STRICT REVERSE MATHEMATICS
Draft

by
Harvey M. Friedman
Department of Mathematics
The Ohio State University
www.math.ohio-state.edu/~friedman/
January 31, 2005

NOTE: This is an expanded version of my lecture at the special session on reverse mathematics, delivered at the Special Session on Reverse Mathematics held at the Atlanta AMS meeting, on January 6, 2005.

TABLE OF CONTENTS

1. INTRODUCTION.

Reverse Mathematics (RM) is now a well developed area of mathematical logic based on a simple robust setting using the rather sparse (two sorted) language of second order arithmetic with standard model (N,P(N);<,=,0,1,+,•,∈). [Si99] serves as the standard text for RM. Unfortunately, it is currently out of print.

As a consequence of the sparse language, coding is needed to state almost every mathematical statement considered.

Fortunately, a great variety of mathematical statements can be treated with a well controlled system of unproblematic coding mechanisms. Most of these coding mechanisms were already in extensive use in recursion theory.

The coding mechanisms can be considered to be problematic in the context of analysis, as the objects are treated as uncountable in ordinary mathematics. They are problematic in terms of the overarching goal of RM - to analyze the logical structure of mathematics.

Nevertheless, even in analysis, coding mechanisms are in place that support a robust development with a virtually unending supply of attractive problems, independently of wider foundational issues.

By ***Strict Reverse Mathematics*** (SRM), we mean a form of RM relying on no coding mechanisms, where every statement considered must be strictly mathematical. In particular, there is no base theory. We will certainly want to single out certain basic sets of statements and work over them, but these statements must themselves be strictly mathematical.

Around the time we founded RM with [Fr74] and [Fr76], we privately circulated the manuscripts [Fr75a], [Fr75b], and [Fr76a], whose aim was to found SRM.

We did not publish these manuscripts because we rightly felt that they did not present a robust program the way [Fr74] and [Fr76] did, and thought it was best to focus attention on the development of RM.

Nevertheless, there are clear traces of the SRM idea in [Fr74] and [Fr76]. In [Fr76], we set up RCA_0 without the use of complexity classes such as □01 and □$^{0}_{1}$. At the beginning of [Fr74], we wrote

"The questions underlying the work presented here on subsystems of second order arithmetic are the following: What are the proper axioms to use in carrying out proofs of particular theorems, or bodies of theorems, in mathematics? What are those formal systems which isolate the essential principles needed to prove them?

Ultimately, answers to these questions will require use of systems that are not subsystems of second order arithmetic, but have variables ranging over objects such as sets of sets of natural numbers.

Such systems would be needed in order to formalize directly theorems about continuous functions on the reals, or measurable sets of reals. But the language of second order arithmetic is sufficient to formalize directly several fundamental theorems, and is basic among the possible languages relevant to the formalization of mathematics. Furthermore, our preliminary investigations reveal that the most important systems not formalized in the language of second order arithmetic are conservative extensions of those that are. In this way, the systematic study reported here of subsystems of second order arithmetic is a necessary and important step in answering the underlying questions."

Inadvertently, only the first three parts of [Fr75a] were mentioned in the historical account in [FS0O].

Ideally, our goal is to formulate a clear robust setup for SRM which lends itself to an attractive focused development. Relying on the existing advanced development of RM, we rethink SRM from scratch, and we generally do not rely on the attempts in [Fr75a], [Fr75b], and [Fr76a]. However, some of the ideas from these early manuscripts are used here.

It is too early to tell whether a single clear robust setup for SRM is feasible and/or desirable, or whether the SRM enterprise naturally divides itself into several related enterprises and subenterprises, with related goals and subgoals, some of which are RM/SRM hybrids. In this paper, we mostly take the latter approach.

2. UNDERLYING LOGIC OF SRM.

The appropriate underlying logic is many sorted free logic. Free logic (uses undefined terms) avoids ad hoc default values. We use $=, \simeq$ between terms of the same sort. $s \simeq t$ means "s = t or s,t are both undefined". $s\downarrow, s\uparrow$ mean "s is defined", "s is undefined". Variables and constants are always defined. If a term is defined then all of its subterms are defined. If a primitive relation holds of terms, then the terms must be defined.

There are well known complete sets of axioms and rules that modify the usual ones for standard logic.

We will use this underlying logic not only for SRM, but also for hybrid developments involving RM.

We only care about finitely axiomatized theories in a finite relational type.

3. CONSERVATIVE AND EXACT EXTENSIONS, CODING.

Let S,T be theories in many sorted free logic. T is a conservative extension of S iff

i) every theorem of S is a theorem of T;
ii) any model of S is a reduct of a model of T.

T is an exact extension of S iff

i) every theorem of S is a theorem of T;
ii) any model M of T can be uniformly defined in its reduct to L(S), without altering the interpretation of L(S).

This last condition needs explanation. If S,T have the same sorts, then it merely says that T is a definitional extension of S as usual.

Let M' be a model of T and M be the reduct of M to L(S). Suppose M' has sorts $B_1,...,B_p$ not in L(S). We must define, in M', partial functions (of several variables) from the objects of M onto $B_1,...,B_p$, respectively. We must also define, in M, the pullbacks in M of any new relations/constants/functions, whether or not they involve the new sorts. All of these definitions must be uniform; i.e., independent of the choice of M' satisfying T.

