Formalizing Scientifically Applicable Mathematics in a Definitional Framework

ARNON AVRON
School of Computer Science, Tel Aviv University

and
LIRON COHEN
School of Mathematical Sciences, Tel Aviv University

In [3] a new framework for formalizing mathematics was developed. The main new features of this framework are that it is based on the usual first-order set theoretical foundations of mathematics (in particular, it is type-free), but it reflects real mathematical practice in making an extensive use of statically defined abstract set terms of the form $\{x \mid \varphi\}$, in the same way they are used in ordinary mathematical discourse.

In this paper we show how large portions of fundamental, scientifically applicable mathematics can be developed in this framework in a straightforward way, using just a rather weak set theory which is predicatively acceptable and essentially first-order. The key property of that theory is that every object which is used in it is defined by some closed term of the theory. This allows for a very concrete, computationally-oriented interpretation of the theory. However, the development is not committed to such interpretation, and can easily be extended for handling stronger set theories (including ZF).

1. INTRODUCTION

While formalized mathematics and mathematical knowledge management (MKM) are bound to ultimately have a huge impact on the culture of mathematical practice and education, the past decades have unfortunately seen an increasing estrangement between the reality of informal mathematical practice and computer-implemented theorem proving. On one hand, type-free set theory is viewed by most mathematicians as the foundation of the mathematics they practice, and as such it is the most natural framework for MKM, especially for goals like those of the AUTOMATH project ([30, 23, 9]) and the QED manifesto ([5, 29]). On the other hand, most of the current work in the field of formalized mathematics and MKM is devoted to approaches and systems that are rather different from the set theoretical one. It either employs sophisticated type theories, with different notions of constructibility and computation that move more and more away from the common ground of "standard" mathematics and its standard first-order foundations (like in Coq [6, 7] or Nuprl [8]), or it uses various fractions of higher-order logic which are able to cover relevant parts of mathematics, without ever aiming at the full spectrum (like in Isabelle/HOL [24]).[1]

[1] Two notable exceptions are Mizar [25, 26] and Metamath [21]. However, the approaches used there are very different from the one we are going to use in this work.

We believe that the use for MKM of *convenient* set-theoretical frameworks could help overcome this increasing rift between what most mathematicians consider to be the basis of mathematics and what existing formal-reasoning systems actually implement, and will allow mathematics to be formalized and managed in as natural terms as possible. However, for doing this satisfactorily one should tackle the serious gaps that exist between the "official" formulations of set theory (such as Zermelo-Fraenkel Set Theory ZF) and actual mathematical practice. In particular: the language of such a framework should provide strong, direct means for defining objects, akin to those used in informal mathematical texts.

In [3] a new framework of the above sort for formalizing mathematics was developed. Its main advantages are that it is close in spirit and formulation to ZF on one hand, while the language it employs has great definitional power on the other (yet this language includes nothing that is not used in ordinary mathematical discourse). In particular: the language is type-free, and makes an extensive use of abstract set terms of the form $\{x \mid \varphi\}$. A crucial property of those terms is that unlike those used in current mathematical texts, their introduction does not depend on proving first corresponding existence theorems. Instead they are *statically* defined in a precise formal way (using the mechanism of safety relations). This feature makes the framework a congenial environment for practicing standard mathematics, which is also appropriate for mechanical manipulations and for interactive theorem proving.

The work reported in this paper is a part of a project which has two main goals:

(1) The first is to explore what parts of "everyday" mathematics can be carried out within the framework suggested in [3], in a way that reflects how rigorous mathematics is (informally) presented in standard textbooks.

(2) In [10, 11, 12] it was forcefully argued by Feferman that already predicative mathematics suffices for developing all of scientifically applicable mathematics, i.e. the mathematics that is actually indispensable to present-day natural science. This predicativist program is essentially based on the principle that higher-order constructs, such as sets or functions, are acceptable only when introduced through non-circular definitions. The second goal of our project is to show that this definitional approach to mathematics can be implemented in a user friendly way, without essential conflicts with mathematical practice.

The goal of this paper is to examine to what extent the above goals can be achieved within the above-mentioned framework when we restrict ourselves to the first-order level, and use a rather weak, predicatively acceptable, set theory. We show that large portions of fundamental scientifically applicable mathematics can be straightforwardly formalized in such a theory. The key feature of the theory we investigate is that it is definitional in the sense that every object which is used is defined by some closed term of the theory. This allows for a very concrete, computationally-oriented interpretation of the theory. However, the development is not committed to such interpretations, and the framework can easily be extended for handling stronger set theories (including ZF).

The paper is organized as follows: In Section 2 we present the basic language and theory. In Section 3 we show how the standard set theoretical notions are dealt with in our system. Section 4 introduces the natural numbers in our framework. In Section 5 we outline how classical analysis can be developed within the resulting framework in a natural, predicatively acceptable way. This includes the introduction of the real line and functions, and formulating and proving the main classical results concerning these notions. We conclude with directions for future continuation of the work.

2. THE LANGUAGE $\mathcal{L}^C_{RST}$ AND THE SYSTEM RST^C

We start by recalling the most basic formal systems for set theory presented in [4, 3]. To avoid confusion, we use different kinds of parentheses for collections in our formal language and in the meta-language in which the paper is written. The parentheses $⦃\,⦄$ will be used in our formal languages $\mathcal{L}^C_{RST}$, while for a collection defined in the meta-language we use $\{\,\}$. We use uppercase letters $X, Y, Z, ...$ for collections in the meta-language, Φ, Θ for sets of variables, and $x, y, z, ...$ for variables in the formal languages. We denote by $Fv(exp)$ the set of free variables of exp, and by $\varphi\left\{\frac{t_1}{x_1}, ..., \frac{t_n}{x_n}\right\}$ the result of simultaneously substituting t_i for the free occurrences of x_i in φ $(i = 1, ..., n)$. Note that at present we take the meta-language to be the language of ZF or more correctly GB [22], and the theorems to follow can all be formulated and proven in GB. However, we believe that this can also be done in weaker systems. This is left for further work.

One of the foundational questions in set theory is which formulas should be excluded from defining sets by an abstract term of the form $\{x \mid \varphi\}$ in order to avoid the paradoxes of naive set theory. More generally, the question is: what formulas can be taken as defining a construction of a set from given objects (including other sets)? Various set theories provide different answers to this question. Usually these answers are based on *semantical* considerations (such as the limitation of size doctrine [13, 15]). Such an approach is not very useful for the purpose of mechanization. In this work we use instead the general *syntactic* methodology of safety relations developed in [1, 3, 4].

A safety relation is a syntactic relation between formulas and sets of variables. The addition of a safety relation to a logical system allows to use in it statically defined abstract set term of the form $\{x \mid \varphi\}$, provided that φ is safe with respect to $\{x\}$. Intuitively, a statement of the form "φ is *safe* with respect to $\{y_1, ..., y_k\}$", where $Fv(\varphi) = \{x_1, ..., x_n, y_1, ..., y_k\}$, has the meaning that for every "accepted" sets $a_1, ..., a_n$, the collection $\{\langle y_1, ..., y_k\rangle \mid \varphi(a_1, ..., a_n, y_1, ..., y_k)\}$ is an "accepted" set, which is constructed from the previously "accepted" sets $a_1, ..., a_n$. Predicatively (or definitionally) acceptable safety relations are those which determine the sets they define in an absolute way, independently of any "surrounding universe".

Definition 1. Let C be a finite set of constants. The language $\mathcal{L}^C_{RST}$ and the associated safety relation $\succ_C$ are simultaneously defined as follows:

—Terms:

—Every variable is a term.

—Every $c \in C$ is a term (taken to be a constant).

—If x is a variable and φ is a formula such that $\varphi \succ_C \{x\}$, then $⦃x \mid \varphi⦄$ is a term (for which $Fv\,(⦃x \mid \varphi⦄) = Fv\,(\varphi) - \{x\}$).

—Formulas:

—If t and s are terms, then $t = s$ and $t \in s$ are atomic formulas.

—If φ and ψ are formulas and x is a variable, then $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi)$, and $\exists x\varphi$ are formulas.

