University of Verona
Minicourse

Ingo Blechschmidt
June 2024

Extracting programs from proofs

Exercise sheet 1: Constructive mathematics

Exercise 1.1. *An epistemic riddle on transcendental numbers*

Verify, using a proof by contradiction, that at least one of the numbers $e+\pi$ and $e-\pi$ is transcendental; and that at least one of the numbers $e+\pi$ and $e\cdot\pi$ is transcendental.

Note. A number is *transcendental* if and only if, like π or e, it is not algebraic. A number is *algebraic* if and only if, like $\sqrt{2}$ or $1/998999$, it is a zero of a monic polynomial with rational coefficients of positive degree. At time of writing, for none of these numbers a (constructive or classical) proof of their transcendence is known.

Exercise 1.2. *Constructive status of classical tautologies*

Which of the following classical tautologies can reasonably be expected to admit constructive proofs?

(a) $\neg(\alpha\vee\beta)\implies\neg\alpha\wedge\neg\beta$

(b) $\neg(\alpha\wedge\beta)\implies\neg\alpha\vee\neg\beta$

(c) $(\alpha\Rightarrow\beta)\implies(\neg\alpha\vee\beta)$

(d) $\big((\alpha\vee\beta)\wedge\neg\alpha\big)\implies\beta$

(e) $\forall n:\mathbb{N}.\ (n=0\vee n\neq 0)$

(f) $\forall x:\mathbb{R}.\ (x=0\vee x\neq 0)$

(g) $\forall x:\mathbb{R}.\ (\neg(\exists y:\mathbb{R}.\ xy=1)\Rightarrow x=0)$

(h) $\forall z:\overline{\mathbb{Q}}.\ (z=0\vee z\neq 0)$

(i) $\forall M:P(X).\ (\exists x:X.\ x\in M)\vee M=\emptyset$ —*already interesting for* $X=\{\star\}$

(j) $\forall f:\mathbb{N}\to\{0,1\}.\ (\neg\neg\exists n:\mathbb{N}.\ f(n)=0)\Rightarrow(\exists n:\mathbb{N}.\ f(n)=0)$ —*Markov's principle*

(k) $\forall f:\mathbb{N}\to\{0,1\}.\ \exists n:\mathbb{N}.\ (f(n)=1\Rightarrow(\forall m:\mathbb{N}.\ f(m)=1))$ —*Drinker's paradox*

(l) $\forall f:\mathbb{N}\to\{0,1\}.\ (\exists n:\mathbb{N}.\ f(n)=0)\vee(\forall n:\mathbb{N}.\ f(n)=1)$

(m) $\forall f:\mathbb{N}_\infty\to\{0,1\}.\ (\exists n:\mathbb{N}_\infty.\ f(n)=0)\vee(\forall n:\mathbb{N}_\infty.\ f(n)=1)$

Remark. The set $\mathbb{N}_\infty$ is the *one-point compactification* of $\mathbb{N}$. A sensible definition of it in constructive mathematics is as the set of decreasing binary sequences $(x_0,x_1,x_2,\ldots)$. The naturals embed into $\mathbb{N}_\infty$ by mapping n to the sequence $1^n0^\omega=(1,\ldots,1,0,\ldots,)$, and an element not in the image of this embedding is $\infty:=1^\omega=(1,1,\ldots)$. Assuming the principle of excluded middle (or already weaker principles), every element of $\mathbb{N}_\infty$ is of one of these two forms. Martín Escardó has worked extensively on unexpected instances of the principle of omniscience for searchable sets like $\mathbb{N}_\infty$ [3, 5, 4].

Exercise 1.3. *Basics on negation*

Recalling that negation is defined as implying absurdity, $\neg\varphi:\equiv(\varphi\Rightarrow\bot)$, verify intuitionistically without recourse to truth tables:

(a) $\varphi\Rightarrow\neg\neg\varphi$

(b) $\neg\neg\neg\varphi\Leftrightarrow\neg\varphi$

(c) $\neg\neg(\varphi\vee\neg\varphi)$

(d) $\neg\neg(\alpha\wedge\beta)\Leftrightarrow(\neg\neg\alpha\wedge\neg\neg\beta)$

(e) $\neg(\alpha\vee\beta)\Longleftrightarrow(\neg\alpha\wedge\neg\beta)$

(f) $\neg(\exists x:X.\ \varphi(x))\Longleftrightarrow(\forall x:X.\ \neg\varphi(x))$

(g) $(\neg\neg\alpha\wedge(\alpha\Rightarrow\neg\neg\beta))\Longrightarrow\neg\neg\beta$

(h) $(\forall\psi.\ (\psi\vee\neg\psi))\Longleftrightarrow(\forall\psi.\ (\neg\neg\psi\Rightarrow\psi))$

Hint for (h). Don't try to verify that double negation elimination for a specific statement ψ implies the principle of excluded middle for that same statement ψ – this cannot be shown. There are subtleties regarding the quantification over ψ (this is not expressible in pure first-order logic), however the exercise is still instructive if we gloss over this issue.