It is simplest to disallow parameters in these definitions. Any uniform definitions according to the previous paragraph constitute what we call a coding of T in L(S).

These uniform definitions are called a coding of T in S if and only if they are a coding of T in L(S) with an additional property: for every model M of S, these uniform definitions define an expansion M' of M that is a model of T.

THEOREM 3.1. Let S,T be theories in many sorted free logic, where T is an extension of S. T is an exact extension of S if and only if there is a coding of T in L(S). T is an exact conservative extension of S if and only if there is a coding of T in S. If T is an exact conservative extension of S then all codings of T in L(S) are codings of T in S.

Proof: Left to the reader. QED

Note that conservative extensions may not be exact, and exact extensions may not be conservative, as the following examples indicate.

Let S be any theory. Then {(□x)(□x = x)} is an exact extension of S, but not a conservative extension of S. Let T be the same as S but with a new constant symbol of an existing sort. Then T is a conservative extension of S but T is not an exact extension of S.

To illustrate the relationship between these notions of extension and coding, consider the simple example where we wish to treat the ordered ring of integers over RCA0.

The usual treatment in RM is by coding. We code integers by pairs (n,k), where k is 0 or 1. We think of 0 as + and 1 as -. We define equality on codes by (n,k) ~ (m,k') □ ((n = m □ k = k')   n = m = 0). We define the integer 0 to be (0,0), the integer 1 to be (1,0), and the operations <,+,-,• in the obvious way. We do not need pairs as objects for this purpose. RCA0 proves that this defines a discrete ordered ring.

We now show how this coding is treated in terms of an exact conservative extension T of RCA0.

T has a new sort Z for integers, together with <,0,1,+,-,•. In addition to RCA_0, T has the discrete ordered ring axioms for Z.

So far, we obviously have a conservative extension of RCA0. However, we do not yet have an exact extension. An easy way to see this is to consider any countable model M of RCA_0 expanded by an uncountable discrete ordered ring for the Z sort. There cannot be any partial surjection of several variables from dom(M) onto the uncountable ring.

We can attempt to crudely add to T, a function symbol i:N □ Z with the axiom that it is a bijection. Here we get a uniform partial surjection that works for all models of this T. However, the resulting binary pullback relation i(n) < i(m) is not definable in the reduct to $L(RCA_0)$, uniformly, for all models of this T. In fact, it is easy to construct a model of this T where this binary pullback relation is not definable at all in the reduct to $L(RCA_0)$.

Instead, we add a function symbol i:N → Z with the axioms that i is one-one onto the nonnegative part of Z, and that i preserves <,0,1,+,•. Both axioms will be used below.

For the uniformly defined partial surjection, we imitate the usual coding in RM. In L(T), we define f(n,k) = i(n) if k = 0   n = 0; -i(n) if n ≠ 0 ∧ k = 1; undefined otherwise. Then in all models of T, f is onto Z. The pullbacks of <,0,1,+,−,• restricted to the nonnegative part of Z are obviously definable in the reduct to L(RCA_0), uniformly in the model of T. This relies on the axiom that i preserves <,0,1,+,•. The pullbacks of <,0,1,+,−,• are obviously uniformly definable in the reduct to L(RCA_0) from the pullbacks restricted to the nonnegative part of Z, in all models of T. Hence they are uniformly definable in the reduct to L(RCA_0), in all models of T.

From this example, we see how various nonproblematic codings lend themselves naturally to exact conservative extensions. In fact, various nonproblematic codings can be viewed as codings from T into S, where T is a natural exact conservative extension of S.

We will apply exact extensions to RM as follows. Start with RCA_0. Then make a series of exact extensions which introduce a great many fundamental notions of basic mathematics. The axioms used in the exact extensions are to be fundamental mathematical facts or theorems.

Many of the problematic codings do not obviously lend themselves to such a treatment with exact or exact conservative extensions. Most notably, the usual coding of continuous functions from ¬ into ¬, or even from [0,1] into ¬, in terms of neighborhood conditions, needs to be revisited in these terms.

Inequivalent codings for the same notion are unacceptable in RM. There is always an attempt to pick one over the other.

However, in the exact (conservative) extension framework, codings are technical devices, and not fundamental. So inequivalent codings simply correspond to studying some different exact (conservative) extensions. This is just a special case of investigating alternative mathematical statements; i.e., business as usual.

4. INEVITABILITY OF LOGICAL STRENGTH.

Here we show how to achieve some logical strength under the severe constraint of SRM.

For our purposes, we say that a theory in many sorted free logic has logical strength if and only if the system $I\Sigma_0(\exp)$ is interpretable in it.

We now define three systems FSZ, FSZE, FSZEXP, corresponding to $I\Sigma_0$, $I\Sigma_0 + \exp$, $I\Sigma_0(\exp)$. These three systems consist entirely of strictly mathematical statements used and/or taught by all mathematicians.

For $I\Sigma_0$, $I\Sigma_0 + \exp$, $I\Sigma_0(\exp)$, and other formal systems of arithmetic, consult [HP98]. As pointed out in [HP98], p. 405, in the notes to Chapter V on Bounded Arithmetic, I discussed (an equivalent form of) $I\Sigma_0(\exp)$ in [Fr80], and the published writeup in [Sm82].

FSZ stands for "finite sequences of integers", FSZE for "finite sequences of integers with exponentiation", and FSZEXP for "finite sequences of integers with exponentiation as primitive".

