

EQUATIONAL REPRESENTATIONS

by

Harvey M. Friedman*

Ohio State University

friedman@math.ohio-state.edu

<http://www.math.ohio-state.edu/%7Efriedman/>

September 23, 2010

NOTE: THIS IS AN ADVANCED DRAFT THAT NEEDS SOME POLISHING BEFORE SUBMISSION FOR PUBLICATION.

1. Preliminaries: $N, \emptyset N, \emptyset \emptyset N$.
2. Fundamental Lemma Concerning Clones.
3. From $(\exists f_1, \dots, f_k) (\forall x_1, \dots, x_p) (\varphi)$ To $(\exists$ binary $f) (\forall x, y) (\varphi)$.
4. From $N, \emptyset N, \emptyset \emptyset N$ to $\emptyset N \cup N, \emptyset (\emptyset N \cup N)$.
5. From $\emptyset N \cup N, \emptyset (\emptyset N \cup N)$ To Binary Sentences Over $(\emptyset N \cup N, \dots)$.
6. From Binary Sentences Over $(\emptyset N \cup N, \dots)$ To Binary Sentences Over $(\emptyset N, \subseteq)$.
7. From Binary Sentences Over $(\emptyset N, \subseteq)$ To Binary Sentences Over $(\mathfrak{R}, <)$.
8. From Binary Sentences Over $(\mathfrak{R}, <)$ To $(\exists f: \mathfrak{R} \rightarrow \mathfrak{R}) (\forall x, y \in \mathfrak{R}) (s = t)$.

1. Preliminaries: $N, \emptyset N, \emptyset \emptyset N$.

We begin by presenting the language $L(N, \emptyset N, \emptyset \emptyset N)$. This is the standard language for presenting third order sentences, using its intended interpretation.

There are variables $n_i, i \geq 1$, over N . Variables $x_i, i \geq 1$, over $\emptyset N$. Variables $A_i, i \geq 1$, over $\emptyset \emptyset N$.

The terms are defined inductively by

Each n_i is a term.

0 is a term.

If s, t are terms, then $S(t), s+t, s \cdot t$ are terms.

The atomic formulas are

$$x_i = x_j.$$

$$A_i = A_j.$$

$$x_i \in A_j.$$

$$t \in x_i, \text{ where } t \text{ is a term.}$$

$$s = t, \text{ where } s, t \text{ are terms.}$$

Formulas of $L(N, \emptyset N, \emptyset \emptyset N)$ are obtained using connectives and quantifiers in the usual way. Their intended meaning is obvious.

The Σ^1_∞ formulas of $L(N, \emptyset N, \emptyset \emptyset N)$ are the formulas without any quantifiers over $\emptyset \emptyset N$.

The Σ^2_1 formulas of $L(N, \emptyset N, \emptyset \emptyset N)$ are the formulas of $L(N, \emptyset N, \emptyset \emptyset N)$ that begin with zero or more existential quantifiers over $\emptyset \emptyset N$, followed by a Σ^1_∞ formula of $L(N, \emptyset N, \emptyset \emptyset N)$.

We use ZC for Zermelo set theory with the axiom of choice, which we will take to be ZFC with Replacement omitted.

The Σ^2_1 sentences of $L(N, \emptyset N, \emptyset \emptyset N)$ are well known to be very expressive. For example, the continuum hypothesis is provably equivalent to a Σ^2_1 sentence, over ZC.

Throughout the paper, we take the Σ^2_1 sentences to be the Σ^2_1 sentences of $L(N, \emptyset N, \emptyset \emptyset N)$.

Here is the main result of this paper.

THEOREM 7.5. The continuum hypothesis (more generally, every Σ^2_1 sentence) is provably equivalent, over ZC, to a sentence of the form

$$(\exists f: \aleph \rightarrow \aleph) (\forall x, y \in \aleph) (s = t)$$

where s, t are terms in $f, x, y, +, \cdot, 0, 1$.

Here are some other results of significance.

THEOREM 6.1. The continuum hypothesis (more generally, every Σ^2_1 sentence) is provably equivalent, over ZC, to a sentence of the form

$$(\exists f: \aleph^2 \rightarrow \aleph) (\forall x, y \in \aleph) (\varphi)$$

where φ is quantifier free in $f, x, y, <$.

THEOREM 5.1. The continuum hypothesis (more generally, every Σ^2_1 sentence) is provably equivalent, over ZC, to a sentence of the form

$$(\exists f: (\emptyset N)^2 \rightarrow \emptyset N) (\forall x, y \in \emptyset N) (\varphi)$$

where φ is quantifier free in f, x, y, \subseteq .

2. Fundamental Lemma Concerning Clones.

We write $\text{FCN}(D, k)$ for the set of all functions from D^k into D . We write $\text{MFCN}(D)$ for the union of all $\text{FCN}(D, k)$, $k \geq 1$. Here MFCN abbreviates "multivariate function).

We will take a logic approach to clones.

We use a master class of variables x_i , $i \geq 1$, and a master class of function symbols $F_{k,n}$, $k, n \geq 1$. Each $F_{k,n}$ is k -ary.

The terms are defined as follows.

- i. Each variable x_i , $i \geq 1$, is a term.
- ii. If t_1, \dots, t_k are terms, then $f(t_1, \dots, t_k)$ is a term.

