THE INEVITABILITY OF LOGICAL STRENGTH: strict reverse mathematics

by
Harvey M. Friedman*
Department of Mathematics
The Ohio State University
http://www.math.ohio-state.edu/%7Efriedman/
August 29, 2007

Abstract. An extreme kind of logic skeptic claims that "the present formal systems used for the foundations of mathematics are artificially strong, thereby causing unnecessary headaches such as the Gödel incompleteness phenomena". The skeptic continues by claiming that "logician's systems always contain overly general assertions, and/or assertions about overly general notions, that are not used in any significant way in normal mathematics. For example, induction for all statements, or even all statements of certain restricted forms, is far too general - mathematicians only use induction for natural statements that actually arise. If logicians would tailor their formal systems to conform to the naturalness of normal mathematics, then various logical difficulties would disappear, and the story of the foundations of mathematics would look radically different than it does today. In particular, it should be possible to give a convincing model of actual mathematical practice that can be proved to be free of contradiction using methods that lie within what Hilbert had in mind in connection with his program". Here we present some specific results in the direction of refuting this point of view, and introduce the Strict Reverse Mathematics (SRM) program.

TABLE OF CONTENTS

11. Conservative extensions, interpretability, synonymy, and logical strength.
12. RM and SRM.

1. Many sorted free logic, completeness.

We present a flexible form of many sorted free logic, which is essentially the same as the one we found presented in [Fe95], section 3. In [Fe95], Feferman credits this form of many sorted free logic to [Pl68], [Fe75], [Fe79], and [Be85], p. 97-99.

We prefer to use many sorted free logic rather than ordinary logic, because we are particularly interested in the naturalness of our axioms, and want to avoid any cumbersome or ad hoc features.

We will not allow empty domains. We allow undefined terms. In fact, the proper use of undefined terms is the main point of free logic.

A signature □ (in many sorted free logic) consists of

i. A nonempty set SRT(□) called the sorts.
ii. A set CS(□) called constant symbols.
iii. A set RS(□) called relation symbols.
iv. A set FS(□) called function symbols.
v. We require that CS(□), RS(□), FS(□) be pairwise disjoint, and not contain =.
vi. A function □ with domain CS(□) □ RS(□) □ FS(□), and with the following properties.
vii. For c □ CS(□), □(c) □ SRT(□). This is the sort of c.
viii. For R □ CS(□), □(R) is a nonempty finite sequence from SRT(□). This is the sort of R.
ix. For F □ CS(□), □(F) is a finite sequence from SRT(□) of length ≥ 2. This is the sort of F.

We make the simplifying assumption that equality is present in each sort.

The □ variables are of the form $v_n^{\square}$, n ≥ 1, where □ □ SRT(□).

The □ terms of □, and their sorts, are defined inductively as follows.

i. The □ variable $v_n^{\square}$ is a □ term of sort □.

ii. If c □ CS(□) then c is a □ term of sort □(c).
iii. If $t_1,\ldots,t_k$ are □ terms of sorts $\square_1,\ldots,\square_k$, k ≥ 1, and F □ FS(□), F has sort $(\square_1,\ldots,\square_{k+1})$, then $F(t_1,\ldots,t_k)$ is a □ term of sort $\square_{k+1}$.

The atomic formulas of □ are defined inductively as follows.

i. If s is a □ term then s↑,s□ are atomic formulas of □.
ii. If s,t are terms of the same sort, then s = t, s □ t are atomic formulas of □.
iii. If $s_1,\ldots,s_k$ are terms of respective sorts $\square_1,\ldots,\square_k$, k ≥ 1, and R □ RS(□) of sort $(\square_1,\ldots,\square_k)$, then $R(s_1,\ldots,s_k)$ is an atomic formula of □.

The □ formulas are defined inductively as follows.

i. Every atomic formula of □ is a □ formula.
ii. If □,□ are □ formulas, then (□□),(□ □ □),(□   □),(□ □ □),(□ □ □) are □ formulas.
iii. If v is a □ variable and □ is a □ formula, then (□v)(□),(□v)(□) are □ formulas.

The free logic aspect is associated with the use of ↑,□,=,□. As will be clear from the semantics, ↑ indicates "undefined", □ indicates "defined", = indicates "defined and equal", □ indicates "either defined and equal, or both undefined". Also variables and constants always denote, and a term is automatically undefined if any subterm is undefined.

We now present the semantics for many sorted free logic.

A □ structure M consists of the following.

i. A nonempty set DOM(□) associated with every sort □ □ SRT(□).
ii. For each c □ CS(□), an element c* □ DOM(□(c)). This is the interpretation of the constant symbol c.
iii. For each R □ RS(□), a relation R* □ $\mathrm{DOM}(\square_1)$ □ ... □ $\mathrm{DOM}(\square_k)$, where R has sort $(\square_1,\ldots,\square_k)$. This is the interpretation of the relation symbol R.
iv. For each F □ FS(□), a partial function F* from $\mathrm{DOM}(\square_1)$ □ ... □ $\mathrm{DOM}(\square_k)$ into $\mathrm{DOM}(\square_{k+1})$, where $\square(F) = (\square_1,\ldots,\square_{k+1})$. This is the interpretation of the function symbol F.

A □ assignment is a function □ which assigns to each □ variable $v_n^{\square}$, □ □ S, an element □($v_n^{\square}$) □ DOM(□).

We inductively define val(M,t,□), where M is a □ structure, t is a □ term, and □ is a □ assignment. Note that val(M,t,□) may or may not be defined.

i. Let v be a □ variable. val(M,v,□) = □(v).
ii. Let c □ CS(□). val(M,c,□) = c*.
iii. Let F(s_1,...,s_k) be a □ term. val(M,F(s_1,...,s_k),□) = F*(val(M,s_1,□),...,val(M,s_k,□)) if defined; undefined otherwise.

Thus in order for val(M,F(s_1,...,s_k,□) to be defined, we require that val(M,s_1,□),...,val(M,s_k,□) be defined.

We inductively define sat(M,□,□), where M is a □ structure, □ is a □ formula, and □ is a □ assignment.

i. sat(M,s↑,□) if and only if val(M,s,□) is undefined.
ii. sat(M,s□,□) if and only if val(M,s,□) is defined.
iii. sat(M,s = t,□) if and only if val(M,s,□) = val(M,t,□). Here we require that both sides be defined.
iv. sat(M,s □ t,□) if and only if val(M,s,□) = val(M,t,□) or val(M,s,□),val(M,t,□) are both undefined.
v. sat(M,R(s_1,...,s_k)) if and only if R*(val(M,s_1,□),..., val(M,s_k,□)). Note that condition implies that each val(M,s_i,□) is defined.
vi. sat(M,□□,□) if and only if not sat(M,□,□).
vii. sat(M,□ □ □,□) if and only if sat(M,□,□) and sat (M,□,□).
viii. sat(M,□ □,□) if and only if sat(M,□,□) or sat(M,□,□).
ix. sat(M,□ □ □,□) if and only if either not sat(M,□,□) or sat(M,□,□).
x. sat(M,□ □ □,□) if and only if either (sat(M,□,□) and sat(M,□,□)) or (not sat (M,□,□) and not sat (M,□,□)).
xi. sat(M,(□$v_n^{\square}$)(□),□) if and only if for all x □ DOM(□), sat(M,□,□[$v_n^{\square}$|x]). Here □[$v_n^{\square}$|x] is the □ assignment resulting from changing the value of □ at $v_n^{\square}$ to x.
xii. sat(M,(□$v_n^{\square}$)(□),□) if and only if there exists x □ DOM(□) such that sat(M,□,□[$v_n^{\square}$|x]).

We say that a □ structure M satisfies a formula □ of □ if and only if sat(M,□,□), for all □ assignments □. We say that a □ structure M satisfies a set T of □ formulas if and only if M satisfies every element of T.

We now give a complete set of axioms and rules of inference for □. It is required that v is a □ variable, c is a □ constant, s,t,r,s_1,...,s_k,t_1,...,t_k are □ terms, □,□,□ are □ formulas, v is not free in □, and t is substitutable for v in □. It is also required that each line be a □ formula.

i. All tautologies.
ii. v□, c□.
iii. t↑ □ □t□, where t is a □ term.
iv. t□ □ t = t.
v. s □ t □ (s = t (s↑ □ t↑)).
vi. F(s_1,...,s_k)□ □ (s_1□ □ ... □ s_k□).
vii. R(s_1,...,s_k) □ (s_1□ □ ... □ s_k□).
viii. s = t □ t = s.
ix. (s = t □ t = r) □ s = r.
x. (s_1 = t_1 □ ... □ s_k = t_k) □ F(s_1,...,s_k) □ F(t_1,...,t_k).
xi. (s_1 = t_1 □ ... □ s_k = t_k) □ (R(s_1,...,s_k) □ R(t_1,...,t_k)).
xii. (t□ □ (□v)(□)) □ □[v/t].
xiii. (t□ □ □[v/t]) □ (□v)(□).
xiv. From □ □ □ derive □ □ (□v)(□).
xv. From □ □ □ derive (□v)(□) □ □.
xvi. From □ and □ □ □, derive □.

A theory is a pair T,□, where □ is a signature, and T is a set of □ formulas.

Let T be a theory with signature □. A proof from T is a nonempty finite sequence of □ formulas, where each entry lies in T, falls under i-xiii, or follows from previous entries by xiv, xv, or xvi.

A proof from T of □ is a proof from T whose last entry is □.

We have the following completeness theorem.

THEOREM 1.1. Let T be a theory in many sorted free logic with signature □. Let □ be a □ formula. The following are equivalent.
a. Every □ structure satisfying T, also satisfies □.
b. There is a proof from T of □.

2. Interpretations, conservative extensions, synonymy.

Let □,□ be signatures in many sorted free logic, and S,T be theories with signatures □,□, respectively. We want to define what we mean by an interpretation of S in T.

We will first present a semantic formulation of this notion. We then discuss syntactic formulations.

It is convenient to first define what we mean by an interpretation □ of □ in □. This notion is used for both semantic and syntactic formulations.

We then define what we mean by an interpretation of S in T.

The notion of interpretation of □ in □ is quite weak; e.g., there is no requirement that the interpretation of function symbols be partial functions.

□ is an interpretation of □ in □ if and only if □ consists of the following data.

i. For each sort □ □ SRT(□), □ assigns a □ defined set □(□) of tuples of objects of various nonzero lengths and various sorts in SRT(□). Only finitely many lengths are allowed, and separate formulas are needed for each length. We also need separate formulas for each sequence of sorts used. Also, □ assigns a □ defined binary relation =(□) which is formally set up to hold only of pairs drawn from □(□). Again, separate formulas are needed for every pair of lengths. We allow prospective parameters, so that a finite list of distinguished free variables is given, for each □, which are for the prospective parameters.

ii. Since we are allowing parameters, there is no need to assign data for any c □ CS(□) of sort □ □ SRT(□). However, we will be interested in the notion of parameterless interpretation. So it is best to have □ assign data to c □ CS(□). □ assigns a □ defined set □(c), with distinguished variables for prospective parameters.

iii. For each R □ RS(□) of sort (□$_1$,...,□$_k$), □ assigns a □ defined set □(R) of k tuples (of tuples of various lengths), with distinguished variables for prospective parameters.

iv. For each F □ FS(□) of sort (□$_1$,...,□$_{k+1}$), □ assigns a □ defined set □(F) of k+1 tuples (of tuples of various lengths), with distinguished variables for prospective parameters.

Let S,T be theories in many sorted free logic, with signatures □,□. We now define the notion of interpretation. We say that □ is an interpretation of S in T if and only if

i. □ is an interpretation of □ in □.
ii. Let M |= T. There exists a choice of parameters from the various domains of M such that □ defines an actual model of S, with the proviso that equality in each sort be interpreted as the associated binary relation in □ (often called a weak model of S when giving, say, the Henkin completeness proof for predicate calculus with equality).

We now give the natural equivalent syntactic notion of interpretation of S in T, in case S is a finite theory in a finite signature.

Let □ be an interpretation of □ in □. Since we are assuming that S is finite, there are only finitely many distinguished variables $v_1,\ldots,v_k$ used for prospective parameters, in □. Let □ be a □ sentence. Then □□ is the □ formula with free variables $v_1,\ldots,v_k$ that asserts that

i. □ defines a □ structure.
ii. □ holds in this □ structure.

The requirement is that if □ is the universal closure of an axiom of S, then (□$v_1,\ldots,v_k$)(□□) is provable in T.

It is obvious by the completeness theorem that this is equivalent to the original semantic definition, provided S is finite.

More generally, the semantic notion has a natural syntactic equivalent if

i. The relational type of S is finite; and
ii. We do not allow parameters.

NOTE: From now on we will only consider *finite* theories S,T, and only interpretations *without parameters*.

Let S,T be theories in many sorted free logic. We say that T is a conservative extension of S if and only if

i. The signature □ of T extends the signature □ of S.
ii. S,T prove the same □ formulas.

We say that T is a definitional extension of S if and only if

i. S,T have the same sorts.
ii. T is logically equivalent to an extension of S that is obtained only by adding axioms which explicitly define the new symbols in T by means of formulas in the signature of S

We say that □ is a faithful interpretation of S in T if and only if □ is an interpretation of S in T, where for all sentences □ in the signature of S, S proves □ if and only if T proves □□.

We consider two important conditions on a pair of interpretations □ of S in T, and □′ of T in S.

The first condition, which we call weak synonymy, asserts that for all models M of S, □□′M □ M, and for all models M of T, □′□M □ M. Here □ is isomorphism.

THEOREM 2.1. Let □,□′ be a weak synonymy of S,T. Then
i. Let M,M* |= S. Then M □ M* □ □′M □ □′M*.
ii. Let M,M* |= T. Then M □ M* □ □M □ □M*.
iii. □ is a faithful interpretation of S in T.
iv. □′ is a faithful interpretation of T in S.

Proof: Let □,□′ be a weak synonymy of S,T. For i, assume M,M* |= S, □′M □ □′M*. Then □□′M □ □□′M* □ M □ M*.

For iii, assume T proves □□. Let M |= S. Then □′M |= T, and hence □′M |= □□. Hence □□′M |= □. Therefore M |= □. Hence S proves □.

Claims ii, iv are by symmetry. QED

The second condition is even stronger, and makes sense when S,T have the same sorts. We say that □,□′ are a synonymy of S,T if and only if

i. □,□′ are domain preserving interpretations of S in T and of T in S, respectively.
ii. For M |= S, □□′M = M.
iii. For M |= T, □′□M = M.

We now show that this notion is the same as another notion that is commonly used to mean synonymy. The first is also model theoretic.

We say that S,T are (weakly) synonymous if and only if there is a (weak) synonymy □,□′ of S,T.

THEOREM 2.2. Let S,T be two theories with the same sorts, but where the symbols have been renamed, if necessary, so that S,T have no symbols in common. There is a synonymy of S,T if and only if S,T have a common definitional extension.

Proof: Let □,□′ is a synonymy of S,T, where S,T have the same sorts, and the symbols have been disjointified. Let R consist of

i. the axioms of S.
ii. the axioms of T.
iii. axioms defining the symbols of T by formulas in the signature of S, via □′.
iv. axioms defining the symbols of S by formulas in the signature of T, via □.

We claim that R is a definitional extension of S. To see this, it suffices to show that i,iii logically imply ii,iv. We now argue in i,iii. To obtain ii, we need only obtain the interpretations of the axioms of T by □′. But these interpretations are provable in S.

We now have to obtain iv. A typical instance of iv would take the form

1) $(\square x_1,\ldots,x_k)(P(x_1,\ldots,x_k)\ \square\ \ \square P(x_1,\ldots,x_k))$.

From iii, we obtain

2) $\square P(x_1,\ldots,x_k)\ \square\ \ \square'\square P(x_1,\ldots,x_k)$.

Since □,□′ are a synonymy,

3) S proves $\square'\square P(x_1,\ldots,x_k)\ \square\ \ P(x_1,\ldots,x_k)$

by the completeness theorem.

Hence by i,iii, we obtain 1).

By the symmetric argument, we also see that R is a definitional extension of T.

Conversely, let R be a definitional extension of both S,T, where the symbols of S,T have been disjointified. We have two axiomatizations of R. The first corresponds to R as a definitional extension of T, and the second corresponds to R as a definitional extension of S. Let □ be a definition of the symbols of S by formulas in the signature of T, viewed as a potential interpretation of S in T. Let □′ be a definition of the symbols of T by formulas in the signature of S, viewed as a potential interpretation of T in S.

Let M |= T. Then (□M,M) satisfies the first axiomatization of R. In particular, □M |= S. Also (□M,M) satisfies the second axiomatization of R. Therefore □′□M = M.

