STRICT REVERSE MATHEMATICS/2

by
Harvey M. Friedman
Distinguished University Professor
of Mathematics, Philosophy, Computer Science Emeritus
Ohio State University
Columbus, Ohio
August 22, 2025
revised August 25, 2025

This first talk focused on SRM for ω based countable mathematics. This second talk focuses on SRM for Z based finite mathematics. I'm giving a third talk on SRM for $\mathfrak{R}$ based analysis. This second talk relies on

[Fr09] H. Friedman, The Inevitability of Logical Strength: strict reverse mathematics, Logic Colloquium '06, ASL, October, 2009.

1. Inevitability of Logical Strength
2. Formalization, sugared predicate calculus
3. SRM for TRUE[0,S,+,<,=] and fragments
4. SRM for PFA
5. SRM for EFA
6. SRM for SEFA
7. Finite SRM for strength

1. INEVITABILITY OF LOGICAL STRENGTH

As you can see from the title there is a big foundational point that is being made in connection with SRM. Is there a way of formalizing mathematics that avoids logical strength and Gödel phenomena entirely, where the consistency problem essentially disappears? Perhaps the logician's way of formalizing mathematics is overkill with its overly general principles, especially infamous logical schemes, and all of this can be avoided. If we just formalize more economically, we can outright prove consistency.

To a large extent this is already refuted by SRM with ETF as discussed in the first lecture. However, one can still "blame" logical strength on that being infinitary mathematics. So it is important to refute this for finite mathematics.

Actually there is a grain of truth in this gross anti foundationalism. RCF and ACF formalize very significant portions of mathematics avoiding Gödel phenomena, and I gave a consistency proof of RCF and ACF in EFA, and showed they were interpretable in Q (Q result also published by Ferreira). Not at all clear how far one can take this. Perhaps the whole of mathematics that isn't somehow combinatorial in nature, but rather algebraic or geometric, can be proved consistent in weak systems. Or perhaps not, shown by spectacular reversals.

2. FORMALIZATION, SUGARED PREDICATE CALCULUS

When we go into formalizing mathematics, we encounter things that are banned from ordinary predicate calculus. Specifically, we need many sorts, undefined terms, function and relation variables, and relativized quantifiers. These are the biggies, and there are more minor things like writing $(\forall x,y)$ and so forth. This is a whole area of sugared predicate calculus. This won't be really important for this lecture although it will be clear that the need for this arises in full formalizations. The reader may perhaps be interested in looking at
https://www.andrew.cmu.edu/user/avigad/Papers/mkm/index.html

Here we can ignore that we should be in free many sorted logic with function and relation variables, although it is illustrated by our presentation of FSQZ in section 4.

The system Q, which already consists of strictly mathematical theorems, will play a role in the discussion here. The signature of Q is $0,S,+,\bullet,<,=$. Q has the nonlogical axioms

Q1. $Sx \neq 0$.
Q2. $Sx = Sy \rightarrow x = y$.
Q3. $x \neq 0 \rightarrow (\exists y)(x = Sy)$
Q4. $x + 0 = x$.
Q5. $x + Sy = S(x + y)$.
Q6. $x \bullet 0 = 0$.
Q7. $x \bullet Sy = (x \bullet y) + x$.
Q8. $x < y \leftrightarrow (\exists z)(z + Sx = y)$.

3. SRM FOR TRUE[...] AND FRAGMENTS

Let ... be a subsequence of the list of five symbols $0,S,+,<,=$. TRUE[...] is the system consisting of all true sentences in the first order language with signature ... . These are 32 systems. Each TRUE[...] is of course very decidable by elimination of quantifiers due to Presburger. We are now in linear arithmetic.

If TRUE[...] is finitely axiomatizable, we look for a logically equivalent theory consisting entirely of strictly mathematical theorems. The rest are not finitely axiomatizable, and we look for T in a strictly mathematical expanded language. What can be required? T consists entirely of finitely many strictly mathematical theorems, L[...] $\subseteq$ L[T], and every sentence in L[...] provable in T is provable in IND[...]. We discuss whether we get even more.

