving a contradiction via Q_3 . If $m < n$ then $(z' + \bar{n} - \bar{m} - 1)' = 0$ by Q_5 again, giving a contradiction via Q_3 . So $\mathbf{Q} \vdash \neg(t_1 < t_2)$. $\square$

inc:inp:s1c: lem:bounded-quant-equiv **Lema inp.36.** Suppose φ is a *fórmula*, t a closed term, and $k = \text{Val}^{\mathfrak{N}}(t)$. Then

1. $\mathbf{Q} \vdash (\forall x < t) \varphi(x)$ iff $\mathbf{Q} \vdash \varphi(\bar{0}) \wedge \cdots \wedge \varphi(\overline{k-1})$.
2. $\mathbf{Q} \vdash (\exists x < t) \varphi(x)$ iff $\mathbf{Q} \vdash \varphi(\bar{0}) \vee \cdots \vee \varphi(\overline{k-1})$.

Prova. We prove the case for the bounded universal quantifier. If $\text{Val}^{\mathfrak{N}}(t) = 0$ then the left-hand side of the equivalence is provable in $\mathbf{Q}$, because there is no $x < \bar{0}$ by **Lema req.23**. Similarly, we can take an empty disjunction to be simply $\top$, which is also provable in $\mathbf{Q}$. We therefore suppose that $\text{Val}^{\mathfrak{N}}(t) = k + 1$ for some natural number k . By **Lema inp.34** we can assume that we are working with a *fórmula* of the form $(\forall x < \overline{k+1}) \varphi(x)$.

Suppose that $\mathbf{Q} \vdash (\forall x < \overline{k+1}) \varphi(x)$, and let $n \leq k$. Since $\mathbf{Q} \vdash \bar{n} < \overline{k+1}$ by **Lema inp.35**, it follows by logic that $\mathbf{Q} \vdash \varphi(\bar{n})$. Applying this fact $k + 1$ times for each $n \leq k$, we get that $\mathbf{Q} \vdash \varphi(\bar{0}) \wedge \cdots \wedge \varphi(\bar{k})$ as desired.

For the other direction, suppose that $\mathbf{Q} \vdash \varphi(\bar{0}) \wedge \cdots \wedge \varphi(\bar{k})$. Working in $\mathbf{Q}$, suppose that $x < \overline{k+1}$. By **Lema req.24** we have that $x = \bar{0} \vee \cdots \vee x = \bar{k}$, so by logic it follows that $\varphi(x)$, and hence the universal claim $(\forall x < \overline{k+1}) \varphi(x)$ follows.

The proof of the equivalence for bounded existentially quantified *fórmulas* is similar. $\square$

Problema inp.8. Give a detailed proof of the existential case in **Lema inp.36**.

inc:inp:s1c: lem:delta0-completeness **Lema inp.37.** If φ is a Δ_0 *sentença* which is true in $\mathfrak{N}$, then $\mathbf{Q} \vdash \varphi$.

Prova. We prove this by induction on **fórmula** complexity. The base case is given by **Lema inp.35**, so we move to the induction step. For simplicity we split the case of negation into subcases depending on the structure of the **fórmula** to which the negation is applied.