Let M |= S. Then (M,□′M) satisfies the second axiomatization of R. In particular, □′M |= T. Also (M,□′M) satisfies the second axiomatization of R. Therefore □□′M = M. QED

THEOREM 2.3. Let S,T be two theories with the same sorts. There is a synonymy of S,T if and only if there are interpretations □ from S in T and □′ from T in S, such that the following holds. For all formulas □ in the signature of S and □ in the signature of T, S proves □ □ □′□□, and T proves □ □ □□′□.

Proof: Let □,□′ be a synonymy of S,T. Let M |= S, and M |= □[□]. Since □′ is domain preserving, □′M |= T, and □′M |= □□[□]. Since □ is domain preserving, □□′M |= S, and □□′M |= □′□□[□]. Hence M |= □′□[□]. Therefore M |= □ □ (□′□)[□]. Since □ is an arbitrary assignment for the signature of S, and M is an arbitrary model of S, we have that □ □ □′□□ is provable in S.

Conversely, assume that S,T,□,□′ are as given. By applying the conditions to atomic formulas □,□, we obtain that for all M |= S, □□′M = M, and for all M |= T, □′□M = M. QED

If S,T obey the equivalent conditions in Theorems 2.2 and 2.3, then we say that S,T are synonymous. If there is a weak synonymy of S,T, then we say that S,T are weakly synonymous.

We will also use the following well known result. A theory is said to be decidable if its set of consequences (in its own signature) is recursive.

THEOREM 2.4. Suppose S is interpretable in T, where T is consistent and decidable. Then S has a consistent decidable extension with the same signature as S.

Proof: Let □ be an interpretation of S in T, where T is decidable. Let S′ consist of the sentences □ in the signature of S such that T proves □□. Clearly S′ extends S, and S′ is a recursive set. Deductive closure and consistency are obvious. QED

3. PFA(N), EFA(N,exp), logical strength.

We now present two very basic and well studied systems of arithmetic. The most comprehensive current reference to fragments of arithmetic is [HP98].

PFA(N), EFA(N,exp) are based on the set N of all nonnegative integers. In the later sections, with the exception of section 4, we focus on systems based on the set Z of all integers.

PFA abbreviates “polynomial function arithmetic”, and EFA abbreviates “exponential function arithmetic”.

PFA(N), EFA(N,exp) build on an earlier system due to R.M. Robinson, called Q (see [Ro52]). We use the notation Q(N), to emphasize that Q is based on N and not on Z.

The signature of Q(N) is L(N). L(N) is one sorted, with 0,S,+,·,<,=. The standard model for L(N) is the usual N,0,S,+,·,<,=.

The signature of PFA(N) is also L(N). The signature of EFA(N,exp) is L(N,exp), which is one sorted, with 0,S,+,·,exp,<,=, where exp is a binary function symbol. The standard model for L(N,exp) is the usual N,0,S,=,·,<,=, where we take exp(0,0) = 1.

The nonlogical axioms of Q(N) are as follows.

Q1. □Sx = 0.
Q2. Sx = Sy □ x = y.
Q3. (□x = 0) □ (□y)(x = Sy).

Q4. x + 0 = x.
Q5. x + Sy = S(x + y).
Q6. x · 0 = 0.
Q7. x · Sy = (x · y) + x.
Q8. x < y □ (□z)(z + Sx = y).

Note that in free logic, these axioms logically imply that 0□, Sx□, x+y□, x·y□.

The □$_0$(N) (□$_0$(N,exp)) formulas are the formulas of L(N) (L(N,exp)) defined as follows.

i) every atomic formula of L(N) (L(N,exp)) is in □$_0$(N) (□$_0$(N,exp));
ii) if □,□ are in □$_0$(N) (□$_0$(N,exp)) then so are □□, □ □ □, □ □, □ □ □, □ □ □;
iii) if □ is □$_0$(N) (□$_0$(N,exp)) and x is a variable not in the term t of L(N) (L(N,exp)), then (□x)(x < t □ □) and (□x)(x < t □ □) are in □$_0$(N) (□$_0$(N,exp)).

In [HP98], the terms t in bounded quantification are required to be variables. This is a minor difference.

PFA(N) is essentially the same as I□$_0$ in [HP98], p. 29. The nonlogical axioms of PFA(N) are as follows.

1. The axioms of Q(N).
2. (□[x/0] □ (□x)(□ □ □[x/Sx])) □ □, where □ is □$_0$(N).

EFA(N,exp) is essentially the same as I□$_0$(exp) in [HP98], p. 37 (although there only base 2 exponentiation is used). The nonlogical axioms of EFA(N,exp) are as follows.

1. The axioms of Q.
2. exp(x,0) = S0, exp(x,Sy) = exp(x,y)·x.
3. (□[x/0] □ (□x)(□ □ □[x/Sx])) □ □, where □ is in □$_0$(N,exp).

We introduced the one sorted system EFA = EFA(N,exp) in [Fr80]. It was also used in the exposition of our work on Translatability and Relative Consistency, in [Sm82]. See [HP98], p. 405, second paragraph, regarding some historical points.

EFA(N,exp) represents the minimum level of formal arithmetic where standard coding mechanisms in arithmetic can be done naturally without worry. For example, we do not have to worry about how to code sets of binary relations on [0,n].

In fact, EFA(N,exp) appears to be quite strong from the mathematical viewpoint. We conjecture that EFA(N,exp) is sufficient to prove any normal theorem of number theory that is adequately formalizable in its language. We can be liberal about “formalizable” here, using the various natural codings available in EFA(N,exp).

For example, we conjecture that Fermat’s Last Theorem is provable in EFA(N,exp). This has never been established. This conjecture captured the imagination of Jeremy Avigad who wrote extensively about it, and related issues, in [Av03].

Accordingly, we now make the following definition.

T has logical strength if and only if EFA(N,exp) is interpretable in T.

The main point of this paper is the presentation of strictly mathematical theories with logical strength. See section 7, and Corollary 11.11.

4. Five related systems of arithmetic with N.

We now introduce six systems of arithmetic on N that are closely related to PFA(N) and EFA(N,exp).

LEMMA 4.1. There is a Δ_0(N) formula Exp(x,y,z) with only the distinct free variables shown such that the following is provable in PFA(N).
i) Exp(x,0,z) $\leftrightarrow$ z = S0;
ii) Exp(x,Sy,z) $\leftrightarrow$ ($\exists$v)(Exp(x,y,v) $\wedge$ z = v·x);
iii) (Exp(x,y,z) $\wedge$ Exp(x,y,w)) $\rightarrow$ z = w.

Proof: See [HP98], p. 299. QED

LEMMA 4.2. Suppose Exp(x,y,z) and Exp’(x,y,z) satisfy the condition in Lemma 4.1. Then PFA(N) proves their equivalence.

Proof: Let Exp(x,y,z), Exp’(x,y,z) obey the conditions in Lemma 4.1. Let n,m,r be such that Exp(n,m,r) $\wedge$ $\neg$Exp’(n,m,r). Fix n,r, and let m be least such that ($\exists$s $\leq$ r)(Exp(n,m,s) $\wedge$ $\neg$Exp’(n,m,s)). Let Exp(n,m,s),

□Exp'(n,m,s), s □ r. Clearly m > 0. Let Exp(n,m-1,t), s = t•n. Then □Exp'(n,m-1,t). Also n = 0   t □ s □ r. The latter is impossible by the choice of m. Hence n = 0, s = 0. Since m > 0, Exp'(n,m,s). This is a contradiction. QED

The sentence EXP(N) is taken to be (□x,y)(□z)(Exp(x,y,z)), where Exp is any formula satisfying the conditions of Lemma 4.1. By Lemma 4.2, this defines EXP(N) up to provable equivalence in PFA(N).

Let CM(N) = "common multiples" be the following sentence in L(N).

CM(N). For all n > 0, the integers 1,2,...,n have a positive common multiple.

The five relevant fragments of arithmetic considered here are as follows.

Q(N), PFA(N), PFA(N) + EXP(N), PFA(N) + CM(N), EFA(N,exp).

Note that the signature of all of these systems is L(N), except for the last, which has signature L(N,exp).

The most basic relationships between these theories are well known, and summarized in the following two theorems.

THEOREM 4.3. Q(N) □ PFA(N) □ PFA(N) + CM(N) = PFA(N) + EXP(N) □ EFA(N,exp). These □ are all proper.

Proof: Assume PFA(N) + EXP(N). Write 2^x, x ≥ 0, according to EXP(N). Fix n ≥ 1. We prove by induction on 1 □ m □ n that 1,...,n have a positive common multiple □ $2^\wedge m^2$. This is obvious for m = 1. Let 1 □ m < n, and x be a positive common multiple of 1,...,m, x □ $2^\wedge m^2$. Then x(m+1) □ $(2^\wedge m^2)(2^m)$ □ $2^\wedge(m+1)^2$. This establishes CM(N).

Now assume PFA(N) + CM(N). Fix n,m ≥ 2. Let x be a positive common multiple of 1,...,nm. We can assume that x is the least positive common multiple of 1,...,nm. Show that every prime factor of x is □ nm. Show that x+1,2x+1,...,(nm)x+1 are pairwise relatively prime. Let y be a positive common multiple of 1,...,nx+1. Code n-tuples as Gödel did, □ y, in order to develop the geometric progression $1,n,n^2,...,n^m$. This establishes EXP(N).

To see that PFA(N) + EXP(N) □ EFA(N,exp), write Exp(n,m,r) for the internal exponentiation relation (in L(N)). Argue that Exp(n,m,r) □ exp(n,m) = r using □$_0$(exp) induction, exactly as in the proof of Lemma 4.2.

To see that Q(N) does not prove PFA(N), consider all of the polynomials in one variable x with integer coefficients, which have a positive leading coefficient, or is 0. These form a model of Q(N) under the usual 0,S,+,·,=, with □ defined according to axiom Q8 of Q(N). This model of Q(N) does not satisfy, for example, (□y)(x = 2y   x = 2y+1).

To see that PFA(N) does not prove EXP(N), let M be a nonstandard model of PFA(N). Let x be a positive nonstandard integer in M, and let M′ be the restriction of M to the integers of M whose magnitude is at most x^n, for some standard n ≥ 1. Them M′ is a model of PFA(N). It is easily verified that 2^x does not exist in M. QED

THEOREM 4.4. EFA(N,exp) is a definitional extension of PFA(N) + EXP(N). PFA(N) is interpretable in Q(N). PFA(N) + EXP(N) is not interpretable in PFA(N).

Proof: For the first claim, note that by the proof of Theorem 4.3 (that PFA(N) + EXP(N) □ EFA(N,exp)), EFA(N,exp) proves that exp(n,m) = r □ Exp(n,m,r).

It remains to show that every axiom of EFA(N,exp) is provable in PFA(N) + EXP(N) + (□n,m,r)(exp(n,m) = r □ Exp(n,m,r)). This is clear by inspection.

The second claim is credited to Wilkie, in the sharp form on p. 367 of [HP98].

For the third claim, see [Wi86], and [HP98], p. 391. QED

5. Five related systems of arithmetic with Z.

We now introduce six systems of arithmetic on Z that are closely related to the six systems of section 4. These are parallel to those systems introduced in section 4, and move us closer to the strictly mathematical theories of section 7.

We first introduce LOID(Z). LOID abbreviates “linearly ordered integral domain”. According to Theorem 5.3 below, LOID is an extremely robust strictly mathematical theory.

The signature of LOID(Z) is L(Z). L(Z) is one sorted, with 0,1,+,-,·,<,=, where - is unary. The standard model for L(Z) is the usual Z,0,1,+,-,·,<,=.

The nonlogical axioms of LOID(Z) are

a. x+0 = x.
b. x+y = y+x.
c. x+(y+z) = (x+y)+z.
d. x+(-x) = 0.
e. x·1 = x.
f. x·y = y·x.
g. x·(y·z) = (x·y)·z.
h. x·(y+z) = (x·y)+(x·z).
i. x·y = 0 □ (x = 0   y = 0).
j. 0 < 1.
k. □x < x.
l. (x < y □ y < z) □ x < z.
m. x < y   x = y   y < x.
n. (0 < x □ 0 < y) □ (0 < x+y □ 0 < x·y).
o. x < y □ -y < -x.

Note that in free logic, these axioms imply 0□, 1□, x+y□, -x□, x·y□.

How do we know that we have included all appropriate axioms in LOID(Z)? We first present some basic development of LOID(Z). Define x > y □ x < y, x ≠ 0 □ □x = 0.

LEMMA 5.1. The following are provable in LOID(Z).
i. --x = x.
ii. -(x+y) = -x + -y.
iii. x+x = 0 □ x = 0.
iii. x·0 = 0.
iv. -x = (-1)·x.
v. (-1)·(-1) = 1.
vi. x,y < 0 □ x·y > 0.
vii. x < 0 □ y > 0 □ x·y < 0.

Proof:
i. By d, -x + --x = 0. Hence x = x + (-x + --x) = (x + -x) + --x = 0 + --x = --x.
ii. By d, x+y + -(x+y) = 0. Hence -x + -y + x + y + -(x+y) = -x + -y = -(x+y).

iii. Use m. If $x = 0$ then we are done. Assume $0 < x$. Then by n, $0 < x+x$, and so $x+x \neq 0$, $x \neq 0$. Assume $x < 0$. By o, $0 < -x$, $0 < -x + -x = -(x+x)$. Hence $-(x+x) \neq 0$, $x \neq 0$.
iv. $(-1)\cdot x + 1\cdot x = 0 = (-1)\cdot x + x$. Hence $0 + -x = ((-1)\cdot x) + x) + -x = (-1)\cdot x$.
v. $(-1)\cdot(-1) = --1 = 1$.
vi. Assume $x,y < 0$. By axioms n,o, $0 < -x,-y$, $(-x)\cdot(-y) > 0$. Now $(-x)\cdot(-y) = (-1)\cdot x\cdot(-1)\cdot y = (-1)\cdot(-1)\cdot x\cdot y = 1\cdot x\cdot y = x\cdot y$.
vii. Assume $x < 0$, $y > 0$. By axioms n,o, $0 < -x,y$, $0 < (-x)\cdot y$. Since $(-x)\cdot y = (-1)\cdot x\cdot y = -(x\cdot y)$, we have $0 < -(x\cdot y)$, $x\cdot y < 0$. QED

The official definition of an ordered field is given in, say, [Ja85], p. 307:

An ordered field (F,P) is a field F together with a subset P (the set of positive elements) of F such that
i. $0 \;\square\; P$.
ii. $a \;\square\; F \;\square\; (a \;\square\; P \quad a = 0 \quad -a \;\square\; P)$.
iii. $a,b \;\square\; P \;\square\; (a+b \;\square\; P \;\square\; a\cdot b \;\square\; P)$.

LEMMA 5.2. Let $M = (D,0,1,+,-,\cdot,<)$ be a model of LOID(Z). There is an ordered field (F,P) and an isomorphism $j:(D,0,1,+,-,\cdot) \;\square\; F$ such that for all $x \;\square\; D$, $jx \;\square\; P \;\square\; x > 0$.

Proof: Let M be as given. By axioms a-i, M is an integral domain. Hence the fraction field construction results in a field F and a canonical isomorphism $j:(D,0,1,+,-,\cdot) \;\square\; F$.

Recall that F consists of the equivalence classes of ordered pairs (x,y), where $x,y \;\square\; D$, $y \neq 0$, under the equivalence relation $(x,y) \;\square\; (z,w) \;\square\; xw = yz$. Define $jx = [(x,1)]$. Obviously j is an isomorphism from M into F.

Define $P = \{[(x,y)]: x,y > 0 \quad x,y < 0\}$. I.e., $P = \{[(x,y)]: x,y$ have the same nonzero sign$\}$. It is obvious that $0^F = [(0,1)] \;\square\; P$.

We claim independence of representatives, in the sense that for all x,y,z,w, if $[x,y] \;\square\; [z,w]$, then

*) x,y have the same nonzero sign □
z,w have the same nonzero sign.

To see this, assume $[x,y] \;\square\; [z,w]$. Then

$$x\cdot w = y\cdot z,\ y,w \neq 0.$$

case 1. $x \neq 0$. Then $x\cdot w \neq 0$, $y\cdot z \neq 0$, $z \neq 0$. By inspection, using Lemma 5.1, vi),vii), we see that *) holds.

case 2. $x = 0$. Then $y\cdot z = 0$, $z = 0$. By inspection using Lemma 5.1, vi),vii), we see that *) holds.

Now let [(x,y)] □ F. If x,y have the same nonzero sign then [(x,y)] □ P. If x,y have opposite nonzero signs, then −x,y have the same nonzero sign, and hence −[(x,y)} = [(-x,y)] □ P. Finally, if x = 0 then [(x,y)] = 0^F.

Now let [(x,y)], [(z,w)] □ P. By the independence of representatives (claim above), we can assume that x,y,z,w > 0. Note that

$[(x,y)] + [(z,w)] = [(x\cdot w + y\cdot z,y\cdot w)]$ □ P.
$[(x,y)] \cdot [(z,w)] = [(x\cdot z,y\cdot w)]$ □ P.

