# THE INEVITABILITY OF LOGICAL STRENGTH

by
Harvey M. Friedman
Department of Mathematics
The Ohio State University
http://www.math.ohio-state.edu/%7Efriedman/
May 31, 2005

An extreme form of logic skeptic claims that "the present formal systems used for the foundations of mathematics are artificially strong, thereby causing headaches such as the Godel 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". Here we present some specific results that sharply refute aspects of this viewpoint.

## 1. EFA = $I\Delta_0$(exp) and logical strength.

For our purposes, we say that a theory in many sorted free logic has *logical strength* if and only if the system EFA = $I\Delta_0$(exp) is interpretable in it. I will elaborate after EFA is presented.

We introduced EFA = exponential function arithmetic, in [Fr80]. It was also used in the exposition of my work on Translatability and Relative Consistency, in [Sm82].

Since then, this system has often been referred to as $I\Delta_0$(exp). See, e.g., [HP98], p. 62. Also see [HP98], p. 405, second paragraph, referring to our presentation. We will use the terminology EFA here.

First we present PFA = $I\Delta_0$. Here PFA stands for “polynomial function arithmetic”.

The language of PFA is based on 0,S,+,•,≤,=. The variables are intended to range over nonnegative integers.

The □$_0$ formulas are the formulas of PFA defined as follows.

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

In iii), the expressions are treated as abbreviations.

The nonlogical axioms of PFA are as follows.

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

The nonlogical axioms of Q are

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 + x = y).

This presentation is slightly different than that given in [HP98]. There □ is not taken as a primitive, but instead is defined by Q8. Also there the terms t in bounded quantification are required to be variables.

We now present EFA. The language of EFA is 0,S,+,•,□,*,=. The new symbol * is a binary function symbol standing for exponentiation.

The □$_0$(exp) formulas are the formulas of EFA defined as follows.

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

The nonlogical axioms of EFA are as follows.

1. The axioms of Q.
2. $x * 0 = S0$, $x * y+S0 = x*y \bullet x$.
3. $(\varphi[x/0] \wedge (\forall x)(\varphi \rightarrow \varphi[x/Sx])) \rightarrow \varphi$, where $\varphi$ is $\Delta_0(exp)$.

There is a closely related system PFA + EXP whose language is the same as PFA (i.e., no *). The sentence EXP is horribly ugly. EXP really refers to a family of sentences, all of which are provably equivalent over PFA.

EXP is based on the following.

THEOREM 1.1. There is a $\Delta_0$ formula Exp(x,y,z) with only the distinct free variables shown such that the following is provable in PFA.
i) $Exp(x,0,z) \leftrightarrow z = 1$;
ii) $Exp(x,Sy,z) \leftrightarrow (\exists v)(Exp(x,y,v) \wedge z = v \bullet x)$.

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

EXP is taken to be

$(\forall x,y)(\exists z)(Exp(x,y,z))$

where Exp is any formula satisfying the conditions of Theorem 1.1.

The following two Theorems are well known.

THEOREM 1.2. If Exp(x,y,z) and Exp'(x,y,z) satisfy conditions in Theorem 1.1, then PFA proves their equivalence. PFA proves the equivalence of any version of EXP.

There is a particularly convenient and natural equivalent of EXP which we call CM = common multiples.

CM. For all $n \geq 1$, the integers $1,2,\ldots,n$ have a positive common multiple.

The following is well known.

THEOREM 1.3. PFA proves the equivalence of any version of EXP with CM.

For this reason, we will always use PFA + CM instead of PFA + EXP. The following is well known.

THEOREM 1.3. EFA and PFA + CM prove the same sentences in the language of PFA. PFA + CM, and EFA are finitely axiomatizable. EFA is interpretable in PFA + CM.

It is not known whether PFA is finitely axiomatizable. This question is related to notorious issues in complexity theory surrounding P = NP.

EFA is the minimum system of arithmetic where standard coding mechanisms in arithmetic can be done naturally without worry. In particular, standard identifications between finite sequences of natural numbers and natural numbers are fully available.

It appears that EFA is very strong from some points of view. We conjectured that EFA was 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.

For example, Fermat's Last Theorem ought to be provable in EFA. This has never been established.

This conjecture captured the imagination of Jeremy Avigad who wrote extensively about it in [Av03].

Our official definition of logical strength is as follows. T has logical strength if and only if EFA is interpretable in T.

