Herbrand's theorem and extractive proof theory

U. Kohlenbach

Department of Mathematics
Technische Universität Darmstadt
Schlossgartenstrasse 7, 64289 Darmstadt, Germany

September 1, 2008

1 Extractive Proof Theory: New results by logical analysis of proofs

Proof theory has its historic origin in foundational issues centered around (relative) consistency proofs (Hilbert's program). Since the 1950's Georg Kreisel pushed for a shift of emphasis in proof theory towards the use of proof theoretic transformations (as developed in the course of Hilbert's program) to analyze given proofs P e.g. of ineffectively proved $\forall\exists$-statements C with the aim to extract new information on C that could not be read off from P directly. Herbrand's fundamental theorem plays an important role in this development. The general situation is as follows:

Input: Ineffective proof P of C

Goal: Additional information on C:

- effective bounds (e.g. on the number of solutions of an ineffectively proven finiteness theorem, see theorem 1.9) or effective rates of convergence in nonlinear analysis (see sections 4 and 5),
- algorithms for computation of actual solutions of ineffectively established existential statements,
- continuous dependency or full independence from certain parameters (e.g. rates of convergence or stability for iterative processes in fixed point theory and ergodic theory that are independent from parameters such as the starting point or the function being iterated, see remark 5.3 below)
- generalizations of proofs: weakening of premises (e.g. replacing boundedness assumptions by bounds on the rate of growth, see corollary 4.4 below).

In this article, when we use terms like 'computable' or 'decidable' for functions $f : \mathbb{N} \to \mathbb{N}$ or subsets $A \subseteq \mathbb{N}$ we always refer to the standard notion of computability as developed by Herbrand, Gödel, Church, Turing, Kleene and others. Herbrand's important role in this development is nicely explained in Coquand's contribution to this volume ([5]).

Now let $C \equiv \forall x \in \mathbb{N}\exists y \in \mathbb{N}\, F(x, y)$.

Naive Attempt: try to extract an explicit computable function f realizing (or bounding) '$\exists y \in \mathbb{N}$': $\forall x \in \mathbb{N}\, F(x, f(x))$.

Unless some restrictions on F are imposed this **naive attempt in general fails** as the following counterexample shows:

Proposition 1.1. *There exists a sentence $A \equiv \forall x\exists y\forall z\, A_{qf}(x, y, z)$ in the language of arithmetic (A_{qf} quantifier-free and hence decidable) such that*

- *A is logically valid,*
- *there is no computable bound f s.t. $\forall x \exists y \leq f(x) \forall z\, A_{qf}(x,y,z)$.*

Proof: Consider any undecidable but semi-decidable predicate $Q(x) \equiv \exists y \in \mathbb{N}\, P(x,y)$ (P may even be taken as a primitive recursive predicate as in the Halting Problem for Turing machines or – if x, y are replaced by tuples of variables and one uses Matiyasevich's diophantine representation of semi-decidable sets – even of the form $p(\underline{x}, \underline{y}) = 0$ with $p \in \mathbb{Z}[\underline{x}, \underline{y}]$). Now consider the logically valid sentence

$$A :\equiv \forall x \in \mathbb{N} \exists y \in \mathbb{N} \forall z \in \mathbb{N}\, \big(P(x,y) \vee \neg P(x,z)\big).$$

Let $f : \mathbb{N} \to \mathbb{N}$ be a bound on '$\exists y \in \mathbb{N}$', i.e.

$$\forall x \in \mathbb{N} \exists y \leq f(x) \forall z \in \mathbb{N}\, (P(x,y) \vee \neg P(x,z)).$$

Then f is not computable since, otherwise, we could use f to decide $Q(x)$. □

However, one can obtain computable bounds and even finitely many witnessing candidates (and so by case decision functions also realizing function(al)s) for a weakened version A^H of A (which, however, is equivalent to A w.r.t. provability in first order theories that do not mention the index function(s) referred to below in their axioms).

Every formula A can be written in a logical equivalent form which has all quantifiers lined up in front of a quantifier-free formula (a so-called prenex formula). For the issues discussed in this paper only the alternations of quantifiers (between $\forall$ and $\exists$) but not the length of blocks of equal quantifiers matter. Hence we will notationally identify single quantifiers and blocks of the same quantifier. Moreover, all relevant phenomena already show up for formulas of rather limited logical complexity. In the following, we will, therefore, restrict ourselves to the formulas mentioned in the next definition:

Definition 1.2. *Let $A \equiv \exists x_1 \forall y_1 \exists x_2 \forall y_2 A_{qf}(x_1, y_1, x_2, y_2)$ with A_{qf} being quantifier-free. Then the Herbrand normal form of A is defined as*

$$A^H :\equiv \exists x_1, x_2 A_{qf}(x_1, f(x_1), x_2, g(x_1, x_2)),$$

where f, g are new function symbols, called index functions.