The language of FSZ and FSZE has the sort Z for integers, and the sort Z* for finite sequences of integers. We use $<,0,1,+,-,\bullet$ on Z. We use lth(x) for the length of the sequence x, which is of sort Z. We use val(x,n) for the n-th term of the sequence x, of sort Z. Lengths of sequences are nonnegative, and the terms of sequences are indexed starting with 1.

We first give the axioms for FSZ informally.

1. Discrete ordered ring axioms for Z.
2. $\mathrm{lth}(x) \geq 0$.
3. $\mathrm{val}(x,n)\downarrow \leftrightarrow 1 \leq n \leq \mathrm{lth}(x)$.
4. Two finite sequences are equal if and only if they have the same length and the same terms in the same positions.
5. The finite sequence (0,...,n) exists.
6. $\mathrm{lth}(x) = \mathrm{lth}(y) \rightarrow -x, x+y, x\bullet y$ exist.
7. The concatenation of x,y exists.
8. For $n \geq 1$, the concatenation of x, n times, exists.
9. There is a finite sequence enumerating the terms of x that are not terms of y, in strictly increasing order.

We now give a more formal presentation of FSZ.

1. Discrete ordered ring axioms for Z.
2. lth(x) ≥ 0.
3. val(x,n)□ □ 1 □ n □ lth(x).
4. x = y □ (□n)(val(x,n) □ val(y,n)).
5. (□x)(□k,n)(val(x,k) = n □ 1 □ k □ m □ n = k-1).
6. lth(x) = lth(y) □ (□z)(□n)(val(z,n) □ -val(x,n)) □ (□z)(□n)(val(z,n) □ val(x,n)+val(y,n)) □ (□z)(□n)(val(z,n) □ val(x,n)•val(y,n)).
7. (□z)(□k,n)(val(z,k) = n □ (val(x,k) = n val(y,k-lth(x)) = n).
8. lth(x) = n □ (□y)(lth(y) = n•n □ (□q,r)(0 □ q < n □ 1 □ r □ n □ val(y,n•q+r) = val(x,r))).
9. (□z)((□k,n)(1 □ k < n □ lth(z) □ val(z,k) < val(z,n)) □ (□k)((□n)(val(z,n) = k □ ((□n)(val(x,n) = k) □ □(□n)(val(y,n) = k))).

FSZE is FSZ together with

10. The integers 1,...,n have a positive common multiple. More formally, (□m)(m > 0 □ (□k)(1 □ k □ n □ (□r)(m = k•r))).

THEOREM 4.1. FSZE has logical strength in the sense that I□$_0$(exp) is interpretable in FSZE. In fact, FSZE and I□$_0$(exp) are mutually interpretable.

We would like to say that FSZ is a conservative extension of I□$_0$ and FSZE is a conservative extension of I□$_0$ + exp. However, I□$_0$ lives in the nonnegative integers, and FSZ lies in the integers.

The best way to reconcile this is to define the trivial variants I□$_0$(Z) and I□$_0$(Z) + exp that live in the integers. A sentence is provable in I□$_0$(Z) and I□$_0$(Z) + exp, respectively, if and only if the corresponding sentence with quantifiers ranging over the nonnegative integers is provable in I□$_0$ and I□$_0$ + exp.

THEOREM 4.2. FSZ is a conservative extension of I□$_0$(Z). FSZE is an exact conservative extension of I□$_0$(Z) + exp.

We also use an obvious modification I□$_0$(Z,exp) of I□$_0$(exp).

The language of FSZEXP is L(FSZ) together with the binary operation symbol exp. FSZEXP extends FSZ by

11. $m \geq 1 \rightarrow (\exp(n,0) = 1 \wedge \exp(n,m+1) = n\bullet(\exp(n,m)) \wedge \exp(n,-m)\uparrow)$.
12. (exp(n,1),exp (n,2),...,exp(n,m)) exists.

THEOREM 4.3. FSZEXP is an exact conservative extension of FSZE. FSZEXP is an exact conservative extension of $I\Sigma_0(Z,\exp)$.

These results follow from an earlier version that is considerably less convincing, which uses finite sets of integers instead of finite sequences of integers. See [Fr01].

There may be considerably simpler versions of these results that are yet more convincing. In addition, logical strength may come from different sources. E.g., from continuous mathematics?

5. A STRICTLY MATHEMATICAL EXACT CONSERVATIVE EXTENSION OF RCA_0.

In section 4, we give a strictly mathematical exact conservative extension FSZEXP of $I\Sigma_0(Z,\exp)$. We now give a strictly mathematical exact conservative extension of RCA_0. In fact, we give a common exact conservative extension of FSZEXP and RCA_0.

we first introduce new sorts FCN(Z) for functions from Z into Z, and BFCN(Z) for binary functions from Z into Z. We use app(f,n) and app(g,n,m), where f is of sort FCN(Z) and g is of sort BFCN(Z).

T_1 extends FSZEXP with:

13. Two unary (binary) functions are equal if and only if they have the same values at the same arguments.
14. Unary identity and constant functions exist.
15. Binary addition, subtraction, first and second projections, and constant functions exist.
16. The unary and binary functions are closed under composition. I.e., f(g(x,y)), f(g(x,y),h(x,y)).
17. There exists binary f and unary g,h such that for all x,y, $g(f(x,y)) = x \wedge h(f(x,y)) = y \wedge f(g(x),h(x)) = x$.
18. Every surjective unary function has an inverse.
19. Let f be a unary function and $n,m \in Z$, where $n \geq 1$. Then the finite sequence $(m,fm,ffm,\ldots,f^{(n)}m)$ exists.

