# The n-Category Café – Weak Systems of Arithmetic

From [golem.ph.utexas.edu/category/2011/10/weak_systems_of_arithmetic.html]

John Baez, Jeffrey Ketland, and others

March 21, 2014

Posted by John Baez

[http://golem.ph.utexas.edu/ distler/blog/mathml.html]

The recent discussion about the consistency of arithmetic made me want to brush up on my logic. I'd like to learn a bit about axioms for arithmetic that are weaker than Peano arithmetic [http://en.wikipedia.org/wiki/Peano_axioms]. The most famous is Robinson arithmetic:

- Robinson arithmetic [http://en.wikipedia.org/wiki/Robinson_arithmetic], Wikipedia.

Robinson arithmetic is also known as $Q$, after a Star Trek character who could instantly judge whether any statement was provable in this system, or not:

Instead of Peano arithmetic's axiom schema for mathematical induction, $Q$ only has inductive definitions of addition and multiplication, together with an axiom saying that every number other than zero is a successor. It's so weak that it has computable nonstandard models! But, as the above article notes:

$Q$ fascinates because it is a finitely axiomatized first-order theory that is considerably weaker than Peano arithmetic (PA), and whose axioms contain only one existential quantifier, yet like PA is incomplete and incompletable in the sense of Gödel's Incompleteness Theorems, and essentially undecidable.

But there are many interesting systems of arithmetic between PA and $Q$ in strength. I'm hoping that if I tell you a bit about these, experts will step in

and tell us more interesting things—hopefully things we can understand!

---

addrhttp://golem.ph.utexas.edu/~distler/blog/mathml.html

For example, there's primitive recursive arithmetic, or PRA:

- Primitive recursive arithmetic [http://en.wikipedia.org/wiki/Primitive_recursive_arithmetic], Wikipedia.

This system lacks quantifiers, and has a separate predicate for each primitive recursive function, together with an axiom recursively defining it.

What's an interesting result about PRA? Here's the only one I've seen: its proof-theoretic ordinal [http://en.wikipedia.org/wiki/Proof-theoretic_ordinal] is $\omega^\omega$. This is much smaller than the proof-theoretic ordinal for Peano arithmetic, namely $\varepsilon_0$.

What's $\varepsilon_0$? It's a big but still countable ordinal which I explained back in week236 [http://math.ucr.edu/home/baez/week236.html]. And what's the proof-theoretic ordinal of a theory?

> Ordinal analysis concerns true, effective (recursive) theories that can interpret a sufficient portion of arithmetic to make statements about ordinal notations. The proof theoretic ordinal of such a theory $T$ is the smallest recursive ordinal that the theory cannot prove is well founded – the supremum of all ordinals $\alpha$ for which there exists a notation o in Kleene's sense such that **T** proves that $\sigma$ is an ordinal notation.

For more details, try this wonderfully well-written article:

- Michael Rathjen, The art of ordinal analysis [http://www.icm2006.org/proceedings/Vol_II/contents/ICM_Vol_2_03.pdf], International Congress of Mathematicians, II, Eur. Math. Soc., Zurich, pp. 45–69.

Climbing down the ladder we eventually meet elementary function arithmetic, or EFA:

- Elementary function arithmetic [http://en.wikipedia.org/wiki/Elementary_function_arithmetic], Wikipedia.

Its proof-theoretic ordinal is just $\omega^3$. It's famous because Harvey Friedman made a grand conjecture about it:

> Every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement) can be proved in EFA. EFA is the weak fragment of Peano Arithmetic based on the usual quantifier-free axioms for 0, 1, $+$, $\times$, exponential, together with the scheme of induction for all formulas in the language all of whose quantifiers are bounded.

Does anyone know yet if Fermat's Last Theorem can be proved in EFA? I seem to remember early discussions where people were wondering if Wiles' proof could be formalized in Peano arithmetic.

But let's climb further down the ladder. How low can we go? I guess $\omega$ is too low to be the proof-theoretic ordinal of any theory "that can interpret a sufficient portion of arithmetic to make statements about ordinal notations." Is that right? How about $\omega + 1$, $2\omega$, and so on?

There are some theories of arithmetic whose proof-theoretic ordinal is just $\omega^2$. One of them is called $I\Delta_0$. This is Peano arithmetic with induction restricted to predicates where all the for-alls and there-exists quantify over variables whose range is explicitly bounded, like this:

$$\forall i \leq n \forall j \leq n \forall k \leq n : i^3 + j^3 \neq k^3$$

Every predicate of this sort can be checked in an explicitly bounded amount of time, so these are the most innocuous ones.

Such predicates lie at the very bottom of the arithmetical hierarchy [http://planetmath.org/encyclopedia/ArithmeticalHierarchy.html], which is a way of classifying predicates by the complexity of their quantifiers. We can also limit induction to predicates at higher levels of the arithmetic hierarchy, and get flavors of arithmetic with higher proof-theoretic ordinals.

But you can always make infinities bigger – to me, that gets a bit dull after a while. I'm more interested in life near the bottom. After all, that's where I live: I can barely multiply 5-digit numbers without making a mistake.

There are even systems of arithmetic too weak to make statements about ordinal

notations. I guess $Q$ is one of these. As far as I can tell, it doesn't even make sense to assign proof-theoretic ordinals to these wimpy systems. Is there some other well-known way to rank them?

Much weaker than $Q$, for example, is Presburger arithmetic:

- Presburger arithmetic [http://en.wikipedia.org/wiki/Presburger_arithmetic], Wikipedia.

This is roughly Peano arithmetic without multiplication! It's so simple you can read all the axioms without falling asleep:

$$\neg(0 = x + 1)x + 1 = y + 1 \Rightarrow x = yx + 0 = x(x + y) + 1 = x + (y + 1)$$

and an axiom schema for induction saying:

$$(P(0) \wedge (P(x) \Rightarrow P(x + 1))) \;\Rightarrow\; P(y)$$

or all predicates $P$ that you can write in the language of Presburger arithmetic.

Presburger arithmetic is so simple, Gödel's first incompleteness theorem doesn't apply to it. It's consistent. It's complete: for every statement in Presburger arithmetic, either it or its negation is provable. But it's also decidable: there's an algorithm that decides which of these two alternatives holds!