Note that for purely existential sentences (and similarly for pure $\forall\exists$-sentences once the $\forall$-quantifier is treated either as a parameter or replaced by a fresh constant understood as a 0-place index function) A and A^H coincide.

In the following, let PL_{--} denote first order logic (without equality).

Remark 1.3. *A^H is nothing else but the negation of the so-called Skolem normal form of the negation*

$$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \neg A_{qf}$$

of A as discussed in section 4.3 of Coquand's article [5] in this volume.

We now consider again the sentence (either as a sentence of first order logic with P as some binary predicate symbol or read in the language of arithmetic with a concrete primitive recursive P s.t. $\exists y \in \mathbb{N}\, P(x,y)$ is undecidable)

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

Whereas (as shown above) for A we not even have a computable bound on '$\exists y$', for the Herbrand normal form A^H of A

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

one can construct a list (of fixed finite length – in the case at hand of length 2 –) of candidates (uniformly in x, g) for '$\exists y$', namely $(x, g(x))$ or $(c, g(c))$ for any constant c s.t.

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

is a tautology.

A tautology still is a tautology when one replaces all occurrences of a term s by a variable y. So if we substitute all g-terms by fresh variables replacing bigger terms first, i.e. $g(g(c))$ by z and then $g(c)$ by y, then the result

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

still is a tautology.
From A^D we can derive A by a so-called direct proof:

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

Theorem 1.4 (J. Herbrand's Theorem ('Théorème fondamental' [14], 1930))**.**
Let $A \equiv \exists x_1 \forall y_1 \exists x_2 \forall y_2 A_{qf}(x_1, y_1, x_2, y_2)$. Then:
$\mathrm{PL}_{-=} \vdash A$ *iff there are terms $s_1, \ldots, s_k, t_1, \ldots, t_n$ (built up out of the constants and free variables of A – possible with the help of some default constant c in case A does not contain any constant or free variable – and the index functions used for the formation of A^H) such that*

$$A^{H,D} :\equiv \bigvee_{i=1}^{k} \bigvee_{j=1}^{n} A_{qf}\big(s_i, f(s_i), t_j, g(s_i, t_j)\big)$$

is a tautology. $A^{H,D}$ is called a Herbrand Disjunction of A and the terms s_i, t_j are called Herbrand terms.
Note that the length of this disjunction is fixed: $k \cdot n$.
The terms s_i, t_j can be extracted from a given $\mathrm{PL}_{-=}$*-proof of A.*

Replacing in $A^{H,D}$ all terms '$f(s_i)$','$g(s_i, t_j)$' by new variables as indicated above results in another tautological disjunction A^D s.t. A can be inferred from A^D by a direct proof.

Corollary 1.5. *Every* $\mathrm{PL}_{-=}$*-proof of a sentence A can be transformed into a direct proof which does not contain any detours via formulas ('lemmas') of greater quantifier complexity than A.*

Discussion:

1. Herbrand's original proof was syntactic and provides an algorithm for the extraction of the Herbrand terms from a given $\mathrm{PL}_{-=}$-proof of A. However, two lemmas in his proof need a correction as was discovered first by K. Gödel in the 40's (unpublished, see [13]) and in the 60's by B. Dreben et al. [6]. After Herbrand's work, alternative syntactic proofs were given by D. Hilbert and P. Bernays (using Hilbert's ε-substitution method) and by G. Gentzen (using his cut elimination procedure for a sequent calculus formulation of $\mathrm{PL}_{-=}$). Most textbook treatments of Herbrand's theorem nowadays are model theoretic and do not yield any term extraction algorithm (with Shoenfield [32] as a notable exception).

2. The forward direction in Herbrand's theorem immediately extends to logic with equality PL and even open theories $\mathcal{T}$ (i.e. theories with purely universal axioms only), where then the Herbrand disjunction is a tautological consequence of finitely many instances of equality axioms ('quasi-tautology') and – in the case of $\mathcal{T}$ – finitely many instances of the universal axioms. To get from such an implicative tautology a proof of A in $\mathcal{T}$ (i.e. the converse direction) it is crucial that the Herbrand index functions f, g are new not only w.r.t. A but also w.r.t. $\mathcal{T}$, i.e. do not occur in the axioms of $\mathcal{T}$. Already for logic with equality the syntactic procedure to eliminate the f, g-terms in the Herbrand disjunction becomes much more complicated if instances of f, g-equality axioms are used (see e.g. Shoenfield [32]).

3. Although Herbrand's theorem constitutes a kind of reduction of predicate logic to propositional logic this does not contradict the undecidability of the former as there is no effective a-priori bound (depending only on A) on the number of Herbrand terms needed but only bounds depending on the data of a given proof P of A. In fact, as was first shown by Statman [35], the required number can be extremely large and, in general, is superexponential in the basic P-data.