—The safety relation $\succ_C$ is defined as follows:

—If φ is an atomic formula, then $\varphi \succ_C \emptyset$.

—If t is a term such that $x \notin Fv(t)$, and $\varphi \in \{x \in x, x \in t, x = t, t = x\}$, then $\varphi \succ_C \{x\}$.

—If $\varphi \succ_C \emptyset$, then $\neg\varphi \succ_C \emptyset$.

—If $\varphi \succ_C \Theta$ and $\psi \succ_C \Theta$, then $\varphi \vee \psi \succ_C \Theta$.

—If $\varphi \succ_C \Theta$ and $\psi \succ_C \Phi$, and either $\Phi \cap Fv(\varphi) = \emptyset$ or $\Theta \cap Fv(\psi) = \emptyset$, then $\varphi \wedge \psi \succ_C \Theta \cup \Phi$.

—If $\varphi \succ_C \Theta$ and $y \in \Theta$, then $\exists y\varphi \succ_C \Theta - \{y\}$.

In case $C = \emptyset$ we write $\mathcal{L}_{RST}$ instead of $\mathcal{L}_{RST}^{\emptyset}$ and $\succ$ instead of $\succ_{\emptyset}$.

Remark 2. The notion of a term being free for substitution in $\mathcal{L}_{RST}^{C}$ has to be generalized, since in $\mathcal{L}_{RST}^{C}$, unlike in first-order logic, a variable can be bound within a term. The generalization amounts to avoiding the capture of free variables within the scope of a binding operator.

Remark 3. It is easy to see that $\succ_C$ has the following properties:

—If $\varphi \succ_C \Theta$ and $\Phi \subseteq \Theta$, then $\varphi \succ_C \Phi$.

—If $\varphi \succ_C \Theta$, $x \in \Theta$, and $y \notin Fv(\varphi)$, then $\varphi\left\{\frac{y}{x}\right\} \succ_C \Theta - \{x\} \cup \{y\}$.

—If $\varphi \succ_C \Theta$ and $x \in \Theta$, then $\varphi\left\{\frac{t}{x}\right\} \succ_C \Theta - \{x\}$.

—If $\varphi \succ_C \Theta$ and $x \notin \Theta$, then $\varphi\left\{\frac{t}{x}\right\} \succ_C \Theta - Fv(t)$.

—If $\varphi \succ_C \{x_1, ..., x_n\}$ and $\psi \succ_C \emptyset$, then $\forall x_1, ..., x_n (\varphi \to \psi) \succ_C \emptyset$. [2]

—If $x \notin Fv(t)$ and $\varphi \succ_C \emptyset$, then $\forall x (x \in t \to \varphi) \succ_C \emptyset$ and $\exists x (x \in t \wedge \varphi) \succ_C \emptyset$. Hence, $\varphi \succ_C \emptyset$ for every Δ_0 formula in $\mathcal{L}_{ZF}$.

Definition 4. The system RST^C is the first-order system in $\mathcal{L}_{RST}^{C}$ which is based on the following axioms:

—Extensionality: $\forall z (z \in x \leftrightarrow z \in y) \to x = y$

—The Comprehension Schema: $\forall x (x \in \{\!\!\{x \mid \varphi\}\!\!\} \leftrightarrow \varphi)$

—The $\in$-induction Schema: $\left(\forall x \left(\forall y \left(y \in x \to \varphi\left\{\frac{y}{x}\right\}\right) \to \varphi\right)\right) \to \forall x\varphi$

Note. As explained in [3], with the exception of the infinity axiom (which will be handled in the sequel), the other comprehension axioms of ZF can be incorporated by adding corresponding clauses to the definition of the safety relation:

—The full power of the separation scheme can be achieved be assuming that $\varphi \succ_C \emptyset$ for any φ (not only atomic ones).

—The power set axiom is equivalent to letting $x \subseteq t \succ_C \{x\}$ in case $x \notin Fv\{t\}$[3].

—The full power of replacement is achieved by letting $\exists y\varphi \wedge \forall y (\varphi \to \psi) \succ_C \Theta$ if $\psi \succ_C \Theta$ and $\Theta \cap Fv(\varphi) = \emptyset$.

[2] Though $\mathcal{L}_{RST}^{C}$ officially does not include $\forall$ and $\to$, we take $\forall x (\varphi \to \psi)$ as an abbreviation for $\neg\exists x (\varphi \wedge \neg\psi)$.

[3] Here we can take the usual definition of $\subseteq$ in terms of $\in$. However, it will be better to add $\subseteq$ as a new primitive symbol, together with the corresponding axiom connecting it to $\in$.

Definition 5. A *universe* (of sets) is a transitive collection of sets which is closed under rudimentary operations [14, 18].[4]

Notation. We denote by $v\,[x := a]$ the x-variant of v which assigns a to x. If $\vec{x}$, $\overrightarrow{a}$ are two vectors of the same length we abbreviate $v\,[x_1 := a_1, ..., x_n := a_n]$ by $v\,[\vec{x} := \overrightarrow{a}]$. We denote by $[x_1 := a_1, ..., x_n := a_n]$ (or just by $[\vec{x} := \overrightarrow{a}]$) any assignment which assigns to each x_i the element a_i.

Definition 6. Let W be a universe which interprets all the constants in C, and let v be an assignment in W. For any term t and formula φ of $\mathcal{L}^C_{RST}$, we recursively define $\|t\|^v_W$ (designed to be an element of W) and $\|\varphi\|^v_W \in \{\mathbf{t}, \mathbf{f}\}$ by:

—$\|x\|^v_W = v\,(x)$ for x a variable.
—$\|c\|^v_W = c^W$ (the interpretation of c in W) for $c \in C$.
—$\|\{\!\!\{x \mid \varphi\}\!\!\}\|^v_W = \left\{a \mid a \in W \wedge \|\varphi\|^{v[x:=a]}_W = \mathbf{t}\right\}$
—$\|t = s\|^v_W = \mathbf{t}$ iff $\|t\|^v_W = \|s\|^v_W$; $\|t \in s\|^v_W = \mathbf{t}$ iff $\|t\|^v_W \in \|s\|^v_W$
—$\|\neg\varphi\|^v_W = \mathbf{t}$ iff $\|\varphi\|^v_W = \mathbf{f}$
—$\|\varphi \wedge \psi\|^v_W = \mathbf{t}$ iff $\|\varphi\|^v_W = t \wedge \|\psi\|^v_W = \mathbf{t}$
—$\|\varphi \vee \psi\|^v_W = \mathbf{t}$ iff $\|\varphi\|^v_W = t \vee \|\psi\|^v_W = \mathbf{t}$
—$\|\exists x\varphi\|^v_W = \mathbf{t}$ iff $\exists a \left(a \in W \wedge \|\varphi\|^{v[x:=a]}_W = \mathbf{t}\right)$

Remark. $\|t\|^v_W$ denotes the value in W that the term t gets under v, and $\|\varphi\|^v_W$ denotes the truth value of the formula φ under W and v.

Proposition 7. *Let W be a universe which interprets all the constants in C. If t is a term of $\mathcal{L}^C_{RST}$, then for any assignment v in W, $\|t\|^v_W$ is an element of W.*

Proof. The proof is carried out by simultaneous induction on terms t and formulas φ, where for the latter we prove the following for any assignment v in W:

—If $\varphi \succ_C \{y_1, ..., y_n\}$ and $n > 0$, then $\left\{\langle a_1, ..., a_n\rangle \in W^n \mid \|\varphi\|^{v[\vec{y}:=\overrightarrow{a}]}_W = \mathbf{t}\right\} \in W$.

—If $\varphi \succ_C \emptyset$ and $X \in W$ then $\left\{\langle a_1, ..., a_n\rangle \in X^n \mid \|\varphi\|^{v[\vec{y}:=\overrightarrow{a}]}_W = \mathbf{t}\right\} \in W$.