Now let's look at finite axiomatizability of the 32 signatures. If we include + then because of the quotient remainder axioms with the arbitrary standard positive integer divisors, it is not finitely axiomatizable. So we just need to look at subsequences of 0,S,<,=. The presence of 0 makes no difference. So for finite axiomatizability, we need only look at subsequences of S,<,=.

1. ∅. yes
2. S. no.
3. <. yes
4. =. yes
5. S,<. yes
6. S,=. no
7. <,=. yes
8. S,<,=. yes

In each of the 6•2 = 12 cases (we can add 0 back), the finite axiomatization that comes to mind is already entirely composed of strictly mathematical theorems. The cases below remain with non finitely axiomatizable.

1. S and 0,S.
2. S,= and 0,S,=.
3. + together with any of sixteen.

For the four ... in 1,2 we can most simply use 0,S,<,= and get T composed of finitely many strictly mathematical theorems where T proves TRUE[...] and every sentence in L[...] provable in T is provable in TRUE[...]. However, there is no interpretation of T in TRUE[...]. Can we have such a T with an interpretation of T in TRUE[...] which is the identity on L[...] where T is in perhaps a totally different language? Haven't had a chance to think this through.

For 3 we also need to expand the language. Let us work with TRUE[0,S,+,<,=]. We choose T with L[T] = 0,S,+,•,<,= and the axioms
1. Equality axioms for L[T].

2. < is a linear ordering with left endpoint 0, where S returns the immediate successor.
3. Division by each $S^n(0)$ with remainder in [0,n), external n > 0.

We will get that T consists entirely of finitely many mathematical theorems in 0,S,+,•,<,=, T proves TRUE[0,S,+,<,=], and every consequence of T in 0,S,+,<,= is a consequence of TRUE[0,S,+,<,=]. But we can ask for more of T. We won't have an interpretation of T in TRUE[0,S,+,<,=] and it is unclear whether T is decidable. We haven't looked carefully at the other TRUE[...,+].

4. SRM FOR PFA

PFA = $I\Sigma_0$ = polynomial function arithmetic. The signature is 0,S,+,•,<,=.

The Σ_0 formulas are defined as follows.

1. Every atomic formula in 0,S,+,•,<,= is a Σ_0 formula.
2. If φ, ψ are Σ_0 formulas then $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$, $\varphi \leftrightarrow \psi$ are Σ_0 formulas.
3. If φ is Σ_0 and x is a variable not in the term t in 0,S,+,•, then $(\exists x \leq t)(\varphi)$ and $(\forall x \leq t)(\psi)$ are Σ_0, with $\leq$ expanded out.

The nonlogical axioms of PFA are as follows.

1. Q
2. $(\varphi[x/0] \wedge (\forall x)(\varphi \rightarrow \varphi[x/S(x)])) \rightarrow \varphi$
where φ is a Σ_0 formula

We follow the SRM treatment of PFA in [Fr09] with some simplifications and amplifications, that rely on the familiarity of coding in the RM literature/folklore - not in SRM. We first convert PFA with ω (the semiring) to PFA with Z (the ring). We assume from the literature/folklore that we know how to use Z in addition to or instead of ω, in PFA, because of familiar coding. We write these three systems as PFA, PFA[Z], PFA[ω,Z] with signatures $\omega;0,1,+,\bullet,<$ with sort ω, $Z;0_Z,1_Z,+_Z,\bullet_Z,<_Z$ with sort Z, and $\omega,Z;0,1,+,\bullet,<,0_Z,1_Z,+_Z,\bullet_Z,<_Z$ with sorts ω and Z. We write L[ω], L[Z], L[ω,Z] for these three signatures, respectively.

We have no idea how to give any strictly mathematical theory logically equivalent to PFA, PFA[Z], or PFA[ω,Z]. These sorts

L[ω], L[Z], L[ω,Z] are just too impoverished. We do know how to give some SRM treatments of these three. by adding sorts.

