Basic Research in Computer Science

BRICS RS-97-30 U. Kohlenbach: Proof Theory and Computational Analysis

Proof Theory and Computational Analysis

Ulrich Kohlenbach

BRICS Report Series **RS-97-30**

ISSN 0909-0878 **November 1997**

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/97/30/`

Proof theory and computational analysis

Ulrich Kohlenbach

BRICS*
Department of Computer Science
University of Aarhus
Ny Munkegade, Bldg. 540
DK-8000 Aarhus C, Denmark
kohlenb@brics.dk

November 1997

Abstract

In this survey paper we start with a discussion how functionals of finite type can be used for the proof-theoretic extraction of numerical data (e.g. effective uniform bounds and rates of convergence) from non-constructive proofs in numerical analysis.

We focus on the case where the extractability of polynomial bounds is guaranteed. This leads to the concept of hereditarily polynomial bounded analysis **PBA**. We indicate the mathematical range of **PBA** which turns out to be surprisingly large.

Finally we discuss the relationship between **PBA** and so-called feasible analysis **FA**. It turns out that both frameworks are incomparable. We argue in favor of the thesis that **PBA** offers the more useful approach for the purpose of extracting mathematically interesting bounds from proofs.

In a sequel of appendices to this paper we indicate the expressive power of **PBA**.

*Basic Research in Computer Science, Centre of the Danish National Research Foundation.

1 Uniform bounds in analysis

There are (at least) two major challenges in computational analysis:

1) to find algorithms for the computation of basic analytical concepts like e.g. the Riemann integral $\int_0^1 f(x)dx$ (as well as more general integrals), the supremum $\sup_{x\in[0,1]} f(x)$ etc. for functions $f \in C[0,1]$ which are efficient at least under additional assumptions on f which are satisfied in many practical applications. Sometimes additional assumptions are needed to ensure at all the computability of the concept in question, e.g. in the problem of finding roots etc.

2) to get a-priori bounds on the stopping problems for certain algorithmic procedures, e.g. the rate of convergence of some iterative algorithm. Typically such algorithms compute solutions x_ε of ε-weakenings $A_\varepsilon(x)$ of an equation or a property $A(x)$ (e.g. ε-best approximations instead of best approximations in Chebycheff approximation theory) where

$$(1)\ (\forall \varepsilon > 0 A_\varepsilon(x)) \leftrightarrow A(x)$$

and

$$(2)\ \forall x \in K, \varepsilon, \tilde{\varepsilon} > 0(\varepsilon < \tilde{\varepsilon} \wedge A_\varepsilon(x) \to A_{\tilde{\varepsilon}}(x)).$$

In general a solution x_ε for $A_\varepsilon(x)$ need not to be close to any actual solution of $A(x)$.

If x varies over some compact metric space (K,d) and $A(x)$ is 'ε-continuous' in the sense

$$(3)\ \forall x \in K \forall \varepsilon > 0 \exists \delta > 0 \forall \tilde{x} \in K(d(x,\tilde{x}) < \delta \wedge A_\varepsilon(\tilde{x}) \to A_{2\varepsilon}(x))$$

and if $(x_n)_{n\in\mathbb{N}} \subset K$ with $A_{\frac{1}{n}}(x_n)$ for all $n \in \mathbb{N}$, then an easy compactness argument shows that there exists a subsequence of $(x_{\frac{1}{n}})_{n\in\mathbb{N}}$ which converges to a solution of $A(x)$.

Example: $A(x) :\equiv (F(x) =_{\mathbb{R}} 0)$, where $F : K \to \mathbb{R}$ is continuous, and $A_\varepsilon(x) :\equiv (|F(x)| \leq_{\mathbb{R}} \varepsilon)$.

Moreover if there exists exactly one solution x_0 of $A(x)$ in K, then the sequence $(x_{\frac{1}{n}})_{n\in\mathbb{N}}$ itself converges to this solution

$$(4)\ n \to \infty \Rightarrow d(x_n, x_0) \to 0,$$

but what is the rate of convergence?

Whereas it seems doubtful whether proof theory is able to contribute to 1) (in a narrow sense) it is a potentially useful tool for 2) as is witnessed e.g. in the area of (Chebycheff) approximation theory where new mathematical results on strong unicity and a new quantitative version of the so-called alternation theorem were obtained by proof-theoretic analysis of well-known (non-constructive) uniqueness proof (see [11],[12],[13]).

Let us discuss this further considering (4) again:
The uniqueness of x_0, i.e.

$$(5)\ \forall x_1, x_2 \in K(A(x_1) \wedge A(x_2) \to x_1 = x_2)$$

can – using $(1), (2)$ – be written as[1]

$$(6)\ \forall x_1, x_2 \in K \forall k \in \mathbb{N} \exists n \in \mathbb{N}(\underbrace{A_{\frac{1}{n}}(x_1) \wedge A_{\frac{1}{n}}(x_2) \to d(x_1, x_2) <_{\mathbb{R}} \frac{1}{k}}_{B(x_1,x_2,k,n)}).$$

Typically (using a suitable representation of analytical objects like $x \in K$ and $y \in \mathbb{R}$) $A_\varepsilon(x)$ can be written as a Π^0_1-formula (as in our example above) and so $B \in \Sigma^0_1$.[2]
The convergence problem is solved quantitatively if we can construct a uniform witness for $\exists n$ which does not depend on $x_1, x_2 \in K$, i.e.

$$(7)\ \forall x_1, x_2 \in K \forall k \in \mathbb{N}(A_{\frac{1}{\Phi k}}(x_1) \wedge A_{\frac{1}{\Phi k}}(x_2) \to d(x_1, x_2) < \frac{1}{k}).$$

One then immediately concludes that

$$(8)\ \forall k \in \mathbb{N}(d(x_{\Phi k}, x_0) < \frac{1}{k})$$

and even (using (2) above)

$$(9)\ \forall k \in \mathbb{N} \forall m \geq \Phi k(d(x_m, x_0) < \frac{1}{k}),$$

where $(x_n)_{n\in\mathbb{N}} \subset K$ such that $A_{\frac{1}{n}}(x_n)$ for all $n \geq 1$ and $x_0 \in K$ such that $A(x_0)$.

[1] For simplicity we tacitly assume here that $k, n \geq 1$ in order to avoid the need to replace $\frac{1}{k}, \frac{1}{n}$ by $\frac{1}{k+1}, \frac{1}{n+1}$.

[2] In the systems we are considering real numbers are represented as (certain) sequences of rational numbers with fixed rate of convergence. Hence $=_{\mathbb{R}}, \leq_{\mathbb{R}} \in \Pi^0_1$ and $<_{\mathbb{R}} \in \Sigma^0_1$ (for details see appendix A1,2).

It is an easy observation (using (2) again) that (6) is monotone w.r.t. '$\exists n$'. Hence any uniform **bound** (not depending on $x_1, x_2 \in K$) provides already a uniform witness. So the whole question comes down to the problem:

How to construct a uniform bound

$$(10)\ \forall x_1, x_2 \in K \forall k \in \mathbb{N} \exists n \leq \Phi k\, B(x_1, x_2, k, n)$$

if

$$(11)\ \forall x_1, x_2 \in K \forall k \in \mathbb{N} \exists n \in \mathbb{N}\, B(x_1, x_2, k, n)$$

holds, where $B \in \Sigma_1^0$?

Using a suitable representation of the compact space K, (11) (when formalized in a system in the language of arithmetic in all finite types) has the form

$$(12)\ \forall x_1, x_2 \leq_1 s \forall k^0 \exists n^0 B(x_1, x_2, k, n)$$

where $\leq_\rho$ is pointwise defined and s is a specific function (given by a closed term of the respective system).

Slightly more general we consider sentences

$$(13)\ \forall x^1 \forall k^0 \forall y \leq_\rho sxk \exists n^0 B(x, k, y, n),$$

where $B(x, k, y, n) \in \Sigma_1^0$ and contains only x, k, y, n as free variables.

Remark 1.1 *In* (13) *above we may have tuples* $\underline{x}$ *of variables* $x_1^{\delta_1}, \ldots, x_m^{\delta_m}$ *with* $deg(\delta_i) \leq 1$ *for* $i = 1, \ldots, m$. *Furthermore* n *may have a type* τ *with* $deg(\tau) \leq 2$ *(we may even have a tuple of such variables) and* B *may be a formula* $\exists \underline{v} B_0$, *where* B_0 *is quantifier-free and the variables* $\underline{v}$ *are of arbitrary types. Also we may have tuples* $\underline{y}$ *of variables* $y_i \leq_\rho sxk$. *For notational simplicity we restrict ourselves to variables* $n, \underline{v}$ *of type* 0. *Note that then without loss of generality we may assume* B *to be quantifier-free.*

Our goal is now to construct a computable functional $\Phi^{0(0)(1)}$ such that

$$(14)\ \forall x^1 \forall k^0 \forall y \leq_\rho sxk \exists n \leq_0 \Phi xk\, B(x, y, k, n).$$

Usually and in particular if (13) has been proved non-constructively (both by the use of classical logic as well as by using non-constructive function existence principles like

the binary König's lemma WKL) one cannot directly read of a bound Φ from the proof of (13) and it is here where proof theory comes into the picture. The applicability of proof theory in this area of course depends on various requirements to be satisfied:

1) The extraction of the bound Φ from a proof of (13) must be relatively simple and should leave the original structure of the proof essentially unchanged (in particular it should not cause an enormous increase of the length of the given proof), i.e. it should have a nice behaviour w.r.t. modus ponens ('modularity').

2) The proof-theoretic method should be applicable to systems formulated in a rich and flexible language which makes it easy to formalize the analytical concepts used in the proof avoiding complicated coding devices and at the same time allows to formalize many interesting theorems in analysis in the form (13) (i.e. the quantifier-free part of the system should already have a great expressive power).

3) It should be able to treat a variety of genuine analytical principles without increasing the complexity of the extraction procedure or the bound extracted.

4) It should faithfully reflect the numerical content w.r.t. bounds of the given proof and provide bounds of low growth (relative to the growth of the terms used in the proof) if no complicated instances of induction are used in the proof.

Condition 1) rules out methods based on cut-elimination or normalization of proofs. Condition 2) makes it desirable to have a method which applies to systems formulated in a language of all finite types instead of second-order languages. Condition 3) rules out the usual Gödel functional interpretation (with a negative translation on top of it). Moreover it provides an additional obstacle to a combination of negative translation followed by the Friedman/Dragalin A-translation and modified realizability interpretation, since the A-translation does not capture the negative translation of the axiom of quantifier-free choice (this will be discussed in a paper under preparation).

A method which we believe fulfils these requirements is the **monotone functional interpretation** which was developed in [13],[15] (the technique used in [10] can be viewed of as a precursor of this method). Monotone functional interpretation is a variant of Gödel's functional interpretation [6] and extracts majorizing functionals (in the sense of Howard [8]) of functionals satisfying the usual Gödel functional interpretation. These majorizing functionals keep control through all finite types of the growth rates involved in a given proof without any normalization. The method applies to (sub-)systems of classical arithmetic in all finite types extended by the axiom schema of quantifier-free choice

$$AC^{\rho,\tau}\text{-qf} \ : \ \forall x^\rho \exists y^\tau A_0(x,y) \to \exists Y^{\tau(\rho)} \forall x^\rho A_0(x, Yx), \quad AC\text{-qf} := \bigcup_{\rho,\tau \in \mathbf{T}} \{AC^{\rho,\tau}\text{-qf}\},$$

where A_0 is a quantifier-free formula,[3] but also to various (mostly non-constructive) analytical axioms Δ covering a great deal of classical analysis (see section 3 below). Furthermore the method can be combined with the elimination of Skolem function procedure from [16] and this combination is able to deal also with principles which go beyond WKL and cannot be treated by the monotone functional interpretation in a direct way.

A case of particular mathematical and computational interest is when Φ is guaranteed to be a **polynomial** in k and (in some sense also in) x. This has led to the study of **hereditarily polynomial bounded analysis** which has to be carefully distinguished from so-called feasible analysis as we are going to discuss now.

2 Hereditarily polynomial bounded analysis versus feasible analysis

By hereditarily polynomial bounded analysis we mean subsystems **PBA** of analysis $\mathfrak{A}$ whose provably recursive functions (and in some sense explained below also functionals) can be bounded by polynomials $p \in \mathbb{N}[k]$. More specific (restricting ourselves for the moment to the special case of (13) where $\forall x^1$ is not present) the following rule is supposed to hold:

$$(15) \quad \begin{cases} \mathbf{PBA} \ \vdash \forall k^0 \forall y \leq_\rho sk \exists z^0 A_0(k,y,z) \\ \Rightarrow \ \text{one can extract a polynomial } p(k) \in \mathbb{N}[k] \text{ such that} \\ \mathbf{PBA}^* \vdash \forall k^0 \forall y \leq_\rho sk \exists z \leq_0 p(k)\, A_0(k,y,z), \end{cases}$$

where $\mathbf{PBA}^*$ is a system closely related to **PBA** (here s is a closed term of **PBA** and $A_0(k,y,z)$ contains only k,y,z as free variables).

[3] Throughout this paper $A_0, B_0, C_0, \ldots$ denote quantifier-free formulas. We allow bounded number quantifiers $\forall x \leq_0 t$, $\exists x \leq_0 t$ to occur in $A_0, B_0, C_0, \ldots$ since they can be expressed in a quantifier-free way using the bounded search-functional μ_b which is included to all systems we are considering. $\mathbf{T}$ denotes the set of all finite types.

If the statement $\forall k^0 \forall y \leq_\rho sk \exists z^0 A_0(k,y,z)$ is monotone w.r.t. '$\exists z$', as is typically the case because of the very way in which sentences of this type arise in analysis (namely as $\forall \varepsilon > 0 \exists \delta > 0$-statements, see section 4 below), then the uniform bound $p(k)$ realizes the quantifier

$$(16)\ \mathbf{PBA}^* \vdash \forall k^0 \forall y \leq_\rho sk\, A_0(k,y,p(k)).$$

Feasible analysis – **FA** for short – in the sense of e.g. [4] in contrast to **PBA** refers to subsystems of analysis with feasible (poly-time) Skolem functions for provable Π^0_2-sentences, i.e.

$$(17)\ \begin{cases} \mathbf{FA}\ \vdash \forall k^0 \exists z^0 A_0(k,z) \\ \Rightarrow \exists f \in Polytime \\ \mathbf{FA}^* \vdash \forall k^0 A_0(k,f(k)). \end{cases}$$

Ferreira introduced in [4] a system of **FA** in the language of second-order arithmetic which includes a suitable version of the binary König's lemma WKL. He in particular proved (17) for his system (where $\mathbf{FA}^* := \mathbf{FA}$ minus WKL).

Both approaches are incomparable:

1) The existence of a bound $p(k) \in \mathbb{N}[k]$ of course yields a bound in $Polytime$[4], namely p, but not a poly-time witness function (not even when A_0 is poly-time decidable which typically will not be the case in **PBA**) since $Polytime$ is not closed under bounded search (but only under sharply bounded search).

2) The existence of a poly-time Skolem function f in (17) does not imply the existence of a bound $p(k) \in \mathbb{N}[k]$ since not every poly-time function is bounded by a polynomial, e.g. $f(k) := k^{log k}$ is poly-time but growths faster than every polynomial.