Exercise 1.4. *Lead astray…?*

Let $f : X \to Y$ be a map. Let $f^{-1}[\cdot] : P(Y) \to P(X)$ be the induced map between powersets, i. e. $f^{-1}[V] = \{x : X \mid f(x) \in V\}$. It is a basic fact that if f is surjective, then $f^{-1}[\cdot]$ is injective. In this exercise we are concerned with the reverse.

(a) Complete the following germ of a classical proof. "Assume for the sake of contradiction that there is an elemenet $y : Y$ which is not in the range of f. Considering $V := Y \setminus \{y\}, \ldots$"

(b) Is there also a constructive proof?

Exercise 1.5. *A stronger form of the irrationality of* $\sqrt{2}$

Mine the proof of the theorem below to give an intuitionistic proof of the fact that for every rational number x, the distance $|\sqrt{2} - x|$ is positive.

> **Thm.** It is not the case that there exists a rational number x such that $x^2 = 2$.
>
> *Proof.* Let a rational number x with $x^2 = 2$ be given. Writing $x = a/b$ with integers a and b, we have $a^2 = 2b^2$. The prime factor 2 occurs an even number of times on the left hand side and an odd number of times on the right hand side; contradiction. □

Note. Strictly speaking, this exercise presupposes familiarity with an intuitionistic account of the basics of undergraduate real analysis. Without it, one cannot really be expected to precisely think about these matters. One such account (though assuming the axiom of dependent choice) is [2]. However, this exercise is insightful even when carried out slightly informally. Keep in mind that, to show that a real number is positive, constructively it is not enough to merely verify that it cannot be zero or negative. A safe way to verify that a real number a is positive is to exhibit a rational number b such that $a \geq b > 0$.

Exercise 1.6. *Minima of sets of natural numbers* ⚙

Prove intuitionistically:

(a) Every inhabited detachable set of natural numbers contains a minimum.

(b) Every inhabited set of natural numbers does *not not* contain a minimum.

(c) If every inhabited set of natural numbers contains a minimum, then the law of excluded middle holds.

(d) Every finitely generated vector space over a residue field does *not not* have a basis.

Note. A *residue field* is a commutative ring such that for every element x, if x is not invertible, then it is zero.

Exercise 1.7. *Markov's principle*

Markov's principle is the statement that

$$\forall f : \mathbb{N} \to \{0, 1\}.\ (\neg\neg\exists n : \mathbb{N}.\ f(n) = 0) \Rightarrow (\exists n : \mathbb{N}.\ f(n) = 0).$$

It is a simple instance of the classical principle of double negation elimination, but not available in (most schools of) constructive mathematics.

(a) Show that Markov's principle implies that Turing machines which do not run forever halt.

(b) How do you feel about Markov's principle?

Exercise 1.8. *Diaconescu's theorem*

The axiom of choice can be put as: "Every surjective map has a section." (A *section* s to a surjective map f is a map in the other direction such that $f \circ s = \mathrm{id}$.) A theorem of Diaconescu states that the axiom of choice implies the principle of excluded middle. To this end, let φ be a statement and consider the subsets

$$U = \{x \in X \mid (x = 0) \vee \varphi\}$$
$$V = \{x \in X \mid (x = 1) \vee \varphi\}$$

of the discrete set $X := \{0, 1\}$.

(a) Verify that $U = V$ if and only if φ.

(b) Using that $x = y \vee x \neq y$ for all elements $x, y \in X$, show that the existence of a section of the surjective map

$$\begin{array}{ccc} X & \longrightarrow & \{U, V\} \\ 0 & \longmapsto & U \\ 1 & \longmapsto & V \end{array}$$

implies $\varphi \vee \neg\varphi$.

Exercise 1.9. *Brouwerian counterexamples*

Show that each of the following statements implies the principle of excluded middle, hence is not available in constructive mathematics.