It is straightforward to see that the result holds when t is a variable or a constant. If t is of the form $\{\!\!\{x \mid \varphi\}\!\!\}$ the claim follows from the induction hypothesis for φ (since $\varphi \succ_C \{x\}$). For atomic formulas the claim easily follows from the induction hypothesis for terms and the fact that W is closed under rudimentary operations. For φ a compound formula the claim again holds since W is closed under rudimentary operations. We demonstrate the most difficult case as an example. So assume that $\varphi = \psi \wedge \theta$, where $\psi \succ_C \Theta$, $\theta \succ_C \Phi$, and $\Phi \cap Fv\,(\psi) = \emptyset$. To simplify notation, assume that $Fv\,(\psi) = \{x, z\}$, $Fv\,(\theta) = Fv\,(\varphi) = \{x, y, z\}$, $\Theta = \{x\}$, and $\Phi = \{y\}$. In this case $\varphi \succ_C \{x, y\}$, and we show that $D = \left\{\langle a, b\rangle \in W^2 \mid \|\varphi\|^{v[x:=a, y:=b]}_w = \mathbf{t}\right\} \in W$.

[4] The standard notion is "rudimentary function". We prefer to use instead the term "rudimentary operation", since we want to reserve the term "function" for functions in the sense used in basic courses in set theory or discrete mathematics, i.e. *sets* of ordered pairs which satisfy the functionality condition.

Since $\psi \succ_C \{x\}$ we have that $\left\{a \in W \mid \|\psi\|_W^{v[x:=a]} = \mathbf{t}\right\} \in W$ for any v. In particular, for any $c \in W$ $A_c = \left\{a \in W \mid \|\psi\|_W^{[x:=a,z:=c]} = \mathbf{t}\right\} \in W$. Since $\theta \succ_C \{y\}$, by the induction hypothesis we have that for any $c \in W$, if $d \in A_c$ then $B_{c,d} = \left\{b \in W \mid \|\theta\|_W^{[x:=d,y:=b,z:=c]} = \mathbf{t}\right\} \in W$. Now, D equals to $\bigcup_{d \in A_c} (\{d\} \times B_{c,d})$. Hence the closure of W under rudimentary operations implies that $D \in W$. □

Notation. In case *exp* is a closed term or a closed formula we denote by $\|exp\|_W$ the value of *exp* in W, and at times we omit the W and simply write $\|exp\|$.

Proposition 8. *Every universe is a model of RST^C.*[5]

Proof. Easily follows from Prop. 7. □

Note. The converse of the last proposition is also true, i.e., any transitive collection of sets which is a model of RST^C is a universe (see [2]).[6]

The following simple lemma will be useful in the sequel.

Lemma 9 (Substitution Theorem)**.** *Let $t, s_1, ..., s_n$ be terms and φ a formula of* $\mathcal{L}_{RST}^C$. If v is an assignment in W, then:

—$\left\|t\left\{\frac{s_i}{x_i}, ..., \frac{s_n}{x_n}\right\}\right\|_W^v = \|t\|_W^{v\left[x_1:=\|s_1\|_W^v,...,x_n:=\|s_n\|_W^v\right]}$

—$\left\|\varphi\left\{\frac{s_i}{x_i}, ..., \frac{s_n}{x_n}\right\}\right\|_W^v = \|\varphi\|_W^{v\left[x_1:=\|s_1\|_W^v,...,x_n:=\|s_n\|_W^v\right]}$

Next we want to show that the meaning of terms in $\mathcal{L}_{RST}^C$ is actually independent of W. The following theorem is a more precise and more general formulation of a theorem proven in [4].

Theorem 10. *Let W_1, W_2 be two universes which agree on the interpretations of all $c \in C$.*

(1) If v_1, v_2 are assignments in W_1 and W_2 respectively that agree on the values of all the free variables in a term t, then $\|t\|_{W_1}^{v_1} = \|t\|_{W_2}^{v_2}$.

(2) If v_1, v_2 are assignments in W_1 and W_2 respectively that agree on the values of all the free variables in a formula φ, then $\|\varphi\|_{W_1}^{v_1} = \|\varphi\|_{W_2}^{v_2}$.

Proof. The proof is carried out by simultaneous induction on t and φ (similar to the proof in [4]). □

Theorem 10 entails that every term of $\mathcal{L}_{RST}^C$ has the same interpretation in all transitive models of RST^C (i.e. universes) which contains the values of its parameters and interprets the constants in C in the same way. Thus the identity of the set denoted by a term t is independent of the exact extension of the assumed surrounding universe of sets. A formula is safe with respect to $\{x_1, ..., x_n\}$ if it has the same extension (which should be a set) in all universes which contains the

[5] The more precise formulation of the proposition is as follows: Let W be a universe. By assigning the obvious interpretations to the symbols $\in$ and $=$ and assigning some interpretations in W for the constants in C, we get a model of RST^C.

[6] The system in [2] was RST, however, the addition of the constants C does not make a difference.

values of its other parameters. In particular: $\varphi \succ_C \emptyset$ iff it is absolute relative to RST^C in the usual sense of set theory (see e.g. [19]), while $\varphi \succ_C Fv\left(\varphi\right)$ iff it is domain-independent in the sense of database theory (see e.g. [27]) for universes. Note again that a universe is here any transitive collection of sets which is closed under rudimentary operations. For instance, we can take W to be V, the cumulative universe of ZF (with the obvious interpretations of the symbols $\in$ and $=$)[7]. We can also take W to be V_κ for any κ such that V_κ is a universe. However, W can also be taken as a much smaller, and very concrete set. Thus in [28], J_2 (the second set in Jensen's constructible hierarchy) was implicitly chosen. This is in fact the minimal universe which includes an infinite set. Still, for our purposes bigger constructible sets, like J_ω or J_{ω^ω}, are better choices.

Definition 11.

—If t is a closed term we say that t *defines the set* $\|t\|_W$. The set X is called *definable* if there is a closed term t such that $\|t\|_W = X$.

—If t is a term with $Fv\left(t\right) \subseteq \{x_1, ...x_n\}$ we say that t *defines the operation* F_t that for any $\langle A_1, ..., A_n\rangle \in W^n$ returns the set $\|t\|_W^{[x_1:=A_1,...,x_n:=A_n]}$.

Note. We use above the term “operation” because F_t might be a proper *class* of ordered pairs. (The existence of such class for every term t can be proved in GB.)

Terminology. From now on we use the term “operation" for functions on the entire universe which are defined by some term.

Notation. If s is a term free for substitution for x in t, and F_t is an operation we write $\hat{F}_t\left(s\right)$ instead of $t\left\{\frac{s}{x}\right\}$. Hence $\hat{F}_t\left(s\right) = y$ is an abbreviation for $t\left\{\frac{s}{x}\right\} = y$, and so if $y \notin Fv\left(t\right) \cup Fv\left(s\right) \setminus \{x\}$, then $\hat{F}_t\left(s\right) = y \succ_C \{y\}$. (Intuitively, $\hat{F}_t\left(s\right) = y$ means that the result of the application of the operation F_t to the object denoted by s is the object denoted by y.)

The following theorem is also proven in [4].

Theorem 12. *If F is an n-ary rudimentary operation, then there exists a formula φ_F such that:*

—$Fv\left(\varphi_F\right) \subseteq \{y, x_1, ..., x_n\}$.

—$\varphi_F \succ_C \{y\}$.

—$F\left(x_1, ..., x_n\right) = \{y \mid \varphi_F\}$.

Corollary 13. *Every rudimentary operation is indeed an operation in the sense defined above (i.e., is definable by some term of $\mathcal{L}^C_{RST}$).*

3. BASIC SET THEORETICAL NOTIONS

In $\mathcal{L}^C_{RST}$ we can introduce as abbreviations many standard notations used in mathematics and prove their basic properties in RST^C. Here are some examples:

—$\emptyset := \{\!\!|x \mid x \in x|\!\!\}$.

—$\{\!\!|t_1, ..., t_n|\!\!\} := \{\!\!|x \mid x = t_1 \vee ... \vee x = t_n|\!\!\}$ (where x is fresh).

[7] As for the constants in C we will use in this paper, each of them will have some obvious intended interpretation too.

