STRICT REVERSE MATHEMATICS

by
Harvey M. Friedman
Ohio State University

November 7, 2009

Reverse Mathematics Workshop
University of Chicago
November 6-8, 2009

The Inevitability of Logical Strength: strict reverse mathematics. Logic Colloquium '06, ASL. October, 2009. Cambridge University Press.

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.

1. Can we get logical strength out of strictly mathematical statements?
2. Can we build appropriate base theories out of strictly mathematical statements?
3. Can we give strictly mathematical versions of my five most basic RM systems?

I basically tried to do this in the unpublished but widely circulated papers leading up to my founding papers of the RM enterprise - the publication of the ICM address given in 1974 and the two JSL abstracts of 1976.

These earlier papers were quite elaborate and evangelical. But the development was premature. They referred to some previous developments (reversals of mine over ACA) that date back to 1969.

I had realized after writing these unpublished papers that matters were not in concise and attractive enough form to be founding a viable subject.

So I consolidated matters and wrote those founding papers - the ICM paper used sets, as is common now, but the ASL abstracts used the most mathematical axiomatizations I could formulate at the time.

More specifically, the most commonly used forms are logically equivalent to both of these early formulations (we now most commonly use sets as opposed to functions). They are considerably less mathematical than my original formulations.

I have recently come back to this issue - and call it STRICT REVERSE MATHEMATICS. I think that some amazing things await us here.

CURRENTLY BIGGEST OPEN PROBLEM IN SRM:

Develop SRM to a point that it competes with RM!

EXTENDING REVERSE MATHEMATICS TO THE UNCOUNTABLE - AND OTHER CONTEXTS

There are issues involved in the extension of RM to the uncountable. Originating with my original founding papers, RM does treat real analysis is a reasonably convincing way through coding back into the countable.

In the unpublished founding papers, I took the issue seriously from the point of view of SRM, taking reals and infinite sequences of reals (and integers) as primitive. The idea even back then was to operate in a coding free fashion.

This definitely needs to be revisited carefully, although here I will not take this aspect of SRM up - but rather some other important aspects.

For each area of mathematics X, there will be SRM of X. The basic concepts of X will be taken as primitive, and purely natural mathematical statements from the practice of X will be used as axioms to be analyzed.

SRM (SRM of X’s) is a far larger and likely far more delicate enterprise, technically, than RM. The foundational significance is rather apparent. The founding papers were scanned and placed on my website a few years ago.

FSTZ = finite sets of integers. FSQZ = finite sequences of integers.
integers, finite sets of integers integers, finite seqs of integers

Well behaved interpretation of FSQZ in FSTZ in PFA (bounded arithmetic, $I\Sigma_0$). Identity on the nonnegative integers.

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

FSQZ - integers and finite sequences of integers. ring operations, <, length of sequence α, i-th term of sequence α (written $\alpha[i]$).

1. Linearly ordered integral domain axioms.
2. $lth(\alpha) \geq 0$.
3. $val(\alpha,n)\downarrow \Leftrightarrow 1 \leq n \leq lth(\alpha)$.
4. The finite sequence (0,...,n) exists.
5. $lth(\alpha) = lth(\beta) \rightarrow -\alpha,\alpha+\beta,\alpha\cdot\beta$ exist.
6. The concatenation of α,β exists.
7. For all $n \geq 1$, 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.

FSTZ

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

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

THEOREM. FSTZ is a weak second order version of bounded arithmetic.

But how to get the scheme of bounded induction?

LEMMA 8.1.

i) $\neg(x < y \wedge y < x+1)$;

ii) (a,b),[a,b),(a,b] exist;

iii) $\emptyset$,{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.

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

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 $n_i = m_i$.

THINK k standard, r general.

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

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.

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.

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

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.

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. $\forall r > 1$ and $A_0, \ldots,A_k \subseteq [0,r)$, $\{x_0r^0 + \ldots + x_kr^{2k}: \varphi \wedge x_0,\ldots,x_k \in [0,r)\}$ exists.