So in short: hereditarily polynomial bounded analysis guarantees the extractability of uniform polynomial bounds whereas feasible analysis guarantees the existence (or when treated proof-theoretically the extractability) of poly-time algorithms. Although the latter approach may yield applications e.g. in the area of analytical number theory, many existential statement in analysis are monotone and therefore the restriction to bounds is no restriction at all here but has tremendous benefits: it allows to incorporate many analytical constructions and principles which are known

[4] $Polytime$ here denotes the set of all poly-time computable n-ary number-theoretic functions.

to be unfeasible (unless the polynomial hierarchy collapses). E.g. the work of H. Friedman and K.-I. Ko (see [9]) shows that almost all basic concepts in analysis, e.g. the Riemann integral, the supremum $\sup_{x\in[0,1]} f(x)$ and many others are not feasible (in general). So to a great extend one can say that there is no such thing as feasible analysis. On the other hand hereditarily polynomial bounded analysis is amazingly rich both w.r.t. to the size of the fragment of analysis which can be carried out in a suitable system for **PBA** and w.r.t. to the great variety of theorems which can be expressed in the form (13) which is due to the fact that e.g. $\int_0^1 f(x)dx$ and $\sup_{x\in[0,1]} f(x)$ can be defined explicitly in **PBA** by certain functionals of type level 2 (see appendix A4 below).

3 The range of hereditarily polynomial analysis

In [14],[15] we proposed a system $\mathrm{G}_2\mathrm{A}^\omega$+ AC-qf $+\Delta$ for **PBA**. Here $\mathrm{G}_2\mathrm{A}^\omega$ is the second system in a hierarchy of subsystems $(\mathrm{G}_n\mathrm{A}^\omega)_{n\in\mathbb{N}}$ of arithmetic in all finite types. The definable type-1-objects of $\mathrm{G}_n\mathrm{A}^\omega$ correspond to the well-known Grzegorczyk hierarchy. Moreover $\mathrm{G}_n\mathrm{A}^\omega$ contains various functionals of higher type, a rule of quantifier-free extensionality in higher types where $s =_\rho t$ is an abbreviation for $\forall \underline{x}(s\underline{x} =_0 t\underline{x})$, and all true universal axioms $\forall \underline{x} A_0(\underline{x})$ where A_0 is a quantifier-free formula and $\underline{x}$ is a tuple of variables of types ≤ 2. Here 'true' refers to validity in the full set-theoretic type structure $\mathcal{S}^\omega$. In particular these universal axioms capture the schema of quantifier-free induction (since bounded quantification can be expressed in a quantifier-free way in $\mathrm{G}_n\mathrm{A}^\omega$ using a bounded search functional). The reason for including all true universal axioms of the type above as axioms instead of using only the schema of quantifier-free induction is that axioms of this form have a trivial (monotone) functional interpretation and therefore do not contribute to the extractable bounds by their proofs but only by the terms used in their formulation. Of course in specific proofs only finitely many of them are used.

In the special case of $\mathrm{G}_2\mathrm{A}^\omega$ we have the $\Pi_{\rho,\tau}, \Sigma_{\delta,\rho,\tau}$-combinators for all types (which allow the definition of λ-abstraction), constants 0^0 (zero), S^{00} (successor), $\min_0$ and $\max_0$ (minimum and maximum of pairs of numbers), $+$ (addition), $\cdot$ (multiplication), bounded predicative recursor constants $\tilde{R}_\rho$, a bounded search functional μ_b, a bounded maximum functional $\Phi_{\max} fx$ $(= \max_0(f0,\ldots,fx)$ and a bounded sum functional $\Phi_\Sigma fx$ $(= \sum_{i=0}^{x} fi)$.

Δ is a set of axioms having the logical form

$$(18)\ \forall x^{\delta}\exists y \leq_{\rho} sx\forall z^{\tau} A_0(x,y,z),$$

where A_0 is quantifier-free (containing only x, y, z as free variables), s is a closed term of $\mathrm{G}_n\mathrm{A}^{\omega}$ and δ, ρ, τ are arbitrary finite types.
It turns out that many non-constructive analytical theorems can be formalized as axioms (18). Nevertheless one of the main features of **monotone** functional interpretation is that axioms (18) can be seen not to contribute to the bound extracted (or to the complexity of the extraction procedure) by their proofs but only by majorizing functionals (in the sense of [8]) for the terms s. Hence we can treat them as axioms as well. However we want to keep track of their use (and therefore do not include them in the definition of $\mathrm{G}_n\mathrm{A}^{\omega}$) since at some places we need to replace them by certain ε-weakenings. The reason for this is that we want to make use also of a certain non-standard axiom

$$(19)\ F^{-} :\equiv \forall \Phi^{2(0)}, y^{1(0)}\exists y_0 \leq_{1(0)} y\forall k^0, z^1, n^0(\bigwedge_{i<_0 n}(zi \leq_0 yki) \to \Phi k(\overline{z,n}) \leq_0 \Phi k(y_0 k)),$$

(where, for $z^{\rho 0}$, $(\overline{z,n})(k^0) :=_{\rho} zk$, if $k <_0 n$ and $:= 0^{\rho}$, otherwise).
F^{-} is not true in $\mathcal{S}^{\omega}$ since it implies that every functional Φ^2 is bounded on all functions $\overline{1,n}$ for all $n \in \mathbb{N}$. However to construct a counterexample to F^{-} one has to use arithmetical comprehension over functions which is not available in our systems. In fact we are able to reduce F^{-} (which has the logical form of an axiom Δ!) in proofs of sentences (13) (relative to $\mathrm{G}_n\mathrm{A}^{\omega} + \Delta +$ AC-qf) to its ε-weakening which is true in S^{ω} and even provable in $\mathrm{G}_3\mathrm{A}^{\omega}$. Combined with $\mathrm{AC}^{1,0}$-qf, F^{-} proves a strong principle of uniform boundedness which allows to give very short proves of various non-constructive analytical principles including a strong version of WKL (for details on this see [15],[17]).

Definition 3.1 *A term $t[x^1, k^0]$ of type 0 is called a polynomial in x, k if it is built up from $0^0, S, +, \cdot, x, k$ only by application.*

Notation 3.2 *1) For f^1 we define $f^M := \Phi_{\max} f$.*

2) $\tilde{\Delta} := \{\exists V \leq_{\delta\gamma} t\forall u^{\gamma}, w^{\tau} G_0(u, Vu, w) : \forall u^{\gamma}\exists v \leq_{\delta} tu\forall w^{\tau} G_0(u,v,w) \in \Delta\}$.

3) $G_n A_i^{\omega}$ denotes the intuitionistic variant of $G_n A^{\omega}$.

4) E-G_nA^ω is the extension of G_nA^ω obtained by adding the extensionality implication for all types.

Theorem 3.3 ([14],[15]) *Let $A_1(x^1,k^0,y^1,z^0)$ be a Σ^0_1-formula which contains only x,k,y,z as free variables and let s be a closed term of G_nA^ω. Furthermore let Δ be a set of closed axioms of the form $\forall u^\gamma \exists u \leq_\delta \forall w^\tau G_0(u,v,w)$ with $deg(\delta)\leq 1$. Then the following rule holds*

$$(20)\quad \begin{cases} \text{E-}G_2A^\omega + AC^{1,0}\text{-qf} + AC^{0,1}\text{-qf} + \Delta + F^- \vdash \forall x^1\forall k^0\forall y \leq_1 sxk\exists z^0 A_1(x,k,y,z) \\ \Rightarrow \text{ one can extract a polynomial } \Phi[x,k] \text{ in } x,k \text{ such that} \\ G_3A_i^\omega + \tilde{\Delta} \vdash \forall x^1\forall k^0\forall y \leq_1 sxk\exists z \leq_0 \Phi[x^M,k]\, A_1(x,k,y,z). \end{cases}$$

Remark 3.4 *1) Note that in the theorem above we extract a polynomial bound whereas its verification uses an (exponential) coding functional $\Phi_{\langle\rangle} fx := \langle f0,\ldots,f(x-1)\rangle$ which is definable in G_3A^ω but not in G_2A^ω.*

2) For G_2A^ω instead of E-G_2A^ω and $\oplus F^-$ instead of $+F^-$ one[5] may have full quantifier-free choice AC-qf and y^ρ for arbitrary type ρ in the theorem above. In this case we also can allow δ in Δ to be an arbitrary finite type. In this form theorem 3.3 is proved in [15]. The present formulation follows by the well-known extensionality elimination procedure, see [15](proof of cor.3.1.4).

The extraction of a bound Ψ in the theorem above which is built up only from $\Pi_{\rho,\tau}, \Sigma_{\delta,\rho,\tau}$ (for certain types δ,ρ,τ), $S,+,\cdot$ is obtained by monotone functional interpretation **without any normalization** involved. It is only if one wants to write Ψxk as a polynomial $\Phi[x,k]$ that one has to use **logical normalization** (i.e. normalization w.r.t. Π,Σ-reductions).

Theorem 3.3 remains true if we add new function symbols φ^ρ ($\deg(\rho)\leq 1$) to $\mathrm{G}_n\mathrm{A}^\omega$ together with certain universal axioms $\forall x^\tau A_0(x)$ ($\deg(\tau)\leq 2$) about them including an axiom of the form $t \geq_\rho \varphi$ for some closed term t of $\mathrm{G}_n\mathrm{A}^\omega$ (see theorem 3.2.8 of [15]). If these axioms are true in $\mathcal{S}^\omega$ for say the intended interpretation of φ, then $\mathcal{S}^\omega$ is a model also for this extension of $\mathrm{G}_n\mathrm{A}^\omega$ and since such extensions don't have any impact on extractable bounds we are free to use them and will do so in appendix B and still denote the resulting system by $\mathrm{G}_n\mathrm{A}^\omega$.

[5]Here $\oplus$ means that F^- must not be used in the proof of the premise of an application of the quantifier–free rule of extensionality QF–ER. $\mathrm{G}_n\mathrm{A}^\omega$ satisfies the deduction theorem w.r.t $\oplus$ but not w.r.t $+$.

Theorem 3.5 ([14],[15],[17])
For suitable axioms Δ of the form $\forall u^1 \exists v \leq_1 tu \forall w^1 G_0(u,v,w)$,
E-G_2A^ω+ $AC^{1,0}$-qf + $AC^{0,1}$-qf +Δ + F^- contains a substantial part of analysis including:

1) *Basic properties of the operations* $+, -, \cdot, (\cdot)^{-1}, |\cdot|, \max, \min$ *and the relations* $=, \leq, <$ *for rational numbers and real numbers (which are given by Cauchy sequences of rationals with fixed Cauchy rate of convergence).*

2) *Basic properties of maximum and sum for sequences of real numbers of variable length.*

3) *Basic properties of uniformly continuous functions* $f : [a,b]^d \to \mathbb{R}$, $\sup_{x\in[a,b]} f(x)$ *and* $\int_a^x f(x)dx$ *for* $f \in C[a,b]$ *where* $a < b$ *and* $x \in [0,1]$.

4) *The Leibniz criterion, the quotient criterion, the comparison test for series of real numbers. The convergence of the geometric series together with its sum formula. The non-convergence of the harmonic series. (But not: The Cauchy property of bounded monotone sequences in* $\mathbb{R}$ *or the Bolzano–Weierstraß property for bounded sequences in* $\mathbb{R}$*).*

5) *Characteristic properties of the trigonometric functions* $\sin, \cos, \tan, \arcsin, \arccos, \arctan$ *and of the restrictions* $\exp_k$ *and* $\ln_k$ *of* $\exp, \ln$ *to* $[-k,k]$ *for every* **fixed** *number* k.

6) *Fundamental theorem of calculus.*

7) *Fejér's theorem on uniform approximation of* 2π*–periodic uniformly continuous functions* $f : \mathbb{R} \to \mathbb{R}$ *by trigonometric polynomials.*

8) *Equivalence (local and global) of sequential continuity and* ε*–*δ*–continuity for* $f : \mathbb{R} \to \mathbb{R}$.

9) *Mean value theorem of differentiation.*

10) *Mean value theorem for integrals.*

11) *Cauchy–Peano existence theorem.*

12) *Brouwer's fixed point theorem for uniformly continuous functions* $f : [a,b]^d \to [a,b]^d$.

13) Attainment of the maximum of $f \in C([a,b]^d, \mathbb{R})$ on $[a,b]^d$.

14) Uniform continuity (together with the existence of a modulus of uniform continuity) of pointwise continuous functions $f : [a,b]^d \to \mathbb{R}$.

15) Sequential form of the Heine–Borel covering property of $[a,b]^d \subset \mathbb{R}^d$.

16) Dini's theorem: Every sequence (G_n) of pointwise continuous functions $G_n : [a,b]^d \to \mathbb{R}$ which increases pointwise to a pointwise continuous function $G : [a,b]^d \to \mathbb{R}$ converges uniformly on $[a,b]^d$ to G and there exists a modulus of uniform convergence.

17) Every strictly increasing pointwise continuous function $G : [a,b] \to \mathbb{R}$ possesses a uniformly continuous strictly increasing inverse function $G^{-1} : [Ga, Gb] \to [a,b]$.

18) a higher type formulation of König's lemma WKL^2_{seq} for sequences of binary trees.[6]

Remark 3.6 *The reason for assuming f to be uniformly continuous in some of the principles 1)-13) mentioned in the theorem, although we can weaken this to pointwise continuity in view of 14), is to make explicit the use of the non-standard axiom F^- which is used only for 14)-18).*

Let us denote from now on E-G_2A^ω+ $AC^{1,0}$-qf + $AC^{0,1}$-qf $+\Delta + F^-$ by **PBA** (for a set of axioms Δ sufficient for theorem 3.5).

Theorem 3.5 is proved in [14]. Various parts of it are published: In [15] we showed that **PBA** (even for $\Delta = \emptyset$) proves 18). In [17] it is shown that **PBA** proves (again with $\Delta = \emptyset$) 13)–17). 9) easily follows from 13). It is an easy exercise that 8) is provable in G_2A^ω+ $AC^{0,1}$-qf. Using a suitable representation of $C([a,b]^d, \mathbb{R})$ which is developed in [14] one can show that 10)-12) can be written directly as axioms Δ. 6) and 7) follow from suitable quantitative versions which can be expressed as universal axioms. 1) is carried out in detail in [18]. In an appendix to this paper we show 2),3) and 4).

[6] See [15] for details. The usual formulation of WKL cannot be written down in G_2A^ω since it requires the coding functional $\Phi_{\langle\rangle} fx := \langle f0, \ldots, f(x-1)\rangle$. In G_3A^ω one can show that WKL^2_{seq} implies WKL.

Theorems 3.3,3.5 can also be viewed as a vast extension of a result by Parikh [19]: Parikh considered a fragment PB of Peano arithmetic PA which contains the schema of induction only for bounded formulas. He shows that if a sentence $\forall x \exists y\, A(x,y)$ ($A(x,y)$ being a bounded formula) is provable in PB then there exists a polynomial p such that PB proves $\forall x \exists y \leq p(x)\, A(x,y)$. So PB can be considered as a (very weak) system of polynomially bounded arithmetic.