—$\langle s,t\rangle := \lBrace\lBrace s\rBrace, \lBrace s,t\rBrace\rBrace$. $\langle t_1,...,t_n\rangle := \langle\langle t_1,...,t_{n-1}\rangle, t_n\rangle$.
—$\lBrace x\in t \mid \varphi\rBrace := \lBrace x \mid x\in t\wedge\varphi\rBrace$, provided $\varphi\succ_C \emptyset$ and $x\notin Fv\left(t\right)$.
—$\lBrace t \mid x\in s\rBrace := \lBrace y \mid \exists x.x\in s\wedge y=t\rBrace$, where y is a fresh variable and $x\notin Fv\left(s\right)$.
—$s\times t := \lBrace x \mid \exists a\exists b.a\in s\wedge b\in t\wedge x=\langle a,b\rangle\rBrace$, where x,a,b are fresh.
—$s\cup t := \lBrace x \mid x\in s\vee x\in t\rBrace$, where x is fresh.
—$s\cap t := \lBrace x \mid x\in s\wedge x\in t\rBrace$, where x is fresh.
—$\cup t := \lBrace x \mid \exists y\in t.x\in y\rBrace$, where x,y are fresh.
—$\cap t := \lBrace x \mid x\in\cup t\wedge\forall y\in t.x\in y\rBrace$, where x,y are fresh.
—$\iota x.\varphi := \cup\lBrace x \mid \varphi\rBrace$, provided $\varphi\succ_C \{x\}$.[8]
—$dom\left(t\right) := \lBrace x \mid \exists z\exists v\exists y.z\in t\wedge v\in z\wedge y\in v\wedge x\in v\wedge z=\langle x,y\rangle\rBrace$, where z,v,x, and y are fresh.
—$rng\left(t\right) := \lBrace y \mid \exists z\exists v\exists x.z\in t\wedge v\in z\wedge y\in v\wedge x\in v\wedge z=\langle x,y\rangle\rBrace$, where z,v,x, and y are fresh.

It is routine to verify that all these terms are indeed well-defined, and that their basic properties are provable in RST^C. For example, $\forall x\left(x\in\cup t\leftrightarrow\exists y\in t.x\in y\right)$ is a trivial consequence of the comprehension axiom and the definition of $\cup t$.

The fact that $\langle s,t\rangle$ is a term in our language implies only that if $z\notin Fv\left(t\right)\cup Fv\left(s\right)$ then $z=\langle s,t\rangle\succ_C\{z\}$ and $\langle s,t\rangle=z\succ_C\{z\}$. However, in [3] another formula was constructed that states that t is equal to the ordered pair $\langle r,s\rangle$:

$$t\check{=}\langle r,s\rangle := \exists u\exists v\left(P\left(t,u,v\right)\wedge P\left(u,r,r\right)\wedge P\left(v,r,s\right)\right)$$

where $P\left(t,x,y\right) = x\in t\wedge y\in t\wedge\forall w\left(w\in t\rightarrow w=x\vee w=y\right)$ and w is a fresh variable. Denote by $\langle r,s\rangle\check{\in}t$ the formula: $\exists u\in t\left(u\check{=}\langle r,s\rangle\right)$ where u is a fresh variable which does not occur in t,r or s. The following is then proved in [3]:

Proposition 14.

(1) $t\check{=}\langle x,y\rangle\succ_C\{x,y\}$ *provided* $x,y\notin Fv\left(t\right)$.
(2) $\langle x,y\rangle\check{\in}t\succ_C\{x,y\}$ *provided* $x,y\notin Fv\left(t\right)$.
(3) $\vdash_{RST^C} r=\langle s,t\rangle\leftrightarrow r\check{=}\langle s,t\rangle$

Note that we can extract the first and second coordinate of a pair by

$$P_1\left(z\right) := \iota x.\exists y.z\check{=}\langle x,y\rangle \;\;,\;\; P_2\left(z\right) := \iota y.\exists x.z\check{=}\langle x,y\rangle$$

Proposition 15. $\{\langle x_1,...,x_n\rangle \mid \varphi\}$ *is a definable set, provided* $\varphi\succ_C\{x_1,...,x_n\}$ *and* $Fv\left(\varphi\right)\subseteq\{x_1,...,x_n\}$.

Proof. For z a fresh variable $\exists x_1...\exists x_n\left(\varphi\wedge z=\langle x_1,...,x_n\rangle\right)\succ_C\{z\}$, and $\{z\} = Fv\left(\exists x_1...\exists x_n\left(\varphi\wedge z=\langle x_1,...,x_n\rangle\right)\right)$, thus $\{\langle x_1,...,x_n\rangle \mid \varphi\}$ is definable by the term $\lBrace z \mid \exists x_1...\exists x_n\left(\varphi\wedge z=\langle x_1,...,x_n\rangle\right)\rBrace$. □

Proposition 16. *Let F_t be an operation. The result of the application of F_t to definable sets is a definable set.*

[8] Due to the extensionality axiom, if $\varphi\succ_C\{x\}$, then the term above for $\iota x.\varphi$ denotes $\emptyset$ if there is no set which satisfies φ, and it denotes the union of all the sets which satisfy φ otherwise. In particular: if there is exactly one set which satisfies φ, then $\iota x.\varphi$ denotes this unique set.

Proof. Suppose $Fv\,(t) = \{x_1, ..., x_n\}$. If $A_1, ..., A_n$ are definable sets then there exist terms $s_1, ..., s_n$ that define them (respectively), and $F_t\,(A_1, ..., A_n) = \left\| t\left\{\frac{s_1}{x_1}, ..., \frac{s_n}{x_n}\right\}\right\|_W = \|t\|_W^{\left[x_1 := \|s_1\|_W, ..., x_n := \|s_n\|_W\right]}$. □

Corollary 17. *The result of any application of a rudimentary operation to definable sets is a definable set. In particular, if X, Y are definable sets, so are $X \cup Y$, $X \cap Y$, $X - Y$, $X \times Y$, $\cup X$, $\cap X$, $dom\,(X)$, and $rng\,(X)$.*

The standard definition of a set being a relation or a function are available in $\mathcal{L}_{RST}$ in the form of formulas which are safe w.r.t $\emptyset$.

—$Rel\,(r) := \forall z \in r \exists x, y.z \check{\doteq} \langle x, y\rangle$
—$Func\,(f) := Rel\,(f) \wedge \forall a, b, c.\,(\langle a, b\rangle \,\check{\in} f \wedge \langle a, c\rangle \,\check{\in} f) \to b = c$

It is straightforward to prove the following:

Lemma 18. *The standard operations on relations (such as: composition, inverse, domain and range) are definable operations, and their basic properties are provable in RST^C.*

In $\mathcal{L}_{RST}^C$ we can also introduce as abbreviations standard notations for handling functions as they are used in mathematics. For example:

—$\lambda x \in s.t := \{\!\{\langle x, t\rangle \mid x \in s\}\!\}$, provided $x \notin Fv\,(s)$.
—$f\,(x) := \iota y.\,\langle x, y\rangle \,\check{\in} f$ where y is a fresh variable.
—$f \restriction s := \{\!\{\langle x, f\,(x)\rangle \mid x \in s\}\!\}$

Proposition 19.

(*1*) *The β and η rules obtain in RST^C, i.e. the followings are provable in RST^C:*

$$u \in s \to (\lambda x \in s.t)\,u = t\left\{\frac{u}{x}\right\} \quad \text{where } u \text{ is free for } x \text{ in } t$$
$$u \notin s \to (\lambda x \in s.t)\,u = \emptyset \quad \text{where } u \text{ is free for } x \text{ in } t$$
$$(\lambda x \in s.t)\,x = t \restriction s \quad \text{where } x \notin Fv\,(t)$$

(*2*) *The following is provable in RST^C:*

$$(Func\,(f)) \to (Func\,(f \restriction a) \wedge \forall x \in a.f\,(x) = (f \restriction a)\,(x))$$

(*3*) *Let f, g be variables. Then there exists a term $g \circ f$ s.t. $Fv\,(g \circ f) = \{g, f\}$ and the following is provable in RST^C:*

$$(Func\,(f) \wedge Func\,(g)) \to (Func\,(g \circ f) \wedge \forall x.\,(g \circ f)\,(x) = g\,(f\,(x)))$$

(*4*) *Let f, g be variables. Then there exists a term $g \dot{\cup} f$ s.t. $Fv\,(g \dot{\cup} f) = \{g, f\}$ and the following is provable in RST^C:*

$$(Func\,(f) \wedge Func\,(g) \wedge Dom\,(f) \cap Dom\,(g) = \emptyset) \to [Func\,(g \dot{\cup} f) \wedge$$
$$(\forall x \in Dom\,(f)\,.\,(g \dot{\cup} f)\,(x) = f\,(x)) \wedge (\forall x \in Dom\,(g)\,.\,(g \dot{\cup} f)\,(x) = g\,(x))]$$

Proof. The proofs are all straightforward. For example, in (3) we take $g \circ f$ to be the term $\{\!\{z \mid \exists a, b, c.\,\langle a, b\rangle \,\check{\in} f \wedge \langle b, c\rangle \,\check{\in} g \wedge \langle a, c\rangle = z\}\!\}$. □

Proposition 20. *If F is an operation (i.e. $F = F_t$ for some term t), then:*

—It is provable in RST^C that for any set A, $F \upharpoonright A$ is a function.

