Chapter 2
Unwinding proofs ('Proof Mining')

2.1 Introductory remark

In this chapter we give – exemplified by a couple of easy but fundamental examples – a kind of tour-de-force through a number of topics which will be developed in detail throughout the rest of this book. The aim of this chapter is to provide the reader with a guiding line by explaining (in more technical terms than in the previous chapter) the main goals we are aiming at in this book and the difficulties one has to address in the course of this. We recommend to read this chapter first at a somewhat informal level skipping maybe some technical details but to revisit it after the study of the material up to chapter 11.

2.2 Informal treatment of ineffective proofs

Proof interpretations of the kind we are going to study in this book are tools to extract constructive (computational) data from given proofs by recursion on the proof. Such data quite often cannot directly be read off from a proof but are hidden behind the use of quantifiers.
G. Kreisel was the first to formulate the program of unwinding proofs under the general question:

'What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?'

The term 'unwinding of proofs' is due to G. Kreisel. More recently, D. Scott suggested to us to use the more catchy slogan 'proof mining' which we find quite appropriate for this area of applied proof theory.

What do we mean by 'constructive data'?

E.g.

1) Realizing terms from a proof of an existential theorem $A \equiv \exists x B(x)$ (closed).
A weaker requirement is to construct a list of terms $t_1, \ldots, t_n$ which are candidates for A, i.e. such that $B(t_1) \vee \ldots \vee B(t_n)$ holds.
More general: If $A \equiv \forall x \exists y B(x,y)$, then one can ask for an algorithm p such that $\forall x B(x, p(x))$ holds (or – weaker – for a bounding function b such that

$$\forall x \exists y \leq b(x) B(x,y),$$

if e.g. y ranges over the natural numbers).
2) weakening of the assumptions used in the proof: e.g. replacing general assumptions by specific instances of them.

What type of information one can expect (in general) depends of course on the structure of the theorem A to be proved and the principles used in its proof.
A first, very rough, division of the structure of a sentence (i.e. a closed formula) A can be made according to the quantifier complexity of A :

From now on $A_0, B_0, C_0, \ldots$ always denote quantifier-free formulas. Sometimes we also write A_{qf}. Instead of a single variable we may have (here and in the following) also a tuple $\underline{x} = x_1, \ldots, x_n$ of variables.

1) A purely universal, i.e. $A \equiv \forall x A_0(x)$, where A_0 is quantifier-free.
Such sentences A, sometimes called complete, don't ask for any witnessing data. So the problem of extracting data is empty here.

2) A purely existential, i.e. $A \equiv \exists x A_0(x)$. We treat this as a special case of

3) $A \equiv \forall x \exists y A_0(x,y)$. Let's consider the case where $x, y \in \mathbb{N}$ and $A_0 \in \mathscr{L}(\mathrm{PA})$ (here PA denotes first order Peano arithmetic which we assume to contain all primitive recursive functions; see chapter 3 for a precise definition). A_0 is decidable (Exercise: $A_0(\underline{x}) \in \mathscr{L}(\mathrm{PA})$, then one can construct a primitive recursive function term t such that $\mathrm{PA} \vdash \forall \underline{x}(t(\underline{x}) = 0 \leftrightarrow A_0(\underline{x}))$) (see proposition 3.8 below) and, therefore, defines a partial recursive function f, namely

$$f(x) := \begin{cases} \min y[A_0(x,y)], \text{ if } \exists y A_0(x,y) \\ \text{undefined, otherwise.} \end{cases}$$

A just says that f is total recursive.

Questions: How to extract a non-trivial program for f (different from simple unbounded search) from a proof of A? What is the complexity and the rate of growth of f if A is proved in a certain theory $\mathscr{T}$?

Theorems expressing that a set $\{y \in \mathbb{N} : A(y)\} \subseteq \mathbb{N}$ is infinite have the form

$$\forall x \in \mathbb{N} \exists y \geq x A(y).$$

Quite often A can be expressed in a quantifier-free way A_0 in PA, so that this falls under the general form $\forall x \exists y B_0(x,y)$, where

$$B_0(x,y) :\equiv (y \geq x \wedge A_0(y)).$$

As an example consider the following

Proposition 2.1. *There are infinitely many prime numbers.*

The predicate $P(x) :\equiv$ 'x is a prime number' can be expressed in a quantifier-free way as a primitive recursive predicate (see e.g. [194, 371]).

Proof 1 (Euclid): Define $a := 1 + \prod_{\substack{p \leq x \\ p \text{ prime}}} p$. a cannot be divided by any prime number $p \leq x$. By the decomposition of every number into prime factors it follows that a contains a prime factor $q \leq a$ with $q > x$. □

From this proof one immediately gets the bound $g(x) := 1 + x! \, (\geq 1 + \prod_{\substack{p \leq x \\ p \text{ prime}}} p)$. By the Stirling formula we obtain

$$g(x) \sim 1 + (2\pi x)^{\frac{1}{2}} (\frac{x}{e})^x = 1 + \sqrt{2\pi} \cdot e^{x \ln x - x + \frac{1}{2} \ln x}.$$

In order to obtain from Euclid's proof an upper bound on the $(r+1)$-th prime number p_{r+1} which only depends on r instead of $x \geq p_r$ one can argue as follows: Euclid's proof yields that

$$p_{r+1} \leq p_1 \cdot \ldots \cdot p_r + 1.$$

From this one obtains (exercise) by induction on r that

$$p_r < 2^{2^r} \text{ for all } r \geq 1.$$

Proof 2 (Euler): Suppose that there are only finitely many prime numbers $p_1, \ldots, p_r$ (listed in increasing order, $r \geq 1$). One has

$$\begin{aligned} &\sum_{0 \leq \alpha_1, \ldots, \alpha_r \leq n} \frac{1}{p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}} = \left(\sum_{i=0}^{n} \frac{1}{p_1^i} \right) \cdot \ldots \cdot \left(\sum_{i=0}^{n} \frac{1}{p_r^i} \right) \\ &< \frac{1}{1 - \frac{1}{p_1}} \cdot \ldots \cdot \frac{1}{1 - \frac{1}{p_r}} = \frac{p_1}{p_1 - 1} \cdot \ldots \cdot \frac{p_r}{p_r - 1} \\ &\leq \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \ldots \cdot \frac{p_r}{p_r - 1} = p_r \end{aligned}$$

(note that this holds for all $n \in \mathbb{N}$).
It follows (using the decomposition into prime numbers) that for all $n \in \mathbb{N}$

$$\sum_{i=1}^{n} \frac{1}{i} \leq p_r.$$

But this contradicts the fact that $\sum_{i=1}^{\infty} \frac{1}{i} = \infty$. □

Quantitative analysis of Euler's proof:
We need a quantitative version of '$\sum_{i=1}^{n} \frac{1}{i} \overset{n\to\infty}{\to} \infty$', more precisely we need a bound on $\exists n\big(\sum_{i=1}^{n} \frac{1}{i} > p_r\big)$. It is known that $\sum_{i=1}^{n} \frac{1}{i} - \ln(n) \searrow C$, where $C \approx 0.5772...$ is the so-called Euler-Mascheroni constant. Hence for $n_r := \lceil e^{p_r - C} \rceil$ we have $\sum_{i=1}^{n_r} \frac{1}{i} > p_r$ (and this is essentially optimal). From the proof above it follows that for all $n \in \mathbb{N}$

$$\sum_{0 \leq \alpha_1, \ldots, \alpha_r \leq n} \frac{1}{p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}} \leq p_r.$$

Hence there must be an i $(1 \leq i \leq n_r)$ which contains a prime factor p with $p_r < p \leq i \leq n_r$. So put together

$$\exists p(p \text{ prime } \wedge p_r < p \leq \lceil e^{p_r - C} \rceil).$$

Applying this argument to all prime numbers $p_1 < \ldots < p_{r_x} \leq x$ we obtain

$$\forall x \exists p(p \text{ prime } \wedge x < p \leq \lceil e^{x - C} \rceil).$$

So we can take $g(x) := \lceil e^{x-C} \rceil$ (or an appropriate upper bound of this to make it computable).

Conclusion: Euler's proof yields a bound that is slightly better than the one from Euclid's proof.

Improvement of the analysis: The estimate at the beginning of Euler's proof can be improved (using that $p_i \geq i+1$) to

$$\begin{aligned}
&\sum_{0 \leq \alpha_1, \ldots, \alpha_r \leq n} \frac{1}{p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}} = \left(\sum_{i=0}^{n} \frac{1}{p_1^i}\right) \cdot \ldots \cdot \left(\sum_{i=0}^{n} \frac{1}{p_r^i}\right) \\
&< \frac{1}{1 - \frac{1}{p_1}} \cdot \ldots \cdot \frac{1}{1 - \frac{1}{p_r}} \leq \frac{1}{1 - \frac{1}{2}} \cdot \ldots \cdot \frac{1}{1 - \frac{1}{r+1}} \\
&= \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \ldots \cdot \frac{r+1}{r} = r+1.
\end{aligned}$$

Analogously to the previous analysis we now get that (for $r \geq 1$) the $r+1$-th prime number p_{r+1} is upper bounded by $g(r) := \lceil e^{r+1-C} \rceil$ which is exponential in r (and no longer in $x \geq p_r$) and constitutes a significant improvement over the double exponential upper bound (in r) from Euclid's proof (e.g. from the former bound one gets the lower bound $\ln x$ for $x \geq 1$ (exercise) for the Euler π-function

$\pi(x) := |\{p : p \text{ prime } \wedge p \leq x\}|$ whereas the bound from Euclid's proof only yields $\ln\ln x$ (for $x \geq 2$) as a lower bound (exercise, see also [149]).