This establishes that (F,P) is an ordered field.

Now let x □ D. If jx = [x,1] □ P then obviously x > 0. If jx = [x,1] □ P then □x > 0, using the independence of representatives. QED

THEOREM 5.3. A purely universal sentence in L(Z) is true in the ordered field of real numbers if and only if it is provable in LOID(Z). LOID(Z) can be axiomatized as the set of all quantifier free formulas in L(Z) which are universally true in the ordered field of real numbers.

Proof: It suffices to show that every purely existential sentence in L(Z) that is true in some model of LOID is true in the ordered field of real numbers.

Let M be a model of LOID satisfying the purely existential sentence □ in L[Z]. By Lemma 5.2, let (F,P) be an ordered field extending M, with an isomorphism j:(D,0,1,+,−,·) □ F, and for all x □ D, jx □ P □ x > 0.

We define < on F by

x < y □ y-x □ P.

We claim that

j:(D,0,1,+,-,·,<) □ (F,<)

is an isomorphism. To see this, let x < y in M. Then y-x > 0, and so j(y-x) □ P. Hence j(y)-j(x) □ P, and so x < y in (F,<). Hence □ is preserved, and so □ holds in (F,<).

Now every ordered field (F,<), where < is defined as above from P, extends to an ordered real closed field, whose < agrees with the < of (F,<). Hence □ holds in some ordered real closed field. Since □ is a first order sentence, □ holds in all ordered real closed fields. Hence □ holds in the ordered field of real numbers.

The final claim follows from the previous claim using the observation that the axioms of LOID(Z) are quantifier free formulas in L(Z) which are universally true in the ordered field of real numbers. QED

The $\square_0$(Z) ($\square_0$(Z,exp)) formulas are the formulas of L(Z) (L(Z,exp)) defined as follows.

i) every atomic formula of L(Z) (L(Z,exp)) is in $\square_0$(Z) ($\square_0$(Z,exp));
ii) if □,□ are in $\square_0$(Z) ($\square_0$(Z,exp)) then so are □□, □ □ □, □ □, □ □ □, □ □ □;
iii) if □ is $\square_0$(Z) ($\square_0$(Z,exp)) and x is a variable not in the term t of L(Z) (L(Z,exp)), then (□x)(-t < x < t □ □) and (□x)(-t < x < t □ □) are in $\square_0$(Z) ($\square_0$(Z,exp)).

Henceforth, we will use x □ y as an abbreviation for x < y x = y, and x ≥ y as an abbreviation for y < x y = x.

The signature of PFA(Z) is L(Z). The nonlogical axioms of PFA(Z) are

1. LOID(Z).
2. (□[x/0] □ (□x)(□ □ □[x/Sx])) □ (x ≥ 0 □ □), where □ is in $\square_0$(Z).

Note that PFA(Z) proves the axiom of discreteness: there is nothing in (0,1). To see this, let □ = x ≥ 0 □ (x < 1 □ x □ 0). Use 2 for □, to obtain (x ≥ 0 □ x < 1) □ x □ 0. Now suppose x < 1. If x > 0 then x □ 0. Hence x □ 0.

L(Z,exp) is one sorted, with 0,1,+,-,·,exp,<,=, where - is unary and exp is binary. The standard model for L(Z,exp) is the usual Z,0,1,+,-,·,exp,<,=, where exp(x,y) is the usual x^y, which is defined if and only if y ≥ 0, and where x^0 = 1.

The signature of EFA(Z,exp) is L(Z,exp). The nonlogical axioms of EFA(Z,exp) are

1. LOID(Z).
2. exp(x,0) = 1.
3. y ≥ 0 □ (exp(x,y+1) = exp(x,y)·x □ exp(x,-y-1)↑).
4. (□[x/0] □ (□x)(□ □ □[x/x+1])) □ (x ≥ 0 □ □), where □ is in □$_0$(Z,exp).

LEMMA 5.4. There is a □$_0$(Z) formula Exp(x,y,z) with only the distinct free variables shown such that the following is provable in PFA(Z).
i) Exp(x,0,z) □ z = S0;
ii) y ≥ 0 □ (Exp(x,y+1,z) □ (□v)(Exp(x,y,v) □ z = v·x));
iii) (Exp(x,y,z) □ Exp(x,y,w)) □ z = w;
iv) Exp(x,y,z) □ y ≥ 0.

Proof: This is a straightforward adaptation of Lemma 4.1 to PFA(Z). QED

LEMMA 5.5. Suppose Exp(x,y,z) and Exp'(x,y,z) satisfies the condition in Lemma 5.4. Then PFA(Z) proves their equivalence.

Proof: This is a straightforward adaptation of Lemma 4.2 to PFA(Z). QED

The sentence EXP(Z) is taken to be (□x,y)(□z)(Exp(x,y,z)), where Exp is any formula satisfying the conditions of Lemma 5.4. By Lemma 5.5, this defines EXP(Z) up to provable equivalence in PFA(Z).

Let CM(Z) = "common multiples" be the following sentence in L(Z).

CM(Z). For all n > 0, the integers 1,2,...,n have a positive common multiple.

Note that CM(Z) is formally the same as CM(N), but it is still convenient to use the notation CM(Z), CM(N).

The five relevant fragments of arithmetic considered here are as follows.

LOID(Z), PFA(Z), PFA(Z) + EXP(Z), PFA(Z) + CM(Z), EFA(Z,exp).

The most basic relationships between these theories are summarized in the following three theorems.

THEOREM 5.6. LOID(Z) □ PFA(Z) □ PFA(Z) + CM(Z) = PFA(Z) + EXP(Z) □ EFA(Z,exp). These □ are all proper.

THEROEM 5.7. EFA(Z,exp) is a definitional extension of PFA(Z) + EXP(Z). PFA(Z) + EXP(Z) is not interpretable in PFA(Z). PFA(Z) is not interpretable in LOID(Z).

Proof: Theorem 5.6, 5.7, with the exception of the final claim of Theorem 5.7, can be proved by an adaptation of the corresponding proofs of Theorems 4.3, 4.4.

For the final claim of Theorem 5.7, the essence of the matter is that Q(N) is not interpretable in the theory of ordered real closed fields, ORCF. If this were not the case, then, since the theory of ordered real closed fields is decidable, by Theorem 2.4 we have Q(N) has a consistent decidable extension with signature L(N). This contradicts the well known essential undecidability of Q(N); see [Ro52]. Obviously PFA(Z) is not interpretable in LOID(Z), since Q(N) is trivially interpretable in PFA(Z). QED

6. Arithmetic on N and arithmetic on Z.

We establish some relationships between the five systems of section 4,

Q(N), PFA(N), PFA(N) + EXP(N), PFA(N) + CM(N), EFA(N,exp).

and the five systems of section 5,

LOID(Z), PFA(Z), PFA(Z) + EXP(Z), PFA(Z) + CM(Z), EFA(Z,exp).

In sections 4,5, we have discussed the relationships between the theories in each of the two groups separately.

We can interpret PFA(N) in PFA(Z), by taking the domain to be the nonnegative elements, and defining 0,S,+,·,<,= in the obvious way. We call this interpretation □(N,Z).

We can interpret PFA(Z) in PFA(N) by taking the domain to be the pairs (n,0), n > 0, and (n,1). Here (n,0) represents the negative integer −n, and (n,1) represents the nonnegative integer n. We define 0,1,+,−,·,<,= in the obvious way. We call this interpretation □(Z,N).

THEOREM 6.1. □(N,Z), □(Z,N) is a weak synonymy of PFA(N), PFA(Z), and is also a weak synonymy of PFA(N) + EXP(N), PFA(Z) + EXP(Z).

Proof: It is obvious that □(N,Z) is an interpretation of PFA(N) in PFA(Z), and □(Z,N) is an interpretation of PFA(Z) in PFA(N). It is also obvious that □(N,Z) is an interpretation of PFA(N) + EXP(N) in PFA(Z) + EXP(Z), and □(Z,N) is an interpretation of PFA(Z) + EXP(Z) in PFA(N + EXP(N).

For weak synonymy, let M |= PFA(N), and within M, form the (n,0),(n,1) interpretation of PFA(Z), according to □', obtaining □'M |= PFA(Z). Within □'M, form the nonnegative element interpretation of PFA(N), according to □, obtaining □□'M. The nonnegative element interpretation just uses the (n,1). Clearly we have an isomorphism from □□'M onto M by sending each (n,1) to n.

Let M |= PFA(Z), and within M, form the nonnegative element interpretation of PFA(N), according to □, obtaining □M |= PFA(N). Within □M, form the (n,0),(n,1) interpretation of PFA(Z), according to □', obtaining □'□M. Clearly we have an isomorphism from □'□M onto M by sending each negative n to (n,0), and each nonnegative n to (n,1). QED

We extend □(N,Z) and □(Z,N) in the obvious way to □(N,Z;exp), □(Z,N;exp).

THEOREM 6.2. □(N,Z,exp), □(Z,N,exp) is a weak synonymy of EFA(N,exp), EFA(Z,exp).

Proof: Argue as for Theorem 6.1. QED

Note that □(N,Z) and □(Z,N) are not domain preserving, and so we cannot use them to establish synonymy. We give new interpretations for this purpose.

We can interpret PFA(N) in PFA(Z), by taking the N to be

0,1,-1,2,-2,...

with the obvious corresponding definition of 0,S,+,·,<,=. Specifically, we first define, in PFA(Z), the function f:Z □ Z by f(x) = the position in the above sequence = 0 if x = 0; 2x-1 if x > 0; -2x if x < 0. Then we define 0′,S′,+′, ·′, <′,=, uniquely, in such a way that f is an isomorphism from Z,0′,S′,+′,·′,<′,= onto {x: x ≥ 0},0,+1,+,·,<,=. Call this □′(N,Z).

We can interpret PFA(Z) in PFA(N), by taking the Z to be

...6,4,2,0,1,3,5,...

with the obvious corresponding definition of 0,1,+,-,·,<,=. Specifically, we first define, in PFA(N), the function g:N □ N □ {0,1} by g(2n+1) = (1,n+1), g(2n+2) = (0,n+1), g(0) = 0. Then we define 0′,1′,+′,-′,·′,<′,=, uniquely, in such a way that g is an isomorphism from N,0′,1′,+′,-′,·′,<,= onto {(x,0): x > 0} □ {(x,1): x ≥ 0} with its usual 0*,1*,+*,-*,·*,<*,=, that makes it look like the arithmetic of Z. Call this □′(Z,N).

LEMMA 6.3. □′(N,Z), □′(Z,N) is a synonymy of PFA(N), PFA(Z), and also of PFA(N) + EXP(N), PFA(Z) + EXP(Z).

Proof: It is obvious that □′(N,Z) is an interpretation of PFA(N) in PFA(Z), and □′(Z,N) is an interpretation of PFA(Z) in PFA(N). This is also obvious with EXP(N) and EXP(Z).

For synonymy, let M |= PFA(N), and within M, form the ...6,4,2,0,1,3,5,... interpretation of PFA(Z), according to □′, obtaining □′M |= PFA(Z). Within □′M, form the 0,1,-1,2,-2,... interpretation of PFA(N), according to □, obtaining □□′M. Note that in □′M, 0,1,-1,2,-2,... is the 0,1,2,3,... of M. Hence □□′M = M.

Let M |= PFA(Z), and within M, form the 0,1,-1,2,-2,... interpretation of PFA(N), according to □, obtaining □M |= PFA(N). Within □M, form the ...6,4,2,0,1,3,5,... interpretation of PFA(Z), according to □′, obtaining □′□M. Note that in □M, ...6,4,2,0,1,3,5,... is the ...,-3,-2,-1,0,1,2,3,... of M. Hence □′□M = M. QED

We extend □(N,Z) and □(Z,N) in the obvious way to □(N,Z;exp), □(Z,N;exp).

LEMMA 6.4. □′(N,Z,exp), □′(Z,N,exp) is a synonymy of EFA(N,exp), EFA(Z,exp).

Proof: Argue as for Lemma 6.3. QED

We now construct a certain model M of Q(N). The domain will consist of certain polynomials in variables $x_{\square}$, $\square < \square_1$, with integer coefficients. We will not be using the ordering of variables.

Let P be such a polynomial. The maximal monomials of P are the monomials of P that are maximal with respect to the divides relation. Note that if P is not the trivial polynomial, 0, then P has at least one maximal monomial.

We take dom(M) to be these polynomials which are either 0, or whose maximal monomials all have positive coefficients.

For M, we use the ordinary 0,S,+,·. We define < as in axiom Q8 of Q(N).

LEMMA 6.5. M is a model of Q(N).

Proof: We first need to verify that dom(M) is closed under +,·. Let P,Q □ dom(M). We can assume that P,Q are not the 0 polynomial. Let □ be a maximal monomial of P+Q. If □ occurs in P and not in Q, or in Q but not in P, then it retains its coefficient, which must be positive. If □ occurs in P and Q, then its coefficient in P+Q is positive. Hence P+Q □ dom(M).

It is trickier to establish that PQ □ dom(M). Let $\square_1,...,\square_n$ be the monomials of P, and $\square_1,...,\square_m$ be the monomials of Q. Since we are assuming that neither P nor Q is 0, we have n,m ≥ 1. Let S be the set of all $\square_i\square_j$ that are maximal among all of the $\square_i\square_j$ (even if the coefficient of $\square_i\square_j$ in PQ is □ 0). Suppose $\square_i\square_j$ □ S. Then obviously $\square_i$ is maximal in P and $\square_j$ is maximal in Q. Now any $\square_p\square_q = \square_i\square_j$, where $\square_p$ is a monomial in P and $\square_q$ is a monomial in Q, must have that $\square_p$ is maximal in P and $\square_q$ is maximal in Q. Hence the coefficient of $\square_i\square_j$ in PQ must be positive (since it is the sum of the coefficients contributed by each of these $\square_p\square_q = \square_i\square_j$). Therefore $\square_i\square_j$ is a monomial of PQ with positive coefficient.

We now claim that every maximal monomial $\square_i\square_j$ of PQ lies in S. To see this, let $\square_i\square_j$ be a maximal monomial of PQ, where

$□_i□_j$ □ S. Let $□_p□_q$ □ S be a proper multiple of $□_i□_j$. By the previous paragraph, $□_p□_q$ is a monomial of PQ (in fact, with positive coefficient), contradicting that $□_i□_j$ is a maximal monomial of PQ.

We have now shown that every maximal monomial $□_i□_j$ of PQ has a positive coefficient. Thus PQ □ dom(M).

The verification of Q2, Q4 - Q7 is by the ring laws for polynomials. Q8 is by definition. Q1 follows from the fact that -1 □ dom(M). For Q3, let P □ dom(M), P not 0. If P is nonconstant then P-1 □ dom(M). If P is constant then P ≥ 1, and so P-1 □ dom(M). QED

LEMMA 6.6. Q(N) and PFA(N) are not weakly synonymous.

Proof: We use the model M of Lemma 6.5. Let M’ be a model of PFA(N) defined in M without parameters. We show that M’ is countable.

Recall that in interpretations, we allow the domain to consist of tuples of varying lengths. We also allow the equality relation to be interpreted by an equivalence relation. This equivalence relation must be definable in M without parameters.

We call two polynomials isomorphic if and only if they are identical up to a permutation of variables. We call two finite sequences of polynomials isomorphic if and only if they are coordinatewise isomorphic via a single permutation. We call the equivalence classes under this equivalence relation on the finite sequences of polynomials, shapes.

Note that by the symmetry of M, for any two tuples of polynomials that are isomorphic, one lies in dom(M’) if and only if the other lies in dom(M’).

case 1. Any two tuples of polynomials in dom(M’) that are isomorphic, and lie in dom(M’), are interpreted to be equal in M’. Since the number of shapes is countable, we see that dom(M’) is countable.

case 2. Let $(P_1,...,P_n)$, $(Q_1,...,Q_n)$ be isomorphic elements of dom(M’), which are not satisfied to be equal in M’. Let □ be an automorphism of the variables $\{x_□: □ < □_1\}$, that interchanges $(P_1,...,P_n)$ and $(Q_1,...,Q_n)$. Then □ extends uniquely to an automorphism □* of M of finite order, which in turn induces an automorphism □ of M’ of finite order. Since □ interchanges the distinct elements [(P_1,...,P_n)] and [(Q_1,...,Q_n)] of dom(M’), we see that □ has finite order. But no model of PFA(N) can have an automorphism of finite order because of the definable linear ordering <, with parameters. So this case is impossible.

Since M’ is countable, and M is uncountable, it is clear that we cannot define, in M’, an isomorphic copy of M. Hence Q(N), PFA(N) are not weakly synonymous. QED

We summarize the synonymy and mutual interpretability results.