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

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 $\psi = (Q_m x_m \in [0,r))\ldots(Q_k x_k \in [0,r))(\varphi)$. The following is provable in FSTZ. For all $A_0,\ldots,A_k \subseteq [0,r)$, $\{x_0 r_0 + \ldots + x_{m-1} r_{2m-2}: \psi \wedge x_0,\ldots,x_{m-1} \in [0,r)\}$ exists.

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 $\{y \in S[r]: y[i_1] = x_1 \wedge \ldots \wedge y[i_p] = x_p\}$ exists.

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

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

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

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

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

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 $c \in [0,y]$, $d \in [-x,0]$.

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

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

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

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

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

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

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

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

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

We now define the class of formulas of FSTZ, $\Sigma_0(Z,fst)$.
i) every atomic formula of FSTZ is in $\Sigma_0(Z,fst)$;
ii) if φ,ψ are in $\Sigma_0(Z,fst)$, then so are $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$, $\varphi \Leftrightarrow \psi$;
iii) if φ is in $\Sigma_0(Z,fst)$, x is an integer variable, s,t are integer terms, x not in s,t, then $(\forall x \in [s,t])(\varphi)$ and $(\exists x \in [s,t])(\varphi)$ are in $\Sigma_0(Z,fst)$.

LEMAM 8.26. Let φ be in $S_0(Z,fst)$. Let $x_1,...,x_k$ be an enumeration without repetition of at least the free variables of φ. The following is provable in FSTZ. Let $r > 1$. Then $\{x_1r^1 + ... + x_kr^k: x_1,...,x_k \in [0,r) \wedge \varphi\}$ exists.

LEMMA 8.27. Let φ lie in $\Sigma_0(Z,fst)$. Let z be an integer variable that does not appear in φ. Then FSTZ proves that $\{y \in [-z,z]: \varphi\}$ exists.

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.

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

FSQZ - integers and finite sequences of integers. ring operations, <, length, i-th term.

1. Linearly ordered integral domain axioms.
2. $\mathrm{lth}(\alpha) \geq 0$.
3. $\mathrm{val}(\alpha,n)\downarrow \Leftrightarrow 1 \leq n \leq \mathrm{lth}(\alpha)$.
4. The finite sequence $(0,\ldots,n)$ exists.
5. $\mathrm{lth}(\alpha) = \mathrm{lth}(\beta) \rightarrow -\alpha,\alpha+\beta,\alpha\cdot\beta$ exist.
6. The concatenation of α,β exists.
7. For all $n \geq 1$, 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.

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).

The interpretation of the integer part is the identity. The interpretation of the sets of integers in FSQZ are the sequences of integers in FSZ. The $\in$ relation is interpreted as

$$n \in x \text{ if and only if } n \text{ is a term of } a.$$

FSTZ

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

FSQZ

1. Linearly ordered integral domain axioms.
2. $\mathrm{lth}(\alpha) \geq 0$.
3. $\mathrm{val}(\alpha,n)\downarrow \Leftrightarrow 1 \leq n \leq \mathrm{lth}(\alpha)$.
4. The finite sequence (0,...,n) exists.
5. $\mathrm{lth}(\alpha) = \mathrm{lth}(\beta) \rightarrow -\alpha, \alpha+\beta, \alpha\cdot\beta$ exist.
6. The concatenation of α,β exists.
7. For all $n \geq 1$, 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.

Logical strength begins with EFA (exponential function arithmetic, $I\Sigma_0(\exp)$). T has logical strength if and only if EFA is interpretable in T.

CONVENIENT WAYS TO GET LOGICAL STRENGTH FROM FSTZ, FSQZ

FSTZ + "every nonempty set of nonzero integers has a common multiple.
FSQZ + "the terms in every nonempty finite sequence of nonzero integers has a common multiple.
FSQZ + "there is a sequence of every nonzero finite length with starts 1 and where each term is twice the previous term".
Conservative over EFA. Mutually interpretable with EFA.