Remark 2.2. Euler's proofs uses as a lemma the fact that $\sum_{i=1}^{\infty} \frac{1}{i} = \infty$, i.e.

$$\forall k \exists n (\sum_{i=1}^{n} \frac{1}{i} \geq k),$$

which itself (just as the conclusion) is of the form $\forall x \exists y A_0(x,y)$. Hence what the analysis of Euler's proof actually provides is a procedure that transforms a rate of divergence of the harmonic series into a bound on a prime number $p \geq x$. In the analysis above we directly applied this to the rate of divergence resulting from

$$\sum_{i=1}^{n} \frac{1}{i} - \ln(n) \searrow C.$$

Proof 3: Let $p_1, \ldots, p_r$ ($r \geq 1$) be the first r primes and define for $x \geq 1$
$N(x) := \{n \leq x : n \geq 1 \wedge n \text{ is not divisible by any prime } p > p_r\}$. We can express $n \in N(x)$ in the form $n = n_1^2 m$ where m is 'squarefree', i.e. is not divisible by a square of any prime.
We have $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_r^{b_r}$, where $b_i \in \{0,1\}$. There are 2^r possible exponents and consequently at most 2^r different values of m. Also, because of $n_1 \leq \sqrt{n} \leq \sqrt{x}$, there are not more than $\sqrt{x}$ different values of n_1. Hence $|N(x)| \leq 2^r \sqrt{x}$. Now if there were only finitely many primes $p_1, \ldots, p_r$, then $|N(x)| = x$ for every x and so $2^r \sqrt{x} \geq x$ for all x which is a contradiction.

From this proof one gets a bound as follows: Let $p_1, \ldots, p_r$ be the first r primes. Define $x := (2^r)^2 + 1 = 2^{2r} + 1$. Then $2^r \sqrt{x} < x$. Hence $\exists n \leq x (n$ is divisible by some prime $p > p_r)$ and so $\exists p (p \text{ prime } \wedge p_r < p \leq 2^{2r} + 1 = 4^r + 1)$.
So we get again a bound $g(r) := 4^r + 1$ which is exponential in r rather than p_r.

For another proof (in fact a variant of proof 3) see the exercise 1. Still further proofs can be found in [2].

Discussion:

1) All three proofs provide more information than the mere fact that 'there are infinitely many primes' is true. By making their quantitative content explicit one can compare them with respect to their numerical quality.
2) The unwindings of the proofs 1)–3) were straightforward and didn't require any tools from logic as guiding principles. However there are more complicated proofs where the use of proof-theoretic tools turned out to be decisive in practice (see e.g. [122, 267, 204, 205]). The final verification of the data extracted will always be again an ordinary mathematical proof (obtained by a proof-theoretic transformation of the original proof) which does not rely on any logical metatheorems (in contrast to the verification of the general procedure of transformation).

This differs from many model theoretic applications to mathematics where the provability or the truth in some model of the conclusion is established without exhibiting a proof which doesn't rely on model theoretic theorems.

3) Already the a-priori information, provided by a general metatheorem, that e.g. a certain computable bound must be extractable from a given proof which is formalizable in a certain system $\mathscr{T}$ can be an important step in actually finding such a bound even if the latter is carried out by ad hoc methods and doesn't follow closely any proof-theoretic procedure.

Remark 2.3. If A does not have the form $\forall x\exists y A_0(x,y)$ right away it may have so after some logical transformations, e.g.

$$A :\equiv \big(\exists x\forall y A_0(x,y) \to \forall u\exists v B_0(u,v)\big)$$

is logically equivalent to the prenex normal form

$$A^{pr} :\equiv \forall u,x\exists v,y\big(A_0(x,y) \to B_0(u,v)\big)$$

so that the reasoning above applies to the A^{pr}.

4) $A \equiv \exists x\forall y A_0(x,y)$: From a proof of A (even in first order logic without equality $\mathrm{PL}_{--=}$) one cannot (in general) obtain a realization $\forall y A_0(t,y)$ nor a list of candidates such that $\bigvee_{i=1}^{n} \forall y A_0(t_i,y)$ ($t,t_1,\ldots,t_n$ not containing y) holds:

Proposition 2.4. *There exists a logically valid sentence $A \equiv \exists x\forall y A_0(x,y) \in \mathscr{L}(\mathrm{PA})$ in the language of Peano arithmetic* PA *such that there is* **no** *list of closed terms $t_1,\ldots,t_k \in \mathscr{L}(\mathrm{PA})$ such that*

$$\mathrm{PA} \vdash \bigvee_{i=1}^{k} \forall y A_0(t_i,y).$$

Proof: Take $P(x) :\equiv Prov_{\mathrm{PA}}(x, \ulcorner \overline{0} = \overline{1} \urcorner)$ and $A_0(x,y) :\equiv P(x) \vee \neg P(y)$ (here '$Prov_{\mathrm{PA}}(x, \ulcorner \overline{0} = \overline{1} \urcorner)$' expresses primitive recursively 'x is the Gödel number of a PA-proof of $0 = 1$' (see e.g. [194]). Suppose there are closed terms $t_1,\ldots,t_k$ such that

$$(1)\ \mathrm{PA} \vdash \bigvee_{i=1}^{k} \forall y A_0(t_i,y).$$

Within PA each t_i can be computed to a numeral $\overline{n}_i$:

$$(2)\ \mathrm{PA} \vdash t_i = \overline{n}_i \text{ for } 1 \le i \le k.$$

By (1) and (2) we have

$$(3)\ \mathrm{PA} \vdash \bigvee_{i=1}^{k} \forall y A_0(\overline{n}_i,y).$$

By the consistency of PA we know that

$$(4)\ \mathbb{N} \models \bigwedge_{i=1}^{k} \neg P(\overline{n}_i).$$

Hence by the numeralwise representability of primitive recursive predicates in PA we have

$$(5)\ \mathrm{PA} \vdash \bigwedge_{i=1}^{k} \neg P(\overline{n}_i).$$

But (3) and (5) imply

$$(6)\ \mathrm{PA} \vdash \forall y \neg Prov_{\mathrm{PA}}(y, \ulcorner \overline{0} = \overline{1} \urcorner),$$

which contradicts Gödel's second incompleteness theorem. □

However, although PA is not able to verify $\bigvee_{i=1}^{k} \forall y A_0(t_i, y)$ for any tuple of terms t_i **we** can (using the consistency of PA) verify this on the meta-level: In fact, for **any** term t, e.g. for 0, we know that $\forall y A_0(t, y)$ is true in $\mathbb{N}$ simply because

$$\mathbb{N} \models \forall y \neg Prov_{\mathrm{PA}}(y, \ulcorner \overline{0} = \overline{1} \urcorner).$$

However, there are other examples where –in general– even this is not possible, e.g. take

$$A_e :\equiv \exists x \forall y \big(T(\overline{e}, \overline{e}, x) \vee \neg T(\overline{e}, \overline{e}, y)\big),$$

where T is the (primitive recursive) Kleene-T-predicate, i.e. $T(x, y, z) :\equiv$ 'the Turing machine with Gödel number x applied to the input y terminates with a computation whose Gödel number is z' (see e.g. [371]).
In general we are not able to determine closed terms $t_1, \ldots, t_k$ such that

$$\mathbb{N} \models \bigvee_{i=1}^{k} \forall y \big(T(\overline{e}, \overline{e}, t_i) \vee \neg T(\overline{e}, \overline{e}, y)\big),$$

since this would allow us to decide whether $\exists x T(\overline{e}, \overline{e}, x)$ or not (simply check whether $\bigvee_{i=1}^{k} T(\overline{e}, \overline{e}, t_i)$ is true or not).

In fact, for

$$A :\equiv \forall x \exists y \forall z \big(T(x, x, y) \vee \neg T(x, x, z)\big)$$

A is provable in PA using only the logical axioms and rules and hence in $\mathrm{PL}_{-=}$, but there is no computable bound g on '$\exists y$', i.e. no computable g such that

$$\forall x \exists y \leq g(x) \forall z \big(T(x, x, y) \vee \neg T(x, x, z)\big)$$

since this would make the (special) halting problem $\{x \in \mathbb{N} : \exists y \in \mathbb{N}(T(x,x,y))\}$ decidable by the then computable function

$$f(x) := \begin{cases} 0, \text{ if } \exists y \leq g(x)(T(x,x,y)) \\ 1, \text{ otherwise.} \end{cases}$$

We sometimes make use of the following definition:

Definition 2.5. A formula $A \in \mathscr{L}(\mathrm{PL})$ in prenex normal form is called Π^0_n-formula if it has n-alternating blocks of equal quantifiers starting with a block of universal quantifiers, i.e.

$$\forall \underline{x}_1 \exists \underline{x}_2 \ldots \forall / \exists \underline{x}_n A_0(\underline{x}_1, \ldots, \underline{x}_n),$$

where $\underline{x}_i$ are tuples of variables. If the formula starts with a block of existential quantifiers

$$\exists \underline{x}_1 \forall \underline{x}_2 \ldots \exists / \forall \underline{x}_n A_0(\underline{x}_1, \ldots, \underline{x}_n)$$

it is called Σ^0_n-formula.

Remark 2.6. The upper index '0' only is relevant in theories with higher order quantifiers (over functions and functionals) where then it indicates that all the quantifiers range over the first order ('base type') variables.
Many theories, such as PA, allow the contraction of tuples of variables into single variables.