However, Fischer and Rabin [www.lcs.mit.edu/publications/pubs/ps/MIT-LCS-TM-043.ps] showed that no algorithm can do this for all statements of length $n$ in less than $2^{2^{cn}}$ steps. So, Presburger arithmetic is still fairly complicated from a practical perspective. (In 1978, Derek Oppen showed an algorithm with triply exponential runtime can do the job.)

Presburger arithmetic can't prove itself consistent: it's not smart enough to even say that it's consistent! However, there are [http://mathoverflow.net/questions/9864/presburger-arithmetic/10027#10027] weak systems of arithmetic that can prove themselves consistent. I'd like to learn more about those. How interesting can they get before the hand of Gödel comes down and smashes them out of existence?

Re: Weak Systems of Arithmetic

Does anyone know yet if Fermat's Last Theorem can be proved in EFA? I seem to remember early discussions where people were wondering if Wiles' proof could be formalized in Peano arithmetic.

I've heard Angus MacIntyre talking about this. He is working on a paper arguing that Wiles' proof translates into PA. I say "arguing" rather than "proving" because all he plans to do is show that the central objects and steps can be formalised in PA, rather than translate the entirety of Wiles' proof, which would be a a ridiculously Herculean task. I don't know if his paper is available yet, but there's some discussion of it here [http://rjlipton.wordpress.com/2011/02/03/infinite-objects-and-deep-proofs/].

Posted by: Richard Elwes on October 11, 2011 8:52 AM

---

[http://golem.ph.utexas.edu/~distler/blog/mathml.html] Richard wrote:

> I've heard Angus MacIntyre talking about this. He is working on a paper arguing that Wiles' proof translates into PA.

Hmm, that's interesting! Sounds like a lot of work—but work that's interesting if you really know and like number theory and logic. Of course one would really want to do this for Modularity Theorem [http://en.wikipedia.org/wiki/Modularity_theorem], not just that piddling spinoff called Fermat's Last Theorem.

> I say "arguing" rather than "proving" because all he plans to do is show that the central objects and steps can be formalised in PA, rather than translate the entirety of Wiles' proof, which would be a a ridiculously Herculean task.

Right. But by the way, I think most logicians would be perfectly happy to say 'proving' here.

---

I think most logicians would be perfectly happy to say "proving" here.

Well, when I heard Angus talk he was keen to emphasise that it would not be a complete proof, but would only focus on the major bits of machinery needed.

So it seems polite to echo the official line!

Of course one would really want to do this for Modularity Theorem, not just that piddling spinoff called Fermat's Last Theorem.

Yes - my notes from the talk are elsewhere, but I think his main focus is indeed on the central modularity result (I don't know whether he addresses the full theorem, or just the case needed for FLT).

In any case, he claims that it is effectively $\Pi^0_1$, and provable in PA.

Posted by: Richard Elwes

---

Regarding FLT, nLab has a short section [http://ncatlab.org/nlab/show/effects+of+foundations+on+%22real%22+mathematics#fermats_last_theorem_3] on this. So any findings to be added there. It mentions Colin McLarty's research.

I have also heard Angus MacIntyre on a sketch of a proof that PA suffices. He seems to have given a number of talks on this, e.g., here [http://www.cs.ox.ac.uk/seminars/128.html] and here [http://www.cs.ox.ac.uk/seminars/355.html], the later mentioning a discussion on FOM.

There's a paper by Jeremy Avigad – Number theory and elementary arithmetic [http://www.andrew.cmu.edu/user/avigad/Papers/elementary.pdf] – which should interest you.

Posted by: David Corfield

---

McLarty has recently shown [http://arxiv.org/abs/1102.1773] (I believe) that finite-order arithmetic is sufficient to define pretty much all of Grothendieck-style algebraic geometry necessary for arithmetic questions. nth-order arithmetic admits quantification over Pn(N), the n-times iterated power set for some given n. The n needed depends on the problem in question, and the hope is that $n < 2$ (PA or weaker) is sufficient for FLT, or even the modularity theorem (since there is a proof of the Modularity Theorem which is simpler than Wiles' original proof of the semistable case).

The trick is defining derived functor cohomology for sheaf coefficients. All the algebra content is apparently very basic from a logic point of view.

Posted by: David Roberts

---

So, I just spent a bit playing around with $I\Delta_0$ to get a sense for it. I wanted to build a Gödel coding, and I found I needed the following lemma (quantifiers range over positive integers):

$$\forall n \exists N \forall k \leq n \exists d : kd = N$$

Easy enough in PA; it's a simple induction on $n$. But in $I\Delta_0$ I can't make that induction because there is no bound on $N$. (There's also no bound on $d$, but $I$ can fix that by changing the statement to $\exists d \leq N$; this is also true and trivially implies the above.) I can't fix it by adding in $N \leq n^{100}$ because that's not true; the least such $N$ is of size $\approx e^n$. I can't write $N \leq 4^n$ because I don't have a symbol for exponentiation. Anyone want to give me a tip as to how to prove this in $I\Delta_0$?

Posted by: David Speyer

---

That's a great puzzle, David! I'm not very good at these things, so I hope someone materializes who can help you out. In the meantime here are some references that might (or might not provide useful clues. At least I found they're somewhat interesting.

First:

- Chris Pollet, Translating $I\Delta_0$ + exp proofs into weaker systems. [http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.7317]

I'm guessing you could do what you want in $I\Delta_0$ + exp, but you're struggling to do it in $I\Delta_0$. A few intriguing quotes:

> Of the commonly studied bounded arithmetic theories, $I\Delta_0$ + exp, the theory with induction for bounded formulas in the language of 0, $S$, +,

> $\times$ together with the axiom saying the exponential function is total, is one of the more interesting...
>
> Wilkie–Paris have shown several interesting connections between $\mathrm{I}\Delta_0 +$ exp and weaker theories. They have shown $\mathrm{I}\Delta_0 +$ exp cannot prove $\mathrm{Con}(Q)$...
>
> Despite the fact that $\mathrm{I}\Delta_0 +$ exp is not interpretable in $\mathrm{I}\Delta_0$, it is known if $\mathrm{I}\Delta_0 +$ exp proves $\forall x : A(x)$ where $A$ is a bounded formula then $\mathrm{I}\Delta_0$ proves
>
> $$\forall x(\exists y : y = 2_k^x) \implies A(x))$$
>
> Here $2_k^x$ is a stack of 2's $k$ high with an $x$ at top.