4. Note that the Herbrand terms do not depend on the predicate symbols in A.

We now give an example that illustrates that already extremely elementary proofs (in open theories) can give rise to Herbrand disjunctions that are far from obvious.

Example (Ulrich Berger): Consider the open first order theory $\mathcal{T}$ 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 $\mathcal{T}$ is $\forall x(S(x) \neq 0)$ (e.g. think of x as ranging over $\mathbb{N}$ including 0 and S as the successor function).

Proposition 1.6. *$\mathcal{T}$ proves that $\exists x\big(f(S(f(x))) \neq x\big)$.*

Proof sketch: Suppose that

$$\forall x\big(f(S(f(x))) = x\big),$$

then f is injective, but also (since $S(x) \neq 0$) surjective on $\{x : x \neq 0\}$ and hence non-injective. Contradiction! □

Analyzing the above proof yields the following Herbrand terms since the sentence in question is purely existential it is already in Herbrand normal form (though not exhibiting the instances of the $=$-equality axioms needed): PL proves that

$$(S(s) \neq 0) \to \bigvee_{j=1}^{3} (f(S(f(t_j))) \neq t_j),$$

where

$$t_1 := 0, t_2 := f(0), t_3 := S(f(f(0))), s := f(f(0)).$$

Remark 1.7. *For sentences $A \equiv \forall x \exists y \forall z\, A_{qf}(x, y, z)$, A^D can always be written in the form*

$$A_{qf}(x, t_1, b_1) \vee A_{qf}(x, t_2, b_2) \vee \ldots \vee A_{qf}(x, t_k, b_k),$$

where the b_i are new variables and the t_i do not contain any b_j with $i \leq j$.

Theorem 1.8 (Roth [31]). *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*

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

Guided by Herbrand's theorem in the form of remark 1.7 and using ideas from Kreisel [26], the following polynomial (in ε) bound on the number of exceptionally good rational approximation was obtained by H. Luckhardt based on a Herbrand analysis of an ineffective proof of Roth's theorem due to Esnault and Viehweg [7]. Previously, only exponential bounds had been known (this shows that logical methods not only can be used to obtain effective bounds 'in principle' but even to yield clear-cut numerically improvements of known bounds).

Theorem 1.9 (Luckhardt [29]). *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 $N_\alpha < \max(21 \log 2h(\alpha), 2\log(1 + |\alpha|)), d = deg(\alpha)$ and $h(\alpha)$ is the absolute homogeneous height of α as defined in [3].

A similar bound was independently also obtained by Bombieri and van der Poorten [4].

Towards generalizations of Herbrand's theorem: allow **functionals** $\Phi(x, f)$ instead of just Herbrand terms. Let's consider again the example (with decidable P)

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

A^H can be realized by a computable functional (of type level 2) which is defined by cases:

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

From this definition it easily follows that

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

If A is not provable in PL or in some open theory but only with a logically complex instance of induction, then more complicated functionals are needed (Kreisel [25]):

Let (a_n) be a nonincreasing sequence in $[0,1]$. Then, clearly, (a_n) is convergent and so a Cauchy sequence which we write as:

$$(1)\ \forall k \in \mathbb{N} \exists n \in \mathbb{N} \forall m \in \mathbb{N} \forall i,j \in [n; n+m]\ (|a_i - a_j| \leq 2^{-k}),$$

where $[n; n+m] := \{n, n+1, \ldots, n+m\}$.
Then the (partial) Herbrand normal form of this statement is

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

By E. Specker [33] ('Specker sequences'), there exist computable such sequences (a_n) even in $\mathbb{Q} \cap [0,1]$ without a computable bound on '$\exists n$' in (1). By contrast, there is a simple (primitive recursive) bound $\Phi^*(g,k)$ on (2) (also referred to as 'metastability' by Tao [36]):

Proposition 1.10. *Let (a_n) be any nonincreasing sequence in $[0,1]$. Then*

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

where

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

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

Remark 1.11. *The previous result can be viewed as a Herbrand disjunction of* **variable (in k) length** *(rather than of fixed length as in Herbrand's theorem):*

$$\bigvee_{i=0}^{2^k-1} \big(|a_{\tilde{g}^{(i)}(0)} - a_{\tilde{g}(\tilde{g}^{(i)}(0))}| \leq 2^{-k}\big).$$

Corollary 1.12 (T. Tao's finite convergence principle, Tao [36])**.**

$$\forall k \in \mathbb{N}, g : \mathbb{N} \to \mathbb{N}\, \exists M \in \mathbb{N}\, \forall\, 0 \leq a_M \leq \ldots \leq a_0 \leq 1\, \exists n \in \mathbb{N}$$
$$\big(n + g(n) \leq M \wedge \forall i, j \in [n; n + g(n)]\, (|a_i - a_j| \ \leq 2^{-k})\big).$$

In fact, one can take $M := \tilde{g}^{(2^k)}(0)$.