THEOREM 6.7. PFA(N), PFA(Z) are synonymous. PFA(N) + EXP(N), EFA(N,exp), PFA(Z) + EXP(Z), EFA(Z,exp) are synonymous. There are no other synonymy, or even weak synonymy, relations between the 10 systems. Q(N), PFA(N), PFA(Z) are mutually interpretable. PFA(N) + EXP(N), EFA(N,exp), PFA(Z) + EXP(Z), EFA(Z,exp) are mutually interpretable. There are no other mutual interpretability relations between the 10 systems. LOID(Z) is interpretable in Q(N), but not vice versa.

Proof: The first claim is by Lemma 6.3. For the second claim, PFA(N) + EXP(N), PFA(Z) + EXP(Z) are synonymous by Lemma 6.3. PFA(N) + EXP(N), EFA(N,exp) are synonymous by Theorems 4.4 and 2.2. PFA(Z) + EXP(Z), EFA(Z,exp) are synonymous by Theorems 5.7 and 2.2. EFA(N,exp), EFA(Z,exp) are synonymous by Lemma 6.4.

For the third claim, PFA(N) + EXP(N) is not interpretable in PFA(N) by Theorem 4.4. That Q(N), PFA(N), PFA(Z) are not interpretable in LOID(Z) comes from (the proof of) Theorem 5.7. That Q(N), PFA(N) are not weakly synonymous comes from Lemma 6.6.

For the fourth claim, use the first claim together with the interpretability of PFA(N) in Q(N), from Theorem 4.4.

The fifth claim follows from the second claim.

The sixth claim follows from PFA(N) + EXP(N) not interpretable in PFA(N), and Q(N) not interpretable in LOID(Z). The former is by Theorem 4.4, and the latter is by the proof of Theorem 5.7.

The seventh claim is by the proof of Theorem 5.7, and the interpretability of ORCF in Q(N) in [FF02].

7. Seven strictly mathematical theories.

Among the twelve theories considered in section 6, only Q(N) and LOID(Z) are strictly mathematical. The rest rely on induction stated for all bounded formulas. However, Q(N) and LOID(Z) do not have logical strength, in the sense used in this paper (see the end of section 3).

We now present six strictly mathematical theories. We will extend the one sorted signatures from sections 3-5,

L(N), L(Z), L(N,exp), L(Z,exp),

with the new many sorted signatures

L(Z,fst), L(Z,fsq), L(Z,fst,fsq), L(Z,exp,fst),
L(Z,bexp,fst), L(Z,exp,fsq).

Here fst abbreviates "finite sets of integers", and fsq abbreviates "finite sequences of integers". Also bexp abbreviates "binary exponentiation".

L(Z,exp,fst) is two sorted. We use Z for sort 1, and fst for sort 2. Here fst abbreviates "finite sets of integers". We use 0,1,+,-,·,exp,<,= on the Z sort. We use □ between sort Z and sort fst.

L(Z,exp,fsq) is two sorted. We use Z for sort 1 and fsq for sort 2. Here fsq abbreviates "finite sequences of integers ". We use 0,1,+,-,·,exp,<,= on the Z sort. We use the unary function symbol lth from sort fsq into sort Z. We use the binary function symbol val from sort fsq cross sort Z, into sort Z.

The standard model for L(Z,exp,fst) has first sort Z, with 0,1,+,-,·,<,= as usual, and exp(n,m) = r if and only if n^m = r □ m ≥ 0, where n^0 = 1. Thus exp(n,m) is defined if and only if m ≥ 0. The second sort, fst, consists of the finite subsets of Z, where □ is as usual.

The standard model for L(Z,exp,fsq) has domain Z, wi†h 0,1,+,-,·,<,= as usual, and exp(n,m) = r if and only if n^m = r □ m ≥ 0, where n^0 = 1. Thus exp(n,m) is defined if and only if m ≥ 0. The second sort, fsq, consists of the finite sequences from Z, where lth is the length function, which takes values in the nonnegative elements of Z. Also val(x,n) is the n-th term of x, counting from 1, and so is defined if and only if 1 □ n □ lth(x).

We also work with the elimination of exp in L(Z,exp,fst), L(Z,exp,fsq).

The signature of FSTZ is L(Z,fst). The nonlogical axioms of FSTZ are stated informally as follows.

1. Linearly ordered integral domain axioms.
2. Finite interval. [x,y] exists.
3. Boolean difference. A\B = {x □ A: x □ B} exists.
4. Set addition. A+B = {x: x+y: x □ A □ x □ B} exists.
5. Set multiplication. A·B = {x: x·y: x □ A □ x □ B} exists.
6. Least element. Every nonempty set has a least element.

The signature of FSQZ is L(Z,fsq). The nonlogical axioms of FSQZ are stated informally as follows.

1. Linearly ordered integral domain axioms.
2. lth(□) ≥ 0.
3. val(□,n)□ □ 1 □ n □ lth(□).
4. The finite sequence (0,...,n) exists.
5. lth(□) = lth(□) □ -□,□+□,□·□ exist.
6. The concatenation of □,□ exists.
7. For all n ≥ 1, the concatenation of □, n times, exists.
8. There is a finite sequence enumerating the terms of □ that are not terms of □.
9. Every nonempty finite sequence has a least term.

Before giving formal versions of these axioms, we make some remarks about the nonlogical axioms of FSQZ.

a. □ indicates “is defined”. See section 1.

b. Axioms 4-8 are presented in terms of the length and values of the finite sequence that is asserted to exist. In the case of axiom 8, this involves the ring operations.

c. Axiom 7 uses n as a variable (not a standard integer).

We now give formal presentations of FSTZ and FSQZ.

The nonlogical axioms of FSTZ are given formally as follows.

1. Linearly ordered commutative ring axioms.
2. Finite interval.
   (□A)(□x)(x □ A □ (y □ x □ x □ z)).
3. Boolean difference.
   (□C)(□x)(x □ C □ (x □ A □ □(x □ B))).
4. Set addition.
   (□C)(□x)(x □ C □ (□y)(□z)(y □ A □ z □ B □ x = y+z)).
5. Set multiplication.
   (□C)(□x)(x □ C □ (□y)(□z)(y □ A □ z □ B □ x = y·z)).
6. Least element.
   (□x)(x □ A) □ (□x)(x □ A □ (□y)(y □ A □ y □ x)).

The nonlogical axioms of FSQZ are given formally as follows.

1. The above linearly ordered commutative ring axioms for Z.
2. 0 □ lth(□).
3. val(□,n)□ □ 1 □ n □ lth(□).
4. The finite sequence (0,...,n) exists.
   (□□)(lth(□) = n+1 □ (□k)(1 □ k □ n+1 □ val(□,k) = k+1)).
5. lth(□) = lth(□) □ -□,□+□,□·□ exist.
   lth(□) = lth(□) □ (□□)(□n)(val(□,n) □ -val(□,n)) □ (□□)(□n)(val(□,n) □ val(□,n)+val(□,n)) □ (□□)(□n)(val(□,n) □ val(□,n)·val(□,n)).
6. The concatenation of □,□ exists.
   (□□)(□k,n)((1 □ k □ lth(□) □ val(□,k) = val(□,k)) □ (1 □ n □ lth(□) □ val(□,lth(□)+n) = val(□,n))).
7. For all n ≥ 1, the concatenation of □, n times, exists.
   lth(□) = n □ (□□)(lth(□) = n·m □ (□q,r)(0 □ q < m □ 1 □ r □ n □ val(□,n·q+r) = val(□,r))).
8. There is a finite sequence enumerating the terms of □ that are not terms of □.
   (□□)((□k)((□n)(val(□,n) = k) □ ((□n)(val(□,n) = k) □ □(□n)(val(□,n) = k))).
9. Every nonempty finite sequence has a least term.
   1 □ lth(□) □ (□k)(□i)(1 □ i □ lth(□) □ val(□,i) □ val(□,k)).

In axiom 5 above, we use the symbol □ from free logic, which means “either both undefined, or equal”. See section 1.

The signature of FSTZEXP is L(Z,exp,fst). FSTZEXP extends

FSTZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. The finite set {exp(n,0),...,exp(n,m)} exists.

We will find that FSTZEXP is quite weak. We let FSTZEXP' extend FSTZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. n ≥ 2 □ 0 □ m < r □ exp(n,m) < exp(n,r).
iv. The finite set {exp(n,0)+0,exp(n,1)+1,...,exp(n,m)+m} exists.

The signature of FSQZEXP is L(Z,exp,fsq). FSQZEXP extends FSQZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. The finite sequence (exp(n,0),...,exp(n,m)) exists.

Recall CM(Z) from section 3, stated in L(Z).

Thus the seven strictly mathematical theories considered here are

FSTZ, FSQZ, FSTZ + CM(Z), FSQZ + CM(Z), FSTZEXP, FSTZEXP', FSQZEXP

in the respective signatures

L(Z,fst), L(Z,fsq), L(Z,fst), L(Z,fsq), L(Z,exp,fst), L(Z,exp,fst), L(Z,exp,fsq).

We offer the following remarks in comparing the strictly mathematical nature of FSQZ and FSTZ.

i. Finite sequences of integers are more commonplace in mathematics than finite sets of integers.
ii. The pointwise ring operations on finite sequences of integers, and the concatenation of finite sequences of integers (including indefinite concatenation), is more commonplace in mathematics than the Boolean ring operations on finite sets of integers, and the addition and multiplication of finite sets of integers.

8. FSTZ.

In this section we show that FSTZ is a conservative extension of PFA(Z). This follows from the particularly convenient axiomatization of FSTZ given in Theorem 8.28:

THEOREM 8.28. FSTZ can be axiomatized as follows.
1. LOID(Z).
2. $(\exists A)(\forall x)(x \in A \leftrightarrow (y < x < z \wedge \varphi))$, where $\varphi \in \Sigma_0(Z,fst)$ and A is not free in φ.
3. Every nonempty set has a least element.

Recall the axioms of FSTZ.

1. Linearly ordered integral domain axioms (LOID(Z)).
2. Finite interval.
3. Boolean difference.
4. Set addition.
5. Set multiplication.
6. Least element.

We will often use scalar addition and scalar multiplication. We write $A+x = x+A = A+\{x\}$, and $A\cdot x = x\cdot A = A\cdot\{x\}$.

In Lemmas 8.1 - 8.27, it is understood that we are asserting provability within FSTZ.

LEMMA 8.1.
i) $\neg(x < y \wedge y < x+1)$;
ii) (a,b),[a,b),(a,b] exist;
iii) ∅,{x} exists;
iv) $x\cdot A = \{x\cdot y: y \in A\}$ exists;
v) every nonempty set has a greatest element;
vi) every set is included in some interval [a,b];
vii) sets are closed under pairwise union and pairwise intersection;
viii) for standard $n \geq 0$, $\{x_1,\ldots,x_n\}$ exists;
ix) the set of all positive (negative, nonnegative, nonpositive) elements of any set exists.

Proof: For i), assume $0 < x < 1$. By LOID(Z), $0 = 0\cdot x < x\cdot x < 1\cdot x = x$. Hence there is no least y such that $0 < y < 1$. By finite interval, (0,1) exists. By least element, there is a least y such that $0 < y < 1$. This is a contradiction. So $\neg(0 < x < 1)$. Now suppose $x < y < x+1$. Then $0 < y-x < 1$, which is a contradiction.

For ii), note that by i), (a,b) = [a+1,b-1], [a,b) = [a,b-1), (a,b] = [a+1,b].

For iii), note that ∅ is the interval (x,x), and by i), {x} is the interval [x,x].

For iv), note that x·A = {x}·A, and apply set multiplication.

For v), Let A be nonempty. Then -A = {-1}·A has a least element x. Clearly -x is the greatest element of A.

For vi), let A be given. Then A □ [min(A),max(A)].

For vii), note that A □ B = A\(A\B). Also note that A □ B = C\(C\A □ C\B), where A,B □ [min(min(A),min(B)), max(max(A),max(B))].

For viii), note that {x_1,...,x_n} = {x_1} □ ... □ {x_n}.

For ix), let A be given. By vi), let A □ [a,b]. Then the set of positive elements of A is A □ [1,b]. The other cases are handled similarly. QED

We write -A for (-1)·A, and A-B for A+(-B).

LEMMA 8.2. Let d ≥ 1 and x be an integer. There exists unique q,r such that x = dq + r and 0 □ r < d.

Proof: For uniqueness, let x = dq + r = dq′ + r′, 0 □ r,r′ < d. Then d(q-q′) + r-r′ = 0, d(q-q′) = r′-r. Hence d|q-q′| = |r′-r| < d. So |q-q′| < 1, and hence q = q′. Therefore 0 = r′-r, and so r = r′.

For existence, fix d,x as given, and first assume x > 0. Let A = {x-dq: q □ [0,x]} = {x} - d·[0,x]. By Lemma 8.1 ix), let A′ be the set of all nonnegative elements of A. Then A′ is nonempty since x-dq > 0 for q = -x. Choose q such that min(A′) = x-dq. Obviously 0 □ x-dq and q □ [0,x].

If q = x then d = 1 and x-dq = 0, in which case we are done. So we can assume that q < x.

Suppose x-dq ≥ d. Then x-d(q+1) ≥ 0 and q+1 □ [0,x], contradicting the choice of q. Hence 0 □ x-dq < d. Set r = x-dq. Then x = dq + r and 0 □ r < d.

We still have to handle the case $x \square 0$. The case $x = 0$ is trivial, and so we assume $x < 0$. Write $-x = dq + r$, $0 \square r < d$. Then $x = d(-q) - r$. If $r = 0$ then we are done, and so we assume $0 < r < d$. Then $x = d(-q-1) + d-r$, $0 \square d-r < d$. QED

LEMMA 8.3. Let $k \geq 0$. The following is provable in FSTZ. For all $r \geq 2$, the elements of $[0,r^{k+1})$ have unique representations of the form $n_0r^0 + \ldots + n_kr^k$, where each n_i lies in $[0,r)$. If $n_0r^0 + \ldots + n_kr^k = m_0r^0 + \ldots + m_kr^k$ and each n_i lies in $(-r/2,r/2)$, then each $n_i = m_i$.

Proof: It is important to note that k is treated as a standard integer.

For uniqueness, suppose $n_0r^0 + \ldots + n_kr^k = m_0r^0 + \ldots + m_kr^k$, where each $n_i,m_i \square [0,r)$. Let i be greatest such that $n_i \neq m_i$. We can assume that $n_i < m_i$. Here we think of i as a standard integer defined by a large number of cases.

Now subtract the second representation from the first. Then we obtain an inequality of the form

$$p_0r^0 + \ldots + p_{i-1}r^{i-1} \geq r^i,$$

where $p_0,\ldots,p_{i-1} \square (-r,r)$.

Note that $p_0r^0 + \ldots + p_{i-1}r^{i-1} \square (r-1)(r^0 + \ldots + r^{i-1}) = r^i-1$. This is the desired contradiction.

The second claim can be established in the same way by subtraction, since any two elements of $(-r/2,r/2)$ must differ by $< r$, and hence at most $r-1$.

For existence, we proceed by external induction on k. The case $k = 0$ is trivial. Suppose existence for all $r \geq 2$ and $x \square [0,r^{k+1})$, has been proved for a given k, where $k \geq 0$. Let $r \geq 2$ and $x \square [0,r^{k+2})$. Write $x = r^{k+1}n_{k+1} + y$, $0 \square y < r^{k+1}$. Note that $0 \square n_{k+1} < r$. By induction hypothesis, write $y = n_0r^0 + \ldots + n_kr^k$, $n_0,\ldots,n_k \square [0,r)$. Then $x = n_0r^0 + \ldots + n_kr^k + r^{k+1}n_{k+1}$, $n_0,\ldots,n^{k+1} \square [0,r)$. QED

Until the end of the proof of Lemma 8.12, we fix a standard integer $k > 0$.

LEMMA 8.4. For all $r > 1$, $S[r] = \{n_0r^0 + n_1r^2 + \ldots + n_ir^{2i} + \ldots + n_kr^{2k}: n_0,\ldots,n_k \square [0,r)\}$ exists. Every element of $S[r]$ is uniquely written in the displayed form.

Proof: $S[r] = [0,r)\cdot r^0 + [0,r)\cdot r^2 + \ldots + [0,r)\cdot r^{2k}$. The second claim follows immediately from Lemma 8.3. QED

For $x \in S[r]$, we write $x[i]$ for n_i in this unique representation.

LEMMA 8.5. For all $r > 1$ and $i \in [0,k]$, $\{x \in S[r]: x[i] = 0\}$ and $\{x \in S[r]: x[i] = 1\}$ exist.