—If A is a definable set, so is $F \upharpoonright A$.

Proof. Denote by $F \upharpoonright a$ the term $\{\!\!\{ \left\langle x, \hat{F}(x) \right\rangle \mid x \in a \}\!\!\}$ for a a fresh variable. It is easy to prove in RST^C that for any a, $F \upharpoonright a$ is a binary relation which satisfies the functionality condition. This proves the first part of the proposition. For the second part, note that if there is a term s_A that defines A then the closed term $(F \upharpoonright a)\left\{\frac{s_A}{a}\right\}$ defines $F \upharpoonright A$. □

Corollary 21 (Restricted axiom of replacement)**.** *If F is an operation, then:*

—It is provable in RST^C that the image of every set under F is a set.

—If A is a definable set, so is $F[A]$.

Proof. The first part easily follows by taking $F[a] := rng(F \upharpoonright a)$. For the second part of the claim, notice that if A is a definable set, so is $F \upharpoonright A$, and by Corollary 17, so is $rng(F \upharpoonright A)$. □

4. THE NATURAL NUMBERS

The collection of hereditary finite sets is the minimal model of RST^C; hence $\mathbb{N}$ (the set of natural numbers) is not definable as a set in $\mathcal{L}^C_{RST}$. Therefore, in order to introduce $\mathbb{N}$ as a set we need to extend our language and our system. There are several ways to do this. One possible route is to extend the safety relation. However, in order to do so while preserving the syntactical, *compositional* approach, one has to extend the language as well. Since in this paper we want to stick to the first-order level, this is best done by adding new constants together with corresponding characterizing axioms.[9] Thus, in this paper we enhance RST^C by including in C a constant whose intended interpretation is the set HF of all hereditary finite sets. In addition, we add to RST^C counterparts of Peano's axioms which ensure (as far as possible on the first-order level) that HF is indeed interpreted as this set.[10]

Conventions.

(1) In the rest of the paper we assume that C includes the constant HF.

(2) From now on we shall use the same symbols in the language and in the meta-language for standard sets, relations, functions and operations. Thus both the formal language and the meta-language will use HF to denote the set of hereditary finite sets, while $\mathbb{N}$ will be used to denote the set of natural numbers, as well the term which defines it in the formal language.

Definition 22. The system RST^C_{HF} for the language $\mathcal{L}^C_{RST}$ is obtained by adding to RST^C the following axioms:

(1) $\emptyset \in HF$.

[9] A different approach, which does not require additional axioms, but is based instead on going beyond the first-order level, was described in [3].

[10] The resulting system is still acceptable from the point of view of the Weil-Feferman predicativist program, since this program accepts the natural numbers and the hereditary finite sets.

(2) $\forall x \forall y \left(x \in HF \wedge y \in HF \rightarrow x \cup \{\!\!\{ y \}\!\!\} \in HF\right)$.

(3) $\emptyset \in y \wedge \forall v, w \in y. v \cup \{\!\!\{ w \}\!\!\} \in y \rightarrow HF \subseteq y$.

Next we prove the most characteristic properties of HF.

Proposition 23. *The followings are provable in RST^{C}_{HF}:*

(1) $x \in HF \leftrightarrow x = \emptyset \vee \exists u, v \in HF. u \cup \{\!\!\{ v \}\!\!\} = x$.

(2) $\left(\varphi\left(\emptyset\right) \wedge \forall x \forall y \left(\varphi\left(x\right) \wedge \varphi\left(y\right) \rightarrow \varphi\left(x \cup \{\!\!\{ y \}\!\!\}\right)\right)\right) \rightarrow \forall x \in HF. \varphi\left(x\right)$ *for* $\varphi \succ_{C} \emptyset$.

(3) $\psi\left\{\frac{HF}{a}\right\} \wedge \forall a \left(\psi\left(a\right) \rightarrow HF \subseteq y\right)$, *where* $\psi\left(a\right)$ *denotes the formula:*
$\forall x \left(x \in a \leftrightarrow x = \emptyset \vee \exists u, v \in a. u \cup \{\!\!\{ v \}\!\!\} = x\right)$

Proof.

(1) The first two axioms for HF imply $x = \emptyset \vee \exists u, v \in HF. u \cup \{\!\!\{ v \}\!\!\} = x \rightarrow x \in HF$ is provable in RST^{C}_{HF}. For the converse define $B := \{\!\!\{ x \in HF \mid x = \emptyset \vee \exists u, v \in HF. u \cup \{\!\!\{ v \}\!\!\} = x \}\!\!\}$. Clearly, there is a proof in RST^{C}_{HF} for $\emptyset \in B \wedge \forall v, w \in B. v \cup \{\!\!\{ w \}\!\!\} \in B$. Thus, by the third axiom of HF we get that $\forall x \in HF. x \in B$, which by the Axiom of Comprehension implies $\forall x \in HF \left(x = \emptyset \vee \exists u, v \in HF. u \cup \{\!\!\{ v \}\!\!\} = x\right)$.

(2) Suppose $\varphi\left(\emptyset\right) \wedge \forall x \forall y \left(\varphi\left(x\right) \wedge \varphi\left(y\right) \rightarrow \varphi\left(x \cup \{\!\!\{ y \}\!\!\}\right)\right)$. Take $\{\!\!\{ z \in HF \mid \varphi\left(z\right) \}\!\!\}$ for y. (This term is legal, since we assume that $\varphi \succ_{C} \emptyset$.) From the assumption and the first two axioms for HF it is easy to see that $\emptyset \in y \wedge \forall v, w \in y. v \cup \{\!\!\{ w \}\!\!\} \in y$. Therefore, by the third axiom for HF we get $\forall x \in HF. x \in \{\!\!\{ z \in HF \mid \varphi\left(z\right) \}\!\!\}$, which by the Axiom of Comprehension implies $\forall x \in HF. \varphi\left(x\right)$.

(3) By part (1) of the proposition, we have $\psi\left\{\frac{HF}{a}\right\}$, and by the third axiom for HF we can easily derive $\forall z \left(\psi\left\{\frac{z}{a}\right\} \rightarrow \forall y \in HF. y \in z\right)$.

□

Note. Actually, Prop 23(2) can be proven for arbitrary φ. This can be done using Prop. 28 below, whose proof in turn depends on the special case stated above. Since we are not using this stronger version in the sequel, we omit the proof.

Next we follow the standard construction of the natural numbers and encode them in the following way:

$$0 := \emptyset,$$
$$n + 1 := S\left(n\right),$$

where $S\left(n\right) = n \cup \{\!\!\{ n \}\!\!\}$. It is easy to see that each $n \in \mathbb{N}$ is a definable set. Clearly $\mathbb{N}$ is contained in the interpretation of HF.