2 Kreisel's No-Counterexample Interpretation

Definition 2.1 (G. Kreisel [25])**.** *Let* $A \equiv \exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A_{qf}(x_1, y_1, \ldots, x_n, y_n)$*. If a tuple of functionals* $\Phi_1, \ldots, \Phi_n$ *realizes the Herbrand normal form* A^H *of* A*, i.e. if*

$$A_{qf}\big(\Phi_1(\underline{f}), f_1(\Phi_1(\underline{f})), \ldots, \Phi_n(\underline{f}), f_n(\Phi_1(\underline{f}), \ldots, \Phi_n(\underline{f}))\big)$$

holds for all functions $\underline{f} = f_1, \ldots, f_n$*, then we say that* $\underline{\Phi}(= \Phi_1, \ldots, \Phi_n)$ *satisfies the* **no-counterexample interpretation** *(n.c.i.) of* A*.*

Motivation for the name 'no-counterexample interpretation': Let A be as above. Then $\neg A$ is equivalent to

$$\forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \neg A_{qf}(x_1, y_1, \ldots, x_n, y_n).$$

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

$$(+)\ \forall x_1, \ldots, x_n\, \neg A_{qf}(x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n))$$

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

More information of the no-counterexample interpretation can be found in [10] and – in particular – [22].

Problems of the no-counterexample interpretation: For principles $F \in \exists\forall\exists$ the n.c.i. no longer is 'correct' in the sense that the functionals sufficient to realize the n.c.i. of F may not reflect the true complexity of extractable bounds from proofs based on F (technically, this problem is due to the bad behavior of the no-counterexample interpretation w.r.t. to the modus ponens rule). We now give an example for the issue involved:

The **Infinitary Pigeonhole Principle (IPP)** is defined as follows:

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

where $C_n := \{0, 1, \ldots, n\}$. It is easy to show that (over weak fragments of arithmetic) IPP implies the induction principle for induction formulas with one quantifier and – consequently – can cause arbitrary **primitive recursive complexity** of bounds extractable from proofs based on IPP. However, the n.c.i. of IPP

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

has a 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 $(\text{IPP})^H$.

Thus M, I do not reflect the true contribution of IPP to the complexity of bounds extractable from IPP-based proofs, while functionals G, I satisfying the Gödel functional interpretation of IPP, discussed in the next section, do.

3 Gödel's Functional Interpretation

In [12], K. Gödel developed a much refined so-called functional interpretation (originally for systems based on intuitionistic logic but combined with his negative embedding of classical systems into intuitionistic ones also for systems based on ordinary classical logic). This interpretation (we in the following tacitly always refer to the combination of negative and functional interpretation) has the property that the equivalence between A and its interpretation A^G can be proved using the axiom schema of choice only for **quantifier-free formulas** though in higher type function spaces

$$\text{QF-AC}: \ \forall x^\rho \exists y^\tau \, A_{qf}(x,y) \to \exists Y^{\rho\to\tau} \forall x^\rho \, A_{qf}(x, Y(x)).$$

Here the type $\mathbb{N}$ in $x^{\mathbb{N}}$ is that of a natural number whereas for types ρ, τ an object $f^{\rho\to\tau}$ is a function from objects of type ρ to objects of type τ. We will not give any details on the general definition of G but just reveal the G-interpretation of IPP:

$$\begin{aligned}
&(\text{IPP}) \quad \overset{\text{QF}-\text{AC}}{\Leftrightarrow} \\
&\forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \exists i \leq n \exists g : \mathbb{N} \to \mathbb{N} \forall k \in \mathbb{N} \big(g(k) \geq k \wedge f(g(k)) = i\big) \\
&\overset{\text{QF}-\text{AC}}{\Leftrightarrow} \\
&(\text{IPP})^G \equiv \left\{ \begin{array}{c} \forall n \in \mathbb{N} \forall f : \mathbb{N} \to C_n \forall K : C_n \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N} \exists i \leq n \exists g : \mathbb{N} \to \mathbb{N} \\ \big(g(K(i,g)) \geq K(i,g) \wedge f(g(K(i,g))) = i\big). \end{array} \right.
\end{aligned}$$

The construction of explicit functionals $I(n, f, K), G(n, f, K)$ producing witnesses for '$\exists i \leq n$' and '$\exists g : \mathbb{N} \to \mathbb{N}$' is remarkably involved (see Oliva [30]). To appreciate the complexity we invite the reader to come up with a solution just for $n = 2$ (i.e. the case with 3 'colors').
For a thorough discussion of the functional interpretation of IPP and its relation to the 'finitary infinite pigeonhole principle' from Tao [36] see Kohlenbach [22].

