

## “True” Arithmetic Can Prove Its Own Consistency

Andrew Boucher

Created: Apr 28, 2002

Last Modified: Sep 7, 2004 (a footnote removed 29 Dec 2010)

[www.andrewboucher.com/papers/consistency.pdf](http://www.andrewboucher.com/papers/consistency.pdf)

### A. Introduction

Godel’s Second Incompleteness Theorem famously shows that any system at least as strong as first-order Peano Arithmetic (**Z1**) cannot prove its own consistency, with the proviso (because of Feferman [F1]) that this consistency must be expressed using an “intensionally correct” provability predicate. Systems which are not stronger than **Z1**, however, can, in some fashion or other, prove their own consistency--call such systems “self-verifying” or “auto-consistent”--, and a large amount of investigation has been conducted in this field, see e.g. most recently [W1], which includes a survey of the literature, and also [G1]. The examples uncovered hitherto have, however, tended to lack naturalness. Here is presented a deduction system, called **F**, which *is* natural, and capable of proving its own consistency or at least consistency in the way Godel formulated it, since the assertion apparently lacks the intensional correctness which is desired. Other deduction systems, closely related to **F**, can overcome this deficiency and prove propositions asserting both the - for lack of better terms - Godel and real consistency. That is, they are able to prove their own consistency in an intensionally correct way. All these auto-consistent systems are ontologically very weak, indeed weaker than Robinson’s Arithmetic **Q** - and this is why Godel’s Second Incompleteness Theorem does not apply to them. Otherwise, however, they are quite strong, and certainly stronger than **Q**, and many standard number-theoretic results go through.

### B. Overview

The **F** deduction system is essentially second-order arithmetic, stripped of almost all assumptions about the existence of (first-order) things; indeed it only assumes that 0 exists (and not even that 0 is a natural number). It is therefore agnostic about the existence of the natural numbers. It can be easily seen that they have as model the standard one, but also any initial segment,  $\{0, 1, \dots, n\}$ . In particular, the singleton  $\{0\}$  can be used to model the system.

In spite of this ontological simplicity, **F**, which is armed with a non-total sequential relationship, is nonetheless strong enough to define addition, multiplication, and exponentiation and prove that these have their normal properties for whatever natural numbers exist. **F** also establishes that, if a natural number exists, then (to speak loosely) all numbers less than it must also exist. Indeed, the system must be normal from that number downward. E.g. if  $n$  exists as a natural number, then sums, products and powers less than or equal to  $n$  exist and behave normally. On the other hand, the system can say nothing about what happens upward, that is what is higher than  $n$ , since the existence of such numbers cannot be established.

Now some memorable theorems in number theory are indeed upward. For instance, the proposition that there are an infinitude of primes and the Chinese Remainder Theorem, both require that, given a finite list of numbers, one forms their product, which is of course greater than any number on the list. Such theorems cannot go through in **F**. On the other hand, many arithmetic assertions are downward, e.g. the Euclidean Algorithm, where one is given numbers and required to find a sequence of smaller numbers, and the existence and

uniqueness of prime factorization, where one is given a number and one must find a unique sequence of lesser numbers. These **F** can prove.

For instance, **F** is not able to prove this version of the Commutative Law of Addition:

$$\forall x \forall y ( Nx \ \& \ Ny \ \& \ (x + y) = (y + x) ).$$

For given the existence of  $x$  and  $y$ , it cannot show that there exist the usually bigger numbers  $(x + y)$  and  $(y + x)$ , so *a fortiori* it cannot prove them equal. On the other hand, **F** can prove this version of the Law:

$$\forall x \forall y \forall z ( Nx \ \& \ Ny \ \& \ Nz \ \& \ (x + y) = z \Rightarrow (y + x) = z ).$$

The difference with the first proposition is that the existence of  $(x + y)$  is here *assumed*. Knowing that, one can then prove that  $(y + x)$  exists and indeed equals  $(x + y)$ .

As we shall see, and so forth.

Now let us follow Godel and the reflection principle, where assertions of consistency and inconsistency are reflected into a logico-mathematical system to be assertions about numbers via some definite method of Godel numbering. The assertion of consistency is then the affirmation that no number exists representing a proof leading to " $\neg 0 = 0$ ". So, to prove a system is consistent, one can proceed by contradiction, by supposing that such a number *does* exist. That is, suppose (in **F**) that a particular system **X** is inconsistent. Then there exists a number, say  $n$ , representing a proof of " $\neg 0 = 0$ ". **F** can prove that there exist numbers from this point downward, and this may, depending on **X**, give enough room to establish that **X** has a model  $M$ , that truth-in- $M$  is definable for wffs of size small enough relative to  $n$ , that all the wffs in the proof of contradiction, being small enough, must be true-in- $M$ , and in turn that **F** is consistent. The assumption of **X** inconsistent therefore leads to a contradiction, so **X** is consistent. When **X** is **F** itself, **F** has proved its own consistency.

The axioms featured in this paper were introduced in [B4]. They have similarities to the work of Frege Arithmetic, for which one may consult Crispin Wright [W2], George Boolos [B1], Richard Heck [H2,H3], and Neil Tennant [T1].

### C. Notation

- $P \equiv Q$  for  $\forall x ( Px \Leftrightarrow Qx )$  or  $\forall x \forall y ( Px,y \Leftrightarrow Qx,y )$
- $P \subseteq Q$  for  $\forall x ( Px \Rightarrow Qx )$
- $P \subset Q$  for  $\forall x ( Px \Rightarrow Qx ) \ \& \ \neg P \equiv Q$
- $P \cup Q$  for  $\{z : Pz \vee Qz\}$  or  $\{y,z : Py,z \vee Qy,z\}$
- $P \cap Q$  for  $\{z : Pz \ \& \ Qz\}$
- $P \setminus Q$  for  $\{z : Pz \ \& \ \neg Qz\}$  or  $\{y,z : Py,z \ \& \ \neg Qy,z\}$
- $R \upharpoonright P$  for  $\{x,y : Px \ \& \ Rx,y\}$
- $R \circ S$  for  $\{x,y : \exists z ( Rx,z \ \& \ Sz,y ) \}$
- $x \leq_{N,M} y$  for  $Nx \ \& \ Ny \ \& \ \exists P \exists Q ( P \subseteq Q \ \& \ Mx,P \ \& \ My,Q )$
- $x <_{N,M} y$  for  $x \leq_{N,M} y \ \& \ \neg x = y$
- $\phi$  for  $\{z : \neg z = z\}$  or  $\{y,z : \neg z = z\}$
- $\mathbb{U}$  for  $\{z : z = z\}$
- $\{a\}$  for  $\{z : z = a\}$
- $\{a,b\}$  for  $\{z : z = a \vee z = b\}$

$\{(a,b)\}$  for  $\{y,z : y = a \ \& \ z = b\}$   
 $x \in P$  for  $Px$  (when  $P$  is unary only)  
 $(R^D)$  for  $\{x : \exists y R_{x,y}\}$   
 $(R^I)$  for  $\{y : \exists x R_{x,y}\}$   
 $f R$  for  $\forall x \forall y \forall z (R_{x,y} \ \& \ R_{x,z} \Rightarrow y = z)$  ( $R$  is a “function”)  
 $1 R$  for  $\forall x \forall y \forall z (R_{x,y} \ \& \ R_{z,y} \Rightarrow x = z)$  ( $R$  is “one-to-one”)  
 $P \sim Q$  for  $\exists R ( f R \ \& \ 1 R \ \& \ (R^D) \equiv P \ \& \ (R^I) \equiv Q )$

In practice  $N$  and  $M$  will be fixed, so only unsubscripted “ $\leq$ ” and “ $<$ ” will be used.

## D. The Logic and System

Consider deductive second-order logic with equality, with a constant  $0$ , a one-place predicate  $N$ , and two two-place predicates  $\sigma$  and  $M$  ( $M$  being third-order).  $Nx$  says that  $x$  is a finite number,  $\sigma_{n,m}$  that  $m$  is a successor of  $n$  in the natural number series, and  $M_{n,P}$  that  $P$  numbers  $n$ .

[B4] explains the connection with Frege Arithmetic (FA). Suffice to say here that FA and its variants assume the existence of a function  $\#$  on predicates, where  $(\#P)$  means “the number of  $P$ ”. The symbolism therefore pre-supposes totality and uniqueness. The motivation for the present formulation may be seen as the introduction of the third-order predicate,  $M$ , which is agnostic about totality and uniqueness. That is,  $M_{n,P}$  is similar to FA’s  $(\#P) = n$ , but it is stripped of the assumptions of uniqueness and existence. Uniqueness will be introduced into the system via an explicit axiom, while totality is never assumed.

Since there are no function symbols, the only lower-case terms are  $0$  and variables. The only upper-case terms are upper-case variables. Also remark that equality (which applies only between lower-case terms) is taken as a primitive and not defined. This is necessary since equality, when defined, is given an impredicative definition, and  $F$  will be restricted to arithmetic comprehension.

Atomic wffs are (with  $t, t_1, \dots, t_n$  lower-case terms,  $P$  upper-case variable):

$t_1 = t_2$   
 $Pt_1, \dots, t_n$   
 $Nt$   
 $\sigma t_1, t_2$   
 $Mt, P$

In fact, in terms of deductive power, the reader can verify that we only use 1-ary and 2-ary predicates, so  $n = 1$  or  $n = 2$ .

Suppose  $\phi$  and  $\psi$  are wffs, and  $x$  and  $P$  variables. Then

$(\phi \Rightarrow \psi)$   
 $(\neg \phi)$   
 $\forall x \phi$   
 $\forall P \phi$

are wffs. Other logical connectives, in particular  $\&$  and  $\exists$ , are given their standard definitions.

Consider any standard axiomatization of deductive second-order logic, e.g. see [S1] (although without [S1]'s version of the axiom of choice stated therein). In particular, full comprehension is, for  $n \geq 1$ , and for  $\phi$  not containing any free "P,"

$$\exists P \forall x_1 \dots \forall x_n ( P x_1, \dots, x_n \Leftrightarrow \phi ),$$

Arithmetic comprehension restricts  $\phi$  to wffs with no quantified upper-case variables. We will write such P as  $\{x_1, \dots, x_n : \phi\}$ .

The mathematical axioms and rules are taken from [B4]:

(F1) Uniqueness of numbering.

$$\forall n \forall m \forall P ( Nn \& Mn, P \& Mm, P \Rightarrow n = m )$$

(F2) Zero.

$$\forall P ( M0, P \Leftrightarrow \neg \exists x Px )$$

(F3) Successoring.

$$\forall n \forall m \forall P \forall Q \forall a ( Nn \& \sigma n, m \& \neg Pa \& \forall x ( Qx \Leftrightarrow Px \vee x = a ) \Rightarrow ( Mn, P \Leftrightarrow Mm, Q ) )$$

(F4) Induction. Let  $\phi$  be a well-formed formula (with no appearance of m). Use  $\phi [x \setminus y]$  to mean x replaces all (free) instances of y. Suppose  $\phi [0 \setminus n]$  and  $\forall n \forall m ( Nn \& \sigma n, m \& \phi \Rightarrow \phi [m \setminus n] )$ . Then  $\forall n ( Nn \Rightarrow \phi )$

Remark that, to prove the Peano Axioms two additional axioms would be needed:

(F5) N0

(F6) Ad infinitum.

$$\forall n \forall P \forall a ( Nn \& Mn, P \& \neg Pa \Rightarrow \exists m ( Nm \& Mm, (P \cup \{a\}) ) )$$

We set  $\mathbf{F} = \{F1, F2, F3, F4\}$  + arithmetic comprehension.  $\mathbf{F} + \{F5\}$  (and so  $\mathbf{F}$ ) has the following model of one lower-term element, 0 (we use the same term to refer to the logical symbol and its interpretation, which should not cause any confusion):

0 satisfies N,

(0,0) does not satisfy  $\sigma$ ,

(0,P) satisfies M if and only if  $P \equiv \phi$

It is the the simplicity of this model, which permits  $\mathbf{F}$  to prove its own consistency via a standard method of Godel numbering, and as well the consistency of  $\mathbf{F} + \{F5\}$ , that of  $\mathbf{F} + \{F6\}$ , and indeed (although only for certain Godel numberings) that of  $\mathbf{F} + \{F6.n\}$ , for any natural number n, where F6.n asserts the existence of all numbers less than or equal to n.

## E. Basic Propositions

Recall from *Systems of Foundations of Arithmetic* [B4] that the following form of induction

may be used:

(F4\*) Suppose  $N_0 \Rightarrow \phi(0)$  and  $\forall n \forall m (N_n \& N_m \& \sigma_{n,m} \& \neg m = 0 \& \phi(n) \Rightarrow \phi(m))$ . Then  $\forall n (N_n \Rightarrow \phi(n))$ .

Recall also that (F1) to (F4) suffice to prove the following propositions:

E.1 *Prop.* Suppose  $\exists n N_n$ . Then  $N_0$ .

E.2 *Prop.*  $\forall P \forall n (M_{n,P} \& \neg n = 0 \Rightarrow \exists x P_x)$

E.3 *Corollary.*  $\forall P \forall n (M_{n,P} \& P \equiv \phi \Rightarrow n = 0)$

E.4 *Prop.*  $\forall n (N_n \& \neg n = 0 \Rightarrow \exists p (N_p \& \sigma_{p,n}))$

E.5 *Prop. (Finite Hume's Principle).*  $\forall n \forall P \forall Q (N_n \& M_{n,P} \Rightarrow (P \sim Q \Leftrightarrow M_{n,Q}))$

E.6 *Prop.*  $\forall n \forall P \forall Q (N_n \& M_{n,P} \& P \equiv Q \Rightarrow M_{n,Q})$

E.7 *Prop.*  $\forall n \forall m \forall P \forall a (N_n \& N_m \& M_{n,P} \& M_{m,(P \cup \{a\})} \& \neg Pa \Rightarrow \sigma_{n,m})$

E.8 *Prop.*  $\forall n (N_n \Rightarrow \neg \sigma_{n,0})$

E.9 *Prop.*

a. If  $N_n \& M_{n,P}$ , then  $0 \leq n$  and  $n \leq n$ .

b. If  $\exists x N_x$ , then both  $0 \leq 0$  and  $\forall z ((0 \leq z \& z \leq 0) \Leftrightarrow z = 0)$

E.10 *Prop. (Pigeon Hole Principle)*  $\forall n \forall P \forall Q (N_n \& M_{n,P} \& M_{n,Q} \& P \subseteq Q \Rightarrow P \equiv Q)$

E.11 *Prop.* Let  $n < m$ . Then  $N_n \& N_m \& \exists P \exists Q (P \subset Q \& M_{n,P} \& M_{m,Q})$ .

E.12 *Prop. (POTINF)*  $\forall n (N_n \Rightarrow \exists P \exists a (M_{n,P} \& \neg Pa))$

E.13 *Prop. (ACTINF)*  $\neg \exists n (N_n \& M_{n,\mathbb{U}})$

*Pf:*

Suppose  $N_n \& M_{n,\mathbb{U}}$  for some  $n$ . By *POTINF* E.12,  $M_{n,P}$  and  $\neg Pa$  for some  $P, a$ . Evidently,  $P \subseteq \mathbb{U}$ . By E.10  $P \equiv \mathbb{U}$ , contradicting  $\neg Pa$ .

E.14 *Corollary.* If  $N_n \& M_{n,P}$ , then  $\neg Pa$  for some  $a$ .

Note that *FOEA* [B3] proves the following (by induction) in **F**:

E.15. *Prop. (IV5.10 in FOEA)*

$\forall n \forall P \forall Q \forall R \forall S (N_n \& M_{n,R} \& P \sim Q \& R \sim S \& R \subseteq P \& S \subseteq Q \Rightarrow (P \setminus R) \sim (Q \setminus S))$

E.16. *Prop* (IV7.20 in FOEA).  
 $\forall n \forall P ( Nn \Rightarrow \exists Q ( Mn,Q \& ( P \subseteq Q \vee Q \subseteq P ) ) )$

The following proposition ensures the “downwards” character of **F** and is thus important:

E.17 *Prop.*  $\forall n \forall P ( Nn \& Mn,P \& Q \subseteq P \Rightarrow \exists k ( Nk \& Mk,Q ) )$

*Pf.*

By induction (F4\*) on  $n$ , with  $\phi$  as  
 $\forall P ( Mn,P \& Q \subseteq P \Rightarrow \exists k ( Nk \& Mk,Q ) )$ .

Suppose  $N0 \& M0,P \& Q \subseteq P$ . Then  $P \equiv \phi$  by (F2). So  $Q \equiv \phi$ . By (F2) again,  
 $M0,Q$ .

Now assume  $Nn \& Nm \& \sigma n,m \& \neg m = 0 \& \phi$ , and suppose  $Mm,P \& Q \subseteq P$ . If  $Q \equiv P$ , then we are done. O.w.  $Q \subseteq P \setminus \{a\}$  for some  $a$  with  $Pa$ . By (F3)  $Mn,P \setminus \{a\}$ . Done by the induction hypothesis.

E.18 *Def.*  $\text{one}(u)$  abbreviates  $Nu \& \sigma 0,u$ .

Of course it cannot be shown that there exists  $u$  s.t.  $\text{one}(u)$ . But if  $u$  exists, then it has all the “downward” properties of one.

In order to render assertions more perspicacious, we introduce a variable  $1$  (adding it to the usual alphabetic variables). In the future, we will use this special variable as the argument of the predicate one.

E.19 *Prop.* Let  $\text{one}(1)$ . Then  $M1,P$  if and only if  $\exists a P \equiv \{a\}$ .