20. For all unary f there exists unary g such that each g(n) is the sum of the finite sequence from i = 0 up through i = n of g(n).

Some remarks are in order in connection with 19 and 20. Here 19 is formulated using lth and val. Also 20 asserts that this finite sequence of partial sums exists. In FSZEXP, we define the sum of finite sequences using the following fact that is provable in FSZEXP (nonobvious). Let □ be a finite sequence. There is a unique finite sequence □ of the same length such that val(□,1) = val(□,1), and for all 1 □ i < lth(□), val(□,i+1) = val(□,i)+val(□,i+1).

T_1 is an exact extension of FSRZEXP, but of course not a conservative extension.

T_1 is "essentially" an exact extension of RCA_0. But we need to make a minor extension.

The language of T_2 extends $L(T_1)$ by

i. The sorts N and PN, as in RCA_0.
iii. <,0,1,+,• on N as in RCA_0.
iv. □ between N and PN as in RCA_0.
vi. j:N □ Z.

T_2 extends T_1 by

21. j is onto the nonnegative part of Z.
22. j preserves <,0,1,+,•.
23. The subsets of N are the inverse images by j of the zero sets of functions from Z into Z.
24. Two subsets of N are equal if and only if they have the same elements.

THEOREM 5.1. T_2 is an exact conservative extension of RCA_0, and also of T_1.

6. STRICTLY MATHEMATICAL EXACT CONSERVATIVE EXTENSIONS OF WKL_0, ACA_0, $□^1{}_1$-CA_0.

It is convenient to first extend T_2 by T_3, where $L(T_3)$ extends $L(T_2)$ by

i. The sort PZ, with □ between Z and PZ.
ii. The sort REL(Z) for binary relations on Z, with app(R,n,m).

T_3 extends T_2 by

25. The subsets of Z are the zero sets of $f:Z \rightarrow Z$.
26. The binary relations on Z are the zero sets of $f:Z^2 \rightarrow Z$.
27. Two subsets of Z are equal if and only if they have the same elements.
28. Two binary relations on Z are equal if and only if they agree at all arguments.

THEOREM 6.1. T_3 is an exact conservative extension of RCA_0 and T_2.

Let T_4 extend T_3 by

29. Let $f,g:Z \rightarrow Z$ have no common values. There exists $A \subseteq Z$ such that A includes all values of f and excludes all values of g.

THEOREM 6.1. T_3 is an exact conservative extension of WKL_0.

Let T_4 extend T_3 by

30. The range of every $f:Z \rightarrow Z$ exists.

THEOREM 6.2. T_4 is an exact conservative extension of ACA_0.

Let T_5 extends T_4 by

31. Any two well orderings of Z are comparable.

THEOREM 6.3. T_5 is an exact conservative extension of ATR_0.

Let T_6 extends T_5 by

32. Every linear ordering of Z has a largest well ordered initial segment.

THEOREM 6.4. T_6 is an exact conservative extension of Π^1_1-CA_0.

7. SRM OVER FSZ, FSZE, FSZEXP.

We can use FSZ as a starting point for SRM. As far as statements in the ring of integers are concerned, FSZ is the same as $I\Sigma_0$. There has been considerable investigation of systems between $I\square_0$ and $I\square_0$ + exp. It is known that "every nontrivial Pell equation has a solution" is equivalent to exp over $I\square_0$, and therefore is equivalent to 11 over FSZ (see work of D'Aquino).

However, the status and relative status, over $I\square_0$, of various number theoretic statements is not known. E.g.,

i. Every nonnegative integer is the sum of 4 squares.
ii. Fermat's last theorem for various specific exponents.
iii. There are infinitely many primes. (See Wilkie).
iv. There are infinitely many primes in suitable arithmetic progressions.
v. For all $n \geq 1$, there is a prime in $[n,2n]$.

FSZ also has finite sequences of integers. It does not appear that FSZ proves enough about sequences in order to have a satisfactory weak theory of them. For example, one would like to be able to take the sum of any finite sequence. For this, the natural fact is that the sequence of initial sums of any sequence is a sequence. This is probably not provable in FSZ.

So one would want to consider adding appropriate recursion principles to FSZ, without running into exponentiation. Does that lead to a robust extension of FSZ? If so, one would want to reaxiomatize it in strictly mathematical terms.

We can use FSZE/FSZEXP as a starting point for SRM. These systems seem to be very robust.

A big challenge is to establish my conjecture that $I\square 0$(exp) is sufficient to prove all celebrated theorems of number theory that are appropriately formalized in its language. Above all, this includes FLT. Equivalently, we conjecture that FSZEXP is sufficient to prove all celebrated theorems of number theory that are appropriately formalized in its language. Avigad has written extensively about my conjecture.

There are some simple ways to obtain strong systems over FSZEXP, without introducing infinitary objects. One way to do this within the language of FSZEXP is our block subsequence theorem, [Fr01a].

33. Let $k \geq 1$. There is a longest finite sequence $x_1,\ldots,x_n$ such that there is no $1 \leq i,j \leq n/2$ where $x_i,\ldots,x_{2i}$ is a subsequence of $x_j,\ldots,x_{2j}$.