General facts about Gödel's functional interpretation

- Functional interpretation was first developed for Peano Arithmetic PA as well as suitable extensions PA^ω+QF-AC to higher type functionals and allows one to extract **primitive recursive programs of higher type** (first considered by Hilbert in 1926 [15]) from proofs of $\forall\exists$-theorems in PA^ω+QF-AC (Gödel, Kreisel, Yasugi). The modus ponens rule this time is treated without any complexity increase.

- Applied to plain logic PL, functional interpretation can be used for an extraction algorithm of Herbrand terms of optimal complexity (Gerhardy-Kohlenbach [8]). In this sense, functional interpretation can be viewed as a generalization of Herbrand's theorem.

- Seminal work of Spector [34] further extended Gödel's functional interpretation to proofs in 'full classical analysis' $\mathcal{A}^\omega$, i.e. to proofs in PA^ω augmented by the full axiom schema of dependent choice DC. Then the extractable programs will no longer be primitive recursive in general but so-called bar recursive functionals (i.e. functionals defined by recursion over well-founded trees).

- The primitive recursive as well as the bar recursive functionals used in the context of functional interpretation not only are computable but enjoy a strong mathematical property called

'majorizability' due to W.A. Howard [16] (which fails for general computable functionals). Making use of this fact one can apply a variant of functional interpretation ('monotone functional interpretation', Kohlenbach [18]) to extract highly **uniform bounds** from given proofs of pointwise existence results.

- Recently, (monotone) functional interpretation (based on a novel majorization relation) has been applied to extensions $\mathcal{A}^\omega[X,\ldots]$ of $\mathcal{A}^\omega$ by **abstract structures** X such as arbitrary metric, hyperbolic, CAT(0), normed, uniformly convex or Hilbert spaces and provides bounds which are uniform even in metrically bounded parameters without any compactness assumption (Kohlenbach [19, 22], Gerhardy-Kohlenbach [9]). In fact, all the applications mentioned in the next two sections are based on this.

4 An application in Metric Fixed Point Theory

In the following

- (X,d,W) is a **hyperbolic space** in the sense of [19] (e.g. a convex subset of a normed space),
- $f: X \to X$ is a **nonexpansive mapping**: $d(f(x),f(y)) \leq d(x,y)$ for all $x,y \in X$,
- (λ_n) is a sequence in $[0,c]$ for some $0 < c < 1$ that is **divergent in sum**,.
- $x_{n+1} = (1-\lambda_n)x_n \oplus \lambda_n f(x_n)$ (Krasnoselski-Mann iteration).

Theorem 4.1 (Ishikawa [17], Goebel-Kirk [11])**.**

$$\text{If } (x_n) \text{ is bounded, then } d(x_n, f(x_n)) \to 0.$$

Logical analysis of the proof of Ishikawa's theorem: Since the sequence $(d(x_n,f(x_n)))_n$ is nonincreasing its convergence towards 0 can be expressed as a $\forall\exists$-statement so that we do not need any Herbrand normal form here.
Let $K \in \mathbb{N}$ and $\alpha: \mathbb{N} \to \mathbb{N}$ be such that

$$(\lambda_n)_{n\in\mathbb{N}} \in [0, 1-\frac{1}{K}]^{\mathbb{N}} \text{ and } \forall n \in \mathbb{N}(n \leq \sum_{i=0}^{\alpha(n)} \lambda_i).$$

A logical metatheorem from Gerhardy-Kohlenbach [9] that is based on a new extension of Gödel's functional interpretation applied to the proof of Ishikawa's theorem yields (primitive recursively) computable Ψ, Φ s.t. for all $l \in \mathbb{N}$ and nonexpansive f

$$\begin{array}{l} \forall i,j \leq \Psi(K,\alpha,b,\tilde{b},l)\ \big(d(x,f(x)) \leq \tilde{b} \wedge d(x_i,x_j) \leq b\big)\ \to \\ \forall m \geq \Phi(K,\alpha,b,\tilde{b},l)\ \big(d(x_m,f(x_m)) < 2^{-l}\big) \end{array}$$

holds in any (nonempty) hyperbolic space (X,d,W). Note that the bounds depend on $x, f, (X,d,W)$ only via $b, \tilde{b}$. To obtain the existence of such highly uniform computable bounds one only has to verify that the proof of Ishikawa's theorem (as given in [11]) can be formalized in a suitable formal system (extending $\mathcal{A}^\omega$ by (X,d,W) as atom as discussed above). In fact, proofs of purely universal lemmas do not need to be considered at all as those can be treated just as additional universal assumptions. A somewhat closer look at the resources used in the proof (relative to those lemmas) already yields a-priori the existence of primitive recursive bounds. Moreover, the **proof** of the logical metatheorem from Gerhardy-Kohlenbach [9] provides an actual algorithm for the extraction of explicit bounds from the given proof. Applied to that proof in [11] this yields the following