1. Suppose $(\varphi \wedge \psi)$ is true in $\mathfrak{N}$, so φ and ψ are true in $\mathfrak{N}$. By the induction hypothesis, $\mathbf{Q} \vdash \varphi$ and $\mathbf{Q} \vdash \psi$, so $\mathbf{Q} \vdash (\varphi \wedge \psi)$ by logic.
2. Suppose $\neg(\varphi \wedge \psi)$ is true in $\mathfrak{N}$, so either $\neg\varphi$ or $\neg\psi$ is true in $\mathfrak{N}$. Without loss of generality, suppose the former. By the induction hypothesis $\mathbf{Q} \vdash \neg\varphi$, and hence $\mathbf{Q} \vdash \neg(\varphi \wedge \psi)$ by logic.
3. Suppose $(\varphi \vee \psi)$ is true in $\mathfrak{N}$, so either φ is true in $\mathfrak{N}$ or ψ is true in $\mathfrak{N}$. Without loss of generality, suppose the former holds. By the induction hypothesis $\mathbf{Q} \vdash \varphi$, and hence $\mathbf{Q} \vdash (\varphi \vee \psi)$ by logic.
4. Suppose $\neg(\varphi \vee \psi)$ is true in $\mathfrak{N}$, so $\neg\varphi$ and $\neg\psi$ are true in $\mathfrak{N}$. Then $\mathbf{Q} \vdash \neg\varphi$ and $\mathbf{Q} \vdash \neg\psi$ by the induction hypothesis. Consequently, $\mathbf{Q} \vdash \neg(\varphi \vee \psi)$ by logic.
5. Suppose that $(\forall x < t) \varphi(x)$ is true in $\mathfrak{N}$, where t is a closed term and $k = \text{Val}^{\mathfrak{N}}(t)$. By the induction hypothesis and logic, if $\varphi(\bar{n})$ is true in $\mathfrak{N}$ for all $n < \text{Val}^{\mathfrak{N}}(t)$ then $\mathbf{Q} \vdash \varphi(\bar{0}) \wedge \dots \wedge \varphi(\bar{k-1})$. By **Lema inp.36** it follows that $\mathbf{Q} \vdash (\forall x < t) \varphi(x)$.
6. The case for the bounded existential quantifier, where we have a **sentença** of the form $(\exists x < t) \varphi(x)$, is similar to that for the bounded universal quantifier.
7. Suppose that $\neg(\forall x < t) \varphi(x)$ is true in $\mathfrak{N}$, where t is a closed term. This **sentença** is equivalent to the **sentença** $(\exists x < t) \neg\varphi(x)$, with the equivalence derivable in $\mathbf{Q}$, so we may apply the reasoning for bounded existential quantifiers.
8. Similarly, suppose that $\neg(\exists x < t) \varphi(x)$ is true in $\mathfrak{N}$, where t is a closed term. This **sentença** is equivalent in $\mathbf{Q}$ to $(\forall x < t) \neg\varphi(x)$, and so we may apply the reasoning for bounded universal quantifiers.
9. Finally, suppose $\neg\varphi$ is true in $\mathfrak{N}$. The only cases remaining are when φ is atomic and when $\neg\varphi \equiv \neg\neg\psi$ for some Δ_0 **sentença** ψ . If φ is atomic then by **Lema inp.35**, $\mathbf{Q} \vdash \neg\varphi$. If $\neg\varphi \equiv \neg\neg\psi$, then by logic it is provably equivalent in $\mathbf{Q}$ to ψ , which is true in $\mathfrak{N}$ since $\neg\varphi$ is true in $\mathfrak{N}$. By the induction hypothesis we therefore have that $\mathbf{Q} \vdash \neg\varphi$. $\square$

Problema inp.9. Give a detailed proof of the existential case in **Lema inp.37**.

Teorema inp.38. If φ is a Σ_1 **sentença** which is true in $\mathfrak{N}$, then $\mathbf{Q} \vdash \varphi$.

*inc:inp:s1c:
thm:sigma1-completeness*

Prova. If $\exists x\varphi(x)$ is a Σ_1 **sentença** which is true in $\mathfrak{N}$, then there exists a natural number n and a variable assignment s such that $s(x) = n$ and $\mathfrak{N}, s \models \varphi(x)$. By standard facts about the satisfaction relation it follows that $\mathfrak{N} \models \varphi(\bar{n})$. But $\varphi(\bar{n})$ is a Δ_0 **fórmula**, so by **Lema inp.37** we have that $\mathbf{Q} \vdash \varphi(\bar{n})$, and hence by logic we also have that $\mathbf{Q} \vdash \exists x \varphi(x)$. $\square$

Créditos das Imagens

Referências Bibliográficas