Here $k$ depends on $x$ in some way. I guess he's saying that while $\mathrm{I}\Delta_0$ can be used to describe a relation deserving of the name $y = 2_k^x$, it can't prove that exponentiation is total, so it can't prove there exists a $y$ such that $y = 2_k^x$. So, we need to supplement its wisdom for it to prove something similar to $\forall x A(x)$. Or in his words:

> Intuitively, this results says: given $x$, if $\mathrm{I}\Delta_0$ knows a big enough $y$ exists then it can show $A(x)$ holds.

Of course you don't want to resort to a trick like this!

Posted by: John Baez

---

That's a great puzzle, David! I'm not very good at these things, so I hope someone materializes who can help you out. In the meantime here are some references that might (or might not provide useful clues. At least I found they're somewhat interesting.

First:

- Chris Pollet, Translating $\mathrm{I}\Delta_0 +$ exp proofs into weaker systems. [http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.7317]

I'm guessing you could do what you want in $\mathrm{I}\Delta_0 +$ exp, but you're struggling to do it in $\mathrm{I}\Delta_0$. A few intriguing quotes:

> Of the commonly studied bounded arithmetic theories, $\mathrm{I}\Delta_0 +$ exp, the theory with induction for bounded formulas in the language of $0$, $S$, $+$,

> $\times$ together with the axiom saying the exponential function is total, is one of the more interesting...
>
> Wilkie–Paris have shown several interesting connections between $\mathrm{I}\Delta_0 + \exp$ and weaker theories. They have shown $\mathrm{I}\Delta_0 + \exp$ cannot prove $\mathrm{Con}(Q)$...
>
> Despite the fact that $\mathrm{I}\Delta_0 + \exp$ is not interpretable in $\mathrm{I}\Delta_0$, it is known if $\mathrm{I}\Delta_0 + \exp$ proves $\forall x : A(x)$ where $A$ is a bounded formula then $\mathrm{I}\Delta_0$ proves
>
> $$\forall x(\exists y : y = 2x^k) \Leftrightarrow A(x))$$
>
> Here $2x^k$ is a stackof 2's $k$ high with an $x$ at top.

Here $k$ depends on $x$ in some way. I guess he's saying that while $\mathrm{I}\Delta_0$ can be used to describe a relation deserving of the name $y = 2x^k$, it can't prove that exponentiation is total, so it can't prove there exists a $y$ such that $y = 2x^k$. So, we need to supplement its wisdom for it to prove something similar to $\forall x : A(x)$. Or in his words:

Intuitively, this results says: given $x$, if $\mathrm{I}\Delta_0$ knows a big enough $y$ exists then it can show $A(x)$ holds.

Of course you don't want to resort to a trick like this!

Posted by: John Baez

---

I think you can bet your sweet bippy that he himself knows how to do it. :-) Hey, maybe someone should ask on Math Overflow!

Posted by: Todd Trimble

---

It looks like the conversation has moved on. In case anyone is still puzzled, let me spell out what Kaveh is saying:

My statement cannot be proved in $\mathrm{I}\Delta_0$ because $\mathrm{I}\Delta_0$ is polynomially bounded.

I think I understand what this means now. Suppose that $\mathrm{I}\Delta_0$ proves

$$\forall n \exists m : \ldots\ldots$$

where the ellipsis are any grammatical statement about $n$ and $m$. Then there

is some polynomial $p(n)$ there exists an $m$ with $m \leq p(n)$.

This is not true for my statement! The smallest valid $N$ is LCM(1,2,. . . ,n),which is $\approx e^n$. (The more obvious choice of $N$ is $n!$, which is even bigger.) So this is a great example of a sentence which is true (as a statement about ordinary integers) and grammatical in $I\Delta_0$, but not provable in $I\Delta_0$, on account of the fact that it involves a fast growing function.

This example really helps me understand the more complicated examples of statements which are known to be undecidable in PA because of fast growing functions, like the Paris-Huntington theorem. I always run into a psychological roadblock with examples like Paris-Huntington, because the encoding of those statements into formal language is so complex. This example is straightforwardly a number theoretic statement, so I think I'll use it as my standard example of a statement which is undecidable for growth rate reasons in the future.

I'll point out that there is plenty of stuff which is provable in $I\Delta_0$. I got through showing "if $x$ divides $y$ then $x \leq y$", "every positive integer is either of the form $2k$ or $2k + 1$", "if $a$ divides $c$ and $b$ divides $c$, then LCM$(a, b)$ divides $c$", and several other standard examples of induction in elementary number theory before trying this one.

Posted by: David Speyer

---

I have two naive questions:

On the wikipedia page "ordinal analysis", RFA (rudimentary function arithmetic) is mentioned as having proof-theoretic ordinal $omega^2$, but nothing is said about it. Has anyone here heard of it? Is it EFA minus exponentiation?

Even if some systems may be too weak to be assigned proof-theoretic ordinals, is it possible to make sense of "if that system had a proof-theoretic ordinal in any reasonable sense, then this ordinal would be. . . "? In view of the wikipedia page on the Grzegorczyk hierarchy (which gives systems of strength $\omega^n$), it is tempting to say that Presburger arithmetic "should" have strength omega.

Posted by: ben

---

While naive, these questions are not sufficiently naive for me to answer them. So, I hope someone else can! They're interesting.

Posted by: John Baez

---

> What's an interesting result about PRA?

It is suggested that PRA is an upper bound for what Hilbert considered to be finitistic reasoning.

---

> Is there some other well-known way to rank them?

There are (e.g. by the class of their provably total functions), but I guess you want something similar to ordinal analysis. In that case check Arnold Beckmann [http://cs.swan.ac.uk/~csarnold/]'s project on dynamic ordinal analysis [http://cs.swan.ac.uk/~csarnold/amllcc/give-page.php?2] .

---

> How interesting can they get before the hand of Gödel comes down and smashes them out of existence?

For most purposes the bounded arithmetic theory $V^0$ (which is quite similar to $\mathrm{I}\Delta_0$) is the natural starting point. The provably total functions of $V^0$ are exactly $\mathrm{AC}^0$ functions (the smallest complexity class complexity theorist usually consider). For comparison, provably total functions of $\mathrm{I}\Delta_0$ are Linear Time Hierarchy (LTH). $V^0$ is capable of talking about sequences using a better encoding that Gödel's beta function (write the numbers in the sequence in binary, add 2 between each consecutive pair, read in base 4). It can also check if a given number encodes the computation of a given Turing machine on a given input.