There are two stronger notions that are particularly convenient.

a. EFA is a subsystem of T. I.e., all axioms of EFA are provable in T.

b. PFA + CM is a subsystem of T. I.e., all axioms of PFA + CM are provable in T.

Obviously a) is appropriate if the language of T includes that of EFA, and b) is appropriate if the language of T includes that of PFA. Clearly a) implies b), but clearly criterion a) is worth stating.

Two minor difficulties arise when using these two criteria.

i. Our strictly mathematical systems do have 0,1,+,•,≤,=, and sometimes *, but not S.

ii. Our strictly mathematical systems have a sort for Z, and not for N. Consequently (∀x)(x ≥ 0) will be refutable in our strictly mathematical systems, whereas (∀x)(x ≥ 0) is provable in PFA.

The most convenient way to get around these difficulties is to modify criteria a,b as follows.

a'. The universal closure of every axiom of EFA, when quantifiers (∀x),(∀y) are replaced by (∀x ≥ 0),(∀y ≥ 0), and all maximal terms SS...S(t) are replaced by 1+1+...+1+t, associated to the right, is a theorem of T.

b'. The universal closure of every axiom of PFA + CM, when quantifiers (∀x),(∀y) are replaced by (∀x ≥ 0),(∀y ≥ 0), and all maximal terms SS...S(t) are replaced by 1+1+...+1+t, associated to the right, is a theorem of T.

Obviously a') implies b') implies T has logical strength.

In the next section, we will present strictly mathematical systems meeting both of these criteria.

## 2. Some strictly mathematical statements.

We now present the strictly mathematical statements that we use to interpret EFA, and in fact meet criteria a'),b'). All of these statements are used and/or taught by all mathematicians.

The language in which we make almost all of these strictly mathematical statements is two sorted. We have a sort Z for integers, and a sort Z* for finite sequences of integers.

We use 0,1,+,-,•,≤ on Z, where - is unary. We use equality only for Z. We use lth(x) for the length of the sequence x, which is of sort Z. Here x must be of sort Z*. We use val(x,n) for the n-th term of the sequence x, which is of sort Z. Here x must be of soft Z* and n must be of sort Z. Lengths of sequences are nonnegative, and the terms of sequences are indexed starting with 1.

Note that we use equality only for Z and not for Z*. It is convenient to define equality for Z* as "having the same values in the same positions". Obviously any two equal sequences must have the same length.

We now give the axioms for FSZ informally. FSZ stands for "finite sequences of integers".

1. Discrete linearly ordered ring axioms for Z.
2. lth(x) ≥ 0.
3. val(x,n)↓ ↔ 1 ≤ n ≤ lth(x).
4. The finite sequence (0,...,n) exists.
5. lth(x) = lth(y) → -x,x+y,x•y exist.
6. The concatenation of x,y exists.
7. For n ≥ 1, the concatenation of x, n times, exists.
8. There is a finite sequence enumerating the terms of x that are not terms of y, in strictly increasing order.

We make some remarks about 1-8.

a. ↓ indicates "is defined". Thus the underlying logic is a well known variant of many sorted predicate calculus with equality, known as free logic. It has a corresponding complete axiomatization.

b. Axiom 4 is presented in terms of the length and values of (0,...,n). I.e., lth(x) = n+1 and val(x,i) = i-1 for 1 ≤ i ≤ n+1.

c. Axiom 5 is also presented in terms of the length and values of the finite sequences –x,x+y,x•y.

d. Axiom 6 is presented in terms of the length and values of the concatenation of x,y. This uses addition and subtraction on indices.

e. Axiom 7 is again presented in terms of the length and values of the n fold concatenation so described. What amounts to modular arithmetic is used for this presentation. Of course, the axioms of FSZ do not directly address modular arithmetic.

f. An alternative is to divide axiom 8 into two parts. First that there is a finite sequence whose terms consist of the terms of x that are not terms of y. Second that there is a strictly increasing sequence whose terms are the same as any given z. It is obvious that axiom 8 follows logically from the conjunction of these two parts. The first part immediately follows from axiom 8. For the second part, first deduce from axiom 8 that there is an empty sequence. Then apply axiom 8 to x and the empty sequence.

g. Our results hold for the following weaker system. Replace 8 by the following two immediate consequences of 8.

8a. There is a finite sequence whose terms are exactly those of x that are not terms of y.
8b. Every nonempty finite sequence has a least term.

We now give a more formal presentation of FSZ.