*Pf.*

Suppose  $M1,P$ . By E.8  $\neg 1 = 0$ . By E.2  $Pa$  for some  $a$ . By (F3)  $M0,(P \setminus \{a\})$ . By (F2)  $(P \setminus \{a\}) \equiv \phi$ . Hence  $P \equiv \{a\}$ .

On the other hand suppose  $P \equiv \{a\}$  for some  $a$ . Since  $M0,\phi$  by (F2),  $M1,P$  by (F3).

E.20 *Prop.* Let  $P \equiv \{a\}$  for some  $a$ , and assume  $N1$ . Then  $\text{one}(1)$  if and only if  $M1,P$ .

*Pf.*

Half follows from E.19. Now suppose  $M1,P$ . Apply E.7.

E.21 *Prop.* Let  $\text{one}(1)$ . Then  $\neg 1 = 0$  and indeed  $0 < 1$ .

*Pf.*

By E.19  $M1,\{0\}$ . By (F2)  $\neg 1 = 0$ . By (F2) again,  $M0,\phi$ . Evidently  $\phi \subseteq \{0\}$ . Hence  $0 \leq 1$ .

E.22. *Prop.* Let  $Nn \& \neg n = 0$ . Then  $\exists 1 \text{one}(1)$ , and moreover  $1 \leq n$ .

*Pf.*

By POTINF E.12,  $Mn,P$  for some  $P$ . By E.2  $Pa$  for some  $a$ . But  $\{a\} \subseteq P$ , so by E.17,  $N1 \& M1,\{a\}$  for some  $1$ . By E.20  $\text{one}(1)$ . Evidently,  $1 \leq n$ .

E.23 *Prop.*

a) *Transitivity.* If  $a \leq b$  and  $b \leq c$ , then  $a \leq c$ .

b) *Dichotomy*.  $\forall a \forall b (Na \& Nb \Rightarrow a \leq b \vee b < a)$

*Pf.*

a) Assume  $a \leq b$  and  $b \leq c$ . Then  $Na \& Nb \& Nc \& A \subseteq B \& Ma, A \& Mb, B \& B' \subseteq C \& Mb, B' \& Mc, C$ . By E.5,  $B \sim B'$ , so there exists one-to-one function  $R$  from  $B$  onto  $B'$ . Set  $A'$  to  $(R \upharpoonright A)^{\downarrow}$ . Evidently  $A \sim A'$  and  $A' \subseteq C$ . So  $Ma, A'$  by E.5, and thus  $a \leq c$ .

b) Assume  $Na \& Nb$ . By *POTINF* E.12,  $Ma, P$  for some  $P$ . By E.16,  $Mb, Q \& (P \subseteq Q \vee Q \subseteq P)$  for some  $Q$ . If  $P \subseteq Q$ , then  $a \leq b$ . And if not  $P \subseteq Q$ , then  $Q \subset P$ . So  $b \leq a$ . If  $b = a$ , then  $P = Q$  by E.10, a contradiction. So  $\neg b = a$ , hence  $b < a$ .

E.24 *Prop.* Suppose  $Nx \& Ny \& \sigma x, y \& \sigma x, z$ . Then  $y = z$ .

*Pf.*

By *POTINF* E.12,  $\exists P \exists a$  such that  $Mx, P \& \neg Pa$ . Set  $Q = P \cup \{a\}$ . By (F3)  $My, Q$  and  $Mz, Q$ . By (F1)  $y = z$ .

## F. Addition

F.1 *Def.* Use  $+(x, y, z)$  to abbreviate:

$$Nx \& Ny \& Nz \& \exists P \exists Q ( (P \cap Q) = \phi \& Mx, P \& My, Q \& Mz, (P \cup Q) )$$

F.2 *Prop. (Uniqueness.)*

$$\forall x \forall y \forall a \forall b ( +(x, y, a) \& +(x, y, b) \Rightarrow a = b )$$

*Pf.*

Assume  $+(x, y, a) \& +(x, y, b)$ . Then by F.1, for some  $P, Q, P', Q'$ ,

$$Nx \& Ny \& Na \text{ and } (P \cap Q) = \phi \& Mx, P \& My, Q \& Ma, (P \cup Q)$$

$$Nx \& Ny \& Nb \text{ and } (P' \cap Q') = \phi \& Mx, P' \& My, Q' \& Mb, (P' \cup Q')$$

Evidently,  $(P \cup Q) \sim (P' \cup Q')$ . By E.5,  $Ma, (P' \cup Q')$ . By (F1),  $a = b$ .

When  $+(x, y, z)$ , we will use  $(x+y)$  to refer to  $z$ , which is legitimate given the previous proposition. Note that the appearance of  $(x+y)$  in an atomic formula  $\phi$  is to be read as  $\exists z (+(x, y, z) \& \phi^*)$  where  $\phi^*$  is  $\phi$  with  $z$  (assumed not to be appearing in  $\phi$ ) replacing  $(x+y)$ .

So e.g.  $(x+y) \leq a$  means

$$\exists z (+(x, y, z) \& z \leq a),$$

and  $(x+y) = z'$  means

$$\exists z (+(x, y, z) \& z = z'), \text{ i.e. } +(x, y, z').$$

F.3 *Prop.*

1) *Commutative Law*.  $\forall x \forall y \forall z ( (x+y) = z \Rightarrow (y+x) = z )$

**Note:** Henceforth we will assume commutative permutations, so e.g. even though 3) only proves  $(0+x) = x$ , we will suppose it proves  $(x+0) = x$  as well.

2) *Zero*.

a)  $\forall x ( Nx \Rightarrow (0+x) = x )$

b)  $\forall x \forall y ( (x+y) = x \Rightarrow y = 0 )$

c)  $\forall x \forall y ( (x+y) = 0 \Rightarrow x = 0 \& y = 0 )$

3) *Associative Law*.

a)  $\forall x \forall y \forall z \forall a ( ((x+y)+z) = a \Rightarrow (x+(y+z)) = a )$

b)  $\forall x \forall y \forall z \forall a ( (x+(y+z)) = a \Rightarrow ((x+y)+z) = a )$

- 4) *Cancellation*.  $\forall x \forall y \forall z ( (x+y) = (x+z) \Rightarrow y = z )$   
 5)  $\forall x \forall y ( x \leq y \Leftrightarrow \exists z (x+z) = y )$   
 6)  $\forall a \forall b \forall x \forall y \forall z ( a \leq x \ \& \ b \leq y \ \& \ (x+y) = z \Rightarrow (a+b) \leq z )$   
**Note:**  $(x+y) = z$  is necessary among the premises in 6), since it provides the assurance that  $+(x,y,k)$  for some  $k$ . This kind of move will often be used.  
 7)  $\forall a \forall x \forall y \forall z ( x \leq y \ \& \ (y+z) = a \Rightarrow (x+z) \leq (y+z) )$   
 8)  $\forall a \forall b \forall c \forall y \forall z ( (x+z) \leq (y+z) \Rightarrow x \leq y )$   
 9)  $\forall x \forall y ( Nx \ \& \ Ny \ \& \ \sigma_{x,y} \Leftrightarrow \exists 1 (one(1) \ \& \ (x+1) = y ) )$   
 10)  $\forall x \forall y \forall 1 ( Nx \ \& \ Ny \ \& \ one(1) \ \& \ \sigma_{x,y} \Rightarrow (x+1) = y )$   
 11)  $\forall x \forall y \forall 1 ( one(1) \ \& \ (x+y) = 1 \ \& \ \neg x = 0 \Rightarrow x = 1 \ \& \ y = 0 )$

- 12)  
 a)  $\forall x \forall n \forall m ( \sigma_{n,m} \Rightarrow ( x \leq n \Leftrightarrow x < m ) )$   
 b)  $\forall x \forall n \forall m ( \sigma_{n,m} \Rightarrow ( x \leq m \Leftrightarrow x \leq n \vee x = m ) )$

*Pf.*

1) Assume  $(x+y) = z$ . Then  $+(x,y,z)$ . By F.1  $Nx \ \& \ Ny \ \& \ Nz$ , and there are  $X, Y$  such that:

$$(X \cap Y) \equiv \phi \ \& \ M_{x,X} \ \& \ M_{y,Y} \ \& \ M_{z,(X \cup Y)}.$$

Evidently  $(Y \cap X) \equiv \phi \ \& \ (Y \cap X) \equiv (X \cup Y)$ . By E.6,  $M_{z,(Y \cup X)}$ . Thus  $+(y,x,z)$ , so  $(y+x) = z$ .

**Note:** In the future, we will pass from  $(x+y) = z$  to  $+(x,y,z)$  and back again, without comment.

2a) Suppose  $Nx$ . By E.1,  $N0$ . By *POTINF* E.12,  $M_{x,P}$  for some  $P$ . By (F2),  $M0,\phi$ .

2b) Suppose  $(x+y) = x$ . Then  $Nx \ \& \ Ny$ , and there are  $X, Y$  such that:

$$(X \cap Y) \equiv \phi \ \& \ M_{x,X} \ \& \ M_{y,Y} \ \& \ M_{x,(X \cup Y)}.$$

Obviously,  $X \subseteq (X \cup Y)$ , so by E.10,  $(X \cup Y) \equiv X$ . Thus  $Y \equiv \phi$ . By E.3  $y = 0$ .

2c) Assume  $(x+y) = 0$ . Then  $Nx \ \& \ Ny$ , and there are  $X, Y$  such that:

$$(X \cap Y) \equiv \phi \ \& \ M_{x,X} \ \& \ M_{y,Y} \ \& \ M0,(X \cup Y).$$

By (F2),  $(X \cup Y) \equiv \phi$ . Evidently,  $X \equiv Y \equiv \phi$ . By E.3,  $x = y = 0$ .

3a) Assume  $((x+y)+z) = a$ . Then  $Nz \ \& \ Na$ , and there are  $C, Z$  such that:

$$(C \cap Z) \equiv \phi \ \& \ M_{c,C} \ \& \ M_{z,Z} \ \& \ M_{a,(C \cup Z)} \ \& \ (x+y) = c.$$

The latter conjunct implies that  $Nx \ \& \ Ny \ \& \ Nc$  and there are  $X, Y$  s.t.

$$(X \cap Y) \equiv \phi \ \& \ M_{x,X} \ \& \ M_{y,Y} \ \& \ M_{c,(X \cup Y)}.$$

By E.5  $(X \cup Y) \sim C$ , so evidently there exist  $X', Y'$  such that

$$X' \sim X \ \& \ Y' \sim Y \ \& \ (X' \cap Y') \equiv \phi \ \& \ (X' \cup Y') \equiv C.$$

By E.5 and E.6  $M_{x,X'} \ \& \ M_{y,Y'} \ \& \ M_{c,(X' \cup Y')}$ .

Evidently,  $(Y' \cap Z) \equiv \phi$  and  $(Y' \cup Z) \subseteq (C \cup Z)$ . By E.17  $M_d,(Y' \cup Z)$  for some  $d$  s.t.  $Nd$ . Note that  $d = (y+z)$ .

Also evidently,  $(X' \cap (Y' \cup Z)) \equiv \phi$  and  $(X' \cup (Y' \cup Z)) \equiv (C \cup Z)$ . Thus  $(x+d) = a$ , and so  $(x+(y+z)) = a$ .

3b) Assume  $(x+(y+z)) = a$ . By two applications of 1),  $((z+y)+x) = a$ . By 3a)  $(z+(y+x)) = a$ . By two more applications of 1),  $((x+y)+z)=a$ .

4) Assume  $(x+y) = (x+z)$ . Then  $Nx \& Ny \& Nz$ , and there are  $X, Y, X'$  and  $Z'$  such that:

$$(X \cap Y) \equiv \phi \& Mx, X \& My, Y \& M(x+y), (X \cup Y) \text{ and}$$

$$(X' \cap Z') \equiv \phi \& Mx, X' \& Mz, Z' \& M(x+z), (X' \cup Z').$$

By E.5  $X \sim X'$  and, since  $(x+y) = (x+z)$ ,  $(X \cup Y) \sim (X' \cup Z')$ . E.15 implies that  $Y \sim Z'$ . So by E.5,  $My, Z'$ . By (F2),  $y = z$ .

5) Suppose  $x \leq y$ . Then  $Nx \& Ny$  and  $P \subseteq Q \& Mx, P \& My, Q$  for some  $P, Q$ . Consider  $P$  and  $Q \setminus P$ . Their union is equivalent to  $Q$  and their intersection is empty. By E.17,  $Mz, (Q \setminus P)$  for some  $z$  s.t.  $Nz$ . By definition F.1  $(x+z) = y$ .

Now suppose  $(x+z) = y$  for some  $z$ . Then  $Nx \& Ny \& Nz$  and

$(P \cap Q) \equiv \phi \& Mx, P \& Mz, Q \& My, (P \cup Q)$  for some  $P, Q$ . Evidently,  $P \subseteq (P \cup Q)$ . But this means  $x \leq y$ .

6) Assume  $a \leq x \& b \leq y \& (x+y) = z$ . By 5)  $(a+a') = x$  and  $(b+b') = y$  for some  $a', b'$ . So  $z = ((a+a')+(b+b'))$ . By various applications of the Commutative and Associative Laws,  $z = ((a+b)+(a'+b'))$ . Reapplying 5),  $(a+b) \leq z$ .

7) Assume  $x \leq y \& (y+z) = a$ . By 5)  $(x+x') = y$ . So  $((x+x')+z) = a$ . Applying the Commutative and Associative Laws,  $((x+z)+x') = a$ . Thus by 5) again,  $(x+z) \leq a$ , and so  $(x+z) \leq (y+z)$ .

8) Assume  $(x+z) \leq (y+z)$ . By 5)  $((x+z)+c) = (y+z)$  for some  $c$ . By Associativity and Commutativity,  $((x+c)+z) = (y+z)$ . By Cancellation 4),  $(x+c) = y$ . By 5),  $x \leq y$ .

9) Suppose  $Nx \& Ny \& \sigma x, y$ . By *POTINF* E.12,  $Mx, P \& \neg Pa$  for some  $P, a$ . By (F3),  $My, (P \cup \{a\})$ . By (F2),  $\neg y = 0$ . By E.17,  $M1, \{a\}$  for some  $1$  s.t.  $N1$ . By E.20,  $\text{one}(1)$ . By definition of addition,  $(x+1) = y$ .

Now suppose  $\text{one}(1) \& (x+1)=y$ , for some  $1$ . Then  $Nx \& Ny \& N1$  and  $(P \cap Q) \equiv \phi \& Mx, P \& M1, Q \& My, (P \cup Q)$ , for some  $P, Q$ . By E.19,  $Q \equiv \{q\}$  for some  $q$ . Evidently,  $(P \cup Q) \equiv (P \cup \{q\})$ , so by E.6,  $My, (P \cup \{q\})$ . So by E.7,  $\sigma x, y$ .

10) Assume  $Nx \& Ny \& \text{one}(1) \& \sigma x, y$ . By 9)  $Nu \& \sigma 0, u \& (x+u) = y$  for some  $u$ . But  $u = 1$  by E.24.

11) Assume  $\text{one}(1) \& (x+y) = 1 \& \neg x = 0$ . Then  $Nx \& Ny$ , and there are  $X, Y$  such that:

$$(X \cap Y) \equiv \phi \& Mx, X \& My, Y \& M1, (X \cup Y).$$

By E.19,  $(X \cup Y) \equiv \{a\}$  for some  $a$ . But  $\neg X \equiv \phi$  by E.3, so evidently  $X \equiv \{a\}$  and  $Y \equiv \phi$ . By E.19, (F1), and E.3,  $x = 1$  and  $y = 0$ .

12a)  $\forall x \forall n \forall m ( \sigma n, m \Rightarrow ( Nm \& x \leq n \Leftrightarrow Nn \& x < m ) )$

Assume  $\sigma n, m$ .

Suppose  $Nm \& x \leq n$ . Then  $(x+z) = n$  for some  $z$ , by 5). Also, by 9),  $\text{one}(1) \& (n+1) = m$  for some  $1$ . So  $((x+z)+1) = m$ . By Associativity 3a),  $(x+(z+1)) = m$ . By 5)  $x \leq m$ . If  $x = m$ , then by 2b) and 2c),  $1 = 0$ . This contradicts E.21.

On the other hand, suppose  $Nn \& x < m$ . Further suppose that  $\neg x \leq n$ . By E.23b,  $n < x$ . So  $\neg x = n$ . By 5),  $(n+z) = x$  and  $(x+z') = m$ , for some  $z, z'$ . Remark that, by 2a),

neither  $z$  nor  $z'$  equals 0. Also, using Associativity,  $(n + (z + z')) = m$ . But by 9)  $(n+1) = m$  for 1 s.t. one(1). Hence by 4)  $(z + z') = 1$ . But this contradicts 11).

12b) Follows directly from 12a).

It is now easy to prove  $\leq$  is Anti-Symmetric:

F.4 Prop.  $\forall x \forall y (x \leq y \ \& \ y \leq x \Rightarrow x = y)$

Pf.

Assume  $x \leq y \ \& \ y \leq x$ . By F.3.5,  $(x+z) = y$  and  $(y+z') = x$  for some  $z, z'$ . Then  $((x+z)+z') = x$ . By Associativity F.3.3a,  $(x+(z+z')) = x$ . So  $(z+z') = 0$  by F.3.2b. By F.3.2c,  $z = 0$ . By F.3.2a,  $x = y$ .