We say that a term t is for F, p if and only if t is a term using at most the function symbol F , and variables x_1, \dots, x_p .

We now define $t[f, p]$ as follows. We require that there exists D such that $f \in \text{MFCN}(D)$, where the arity of f is the same as the arity of F .

We take $t[f, p] \in \text{FCN}(D, p)$ to be given by

$$t(f, p)(x_1, \dots, x_p) \text{ is the value of } t \text{ at } x_1, \dots, x_p \in D \text{ using } f \text{ for } F.$$

THEOREM 2.1. Let F be a k -ary function symbol, $k \geq 2$, and $p \geq 1$. There exist terms t_1, t_2, \dots for F, p such that the following holds. For all $f_1, f_2, \dots \in \text{FCN}(D, p)$, there exists $g \in \text{FCN}(D, k)$ such that $t_1[g, p], t_2[g, p], \dots = f_1, f_2, \dots$.

Proof: This result has a complicated history. I am consulting an expert on this topic, George McNulty, for attributions. QED

3. From $(\exists f_1, \dots, f_k) (\forall x_1, \dots, x_p) (\varphi)$ to $(\exists \text{ binary } f) (\forall x, y) (\varphi)$.

This section concerns a very general reduction from multivariate functions and multiple quantifiers to binary functions and two quantifiers.

Throughout this section, FT will be a finite relational type in ordinary predicate calculus with equality.

We let FT[MFCN] be the language that expands FT, with first order variables x_i , $i \geq 1$, and function variables f^i_k , $i, k \geq 1$.

The terms of FT[MFCN] are inductively defined by

Each x_i , $i \geq 1$ is a term.

All constants of FT are terms.

If F is a k-ary function symbol of FT and t_1, \dots, t_k are terms, then $F(t_1, \dots, t_k)$ is a term.

If t_1, \dots, t_k are terms then $f^i_k(t_1, \dots, t_k)$ is a term.

The atomic formulas of FT[MFCN] are of the form

$s = t$, where s, t are terms.

$R(t_1, \dots, t_k)$, where R is a k-ary relation symbol of FT, and t_1, \dots, t_k are terms.

Formulas of FT[MFCN] are obtained from atomic formulas of FT[MFCN] using connectives, first order quantifiers, and function quantifiers of each single arity.

The Σ^1_∞ formulas of FT[MFCN] are the formulas of L[MFCN] with no function quantifiers.

The Σ^2_1 formulas of FT[MFCN] are the formulas of FT[MFCN] beginning with zero or more function quantifiers, followed by a Σ^1_∞ formula.

LEMMA 3.1. For every Σ^2_1 sentence α in FT[MFCN], there is a Σ^2_1 sentence β in FT[M, MFCN] of the form $(\exists f_1, \dots, f_k) (\forall x_1, \dots, x_p) (\varphi)$, φ quantifier free, such that the following holds. ZC proves that for all structures M of type FT, $\alpha \leftrightarrow \beta$ holds in M.

Proof: First put α in prenex form as

$$(\exists g_1, \dots, g_n) (QY_1) \dots (QY_m) (\varphi)$$

where φ is quantifier free in FT[MFCN]. Now successively introduce Skolem functions to remove the existential quantifiers $\exists y_i$ from left to right. In this way, we arrive at

$$(\exists f_1, \dots, f_k) (\forall z_1, \dots, z_s) (\psi)$$

where ψ is quantifier free. QED

LEMMA 3.2. For every Σ^2_1 sentence α in $L(M, \text{MFCN})$, there is a sentence β in $L(M, \text{MFCN})$ of the form $(\exists \text{ binary } f) (\forall x, y) (\varphi)$, φ quantifier free, such that the following holds. ZC proves that for all structures M of type FT, $\alpha \leftrightarrow \beta$ holds in M .

Proof: By Lemma 2.1, we start with the Σ^2_1 sentence in $\text{FT}[M, \text{MFCN}]$

$$(\exists f_1, \dots, f_k) (\forall x_1, \dots, x_p) (\varphi)$$

where φ is quantifier free in FT.

This is equivalent to

$$(\exists f_1, \dots, f_k, g, h_1, h_2) (\forall x, y) (h_1(g(x, y)) = x \wedge h_2(g(x, y)) = y \wedge \psi)$$

where ψ is obtained from φ by replacing x_1, \dots, x_p by $h_1(x), h_1(h_2(x)), \dots, h_1(h^{p-1}(x))$.

By adding dummy variables, we can arrange that $f_1, \dots, f_k, g, h_1, h_2$ are all r -ary, and $r \geq 2$.

By Theorem 2.1, let t_1, \dots, t_k be terms for F, r , where F is binary, such that the following holds. For any For all $f_1, \dots, f_{k+3} \in \text{FCN}(D, r)$, there exists $g: D^2 \rightarrow D$ such that $t_1[g, r], \dots, t_{k+3}[g, r] = f_1, \dots, f_k, g, h_1, h_2$.

Thus we obtain the equivalent statement

$$(\exists \text{ binary } f) (\forall x, y) (\psi)$$

where ψ is obtained from φ by using t_1, \dots, t_{k+3} . QED

It is convenient to refer to the sentences displayed in Lemma 3.2 as the binary sentences of $L(M, \text{MFCN})$.