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

8a. (□z)(□k)((□n)(val(z,n) = k) □ ((□n)(val(x,n) = k) □ □(□n)(val(y,n) = k))).
8b. 1 □ lth(x) □ (□k)(□i)(val(x,k) □ val(x,i)).

In axioms 4 and 6 above, we use the symbol □ from free logic, which means "either both undefined, or equal". Equality always implies definedness. If a term is defined then all subterms are defined.

Free logic has a perfectly good axiomatization without using ↑,□,□. However, without these three symbols, formulas become unwieldy. I.e.,

t□ is defined as (□x)(x = t).
t↑ is defined as □(□x)(x = t).
s □ t is defined as (□x)(x = s □ x = t) (□(□x)(x = s) □ □(□x)(x = t)).

FSZE is FSZ together with CM, as presented in section 1.

THEOREM 2.1. FSZ + CM meets criteria b’).

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

9. m ≥ 0 □ (n * 0 = 1 □ n * m+1 = n•(n * m)).
10. m < 0 □ (n * m)↑.
11. (n*1,n*2,...,n*m) exists.

THEOREM 2.2. FSZEXP meets criteria a’).

We will now focus on a sketch of the proof of Theorem 2.1.

We had an earlier version of mathematical statements that combine to form a system of logical strength. However, it was considerably less convincing, and used finite sets of integers instead of finite sequences of integers as we do here. See [Fr01].

## 3. FSZ and $T_0$.

$T_0$ of [Fr01] is in the two sorted language with variables over integers and variables over finite sets of integers. For the integer sort, we use the language 0,1,+,-,•,<,= of linearly ordered rings, as we do for FSZ. We use □ between integers and sets. Equality is used only between integers. The nonlogical axioms of $T_0$ are as follows.

1. Linearly ordered 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)).

THEOREM 3.1. The universal closure of every axiom of PFA, when quantifiers (□x),(□y) are replaced by (□x ≥ 0),(□y ≥ 0), and all terms S(t) are replaced by 1+1+...+1+t, associated to the right, is a theorem of $T_0$.

Proof: See [Fr01]. QED

Since PFA is not known to be finitely axiomatizable, we cannot witness Theorem 3.1 by a finite amount of data. So we remark that Theorem 3.1 is very effectively true. In fact, there is a polynomial time algorithm which, provably in EFA, converts any axiom of PFA to a proof in $T_0$ of the replacement of that axiom given in the statement of Theorem 3.1.

We now prove that Theorem 3.1 holds for FSZ. For this, we give an interpretation of $T_0$ in FSZ which is the identity on the Z sort.

This interpretation of $T_0$ in FSZ is the obvious one. 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 $\in$ relation is interpreted as

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

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

i. lth(x) = max(0,m-n+1).
ii. For all $1 \leq i \leq$ lth(x), val(x,i) = n+i-1.

LEMMA 3.2. The empty sequence exists. For all n, (n) exists.

Proof: The empty sequence is from axiom 8.

Clearly (0) exists by axiom 4. Let n > 0. Form (0,...,n-1),(0,...,n) by axiom 4, and delete the latter from the former by axiom 8. If n < 0 then form (-n), and then form (n) by axiom 5. QED

LEMMA 3.3. 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 3.2. Let k ≥ 1. The sequence consisting of all n's of length k is obtained by axiom 7. QED

LEMMA 3.4. 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 4, form (0,...,m-n). By Lemma 3.3, form (n,...,n) of length m-n+1. By axiom 5, form (0,...,m-n) + (n,...,n) = (n upthru m). QED

LEMMA 3.5. The interpretation of Boolean Difference holds.

Proof: Let x,y be given. By axiom 8a, we obtain the required sequence. QED

LEMMA 3.6. The interpretation of Least Element holds.

Proof: Let x be nonempty. Apply axiom 8b. 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. The uniqueness part of QRT follows from axiom 1.

LEMMA 3.7. Let d ≥ 1 and n ≥ d. There is a greatest multiple of d that is at most n.

Proof: By Lemma 3.3, form (d,d,...,d) of length n. By Lemma 3.4 and axiom 5, form (d,2d,...,dn) of length n. By Lemma 3.3 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, and form -(0,...,dn-n) by axioms 4,5. By axiom 8a, delete -(0,...,dn-n) from (n-d,n-2d,...,n-dn). The result has least element n-id, for some 1 ≤ i ≤ d. Hence id must be the greatest multiple of d that is at most n. QED

LEMMA 3.8. The Quotient Remainder Theorem holds. I.e., for all d ≥ 1 and n, there exists unique q,r such that n = dq + r and 0 ≤ r < d.