F.5 Prop. *Well-Ordering Principle*. Let  $N_n$  and let  $\phi(x)$  be any formula with one free variable. Then:

1) Either:

$$\forall x (x \leq n \Rightarrow \neg(\phi(x)))$$

or

$$\exists x (x \leq n \ \& \ (\phi(x)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow x \leq y)$$

2) Either:

$$\forall x (Nx \Rightarrow \neg(\phi(x)))$$

or

$$\exists x (Nx \ \& \ (\phi(x)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow x \leq y)$$

3) Either:

$$\neg \exists x (Nx \ \& \ (\phi(x)))$$

or

$$\exists x (Nx \ \& \ (\phi(x)) \ \& \ \forall y (y < x \Rightarrow \neg(\phi(y)))$$

Pf:

1) Proceed by induction (F4\*), with  $\phi$  as

$$(\forall x (x \leq n \Rightarrow \neg(\phi(x))) \vee \exists x (x \leq n \ \& \ (\phi(x)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow x \leq y)).$$

Trivial when  $n = 0$ , since either  $(\phi(x))$  or  $\neg(\phi(x))$ . Now assume  $N_n \ \& \ N_m \ \& \ \sigma_{n,m} \ \& \ \neg m = 0 \ \& \ \phi$ . By F.3.12b, one of these cases obtains:

$$\begin{aligned} &\forall x (x \leq m \Rightarrow \neg(\phi(x))) \\ &\forall x (x \leq n \Rightarrow \neg(\phi(x))) \ \& \ \phi(m) \text{ or} \\ &\exists x (x \leq n \ \& \ (\phi(x))) \end{aligned}$$

In the first case we are done. In the second it is easy to show that

$$m \leq m \ \& \ (\phi(m)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow m \leq y).$$

And in the third, let  $w$  be s.t.  $w \leq n \ \& \ (\phi(w))$ . Then by the Induction Hypothesis,

$$\exists x (x \leq n \ \& \ (\phi(x)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow x \leq y),$$

so of course

$$\exists x (x \leq m \ \& \ (\phi(x)) \ \& \ \forall y (Ny \ \& \ (\phi(y)) \Rightarrow x \leq y).$$

2) Follows from 1).

3) Follows from 2) and E.23b.

F.6 Prop. Suppose  $\forall x (\psi(x) \Rightarrow x \leq n)$  and  $\exists x \psi(x)$ . Then

$$\exists z (\psi(z) \ \& \ \forall y (\psi(y) \Rightarrow y \leq z)).$$

*Pf:*

Proceed by induction ( $F4^*$ ), with  $\phi$  as

$$\forall P ( \forall x (\psi(x) \Rightarrow x \leq n) \ \& \ \exists x \psi(x) \\ \Rightarrow \exists z (\exists x \psi(x) \ \& \ \forall y (\psi(y) \Rightarrow y \leq z)) ).$$

Case  $n = 0$ . Suppose  $\forall x (\psi(x) \Rightarrow x \leq n) \ \& \ \exists x \psi(x)$ . So  $\psi(a)$  for some  $a$ . So  $a \leq 0$ . Thus  $N0$ . Similarly, if  $\psi(x)$ , then  $x \leq 0$ , so by E.9.b,  $x = 0$ . Hence  $\forall x (\psi(x) \Leftrightarrow x = 0)$ , i.e.  $\psi(0)$ , and if  $\psi(y)$ , then  $y = 0$ , so  $0 \leq 0$ .

Induction Step. Now assume  $Nn \ \& \ Nm \ \& \ \sigma_{n,m} \ \& \ \neg m = 0 \ \& \ \phi$ . And suppose  $\forall x (\psi(x) \Rightarrow x \leq m) \ \& \ \exists x \psi(x)$ . If  $\neg \psi(m)$ , then  $\forall x (\psi(x) \Rightarrow x \leq n)$  by F.3.12b, and the result follows from the Induction Hypothesis.

On the other hand, suppose  $\psi(m)$ . Evidently, if  $\psi(y)$ , then  $y \leq m$ .

## G. Multiplication.

G.1 *Def.* Use  $*(x,y,z)$  to abbreviate:

$$Nx \ \& \ Ny \ \& \ Nz \ \& \\ \exists P \exists R ( 1 \ R \ \& \ M_{x,P} \ \& \ \forall u (Pu \Rightarrow My, \{v : Ru, v\}) \\ \ \& \ M_{z, \{v : \exists u (Pu \ \& \ Ru, v)\}} )$$

G.2 *Prop.*

1) *Zero (Left)*  $\forall x ( Nx \Rightarrow *(0,x,0) )$

2)  $\forall n \forall y \forall m \forall a \forall b ( *(n,y,a) \ \& \ (a+y) = b \ \& \ Nm \ \& \ \sigma_{n,m} \Rightarrow *(m,y,b) )$

3)  $\forall n \forall y \forall z \forall m \forall b ( *(m,y,z) \ \& \ Nn \ \& \ \sigma_{n,m} \Rightarrow \exists b ( *(n,y,b) \ \& \ (b+y) = z )$

4) *Zero (Right)*.  $\forall x ( Nx \Rightarrow *(x,0,0) )$

5) *Uniqueness*.  $\forall x \forall y \forall a \forall b ( *(x,y,a) \ \& \ *(x,y,b) \Rightarrow a = b )$

**Note:** From now on, as with addition, use  $(x^*y)$  to refer to that  $z$  (if it exists) such that  $*(x,y,z)$ , guaranteed to be unique by 5).

6)  $\forall x ( (x^*y) = 0 \Rightarrow x = 0 \vee y = 0 )$

7a)  $\forall n \forall 1 ( Nn \ \& \ \text{one}(1) \Rightarrow (1^*n) = n )$

7b)  $\forall x \forall y \forall 1 ( \text{one}(1) \ \& \ (x^*y) = 1 \Rightarrow x = 1 \ \& \ y = 1 )$

8) *Distributive Laws*

a)  $\forall n \forall x \forall y \forall a ( Nn \ \& \ Nx \ \& \ Ny \ \& \ ((x+y)^*n) = a \Rightarrow ((x^*n) + (y^*n)) = a )$

b)  $\forall n \forall x \forall y \forall a ( Nn \ \& \ Nx \ \& \ Ny \ \& \ (n^*(x+y)) = a \Rightarrow ((n^*x) + (n^*y)) = a )$

c)  $\forall n \forall x \forall y \forall a ( Nn \ \& \ Nx \ \& \ Ny \ \& \ ((n^*x) + (n^*y)) = a \ \& \ \neg n = 0 \\ \Rightarrow (n^*(x+y)) = a )$

**Note:** In 8c) " $\neg n = 0$ " is needed, since one may have  $((0^*x) + (0^*y)) = 0$  without  $(x+y)$  existing.

9)  $\forall x \forall y \forall z \forall a ( ((y^*x) + y) = a \ \& \ \sigma_{x,z} \Rightarrow (y^*z) = a )$

10) *Commutative Law*.  $\forall x \forall y \forall z ( (x^*y) = z \Rightarrow (y^*x) = z )$

**Note:** From now on, as with addition, propositions will only state one form of commutative permutations, and assume the rest as granted.

11) *Associative Laws*.

a)  $\forall x \forall y \forall z \forall a ( ((x^*y)^*z) = a \ \& \ \neg x = 0 \Rightarrow (x^*(y^*z)) = a )$

b)  $\forall x \forall y \forall z \forall a ( ((0^*y)^*z) = a \ \& \ (y^*z) = x \Rightarrow (0^*(y^*z)) = a )$

c)  $\forall x \forall y \forall z \forall a ( (x^*(y^*z)) = a \ \& \ \neg z = 0 \Rightarrow ((x^*y)^*z) = a )$

d)  $\forall x \forall y \forall z \forall a ( (x^*(y^*0)) = a \ \& \ (x^*y) = z \Rightarrow ((x^*y)^*0 = a )$

**Note:** The generalized Associative Laws do not go through since e.g. the assumption of

- $((0^*y)^*z) = a$  does not ensure that  $(y^*z)$  exists.
- 12) *Cancellation.*  $\forall x \forall y \forall z ( (y^*x) = (z^*x) \ \& \ \neg x = 0 \Rightarrow y = z )$
- 13)  $\forall x \forall 1 ( (x^*1) = x \ \& \ \neg x = 0 \Rightarrow \text{one}(1) )$
- 14)
- a)  $\forall x \forall y \forall z \forall a ( x \leq y \ \& \ (y^*z) = a \Rightarrow (x^*z) \leq a )$ .
- b)  $\forall x \forall x' \forall y \forall z \forall a ( x \leq y \ \& \ x' \leq z \ \& \ (y^*z) = a \Rightarrow (x^*x') \leq a )$
- 15)  $\forall x \forall y \forall z ( (x^*z) \leq (y^*z) \ \& \ \neg z = 0 \Rightarrow x \leq y )$

*Pf.*

1) Assume  $Nx$ .  $M0, \phi$  by (F2). Vacuously,  $\forall u(\phi u \Rightarrow My, \{v : \phi u, v\})$ . (Remark: the first instance of  $\phi$  is one-place and the second is two-place.) Also vacuously,  $1 \phi$ . Finally,  $\{v : \exists u (\phi u \ \& \ \phi u, v)\} \equiv \phi$ , so by (F2)  $M0, \{v : \exists u (\phi u \ \& \ \phi u, v)\}$ . Hence  $*(0, x, 0)$ .

2) Assume  $*(n, y, a) \ \& \ (a+y) = b \ \& \ Nm \ \& \ \sigma n, m$ . Then  $Nn \ \& \ Ny \ \& \ Na \ \& \ Nb$  and for some  $P, R, A, B$

$$1 \ R \ \& \ Mn, P \ \& \ \forall u (Pu \Rightarrow My, \{v : Ru, v\}) \ \& \ Ma, \{v : \exists u (Pu \ \& \ Ru, v)\}$$

and

$$(A \cap B) \equiv \phi \ \& \ Ma, A \ \& \ My, B \ \& \ Mb, (A \cup B).$$

By *POTINF* E.12, there exists  $p$  s.t.  $\neg Pp$ . Using predicative comprehension, define  $P' = (P \cup \{p\})$ . By (F3)  $Mm, P'$ . By E.5,  $\{v : \exists u (Pu \ \& \ Ru, v)\} \sim A$ . Let  $S$  be the one-to-one function onto  $A$  with domain  $\{v : \exists u (Pu \ \& \ Ru, v)\}$ . Evidently,  $\{v : \exists u (Pu \ \& \ (R \circ S)u, v)\} \equiv A$ .

Using predicative comprehension, define

$$R' = \{u, v : (Pu \ \& \ (R \circ S)u, v) \vee (u = p \ \& \ Bv)\}.$$

Because  $R$  and  $S$  are one-to-one,  $(R \circ S)$  is one-to-one. But  $A$  and  $B$  are disjoint, and  $\neg Pp$ , so  $R'$  is also one-to-one.

Assume  $P'u$ . So either  $Pu$  or  $u = p$ . Suppose  $Pu$ . Then  $My, \{v : Ru, v\}$ . But  $S$  correlates  $\{v : Ru, v\}$  with  $\{v : (R \circ S)u, v\}$ , so  $My, \{v : (R \circ S)u, v\}$  by E.5.  $\neg p = u$  since  $Pu$ . So  $\{v : (R \circ S)u, v\} \equiv \{v : (Pu \ \& \ (R \circ S)u, v) \vee (u = p \ \& \ Bv)\}$ , and thus  $\{v : (R \circ S)u, v\} \equiv \{v : R'u, v\}$ . So  $My, \{v : R'u, v\}$ . Similar reasoning shows that  $Mu, \{v : R'u, v\}$  when  $u = p$ .

Finally, it is easy to see that  $\{v : \exists u (Pu \ \& \ R'u, v)\} \equiv (A \cup B)$ , so by E.6,  $Mb, \{v : \exists u (Pu \ \& \ R'u, v)\}$ .

Putting all this together, we can conclude that  $*(m, y, b)$ .

3) Assume  $*(m, y, z) \ \& \ Nm \ \& \ \sigma n, m$ . Then

$Nm \ \& \ Ny \ \& \ Nz$  and for some  $P, R$

$$1 \ R \ \& \ Mm, P \ \& \ \forall u (Pu \Rightarrow My, \{v : Ru, v\}) \ \& \ Mz, \{v : \exists u (Pu \ \& \ Ru, v)\}$$

By E.8,  $\neg m = 0$ . By E.2,  $Pp$  for some  $p$ . Set  $P' = P \setminus \{p\}$  and  $R' = R \upharpoonright P'$ . By (F3)  $Mn, P'$ .

Evidently,  $1 \ R'$  and  $\forall u (P'u \Rightarrow My, \{v : R'u, v\})$ . Also,

$\{v : \exists u (P'u \ \& \ R'u, v)\} \subseteq \{v : \exists u (Pu \ \& \ Ru, v)\}$ , so by E.17,  $Mb, \{v : \exists u (P'u \ \& \ R'u, v)\}$  for some  $b$  s.t.  $Nb$ . Hence,  $*(n, y, b)$ .

But also

$$\{v : \exists u (Pu \ \& \ Ru, v)\} \equiv \{v : \exists u (P'u \ \& \ R'u, v)\} \cup \{v : Rp, v\}$$

and, because  $R$  is one-to-one,

$$\{v : \exists u (P'u \ \& \ R'u, v)\} \cap \{v : Rp, v\} \equiv \phi.$$

Since  $My, \{v : Rp, v\}$ , we conclude that  $(b+y) = z$ .

4) Proceed by induction (F4\*), with  $\phi$  as  $*(n,0,0)$ .

If N0, then  $*(0,0,0)$  by 1).

Now assume  $Nn \& Nm \& \sigma_{n,m} \& \neg m = 0 \& \phi$ . Then N0 by E.1, so  $(0+0) = 0$  by F.3.2a. Hence  $*(n,0,0) \& (0+0) = 0 \& Nm \& \sigma_{n,m}$ . By 2)  $*(m,0,0)$ .

5) Proceed by induction (F4\*), with  $\phi$  as

$\forall y \forall a \forall b ( *(n,y,a) \& *(n,y,b) \Rightarrow a = b )$ .

Suppose  $*(0,y,a) \& *(0,y,b)$ . The first conjunct implies that  $Ny \& Na$  and, for some P,R,

$1 R \& M0,P \& \forall u(Pu \Rightarrow My, \{v : Ru,v\}) \& Ma, \{v : \exists u (Pu \& Ru,v)\}$

But then  $P \equiv \phi$  by (F2), so evidently  $\{v : \exists u (Pu \& Ru,v)\} \equiv \phi$ . By E.3,  $a = 0$ . Similar reasoning shows that  $b = 0$ . Thus  $a = b$ .

Now assume  $Nn \& Nm \& \sigma_{n,m} \& \neg m = 0 \& \phi$ . And suppose  $*(m,y,a) \& *(m,y,b)$ .

By 4)  $*(n,y,c) \& +(c,y,a)$  and  $*(n,y,d) \& +(d,y,b)$ , for some c,d. By the inductive hypothesis,  $c = d$ . By F.2 (Uniqueness for Addition),  $a = b$ .

6) Assume  $(x*y) = 0$ . Then

$Nx \& Ny$

and for some P,R

$1 R \& Mx,P \& \forall u(Pu \Rightarrow My, \{v : Ru,v\}) \& M0, \{v : \exists u (Pu \& Ru,v)\}$ .

By (F2)  $\{v : \exists u (Pu \& Ru,v)\} \equiv \phi$ . Suppose neither x nor y is zero. Then  $\neg P \equiv \phi$  and  $\neg R \equiv \phi$ . But then  $\neg \{v : \exists u (Pu \& Ru,v)\} \equiv \phi$ , a contradiction.

7a) Assume  $Nn \& \text{one}(1)$ . By *POTINF* E.12, there exists P,Q s.t.  $M1,P$  and  $Mn,Q$ . By E.19,  $P \equiv \{a\}$ . Using predicative comprehension, set R to  $\{x,y : x = a \& Qy\}$ . Clearly  $1 R$  and  $\forall u(Pu \Rightarrow Mn, \{v : Ru,v\})$ . Also,  $\{v : \exists u (Pu \& Ru,v)\} \equiv Q$ , so by E.6  $Mn, \{v : \exists u (Pu \& Ru,v)\}$ . Hence  $(1*n) = n$ .

7b) Assume  $\text{one}(1) \& (x*y) = 1$ . By 6) and E.21,  $\neg x = 0$  and  $\neg y = 0$ . Also,  $Nx \& Ny$  and for some P,R

$1 R \& Mx,P \& \forall u(Pu \Rightarrow My, \{v : Ru,v\}) \& M1, \{v : \exists u (Pu \& Ru,v)\}$ .

By E.19,

(\*)  $\{v : \exists u (Pu \& Ru,v)\} \equiv \{b\}$  for some b.

Then,  $Pa \& Ra,b$  for some a. Suppose  $Pc$  for some c where  $\neg c = a$ . Then  $\neg \{v : Rc,v\} \equiv \phi$  by E.3. But then  $Rc,d$  for some d, and  $\neg d = b$  since  $1 R$ . This contradicts (\*). So  $P \equiv \{a\}$ , and by E.19 and (F1),  $x = 1$ . If  $\neg y = 1$ , then  $\{v : Ra,v\}$  for at least one other thing other than b, by (E19) and (F1), say e. But this again contradicts (\*). So  $y = 1$  as well.

