THE JOURNAL OF SYMBOLIC LOGIC
Volume 00, Number 0, XXX 0000

GROUNDWORK FOR WEAK ANALYSIS

ANTÓNIO M. FERNANDES AND FERNANDO FERREIRA

Abstract. This paper develops the very basic notions of analysis in a weak second-order theory of arithmetic BTFA whose provably total functions are the polynomial time computable functions. We formalize within BTFA the real number system and the notion of a continuous real function of a real variable. The theory BTFA is able to prove the intermediate value theorem, wherefore it follows that the system of real numbers is a real closed ordered field. In the last section of the paper, we show how to interpret the theory BTFA in Robinson's theory of arithmetic Q. This fact entails that the elementary theory of the real closed ordered fields is interpretable in Q.

§1. Introduction. The formalization of mathematics within second-order arithmetic has a long and distinguished history. We may say that it goes back to Richard Dedekind, and that it has been pursued by, among others, Hermann Weyl, David Hilbert, Paul Bernays, Harvey Friedman, and Stephen Simpson and his students (we may also mention the insights of Georg Kreisel, Solomon Feferman, Peter Zahn and Gaisi Takeuti). Stephen Simpson's recent *magnum opus* "Subsystems of Second Order Arithmetic" [23] – claiming to be a continuation of Hilbert/Bernays "Grundlagen der Mathematik" [13] – provides the state of the art of the subject, with an emphasis on calibrating the logico-mathematical strength of various theorems of ordinary mathematics. It is also a superb reference for the pertinent bibliography. The weakest second-order system studied in Simpson's book is RCA_0, a theory whose provably total functions are the primitive recursive functions. Scant attention has been paid to weaker systems and, in particular, to systems related to conspicuous classes of computational complexity. The exceptions that we found in the literature are some papers of Simpson and his students on algebraic questions within a second-order theory related to the elementary functions (see [25], [12] and [24]), Ferreira's work on second-order theories related to polynomial time computability ([5] and [8]), and subsequent papers by Andrea Cantini [4] and Takeshi Yamazaki [29], [28]. In a different setting, viz. finite type arithmetic, we should also mention Ulrich Kohlenbach's

2000 *Mathematics Subject Classification.* Primary: 03F35; Secondary: 03B30.
Key words and phrases. Weak analysis, polytime computability, interpretability.
Both authors were partially supported by CMAF (Fundação para a Ciência e Tecnologia, Portugal). The results of the last section were obtained by the second-named author.

0022-4812/00/0000-0000/$00.00

single-handed work in "proof mining" where concerned with theories related to the various Grzegorczyk classes (e.g., [17], [18] and [19]).

This work is an essay on a subject that we may call *weak analysis*: the formalization and study of mathematics in weak (i.e., mainly sub-exponential) subsystems of second-order arithmetic. More specifically, in this paper we study the formalization of the very basic ideas of analysis in a feasible theory, that is, in a theory whose provably total functions (with appropriate graphs) are the polynomial time computable functions. Plainly, the work of Harvey Friedman and Ker-I Ko on the complexity of computations on the reals – as exposed in [16] – is bound to be of great importance for the pursuit of weak analysis, comparable to the importance of recursive analysis as a well-spring of ideas and constructions for the development of analysis over RCA_0. That not withstanding, the import of Friedman and Ko's work in the present paper is not yet apparent.

In section 2, we briefly review and discuss the *base theory for feasible analysis* BTFA introduced by Ferreira in [8]: this is the second-order theory of arithmetic that shall concern us here. In section 3, we define the real number system within BTFA to the point where it is shown that it forms an ordered field. The following section deals with continuous functions and proves, within BTFA, the intermediate value theorem for continuous real functions of a real variable. As a consequence, the real number system forms a real closed ordered field, provably in BTFA.

The last section shows that the theory BTFA is interpretable in Raphael Robinson's theory of arithmetic Q. This result, together with the fact that the elementary theory of the real closed ordered fields RCOF is interpretable in BTFA, entails that RCOF is interpretable in Q (Harvey Friedman has also claimed this latter result – albeit without giving a proof – in a well-known web discussion forum for the foundations of mathematics: see [10]). *Prima facie*, this is a somewhat surprising result. After all, RCOF is a theory whose intended model is the *continuum* of real numbers, strong enough for the development of all analytic geometry, whereas the theory Q purports to speak very sparingly (since no induction is present in its axioms) about the natural numbers. Q is the usual textbook example (e.g., [1]) of a finitely axiomatizable, essentially undecidable, theory. On the other hand, RCOF is a decidable theory – this being an old and famous result of Tarski [27]. Therefore, Robinson's Q is not interpretable in RCOF. Summing up: the theory RCOF is, in a precise sense, proof theoretically weaker than Q.

What are we to make of the interpretability of RCOF in Q? Is this a freak and isolated phenomenon? The proof that we present in this paper clearly indicates that this is *not* the case. It is rather the conjugation of the facts that many bounded theories of arithmetic (in which the totality of exponentiation fails) are interpretable in Q, and that a *modicum* of analysis can be done over theories which are interpretable in one of these bounded theories. How extensive is this *modicum*? On this regard, BTFA is a case in point: the more analysis you do in BTFA, the more analysis you interpret in Q. We should remark that the reals that we construct inside BTFA are not *merely* models of RCOF: They have a canonical integer part whose positive elements are (essentially) given by the first-order part of BTFA, thus assenting to a pertinent induction principle. Presumably, BTFA is sufficient for the development of some transcendental function theory, but insufficient for developing Riemannian integration for (general) continuous functions with a modulus of uniform continuity. However, stronger theories than BTFA, still interpretable in Q, should be able to develop Riemannian integration and more. We suspect that the amount of analysis that can be done in weak systems of second-order arithmetic – even in feasible systems – is mathematically significant, and far from trivial. These matters, we are convinced, are well worth further studying.

§2. A base theory for feasible analysis. A language for directly describing finite sequences of zeros and ones (as opposed to a number theoretic language) is specially perspicuous for dealing with sub-exponential complexity classes and, in particular, for dealing with polynomial time computability. The second-order theory BTFA is stated in such a language, and it is based on the first-order theory Σ^b_1−NIA ('NIA' stands for *notation induction axioms*). The language $\mathcal{L}$ of Σ^b_1−NIA consists of three constant symbols ϵ, 0 and 1, two binary function symbols $\frown$ (for *concatenation*, usually omitted) and $\times$, and a binary function symbol $\subseteq$ (for *initial subwordness* or *prefixing*). The standard structure for this language has domain $2^{<\omega}$, the set of finite sequences of zeros and ones (binary words or strings), and interprets the symbols of $\mathcal{L}$ in the usual way ($x \times y$ is the word x concatenated with itself length of y times). The axioms of the theory Σ^b_1−NIA consist of fourteen open axioms governing some basic features of the given constants, operations and relations (see [8] for the list) together with the scheme of induction on notation for the so-called Σ^b_1-formulas. Let us briefly describe these formulas and this kind of induction.

The class of *subword quantification* formulas (sw.q.-formulas, for short) is the smallest class of formulas that contains the atomic formulas and that is closed under Boolean connectives and *subword* or *part-of* quantifications, i.e., quantifications of the form $\forall x(x \subseteq^* t \to \phi)$ or $\exists x(x \subseteq^* t \wedge \phi)$, where $x \subseteq^* t$ abbreviates the formula $\exists z(z \frown x \subseteq t)$. The Σ^b_1*-formulas* are the formulas of the form $\exists x(x \preccurlyeq t \wedge \phi)$, where ϕ is a sw.q.-formula and $x \preccurlyeq t$ abbreviates $1 \times x \subseteq 1 \times t$ (i.e., the length of x is less than or equal to the length of t). The Σ^b_1-formulas define exactly the NP predicates in the standard model (see [5] for a proof of this). The scheme of induction on notation for Σ^b_1-predicates consists of all formulas of the form

$$\text{(NIA)} \qquad \phi(\epsilon) \wedge \forall x(\phi(x) \to \phi(x0) \wedge \phi(x1)) \to \forall x\, \phi(x),$$

where ϕ is a Σ^b_1-formula, possibly with parameters. The theory Σ^b_1−NIA is interpretable in Buss' well-known theory S^1_2, and *vice-versa*. With one such smooth interpretation in mind, it is possible to appeal to Buss' main theorem of [3] and infer the following property: whenever Σ^b_1−NIA proves the sentence $\forall x \exists y \phi(x, y)$, where $\phi(x, y)$ a Σ^b_1-formula, there is a polynomial time computable function $f : 2^{<\omega} \mapsto 2^{<\omega}$ such that, for all $\sigma \in 2^{<\omega}$, $\phi(\sigma, f(\sigma))$ (see [6] or [2] for a direct proof of this result). This is the precise sense of saying that the provably total functions of Σ^b_1−NIA are the polynomial time computable functions.

It is possible to extend by definitions the language $\mathcal{L}$ in order to obtain a language $\mathcal{L}_P$ with a function symbol for every (description of a) polynomial time computable function – this extension by definitions is carefully described in [5] and in [6]. If this is done in the right way, the above induction scheme (NIA) holds even if we include the new atomic formulas of $\mathcal{L}_P$ in the definition of sw.q.-formulas (for the sake of clarity, let us call the members of this extended class the *PTC formulas*). Unless otherwise stated (by a harmless abuse of language), we will henceforth assume that the theory $\Sigma^b_1-\mathsf{NIA}$ includes the function symbols of $\mathcal{L}_P$ and appropriate open axioms regulating them.

We say that a word x is *tally* if it is a sequence of ones (formally, if $x = 1 \times x$). The tally part of a model of $\Sigma^b_1-\mathsf{NIA}$ is a model of the bounded arithmetical theory $\mathsf{I}\Delta_0$ in a natural way: zero is given by ϵ, successor $'$ by concatenation with 1, addition $+$ by concatenation, multiplication by $\times$, and the less than or equal relation by $\subseteq$ ([11] is a good reference for first-order theories of arithmetic, including bounded theories). In general, one has the following form of induction, called *tally induction*:

$$\phi(\epsilon) \wedge \forall x(x \text{ is tally} \wedge \phi(x) \to \phi(x')) \to \forall x(x \text{ is tally} \to \phi(x)),$$

where ϕ is a Σ^b_1-formula. Using well-known tricks, it can be shown that the following *least tally number principle* is a consequence of the the above tally induction scheme:

$$\forall z(z \text{ is tally} \wedge \phi(z) \to \exists x \subseteq z(\phi(x) \wedge \forall w \subset x \neg\phi(w))),$$

where ϕ is a Σ^b_1-formula, and $w \subset x$ abbreviates $w \subseteq x \wedge w \neq x$. Note that the bounded formulas of the language of tally arithmetic correspond exactly to the sw.q.-formulas (of $\mathcal{L}$) and, thus, are *included* in the above tally induction scheme (and in the least tally number principle). In fact, the tally parts of models of $\Sigma^b_1-\mathsf{NIA}$ are more than mere models of $\mathsf{I}\Delta_0$: they basically are models of Buss' theory V^1_1 (this is an instance of the so-called RSUV-isomorphisms – see [9], [21] or [26]).