4 The expressive power of sentences $\forall x^1 \forall k^0 \forall y \leq_1 sxk \exists z^0 A_1$ in $\mathbf{G_2A^\omega}$

For the applicability of theorems 3.3,3.5 it is of relevance what kind of analytical theorems are formalizable in $\mathrm{G_2A}^\omega$ as sentences

$$(21)\ \forall x^1 \forall k^0 \forall y \leq_1 sxk \exists z^0 A_1(x,k,y,z),$$

where $A_1 \in \Sigma^0_1$.
Sentences (21) typically arise as follows: Let X be a complete separable metric space, K a compact metric space and $F, G : X \times K \to \mathbb{R}$ constructively definable (and therefore continuous) functions. Many interesting theorems in analysis (e.g. a large class of uniqueness theorems, see [11]) can be written in the form

$$(22)\ \forall x \in X \forall y \in K (F(x,y) = 0 \to G(x,y) = 0)$$

and thus

$$(23)\ \forall x \in X \forall y \in K \forall k \in \mathbb{N} \exists n \in \mathbb{N} (|F(x,y)| \leq \frac{1}{n+1} \to |G(x,y)| < \frac{1}{k+1}).$$

In order to formalize (23) as a sentence (21) in $\mathrm{G_2A}^\omega$ one has to represent quantification over X (resp. over K) by quantification of the form '$\forall x^1 (A_X(x) \to \dots)$' (resp. '$\forall y \leq_1 s(A_K(y) \to \dots)$' for a closed term s of $\mathrm{G_2A}^\omega$) where $A_X, A_K \in \Pi^0_1$ and F, G are definable in $\mathrm{G_2A}^\omega$ (and provably extensional w.r.t. $=_{X \times K}, =_{\mathbb{R}}$) by functionals $\Phi_F^{1(1)(1)}, \Phi_G^{1(1)(1)}$ (given by closed terms of $\mathrm{G_2A}^\omega$). Then (23) has the form

$$(24)\ \forall x^1 \forall y \leq_1 s \forall k^0 \exists n^0 (A_X(x) \wedge A_K(y) \wedge |\Phi_F(x,y)| \leq_{\mathbb{R}} \frac{1}{n+1} \to |\Phi_G(x,y)| <_{\mathbb{R}} \frac{1}{k+1}),$$

where '$(\dots)$' can be prenexed into a Σ^0_1-formula.

In finite type systems of the sort we are considering many spaces X, K can be represented even in such a way that the predicates A_X, A_K do not occur (see e.g.[1],[11]). In [14] we have shown that e.g. the spaces $\mathbb{R}^d$, $C([a,b]^d, \mathbb{R})$ and the compact space $[a_1, b_1] \times \ldots [a_d, b_d]$ can be represented in this way already in $\mathrm{G_2A}^\omega$ (for $d = 1$ we show this in the appendix A2,3 to this paper). Whereas the fact that one can get rid of A_X, A_K is crucial in recognizing that certain (non-constructive) analytical tools (e.g. Brouwer's fixed point theorem) can be written as axioms Δ, it is not necessary for the formalization of (23) in the form (24) which allows very simple representations. E.g. (using the representation of rational numbers and reals from [18]) continuous functions $F \in C[0,1]$ can be represented simply as pairs $(f^{1(0)}, \omega_f^1)$ where f represents a function $[0,1] \cap \mathbb{Q} \to \mathbb{R}$ and ω_f a modulus of uniform continuity of f, i.e.

$$(25)\ \forall x^0, y^0, k^0 (0 \leq_{\mathbb{Q}} x, y \leq_{\mathbb{Q}} 1 \wedge |x -_{\mathbb{Q}} y| \leq_{\mathbb{Q}} \frac{1}{\omega(k)+1} \to |fx -_{\mathbb{R}} fy| \leq_{\mathbb{R}} \frac{1}{k+1}).$$

Note that $(25) \in \Pi_1^0$.

The expressive power of sentences (22) crucially depends on what functions F, G are definable in $\mathrm{G_2A}^\omega$. In appendix A4 we show that e.g. $F : C[0,1] \to \mathbb{R}$, $F(f) := \sup_{x \in [0,1]} f(x)$ and $G : C[0,1] \to \mathbb{R}$, $G(f) := \int_0^1 f(x)dx$ are definable in $\mathrm{G_2A}^\omega$. So in our sentences (22) we are free to use these functions although they are not feasible and are still able to extract polynomial (and hence poly-time) bounds from proofs in **PBA**.

The definability of F, G in $\mathrm{G_2A}^\omega$ is due to the fact that we have the functionals $\Phi_{\max}, \Phi_\Sigma$ available. Both functionals are not feasible (and therefore not allowed in **FA**) but don't cause any problems in the framework of **PBA** since they can be majorized (in the sense of Howard [8]) by $\lambda f, x.f(x)$ resp. $\lambda f, x.(x+1) \cdot f(x)$.

References

[1] Beeson, M., Foundations of Constructive Mathematics. Springer Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, Band 6. Springer Berlin Heidelberg New York Tokyo 1985.

[2] Bishop, E.– Bridges, D. , Constructive analysis. Springer Grundlehren der mathematischen Wissenschaften vol.279, Berlin 1985.

[3] Brown, D.K.– Simpson, S.G., Which set existence axioms are needed to prove the separable Hahn–Banach theorem? Ann. Pure Appl. Logic **31**, pp. 123–144 (1986).

[4] Ferreira, F., A feasible theory for analysis. J. Smybolic Logic **59**, pp. 1001–1011 (1994).

[5] Forster, O., Analysis 1. Vieweg, Braunschweig/Wiesbaden (1976).

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

[7] Heuser, H., Lehrbuch der Analysis: Teil 1. Teubner, Stuttgart (1980).

[8] Howard, W.A., Hereditarily majorizable functionals of finite type. In: Troelstra (1973).

[9] Ko, K.–I., Complexity theory of real functions. Birkhäuser; Boston, Basel, Berlin (1991).

[10] Kohlenbach, U., Effective bounds from ineffective proofs in analysis: an application of functional interpretation and majorization. J. Symbolic Logic **57**, pp. 1239–1273 (1992).

[11] Kohlenbach, U., Effective moduli from ineffective uniqueness proofs. An unwinding of de La Vallée Poussin's proof for Chebycheff approximation. Ann. Pure Appl. Logic **64**, pp. 27–94 (1993).

[12] Kohlenbach, U., New effective moduli of uniqueness and uniform a–priori estimates for constants of strong unicity by logical analysis of known proofs in best approximation theory. Numer. Funct. Anal. and Optimiz. **14**, pp. 581–606 (1993).

[13] 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).

[14] Kohlenbach, U., Real growth in standard parts of analysis. Habilitationsschrift, pp. xv+166, Frankfurt (1995).

[15] Kohlenbach, U., Mathematically strong subsystems of analysis with low rate of provably recursive functionals. Arch. Math. Logic **36**, pp. 31–71 (1996).

[16] Kohlenbach, U., Elimination of Skolem functions for monotone formulas. To appear in: Archive for Mathematical Logic.

[17] Kohlenbach, U., The use of a logical principle of uniform boundedness in analysis. To appear in: Proc. 'Logic in Florence 1995'.

[18] Kohlenbach, U., Arithmetizing proofs in analysis. To appear in: Proc. Logic Colloquium 96 (San Sebastian).

[19] Parikh, R.J. Existence and feasibility in arithmetic. J. Symbolic Logic **36**, pp.494–508 (1971).

[20] Troelstra, A.S. (ed.) Metamathematical investigation of intuitionistic arithmetic and analysis. Springer Lecture Notes in Mathematics **344** (1973).

[21] Troelstra, A.S. – van Dalen, D., Constructivism in mathematics: An introduction. Vol. I,II. North–Holland, Amsterdam (1988).

In the following two appendices we present some technical details about the representability of basic analytical concepts in $\mathrm{G_2A}^\omega$ from [14] which have been unpublished hitherto but which are of relevance for the material presented in this paper. We assume some familiarity with notions introduced in [15]. $\mathrm{G}_n\mathrm{R}^\omega$ denotes the set of all closed terms of $\mathrm{G}_n\mathrm{A}^\omega$. For the treatment of higher non-constructive analytical principles (mentioned in this article) see [15],[17],[18].

A $C[0,1]$, $\sup_{x\in[0,1]} f(x)$ and $\int_0^1 f(x)dx$ in $\mathbf{G_2A}^\omega$

A.1 Real numbers in $\mathbf{G_2A}^\omega$

We recall the representation of real numbers used in [18] on which the representation of continuous functions developed in the next section is based. We have to start with the **representation of $\mathbb{Q}$**: Rational numbers are represented as codes $j(n,m)$ of pairs (n,m) of natural numbers n,m. $j(n,m)$ represents

$$\text{the rational number } \frac{\frac{n}{2}}{m+1}, \text{ if } n \text{ is even, and the negative rational } -\frac{\frac{n+1}{2}}{m+1} \text{ if } n \text{ is odd.}$$

Here $j \in \mathrm{G_2R}^\omega$ is the surjective pairing function $j(x,y) := \frac{1}{2}((x+y)^2+3x+y)$. On the codes of $\mathbb{Q}$, i.e. on $\mathbb{N}$, we have an equivalence relation by

$$n_1 =_{\mathbb{Q}} n_2 :\equiv \frac{\frac{j_1 n_1}{2}}{j_2 n_1 + 1} = \frac{\frac{j_1 n_2}{2}}{j_2 n_2 + 1} \text{ if } j_1 n_1, j_1 n_2 \text{ both are even}$$

and analogously in the remaining cases, where $\frac{a}{b} = \frac{c}{d}$ is defined to hold iff $ad =_0 cb$ (for $bd > 0$).
On $\mathbb{N}$ one easily defines functions $|\cdot|_{\mathbb{Q}}, +_{\mathbb{Q}}, -_{\mathbb{Q}}, \cdot_{\mathbb{Q}} :_{\mathbb{Q}}, \max_{\mathbb{Q}}, \min_{\mathbb{Q}} \in \mathrm{G_2R}^\omega$ and (quantifier–free) relations) $<_{\mathbb{Q}}, \leq_{\mathbb{Q}}$ which represent the corresponding functions and relations on $\mathbb{Q}$. We sometimes omit the index $\mathbb{Q}$ if this does not cause any confusion.

Notational convention: For better readability we often write e.g. $\frac{1}{k+1}$ instead of its code $j(2,k)$ in $\mathbb{N}$. So e.g. we write $x^0 \leq_{\mathbb{Q}} \frac{1}{k+1}$ for $x \leq_{\mathbb{Q}} j(2,k)$.

By the coding of rational numbers as natural numbers, **sequences of rationals** are just functions f^1 (and every function f^1 can be conceived as a sequence of rational numbers in a unique way). So real numbers can be represented by functions f^1 modulo this coding. We now show that **every** function can be conceived as an representative of a uniquely determined Cauchy sequence of rationals with modulus $1/(k+1)$ and therefore can be conceived as an representative of a uniquely determined real number.

Definition A.1.1 *The functional $\lambda f^1.\widehat{f} \in G_2R^\omega$ is defined such that*

$$\widehat{f}n = \begin{cases} fn, \ \textit{if } \forall k,m,\tilde{m} \leq_0 n(m,\tilde{m} \geq_0 k \to |fm -_{\mathbb{Q}} f\tilde{m}| \leq_{\mathbb{Q}} \frac{1}{k+1}) \\ f(n_0 - 1) \textit{ for } n_0 := \min l \leq_0 n[\exists k,m,\tilde{m} \leq_0 l(m,\tilde{m} \geq_0 k \wedge |fm -_{\mathbb{Q}} f\tilde{m}| >_{\mathbb{Q}} \frac{1}{k+1})], \\ \textit{otherwise.} \end{cases}$$

It is clear that (provable in $\mathrm{G_2A}^\omega$)

1) if f^1 represents a Cauchy sequence of rational numbers with modulus $1/(k+1)$, then $\forall n^0(fn =_0 \widehat{f}n)$,

2) for every f^1 the function $\widehat{f}$ represents a Cauchy sequence of rational numbers with modulus $1/(k+1)$.

Hence every function f gives a uniquely determined real number, namely that number which is represented by $\widehat{f}$. Quantification $\forall x \in \mathbb{R}\, A(x)$ $(\exists x \in \mathbb{R}\, A(x))$ so reduces to the quantification $\forall f^1 A(\widehat{f})$ $(\exists f^1 A(\widehat{f}))$ for properties A which are extensional w.r.t. $=_{\mathbb{R}}$ below (i.e. which are really properties of real numbers). **Operations** $\Phi : \mathbb{R} \to \mathbb{R}$ are given by functionals $\Phi^{1(1)}$ (which are extensional w.r.t.$=_1$). A real function : $\mathbb{R} \to \mathbb{R}$ is given by a functional $\Phi^{1(1)}$ which (in addition) is extensional w.r.t. $=_{\mathbb{R}}$. For convenience we often write (x_n) instead of fn and $(\widehat{x}_n)$ instead of $\widehat{f}n$.
One easily defines in $\mathrm{G_2A}^\omega$ the usual relations and operations of $\mathbb{R}$ on the representatives of the reals:

Definition A.1.2 *1)* $(x_n) =_{\mathbb{R}} (\tilde{x}_n) :\equiv \forall k^0(|\widehat{x}_k -_{\mathbb{Q}} \widehat{\tilde{x}}_k| \leq_{\mathbb{Q}} \frac{3}{k+1})$;

2) $(x_n) <_{\mathbb{R}} (\tilde{x}_n) :\equiv \exists k^0(\widehat{\tilde{x}}_k - \widehat{x}_k >_{\mathbb{Q}} \frac{3}{k+1})$;

3) $(x_n) \leq_{\mathbb{R}} (\tilde{x}_n) :\equiv \neg(\widehat{\tilde{x}}_n) <_{\mathbb{R}} (\widehat{x}_n)$;

4) $(x_n) +_{\mathbb{R}} (\tilde{x}_n) := (\widehat{x}_{2n+1} +_{\mathbb{Q}} \widehat{\tilde{x}}_{2n+1})$;

5) $(x_n) -_{\mathbb{R}} (\tilde{x}_n) := (\widehat{x}_{2n+1} -_{\mathbb{Q}} \widehat{\tilde{x}}_{2n+1})$;

6) $|(x_n)|_{\mathbb{R}} := (|\widehat{x}_n|_{\mathbb{Q}})$;

7) $(x_n) \cdot_{\mathbb{R}} (\tilde{x}_n) := (\widehat{x}_{2(n+1)k} \cdot_{\mathbb{Q}} \widehat{\tilde{x}}_{2(n+1)k})$, *where* $k := \lceil \max_{\mathbb{Q}}(|x_0|_{\mathbb{Q}} + 1, |\tilde{x_0}|_{\mathbb{Q}} + 1)\rceil$;

8) For (x_n) *and* l^0 *we define*

$$(x_n)^{-1} := \begin{cases} (\max_{\mathbb{Q}}(\widehat{x}_{(n+1)(l+1)^2}, \frac{1}{l+1})^{-1}), & \textit{if } \widehat{x}_{2(l+1)} >_{\mathbb{Q}} 0 \\ (\min_{\mathbb{Q}}(\widehat{x}_{(n+1)(l+1)^2}, \frac{-1}{l+1})^{-1}), & \textit{otherwise}; \end{cases}$$

9) $\max_{\mathbb{R}}((x_n),(\tilde{x}_n)) := (\max_{\mathbb{Q}}(\widehat{x}_n, \widehat{\tilde{x}}_n))$, $\min_{\mathbb{R}}((x_n),(\tilde{x}_n)) := (\min_{\mathbb{Q}}(\widehat{x}_n, \widehat{\tilde{x}}_n))$.

$\mathrm{G_2A}^\omega$ suffices to prove the usual properties of the relations and operations represented above (see [18] for details).