To simplify the discussion, let us focus on SRM for PFA[Z]. There are two main approaches in [Fr09]. For the first main approach, way, we add a sort for finite subsets of Z and ep. We write this signature as L[Z,FIN(Z)] = Z,FIN[Z];0_Z,1_Z,$+_Z$,$\bullet_Z$,$<_Z$,∈.

The nonlogical axioms of FSTZ are

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+y: x ∈ A ∧ y ∈ B} exists.
5. Set multiplication. A•B = {x•y: x ∈ A ∧ y ∈ B} exists.
6. Least element. Every nonempty set has a least element.

NOTE: At some places in [Fr09] I wrote the weaker "linearly ordered commutative ring axioms" instead of "linearly ordered integral domain axioms". I am pretty sure I meant the latter, but also it may not make any difference.

THEOREM 4.1. [Fr09]. FSTZ proves PFA[Z]. Every theorem of FSTZ in L[Z] is provable in PFA[Z].

There is a stronger form of Theorem 4.1 that wasn't featured in [Fr09].

THEOREM 4.2. FSTZ proves PFA[Z]. There is an interpretation of FSTZ into PFA[Z] that is the identity on L[Z].

The idea here is to code finite sets of integers as a single integer code. One needs to take care since we don't have exponentiation and so we don't have full finite sequence coding in the usual sense. However, this kind of argument doesn't appear to establish the existence of a faithful interpretation of FSTZ into PFA[Z].

We can adhere to PFA rather than PFA[Z] by using the obvious form of FSTZ that incorporates ω. This extends FSTZ by adding the proper linkage between ω and Z which induces the proper linkage between FIN(ω) and FIN(Z). We write this as FSTZ[ω,Z].

THEOREM 4.3. FSTZ[ω,Z] proves PFA. There is an interpretation of FSTZ[ω,Z] into PFA that is the identity on L[ω]. Moreover, FSTZ[ω,Z] proves PFA[ω,Z]. There is an interpretation of FSTZ[ω,Z] into PFA[ω,Z] that is the identity on L[ω,Z].

For the second main approach, we instead add a sort for finite sequences of integers. We have the ring operations, <, length of a sequence lth(α), and i-th term of sequence α (written α[i]). The signature of FSQZ is $(Z,FSQ[Z];0_Z,1_Z,+_Z,\bullet_Z,<_Z,lth,val)$. The nonlogical axioms of FSQZ are

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

In [Fr09] we see

THEOREM 4.4. [Fr09]. FSQZ proves PFA[Z]. Every theorem of FSQZ in L[Z] is provable in PFA[Z].

Theorems 4.2 and 4.4 are the hard core of [Fr09]. What we talk about below are reworkings of other material from [Fr09], most of which need to be revisited.

There is a stronger form:

THEOREM 4.5. FSQZ proves PFA[Z]. There is an interpretation of FQTZ into PFA[Z] that is the identity on L[Z].

THEOREM 4.6. FSQZ[ω,Z] proves PFA. There is an interpretation of FSQZ[ω,Z] into PFA that is the identity on L[ω]. Moreover, FSQZ[ω,Z] proves PFA[ω,Z]. There is an interpretation of FSQZ[ω,Z] into PFA[ω,Z] that is the identity on L[ω,Z].

5. SRM FOR EFA

EFA = $I\Sigma_0$(exp) = exponential function arithmetic. The signature of EFA is ω;0,S,+,•,exp,<,=. The intended interpretation has exp(n,0) = 1. Here exp is a symbol for binary exponentiation and is to be distinguished from the well known complicated Σ_0

formalization of partial exponentiation (the ternary exponentiation relation) already present in PFA.

The Σ_0(exp) formulas are defined as follows.

1. Every atomic formula in ω;0,S,+,•,exp,<,= is a Σ_0(exp) formula.

2. If φ,ψ are Σ_0 formulas then $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$, $\varphi \leftrightarrow \psi$ are Σ_0(exp) formulas.
3. If φ is Σ_0 and x is a variable not in the term t in 0,S,+,•, then $(\exists x \leq t)(\varphi)$ and $(\forall x \leq t)(\psi)$ are Σ_0(exp) with ≤ expanded out.