The second-order language $\mathcal{L}_2$ that shall concern us in this paper extends the language $\mathcal{L}$ with set variables $X, Y, Z, \ldots$, intended to vary over subsets of $2^{<\omega}$. $\mathcal{L}_2$ has a binary relation symbol for the membership relation $\in$ that infixes between a term t of $\mathcal{L}$ and a second-order variable X, yielding the atomic formula $t \in X$. Equality between second-order variables is not a primitive notion, rather being defined by extensionality. Observe that the set-up of $\mathcal{L}_2$ is very much in the spirit of the treatment of second-order arithmetic in Stephen Simpson's book [23]. A structure for $\mathcal{L}_2$ is a pair consisting of a structure for the first-order part of $\mathcal{L}_2$ (i.e., a structure for $\mathcal{L}$), together with a subset $\mathcal{S}$ of the power set of the domain of that structure. The second-order variables range over $\mathcal{S}$. In the sequel, when speaking of a given $\mathcal{L}_2$-structure, we use the letter $\mathbb{W}$ (for *words*) to denote its first-order domain. The tally part of $\mathbb{W}$ is denoted by $\mathbb{T}$.

The class of Σ^b_1-formulas of $\mathcal{L}_2$ is defined as in the first-order case, except that it has a wider class of atomic formulas to reckon with (namely, the formulas of the form $t \in X$). In other words, Σ^b_1-formulas of $\mathcal{L}_2$ may have set parameters. A technically important class of $\mathcal{L}_2$-formulas is the class of *bounded formulas* or Σ^b_∞*-formulas*: this is the smallest class of formulas containing the sw.q.-formulas and closed under bounded quantifications, i.e., quantifications of the form $\forall x(x \preccurlyeq t \to \phi)$ or $\exists x(x \preccurlyeq t \wedge \phi)$. With this notion of bounded formulas, we may speak (as usual) of Π^0_1, Σ^0_1, Π^0_2 formulas, etc. The scheme of bounded collection $B\Sigma^b_\infty$ consists of the formulas:

$$\forall x \preccurlyeq z\, \exists y\, \phi(x,y) \to \exists w\, \forall x \preccurlyeq z\, \exists y \preccurlyeq w\, \phi(x,y),$$

where ϕ is a bounded formula, possibly with first and second-order parameters. The comprehension scheme Δ^0_1(PT)-CA consists of:

$$\forall x(\exists y \phi(x,y) \leftrightarrow \forall y \neg\psi(x,y)) \to \exists X \forall x(x \in X \leftrightarrow \exists y \phi(y,x)),$$

where ϕ and ψ are Σ^b_1-formulas, possibly with first and second-order parameters.

Definition 1. BTFA is the theory of $\mathcal{L}_2$ having the following axioms: the fourteen basic open axioms, the scheme of induction on notation (NIA) for the Σ^b_1-formulas of $\mathcal{L}_2$, the scheme of bounded collection, and the comprehension scheme Δ^0_1(PT)-CA.

The following theorem was proved in [8]:

Theorem 1. *The theory* BTFA *is Π^0_2-conservative over the theory* Σ^b_1−NIA.

The reader should observe that the quantifiers $\exists y$ and $\forall y$ appearing in the Δ^0_1(PT)-CA scheme are *unbounded*. This is extremely convenient for dealing with functions in our setting. In our setting, a function $f : X \mapsto Y$ is given by the appropriate set of (codes of) ordered pairs. One can state $f(x) \in Z$ in two ways: by $x \in X \wedge \exists y((x,y) \in f \wedge y \in Z)$, or by $x \in X \wedge \forall y((x,y) \in f \to y \in Z)$. Thus, $\{x \in X : f(x) \in Z\}$ is a set in our framework. The composition of two functions $f : X \mapsto Y$ and $g : Y \mapsto Z$ is also a function since $gf(x) = z$ iff $x \in X \wedge \exists y((x,y) \in f \wedge (y,z) \in g)$ iff $x \in X \wedge \forall y((x,y) \in f \to (y,z) \in g)$.

Using the Σ^b_1-induction on notation scheme, it is easy to see that BTFA allows definition of functions by bounded recursion on notation. That is, given functions $f : \mathbb{W}^k \mapsto \mathbb{W}$, $g_0 : \mathbb{W}^{k+2} \mapsto \mathbb{W}$, $g_1 : \mathbb{W}^{k+2} \mapsto \mathbb{W}$ and $b : \mathbb{W}^{k+1} \mapsto \mathbb{W}$, there is a unique function $h : \mathbb{W}^{k+1} \mapsto \mathbb{W}$ defined by

$$\begin{aligned} h(0, x_1, \ldots, x_k) &= f(x_1, \ldots, x_k) \\ h(z0, x_1, \ldots, x_k) &= g_0(h(z, x_1, \ldots, x_k), z, x_1, \ldots, x_k) \upharpoonleft_{b(z,x_1,\ldots,x_k)} \\ h(z1, x_1, \ldots, x_k) &= g_1(h(z, x_1, \ldots, x_k), z, x_1, \ldots, x_k) \upharpoonleft_{b(z,x_1,\ldots,x_k)} \end{aligned}$$

where $w \upharpoonleft_b$ is the truncation of the word w at the length of the word b. Note that first and second-order parameters may appear in the definition above.

Let $\phi(x)$ be a formula of $\mathcal{L}_2$ with a distinguished first-order free variable x. We say that $\phi(x)$ defines an infinite path, and write $Path(\phi_x)$, if

$$\forall x_1 \forall x_2(\phi(x_1) \wedge \phi(x_2) \to x_1 \subseteq x_2 \vee x_2 \subseteq x_1) \wedge \forall n \in \mathbb{T}\, \exists x(\ell(x) = n \wedge \phi(x)),$$

where $\ell(x)$ stands for $1 \times x$, a more friendly way of denoting the tally length of x. The following is a useful observation:

Proposition 1. *The theory* BTFA *proves the* $\exists\Sigma^b_1$-path comprehension scheme, *that is, the following holds in any model of* BTFA*:*

$$Path(\phi_x) \to \exists X \forall x(\phi(x) \leftrightarrow x \in X),$$

where ϕ is a formula of the form $\exists z \psi$, with ψ a Σ^b_1-formula.

PROOF. Observe that $\phi(x)$ is equivalent to $\forall y(\ell(y) = \ell(x) \wedge y \neq x \rightarrow \neg\phi(x))$ and apply the Δ^0_1(PC)-comprehension scheme. ⊣

We finish this section with some notation concerning (infinite) paths. Given a second-order variable X, we write $Path(X)$ instead of the more cumbersome $Path((x \in X)_x)$. If $Path(X)$ and $n \in \mathbb{T}$, $X[n]$ denotes the unique element $x \in X$ such that $\ell(x) = n$; $X(n)$ is the $(n+1)$-th bit of X.

§3. The real number system. The main purpose of this section is to formalize the real number system within BTFA and, in particular, to show that it is provably an ordered field (in the next section, we show that it is in fact a real closed ordered field). In order to do this, we essentially follow the strategy outlined by Takeshi Yamazaki in [28]. Let us start with the natural numbers. Natural numbers y are represented by binary strings of zeros and ones of the form $1x$ (with $x \in \mathbb{W}$) or by the empty string ϵ. If $x = x_1x_2\cdots x_{n-1}$, where each x_i is 0 or 1, then we should view y as the number $y = \sum_{i=0}^{n-1} x_i 2^{n-i-1}$, where $x_0 = 1$. If y is the empty string, we should view it as representing the number zero: as usual, this number is denoted by 0 (we hope that no confusion arises between the number 0, which is the string ϵ, and the string 0). These are the so-called *dyadic natural numbers*, denoted by $\mathbb{N}_2$. Note that the ordering according to length and, within the same length, lexicographically, induces a total relation in $\mathbb{N}_2$, giving the less than $<$ relation. It is also convenient to speak of *tally numbers*: these are identified with the tally part $\mathbb{N}_1 = \mathbb{T}$ of $\mathbb{W}$. As we have discussed in the previous section, the arithmetic of these numbers *qua* tally numbers (since tally numbers can also be viewed as dyadic natural numbers) is very simple. The arithmetic of the dyadic natural numbers is not so straightforward. It is well known that the four basic processes of arithmetic, namely: addition, subtraction, multiplication, and division have polynomial time computable algorithms (see, for instance, section 4.3 of [15]). Moreover, these algorithms provably do what they are supposed to do in Σ^b_1−NIA. However, to formally define the algorithms and to formally check that they work is a tedious and unsavory task. The next proposition and remarks state what will be needed in the sequel:

PROPOSITION 2. *There are binary $\mathcal{L}_P$-symbols $+$, $\dot{-}$, $\cdot$, $q(,)$ and $r(,)$ such that the theory Σ^b_1−NIA proves that $(\mathbb{N}_2, 0, 1, +, \cdot, <)$ is a discretely ordered semi-ring. Moreover, the following properties also hold:*

1. $x < y \rightarrow x + (y \dot{-} x) = y$
2. $x \neq 0 \rightarrow y = x \cdot q(y, x) + r(y, x) \wedge r(y, x) < x$

By a discretely ordered semi-ring, we mean a structure that satisfies the following sixteen axioms:

Ax. 1	$(x+y)+z = x+(y+z)$	Ax. 2	$x+y = y+x$
Ax. 3	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	Ax. 4	$x \cdot y = y \cdot x$
Ax. 5	$x \cdot (y+z) = (x \cdot y) + (x \cdot z)$	Ax. 6	$x+0 = x \wedge x \cdot 0 = 0$
Ax. 7	$x \cdot 1 = x$	Ax. 8	$\neg x < x$
Ax. 9	$x < y \wedge y < z \to x < z$	Ax. 10	$x < y \vee x = y \vee y < x$
Ax. 11	$x < y \to \exists z(x+z = y)$	Ax. 12	$x < y \to x+z < y+z$
Ax. 13	$0 < z \wedge x < y \to x \cdot z < y \cdot z$	Ax. 14	$0 < 1$
Ax. 15	$\forall x(0 < x \to x = 1 \vee 1 < x)$	Ax. 16	$\forall x(x = 0 \vee 0 < x)$

We refer the reader to Richard Kaye's book [14] for the discussion of the fundamental consequences these axioms. Of course, the structure $(\mathbb{N}_2, 0, 1, +, \cdot, <)$ satisfies much more than the above, since it inherits the Σ^b_1-induction on notation scheme from BTFA (as a matter of fact, one has to make heavy use of Σ^b_1-induction on notation in order to prove the above Proposition 2). Thus, if $\phi(x)$ is a Σ^b_1-formula, possibly with first and second-order parameters, the following holds in BTFA:

$$\phi(0) \wedge \forall x \in \mathbb{N}_2(\phi(x) \to \phi(2x) \wedge \phi(2x+1)) \to \forall x \in \mathbb{N}_2\, \phi(x)$$

where in the above 0 stands for the dyadic number zero (i.e., 0 is really ϵ). The usual (non-notation) sort of induction is available in BTFA for *sets* (see [3, Theorem 22] or [7, page 167]):

$$\forall X[0 \in X \wedge \forall x \in \mathbb{N}_2(x \in X \to x+1 \in X) \to \forall x \in \mathbb{N}_2\, x \in X]$$

where the above proviso concerning zero also applies. As a matter of fact, the structure $(\mathbb{N}_2, 0, 1, +, \cdot, <)$ can be suitably expanded to yield a model of Buss' theory S^1_2: this is actually the way to show that S^1_2 is interpretable in $\Sigma^b_1{-}\mathsf{NIA}$.