Proof: QRT easily follows from Lemma 3.7 by axiom 1. QED

LEMMA 3.9. Let lth(x) = n and m be given. The sequence $x^{(m)}$ given by axiom 7 is unique and has the same terms as x.

Proof: Recall from axiom 7 that $x^{(m)}$ has length nm, and for all q,r with 0 ≤ q < m ≤ 1 ≤ r ≤ n, val($x^{(n)}$,n•q+r) =

val(x,r))).

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

LEMMA 3.10. Let lth(x) = n+1 and lth(y) = n, where n ≥ 1. Let $x^{(n)}$ and $y^{(n+1)}$ be given by axiom 7. For all 1 ≤ i ≤ j ≤ n, val($x^{(n)}$,jn-in+j) = val(x,i) and val($y^{(n+1)}$,jn-in+j) = val(y,j).

Proof: Let x,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($x^{(n)}$,jn-in+j) = val($x^{(n)}$,(j-i)(n+1)+i) = val(x,i).
val($y^{(n+1)}$,jn-in+j) = val($y^{(n+1)}$,(j-i)(n)+j) = val(y,j).

QED

LEMMA 3.11. Let x,y be nonempty. There exists z,w such that
i. x,z have the same terms.
ii. y,w have the same terms.
iii. lth(z) = lth(w)+1.
iv. Let a be a term of x and b be a term of y. Then there exists 1 ≤ i ≤ j < lth(w) such that val(z,i) = a and val(w,j) = b.

Proof: Let x,y be nonempty, lth(x) = n, lth(y) = m. Let u be the last term of x and v be the last term of y. Let x′ be x concatenated with $(u)^m$, and let y′ be y concatenated with $(v)^n$. Then lth(x′) = lth(y′), and x′ has the same terms as x, and y′ has the same terms as y. Finally, let z = x′ concatenated with x′ concatenated with u, and w = y′ concatenated with y′. QED

LEMMA 3.12. The interpretations of Set Addition and Set Multiplication hold.

Proof: Let x,y be given. We can assume that x,y are nonempty. Let z,w be as given by Lemma 3.11, say with lengths n+1,n. Let a be a term of x and b be a term of y. By Lemma 3.11, there exists 1 ≤ i ≤ j ≤ n such that val(z,i) = a and val(w,j) = b. By Lemma 3.10, there exists k such that val($z^{(n)}$,k) = a and val($w^{(n+1)}$,k) = b. Hence

a+b is a term of $z^{(n)}+w^{(n+1)}$.
a•b is a term of $z^{(n)}\bullet w^{(n+1)}$.

On the other hand, by Lemma 3.9, $z^{(n)}$ has the same terms as x and $w^{(n+1)}$ has the same terms as y. Hence

i. the terms of $z^{(n)}+w^{(n+1)}$ are exactly the result of summing a term of x and a term of y.
ii. the terms of $z^{(n)} \bullet w^{(n+1)}$ are exactly the result of multiplying a term of x and a term of y.

Thus

iii. $z^{(n)}+w^{(n+1)}$ witnesses Set Addition for x,y.
iv. $z^{(n)} \bullet w^{(n+1)}$ witnesses Set Multiplication for x,y.

QED

LEMMA 3.13. The interpretation of every axiom of $T_0$ is a theorem of FSZ.

Proof: By the above. QED

THEROEM 3.14. The universal closure of every axiom of PFA, when quantifiers $(\forall x),(\forall y)$ are replaced by $(\forall x \geq 0),(\forall y \geq 0)$, and all terms S(t) are replaced by 1+1+...+1+t, associated to the right, is a theorem of FSZ.

Proof: By Theorem 3.1 and Lemma 3.13. QED

We have now proved

THEOREM 2.1. FSZ + CM meets criterion b'.

Proof: Theorem 3.14 immediately implies Theorem 3.14 with PFA replaced by PFA + CM and FSZ replaced by FSZ + CM. QED

## 4. Further developments.

The plan is to generate much greater logical strength from strictly mathematical statements. This project is of course greatly facilitated now that we have the essential and fundamental infrastructure of EFA or PFA + CM at hand.

Initial developments along the lines of greater logical strength are discussed in [Fr05].

**REFERENCES**

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

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

[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/

[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.

[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.