As we discussed above, infinity statements (for quantifier-free properties) in number theory have the form of Π^0_2-formulas. So an important class of Σ^0_2-formulas are finiteness statements, i.e.

$$\exists x \forall y > x \neg A_0(y,a),$$

where a, y are the only free variables in $A_0(y,a)$. We now may ask for

- a computable bound $h(a)$ on the height of the solutions, i.e.

$$\forall a \forall y > h(a) \neg A_0(y,a)$$

or

- a computable bound $N(a)$ on the number of solutions, i.e.

$$N(a) \geq |\{y : A_0(y,a)\}|.$$

It is clear that any h also is an upper bound N on the number of solutions but in general the existence of a computable function N does not imply the existence of a computable height function h as the following example (due to [267]) shows: consider again Kleene's T-predicate and define

$$A_0(y,a) :\equiv T(a,a,y).$$

Then clearly $N(a) := 1$ is a bound on the number of solutions but by the undecidability of the special halting problem there is no computable (in a) bound $h(a)$ on y.

In general, for Σ^0_2-finiteness theorems not even a computable (in the parameters) bound N exists ([267]): Let

$$A_0(y,a) :\equiv T(a,a,j_2(y)) \wedge 0 < j_1(y) \leq j_2(y),$$

where we refer to some standard pairing/unpairing functions j, j_1, j_2 (see definition 3.30 below). Here the number of solutions and their maximal size coincide and so neither of them is computable.

Famous finiteness theorems in mathematics are Roth's theorem ([317]) on the number of exceptionally good rational approximations of irrational algebraic numbers and Falting's theorem establishing the Mordell conjecture ([97]). In both cases effective bounds N are known but no computable bounds h.

Roth's theorem says the following

Theorem 2.7 (Roth [317]). An algebraic irrational number α has only finitely many exceptionally good rational approximations, i.e. for $\varepsilon > 0$ there are only finitely many $q \in \mathbb{N}$ such that

$$R(q) :\equiv q > 1 \wedge \exists! p \in \mathbb{Z} : (p,q) = 1 \wedge |\alpha - pq^{-1}| < q^{-2-\varepsilon}.$$

The first polynomial bound N in the case of Roth's theorem was obtained in Luckhardt [267] by extracting Herbrand terms (see theorem 2.18 and the subsequent discussion below) from a proof of Roth's theorem due to Esnault and Viehweg [94] using certain growth properties of these terms (following general ideas from Kreisel [249]).

Theorem 2.8 (Luckhardt [267]). The following upper bound on $\#\{q : R(q)\}$ holds:

$$\#\{q : R(q)\} < \frac{7}{3}\varepsilon^{-1}\log N_\alpha + 6 \cdot 10^3 \varepsilon^{-5} \log^2 d \cdot \log(50\varepsilon^{-2}\log d),$$

where $N_\alpha < \max(21\log 2h(\alpha), 2\log(1+|\alpha|))$ and h is the logarithmic absolute homogeneous height.

Independently, a roughly similar bound was obtained in Bombieri-van der Poorten [38] using a more ad hoc strategy.

Two elementary examples of non-constructive proofs in number theory:

Proposition 2.9. $\exists a,b \in \mathbb{R}\big(a,b \text{ irrational } \wedge a^b \text{ rational}\big)$.

Proof: Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Put $a := b := \sqrt{2}$.
Case 2: $\sqrt{2}^{\sqrt{2}}$ irrational. Put $a := \sqrt{2}^{\sqrt{2}}, b := \sqrt{2}$. □

Remark 2.10. In the example above, the matrix 'a,b irrational $\wedge a^b$ rational' is more complex than Π^0_1 : Using the representation of real number from chapter 4 below 'a,b irrational' is in Π^0_2 and 'a^b rational' is in Σ^0_2.

From this proof we get two candidates for (a,b), namely $(\sqrt{2},\sqrt{2})$ and $(\sqrt{2}^{\sqrt{2}},\sqrt{2})$ but no decision which one satisfies the proposition.

Remark 2.11. 1) From a deep result of Gelfand and Schneider, stating that if a,b are algebraic, $a \neq 0,1$ and b irrational, then a^b is transcendental, it follows that $\sqrt{2}^{\sqrt{2}}$ is transcendental and, therefore, irrational. So it is the pair $(\sqrt{2}^{\sqrt{2}},\sqrt{2})$ which satisfies the proposition.

2) While it requires the Gelfand-Schneider theorem to determine which of the candidates $(\sqrt{2},\sqrt{2})$ and $(\sqrt{2}^{\sqrt{2}},\sqrt{2})$ satisfies the proposition, there is a trivial argument (which we learned from G. Stolzenberg) that provides an explicit solution to proposition 2.9: take $a := \sqrt{2}$ and $b := 2\log_2(3)$. b is irrational since $\log_2(3) = m/n$ for some $m,n \in \mathbb{N}^*$ would imply that $2^m = 3^n$ which is impossible. Clearly, $a^b = 3$ is rational.

Here is another example (communicated by H. Friedman) of a simple non-constructive proof in number theory:

Proposition 2.12. *$(e-\pi$ is irrational$)$ or $(e+\pi$ is irrational$)$.*

Proof: One easily formalizes the proof of the irrationality of e as given e.g. in [149] in PA. If both $e-\pi$ and $e+\pi$ were rational, then also their sum $2e$ and, therefore, e would be rational which is a contradiction. □

Remark 2.13. In 1996, it was proved by Yu.V. Nesterenko ([285]) that e^π and π are algebraically independent and hence $\pi + e^\pi$ is transcendental whereas for $e+\pi$ and $e-\pi$ individually the question of transcendence is still open.

2.3 Herbrand's theorem and the no-counterexample interpretation

We have seen that already for Σ^0_2, Π^0_3-sentences A (i.e. $A \equiv \exists n \forall m A_0(n,m)$ or $A \equiv \forall k \exists n \forall m A_0(k,n,m)$ where A_0 is recursive) it is not possible in general to compute witnesses resp. bounds. However one can obtain such witness candidates and bounds (and even realizing function(al)s) for a weakened version of A, namely its so-called Herbrand normal form A^H:

Definition 2.14. $A \equiv (\forall y_0)\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0(y_0,x_1,y_1,\ldots,x_n,y_n)$. Then the Herbrand normal form of A is defined as

$$A^H :\equiv (\forall y_0)\exists x_1,\ldots,x_n A_0(y_0,x_1,f_1(x_1),\ldots,x_n,f_n(x_1,\ldots,x_n)),$$

where $f_1,\ldots,f_n$ are new function symbols, called Herbrand index functions.

Remark 2.15. In theories with function variables and function quantifiers we take the Herbrand normal form of A to be

$$A^H :\equiv \forall(y_0), f_1, \ldots, f_n \exists x_1, \ldots, x_n A_0(y_0, x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)).$$

In the following PL denotes first order predicate logic with equality.
For prenex sentences A, A and A^H are equivalent with respect to logical validity, i.e.

$$\models A \Leftrightarrow \models A^H$$

(this fact is also expressed by saying that A^H is a validity normal form) but are not logically equivalent since in general

$$\mathrm{PL} \nvdash A^H \to A.$$

However the converse implication holds

$$\mathrm{PL}_{-=} \vdash A \to A^H.$$

Remark 2.16. The dual normal form in which the existentially quantified variables in a prenex normal formula are replaced by new function symbols depending on the universally quantified variables from the universal quantifiers to the left is called Skolem normal form and denoted by A^S, i.e. for

$$A :\equiv \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n A_0(x_1, y_1, \ldots, x_n, y_n)$$

$$A^S :\equiv \forall x_1, \ldots, x_n A_0(x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)).$$

The function symbols $f_1, \ldots, f_n$ are called Skolem functions.
For prenex sentences A, the Skolem normal form is a satisfiability normal form.
Unfortunately, the terminology differs for different authors. Sometimes the name Skolem normal form is used for what we call Herbrand normal form.

Let $\mathrm{PL}^2_{(-=)}$ denote the extension of $\mathrm{PL}_{(-=)}$ obtained by the addition of n-ary function variables (for every n) and function quantifiers.
Let furthermore AC denote the schema of choice

$$\mathrm{AC}\colon \forall \underline{x} \exists y A(\underline{x}, y) \to \exists f \forall \underline{x} A(\underline{x}, f(\underline{x})) \quad (\underline{x} = x_1, \ldots, x_n),$$

then it is an easy exercise to show that

$$\mathrm{PL}^2_{-=} + \mathrm{AC} \vdash A \leftrightarrow A^H.$$

We now consider again the sentence

$$A \equiv \forall x \exists y \forall z \big(P(x, y) \vee \neg P(x, z)\big),$$

where P is some predicate symbol. In contrast to A, the Herbrand normal form A^H of A

$$A^H \equiv \exists y\big(P(x,y) \vee \neg P(x,g(y))\big)$$

allows an interpretation in form of a list of candidates (uniformly in x,g) for '$\exists y$', namely (x,gx) and also (c,gc) for any constant c does the job since the disjunction

$$A^{H,D} :\equiv \big(P(x,c) \vee \neg P(x,g(c))\big) \vee \big(P(x,g(c)) \vee \neg P(x,g(g(c)))\big)$$

is a tautology.
A tautology remains a tautology if we replace all occurrences of a term s by a variable y: Replace $g(c)$ by y and $g(g(c))$ by z. Then $A^{H,D}$ becomes

$$A^D :\equiv \big(P(x,c) \vee \neg P(x,y)\big) \vee \big(P(x,y) \vee \neg P(x,z)\big),$$

which still is a tautology. From A^D we can derive A by a so-called direct proof (which uses only appropriate quantifier introduction rules, the shift of quantifiers over $\vee$ and contraction):

$$\begin{array}{c}
P(x,c) \vee \neg P(x,y) \vee P(x,y) \vee \neg P(x,z) \\
\Downarrow (\forall\text{-introduction}) \\
P(x,c) \vee \neg P(x,y) \vee \forall z\big(P(x,y) \vee \neg P(x,z)\big) \\
\Downarrow (\exists\text{-introduction}) \\
P(x,c) \vee \neg P(x,y) \vee \exists y \forall z\big(P(x,y) \vee \neg P(x,z)\big) \\
\Downarrow (\forall\text{-introduction}) \\
\forall y\big(P(x,c) \vee \neg P(x,y)\big) \vee \exists y \forall z\big(P(x,y) \vee \neg P(x,z)\big) \\
\Downarrow (\exists\text{-introduction}) \\
\exists u \forall y\big(P(x,u) \vee \neg P(x,y)\big) \vee \exists y \forall z\big(P(x,y) \vee \neg P(x,z)\big) \\
\Downarrow (\text{contraction}) \\
\exists y \forall z\big(P(x,y) \vee \neg P(x,z)\big) \\
\Downarrow (\forall\text{-introduction}) \\
\forall x \exists y \forall z\big(P(x,y) \vee \neg P(x,z)\big)
\end{array}$$

Definition 2.17. A formula A in the language of first order predicate logic with equality (PL) is called a quasi-tautology if it is a tautological consequence of instances of $=$-axioms.