But a more natural theory to work with might be $\mathrm{VTC}^0$ whose provably total functions are complexity class $\mathrm{TC}^0$ which can also parse syntax. See Cook and

Nguyen [http://www.cambridge.org/gb/knowledge/isbn/item2708116/?site_locale=en_GB] (draft [http://www.cs.toronto.edu/~sacook/homepage/book/] ) for more information.

I think self-verifying theories [http://en.wikipedia.org/wiki/Self-verifying_theories] that can prove their own consistency (in the usual formalization) are artificial. For more information about them see:

Dan Willard, "Self Verifying Axiom Systems, the Incompleteness Theorem and the Tangibility Reflection Principle", Journal of Symbolic Logic 66 (2001) pp. 536-596.

Dan Willard, "An Exploration of the Partial Respects in which an Axiom System Recognizing Solely Addition as a Total Function Can Verify Its Own Consistency", Journal of Symbolic Logic 70 (2005) pp. 1171-1209.

---

I just spent a bit playing around with $I\Delta_0$ to get a sense for it. I wanted to build a Gödel coding...

You cannot prove that in $I\Delta_0$ because that would give a exponentially growing function while $I\Delta_0$ is a polynomially bounded theory.

---

On the wikipedia page "ordinal analysis", RFA (rudimentary function arithmetic) is mentioned as having proof-theoretic ordinal $\omega^2$, but nothing is said about it.

Rudimentary sets are defined in Smullyan 1961. They are essentially $\Delta_0$ =LTH. I am not sure about the theory RFA but I would guess it is essentially $I\Delta_0$. EFA is $I\Delta_0$ + EXP (where EXP expresses that the exponential function is total).

---

Even if some systems may be too weak to be assigned proof-theoretic ordinals... See above (the part about Beckmann's research).

Posted by: Kaveh

---

Thanks for posting this, John.

(Small quibble though - you have "$Q$ only has inductive definitions of addition, multiplication and exponentiation", but $Q$ lacks the primitive recursive defn for exponentiation. Those axioms would be:

$$\forall x : (x^0 = S(0)) \tag{1}$$

$$\forall x \forall y : (x^{S(y)} = x \times x^y) \tag{2}$$

But in standard logic, simply assuming a function symbol more or less presupposes the totality of corresponding function, i.e., exponentiation in this case. I.e., if we have a primitive binary symbol (i.e., $x^y$), then $\forall x \forall y \exists z (z = x^y)$ is a theorem of logic! For if $f$ is, say, a 1-place function symbol, then $\vdash \forall x : (f(x) = f(x))$. And this gives us $\vdash \forall x \exists y : (y = f(x))$. Quick indirect proof: suppose $\exists x \forall y (y \neq f(x))$. So, $\forall y : (y \neq f(c))$, by introducing a new constant c; which gives the contradiction $f(c) \neq f(c)$.)

When Joel David Hamkins says that any weak system in the hierarchy $\mathrm{I}\Sigma_n$ simulates computation, I think (I am guessing) he just means that any recursive function is representable in $Q$ and its extensions. E.g., if $f : \mathbb{N}^p \to \mathbb{N}$ is a partial recursive function, then there is an LA-formula $\phi(y, x_1, \ldots, x_p)$ such that, for all $k$, $n_1$,..., $n_p \in \mathbb{N}$,

$$\text{if } \; k = f(n_1, \ldots, n_p), \;\; \text{then } \; Q \vdash \forall y : (y = \underline{k} \Leftrightarrow \phi(y, n_1, \ldots, n_p))$$

In particular,exponentiation, $f(a, b) = a^b$,is recursive. So, there is an LA-formula $\mathrm{Exp}(y, x_1, x_2)$ such that, for all $n$, $m$, $k \in \mathbb{N}$,

$$\text{if } \; k = n^m \text{then} Q \vdash \forall y : (y = \underline{k} \Leftrightarrow \mathrm{Exp}(y, \underline{n}, \underline{m}))$$

So $\mathrm{Exp}(y, x_1, x_2)$ represents exponentiation. However, $Q$ cannot prove it total. I.e., for any such representing formula Exp

$$Q \nvdash \forall x_1 \forall x_2 \exists y : \mathrm{Exp}(y, x_1, x_2)$$

It's a long time since I worked through some of the details of bounded arithmetic, and my copy of Hayek and Pudlack is in Munich. So I can't see immediately how to give a model for this. Still, $Q$ is very, very weak and here

is a simple non-standard model. (From Boolos and Jeffrey's textbook). Let $A = dom(\Box) = \omega \cup \{a, b\}$, where $a$ and $b$ are new objects not in $\omega$. These will behave like "infinite numbers". We need to define functions $S^{\Box}$, $+^{\Box}$ and $\times^{\Box}$ on $A$ interpreting the LA-symbols $S$, $+$ and $\times$. Let $S^{\Box}$ have its standard values on $n \in \omega$ (i.e., $S^{\Box}(2) = 3$, etc.), but let $S^{\Box}(a) = a$ and $S^{\Box}(b) = b$. Similarly, $+$ and $\times$ are interpreted standardly on $\omega$, but one can define an odd multiplication table for the values of $a +^{\Box} a$, $a +^{\Box} b$, $a \times^{\Box} b$, etc. Then one proves $\Box \models Q$, even though $\Box \not\approx \mathbb{N}$. This model is such that,

1. $\Box \not\models \forall x \forall y : (x + y = y + x)$
2. $\Box \not\models \forall x \forall y : (x \times y = y \times x)$

So, this tells us that $Q$ doesn't prove that $+$ and $\times$ are commutative.

I don't think this simple model $\Box$ with two infinite elements, $a$ and $b$, is enough to show that $Q$ doesn't prove that exponentiation is total.

The idea would be to find a model $\mathcal{B} \models Q$ such that $B \not\models \forall x_1 \forall x_2 \exists y : \phi(y, x_1, x_2)$, for any LA-formula $\phi(y, x_1, x_2)$ that represents $f(a, b) = a^b$ in $Q$. I don't know off-hand what such a model $\mathcal{B}$ looks like though.

Posted by: Jeffrey Ketland

---

On one of Kaveh's points, another property of PRA is that if $\phi$ is a $\Pi_1 1$-sentence, then:

$$I\Sigma_1 \vdash \phi \text{ iff } PRA \vdash \phi$$

(Parsons 1970). Yes, Tait has argued that PRA represents the upper limit on what a finitist should "accept". However, I think that Kreisel had argued earlier that it should be PA.