Proposition 24. *The set of natural numbers is a definable set.*

Proof. Denote by $Ord\left(n\right)$ the formula $Trans\left(n\right) \wedge Linear\left(n\right)$, where

$$Linear\left(n\right) := \forall x \forall y \left(x \in n \wedge y \in n \rightarrow \left(x \in y \vee y \in x \vee x = y\right)\right)$$
$$Trans\left(n\right) := \forall x \forall y \left(y \in n \wedge x \in y \rightarrow x \in n\right)$$

It is easy to see that $Ord\left(n\right) \succ_{C} \emptyset$. Hence the set of natural numbers is definable by the term $\mathbb{N} := \{\!\!\{ n \in HF \mid Ord\left(n\right) \}\!\!\}$. □

Lemma 25. *The followings are provable in* RST^{C}_{HF} *:*

(1) $\forall a.Ord\,(a) \rightarrow \forall z \in a.Ord\,(z)$

(2) $\forall a, b.\,(Ord\,(a) \wedge Ord\,(b)) \rightarrow (a \in b \vee b \in a \vee a = b)$

Lemma 26. *The following is provable in* RST^{C}_{HF}*:*

$$\forall x \in HF.x = \emptyset \vee \exists z \in x \neg Ord\,(z) \vee \exists z \in x.max\,(x) = z$$

where $max\,(x) = z$ denotes the formula $\forall w \in x.w \in z \vee w = z$.

Proof. Let $\varphi\,(x)$ be the formula $x = \emptyset \vee \exists z \in x \neg Ord\,(z) \vee \exists z \in x.max\,(x) = z$. Then $\varphi \succ_{C} \emptyset$, and so we can prove $\forall x \in HF.\varphi$ by induction on HF (Prop. 23(2)). Clearly we have $\varphi\,(\emptyset)$. Assume $\varphi\,(x) \wedge \varphi\,(y)$. We prove $\varphi\,(x \cup \lBrace y \rBrace)$. If $x = \emptyset$ then $max\,(x \cup \lBrace y \rBrace) = y$, thus $\varphi\,(x \cup \lBrace y \rBrace)$. If $\exists z \in x \neg Ord\,(z)$ then $\exists z \in x \cup \{y\}\,.\neg Ord\,(z)$ and again $\varphi\,(x \cup \lBrace y \rBrace)$. Otherwise, we have that $x \neq \emptyset \wedge \forall z \in xOrd\,(z) \wedge \exists z \in x.max\,(x) = z$. If y is not an ordinal then $\exists z \in x \cup \{y\}\,.\neg Ord\,(z)$, otherwise, denote by z_0 the maximum of x. Then we have $Ord\,(y) \wedge Ord\,(z_0)$ and by Lemma 25(2) we get $y \in z_0 \vee z_0 \in y \vee y = z_0$. If $y \in z_0$ or $y = z_0$ then $max\,(x \cup \lBrace y \rBrace) = z_0$, otherwise the transitivity of y implies that $max\,(x \cup \lBrace y \rBrace) = y$. □

Proposition 27. $\vdash_{RST^{C}_{HF}} \forall n \in \mathbb{N}.n = 0 \vee \exists k \in n.n = S(k)$.

Proof. Let n be an element in $\mathbb{N}$. Then $Ord\,(n)$ and $n \in HF$. By Lemma 25(1) we get $\forall z \in n.Ord\,(z)$. Hence Lemma 26 implies that $n = \emptyset \vee \exists z \in n.max\,(n) = z$. If $n = \emptyset$ we are done. Otherwise, denote by z_0 the maximum of n. We prove that $n = S\,(z_0)$. If $x \in n$ then $x \in z_0$ (i.e. $x \in z_0 \vee x = z_0$) by the maximality of z_0. For the converse, assume $x \in z_0$. If $x = z_0$ then clearly $x \in n$. If $x \in z_0$ then by the transitivity of n we again conclude that $x \in n$. □

The next proposition shows that we can prove within our formal system the full induction rule of Peano's arithmetics.

Proposition 28. $\vdash_{RST^{C}_{HF}} (\varphi\,(0) \wedge \forall x\,(\varphi\,(x) \rightarrow \varphi\,(S\,(x)))) \rightarrow \forall x \in \mathbb{N}\varphi\,(x)$

Proof. By $\in$-induction, the following strong induction in $\mathbb{N}$ is provable in RST^{C}_{HF}:

$$\forall x \in \mathbb{N}\,((\forall y \in \mathbb{N}\,(y \in x \rightarrow \varphi\,(y))) \rightarrow \varphi\,(x)) \rightarrow \forall x \in \mathbb{N}.\varphi\,(x)$$

From this the standard induction principle formulated above can easily be derived with the help of Proposition 27. □

Proposition 29. *Let F be a binary operation which for elements of HF returns an element of HF. Then it is provable in RST^{C}_{HF} that for any $A \in HF$ there is a definable function H^{F}_{A} with domain $\mathbb{N}$ s.t.*

$$H^{F}_{A}\,(0) = A$$
$$H^{F}_{A}\,(S\,(n)) = F\left(A, H^{F}_{A}\,(n)\right)$$

Proof. By a well-known theorem (see, e.g., [16]), the proof of which can easily be reproduced in RST^{C}_{HF}, it suffices to show that given a definable unary operation F with the same property, there is a function H^{F}_{A} with domain $\mathbb{N}$ s.t.

$$H^{F}_{A}\,(0) = A$$
$$H^{F}_{A}\,(S\,(n)) = F\left(H^{F}_{A}\,(n)\right)$$

Let $Seq_{fin}\left(f\right)$ stand for the formula $Func\left(f\right) \wedge \exists m \in \mathbb{N}.dom\left(f\right) = S\left(m\right)$, and take FIN_a^F to be:

$$\{\!\{ f \in \mathit{HF} \mid Seq_{fin}(f) \wedge \langle 0, a\rangle \in f \wedge \forall n < S\left(m\right) \forall z \left(\langle n, z\rangle \check{\in} f \rightarrow \left\langle S\left(n\right), \hat{F}\left(z\right)\right\rangle \in f\right) \}\!\}$$

Next, define H_a^F to be $\bigcup FIN_a^F$. Since $A \in \mathit{HF}$, there is a term t_A which defines it. Then $H_a^F \left\{\frac{t_A}{a}\right\}$ is a closed term which defines H_A^F. □

Proposition 30. *The following holds:*

(*1*) *The standard ordering $\leq$ on $\mathbb{N}$ is a definable relation.*

(*2*) *Any primitive recursive function is a definable function.*

Proof.

(1) The standard ordering $<$ on $\mathbb{N}$ coincides with $\in$. Thus the term $\{\!\{ \langle m, n\rangle \mid m \in \mathbb{N} \wedge n \in \mathbb{N} \wedge (m = n \vee m \in n) \}\!\}$ defines $\leq$ by Prop. 15.

(2) The result immediately follows from Prop. 29.

□

5. THE REAL LINE

We now turn to real analysis. Once we have the natural numbers, it is straightforward to translate into our framework the standard constructions of $\mathbb{Z}$ (the integers) and $\mathbb{Q}$ (the rationals), to define (as sets) the basic relations and functions on them (such as, $<, +, \cdot$), and to prove in RST_{HF}^C their basic properties. Note that by defining a relation like $<$ *as a set* we not only mean that there is a formula φ that defines it, but that there is a term t whose interpretation is the relation $<$ taken as a set of ordered pairs. This is equivalent to requiring that the defining formula $\varphi\left(x, y\right)$ is safe w.r.t. $\{x, y\}$.

Next we define the real line using the standard construction of the real numbers as Dedekind cuts (see, e.g. [20]). However, in our current language and system it is again not possible to define the statement "x is a real number" using a formula which is safe with respect to x. Therefore, much like in the case of the natural numbers, in order to introduce the real numbers as a set we again extend our language and our system. For this we include in C a new constant symbol U, to be interpreted as an element of W that includes *HF* and is a universe (and so it is closed under rudimentary operations). This imposes some constraints on W which now must contain as an element both *HF* and some universe. The minimal such W is J_3 in which we can take the interpretation of U to be J_2. From a definitional/computational/constructive point of view, a better choice for W might be J_{ω^ω}, the use of which is still justified from a predicative point of view (see [4]). In J_{ω^ω} one can use e.g. J_ω as a sufficiently extensive interpretation of U.

In what follows C is any set of constants that includes both HF and U.