8a) Assume  $Nn \& Nx \& Ny \& ((x+y)*n) = a$ . Then

$N(x+y) \& Nn \& Na$  and for some C,R

$1 R \& M(x+y),P \& \forall u(Pu \Rightarrow Mn, \{v : Ru,v\}) \& Ma, \{v : \exists u (Pu \& Ru,v)\}$

So  $Nx \& Ny$  and for some X,Y

$(X \cap Y) \equiv \phi \& Mx,X \& My,Y \& M(x+y), (X \cup Y)$

By E.5  $P \sim (X \cup Y)$ . Evidently, there are  $X'$  and  $Y'$  s.t.  $X' \sim X$ ,  $Y' \sim Y$ ,  $(X' \cap Y') \equiv \phi$ , and  $(X' \cup Y') \equiv P$ . By E.5 again,  $Mx,X'$ .  $\forall u(X'u \Rightarrow Mn, \{v : Ru,v\})$  since  $X' \subseteq P$ . Evidently,

$\{v : \exists u (X'u \& Ru,v)\} \subseteq \{v : \exists u (Pu \& Ru,v)\}$ , so by E.17,  $\exists b, \{v : \exists u (X'u \& Ru,v)\}$  for some  $b$  s.t.  $Nb$ . Thus  $(x^*n) = b$ . Similarly,  $(y^*n) = c$  for some  $c$  s.t.  $Nc \& Mc, \{v : \exists u (Y'u \& Ru,v)\}$ . Evidently,

$$\begin{aligned} & \{v : \exists u (X'u \& Ru,v)\} \cap \{v : \exists u (Y'u \& Ru,v)\} \equiv \phi \text{ and} \\ & \{v : \exists u (X'u \& Ru,v)\} \cup \{v : \exists u (Y'u \& Ru,v)\} \\ & \quad \equiv \{v : \exists u (Pu \& Ru,v)\}. \end{aligned}$$

Thus  $((x^*n) + (y^*n)) = a = ((x+y)^*n)$ .

8b) Proceed by induction (F4\*), with  $\phi$  as

$$\forall x \forall y \forall a (Nx \& Ny \& (n^*(x+y)) = a \Rightarrow ((n^*x) + (n^*y)) = a)$$

Case  $n = 0$ . Assume  $N0 \& Nx \& Ny \& (0^*(x+y)) = a$ . By 1)  $a = 0$  and  $(0^*x) = (0^*y) = 0$ . By F.3.2a,  $(0+0) = 0$ . Hence  $((0^*x) + (0^*y)) = a$ .

Induction step. Assume  $Nn \& Nm \& \sigma n,m \& \neg m = 0 \& \phi$ . And suppose  $Nx \& Ny \& (m^*(x+y)) = a$ . By 3),  $(n^*(x+y)) = b \& (b+(x+y)) = a$  for some  $b$ . So

$$\begin{aligned} a &= (b+(x+y)) \\ &= ((n^*(x+y))+(x+y)) \\ &= (((n^*x) + (n^*y))+(x+y)) && \text{by the Induction Hypothesis} \\ &= (((n^*x) + x) + ((n^*y) + y)) && \text{by Additive Commutativity and} \\ & && \text{Associativity} \\ &= ((m^*x) + (m^*y)) && \text{by 2)} \end{aligned}$$

8c) Proceed by induction (F4\*), with  $\phi$  as

$$\begin{aligned} & \forall x \forall y \forall a (Nx \& Ny \& ((n^*x) + (n^*y)) = a \& \neg n = 0 \\ & \quad \Rightarrow (n^*(x+y)) = a) \end{aligned}$$

Case  $n = 0$ . Trivial.

Induction step. Assume  $Nn \& Nm \& \sigma n,m \& \neg m = 0 \& \phi$ . And suppose  $Nx \& Ny \& ((m^*x) + (m^*y)) = a \& \neg m = 0$ . By 3),  $(m^*x) = ((n^*x)+x)$  and  $(m^*y) = ((n^*y)+y)$ .

Suppose  $n = 0$ . Then one(m). By 7a),  $(m^*x) = x$  and  $(m^*y) = y$ . So  $(x+y) = a$ , and  $(m^*(x+y)) = (m^*a) = a$ , again by 7a).

Otherwise,  $\neg n = 0$ . Then

$$\begin{aligned} & ((m^*x) + (m^*y)) \\ &= ( ((n^*x)+x) + ((n^*y)+y) ) \\ &= ( ((n^*x)+(n^*y)) + (x+y) ) \end{aligned}$$

by Associativity and Commutativity of Addition

$$\begin{aligned} &= ( (n^*(x+y)) + (x+y) ) && \text{by the Induction Hypothesis} \\ &= (m^*(x+y)) && \text{by 2)} \end{aligned}$$

9) Proceed by induction (F4\*), with  $\phi$  as

$$\forall x \forall z \forall a ( ((n^*x) + n) = a \& \sigma x,z \Rightarrow (n^*z) = a )$$

Assume  $((0^*x) + 0) = a$ . By 1) and F.3.2a,  $a = 0$ . But  $(0^*z) = 0$  by 1) again.

Now assume  $Nn \& Nm \& \sigma n,m \& \neg m = 0 \& \phi$ . And suppose  $((m^*x) + m) = a \& \sigma x,z$ . By 3),  $(m^*x) = ((n^*x) + x)$ , hence  $((n^*x) + x) + m = a$ . By E.22, one(1) for some 1. By F.3.10,  $(x+1) = z$  and  $(n+1) = m$ . So  $((n^*x) + x) + (n+1) = a$ . By Associativity and Commutativity of Addition,  $((n^*x) + n) + (x+1) = a$ , hence  $((n^*x) + n) + z = a$ . By the induction hypothesis,  $((n^*x) + n) = (n^*z)$ , so  $((n^*z) + z) = a$ . By 2),  $(m^*z) = a$ .

10) Proceed by induction (F4\*), with  $\phi$  as

$$\forall y \forall z ( (n^*y) = z \Rightarrow (y^*n) = z )$$

Assume  $(0^*y) = z$ . Then  $(y^*0) = 0 = z$  by 1) and 4).

Now assume  $Nn \ \& \ Nm \ \& \ \sigma_{n,m} \ \& \ \neg m = 0 \ \& \ \phi$ . And suppose  $(m^*y) = z$ . Then by 3),  $((n^*y) + y) = z$ . By the induction hypothesis,  $(n^*y) = (y^*n)$ , so  $z = ((y^*n) + y)$ . By 9)  $(y^*m) = z$ .

11a) Proceed by induction (F4\*), with  $\phi$  as

$$\forall y \forall z \forall a ( ((n^*y)^*z) = a \ \& \ \neg n = 0 \Rightarrow (n^*(y^*z)) = a )$$

Case  $n = 0$ . Trivial.

Induction step. Assume  $Nn \ \& \ Nm \ \& \ \sigma_{n,m} \ \& \ \neg m = 0 \ \& \ \phi$ . And suppose  $((m^*y)^*z) = a \ \& \ \neg m = 0$ .

Suppose  $n = 0$ . Then one(m) by E.18, and so by 7a),  $(m^*y) = y$

$$a = ((m^*y)^*z) = (y^*z).$$

But then by 7a) again,  $(m^*(y^*z)) = (y^*z) = a$ .

Now suppose  $\neg n = 0$ . By 3)  $(m^*y) = ((n^*y) + y)$ . By 8a),

$$(((n^*y) + y)^*z) = (((n^*y)^*z) + (y^*z))$$

By the Induction Hypothesis,

$$((n^*y)^*z) = (n^*(y^*z)).$$

So

$$\begin{aligned} (m^*(y^*z)) &= ((n^*(y^*z)) + (y^*z)) \\ &= (m^*(y^*z)) \quad \text{by 2)}. \end{aligned}$$

11b) Assume  $((0^*y)^*z) = a \ \& \ (y^*z) = x$ . By two applications of 1),  $a = 0$ . By another,  $(0^*(y^*z)) = 0$ .

11c) Assume  $(x^*(y^*z)) = a \ \& \ \neg z = 0$ . Then

$$\begin{aligned} a &= ((y^*z)^*x) && \text{by 10)} \\ &= ((z^*y)^*x) && \text{by 10)} \\ &= (z^*(y^*x)) && \text{by 11a)} \\ &= ((y^*x)^*z) && \text{by 10)} \\ &= ((x^*y)^*z) && \text{by 10)} \end{aligned}$$

11d) Proof like that of 11c).

12) Proceed by induction (F4\*), with  $\phi$  as

$$\forall x \forall z ( (n^*x) = (z^*x) \ \& \ \neg x = 0 \Rightarrow n = z )$$

Case  $n = 0$ . Assume  $(0^*x) = (z^*x) \ \& \ \neg x = 0$ . Then  $(0^*x) = 0$  by 1). So by 6)  $z = 0$ .

Induction step. Assume  $Nn \ \& \ Nm \ \& \ \sigma_{n,m} \ \& \ \neg m = 0 \ \& \ \phi$ . And suppose

$(m^*x) = (z^*x) \ \& \ \neg x = 0$ . By 3),  $(m^*x) = ((n^*x) + x)$ . If  $z = 0$ , then  $(z^*x) = 0$  and so  $(m^*x) = 0$  using 1), contradicting 6). Hence  $\neg z = 0$ . By E.4,  $\sigma z',z$  for some  $z'$  s.t.  $Nz'$ . By 3),  $(z^*x) = ((z'^*x) + x)$ . Thus

$$((n^*x) + x) = ((z'^*x) + x).$$

By Cancellation for Addition F.3.4,

$$(n^*x) = (z'^*x).$$

By the Induction Hypothesis,  $n = z'$ . By E.24,  $m = z$ .

13) Suppose  $(x^*z) = x \ \& \ \neg x = 0$ . Then  $N1 \ \& \ \sigma_{0,1}$  for some 1. By 7a)  $(x^*1) = x$ . By 12)  $z = 1$ .

14a) Assume  $x \leq y$  &  $(y^*z) = a$ . So  
 $(y^*z) = ((x+x')^*z)$  for some  $x'$  by F.3.5  
 $= ((x^*z)+(x'^*z))$  by 8a)  
Hence by F.3.5 again,  $(y^*z) \geq (x^*z)$ .

14b) Apply 14a), Commutativity of Multiplication, and Transitivity of  $\leq$ .

15) Assume  $(x^*z) \leq (y^*z)$  &  $\neg z = 0$ . Then  $Nx$  &  $Ny$ , so by E.23b,  $x \leq y \vee y < x$ . Suppose  $\neg x \leq y$ . Then  $y < x$ . So  $y \leq x$ . By 14),  $(y^*z) \leq (x^*z)$ . By F.4,  $(x^*z) = (y^*z)$ . By 12)  $x = y$ , a contradiction.

### G.3 Prop. Division Algorithm.

1) Existence.

$\forall y \forall z ( Ny \& Nz \& \neg z = 0 \Rightarrow \exists q \exists r ( y = ((q^*z)+r) \& r < z ) )$

2) Uniqueness.

$\forall y \forall z \forall q \forall r \forall q' \forall r' ( \neg z = 0 \& y = ((q^*z)+r) \& r < z \& y = ((q'^*z)+r') \& r' < z \Rightarrow q = q' \& r = r' )$

*Pf:*

1) Assume  $Ny$  &  $Nz$  &  $\neg z = 0$ . Use the Well-Ordering Principle, with  $\phi(x)$  as the formula  $\exists q y = ((q^*z)+x)$

Note first that  $\exists x ( Nx \& (\phi(x)) )$ , since  $x = ((0^*z)+x)$  by G.2.1 and F.3.2a. By F.5.3,  $( Nw \& (\phi(w)) \& \forall y ( y < w \Rightarrow \neg (\phi(y)) ) )$

for some  $w$ . Hence

$$y = ((q^*z)+w)$$

for some  $q$ .

Suppose  $\neg w < z$ . Of course,  $Nw$ , so by E.23b,  $z \leq w$ . By F.3.5,  $(z+c) = w$  for some  $c$ . By F.3.5 again,  $c \leq w$ . Because  $\neg z = 0$ , by F.3.2b,  $c < w$ . Note that one(1) for some 1 by E.22.

So

$$\begin{aligned} y &= ((q^*z) + (z+c)) \\ &= (((q^*z)+z) + c) && \text{by Associativity of Addition F.3.3b} \\ &= (((q^*z) + (1^*z)) + c) && \text{by G.2.7a} \\ &= (((q+1)^*z) + c) && \text{by G.2.8c} \end{aligned}$$

But this contradicts  $\forall y ( y < w \Rightarrow \neg (\phi(y)) )$ . Therefore  $w < z$ .

2) Assume  $\neg z = 0$  &  $y = ((q^*z)+r) \& r < z$  &  $y = ((q'^*z)+r') \& r' < z$ .

Suppose  $\neg q = q'$ . WLOG by E.23b, suppose  $q < q'$ . Then  $(q+x) = q'$  by F.3.5, where  $\neg x = 0$  by F.3.2a. Then

$$\begin{aligned} y &= (((q+x)^*z)+r') \\ &= (((q^*z) + (x^*z)) + r') && \text{by G.2.8a} \\ &= ((q^*z) + ((x^*z) + r')) && \text{by Associativity of Addition F.3.3a} \end{aligned}$$

By Cancellation F.3.4,  $((x^*z)+r') = r$ . But one(1) for some 1 and  $1 \leq x$  by E.22, so

$$\begin{aligned} z &= (1^*z) && \text{by G.2.7a} \\ &\leq (x^*z) && \text{by G.2.14a} \\ &\leq ((x^*z) + r') && \text{since } 0 \leq r', \text{ by F.3.2a, F.3.7, and Transitivity of } \leq \\ &\leq r \end{aligned}$$

But recall  $r < z$ , so this contradicts Anti-Symmetry F.4. Thus  $q = q'$ . By Cancellation F.3.4,  $r =$

r'.

## H. Division

H.1 *Def.*  $x \mid y$  abbreviates  $\exists z (x^*z) = y$ .

H.2 *Prop.*

- 1)  $\forall x (Nx \Rightarrow x \mid 0)$
- 2)  $\forall x (0 \mid x \Rightarrow x = 0)$
- 3)  $\forall x (Nx \Rightarrow x \mid x)$
- 4)  $\forall x \forall 1 (Nx \& \text{one}(1) \Rightarrow 1 \mid x)$
- 5)  $\forall x \forall y (x \mid y \& \neg y = 0 \Rightarrow x \leq y)$
- 6)  $\forall x \forall y (x \mid y \& y \mid x \Rightarrow x = y)$
- 7)  $\forall x \forall y \forall z (x \mid y \& y \mid z \Rightarrow x \mid z)$
- 8)  $\forall x \forall y \forall z \forall a \forall b \forall c (x \mid y \& x \mid z \& ((a^*y) + (b^*z)) = c \Rightarrow x \mid c)$
- 9)  $\forall x \forall y \forall z \forall a \forall b \forall c (x \mid y \& x \mid z \& ((b^*z) + c) = (a^*y) \Rightarrow x \mid c)$

*Pf:*

3) Suppose  $Nx$ . If  $x = 0$ , then follows from 1). Otherwise, suppose  $\neg x = 0$ . By E.22, there exists 1 s.t.  $\text{one}(1)$ . By G.2.7a,  $(x^*1) = x$ .

7) Assume  $x \mid y \& y \mid z$ . Then  $(x^*a) = y$  and  $(y^*b) = z$  for some  $a, b$ . So  $z = ((x^*a)^*b)$ . If  $x = 0$ , then  $z = 0$  by two applications of G.2.1. But then  $x \mid z$  by 1). On the other hand, if  $\neg x = 0$ , then  $z = (x^*(a^*b))$  by G.2.11a. Hence  $x \mid z$ .

9) Assume  $x \mid y \& x \mid z \& ((b^*z) + c) = (a^*y)$ . If  $y = 0$ , then  $c = 0$  by F.3.2c. So the result follows by 1). And if  $z = 0$ , then  $c = (a^*y)$  by G.2.4 and F.3.2a. So assume  $\neg y = 0$  and  $\neg z = 0$ . Now  $(x^*u) = y$  and  $(x^*v) = z$  for some  $u, v$ . By G.2.4,  $\neg u = 0 \& \neg v = 0$ .

Substituting,

$$((b^*(x^*v)) + c) = (a^*(x^*u))$$

Applying Commutativity and Associativity of Multiplication,

$$((x^*(b^*v)) + c) = (x^*(a^*u)).$$

$(b^*v) \leq (a^*u)$ , so by F.3.5,  $((b^*v) + w) = (a^*u)$ . Substitute, distribute, cancel, to get  $c = (x^*w)$ .

H.3 *Prop. Existence and Uniqueness of a Greatest Common Divisor.* Let  $Nx \& Ny \& (\neg x = 0 \vee \neg y = 0)$ . Then, for some  $z$ ,

$$z \mid x \& z \mid y \& \forall c (c \mid x \& c \mid y \Rightarrow c \leq z).$$

If  $z' \mid x \& z' \mid y \& \forall c (c \mid x \& c \mid y \Rightarrow c \leq z')$ , then  $z' = z$ .

*Pf:*

Suppose  $x = 0$ . Then  $\neg y = 0$ . Then  $y \mid x$  by H.2.1 and  $y \mid y$  by H.2.3. If  $c \mid x \& c \mid y$ , then  $c \leq y$  by H.2.5. Similar reasoning succeeds in the case  $y = 0$ .

Now suppose  $\neg x = 0 \& \neg y = 0$ . Set  $\psi(v)$  to  $v \mid x \& v \mid y$ . Then by H.2.5,  $\forall v (\psi(v) \Rightarrow v \leq x)$ . By E.22  $\text{one}(1)$  for some 1. So by H.2.4,  $\psi(1)$ . By F.6, there exists  $z$  s.t.  $\psi(z) \& \forall c (\psi(c) \Rightarrow c \leq z)$ .

Finally, suppose  $z' \mid x \& z' \mid y \& \forall c (c \mid x \& c \mid y \Rightarrow c \leq z')$ . Then both  $z \leq z'$  and  $z' \leq z$ .

So by F.4,  $z' = z$ .

H.4 *Def.* Suppose  $Nx \ \& \ Ny \ \& \ (\neg x = 0 \vee \neg y = 0)$ . Use  $(x \ \Delta \ y)$  to refer to that unique  $z$  guaranteed by the previous proposition.