We will need to be specific about the defining equations EXP for exp.

$$\text{EXP} = \exp(n,0) = 1,$$
$$\exp(n,m+1) = n \bullet \exp(n,m)$$

The nonlogical axioms of EFA are

Q
EXP
$(\varphi[x/0] \wedge (\forall x)(\varphi \rightarrow \varphi[x/S(x)])) \rightarrow \varphi,$
φ is Σ_0(exp)

We first treat EFA by extending FSTZ and FSQZ with the following strictly mathematical statement.

CM. For all n > 0 the integers 1,...,n have a common nonzero multiple.

THEOREM 5.1. [Fr09]. There is an interpretation of EFA into FSTZ + CM. The same is true of FSQZ.

Theorem 5.1 already establishes the inevitability of logical strength for Z based finite mathematics. The interpretation power of EFA is generally considered the start of logical strength.

At the core of Theorem 5.1 is the following. Let expo[ω], expo[Z] be the standard formalizations of the totality of exponentiation formulated by a Σ_0 ternary relation in L[ω], L[Z] respectively.

THEOREM 5.2. [Fr09]. PFA proves CM ↔ expo[ω]. PFA[Z] proves CM iff expo[Z].

With expo[Z], because it is in L[Z], we get the strong kind of SRM for PFA[Z] + expo[Z].

THEOREM 5.3. There is a faithful interpretation of FSTZ + CM into PFA[Z] + expo[Z] which is the identity on L[Z]. The same holds for FSQZ + CM.

So far we have followed [Fr09]. However we now make new improvements over [Fr09] with regard to SRM for EFA. We are careful to distinguish the two sorted EFA from PFA + expo[ω]. We focus on FSTZ[ω,Z], FSQZ[ω,Z].

We first expand the language of FSTZ[ω,Z] and FSQZ[ω,Z] with the binary function symbol exp from EFA on sort ω and import the defining axioms EXP for exp from EFA. So exp is a binary function symbol new to FSTZ[ω,Z] and FSQZ[ω,Z]. Write these as FSTZ[ω,Z] + EXP and FSQZ[ω,Z] + EXP. We use capital letters to distinguish EXP from the complicated standard Σ_0 formalization of partial exponentiation in PFA.

We certainly do not have FSTZ[ω,Z] + EXP and FSQZ[ω,Z] + EXP proves EFA. The problem is that the binary exp function has not been properly internalized into FSTZ[ω,Z] and FSQZ[ω,Z]. For FSQZ this is straightforward. We write EXPSEQ in L[ω,Z,exp] for the sentence

EXPSEQ = for all n,m there exists sequence x of length m, of sort FSQ[Z], where for all 1 ≤ i ≤ m, x(i) = exp(n,i)

FSQZ[ω,Z] + EXP + EXPSEQ is just what we need for SRM for EFA. We argue in FSQZ[ω,Z] + EXP + EXPSEQ. Fix n,x from EXPSEQ. We have for the x given by EXPSEQ,

1) x(1) = n, and for all 1 ≤ i < m, x(i+1) = n•x(i)
2) for all 1 ≤ i ≤ m, x(i) = n^i
3) for all m, n^m exists and is exp(n,m)

where in 2), we are using the standard Σ_0 formalization of partial exponentiation in PFA. 2) follows from 1) using FSQZ[ω,Z]. 3) follows from 2) using the choice of x. It is now obvious that FSQZ[ω,Z] + EXP + EXPSEQ proves EFA.

THEOREM 5.2. FSQZ[ω,Z] + EXP + EXPSEQ has a faithful interpretation into EFA that is the identity on L[EFA].