Theorem 4.2 (Kohlenbach [22]). *Logical analysis of a proof from [11] yields an explicit rate of convergence Φ of $(d(x_n, f(x_n))$ (depending only on $K, \alpha, b, \tilde{b}$ and $\varepsilon = 2^{-l}$) as well as quantitative information on 'the amount of boundedness of (x_n)' needed.*
More precisely, let $(X, d, W), (\lambda_n), K$ be as above and $f : X \to X$ nonexpansive. Then the following holds for all $\varepsilon, b, \tilde{b} > 0$:

$$\text{If } d(x, f(x)) \leq \tilde{b} \text{ and } \forall i \leq \Phi \forall j \leq \alpha(\Phi, M)\ (d(x_i, x_{i+j}) \leq b), \text{ then } \forall n \geq \Phi\ \big(d(x_n, f(x_n)) \leq \varepsilon\big),$$

where

$$\Phi := \Phi(K, \alpha, b, \tilde{b}, \varepsilon) := \widehat{\alpha}\left(\left\lceil \frac{\tilde{b} \cdot \exp\left(K \cdot \left(\frac{3\tilde{b}+b}{\varepsilon}+1\right)\right)}{\varepsilon} \right\rceil \dot{-} 1, M\right),$$
$$M := \left\lceil \frac{3\tilde{b}+b}{\varepsilon} \right\rceil,$$
$$\widehat{\alpha}(0, n) := \tilde{\alpha}(0, n),\ \widehat{\alpha}(i+1, n) := \tilde{\alpha}(\widehat{\alpha}(i, n), n) \text{ with}$$
$$\tilde{\alpha}(i, n) := i + \alpha(i, n)\ \ (i, n \in \mathbb{N})$$

with α s.t.[1]

$$\forall i, n \in \mathbb{N}\big((\alpha(i, n) \leq \alpha(i+1, n)) \wedge (n \leq \sum_{s=i}^{i+\alpha(i,n)-1} \lambda_s)\big).$$

For related results see Kohlenbach-Leuştean [23].

Remark 4.3. *If (λ_n) is in $[\frac{1}{K}, 1 - \frac{1}{K}]$, then we may take $\alpha(i, n) := K \cdot n$.*

The above bound can be used in this case to weaken the assumption of (x_n) being bounded in Ishikawa's theorem:

Corollary 4.4 (Kohlenbach [22]). *Let (λ_n) in $[a, b] \subset (0, 1)$.*

$$\text{If } \lim_{n\to\infty} \frac{c(n)}{n} \to 0, \text{ where } c(n) := \max\{d(x, x_j) : j \leq n\}, \text{ then } \lim_{n\to\infty} d(x_n, f(x_n)) = 0.$$

The result is optimal: $c(n) \leq C \cdot n$ for some $C > 0$ is not sufficient!
For a survey of numerous other applications of proof theory to metric fixed point theory see [20].

5 An application in Ergodic Theory

Let X be a Hilbert space, $f : X \to X$ linear and nonexpansive. Define

$$A_n(x) := \frac{1}{n+1} S_n(x), \text{ where } S_n(x) := \sum_{i=0}^{n} f^i(x) \qquad (n \geq 0).$$

Theorem 5.1 (von Neumann Mean Ergodic Theorem).
For every $x \in X$, the sequence $(A_n(x))_n$ converges.

As shown in Avigad et al. [1], even in simple cases there already is no computable rate of convergence so that one has to consider the 'metastable' Herbrand normal form of the Cauchy property as in the finite convergence principle (see (2) above):

$$\forall \varepsilon > 0\, \forall g : \mathbb{N} \to \mathbb{N}\, \exists n \forall i, j \in [n; n + g(n)]\ \big(\|A_i(x) - A_j(x)\| < \varepsilon\big).$$

The von Neumann Mean Ergodic Theorem was generalized in 1939 to uniformly convex Banach spaces by Garrett Birkhoff [2] with a proof that nicely formalizes in (a weak fragment of) the system $\mathcal{A}^\omega[X, \|\cdot\|, \eta]$ (see the end of section 3) to which functional interpretation applies.[2] In fact, a logical

[1] Such a function can easily be constructed from any unary function satisfying the previous condition.
[2] Also in 1939, E.R. Lorch [28] extended the Mean Ergodic Theorem to general reflexiv Banach spaces but his proof is less suited for a logical analysis.

metatheorem from Kohlenbach [19] based on functional interpretation guarantees the extractability of a computable bound Φ on '$\exists n$' that only depends on ε, g, a modulus of uniform convexity η of X and some norm upper bound $b \geq \|x\|$. Running the extraction procedure on Birkhoff's proof has led to following explicit bound:

Theorem 5.2 (Kohlenbach-Leuştean [24]). *Assume that X is a uniformly convex Banach space, η is a modulus of uniform convexity and $f : X \to X$ is a nonexpansive linear operator. Let $b > 0$. Then for all $x \in X$ with $\|x\| \leq b$,*

$$\forall \varepsilon > 0 \, \forall g : \mathbb{N} \to \mathbb{N} \, \exists n \leq \Phi(\varepsilon, g, b, \eta) \, \forall i, j \in [n; n + g(n)] \left(\|A_i(x) - A_j(x)\| < \varepsilon \right), \text{ where}$$

$$\begin{aligned} &\Phi(\varepsilon, g, b, \eta) := M \cdot \tilde{h}^K(0), \text{ with} \\ &M := \left\lceil \tfrac{16b}{\varepsilon} \right\rceil, \gamma := \tfrac{\varepsilon}{16} \eta\left(\tfrac{\varepsilon}{8b}\right), \quad K := \left\lceil \tfrac{b}{\gamma} \right\rceil, \\ &h, \tilde{h} : \mathbb{N} \to \mathbb{N}, \; h(m) := 2(Mm + g(Mm)), \quad \tilde{h}(m) := \max_{i \leq m} h(i). \end{aligned}$$

If $\eta(\varepsilon)$ can be written as $\varepsilon \cdot \tilde{\eta}(\varepsilon)$ with $0 < \varepsilon_1 \leq \varepsilon_2 \to \tilde{\eta}(\varepsilon_1) \leq \tilde{\eta}(\varepsilon_2)$, then we can replace η by $\tilde{\eta}$ and the constant '16' by '8' in the definition of γ in the bound above.

Remark 5.3. *Note that the above bound Φ is independent from f and depends on the space X and the starting point $x \in X$ only via the modulus of convexity η and the norm upper bound $b \geq \|x\|$. Moreover, it is easy to see that the bound depends on b and ε only via b/ε.*

Specialized to the case where X is a Hilbert space, theorem 5.2 yields the following result which improves a prior bound (also guided by [19]) from Avigad et al. [1] (see also Tao [37]):

Corollary 5.4 (Kohlenbach-Leuştean [24]). *Assume that X is a Hilbert space and $f : X \to X$ is a nonexpansive linear operator. Let $b > 0$. Then for all $x \in X$ with $\|x\| \leq b$,*

$$\forall \varepsilon > 0 \, \forall g : \mathbb{N} \to \mathbb{N} \, \exists n \leq \Phi(\varepsilon, g, b) \, \forall i, j \in [n; n + g(n)] \left(\|A_i(x) - A_j(x)\| < \varepsilon \right),$$

where Φ is defined as above, but with $K := \left\lceil \frac{512 b^2}{\varepsilon^2} \right\rceil$.

Acknowledgement: I am grateful to E.M. Briseid and L. Leuştean for helpful comments on an earlier version of this paper.

References

[1] Avigad, J., Gerhardy, P., Towsner, H., Local stability of ergodic averages. To appear in: Trans. Amer. Math. Soc.

[2] Birkhoff, G., The mean ergodic theorem. Duke Math. J. 5 (1939), no. 1, 19-20.

[3] Bombieri, E., On the Thue-Siegel-Dyson theorem. Acta Mathematica **148**, pp. 255-296 (1982).

[4] Bombieri, E., van der Poorten, A.J., Some quantitative results related to Roth's theorem. J. Austral. Math. Soc. (Series A) **45**, pp. 233-248 (1988).

[5] Coquand, T., Herbrand et le programme de Hilbert. This volume.

[6] Dreben B., Andrews, P., Aanderaa, S., False lemmas in Herbrand. Bull. Amer. Math. Soc. **69**, pp. 699-706 (1963).

[7] Esnault, H., Viehweg, E., Dyson's lemma for polynomials in several variables (and the theorem of Roth). Inventiones Mathematicae **78**, pp. 445-490 (1984).

[8] Gerhardy, P., Kohlenbach, U., Extracting Herbrand disjunctions by functional interpretation. Arch. Math. Logic **44**, pp. 633-644 (2005).

[9] Gerhardy, P., Kohlenbach, U., General logical metatheorems for functional analysis. Trans. Amer. Math. Soc. **360**, pp. 2615-2660 (2008).

[10] Girard, J.-Y., Proof Theory and Logical Complexity Vol.I. Studies in Proof Theory. Bibliopolis (Napoli) and Elsevier Science Publishers (Amsterdam) 1987.

[11] Goebel, K., Kirk, W.A., Iteration processes for nonexpansive mappings. In: Singh, S.P., Thomeier, S., Watson, B., eds., Topological Methods in Nonlinear Functional Analysis. Contemporary Mathematics **21**, AMS, pp. 115-123 (1983).

[12] Gödel, K., Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. Dialectica **12**, pp. 280–287 (1958).