A *dyadic rational number* is a triple of the form $(\pm, x, y)$, where x (resp., y) is the empty string or a string starting with 1 (resp., ending with 1). We assume that the triples are coded as strings in a smooth way. If $x = x_0 x_1 \cdots x_{n-1}$ and $y = y_0 y_1 \cdots y_{m-1}$, where each x_i and y_j is 0 or 1 (note that x_1 must be 1 and y_m must be 1), then we should view the triple $(\pm, x, y)$ as representing the rational number $\pm(\sum_{i=0}^{n-1} x_i 2^{n-i-1} + \sum_{j=0}^{m-1} \frac{y_j}{2^{j+1}})$. Usually, we represent this number by $\pm x_0 x_1 \cdots x_{n-1}.y_0 \cdots y_{m-1}$. The dot that appears between x_{n-1} and y_0 is called the *radix point* of the dyadic representation. Given $x \in \mathbb{W}$, it is convenient to denote by x^* the word x with its rightmost zeros chopped off. In this way, $.x^*$ is the dyadic rational number $\sum_{i<\ell(x)} \frac{x_i}{2^{i+1}}$, where x_i is the $(i+1)$-th bit of the word x (for a tally i less than $\ell(x)$). The arithmetic of the non-negative dyadic rational numbers reduces to the arithmetic of the the dyadic natural numbers in a straightforward and feasible manner: one has just to keep track of the radix point. This arithmetic extends in the usual way to all the dyadic rational numbers $\mathbb{D}$, yielding an ordered ring $(\mathbb{D}, 0, 1, +, \cdot, <)$, i.e., a structure that satisfies the first fourteen axioms listed after Proposition 2 and the axiom $\forall x \exists y(x+y = 0)$. We abbreviate $x < y \vee x = y$ by $x \leq y$, and we define the absolute value function ($\mathcal{L}_P$ symbol) $|x|$ as usual.

Clearly, $(\mathbb{D}, <)$ is a dense linear order without endpoints. Given a tally n, let us abbreviate by 2^n the following dyadic rational number:

$$(+, 1\underbrace{00\ldots0}_{n \text{ zeros}}, \epsilon).$$

It is clear that these numbers are cofinal in $\mathbb{D}$. In the introduction, we said that BTFA is a system of weak analysis, i.e., one in which one cannot prove the totality of the exponential function. Given that we have just introduced an "exponential" notation of the form 2^n, let us spend a few lines with a brief discussion of these matters. There is a binary $\mathcal{L}_P$ relation symbol Exp such that the Σ_1^b−NIA proves the following properties: $Exp(0,1)$, $\forall x, y \in \mathbb{N}_2(Exp(x,y) \to Exp(x+1, y+y))$, and $\forall x, y, z \in \mathbb{N}_2(Exp(x,y) \wedge Exp(x,z) \to y = z)$. As we have remarked, 1) the theory Σ_1^b−NIA does not prove that $\forall x \in \mathbb{N}_2 \exists y \in \mathbb{N}_2 Exp(x,y)$, and 2) for a given tally number n, 2^n is *always* defined as the dyadic rational number above. However, for the very same n, it need not be the case that $\exists y \in \mathbb{N}_2 Exp(n,y)$, i.e., the number n, *qua* dyadic natural number, need not have exponentiation in base 2. The following result may clarify the situation:

PROPOSITION 3. *The theory* Σ_1^b−NIA *proves the following:*

$$\forall n \in \mathbb{N}_1 \exists! x \in \mathbb{N}_2\, Exp(x, 2^n).$$

PROOF. Show that $\forall n \in \mathbb{N}_1 \exists x \in \mathbb{N}_2(x \preceq n \wedge Exp(x, 2^n))$ by tally induction on n. This is a proof in the theory $\Sigma_1^b -$ NIA, since the above existential quantifier is bounded. The uniqueness proof poses no particular problem. ⊣

This means that the tally numbers have dyadic counterparts. The reverse is true in a model of Σ_1^b−NIA if, and only if, exponentiation is always defined in the model. More precisely, the sentence $\forall x \in \mathbb{N}_2 \exists y \in \mathbb{N}_2 Exp(x,y)$ is equivalent (within Σ_1^b−NIA) to the sentence $\forall x \in \mathbb{N}_2 \exists n \in \mathbb{N}_1 Exp(x, 2^n)$.

Given n a non-zero tally, let the expression $\frac{1}{2^n}$, or 2^{-n}, abbreviate the dyadic rational number

$$(+, \epsilon, \underbrace{00\ldots0}_{n-1 \text{ zeros}}1).$$

Clearly, for every positive dyadic rational number x there is $n \in \mathbb{N}_1$ such that $2^{-n} < x$. In the sequel, we will make use of some simple arithmetic equations that govern the tally powers of two. Thus, $2^0 = 1$ and, for tallies n and m, $2^n \cdot 2^{-n} = 1$, $2^n \cdot 2^m = 2^{n+m}$, and $2^{-n} \cdot 2^{-m} = 2^{-(n+m)}$, where the multiplication signs stand for dyadic multiplication, and the plus signs stand for the tally summation. We also have $2^n + 2^n = 2^{n+1}$ and $2^{-n} + 2^{-n} = 2^{-(n-1)}$. Of course, the above laws also hold for *negative* tally numbers, had we cared to have defined them. The following property will also be used: for n and m in $\mathbb{N}_1$, $n < m$ iff $2^n < 2^m$ iff $2^{-m} < 2^{-n}$. Note that the first $<$ sign in the previous sentence is really $\subsetneq$, while the other two $<$ signs stand for the less than relation in $\mathbb{N}_2$. Whether one is using tally or dyadic arithmetic is usually clear from the context.

Given $s = (s_i)_{i<n}$ (the code of) a finite sequence of dyadic rational numbers of length n, where n is a tally number, it makes sense to speak of $\sum_{i=0}^{n-1} s_i$, $\max_{i<n} s_i$ and $\prod_{i=0}^{n-1} s_i$ in Σ_1^b−NIA, since these operations are easily defined by bounded recursion (along the tally part). If the sequence s happens to code the bit expansion of a dyadic rational number x, i.e., if $s = (x_i 2^{n-i-1})_{i<n}$ and $x = x_0 x_1 \cdots x_{n-1}$, then $\sum_{i=0}^{n-1} x_i 2^{n-i-1}$ is not only a manner of speaking, but a formally defined object in its own right. Clearly, one can prove that this object is indeed x, i.e., that $x = \sum_{i=0}^{n-1} x_i 2^{n-i-1}$. We shall be loose and informal in using

this and other similar notations, and often ambiguous between the formally defined and the "manner of speaking" modes of speaking. This is harmless because these notions do not pose any particular problems within $\Sigma_1^b-\mathsf{NIA}$. Of course, we shall also use some simple identities concerning summation: e.g., $\sum_{i=0}^{n-1} 2^i = 2^n - 1$ or $\sum_{i=1}^{n} 2^{-i} = 1 - 2^{-n}$. They are straightforwardly provable by tally induction.

The dyadic rational numbers do not form a field, even though it is *always* permissible to divide by tally powers of 2. We will nevertheless need the following result:

PROPOSITION 4. *There are ternary $\mathcal{L}_P$ symbols Q and R such that the theory $\Sigma_1^b-\mathsf{NIA}$ proves the following:*

1. $d_1, d_2 \in \mathbb{D}^+ \wedge n \in \mathbb{N}_1 \rightarrow Q(d_1, d_2, n) \in \mathbb{D}_0^+$,
2. $d_1, d_2 \in \mathbb{D}^+ \wedge n \in \mathbb{N}_1 \rightarrow R(d_1, d_2, n) \in \mathbb{D}_0^+ \wedge R(d_1, d_2, n) < 2^{-n}$,
3. $d_1, d_2 \in \mathbb{D}^+ \wedge n \in \mathbb{N}_1 \rightarrow d_1 = Q(d_1, d_2, n) \cdot d_2 + R(d_1, d_2, n)$,

where $\mathbb{D}^+$ is the system of all positive dyadic rational numbers, and $\mathbb{D}_0^+$ is $\mathbb{D}^+$ together with the rational number zero.

PROOF. This theorem is an easy consequence of long division. Suppose that $d_1 = x_0 \cdots x_{k-1}.y_0 \cdots y_{m-1}$ and $d_2 = w_0 \cdots w_{l-1}.z_0 \cdots z_{s-1}$. Let x be $2^s d_2$ and y be $2^{m+n+l+s+1} d_1$. Note that x and y can be considered dyadic natural numbers:

$$x = w_0 \cdots w_{l-1} z_0 \cdots z_{s-1} \qquad \text{and} \qquad y = x_0 \cdots x_{k-1} y_0 \cdots y_{m-1} \overbrace{00 \cdots 0}^{(n+l+s+1) \text{ zeros}}.$$

By 2 of Proposition 2, we have $y = x \cdot q(y, x) + r(y, x)$, with $r(y, x) < x$. Multiplying both members of the previous equality by $2^{-(m+n+l+s+1)}$, we get:

$$d_1 = d_2 \cdot 2^{-(m+n+l+1)} \cdot q(y, x) + 2^{-(m+n+l+s+1)} \cdot r(y, x).$$

Note that $2^{-(m+n+l+s+1)} \cdot r(y, x) < 2^{-(m+n+l+s+1)} \cdot x < 2^{-(m+n+l+s+1)} \cdot 2^{l+s+1} \leq 2^{-(m+n)} \leq 2^{-n}$. From the above discussion, one can easily define the desired function symbols. ⊣

DEFINITION 2. (BTFA) We say that a function $\alpha : \mathbb{N}_1 \mapsto \mathbb{D}$ is a *real number* if $|\alpha(n) - \alpha(m)| \leq 2^{-n}$ for all $n \leq m$. Two real numbers α and β are said to be *equal*, and we write $\alpha = \beta$, if $\forall n \in \mathbb{N}_1 |\alpha(n) - \beta(n)| \leq 2^{-n+1}$.

The above definition follows closely the definition of real numbers in [23]. It has a noteworthy feature, though: the domain of the reals are the tally numbers, not the dyadic natural numbers. When discussing real numbers within BTFA, we shall often use the symbol $\mathbb{R}$ informally to denote the set of all real numbers. For instance, $\forall \alpha \in \mathbb{R}(\cdots)$ means $\forall \alpha$(if α is a real number then $\cdots$). Within BTFA, we can embed the dyadic rational numbers into $\mathbb{R}$ by identifying $x \in \mathbb{D}$ with the real number α_x given by the constant law $\alpha_x(n) = x$. A natural generalization of the dyadic rational numbers are the so-called *dyadic real numbers*. A dyadic real number is a triple $(\pm, x, X)$, where $x \in \mathbb{N}_2$ and X is an infinite path. The usual (radix point) notation for these numbers is $\pm x.X$. Informally, such a dyadic real numbers stand for the real number $\pm(\sum_{i=0}^{n-1} x_i 2^{n-i-1} + \sum_{i=0}^{\infty} \frac{X(i)}{2^{i+1}})$. More precisely: to a dyadic real number $(\pm, x, X)$ we associate a function $\alpha : \mathbb{N}_1 \mapsto \mathbb{D}$ given by the law $\alpha(n) = \pm x.X[n]^*$. It is easy to see that α is a real number according to the definition above, and we shall usually identify the dyadic real number triples with the real numbers associated with it. In the next section, we will see that BTFA is able to prove that every real number is equal to a dyadic real number.

In order to define the product of two real numbers, we use in the next definition the least tally number principle (see the previous section). This principle is very convenient, and will be used often in the paper without explicit mentioning.