This is clear from the above. QED

We now develop such an SRM for EFA extending FSTZ[ω,Z]. EXPSEQ gave a finite sequential internalization of the EXP axioms (defining equations for binary exp). We now give a finite set internalization of the EXP axioms. The most natural way to do this is to add the following two axioms to FSTZ[ω,Z]:

$$\text{EXP} = \exp(n,0) = 1,$$
$$\exp(n,m+1) = n\bullet\exp(n,m),$$

$$\text{EXPSET} = \text{for all } n,m,$$
$$\{\exp(n,i)+i:\ 0 \le i \le m\}$$
$$\text{exists in sort FIN[Z]}$$

Unfortunately we do not know how to make FSTZ[ω,Z] + EXPSET + EXP work. Even just to prove EFA, we use the following modifications.

$$\text{EXP}' = \exp(n,0) = 1,$$
$$\exp(n,m+1) = n\bullet\exp(n,m),$$
$$m < r \to \exp(n+2,m) < \exp(n+2,r)$$

$$\text{EXPSET}' = \text{for all } n,m,$$
$$\{\exp(n,i):0 \le i \le m\},\ \{\exp(n,i)+i:\ 0 \le i \le m\}$$
$$\text{exist in sort FIN[Z]}$$

We work in FSTZ[ω,Z] + CM + EXP' + EXPSET'. For n,m ≥ 0, let A[n,m] = {exp(n,i): 0 ≤ i ≤ m}, B[n,m] = {exp(n,i)+i: 0 ≤ i ≤ m}, which are in sort FSET[Z] by EXPSET'.

LEMMA 5.3. (FSTZ[ω,Z] + CM + EXP' + EXPSET) A[n+2,m] in sort FIN[Z] has the following properties.
1. The least element is 1.
2. The greatest element is exp(n+2,m).
3. If r ∈ A[n+2,m], r < max(A[n+2,m], then (n+3)•r ∈ A[n+2,m].

Proof: 1,2 follows from exp(n+2,0) = 1 and EXP'. For 3, let exp(n+2,i) < exp(n+2,m), i ≤ m. Then i < m and so exp(n+2,i+1) = (n+2)•exp(n+2,i) lies in A[n+2,m]. QED

Using FSTZ + CM, we have enumerations of finite sets of integers. All enumerations are strictly increasing.

LEMMA 5.4. (FSTZ[ω,Z] + CM + EXP' + EXPSET) The enumeration of A[n+2,m] is $(n+2)^0,(n+2)^1,...,(n+2)^r$, for some $0 \leq i \leq r$, formulated using the Σ_0 exponentiation in PFA + CM.

Proof: A[n+2,m] obeys 1,3 in Lemma 5.3. Using FSTZ[ω,Z] + CM we can enumerate A[n+2,m] and apply Σ_0 induction. QED

LEMMA 5.5. (FSTZ[ω,Z] + CM + EXP' + EXPSET') The enumeration of B[n+2,m] is $(n+2)^0+0,(n+2)^1,...,(n+2)^m+m$. The enumeration of A[n+2,m] is $(n+2)^0,n+2)^1,...,(n+2)^m$.

Proof: By Lemma 5.4, the enumeration of B[n+2,m] takes the form

$$(n+2)^{j\_0}+0,(n+2)^{j\_1}+1,...,(n+2)^{j\_m}+m$$

where $0 \leq j_0,...,j_m \leq m$, with each $(n+2)^j \in A[n+2,m]$, using Lemma 5.4. It is easy to see that $0 = j_0 \leq ... \leq j_m = m$, using Lemma 5.3. The $\leq$ are strict because otherwise we would have some j = j' with

$$\begin{gathered}\exp(n+2,j)+i+1 = \exp(n+2,j')+i \\ \exp(n+2,j)+1 = \exp(n+2,j') \\ j = 0,\ j' = 1\end{gathered}$$

violating that each exp(n+2,j) is divisible by n+2 unless j = 0. Also $j_0,...,j_m = 0,...,m$ because of the < and $j_m = m$. Since each $(n+2)^j$ lies in A[n+2,m], we see that A[n+2,m] has the enumeration $(n+2)^0,...,(n+2)^m$. QED

THEOREM 5.6. FSTZ[ω,Z] + CM + EXP' + EXPSET' proves EFA. There is a faithful interpretation of FSTZ + CM + EXP' + EXPSET' which is the identity on L[ETF].