Proof: The first set is

$$[0,r)\cdot r^0 + \ldots + [0,r)\cdot r^{2i-2} + [0,r)\cdot r^{2i+2} + \ldots + [0,r)\cdot r^{2k}.$$

The second set is

$$[0,r)\cdot r^0 + \ldots + [0,r)\cdot r^{2i-2} + r^{2i} + [0,r)\cdot r^{2i+2} + \ldots + [0,r)\cdot r^{2k}.$$ QED

LEMMA 8.6. Let $r > 1$ and $i,j,p \in [0,k]$. Then $\{x \in S[r]: x[i] + x[j] = x[p]\}$ exists.

Proof: Let r,i,j,p be as given. If $i = p$ then $\{x \in S[r]: x[i] + x[j] = x[p]\} = \{x \in S[r]: x[j] = 0\}$. If $j = p$ then $\{x \in S[r]: x[i] + x[j] = x[p]\} = \{x \in S[r]: x[i] = 0\}$. Both of these cases are covered by Lemma 8.5.

We now handle the case $i = j \neq p$. We wish to show that $A = \{x \in S[r]: 2x[i] = x[p]\}$ exists, where $i \neq p$.

Now $D = \{x: (\exists a \in [0,r)(x = ar^{2i} + 2ar^{2p}\}$ exists, since $D = [0,r)\cdot(r^{2i} + 2r^{2p})$.

Let T be the sum of the sets $[0,r)\cdot r^{2q}$, where $q \in [0,k]\backslash\{i\}$. We claim that $A = (D + T) \cap S[r]$.

To see this, obviously every element of A lies in $(D + T) \cap S[r]$. On the other hand, let $x \in (D + T) \cap S[r]$. Write

$$x = ar^{2i} + 2ar^{2p} + y$$

where $a,b \in [0,r)$ and $y \in T$. Since $2a < r^2$, this is the representation of $x \in S[r]$. Evidently, $x \in A$.

We now handle the case $i \neq j \neq p$. We wish to show that $B = \{x \in S[r]: x[i] + x[j] = x[p]\}$ exists.

Now $E = \{x: (\exists a,b \in [0,r))(x = ar^{2i} + br^{2j} + (a+b)r^{2p}\}$ exists, since $E = \{x: (\exists a,b \in [0,r))(x = a(r^{2i} + r^{2p}) + b(r^{2j} + r^{2p}))\} = ([0,r)\cdot(r^{2i} + r^{2p}) + [0,r)\cdot(r^{2j} + r^{2p}))$.

Let V be the sum of the sets $[0,r)\cdot r^{2q}$, where $q \in [0,k]\backslash\{i,j,p\}$. We claim that $B = (E + V) \cap S[r]$.

To see this, obviously every element of B lies in $(E + V) \cap S[r]$. On the other hand, let $x \in (E + V) \cap S[r]$. Write

$x = ar^{2i} + br^{2j} + (a+b)r^{2p} + y$

where $a,b \in [0,r)$ and $y \in V$. Since $a+b < r2$, this is the representation of $x \in S[r]$. Evidently, $x \in B$. QED

We define $a|b \leftrightarrow (\exists c)(b = a\cdot c)$.

LEMMA 8.7. For all $r > 1$ and $i,j \in [0,k]$, $\{x \in S[r]: x[i]|x[j]\}$ exists.

Proof: If $i = j$ then $\{x \in S[r]: x[i]|x[j]\} = S[r]$, which is handled by Lemma 8.4. Assume $i \neq j$. We want to prove that $A = \{x \in S[r]: x[i]|x[j]\}$ exists.

Now $E = \{x: (\exists a,b \in [0,r))(x = ar^{2i} + abr^{2j})\}$ exists, since $E = \{x: (\exists a,b \in [0,r))(x = a(r^{2i} + br^{2j}\}\} = [0,r)\cdot(r^{2i} + [0,r)\cdot r^{2j})$.

Let D be the sum of the sets $[0,r)\cdot r^{2q}$, where $q \in [0,k]\backslash\{i,j\}$. We claim that $A = (E + D) \cap S[r]$.

To see this, obviously every element of A lies in $(E + D) \cap S[r]$. On the other hand, let $x \in (E + D) \cap S[r]$. Write

$x = ar^{2i} + abr^{2j} + y$

where $a,b \in [0,r)$ and $y \in D$. Since $ab < r^2$, this is the representation of $x \in S[r]$. Evidently $x \in A$. QED

LEMMA 8.8. For all $r > 1$, $i \in [0,k]$, and $A \subseteq [0,r)$, $\{x \in S[r]: x[i] \in A\}$ exists.

Proof: Note that $\{x \in S[r]: x[i] \in A\}$ is $[0,r)\cdot r^0 + \ldots + [0,r)\cdot r^{2i-2} + A\cdot r^{2i} + [0,r)\cdot r^{2i+2} + \ldots + [0,r]\cdot r^{2k}$. QED

LEMMA 8.9. Let φ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $x_i|x_j$, $x_i \in A_j$, where $i,j,p \in$

$[0,k]$. The following is provable in FSTZ. For all $r > 1$ and $A_0,\ldots,A_k \subseteq [0,r)$, $\{x_0r^0 + \ldots + x_kr^{2k}\colon \varphi \wedge x_0,\ldots,x_k \in [0,r)\}$ exists.

Proof: For atomic φ, this follows from Lemmas 8.4 - 8.8. The propositional combinations are handled by the fact that the subsets of $S[r]$ form a Boolean algebra. QED

LEMMA 8.10. For all $r > 1$, $i \in [0,k]$, and $E \subseteq S[r]$, $\{x \in S[r]\colon (\exists y \in E)(\forall j \in [0,k]\backslash\{i\})(x[j] = y[j])\}$ exists.

Proof: We first claim that $A = \{x \in S[r]\colon (\exists y \in E)(\forall j \in [0,k]\backslash\{i\})(x[j] = y[j])\} \subseteq E + (-r,r)\cdot r^{2i}$. To see this, suppose $x \in S[r]$, $y \in E$, and $\forall j \in [0,k]\backslash\{i\}$, $x[j] = y[j]$. Since the coefficients of r^{2i} in x and y both lie in $[0,r)$, we see that $x-y \in (-r,r)\cdot r^{2i}$. Hence $x \in (-r,r)\cdot r^{2i} + y \subseteq E + (-r,r)\cdot r^{2i}$.

We claim that $A = (E + (-r,r)\cdot r^{2i}) \cap S[r]$. To see this, let $x \in (E + (-r,r)\cdot r^{2i}) \cap S[r]$. Write

$$x = y + a\cdot r^{2i}$$

where $y \in E$ and $a \in (-r,r)$. In this equation, the coefficient of r^{2i} is the coefficient of r^{2i} in y plus a, which must lie in $(-r,2r)$. Hence this must be the representation of $x \in S[r]$. Evidently, x agrees with an element of E (namely y) at all positions other than at r^{2i}. QED

LEMMA 8.11. Let φ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $x_i|x_j$, $x_i \in A_j$, where $i,j,p \in [0,k]$. Let $m \in [1,k]$. Let $\psi = (Q_mx_m \in [0,r))\ldots(Q_kx_k \in [0,r))(\varphi)$. The following is provable in FSTZ. For all $A_0,\ldots,A_k \subseteq [0,r)$, $\{x_0r^0 + \ldots + x_{m-1}r^{2m-2}\colon \psi \wedge x_0,\ldots,x_{m-1} \in [0,r)\}$ exists.

Proof: Here Q_i is $\forall$ or $\exists$. Lemma 8.9 handles φ. Lemma 8.10 handles existential quantifiers. Universal quantifiers are taken care of by relative complementation. QED

LEMMA 8.12. Let $r > 1$, $E \subseteq S[r]$, $i_1 < \ldots < i_p \in [0,k]$, and $x_1,\ldots,x_p \in [0,r)$. Then $\{y \in S[r]\colon y[i_1] = x_1 \wedge \ldots \wedge y[i_p] = x_p\}$ exists.

Proof: Note that this set is $A \cap B_1 \cap \ldots \cap B_p$, where for all $j \in [1,p]$, $B_j = \{y \in S[r]\colon y[i_j] = x_j\} = [0,r)\cdot r^0 + \ldots$

$+ [0,r)\cdot r^{2k}$ where the term with exponent 2j is replaced by $x_j r^{2j}$. QED

We now release the fixed standard integer k. For formulas □ without bound set variables, and integer variables z not in □, Let $□^z$ be the result of relativizing all quantifiers in □ to [-z,z].

LEMMA 8.13. Let □ be a formula without bound set variables whose atomic subformulas are of the form $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $x_i|x_j$, x_i □ A_j. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZ proves that {y □ [0,z]: $□^z$} exists. Also FSTZ proves that {y □ [-z,z]: $□^z$} exists.

Proof: Note that the conclusion should be viewed as a separation principle with parameters (represented by the free variables of □ other than y.

By changing variables, we can assume that y is x_0, the free variables of □ are among $x_0,\ldots,x_{m-1}$, and the quantified variables are among $x_m,\ldots,x_k$. Also replace the relativizations to [-z,z] with relativizations to [0,z], by appropriately modifying the formula.

Now apply Lemma 8.11 with r = z+1. We obtain $\{x_0r^0 + \ldots + x_{m-1}r^{2m-2}$: □′ □ $x_0,\ldots,x_{m-1}$ □ [0,z]}. Now apply Lemma 8.12 with p = m-1, $i_1,\ldots,i_p = 1,\ldots,m-1$, and r = z+1. We obtain {x_0 □ [0,z]: □′} = {y □ [0,z]: $□^z$}.

The second claim follows from the first. QED

LEMMA 8.14. Let □ be a formula without bound set variables whose atomic subformulas are of the form s = t, s < t, s|t, or t □ A_j, where s,t are terms without •. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZ proves that {y □ [-z,z]: $□^z$} exists.

Proof: By inductively introducing existential quantifiers needed to unravel the terms. A bound can be placed on the existential quantifiers introduced which depends only on □ and the value of the bound z. Since the terms do not use •, the expansion stays within the form in Lemma 8.13. QED

Formulas of the form in Lemma 8.14 are called special formulas.

Note that we do not allow · in special formulas. We first need to use Lemma 8.14 to obtain some basic number theory before we can handle · appropriately.

LEMMA 8.15. $x,y \neq 0 \rightarrow \gcd(x,y),\mathrm{lcm}(x,y)$ exist. $x > 1 \rightarrow x$ is divisible by a prime.

Proof: For the first claim, let $x,y \neq 0$. By Lemma 8.14, $\{a \in [1,|xy|]: a|x \wedge a|y\}$ exists. Then $\gcd(x,y)$ is its greatest element. By Lemma 8.14, $\{a \in [1,|xy|]: x|a \wedge y|a\}$ exists. Then $\mathrm{lcm}(x,y)$ is its least element.

For the second claim, let $x > 1$. By Lemma 8.14, $\{p \in [2,x]: p|x\}$ exists. Let p be the least element. Then p is a prime divisor of x. QED

LEMMA 8.16. Suppose $x,y > 1$ and $ax + by = 1$. Then there exists $cx + dy = 1$, where $c \in (0,y)$, $d \in (-x,0)$. Suppose $x,y > 0$ and $ax + by = 1$. Then there exists $cx + dy = 1$, where $c \in [0,y]$, $d \in [-x,0]$.

Proof: Let x,y,a,b be as given. By symmetry we can assume that $a \geq 0$.

Let $A = \{s \in [0,ax]: (\exists t \in [1-ax,0])(x|s \wedge y|t \wedge s + t = 1)\} = \{s \in [0,ax]: (\exists t)(x|s \wedge y|t \wedge s + t = 1)\} = \{s \in [0,ax]$: there is a multiple of x and a multiple of y, which add up to $1\}$. Note that A exists by Lemma 8.14, and A is nonempty since it includes $s = ax$, with $t = by$. Let cx be the least element of A.

Write $cx + dy = 1$. Note that $(c-y)x + (d+x)y = 1$. By the choice of c, $\neg(0 \leq c-y < c)$, and so $c-y < 0$ or $c-y \geq c$. Hence $c \in [0,y)$.

Note that $1 = cx + dy \leq xy + dy = (x+d)y$. Hence $x+d > 0$, and so $d > -x$. Hence $d \in (-x,0]$.

Note that $c \neq 0$ and $d \neq 0$ because of $cx + dy = 1$, $x,y > 1$.

For the second claim, we need only consider the case $(x = 1 \vee y = 1)$. By symmetry, assume $x = 1$. Then take $c = 1$ and $d = 0$. QED

We say that x,y are relatively prime if and only if $x,y \neq 0$ and the only common divisors of x,y are 1 and -1.

LEMMA 8.17. Let x,y be relatively prime. Then there exists a solution to $ax + by = 1$.

Proof: We fix a positive integer t. We wish to show by induction (equivalently, least element principle) that the following holds for every 0 < s □ t. For all 0 < x,y □ s, if x,y are relatively prime then $ax + by = 1$ has a solution.

We need to express this condition by a special formula.

(□x,y □ [-t,t])((0 < x,y □ s □ x,y relatively prime) □ ax + by = 1 has a solution).

(□x,y □ [-t,t])((0 < x,y □ s □ nothing in [1,x] divides both x,y) □ ax + by = 1 has a solution in [-s,s]).

Here we have used Lemma 8.16, which provides a bound on solutions to $ax + by = 1$.

The basis case $s = 1$ is trivial. Suppose true for a fixed $s \geq 1$. Let x,y □ s+1 be relatively prime. We can assume $1 < y < x = s+1$. Write x = qy + r, 0 □ r < y. Since x,y are relatively prime, we have $0 < r < y$.

Note that y,r are relatively prime and positive. Hence by induction hypothesis write $cy + dr = 1$. Now $dx +(c-dq)y = 1$.

We still have to consider the case where x or y is negative. But then we can merely change the sign or signs of one or more of a,b. QED

LEMMA 8.18. Let p be a prime and suppose $p|xy$. Then $p|x$ or $p|y$.

Proof: Let p,x,y be as given. Suppose the contrary. Then $x,y \neq 0$, and p,x are relatively prime, and p,y are relatively prime. By Lemma 8.17, write $ap + bx = 1$, $cp + dy = 1$. Then $apcp + apdy + bxcp + bxdy = 1$. Note that p divides every summand, and so p divides 1, which is a contradiction. QED

LEMMA 8.19. Let x,y be relatively prime and let x,z be relatively prime. Suppose $x|yz$. Then $x = 1$ or -1.

Proof: Let x,y,z be as given. Write ax + by = 1 and cx + dz = 1. Then axcx + axdz + bycx + bydz = 1. Since x divides every summand, x divides 1. Hence x = 1 or -1. QED

LEMMA 8.20. Let x,y be relatively prime and x|yz. Then x|z.

Proof: Let x,y,z be as given. We can assume that z ≠ 0. It suffices to prove this for x,y,z > 0.

Now x/gcd(x,z) divides y(z/gcd(x,z)) via the integer factor yz/x. Also note that x/gcd(x,z) and y are relatively prime.

We claim that x/gcd(x,z) and z/gcd(x,z) are relatively prime. To see this, suppose they have a common factor u > 1. Then gcd(x,z)u is a factor of x and also a factor of z, contradicting that gcd(x,z) is the greatest common factor of x,z.

By Lemma 8.19, x/gcd(x,z) = 1. I.e., gcd(x,z) = x. So x|z. QED

LEMMA 8.21. Let a,b be relatively prime. Then the least positive common multiple of a,b is ab.

Proof: Let a,b be as given, and let x be a positive common multiple of a,b. Write x = ay.

Since b|ay, by see by Lemma 8.20 that b|y. Hence b □ y. Therefore x = ay ≥ ab as required. QED

Lemmas 8.22, 8.23 finally tell us how to handle • appropriately.

LEMMA 8.22. There is a special formula □ with free variables among x,y such that the following is provable in FSTZ. For all z there exists z′ > z such that (□x,y □ [-z,z])($x = y^2$ □ $□^{z'}$).

Proof: Let □ express x+y = lcm(y,y+1). Let z be given. If y □ [-1,0] then gcd(y,y+1) = 1, and hence by Lemma 8.10, lcm(y,y+1) = y(y+1). Therefore (□x,y □ [-z,z]\[-1,0])(□ □ x+y = y(y+1)). Hence (□x,y □ [-z,z]\[-1,0])(□ □ $x = y^2$). The quantifiers in □ can be bounded to an integer z′ that depends only on z.

We still have to modify □ in order to handle [-1,0]. Take □′ to be (□ □ x,y □ [-1,0])   x = y = 0   (x = 1 □ y = -1). QED

LEMMA 8.23. There is a special formula □ with free variables among u,v,w, such that the following is provable in FSTZ. For all z there exists z′ > z such that (□u,v,w □ [-z,z])(u·v = w □ $□^{z'}$).