Notational convention: For notational simplicity we often omit the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$, e.g. $x^1 \leq_{\mathbb{R}} y^0$ stands for $x \leq_{\mathbb{R}} \lambda n.y^0$. From the type of the objects it will be always clear what is meant.

If $(f_n)_{n\in\mathbb{N}}$ of type 1(0) represents a $\frac{1}{k+1}$–Cauchy sequence of **real** numbers, then (provably in $\mathrm{G_2A}^\omega$) $f(n) := \widehat{f}_{3(n+1)}(3(n+1))$ represents the limit of this sequence, i.e. $\forall k(|f_k -_{\mathbb{R}} f| \leq_{\mathbb{R}} \frac{1}{k+1})$.

A.2 Representation of [0,1]$\subset \mathbb{R}$ in $\mathbf{G_2A}^\omega$

Every element of $[0,1]$ can be represented already by a bounded function $f \in \{f : f \leq_1 M\}$, where M is a fixed function from $\mathrm{G_2R}^\omega$ and that every function from this set can be conceived as an (representative of an) element in [0,1]: Define a function
$q \in \mathrm{G_2R}^\omega$ by

$$q(n) := \begin{cases} \min l \leq_0 n[l =_{\mathbb{Q}} n], & \text{if } 0 \leq_{\mathbb{Q}} n \leq_{\mathbb{Q}} 1 \\ 0^0, & \text{otherwise.} \end{cases}$$

Every rational number $\in [0,1] \cap \mathbb{Q}$ has a unique code by a number $\in q(\mathbb{N})$ and $\forall n^0(q(q(n)) =_0 q(n))$. Also every such number codes an element of $\in [0,1] \cap \mathbb{Q}$. We may conceive every number n as a representative of a rational number $\in [0,1] \cap \mathbb{Q}$, namely of the rational coded by $q(n)$.
In contrast to $\mathbb{R}$ we can restrict the set of representing functions for [0,1] to the compact (in the sense of the Baire space) set $f \in \{f : f \leq_1 M\}$, where $M(n) := j(6(n+1), 3(n+1)-1)$: Each fraction r having the form $\frac{i}{3(n+1)}$ (with $i \leq 3(n+1)$) is represented by a number $k \leq M(n)$, i.e. $k \leq M(n) \wedge q(k)$ codes r. Thus $\{k : k \leq M(n)\}$ contains (modulo this coding) an $\frac{1}{3(n+1)}$–net for [0,1]. Let $\lambda f.\tilde{f} \in \mathrm{G_2R}^\omega$ be such that

$\tilde{f}(k) = q(i_0)$,
where $i_0 = \mu i \leq_0 M(k)[\forall j \leq_0 M(k)(|\widehat{f}(3(k+1)) -_{\mathbb{Q}} q(j)| \geq_{\mathbb{Q}} |\widehat{f}(3(k+1)) -_{\mathbb{Q}} q(i)|)]$.

$\tilde{f}$ has (provably in $\mathrm{G_2A}^\omega$) the following properties:

1) $\forall f^1(\tilde{f} \leq_1 M)$.

2) $\forall f^1(\widehat{\tilde{f}} =_1 \tilde{f})$.

3) $\forall f^1(0 \leq_{\mathbb{R}} \tilde{f} \leq_{\mathbb{R}} 1)$.

4) $\forall f^1(0 \leq_{\mathbb{R}} f \leq_{\mathbb{R}} 1 \to f =_{\mathbb{R}} \tilde{f})$.

5) $\forall f^1(\tilde{\tilde{f}} =_{\mathbb{R}} \tilde{f})$.

Using this construction we can reduce quantification $\forall x \in [0,1]\ A(x)$ and $\exists x \in [0,1]\ A(x)$ to quantification of the form $\forall f \leq_1 M\ A(\tilde{f})$ and $\exists f \leq_1 M\ A(\tilde{f})$ for properties A which are $=_{\mathbb{R}}$–extensional (for f_1, f_2 such that $0 \leq_{\mathbb{R}} f_1, f_2 \leq_{\mathbb{R}} 1$), where $M \in \mathrm{G_2R}^\omega$. Analogously one can define a representation of $[a,b]$ for variable a^1, b^1 such that $a <_{\mathbb{R}} b$ by bounded functions $\{f^1 : f \leq_1 M(a,b)\}$. However one can easily reduce the quantification over $[a,b]$ to quantification over $[0,1]$ using the convex combination $a(1-x)+bx$ where x varies over $[0,1]$ so that we do not need this generalization. But on some occasions it is convenient to have an explicit representation for $[-k,k]$ for all natural numbers k. This representation is analogous to the representation of $[0,1]$ except that we now define $M_k(n) := j(6k(n+1), 3(n+1)-1)$ as the bounding function. The construction corresponding to $\lambda f.\tilde{f}$ is also denoted by $\tilde{f}$ since it will be always clear from the context what interval we have in mind.

A.3 Representation of continuous functions $f : [0,1] \to \mathbb{R}$ by number theoretic functions

Functions $f : [a,b] \to \mathbb{R}$ $(a,b \in \mathbb{R}, a < b)$ are represented in $\mathrm{G}_n\mathrm{A}^\omega$ by functionals $\Phi^{1(1)}$ which are $=_{\mathbb{R}}$–extensional:

$$\forall x^1, y^1 (a^1 \leq_{\mathbb{R}} x, y \leq_{\mathbb{R}} b^1 \wedge x =_{\mathbb{R}} y \to \Phi x =_{\mathbb{R}} \Phi y).$$

Let $f : [a,b] \to \mathbb{R}$ be a pointwise continuous function. Then (classically) f is uniformly continuous and possesses a modulus $\omega : \mathbb{N} \to \mathbb{N}$ of uniform continuity, i.e.

$$\forall x, y \in [a,b], k \in \mathbb{N} (|x-y| \leq \frac{1}{\omega(k)+1} \to |fx - fy| \leq \frac{1}{k+1}).$$

In $\mathrm{G}_n\mathrm{A}^\omega$ this reads as follows

$$(+)\ \forall x^1, y^1, k^0 (a^1 \leq_{\mathbb{R}} x, y \leq_{\mathbb{R}} b \wedge |x -_{\mathbb{R}} y| \leq_{\mathbb{R}} \frac{1}{\omega(k)+1} \to |\Phi x -_{\mathbb{R}} \Phi y| \leq_{\mathbb{R}} \frac{1}{k+1}).$$

Thus quantification over continuous functions : $[a,b] \to \mathbb{R}$ corresponds in $\mathrm{G}_n\mathrm{A}^\omega$ to quantification over all $\Phi^{1(1)}, \omega^1$ which fulfil $(+)$.
In the following we show how this quantification over objects of type level 2 can be reduced to type–1–quantification and how the condition $(+)$ can be eliminated so that quantification over continuous functions on $[a,b]$ corresponds exactly to (unrestricted) quantification over f^1. We do this first for $a = 0, b = 1$ and reduce the general case to this situation. For a generalization of our treatment to functions on $[0,1]^d$ (and $[a_1,b_1] \times \ldots \times [a_d,b_d]$) see [14].

Let $f : [0,1] \to \mathbb{R}$ be a uniformly continuous function with modulus of uniform continuity ω_f.
f is already uniquely determined by its restriction to $[0,1] \cap \mathbb{Q}$. Thus continuous functions $f : [0,1] \to \mathbb{R}$ can be conceived as a pair (f_r, ω_f) of functions $f_r : [0,1] \cap \mathbb{Q} \to \mathbb{R}$, $\omega_f : \mathbb{N} \to \mathbb{N}$ which satisfy

$$(*)\ \forall k \in \mathbb{N}, x, y \in [0,1] \cap \mathbb{Q} (|x-y| \leq \frac{1}{\omega_f(k)+1} \to |f_r x - f_r y| \leq \frac{1}{k+1})$$

(See also [21] and [2]).

Remark A.3.1 *To represent a continuous function $f \in C[0,1]$ as a pair including a modulus of uniform continuity is a numerical enrichment of the given data which we use here for reasons which are similar to the endowment of real numbers with a Cauchy modulus: As we will see below quantification over $C[0,1]$ so reduces to quantification over functions of type 1. Furthermore many functions on $C[0,1]$ as e.g. $\int_0^1 f(x)dx$ or $\sup_{x \in [0,1]} f(x)$ are given*

by functionals $\in G_2R^\omega$ in these data (see below). This has as a consequence that many important theorems on continuous functions have the logical form of axioms Δ in theorem 3.3. Also many sentences $\forall f \in C[0,1]\forall x \in \mathbb{R}\forall y \in [0,1]\exists z \in \mathbb{N}\ A(f,x,y,z)$ have the logical form $\forall f^1, x^1 \forall y \leq_1 M \exists z^0\ \tilde{A}(f,x,y,z)$ with $\tilde{A} \in \Sigma_1^0$ so that theorem 3.5 applies yielding bounds on $\exists z$ which depend only on f, x (if f is represented with a modulus of continuity). In the presence of the axiom F^- it follows that every pointwise continuous function $f : [0,1] \to \mathbb{R}$ is uniformly continuous and possesses a modulus of uniform continuity (see [17]). Hence under F^- the enrichment by such a modulus does not imply a restriction on the class of functions.

Modulo our representation of $\mathbb{Q}$ and $\mathbb{R}$, f_r is an object of type 1(0) (i.e. a sequence of number theoretic functions). Quantification over continuous functions on [0,1] reduces to quantification over all pairs $(f^{1(0)}, \omega^1)$ (and therefore by suitable coding to quantification over all functions of type 1) which satisfy $(*)$ by substituting $\lambda x^1.f(x)_{\mathbb{R}}$ for (f,ω) in the matrix where $f(x)_{\mathbb{R}} := \lim\limits_{k\to\infty} f(\tilde{x}(\omega(k)))$ $(\lambda k^0.f(\tilde{x}(\omega(k)))$ is a Cauchy sequence of real numbers with modulus $\frac{1}{k+1}$ and so its limit is definable in $\mathrm{G_2A}^\omega$).
For the applicability of the axioms Δ in theorem 3.5 it is of importance to be able to eliminate the implicative premise $(*)$: Let us consider the theorem of the attainment of the maximum of a continuous function on [0,1]

$$\forall f \in C[0,1]\exists x_0 \in [0,1]\forall x \in [0,1](f(x_0) \geq fx).$$

Without the need of the implicative premise $(*)$ on (f,ω) this theorem would have (using our representation) the logical form

$$\forall f^1 \exists x_0 \leq_1 M \forall x^1\ A(f,x_0,x),$$

where $A \in \Pi_1^0$, i.e. the logical form of an axiom Δ in theorems 3.5. Similarly many other important non–constructive theorems would have the logical form of an axiom Δ and thus do not contribute to the rate of growth of the uniform bounds extracted from proofs which use these theorems.
In fact below we will show that the premise $(*)$ can be eliminated by constructing functionals $\tilde{\Psi}_1, \tilde{\Psi}_2 \in \mathrm{G_2R}^\omega$ such that the following holds

1) If $(f^{1(0)}, \omega^1)$ fulfils $(*)$, then $f =_{1(0)} \tilde{\Psi}_1 f\omega$ and $\tilde{\Psi}_2 f\omega$ is also a modulus of uniform continuity for f.

2) For every pair $(f^{1(0)}, \omega^1)$ the pair $(\tilde{\Psi}_1 f\omega, \tilde{\Psi}_2 f\omega)$ satisfies $(*)$.

By this construction the quantification

$$\forall (f^{1(0)}, \omega^1)((*) \to A(f,\omega))$$

reduces to

$$\forall(f^{1(0)},\omega^1)\ A(\tilde{\Psi}_1 f\omega,\tilde{\Psi}_2 f\omega)$$

(and likewise for $\exists$) for properties A which are extensional in the sense of $=_{C[0,1]}$.
In the following we write more suggestively f_ω,ω_f for $\tilde{\Psi}_1 f\omega,\tilde{\Psi}_2 f\omega$.

The underlying intuition for the following definition is roughly as follows: If f is uniformly continuous with modulus ω, then $f_\omega(n) := f(n)$. In the case that the continuity property is violated at the first time at a point n, then we define f_ω as a simple polygon using the f–values on the previous points:

Definition A.3.2 *For $f^{1(0)},\omega^1$ we define f_ω,ω_f as follows:*

$$f_\omega(n) :=_1 \begin{cases} f(n), \text{ if } A_0(f,\omega,n) :\equiv \forall m,\tilde{m} \leq_0 \Phi_\omega(3n)\forall k \leq_0 n^2 \\ \qquad\qquad (|q(m) -_{\mathbb{Q}} q(\tilde{m})| \leq \frac{1}{\tilde{\omega}(k)+1} \to |(\widehat{f(qm)})k -_{\mathbb{Q}} (\widehat{f(q\tilde{m})})k| \leq \frac{3}{k+1}) \\ \\ p_{n_0,f}(n), \text{ for } n_0 \leq_0 n \text{ minimal such that } \neg A_0(f,\omega,n_0), \text{otherwise}, \end{cases}$$

$$\overline{\omega}_f(n) :=_0 \begin{cases} \tilde{\omega}(3n), \text{ if } A_0(f,\omega,n) \\ \\ \max_0\left(\left(\max_0\left\{\left\lceil\left|\frac{f(qi)\widehat{-_{\mathbb{R}}}f(qj)}{qi-_{\mathbb{Q}}qj}\right|(1)\right\rceil + 1 : i,j \leq_0 \Phi_\omega(3n_0), q(i)\neq q(j)\right\}\right)\cdot(n+1),\tilde{\omega}(n)\right) \\ \qquad\qquad \text{for } n_0 \leq_0 n \text{ minimal such that } \neg A_0(f,\omega,n_0), \text{otherwise}, \end{cases}$$

(here $|\ldots|(1)$ is the value of the sequence $|\ldots|$ at 1) where
$p_{n_0,f}$ is the polygon defined by $f(q0),\ldots,f(q(\Phi_\omega(3(n_0 \dot{-} 1))))$,
$\tilde{\omega}(k) :=_0 \max_0(k,1)^2\cdot(\max_{i\leq k}\omega(i)+1)$, $\omega_f(n) := \overline{\omega}_f(5(n+1))$ and
$\Phi_\omega(n) :=_0 j(2(\tilde{\omega}(n)+1),\tilde{\omega}(n)+1)$ (Note that $0,1$ are coded by $0, j(2,0) \leq_0 \Phi_\omega(3(n_0 \dot{-} 1))$).

Remark A.3.3 *f_ω and ω_f are definable in G_2R^ω (as functionals in f,ω) since A_0 can be expressed quantifier–free and $p_{n_0,f}$ can be written as*

$$p_{n_0,f}(n) =_1 f(qi) +_{\mathbb{R}} \frac{f(qi) -_{\mathbb{R}} f(qj)}{qi -_{\mathbb{Q}} qj} \cdot_{\mathbb{R}} (qn -_{\mathbb{Q}} qi),$$

where $i,j \leq_0 \Phi_\omega(3(n_0 \dot{-} 1))$ are such that $qi \leq_{\mathbb{Q}} qn \wedge (|qi -_{\mathbb{Q}} qn| \text{ minimal}) \wedge qj >_{\mathbb{Q}} qn \wedge (|qj -_{\mathbb{Q}} qn| \text{ minimal})$ (If $q(n) =_{\mathbb{Q}} 1$, then $p_{n_0,f}(n) =_1 f(q(n))$).