Proof: By Lemmas 5.3 and 5.5, max(A[n+2,m]) = exp(n+2,m) = $(n+2)^m$. This takes care of bases $\geq$ 2. Bases 0,1 are trivial. QED

6. SRM FOR SEFA

SEFA = $I\Sigma_0$(superexp) = superexponential function arithmetic. It's language is based on 0,S,+,•,exp,superexp,<,=. The intended interpretation has superexp(0,n) = n.

The Σ_0(superexp) formulas are defined as follows.

1. Every atomic formula in 0,S,+,•,<,= is a Σ_0(superexp) formula.
2. If φ, ψ are Σ_0 formulas then $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$, $\varphi \leftrightarrow \psi$ are Σ_0(superexp) formulas.
3. If φ is Σ_0(superexp) and x is a variable not in the term t in 0,S,+,•,exp,superexp, then $(\exists x \leq t)(\varphi)$ and $(\forall x \leq t)(\psi)$ are Σ_0(exp,superexp), with $\leq$ expanded out.

The nonlogical axioms of SEFA are
EFA
Defining equations for superexp
$(\varphi[x/0] \wedge (\forall x)(\varphi \rightarrow \varphi[x/S(x)])) \rightarrow \varphi$
where φ is Σ_0(exp,superexp)

As we did SRM for EFA in two ways, we also do SRM for SEFA in two ways, one extending FSQZ[ω,Z] and the other extending FSTZ[ω,Z].

On the function side, we use FSQZ[o,Z] + EXP + SUPEREXP + EXPSEQ + SUPEREXPSEQ, where

SUPEREXP = superexp(n,0) = 1,
superexp(n,m+1) = exp(n,exp(n,m)),

SUPEREXPSEQ = for all n,m there exists sequence x of length m, of sort FSQ[Z], where for all $1 \leq i \leq m$, x(i) = superexp(n,i)

THEOREM 6.1. FSQZ[o,Z] + EXP + EXPSEQ + SUPEREXP + SUPEREXPSEQ has a faithful interpretation into SEFA which is the identity on L[SEFA].

Again the set side is not as easy. We use

SUPEREXP' = superexp(n,0) = 1,
superexp(n,m+1) = exp(n,exp(n,m)),
$m < r \rightarrow$ superexp(n+2,m) < superexp(n+2,r)

SUPEREXPSET' = for all n,m,
{superexp(n,i):$0 \leq i \leq m$}, {superexp(n,i)+i: $0 \leq i \leq m$}
exist in sort FIN[Z]

THEOREM 6.2. FSQZ[ω,Z] + CM + EXP' + EXPSET' + SUPEREXP' + SUPEREXPSET' has a faithful interpretation into SEFA which is the identity on L[SEFA].

7. FINITE SRM FOR STRENGTH

Here we build on FSTZ and FSQZ by introducing finite binary relations on Z and finite sequences of finite binary relations on Z. We then introduce finite rooted trees whose vertices are in Z as certain binary relations on Z. Also introduce the cardinality of finite rooted trees whose vertices are in Z. Then introduce inf preserving embeddings from one finite rooted tree in Z into another. Then state my finite form of Kruskal's theorem. This results in a strictly mathematical theory in Z based finite mathematics of high strength or interpretation power, roughly that of Kruskal's theorem which is proof theoretically measured by $\theta\_\Omega^{\omega}(0)$, and closely corresponds to Π^1_2-TI_0. See

[RW93] M. Rathjen, A. Weiermann, Proof-theoretic investigations on Kruskal's theorem, Annals of Pure and Applied Logic 60(1):49-88(1993).

We can go further with the graph minor theorem corresponding to Π^1_2-CA_0 and proof theoretic ordinal $\theta\_\Omega_\omega(0)$.

Z based finite mathematics is arising from my work on Tangible Incompleteness, and the explicitly Pi01 sentences there are readily used for SRM.