4. From $N, \emptyset N, \emptyset \emptyset N$ to $\emptyset N \cup N, \emptyset (\emptyset N \cup N)$.

The language $L(\emptyset N \cup N, \emptyset (\emptyset N \cup N))$ is two sorted. It combines sorts $\emptyset N$ and N into one sort, $\emptyset N \cup N$. Under the intended interpretation, $\emptyset N$ and N are disjoint. We also use the sort $\emptyset (\emptyset N \cup N)$. We will not use equality for $\emptyset (\emptyset N \cup N)$.

There are no function symbols in $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$. Instead, we use relation symbols.

We have variables x_i , $i \geq 1$, over $\emptyset N \cup N$. We have variables A_i , $i \geq 1$, over $\emptyset(\emptyset N \cup N)$. We have constants $0, 1$. The terms of sort $\emptyset N \cup N$ are the x_i and $0, 1$.

The atomic formulas of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$ are

$s = t$, $s < t$, $s \in t$, where s, t are terms.
 $SET(t)$, $NAT(t)$, where t is a term.
 $ADD(r, s, t)$, $MULT(r, s, t)$, where r, s, t are terms.

Formulas of L_1 are obtained by applying the connectives and two sorts of quantifiers to the atomic formulas in the usual way.

The intended interpretation of $\emptyset N \cup N$ is obvious, where $N, \emptyset N$ are considered disjoint. (In some set theoretic interpretations, N is the ordinal ω , and so $\omega \subseteq \emptyset \omega$). $v < w$ is interpreted as $v, w \in N$ and v is less than w . $v \in w$ is interpreted as $v \in N$, $w \in \emptyset N$, and v is an element of w . $SET(v)$ is interpreted as $v \in \emptyset N$. $NAT(v)$ is interpreted as $v \in N$. $ADD(u, v, w)$ is interpreted as $u, v, w \in N$ and u plus v is w . $MULT(u, v, w)$ is interpreted as $u, v, w \in N$ and u times v is w .

The Σ^1_∞ formulas of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$ are the formulas without any quantifiers over $\emptyset(\emptyset N \cup N)$.

The Σ^2_1 formulas of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$ are the formulas of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$ that begin with zero or more existential quantifiers over $\emptyset(\emptyset N \cup N)$, followed by a Σ^1_∞ formula of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$.

LEMMA 4.1. Every Σ^2_1 sentence is provably equivalent, over ZC , to a Σ^1_∞ sentence of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$.

Proof: Let $(\exists A_1, \dots, A_k)(\varphi)$ be given, where φ is Σ^1_∞ in $L(N, \emptyset N, \emptyset \emptyset N)$. Put this in prenex form, $(\exists A_1, \dots, A_k)(QV_1) \dots (QV_p)(\varphi)$, where φ is quantifier free in $L(N, \emptyset N, \emptyset \emptyset N)$.

Staying within $L(N, \emptyset N, \emptyset \emptyset N)$, first flatten out all uses of compound terms of sort N by adding a block of quantifiers over N after (QV_p) . Thus we now have

$$(\exists A_1, \dots, A_k)(QV_1) \dots (QV_p)(\exists m_1, \dots, m_q)(\psi)$$

where v 's are of sort $\emptyset N$, m 's are of sort N , ψ is quantifier free, and the atomic formulas in ψ are among

$$\begin{aligned} A_i &= A_j. \\ x_i &= x_j. \\ n_i &\in x_j. \\ n_i + 1 &= n_j. \\ n_i + n_j &= n_r. \\ n_i \cdot n_j &= n_r. \\ n_i &< n_j. \\ n_i &= n_j. \end{aligned}$$

Next, we pass to

$$(\exists A_1, \dots, A_k) ((\forall x) (x \in A_1 \vee \dots \vee x \in A_k \rightarrow \text{SET}(x)) \wedge (\text{QV}_1 | \text{SET}(v_1)) \dots (\text{QV}_p | \text{SET}(v_p)) (\exists y_1 | \text{NAT}(y_1)) \dots (\exists y_q | \text{NAT}(y_q)) (\rho))$$

where ρ is obtained from ψ as follows.

1. Replace m_1, \dots, m_q by y_1, \dots, y_q .
2. Replace $+$ by ADD, \cdot by MULT.
3. Replacing $A_i = A_j$ by $(\forall x_1) (x_1 \in A_i \leftrightarrow x_1 \in A_j)$.

This is Σ_1^2 in $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$. QED

5. From $\emptyset N \cup N, \emptyset(\emptyset N \cup N)$ to binary sentences over $(\emptyset N \cup N, \dots)$.

The language $L(\emptyset N \cup N, \dots, \text{MFCN})$ conforms to the notation introduced in section 2, and is subject to Lemma 3.2.

This language eliminates variables over $\emptyset(\emptyset N \cup N)$ in favor of variables over multivariate functions from $\emptyset N \cup N$ into $\emptyset N \cup N$. The three dots signify a list of additional constructs on $\emptyset N \cup N$.

$L(\emptyset N \cup N, \dots)$ uses SET, NAT, 0,1, ADD, MULT, =, <, \in , as in $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$. I.e., all of these items, except 0,1, are relation symbols.

LEMMA 5.1. Every Σ_1^2 sentence is provably equivalent, over ZC, to a Σ_1^2 sentence over $(\emptyset N \cup N, \dots)$.