H.5 *Prop.*

$$1) \ \forall x \forall y \ ( \ Nx \ \& \ Ny \ \& \ (\neg x = 0 \vee \neg y = 0) \Rightarrow (x \ \Delta \ y) = (y \ \Delta \ x) )$$

**Note:** As usual, only one form of commutative permutations will be asserted, and the rest will be assumed.

$$2) \ \forall x \forall y \ ( \ Nx \ \& \ Ny \ \& \ (\neg x = 0 \vee \neg y = 0) \Rightarrow (x \ \Delta \ y) \mid x )$$

$$3) \ \forall x \forall y \ ( \ Nx \ \& \ Ny \ \& \ (\neg x = 0 \vee \neg y = 0) \Rightarrow (x \ \Delta \ y) \leq x )$$

$$4) \ \forall x \forall y \ ( \neg x = 0 \ \& \ x \mid y \Rightarrow (x \ \Delta \ y) = x )$$

$$5) \ \forall x \forall y \forall z \forall a \forall b \ ( \ (\neg x = 0 \vee \neg y = 0) \ \& \ ((a^*x) + (b^*y)) = z \\ \Rightarrow (x \ \Delta \ y) \mid z )$$

$$6) \ \forall x \forall y \forall z \forall a \forall b \ ( \ (\neg x = 0 \vee \neg y = 0) \ \& \ ((a^*x) + z) = (b^*y) \\ \Rightarrow (x \ \Delta \ y) \mid z )$$

$$7) \ \forall q \forall r \forall a \forall b \ ( \ \neg b = 0 \ \& \ a = ((q^*b) + r) \Rightarrow (a \ \Delta \ b) = (b \ \Delta \ r) )$$

$$8) \ \forall x \ ( \ Nx \Rightarrow (x \ \Delta \ 0) = x )$$

$$9) \ \forall x \forall 1 \ ( \ Nx \ \& \ \text{one}(1) \Rightarrow (x \ \Delta \ 1) = 1 )$$

$$10) \ \forall x \forall y \forall k \ ( \ k \mid x \ \& \ k \mid y \ \& \ (\neg x = 0 \vee \neg y = 0) \Rightarrow k \mid (x \ \Delta \ y) )$$

$$11) \ \forall x \forall y \forall a \forall b \forall 1 \ ( \ (a^*(x \ \Delta \ y)) = x \ \& \ (b^*(x \ \Delta \ y)) = y \ \& \ \text{one}(1) \Rightarrow (a \ \Delta \ b) = 1 )$$

*Pf:*

5) Assume  $(\neg x = 0 \vee \neg y = 0) \ \& \ ((a^*x) + (b^*y)) = z$ . Then  $(x \ \Delta \ y) \mid x$  and  $(x \ \Delta \ y) \mid y$  by 2). The result follows from H.2.8.

7) Assume  $\neg b = 0 \ \& \ a = ((q^*b) + r)$ . Then by E.22,  $\text{one}(1)$  for some 1. So  $a = ((q^*b) + (1^*r))$  by G.2.7a. Then  $(b \ \Delta \ r) \mid a$  by 5). By 2),  $(b \ \Delta \ r) \mid b$ . Now suppose  $y \mid a \ \& \ y \mid b$ . Again,  $(1^*a) = ((q^*b) + r)$ . By H.2.9,  $y \mid r$ . Thus,  $y \leq (b \ \Delta \ r)$ . Hence  $(b \ \Delta \ r) = (a \ \Delta \ b)$ .

10) Suppose not, and by F.5.3 suppose  $x$  is the smallest number s.t.

$$k \mid x \ \& \ k \mid y \ \& \ (\neg x = 0 \vee \neg y = 0) \ \& \ \neg k \mid (x \ \Delta \ y).$$

Then  $x \leq y$ . If  $x = 0$ , then  $\neg y = 0$ , and  $(x \ \Delta \ y) = y$  by 8), a contradiction. So suppose  $\neg x = 0$ . Then  $y = ((q^*x) + r) \ \& \ r < x$  for some  $q, r$ , by the Division Algorithm G.3.1. By E.22  $\text{one}(1)$  for some 1, and  $(1^*y) = y$  by G.2.7a. By H.2.9,  $k \mid r$ . By assumption of the leastness of  $x$ ,  $k \mid (x \ \Delta \ r)$ . By 7),  $k \mid (x \ \Delta \ y)$ .

## I. Other Numbers

I.1 *Defs.*

two( $w$ ) abbreviates  $\exists u \ ( \ \text{one}(u) \ \& \ Nw \ \& \ \sigma u, w )$ .

three( $t$ ) abbreviates  $\exists w \ ( \ \text{two}(w) \ \& \ Nt \ \& \ \sigma w, t )$ .

four( $f$ ) abbreviates  $\exists t \ ( \ \text{three}(t) \ \& \ Nf \ \& \ \sigma t, f )$ .

and so forth. As before, we introduce special variables 2, 3, and 4, which will serve as arguments of two, three, and four, respectively.

Remark that of course it cannot be shown that there exists 2 s.t.  $\text{two}(2)$ . On the other hand, if

such a 2 does exist, then it has all the “downward” properties of two, including that it is preceded by a finite number one (which must exist). Similar remarks hold for three(3) and four(4). Specifically, if four(4) for some 4, then there are numbers 1, 2, and 3 s.t. one(1), two(2), and three(3).

I.2 *Prop.* Suppose two(2). Then  $M_{2,P}$  if and only if  $\exists a \exists b (\neg a = b \ \& \ P \equiv \{a,b\})$ .

I.3 *Prop.* Suppose  $P \equiv \{a,b\}$  for some  $a,b$  with  $\neg a = b$ , and suppose  $N_2$ . Then two(2) if and only if  $M_{2,P}$ .

I.4 *Prop.* Let one(1) & two(2). Then  $\neg 2 = 0 \ \& \ \neg 2 = 1$ . Indeed,  $1 < 2$ .

I.5 *Prop.* Suppose one(1) & two(2) &  $x < 2$ . Then  $x = 0 \vee x = 1$ .

I.6 *Prop.* Suppose  $N_n \ \& \ \neg n = 0 \ \& \ \neg n = 1$ . Then  $\exists 2$  two(2) and  $2 \leq n$ .

Similar propositions can be stated for three(3) and four(4) and larger numbers. These will be referenced using the Propositions for two(2).

## J. Intervals and Sequences

Recall from *Systems of Foundations of Arithmetic* that

J.1 *Prop.*  $\forall n ( N_n \Rightarrow \exists P \forall z ( 0 \leq z \ \& \ z \leq n \Leftrightarrow Pz ) )$

Indeed:

J.2 *Prop.*  $\forall k \forall n ( N_k \ \& \ N_n \Rightarrow \exists P \forall z ( k \leq z \ \& \ z \leq n \Leftrightarrow Pz ) )$

J.3 *Def.* Use  $[k \_ n]$  to represent--obviously unique up to equivalence--any  $P$  s.t.  $\forall z ( k \leq z \ \& \ z \leq n \Leftrightarrow Pz )$ , where  $N_n$ .

Use  $(k \_ n]$  to represent

$\{x : \neg x = k \ \& \ [0 \_ n]x\}$

and  $(k \_ n)$  to represent

$\{x : \neg x = k \ \& \ \neg x = n \ \& \ [k \_ n]x\}$

Evidently,  $(k \_ n]i$  if and only if  $k < i \ \& \ i \leq n$ .

Note that if  $(0 \_ n]$  is non-empty, then there exists a non-zero natural number. Hence one(1) for some 1, and indeed 1 is the smallest element of  $(0 \_ n]$ .

J.4 *Prop.* Suppose  $i \leq j \ \& \ k \leq n$  and  $N_j$ . Then  $(j \_ k] \subseteq (i \_ n]$ .

J.5 *Def.* Let  $N_n$ , and suppose  $f R \ \& \ (R^D) \equiv (0 \_ n]$ . Call  $R$  a *sequence of length n*, and write  $\text{Seq}(R,n)$  or simply  $\text{Seq}(R)$  if  $n$  is not important. When  $\text{Seq}(R,n)$  and  $(R^D)_i$ , write  $(R^i)$  to represent that unique  $y$  such that  $R_i, y$ .

Note that the empty relationship is a sequence of length 0, and that if R is any non-empty sequence, then it has length n, for some n s.t.  $Nn \ \& \ \neg n = 0$ .

J.6 Prop. Suppose  $\text{Seq}(R,n) \ \& \ k \leq n$ . Then  $\text{Seq}(R \upharpoonright (0 \_ k],k)$ .

*Pf:*

By J.4,  $(0 \_ k] \subseteq (0 \_ n]$ . Evidently,  $R \upharpoonright (0 \_ k]$  is a function since R is.

J.7 Prop. Suppose one(1) and that x exists. Then there exists R s.t.  $\text{Seq}(R,1)$  and  $(R'1) = x$ .

*Pf:*

By Predicative Comprehension,  $\{(1,x)\}$  exists.

Use  $\langle x \rangle$  to represent a sequence of length 1, where  $\langle x \rangle'1 = x$ .

J.8 Prop. Suppose  $\text{Seq}(R,k)$  and  $\text{Seq}(S,n)$ , and that  $(k+n)$  exists. Then there exists T such that:

- 1)  $\text{Seq}(T,(k+n))$
- 2)  $\forall i ( (0 \_ k]i \Rightarrow (T'i) = (R'i) )$
- 3)  $\forall i ( (0 \_ n]i \Rightarrow (T'(k+i)) = (S'i) )$

*Pf:*

By induction on n. When  $n = 0$ , S is just the empty relationship, and one may use R for T.

Now assume true for n, that  $Nn \ \& \ \sigma n,m$  and that  $(k+m)$  exists. Also suppose  $\text{Seq}(R,k)$  and  $\text{Seq}(S,m)$ . Set U to  $S \upharpoonright (0 \_ n]$ . By J.6  $\text{Seq}(U,n)$ . By the induction hypothesis, there exists T which satisfies 1), 2) and 3) (with of course U in place of S in the third condition). Set T' to  $T \cup \{((k+m),Um)\}$ , which exists by Predicative Comprehension.

Hence if four(4), and a,b,c,d exist, then there exists R s.t.  $\text{Seq}(R,4)$  and  $(R'1) = a$ ,  $(R'2) = b$ ,  $(R'3) = c$ , and  $(R'4) = d$ , where one(1), two(2), and three (3).

## K. The Euclidean Algorithm

K.1 Lemma. Suppose  $0 < b \ \& \ b \leq a \ \& \ a \leq n$ , and suppose three(3). Then there exist Q,R,c such that:

- $$\begin{aligned} & (c+2) \leq a \ \& \ \text{Seq}(Q,c) \ \& \ \text{Seq}(R,(c+2)) \\ & \ \& \ (R'1) = a \ \& \ (R'2) = b \ \& \ (R'(c+1)) = (a \ \Delta \ b) \ \& \ (R'(c+2)) = 0 \\ & \ \& \ \forall i ( (0 \_ c]i \Rightarrow (R'i) = (((Q'i)*(R'(i+1)))) + (R'(i+2))) \\ & \ \& \ (R'(i+2)) < (R'(i+1)) \end{aligned}$$

where one(1) and two(2).

*Pf:*

Since three(3), we have that two(2) and one(1) for some 1 and 2, by I.1.

Now proceed by induction ( $F4^*$ ) on n. Trivial when  $n = 0$ , since this leads to a contradiction. Suppose true for n, and assume  $Nn \ \& \ Nm \ \& \ \sigma n,m \ \& \ \neg m = 0$ . Suppose  $0 < b \ \& \ b \leq a \ \& \ a \leq m$ .

If  $a \leq n$ , then use the Induction Hypothesis to conclude the result. Otherwise,  $a = m$ .

By the Division Algorithm G.3.1,  $a = ((q*b)+r) \ \& \ r < b$  for some q,r.

If  $r = 0$ , then  $c = 1$ ,  $(R'1) = a$ ,  $(R'2) = b$ ,  $(R'(c+1)) = (R'2) = b = (a \ \Delta \ b)$  (the last equality

by H.5.4), and  $(R'3) = 0$ . Otherwise, suppose  $\neg r = 0$ .

If  $b = m$ , then by the uniqueness of the Division Algorithm G.3.2,  $q = 1$  and  $r = 0$ , a contradiction. So  $b < m$ , and thus  $b \leq n$ .

Hence  $0 < r$  &  $r \leq b$  &  $b \leq n$ . So by the Induction Hypothesis, there exist  $Q, R, c$  such that

$$\begin{aligned} & (c+2) \leq b \text{ \& Seq(Q,c) \& Seq(R,(c+2))} \\ & \text{\& (R'1) = b \& (R'2) = r \& (R'(c+1)) = (b \Delta r) \& (R'(c+2)) = 0} \\ & \text{\& } \forall i ( (0 \_ c]i \Rightarrow (R'i) = (((Q'i)*(R'(i+1)))) + (R'(i+2))) \\ & \text{\& (R'(i+2)) < (R'(i+1)) ).} \end{aligned}$$

By J.7 there exists  $A$  and  $B$  s.t.  $\text{Seq}(A,1)$ ,  $\text{Seq}(B,1)$ ,  $(A'1) = a$ , and  $(B'1) = q$ . Remark that  $(c+2) \leq b$  and  $b < m$ , so  $(c+3)$  exists and indeed  $((c+1)+2) \leq a$ . Hence by J.8 there exists  $C$  and  $D$  s.t.

$$\begin{aligned} & \text{Seq}(C,((c+1)+2)), \\ & \text{Seq}(D,(c+1)), \\ & (C'1) = (A'1) = a, \\ & (D'1) = (B'1) = q, \\ & \forall i ( (0 \_ (c+2)]i \Rightarrow (C'(i+1)) = (R'i) ), \text{ and} \\ & \forall i ( (0 \_ c]i \Rightarrow (D'(i+1)) = (Q'i) ). \end{aligned}$$

It is straightforward to verify that  $C, D$ , and  $(c+1)$  prove the result.

**K.2 Prop. The Euclidean Algorithm (Existence).** Suppose  $0 < a$ ,  $0 < b$ , and three(3).

Then there exist  $Q, R, c$  such that:

$$\begin{aligned} & \text{Seq(Q,c) \& Seq(R,(c+2))} \\ & \text{\& (R'1) = a \& (R'2) = b \& (R'(c+1)) = (a \Delta b) \& (R'(c+2)) = 0} \\ & \text{\& } \forall i ( (0 \_ c]i \Rightarrow (R'i) = (((Q'i)*(R'(i+1)))) + (R'(i+2))) \\ & \text{\& (R'(i+2)) < (R'(i+1)) )} \end{aligned}$$

where one(1) and two(2).

*Pf.*

Assume  $b > a$ . Then  $a = (0*b) + a$ , where  $a < b$ . Then  $0 < a$  &  $a \leq b$  &  $a \leq a$ . The result follows from the lemma, since  $(a \Delta b) = (b \Delta a)$ .

Otherwise, by E.23b,  $b \leq a$ . Then  $0 < b$  &  $b \leq a$  &  $b \leq b$ . Apply now the lemma K.1.

## L. Prime Numbers

L.1 *Def.*  $\pi(x)$  ("x is prime") abbreviates

$$\text{Nx \& } \neg x = 0 \text{ \& } \neg \text{one}(x) \text{ \& } \forall y \forall 1 ( y | x \Rightarrow \text{one}(y) \vee y = x ).$$

**Note:** " $\neg x = 0$ " is added since otherwise 0 would be prime if only zero and one exist.

L.2 *Prop.*  $\forall x \forall n ( \pi(x) \text{ \& } n | x \Rightarrow \text{one}(n) \vee n = x )$

*Pf.*

Assume  $\pi(x)$  &  $n | x$ . Then  $\text{Nx}$  &  $\neg \text{one}(x)$  &  $\neg x = 0$ . Then by E.22 one(1) for some 1. By the definition of  $\pi$ ,  $n = 1 \vee n = x$ .

L.3 *Prop.*  $\forall 2 ( \text{two}(2) \Rightarrow \pi(2) )$

*Pf.* Assume two(2). By I.4,  $\neg 2 = 0$  and  $\neg \text{one}(2)$ . Suppose  $y | 2$  &  $\text{one}(1)$ . Then by H.2.5,

$y \leq 2$ . By I.5  $y = 0 \vee y = 1 \vee y = 2$ . But  $y = 0$  contradicts L.1.

L.4 Prop.

- 1)  $\forall x \forall 2 (\pi(x) \& \text{two}(2) \Rightarrow 2 \leq x)$
- 2)  $\forall x (Nx \& \neg x = 0 \& \neg \text{one}(x) \Rightarrow \exists y (\pi(y) \& y \mid x))$
- 3)  $\forall x \forall y \forall 1 (\pi(x) \& Ny \& \text{one}(1) \Rightarrow (x \Delta y) = 1 \vee (x \Delta y) = x)$
- 4)  $\forall x \forall y (\pi(x) \& x \mid (x \Delta y) \Rightarrow x \mid y)$

*Pf.*

- 1) By L1  $\neg x = 0 \& \neg \text{one}(x)$ . By I.6  $2 \leq x$ .
- 2) WLOG suppose  $x$  is the least number s.t.  $Nx \& \neg x = 0 \& \neg \text{one}(x)$  but  $\neg \exists y (\pi(y) \& y \mid x)$ .  $x \mid x$  by H.2.3, so  $\neg \pi(x)$ . Then for some  $z, 1$ , we have that  $z \mid x \& \text{one}(1)$  but  $\neg z = 1$  and  $\neg z = x$ . By H.2.2,  $\neg z = 0$ . By H.2.5,  $z \leq x$ , so  $z < x$ . By assumption of the leastness of  $x$ ,  $\pi(y) \& y \mid z$ , for some  $y$ . But by H.2.7,  $y \mid x$ , a contradiction.
- 3) Assume  $\pi(x) \& Ny \& \text{one}(1)$ . Because  $\pi(x)$ ,  $\neg x = 0$ . So by H.5.2,  $(x \Delta y) \mid x$ . Hence  $(x \Delta y) = 1$  or  $(x \Delta y) = x$ .
- 4) By 3),  $(x \Delta y) = 1 \vee (x \Delta y) = x$ . The former produces a contradiction, since it forces  $x \leq 1$ . The latter implies that  $x = (x \Delta y) \mid y$ .