(a) "Every ideal of $\mathbb{Z}$ is finitely generated."

Hint. Use that finitely generated ideals of $\mathbb{Z}$ are principal ideals and consider the ideal $\mathfrak{a} := \{x \in \mathbb{Z} \mid x = 0 \vee \varphi\}$.

Remark. The failure of every ideal of $\mathbb{Z}$ to be finitely generated should not be misconstrued to exclaim that in constructive mathematics, there suddenly would be ideals of $\mathbb{Z}$ of infinite rank. The failure is simply because, given an abstract ideal, we cannot pinpoint a finite system of generators.

(b) "Over every field, the polynomial $X^2 + 1$ is either reducible or irreducible."

Hint. Consider the field $K := \{z \in \mathbb{Q}(i) \mid z \in \mathbb{Q} \vee \varphi\}$.

(c) "Subsets of Kuratowski-finite sets are Kuratowski-finite."

Note. A set X is *Kuratowski-finite* if and only if, for some number $n \in \mathbb{N}$, there is a surjective map $[n] \to X$, where $[n] = \{0, 1, \ldots, n-1\}$. More briefly, a set X is Kuratowski-finite iff its elements can be enumerated: $X = \{x_1, \ldots, x_n\}$.

(d) "Every subset of the (Cauchy or Dedekind) reals which is inhabited and bounded from above has a supremum."

Note. A *supremum* of a set M of reals is a number s such that $M \leq s$ (that is $x \leq s$ for all $x \in M$) and such that for every number s' with $M \leq s'$, $s \leq s'$. In constructive mathematics, we can make finer distinctions between the classically equivalent constructions of the real numbers: The reals constructed using Cauchy sequences inject into the reals constructed using Dedekind cuts which in turn inject into the MacNeille reals, and each serve a different purpose. The Cauchy and Dedekind reals cannot constructively be shown to be complete in the sense of this exercise, while the MacNeille reals can. Conversely, the rationals can be shown to be dense in the first two kinds of reals but not in the MacNeille reals [6, Section D4.7].

Show that the following statement implies Markov's principle (from Exercise 1.2):

(e) "Every real number which is not zero is invertible."

Brouwerian counterexamples abound in constructive mathematics; when developing a constructive account of a theory, they help to clearly demarcate its limits. As such additional Brouwerian counterexamples can be found in most texts on constructive mathematics, such as [8]; a compilation mainly from constructive analysis can be found in [7].

Ingo Blechschmidt

Extracting programs from proofs

Exercise sheet 2: Realizability theory

$$\frac{}{\varphi \vdash_{\vec{x}} \varphi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi}{\varphi[\vec{s}/\vec{x}] \vdash_{\vec{y}} \psi[\vec{s}/\vec{x}]} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \chi}$$

$$\frac{}{\varphi \vdash_{\vec{x}} \top} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \varphi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \wedge \chi}$$

$$\frac{}{\bot \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{}{\psi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \chi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vee \psi \vdash_{\vec{x}} \chi}$$

$$\frac{\varphi \wedge \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \Rightarrow \chi}$$

$$\frac{\varphi \vdash_{\vec{x},y} \psi}{\exists y : Y.\, \varphi \vdash_{\vec{x}} \psi} \ (y \text{ not occurring in } \psi) \qquad \frac{\varphi \vdash_{\vec{x},y} \psi}{\varphi \vdash_{\vec{x}} \forall y : Y.\, \psi} \ (y \text{ not occurring in } \varphi)$$

$$\frac{}{\top \vdash_x x = x} \qquad \frac{}{(\vec{x} = \vec{y}) \wedge \varphi \vdash_{\vec{z}} \varphi[\vec{y}/\vec{x}]}$$

("$\vec{x} = \vec{y}$" is short for "$x_1 = y_1 \wedge \cdots \wedge x_n = y_n$".)

The rules of sequent calculus.