Lemma A.3.4 *1)* $k_1 \geq_0 k_2 \to \tilde{\omega}(k_1) \geq_0 \tilde{\omega}(k_2)$.

2) $\tilde{\omega}(k) \geq_0 k$ *and* $\tilde{\omega}(k) \geq_0 \omega(k)$.

3) $\tilde{\omega}(3 \cdot k) \geq_0 3 \cdot \tilde{\omega}(k) + 3$ *for* $k \geq 1$.

Proof: 1) and 2) follow immediately from the definition of $\tilde{\omega}$.

3) $\tilde{\omega}(3k) \overset{k\geq 1}{\geq} 9k^2 \cdot (\max_{i\leq k} \omega(i) + 1) \geq 3k^2 \cdot (\max_{i\leq k} \omega(i) + 1) + 6k^2$

$\overset{k\geq 1}{\geq} 3k^2(\max_{i\leq k} \omega(i) + 1) + 3 = 3 \cdot \tilde{\omega}(k) + 3.$

Lemma A.3.5 *If* $f^{1(0)}$ *represents a uniformly continuous function* $F : [0,1] \to \mathbb{R}$ *with a modulus* ω^1 *of uniform continuity, i.e.*
$\forall m, \tilde{m}, k(|qm -_{\mathbb{Q}} q\tilde{m}| \leq_{\mathbb{Q}} \frac{1}{\omega(k)+1} \to |f(qm) -_{\mathbb{R}} f(q\tilde{m})| \leq_{\mathbb{R}} \frac{1}{k+1})$,
then $f_\omega =_{1(0)} f$ *and* ω_f *is also a modulus of uniform continuity for* F.

Proof: The first part of the lemma follows from the definition of f_ω observing that the case 'otherwise' never occurs because of the assumption, since

$$|qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{\tilde{\omega}(k)+1} \overset{l.A.3.4}{\leq} \frac{1}{\omega(k)+1}$$

implies that

$$|(f\widehat{(qm)})k -_{\mathbb{Q}} (f\widehat{(q\tilde{m})})k| \leq |f(qm) -_{\mathbb{R}} f(q\tilde{m})| + \frac{2}{k+1} \leq \frac{3}{k+1}.$$

Furthermore $\overline{\omega}_f(n) = \tilde{\omega}(3n) \overset{l.A.3.4}{\geq_0} \omega(n)$. Hence together with ω also $\overline{\omega}_f$ and thus a fortiori ω_f is a modulus of uniform continuity.

Lemma A.3.6 *For every pair* $(f^{1(0)}, \omega^1)$ *the following holds:*
f_ω *represents a uniformly continuous function :* $[0,1] \cap \mathbb{Q} \to \mathbb{R}$ *and* ω_f *is a modulus of uniform continuity for this function, i.e.*

$$\forall m, \tilde{m}, k(|qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{\omega_f(k)+1} \to |f_\omega(qm) -_{\mathbb{R}} f_\omega(q\tilde{m})| \leq \frac{1}{k+1}).$$

Proof: Let $m, \tilde{m}, k \in \mathbb{N}$ be such that $|qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{\overline{\omega}_f(k)+1}$.
We may assume that $qm >_0 q\tilde{m}$.
Case 1: $A_0(f, \omega, qm)$. Then also $A_0(f, \omega, q\tilde{m})$ since the monotonicity of $\Phi_\omega(3n)$ and n^2 implies

$$n_1 \geq_0 n_2 \wedge A_0(f, \omega, n_1) \to A_0(f, \omega, n_2).$$

Hence $f(qm) =_{\mathbb{R}} f_\omega(qm)$ and $f(q\tilde{m}) =_{\mathbb{R}} f_\omega(q\tilde{m})$. By $\overline{\omega}_f(k) \geq_0 \tilde{\omega}(k), k$ the assumption on $m, \tilde{m}, k$ yields

$$(+)\ |qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{\tilde{\omega}(k)+1} \text{ and } (++)\ |qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{k+1}.$$

$(++)$ implies that $k \leq_0 (qm)^2$ (Because of $j_2(qm), j_2(q\tilde{m}) <_0 qm$, the (distinct) fractions coded by $qm, q\tilde{m}$ have denominators $a, b \leq_0 qm$. Thus $|\frac{i}{a} - \frac{j}{b}| \geq \frac{1}{ab} \geq \frac{1}{(qm)^2}$). Furthermore $qm, q\tilde{m} \leq_0 \Phi_\omega(3(qm))$. Hence $(+)$ and $A_0(f, \omega, qm)$ yield (using $\forall x^0(q(qx) =_0 qx)$)

$$|(f\widehat{(qm)})k -_{\mathbb{Q}} (f\widehat{(q\tilde{m})})k| \leq \frac{3}{k+1}$$

and therefore

$$|f_\omega(qm) -_{\mathbb{R}} f_\omega(q\tilde{m})| =_{\mathbb{R}} |f(qm) -_{\mathbb{R}} f(q\tilde{m})| \leq \frac{5}{k+1}.$$

Case 2: $\neg A_0(f, \omega, qm)$.
2.1 $k \geq_0 n_0 := \min n \leq_0 qm \neg A_0(f, \omega, n)$:
In this case we have $f_\omega(qm) =_{\mathbb{R}} p_{n_0,f}(qm)$ and $f_\omega(q\tilde{m}) =_{\mathbb{R}} p_{n_0,f}(q\tilde{m})$ (In the case $A_0(f, \omega, q\tilde{m})$ we have $q\tilde{m} < n_0 \leq \Phi_\omega(3(n_0 - 1))$ and so $f_\omega(q\tilde{m}) = f(q\tilde{m})$ is one of the f–values used in defining $p_{n_0,f}$). Since $\overline{\omega}_f$ is a modulus of uniform continuity for $p_{n_0,f}$ for $k \geq n_0$, the assumption on $m, \tilde{m}$ implies

$$|f_\omega(qm) -_{\mathbb{R}} f_\omega(q\tilde{m})| \leq \frac{1}{k+1}.$$

2.2 $1 \leq_0 k <_0 n_0$: Then $A_0(f, \omega, k)$ and therefore $\overline{\omega}_f(k) = \tilde{\omega}(3k)$. Since all fractions $\frac{i}{\tilde{\omega}(3(n_0-1))+1}$ with $i \leq_0 \tilde{\omega}(3(n_0-1))+1$ have a code $\leq_0 \Phi_\omega(3(n_0-1))$, the maximal distance between two adjacent breaking points of $p_{n_0,f}$ is $\leq \frac{1}{\tilde{\omega}(3(n_0-1))+1}$. Hence there are $m^*, \tilde{m}^* \leq_0 \Phi_\omega(3(n_0-1))$ (i.e. 'breaking points' of the polygon $p_{n_0,f}$ next to $m, \tilde{m}$ satisfying (2) below) such that

$$(1)\ \begin{cases} |qm^* -_{\mathbb{Q}} q\tilde{m}^*| \leq \frac{1}{\overline{\omega}_f(k)+1} + \frac{2}{\tilde{\omega}(3(n_0-1))+1} \overset{l.A.3.4}{\leq} \frac{3}{\tilde{\omega}(3k)+1} \overset{l.A.3.4}{\leq} \frac{3}{3\tilde{\omega}(k)+3+1} \\ \leq \frac{1}{\tilde{\omega}(k)+1} \end{cases}$$

and

$$(2)\ |\underbrace{p_{n_0,f}(q\tilde{m}^*)}_{=_{\mathbb{R}} f(q\tilde{m}^*)} -_{\mathbb{R}} \underbrace{p_{n_0,f}(qm^*)}_{=_{\mathbb{R}} f(qm^*)}| \geq_{\mathbb{R}} |\underbrace{p_{n_0,f}(q\tilde{m})}_{=_{\mathbb{R}} f_\omega(q\tilde{m})} -_{\mathbb{R}} \underbrace{p_{n_0,f}(qm)}_{=_{\mathbb{R}} f_\omega(qm)}|.$$

Since $A_0(f,\omega,n_0-1)$ and $k \leq_0 (n_0-1)^2$, (1) and (2) imply

$$|f_\omega(qm) -_{\mathbb{R}} f_\omega(q\tilde{m})| \overset{(2)}{\leq} |f(qm^*) -_{\mathbb{R}} f(q\tilde{m}^*)| \leq |(f\widehat{(qm^*)})k -_{\mathbb{Q}} (f\widehat{(q\tilde{m}^*)})k| + \tfrac{2}{k+1}$$
$$\overset{(1)}{\leq} \tfrac{3}{k+1} + \tfrac{2}{k+1} = \tfrac{5}{k+1}.$$

Put together we have shown that in both cases (for $k \geq 1$)

$$|qm -_{\mathbb{Q}} q\tilde{m}| \leq \frac{1}{\overline{\omega}_f(k)+1} \to |f_\omega(qm) -_{\mathbb{R}} f_\omega(q\tilde{m})| \leq \frac{5}{k+1}.$$

Hence ω_f is a modulus of uniform continuity for f_ω.

Since every pair $(f^{1(0)},\omega^1)$ can be conceived now as a representation of a uniformly continuous function $[0,1]\cap\mathbb{Q} \to \mathbb{R}$, namely that function which is represented by $(\tilde{\Psi}_1 f\omega, \tilde{\Psi}_2 f\omega)$ (where $\tilde{\Psi}_1 f\omega := f_\omega \circ q, \tilde{\Psi}_2 f\omega := \omega_f$).[7] And every function g^1 can be conceived as a pair (f,ω) by $g \mapsto (\lambda k^0,n^0.(j_1 g)(j(k,n)), j_2 g)$ (where $j_i g := \lambda x^0.j_i(gx)$), so g^1 represents the continuous function $(\Psi_1 g, \Psi_2 g)$, where $\Psi_1 g := \tilde{\Psi}_1(\lambda k^0,n^0.(j_1 g)(j(k,n)), j_2 g)$ and $\Psi_2 g := \tilde{\Psi}_2(\lambda k^0,n^0.(j_1 g)(j(k,n)), j_2 g)$. Since every pair (f,ω) can be coded by a function g, every uniformly continuous function $[0,1]\cap\mathbb{Q} \to \mathbb{R}$ is represented by some function g. Together with $\tilde{\Psi}_i$ also the Ψ_i are in $\mathrm{G_2R}^\omega$.
Now we define the continuation on full $[0,1]$:

Definition A.3.7 *The functional $\lambda g^1, x^1.g(x)_{\mathbb{R}} \in G_2R^\omega$ is defined by*
$(g(x)_{\mathbb{R}})(k^0) :=_0 \Psi_1 g(\tilde{x}(\Psi_2\widehat{g(3}(k+1))))(3(k+1))$, *$\tilde{x}$ is the construction used in our representation of $[0,1]$.*

Remark A.3.8 *$g(x)_{\mathbb{R}}$ represents the value of the function $\in C[0,1]$, which is represented by g, applied to the real $\in [0,1]$, which is represented by x.*
Notation: If a function $\in C[0,1]$ is given as a pair $(f^{1(0)},\omega^1)$ we also use the notation $f(x)_{\mathbb{R}}$ in order to avoid the need of spelling out the coding $(f,\omega)\mapsto g^1$.

Remark A.3.9 *Quantification over $C[a,b]$ (where $a<b$) reduces to quantification over $C[0,1]$ by*
$f \in C[a,b] \mapsto g := \lambda x.f(a(1-x)+bx) \in C[0,1]$ and
$g \in C[0,1] \mapsto f := \lambda x.g(\frac{x-a}{b-a}) \in C[a,b]$.

[7] By switching from f_ω to $f_\omega \circ q$ we can formulate the continuity of $\tilde{\Psi}_1 f\omega$ now as $\forall m,\tilde{m}\big(0 \leq_{\mathbb{Q}} m,\tilde{m} \leq_{\mathbb{Q}} 1 \wedge |m -_{\mathbb{Q}} \tilde{m}| \leq \frac{1}{\omega_f(k)+1} \to |(\tilde{\Psi}_1 f\omega)(m) -_{\mathbb{R}} |(\tilde{\Psi}_1 f\omega)(\tilde{m})| \leq \frac{1}{k+1}\big)$, i.e. without mentioning q anymore.

In [11] we used a different representation of the space $C[0,1]$ (following [3]) based on the Weierstraß approximation theorem: A function $f \in C[0,1]$ was represented as a Cauchy sequence w.r.t. $\|\cdot\|_\infty$ (with modulus $1/(k+1)$) of polynomials with rational coefficients. Then we applied a construction, similarly to $\widehat{f}$ used in our representation of $\mathbb{R}$ above, to ensure that every function f^1 could be conceived as such a Cauchy sequence.
However this representation is not convenient for our theory $\mathrm{G_2A}^\omega$ since the coding of an arbitrary sequence of polynomials requires the coding of finite sequences of natural numbers (the codes of the coefficients) of variable length which can be carried out in $\mathrm{G_3A}^\omega$ but not in $\mathrm{G_2A}^\omega$. Furthermore in practice the computation of an approximating sequence of polynomials to a given function is quite complicated (and even more when one deals with functions in several variables) whereas for most functions occurring in mathematics a modulus of continuity can be written down directly. Hence it is much more useful to extract bounds which require as a function input only the function endowed with a modulus of uniform continuity than an approximating sequence of polynomials. In our applications to approximation theory we always obtained bounds in functions with a modulus of continuity. Because of this we conjectured in [11] that this will always hold for extractions of bounds from concrete proofs. By our new representation of $C[0,1]$ this conjecture is theoretically justified: From a proof of a sentence

$$\forall f \in C[0,1] \exists y^0 \; A(f,y), \text{ where } A \in \Sigma_1^0$$

we obtain a bound on y in a representative of f in our sense, i.e. in f endowed with a modulus of uniform continuity.

The construction of f_ω, ω_f looks quite complicated. However if f is already given with a modulus ω (as in concrete applications) then f_ω does not change anything and $\omega_f(n)$ is just a slight modification of ω and the proof of this (A.3.5) is almost trivial. The complicated clause in the definition of f_ω, ω_f is needed only to ensure that an arbitrary given pair (f,ω) is transformed into a continuous function. The quite complicated proof of lemma A.3.6 is not relevant for the extraction process since the statement of this lemma is a purely universal sentence and therefore an axiom of $\mathrm{G_2A}^\omega$.

A.4 The functionals $\max_{\mathbb{R}}, +_{\mathbb{R}}$ for sequences of variable length and $\sup_{x\in[a,b]} fx$, $\int_a^b f(x)dx$ in $\mathbf{G_2A}^\omega$

For the computation of $\sup_{x\in[a,b]} fx$ and $\int_a^b f(x)dx$ for $f \in C[a,b]$ we need the maximum and the sum of a sequence of real numbers of variable length, i.e. $\max_{\mathbb{R}} \{f(r_i) : i \le k\}$ and

$f(r_0) +_{\mathbb{R}} \ldots +_{\mathbb{R}} f(r_k)$ for a sequence of rational numbers r_i. For the construction of such operations in $\mathrm{G_2R}^\omega$ we need a special form of our representation of real numbers:
The computation of the addition of a sequence of x real numbers $a_0, \ldots, a_x$ requires the addition of corresponding sequences of the n–th rational approximations $\widehat{a}_0(n), \ldots, \widehat{a}_x(n)$ of these real numbers (for all n). For this we need the computation of a common divisor of $\widehat{a}_0(n), \ldots, \widehat{a}_x(n)$. However the size of such a common divisor will (in general) have an exponential growth in x and therefore is not definable in $\mathrm{G_2R}^\omega$ but only in $\mathrm{G_3R}^\omega$. This difficulty is avoided by modifying representatives f of real numbers to representatives f' such that $f =_{\mathbb{R}} f'$ and the n–th rational approximation $f'n$ of f' is a (code of a) fraction with a fixed denominator. We choose $3(n+1)+1$ as this denominator in order to ensure the right rate of convergence such that $\widehat{f'} =_1 f'$. For the computation of $\max_{\mathbb{R}}(a_0, \ldots, a_x)$ this modification is (although not necessary) very convenient.