Proof: Let □ = (□x,y,a,b)(x = y^2 □ y = u+v □ a = u^2 □ b = v^2 □ 2w = x-a-b). Let z be given. Then (□u,v,w □ [-z,z])(u·v = w □ □). Use the □ from Lemma 8.22 to remove the first, third, and fourth displayed equations, to make □ special. The quantifiers can be bounded to z′ > z, where z′ depends only on z. QED

We now extend Lemma 8.14.

LEMMA 8.24. Let □ be a formula without bound set variables whose atomic subformulas are of the form x_i = 0, x_i = 1, x_i+x_j = z, x_i·x_j = x_p, x_i □ A_j. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZ proves that {y □ [-z,z]: $□^z$} exists.

Proof: Let □ be as given. Replace each atomic subformula of the form x·y = z by the □ of Lemma 8.23, with an appropriate change of variables. Call this expansion □. Let z be given. Then there exists z′ > z depending only on z such that for all y □ [-z,z], $□^z$ □ $□^{z'}$. By Lemma 8.14, {y □ [-z′,z′]: $□^{z'}$} exists. Hence {y □ [-z′,z′]: $□^z$} exists. Hence {y □ [-z,z]: $□^z$} exists. QED

LEMMA 8.25. Let □ be a formula without bound set variables. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZ proves that {y □ [-z,z]: $□^z$} exists.

Proof: Let □ be as given, and let z be given. Expand the terms appearing in □ using existential quantifiers. Apply Lemma 8.24 with appropriately chosen z′, where z′ depends only on z and the terms that appear. QED

We now define the class of formulas of FSTZ, $□_0$(Z,fst).

i) every atomic formula of FSTZ is in $□_0$(Z,fst);
ii) if □,□ are in $□_0$(Z,fst), then so are □□, □ □ □, □   □, □ □ □, □ □ □;

iii) if □ is in □$_0$(Z,fst), x is an integer variable, s,t are integer terms, x not in s,t, then (□x □ [s,t])(□) and (□x □ [s,t])(□) are in □$_0$(Z,fst).

LEMAM 8.26. Let □ be in □$_0$(Z,fst). Let $x_1,...,x_k$ be an enumeration without repetition of at least the free variables of □. The following is provable in FSTZ. Let r > 1. Then $\{x_1r^1 + ... + x_kr^k$: $x_1,...,x_k$ □ [0,r) □ □} exists.

Proof: By induction on □. Let □ be atomic. Then this follows from Lemma 8.25. Suppose this is true for □,□ in □$_0$(Z,fst). Let □ be among □□, □ □, □ □ □, □ □ □, □ □ □. Then obviously this holds for □.

Now suppose this holds for □ in □$_0$(Z,fst). Let □ = (□x □ [s,t])(□). Let $x_1,...,x_k$ be an enumeration without repetition of at least the free variables of □. Then $x_1,...,x_k$,x is an enumeration without repetition of at least the free variables of □.

We want to show that

A = $\{x_1r^1 + ... + x_kr^k$: $x_1,...,x_k$ □ [0,r) □ (□x □ [s,t])(□)}

provably exists for all r > 1. We know that

B = $\{x_1r^1 + ... + x_kr^k + xr^{k+1}$: $x_1,...,x_k$,x □ [0,r) □ □}

provably exists for all r > 1. We can define A from B appropriately so that we can simply apply Lemma 8.25. QED

LEMMA 8.27. Let □ lie in □$_0$(Z,fst). Let z be an integer variable that does not appear in □. Then FSTZ proves that {y □ [-z,z]: □} exists.

Proof: From Lemmas 8.25 and 8.26. QED

THEOREM 8.28. FSTZ can be axiomatized as follows.
1. LOID(Z).
2. (□A)(□x)(x □ A □ (y < x < z □ □)), where □ □ □$_0$(Z,fst) and A is not free in □.
3. Every nonempty set has a least element.

Proof: Axiom scheme 2 is derivable from FSTZ by Lemma 8.27. For the other direction, first note that we can derive (□A)(-A exists). Hence every set has a greatest element. Then it is easy to see that finite interval, Boolean difference, set addition, and set multiplication are special cases of axiom scheme 2 above. QED

THEOREM 8.29. FSTZ is a conservative extension of PFA(Z).

Proof: By Theorem 8.28, FSTZ proves PFA(Z). It now suffices to show that any model M of PFA(Z) can be expanded by attaching sets to form a model of FSTZ. Take the sets of integers to be those sets of the form

$\{x \in [-n,n]: \varphi\}$

where φ is a formula in $\Sigma_0(Z)$ with parameters allowed, interpreted in the model M. The verification of FSTZ in the expansion is straightforward. QED

9. FSTZ = FSTZD = FSTZS.

We show that FSTZ is equivalent to two interesting weakenings of FSTZ. These results are of independent interest, and not central to the paper.

The signature of FSTZD is the same as that of FSTZ, which is L(Z,fst). FSTZD = “finite sets of integers with duplication”. The nonlogical axioms of FSTZD are as follows.

1. Linearly ordered commutative ring axioms.
2. Finite interval.
3. Boolean difference.
4. Duplicate set addition.
   $(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(\exists z)(y \in A \wedge z \in A \wedge x = y+z))$.
5. Duplicate set multiplication.
   $(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(\exists z)(y \in A \wedge z \in A \wedge x = y \cdot z))$.
6. Every set has a least and greatest element.

Axiom 4 asserts the existence of A+A, and axiom 5 asserts the existence of A·A.

Lemmas 9.1 - 9.8 refer to provability in FSTZD.

LEMMA 9.1. i)-iii),v)-ix) of Lemma 8.1.

Proof: Straightforward. QED

LEMMA 9.2. Let $A \subseteq [-x,x]$, $x \geq 0$, and $|y| > 3x$. Then A+y exists.

Proof: Let A,x be as given. By Lemma 9.1, let B = A □ {y}. Then B+B is composed of three parts: A+A, A+y, {2y}. We don’t know yet that the second part is a set. Note that A+A □ [-2x,2x] and A+y □ [-x+y,x+y].

First assume y > 0. Note that 2x < -x+y and x+y < 2y. Hence these three parts are pairwise disjoint. Since B+B and the first and third parts exist, clearly the second part exists.

Now assume y < 0. Note that -2x > x+y and -x+y > 2y. Hence these three parts are pairwise disjoint. So the second part exists. QED

LEMMA 9.3. Let A □ [7z/8,9z/8], z > 0, w < -z/2. Then A+w exists.

Proof: Let A,z,w be as given. Let B = A □ {w}. Then B+B is composed of three parts: A+A, A+w, {2w}. Note that A+A □ [7z/4,9z/4] and A+w □ [7z/8 + w,9z/8 + w].

Note that 9z/8 + w < 7z/4. Hence the first two parts are disjoint. Therefore A+w is among B+B\A+A, B+B\A+A □ {2w}, B+B\A+A\{2w}. Hence A+w exists. QED

LEMMA 9.4. A+y exists.

Proof: Let A □ [-x,x], x > 0, and y be given. We can assume that y is nonzero. Write y = z+w, where z > 3x, A+z □ [7z/8,9z/8], w < -z/2. By Lemma 9.2, A+z exists. By Lemma 9.3, A+z+w exists. But A+z+w = A+y.

It remains to show how z,w can be chosen. Set z = 9max(x,|y|). Set w = y-z = y-9max(x,|y|). Note that A+z □ [-x+z,x+z] □ [7z/8,9z/8].

We have only to verify that w < -z/2. I.e., y - 9max(x,|y|) < -9max(x,|y|)/2, which is y < 9max(x,|y|)/x. This follows from x > 0 and y ≠ 0. QED

LEMMA 9.5. A+B exists.

Proof: Let A,B be given. Let A,B □ [-x,x], x ≥ 0. By Lemma 9.2, let C = B+4x. Consider A□C + A□C. This is composed of three parts: A+A, A+C, C+C. We don’t know yet that the second part is a set.

Note that A+A □ [-2x,2x], A+C □ [3x,5x], C+C □ [6x,10x]. Hence these three parts are pairwise disjoint. Since A□C + A□C and the first and third parts exist, clearly the second part exists. I.e., A+C exists.

Observe that A+C = A+B+4x, and so A+B = A+C+-4x, which exists by Lemma 3.4. QED

LEMMA 9.6. -A exists.

Proof: Let A be given. First assume that A □ [1,x], x > 1. Let B = A □ {-1}. Note that B·B = A·A □ {1} □ -A, where we don’t know yet that -A exists. However, -A is disjoint from A·A □ {1}. Hence -A exists.

Now assume that A □ [-x,-1], x > 1. Using Lemmas 9.1 and 9.4, let B = A+-x^3. Consider B□{-1} · B□{-1}. This is composed of three parts: B·B, -B, {1}, where we don’t know yet that -B exists. Note that B·B □ [x^3+1)^2,(x^3+x)^2], -B □ [1+x^3,x+x^3]. Hence the three parts are pairwise disjoint. Therefore -B exists.

Finally, let A be arbitrary. Write A = A^+ □ A^- □ A^0, where A^+ is the positive part of A, A^- is the negative part of A, and A^0 is the 0 part of A, which is {0} if 0 □ A and ∅ if 0 □ A.

Note that -A = -(A^+) □ -(A^-) □ A^0, and so -A exists. QED

LEMMA 9.7. A·x exists.

Proof: First assume A □ [y^2,y^3), y > x > 1. Consider A□{x} • A□{x}. This is composed of three parts: A·A, A·x, {x^2}, where we don’t know yet that A•x exists. Note that A·A □ [y^4,y^6], A·x □ [xy^2,xy^3]. Hence the three parts are pairwise disjoint. Therefore A·x exists.

Now assume A is arbitrary and x > 1. We can choose y > x such that B □ [y^2,y^3], where B is a translation of A. Then B·x exists.

Let A = B+c. Then A·x = (B+c)·x = B·x + {cx}. Therefore A·x exists.

The case x = 0 is trivial. Finally suppose A is arbitrary and x < -1. Then A·x = -(A·-x), and -x > 1. Therefore A·x exists. QED

LEMMA 9.8. A·B exists.

Proof: Let A,B be given. We first assume that A,B □ [1,x], x > 1. Let C = A □ -B. Then C·C exists. Its negative part is obviously A·−B, which therefore exists. Note that A·B = -(A·−B), and therefore A·B exists.

For the general case, write A = A^+ □ A^- □ A^0, B = B^+ □ B^- □ B^0. Then A·B is the union of the nine obvious cross products. There are only three of them that we have to check exist, the other six obviously existing. These are $A^+ \cdot B^-$, $A^- \cdot B^+$, $A^- \cdot B^-$. However, it is easy to see that these are, respectively, -(A·B), -(A·B), A·B, and therefore exist. QED

THEOREM 9.9. FSTZ and FSTZD are equivalent.

Proof: By Lemmas 9.5 and 9.8. QED

We now present another variant of FSTZ which we call FSTZS = "finite sets of integers with scalars and squares". Here we replace A•B in favor of scalar multiplication and squares.

The signature of FSTZS is L(Z,fst). The nonlogical axioms of FSTZS are as follows.

1. Linearly ordered ring axioms.
2. Finite interval.
3. Boolean difference.
4. Duplicate set addition.
5. Scalar multiplication.
   (□B)(□x)(x □ B □ (□y)(y □ A □ x = y·z)).
6. Squares.
   (□A)(□x)(x □ A □ (□y)(0 < y □ y < z □ x = y^2)).
7. Least element.

Axiom 5 asserts that each c·A exists. Axiom 6 asserts that each $\{1^2,2^2,...,n^2\}$, n ≥ 0, exists.

Lemmas 9.10 - 9.27 refer to provability in FSTZS.

LEMMA 9.10. i)-ix) of Lemma 3.1. A+B exists.

Proof: For the first claim, we need only observe that by scalar multiplication, -A exists. From this we obtain that every nonempty set has a greatest element. For the second claim, we can repeat the proof of Lemma 9.5. QED

To show that FSTZS is equivalent to FSTZ, it suffices to prove that A·B exists in FSTZS. We do not know a clean way of doing this. Instead, we recast the proof of Lemma 8.23 for FSTZS in order to derive that A•B exists. Much of the proof will be the same. The key point is to avoid use of | in the auxiliary languages, and instead use a monadic predicate for "being a square".

LEMMA 9.11. Let $d \geq 1$ and x be an integer. There exists unique q,r such that $x = dq + r$ and 0 □ $r < d$.

Proof: See Lemma 9.2. QED

LEMMA 9.12. Let $k \geq 0$. The following is provable in T_2. For all $r \geq 2$, the elements of $[0,r^{k+1})$ have unique representations of the form $n_0r^0 + ... + n_kr^k$, where each ni lies in $[0,r)$. If $n_0r^0 + ... + n_kr^k = m_0r^0 + ... + m_kr^k$ and each n_i lies in $(-r/2,r/2)$, then each $n_i = m_i$.

Proof: See Lemma 9.3. QED

Until the end of the proof of Lemma 8.21, we fix a standard integer $k > 0$.

LEMMA 9.13. For all $r > 1$, $S[r] = \{n_0r^0 + n_1r^2 + ... + n_ir^{2i} + ... + n_kr^{2k}$: $n_0,...,n_k$ □ $[0,r)\}$ exists. Every element of S[r] is uniquely written in the displayed form.

Proof: See Lemma 9.4. QED

LEMMA 9.14. For all $r > 1$ and i □ [0,k], {x □ S[r]: x[i] = 0} and {x □ S[r]: x[i] = 1} exist.

Proof: See Lemma 9.5. QED

LEMMA 9.15. For all $r > 1$ and i,j,p □ [0,k], {x □ S[r]: x[i] + x[j] = x[p]} exists.

Proof: See Lemma 9.6. QED

Note that we cannot use Lemma 9.7 here since it involves multiplication of sets, as opposed to just scalar multiplication of sets.

LEMMA 9.16. For all $r > 1$, i □ $[0,k]$, and A □ $[0,r)$, $\{x$ □ $S[r]: x[i]$ □ $A\}$ exists.

Proof: See Lemma 9.8. QED

LEMMA 9.17. For all $r > 1$ and i □ $[0,k]$, $\{x$ □ $S[r]: x[i]$ is a square$\}$ exists.

Proof: Use Lemma 9.16 with $A = \{1^2,\ldots,r^2\}$. QED

LEMMA 9.18. Let □ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $Sq(x_i)$, x_i □ A_j, where i,j,p □ $[0,k]$. The following is provable in T_4. For all $A_0,\ldots,A_k$ □ $[0,r)$, $\{x_0r^0 + \ldots + x_kr^{2k}$: □ □ $x_0,\ldots,x_k$ □ $[0,r)\}$ exists.

Proof: See Lemma 9.9. $Sq(x_i)$ means "x_i is a square". QED

LEMMA 9.19. For all $r > 1$ and i □ $[0,k]$ and E □ $S[r]$, $\{x$ □ $S[r]$: (□y □ E)(□j □ $[0,k]\backslash\{i\})(x[j] = y[j])\}$ exists.

Proof: See Lemma 9.10. QED

LEMMA 9.20. Let □ be a propositional combination of formulas $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $Sq(x_i)$, x_i □ A_j, where i,j,p □ $[0,k]$. Let m □ $[1,k]$. Let □ = $(Q_mx_m$ □ $[0,r))\ldots(Q_kx_k$ □ $[0,r))$(□). The following is provable in T_4. For all $A_0,\ldots,A_k$ □ $[0,r)$, $\{x_0r^0 + \ldots + x_{m-1}r^{2m-2}$: □ □ $x_0,\ldots,x_{m-1}$ □ $[0,r)\}$ exists.

Proof: See Lemma 9.11. QED

LEMMA 9.21. Let $r > 1$, E □ $S[r]$, $i_1 < \ldots < i_p$ □ $[0,k]$, and $x_1,\ldots,x_p$ □ $[0,r)$. Then $\{y$ □ $S[r]: y[i_1] = x_1$ □ ... □ $y[i_p] = x_p\}$ exists.

Proof: See Lemma 9.12. QED

We now release the fixed standard integer k.

LEMMA 9.22. Let □ be a formula without bound set variables whose atomic subformulas are of the form $x_i = 0$, $x_i = 1$, $x_i+x_j = x_p$, $Sq(x_i)$, x_i □ A_j. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZS proves that {y □ [0,z]: $\square^z$} exists. Also T_4 proves that {y □ [-z,z]: $\square^z$} exists.

Proof: See Lemma 9.13. QED

LEMMA 9.23. Let □ be a formula without bound set variables whose atomic subformulas are of the form s = t, s < t, Sq(t), or t □ A_j, where s,t are terms without •. Let y,z be distinct integer variables, where z does not appear in □. Then FSTZS proves that {y □ [-z,z]: $\square^z$} exists.

Proof: See Lemma 9.14. QED

We call the formulas given in Lemma 9.23, good formulas.

LEMMA 9.24. Let $x = y^2$, y ≥ 0. Then the next square after x is $(y+1)^2$, and this is at most 3x+1.