$e \Vdash s = t$	iff $s = t$.
$e \Vdash \top$	iff true.
$e \Vdash \bot$	iff false.
$e \Vdash (\varphi \wedge \psi)$	iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_1 \cdot e \Vdash \varphi$ and $\pi_2 \cdot e \Vdash \psi$.
$e \Vdash (\varphi \vee \psi)$	iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and if $\pi_1 \cdot e = 0$ then $\pi_2 \cdot e \Vdash \varphi$, and if $\pi_1 \cdot e \neq 0$ then $\pi_2 \cdot e \Vdash \psi$.
$e \Vdash (\varphi \Rightarrow \psi)$	iff for every $r \in \mathbb{N}$ such that $r \Vdash \varphi$, $e \cdot r \downarrow$ and $e \cdot r \Vdash \psi$.
$e \Vdash (\forall n : N.\, \varphi(n))$	iff for every $n_0 \in \mathbb{N}$, $e \cdot n_0 \downarrow$ and $e \cdot n_0 \Vdash \varphi(n_0)$.
$e \Vdash (\exists n : N.\, \varphi(n))$	iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_2 \cdot e \Vdash \varphi(\pi_1 \cdot e)$.
$e \Vdash (\forall f : N^N.\, \varphi(f))$	iff for every $f_0 : \mathbb{N} \to \mathbb{N}$ and every $r_0 \in \mathbb{N}$ such that f_0 is computed by the r_0-th machine and $e \cdot r_0 \downarrow$ and $e \cdot r_0 \Vdash \varphi(f_0)$.
$e \Vdash (\exists f : N^N.\, \varphi(f))$	iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and the $(\pi_1 \cdot e)$-th machine computes a function $f_0 : \mathbb{N} \to \mathbb{N}$ and $\pi_2 \cdot e \Vdash \varphi(f_0)$.

The realizability semantics.

Exercise 2.1. *Schwichtenberg's paradox*

Using advanced methods in algebraic and arithmetic geometry, Wiles and Taylor proved *Fermat's Last Theorem*: For all positive natural numbers x, y, z, n with $n \geq 3$, $x^n + y^n \neq z^n$. Without mining their proof, write down a simple realizer for this statement.

Exercise 2.2. *Soundness of realizability*

Verify in detail the soundness theorem: If Heyting arithmetic proves a sequent $\varphi \vdash_{\vec{x}} \psi$, then the statement $\forall \vec{x}.\ (\varphi \Rightarrow \psi)$ is realizable.

Exercise 2.3. *Markov's principle, revisited*

Show that Markov's principle (from Exercise 1.7) is realized by a Turing machine—assuming that Markov's principle is available in the metatheory.

Hint. "Unbounded search." You need the metatheoretic principle only to verify the correctness of your machine, not to construct it.

Exercise 2.4. *Realizability using infinite time Turing machines*

Which of the following statements are validated by the realizability model built on infinite time Turing machines instead of ordinary Turing machines?

(a) "For every function $f : \mathbb{N} \to \mathbb{N}$ there is either an input n such that $f(n) = 0$, or $f(n) \neq 0$ for all inputs n."

(b) "Every function $\mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ is continuous."

Note. By definition (matching the structure of a metric space we can put on $\mathbb{N}^{\mathbb{N}}$), a function $P : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ is *continuous* if and only if for every function $\alpha : \mathbb{N} \to \mathbb{N}$, there is a number $N \in \mathbb{N}$ such that for all functions $\beta : \mathbb{N} \to \mathbb{N}$ with $\alpha(k) = \beta(k)$ for all $k < N$, $P(\alpha) = P(\beta)$.

(c) "If $\forall n : N.\ \neg\neg\varphi(n)$, then $\neg\neg\forall n : N.\ \varphi(n)$."

(d) Defying classical expectations on sizes of sets, exhibit an infinite time Turing machine realizing the following statement:

$$\exists P : N^{N^N}.\ \forall \alpha : N^N.\ \forall \beta : N^N.\ (P(\alpha) = P(\beta) \Rightarrow \alpha = \beta).$$

Note. The claim amounts to the existence of an infinite time Turing machine which inputs the source of an infinite time Turing machine A computing a function $\mathbb{N} \to \mathbb{N}$ and outputs a number $n(A)$ such that $n(A) = n(B)$ if and only if A and B compute the same function. This result is due to Andrej Bauer, who pioneered combining realizability and infinite time Turing machines [1].

Exercise 2.5. *Countable choice*

(a) Verify—without appealing to countable choice in the metatheory—that the realizability model validates countable choice:

$$\big(\forall x : N.\ \exists y : N.\ \varphi(x, y)\big) \Longrightarrow \big(\exists f : N^N.\ \forall x : N.\ \varphi(x, f(x))\big)$$

(b) What goes wrong with choice for functions?

$$\big(\forall x : N^N.\ \exists y : N.\ \varphi(x, y)\big) \Longrightarrow \big(\exists f : N^{N^N}.\ \forall x : N^N.\ \varphi(x, f(x))\big)$$

(c) Prove that choice for functions *is* realized by an infinite time Turing machine.