Definition A.4.1

$$\check{f}n :=_0$$
$$\begin{cases} \min k \leq_0 j_1(\widehat{f}(3(n+1))) \cdot (3(n+1)+1)[\frac{\frac{k}{2}}{3(n+1)+1} \leq_{\mathbb{Q}} \widehat{f}(3(n+1)) <_{\mathbb{Q}} \frac{\frac{k}{2}+1}{3(n+1)+1} \\ \qquad\qquad \wedge k \text{ even}] \text{ if it exists and } j_1(\widehat{f}(3(n+1))) \text{ is even} \\ \\ \min k \leq_0 (j_1(\widehat{f}(3(n+1))) + 1) \cdot (3(n+1)+1)[\frac{-\frac{k+1}{2}}{3(n+1)+1} \leq_{\mathbb{Q}} \widehat{f}(3(n+1)) <_{\mathbb{Q}} \frac{-\frac{k+1}{2}+1}{3(n+1)+1} \\ \qquad\qquad \wedge k \text{ odd}] \text{ if it exists and } j_1(\widehat{f}(3(n+1))) \text{ is odd} \\ \\ 0^0, \quad \text{otherwise.} \end{cases}$$

$f'(n) := j(\check{f}n, 3(n+1))$.

Remark A.4.2 *Together with $\lambda f.\widehat{f}$ also $\lambda f.\check{f}$ and therefore $\lambda f.f'$ are definable in G_2R^ω.*

Lemma A.4.3 $G_2A^\omega \vdash \forall f^1(f' =_{\mathbb{R}} f)$.

Definition A.4.4 *$\chi^1, \psi^{1(1)} \in G_2R^\omega$ are defined such that (provably in G_2A^ω)*

$$\chi n^0 =_0 \begin{cases} 1, & \text{if } \exists m \leq_0 n(n =_0 2m) \\ 0, & \text{otherwise.} \end{cases}$$

and

$$\psi g^1 k^0 =_0 \begin{cases} \max\limits_{i \leq k} (g(i) \cdot \chi(gi)), & \text{if } \exists i \leq_0 k(\chi(gi) =_0 1) \\ \min\limits_{i \leq k} g(i), & \text{otherwise.} \end{cases}$$

Definition A.4.5 $\Phi_{\max_{\mathbb{R}}} \in G_2R^\omega$ *is defined by*
$\Phi_{\max_{\mathbb{R}}} := \lambda f^{1(0)}, k^0, n^0.j(\psi(\lambda i^0.j_1((fi)'n), k), 3(n+1))$.

Lemma A.4.6

$G_2A^\omega \vdash \forall k^0, f^{1(0)}(\Phi_{\max_{\mathbb{R}}} f0 =_{\mathbb{R}} f0 \wedge \Phi_{\max_{\mathbb{R}}} f(k+1) =_{\mathbb{R}} \max_{\mathbb{R}}(\Phi_{\max_{\mathbb{R}}} fk, f(k+1)))$.

Lemma A.4.7 *1)* $G_2A^\omega \vdash \forall f^{1(0)}, m^0, \tilde{m}^0(m \geq_0 \tilde{m} \to \Phi_{\max_{\mathbb{R}}} fm \geq_{\mathbb{R}} \Phi_{\max_{\mathbb{R}}} f\tilde{m}, f\tilde{m})$.

2) $G_2A^\omega + AC^{0,0}\text{-}qf \vdash \forall f^{1(0)}, m^0 \exists k \leq_0 m(fk =_{\mathbb{R}} \Phi_{\max_{\mathbb{R}}} fm)$.

Remark A.4.8 *1) The elementary but tedious proofs for the two lemmas above (which we don't carry out here) have no impact on the extraction of bounds: Lemma A.4.6 and A.4.7 1) are purely universal sentences. Since one can verify their truth they are treated as axioms. Lemma A.4.7 2) (although not being universal) has the logical form* $\forall x \exists y \leq sx \forall z A_0$ *of an axiom* $\in \Delta$ *and therefore is treated as an axiom by our monotone (but not by the usual) functional interpretation. The same is true for the next lemma.*

2) $\Phi_{\min_{\mathbb{R}}} fm$ *can be defined from* $\Phi_{\max_{\mathbb{R}}} fm$ *by* $:= -_{\mathbb{R}} \Phi_{\max_{\mathbb{R}}}(\lambda k.(-_{\mathbb{R}} fk), m)$.

Using $\Phi_{\max_{\mathbb{R}}}$ we are able to define $\sup_{x \in [0,1]} f(x)$ for $f \in C[0,1]$:

Definition A.4.9 $\Phi^{1(1)}_{\sup_{[0,1]}} \in G_2R^\omega$ *is defined as follows*

$$\Phi^{1(1)}_{\sup_{[0,1]}} := \lambda f^1, n^0.\Phi_{\max_{\mathbb{R}}}(\Psi_1 f, h(\Psi_2 f(3(n+1))))(3(n+1)),$$

where $hn := j(2n, n)$ *and* $\Psi_1, \Psi_2 \in G_2R^\omega$ *are the functionals used in the representation of* $C[0,1]$.

Lemma A.4.10

$$G_2A^\omega \vdash \forall f \in C[0,1](\forall x \in [0,1](\Phi_{\sup_{[0,1]}} f \geq_{\mathbb{R}} fx) \wedge \forall k^0 \exists x \in [0,1](\Phi_{\sup_{[0,1]}} f -_{\mathbb{R}} fx \leq \frac{1}{k+1})).$$

From now on we make liberal use of the usual mathematical expressions '$\sup_{x \in [0,1]} fx$' and '$f \in C[0,1]$' and go back to the details of the actual representation of these notions in $\mathrm{G_2A}^\omega$ only when this is needed to determine the logical form of a sentence which involves these notions.
For a function $f \in C[a,b]$ we can express $\sup_{x \in [a,b]} fx$ as $\sup_{x \in [0,1]} \tilde{f}x$, where $\tilde{f}x := f((1-x)a + xb)$.

For the definition of the sum of a sequence of real numbers of length x we need the following constructions.

Definition A.4.11 *The functionals* $\zeta, \overline{\zeta}, \xi \in G_2R^\omega$ *are defined such that*

$$\zeta n^0 =_0 \begin{cases} n, & \text{if } \exists m \leq n(n = 2m) \\ 0, & \text{otherwise.} \end{cases}$$

$$\overline{\zeta} n^0 =_0 \begin{cases} n+1, & \text{if } \exists m \leq n(n = 2m+1) \\ 0, & \text{otherwise.} \end{cases}$$

$$\xi n^0 m^0 =_0 \begin{cases} n \dot{-} m, & \text{if } n \geq m \\ m \dot{-} n \dot{-} 1, & \text{otherwise.} \end{cases}$$

Using these functions we are now able to define a variable summation:

Definition A.4.12 $\Phi_{\Sigma_{\mathbb{R}}} \in G_2R^\omega$ *is defined as*
$\Phi_{\Sigma_{\mathbb{R}}} := \lambda f^{1(0)}, k^0, n^0.j(\xi(\sum\limits_{i=0}^{k} \zeta(j_1[(fi)'(\alpha(k,n))]), \sum\limits_{i=0}^{k} \overline{\zeta}(j_1[(fi)'(\alpha(k,n))])), 3(\alpha(k,n)+1))$,
where $\alpha(k,n) := 2(k+1)(n+1)$.

Lemma A.4.13 $G_2A^\omega \vdash \forall f^{1(0)}, k^0(\Phi_{\Sigma_{\mathbb{R}}} f0 =_{\mathbb{R}} f0 \wedge \Phi_{\Sigma_{\mathbb{R}}} f(k+1) =_{\mathbb{R}} \Phi_{\Sigma_{\mathbb{R}}} fk +_{\mathbb{R}} f(k+1))$.

Using $\Phi_{\Sigma_{\mathbb{R}}}$ we now define the Riemann integral $\int_0^1 f(x)dx$ for $f \in C[0,1]$:
Let $S_n := \frac{1}{\omega_f(n)+1} \cdot \sum\limits_{i=0}^{\omega_f(n)} f(\frac{i}{\omega_f(n)+1})$ denote the n–th Riemann sum (where ω_f is the modulus of uniform continuity from the representation of f). One easily follows from the usual proof of the convergence of the sequence of Riemann sums that $(S_n)_{n\in\mathbb{N}}$ is a Cauchy sequence with Cauchy modulus $2/(n+1)$ (which converges to $\int_0^1 f(x)dx$). Therefore we define:

Definition A.4.14 *1)* $\Phi_S \in G_2R^\omega$ *is defined as*
$\Phi_S := \lambda f^1, n^0.j(2, \Psi_2 fn) \cdot_{\mathbb{R}} \Phi_{\Sigma_{\mathbb{R}}}(\lambda i.(\Psi_1 f)(j(2i, \Psi_2 fn)), \Psi_2 fn)$.

2) $\Phi_I \in G_2R^\omega$ *is defined as*
$\Phi_I := \lambda f^1, n^0.[\Phi_S f(2(3(n+1))+1)](3(n+1))$.

Proposition A.4.15 $\Phi_I f^1$ *represents the real number* $\int_0^1 F(x)dx$, *where* F *is the function* $\in C[0,1]$ *which is represented by* f.

Proof: Since $j(2i, \Psi_2 fn)$ codes $\frac{i}{\Psi_2 fn+1}$ and Ψ_2 is a modulus of uniform continuity for the function : $[0,1] \cap \mathbb{Q} \to \mathbb{R}$ which is represented by Ψ_1, Φ_S is just the n–th Riemann sum for the function represented by f. As we have mentioned already above, these Riemann sums S_n form a Cauchy sequence with modulus $2/(n+1)$. Hence $(S_{2n+1})_{n\in\mathbb{N}}$ is a Cauchy sequence with modulus $1/(n+1)$. $\Phi_I f$ represents the limit of this sequence.

In the following we use the usual notation $\int_0^1 f(x)dx$ instead of Φ_I.

Proposition A.4.16 *The following properties of $\int_0^1$ are provable in G_2A^ω ($f, f_n, g \in C[0,1], \lambda \in \mathbb{R}$):*

1) $\int_0^1 (f+g)(x)dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx$.

2) $\int_0^1 (\lambda \cdot f)(x)dx = \lambda \int_0^1 f(x)dx$.

3) $f \le g \to \int_0^1 f(x)dx \le \int_0^1 g(x)dx$.

4) $\left|\int_0^1 f(x)dx\right| \le \int_0^1 |f|(x)dx \le \|f\|_\infty$.

5) $f_n \overset{\|\cdot\|_\infty}{\to} f \Rightarrow \int_0^1 f_n(x)dx \to \int_0^1 f(x)dx$.

Proof: It is clear from the usual proofs in analysis that 1)–5) are true. Since 1),2) and 4) are purely universal, they are axioms of $\mathrm{G_2A}^\omega$. 3) can be transformed into a purely universal sentence

$$3)' \quad \int_0^1 f(x)dx \le \int_0^1 \max(f,g)(x)dx.$$

The proof of the equivalence of 3) and 3)' uses the extensionality of $\int_0^1$, which follows immediately from 4) and thus is also provable in $\mathrm{G_2A}^\omega$. 5) follows from 1),2) and 4).

Our definition of $\int_0^1$ easily generalizes to $\int_a^b F(x)dx$ for $F \in C[a,b]$ $(a<b)$. Let F be given as a pair $(\Psi^{1(1)}, \omega)$, where Ψ represents a function : $[a,b] \to \mathbb{R}$ which has the modulus of uniform continuity ω. Then a representative of $\int_a^b F(x)dx$ can be computed in Ψ, ω, a, b by a functional in $\mathrm{G_2R}^\omega$. For this one has to replace the partition

$$\frac{0}{\omega(n)+1}, \ldots, \frac{\omega(n)+1}{\omega(n)+1}$$

of [0,1] by the partition

$$a_0, \ldots, a_{k(\omega(n)+1)}, \text{ where } a_i := a +_{\mathbb{R}} i(b-a) \cdot_{\mathbb{R}} \frac{1}{k(\omega(n)+1)} \text{ and } \mathbb{N} \ni k \ge b-a,$$

of $[a,b]$ which also has mesh $\leq 1/(\omega(n)+1)$.

We can define also a functional $\Phi_{I_a^x} \in \mathrm{G_2R}^\omega$ such that $\Phi_{I_a^x}(x^1, a^1, \Psi^{1(1)}, \omega^1)$ represents the integral $\int_a^x \Psi x dx$ if Ψ represents a function $[a,b] \to \mathbb{R}$ $(a<b)$, which is uniformly continuous with modulus ω, and $x \in [a,b]$:

$$\Phi_{I_a^x}(x^1, a^1, \Psi^{1(1)}, \omega^1) := \lim_{n\to\infty} S_n(x, a, \Psi, \omega),$$

where

$$S_n(= S_n(x,a,\Psi,\omega)) := \frac{x -_{\mathbb{R}} a}{n+1} \cdot_{\mathbb{R}} \Phi_\Sigma(\lambda i.\Psi(a +_{\mathbb{R}} i(x -_{\mathbb{R}} a) \cdot_{\mathbb{R}} \frac{1}{n+1}), n+1).$$

From our reasoning above it is clear that (S_n) is a Cauchy sequence which converges to $\int_a^x \Psi x dx$. In order to be able to define $\lim_{n\to\infty} S_n$ in $\mathrm{G_2R}^\omega$ we have to construct a Cauchy modulus for this sequence in $\mathrm{G_2R}^\omega$. This however is possible since

$$|S_{k(\omega(n)+1)} - \int_a^x \Psi x dx| \leq \frac{k}{n+1},$$

where $k \in \mathbb{N}$ such that $k \geq x - a$.

The formula

$$\int_a^c f(x)dx + \int_c^b f(x)dx = \int_a^b f(x)dx \text{ for } a < c < b$$

is purely universal and hence an axiom of $\mathrm{G_2A}^\omega$.

B Trigonometric functions in $\mathrm{G_2A}^\omega$: Moduli and universal properties

B.1 The functions sin, cos and tan in $\mathrm{G_2A}^\omega$

In the following we introduce the functions **sin , cos** axiomatically by adding to $\mathrm{G_2A}^\omega$ new function constants $\Phi_{\sin}, \Phi_{\cos}$ of type 1(0) which represent the restriction of sin and cos to $\mathbb{Q}$. Then the Lipschitz continuity of $\sin, \cos$ is used to continue these functions to $\mathbb{R}$ (If we would introduce $\sin, \cos$ directly as functions on $\mathbb{R}$, this would require new constants for **functionals** of type 1(1). In order to express their extensionality by universal axioms we also would have to make use of the Lipschitz continuity, since uniform continuity is just a uniform quantitative version of extensionality).