Proof: By Lemma 4.1, it suffices to show that every Σ_1^2 sentence of $L(\emptyset N \cup N, \emptyset(\emptyset N \cup N))$ is provably equivalent, over ZC, to a Σ_1^2 sentence over $(\emptyset N \cup N, \dots)$. This is

clear, by identifying subsets of $\emptyset\mathbb{N} \cup \mathbb{N}$ with their characteristic functions. QED

LEMMA 5.2. Every Σ_1^2 sentence is provably equivalent, over ZC, to a binary sentence over $(\emptyset\mathbb{N} \cup \mathbb{N}, \dots)$.

Proof: By Lemmas 5.1 and 3.2. QED

6. From binary sentences over $(\emptyset\mathbb{N} \cup \mathbb{N}, \dots)$ to binary sentences over $(\emptyset\mathbb{N}, \subseteq)$.

We begin by placing some universal conditions on some unary and binary functions. We use $x \subseteq \neq y$ for $x \subseteq y \wedge \neg y \subseteq x$.

$$1. F_1(x) = x \wedge (\forall y \subseteq x) (x \subseteq y), \text{ or } F_1(x) \subseteq \neq x.$$

Thus $x = \emptyset$ if and only if $F_1(x) = x$.

$$2. F_2(x) = x \wedge (\forall y \subseteq x) (y = x \vee y = \emptyset), \text{ or } F_2(x) \subseteq \neq x, \text{ or } x = \emptyset \wedge F(x) \neq x.$$

Thus x is a singleton if and only if $F_2(x) = x$.

$$3. F_3(x) = x \wedge x \neq \emptyset \wedge (\forall y \in x) (y = \emptyset), \text{ or } F_3(x) \in x \wedge x \neq \emptyset, \text{ or } x = \emptyset.$$

Thus $x = \{\emptyset\}$ if and only if $F_3(x) = x \wedge x \neq \emptyset$.

$$4. F_4(x, y) = \emptyset \vee F_4(x, y) = \{\emptyset\} \leftrightarrow x, y \text{ are singletons. If } x, y \text{ are singletons, then } F_4(x, x) = \emptyset, x = y \vee F_4(x, y) = \{\emptyset\} \vee F_4(y, x) = \{\emptyset\}, F_4(x, y) = F_4(y, z) = \{\emptyset\} \rightarrow F_4(x, z) = \{\emptyset\}.$$

Thus F_4 is the characteristic function of a strict linear ordering of the singletons. We write $x <' y$ for this strict linear ordering of the singletons.

$$5. \text{ Suppose } y \subseteq x, \text{ where } y \text{ is a singleton. Then } F_5(x) \text{ is the } <' \text{ least singleton } \subseteq x.$$

Thus $<'$ is a well ordering of the singletons.

$$6. \text{ Suppose } x <' y. \text{ Then } F_6(y) < y \wedge (\forall z) (\neg F_6(y) < z < y).$$

Thus every singleton that is not $<'$ least has an immediate $<'$ predecessor. Hence $<'$ is of order type ω .

$$7. F_7 \text{ is constantly the } <' \text{ least singleton.}$$

Thus $<$ starts with any $F_7(x)$.

8. F_8 is the $<$ successor function on the singletons; \emptyset otherwise.

9. For singletons x, y , $F_9(x, F_7(y)) = x$, $F_8(x, F_8(y)) = F_8(F_9(x, y))$.

Thus F_9 is the addition function on $<$.

10. For singletons x, y , $F_{10}(x, F_7(y)) = \emptyset$, $F_{10}(x, F_8(y)) = F_9(F_{10}(x, y), x)$.

Thus F_{10} is the multiplication function on $<$.

We now want to build the rest of the tools needed for interpreting the $L(\emptyset N \cup N, \dots)$.

We already have an appropriate interpretation of N as the set of singletons, using F_2 . We interpret $<$ on N by $<$ on the singletons. We take 0 to be any $F_7(x)$. We take 1 to be any $F_8(F_7(x))$. We interpret ADD and MULT by F_9 and F_{10} .

We interpret the elements of $\emptyset N$ to be the x such that any $F_8(y)$, $F_8(F_7(y))$ are $\subseteq x$. Thus the interpretations of N and $\emptyset N$ are disjoint. The \in relation is interpreted as follows. Let z be a singleton and let x be such that any $F_8(y)$, $F_8(F_7(y)) \subseteq x$. Then $z \in x$ if and only if $F_8(F_8(z)) \subseteq x$.

The functions of several variables on $\emptyset N \cup N$ are interpreted to be the functions of several variables on $\emptyset N$, which are \emptyset outside the interpretation of $\emptyset N \cup N$, and which map $\emptyset N \cup N$ into $\emptyset N \cup N$.

THEOREM 6.1. Every Σ_1^2 sentence is provably equivalent, over ZC, to a sentence $(\exists f: (\emptyset N)^2 \rightarrow \emptyset N) (\forall x, y) (\varphi)$, where φ is quantifier free over $(\emptyset N, \subseteq)$.