Exercise 2.6. *A counterexample to the axiom of choice*

Let M_x be the x'th Turing machine in some adequate enumeration of all Turing machines. We define an equivalence relation on $\mathbb{N}$ by setting $x \sim y$ if and only if M_x and M_y have the same halting behavior (on empty input), i. e. M_x terminates iff M_y terminates.

(a) Prove constructively that every Turing machine terminates (on empty input) or does not terminate, if there is a function $\mathbb{N}/\!\sim \to \mathbb{N}$ which maps every equivalence class to one of its representatives.

(b) Conclude that the realizability model falsifies the axiom of choice.

University of Verona
Minicourse

Ingo Blechschmidt
June 2024

Extracting programs from proofs

Exercise sheet 3: Double negation

The double negation translation $\varphi^{\neg\neg}$ of a formula φ is obtained by replacing

$$\begin{array}{rcll} \exists & \rightsquigarrow & \exists^{\mathrm{cl}}, & \text{where} \quad \exists^{\mathrm{cl}} :\equiv \neg\neg\exists, \\ \vee & \rightsquigarrow & \vee^{\mathrm{cl}}, & \text{where} \quad \alpha \vee^{\mathrm{cl}} \beta :\equiv \neg\neg(\alpha \vee \beta), \\ = & \rightsquigarrow & =^{\mathrm{cl}}, & \text{where} \quad s =^{\mathrm{cl}} t :\equiv \neg\neg(s = t). \end{array}$$

The double negation translation.

Exercise 3.1. *Drinker's paradox*

The Drinker's paradox is the tautology

$$\forall f : \mathbb{N} \to \{0,1\}.\ \exists n : \mathbb{N}.\ (f(n) = 1 \Rightarrow (\forall m : \mathbb{N}.\ f(m) = 1))$$

of classical logic. A proof proceeds as follows: By the principle of excluded middle, either there is a number n such that $f(n) = 0$ or not. In the first case, we can take such a number n as the desired n. In the second case, we can take $n := 0$.

(a) Determine the double negation translation of the Drinker's paradox.

(b) Tell a classical logic fairy tale for Drinker's paradox similar to the story for Dickson's lemma. The protagonist of the story will change their mind regarding the correct value of n; what is their first choice?

(c) Connect the Drinker's paradox to the issue of minima of sets of natural numbers.

Exercise 3.2. *The infinite pidgeonhole principle [G. Stolzenberg]*

The infinite pidgeonhole principle states that for every function $f : \mathbb{N} \to \{0,1\}$,

$$\big(\forall a : \mathbb{N}.\ \exists b : \mathbb{N}.\ b \geq a \wedge f(b) = 0\big) \quad \vee \quad \big(\forall a : \mathbb{N}.\ \exists b : \mathbb{N}.\ b \geq a \wedge f(b) = 1\big);$$

in other words, there is a value which is attained infinitely often.

(a) Give a classical proof of this principle.

(b) Explain that the infinite pidgeonhole principle does not admit a constructive proof by considering which feat a hypothetical realizer would need to accomplish.

(c) A consequence of the infinite pidgeonhole principle is that for every function $f : \mathbb{N} \to \{0,1\}$, there are numbers $i < j$ such that $f(i) = f(j)$. Find a direct constructive proof of this consequence.

(d) Deduce a constructive proof of the consequence studied in (c) by applying the double negation translation with the continuation escape trick to the classical proof of (a). Does the algorithm described by this constructive proof agree with the algorithm which computes $f(0)$, $f(1)$ and $f(2)$ and looks for two equal values among these three?

Exercise 3.3. *The fundamental features of the double negation translation*

Verify the following features of the double negation translation.

(a) For every formula φ (in the language of arithmetic), intuitionistic logic proves $\neg\neg\varphi^{\neg\neg} \Rightarrow \varphi^{\neg\neg}$.

(b) For every *coherent formula* φ (a formula in which only $= \top \bot \wedge \vee \exists$ occur, but no $\Rightarrow \forall$), intuitionistic logic proves $\varphi^{\neg\neg} \Leftrightarrow \neg\neg\varphi$.