Definition 3. (BTFA) Let α and β be two real numbers.

1. $\alpha + \beta$ is the real number $n \to \alpha(n+1) + \beta(n+1)$.
2. $\alpha - \beta$ is the real number $n \to \alpha(n+1) - \beta(n+1)$.
3. $\alpha \cdot \beta$ is the real number $n \to \alpha(n+k) \cdot \beta(n+k)$, where k is the least tally number such that $|\alpha(0)| + |\beta(0)| + 2 \leq 2^k$.
4. $\alpha \leq \beta$ if $\forall n(\alpha(n) \leq \beta(n) + 2^{-n+1})$.

It is clear that $\alpha = \beta$ if, and only if, $\alpha \leq \beta$ and $\beta \leq \alpha$. As usual, we say that $\alpha < \beta$ if $\alpha \leq \beta \wedge \alpha \neq \beta$. The usual proof that these operations are congruent with the notion of equality between real numbers given in Definition 2 formalizes readily in BTFA. Note that formulas such as $\alpha = \beta$, $\alpha \leq \beta$, $\alpha + \beta = \gamma$, ... are $\forall\Pi_1^b$-formulas, while $x \neq y$, $x < y$, ... are $\exists\Sigma_1^b$-formulas.

Proposition 5. (BTFA)

1. $\forall \alpha, \beta, \gamma \in \mathbb{R}\, (\alpha \leq \beta \wedge \beta \leq \gamma \to \alpha \leq \gamma)$*;*
2. $\forall \alpha \in \mathbb{R}\, \forall n \in \mathbb{N}_1\, (\alpha(n) - 2^{-n} \leq \alpha \leq \alpha(n) + 2^{-n})$.
3. $\forall \alpha, \beta \in \mathbb{R}\, (\alpha \neq \beta \to \alpha < \beta \vee \beta < \alpha)$.
4. $\forall \alpha, \beta \in \mathbb{R}\, (\alpha < \beta \to \exists x \in \mathbb{D}(\alpha < x < \beta))$.

Proof. There is no special difficulty in proving this proposition. Suppose that $\alpha \leq \beta$ and $\beta \leq \gamma$. Fix an arbitrary tally number n. Then, for all tallies $m \geq n$ we have that the difference $\alpha(n) - \gamma(n)$ is equal to:

$$(\alpha(n) - \alpha(m)) + (\alpha(m) - \beta(m)) + (\beta(m) - \gamma(m)) + (\gamma(m) - \gamma(n)).$$

This, in turn, does not exceed $2^{-n} + 2^{-m+1} + 2^{-m+1} + 2^{-n} = 2^{-n+1} + 2^{-m+2}$. Since m is arbitrarily large, we may conclude that $\alpha(n) - \gamma(n) \leq 2^{-n+1}$. Since n was an arbitrary tally, we get $\alpha \leq \gamma$. Assertion 2) follows from a straightforward computation. To prove 3), suppose that $\alpha \neq \beta$. Take a tally number k such that $|\alpha(k) - \beta(k)| > 2^{-k+1}$. Without loss of generality, assume $\alpha(k) + 2^{-k+1} < \beta(k)$, i.e., $\alpha(k) + 2^{-k} < \beta(k) + 2^{-k}$. Thus, by 1) and 2), we may conclude that $\alpha < \beta$. A similar argument works for part 4), putting $x = \frac{1}{2}(\alpha(k) + \beta(k))$ for a suitable tally k. ⊣

An ordered field is an ordered ring which is a field:

Theorem 2. *The theory* BTFA *proves that the real number system is an ordered field.*

Proof. All the axioms of ordered rings can be proved in a routine (if tedious) way. We only show in detail that, for every positive real number α, there is a real number β such that $\alpha \cdot \beta = 1$. By Proposition 5, there is a tally n_0 such that, for all tallies $n \geq n_0$, one has $2^{-n_0} \leq \alpha(n)$. By Proposition 4, there are functions β' and ρ defined in $\mathbb{N}_1$ such that, for all tallies n, $\alpha(n + n_0 + 1)\beta'(n) = 1 - \rho(n)$, with $0 \leq \rho(n) < 2^{-(n+2)}$. Note that this implies that $\beta'(n) \leq 2^{n_0}$, for all tallies n. Define β by $\beta(n) = \beta'(n + n_0)$. Let us first check that β is a real number. Take arbitrary tallies n and m with $n \leq m$. We have:

$$\begin{aligned}\frac{1}{2^{n_0}}|\beta(n) - \beta(m)| &\leq \alpha(n + 2n_0 + 1)|\beta(n) - \beta(m)| \\ &= |\alpha(n + 2n_0 + 1)\beta(n) - \alpha(n + 2n_0 + 1)\beta(m)|\end{aligned}$$

The above is less than or equal to the sum of

$$|\alpha(n + 2n_0 + 1)\beta(n) - \alpha(m + 2n_0 + 1)\beta(m)|$$

with

$$|\alpha(m + 2n_0 + 1)\beta(m) - \alpha(n + 2n_0 + 1)\beta(m)|.$$

Using the fact that α is a real number, the above is less than or equal to

$$\rho(n + n_0) + \rho(m + n_0) + \beta(m)\frac{1}{2^{n+2n_0+1}}.$$

Thus,

$$|\beta(n) - \beta(m)| \leq 2^{n_0}(\frac{2}{2^{n+n_0+2}} + \frac{1}{2^{n+n_0+1}}) \leq \frac{2^{n_0}}{2^{n+n_0}} \leq \frac{1}{2^n}.$$

Now, notice that for all tallies n:

$$|\alpha(n + 2n_0 + 1)\beta(n) - 1| = \rho(n + n_0) \leq \frac{1}{2^{n+n_0+2}} \leq \frac{1}{2^{n-1}}.$$

This entails that $\alpha' \cdot \beta = 1$, where α' is the real defined by the law $\alpha'(n) = \alpha(n + 2n_0 + 1)$. As it happens, α and α' are the same real. We are done. ⊣

§4. Continuous functions and their values. The last part of Ferreira's unpublished thesis [5] studied some basic weak analysis in the Cantor space. This space is specially perspicuous within BTFA because its elements are just the infinite paths through $\mathbb{W}$. Codes for continuous (partial) functions are very simple in the Cantor space setting, as well as the proofs of the fundamental facts concerning them (e.g., Theorem 3 below is a rather delicate matter, while in the Cantor space setting has a very simple proof). The Cantor space case should be regarded as a test case for what really matters: the real number case. This section is concerned with the formalization of the notion of continuous (partial) real function of a real variable within the framework of BTFA, and with the study of some simple properties concerning this notion. It follows from this study that the structure of the real numbers forms a real closed ordered field in BTFA.

The following definition is based on the notion of (partial) continuous function given in Simpson's book [23].

Definition 4. Within BTFA, a (code for a) *continuous partial function* from $\mathbb{R}$ into $\mathbb{R}$ is a set of quintuples $\Phi \subseteq \mathbb{W} \times \mathbb{D} \times \mathbb{N}_1 \times \mathbb{D} \times \mathbb{N}_1$ such that:

1. if $(x, n)\Phi(y, k)$ and $(x, n)\Phi(y', k')$, then $|y - y'| \leq 2^{-k} + 2^{-k'}$;
2. if $(x, n)\Phi(y, k)$ and $(x', n') < (x, n)$, then $(x', n')\Phi(y, k)$;
3. if $(x, n)\Phi(y, k)$ and $(y, k) < (y', k')$, then $(x, n)\Phi(y', k')$;

where $(x, n)\Phi(y, k)$ abbreviates the $\exists\Sigma^b_1$-relation $\exists w(w, x, n, y, k) \in \Phi$, and where the notation $(x', n') < (x, n)$ means that $|x - x'| + 2^{-n'} < 2^{-n}$.

If α is a real number, $(\alpha(m+1), m) < (\alpha(n+1), n)$ for tallies $n+1 < m$. This is a handy fact that we shall often use in the sequel.

Here follows some basic examples of continuous functions:

I. The *identity function* is defined by the clause $(x,n)Id(y,k)$ if $x, y \in \mathbb{D}$, $n, k \in \mathbb{N}_1$, and $(x,n) < (y,k)$. Note that this is a correct definition. In particular, notice that the defining clause is a PTC formula. Thus, the set of quintuples $\{(\epsilon, x, n, y, k) : \theta(x, n, y, k)\}$ exists, and is officially the function Id.

II. Given γ a real number, we define the *constant function* C_γ of value γ by the clause $(x,n)C_\gamma(y,k)$ if $x, y \in \mathbb{D}$, $n, k \in \mathbb{N}_1$, and $|\gamma - y| < 2^{-k}$. Notice that the above clause $\theta(x, n, y, k)$ is given by a $\exists\Sigma_1^b$-formula, i.e., a formula of the form $\exists w \theta'(w, x, n, y, k)$, with θ a sw.q.-formula. Thus, the set of quintuples $\{(w, x, n, y, k) : \theta'(w, x, n, y, k)\}$ exists, and is officially the function C_γ.

III. Let Φ_1 and Φ_2 be continuous function. Their *sum* is the continuous function $\Phi_1 + \Phi_2$ defined according to the clause $(x,n)[\Phi_1 + \Phi_2](y,k)$ if there are pairs (y_1, k_1) and (y_2, k_2) such that $(x,n)\Phi_1(y_1,k_1)$, $(x,n)\Phi_2(y_2,k_2)$, and $|y - (y_1 + y_2)| \leq 2^{-k} - (2^{-k_1} + 2^{-k_2})$. Notice that this clause is given by a $\exists\Sigma_1^b$-formula.

IV. Let Φ_1 and Φ_2 be continuous function. Their *product* is the continuous function $\Phi_1 \cdot \Phi_2$ defined according to the clause $(x,n)[\Phi_1 \cdot \Phi_2](y,k)$ if there are pairs (y_1, k_1) and (y_2, k_2) such that $(x,n)\Phi_1(y_1,k_1)$, $(x,n)\Phi_2(y_2,k_2)$, and
$$|y - y_1 y_2| \leq \frac{1}{2^k} - \left(|y_1| \frac{1}{2^{k_2}} + |y_2| \frac{1}{2^{k_1}} + \frac{3}{2^{k_1+k_2}} \right).$$
Notice that the above clause is given by a $\exists\Sigma_1^b$-formula.

The above examples entail that all polynomials of standard degree give rise to continuous functions in BTFA.