## M. Exponentiation

M.1 Prop. Suppose  $\text{one}(1)$  and that

$$\begin{aligned} & Nx \& Nn \& Ny \& \neg x = 0 \& \\ & ((n = 0 \& y = 1) \vee \\ & \exists R (Rn, y \& \text{Seq}(R, n) \& (R'1) = x \\ & \& \forall i ((1 \_ n)^i \Rightarrow (R'(i+1)) = ((R'(i))^*x))) \end{aligned}$$

and

$$\begin{aligned} & Nx \& Nn \& Nz \& \neg x = 0 \& \\ & ((n = 0 \& z = 1) \vee \\ & \exists R (Rn, z \& \text{Seq}(R, n) \& (R'1) = x \\ & \& \forall i ((1 \_ n)^i \Rightarrow (R'(i+1)) = ((R'(i))^*x))) \end{aligned}$$

Then  $y = z$ .

*Pf.*

By induction on  $n$ . When  $n = 0$ ,  $y = 1$  and  $z = 1$ . Now assume true for  $n = 0$ , and let  $Nm \& \sigma n, m \& \neg m = 0$ . Suppose  $Rm, y \& Sm, z$ . Then

$$\begin{aligned} & Rm, y \& \text{Seq}(R, m) \& (R'1) = x \\ & \& \forall i ((1 \_ m)^i \Rightarrow (R'(i+1)) = ((R'(i))^*x)) \end{aligned}$$

and

$$\begin{aligned} & Sm, z \& \text{Seq}(S, m) \& (S'1) = x \\ & \& \forall i ((1 \_ m)^i \Rightarrow (S'(i+1)) = ((S'(i))^*x)) \end{aligned}$$

for some  $R, S$ . Set  $A$  to  $R \uparrow (0 \_ n]$  and  $B$  to  $S \uparrow (0 \_ n]$ . Then by the Induction Hypothesis,  $(R'n) = (S'n)$ . But then

$$(R'm) = ((R'n)^*x) = ((S'n)^*x) = (S'm).$$

M.2 Def. Suppose  $\text{one}(1)$ . Use  $(x \wedge n)$  to refer to that unique (by M.1)  $y$  (if it exists) such that:

$$Nx \& Nn \& Ny \& \neg x = 0 \&$$

$$\begin{aligned} & ((n = 0 \ \& \ y = 1) \vee \\ & \exists R ( Rn, y \ \& \ \text{Seq}(R, n) \ \& \ (R'1) = x \\ & \ \& \ \forall i ( (1 \_ n)i \Rightarrow (R'(i+1)) = ((R'(i))^*x) ) ) \end{aligned}$$

M.3 Prop.

- 1)  $\forall x \forall 1 ( Nx \ \& \ \neg x = 0 \ \& \ \text{one}(1) \Rightarrow (x \wedge 0) = 1 )$
- 2)  $\forall x \forall 1 ( Nx \ \& \ \neg x = 0 \ \& \ \text{one}(1) \Rightarrow (x \wedge 1) = x )$
- 3)
  - a)  $\forall x \forall y \forall n \forall 1 ( \text{one}(1) \ \& \ (x \wedge (n+1)) = y \Rightarrow (x \wedge (n+1)) = ((x \wedge n) * x) )$
  - b)  $\forall x \forall y \forall z \forall n \forall 1 ( \text{one}(1) \ \& \ ((x \wedge n) * x) = y \ \& \ (\neg x = 1 \vee (n+1) = z) \Rightarrow (x \wedge (n+1)) = ((x \wedge n) * x) )$
- 4)
  - a)  $\forall x \forall y \forall z \forall n ( ((x*y) \wedge n) = z \Rightarrow ((x \wedge n) * (y \wedge n)) = z )$
  - b)  $\forall x \forall y \forall z \forall z' \forall n ( ((x \wedge n) * (y \wedge n)) = z \ \& \ (x*y) = z' \Rightarrow ((x*y) \wedge n) = z )$
- 5)  $\forall x \forall y \forall n ( \neg x = 0 \ \& \ x \leq a \ \& \ y \leq b \ \& \ (a \wedge b) = c \Rightarrow (x \wedge y) \leq c )$
- 6)  $\forall x \forall y \forall n ( \neg \text{one}(x) \ \& \ (x \wedge n) = y \Rightarrow n \leq y )$
- 7)  $\forall x \forall a \forall b \forall c \forall n \forall m ( \neg x = 0 \ \& \ \neg \text{one}(x) \ \& \ (x \wedge n) = a \ \& \ (x \wedge m) = b \ \& \ (a*b) = c \Rightarrow (x \wedge (n+m)) = c )$

**Note:** The condition that  $\neg \text{one}(x)$  is necessary, since we may have that  $(1 \wedge 1) = 1$ , but not that two(2) for any 2, so evidently  $(1 \wedge (1+1))$  does not exist and *a fortiori* does not equal 1.

*Pf.*

2) Assume  $Nx \ \& \ \neg x = 0 \ \& \ \text{one}(1)$ . By J.7 there exists R such that  $\text{Seq}(R, 1) \ \& \ (R'1) = x$ . Remark that  $(1 \_ n)$  is empty, so

$$\forall i ( (1 \_ n)i \Rightarrow (R'(i+1)) = ((R'(i))^*x) )$$

holds vacuously. Hence  $(x \wedge 1) = x$ .

5) Assume  $\neg x = 0 \ \& \ \neg a = 0 \ \& \ x \leq a \ \& \ y \leq b \ \& \ (a \wedge b) = c$ . An induction and G.2.14b shows that  $(x \wedge b) \leq c$ . Another induction show that  $(x \wedge a) \leq (x \wedge b)$ .

7) Assume  $\neg x = 0 \ \& \ \neg \text{one}(x) \ \& \ (x \wedge n) = a \ \& \ (x \wedge m) = b \ \& \ (a*b) = c$ . By 6),  $n \leq a$  and  $m \leq b$ . If  $n = 0$ , then evidently  $0 \leq y$ . Otherwise,  $\neg n = 0$ , and  $a \geq x \geq 2$  and  $b \geq x \geq 2$ , where two(2), existing by I.6. It is easy to show that  $(a+b) \leq (a*b)$ , hence  $(n+m)$  exists by F.3.7. By an induction on n and using 3), the result follows.

M.4 Prop. Prime Factorization: Existence.

Suppose  $Nn \ \& \ \neg n = 0 \ \& \ \neg n = 1$ , where  $\text{one}(1)$ . Then  $\exists v \exists R \exists S \exists T$  s.t.  $Nv \ \& \ \neg v = 0$  and

$$\begin{aligned} & v \leq n, \\ & \text{Seq}(R, v), \\ & \text{Seq}(S, v), \\ & \text{Seq}(T, v), \\ & \forall i ( (0 \_ v)i \Rightarrow \pi((R'i)) ), \\ & \forall i ( (0 \_ v)i \Rightarrow ((R'(i+1)) > (R'i)) ), \\ & \forall i ( (0 \_ v)i \Rightarrow S'i > 0 ), \\ & (T'1) = ((R'1) \wedge (S'1)), \text{ and} \\ & \forall i ( (1 \_ v)i \Rightarrow (T'(i+1)) = ((T'i) * ((R'(i+1) \wedge (S'(i+1)))) ) ). \end{aligned}$$

**Note:** Write the product as  $(p_1 \wedge s_1)(p_2 \wedge s_2) \dots (p_v \wedge s_v)$ . Remark that we will use the same notation even when some  $s_i = 0$ , representing that the factor  $(p_i \wedge s_i)$  is 1 and can be eliminated. Evidently, if all the exponents are 0, then the product represents 1.

*Pf.*

By I.6, two(2) for some 2, with  $2 \leq n$ .

The proposition is trivially true for  $n = 0$ . By F.5.2, WLOG we may suppose it is true for all  $k < n$ .

By L.4.2 there exists a prime  $p$  s.t.  $p \mid n$ . WLOG by F.5.2 again we may suppose  $p$  is the least such prime. Of course,  $\neg p = 0$  and  $\neg p = 1$ . So if  $(p \wedge i) \mid n$ , then  $i \leq n$  by M.3.6. By F.6 there is a greatest element  $j$  of  $[0 \_ n]$  s.t.  $(p \wedge j) \mid n$ . So  $((p \wedge j) * n') = n$  for some  $n'$ . If  $n' = 1$ , then we are done. O.w. suppose  $\neg n' = 1$ . By the induction hypothesis,  $n'$  has a prime factorization, with length  $\leq n'$ . If  $q < p$  is s.t.  $q \mid n'$ , then  $q \mid n$ , a contradiction. On the other hand, suppose  $p \mid n'$ . Then  $(n'' * p) = n'$  for some  $n''$ . Hence  $((p \wedge j) * p) \mid n$ . By M.3.3b,  $(p \wedge (j+1)) \mid n$ , contradicting the maximality of  $j$ .

## N. Uniqueness of Prime Factorization

Our proof that prime factorization is unique is a little more involved than the normal. There is perhaps an easier way.

N.1 *Prop.* Assume  $k \mid (x^*y)$ ,  $\text{one}(k \Delta y)$ , and that  $(k^*x)$  exists. Then  $k \mid x$ .

**Note:** It will be shown later that the condition that  $(k^*x)$  exist can be eliminated.

*Pf.*

Suppose  $(x^*y) = 0$ . If  $\neg y = 0$ , then  $x = 0$  by G.2.6, so  $k \mid x$  by H.2.1. Otherwise, assume  $y = 0$ . Then  $\text{one}(k \Delta y)$  implies  $k = 1$ , where  $\text{one}(1)$ , by H.5.8. So by H.2.4,  $k \mid x$ .

Otherwise, assume  $\neg (x^*y) = 0$ . And suppose  $(x^*y) = 1$ , where  $\text{one}(1)$ . Then  $k = 1$  by G.2.7b. So  $k \mid x$  by H.2.4.

Otherwise, assume  $\neg (x^*y) = 1$ . And suppose  $(x^*y) = 2$ , where two(2). Then  $k \mid 2$  implies  $k = 1$  or  $k = 2$ , as well as  $y = 1$  or  $y = 2$ , by L.3. If  $k = 1$ , then  $k \mid x$  by H.2.4. And if  $k = 2$ , then  $\text{one}(k \Delta y)$  implies that  $y = 1$ , so  $x = 2$ , by G.2.13. Hence  $k \mid x$  by H.2.3.

Thus we may suppose that  $(x^*y)$  is not 0, 1, or 2. Hence by I.6, three(3) for some 3.

If  $k = 0$ , then  $(x^*y) = 0$  by H.2.2, a contradiction. So assume  $\neg k = 0$ , i.e.  $0 < k$ . By G.2.4,  $\neg y = 0$ , i.e.  $0 < y$ . Hence, by the Euclidean Algorithm K.2, there exist  $Q, R, c$  such that:

$$\begin{aligned} & \text{Seq}(Q, c) \ \& \ \text{Seq}(R, (c+2)) \\ & \& \ (R^1) = k \ \& \ (R^2) = y \ \& \ (R^i(c+1)) = (k \Delta y) \ \& \ (R^i(c+2)) = 0 \\ & \& \ \forall i \ (0 \_ c]i \Rightarrow (R^i) = (((Q^i)^*(R^{i+1}))) + (R^{i+2})) \\ & \qquad \qquad \qquad \& \ (R^{i+2}) < (R^{i+1}) \end{aligned}$$

In particular,  $(R^1) = (((Q^1)^*(R^2)) + (R^3))$ , that is

$$k = (q^*y) + r,$$

where  $q = (Q^1)$  and  $r = (R^3)$ . By assumption,  $(x^*k)$  exists, so

$$(x^*k) = (x^*(q^*y)) + (x^*r).$$

Hence,

$$\begin{aligned} k \mid (x^*(R^1)) &= (x^*k), \\ k \mid (x^*(R^2)) &= (x^*(q^*y)) = (q^*(x^*y)), \end{aligned}$$

and by H.2.9,

$$k \mid (x^*(R^3)).$$

An easy induction shows that  $k \mid (x^*(R^i))$  for all  $i$  s.t.  $(0 \_ (c+1)]i$ , so in particular  $k \mid (x^*(R^{c+1}))$ . But  $(R^{c+1}) = (k \Delta y) = 1$ , so  $k \mid x$ .

N.2 *Prop.* Assume  $\pi(p)$  &  $p \mid (x^*y)$ . And suppose that either  $(p^*x)$  or  $(p^*y)$  exists. Then  $p \mid x$  or  $p \mid y$ .

*Pf.*

Suppose  $(p^*x)$  exists. By L.4.3,  $(p \Delta y) = 1 \vee (p \Delta y) = p$ , where  $\text{one}(1)$ . If  $(p \Delta y) = p$ , then by L.4.4,  $p \mid y$ , and we are done. Otherwise, suppose  $(p \Delta y) = 1$ . By N.1,  $p \mid x$ .

We now improve on the previous proposition, by dropping the condition that either  $(p^*x)$  or  $(p^*y)$  exists.

N.3 *Prop.* Assume  $\pi(p)$  &  $p \mid (x^*y)$ . Then  $p \mid x$  or  $p \mid y$ .

*Pf.*

Suppose not. If  $x = 0$ , then  $p \mid x$  by H.2.1.

Otherwise, assume  $\neg x = 0$ . If  $p \leq x$ , then  $(p^*y) \leq (x^*y)$  by G.2.14a, i.e.  $(p^*y)$  exists. Then by N.2, the result follows.

So assume  $p > x$ . By the Division Algorithm,

$$p = (q^*x) + r \text{ \& } r < x$$

for some  $q, r$ . By H.5.7,  $(p \Delta x) = (x \Delta r)$ . If  $\neg (p \Delta x) = 1$ , where  $\text{one}(1)$  (which exists because  $p$  exists), then  $(p \Delta x) = p$  by L.4.3. So  $p \mid x$ .

So assume  $(p \Delta x) = 1$ . Hence  $(x \Delta r) = 1$ . Now  $p \mid (x^*y)$ , so  $(p^*a) = (x^*y)$  for some  $a$ . Thus

$$(p^*a) = ((q^*x)^*a) + (r^*a).$$

Of course  $x \mid (x^*y) = (p^*a)$ , so  $x \mid (r^*a)$  by H.2.9. Now  $(p^*a)$  exists and  $x \leq p$ , so  $(x^*a)$  exists. By N.1,  $x \mid a$ . So  $(x^*v) = a$  for some  $v$ . So

$$(p^*(x^*v)) = (p^*a) = (x^*y).$$

If  $v = 0$ , then  $a = 0$ , and  $(x^*y) = 0$ ; so  $x = 0$  or  $y = 0$ , so  $p \mid x$  or  $p \mid y$ . By Commutativity, Associativity, and Cancellation,  $(p^*v) = y$ , thus  $p \mid y$ .

N.4 *Prop.* Let  $\pi(n)$  &  $\neg n = 0$  and  $\neg \text{one}(n)$ . Then  $n$  has a unique prime factorization.

*Pf.*

Standard proof using N.3.

N.5. *Prop.* (Euclid's Lemma) Assume  $k \mid (x^*y)$  and  $\text{one}(k \Delta y)$ . Then  $k \mid x$ .

*Pf.*

The cases  $(x^*y) = 0$  and  $(x^*y) = 1$ , where  $\text{one}(1)$ , are easy to handle. Otherwise, write  $(x^*y)$  in its unique prime factorization. By uniqueness, this gives a prime factorization of  $x$ ,  $y$ , and of  $k$  with the same primes, although perhaps with 0 exponents. None of the primes which appear in the factorization of  $y$  and of  $k$  can both have non-zero exponents, since  $\text{one}(k \Delta y)$ . Thus the non-zero exponents of  $k$  for a particular prime must be less than or equal to the exponents of  $x$  for the same prime. Hence  $k \mid x$ .

## O. The Godel Auto-Consistency of F

In this section it will be established that **F** can prove its own consistency, when this is expressed using the standard technique of Godelization - that is, when wffs are represented as products of prime numbers to some power.

Our proof will rely crucially on the fact that **F** has the following model:

- 0 satisfies N,
- (0,0) does not satisfy  $\sigma$ ,
- (0,P) satisfies M if and only if  $P \equiv \phi$

I.e. it has a model with only one lower-case element. In this model, for any given arity, there are then only two sorts of upper-case elements, those which are empty, and those which are satisfied by the unique element of that arity. For instance, for the arity 3, there is the empty relationship and the relationship  $\{(0,0,0)\}$ .

A little more formally, let  $s,t$  be lower-case terms,  $R$  an upper-case variable, and fix an interpretation  $\mathcal{I}$ . Because there is no choice as to where to map the lower-case variables,  $\mathcal{I}$  may be considered a mapping from the upper-case variables to either empty or non-empty. The following are then true-in- $\{0\}$  under  $\mathcal{I}$ :

$Rt$   
 $Rs,t$   
 $s = t$   
 $Nt$

$Mt,P$  if and only if  $P^{\mathcal{I}}$  is empty  
 $\forall x \phi$  if and only if  $\phi$  is true-in- $\{0\}$  under  $\mathcal{I}$   
 $\phi \vee \psi$  if and only if either  $\phi$  or  $\psi$  is true-in- $\{0\}$  under  $\mathcal{I}$   
 $\neg \phi$  if and only if  $\phi$  is not true-in- $\{0\}$  under  $\mathcal{I}$

$\sigma s,t$  is *not* true-in- $\{0\}$  under  $\mathcal{I}$ .