According to [Fr01a], BST is provable in Σ^0_3 induction but not in Σ^0_2 induction. It is equivalent, over $I\Sigma_0(\exp)$, to the 1-consistency of Σ^0_2 induction. Another form of these results is the following.

THEOREM 7.1. FSZEXP + 33 is provably equivalent to FSZEXP + "every multirecursive function exists".

For stating stronger combinatorial theorems such as various forms of Paris/Harrington and various forms of finite Kruskal's theorem, one wants to have finite multivariate relations. In fact, the addition of finite multivariate relations nicely supports a great deal of finite combinatorics.

So we define FSZEXPREL to extend FSZEXP as follows. We add a sort FREL(Z) for finite multivariate relations on Z. We use dim(R) and app(R,x). FSZEXPREL extends FSZEXP by

34. $\dim(R) \geq 1$.
35. $\mathrm{app}(R,x) \rightarrow \mathrm{lth}(x) = \dim(R)$.
36. The relations of dimension k are given by the sequences of length $n \cdot k$, $(x_1,\ldots,x_{n\cdot k})$, where R holds of exactly the $(x_{n\cdot i+1},\ldots,x_{n\cdot i+k})$, $0 \leq i < k$.

In particular, trees on [1,n] are just certain R of dimension 2. Also finite k-ary functions on Z are just certain R of dimension k+1.

So the state of the art finite forms of Kruskal's theorem and extended Kruskal's theorem all have obvious coding free formalizations in FSZEXPREL. See [Fr02]. When singly added to FSZEXPREL, they have the logical strengths indicated in [Fr02].

The finite forms of Kruskal's theorem, extended Kruskal's theorem, and the graph minor theorem, in terms of finite sequences of trees and graphs, can still be formalized in the language of FSZEXPREL, but if we do so, we are at least arguably breaking the spirit of SRM by using coding. From the point of view of SRM, it is clearly preferable to introduce a new sort for finite sequences of finite multivariate relations on integers.

We can obviously build an appropriate exact conservative extension of FSZEXPREL based on this new sort, together with lth and app, by asserting that the finite sequences of finite multivariate relations on integers correspond to certain finite multivariate relations on integers.

So one appropriate methodology of SRM over FSZEXP emerges. Suppose one wishes to treat a collection of finite mathematical statements. Identify whatever expansion of the language, possibly with new sorts, is appropriate in order to give a coding free formalization of those statements.

More troublesome is the handling of combined sorts. Suppose we want to work with finite sequences of: integers and finite sequences of integers. We want a sort of: integers and finite sequences of integers. Recall that we do not have any general equality relation - just equality in each sort.

The best way to treat such combined sorts is as a disjoint union of copies. Thus we introduce a sort Z+Z* together with embeddings $i:Z \to Z+Z^*$ and $j:Z^* \to Z+Z^*$. We have the axiom that Z+Z* is partitioned into the values of i and the values of j. It is also natural to add unary predicates carving out the values of i and the values of j. We can also add the axioms asserting that i,j preserve the primitive operations and relations on and between Z,Z*.

In the next section, we provide a single sorted basis for finite SRM.

8. FINITE SET THEORY FOR FINITE SRM.

In this section, we discuss how we can obtain a particularly smooth development of finite SRM (at the level of $I\Sigma_0(\exp)$ and higher) by compromising the SRM ideal somewhat.

The compromise is that we use a finite set theory FBTZ (finite base theory over Z) as a base theory. Although formally elegant, FBTZ compromises the SRM ideal on at least two grounds. One is that it is based on hereditarily finite sets (over Z), which is not universally used in mathematics as, say, finite sets of integers. Secondly, it uses the scheme of Δ_0 separation. Nevertheless, it supports finite SRM without coding.

The language of FBTZ is two sorted, with sorts Z and FSET (finite sets). We use $\in$ between Z and FSET, and between FSET and FSET. We also have the ordered ring primitives <,+,-,• on Z.

The axioms of FBTZ are as follows.

1. The ordered ring axioms for Z.
2. Any two sets with the same integer and set elements are equal.
3. For all integers a,b, {x: a < x < b} exists.
4. Every nonempty set of integers has a least element.
5. Pairing.
6. Union.
7. Power set.
8. Δ_0 separation.
9. Every set is in one-one correspondence with some interval (a,b) of integers.

THEOREM 8.1. FBTZ is finitely axiomatizable. FBTZ is mutually interpretable in $I\Delta_0(\exp)$.

It is clear how we can define integer exponentiation in FBTZ in the obvious way using, especially, axioms 7 and 9.

THEOREM 8.2. FBTZ is a conservative extension of $I\Delta_0(Z,\exp)$, using the definition of exp mentioned above.

9. WEAK INFINITE SET THEORY FOR COUNTABLE SRM.

In this section, we discuss how we can obtain a particularly smooth development of countable SRM (at the level of RCA_0 and higher) by compromising the SRM ideal somewhat.

The compromise is that we use a countable set theory CBTZ (countable base theory over Z) as a base theory. Although formally elegant, CBTZ compromises the SRM ideal on at least two grounds. One is that it is based on hereditarily countable sets (over Z), which is not universally used in mathematics as, say, sets of integers. Secondly, it uses variants of the schemes used in RCA_0. Nevertheless, it supports countable SRM without coding.