DEFINITION 5. (BTFA) Let Φ be a continuous partial real function of a real variable. We say that a real number α is in the domain of Φ and, with abuse of language, write $\alpha \in dom(\Phi)$, if
$$\forall k \in \mathbb{N}_1 \exists n \in \mathbb{N}_1 \exists x \in \mathbb{D} \exists y \in \mathbb{D} \left(|\alpha - x| < 2^{-n} \wedge (x,n)\Phi(y,k) \right).$$

LEMMA 1. (BTFA) *Given Φ be a continuous partial real function of a real variable, a real number α is in the domain of Φ if, and only if,*
$$\forall k \in \mathbb{N}_1 \exists n \in \mathbb{N}_1 \exists y \in \mathbb{D}\, (\alpha(n+1), n)\Phi(y,k).$$

PROOF. For the right to left direction, just take $x = \alpha(n+1)$ (use 2 of Proposition 5). Conversely, let k be an arbitrary tally number. By hypothesis, there are $n \in \mathbb{N}_1$ and $x, y \in \mathbb{D}$ such that $|\alpha - x| < 2^{-n}$ and $(x,n)\Phi(y,k)$. Take $m \in \mathbb{N}_1$ with $|\alpha - x| < 2^{-n} - 2^{-m}$. We get,
$$|\alpha(m+2) - x| + \frac{1}{2^{m+1}} \leq |\alpha(m+2) - \alpha| + |\alpha - x| + \frac{1}{2^{m+1}}$$
$$\leq |\alpha - x| + \frac{1}{2^{m+2}} + \frac{1}{2^{m+1}} < |\alpha - x| + \frac{1}{2^m} < \frac{1}{2^n}.$$

Hence, $(\alpha(m+2), m+1) < (x, n)$. Thus, by property 2 of Definition 4, we may conclude that $(\alpha(m+2), m+1)\Phi(y, k)$. ⊣

Definition 6. (BTFA) Let Φ be a continuous partial real function of a real variable, and let α be a real number in the domain of Φ. We say that a real number β is the *value of* α *under the function* Φ, and write $\Phi(\alpha) = \beta$, if

$$\forall x, y \in \mathbb{D} \forall n, k \in \mathbb{N}_1 \left((x, n)\Phi(y, k) \wedge |\alpha - x| < \frac{1}{2^n} \to |\beta - y| \leq \frac{1}{2^k} \right).$$

It is not difficult to check that the examples that we gave of continuous functions have the intended properties. All reals α are in the domain of the identity function, and $Id(\alpha) = \alpha$. All reals α are in the domain of any constant function C_γ, and $C_\gamma(\alpha) = \gamma$. If a real α is in the domain of both Φ_1 and Φ_2, $\Phi_1(\alpha) = \beta_1$ and $\Phi_2(\alpha) = \beta_2$, then α is in the domain of $\Phi_1 + \Phi_2$ and in the domain of $\Phi_1 \cdot \Phi_2$. Moreover, $[\Phi_1 + \Phi_2](\alpha) = \beta_1 + \beta_2$ and $[\Phi_1 \cdot \Phi_2](\alpha) = \beta_1 \cdot \beta_2$.

The above facts entail that polynomial functions (of standard degree) are defined everywhere and have a value at every point. This result is a particular case of a more general situation, namely that if a real number α is in the domain of a continuous function Φ, then it indeed has a (unique) value β under Φ. It turns out that proving this result is a somewhat delicate affair. The proof hinges on the discussion of two alternative cases: either the dyadic notation of $\Phi(\alpha)$ has infinitely many zeros *and* ones or, else, $\Phi(\alpha)$ is in $\mathbb{D}$.

We start with a simple lemma:

Lemma 2. (BTFA) *Let* $x, y \in \mathbb{W}$. *Then*

$$|.x1 - .y1| \leq \frac{1}{2^{\ell(x)+2}} + \frac{1}{2^{\ell(y)+2}} \to x \subseteq y \vee y \subseteq x.$$

Proof. To prove the implication, let us assume its antecededent and suppose, in order to get a contradiction, that $\ell(x) \leq \ell(y)$ but $x \not\subseteq y$ (the other case is symmetric). Under the above supposition, the hypothesis of the implication entails that $|.x1 - .y1| \leq 2^{-(\ell(x)+1)}$. There are two cases to consider. In the first case, we can put $x = z0w$ and $y = z1uv$, with $\ell(w) = \ell(u)$. We get,

$$|.x1 - .y1| = .y1 - .x1 \geq .z1(u \times 0)(v \times 0)1 - .z0(w \times 1)1$$

$$> .z1 - .z0(w \times 1)1 = .(z \times 0)0(w \times 0)1 = \frac{1}{2^{\ell(x)+1}},$$

which contradicts the bound above. In the second case, we can put $x = z1w$ and $y = z0uv$, with $\ell(w) = \ell(u)$. Then,

$$|.x1 - .y1| = .x1 - .y1 \geq z1(w \times 0)1 - .z0(u \times 1)(v \times 1)1$$

$$> .z1(w \times 0)1 - .z1 = .(z \times 0)0(w \times 0)1 = \frac{1}{2^{\ell(x)+1}},$$

again contradicting the bound above. ⊣

Theorem 3. (BTFA) *Let* Φ *be a continuous partial real function of a real variable, and let* α *be a real number in the domain of* Φ. *Then there is a dyadic real number* β *such that* $\Phi(\alpha) = \beta$. *Moreover, this real number is unique.*

Proof. The uniqueness part of the theorem is clear. Let now Φ and α be as in the hypothesis of the theorem. Without loss of generality, we may suppose that all the dyadic rational numbers appearing in the penultimate components of Φ are of the form $(+, \epsilon, z1)$, i.e., are positive dyadic rational numbers with no integer part (to see this, just make a convenient linear transformation with dyadic coeficients, and restrict your attention to a suitable neighborhood). There are two cases to be discussed.

The first case is when

$$\forall k \in \mathbb{N}_1 \exists n \in \mathbb{N}_1 \exists z \in \mathbb{W} \left(\ell(z) \geq k \wedge (\alpha(n+1), n)\Phi(.z1, \ell(z)+2)\right).$$

In this case, consider the following $\exists\Sigma_1^b$-formula $\theta(y)$:

$$\exists n \in \mathbb{N}_1 \exists z \in \mathbb{W} \left(y \subseteq z \wedge (\alpha(n+1), n)\Phi(.z1, \ell(z)+2)\right).$$

We make three claims:

1. $\theta(y) \wedge y' \subseteq y \to \theta(y')$;
2. $\theta(y) \wedge \theta(y') \to y \subseteq y' \vee y' \subseteq y$; and
3. $\forall k \in \mathbb{N}_1 \exists y(\theta(y) \wedge \ell(y) = k)$.

The first claim is evident, while the last claim follows because we are in the first case. Let us now argue for the second claim. Let y and y' be such that $\theta(y)$ and $\theta(y')$. Then there are $z, z' \in \mathbb{W}$ and $n, n' \in \mathbb{N}_1$ with $y \subseteq z$, $y' \subseteq z'$, $(\alpha(n+1), n)\Phi(.z1, \ell(z)+2)$, and $(\alpha(n'+1), n')\Phi(.z'1, \ell(z')+2)$. Without loss of generality, we may assume that $n = n'$ (just use clause 2 of the definition of continuous function and the handy result mentioned afterwards). By the first clause of the same definition, we get $|.z'1 - .z1| \leq 2^{-(2+\ell(z'))} + 2^{-(2+\ell(z))}$. By the previous lemma, either $z \subseteq z'$ or $z' \subseteq z$. In the former case, we have that both y and y' are prefixes of z' and, thus, one of them is a prefix of the other. The latter case is similar.

By $\exists\Sigma_1^b$-path comprehension, the set $Y = \{y \in \mathbb{W} : \theta(y)\}$ exists. We now argue that the real number β given by the dyadic real number $.Y$, i.e. given by the triple $(+, \epsilon, Y)$, is the value of α under Φ. Let $(x, n)\Phi(y, k)$ and $|\alpha - x| < 2^{-n}$. Take an arbitrary $m \in \mathbb{N}_1$. Since Y is an infinite path, take a sufficiently large tally $r \geq m$ with $2^{-(r+1)} < 2^{-n} - |\alpha - x|$, and for which there is $z \in \mathbb{W}$ such that $(\alpha(r+1), r)\Phi(.z1, \ell(z)+2)$ and $Y[m] \subseteq z$. Notice that the above entails that $(\alpha(r+1), r) < (x, n)$, and hence (by 2 of Definition 4) that $(\alpha(r+1), r)\Phi(y, k)$. Now:

$$|\beta - y| \leq |\beta - \beta(r)| + |\beta(r) - \beta(m)| + |\beta(m) - .z1| + |.z1 - y|.$$

The first summand above is less than or equal to 2^{-r}, and *a fortiori*, less than or equal to 2^{-m}. Regarding the second summand, notice that $\beta(r)$ and $\beta(m)$ are, by definition, $.Y[r]^*$ and $.Y[m]^*$ (respectively). This entails that the second summand is less than or equal to 2^{-m}. Since $Y[m] \subseteq z$ and since $\beta(m) = .Y[m]^*$, we conclude that the third summand is also less than or equal to 2^{-m}. Finally, using the first requirement of Definition 4, the fourth summand is less than or equal to $2^{-k} + 2^{-(\ell(z)+2)}$. In sum, $|\beta - y| < 2^{-k} + 2^{-(m-2)}$. Since m was arbitrary, we conclude that $|\beta - y| \leq 2^{-k}$, as we wanted.

We now consider the second case, viz. when there is a tally k_0 such that

$$(\star) \qquad \forall n \in \mathbb{N}_1 \forall z \in \mathbb{W}\,(\ell(z) \geq k_0 \rightarrow \neg(\alpha(n+1), n)\Phi(.z1, \ell(z)+2))\,.$$

Let us start by proving the following fact:

FACT. Let $r > k_0$ be a tally number. If $(\alpha(n+1), n)\Phi(.z1, r)$, where $n \in \mathbb{N}_1$ and $z \in \mathbb{W}$, then either

a) $\forall i \in \mathbb{N}_1\,(k_0 \leq i < r-4 \rightarrow z_i = 1)$, or
b) $\forall i \in \mathbb{N}_1\,(k_0 \leq i < r-4 \rightarrow (z_i = 0 \wedge i < \ell(z)) \vee i \geq \ell(z))$.

PROOF OF THE FACT. Assume that $(\alpha(n+1), n)\Phi(.z1, r)$ as above. By $(\star)$ and clause 3 of the definition of continuous function, we cannot have $k_0 \leq \ell(z) < r-1$. On the other hand, if $\ell(z) \leq k_0$, then we have b) above. Thus, we may assume that $\ell(z) \geq r-1 \geq k_0$. Let us suppose, in order to get a contradiction, that neither a) nor b) above hold. The following two cases exhaust the possibilities. The first case is when we have a tally i such that $k_0 < i < r-3$ and $z_{i-1} = 0$ and $z_i = 1$ (note that $\ell(z) \geq r-1 \geq i+3$). The second case is when we have a tally i such that $k_0 < i < r-4$, $z_{i-1} = 1$, and $z_i = 0$ (note that $\ell(z) \geq r-1 \geq i+4$).

In the first of these two cases, we have $z1 = z\!\upharpoonright_{i-1} 01w_1\delta w_2$, where $w_1, w_2 \in \mathbb{W}$ and $(z1)_{r-1} = \delta$. Note that $\ell(w_1) \geq 2$. Suppose that w_1 is *not* a string of zeros. Then, for a certain tally j with $i+1 < j < r$,

$$|.z\!\upharpoonright_{i-1} 1 - .z1| + \frac{1}{2^r} \leq .z\!\upharpoonright_{i-1} 1 - .z\!\upharpoonright_{i-1} 01 - \frac{1}{2^j} + \frac{1}{2^r}$$

$$< .z\!\upharpoonright_{i-1} 1 - .z\!\upharpoonright_{i-1} 01 = \frac{1}{2^{i+1}}.$$

Therefore, $(.z1, r) < (.z\!\upharpoonright_{i-1} 1, i+1)$. This contradicts $(\star)$.