The following purely universal assertions on the function constants $\Phi_{\sin}, \Phi_{\cos}$ express true propositions on $\sin, \cos$ and are therefore taken as axioms in $\mathrm{G_2A}^\omega \cup \{\Phi_{\sin}, \Phi_{\cos}\}$ (which we also denote by $\mathrm{G_2A}^\omega$):

1) $\forall x^0((\widehat{\Phi_{\sin}x}) =_1 \Phi_{\sin}x \leq_1 M \wedge (\widehat{\Phi_{\cos}x}) =_1 \Phi_{\cos}x \leq_1 M \wedge -1 \leq_{\mathbb{R}} \Phi_{\sin}x, \Phi_{\cos}x \leq_{\mathbb{R}} 1)$, where $M^1 \in \mathrm{G_2R}^\omega$ is the boundedness function from the representation of $[-1,1]$ (one may take $M := \lambda n^0.j(6(n+1), 3(n+1)-1)$ see [0,1]).

2) $\forall x^0, y^0, q^0(|x -_{\mathbb{Q}} y| \leq_{\mathbb{Q}} q \to |\Phi_{\sin}x -_{\mathbb{R}} \Phi_{\sin}y| \leq_{\mathbb{R}} q \wedge |\Phi_{\cos}x -_{\mathbb{R}} \Phi_{\cos}y| \leq_{\mathbb{R}} q)$.
(2) (together with 1)) asserts that $\Phi_{\sin}$ and $\Phi_{\cos}$ represent functions : $\mathbb{Q} \to [-1,1]$ which are Lipschitz continuous on $\mathbb{Q}$ with Lipschitz constant $\lambda = 1$).

3) $\forall x^0(\Phi_{\sin}(-_{\mathbb{Q}}x) =_{\mathbb{R}} -_{\mathbb{R}}\Phi_{\sin}x \wedge \Phi_{\cos}(-_{\mathbb{Q}}x) =_{\mathbb{R}} \Phi_{\cos}x)$, $\Phi_{\cos}0 =_{\mathbb{R}} 1$.

4) $\forall x^0, y^0(\Phi_{\sin}(x +_{\mathbb{Q}} y) =_{\mathbb{R}} (\Phi_{\sin}x) \cdot_{\mathbb{R}} (\Phi_{\cos}y) +_{\mathbb{R}} (\Phi_{\cos}x) \cdot_{\mathbb{R}} (\Phi_{\sin}y) \wedge$
$\Phi_{\cos}(x +_{\mathbb{Q}} y) =_{\mathbb{R}} (\Phi_{\cos}x) \cdot_{\mathbb{R}} (\Phi_{\cos}y) -_{\mathbb{R}} (\Phi_{\sin}x) \cdot_{\mathbb{R}} (\Phi_{\sin}y))$.
$\forall x^0, y^0(\Phi_{\sin}x -_{\mathbb{R}} \Phi_{\sin}y = 2 \cdot \Phi_{\cos}(\frac{x+_{\mathbb{Q}}y}{2}) \cdot_{\mathbb{R}} \Phi_{\sin}(\frac{x-_{\mathbb{Q}}y}{2}) \wedge$
$\Phi_{\cos}x -_{\mathbb{R}} \Phi_{\cos}y = -2 \cdot \Phi_{\sin}(\frac{x+_{\mathbb{Q}}y}{2}) \cdot_{\mathbb{R}} \Phi_{\sin}(\frac{x-_{\mathbb{Q}}y}{2}))$.

5) $\forall x^0(0 <_{\mathbb{Q}} |x| \to \left|\frac{\Phi_{\sin}x}{x} -_{\mathbb{R}} 1\right| \leq_{\mathbb{R}} \frac{|x|^2}{6})$.
This proposition on sin (which is proved e.g. in [5]) provides a quantitative version of the proposition $\frac{\sin x}{x} \overset{x\to 0}{\to} 1$. Only by this quantitative strengthening the proposition becomes purely universal (and therefore an axiom of $\mathrm{G_2A}^\omega$).

Because of axiom 2) there are unique continuous extensions of the functions : $\mathbb{Q} \to \mathbb{R}$, which are represented by $\Phi_{\sin}, \Phi_{\cos}$, to the whole space $\mathbb{R}$. These extensions are represented by

$$\tilde{\Phi}^{1(1)}_{\sin}x^1 := \lambda k^0.\Phi_{\sin}(\widehat{x}(3(k+1)))(3(k+1)),$$

$$\tilde{\Phi}^{1(1)}_{\cos}x^1 := \lambda k^0.\Phi_{\cos}(\widehat{x}(3(k+1)))(3(k+1)).$$

Remark B.1.1 *1) It is well–known that 2)–5) already characterize* $\sin, \cos$ *(see e.g. [7]).*

2) By the axioms 1) $\Phi_{\sin}$ *and* $\Phi_{\cos}$ *are majorizable by* $\lambda x^0, n^0.j(6(n+1), 3(n+1)-1) \in G_2R^\omega_-$. *Hence theorem 3.2.8 from [15] applies.*

3) In G_3A^ω *we can* **define** *constants* $\Phi'_{\sin}, \Phi'_{\cos}$ *which satisfy (provable in* G_3A^ω*)* $-1 \leq \Phi'_{\sin}x, \Phi'_{\cos}x \leq 1$ *and 2)–5) above using the usual definition via the Taylor expansion of* $\sin$ *and* $\cos$. *If we now define* $\Phi_{\sin}x := (\widetilde{\Phi'_{\sin}x})$ *and* $\Phi_{\cos}x := (\widetilde{\Phi'_{\cos}x})$ *(where* $\lambda y^1.\tilde{y} \in G_2R^\omega$ *is the construction corresponding to our representation of* $[-1,1]$ *such that* $\tilde{y} \leq_1 M$, $y =_{\mathbb{R}} \tilde{y}$ *if* $-1 \leq_{\mathbb{R}} y \leq_{\mathbb{R}} 1$, *and* $-1 \leq_{\mathbb{R}} \tilde{y} \leq_{\mathbb{R}} 1$ *for all* y^1*), then these functionals satisfy 1)–5).*

In the following we will write $\Phi_{\sin}$,$\Phi_{\cos}$ also for $\tilde{\Phi}_{\sin}, \tilde{\Phi}_{\cos}$ since from the type of the argument it will always be clear whether $\Phi_{\sin}$,$\Phi_{\cos}$ or their extensions $\tilde{\Phi}_{\sin}, \tilde{\Phi}_{\cos}$ are meant.

In the following we will introduce $\frac{\pi}{2}$ (and thus π) as the uniquely determined zero of the function cos on $[0,2]$. This is possible since $\Phi_{\cos}0 =_{\mathbb{R}} 1$, $\Phi_{\cos}2 \leq_{\mathbb{R}} -\frac{1}{3}$ and

$$(*)\ \forall x^0, y^0(0 \leq_{\mathbb{Q}} y \leq_{\mathbb{Q}} x \leq_{\mathbb{Q}} 2 \to \Phi_{\cos}x -_{\mathbb{R}} \Phi_{\cos}y \leq_{\mathbb{R}} -\frac{(x -_{\mathbb{Q}} y)^2}{18})$$

are true purely universal assertions on cos (see below for the verification of $(*)$) and hence axioms of $\mathrm{G_2A}^\omega$.
$(*)$ is a uniform quantitative version of the strict monotonicity of cos on $[0,2]$. This strict monotonicity implies the uniqueness and hence (by a general meta–theorem from [11]) the effectivity of the uniquely determined zero of cos $[0,2]$. This can be seen also directly as follows: The quantitative monotonicity $(*)$ immediately yields a modulus of uniqueness (in the sense of [11]) $\omega \in \mathrm{G_2R}^\omega$, namely $\omega(n) := \frac{1}{36(n+1)^2}$ and thus the computability of the zero of cos in $\mathrm{G_2R}^\omega \cup \Phi_{\cos}$:
Let $x_m, x_{\tilde{m}} \in [0,2]$ be such that

$$|\cos x_m|, |\cos x_{\tilde{m}}| < \frac{1}{36(n+1)^2} \text{ and therefore } |\cos x_m - \cos x_{\tilde{m}}| < \frac{1}{18(n+1)^2}.$$

Then –by $(*)$– $|x_m - x_{\tilde{m}}| < \frac{1}{n+1}$, i.e. ω is a modulus of uniqueness. We define a partition of $[0,2]$ by

$$x_i := \frac{i}{3 \cdot 36(n+1)^2} \text{ for } i = 0, \ldots, 6 \cdot 36(n+1)^2$$

and compute for each i a rational $1/(6 \cdot 36(n+1)^2)$–approximation y_i of $|\cos x_i|$. Next we compute an i_n such that

$$|y_{i_n}| = \min\left\{|y_i| : i = 0, \ldots, 6 \cdot 36(n+1)^2\right\}.$$

It follows

$$|\cos(x_{i_n})| \leq \min_{i \leq 6 \cdot 36(n+1)^2} |\cos x_i| + \frac{1}{3 \cdot 36(n+1)^2} \leq \inf_{x \in [0,2]} |\cos x| + \frac{2}{3 \cdot 36(n+1)^2} < \frac{1}{36(n+1)^2}.$$

Hence (x_{i_n}) is a Cauchy sequence in $[0,2]$ with Cauchy modulus $1/(n+1)$. (x_{i_n}) can be computed by a term t^1 in $\mathrm{G_2R}^\omega \cup \Phi_{\cos}$. Therefore we may define $\pi :=_1 2 \cdot_{\mathbb{R}} t$.

The following propositions on $\pi, \Phi_{\sin}, \Phi_{\cos}$ are purely universal and therefore axioms of $\mathrm{G_2A}^\omega$:

1) $2 \leq_{\mathbb{R}} \pi \leq_{\mathbb{R}} 4,\ \Phi_{\cos}(\frac{\pi}{2}) =_{\mathbb{R}} 0.$

2) $\forall x^1(\Phi_{\cos}(x +_{\mathbb{R}} 2\pi) =_{\mathbb{R}} \Phi_{\cos}x \wedge \Phi_{\sin}(x +_{\mathbb{R}} 2\pi) =_{\mathbb{R}} \Phi_{\sin}x \wedge$
$\Phi_{\cos}(x +_{\mathbb{R}} \pi) =_{\mathbb{R}} -\Phi_{\cos}x \wedge \Phi_{\sin}(x +_{\mathbb{R}} \pi) =_{\mathbb{R}} -\Phi_{\sin}x \wedge$
$\Phi_{\cos}x =_{\mathbb{R}} \Phi_{\sin}(\frac{\pi}{2} -_{\mathbb{R}} x) \wedge \Phi_{\sin}x =_{\mathbb{R}} \Phi_{\cos}(\frac{\pi}{2} -_{\mathbb{R}} x)).$

3) Uniform quantitative strict monotonicity:
$\forall x^0, y^0((0 \leq_{\mathbb{Q}} y \leq_{\mathbb{Q}} x \leq_{\mathbb{Q}} 4 \to \Phi_{\cos}(\tilde{x}) -_{\mathbb{R}} \Phi_{\cos}(\tilde{y}) \leq_{\mathbb{R}} -\frac{(\tilde{x} -_{\mathbb{R}} \tilde{y})^2}{18}) \wedge$
$(-2 \leq_{\mathbb{Q}} y \leq_{\mathbb{Q}} x \leq_{\mathbb{Q}} 2 \to \Phi_{\sin}(\check{x}) -_{\mathbb{R}} \Phi_{\sin}(\hat{y}) \geq_{\mathbb{R}} \frac{(\check{x} -_{\mathbb{R}} \hat{y})^2}{18})),$
where $\tilde{z} := \min_{\mathbb{R}}(z, \pi)$, $\check{z} := \min_{\mathbb{R}}(z, \pi/2)$ and $\hat{z} := \max_{\mathbb{R}}(z, -\pi/2)$.

3) implies (together with 1) and the continuity of $\cos, \sin$):

$$3)'\ \forall x^1, y^1((0 \leq_{\mathbb{R}} y \leq_{\mathbb{R}} x \leq_{\mathbb{R}} \pi \to \Phi_{\cos}(x) -_{\mathbb{R}} \Phi_{\cos}(y) \leq_{\mathbb{R}} -\tfrac{(x -_{\mathbb{R}} y)^2}{18}) \wedge$$
$$(-\tfrac{\pi}{2} \leq_{\mathbb{R}} y \leq_{\mathbb{R}} x \leq_{\mathbb{R}} \tfrac{\pi}{2} \to \Phi_{\sin}(x) -_{\mathbb{R}} \Phi_{\sin}(y) \geq_{\mathbb{R}} \tfrac{(x -_{\mathbb{R}} y)^2}{18})).$$

The reason for our somewhat complicated formulation 3) instead of 3)' is that 3) is in Π^0_1 (in contrast to 3)').
Proof of 3)' (and hence of 3) and $(*)$ above):
Since $\sin z \geq \frac{z}{3}$ for all $z \in [0, 2]$ (see e.g. [5]), we obtain for all x, y such that $0 \leq y \leq x \leq \frac{\pi}{2}$:

$$\cos x - \cos y = -2\sin(\frac{x+y}{2})\sin(\frac{x-y}{2}) \leq -2(\frac{x+y}{6})(\frac{x-y}{6}) \leq -\frac{(x-y)^2}{18}.$$

Because of $\cos x = -\cos(\pi - x)$, the claim follows for $x, y \in [0, \frac{\pi}{2}]$ and $x, y \in [\frac{\pi}{2}, \pi]$. Now assume that $x \geq \frac{\pi}{2} \wedge y \leq \frac{\pi}{2}$: Then
$\cos x - \cos y = \cos x - \cos\frac{\pi}{2} + \cos\frac{\pi}{2} - \cos y \leq -2(\frac{x^2-y^2}{36}) \leq -\frac{(x-y)^2}{18}$. Put together this yields the claim for $[0, \pi]$.
By $\sin x = -\cos(\frac{\pi}{2} + x)$ the corresponding claim for sin follows.