Proof: By Lemma 5.2, we start with a sentence

$$(\exists f: \emptyset N \cup N)^2 \rightarrow \emptyset N \cup N) (\forall x, y) (\varphi)$$

where φ is quantifier free over $(\emptyset N \cup N, \dots)$. The result is immediate from the interpretation of $(\emptyset N \cup N, \dots)$, followed by an application of Theorem 3.2. QED

7. From binary sentences over $(\emptyset N, \subseteq)$ to binary sentences over $(\mathfrak{N}, <)$.

It will be convenient to use the constants $-2, -1, 0, 1, 2, \dots$. In this section, we show that every Σ^2_1 sentence is provably equivalent, over ZC, to a binary sentence over $\mathfrak{N}, <, -2, -1, 0, 1, 2$.

The constants $-2, -1, 0, 1, 2$ are used for convenience. In the next section, we remove them.

We say that S, P is an SP pair (successor predecessor pair) if and only if

- i. $S, P: \mathfrak{N} \rightarrow \mathfrak{N}$.
- ii. $(\forall x \in \mathfrak{N}) (Sx > x \wedge Px < x \wedge S(P(x)) = P(S(x)) = x)$.
- iii. $(\forall x, y) (x < y \rightarrow S(x) < S(y) \wedge P(x) < P(y))$.
- iv. $S(-2) = -1, S(-1) = 0, S(0) = 1, S(1) = 2$.

Note that this definition is in the form $(\forall x, y \in \mathfrak{N}) (\varphi)$.

LEMMA 7.1. Let S, P be an SP pair and $x \in \mathfrak{N}$. Then $x, S(x), S(S(x)), \dots$ is unbounded above, and $x, P(x), P(P(x)), \dots$ is unbounded below.

Proof: Suppose $x, S(x), S(S(x)), \dots$ is bounded. Let y be the least upper bound. Since $P(y) < y$, let $P(y) < S^n x$. Then $S(P(y)) < S^{n+1} x$, and so $y < S^{n+1} x$. This contradicts the choice of y .

The second claim is proved analogously. QED

We now fix any SP pair S, P . We regard S, P as "internal". If we blurred the distinction between internal and external, we would have defined S, P as the actual successor and predecessor functions on \mathfrak{N} .

All of the internal functions introduced below, until \dots , will be functions from \mathfrak{N} into \mathfrak{N} that are introduced by universal conditions. In all cases except that of IPR_1, IPR_2 , the functions are uniquely characterized by the universal conditions. Even with IPR_1, IPR_2 , there is a kind of uniqueness.

Various external functions and relations and sets will be introduced in order to intelligibly reason about the internal functions.

Internal functions will have names consisting of capital English letters and numeral subscripts. External notions will have names not of this form.

We will write Int for $\{\dots, P(P(0)), P(0), 0, S(0), S(S(0)), \dots\}$. We write Nint for $\{0, S(0), S(S(0)), \dots\}$.

$\text{FLR}: \mathfrak{N} \rightarrow \mathfrak{N}$ (floor function) is unique such that

$$(\forall x \in \mathfrak{N}) ((0 \leq x < 1 \rightarrow \text{FLR}(x) = 0) \wedge \text{FLR}(S(x)) = S(\text{FLR}(x))).$$

$\text{FRA}: \mathfrak{N} \rightarrow \mathfrak{N}$ (fractional part function) is unique such that

$$(\forall x \in \mathfrak{N}) ((0 \leq x < 1 \rightarrow \text{FRA}(x) = x) \wedge \text{FRA}(Sx) = \text{FRA}(x)).$$

Note that $x \in \text{Int} \leftrightarrow \text{FRA}(x) = 0$. Also $x \in \text{Nint} \leftrightarrow \text{FRA}(x) = 0 \wedge x \geq 0$.

We introduce inverse pairing functions $\text{IPN}_1, \text{IPN}_2$ for Nint , implicitly as follows.

- i. $(\forall x \notin \text{Nint}) (\text{IPN}_1(x) = \text{IPN}_2(x) = -1)$.
- ii. Suppose $\text{IPN}_2(x) \neq 0$. Then $\text{IPN}_1(Sx) = S(\text{IPN}_1(x)) \wedge \text{IPN}_2(S(x)) = P(\text{IPN}_2(x))$.
- iii. Suppose $\text{IPN}_2(x) = 0$. Then $\text{IPN}_1(Sx) = 0 \wedge \text{IPN}_2(Sx) = S(\text{IPN}_1(x))$.

We use the key property

$$(\forall x, y \in \text{Nint}) (\exists! z \in \text{Nint}) (\text{IPN}_1(z) = x \wedge \text{IPN}_2(z) = y).$$

We write $\langle x, y \rangle$ for this unique z , provided $x, y \in \text{Nint}$; undefined otherwise.

We can define ADD on Nint as a unary function as follows. For all $x \in \mathfrak{N}$,

$$\begin{aligned} x \notin \text{Nint} &\rightarrow \text{ADD}(x) = -1. \\ (x \in \text{Nint} \wedge \text{IPN}_2x = 0) &\rightarrow \text{ADD}(x) = \text{IPN}_1x. \\ (x, y \in \text{Nint} \wedge \text{IPN}_1x = \text{IPN}_1y \wedge \text{IPN}_2y = S(\text{IPN}_2x)) &\rightarrow \text{ADD}y = S(\text{ADD}x). \end{aligned}$$

Note that we have for all $x, y \in \text{Nint}$,

$$\begin{aligned} \text{ADD}(\langle x, 0 \rangle) &= x. \\ \text{ADD}(\langle x, Sy \rangle) &= S(\text{ADD}(\langle x, y \rangle)). \end{aligned}$$

In this same way, we can use IPN_1, IPN_2, S to introduce such implicit definitions for all multivariate primitive recursive functions from N_{int} into N_{int} , as unary functions. Here "primitive recursive" means relative to N_{int} , which starts with $0, 1, 2$, and continues increasing to infinity, arbitrarily. If not all arguments for a primitive recursive function lie in N_{int} , then we use -1 for the default value.