Now, suppose that w_1 is a string of zeros. Then,

$$|.z1 - .z\!\upharpoonright_{i-1} 01| + \frac{1}{2^r} = .z\!\upharpoonright_{i-1} 01(0 \times w_1)\delta w_2 - .z\!\upharpoonright_{i-1} 01 + \frac{1}{2^r}$$

$$< .z\!\upharpoonright_{i-1} 0101 - .z\!\upharpoonright_{i-1} 01 + \frac{1}{2^r} = \frac{1}{2^{i+3}} + \frac{1}{2^r} < \frac{1}{2^{i+3}} + \frac{1}{2^{i+3}} = \frac{1}{2^{i+2}}.$$

Therefore, $(.z1, r) < (.z\!\upharpoonright_{i-1} 01, i+2)$, again contradicting $(\star)$.

Let us now consider the second case, namely when there is a tally i such that $k_0 < i < r-4$, $z_{i-1} = 1$ and $z_i = 0$. Thus, $z1 = z\!\upharpoonright_{i-1} 10w_1\delta w_2$, where $w_1, w_2 \in \mathbb{W}$ and $(z1)_{r-1} = \delta$. Note that $\ell(w_1) \geq 3$. If $z_{i+1} = 1$, we fall into the first case. Finally, if $z_{i+1} = 0$ we get,

$$|.z1 - .z\!\upharpoonright_{i-1} 1| + \frac{1}{2^r} = .z\!\upharpoonright_{i-1} 10w_1\delta w_2 - .z\!\upharpoonright_{i-1} 1 + \frac{1}{2^r}$$

$$< .z\!\upharpoonright_{i-1} 101 - .z\!\upharpoonright_{i-1} 1 + \frac{1}{2^r} = \frac{1}{2^{i+2}} + \frac{1}{2^r} < \frac{1}{2^{i+2}} + \frac{1}{2^{i+2}} = \frac{1}{2^{i+1}}.$$

Therefore, $(.z1, r) < (.z\!\upharpoonright_{i-1} 1, i+1)$, contradicting $(\star)$. $\dashv$ (of Fact)

If α is in the domain of Φ, it is easy to argue that for every $r \in \mathbb{N}_1$, there is $n \in \mathbb{N}_1$ and $z \in \mathbb{D}$ such that $(\alpha(n+1), n)\Phi(.z1, r)$ and $\ell(z) \geq r-4$. Using this remark and the fact proven above, we have the following two alternatives: either a') for arbitrarily large tallies $r > k_0$, there is a tally n and a binary string z such that $(\alpha(n+1), n)\Phi(.z1, r)$ and $\forall i \in \mathbb{N}_1(k_0 \leq i < r-4 \to z_i = 1)$, or

b') for arbitrarily large tallies $r > k_0$, there is a tally n and a binary string z such that $(\alpha(n+1), n)\Phi(.z1, r)$ and $\forall i \in \mathbb{N}_1(k_0 \leq i < r-4 \to z_i = 0)$.

Suppose alternative a') holds. Then, for arbitrarily large tallies $r > k_0$, there are $n \in \mathbb{N}_1$ and $z \in \mathbb{W}$ with $(\alpha(n+1), n)\Phi(.z1, r)$ and $\forall i(k_0 \leq i < r-1 \to z_i = 1)$. To see this, just consider $r+3$ in a'). Now, given tallies $r_1, r_2 > k_0 + 2$ and $n_1, n_2 \in \mathbb{N}_1$, and $z_1, z_2 \in \mathbb{D}$ such that,

$$(\alpha(n_1+1), n_1)\Phi(.z_1 1, r_1) \wedge \forall i \in \mathbb{N}_1(k_0 \leq i < r_1 - 1 \to (z_1)_i = 1)$$

and

$$(\alpha(n_2+1), n_2)\Phi(.z_2 1, r_2) \wedge \forall i \in \mathbb{N}_1(k_0 \leq i < r_2 - 1 \to (z_2)_i = 1)$$

we must have $z_1\!\upharpoonright_{k_0} = z_2\!\upharpoonright_{k_0}$. For, if $r_1 \leq r_2$ (say) and $z_1\!\upharpoonright_{k_0} \neq z_2\!\upharpoonright_{k_0}$ then,

$$|.z_1 1 - .z_2 1| \geq \frac{1}{2^{k_0}} - \frac{1}{2^{r_1-1}} > \frac{1}{2^{r_1-2}} - \frac{1}{2^{r_1-1}} = \frac{1}{2^{r_1-1}},$$

contradicting the fact that, by clause 1 of the definition of continuous function,

$$|.z_1 1 - .z_2 1| \leq \frac{1}{2^{r_1}} + \frac{1}{2^{r_2}} \leq \frac{1}{2^{r_1}} + \frac{1}{2^{r_1}} = \frac{1}{2^{r_1-1}}.$$

Let then y be the common value above, and define Y to be the infinite path $y111\cdots$. We claim that $\Phi(\alpha) = \beta$, where β is the dyadic real number $.Y$. To see this, suppose that $(x, n)\Phi(w, k)$ and $|\alpha - x| < 2^{-n}$, in order to show that $|\beta - w| \leq 2^{-k}$. Let m be an arbitrary tally. Chose tallies $r > max\{k_0+2, m\}$, $n' \geq m$, and $z' \in \mathbb{D}$ with

$$(\alpha(n'+1), n')\Phi(.z'1, r) \wedge \forall i \in \mathbb{N}_1(k_0 \leq i < r-1 \to z'_i = 1)$$

and $2^{-(n'-1)} < 2^{-n} - |\alpha - x|$. Note that $Y[m] \subseteq z'$ and $(\alpha(n'+1), n') < (x, n)$. Thus, $(\alpha(n'+1), n')\Phi(w, k)$. Now,

$$|\beta - w| \leq |\beta - \beta(m)| + |\beta(m) - .z'1| + |.z'1 - w|.$$

The first summand above is less than or equal to 2^{-m}. The second summand is also less than or equal to 2^{-m}, since $\beta(m) = .Y[m]^*$. By clause 1 of the definition of continuous function, the last summand is less than or equal to $2^{-r} + 2^{-k}$, and hence less than or equal to $2^{-m} + 2^{-k}$. Since m is an arbitrary tally, we conclude that $|\beta - w| \leq 2^{-k}$, as we wanted.

It remains to study alternative b'). Similarly to the previous alternative, we have that, for arbitrarily large tallies $r > k_0$, there are $n \in \mathbb{N}_1$ and $z \in \mathbb{W}$ such that $(\alpha(n+1), n)\Phi(.z1, r)$ and $\forall i(k_0 \leq i < r-1 \to z_i = 0)$. Take tallies $r > k_0 + 2$ and n, and take $z \in \mathbb{D}$ such that,

$$(\alpha(n+1), n)\Phi(.z1, r) \wedge \forall i \in \mathbb{N}_1(k_0 \leq i < r-1 \to z_i = 0).$$

Let $y = z\!\upharpoonright_{k_0}$. As before, this y does not depend of the choice of the z above. Define Y to be the infinite path $y000\cdots$. Similarly to the previous case, one can show that $\Phi(\alpha) = \beta$, where β is the dyadic real number $.Y$. $\dashv$ (of Theorem 3)

In the theorem above, the value of a function at a point of its domain can be taken to be a real number of a very particular form: a dyadic real number. Applying this fact to the identity function we get,

COROLLARY 1. (BTFA) *Every real number is equal to a dyadic real number.*

In the vein of Simpson [23], we now prove Bolzano's intermediate value theorem in BTFA.

THEOREM 4. (BTFA) *If Φ is a continuous function which is total in the closed interval* $[0,1]$ *and if* $\Phi(0) < 0 < \Phi(1)$*, then there is a real number* $\alpha \in [0,1]$ *such that* $\Phi(\alpha) = 0$.

PROOF. Assume that there is no dyadic rational number $x \in [0,1]$ such that $\Phi(x) = 0$ (otherwise we are done). Consider the $\exists\Sigma_1^b$-formulas $\phi(x)$ and $\phi'(x)$ defined as follows: $x \in \mathbb{D} \cap [0,1] \wedge \Phi(x) < 0$ and $x \in \mathbb{D} \cap [0,1] \wedge \Phi(x) > 0$, respectively. Notice that $\neg\phi(x)$ is equivalent to $x \notin \mathbb{D} \cap [0,1] \vee \phi'(x)$, and that $\neg\phi'(x)$ is equivalent to $x \notin \mathbb{D} \cap [0,1] \vee \phi(x)$. By Δ_1^0(PT)-CA, we can form the sets $X = \{x : \phi(x)\}$ and $X' = \{x : \phi'(x)\}$. We now proceed with a binary search: Define, by bounded recursion along the tally part, the function $f : \mathbb{N}_1 \to \mathbb{D} \times \mathbb{D}$ according to the clauses $f(0) = (0,1)$ and

$$f(n+1) = \begin{cases} ((f_0(n) + f_1(n))/2, f_1(n)), & \text{if } (f_0(n) + f_1(n))/2 \in X \ ; \\ (f_0(n), (f_0(n) + f_1(n))/2), & \text{otherwise;} \end{cases}$$

where f_0 and f_1 are the first and second projections of f (respectively). Note that this is indeed a definition by *bounded* recursion since (for $n \neq 0$) the number of bits of $f_0(n)$ and $f_1(n)$ is always less than or equal to n. It is now straightforward to prove by Σ_1^b-induction on notation that, for all $n \in \mathbb{N}_1$, $f_0(n) \in X$, $f_1(n) \in X'$, $f_0(n) \leq f_0(n+1)$, $f_1(n+1) \leq f_1(n)$, $f_0(n) < f_1(n)$, and $f_1(n) - f_0(n) = 2^{-n}$. Therefore, f_0 and f_1 are the same real. If we call this common real α, it is easy to argue that $\Phi(\alpha) = 0$. ⊣

An ordered field K is *real closed*, if it has the intermediate value property for polynomials, i.e., if for all polynomials $p(X) \in K[X]$ and all elements $a, b \in K$, if $a < b$, $p(a) < 0$ and $p(b) > 0$ there exists $c \in K$ such that $a < c < b$ and $p(c) = 0$. The intermediate value theorem and the continuity of every standard polynomial function entail that the elementary theory of the real closed ordered fields is interpretable in BTFA. In sum, we have proved the following result:

THEOREM 5. *The elementary theory of the real closed ordered fields* RCOF *is interpretable in* BTFA.

The above theorem does not quite say that BTFA *proves* that the real number system is a real closed ordered field, since the polynomials considered so far are of standard degree. But, in fact, this stronger result is also true. Since there are some distintictive features when working with systems in which exponentiation is not a total function, in the remaining part of this section we illustrate the sort of features that we have in mind by defining polynomials of real coefficients in BTFA (and by proving that they do define continuous functions).