Remark B.1.2 The proof of 3)' above can be conceived as an instance of theorem 3.3 (of course a very simple one): When formalized within $\mathrm{G_2A}^\omega$, the strict monotonicity of cos has (modulo a suitable prenexation) the logical form

$$(+)\ \forall x, y \leq_1 M_\pi, k^0 \exists n^0(\underbrace{x \geq_{\mathbb{R}} y + \frac{1}{k+1} \to \Phi_{\cos}x - \Phi_{\cos}y <_{\mathbb{R}} -\frac{1}{n+1}}_{\equiv: A \in \Sigma^0_1 (\text{modulo prenexation})}).$$

Since $(+)$ is provable in $\mathrm{G_2A}^\omega$, theorem 3.3 implies the extractability of a polynomial pk providing a bound on n which does not depend on x, y. Since A is monotone w.r.t. n, this

bound in fact realizes '$\exists n$', i.e.

$$\mathrm{G_2A}^\omega \vdash \forall x, y \in [0,\pi], k^0(x \geq_{\mathbb{R}} y + \frac{1}{k+1} \to \Phi_{\cos} x - \Phi_{\cos} y <_{\mathbb{R}} -\frac{1}{pk+1}).$$

Our proof of 3)' yields $pk := 18(k+1)^2$. The majorization used in this proof to eliminate the dependence on x, y is simply the inequality

$$(x+y)(x-y) \geq (x-y)^2 \geq \frac{1}{(k+1)^2} \text{ for } x \geq y + \frac{1}{k+1} \geq \frac{1}{k+1}.$$

The **tangent** function $\tan x := \frac{\sin x}{\cos x}$ is represented by a term $\Phi^{1(0)(1)}_{\tan} \in \mathrm{G_2R}^\omega \cup \{\Phi_{\sin}, \Phi_{\cos}\}$ such that

$$\forall x^1, n^0(-\frac{\pi}{2} + \frac{1}{n+1} \leq_{\mathbb{R}} x \leq_{\mathbb{R}} \frac{\pi}{2} - \frac{1}{n+1} \to \Phi_{\tan} x n =_{\mathbb{R}} \frac{\Phi_{\sin} x}{\Phi_{\cos} x}).$$

B.2 The functions arcsin, arccos and arctan in $\mathbf{G_2A}^\omega$

As we have seen above, $\sin x$ is strictly monotone on $[-\frac{\pi}{2}, \frac{\pi}{2}]$ with the 'modulus of uniform strict monotonicity' $\omega(\varepsilon) := \frac{\varepsilon^2}{18}$. Since $\sin x$ has the Lipschitz constant $\lambda = 1$, $\forall y \in [-1,1] \exists x \in [-\frac{\pi}{2}, \frac{\pi}{2}](\sin x = y)$ implies

$$(*)\ \forall y \in [-1,1], n \in \mathbb{N} \exists r_n \in \{q_1, \ldots, q_{l_n}\}(|\sin r_n - y| \leq \frac{1}{n+1}),$$

where $\{q_1, \ldots, q_{l_n}\} \subset [-\frac{\pi}{2}, \frac{\pi}{2}] \cap \mathbb{Q}$ is a $1/(n+1)$–net for $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Similarly to the function M used in our representation of $[0,1]$ one constructs a function $M_\pi \in \mathrm{G_2R}^\omega$ such that $\{i : i \leq_0 M_\pi n\}$ contains (modulo our coding of $\mathbb{Q}$) such a $1/(n+1)$–net (e.g. $M_\pi n := j(8(n+1), n)$). $(*)$ implies

$$\forall y \leq_1 M, n^0 \exists q \leq_0 M_\pi n((\widehat{-\frac{\pi}{2}})(n) + \frac{1}{n+1} \leq_{\mathbb{Q}} q \leq_{\mathbb{Q}} (\frac{\widehat{\pi}}{2})(n) - \frac{1}{n+1} \wedge |\Phi_{\sin} q -_{\mathbb{R}} \tilde{y}| \leq_{\mathbb{R}} \frac{3}{n+1})^8$$

and therefore

$$\forall y \leq_1 M, n^0 \exists q \leq_0 M_\pi n$$
$$((\widehat{-\tfrac{\pi}{2}})(n) + \tfrac{1}{n+1} \leq_{\mathbb{Q}} q \leq_{\mathbb{Q}} (\tfrac{\widehat{\pi}}{2})(n) - \tfrac{1}{n+1} \wedge |(\Phi_{\sin} q)(n) -_{\mathbb{Q}} \tilde{y}(n)| \leq_{\mathbb{Q}} \tfrac{5}{n+1}).$$

[8] Here again $\lambda y^1.\tilde{y} \in \mathrm{G_2R}^\omega$ is the construction corresponding to our representation of $[-1,1]$ such that $\tilde{y} \leq_1 M$, $y =_{\mathbb{R}} \tilde{y}$ if $-1 \leq_{\mathbb{R}} y \leq_{\mathbb{R}} 1$, and $-1 \leq_{\mathbb{R}} \tilde{y} \leq_{\mathbb{R}} 1$ for all y^1.

Bounded μ–search provides a functional $\tilde{\Psi}^{1(1)} \in \mathrm{G_2R}^\omega \cup \{\Phi_{\sin}\}$ such that

$$\forall y \leq_1 M, n^0$$
$$((\widehat{-\tfrac{\pi}{2}})(n) + \tfrac{1}{n+1} \leq_{\mathbb{Q}} \tilde{\Psi} yn \leq_{\mathbb{Q}} (\widehat{\tfrac{\pi}{2}})(n) - \tfrac{1}{n+1} \wedge |\Phi_{\sin}(\tilde{\Psi} yn))(n) -_{\mathbb{Q}} \tilde{y}(n)| \leq_{\mathbb{Q}} \tfrac{5}{n+1})$$

and therefore

$$\forall y \leq_1 M, n^0((\widehat{-\frac{\pi}{2}})(n) + \frac{1}{n+1} \leq_{\mathbb{Q}} \tilde{\Psi} yn \leq_{\mathbb{Q}} (\frac{\widehat{\pi}}{2})(n) - \frac{1}{n+1} \wedge |\Phi_{\sin}(\tilde{\Psi} yn) -_{\mathbb{R}} \tilde{y}| \leq_{\mathbb{R}} \frac{7}{n+1})$$

Hence for $\Psi yn := \tilde{\Psi} y(7 \cdot 36(n+1)^2)$

$$\forall y \in [-1,1], n \in \mathbb{N}(|\Phi_{\sin}(\Psi yn) -_{\mathbb{R}} \tilde{y}| < \frac{1}{36(n+1)^2}).$$

From the fact that $\omega(\varepsilon)$ is a modulus of strict monotonicity for sin we obtain that $(\Psi yn)_{n\in\mathbb{N}}$ is a Cauchy sequence in $[-\frac{\pi}{2}, \frac{\pi}{2}]$ with Cauchy modulus $1/(n+1)$: Suppose that $m, \tilde{m} \geq_0 n$, then

$$|\Phi_{\sin}(\Psi ym) - \Phi_{\sin}(\Psi y\tilde{m})| \leq |\Phi_{\sin}(\Psi ym) - \tilde{y}| + |\tilde{y} - \Phi_{\sin}(\Psi y\tilde{m})| < \frac{1}{18(n+1)^2}$$

and therefore $|\Psi ym -_{\mathbb{Q}} \Psi y\tilde{m}| < \frac{1}{n+1}$.
Hence $\Phi_{\arcsin} y := \Psi \tilde{y}$ represents the inverse function of sin on $[-\frac{\pi}{2}, \frac{\pi}{2}]$ and is uniformly continuous on $[-1,1]$ with ω as a modulus of uniform continuity.
The inverse arccos of cos on $[0,\pi]$ is defined analogously.
Similarly to arcsin, arccos one can finally define arctan in $\mathrm{G_2A}^\omega$.

B.3 The exponential functions $\exp_n$ and $\exp$ in $\mathbf{G_2A}^\omega$ and $\mathbf{G_3A}^\omega$

Since all terms $t^1 \in \mathrm{G_2R}^\omega$ are bounded by a polynomial (see [15],prop.2.2.29) it is clear that exp can neither be defined in $\mathrm{G_2A}^\omega$ nor can exp be represented by a new function constant which is majorized by a term from $\mathrm{G_2R}^\omega$. However for every **fixed** number $n \geq_0 1$ we can introduce the restriction of exp to $[-n,n](\subset \mathbb{R})$ by such a constant. This means that we can deal locally with exp in $\mathrm{G_2A}^\omega$ and e.g. may use exp for the solution of ordinary differential equations etc.

We add to $\mathrm{G_2A}^\omega$ a function constant $\Phi^{1(0)}_{\exp_n}$ which is intended to represent the restriction of exp on $[-n,n] \cap \mathbb{Q}$. Since exp is Lipschitz continuous on $[-n,n]$ with a Lipschitz constant

e.g. $\lambda := 3^n$, we have the following universal axioms on $\Phi^{1(0)}_{\exp_n}$ in $\mathrm{G_2A}^\omega$[9]

$$(1)\ \forall x^0(\widehat{\Phi_{\exp_n}}x =_1 \Phi_{\exp_n}x \leq_1 M_n \wedge 0 \leq_{\mathbb{R}} \Phi_{\exp_n}x \leq_{\mathbb{R}} 3^n),$$

where M_n is the boundedness function used in the representation of $[0, 3^n]$ (e.g. $M_n(k) := j(6 \cdot 3^n(k+1), 3(k+1)-1)$).[10]

$$(2)\ \forall x^0, y^0, q^0(-n \leq_{\mathbb{Q}} x, y \leq_{\mathbb{Q}} n \wedge |x -_{\mathbb{Q}} y| \leq_{\mathbb{Q}} \frac{q}{3^n} \to |\Phi_{\exp_n}x -_{\mathbb{R}} \Phi_{\exp_n}y| \leq_{\mathbb{R}} q).$$

As in the case of $\Phi_{\sin}$, by (2) we can extend $\Phi_{\exp_n}$ to a constant $\tilde{\Phi}^{1(1)}_{\exp_n} \in \mathrm{G_2R}^\omega$ which represents the continuation of the function represented by $\Phi_{\exp_n}$ to $[-n, n]$. As for $\Phi_{\sin}$ we will denote this extension also by $\Phi_{\exp_n}$. The most important properties of exp (restricted on $[-n, n]$) can be expressed by purely universal sentences and thus are axioms of $\mathrm{G_2A}^\omega$:

$$(3)\ \forall x^0, y^0(-n \leq_{\mathbb{Q}} y \leq_{\mathbb{Q}} x \leq_{\mathbb{Q}} n \to \int_y^x (\Phi_{\exp_n}t)dt =_{\mathbb{R}} \Phi_{\exp_n}x -_{\mathbb{R}} \Phi_{\exp_n}y),\ \Phi_{\exp_n}0 =_{\mathbb{R}} 1,$$

$$(4)\ \forall x^0, y^0(-n \leq_{\mathbb{Q}} x, y, x +_{\mathbb{Q}} y \leq_{\mathbb{Q}} n \to \Phi_{\exp_n}(x +_{\mathbb{Q}} y) =_{\mathbb{R}} \Phi_{\exp_n}(x) \cdot_{\mathbb{R}} \Phi_{\exp_n}(y)).$$

By the continuity of $\Phi_{\exp_n}$, (3) and (4) immediately generalize to real arguments. Furthermore by the theorem that the derivative of $\int_0^x f(x)dx$ is f (which can be expressed as a universal axiom in $\mathrm{G_2A}^\omega$), (3) implies

$$(3)'\ \forall x^1(-n \leq_{\mathbb{R}} x \leq_{\mathbb{R}} n \to \Phi'_{\exp_n}x =_{\mathbb{R}} \Phi_{\exp_n}x),\ \text{where } ' \text{ denotes the derivative.}$$

In contrast to $\mathrm{G_2A}^\omega$ we can define the unrestricted exponential function in $\mathrm{G_3A}^\omega$ as usual via the exponential series:[11] one easily defines the sequence of partial sums of this series for rational arguments. From the quotient criterion one gets the convergence of this series together with a modulus of convergence. By the continuity of this series in $x \in \mathbb{R}$ with the modulus
$\omega(x, n) := 3^{\lceil |\widehat{x}(0)|+1 \rceil} \cdot (n+1)$ we can continue it on $\mathbb{R}$.

Analogously to the definition of arcsin we can define the inverse function $\ln_n$ of $\exp_n$ using the fact that e.g. $\omega(\varepsilon) := \varepsilon \cdot 3^{-n}$ is a modulus of strict monotonicity for $\exp_n$ on $[-n, n]$.

[9] As in the case of $\Phi_{\sin}$ and $\Phi_{\cos}$ we denote (according to the discussion in connection with theorem 3.2.8 in [15]) $\mathrm{G_2A}^\omega \cup \{\Phi^{1(0)}_{\exp_n}\}$ also by $\mathrm{G_2A}^\omega$

[10] For notational simplicity we identify in the following the natural number n with its code $j(2n, 0)$ as a rational number, e.g. we write $x^0 \leq_{\mathbb{Q}} n$ instead of $x^0 \leq_{\mathbb{Q}} j(2n, 0)$ in order to express that the rational number which is coded by x is $\leq$ the natural number n.

[11] In particular we can define a term $\Phi_{\exp_n}$ in $\mathrm{G_3A}^\omega$ which satisfies (provably) (1)–(4).

In this appendix we have seen that $\sin, \cos$ can be introduced relatively to $\mathrm{G_2A}^\omega$ via new constants $\Phi^{1(0)}_{\sin}, \Phi^{1(0)}_{\cos}$ and purely universal axioms which express the usual (characterizing) properties of $\sin, \cos$. $\tan$ and the inverse functions $\arcsin, \arccos, \arctan$ of $\sin, \cos, \tan$ as well as π can be defined in $\mathrm{G_2A}^\omega$ using $\Phi_{\sin}, \Phi_{\cos}$. Furthermore for each **fixed** $n \in \mathbb{N}$ the restriction $\exp_n$ of the exponential function $\exp$ to $[-n, n]$ can be introduced relatively to $\mathrm{G_2A}^\omega$ via a new constant $\Phi^{1(0)}_{\exp_n}$ and its characterizing properties can be expressed as universal axioms. Thus by theorem 3.2.8 from [15] the use of $\sin, \cos, \tan, \arcsin, \arccos, \arctan, \pi$ and the **local** use of $\exp$ only contributes to the growth of provably functionals by majorants $\in \mathrm{G_2R}^\omega$ for the constants $\Phi^{1(0)}_{\sin}, \Phi^{1(0)}_{\cos}, \Phi^{1(0)}_{\exp_n}$ and the terms used in the formulation of their universal axioms and in the definition of $\pi, \arcsin, \arccos, \arctan$.

Recent BRICS Report Series Publications

RS-97-30 **Ulrich Kohlenbach.** ***Proof Theory and Computational Analysis*****. November 1997. 38 pp.**

RS-97-29 **Luca Aceto, Augusto Burgueño, and Kim G. Larsen.** ***Model Checking via Reachability Testing for Timed Automata*****. November 1997. 29 pp.**

RS-97-28 **Ronald Cramer, Ivan B. Damgård, and Ueli Maurer.** ***Span Programs and General Secure Multi-Party Computation*****. November 1997. 27 pp.**

RS-97-27 **Ronald Cramer and Ivan B. Damgård.** ***Zero-Knowledge Proofs for Finite Field Arithmetic or: Can Zero-Knowledge be for Free?*** **November 1997. 33 pp.**

RS-97-26 **Luca Aceto and Anna Ingólfsdóttir.** ***A Characterization of Finitary Bisimulation*****. October 1997. 9 pp. To appear in** ***Information Processing Letters*****.**

RS-97-25 **David A. Mix Barrington, Chi-Jen Lu, Peter Bro Miltersen, and Sven Skyum.** ***Searching Constant Width Mazes Captures the*** AC^0 ***Hierarchy*****. September 1997. 20 pp. To appear in** ***STACS '98: 15th Annual Symposium on Theoretical Aspects of Computer Science Proceedings*****, LNCS, 1998.**

RS-97-24 **Søren B. Lassen.** ***Relational Reasoning about Contexts*****. September 1997. 45 pp. To appear as a chapter in the book** ***Higher Order Operational Techniques in Semantics*****, eds. Andrew D. Gordon and Andrew M. Pitts, Cambridge University Press.**

RS-97-23 **Ulrich Kohlenbach.** ***On the Arithmetical Content of Restricted Forms of Comprehension, Choice and General Uniform Boundedness*****. August 1997. 35 pp.**

RS-97-22 **Carsten Butz.** ***Syntax and Semantics of the logic*** $\mathcal{L}^{\lambda}_{\omega\omega}$**. July 1997. 14 pp.**

RS-97-21 **Steve Awodey and Carsten Butz.** ***Topological Completeness for Higher-Order Logic*****. July 1997. 19 pp.**

RS-97-20 **Carsten Butz and Peter T. Johnstone.** ***Classifying Toposes for First Order Theories*****. July 1997. 34 pp.**