The language of CBTZ is two sorted, with sorts Z and CSET (countable sets). We use $\in$ between Z and CSET, and between

CSET and CSET. We also have the ordered ring primitives <,+,-,• on Z.

The axioms of CBTZ are as follows.

1. The ordered ring axioms for Z.
2. Any two sets with the same integer and set elements are equal.
3. For all integers a,b, {x: a < x < b} exists.
4. Bounded $□_1$ induction on the integers.
5. Pairing.
6. Union.
7. The set of all finite subsets of any set exists.
8. Bounded $□_1$ separation. Z exists.
9. Every set is in one-one correspondence with Z or some interval (a,b) of integers.
10. Every nonempty set has an epsilon minimal element.

THEOREM 9.1. CBTZ is finitely axiomatizable. CBTZ is mutually interpretable in RCA_0.

It is clear that we can view CBTZ as an extension of RCA_0 by considering quantifiers ranging only over subsets of Z, and also reformulating RCA0 trivially using Z instead of N.

THEOREM 9.2. CBTZ is a conservative extension of RCA_0, using the above remark.

We would not be surprised to see that there are stronger conservative extensions of CBTZ that serve its purpose better. CBTZ is at least a useful step.

10. 3RM - THIRD ORDER ARITHMETIC COMPREHENSION AS A BASE THEORY FOR RM.

We now discuss a form of third order reverse mathematics based on third order arithmetic comprehension.

Third order reverse mathematics is suggested by the awkwardness of and issues raised by coding third order objects as second order objects in RM.

This approach replaces RCA_0 by $3ACA_0$ when considering naturally third order mathematics. The idea is to create a development that shares a lot of the attractive robustness of RM over RCA_0, but where one is much closer to the ideal of SRM in the context of third order objects.

$3ACA_0$ is quite a robust formal system on a par with the robustness of ACA_0. We postpone discussion of $3RCA_0$ until the next section, as the useful robustness is not nearly as clear.

We set up $3ACA_0$ as an extension of ACA_0. The language of $3ACA_0$ extends the language of ACA_0 by a third sort 3FCN for functions from PN into PN. We use function variable notation so that we can build compound terms using these function variables.

The axioms of $3ACA_0$ are as follows.

1. Usual axioms for the discrete ordered semiring N.
2. {n: A}, where A is a formula all of whose quantifiers range over N.
3. We can define F(x) = {n: A(n,x)}, where A is a formula all of whose quantifiers range over N.
4. Every nonempty subset of N has a least element.

Parameters of any three sorts are of course allowed on 2,3.

Obviously real numbers are coded as Dedekind cuts as in ACA_0, and so we can directly talk about functions on the reals.

THEOREM 10.1. $3ACA_0$ is finitely axiomatizable. $3ACA_0$ is a conservative extension of ACA_0. However, $3ACA_0$ is not interpretable in ACA_0. It is interpretable in ACA.

A very large amount of real analysis can be conveniently carried out in $3ACA_0$ without coding, including lots of measure theory.

Of course, the least upper bound principle for nonempty bounded sets of reals lies well beyond $3ACA_0$ and can be nicely reversed. No serious coding involved here.

Also one can nicely analyze closed sets have perfect kernels.

At the ATR_0 level, there are the usual comparability of well ordering statements, but also my

given any two countable sets of reals, one can be pointwise continuously embedded in the other analyzed in one of my two papers in [Si05].

One can directly study metric spaces. The underlying points are subsets of N, and the metric is a (partial) function from PN $\times$ PN into PN. Of course, one can safely identify PN with ¬ in $3ACA_0$. Subsets of and mappings between metric spaces are fine in $3ACA_0$.

One can directly study topology. The underlying points are again subsets of N. One specifies the topology by a basis. A set of points is defined to be open if and only if every element lies in an element of the basis which is included ($\subseteq$) in the set. The basis is a family of sets of points, where the family is indexed by subsets of N. Of course, in the case of Polish spaces, this family is countable and can be indexed by integers. More generally, this allows us to directly handle nonseparable topologies. We can then consider various theorems from topology, especially metrizability theorems.

Measure theory and the theory of Borel sets should form rich arenas of study over $3ACA_0$.

11. 3RM - THIRD ORDER RECURSIVE COMPREHENSION AS A BASE THEORY FOR RM.

An obvious drawback to using $3ACA_0$ for 3RM is that it eliminates any reverse mathematics at levels at WKL_0 and RCA_0. So we should try to work with $3RCA_0$.

It will not be clear just how to go about this without much more study.

12. A COMPREHENSIVE CONSERVATIVE EXTENSION OF PA THAT SUPPORTS CODING FREE RM - THE SYSTEMS ALPO.

ALPO is analysis with the limited principal of omniscience, and is an intuitionistic theory which is classical with regards to quantification over N. The idea is that a large amount of basic mathematics is directly formalizable provided one does not venture into higher types. When one ventures into higher types, one has to be constructive about it.

ALPO has not been revisited to my knowledge in the light of RM.

See [Fr80]. You may also be interested in [Fr77], which is purely intuitionistic.

13. SOME EXACT CONSERVATIVE EXTENSIONS OF RCA_0.

We present some exact conservative extensions of RCA_0. Recall $L(RCA_0)$: sorts **N** and **P(N)**.