A moment's thought will convince the reader that, within BTFA, we can only effectually define polynomials of tally degree. Given $d \in \mathbb{N}_1$, a sequence $(\gamma)_{i \leq d}$

of real numbers of length $d+1$ is a function $F : \{i \in \mathbb{N}_1 : i \leq d\} \times \mathbb{N}_1 \to \mathbb{D}$ such that, for every $i \leq d$, the function γ_i defined by $\gamma_i(n) = F(i,n)$ is a real number. A real polynomial $P(X)$ of degree d is just such a sequence with the proviso that $\gamma_d \neq 0$. As usual, we write

$$P(X) = \gamma_d X^d + \cdots + \gamma_1 X + \gamma_0. \tag{1}$$

It is not difficult to define smoothly $P(\alpha)$, for α a real number. Just for the record, we can take $P(\alpha)$ according to the law that maps each tally n to the dyadic rational number

$$\sum_{i=0}^{d} \gamma_i(n+d+k)\alpha(n+d+k)^i,$$

where k is the least tally such that

$$(|\alpha(0)|+1)^{d-1}(d \max_{i\leq d}(|\gamma_i(0)|+1) + |\alpha(0)|+1) \leq 2^k.$$

Lemma 3. (BTFA) *Let $i \in \mathbb{N}_1$. There is a continuous total function Φ such that $\Phi(\alpha) = \alpha^i$ for all reals α.*

Proof. Just define $(x,n)\Phi(y,k)$ by $x, y \in \mathbb{D}$, $n, k \in \mathbb{N}_1$, and

$$|y - x^i| \leq \frac{1}{2^k} - \frac{i}{2^n}(|x|+1)^{i-1}.$$ ⊣

Proposition 6. (BTFA) *Let $P(X)$ be a polynomial as in (1). There is a continuous total function Φ such that $\Phi(\alpha) = P(\alpha)$ for all reals α.*

Proof. By the above lemma, for each tally i, with $i \leq d$, there is a continuous total function Φ_i such that $\Phi_i(\alpha) = \gamma_i\alpha^i$, for all real numbers α. By construction, the 5-ary relation $(x,n)\Phi_i(y,k)$ on x, n, y, k and i is a $\exists\Sigma_1^b$-relation. We can now define the sought after function Φ by $(x,n)\Phi(y,k)$ if

$$\exists(y_i)_{i\leq d}\exists(k_i)_{i\leq d}\forall i \leq d \left((x,n)\Phi_i(y_i,k_i) \wedge |y - \sum_{i=0}^{d} y_i| \leq \frac{1}{2^k} - \sum_{i=0}^{d}\frac{1}{2^{k_i}} \right).$$

Note that the universal quantifier above is a subword quantification. Thus, the above relation is a $\exists\Sigma_1^b$-relation. ⊣

Hence, under the above definitions, we have proved:

Theorem 6. *The theory* BTFA *proves that the real number system is a real closed ordered field.*

§5. Interpretability in Q. The main result of this section is the following theorem:

Theorem 7. *The theory* BTFA *is interpretable in Robinson's theory of arithmetic* Q.

As a corollary to the above theorem and Theorem 5, we obtain:

Theorem 8. *The elementary theory of the real closed ordered fields* RCOF *is interpretable in* Q.

We are here using the extended notion of interpretation according to which the equality sign need not be interpreted by equality itself (see [22, pages 61-65 and, specially, page 260]). The proof of Theorem 7 will proceed via a sequence of three lemmas. These lemmas ultimately show that BTFA is interpretable in Σ_1^b−NIA. As we have remarked in section 2, the theories Σ_1^b−NIA and S_2^1 are mutually interpretable. Now, the latter theory is interpretable in Q. Therefore, the theorem follows.

The fact that S_2^1 is interpretable in Q is mainly due to Edward Nelson, with a little help from Alex Wilkie: A long and somewhat technical proof of Nelson in [20] showed that the bounded arithmetic theory $\mathsf{I}\Delta_0$ is *locally* interpretable in Q, i.e., that every finite subset of $\mathsf{I}\Delta_0$ is interpretable in Q; sometime later, Wilkie (in an unpublished manuscript) showed that the locality assumption could be dropped. The result follows, since S_2^1 is interpretable in $\mathsf{I}\Delta_0$. The reader can find an exposition of these matters in chapter V.5 of Hájek and Pudlák's book [11].

Let us now state and prove the three above referred lemmas:

LEMMA 4. *The theory* $\mathsf{I}\Delta_0 + \mathsf{B}\Sigma_1$ *is interpretable in* Σ_1^b−NIA.

Note. $\mathsf{B}\Sigma_1$ is the sheme of collection for bounded arithmetic formulas, i.e., the scheme formed by the formulas

$$\forall x \leq z \exists y \phi(x,y) \to \exists w \forall x \leq z \exists y \leq w \phi(x,y),$$

where ϕ is a bounded formula of arithmetic, possibly with parameters (see [14]).

PROOF. We observed in section 2 that the tally part of a model of Σ_1^b−NIA is a model of $\mathsf{I}\Delta_0$ in a natural way. We will interpret the theory $\mathsf{I}\Delta_0 + \mathsf{B}\Sigma_1$ in a suitable cut of this tally part. In order to define this cut, we appeal to the following universal property:

(U) There is a 6-ary sw.q.-formula $U(e,x,y,z,p,c)$ such that for every 4-ary sw.q.-formula $\psi(x,y,z,p)$ there is a (standard) $e \in 2^{<\omega}$ and a 4-ary term $t(x,y,z,p)$ with

$$\Sigma_1^b - \mathsf{NIA} \vdash \forall x \forall y \forall z \forall p (\psi(x,y,z,p) \leftrightarrow \exists c\, U(e,x,y,z,p,c)).$$

Moreover, this c is (provably) unique and of length less than or equal to the length of $t(x,y,z,p)$. (Abusing notation, we identified above the binary word e with its corresponding "numeral.")

The sw.q.-formula $U(e,x,y,z,p,c)$ essentially says that c is the Gödel (binary string) code of a computation on input (x,y,z,p) according to the instructions of the Turing machine with Gödel (binary string) code e. The existence of such e, c and term t relies on the fact that sw.q.-formulas define relations that can be decided by polytime computations, and that such computations can be smoothly formalized in $\Sigma_1^b - \mathsf{NIA}$: see, for instance, section V-4(c) of [11] or [5].

Let $J(u)$ be the formula defined as the conjunction of $u \in \mathbb{N}_1$ together with:

$$\forall e \forall p (\forall v \subseteq u \exists z U(e,u,v,z_0,p,z_1) \to \exists w \forall v \subseteq u \exists z \subseteq^* w\, U(e,u,v,z_0,p,z_1))$$

where z_0 and z_1 are the projections of z when z is regarded as coding an ordered pair. It is clear that, given any sw.q.-formula $\psi(u,v,z,\overline{p})$ and u in the cut J, the following holds:

(B) $\forall \overline{p}(\forall v \subseteq u \exists z \psi(u, v, z, \overline{p}) \rightarrow \exists w \forall v \subseteq u \exists z \subseteq^* w\, \psi(u, v, z, \overline{p}))$.

Note that J has all the tally standards. Moreover, it has the following two properties:

1. $J(u) \wedge u' \subseteq u \rightarrow J(u')$
2. $J(u) \rightarrow J(u \times u)$

We can prove the first property straightforwardly: just apply (B) to the sw.q.-formula $(v \subseteq u' \wedge U(e, u', v, z_0, p, z_1)) \vee (\neg v \subseteq u' \wedge z = \epsilon)$. To argue for the second property, assume $J(u)$ and $\forall v \subset u \times u \exists z U(e, u \times u, v, z_0, p, z_1)$. Fix $q \subset u$. We have, in particular, $\forall r \subset u \exists z U(e, u \times u, (q \times u) + r, z_0, p, z_1)$. By (B) we may conclude that $\exists w \forall r \subset u \exists z \subseteq^* w\, U(e, u \times u, (q \times u) + r, z_0, p, z_1)$. Since q is an arbitrary proper initial subword of u we indeed have,

$$\forall q \subset u \exists w \forall r \subset u \exists z \subseteq^* w\, U(e, u \times u, (q \times u) + r, z_0, p, z_1).$$

Using (B) once again we infer

$$\exists x \forall q \subset u \exists w \subseteq^* x \forall r \subset u \exists z \subseteq^* w\, U(e, u \times u, (q \times u) + r, z_0, p, z_1).$$

Therefore, $\exists x \forall q \subset u \forall r \subset u \exists z \subseteq^* x\, U(e, u \times u, (q \times u) + r, z_0, p, z_1)$, and, as a consequence, $\exists x \forall v \subset u \times u \exists z \subseteq^* x\, U(e, u \times u, v, z_0, p, z_1)$. In sum, the second property is verified.

Accordingly to these two properties, J is a tally cut closed under $\times$. Thus $\mathsf{I}\Delta_0$ holds in J. We now finish the proof by showing that the scheme of collection for bounded arithmetical formulas also holds in this tally cut. Let $\psi(u, v, z, \overline{p})$ be a bounded formula for the tally part (thus, a sw.q.-formula of the binary language). Suppose u and $\overline{p}$ are in J and that $\forall v \subseteq u \exists z(J(z) \wedge \psi(u, v, z, \overline{p}))$. In particular, $\forall v \subseteq u \exists z(z \in \mathbb{N}_1 \wedge \psi(u, v, z, \overline{p}))$. By (B) we infer

$$\exists w \forall v \subseteq u \exists z \subseteq^* w(z \in \mathbb{N}_1 \wedge \psi(u, v, z, \overline{p})).$$

Thus, there is a tally w such that $\forall v \subseteq u \exists z \subseteq w\, \psi(u, v, z, \overline{p})$. By the least tally number principle, let be w_0 the least such w. Then there is v_0 with $v_0 \subseteq u$ such that $\forall z \subset w_0 \neg\psi(u, v_0, z, \overline{p})$. On the other hand, by hypothesis, there is z in the cut J such that $\psi(u, v_0, z, \overline{p})$. This entails that $w_0 \subseteq z$. By property 1 above, w_0 is also in the cut J. ⊣

Lemma 5. *The theory* $\mathsf{I}\Delta_0 + \Omega_1 + \mathsf{B}\Sigma_1$ *is interpretable in* $\mathsf{I}\Delta_0 + \mathsf{B}\Sigma_1$.

Proof. The axiom Ω_1 says that $\forall x \forall y(x^{\log_2(\lceil y+1 \rceil)}\text{exists})$. It is well known that $\mathsf{I}\Delta_0 + \Omega_1$ is interpretable in $\mathsf{I}\Delta_0$ via the cut $C(x)$ defined by the formula $\forall y(x^{\log_2(\lceil y+1 \rceil)}$ exists): see, for instance, [11]. This very same cut provides an interpretation of $\mathsf{I}\Delta_0 + \Omega_1 + \mathsf{B}\Sigma_1$ into $\mathsf{I}\Delta_0 + \mathsf{B}\Sigma_1$. One has only to check that the scheme of collection for bounded arithmetic formulas holds in the cut C of a model of $\mathsf{I}\Delta_0 + \mathsf{B}\Sigma_1$. This follows from a minimality argument, as in the final step of the proof of the previous lemma. ⊣

Lemma 6. *The theory* BTFA *is interpretable in* $\mathsf{I}\Delta_0 + \Omega_1 + \mathsf{B}\Sigma_1$.