(c) A sequent $\varphi \vdash_{\vec{x}} \psi$ is provable (from some set Γ of axioms) in classical predicate logic if and only if the sequent $\varphi^{\neg\neg} \vdash_{\vec{x}} \psi^{\neg\neg}$ is provable (from the set $\{\alpha^{\neg\neg} \mid \alpha \in \Gamma\}$ as axioms) in intuitionistic predicate logic.

Exercise 3.4. *Stability of the axioms*

Peano arithmetic (PA) is set in the language $(0, S, +, \cdot)$ and has the following axioms (where leading universal quantifiers are supressed for brevity):

(1) $x + 0 = x$

(2) $x + Sy = S(x + y)$

(3) $x \cdot 0 = 0$

(4) $x \cdot Sy = (x \cdot y) + x$

(5) $Sx \neq 0$

(6) $Sx = Sy \Rightarrow x = y$

(7) $y = 0 \vee (\exists x.\ y = Sx)$

(8) $P(0) \wedge (\forall n.\ P(n) \Rightarrow P(Sn)) \Longrightarrow (\forall n.\ P(n))$ (one axiom for each formula $P(n)$)

Heyting arithmetic (HA) has exactly the same axioms, but is based on intuitionistic logic instead of classical logic.

(a) Show that HA proves the double negation translation of each axiom of PA.

(b) Look up the axioms of Intuitionistic Zermelo–Fraenkel set theory, IZF, and convince yourself that IZF does not prove the double negation translation of the axiom of choice.

Remark. As a result, the double negation translation alone is insufficient to extract constructive content from proofs using the axiom of choice. Advanced techniques, for instance rooted in pointfree topology, are required.

Exercise 3.5. *A largest natural number…?*

"Obviously, 0 is the largest number. Oh, 1 is larger than 0 you say? Okay, let's backtrack. Obviously, 1 is the largest number. Oh, 2 is larger than 1? Okay, let's backtrack. Obviously, 2 is the largest number…" Explain carefully why this non-terminating procedure, as exemplified by the Agda code below, *fails* to realize the double negation translation of the refutable claim "$\exists n : \mathbb{N}.\ \forall m : \mathbb{N}.\ n \geq m$".

```
maximum : ¬ ¬ ∃[ n ] ((m : ℕ) → ¬ ¬ n ≥ m)
maximum = go 0
  where
  go : ℕ → ¬ ¬ ∃[ n ] ((m : ℕ) → ¬ ¬ n ≥ m)
  go n k = k (n , h)
    where
    h : (m : ℕ) → ¬ ¬ n ≥ m
    h m with ≤-<-connex m n
    ... | inj₁ m≤n = return m≤n
    ... | inj₂ n<m = λ k' → go m k
```

Exercise 3.6. *No constructive content*

Let $\mathsf{Prf}(p)$ be a formula of arithmetic expressing that p is a correct encoding of a PA-proof of $\bot$. A consequence of Gödel's second incompleteness theorem is that there is no PA-proof of

$$G :\equiv (\forall p.\ \neg \mathsf{Prf}(p)),$$

even though for each number p_0 it is actually the case that (and PA can verify that) p_0 does not constitute a correct encoding of a PA-proof of $\bot$.

(a) Give a PA-proof, using the principle of excluded middle, of the statement

$$\exists q.\ (\mathsf{Prf}(q) \vee G).$$

(b) Show that for no number $q_0 \in \mathbb{N}$, the statement "$\mathsf{Prf}(\underline{q_0}) \vee G$" admits a PA-proof. In this sense no witness can be extracted from the classical proof in (a).

References

[1] A. Bauer. "An injection from the Baire space to natural numbers". In: *Math. Structures Comput. Sci.* 25.7 (2015), pp. 1484–1489.

[2] E. Bishop and D. Bridges. *Constructive Analysis*. Springer, 1985.

[3] M. Escardó. *Infinite sets that satisfy the principle of omniscience in all varieties of constructive mathematics*. Slides for Dagstuhl 2011, available online. 2011.

[4] M. Escardó. "Infinite sets that satisfy the principle of omniscience in any variety of constructive mathematics". In: *J. Symbolic Logic* 78.3 (2013), pp. 764–784.

[5] M. Escardó. *Infinite sets that satisfy the principle of omniscience in constructive type theory*. Slides for Tallinn 2017, available online. 2017.

[6] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*. Oxford University Press, 2002.

[7] M. Mandelkern. "Brouwerian counterexamples". In: *Math. Mag.* 62.1 (1989), pp. 3–27.

[8] R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer, 1988.