Posted by: Jeffrey Ketland

---

Here's another system (call it FPA) which proves its own consistency. Work in 2-nd order logic, with predicative comprehension. Let 0 be a constant; let $N$

be a (1-ary) predicate, meant to represent being a natural number; and let $S$ be a (2-ary) relationship, meant to represent the successor relationship. Do not assume the totality of $S$. Instead assume

1. $S$ is functional, i.e. $Nx$ and $Sx, y$ and $Sx, z$ implies $y = z$
2. $S$ is one-to-one, i.e. $Nx$ and $Ny$ and $Sx, z$ and $Sy, z$ implies $x = y$
3. For all $n$, not $Sn, 0$
4. Induction (full induction, as a schema)

Because the totality of $S$ is not assumed, FPA has the singleton model $\{0\}$. It also has all the initial segments as models, as well as the standard model (well, whichever of those models actually exist). In a nutshell, FPA is "downward"; if you assume that a number $n$ exists, then all numbers less than $n$ exist and behave as you expect. Most of arithmetic is, in fact, "downward", so FPA can prove most familiar propositions, or at least versions of them. It can prove (unlike $Q$) the commutative laws of addition and multiplication. It can prove Quadratic Reciprocity. It cannot prove that there are an infinite number of primes (it cannot even prove the existence of 2, after all), but it can prove that between $n/2$ and $n$ for any $n > 2$, there always exists a prime. It's not far-fetched to think that FPA can prove Fermat's Last Theorem. So, mathematically anyway, it's pretty strong. (Still it's neither stronger nor weaker than $Q$. It's incomparable, because it assumes induction, which $Q$ does not, but does not assume the totality of successoring, which $Q$ does.)

In particular FPA can talk about syntax because syntactical elements can be defined in a downward way. Something is a term if it can be decomposed in a particular way. Something is a wff if it can be decomposed in a particular way. Etc.

Now, to prove its own consistency, it suffices for FPA to show that the assumption of a proof in FPA of "not 0=0" leads to a contradiction. But a proof is a number (in Gödel's manner of representing syntactical elements) and, in fact, a very large number. This large number then gives enough room, in FPA, to formalize truth-in-the-singleton-model and to prove that any sentence in the

inconsistency proof must be true. But "not 0=0" isn't true. Contradiction! Therefore FPA has proven its own consistency.

Here's a link to a book-long treatise, if it interests anyone:

- Andrew Boucher, Arithmetic Without the Successor Axiom [http://www.andrewboucher.com/papers/arith-succ.pdf].

It's possible to formalize everything in a first-order system, if the second-order is bothersome for some.

Posted by: t

---

Wow, that's quite interesting! Thanks!

Since this post grew out of our earlier discussions of ultrafinitism [http://golem.ph.utexas.edu/category/2011/09/the_inconsistency_of_arithmeti.html] , I couldn't help noting that this axiom system should be an ultrafinitist's dream, since you can take any model of Peano Arithmetic, throw out all numbers $> n$, and be left with a model of this one!

Indeed I see Andrew Boucher writes:

> Most sub-systems of Peano Arithmetic have focused on weakening induction. Indeed perhaps the most famous sub-system, Robinson's $Q$, lacks an induction axiom altogether. It is very weak in many respects, unable for instance to prove the Commutative Law of Addition (in any version). Indeed, it is sometimes taken to be the weakest viable system; if a proposition can be proved in $Q$, then that is supposed to pretty much established that all but Berkleyan skeptics or fools are compelled to accept it.
>
> But weakness of systems is not a linear order, and $F$ is neither stronger nor weaker than $Q$. $F$ has induction, indeed full induction, which $Q$ does not. But $F$ is ontologically much weaker than $Q$, since $Q$ supposes the Successor Axiom. $Q$ assumes the natural numbers, all of them, ad infinitum. So in terms of strength, $F$ and $Q$ are incomparable. In actual practice, $F$ seems to generate more results of standard arithmetic; and so in that sense only, it is "stronger".
>
> One of the most important practitioners of $Q$ has been Edward Nelson of Princeton, who has developed a considerable body of arithmetic in $Q$. While Nelson's misgivings with classical mathematics seemed to have their source in doubts about the existence of the natural numbers, the brunt of his skepticism falls on induction, hence his adoption of $Q$. "The induction

> principle assumes that the natural number series is given." [p. 1, Predicative Arithmetic] Yet it would seem that induction is neither here nor there when it comes to ontological supposition. Induction states conditions for when something holds of all the natural numbers, and says nothing about how many or what numbers there are. So a skeptic about the natural numbers should put, so to speak, his money where his doubts are, and reject the assumption which is generating all those numbers — namely the Successor Axiom – and leave induction, which those doubts impact at worst secondarily, alone.

He also mentions other systems capable of proving their own consistency:

> A number of arithmetic systems, capable of proving their own consistency, have become known over the years. Jeroslow [Consistency Statements] had an example, which was a certain fixed point extension of $Q \vee \forall x \forall y : (x = y)$. More recently, Yvon Gauthier [Internal Logic and Internal Consistency] used indefinite descent and introduced a special, called "effinite", quantifier. And Dan Willard [Self-Verifying Axiom Systems] has exhibited several cases, based on seven "grounding" functions. These systems lack a certain naturalness and seem to be constructed for the express purpose of proving their own consistency. Finally, Panu Raatikainen constructed what is effectively a first-order, weaker variant of $F$; this system can prove that it has a model [Truth in a Finite Universe], but its weakness does not allow the author to draw conclusions about intensional correctness and so it seems to fall short of the ability to prove its own self-consistency.

Posted by: John Baez

---

I remember Andrew Boucher describing his theory $F$ on sci.logic years back; the problem is that it doesn't interpret syntax (e.g., Tarski's TC). (The current state of play is that TC is interpretable in $Q$.)

The language LF is a second-order language with a binary relation symbol $S$ instead of the usual unary function symbol. Even with this small modification (so as to drop the automatic existence of successors), the syntax of LF is still that of a standard language, with, say, symbols 0, $S$, $=$ and $\neg$, $\rightarrow$ , $\forall$ and variables $v$, $v'$ , $v''$, etc. It is straightforward to prove, based merely on the description of LF and the usual assumptions about concatenation, that:

$$|LF| = \aleph_0.$$

So the language LF itself is countably infinite. Denying the existence of numbers

while asserting the existence of infinitely many syntactical entities is incoherent, as one of Gödel's basic insights is: syntax = arithmetic.