Proof. In fact, we show that BTFA is interpretable in $\Sigma^b_1 - \mathsf{NIA} + \mathsf{B}\Sigma_1$. *Prima facie*, the language $\mathcal{L}_2$ of BTFA has two sorts of variables: the individual sort and the set sort. In the first-order language $\mathcal{L}_1$ of the theory $\Sigma^b_1 - \mathsf{NIA} + \mathsf{B}\Sigma_1$, we reserve the even numbered variables v_0, v_2, v_4, etc. for the interpretation of the individual variables of $\mathcal{L}_2$, while the odd numbered variables v_1, v_3, v_5, etc. are reserved for the interpretation of the set variables of $\mathcal{L}_2$. To keep the notation simple, we will in fact identify the even numbered variables of $\mathcal{L}_1$ with the individual variables of $\mathcal{L}_2$. Moreover, we suppose that each set variable X_i of $\mathcal{L}_2$ is associated with the odd numbered variable v_{2i+1} of $\mathcal{L}_1$, and we will use Greek letters α, β, γ, etc. to stand for these odd numbered variables. In order to describe the domain of these Greek variables (no restriction is made in the domain of the even numbered variables), we consider – in the manner of a previous lemma – a 5-ary sw.q.-formula $U(e,x,y,p,c)$ with the universal property according to which, for every ternary sw.q.-formula $\psi(x,y,p)$, there is a (standard) $e \in 2^{<\omega}$ such that

$$\Sigma_1^b - \mathsf{NIA} \vdash \forall x \forall y \forall p(\psi(x,y,p) \leftrightarrow \exists c\, U(e,x,y,p,c)).$$

Now, the domain of the Greek variables is restricted to the formula

$$Set(\alpha) := \forall x(\exists w U(\alpha_0,x,w_0,\alpha_1,w_1) \leftrightarrow \forall w \neg U(\alpha_2,x,w_0,\alpha_3,w_1)),$$

where α is seen as the quadruple $(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$, and the variables w are seen as pairs (w_0,w_1). The identity interpretation (and the above remark on the identification of variables) takes care of the common language of $\mathcal{L}_1$ and $\mathcal{L}_2$, viz. $\mathcal{L}_1$. It remains to interpret the membership relation. It is done as follows:

$$x \in X :\leftrightarrow \exists w U(\alpha_0,x,w_0,\alpha_1,w_1),$$

where the variable X is associated with α. The above set-up induces, in a natural way, a translation ^{T} of formulas $\phi(\overline{x},\overline{X})$ of $\mathcal{L}_2$ into formulas $\phi^T(\overline{x},\overline{\alpha})$ of $\mathcal{L}_1$. It remains to check that the theory $\Sigma_1^b - \mathsf{NIA} + \mathsf{B}\Sigma_1$ proves all sentences ψ^T, whenever ψ is an axiom of BTFA. A proof of this fact follows closely the arguments of the proof of the last theorem of [8], viz. the result that BTFA is a conservative extension of the theory $\Sigma_1^b - \mathsf{NIA} + \mathsf{B}\Sigma_1$. In the following paragraphs we briefly outline those arguments.

Using bounded collection (a fragment thereof, to be more precise), we can recursively associate to each sw.q.-formula $\phi(\overline{x},\overline{X})$ two formulas $\phi_\Sigma(\overline{x},\overline{\alpha})$ and $\phi_\Pi(\overline{x},\overline{\alpha})$ of the form $\exists z \phi'_\Sigma(\overline{x},\overline{\alpha},z)$ and $\forall z \phi'_\Pi(\overline{x},\overline{\alpha},z)$ (respectively), with both $\phi'_\Sigma(\overline{x},\overline{\alpha},z)$ and $\phi'_\Pi(\overline{x},\overline{\alpha},z)$ sw.q.-formulas, such that the theory $\Sigma_1^b - \mathsf{NIA} + \mathsf{B}\Sigma_1$ proves

1. $\forall \overline{\alpha}[Set(\overline{\alpha}) \to \forall \overline{x}(\phi_\Sigma(\overline{x},\overline{\alpha}) \leftrightarrow \phi_\Pi(\overline{x},\overline{\alpha}))]$, and
2. $\forall \overline{\alpha}[Set(\overline{\alpha}) \to \forall \overline{x}(\phi^T(\overline{x},\overline{\alpha}) \leftrightarrow \phi_\Sigma(\overline{x},\overline{\alpha}))]$,

where, for $\overline{\alpha}$ the sequence $\alpha_1,\ldots,\alpha_n$, $Set(\overline{\alpha})$ abbreviates $\bigwedge_{k=1}^n Set(\alpha_k)$.

The universal property above and the existence of these formulas easily entail that the axioms of Δ_1^0(PT)-CA translate to sentences provable in $\Sigma_1^b - \mathsf{NIA} + \mathsf{B}\Sigma_1$.

Consider now a formula $\psi(x)$ of the form $\exists w \preccurlyeq t\, \phi(x,w)$, with ϕ a sw.q.-formula (ϕ may also have individual or set parameters, but we omit them for ease of reading). Take a such that $\psi^T(\epsilon) \wedge \neg\psi^T(a)$, in order to prove the existence of a c such that $c \subset a$, $c0 \subseteq a$ (say), $\psi^T(c)$, and $\neg\psi^T(c0)$. Using bounded collection (again, only a fragment thereof), it is not difficult to argue for the existence of an element b such that

$$\forall x \subseteq a \forall w \preccurlyeq t(\exists z \preccurlyeq b\, \phi'_\Sigma(x,w,z) \leftrightarrow \forall z \preccurlyeq b\, \phi'_\Pi(x,w,z)).$$

Therefore, $\forall x \subseteq a(\psi^T(x) \leftrightarrow \exists w \preccurlyeq t \exists z \preccurlyeq b\, \phi'_\Sigma(x, w, z))$. The element c can now be found by induction on notation applied to the Σ^b_1-formula $\exists w \preccurlyeq t \exists z \preccurlyeq b\, \phi'_\Sigma(x, y, z)$.

Finally, we need to argue that the translation of the bounded collection axioms are provable in $\Sigma^b_1 - \mathsf{NIA} + \mathsf{B}\Sigma_1$. This is a straightforward consequence of the fact that the mapping $\phi \mapsto (\phi_\Sigma, \phi_\Pi)$ can be extended to all bounded formulas ϕ, still assenting to properties 1 and 2 above, provided that we allow the formulas ϕ'_Σ and ϕ'_Π to be bounded (as opposed to mere sw.q.-formulas). Of course, extending this mapping uses (full) bounded collection essentially. ⊣

REFERENCES

[1] GEORGE BOOLOS and RICHARD JEFFREY, ***Computability and logic***, 2 ed., Cambridge University Press, 1990.

[2] WILFRIED BUCHHOLZ and WILFRIED SIEG, *A note on polynomial time arithmetic*, ***Logic and computation*** (Wilfried Sieg, editor), American Mathematical Society, 1990, pp. 51–55.

[3] SAMUEL BUSS, *Bounded arithmetic*, ***Ph.D. thesis***, Princeton University, June 1985, a revision of this thesis was published by Bibliopolis in 1986.

[4] ANDREA CANTINI, *Asymmetric interpretations for bounded theories*, ***Mathematical Logic Quarterly***, vol. 42 (1996), no. 1, pp. 270–288.

[5] FERNANDO FERREIRA, *Polynomial time computable arithmetic and conservative extensions*, ***Ph.D. thesis***, Pennsylvania State University, December 1988, pp. vii + 168.

[6] ———, *Polynomial time computable arithmetic*, ***Logic and computation*** (Wilfried Sieg, editor), American Mathematical Society, 1990, pp. 161–180.

[7] ———, *Stockmeyer induction*, ***Feasible mathematics*** (Samuel Buss and Philip Scott, editors), Birkhäuser, 1990, pp. 161–180.

[8] ———, *A feasible theory for analysis*, this JOURNAL, vol. 59 (1994), pp. 1001–1011.

[9] ———, *On end-extensions of models of ¬exp*, ***Mathematical Logic Quarterly***, vol. 42 (1996), pp. 1–18.

[10] HARVEY FRIEDMAN, *FOM: 73:Hilbert's program wide open?*, FOM e-mail list: http://www. math.psu.edu/simpson/fom/, December 20, 1999.

[11] PETR HÁJEK and PAVEL PUDLÁK, ***Metamathematics of first-order arithmetic***, Perspectives in Mathematical Logic, Springer-Verlag, 1993.

[12] KOSTAS HATZIKIRIAKOU, *Algebraic disguises of Σ^0_1 induction*, ***Archive for Mathematical Logic***, vol. 29 (1989), pp. 47–51.

[13] DAVID HILBERT and PAUL BERNAYS, ***Grundlagen der Mathematik***, 2 ed., Grundlehren der mathematischen Wißenschaften, Springer-Verlag, 1968-1970, two volumes.

[14] RICHARD KAYE, ***Models of Peano arithmetic***, Oxford Logic Guides, vol. 15, Clarendon Press, 1991.

[15] DONALD KNUTH, ***The art of computer programming. Seminumerical algorithms***, 2 ed., vol. 2, Addison-Wesley, 1981.

[16] KER-I KO, ***Complexity theory of real functions***, Birkhauser, 1991.

[17] ULRICH KOHLENBACH, *Mathematically strong subsystems of analysis with low rate of growth of provably recursive functionals*, ***Archive for Mathematical Logic***, vol. 36 (1996), pp. 31–71.

[18] ———, *Arithmetizing proofs in analysis*, ***Proceedings of the logic colloquium (1996)*** (J. Larrazabal, J. Lascar, and G. Mints, editors), Springer Lecture Notes in Logic, vol. 12, Springer-Verlag, 1998, pp. 115–158.

[19] ———, *Proof theory and computational analysis*, ***Electronic Notes in Theoretical Computer Science***, vol. 13 (1998), p. 34 pages, (http://www.elsevier.nl.locate/entcs/volume13.html).

[20] EDWARD NELSON, ***Predicative arithmetic***, Mathematical Notes, Princeton University Press, 1986.

[21] ALEXANDER RAZBOROV, *An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic*, ***Arithmetic, proof theory and computational complexity*** (Peter Clote and Jan Krajíček, editors), Clarendon Press, 1993, pp. 247–277.

[22] JOSEPH SHOENFIELD, ***Mathematical logic***, Addison-Wesley, 1967. Reprinted by Association for Symbolic Logic, 2001.

[23] STEPHEN SIMPSON, ***Subsystems of second-order arithmetic***, Perspectives in Mathematical Logic, Springer-Verlag, 1999.

[24] STEPHEN SIMPSON and JU RAO, *Reverse algebra*, ***Handbook of recursive mathematics. Volume 2: Recursive algebra, analysis and combinatorics***, Studies in Logic and the Foundations of Mathematics, vol. 139, Elsevier, 1998, pp. 1355–1372.

[25] STEPHEN SIMPSON and RICK SMITH, *Factorization of polynomials and Σ_1^0 induction*, ***Annals of Pure and Applied Logic***, vol. 31 (1986), pp. 289–306.

[26] GAISI TAKEUTI, *RSUV isomorphisms*, ***Arithmetic, proof theory and computational complexity*** (Peter Clote and Jan Krajíček, editors), Clarendon Press, 1993, pp. 364–386.

[27] ALFRED TARSKI, *A decision method for elementary algebra and geometry*, ***Technical report***, Rand Corporation, 1958.

[28] TAKESHI YAMAZAKI, *Reverse mathematics and basic feasible systems of 0-1 strings*, manuscript, 8 pages, 2000. To appear in "Reverse Mathematics 2001" (ed. Stephen Simpson).

[29] ———, *Some more conservation results on the Baire category theorem*, ***Mathematical Logic Quarterly***, vol. 46 (2000), pp. 105–110.

DEPARTAMENTO DE MATEMÁTICA, INSTITUTO SUPERIOR TÉCNICO
AV. ROVISCO PAIS, 1096 LISBOA CODEX, PORTUGAL
E-mail: amfernandes@netcabo.pt

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE DE LISBOA
RUA ERNESTO DE VASCONCELOS, BLOCO C1-3, P-1749-016 LISBOA, PORTUGAL
E-mail: ferferr@cii.fc.ul.pt