Theorem 2.18 (Herbrand's Theorem).
Let $A \equiv \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0(x_1,y_1,\ldots,x_n,y_n)$. Then the following holds:
$\mathrm{PL}_{-=} \vdash A$ *iff there are terms $t_{1,1},\ldots,t_{1,k_1},\ldots,t_{n,1},\ldots,t_{n,k_n}$ (built up out of the constants, free variables and function symbols of A and the index functions used for the*

formation of A^H) such that

$$A^{H,D} :\equiv \bigvee_{j_1=1}^{k_1} \dots \bigvee_{j_n=1}^{k_n} A_0\big(t_{1,j_1}, f_1(t_{1,j_1}), \dots, t_{n,j_n}, f_n(t_{1,j_1}, \dots, t_{n,j_n})\big)$$

is a tautology.
The terms $t_{i,j}$ can be extracted constructively from a given $\mathrm{PL}_{-=}$*-proof of A and conversely one can construct a* $\mathrm{PL}_{-=}$*-proof for A out of a given tautology $A^{H,D}$.*
The theorem holds for PL *if 'tautology' is replaced by 'quasi-tautology'.*

Proof: See e.g. [332]. □

The most difficult part of the proof of Herbrand's theorem is the construction of the Herbrand terms $t_{i,j}$. The reverse direction for $\mathrm{PL}_{-=}$ follows similar to the special case treated above: the f_i-terms in $A^{H,D}$ are replaced by new variables (starting from terms of maximal size) yielding an index-function-free Herbrand disjunction A^D. From this A is derived by a direct proof. For PL the reverse direction is more complicated to establish since also instances of equality axioms $\underline{x} = \underline{y} \to f_i(\underline{x}) = f_i(\underline{y})$ are now allowed in the proof of $A^{H,D}$.

In applications, the Herbrand disjunction A^D without index function has been particular useful (see [249],[267]). Although it is quite complicated to write down the general form of such a disjunction it is easy for Π^0_3-sentences (which is sufficient for many applications in mathematics):

For sentences $A \equiv \forall x \exists y \forall z A_0(x,y,z)$, A^D can always be written in the form

$$A_0(x,t_1,b_1) \vee A_0(x,t_2,b_2) \vee \dots \vee A_0(x,t_k,b_k),$$

where the b_i are new variables and t_i does not contain any b_j with $i \leq j$ (see [249]).

Herbrand's theorem immediately extends to so-called open theories, i.e. first order theories $\mathscr{T}$ whose non-logical axioms $G_1, \dots, G_m$ are all purely universal ($G_i \equiv \forall a_i G_0^i(a_i)$), if '(quasi-)tautology' is replaced by 'tautological consequence of instances of equality axioms and the non-logical axioms'.

Proof: Apply Herbrand's theorem for logic to

$$\tilde{A} :\equiv \exists x_1 \forall y_1 \dots \exists x_n \forall y_n \exists a_1, \dots, a_m \big(\bigwedge_{i=1}^{m} G_0^i(a_i) \to A_0(x_1, y_1, \dots, x_n, y_n)\big).$$

□

Warning: For the extension of Herbrand's theorem to open theories $\mathscr{T}$ it is important that the index function used in defining A^H are new and do not occur in the

non-logical axioms. In particular if we have a schema of purely universal axioms then in the statement of Herbrand's theorem this schema is always understood with respect to the original language (without the index functions). Otherwise the reverse direction in Herbrand's theorem in general would fail (see [202] for a discussion of this and related matters thereby pointing out errors in the literature).

In general Herbrand's theorem in the form stated above does not hold for theories which are not open, e.g. it fails for PA.
However there are ways to extend the general idea behind Herbrand's theorem to theories like PA and beyond: in this book we will discuss various forms of Gödel's functional interpretation (chapters 8, 9, 10) and the so-called no-counterexample interpretation (due to G. Kreisel [241, 242], see further below in this chapter and chapter 10). We conclude this chapter by motivating the latter and also indicating its limitations:

Let's consider again the example

$$A \equiv \forall x \exists y \forall z \big(P(x,y) \vee \neg P(x,z)\big).$$

If P is formulated in some theory like PA with decidable prime formulas, e.g. if $P(x,y) \equiv T(x,x,y)$, then we can realize the Herbrand normal form A^H of A instead of using a disjunction also by a computable functional of type level 2 which is defined by cases:

$$\Phi(x,g) := \begin{cases} x & \text{if } \neg T(x,x,g(x)) \\ g(x) & \text{otherwise.} \end{cases}$$

From this definition it easily follows that

$$\forall x,g \big(T(x,x,\Phi(x,g)) \vee \neg T(x,x,g(\Phi(x,g)))\big).$$

If A is not provable in PL but e.g. in PA we no longer can expect that functionals as simple as Φ above will be sufficient. In addition to the use of definition by cases we also have to allow certain recursive definitions whose complexity depends on the strength of the theory in which A is proved. In this book we will show e.g. in the case of PA (and subsystems) what functionals are needed.

Definition 2.19. Let $A \equiv \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_0(x_1,y_1,\ldots,x_n,y_n)$. If a tuple of functionals $\Phi_1,\ldots,\Phi_n$ realizes the Herbrand normal form A^H of A, i.e. if

$$\forall \underline{f} A_0\big(\Phi_1(\underline{f}), f_1(\Phi_1(\underline{f})),\ldots,\Phi_n(\underline{f}), f_n(\Phi_1(\underline{f}),\ldots,\Phi_n(\underline{f}))\big)$$

is true (where $\underline{f} = f_1,\ldots,f_n$), then we say that $\underline{\Phi}(= \Phi_1,\ldots,\Phi_n)$ satisfies the no-counterexample interpretation of A (short: $\underline{\Phi}$ n.c.i. A).
If A starts with a universal quantifier $\forall y_0$ then y_0 is considered as a 0-place index function and Φ_i now depends on y_0 and $\underline{f}$.

Motivation for the name 'no-counterexample interpretation':

Let A be as above. Then $\neg A$ is equivalent to

$$\forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \neg A_0(x_1, y_1, \ldots, x_n, y_n).$$

So a counterexample to A is given by functions $f_1, \ldots, f_n$ such that

$$(+)\ \forall \underline{x} \neg A_0(x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n))$$

holds. Hence functionals $\underline{\Phi}$ satisfying the n.c.i. of A produce a counterexample to $(+)$ i.e. to the existence of counterexample functions $f_1, \ldots, f_n$.

The no-counterexample interpretation can indeed be realized for many interesting classical theories (in particular Peano arithmetic **PA** for which it was designed by Kreisel) and fragments thereof by certain subrecursive classes of functionals. E.g. we will show in chapter 10 that theorems of the fragment $\mathbf{PA}_1$ of **PA** with the schema of induction restricted to purely existential (Σ^0_1-)formulas always have functionals satisfying the no-counterexample interpretation which are primitive recursive in the sense of Kleene. This was first shown by Parsons ([299]) and will be proved in chapter 10. Full Peano arithmetic requires primitive recursive functionals in higher types in the extended sense of Gödel [133] (see chapter 3 and – again – chapter 10 below).

Definition 2.20. A function $f : \mathbb{N}^k \to \mathbb{N}$ is called primitive recursive if it can be defined by the following schemas:

1) The initial functions $Z(x) = 0$ (Zero), $P^p_i(x_0, \ldots, x_{p-1}) = x_i$ $p \geq 1, i < p$ (Projections), $S(x) = x + 1$ (Successor) are primitive recursive.
2) If $h_0(x_0, \ldots, x_{p-1}), \ldots, h_{l-1}(x_0, \ldots, x_{p-1})$ and $g(y_0, \ldots, y_{l-1})$ are primitive recursive functions, then also

$$f(x_0, \ldots, x_{p-1}) = g(h_0(x_0, \ldots, x_{p-1}), \ldots, h_{l-1}(x_0, \ldots, x_{p-1}))$$

is primitive recursive.
3) If $g(x_0, \ldots, x_{p-1})$ and $h(z, y, x_0, \ldots, x_{p-1})$ are primitive recursive functions, then also f defined by

$$f(0, x_0, \ldots, x_{p-1}) = g(x_0, \ldots, x_{p-1}),$$
$$f(y+1, x_0, \ldots, x_{p-1}) = h(f(y, x_0, \ldots, x_{p-1}), y, x_0, \ldots, x_{p-1})$$

is primitive recursive.