Definition 31. The system $RST_{\mathit{HF},U}^C$ for the language $\mathcal{L}_{RST}^C$ is obtained by adding to RST_{HF}^C the following axioms:

(1) $\mathit{HF} \in U$.

(2) $\forall x \forall y \, (x \in U \wedge y \in x \rightarrow y \in U)$.

(3) $\forall y_1, ..., y_n \in U . \lbrace\!\!\lbrace x \mid \varphi \rbrace\!\!\rbrace \in U$, provided $\varphi \succ_C \{x\}$, $Fv\,(\varphi) = \{y_1, ..., y_n\}$, and U does not occur in φ.[11]

Note. While for *HF* we have a unique interpretation, the interpretation of U is deliberately left open to allow stronger extensions of the system. The development of scientifically applicable mathematics which is outlined below is independent of the interpretation of U.

Now define $\psi\,(u) := \forall x, y \in \mathbb{Q}\,(x \in u \wedge y < x \rightarrow y \in u)$, $\varphi\,(u) := \neg \exists x \in u \forall y \in u . x \leq y$ and $\theta\,(u) := u \neq \mathbb{Q} \wedge u \neq \emptyset \wedge \forall x \in u . x \in \mathbb{Q}$, where $x \leq y$ is an abbreviation for $x < y \vee x = y$. The formula $\psi\,(u)$ states that u contains every rational number less than any rational number it contains, $\varphi\,(u)$ states that u has no greatest element, and $\theta\,(u)$ asserts that u is a non empty proper subset of $\mathbb{Q}$. It is easy to check that $\psi\,(u)\,, \varphi\,(u)\,, \theta\,(u) \succ_C \emptyset$. This fact justifies our next definition.

Definition 32 (The reals $\mathbb{R}$)**.**

$$\mathbb{R} = \lbrace\!\!\lbrace u \in U \mid \theta\,(u) \wedge \psi\,(u) \wedge \varphi\,(u) \rbrace\!\!\rbrace$$

Note. It is important to notice that the interpretation of the term $\mathbb{R}$ in W may not be the "real" real-line (if such a thing really exists), as it depends on the interpretation of U. However, standard real numbers such as $\sqrt{2}, \pi$,etc. are elements of $\mathbb{R}$ for any legal choice of W and any interpretation of U in it. For example, to see that π is a member of $\mathbb{R}$ it suffices to know that π is the interpretation of the term: $\lbrace\!\!\lbrace r \in \mathbb{Q} \mid \exists n \in \mathbb{N} . r < 4 \cdot \sum\limits_{k=0}^{n} \left(\frac{1}{4k+1} - \frac{1}{4k+3} \right) \rbrace\!\!\rbrace$ (a variant of the Leibniz series).

It is again straightforward to show that the standard ordering $<$ on $\mathbb{R}$ and the standard addition and multiplication of reals are definable elements of W, and to prove in $RST^{C}_{HF,U}$ that $\mathbb{R}$ equipped with them is an Archimedean ordered field. Next we show that the least upper bound principle is provable in $RST^{C}_{HF,U}$.

Proposition 33. *It is provable in $RST^{C}_{HF,U}$ that every nonempty bounded subset of $\mathbb{R}$ has a least upper bound. Also, the map that takes each nonempty bounded subset of $\mathbb{R}$ to its least upper bound is an operation.*

Proof. Let X be a nonempty subset of $\mathbb{R}$ that is bounded above. $\cup X$ is a set that belongs to $\mathbb{R}$ since X is bounded above. Since the order relation $\leq$ coincides with the inclusion relation, it follows that $\cup X$ is a least upper bound for X. Moreover, the mapping of X to $\cup X$ is a rudimentary operation, and hence it is an operation (by Corollary 13). □

Next we show that we are able to express real recursive functions in our framework.

Proposition 34. *Let F be an operation which for elements of U returns an element of U. Then:*

[11] To be more precise, for a concrete C we should specify which other constants may occur in φ or not. *HF* is always allowed. As for the other constants in C this will depend on their intended interpretation. In this paper we may assume that $C = \{HF, U\}$.

—*It is provable in $RST^{C}_{HF,U}$ that for any $A \in U$ there is a function H^{F}_{A} in U with domain $\mathbb{N}$ s.t.*

$$H^{F}_{A}(0) = A$$
$$H^{F}_{A}(S(n)) = F\left(A, H^{F}_{A}(n)\right)$$

—*If A is a definable set, then H^{F}_{A} is a definable function.*

Proof. The proof is similar to the proof of Prop. 29, replacing $f \in HF$ by $f \in U$ in the definition of FIN^{F}_{a} □

Definition 35. Let X be a set. A *sequence* in X is a function with domain $\mathbb{N}$ whose range is contained in X.

Lemma 36. *It is provable in $RST^{C}_{HF,U}$ that every Cauchy sequence in $\mathbb{R}$ converges to a limit in $\mathbb{R}$, and the map (lim) that takes a Cauchy sequence in $\mathbb{R}$ to its limit is an operation.*

Proof. Let a be a Cauchy sequence, and let a_k abbreviate $a(k)$. For each $n \in \mathbb{N}$ define $v_n := \bigcap\limits_{k \geq n} a_k$ (by Prop. 34 there is a function for $\lambda n. \bigcap\limits_{k \geq n} a_k$ in U). The least upper bound of $\lambda n.v_n$ is equal to the limit of $\lambda n.a_n$ (See [17]). Thus, $lim\, \lambda n.a_n := \bigcup \{\!\{ v_n \mid n \in \mathbb{N} \}\!\}$. □

Given sets X and Y, we next want to talk about sequence of functions from X to Y. However, we cannot apply Definition 35 as is because the collection of all functions from X to Y is not necessarily a set in our framework. Instead we use the standard procedure of Currying.

Definition 37. Let X and Y be sets. A *sequence of functions* with domain X and range contained in Y is a function F with domain $\mathbb{N} \times X$ whose range is contained in Y. (Intuitively, F denotes the sequence $f(0), f(1), f(2), \ldots$ where $f(n) = \lambda x \in X.\hat{F}(n, x)$).

Proposition 38. *Let $X \subseteq \mathbb{R}$ be a set. It is provable in $RST^{C}_{HF,U}$ that any pointwise limit of a sequence of functions with domain X whose range is contained in $\mathbb{R}$ is a function.*

Proof. Let F be a sequence of functions with domain X whose range is contained in $\mathbb{R}$. Suppose that for each $a \in X$ the sequence $\lambda n.\hat{F}(n, a)$ is converging, and so is a Cauchy sequence. Define: $G_a := \{\!\{ \left\langle n, \hat{F}(n, a) \right\rangle \mid n \in \mathbb{N} \}\!\}$. Then, $\lambda a \in X.lim\, G_a$ (where lim is the operation defined in Lemma 36) is the desired function. □

Corollary 39. *All elementary functions on $\mathbb{R}$ are available in $RST^{C}_{HF,U}$.*

Note. We should be careful here as to what we mean by elementary functions on $\mathbb{R}$. For example, by saying that all constant functions are available in $RST^{C}_{HF,U}$ we mean that $\forall y \in \mathbb{R}.Func(\lambda x \in \mathbb{R}.y)$ is provable in $RST^{C}_{HF,U}$. This of course does not mean that $\lambda x \in \mathbb{R}.y$ exists in W for any "real" number y (in V), but only for those who are elements of the interpretation of U. Unfortunately, we find it very difficult to express the exact intention of the proposition in a way which will be both precise and readable. Still, we trust the reader to understand the content of the proposition.

Proof. All polynomials on $\mathbb{R}$ are available in $RST^{C}_{HF,U}$ since $+$ and $\cdot$ are functions. Constant functions, the identity map on $\mathbb{R}$, and compositions of functions are also available in $RST^{C}_{HF,U}$ (as they are rudimentary operations and $\mathbb{R}$ is a definable set). Hence, the proposition easily follows from Prop. 38. □

Note. It is not difficult to see that many discontinuous functions (such as the jump function) are also available in $RST^{C}_{HF,U}$.