Proof: Suppose $y^2 < z^2 < (y+1)^2$. We can assume z ≥ 0. Clearly y < z < y+1 since squaring is strictly increasing on the nonnegative integers. For the second claim, first note that y □ x. Then observe that $(y+1)^2 = y^2+2y+1 = x+2y+1$ □ 3x+1. QED

LEMMA 9.25. $x = y^2$ if and only if x is a square and the next square after x is x+2y+1. The next square after x is at most 2x+1.

Proof: The forward direction is by Lemma 9.24. For the reverse direction, let x be a square and the next square after x is x+2y+1. Let $x = z^2$. Then the next square after x is $(z+1)^2$. So $(z+1)^2 = z^2+2y+1 = z^2+2z+1$. Hence y = z. QED

LEMMA 9.26. There is a good formula □ with at most the free variables among x,y, such that the following is provable in FSTZS. For all z there exists z′ > z such that (□x,y □ [-z,z])($x = y^2$ □ $\square^{z'}$).

Proof: Let z be given. We can assume that z ≥ 0. Let □(x,y) be (y ≥ 0 □ Sq(x) □ Sq(x+2y+1) □ (□w)(Sq(w) □ □(x < w < x+2y+1)))). Note that □ expresses that x is a square, y ≥ 0, and x+2y+1 is the next square after x. Note also that when bounded to [-3z+1,3z+1], the meaning remains unchanged. This works for x,y □ [0,z], and can be easily modified to work for x,y □ [-z,z]. QED

LEMMA 9.27. There is a good formula □ with at most the free variables u,v,w, such that the following is provable in FSTZS. For all z there exists z′ > z such that $(\square x,y,z \square [-z,z])(u\cdot v = w \square \square^{z'})$.

Proof: Let z be given. As in the proof of Lemma 3.23, use □ = $(\square x,y,a,b)(x = y^2 \square y = u+v \square a = u^2 \square b = v^2 \square 2w = x-a-b)$ and Lemma 5.26. We can easily bound the quantifiers to an appropriately chosen [-z′,z′]. QED

THEOREM 9.28. FSTZ, FSTZD, FSTZS are equivalent.

Proof: It suffices to show that A·B exists within FSTZS. Let A,B be given, where A,B □ [-z,z]. Then A·B □ $[-z^2,z^2]$, but we don't know yet that A·B exists.

Let z′ be according to Lemma 9.27 for z^2. Then A·B = $\{y \square [-z^2,z^2]: (\square u,v,w)(u \square A \square v \square B \square \square^{z'})\} = \{y \square [-z^2,z^2]: (\square u,v,w)(u \square A \square v \square B \square \square)^{z'}\}$ which exists by Lemma 9.23.

The second claim follows immediately from the first. QED

10. FSQZ.

We now give a very simple interpretation of FSTZ in FSQZ, which is the identity on the Z sort. It follows immediately that FSQZ proves PFA(Z). We then show that FSQZ is a conservative extension of PFA(Z).

Recall the axioms of FSQZ.

1. Linearly ordered integral domain axioms.
2. lth(□) ≥ 0.
3. val(□,n)□ □ 1 □ n □ lth(□).
4. The finite sequence (0,...,n) exists.
5. lth(□) = lth(□) □ -□,□+□,□·□ exist.
6. The concatenation of □,□ exists.
7. For all n ≥ 1, the concatenation of □, n times, exists.
8. There is a finite sequence enumerating the terms of □ that are not terms of □.
9. Every nonempty finite sequence has a least term.

The interpretation of the integer part is the identity. The interpretation of the sets of integers in T_0 are the sequences of integers in FSZ. The □ relation is interpreted as n □ x if and only if n is a term of □.

We write (n upthru m) for the finite sequence □, if it exists, such that

i. lth(□) = max(0,m-n+1).
ii. For all 1 □ i □ lth(□), val(□,i) = n+i-1.

LEMMA 10.1. The empty sequence exists. For all n, (n) exists.

Proof: The empty sequence is from axiom 9 of FSQZ.

Clearly (0) exists by axiom 5. Let n > 0. Form (0,...,n-1),(0,...,n) by axiom 5, and delete the latter from the former by axiom 9, to obtain (n). If n < 0 then form (-n), and then form (n) by axiom 6. QED

LEMMA 10.2. For all n there is a sequence consisting of all n's of any length ≥ 0.

Proof: Let n be given. Form (n) by Lemma 10.1. Let k ≥ 1. The sequence consisting of all n's of length k is obtained by axiom 8. QED

LEMMA 10.3. For all n,m, (n upthru m) exists. The interpretation of Finite Interval holds.

Proof: Let n,m be given. We can assume that n □ m. By axiom 5, form (0,...,m-n). By Lemma 10.2, form (n,...,n) of length m-n+1. By axiom 6, form (0,...,m-n) + (n,...,n) = (n upthru m). QED

LEMMA 10.4. The interpretation of Boolean Difference holds.

Proof: Let x,y be given. By axiom 9, we obtain the required sequence. QED

LEMMA 10.5. The interpretation of Least Element holds.

Proof: Let □ be nonempty. Apply axiom 10. QED

We now come to the most substantial part of the verification - Set Addition and Set Multiplication.

We first need to derive QRT = quotient remainder theorem. This asserts that

for all d ≥ 1 and n, there exists unique q,r
such that n = dq+r □ 0 □ r < d.

LEMMA 10.6. For all d ≥ 1 and n, there is at most one q,r such that n = dq+r.

Proof: Let d ≥ 1, dq+r = dq′+r′, and 0 □ r,r′ < d. Then d(q-q′) = r′-r. Suppose q ≠ q′. By discreteness, |q-q′| ≥ 1, and so |d(q-q′)| ≥ d. However, |r′-r| < d. This is a contradiction. Hence q = q′. Therefore r′-r = 0, r = r′. QED

LEMMA 10.7. Let d ≥ 1 and n ≥ d. There is a greatest multiple of d that is at most n.

Proof: By Lemma 10.3, form (d,d,...,d) of length n. By Lemma 10.3 and axiom 6, form (1,2,...,n)·(d,...,d) = (d,2d,...,dn) of length n. By Lemma 10.3 and axiom 5, form (n,...,n) and (-d,-2d,...,-dn). By axiom 5 form (n-d,n-2d,...,n-dn).

We now wish to delete the negative terms from (n-d,n-2d,...,n-dn). If n-dn ≥ 0 then there is nothing to delete. Assume n-dn < 0. Obviously, the negative terms of (n-d,n-2d,...,n-dn) are in [n-dn,-1]. Form -(1,...,dn-n) by Lemma 10.3 and axiom 6. By axiom 9, delete -(0,...,dn-n) from (n-d,n-2d,...,n-dn). The result lists the nonnegative n-id, 1 □ i □ n. By axiom 10, let n-id be least among the nonnegative n-id with 1 □ i □ n. Then id is the greatest multiple of d that is at most n. QED

LEMMA 10.8. The Quotient Remainder Theorem holds.

Proof: Let d ≥ 1 and n be given.

case 1. n ≥ d. By Lemma 10.7, let dq be the greatest multiple of d that is at most n. Then n-dq ≥ 0. If n-dq ≥ d, then d(q+1) = dq+d is a greater multiple of d that is at most n. This is a contradiction. Hence 0 □ n-dq < d, and set r = n-dq.

case 2. 0 □ n < d. Set q = 1, r = n.

case 3. –d □ n < 0. Set q = -1, r = n+d.

case 4. n < -d. Then –n > d. By case 1, write –n = dq+r, where 0 □ r < d. Then n = d(-q)-r = d(-q-1)+d-r, and 0 < d-r □ d. If r = 0 write n = d(-q)+0. Otherwise write n = d(-q-1)+d-r, 0 < d-r < d.

QED

LEMMA 10.9. Let lth(□) = n and m be given. The sequence $□^{(m)}$ given by axiom 8 is unique and has the same terms as □.

Proof: Recall from axiom 8 that $□^{(m)}$ has length nm, and for all q,r with 0 □ q < m □ 1 □ r □ n, val($□^{(n)}$,n·q+r) = val(x,r))).

According to the QRT, this defines all values at all positions of $□^{(m)}$. Thus $□^{(m)}$ is unique and obviously has the same terms as x. QED

LEMMA 10.10. Let lth(□) = n+1 and lth(□) = n, where n ≥ 1. Let $□^{(n)}$ and $□^{(n+1)}$ be given by axiom 8. For all 1 □ i □ j □ n, val($□^{(n)}$,jn-in+j) = val(□,i) and val($□^{(n+1)}$,jn-in+j) = val(□,j).

Proof: Let □,n,i,j be as given. Note that jn-in+j = (j-i)(n+1)+i = (j-i)(n)+j. Since 0 □ j-i < n,

val($□^{(n)}$,jn-in+j) = val($□^{(n)}$,(j-i)(n+1)+i) = val(□,i).
val($□^{(n+1)}$,jn-in+j) = val($□^{(n+1)}$,(j-i)(n)+j) = val(□,j).

QED

LEMMA 10.11. Let □,□ be nonempty. There exists □,□ such that
i. □,□ have the same terms.
ii. □,□ have the same terms.
iii. lth(□) = lth(□)+1.
iv. Let a be a term of □ and b be a term of □. Then there exists 1 □ i □ j < lth(□) such that val(□,i) = a and val(□,j) = b.

Proof: Let □,□ be nonempty, lth(□) = n, lth(□) = m. Let u be the last term of □ and v be the last term of □. Let □′ be □u^m, and □′ = □v^n, where here multiplication is concatenation. Then lth(□′) = lth(□′), □′ has the same terms as □, and □′ has the same terms as □. Finally, let □ = □′□′u, and □ = □′□′. Obviously lth(□) = lth(□+1). Clearly every term in □ is a term of the first □′ in □′□′u, and every term in □ is a term in the second □′ in □′□′. We never have to use the last term of □ since the last two terms of

□’ are the same. QED

LEMMA 10.12. The interpretations of Set Addition and Set Multiplication hold.

Proof: Let □,□ be given. We can assume that □,□ are nonempty. Let □,□ be as given by Lemma 10.11, say with lengths n+1,n. Let a be a term of □ and b be a term of □. By Lemma 10.11, there exists 1 □ i □ j □ n such that val(□,i) = a and val(□,j) = b. By Lemma 10.10, there exists k such that val(□$^{(n)}$,k) = a and val(□$^{(n+1)}$,k) = b. Hence

a+b is a term of □$^{(n)}$+□$^{(n+1)}$.
a·b is a term of □$^{(n)}$·□$^{(n+1)}$.

On the other hand, by Lemma 10.9, □$^{(n)}$ has the same terms as □ and □$^{(n+1)}$ has the same terms as □. Hence

i. the terms of □$^{(n)}$+□$^{(n+1)}$ are exactly the result of summing a term of □ and a term of □.
ii. the terms of □$^{(n)}$·□$^{(n+1)}$ are exactly the result of multiplying a term of □ and a term of □.

Thus

iii. □$^{(n)}$+□$^{(n+1)}$ witnesses Set Addition for □,□.
iv. □$^{(n)}$·□$^{(n+1)}$ witnesses Set Multiplication for □,□.

QED

THEOREM 10.14. The interpretation of every axiom of FSTZ is a theorem of FSQZ.

Proof: By Lemmas 10.3, 10.4, 10.7, and 5.12. QED

THEROEM 10.15. FSQZ proves PFA(Z).

Proof: Since the interpretation of FSTZ in FSQZ used here is the identity on the Z sort, the result follows immediately from Theorem 5.29 and Lemma 10.14. QED

THEROEM 10.16. FSQZ is a conservative extension of PFA(Z).

Proof: By Theorem 10.15, it suffices to expand any model M of PFA(Z) to a model of FSQZ. Use the bounded □$_0$(Z) binary relations of M which are univalent, with domain some {1,...,n}, as the finite sequences. QED

11. Conservative extensions, interpretability, synonymy, and logical strength.

The ten systems of arithmetic considered here are

Q(N), PFA(N), PFA(N) + EXP(N), PFA(N) + CM(N), EFA(N,exp).

LOID(Z), PFA(Z), PFA(Z) + EXP(Z), PFA(Z) + CM(Z), EFA(Z,exp).

These were presented in sections 4,5, and relationships between these twelve systems were established in sections 4,5,6 - especially see Theorem 6.7.

The seven strictly mathematical theories considered here were presented in section 7:

FSTZ, FSQZ, FSTZ + CM(Z), FSQZ + CM(Z), FSTZEXP, FSTZBEXP, FSQZEXP.

Recall that FSTEXP extends FSTZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. The finite set {exp(n,0),...,exp(n,m)} exists.

FSTZEXP’ extends FSTZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. n ≥ 2 □ 0 □ m < r □ exp(n,m) < exp(n,r).
iv. The finite set {exp(n,0)+0,exp(n,1)+1,...,exp(n,m)+m} exists.

FSQZEXP extends FSQZ by

i. exp(n,0) = 1.
ii. m ≥ 0 □ (exp(n,m+1) = exp(n,m)·n □ exp(n,-m-1)↑).
iii. The finite sequence (exp(n,0),...,exp(n,m)) exists.

LEMMA 11.1. FSTZEXP’ proves PFA(Z) + (□n)({exp(n,0),..., exp(n,m)} exists).

Proof: Recall from Theorem 8.28 that FSTZ proves bounded □$_0$(Z,fst) separation:

*) (□A)(□x)(x □ A □ (y < x □ x < z □ □)),

where □ □ $\square_0$(Z,fst) and A is not free in □.

We argue in FSTZEXP’. Fix n ≥ 0. Let A = {exp(n,0)+0,..., exp(n,m+1)+m+1}. Note that for all 0 □ r □ m, the next element of A after exp(n,r)+r is exp(n,r+1)+r+1. Let B be the set of successive differences of elements of A. Then B = {exp(n,r+1)+r+1-(exp(n,r)+r): 0 □ r □ m} = {exp(n,r)+1: 0 □ r □ m}. Hence B -{1} = {exp(n,r): 0 □ r □ m}. QED

We use n^m for the partial exponential function, according to PFA(Z). By [HP98], p. 299, the relation r = n^m is given by a bounded formula in PFA(Z). Note that the relation “r is of the form n^m” is also given by a bounded formula in PFA(Z).

LEMMA 11.2. FSTZEXP’ proves that for n,m ≥ 0, every exp(n,m) is of the form n^r.

Proof: Fix n,m ≥ 0. By Lemma 11.1, let A = {exp(n,0),..., exp(n,m)}. Let B be the set of all elements of A that are not of the form n^r. Let exp(n,t) be the least element of B. Then t > 0 and exp(n,t-1) is of the form n^r. Hence exp(n,t) is of the form n^r. This is a contradiction. QED

LEMMA 11.3. FSTZEXP’ proves n,m ≥ 0 □ exp(n,m) = n^m.

Proof: We can assume that n ≥ 2 and m ≥ 0. Let A = {exp(n,0)+0,...,exp(n,m)+m}. We first show the following. Let exp(n,r-2)+r-2, exp(n,r-1)+r-1 both be of the form n^s+s, where r ≥ 2. Then exp(n,r) = n^r.

ultimately change m to s and s to t.

By Lemma 11.2, write

exp(n,r-2) = n^p.
exp(n,r-1) = n^{p+1}.
n^p+r-2 = n^s+s.
n^{p+1}+r-1 = n^t+t.
s < t.

Hence

n^{p+1}+r-1-(n^p+r-2) = n^{p+1}-n^p+1 = n^t+t-(n^s+s) = n^t-n^s+t-s.

Also by n^p+r-2 = n^s+s, we have p □ s.

case 1. p+1 < t. Then n^{p+1} □ $n^t-n^s < n^t-n^s+t-s = n^{p+1}-n^p+1$ □ n^{p+1}, which is a contradiction.

case 2. t □ p. Then n^t-n^s+t-s □ $n^p-n^p+p-p = 0 < n^{p+1}-n^p+1$, which is a contradiction.

case 3. t = p+1. The only possible case.

So t = p+1, r-1 = t, p = r-2, exp(n,r-2) = 2^{r-2}. Hence exp(2,r) = 2^r.

Next we claim that every element of A is of the form n^s+s. Suppose exp(n,r)+r is the least element of A that is not of the form n^s+s. Clearly r ≥ 2 and exp(n,r-2)+r-2, exp(n,r-2)+r-1 are both of the form n^s+s. By the claim, we have exp(n,r) = 2^r, and so exp(n,r)+r = n^r+r. This is a contradiction.

In particular, exp(n,m-2) and exp(n,m-1) are of the form n^s+s, and so by the claim, exp(n,m) = n^m. QED

LEMMA 11.4. FSTZEXP' is a definitional extension of FSTZ + CM(Z).