Definition 2.21. A functional F is called primitive recursive (of level or 'type' ≤ 2) in the sense of Kleene if it can be defined by the following schemas ($\underline{x} = x_0, \ldots, x_{p-1}$ is a list of number variables and $\underline{f} = f_0, \ldots, f_{q-1}$ is a list of function variables for any $p, q \geq 1$):

(i) (Projections) $F(\underline{x},\underline{f}) = x_i$ (for $i < p$) and (Zero) $F(\underline{x},\underline{f}) = 0$,
(ii) (Function application) $F(\underline{x},\underline{f}) = f_i(x_{j_0},\dots,x_{j_{l-1}})$
(for $i < q$ and $j_0,\dots,j_{l-1} < p$ and f_i of arity l),
(iii) (Successor) $F(\underline{x},\underline{f}) = x_i + 1$ (for $i < p$),
(iv) (Substitution)
$F(\underline{x},\underline{f}) = G(H_0(\underline{x},\underline{f}),\dots,H_{l-1}(\underline{x},\underline{f}),\lambda y.K_0(y,\underline{x},\underline{f}),\dots,\lambda y.K_{j-1}(y,\underline{x},\underline{f}))$,
(v) (Primitive recursion)
$F(0,\underline{x},\underline{f}) = G(\underline{x},\underline{f})$, $F(y+1,\underline{x},\underline{f}) = H(F(y,\underline{x},\underline{f}),y,\underline{x},\underline{f})$.

Remark 2.22. The class of primitive recursive functionals of level ≤ 2 in the sense of Kleene which do not have any function arguments $\underline{f}$ coincides with the class of primitive recursive functions. Exercise!

We will now demonstrate the no-counterexample on two simple examples (the second of which will play an important role in applications to metric fixed point theory in chapter 18 below):

Example 1: Consider the following proposition which is an immediate consequence of the least number principle for natural numbers (which can formally be proved using Σ^0_1-induction):

$$(+)\ \forall f : \mathbb{N} \to \mathbb{N} \forall k \in \mathbb{N} \exists n \geq k \forall m \geq k (f(n) \leq f(m)).$$

$(+)$ is ineffective in the sense that there is no computable bound $\Phi(f,k)$ on n. In fact, the next two propositions give even stronger results:

Proposition 2.23. *There is no computable functional $\Phi : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ such that*

$$\forall f : \mathbb{N} \to \mathbb{N} \exists n \leq \Phi(f) \forall m \in \mathbb{N} (f(n) \leq f(m)).$$

Proof: Assume that on the contrary such a computable Φ would exist. Consider the constant-1 function $1 := \lambda k.1$. Since Φ is computable, $\Phi(f)$ only depends on finitely many values of f, i.e. $\Phi : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ is continuous w.r.t. the product topology on $\mathbb{N}^{\mathbb{N}}$ and the discrete topology on $\mathbb{N}$. Hence

$$(*)\ \exists l \in \mathbb{N} \forall g : \mathbb{N} \to \mathbb{N} (\forall i \leq l (g(i) = 1) \to \Phi(1) = \Phi(g)).$$

Now define

$$g(i) := \begin{cases} 1, \text{ if } i \leq \max(l, \Phi(1)) \\ 0, \text{ otherwise.} \end{cases}$$

Then $\Phi(g) = \Phi(1)$ by $(*)$, but also $\Phi(g) > \Phi(1)$ since $g(j) = \min\{g(i) : i \in \mathbb{N}\} = 0$ for some $j \leq \Phi(g)$, whereas $g(i) = 1$ for all $i \leq \Phi(1)$. □

Proposition 2.24. *There exists a primitive recursive function $f_0 : \mathbb{N} \to \mathbb{N}$ such that there is no computable function $\Phi : \mathbb{N} \to \mathbb{N}$ with*

$$\forall k \in \mathbb{N} \exists n \leq \Phi(k) \big(n \geq k \wedge \forall m \geq k (f_0(n) \leq f_0(m))\big).$$

Proof: Let $e \in \mathbb{N}$ be such that

$$\{k \in \mathbb{N} : \{e\}(k) \downarrow\} = \{k \in \mathbb{N} : \exists n \in \mathbb{N}\, T(e,k,n)\}$$

is undecidable, where the primitive recursive Kleene T-predicate satisfies

$$(1)\ \forall k, n_1, n_2 \in \mathbb{N}(T(e,k,n_1) \wedge T(e,k,n_2) \to n_1 = n_2).$$

Define $f_0(n) := g(j_1(n), j_2(n))$, where

$$g(k,n) := \begin{cases} j(k,0), \text{ if } T(e,k,n) \\ j(k,n+1), \text{ otherwise} \end{cases}$$

and $j : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is any primitive recursive bijection with primitive recursive projections j_1, j_2 (e.g. we may take as j the standard Cantor pairing function, see definition 3.30 below). It is clear that f_0 is primitive recursive. Now suppose that $\Phi : \mathbb{N} \to \mathbb{N}$ is computable and satisfies

$$(2)\ \forall k \in \mathbb{N} \exists n \leq \Phi(k)\big(n \geq k \wedge \forall m \geq k(f_0(n) \leq f_0(m))\big).$$

Define (primitive recursively in Φ) a function $\tilde{\Phi} : \mathbb{N} \to \mathbb{N}$ by

$$(3)\ \tilde{\Phi}(0) := 0,\ \tilde{\Phi}(l+1) := \max\{\tilde{\Phi}(l), \Phi(\tilde{\Phi}(l)) + 1\}.$$

By induction on l we show that

$$(4)\ \forall l \in \mathbb{N} \forall m \geq \tilde{\Phi}(l)\,(f_0(m) \geq l) :$$

The case $l = 0$ is trivial. $l \mapsto l+1$: By induction hypothesis we have

$$(5)\ \min\{f_0(m) : m \geq \tilde{\Phi}(l)\} \geq l.$$

(2) yields

$$(6)\ \exists n \leq \Phi(\tilde{\Phi}(l))\,\big(n \geq \tilde{\Phi}(l) \wedge f_0(n) = \min\{f_0(m) : m \geq \tilde{\Phi}(l)\}\big).$$

The injectivity of f_0 (which follows using (1)) implies that n is uniquely determined by $f_0(n) = \min\{f_0(m) : m \geq \tilde{\Phi}(l)\}$ and thus (using (3))

$$\forall m \geq \tilde{\Phi}(l+1) = \max\{\tilde{\Phi}(l), \Phi(\tilde{\Phi}(l)) + 1\}\,\big(f_0(m) > \min\{f_0(k) : k \geq \tilde{\Phi}(l)\}.$$

Hence (using (5))

$$\forall m \geq \tilde{\Phi}(l+1)\,\big(f_0(m) \geq l+1\big)$$

which finishes the proof of (4).
Now let $k_0 := \tilde{\Phi}(j(k,0)+1)$. Then by (4)

$$(7)\ \forall m \geq k_0\big(f_0(m) > j(k,0)\big).$$

Hence

$$\{e\}(k)\downarrow \leftrightarrow \exists n\, T(e,k,n) \leftrightarrow \exists m\big(j_1(m)=k \wedge f_0(m)=j(k,0)\big)$$
$$\leftrightarrow \exists m < k_0\big(j_1(m)=k \wedge f_0(m)=j(k,0)\big),$$

where the latter clearly is decidable which is a contradiction. □

In contrast to these negative results we have a primitive recursive (in the sense of Kleene) functional Φ satisfying the no-counterexample interpretation of $(+)$:

Proposition 2.25. *There exists a primitive recursive (in the sense of Kleene) functional Φ such that for all $f,g:\mathbb{N}\to\mathbb{N}$*

$$\forall k\in\mathbb{N}\big(\Phi(f,g,k)\geq k \wedge \big(g(\Phi(f,g,k))\geq k \to f(\Phi(f,g,k))\leq f(g(\Phi(f,g,k)))\big)\big).$$

Proof: We construct an upper bound $\Phi^*(f,g,k)$ for $\Phi(f,g,k)$, i.e.

$$\forall k\in\mathbb{N}\exists n\leq \Phi^*(f,g,k)\,\big(n\geq k\wedge(g(n)\geq k\to f(n)\leq f(g(n)))\big).$$

Φ can then be constructed from Φ^* by primitive recursive bounded search.
Let $f,g:\mathbb{N}\to\mathbb{N}, k\in\mathbb{N}$. We first show that

$$(*)\ \exists i\leq f(k)\,\big(g^{(i)}(k)\geq k\wedge(g^{(i+1)}(k)\geq k\to f(g^{(i)}(k))\leq f(g^{(i+1)}(k)))\big),$$

where $g^{(0)}(k):=k, g^{(i+1)}(k):=g(g^{(i)}(k))$.
Case 1: $\exists i<f(k)\,\big(g^{(i+1)}(k)<k\big)$. Let i_0 be the least such i. Then
$g^{(i_0+1)}(k)<k\wedge g^{(i_0)}(k)\geq k$. Hence the claim is satisfied with i_0.
Case 2: $\forall i<f(k)\,\big(g^{(i+1)}(k)\geq k\big)$ and hence $\forall i\leq f(k)\,\big(g^{(i)}(k)\geq k\big)$. Assume that

$$\forall i\leq f(k)\,\big(f(g^{(i)}(k))>f(g^{(i+1)}(k))\big).$$

Then

$$f(g^{(f(k)+1)}(k))<f(k)-f(k)$$

which is a contradiction. So again $(*)$ follows for some $i\leq f(k)$.
Now define

$$\Phi^*(f,g,k):=\max\{g^{(i)}(k): i\leq f(k)\}.$$

□

Example 2: Let $(a_n)_{n\in\mathbb{N}}$ be a nonincreasing sequence of rational numbers in $[0,1]$. Since rational numbers can be coded by natural numbers one can consider (a_n) as a number theoretic function. The order relation $\leq$ and the usual arithmetical operations between rational numbers are primitive recursive in their codes (identifying below '2^{-k}' with its encoding).