[13] Goldfarb, W., Herbrand's error and Gödel's correction. Modern Logic **3**, no. 2, pp. 103-118 (1993).

[14] Herbrand, J., Logical writings. Edited by W. Goldfarb. A translation of the Écrits logiques, edited by Jean van Heijenoort and including contributions by Claude Chevalley and Albert Lautman. Harvard University Press, Cambridge, Mass., 1971. viii+312 pp.

[15] Hilbert, D., Über das Unendliche. Math. Ann. **95**, pp. 161-190 (1926).

[16] Howard, W.A., Hereditarily majorizable functionals of finite type. In: Troelstra (ed.), Metamathematical investigation of intuitionistic arithmetic and analysis, pp. 454-461. Springer LNM 344 (1973).

[17] Ishikawa, S., Fixed points and iterations of a nonexpansive mapping in a Banach space. Proc. Amer. Math. Soc. **59**, pp. 65-71 (1976).

[18] Kohlenbach, U., Analysing proofs in analysis. In: W. Hodges, M. Hyland, C. Steinhorn, J. Truss, editors, *Logic: from Foundations to Applications. European Logic Colloquium* (Keele, 1993), pp. 225–260, Oxford University Press (1996).

[19] Kohlenbach, U., Some logical metatheorems with applications in functional analysis. Trans. Amer. Math. Soc. vol. 357, no. 1, pp. 89-128 (2005).

[20] Kohlenbach, U., Effective uniform bounds from proofs in abstract functional analysis. In: Cooper, B., Löwe, B., Sorbi, A. (eds.), New Computational Paradigms: Changing Conceptions of What is Computable. Springer Publisher, pp. 223-258 (2008).

[21] Kohlenbach, U., Gödel's functional interpretation and its use in current mathematics. To appear in: Baaz, M. et al. (eds.), Horizons of Truth, Gödel Centenary. Cambridge University Press. Reprinted in: dialectica Vol. 62, no. 2, pp. 223-267 (2008).

[22] Kohlenbach, U., Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Springer Monographs in Mathematics. xx+536pp., Springer Heidelberg-Berlin, 2008.

[23] Kohlenbach, U., Leuştean, L., Mann iterates of directionally nonexpansive mappings in hyperbolic spaces. Abstract and Applied Analysis, vol. 2003, no.8, pp. 449-477 (2003).

[24] Kohlenbach, U., Leuştean, L., A quantitative mean ergodic theorem for uniformly convex Banach spaces. arXiv:0804.3844[math.DS] (2008), submitted.

[25] Kreisel, G., On the interpretation of non-finitist proofs, part I. J. Symbolic Logic **16**, pp.241-267 (1951).

[26] Kreisel, G., Finiteness theorems in arithmetic: an application of Herbrand's theorem for Σ_2-formulas. Proc. of the Herbrand symposium (Marseille, 1981), North-Holland (Amsterdam), pp. 39-55 (1982).

[27] Kreisel, G., Macintyre, A., Constructive logic versus algebraization I. Proc. L.E.J. Brouwer Centenary Symposium (Noordwijkerhout 1981), North-Holland (Amsterdam), pp. 217-260 (1982).

[28] Lorch, E.R., Means of iterated transformations in reflexive vector spaces. Bull. Amer. Math. Soc. **45**, pp. 945-947 (1939).

[29] Luckhardt, H., Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. J. Symbolic Logic **54**, pp. 234-263 (1989).

[30] Oliva, P., Understanding and using Spector's bar recursive interpretation of classical analysis. In: Proceedings of CiE 2006, Springer LNCS **3988**, pp. 423-434 (2006).

[31] Roth, K.F., Rational approximations to algebraic numbers. Mathematika **2**, pp. 1-20 (1955).

[32] Shoenfield, J.S., Mathematical Logic. Addison-Wesley Publishing Company (Reading, Massachusetts) 1967.

[33] Specker, E., Nicht konstruktiv beweisbare Sätze der Analysis. J. Symb. Logic **14**, pp. 145-158 (1949).

[34] Spector, C., Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles formulated in current intuitionistic mathematics. In: Recursive function theory, Proceedings of Symposia in Pure Mathematics, vol. 5 (J.C.E. Dekker (ed.)), AMS, Providence, R.I., pp. 1-27 (1962).

[35] Statman, R., Lower bounds on Herbrand's theorem. Proc. Amer. Math. Soc. **75**, pp. 104-107 (1979).

[36] Tao, T., Soft analysis, hard analysis, and the finite convergence principle. Essay posted May 23, 2007. Available at: http://terrytao.wordpress.com/2007/05/23/soft-analysis-hard-analysis-and-the-finite-convergence-principle/.

[37] Tao, T., Norm convergence of multiple ergodic averages for commuting transformations. Ergodic Theory and Dynamical Systems **28**, pp. 657-688 (2008).