Suppose we then begin to try and interpret the syntax of LF in $F$ itself. Ignore the second order part, as it introduces needless complexities. In the metatheory, suppose we assign Gödel codes as follows:

$$\begin{array}{llll} \#(0) = 1 & \#(S) = 2 & \#(=) = 3 & \#(\neg) = 4 \\ \#(\rightarrow) = 5 & \#(\forall) = 6 & \#(v) = 7 & \#(') = 8 \end{array}$$

Incidentally, this already goes beyond $F$ itself, as the metatheory already implicitly assumes the distinctness of these numbers. How would this be done, given that one cannot even prove the existence of 1?

In LA, we encode any string (sequence of primitive symbols) as the sequence of its codes, and we encode a sequence $(n_1, \ldots, n_k)$ of numbers as a sequence number, e.g., as

$$\langle n_1, \ldots, n_k \rangle = (p1)^{n_1+1} \times \ldots \times (pk)^{n_k+1}.$$

For example, the string $\forall\forall S$ is really the sequence $(\forall, \forall, S)$, and is coded as the sequence (6, 6, 2), which becomes the sequence number $27 \times 3^7 \times 5^3$.

But what, in $F$, is the corresponding numeral for any expression of the language LF? In the usual language LA of arithmetic, an expression $\varepsilon$ with code $n$ is assigned the numeral $\underline{n}$, written $[\varepsilon]$, which is $S \ldots S0$. That is, 0 prefixed by $n$ occurrences of $S$, where $S$ is a function symbol. (Can't get "ulcorner" to work!)

How would this work in $F$? Consequently, $F$ does not numeralwise represent non-identity of syntactical entities.

For example, in syntax we have

$A$: "The quantifier $\forall$ is distinct from the conditional $\rightarrow$".

Under the coding above, this becomes

$$A' : \underline{6} \neq \underline{5}$$

which is trivially provable in $Q$.

Now it's very unclear to me how one even expresses $\underline{6} \neq \underline{5}$ in LF. But however it is done, we get that

$$F \nvdash \underline{6} \neq \underline{5}$$

A requirement on a theory $T$ that interprets syntax is that, for expressions $\varepsilon_1$ , $\varepsilon_2$ , we have unique singular terms $[\varepsilon_1]$, $[\varepsilon_2]$ such that,

$$\text{if } \varepsilon_1 \neq \varepsilon_2 \text{ then } T \vdash [\varepsilon_1] \neq [\varepsilon_2]$$

But $F$ doesn't give this. Instead, we have

$$F \nvdash [\forall] \neq [\rightarrow]$$

So, alleged "agnoticism" about numbers has become "agnoticism" about syntax. Which contradicts the non-agnoticism of the description of syntactical structure of LF itself.

There is no faithful interpretation of the syntax of LF into $F$. So, syntactical claims about the properties of $F$ cannot be translated into $F$. The meta-theory of the syntax of $F$ already assumes an infinity of distinct syntactical entities. In particular, claims about consistency cannot be translated into $F$.

Posted by: Jeffrey Ketland

---

Thanks for your comment. Unfortunately, I don't think it's quite right and $F$ does indeed interpret syntax adequately, so that it does express notions of consistency.

First, just as $F$ is agnostic about the infinity of the natural numbers, it is agnostic about the infinity of the syntax. The infinity of syntax comes from assuming that there are an infinite number of variables; $F$ doesn't make this assumption. I guess a stickler might say this is no longer second- (or first-) order logic because these assume that there are an infinite number of variable symbols. But I would hope most would agree this is not an essential feature of the logic.

JK: "Incidentally, this already goes beyond F itself, as the metatheory already implicitly assumes the distinctness of these numbers. How would this be done,

given that one cannot even prove the existence of 1?"

While one cannot prove that 1 exists, it is possible to prove that anything which *is* one is unique (and so distinct). That is, it is possible to define a predicate one($x$) as ($Nx$ and $S0, x$). It is not possible to prove that there exists $x$ s.t. one($x$), but it *is* possible to prove that $(x)(y)$(one($x$) and one($y$) implies$x = y$) So proof of existence, no; proof of distinctness, yes. One can define two($x$) as

$$Nx \text{ and there exists } y \text{ such that one}(y) \text{ and } Sy, x$$

And so forth as far as one wants or has energy to go.

Moreover, one can define the concepts of odd and even. One defines even($x$) iff $Nx$ and (there exists $y$)($y + y = x$). Again, no assertion that one can prove that even($x$) or odd($x$) for any $x$. But one *can* prove that there is no $x$ such that both even($x$) and odd($x$). Again, existence no, distinctness yes.

So one can represent the syntax. Define predicates one, two, three, ..., ten. Define Big($x$) as $Nx$ and not one($x$) and not two($x$) and ... and not ten($x$). Then $x$ represents a left parentheses if $x = 0$. $x$ represents a right parenthesis if one($x$). $x$ represents the implication sign if two($x$). $x$ represents the negation sign if three($x$). $x$ represent the equal sign if four($x$). And so forth. $x$ represents a small-letter variable if Big($x$) and even($x$). $x$ represents a big-letter variable if Big($x$) and odd($x$).

One gives the usual recursive definitions to syntactical entities like AtomicWff($x$) and Proof($x$). Again, one cannot show there exist any $x$ such that AtomicWff($x$). But one can show that, *if* AtomicWff($x$), then $x$ has all the properties that it should have.

So, given that $x$ cannot prove there exist any syntactical entities, how can it prove its own consistency? Because consistency means there is no proof of "not $0 = 0$". So a proof of consistency is not a proof that something exists, but a proof that something does not exist. It *assumes* the existence of a syntactical entity, in this case a proof of "not $0 = 0$", and shows that the assumption of the existence of this entity leads to a contradiction. Thus $F$ is able to prove a system's consistency. (What $F$ cannot prove is prove that a

system is inconsistent; because then it would have to prove that there exists something, namely a proof of "not $0 = 0$", and that it cannot do.)

Anyway, all this is described in gory detail in the link that I gave.

---

"The infinity of syntax comes from assuming that there are an infinite number of variables; F doesn't make this assumption."