Firstly, there are standard definitional extensions that stay within these two sorts. E.g., modular arithmetic, cutoff subtraction, absolute value, min, max, divisibility, exponentiation, etc. This does not raise any issues of concern to us here.

We introduce a new sort **Z** for integers, with the ordered ring symbols 0,1,+,-,•,<. We need the injection $i:N \to Z$. We extend RCA_0 with the discrete ordered ring axioms for Z, that i preserves 0,1,+,•, <, and that i is onto the nonnegative part of **Z**. Call this K_1.

K_1 is an exact conservative extension of RCA_0: use the map from **N** onto **Z** sends 2n to i(n), and 2n+1 to -i(n+1), which is provably surjective in K_1. The pullbacks of the ordered ring primitives of Z are given by obvious definitions in RCA_0 that are provably correct in K_1. Obviously every model of RCA_0 is a reduct of a model of K_1.

We introduce a new sort **Q** for rationals, with the ordered ring symbols 0,1,+,-,•,<. We need the injection $j:\mathbf{Z} \to \mathbf{Q}$. We extend K_1 with the ordered field axioms for **Q**, that j preserves 0,1,+,-,•,<, and that every element of **Q** is the ratio between two values of j. This K_2 is an exact conservative extension of K_1.

We introduce a new sort **P(Z)** for subsets of **Z**. We need $\in$ between **Z** and **P(Z)**. We extend K_2 with extensionality, and the subsets of **Z** are exactly of the form $\{i(n): n \in A\} \cup \{-i(n): n \in B\}$, $A,B \subseteq \mathbf{N}$. This K_3 is an exact conservative extension of K_2.

We introduce a new sort for functions from **N** into **N**, via another exact conservative extension. This is straightforward if we use some specific one-one binary quadratic function from **N** into **N**. But the use of a specific function here is too artificial for our purposes.

There is a good, nontrivial way around this, also introducing other important sorts. We introduce the following new sorts:

a. Unary functions from **Z** into **Z**.
b. Binary functions from **Z** into **Z**.
c. Binary relations on **Z**.

We introduce
d. app(f,x) for unary f and integers x.
e. app(f,x,y) for binary f and integers x,y.
f. hld(R,x,y) for binary R and integers x,y.

We extend K_3 by
i. The unary and binary functions are closed under substitution (a small set of axioms).
ii. Binary +,-,•,max,min are binary functions.
iii. Every surjective unary function has a right inverse.
iv. Every surjective binary function has a right inverse (two unary functions).
v. The inverse image of any subset of **Z** under any unary function is a subset of **Z**.
vi. The inverse image of any subset of **Z** under any binary function is a binary relation on **Z**.
vii. Every total univalent binary relation on **Z** yields a unary function on **Z**.
viii. Ext for all 3 new sorts.

This K_4 is an exact conservative extension of K_3.

We introduce a new sort for functions from **Z** into **Q**. We use app(f,x) for such f and integers x. Extend K_4 with extensionality, and the f:**Z** → **Q** are exactly the ratios of any g:**Z** → **Z** and h:**Z** → **Z**, provided h is nowhere 0. This K_5 is an exact conservative extension of K_4.

We introduce a new sort for subsets of **Q**. We use ∈ between rationals and sets of rationals. We extend K_5 by ext, and the subsets of **Q** are the forward images of subsets of **Z** under any fixed bijection from **Z** onto **Q**. This K_6 is an exact conservative extension of K_5.

We introduce the same new sorts and associated primitives for **Q** that we introduced for **Z** in K_4. We can give an appropriate exact conservative extension K_7 of K_6 relying on the provability in K_6 of a bijection from **Z** onto **Q**.

We introduce a new sort ¬ for real numbers. We use the ordered ring symbols 0,1,+,-,•,< on ¬, and i:Q → ¬. We extend K6 by the ordered field axioms, i is an isomorphism from the ordered field Q into the ordered field ¬, every real number is less than a value of i, and the {q ∈ Q: q < x}, x ∈ ¬, are exactly the left cuts. This K_8 is an exact conservative extension of K_7.

We introduce a new sort for sequences of functions from **Q** into **Q**. We use app(f,n) for such sequences f, where n ∈ **N**. We extend K_7 by ext, and these sequences are given by binary functions from **Q** into **Q** by adjunction. This K_9 is an exact conservative extension of K_8.

We say that a sequence of functions from **Q** into **Q**, $f_0,f_1,\ldots$, locally uniformly converges iff ∃ h:**N** → **N** such that $(\forall n \in \mathbf{N})(\forall q,r \in \mathbf{Q})((i,j > h(n) \wedge q,r \in [-h(n),h(n)] \wedge |q-r| < 1/h(n)) \rightarrow |f_i(q)-f_j(r)| < 1/n)$.

We introduce a new sort for continuous functions from ¬ into ¬. We use app(f,x) for such functions f, where x ∈ ¬. We extend K_9 by ext, and these functions are exactly the pointwise limits of locally uniformly convergent sequences of functions from **Q** into **Q**. This K_{10} is an exact conservative extension of K_9.

We now come to abstract mathematics - e.g., complete separable metric spaces.

Our approach is to first introduce a sort for "abstract points". These are the points used in various countable structures such as countable metric spaces.

We then introduce sorts for points in various kinds of completions of countable structures. In the case in question, we introduce a sort for "points in completions of countable metric spaces". The points used in any completion are disjoint from the points used in any other completion.