Proof: By Lemma 11.3, FSTZEXP' proves FSTZ + "exponentiation is total". Hence FSTZEXP' proves FSTZ + CM(Z). Also, by Lemma 11.3, FSTZEXP' proves exp(n,m) = n^m, defining exp. QED

LEMMA 11.5. FSQZEXP proves n ≥ 0 □ exp(n,m) = n^m.

Proof: By Theorem 10.15, FSQZEXP proves PFA(Z). We now argue in FSQZEXP. Fix n ≥ 0. Let □ be the sequence (exp(n,0),...,exp(n,m)). By using the ring operation axioms of FSQZ, we obtain the sequence □ =

(<0,exp(n,0)>,<1,exp(n,1)>,...,<n,exp(n,m)>)

where <x,y> = $(x+y)^2+x$.

By the separation in Theorem 6.28, and Theorem 10.13, we obtain a sequence □ whose terms comprise the terms of □ which are not of the form <t,n^t>. (Only bounded quantifiers are involved in this construction). Let <k,exp(n,k)> be the least term of □. Then k > 0, and <k-1,exp(n,k-1)> is of the form <t,nt>. I.e., exp(n,k-1) = n^{k-1}. Therefore exp(n,k) =

n^k, and <k,exp(n,k)> is a term of □ of the form <k,n^k>. This is a contradiction. Hence □ is empty. Therefore every term of □ is of the form <t,n^t>. In particular, <m,exp(n,m)> is of the form <t,n^t>. Therefore exp(n,m) = n^m. QED

LEMMA 11.6. FSQZEXP is a definitional extension of FSQZ + CM(Z). FSQZEXP is a conservative extension of EFA(Z,exp).

Proof: The first claim is immediate from Lemma 11.5 and Theorem 10.15. For the second claim, first note that FSQZEXP proves EFA(Z,exp). This is because given any formula in $\square_0$(Z,exp), we can replace all occurrences of exp in favor of internal exponentiation, using Lemma 11.5, thereby obtaining a $\square_0$(Z) formula, to which we can apply induction in PFA(Z) □ FSQZEXP.

Now let M be a model of EFA(Z,exp). We can expand M to M’ by adding the finite sequences, and associated apparatus, that is internal to M. Then M’ |= FSQZEXP. QED

LEMMA 11.7. FSTZEXP is a conservative extension of FSTZ.

Proof: Let M be a model of FSTZ. For n ≥ 0, define exp(0,n) = 1 if n = 0; 0 otherwise, and exp(1,n) = 1. Now let n ≥ 2. Clearly {n^m: m ≥ 0} is unbounded. If n^m exists, define exp(n,m) = n^m. If nm does not exist, m ≥ 0, then define exp(n,m) = 0. Note that the sets {exp(n,0),...,exp(n,m)} are already present in M. Hence (M,exp) is a model of FSTZEXP. QED

LEMMA 11.8. Q(N), FSTZ, FSQZ, FSTZEXP are mutually interpretable.

Proof: Since Q(N) and PFA(Z) are mutually interpretable, it suffices to show that PFA(Z), FSTZ, FSQZ, FSTZEXP are mutually interpretable. Since PFA(Z) is provable in FSTZ, FSQZ, it suffices to show that FSTZ, FSQZ are interpretable in PFA(Z). It therefore suffices to show that FSTZ, FSQZ are interpretable in PFA(N).

Let M be a model of PFA(N). In M, look at the cut I of all n such that the internal 2^n exists. If I is a proper cut, then by cut shortening, we can assume that I forms a model of PFA(N). We can then expand I with all of the internal subsets of I bounded by an element of I, and all of the internal sequences from I whose length is an element of I, and whose terms are bounded by an element of I, to form the required models of FSTZ, FSQZ, FSTZEXP (using the proof of Lemma 11.7) QED

LEMMA 11.9. EFA(N,exp), FSTZ + CM(Z), FSQZ + CM(Z), FSTZEXP', FSQZEXP are mutually interpretable.

Proof: EFA(N,exp) is interpretable in PFA(Z) + CM(Z) by Theorems 5.6 and 6.7, which is provable in FSTZ + CM(Z) and FSQZ + CM(Z) by Theorems 8.28 and 10.15.

FSTZ + CM(Z) is provable in FSTZBEXP by Lemma 11.4. FSQZ + CM(Z) is provable in FSQZEXP by Lemma 11.6.

So it suffices to interpret FSTZBEXP, FSQZEXP in EFA(N,exp). Interpret the finite sets and finite sequences by finite coding in EFA(N,exp). QED

LEMMA 11.10. EFA(N,exp), FSTZ + CM(Z) are synonymous.

Proof: By Theorem 6.7, EFA(N,exp) and EFA(Z,exp) are synonymous. It now suffices to show that EFA(Z,exp), FSTZ + CM(Z) are synonymous.

We interpret EFA(Z,exp) in FSTZ + CM(Z) by preserving the Z sort, and interpreting exp as internal exponentiation in PFA(Z) + CM(Z). We interpret FSTZ + CM(Z) in EFA(Z,exp) by preserving the Z sort and interpreting the finite sets by codes in EFA(Z,exp). Let M be a model of EFA(Z,exp). M will be sent to a model M' of FSTZ + CM(Z) with the same ordered ring, but where exp is gone. Since CM(Z) must still hold, we have an internal exponentiation in M', and so when going back, we recover the old exp. For the other compositional identity, let M be a model of FSTZ + CM(Z). Then the Z part of M is a model of PFA(Z) + CM(Z), and therefore has an internal exponentiation. M is sent to a model M' of EFA(Z,exp), where exp agrees with the internal exponentiation in M. When we go back, we must have the same ordered ring structure, and the sets are those given internally from the ordered ring structure of M.

Thus it suffices to verify that in M, the sets are exactly those sets coded internally in the ordered ring structure of M. By Theorem 8.28, FSTZ proves separation for formulas in □0(Z,fst). We can use this to prove in FSTZ + CM(Z) = FSTZ + EXP(Z) that every set is coded internally in the ordered ring structure, as in the proof of Lemma 11.2. Recall that internal exponentiation is used in that argument to make sure that the induction or separation needed has only bounded quantifiers. QED

We now summarize these results.

THEOREM 11.11. FSTZEXP’, FSQZEXP are definitional extensions of FSTZ + CM(Z), FSQZ + CM(Z), respectively. FSTZEXP is a definitional extension of FSTZ. FSQZEXP is a conservative extension of EFA(Z,exp). EFA(N,exp), FSTZ + CM(Z), FSQZ + CM(Z), FSTZEXP’, FSQZEXP are mutually interpretable. EFA(N,exp), FSTZ + CM(Z) are synonymous. FSTZ, FSQZ, FSTZEXP are conservative extensions of PFA(Z). Q(N), FSQZ, FSTZ, FSTZEXP are mutually interpretable.

COROLLARY 11.12. FSTZ + CM(Z), FSQZ + CM(Z), FSTZEXP, FSTZEXP’, FSQZEXP are strictly mathematical theories with logical strength. I.e., they interpret EFA(N,exp).

12. RM and SRM.

The Reverse Mathematics program originated with [Fr75], [Fr76], and the widely distributed manuscripts [Fr75,76], which refer to some of our earlier insights from 1969 and 1974. Also see [FS00].

RM is the main focus of the highly recommended [Si99]. This book has unfortunately been out of print soon after it appeared, but there are ongoing efforts to have it reprinted.

In RM, the standard base theory, RCA_0, introduced in [Fr76], is not strictly mathematical. However, in RM, we add strictly mathematical statements to RM and classify the resulting theories according to implications, equivalences, and logical strengths.

Often, the formulations of the mathematical statements investigated in RM involve coding. Usually these codings are rather robust, but nevertheless constitute another place where elements that are not of a strictly mathematical nature appear.

Fortunately, there are substantial areas of mathematics and a substantial variety of mathematical statements whose formulations are sufficiently robust to support the vigorously active development of RM. RM has continued to grow very substantially since its inception in the 1970s.

We fully expect an accelerating development of RM for the foreseeable future.

However, there is a much greater body of mathematical activity which is currently not in any kind of sufficiently robust logical form to support an RM treatment. The bulk of the relevant mathematical statements are probably too weak, in terms of logical strength, for an RM development, since RM starts at the logical strength level of PRA (primitive recursive arithmetic). PRA is far stronger, logically, than the nonzero level of logical strength on which this paper is based - that of EFA(N,exp), or equivalently, I□$_0$(exp), and lower.

We view this paper as an introduction to what we call Strict Reverse Mathematics, or SRM.

In SRM, the focus is on theories where all statements are strictly mathematical - including all axioms in any base theory. In a sense, SRM is RM with no base theories at all!

Here we have shown that one can achieve logical strength using only strictly mathematical statements. Without this fundamental fact, there cannot be any SRM.

The major goal of SRM is to rework and extend RM using only strictly mathematical statements. SRM should strive to create sensible logical structure out of a vastly increased range of mathematics, going far beyond what can be analyzed with conventional RM.

An integral part of SRM is to take the standard natural formal systems developed in the foundations of mathematics - whose axioms are very far from being strictly mathematical - and reaxiomatize them with strictly mathematical statements. Such axiomatizations may take the form of conservative extensions or mutually interpretable or synonymous systems, as we have done here for PFA(N) (i.e., I□$_0$), and for EFA(N,exp) (i.e., I□$_0$(exp)).

In this vein, we mention some SRM challenges.

1. Find a strictly mathematical axiomatization of PFA(Z), in its signature L(Z).

2. Find a strictly mathematical axiomatization of PFA(Z) + EXP(Z), in its signature L(Z).

Some work in the direction of 1,2 is contained in [Fr00].

3. Find a strictly mathematical axiomatization of EFA(Z,exp), in its signature L(Z,exp).

4. FSQZ appears to be too weak to be naturally synonymous, or even synonymous, with FSTZ. The same can be said of FSQZ + CM(Z), FSTZ + CM(Z), and also FSQZEXP.

However, we can extend FSQZ to FSQZ# and obtain synonymy. FSQZ# is axiomatized by

1. LOID(Z).
2. Discreteness.
3. lth(□) ≥ 0.
4. val(□,n)□ □ 1 □ n □ lth(□).
5. $\square_0$(Z,fsq) comprehension for finite sequences.
(n ≥ 0 □ (□i)(□!j)(□)) □ (□□)(lth(□) = n □ (□i)(1 □ i □ n □ □[j/val(□,i)])), where □ is a $\square_0$(Z,fsq) formula in which □ is not free.
6. Every sequence of length ≥ 1 has a least term.

The challenge is to give a strictly mathematical axiomatizations of FSQZ#, FSQZ# + EXP(Z), FSQZ#EXP, in their respective signatures L(Z,fsq), L(Z,fsq), L(Z,exp,fsq).

The notion "strictly mathematical" is sufficiently clear to support the SRM enterprise. However, there are still fine distinctions that can be profitably drawn among the strictly mathematical. We have drawn such distinctions in our discussion of the relative merits of FSTZ and FSQZ at the end of section 7.

It is clear from the founding papers of RM, [Fr75,76], [Fr75], [Fr76], that we envisioned a development like SRM. We spoke of raw text, and our original axiomatizations of main base theory RCA$_0$ and our other principal systems WKL$_0$, ACA$_0$, ATR$_0$, and $\square^1_1$-CA$_0$, of RM, were considerably more mathematical than the formally convenient ones that are mostly used today. However, any major development of SRM before that of RM would have been highly premature.

[Fr01] and [Fr05a] are technical precursors of this paper, dealing with FSTZ and FSQZ, respectively. [Fr05] is a preliminary report on SRM, attempting to develop SRM at higher levels of strength, and in many ways goes beyond what we have done very carefully here. However, this earlier work will undergo substantial revisions and upgrading in light of this initial publication.

REFERENCES

[Av03] J. Avigad, Number theory and elementary arithmetic *Philosophia Mathematica* 11:257-284, 2003. http://www.andrew.cmu.edu/user/avigad/

[Be85] M. Beeson, Foundations of Constructive Mathematics, Springer-Verlag (Berlin).

[Bo65] Karel de Bouvere, Synonymous theories, in: The Theory of Models, ed. Addison, Henkin, Tarski, North-Holland, 1965, p. 402-406.

[Fe75] S. Feferman, A language and axioms for explicit mathematics, in Algebra and Logic, Lecture Notes in Mathematics 450, 87-139.

[Fe79] S. Feferman, Constructive theories of functions and classes, in Logic Colloquium '78, North-Holland (Amsterdam), 159-224.

[Fe95] S. Feferman, Definedness, Erkenntnis 43 (1995) 295-320.
http://math.stanford.edu/~feferman/papers/definedness.pdf

[FF02] A. Fernandes and F. Ferreira, The Journal of Symbolic Logic 67, pp. 557-578, 2002.

[Fr75,76] H. Friedman, The Analysis Of Mathematical Texts, And Their Calibration In Terms Of Intrinsic Strength I, April 3, 1975, 7 pages. The Analysis Of Mathematical Texts, And Their Calibration In Terms Of Intrinsic Strength II, April 8, 1975, 5 pages. The Analysis Of Mathematical Texts, And Their Calibration In Terms Of Intrinsic Strength III, May 19, 1975, 26 pages. The Analysis Of Mathematical Texts, And Their Calibration In Terms Of Intrinsic Strength IV, August 15, 1975, 32 pages. The Logical Strength Of Mathematical Statements, October 15, 1975, 1 page. The Logical Strength Of Mathematical Statements I, August, 1976, 20 pages. http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html

[Fr75] H. Friedman, Some Systems of Second Order Arithmeitc and Their Use, Proceedings of the 1974 International Congress of Mathematicians, Vol. 1, (1975), pp. 235-242.

[Fr76] Subsystems of Second Order Arithmetic with Restricted Induction I,II, abstracts, J. of Symbolic Logic, Vol. 1, No. 2 (1976), pp. 557-559.

[Fr80] H. Friedman, A Strong Conservative Extension of Peano Arithmetic, Proceedings of the 1978 Kleene Symposium, North Holland, (1980), pp. 113-122.

[Fr00] H. Friedman, Quadratic Axioms, January 3, 2000, 9 pages, draft.
http://www.math.ohio-state.edu/%7Efriedman/

[Fr01] H. Friedman, Finite reverse mathematics, October 19, 2001, 28 pages, draft.
http://www.math.ohio-state.edu/%7Efriedman/

[Fr05] H. Friedman, Strict reverse mathematics, January 31, 2005, 24 pages, draft.
http://www.math.ohio-state.edu/%7Efriedman/

[Fr05a] H. Friedman, The inevitability of logical strength, May 31, 2005, 13 pages, draft.
http://www.math.ohio-state.edu/%7Efriedman/

[FS00] H. Friedman, S. Simpson), Issues and Problems in Reverse Mathematics, in: Computability Theory and its Applications, Contemporary Mathematics, volume 257, 2000, 127-144.

[HP98] P. Hajek, P. Pudlak, Metamathematics of First-Order Arithmetic, Perspectives in Mathematical logic, Springer, 1998. ISBN 0-387-50632-2, ISBN 3-540-50632-2.

[Ja85] N. Jacobsen, Basic Algebra I, second edition, 1985, Freeman and Company, 499 pages.

[La03] Lambert, Karel, Free logic: Selected essays, Cambridge University Press, 2003.

[La91] Lambert, Karel, (ed.). *Philosophical Applications of Free Logics*, Oxford University Press, 1991.

[MT93] Mainke, K., Tucker, John V., Many-Sorted Logic and

Its Applications, Wiley Professional Computing Series, 1993.

[Pl68] R. A. Pljuskevicus [1968], A sequential variant of constructive logic calculi for normal formulas not containing structural rules, in: The Calculi of Symbolic Logic, I, Proc. of the Steklov Inst. of Mathematics 98, AMS Translations (1971), 175-229.

[Ro52] R.M. Robinson, An essentially undecidable axiom system, Proceedings of the 1950 International Congress of Mathematicians, Cambridge MA, 1952, pp. 729-730.

[Sc68] R. Schock, *Logics Without Existence Assumptions,* Stockholm: Almqvist and Wiksell, 1968.

[Si99] S. Simpson, Subsystems of Second Order Arithmetic, Springer Verlag, 1999.

[Sm82] C. Smorynski, Nonstandard models and related developments. In: Harvey Friedman's Research on the Foundations of Mathematics, North Holland: Amsterdam, 1985, pp. 179-229.

[Tu84] R. Turner, *Logics for Artificial Intelligence*. Ellis Horwood Ltd., 1984. Chapter 8.

[Wa52] Wang, Hao, Logic of Many-Sorted Theories, *The Journal of Symbolic Logic*, Vol. 17, No. 2 (Jun., 1952), pp. 105-116.

[Wi86] A.J. Wilkie, On sentences interpretable in systems of arithmetic,. In: Logic Colloquium '84, North-Holland, 1986. pp. 329-342.

*This research was partially supported by NSF Grant DMS-0245349.