Consider the proposition stating that (a_n) is a Cauchy sequence, i.e.

$$(++)\ \forall k\in\mathbb{N}\exists n\in\mathbb{N}\forall m\in\mathbb{N}\ (|a_{n+m}-a_n|<_{\mathbb{Q}}2^{-k}).$$

By a well-known result of E. Specker [342] even for certain primitive recursive sequences (a_n) (so-called Specker sequences) there is in general no computable bound $f(k)$ on n. However, we have the following:

Proposition 2.26. *There exists a primitive recursive functional in the sense of Kleene satisfying the no-counterexample interpretation of* $(++)$. *In fact, there exists a primitive recursive* Φ *such that*

$$\forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists n \leq \Phi(g,k)\ (|a_{n+g(n)} - a_n| <_{\mathbb{Q}} 2^{-k}).$$

Proof: For $g : \mathbb{N} \to \mathbb{N}$ define $\tilde{g} : \mathbb{N} \to \mathbb{N}$ by $\tilde{g}(n) := n + g(n)$. We first show that

$$(*)\ \forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists i \leq 2^k \big(a_{\tilde{g}^{(i)}(0)} - a_{\tilde{g}^{(i+1)}(0)} <_{\mathbb{Q}} 2^{-k}\big).$$

Assume that on the contrary for some $k \in \mathbb{N}$ and $g \in \mathbb{N}^{\mathbb{N}}$

$$\forall i \leq 2^k \big(a_{\tilde{g}^{(i)}(0)} - a_{\tilde{g}^{(i+1)}(0)} \geq_{\mathbb{Q}} 2^{-k}\big).$$

Then (using that $\tilde{g}^{(0)}(0) = 0$)

$$a_0 - a_{\tilde{g}^{(2^k+1)}(0)} \geq (2^k + 1) \cdot 2^{-k} > 1$$

which is a contradiction and so finishes the proof of $(*)$.
Since (a_n) is nonincreasing, $(*)$ implies that

$$\forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists i \leq 2^k \big(|a_{\tilde{g}^{(i)}(0)} - a_{\tilde{g}^{(i)}(0)+g(\tilde{g}^{(i)}(0))}| <_{\mathbb{Q}} 2^{-k}\big).$$

We now take $\Phi(g,k) := \tilde{g}^{(2^k)}(0)$ $(= \max\{\tilde{g}^{(i)}(0) : i \leq 2^k\})$. □

Using the primitive recursive decidability of $<_{\mathbb{Q}}$ one can apply primitive recursive bounded search to get a primitive recursive realizer $\Psi((a_n),g,k)$ for '$\exists n$' from the bound $\Phi(g,k)$ in proposition 2.26. The bound $\Phi(g,k)$ is also valid for sequences (a_n) of real numbers in $[0,1]$. Moreover, using the monotonicity of (a_n) and the proof above we can state the result as follows (where $[n;n+g(n)] := \{i \in \mathbb{N} : n \leq i \leq n+g(n)\}$):

Proposition 2.27. *Let* (a_n) *be any nonincreasing sequence in* $[0,1]$ *then*

$$\forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists n \leq \Phi(g,k) \forall i,j \in [n;n+g(n)](|a_i - a_j| <_{\mathbb{R}} 2^{-k}),$$

where

$$\Phi(g,k) := \tilde{g}^{(2^k)}(0) \text{ with } \tilde{g}(n) := n + g(n).$$

Moreover, there exists an $i \leq 2^k$ *such that* n *can be taken as* $\tilde{g}^{(i)}(0)$.

Note that the bound $\Phi(g,k)$ in proposition 2.27 does not depend on (a_n) at all. Hence, using the fact that only sequence elements a_k for $k \leq n + g(n)$ are touched,

we obtain the following (explicit version of a) 'finite convergence principle' which recently was considered by T. Tao ([357, 358]):

Corollary 2.28. *For all $k \in \mathbb{N}, g \in \mathbb{N}^{\mathbb{N}}$ there exists an $M \in \mathbb{N}$ such that for all nonincreasing finite sequences $0 \le a_M \le \ldots \le a_0 \le 1$ of length $M+1$ in $[0,1]$ there exists an $n \in \mathbb{N}$ with*

$$n + g(n) \le M \wedge \forall i, j \in [n; n+g(n)](|a_i - a_j| <_{\mathbb{R}} 2^{-k}).$$

Moreover, we can compute M as $M := \tilde{g}^{(2^k+1)}(0)$, where $\tilde{g}(n) := n + g(n)$.

Remark 2.29. 1) For nonincreasing sequences in $[0,C]$ for some $C \in \mathbb{N}$ one can take $\Phi(g,k,C) := \tilde{g}^{(C \cdot 2^k)}(0)$ and M as $\tilde{g}^{(C \cdot 2^k+1)}(0)$.

2) The property

$$\forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists n \in \mathbb{N} \forall i, j \in [n; n+g(n)] \, (|a_i - a_j| <_{\mathbb{R}} 2^{-k})$$

of a sequence (a_n) of reals, which is nothing else but the Herbrand normal form of the following (equivalent) reformulation of the usual Cauchy property of (a_n) (treating '$\forall i, j(\ldots)$' as a Σ^0_1-formula to which it is equivalent since $<_{\mathbb{R}}$ is Σ^0_1 and the universal quantifiers are bounded)

$$\forall k \in \mathbb{N} \exists n \in \mathbb{N} \forall m \in \mathbb{N} \forall i, j \in [n; n+m] \, (|a_i - a_j| <_{\mathbb{R}} 2^{-k}),$$

is (for given k, g) called 'metastability' in Tao [357] and $[n; n+g(n)]$ a region where (a_n) is 'metastable' with error 2^{-k}.

There is, however, a problem in using the no-counterexample interpretation as a tool to extract such realizing functionals in a modular way i.e. by a recursion over the proof-tree which keeps the basic structure of the proof unchanged (which is of crucial importance for actually analyzing concrete and – in particular – not fully formalized proofs). In fact, Parsons' and Gödel's results where obtained by using a different more complicated interpretation, the so-called Gödel functional ('Dialectica') interpretation ([133]), which we will treat in chapters 8, 9,10. In contrast to the no-counterexample interpretation, which only refers to functionals of type level 2, functional interpretation uses – even for first order systems like **PA** – functionals of arbitrary finite types to achieve an interpretation which respects the modus ponens. We conclude this chapter by indicating why functionals of type 2 are not sufficient whereas higher types allow one to resolve the problem.

The modus ponens problem:

Consider an instance

$$\frac{A \quad A \to B}{B}$$

of the modus ponens rule where A, B are sentences in $\mathscr{L}(\mathbf{PA})$ of the form

$$A :\equiv \forall x \exists y \forall z A_0(x,y,z) \text{ and } B :\equiv \forall u \exists v B_0(u,v),$$

and A_0, B_0 are quantifier-free and suppose we have functionals satisfying the no-counterexample interpretation of A and $A \to B$. In order to make the latter precise we first have to choose a prenex normal form of $A \to B$, say

$$(A \to B)^{pr} :\equiv \forall u \exists x \forall y \exists z, v \big(A_0(x,y,z) \to B_0(u,v)\big).$$

The no-counterexample interpretation of A and $(A \to B)^{pr}$ asks for functionals realizing the Herbrand normal forms

$$A^H :\equiv \forall x, g \exists y A_0(x,y,g(y))$$

and

$$\big((A \to B)^{pr}\big)^H :\equiv \forall u, f \exists x, z, v \big(A_0(x,f(x),z) \to B_0(u,v)\big)$$

of A and $(A \to B)^{pr}$, i.e. for functionals $\varphi_0, \varphi_1, \varphi_2, \varphi_3$ such that

$$\forall x, g A_0(x, \varphi_0(x,g), g(\varphi_0(x,g)))$$

and

$$\forall u, f \big(A_0(\varphi_1(u,f), f(\varphi_1(u,f)), \varphi_2(u,f)) \to B_0(u, \varphi_3(u,f))\big).$$

In order to solve the modus problem one has to solve (in the parameter u) the following system of equations for solutions x, f, g :

$$\begin{cases} x = \varphi_1(u,f), \\ \varphi_0(x,g) = f(\varphi_1(u,f)), \\ g(\varphi_0(x,g)) = \varphi_2(u,f). \end{cases}$$

However, we will show that no primitive recursive functional – not even in the extended sense of Gödel allows one to solve this system of equations as a functional in $u, \varphi_0, \varphi_1, \varphi_2$. Indeed, the solvability of this system of equation will turn out to correspond to the consistency of the schema of arithmetical comprehension

$$\exists f \forall x \big(f(x) = 0 \leftrightarrow A(x)\big),$$

where $A(x)$ contains only number quantifiers but maybe function parameters (see chapter 11).
The solution requires so-called bar recursion (of type 0) which was introduced by C. Spector [343] and which goes beyond Gödel's primitive recursive functionals. We will discuss this further in chapter 11 below.

Moreover, one can construct concrete sentences A and B of the logical form as above such that A and any prenex normal form of $A \to B$ have primitive recursive functionals in the sense of Kleene satisfying their no-counterexample interpretations but where B has no primitive recursive realizing function (but only one in the extended sense of Gödel's primitive recursion in higher types defined in chapter 3). For A of the form $\forall x \exists y \forall z A_0(x,y,z)$ primitive recursion with equality between functions,

i.e. of type 1 (see chapter 3), suffices for B but for more complex formulas A one has to exhaust all finite types to realize B while A and $A \to B$ in general still have no-counterexample interpretations using only primitive recursion of type 0, i.e. in the sense of Kleene (these results are proved in [215] which provides a thorough discussion of the modus ponens problem for the no-counterexample interpretation).