This is not correct. A propositional language $L$ with a single unary connective $\neg$ and a single atom $p$ has infinitely many formulas. So, $\mathrm{Form}(L) = \{p, \neg p, \neg\neg p, \ldots\}$ and

$$|\mathrm{Form}(L)| = \aleph_0$$

The potential infinity here is a consequence of the implicit assumptions governing the concatenation operation *. Formulas are, strictu dictu, finite sequences of elements of the alphabet. It is assumed that sequences are closed under concatenation. If $\alpha$, $\beta$ are sequences, then $\alpha * \beta$ is a sequence.

"I guess a stickler might say this is no longer second- (or first-) order logic because these assume that there are an infinite number of variable symbols."

As noted, it has nothing to do with variables. The strings of the propositional language $L$ above form an $\omega$-sequence. In general, if $\alpha$ and $\beta$ are strings from the language $L$, then $\alpha * \beta$ is a string. This is simply assumed.

"But I would hope most would agree this is not an essential feature of the logic." That any standard language $L$ for propositional logic (containing at least one atom and one connective) or first-order logic has cardinality $\aleph_0$ is usually a preliminary exercise in logic.

Posted by: Jeffrey Ketland

---

Well, obviously I wouldn't assume the totality of the concatenation operator.

"As noted, it has nothing to do with variables." This is not correct. Your language is infinitary if the number of variables is infinitary.

"That any standard language $L$ for propositional logic (containing at least one

atom and one connective) or first-order logic has cardinality $\aleph_0$ is usually a preliminary exercise in logic."

Of course. But it's not an essential feature of the logic, in the sense one could give an adequate description of the logic without this feature.

Posted by: t

---

Indeed, the infinitude of variable symbols is entirely a red herring. For those who want a finite alphabet, the standard (AIUI) solution is to have a symbol $x$ and a symbol $'$ such that $x$ is a variable and $v'$ is a variable whenever $v$ is. (Thus the variable symbols are $x$, $x'$, $x''$, etc.)

Posted by: Toby Bartels

---

t, "One gives the usual recursive definitions to syntactical entities like AtomicWff($x$) and Proof($x$)."

What, exactly, are these entities AtomicWff($x$) and Proof($x$)? How many symbols do they contain? Are they distinct? How does one prove this? Have you ever tried to estimate how many symbols occur in the arithmetic translation of the sentence

"the formula $\forall x : (x = x)$ is the concatenation of $\forall x$ with $(x = x)$"?

You're assuming something that you then claim to "doubt". You do not, in fact, "doubt" it: you assume it.

One never says, in discussing the syntax of a language, "if the symbol $\forall$ is distinct from the symbol $v$ ...". Rather, one says, categorically, "the symbol $\forall$ is distinct from the symbol $v$". The claim under discussion amounts to the view that one ought to be "agnostic" about the distinctness of, for example, the strings $\forall x : (x = 0)$ and $\forall y : (y \neq 0)$.

One <u>can</u> write down a formal system of arithmetic which has a "top" – called "arithmetic with a top". But it is not as extreme as $F$. Such theories have been studied in detail by those working in computational complexity and bounded

arithmetic (see, e.g., the standard monograph by Hajek and Pudlak, which I don't have with me).

---

See, e.g., this: [http://www.math.cas.cz/~thapen/nthesis.ps]

Agnosticism about numbers = agnosticism about syntax. You can't have your "strict finitist" cake, while eating your syntactic cake, as they're the same cake!

Jeff

---

"What, exactly, are these entities AtomicWff($x$) and Proof($x$)?"

They are syntactical entities. I could write them down for you explicitly here, but as you can probably tell, I'm not gifted writing down logical symbols in these comments. Or you can look at the top of page 110 and on page 111 of the link, where you will find them already written down explicitly.

"Are they distinct? How does one prove this?"

I'm not sure whether you are talking about meta-theory or theory. In the theory $F$, if you assume there exists something which represents AtomicWff($x$) and another thing which represents Proof($x$), then you would be able to prove these things distinct, because their $i$th symbols will be different for some $i$. But one doesn't need to prove this, certainly not in the proof that the system is consistent. In the meta-theory the two syntactical entities are different, and you see this by writing them down.

"You're assuming something that you then claim to "doubt"."

No I'm not. Again you seem to be confusing meta-theory with theory, or assuming that there must be some tight connection between them. You can't prove that 1 exists in $F$. You agree, right? So $F$ makes no assumptions that I doubt. Sure I can write down a formula in $F$ which has more than one symbol. So? That has no bearing on what $F$ does or does not assume. In any case my doubts are not that 1 exists, or that 10 exists, but that *every* natural number has a successor. And the fact that I can write down a formula with 1

million symbols (well, if you pay me enough) cannot erase my doubts, nor has any bearing on these doubts.

"One never says, in discussing the syntax of a language, "if the symbol $\forall$ is distinct from the symbol $v$ ...".

Your manner of expression is again not clear. "One never says..." Are you talking theory, meta-theory, what? $F$ can prove: "if the symbols $\forall$ and $v$ exist (or to be more precise, if the numbers used to represent them exist), then they are distinct."

"Rather, one says, categorically, "the symbol $\forall$ is distinct from the symbol $v$"." Well, $F$ cannot prove that the numbers representing the symbols exist. But, in order to prove the consistency of itself, $F$ doesn't need to. Proving the consistency of a system, does not require $F$ to show that anything exists. Rather, it has to show that something does *not* exist.

"The claim under discussion amounts to the view that one ought to be "agnostic" about the distinctness of, for example, the strings $\forall x : (x = 0)$ and $\forall y : (y \neq 0)$."

No, no, no. For some reason you are hung up on distinctness. $F$ can prove distinctness. Again, it can prove that if these strings (or more precisely, the sequences representing them) exist, then they are distinct. So $F$ is most certainly not agnostic about their distinctness. All that $F$ cannot prove is: the strings exist.

"One can write down a formal system of arithmetic which has a "top" - called "arithmetic with a top". But it is not as extreme as F. "

Again, you are making imprecise claims. $F$ allows for the possibility of the standard model. Formal systems with a "top" do not. Everything that $F$ proves will be true in PA. There are things that "top" formal systems prove that are false in PA. So what on earth does "extreme" mean?

Posted by: t

---

"So what on earth does 'extreme' mean?"

---

A theory of syntax that doesn't prove that $\forall$ is distinct from $=$?

---

ROTFL. Ok, you win. I'll grant you that $F$ doesn't "prove that symbols are distinct" in the sense of "prove that they exist." And I'll grant you that this means that its "theory of syntax" is "extreme."