In particular, we introduce a coding for nonempty finite sequences from N_{int} by elements of N_{int} . We define the relevant primitive recursive functions LTH , APP , and obtain the following property.

For every finite sequence $n_1, \dots, n_k \in N_{int}$, $k \geq 0$, there is a unique $m \in N_{int}$ such that $LTH(m) = S^k 0 \wedge APP(\langle m, S^1 0 \rangle), \dots, APP(\langle m, S^k 0 \rangle) = n_1, \dots, n_k$, respectively.

Externally, for $n_1, \dots, n_k \in N_{int}$, we write $Code(n_1, \dots, n_k)$ for this unique $m \in N_{int}$.

We use the set $02Code$ of codes for finite sequences of 0 's and 2 's, which is available internally through primitive recursion.

We also use the transitive and reflexive ordering \leq^* , given by

$x \leq^* y \leftrightarrow x, y \in 02Code$ and the base 3 rational $.n_1 \dots n_k$ is at most the base 3 rational $.m_1 \dots m_p$, where x codes n_1, \dots, n_k , and y codes m_1, \dots, m_p .

We have internal access to \leq^* because of primitive recursion.

We define the internal function $F: \mathfrak{N} \rightarrow \mathfrak{N}$ with the following two conditions.

- i. If $x \in 02Code$ then $0 \leq Fx < 1$. Otherwise, $Fx = -1$.
- ii. Suppose $x, y \in 02Code$. Then $Fx \leq Fy \leftrightarrow x \leq^* y$.

Externally, for $x \in [0, 1)$ and $k \geq 1$, let $3Exp(x, k)$ be the k digit base 3 expansion of x . This is externally defined to be the $t \in 02Code$, $LTH(t) = k$, such that for all $t' \in 02Code$, $LTH(t') = k$, we have $Ft' \leq Ft \leq x$.

Unfortunately, $3Exp$ is binary. So we introduce $G: \mathfrak{N} \rightarrow \mathfrak{N}$ by

- i. If $x \geq 1$ then $G(x) = 3\text{Exp}(x, \text{FLR}(x))$.
- ii. If $x < 1$ then $G(x) = -1$.

We need an internal relation $x \in y$ which is to mean "the $x \in \text{Nint}$ lies in y viewed as a subset of Nint ".

Externally, we define $k \in x$ if and only if

- i. $k \in \text{Nint}$.
- ii. $0 \leq x < 1$.
- iii. For the unique y with $\text{FRA}(y) = x \wedge \text{FLR}(y) = k$, the last base 3 digit of the sequence coded by $G(y)$ is 2.

We do not have the kind of internal access to $k \in x$ that we have been accustomed to. But we do have both universal and existential definitions of $k \in x$ by examining iii).

Externally, we define $x \approx y$ if and only if $x, y \in [0, 1) \wedge (\forall k) (k \in x \leftrightarrow k \in y)$, and $x \subseteq y$ if and only if $x, y \in [0, 1) \wedge (\forall k) (k \in x \rightarrow k \in y)$.

Note that every subset of Nint is of the form $\{k: k \in x\}$ for some $x \in [0, 1)$. The x may not be unique, but this will not cause difficulties.

We now introduce inverse pairing functions $\text{IPR}_1, \text{IPR}_2$ for $[0, 1)$, implicitly as follows.

- i. $(\forall x \notin [0, 1)) (\text{IPR}_1(x) = \text{IPR}_2(x) = -1)$.
- ii. $(\forall x \in [0, 1)) (\forall k \in \text{Nint}) ((k \in \text{IPR}_1(x) \leftrightarrow 2k-1 \in x) \wedge (k \in \text{IPR}_2(x) \leftrightarrow 2k \in x))$.

It is clear that for each $x, y \in [0, 1)$, there exists $z \in [0, 1)$ such that $\text{IPR}_1(z) \approx x \wedge \text{IPR}_2(z) \approx y$. Moreover, the z is unique up to \approx .

We can now give internal forms of \approx, \subseteq by introducing the functions EQ and INC by the following conditions.

- i. $(\forall x \notin [0, 1)) (\text{EQ}(x) \wedge \text{INC}(x) = -1)$.
- ii. $(\forall x \in [0, 1)) ((\text{INC}(x) = -1 \wedge \text{IPR}_1(x) \subseteq \text{IPR}_2(x)) \vee (\text{INC}(x) \in \text{IPR}_1(x) \wedge \text{INC}(x) \notin \text{IPR}_2(x)))$.
- iii. $(\forall x \in [0, 1)) ((\text{EQ}(x) = -1 \wedge \text{IPR}_1(x) \approx \text{IPR}_2(x)) \vee (\text{EQ}(x) \in \text{IPR}_1(x) \leftrightarrow \text{EQ}(x) \notin \text{IPR}_2(x)))$.