The reason for the weakness of the no-counterexample interpretation is the weakness of the Herbrand normal form F^H of formulas F of complexity $\exists x \forall y \exists z F_0(x,y,z)$ or higher (such as $(A \to B)^{pr}$ above). Then the passage from F^H to F requires AC (though only from numbers to numbers) for $\forall$-formulas (and beyond), which in general are undecidable. I.e. one has to apply F^H to noncomputable index functions to derive F. For A of the form above, AC for the quantifier-free (and hence decidable) formula $\neg A_0$ is enough to prove $A^H \to A$ but already for $(A \to B)^{pr}$ this no longer is the case. In chapter 13 we will show that for **any** theorem A of full Peano arithmetic one can define a logically equivalent sentence $\tilde{A}$ in prenex normal form such that $\tilde{A}^H$ is provable using only quantifier-free induction (see proposition 13.1).

For the time being we confine ourselves with indicating how the above instance of the modus ponens can be treated if one uses an interpretation which doesn't stop at type level 2, namely Gödel's functional interpretation ([133]) which – for classical proofs (where it always is combined with the so-called negative translation) – will be developed in chapter 10:

The functional interpretation of A and $A \to B$:
Whereas we don't change the interpretation of A we use the following transformations of $A \to B$:

$$
\begin{aligned}
&(A \to B) \quad \rightsquigarrow \\
&\big(\forall x, g \exists y A_0(x,y,g(y)) \to \forall u \exists v B_0(u,v)\big) \quad \rightsquigarrow \\
&\big(\exists Y \forall x, g A_0(x, Y(x,g), g(Y(x,g))) \to \forall u \exists v B_0(u,v)\big) \quad \rightsquigarrow \\
&(+)\ \forall u, Y \exists x, g, v \big(A_0(x, Y(x,g), g(Y(x,g))) \to B_0(u,v)\big).
\end{aligned}
$$

Note that only AC applied to quantifier-free formulas (though to objects more complicated than numbers only) is needed to prove the equivalence between $A \to B$ and $(+)$.

We say that the functionals $\Phi_0, \Phi_1, \Phi_2, \Phi_3$ satisfy the functional interpretation of A and $A \to B$ if

$$\forall x, g A_0(x, \Phi_0(x,g), g(\Phi_0(x,g)))$$

and

$$\Phi_1(u,Y), \Phi_2(u,Y), \Phi_3(u,Y) \text{ realize } x, g, v \text{ in } (+).$$

A solution of the modus ponens problem is then given just by putting

$$Y := \Phi_0,\ x := \Phi_1(u, \Phi_0),\ g := \Phi_2(u, \Phi_0)$$

yielding the conclusion

$$\forall u B_0(u, \Phi_3(u, \Phi_0)).$$

So a realizing function for $\forall u \exists v B_0(u,v)$ is simply obtained by applying Φ_3 to Φ_0. Note that Φ_0 already is a functional $\mathbb{N} \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ (i.e. has type level 2 in the sense of chapter 3) and so $\Phi_3 : \mathbb{N} \times \mathbb{N}^{(\mathbb{N} \times \mathbb{N}^{\mathbb{N}})} \to \mathbb{N}$ has type level 3 which goes beyond the realm of the no-counterexample interpretation.

Let us compare further the no-counterexample interpretation and the functional interpretation (combined with negative translation): consider the so-called 'Infinite Pigeonhole Principle' (IPP) stating that for any partition of $\mathbb{N}$ into finitely many subsets at least one of these sets has infinitely many elements: Let $C_n := \{0, \dots, n\}$.

$$\text{(IPP)}: \forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \exists i \leq n \forall k \in \mathbb{N} \exists m \geq k \big(f(m) = i\big).$$

The Herbrand normal form of (IPP) is

$$\text{(IPP)}^H \equiv \forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \forall F : C_n \to \mathbb{N} \exists i \leq n \exists m \geq F(i) \big(f(m) = i\big).$$

The no-counterexample interpretation of (IPP) has the following trivial solution:

$$M(n,f,F) := \max\{F(i) : i \leq n\} \text{ and } I(n,f,F) := f(M(n,f,F))$$

are realizers for '$\exists m$' and '$\exists i$' in (IPP)^H. These realizers by no means reflect the true complexity of (IPP) and its potential contribution to the complexity of programs or bounds extractable from proofs based on (IPP). In fact, (IPP) corresponds to the so-called bounded collection principle for universal formulas whose strength is known to be in between induction for Σ^0_2-formulas (called Σ^0_2-IA) and induction for Σ^0_1-formulas (called Σ^0_1-IA and defined in the exercises below). For a detailed study of these principles see e.g. [211] and chapter 13. In particular, as (IPP) implies Σ^0_1-IA it may cause arbitrary primitive recursive growth of functions provably total by the use of (IPP) (this is not in conflict with the trivial solution of the n.c.i of (IPP) but just shows again the failure of n.c.i. to interpret the modus ponens rule without causing a complexity explosion).

The functional interpretation of (the negative translation of) (IPP) (i.e. the ND-interpretation in the sense of chapter 10 of (IPP)) is arrived at in the following way

$$\begin{aligned}
&\text{(IPP)} \;\rightsquigarrow \\
&\forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \exists i \leq n \exists g : \mathbb{N} \to \mathbb{N} \forall k \in \mathbb{N} \big(g(k) \geq k \wedge f(g(k)) = i\big) \rightsquigarrow \\
&\forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \forall K : C_n \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N} \exists i \leq n \exists g : \mathbb{N} \to \mathbb{N} \\
&\qquad\qquad \big(g(K(i,g)) \geq K(i,g) \wedge f(g(K(i,g))) = i\big) =: \text{(IPP)}^{ND}.
\end{aligned}$$

The functional interpretation of (IPP) requires functionals $I(n,f,K)$ and $G(n,f,K)$ realizing '$\exists i$' and '$\exists g$'. As follows from the soundness theorem for ND in chapter 10 (theorem 10.7) I and G precisely constitute the computational contribution resulting

from the use of (IPP) in a proof. Such functionals can be defined by a complicated (though very restricted form of) primitive recursion of level 1 (see chapter 10) which, however, can be written in a rather short form using a finite version of bar recursion as was shown by P. Oliva [293] (see chapter 11).

It is clear that to derive (IPP) from $(\mathrm{IPP})^{ND}$ one only has to consider computable (in f) functionals K which, therefore, are continuous in g (in the sense of the Baire space topology (see chapter 4). One then can replace g by some finite initial segment of g that can be encoded into a number m (see chapter 3).
Let $[m](i) := g(i)$ for $i < \mathrm{length}(m)$ and $[m](i) := 0$ otherwise. Then we can reformulate $(\mathrm{IPP})^{ND}$ as

$$\forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \forall K : C_n \times \mathbb{N}^{\mathbb{N}} \overset{cont.}{\to} \mathbb{N} \exists i \leq n \exists m \in \mathbb{N}$$
$$\big([m](K(i,[m])) \geq K(i,[m]) \wedge f([m](K(i,[m]))) = i\big).$$

One can now define a functional $\Omega(n,f,K)$ which searches for the least code $\langle i,m\rangle$ of a pair (i,m) satisfying

$$i \leq n \wedge \big([m](K(i,[m])) \geq K(i,[m]) \wedge f([m](K(i,[m]))) = i\big).$$

Clearly, Ω is computable in its arguments and hence for continuous K it is continuous in f. In the case at hand this is obvious (even for general K) as f is only evaluated at the argument $[m](K(i,[m]))$. Hence $\Omega(n,\cdot,K)$ is bounded on the whole compact subspace $(C_n)^{\mathbb{N}}$ of $\mathbb{N}^{\mathbb{N}}$. This allows one to conclude the following 'finite' version of (IPP)

$$\forall n \in \mathbb{N} \forall K : C_n \times \mathbb{N}^{\mathbb{N}} \overset{cont.}{\to} \mathbb{N} \exists M \in \mathbb{N} \forall f : C_M \to C_n \exists i \leq n \exists m \leq M$$
$$\big(Image([m]) \subseteq C_M \wedge [m](K(i,[m])) \geq K(i,[m]) \wedge f([m](K(i,[m]))) = i\big).$$

It is possible to represent continuous functionals K by number theoretic functions $\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that (see also definition 3.58 in chapter 3)

$$\forall i \leq n \forall g \in \mathbb{N}^{\mathbb{N}} \exists m \in \mathbb{N}\,(\alpha_K(i,\overline{g}m) \neq 0)$$

and

$$\forall i \leq n \forall g \in \mathbb{N}^{\mathbb{N}}\,(\alpha_K(i,\overline{g}(\min m\,[\alpha_K(i,\overline{g}m) \neq 0])) - 1 = K(i,g)).$$

Here $\overline{g}m$ encodes the initial segment of g of length m (see definition 3.30). As the last equation shows, K can effectively be recovered from α (this would no longer be the case if we simply had taken $\alpha'(i,m) := K(i,[m])$ as we then have to search for the least k such that $\alpha'(i,\overline{g}l)$ remains constant for all $l \geq k$ which is not effective). Without loss of generality one may assume that α satisfies

$$\forall i \leq n \forall m,k \in \mathbb{N}\,(m \subseteq k \wedge \alpha(m) > 0 \to \alpha(i,m) = \alpha(i,k)),$$

where $m \subseteq k$ expresses that the finite sequence encoded by m is an initial segment of the finite sequence encoded by k (for more information on this see Kohlenbach [223]).