Finally, for any interpretation  $\mathcal{I}$  and any predicate letter  $R$ , let  $\mathcal{I}(R)$  be the same interpretation as  $\mathcal{I}$ , except that it differs in the assignment of  $R$ , i.e. if  $\mathcal{I}$  assigns  $R$  the empty property or relationship, then  $\mathcal{I}(R)$  assigns it the non-empty property or relationship. Then:

$\forall R \phi$  is true-in- $\{0\}$  under  $\mathcal{I}$  if and only if  $\phi$  is both true-in- $\{0\}$  under  $\mathcal{I}$  and true-in- $\{0\}$  under  $\mathcal{I}(R)$ .

Now, to see that it is possible to Godelize **F**, or indeed any recursively axiomatizable system, within **F**, it is really only necessary to note that Godelization is a “downwards” process since **F** is second-order. For instance, Godelization defines a number  $n$  to be a wff essentially by recourse to a sequence representing the formation of the wff from its sub-wffs. In first-order logic this sequence is represented by the coding of a much larger number than  $n$ , and so the process is “upwards”. In second-order logic, however, the sequence can be represented by an upper-case letter, and so the process stays “downwards”.

Because of unique prime factorization, we may let  
 $(a \alpha b \alpha c \dots)$  refer (if it exists) to the number  $(2 \wedge a)(3 \wedge b)(5 \wedge c) \dots$

We suppose that characters of the language (variables, constants, logical constants, and

parentheses) have been assigned Godel numbers in some fashion. Use  $g(c)$  to be the Godel number of character  $c$ . An expression i.e. a concatenation of characters  $c_1c_2 \dots c_n$  (which of course could be a wff) receives the Godel number  $(g(c_1) \alpha g(c_2) \alpha \dots \alpha g(c_n))$ .

Define (in the standard way) predicates

$AtomicWff_g(w)$ , so that  $w$  is the Godel number of an atomic wff;

$Or_g(e_1, e_2, e_3)$ , so that  $e_3$  is the Godel number of an expression which is the disjunction of expressions with Godel numbers  $e_2$  and  $e_3$ ;

$Neg_g(e_1, e_2)$ , so that  $e_2$  is the Godel number of an expression which is the negation of the expression with Godel number  $e_1$ ;

$Gen1_g(v, e_1, e_2)$ , so that  $e_2$  is the Godel number of an expression which is the first-order generalization of the expression with Godel number  $e_1$ , using the lower-case variable which has Godel number  $v$ ; and

$Gen2_g(v, e_1, e_2)$ , so that  $e_2$  is the Godel number of an expression which is the second-order generalization of the expression with Godel number  $e_1$ , using the upper-case variable which has Godel number  $v$ .

$Wff_g(w)$ , that is  $w$  is the Godel number of a wff, can then be defined as:

$$\begin{aligned} \exists R \exists n ( \text{Seq}(R, n) \ \& \ (R'n) = w \ \& \\ \forall k ( k \leq n \Rightarrow AtomicWff_g((R'k)) \vee \\ \exists i \exists j \exists v ( i < k \ \& \ j < k \ \& \\ ( Or_g((R'i), (R'j), (R'k)) \vee Neg_g((R'i), (R'k)) \\ \vee Gen1_g(v, (R'i), (R'k)) \vee Gen2_g(v, (R'i), (R'k)) ) ) ) ) \end{aligned}$$

$GProve_g, \mathbf{F}(w)$ , that is  $w$  is provable in  $\mathbf{F}$ , may be defined similarly: when there exists  $R, n$  s.t.  $\text{Seq}(R, n) \ \& \ (R'n) = w$  and every element in the sequence is either an axiom or inferred from previous elements according to the rules of deduction.

The assertion of consistency is simply  $\neg GProve_g, \mathbf{F}(f)$ , where  $f$  is defined to be the Godel number of “ $! 0 = 0$ ”. Abbreviate this assertion as  $GCon_g, \mathbf{F}$ .

Now work in  $\mathbf{F}$  and assume that  $\mathbf{F}$  is inconsistent, i.e.  $\neg GCon_g, \mathbf{F}$ , i.e.  $GProve_g, \mathbf{F}(f)$ . Evidently  $f$  is larger than 1. Thus it may be inferred that at least 0 and 1 exist.

Let  $w$  be the Godel number of any wff appearing in the sequence of the proof of  $f$ .

Evidently, we can define the predicates

$\kappa(w, k)$ , where  $k$  equals the number of relationship symbols, counting separately the same symbol if it is used within different scopes, appearing in the wff represented by  $w$

$\lambda(w, k)$ , where  $k$  equals the number of logical connectives in the wff represented by  $w$

Evidently  $(2 \wedge ((\kappa'w) + (\lambda'w) + 1)) < w$ , so it exists (provided  $w$  does). WLOG we will suppose that the same relationship symbol does not appear in more than one scope; this will make the proof slightly easier to describe. So  $(\kappa'w)$  = the number of relationship symbols

appearing in the wff represented by  $w$ .

As already stated there is only one way to interpret a lower-case symbol, and each relationship symbol can be interpreted in one of two ways. So for the wff  $w$ , there are  $(2 \wedge (\kappa'w))$  possible interpretations. Use  $[1 \_ (2 \wedge (\kappa'w))]$  to represent each of these possible interpretations, using some kind of ordering, such as lexicographic. Call these numbers *assignments*. It is evidently possible to define predicates

$DiffAssign(w,n,m,i)$ , to represent  $n$  is an assignment for the relationships symbols in the wff  $w$ , which maps all the relationship symbols but the  $i$ -th in the same way as assignment  $m$ , and assigns the  $i$ -th to a different one (i.e. empty if  $m$  assigns it to the non-empty, and *vice versa*).

$VarNumb(w,v,i)$ , to represent  $v$  is the  $i$ -th upper-case relationship symbol in  $w$

Let  $s$  be an atomic wff of a wff  $w$ . Then  $s$  is satisfied by an assignment  $t$  of  $w$  if it is of the form

- 1)  $Nx$  ( $x$  a variable or 0)
- 2)  $Mn,P$ , and  $t$  maps  $P$  to 0 ( $n$  a variable or 0)
- 3)  $x = y$  ( $x,y$  a variable or 0)
- 4)  $Rx,\dots,y$ , where  $a$  maps the  $i$ -th relationship (which  $R$  is) to 1 ( $R$  a variable,  $x,\dots,y$  variables or 0).

Use  $AtomSat(w,s,t)$  to abbreviate this predicate.

Now extend this definition of satisfaction to wffs in general, using *true* to abbreviate 1 and *false* to abbreviate 0, in order to make the definition more perspicacious.

Let  $Sat(w,t)$  be

$$\begin{aligned} & \exists R \exists V \exists A \exists n ( Seq(R,n) \ \& \ (R'n) = w \ \& \ (V'n) = true \ \& \ (A'n) = t \ \& \\ & \ \& \ \forall k ( k \leq n \Rightarrow (V'k) = true \vee (V'k) = false ) \ \& \\ & \ \& \ \forall k ( k \leq n \Rightarrow \\ & \ ( AtomicWff((R'k)) \ \& \ ((V'k) = true \Leftrightarrow AtomSat(w,(R'k),(A'k))) \\ & \ \vee \ \exists i \exists j \exists v ( i < k \ \& \ j < k \ \& \\ & \ \ ( ( Or((R'i),(R'j),(R'k)) \\ & \ \ \ \& \ ((V'k) = true \Leftrightarrow (V'i) = true \vee (V'j) = true) \\ & \ \ \ \& \ (A'k) = (A'i) \ \& \ (A'k) = (A'j) ) \\ & \ \vee \ ( Neg((R'i),(R'k)) \ \& \ (V'k) = true - (V'i) \\ & \ \ \ \& \ (A'k) = (A'i) ) \\ & \ \vee \ ( Gen1(v,(R'i),(R'k)) \ \& \ (V'k) = (V'i) \ \& \ (A'k) = (A'i) ) \\ & \ \vee \ ( Gen2(v,(R'i),(R'k)) \ \& \ (V'k) = ((V'i) * (V'j)) \\ & \ \ \ \& \ (A'k) = (A'i) \ \& \\ & \ \ \ \ \& \ \exists c ( DiffAssign(w,(A'k),(A'j),c) \\ & \ \ \ \ \ \& \ VarNumb(w,v,c) ) ) ) ) ) ). \end{aligned}$$

In order to understand this proposition, first consider the tree representing the break-down of a wff into its subwffs. That is, the root is the wff itself. If a node is of the form  $\phi \vee \psi$ , then it has two children, one  $\phi$  and the other  $\psi$ . If a node is of the form  $\neg \phi$ , then it has a single child, being  $\phi$ . If a node is of the form  $\forall R \phi$ , then it has a single child, being  $\phi$ . And so forth. The leaves (the nodes without children) are the atomic subwffs of the wff.

Now modify this tree structure in the following way. Attach assignments to each node, to join

the subwff. If a node is of the form  $(\phi \vee \psi, \mathcal{Q})$  then the modified tree has two children, one  $(\phi, \mathcal{Q})$  and the other  $(\psi, \mathcal{Q})$ . If a node is of the form  $(\neg \phi, \mathcal{Q})$ , then it has a single child, being  $(\phi, \mathcal{Q})$ . And so forth. The only real change is when a node is of the form  $(\forall R \phi, \mathcal{Q})$ , which instead of having one child, now has two,  $(\phi, \mathcal{Q})$  and  $(\phi, \mathcal{Q}(R))$ , where  $\mathcal{Q}(R)$  is the same assignment as  $\mathcal{Q}$ , except that it differs in the assignment of R, i.e. if  $\mathcal{Q}$  assigns R the empty property or relationship, then  $\mathcal{Q}(R)$  assigns it the non-empty property or relationship, and *vice versa*. Again, the leaves are the atomic subwffs of the wff, with some associated assignment.

*Sat*'s definition mirrors the tree we have just described. It is important that the n after the existential quantifier in the definition - which is equivalent to the number of vertices of the tree - will be  $\leq (2^{(\kappa \cdot w)} + (\lambda \cdot w) + 1) < w$ . If n is smaller, then R,V,A,n exist so long as w is indeed satisfied by the assignment t.

A wff w is *true* if it is satisfied by all its assignments. That axioms are true and rules of inference go from truths to truths is straightforward to check. But " $! 0 = 0$ " would be evaluated as non-true, which contradicts the assumption of inconsistency.

In summary, the inconsistency of **F** is contradictory in **F**. Thus **F** proves  $GCon_{\mathbf{F}}$  and so **F** is Godel auto-consistent.

The same technique works for **F** to prove the consistency of **F + F5** and **F + F6**. Indeed **F + F5** has the same model as **F** which was mentioned above, and **F + F6** also has a model with a singleton domain  $\{0\}$ , where

0 does *not* satisfy N,  
 (0,0) does not satisfy  $\sigma$ ,  
 (0,P) satisfies M if and only if  $P \equiv \phi$

Remark that nothing changes with the addition of full (impredicative) comprehension to **F**, **F + F5**, and **F + F6**, since they all would retain a model of one element. That is **F** (with only predicative comprehension) can prove the consistency of these extensions with *full* comprehension. Note that **F + F6** with full comprehension is in fact a very strong theory, and in particular once a natural number exists, becomes **Z2** (because **F + F5 + F6 + {full comprehension}** is just **Z2**).

Finally, remark that the reasoning can also be formulated in **Z1**, first-order Peano Arithmetic. So **Z1** also proves the Godel consistency of **F**, **F + F5**, and **F + F6**.

## P. Further Proofs

Abbreviate

$\exists x_1 \dots \exists x_{n-1} (N0 \ \& \ \sigma_{0,x_1} \ \& \ N_{x_1} \ \& \ \sigma_{x_1,x_2} \ \& \ N_{x_2} \ \& \ \dots \ \& \ \sigma_{x_{n-1},x_n} \ \& \ N_{x_n})$

by  $(\sigma^n) = x_n$  or just **F6.n**. Note that  $(\sigma^0) = x_0$  will be held to abbreviate "**N0**". **F6.n** asserts the existence of the natural number n (as well as all numbers less than it), and so the

sequence **F6.0**, **F6.1**, ... is a better and better approximation of **F + F5 + F6**, which is full second-order arithmetic. By Godel's Second Incompleteness Theorem **F** will of course not be able to prove that **F + F5 + F6** is consistent.

Set **F<sub>n,k</sub>** to be the system **F + {F6.n} + {full comprehension}**, where *k* is a maximum arity allowed for relationship symbols. We will show that **F** proves the consistency of **F<sub>n,k</sub>**, for any *n* and *k*, under some system of Godel numbering.

Let  $N = (2 \wedge ((n + 1) \wedge k))$ , which is the number of *k*-arity relationships in a domain of  $(n+1)$  things. Letting *u* be the maximum number of relationship symbols and logical constants in the wff of any purported proof, it can be verified that, in order for the proof of the previous section to go through, it suffices that  $((N \wedge u) - N)/(N - 1)$  exist.

Now a standard Godel numbering method will not, of course, ensure that this number does exist. But clearly there exists *some*, especially gluttonous Godel numbering which implies the existence of this number, e.g. one based on the Ackermann function. A sentence **S** asserting consistency, formulated with this Godel numbering, can then be proven in **F**.

### Q. Intensional Correctness, or What **F** has *not* Proved

Return now to the question of the intensional correctness of  $GCon_{g,F}$ . What  $GCon_{g,F}$  *really* says, is that there does not exist a number representing, under a Godel numbering *g*, a proof which ends in a contradiction. This is apparently not, alas, the same thing as consistency itself. Indeed, it would seem conceivable that there is a proof of a contradiction, but that there are just no numbers as big as  $2^n$  to represent the proof. One can see this especially in the case of the proof that **F + F6.n** proves its own consistency; there is a need, not just for any Godel numbering, but a Godel coding with especially large numbers. The existence of the coding, and the reflection of assertions about syntax in terms of numbers, is itself a supposition. That is,  $\neg GCon_{g,F}$  asserts *more* than **F**'s inconsistency, since it also asserts the existence of certain numbers. So  $GCon_{g,F}$  asserts *less* than **F**'s consistency. That **F** has proved  $GCon_{g,F}$  is, then, all well and good, but unfortunately **F** hasn't really proved its own consistency. It's proved something like it, but still something less.

### R. Intensionally Correct Provability and So Consistency Formulas

Nonetheless, we should not doubt the fundamental theme of our argument. To prove the consistency of a system, it is sufficient to work by contradiction, in supposing that it is inconsistent. And the inconsistency of a system, implies the existence of an object, indeed not just any old object, but a proof object, which is highly complex and itself implies the existence of other objects. Only one must be careful about not entangling the ontological implications of the proof object with those from the Godel coding.

So first, let us produce a formula which can be held to *really* assert a system's consistency. The surest and most direct way is to produce a system which *really* talks about the syntactical elements necessary for deductions - terms, wffs, proofs, and so on.

That route will not be taken here, because our primary interest is in arithmetic, and so in an

arithmetical system capable of proving its own consistency. What we will do, is produce an arithmetical formula which asserts the consistency of a system, using a bare minimum of Godelization.

Now it would seem that a proof is a particular type of sequence, a sequence of symbols which satisfies certain rules. For instance, the (very basic) proof

0 = 0  
 $\exists x x = x$

is a sequence of 9 symbols: 0, =, 0, ,,  $\exists$ , x, x, =, x, where the symbol “;” serves to separate the two distinct lines in the proof.

Clearly one of the basic rules of a proof sequence is that it be of the form

$$a_{1,1}, a_{1,2}, \dots, a_{1,n_1}, ;, a_{2,1}, a_{2,2}, \dots, a_{2,n_2}, ;, \dots, a_{k,1}, a_{k,2}, \dots, a_{k,n_k}$$

where each of the  $a_{i1}, a_{i2}, \dots, a_{in_i}$  are themselves sequences following rules fixing what it is to be a wff. Another rule would be that the sequence wffs either be axioms, examples of axiom schemes, or follow from previous sequence wffs using the appropriate rules of logical inferences. And so forth.

The reader may recall that Godel numbering interceded in Section O. when wffs were coded by numbers. Proofs were there represented by sequences of wffs. That has now changed, and both wffs and proofs are now sequences of symbols. True, a minimal Godel coding is still necessary, since numbers must be used to represent the symbols of the language. And one cannot downplay this coding, because one could be wastrel and choose, for instance, to map the i-th predicate variable symbol to some large number, e.g.  $2^i$ , whereby the proof in Section O. could then go through. To be fair - and for the result to be independent of the particular Godel numbering methodology used - one needs to insist that the representation of symbols not be wasteful, or that there only should be a finite number of symbols to begin with. For instance, to implement this last idea, one might insist that in one's language predicate variable symbols are a unique symbol followed by a distinguishing number of another symbol (so one would have, e.g. R%% and R%%%% as predicate variable symbols). In any case there seem to be ways where the issue of coding the symbols of the language does not damage the intensional correctness of the assertions produced.