FINITE SRM

FSQZO

We now go beyond the scope of
The Inevitability of Logical Strength: strict reverse mathematics. Logic Colloquium '06, ASL. October, 2009. Cambridge University Press.

We leverage off of FSQZ + EXP to get FSQ.

1. Variables over integers, objects, and finite sequences of objects. Integers and finite sequences are objects.
2. FSQZ for finite sequences of integers.
3. FSQZ for finite sequences, where it makes sense.
4. Elimination of repetitions in finite sequences.
5. Characterization of the finite sequences whose terms are among a given finite sequence.
6. Characterization of finite sequences of finite sequences using three finite sequences.

FSTSQO

1. Variables over integers, objects, finite sets, and finite sequences. Everything is an object.
2. Extensionality for sets. Sets correspond to ranges of sequences.
3. Sequences of sets correspond to sequences of sequences using ranges.

WHAT ABOUT INFINITE SRM?

Pleasant surprise!

Three sorts: N,Z,SQ. SQ stands for functions from N into Z. Variables n_i over N. Variables x_i over Z. Variables α_i over SQ. +,−,·,<,| |,0,1,=. Also application, α[t], where t is of sort N. This has sort Z.

STRICT RCA_0

1. Appropriate flavor of first order predicate calculus with equality.
2. Discrete ordered ring axioms.
3. Relationship between N and Z. $(\forall x)(x \geq 0 \text{ iff } (\exists n)(x = n))$.
4. Extensionality for sequences..
5. If β is entirely N valued, then α[β[n]] defines a sequence.
6. The constant sequences and the identity sequence exists.
7. Closure of the sequences under addition, multiplication, subtraction.
8. Iteration. If β is entirely N valued, then we can define α[0] = t, α[n+1] = β[α[n]].
9. Every sequence has a term of least magnitude.
10. Every eventually constant sequence has a least term.
11. Let α be unbounded above. Define β[n] = first term of α that is > n.

Outright equivalent to RCA_0 for its language!

Three sorts: N,Z,SQ. SQ stands for functions from N into Z. Variables n_i over N. Variables x_i over Z. Variables α_i over SQ.
$+,-,\cdot,<,| |,0,1,=$. Also application, $\alpha[t]$, where t is of sort N. This has sort Z.

STRICT RCA_0

1. Appropriate flavor of first order predicate calculus with equality.
2. Discrete ordered ring axioms.
3. Relationship between N and Z. $(\forall x)(x \geq 0 \text{ iff } (\exists n)(x = n))$.
4. Extensionality for sequences..
5. If β is entirely N valued, then $\alpha[\beta[n]]$ defines a sequence.
6. The constant sequences and the identity sequence exists.
7. Closure of the sequences under addition, multiplication, subtraction.
8. Iteration. If β is entirely N valued, then we can define $\alpha[0] = t$, $\alpha[n+1] = \beta[\alpha[n]]$.
9. Every sequence has a term of least magnitude.
10. Every eventually constant sequence has a least term.
11. Let α be unbounded above. Define $\beta[n]$ = first term of α that is $> n$.

Outright equivalent to RCA_0 for its language!

STRICT WKL_0

1. Strict RCA_0.
2. For every bit sequence α there exists a bit sequence β such that every finite initial segment of β is extended by some block in α of the form $\alpha[n],\ldots,\alpha[2n]$.

Outright equivalent to WKL_0 for its language!

Three sorts: N,Z,SQ. SQ stands for functions from N into Z. Variables n_i over N. Variables x_i over Z. Variables α_i over SQ.
+,-,·,<,| |,0,1,=. Also application, $\alpha[t]$, where t is of sort N. This has sort Z.