Here are some details. We introduce the sort AP for "abstract points". We have a unary function symbol from **P(N)** one-one onto AP. We extend K_{10} with the axiom "the symbol is one-one onto AP". This K_{11} is an exact conservative extension of K_{10}.

We introduce the sort CMS for "countable metric spaces". We have ∈ between abstract points and countable metric spaces

M. We have d(M,x,y) for the distance in M between x,y □ M, where for other pairs of abstract points x,y, d(M,x,y) is undefined. We have the usual metric inequalities. We have "there is a surjection from **N** onto the pullback of the points in M". This K_{12} is an exact conservative extension of K_{11}.

We introduce the sort CMSCP (countable metric space completion points), with a unary function symbol from **P(N)** one-one onto AP. As for K_{11} over K_{10}, we have an exact conservative extension K_{13} over K_{12}.

We introduce a sort for infinite sequences from CMSCP. We obtain an appropriate exact conservative extension K_{14} over K_{13}.

We introduce the sort CCMS for "completion of countable metric spaces". We use a function symbol "completion" from CMS to CCMS, and a function symbol for embeddings of countable metric spaces into their completions. We use □ between CMSCP and CCMS. We use the completion axiom involving infinite sequences from CMSCP. We assert that each CMSCP point lies in a unique completion. We obtain an appropriate exact conservative extension K_{15} over K_{14}.

This development illustrates how we can go about constructing a suitably comprehensive exact conservative extension **E** of RCA_0.

Another approach to continuous functions from $¬^n$ into $¬^m$ is to use the Stone Weierstrass theorem asserting that the continuous functions from $[0,1]^k$ into ¬ are exactly the limits of uniformly converging sequences of polynomials. This requires some exact conservative extensions surrounding polynomials (formal polynomials first, and then their action). There is the drawback that polynomials don't make sense in the metric space context. However, one can try to use the more abstract "separate points" form of the theorem.

14. GENERAL SRM, AND THE INTERPRETABILITY CONJECTURE.

General SRM refers to free form SRM where one is not tied to any base theory, even if that base theory is strictly mathematical. Of course, I am engaging in free form SRM when I try to uncover some good strictly mathematical base theories, as I have tried to here.

SRM is so unexplored and far ranging, that it is important for people to engage in free form SRM, in this sense. Undoubtedly one will uncover rather dramatic findings of two kinds. One is that various simple mathematical statements, when combined (over no base theory), have surprising logical strength. The other is that various large bodies of mathematical statements, when combined, do not have any logical strength.

We have not touched on this second kind of result. One can make at least a start by taking various combinations that have strength and delete or weaken one of the components. This should lead to some very interesting specific problems with novel methods of solution.

We now make our interpretability conjecture. This sort of conjecture is discussed, for example, in [FS00].

Let S,T be finite sets of mathematical statements from the published mathematical literature appearing before 2005, with an AMS classification number that is not under logic. Assume that S,T are appropriately presented in many sorted free logic, reflecting their mathematical meaning. Furthermore, assume that S,T each have logical strength in the sense that $I\Sigma_0(\exp)$ is interpretable in S,T. Then S is interpretable in T or T is interpretable in S.

REFERENCES

[Fr74] H. Friedman, Some systems of second order arithmetic and their use, Proceedings of the International Congress of Mathematicians, Vancouver 1974, vol. 1, Canadian Mathematical Congress, 1975, 235-242.

[Fr75a] H. Friedman, The analysis of mathematical text, and their calibration in terms of intrinsic strength, I-IV, State University of New York at Buffalo, April 3, April 8, May 19, August 15, 1975, 70 pages, privately circulated. www.math.ohio-state.edu/~friedman/

[Fr75b] H. Friedman, The Logical strength of mathematical statements, October 15, 1975, 1 page, privately circulated. www.math.ohio-state.edu/~friedman/

[Fr76] H. Friedman, Systems of second order arithmetic with restricted induction, I,II (abstracts), Journal of Symbolic

Logic 41 (1976), 557-559.

[Fr76a] H. Friedman, The logical strength of mathematical statements 1, State University of New York at Buffalo, August 1976, 20 pages, privately circulated. www.math.ohio-state.edu/~friedman/

[Fr77] H. Friedman, Set Theoretic Foundations for Constructive Analysis, Annals of Mathematics, Vol. 105, (1977), pp. 1-28.

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

[Fr80a], H. Friedman, Translatability and relative consistency II, Ohio State University, September, 1980, 6 pages, privately circulated.

[Fr01] H. Friedman, Finite reverse mathematics, October 19, 2001, 28 pages, draft. www.math.ohio-state.edu/~friedman/

[Fr01a] Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

[Fr02] Internal finite tree embeddings, Reflections on the Foundations of Mathematics: Essays in honor of Solomon Feferman, ed. Sieg, Sommer, Talcott, Lecture Notes in Logic, volume 15, 62-93, 2002, ASL.

[FS00] H. Friedman, S. Simpson, Issues and Problems in Reverse Mathematics, in: Computability Theory and Its Applications, ed. P. Cholak, S. Lempp, M. Lerman, R. Shore, AMS Contemporary Mathematics 257, 2000, 127-144.

[HP98] P. Hajek, P. Pudlak, Metamathematics of First-Order Arithmetic, Perspectives in Mathematical logic, Springer, 1998.

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

[Si05] S. Simpson, Reverse Mathematics, ASL, 2005.

[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.