In brief, given a deductive system **X**, one can define in **F** a predicate *Proof X*, where *Proof X*(R,S) if and only if both S is a sequence of symbols which is a wff in **X**, and R is a sequence of symbols which is a proof in **X** of that wff. For instance, if R is the sequence

$$a_{1,1}, a_{1,2}, \dots, a_{1,n_1}, ;, a_{2,1}, a_{2,2}, \dots, a_{2,n_2}, ;, \dots, a_{k,1}, a_{k,2}, \dots, a_{k,n_k}$$

then one condition of *Proof X* would be that S is the sequence  $a_{k,1}, a_{k,2}, \dots, a_{k,n_k}$ . (A proof finishes with the wff it is trying to prove.) Consistency is then asserted by the wff

$\neg \text{Proof}_{\mathbf{X}}(R,C)$ , where  $C$  is the sequence of length 4 with  $C'1 = "\neg"$ ,  $C'2 = "0"$ ,  $C'3 = "="$ , and  $C'4 = "0"$ . Abbreviate this wff as  $\text{Con}_{\mathbf{X}}$ , which now *really* asserts the consistency of  $\mathbf{X}$ .

Let  $G\text{Proof}_{g,\mathbf{X}}(R,w)$  be the wff, according to the methodology of Section O., which asserts that  $R$  is a proof of the wff  $w$ . Then  $\text{Proof}_{\mathbf{X}}$  and  $G\text{Proof}_{g,\mathbf{X}}$  are *not* equivalent in  $\mathbf{F}$ .  $\text{Proof}_{\mathbf{X}}$  only asserts the existence of second-order elements, so of course it cannot imply the existence of first-order numbers, which are required by  $G\text{Proof}_{g,\mathbf{X}}$ . On the other hand, should  $G\text{Proof}_{g,\mathbf{X}}$  hold of some  $R$  and  $w$ , it can be seen that there are sequences  $R^*$  and  $W^*$  representing the same, where  $\text{Proof}_{\mathbf{X}}(R^*,W^*)$ . That is, as we have already suggested,  $G\text{Proof}_{g,\mathbf{X}}$  is a stronger claim than simply asserting something is a proof of a wff; it also carries with it an assertion about the existence of largish numbers. It would seem that  $G\text{Proof}_{g,\mathbf{X}}$  is not intensionally correct, while  $\text{Proof}_{\mathbf{X}}$  is.

Now the same sort of reasoning which was used to prove  $G\text{Con}_{g,\mathbf{F}}$  in  $\mathbf{F}$  could be used to prove  $\text{Con}_{\mathbf{F}}$ . For suppose  $\neg \text{Con}_{\mathbf{F}}$ . There there exists a sequence which is a proof of a contradiction, so there exists a number, namely the length of the proof sequence. The only difficulty is, it does not seem that this number is large enough to ensure the definition of truth in the singleton model. In any case the definition produced in Section O. requires a number which is the order of an exponential. The desired contradiction cannot be reached.

Perhaps there is a way around this difficulty, and perhaps  $\mathbf{F}$  can prove  $\text{Con}_{\mathbf{F}}$ . It would seem, of course, that any proof leading to an inconsistency would have to be very, very long. More than that, what one needs for the proof of  $\text{Con}_{\mathbf{F}}$  to go through in  $\mathbf{F}$  (at least, as the author envisions the proof), is that the proof be very much longer than the number of quantifier blocks of any line in the proof. That looks harder.

If that approach cannot succeed, then there are other systems which *do* prove their real consistency. Two will be presented.

## S. One Arithmetic

Modify  $\mathbf{F}$  by beginning the natural number series at 1, and modify comprehension by insisting that predicates be non-empty, so that one cannot prove that there is an empty predicate. (There *may* be an empty predicate, since such has not been formally excluded. However, its existence is not assured.) Formally, comprehension will be:

For  $n \geq 1$ , for  $\phi$  not containing any free "P," and  $\phi$  containing no quantified upper-case variables.

$$\exists x_1 \dots \exists x_n \phi \Rightarrow \exists P \forall x_1 \dots \forall x_n ( P x_1, \dots, x_n \Leftrightarrow \phi )$$

Second-order logic is changed, to the extent that we do not allow "N" or "σ" to be substituted for universally quantified big-letters. (We will see why, in a moment.)

The arithmetic axioms/scheme are:

(N1)  $\forall n \forall m \forall P ( Nn \& Mn,P \& Mm,P \Rightarrow n = m )$

(N2)  $\forall P ( M1,P \Leftrightarrow \exists x P \equiv \{x\} )$

(N3a)  $\forall n \forall m \forall P \forall Q \forall a ( Nn \& \sigma n,m \& \neg Pa \& \forall x(Qx \Leftrightarrow Px \vee x = a) \& Mn,P \Rightarrow Mm,Q )$

(N3b)  $\forall n \forall m \forall Q ( Nn \& \sigma n,m \& Mm,Q \Rightarrow \exists a (Qa \& Mn,(Q\{a\})) )$

(N4) Induction. Let  $\phi$  be a well-formed formula (with no appearance of  $m$ ). Use  $\phi [x/y]$  to mean  $x$  replaces all (free) instances of  $y$ . Suppose  $\phi [1/n]$  and  $\forall n \forall m ( Nn \& \sigma n,m \& \phi \Rightarrow \phi [m/n] )$ . Then  $\forall n ( Nn \Rightarrow \phi )$

The **N** system, like **F**, has a model of one first-order element, in its case  $\{1\}$ . But while **F** has two second-order elements in its singleton model, **N** may have only one - the non-empty relationship - because of course comprehension has been rigged so that there need be no empty properties or relationships. Such a model with one first-order and one second-order element, has only one interpretation, which assigns all lower-case variables to 1 and all upper-case variables to the non-empty relationship. Truth-in $\{1\}$  can therefore be defined as follows:

$R_t$  is true  
 $R_{s,t}$  is true  
 $s = t$  is true  
 $N_t$  is true  
 $\sigma_{s,t}$  is *not* true  
 $M_{t,P}$  is true  
 $\forall x \phi$  is true if and only if  $\phi$  is true  
 $\forall R \phi$  is true if and only if  $\phi$  is true  
 $\phi \vee \psi$  is true if and only if either  $\phi$  or  $\psi$  is true  
 $\neg \phi$  is true if and only if  $\phi$  is not true

Remark that our restriction on substitution - that  $N$  and especially  $\sigma$  may not be substituted for universally quantified big letters - results from our need that  $\sigma_{s,t}$  not be true. For, by the previous definition,  $\forall R R_{1,1}$  is true, yet  $\sigma_{1,1}$  is not. Thus somehow we must block this inference from being valid in the deductive system, to maintain the claim that inferences always lead from truths to truths. It can be verified that the development of mathematics exhibited in this paper, never uses these substitutions, so they may be excluded without causing any problem.

It can be readily seen that the number of nodes needed to define the notion of truth-in $\{1\}$  is the same as the number of sub-wffs, which can be seen to be less than the length of the wff. Thus, suppose  $\neg Con \mathbf{N}$ . Then there is a proof of the contradiction " $\neg 1 = 1$ ". Every wff in the proof can be seen to be true-in $\{1\}$ , since all axioms are true and all rules of inference infer truths from truths. But " $\neg 1 = 1$ " is not true-in $\{1\}$ , so it cannot be a line in the proof after all. Hence  $Con \mathbf{N}$ .

The only matter left to verify is that indeed this proof can be conducted in **N** and indeed that **N** can build the whole arithmetical mechanism constructed in **F**. We will not bore the reader with

the same level of detail again, but instead restrict the validation to certain highlights.

*Prop.*  $\forall n \forall P (N_n \& M_n, P \Rightarrow \exists x P_x)$ .

*Pf* (in **N**):

By induction, with  $\phi$  as  $\forall P (N_n \& M_n, P \Rightarrow \exists x P_x)$ .

$\forall P (N_1 \& M_1, P \Rightarrow \exists x P_x)$  holds because of (N2).

Now assume  $N_n \& \sigma_{n,m} \& \phi$  and also  $N_m \& M_m, P$ . Then by (N3b) there exists a s.t.  $P_a \& M_n, (P\{a\})$ .

*Prop. Finite Hume's Principle.*  $\forall n \forall P \forall Q (N_n \& M_n, P \Rightarrow (P \sim Q \Leftrightarrow M_n, Q))$ .

*Pf* (in **N**):

By induction, with  $\phi$  as  $\forall P \forall Q (N_n \& M_n, P \Rightarrow (P \sim Q \Leftrightarrow M_n, Q))$ .

Assume first  $N_1 \& M_1, P$ . Then by (N2)  $P \equiv \{p\}$  for some  $p$ . If  $P \sim Q$ , then evidently  $Q \equiv \{q\}$  for some  $q$ , and so by (N2)  $M_1, Q$ . On the other hand, if  $M_1, Q$ , then by (N2)  $Q \equiv \{q\}$  for some  $q$ , and thus  $P \sim Q$ .

Now assume  $N_n \& \sigma_{n,m} \& \phi$  and also  $N_m \& M_m, P$ . Then by (N3b) there exists a s.t.  $P_a \& M_n, (P\{a\})$ . By the previous proposition  $\exists x \neg (P\{a\})_x$ .

Suppose  $P \sim Q$ . Then  $Q_b$  for some  $b$  where  $\exists x \neg (Q\{b\})_x$ . Evidently (this uses the fact that neither are empty),  $P\{a\} \sim Q\{b\}$ . By the induction hypothesis,  $M_n, (Q\{b\})$ . By (N3a)  $M_m, Q$ .

Now suppose  $M_m, Q$ . Then by (N3b) there exists  $b$  s.t.  $Q_b \& M_n, (Q\{b\})$ . By the induction hypothesis,  $(P\{a\}) \sim (Q\{b\})$ , whence  $P \sim Q$ .

*Prop. (Pigeon Hole Principle)* (E.10)  $\forall n \forall P \forall Q (N_n \& M_n, P \& M_n, Q \& P \subseteq Q \Rightarrow P \equiv Q)$

*Pf* (in **N**):

By induction, with  $\phi$  as  $\forall P \forall Q (N_n \& M_n, P \& M_n, Q \& P \subseteq Q \Rightarrow P \equiv Q)$ .

When  $n = 1$ ,  $\phi$  follows from (N2).

Now assume  $N_n \& \sigma_{n,m} \& \phi$  and also  $N_m \& M_m, P \& M_m, Q \& P \subseteq Q$ . By (N3b)  $P_a \& M_n, (P\{a\}) \& Q_b \& M_n, (Q\{b\})$  for some  $a, b$ . Since evidently  $(Q\{a\}) \sim (Q\{b\})$ , by *Finite Hume's Principle*,  $M_n, (Q\{a\})$ . Evidently  $(P\{a\}) \subseteq (Q\{a\})$ , so by the induction hypothesis,  $(P\{a\}) \equiv (Q\{a\})$ . Thus  $P \equiv Q$ .

Perhaps the most important proposition early on which **N** cannot prove, is *POTINF*, namely  $\forall n (N_n \Rightarrow \exists P \exists a (M_n, P \& \neg P_a))$ . *POTINF* is not even true-in- $\{1\}$ . Still, **N** can prove *WEAKPOTINF*, that is,  $\forall n (N_n \Rightarrow \exists P M_n, P)$ . The proof of *WEAKPOTINF* is substantially the same as that in **F** of *POTINF*, which was given in *Systems For a Foundation of Arithmetic*.

It can be checked that most appeals to *POTINF* in **F**'s reconstruction of elementary arithmetic can in fact be replaced by appeals to *WEAKPOTINF*.

Consider, however, one case, proposition E.24, which indeed needs *POTINF* in the case of **F**, but can be proven in the case of **N** with only *WEAKPOTINF*.

*Prop.* (E.24) Suppose  $N_x \& N_y \& \sigma_{x,y} \& \sigma_{x,z}$ . Then  $y = z$ .

*Pf* (in **N**):

By *WEAKPOTINF*  $\forall y, P$  for some  $y$ . By (N3b)  $\exists a, P(a)$  for some  $a$ . By (N3a)  $\exists z, P(z)$ . So by (N1)  $y = z$ .

So it can be seen that **N** has substantially the same power as **F**. In particular, it is able to prove the Euclidean Algorithm and Unique Prime Factorization, and finally write and prove *Con N*.

**N** is *really* auto-consistent. Moreover, it is easy to see that **N** can prove the *real* consistency of the stronger systems,  $\mathbf{N} + \{\text{"N1"}\}$  and  $\mathbf{N} + \{F6\}$ .

## T. Third-Order F

Recall that **F** has a single third-order (constant) predicate "M". Extend its language to a limited third-order language, where there are now variable third-order letters (written in upper-case bold) of arity 1, whose argument is a second-order letter, and of arity 2, whose first argument takes a first-order letter and whose second takes a second-order letter. Add in the appropriate arithmetical comprehension for these third-order letters, as well as using the standard third-order deductive system.

The mathematical axioms remain the same. Call the resulting system **F<sup>3</sup>**. It can be readily seen that **F<sup>3</sup>** has a model of one first-order element (still 0), two second-order elements (again, the empty and the non-empty), and four third-order elements. An interpretation assigns second-order variables to either the empty or non-empty relationship, and third-order variables to one of the four possible third-order elements. The tree needed to define true-in- $\{0\}$  is like that for **F**, except that when a node represents  $\forall X \phi$  and an assignment  $\mathcal{Q}$ , it has four children, representing  $\phi$  and the four assignments which agree with  $\mathcal{Q}$  except possibly for the mapping of **X**.

Now a second-order relationship can be used to represent a node in the truth-defining tree. That is, let  $n$  be the length of the wff. Then all the sub-wffs can be represented by distinct numbers in  $\{1, \dots, n\}$ . To represent a node - which is a 2-tuple, consisting of a sub-wff and an assignment - one may thus use a sequence  $R$ , where  $R_0$  points to the number used to represent the sub-wff and  $(R \setminus \{(0, R_0)\})$  to an assignment which assigns the  $i$ -th predicate letter to either 0 or 1 (if second-order), or 0, 1, 2, or 3 (if third-order). It is therefore possible to talk of a particular tree existing by asserting the existence of a third-order relationship, and so the third-order quantification present in **F<sup>3</sup>** allows the definition of true-in- $\{0\}$ . With this in hand, **F<sup>3</sup>** can prove its own real consistency, as well as the consistency of the usual stronger systems.

## U. Conclusion

This result can undoubtedly be replicated in other systems.

It seems possible that weaker systems might be able to prove the consistency of **F**, **N**, or **F<sup>3</sup>**. Possibilities would be to weaken the Induction axiom or to eliminate uniqueness (F2).

To finish, some remarks about the use of "True" in the title of this paper. More and more, it seems to the author that the *Ad Infinitum* assumption (F6) is the serpent in the garden, and that while (F1) through (F4) and their consequences should be called "true", *Ad*

*Infinitem* is not, or at least is a different (“lesser”?) sort of truth. Since much, if not most, but not all, arithmetic is a consequence of (F1) through (F4), arithmetic would have a dual status, one logical, and the other not. That is, some arithmetic assertions are indeed logical, such as the Euclidean Algorithm and the Commutative Laws of Addition and Multiplication (suitably formulated), while others, such as the Chinese Remainder Theorem, are not. In this way the answer to Frege’s question, “What is the status of arithmetic truths?”, is given, although of course it is not completely as he envisioned.

## BIBLIOGRAPHY

[B1] G. BOOLOS, *Logic, Logic, and Logic* (Cambridge, MA: Harvard University Press, 1998).

[B2] G. BOOLOS and R. JEFFREY, *Computability and Logic 3rd ed.* (Cambridge, UK: Cambridge University Press, 1989).

[B3] A. BOUCHER, *A Foundation of Elementary Arithmetic*,  
[www.andrewboucher.com/papers/foea/index.htm](http://www.andrewboucher.com/papers/foea/index.htm)

[B4] A. BOUCHER, *Systems of Foundations of Arithmetic*,  
[www.andrewboucher.com/papers/foundations.pdf](http://www.andrewboucher.com/papers/foundations.pdf)

[F1] S. FEFERMAN, *Arithmetization of metamathematics in a general setting*,  
*Fundamenta Mathematicae*, vol. 49 (1960), pp. 35-92.

[F2] F. FERREIRA, *A Note on finiteness in the predicative foundations of arithmetic*,  
*Journal of Philosophical Logic*, vol. 28 (1999), pp. 165-174.

[F3] F. FERREIRA, *Amending Frege’s Grundgesetze der Arithmetik*, to appear.

[F4] G. FREGE. *The Foundations of Arithmetic*, 2nd. ed., trans. by J.L. Austin (Evanston IL: Northwestern University Press, 1953).

[H1] R. HECK, JR., *The Consistency of Predicative Fragments of Frege’s Grundgesetze der Arithmetik*, *History and Philosophy of Logic*, vol.17 (1996), pp. 209-220.

[G1] Y. GAUTHIER, *The Internal Consistency of Arithmetic With Infinite Descent*, *Modern Logic*, vol. 8 no 1/2 (January 1998-April 2000), pp. 47-86.

[H2] R. HECK, JR., *Finitude and Hume’s Principle*, *Journal of Philosophical Logic*, vol. 26 (1997), pp. 589-617.

[H3] R. HECK, JR., *Cardinality, Counting, and Equinumerosity*, to appear.

[S1] S. SHAPIRO, *Foundations without Foundationalism* (Oxford: Clarendon Press, 1991), especially pp. 65-6.

[T1] N. TENNANT, *Anti-Realism and Logic: Truth as Eternal* (Oxford: Clarendon Press, 1987), especially Chapter 25, pp. 275-300.

[W1] D. WILLARD, *Self-verifying Axiom Systems, The Incompleteness Theorem and Related Reflection Principles*, **Journal of Symbolic Logic**, vol. 66 (2001), pp. 536-596.

[W2] C. WRIGHT, *Frege's Conception of Numbers as Objects* (Aberdeen: Aberdeen University Press, 1983).