In the above, we use both the universal and existential form of \in .

We introduce $\text{WIT}(x)$, (witness of x), by the condition

$$(\forall x \in \mathfrak{N}) (\text{WIT}(x) \in x \vee (\text{WIT}(x) = -1 \wedge (\forall y) (y \notin x))).$$

Externally, we define $\text{Max}(x)$ to be -2 if there are infinitely many $k \in x$; -1 if there are no $k \in x$; k if k is the largest $k \in x$.

We now give an internal form of Max . We introduce the function H by the following conditions.

- i. Let $x < 0$. Then $H(x) = -1$.
- ii. Let $x \geq 0 \wedge \text{FLR}(x) \notin \text{FRA}(x)$. Then $H(x) = -1$.
- iii. Let $x \geq 0 \wedge \text{FLR}(x) \in \text{FRA}(x)$. Then $H(x) = \text{FLR}(x) \wedge (\forall y \in \text{FRA}(x)) (y \leq x)$, or $H(x) > \text{FLR}(x) \wedge H(x) \in \text{FRA}(x)$.

We introduce the function J by the following conditions.

- i. Let $\text{WIT}(x) = -1$. Then $J(x) = -1$.
- ii. Let $\text{WIT}(x) \in x$. Then $H(J(x)) = \text{FLR}(x) \vee (J(x) = -2 \wedge (\forall y) (H(y) \neq \text{FLR}(y)))$.

Note that for all $x \in \mathfrak{N}$,

- i. If there are infinitely many $k \in x$ then $J(x) = -2$.
- ii. If there are no $k \in x$ then $J(x) = -1$.
- iii. If there is a largest $k \in x$ then $J(x)$ is the unique y with $\text{FRA}(y) = x$ and $\text{FLR}(y) = k$.

We now introduce MAX by $\text{MAX}(x) = 0$ if $J(x) = -2$; 1 if $J(x) = -1$; $\text{FLR}(J(x))$ otherwise.

Note that $\text{MAX}(x) = 0$ if there are infinitely many $k \in x$; 1 if there are no $k \in x$; the maximum $k \in x$ plus 2 otherwise.

We now use $[0,1)$, Nint , \in' .

Interpret subsets of N as elements of \mathfrak{N} .

Interpret elements of N as elements of Nint .

Interpret membership in subsets of N by \in' .

Interpret equality between subsets of N by \approx .

Interpret subsets of $\wp N$ by functions from \mathfrak{N} into $\{0,1\}$.

Interpret $0, S, +, \cdot, <$ by the corresponding relations on Nint .

THEOREM 7.2. Every Σ^2_1 sentence is provably equivalent, over ZC , to a binary sentence over $\mathfrak{N}, <$.

Proof: By Lemma 6.1, we start with a sentence $(\exists f: (\emptyset N)^2 \rightarrow \emptyset N) (\forall x, y) (\varphi)$, where φ is quantifier free over $(\emptyset N, \subseteq)$. Now use the interpretation of $\emptyset N, \subseteq$ developed above to obtain an equivalent Σ_1^2 sentence over $(\mathfrak{R}, <, -2, -1, 0, 1, 2)$. We can existentially quantify out these five constants, obtaining an equivalent Σ_1^2 sentence over $(\mathfrak{R}, <)$. Now Apply Lemma 3.2. QED

8. From binary sentences over $(\mathfrak{R}, <)$ to $(\exists f: \mathfrak{R} \rightarrow \mathfrak{R}) (\forall x, y \in \mathfrak{R}) (s = t)$.

LEMMA 8.1. Let $x, y, z, w \in \mathfrak{R}$. Assume that the list of 20 positive reals $2x^2+x+1 + (0, 1, 2, 3, 4)$, $2x^2-x+1 + (0, 5, 10, 15, 20)$, $2y^2+y+1 + (0, 21, 42, 63, 84)$, $2y^2-y+1 + \{0, 85, 170, 255, 340\}$, are a permutation of the list of 20 positive reals $2z^2+z+1 + (0, 1, 2, 3, 4)$, $2z^2-z+1 + (0, 5, 10, 15, 20)$, $2w^2+w+1 + (0, 21, 42, 63, 84)$, $2w^2-w+1 + \{0, 85, 170, 255, 340\}$. Then $x = z \wedge y = w$.

Proof: Let x, y, z, w and the two 20 term lists be as given. Each of the two lists is divided into four groups. Five of the second list of 20 reals form an arithmetic progression with increment 1. Two of these reals must lie in the same group of five, and differ by at most 4. This can only be the group with $\{0, 1, 2, 3, 4\}$. Hence the two first groups of five are the same.

Five of the second list of 20 reals form an arithmetic progression with increment 5. Two of these reals must lie in the same group of five, and differ by at most 20. Hence the two second groups of five are the same.

By the same reasoning, the two lists of 20 reals must be identical. Hence $2x^2+x+1 = 2z^2+z+1 \wedge 2x^2-x+1 = 2z^2-z+1 \wedge 2y^2+y+1 = 2w^2+w+1 \wedge 2y^2-y+1 = 2w^2-w+1$. Therefore $x = z$ and $y = w$. QED

LEMMA 8.2. There is a term t in unary f and $x, y, +, \cdot, 0, 1$ such that the following holds. Let $g: \mathfrak{R}^2 \rightarrow \mathfrak{R}$. There exists $f: \mathfrak{R} \rightarrow \mathfrak{R}$ such that g is t .