The next step is to define and prove in $RST^{C}_{HF,U}$ the basic properties of continuous functions (such as the intermediate value theorem). Now the collection of all (continuous) functions from $\mathbb{R}$ to $\mathbb{R}$ is not available as a set in $RST^{C}_{HF,U}$. Fortunately, we do not need it for our current task. It suffices for it to have the property of being a partial function from $\mathbb{R}$ to $\mathbb{R}$ definable in our language by a formula which is safe with respect to $\emptyset$. This can be done by the formula:

$$realFunc\,(f) := Func\,(f) \wedge dom\,(f) \subseteq \mathbb{R} \wedge rng\,(f) \subseteq \mathbb{R}$$

Below is an example of a standard theorem about real functions, whose classical proof can be reproduced in $RST^{C}_{HF,U}$ without any difficulty, using the completeness of $\mathbb{R}$ which is provable in $RST^{C}_{HF,U}$ (see Prop. 33).

Proposition 40 (Intermediate value theorem)**.** *Let*

$$|a-b| < c := b - c < a < b + c$$

$$Cont\,(f) := \forall c \in dom\,(f)\, \forall \epsilon > 0 \exists \delta > 0 \forall x \in dom\,(f)\,.\, |x - c| < \delta \rightarrow |f\,(x) - f\,(c)| < \epsilon$$

$$[a,b] := \{\!\!\{x \in \mathbb{R} \mid a \leq x \leq b\}\!\!\}$$

The following is provable in $RST^{C}_{HF,U}$*:*

$$\begin{gathered}\forall a, b \in \mathbb{R} \forall f\, [(realFunc\,(f) \wedge dom\,(f) = [a,b] \wedge Cont\,(f)) \rightarrow \\ \forall u \in \mathbb{R}. f\,(a) < u < f\,(b) \rightarrow \exists c \in \mathbb{R}\,(a < c < b \wedge f\,(c) = u)]\end{gathered}$$

6. CONCLUSIONS AND FURTHER RESEARCH

This paper is devoted to the task of developing scientifically applicable mathematics within the framework of [3], using a predicatively acceptable yet mechanizable set theory. A lot of work is of course still required in order to develop larger parts of mathematics within this framework. Obviously, at later stages of the project predicative set theories as used here will not suffice, and so stronger set theories will be used (see the Note after Definition 4). However, this should not be necessary at the current stage, in which the efforts are still devoted to the fundamentals of basic mathematical areas, like discrete mathematics and analysis. In all stages an important criterion for success will again be the extent to which things will be done in a natural way, as close as possible to rigorous mathematical practice.

Further work will also be devoted to investigate different directions for strengthening our framework:

—Since $realFunc\,(f) \succ_C \emptyset$, another direction for how we can further develop analysis is to continue the method of introducing new constants for bigger universes (similar to what we have done in this paper with HF and U), from which we are going to take our real functions. This can still be done in our definitional framework if we take W to be J_{ω^ω}, the interpretation of U as J_ω, and handling n-order constructs as elements of J_{ω^n}, after introducing the necessary constant symbols. In practice, scientifically applicable mathematics uses at most 4-order constructs, so we shall not need more than a finite number of constants.

—Another research direction is to explore the possibility of replacing the static approach to terms described above with a *dynamic* approach, in which both being a legal term and equality of terms are major judgements. Our goal is that a user would be able to introduce any term s/he finds natural and useful. For this we might like $\{x \mid \varphi\}$ to be a valid term whenever $\{x \mid \psi\}$ is a valid term, and φ is logically equivalent to ψ (according to the formal logical system which underlies the set-theory used). Note that in such a dynamic framework *all* parts of a theory (terms, formulas, safety relation, logical principles and non-logical axioms) are defined by a simultaneous recursion.

It is also important to determine to what extent do previous works concerned with predicative set theory fit into our framework. This includes Feferman's various systems for predicative mathematics, as well as the works on constructive set theory by Aczel, Beeson, Friedman, Gambino, Rathjen, and others.

Acknowledgment

This research was partially supported by the Ministry of Science, Technology and Space, Israel.

References

[1] Arnon Avron. Formalizing set theory as it is actually used. In *Mathematical Knowledge Management*, pages 32–43. Springer, 2004.

[2] Arnon Avron. Constructibility and decidability versus domain independence and absoluteness. *Theoretical Computer Science*, 394(3):144–158, 2008.

[3] Arnon Avron. A framework for formalizing set theories based on the use of static set terms. In *Pillars of computer science*, pages 87–106. Springer, 2008.

[4] Arnon Avron. A new approach to predicative set theory. *Ways of Proof Theory*, pages 31–63, 2010.

[5] Robert Boyer et al. The QED manifesto. *Automated Deduction–CADE*, 12:238–251, 1994.

[6] Adam Chlipala. An introduction to programming and proving with dependent types in Coq. *Journal of Formalized Reasoning (JFR)*, 3(2):1–93, 2010.

[7] Adam Chlipala. *Certified Programming with Dependent Types.* MIT Press, Cambridge, MA, 2013.

[8] Robert L. Constable, Stuart F. Allen, Mark Bromley, Rance Cleaveland, J. F. Cremer, R. W. Harper, Douglas J. Howe, Todd B. Knoblock, N. P. Mendler, Prakash Panangaden, James T. Sasaki, and Scott F. Smith. *Implementing mathematics with the Nuprl proof development system.* Prentice Hall, 1986.

[9] N. G. de Bruijn. *A survey of the project AUTOMATH.*

[10] Solomon Feferman. Systems of predicative analysis. *Journal of Symbolic logic*, pages 1–30, 1964.

[11] Solomon Feferman. Systems of predicative analysis, ii: Representations of ordinals. *Journal of Symbolic Logic*, pages 193–220, 1968.

[12] Solomon Feferman. A more perspicuous formal system for predicativity. *Konstruktionen versus Positionen*, 1:68–93, 1978.

[13] Abraham Adolf Fraenkel, Yehoshua Bar-Hillel, and Azriel Levy. *Foundations of set theory.* Elsevier, 1973.

[14] Robin Oliver Gandy. Set-theoretic functions for elementary syntax. In *Proc. Symp. in Pure Math*, volume 13, pages 103–126, 1974.

[15] Michael Hallett. *Cantorian set theory and limitation of size.* Clarendon Press Oxford, 1984.

[16] Karel Hrbacek and Thomas Jech. *Introduction to Set Theory, Revised and Expanded*, volume 220. Crc Press, 1999.

[17] Albert E. Hurd and Peter A. Loeb. *An introduction to nonstandard real analysis*, volume 118. Academic Press, 1985.

[18] R. Björn Jensen. The fine structure of the constructible hierarchy. *Annals of Mathematical Logic*, 4(3):229–308, 1972.

[19] Kenneth Kunen. Set theory. an introduction to independence proofs, 2nd print. *Studies in Logic and the Foundations of Mathematics*, 102.

[20] Azriel Levy. Basic set theory perspectives in mathematical logic. *Berlim: Spring*, 1979.

[21] Norman Megill. Metamath: A computer language for pure mathematics. 1997.

[22] Elliott Mendelson. *Introduction to mathematical logic.* CRC press, 1997.

[23] Rob P. Nederpelt, Jan Herman Geuvers, and R.C. De Vrijer. *Selected papers on Automath.* Elsevier, 1994.

[24] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL: a proof assistant for higher-order logic*, volume 2283. Springer, 2002.

[25] Piotr Rudnicki. An overview of the mizar project. In *Proceedings of the 1992 Workshop on Types for Proofs and Programs*, pages 311–330, 1992.

[26] Andrzej Trybulec and Howard A. Blair. Computer aided reasoning. In *Logics of Programs*, pages 406–412. Springer, 1985.

[27] Jeffrey D. Ullman. *Principles of Database and Knowledge-base Systems, Vol. I.* Computer Science Press, Inc., New York, NY, USA, 1988.

[28] Nik Weaver. Analysis in J_2. *arXiv preprint math/0509245*, 2005.

[29] Freek Wiedijk. The QED manifesto revisited. *Studies in Logic, Grammar and Rhetoric*, 10(23):121–133, 2007.

[30] Jeff Zucker. Formalization of classical mathematics in automath. *Studies in Logic and the Foundations of Mathematics*, 133:127–139, 1994.