STRICT RCA_0

1. Appropriate flavor of first order predicate calculus with equality.
2. Discrete ordered ring axioms.
3. Relationship between N and Z. $(\forall x)(x \geq 0$ iff $(\exists n)(x = n))$.
4. Extensionality for sequences..
5. If β is entirely N valued, then $\alpha[\beta[n]]$ defines a sequence.
6. The constant sequences and the identity sequence exists.
7. Closure of the sequences under addition, multiplication, subtraction.
8. Iteration. If β is entirely N valued, then we can define $\alpha[0] = t$, $\alpha[n+1] = \beta[\alpha[n]]$.
9. Every sequence has a term of least magnitude.
10. Every eventually constant sequence has a least term.
11. Let α be unbounded above. Define $\beta[n]$ = first term of α that is > n.

Outright equivalent to RCA_0 for its language!

STRICT ACA_0

1-8. As in Strict RCA_0.
9. If α is bounded below, and no term of α appears arbitrarily far out, then α has a permutation which is increasing ($\leq$).

Three sorts: N,Z,SQ. SQ stands for functions from N into Z. Variables n_i over N. Variables x_i over Z. Variables α_i over SQ.
+,-,·,<,| |,0,1,=. Also application, α[t], where t is of sort N. This has sort Z.

STRICT ACA_0

1. Appropriate flavor of first order predicate calculus with equality.
2. Discrete ordered ring axioms.
3. Relationship between N and Z. $(\forall x)(x \geq 0 \text{ iff } (\exists n)(x = n))$.
4. Extensionality for sequences..
5. If β is entirely N valued, then α[β[n]] defines a sequence.
6. The constant sequences and the identity sequence exists.
7. Closure of the sequences under addition, multiplication, subtraction.
8. Iteration. If β is entirely N valued, then we can define α[0] = t, α[n+1] = β[α[n]].
9. If α is bounded below, and no term of α appears arbitrarily far out, then α has a permutation which is increasing (≤).

Outright equivalent to ACA_0 for its language!

Strict ATR_0

Three sorts: N,Q,SQ. SQ stands for functions from N into Q. Variables n_i over N. Variables q_i over Q. Variables α_i over SQ.
+,-,·,<,/,| |,0,1,=,floor,ceiling. Also application, α[t], where t is of sort N. This has sort Q.

1-9. From Strict ACA_0, adapted for N and Q. In 9, a is entirely N valued.
10. Given any two sequences, either there is a pointwise continuous 1-1 map from the range of the first into the range of the second, or a pointwise continuous 1-1 map from the range of the second into the range of the first. Formulated using maps from indices to indices.

Outright equivalent to ATR_0 for its language!

Three sorts: N,Z,SQ. SQ stands for functions from N into Z. Variables n_i over N. Variables x_i over Z. Variables α_i over SQ.
+,-,·,<,| |,0,1,=. Also application, $\alpha[t]$, where t is of sort N. This has sort Z.

STRICT ACA_0

1. Appropriate flavor of first order predicate calculus with equality.
2. Discrete ordered ring axioms.
3. Relationship between N and Z. $(\forall x)(x \geq 0 \text{ iff } (\exists n)(x = n))$.
4. Extensionality for sequences..
5. If β is entirely N valued, then $\alpha[\beta[n]]$ defines a sequence.
6. The constant sequences and the identity sequence exists.
7. Closure of the sequences under addition, multiplication, subtraction.
8. Iteration. If β is entirely N valued, then we can define $\alpha[0] = t$, $\alpha[n+1] = \beta[\alpha[n]]$.
9. If α is bounded below, and no term of α appears arbitrarily far out, then α has a permutation which is increasing ($\leq$).

Outright equivalent to ACA_0 for its language!

Strict $\Pi 11\text{-}CA_0$

Three sorts: N,Q,SQ. SQ stands for functions from N into Q. Variables n_i over N. Variables q_i over Q. Variables α_i over SQ.
+,-,·,<,/,| |,0,1,=,floor,ceiling. Also application, $\alpha[t]$, where t is of sort N. This has sort Q.

1-9. From Strict ACA_0, adapted for N and Q. In 9, α is entirely N valued.
10. Any sequence with a subsequence whose range has "between any elements there is a third", has such a subsequence whose range is maximal.

Outright equivalent to $\Pi 11\text{-}CA_0$ for its language!