Proof: Let $S \subseteq \mathfrak{R}^-$ be a set of cardinality c which is linearly independent over the rationals. Let $f: \mathfrak{R}^+ \rightarrow S$ be a bijection.

Note that the list of 20 items in Lemma 8.1 forms a list of 20 quadratics in x, y (in fact, quadratics in x, y

separately). Let $h(x,y)$ be the sum of the values of f at these 20 quadratics.

By the choice of S , we see that if $h(x,y) = h(z,yw)$ then (x,y) must be a permutation of (z,w) . By Lemma 8.1, $x = z \wedge y = w$. Hence h is one-one from \mathfrak{R}^2 into \mathfrak{R} . For every $h(x,y)$, define $f(h(x,y)) = g(x,y)$. Now extend f in any way to be defined at all of \mathfrak{R} . Then for all $x,y \in \mathfrak{R}$, $f(h(x,y)) = g(x,y)$, and $f(h(x,y))$ is given by a term in $f, x, y, +, \cdot, 0, 1$. QED

LEMMA 8.3. There are terms t_1, t_2, \dots in unary f and $x, y, +, \cdot, 0, 1$ such that the following holds. Let $g_1, g_2, \dots: \mathfrak{R}^2 \rightarrow \mathfrak{R}$. There exists $f: \mathfrak{R} \rightarrow \mathfrak{R}$ such that g_1, g_2, \dots are $t_1[f, +, \cdot, 0, 1; 2], t_2[f, +, \cdot, 0, 1; 2], \dots$ respectively.

Proof: Take t_1 to be the t of Lemma 7.2, that uses unary $f, x, y, +, \cdot, 0, 1$. Let s_1, s_2, \dots be terms for $F, 2, F$ binary, according to Theorem 2.1. Take each t_{i+1} to be s_i with F replaced by t_1 . I.e., with all subterms $F(\alpha, \beta)$ replaced by $t_1(\alpha, \beta)$, with x replaced by α and y replaced by β . By Lemma 7.2, we can choose f such that t_1 is a binary function on \mathfrak{R} that is suitably chosen for application of Theorem 2.1. QED

LEMMA 8.4. Every quantifier free formula $\varphi(y_1, \dots, y_n)$ in $+, \cdot, 0, 1, <$ is equivalent to a formula $(\exists x_1, \dots, x_k) (\forall z) (s = t)$, for all $y_1, \dots, y_n \in \mathfrak{R}$, where t is a term in $x_1, \dots, x_k, y_1, \dots, y_n, +, \cdot, 0, 1$.

Proof: First put φ in disjunctive normal form. First replace every $s < t$ with $t - s > 0$, and every $s \leq t$ with $t - s \geq 0$. So we have a disjunction of conjunctions of inequalities $t > 0, t \geq 0$. Replace $t \geq 0$ by $(\exists x) (t = x^2)$. Replace $t > 0$ by $(\exists x) (t = x^2) \wedge (\exists x) (x \cdot t = 1)$. For each conjunction, combine the existential quantifiers, with changed variables, followed by a conjunction of equations. The conjunction of equations is reduced to a single equation $t = 0$ using sums of squares.

We have a disjunction of such existentially quantified equations. This is equivalent to an existentially quantified disjunction of equations, which reduces to an existentially quantified equation $t = 0$ by multiplication of terms.

We thus arrive at

$$(\exists x_1, \dots, x_p) (s = t)$$

where s, t are term in $x_1, \dots, x_p, y_1, \dots, y_n, +, \cdot, 0, 1$. QED

THEOREM 8.5. Every Σ^2_1 sentence is provably equivalent, over ZC, to a sentence of the form $(\exists f: \mathfrak{N} \rightarrow \mathfrak{N}) (\forall x, y \in \mathfrak{N}) (s = t)$, where s, t are terms in $f, x, y, +, \cdot, 0, 1$.

Proof: By Theorem 7.2, we start with

$$(\exists f: \mathfrak{N}^2 \rightarrow \mathfrak{N}) (\forall x, y \in \mathfrak{N}) (\varphi)$$

where φ is quantifier free in \langle . By Lemma 8.4, this is equivalent to

$$(\exists f: \mathfrak{N}^2 \rightarrow \mathfrak{N}) (\forall x, y \in \mathfrak{N}) (\exists z_1, \dots, z_k) (s = t)$$

where s, t are terms in $f, x, y, z_1, \dots, z_k, +, \cdot, 0, 1$. Using Skolem functions, this takes the form

$$(\exists f_1, \dots, f_r: \mathfrak{N}^2 \rightarrow \mathfrak{N}) (\forall x, y \in \mathfrak{N}) (s = t)$$

where s, t are terms in $f_1, \dots, f_r, x, y, +, \cdot, 0, 1$.

We now use Lemma 8.3 for t_1, \dots, t_r to put this in the form

$$(\exists f: \mathfrak{N} \rightarrow \mathfrak{N}) (\forall x, y \in \mathfrak{N}) (s = t)$$

where s, t are terms in $f, x, y, +, \cdot, 0, 1$. QED

*This research was partially supported by grant ID#15557 from the John Templeton Foundation.