The above 'finite' version of (IPP) is very similar to T. Tao's ([357]) formulation of his 'finite' version of this principle. As mentioned by Tao, the principle is not fully finitizable due to the hidden quantifiers in the continuity assumption (resp. the assumption that a certain finite set-function – corresponding to α' above – is eventually constant in Tao's formulation). This is also the reason why to compute M in this finite version one either needs unbounded search or has to enrich K with a modulus of uniform continuity functional $\omega_K(h)$ on $\{g : g \leq_1 h\}$ (see below for the latter).

Because of this it is not the finite version of (IPP) which is useful in concrete unwindings of proofs involving the principle (IPP) but the (primitive recursive in the sense of Gödel) functionals $I(n,f,K), G(n,f,K)$ realizing $(\mathrm{IPP})^{ND}$ which, combined with the majorization technique developed in chapter 6 below, yield a uniform (and monotone) 'bound' (in the sense of being a majorant of G) $G^*(n,K)$ that no longer depends on f (for I the construction of $I^*(n,K) := I^*(n) := n$ is trivial).

Remark 2.30. G^* being a majorant of G (essentially) means that for all K^* being a majorant of K in sense of

$$\forall n^*, n, g^*, g\,(n^* \geq n \wedge g^*\ maj\ g \to K^*(n^*, g^*) \geq K(n,g))$$

one has

$$\forall n^*, n \forall f : \mathbb{N} \to C_n\,(n^* \geq n \to G^*(n^*, K^*)\ maj\ G(n,f,K)),$$

where for functions g^*, g :

$$g^*\ maj\ g :\equiv \forall n^*, n\,(n^* \geq n \to g^*(n^*) \geq g(n)).$$

So, in particular, for all $n \in \mathbb{N}$ and $f : \mathbb{N} \to C_n$

$$\forall k\,(G^*(n,K^*)(k) \geq G(n,f,K)(k)).$$

Now let $\omega_K(i,h)$ be a modulus of uniform continuity for $K(i,g)$ on $\{g : g \leq h\}$ (where $\leq$ is defined pointwise) for $i \leq n$, i.e.

$$\forall i \leq n \forall g_1, g_2 \leq h\,(\forall k \leq \omega_K(i,h)(g_1(k) = g_2(k)) \to K(i,g_1) = K(i,g_2)\big).$$

Given ω_K one can easily compute a majorant K^* of K and applying subsequently $\omega_K(i,h)$ to the bound $h := G^*(n,K^*)$ one can construct (in n, K, ω_K) a bound on the 'finite' version of (IPP) above which no longer relies on unbounded search.

The variant of functional interpretation which directly extracts such uniform bounds ('majorants') G^* we call monotone functional interpretation (see chapter 9 and – combined with negative translation – chapter 10). By the soundness theorem of monotone functional interpretation (and the soundness of negative translation) such majorizing terms, as provided by monotone functional interpretation, of principles

or lemmas used in a proof are all that is needed in extracting uniform bounds from proofs.

2.4 Exercises, historical comments and suggested further reading

Exercises:

1) Verify the estimate $p_r < 2^{2^r}$ stated in the discussion of Euclid's proof of proposition 2.1.
2) Let $\pi(x)$ be the number of all primes $\leq x$ (for $x \geq 1$). From the estimates we obtained by analyzing proofs 1)-3) of proposition 2.1 derive the following lower bounds on $\pi(x)$:

   a. From Proof 1 (Euclid): $\pi(x) \geq \ln\ln x$ for $x \geq 2$.
   b. From Proof 2 (Euler): $\pi(x) \geq \ln x$ for $x \geq 1$.
   c. From Proof 3: $\pi(x) \geq \frac{\ln x}{2\ln 2}$ for $x \geq 1$.

3) Consider
   $\Psi(x) := |\{n \in \mathbb{N} : 1 \leq n \leq x \wedge n \text{ is not divisible by any square number} \neq 1\}|$.
   Show that $\Psi(x) \geq x - \sum_{\substack{p \text{ prime} \\ p \leq x}} [\frac{x}{p^2}]$ and use this to show that there are infinitely many primes. Use this proof to obtain an upper bound $g(j)$ for the next prime p_{j+1} as in the 3rd proof of this statement above. Can you improve the bound we obtained from the latter (see Hacks [148])?
4) (Ulrich Berger) Consider the open first order theory $\mathscr{T}$ in the language of first order logic with equality and a constant 0 and two unary function symbols S, f. The only non-logical axiom of $\mathscr{T}$ is $\forall x(S(x) \neq 0)$.

   (i) Prove that $\mathscr{T} \vdash \exists x\big(f(S(f(x))) \neq x\big)$.
   (ii) Construct from the proof finitely many closed terms $s_1, \ldots, s_m$ and $t_1, \ldots, t_n$ such that
   $$\text{PL} \vdash \bigwedge_{i=1}^{m} (S(s_i) \neq 0) \to \bigvee_{j=1}^{n} (f(S(f(t_j))) \neq t_j).$$

5) Prove remark 2.22.
6) ([306, 231]) Let $(a_n), (b_n), (c_n)$ be sequences in $\mathbb{R}_+$ such that $\sum b_n$ and $\sum c_n$ are bounded and
   $$\forall n \in \mathbb{N}(a_{n+1} \leq (1 + b_n)a_n + c_n).$$
   Show that (a_n) is convergent and hence a Cauchy sequence. Construct a primitive recursive functional $\Phi(A, B, C, g, k)$ such that
   $$\forall k \in \mathbb{N} \forall g \in \mathbb{N}^{\mathbb{N}} \exists n \leq \Phi(A, B, C, g, k) \forall i, j \in [n; n + g(n)]\ (|a_i - a_j| < 2^{-k})$$
   for all $A, B, C \in \mathbb{N}$ be such that

$$a_0 \le A,\ \sum b_n \le B,\ \sum c_n \le C.$$

7) Construct primitive recursive functionals $\underline{\Phi}$ which satisfy the n.c.i. of (some prenex normal form of) the second order axiom of Σ^0_1-induction:

$$\Sigma^0_1\text{-IA}: \begin{cases} \forall f\big(\exists y(f(0,y)=0) \wedge \forall x(\exists y(f(x,y)=0) \to \exists y(f(x+1,y)=0)) \\ \qquad \to \forall x \exists y(f(x,y)=0)\big) \end{cases}$$

uniformly as a functional in f and the index functions.

8) Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of non-negative rational numbers. Use Σ^0_1-IA to prove that

$$(+)\ \forall k \exists n \forall m (a_n \le_{\mathbb{Q}} a_m + 2^{-k})$$

and construct a primitive recursive functional satisfying the no-counterexample interpretation of $(+)$ (see also exercise 3 in chapter 4 below).

Historical comments and suggested further reading:

1) More information on the general program of unwinding proofs (proof mining) can be found in [249, 250, 252, 251, 99, 268, 84, 16, 122, 206, 210, 219, 226, 236, 229, 270].
2) For detailed accounts of Herbrand's theorem see [62, 122, 202, 332, 249, 267, 114].
3) More material on the no-counterexample interpretation can be found in [122, 215, 241, 242, 350, 351, 353, 326] as well as chapter 10 below.

In particular, Kohlenbach [215] provides a thorough discussion of the modus ponens problem for the no-counterexample interpretation.

A partially modular approach to Herbrand's theorem via Gödel's functional interpretation (see chapter 8) can be found in Gerhardy-Kohlenbach [118].

A detailed complexity analysis of Herbrand's theorem and the closely related cut elimination theorem is given in Gerhardy's articles [114] and [115].

For early applications of the no-counterexample interpretation as well as the ε-substitution method (originally due to D. Hilbert and W. Ackermann), which is closely related to Herbrand's theorem and on which Kreisel's original treatment of his no-counterexample interpretation is based, to proofs in number theory (e.g. Littlewood's theorem on the sign changes of $\pi(n) - li(n)$) and algebra see Kreisel's original papers on the subject [241, 242] and also [243]. As briefly discussed above, Luckhardt [267] presents (inspired by Kreisel [249]) an important application of Herbrand terms extracted from two proofs of Roth's theorem in diophantine approximation resulting in the first polynomial bounds on the number of solutions

(see also Luckhardt [268]). Applications of the ε-substitution method to the solution of Hilbert's 17th problem and subsequent work in this direction are discussed in Delzell [84] (see also Delzell's papers [79, 80, 81, 82, 83] although some do not use proof theory directly). Again this work is inspired by ideas of G. Kreisel going back to the 50's (see e.g. Kreisel [245]). An analysis of two variants of the proof of Furstenberg and Weiss of van der Waerden's theorem by means of cut-elimination and the no-counterexample interpretation, respectively, is given in Girard [122] (see pp. 237–251 and 483–496). Bellin [16] presents an application of the no-counterexample interpretation to Ramsey's theorem.

Applications of cut-elimination to coherence theorems in category theory are given in Mints [276, 278, 279] and Babaev-Solovjov [9].

For other approaches to proof mining not (or only briefly) treated in this book see e.g. the work of Coquand et al. [72, 73] and Berger-Schwichtenberg [21] (see, however, chapter 14). Interesting connections between proof theory and combinatorics can be found in Ketonen-Solovay [181] and – recently – Weiermann [376].

http://www.springer.com/978-3-540-77532-4

Applied Proof Theory: Proof Interpretations and their Use in Mathematics

Kohlenbach, U.

2008, XX, 536 p., Hardcover
ISBN: 978-3-540-77532-4