Still, in order to prove that a system is consistent, one can work with an "extreme" "theory of syntax" which doesn't "prove that symbols are distinct" because, to prove a system is consistent, one needs to prove that something *doesn't* exist, not to prove that something *does*. (In your terminology, would this be, "one needs to prove that something isn't distinct, not to prove that something is"??) If you or anyone else thinks that $F$ is inconsistent, then you must come up with a proof of "not $0 = 0$". And, by the mere fact of that proof supposedly existing, $F$ can show that it is able to model truth-in-$\{0\}$ for the statements in the proof and so that "not $0 = 0$" cannot be a statement in the proof. Contradiction. Therefore you, or anyone else, cannot come up with a proof. And since all this reasoning can be done in $F$, $F$ can prove its own consistency. It's that simple.

Posted by: t

---

t, I see what you wish to do with this theory $F$. But you lack numerals, since $S$ is not a function symbol. So, instead, for example, one might express $0 \neq 1$ by a formula

$$\forall x \forall y : ((\underline{0}(x) \wedge \underline{1}(y)) \implies x \neq y)$$

where the formulas $\underline{n}(x)$ are given by a recursive definition

$$\begin{aligned} \underline{0}(x) &\Leftrightarrow x = 0 \\ \underline{n+1}(x) &\Leftrightarrow \exists y : (\underline{n}(y) \wedge S(x, y)) \end{aligned}$$

So, to assert the existence of the number 7, for example, you have $\exists x : (\underline{7}(x))$.

And, presumably, for all $k \leq n$,

$$F \vdash \exists x : (\underline{n}(x)) \implies \exists x(\underline{k}(x))$$

Then define $\mathrm{NotEq}_{n,m}$ to be the formulas

$$\forall x \forall y : ((\underline{n}(x) \wedge \underline{k}(y)) \implies x \neq y)$$

Then I believe one has: for all $n$, $k \in \mathbb{N}$,

$$\text{if } n \neq k, \text{ then } F \vdash \mathrm{NotEq}_{n,k}$$

As for syntactic coding, since $\forall$ is coded as 6 and $=$ as 3, then $F$ can define, e.g.,:

$$\begin{aligned} \underline{\forall}(x) &\Leftrightarrow \underline{6}(x) \\ \underline{=}(x) &\Leftrightarrow \underline{3}(x) \end{aligned}$$

Then (I think), $F$ does prove the distinctness of $\forall$ and $=$ in a conditional manner, namely,

$$F \vdash \forall x \forall y : ((\underline{\forall}(x) \wedge \underline{=}(y)) \implies x \neq y)$$

But no, I don't accept that $F$ "proves its own consistency". Just to begin with, one doesn't have a proof predicate which strongly represents the proof relation for $F$.

And to return to the central issue, you are assuming the existence of a language $L_F$ whose cardinality (the cardinality of its set of formulas) is $\aleph_0$ . You're assuming this already in the metatheory. You already have $\aleph_0$ syntactical entities. What is the point of being "agnostic" about, say, the number 1 if you are already assuming, in your informal metatheory, the existence of $\aleph_0$-many syntactical entities? In other words, I am doubting your "agnosticism". You're simply trying to have your syntactic cake while eating (i.e., professing) the "strict finitism" cake. It doesn't work, because they are the same cake.

To repeat: form the point of view of ontology, interpretability, etc., syntax = arithmetic. The same thing. They can be modelled in each other. To "doubt" arithmetic while accepting syntax is incoherent.

To make it work, you need to develop a separate "strictly finite" syntax, for example, a la Quine and Goodman 1947. It would have to drop the totality of concatenation on syntactical entities. It really is not worth bothering with, as it doesn't work, though. At the very best, you simply end up reinventing, in a weird way, all the things that have been discussed countlessly many times in the very rich research literature about nominalism. See, for example,

Burgess, J and Rosen, G. 1997. A Subject with No Object. OUP. Jeff

Posted by: Jeffrey Ketland

---

"(a lot of things snipped)"

You clearly haven't read the linked paper, or even (I imagine) glanced over it, right? That doesn't seem to faze you in the least, though, in making various definitive pronouncements.

"Just to begin with, one doesn't have a proof predicate which strongly represents the proof relation for $F$."

Well, you will have to give a reasoned argument why (the technical notion of) representability is essential to (the intuitive notion of) expressability. Consider the simpler case of even($x$), which can be defined in $F$ as (there exists $y$)($y + y = x$). Because of $F$'s ontological limitations, even($x$) doesn't represent evenness. Yet even($x$) clearly expresses the notion of evenness. I think you can be most succinct in your point by noting that the Hilbert-Bernays conditions of provability do not hold for the provability predicate in $F$. But as I mention in the linked paper, the Hilbert-Bernays conditions do not adequately capture the (intuitive) notion of provability.

"And to return to the central issue, you are assuming the existence of a language LF whose cardinality (the cardinality of its set of formulas) is $\aleph_0$."

If that's the central issue, then you are wrong, as I am not. Look, you obviously haven't read or thought hard about what I've done or written, so perhaps you should stop saying that I am making assumptions which I do not make. Right? That's only fair, right?

"It would have to drop the totality of concatenation on syntactical entities."

Obviously. I see now you have replied in another place about this, so I will now switch there.

Posted by: t

---

I'm trying to understand this discussion. It seems to me that Jeffrey Ketland is saying, roughly, that because our usual theory of syntax can prove that the system $F$ has infinitely many formulas, while $F$ has finite models (as well as infinite ones), the system $F$ is "incoherent" as a theory of arithmetic. For example, he says:

> To repeat: form the point of view of ontology, interpretability, etc., syntax = arithmetic. The same thing. They can be modelled in each other. To "doubt" arithmetic while accepting syntax is incoherent.
>
> So the language LF itself is countably infinite. Denying the existence of numbers while asserting the existence of infinitely many syntactical entities is incoherent, as one of Gödel's basic insights is: syntax = arithmetic.

But this is puzzling in two ways. First of all, I don't think F "denies the existence of numbers": any model of Peano arithmetic will be a model of F, so you can have all the natural numbers you might want. There's a difference between denying something and not asserting something.

But more importantly, I don't really care whether $F$ is "incoherent" from the point of view of "ontology" due to some claimed mismatch between the syntax of theory $F$ (which has infinitely many formulas, according to standard mathematics) and the models $F$ has (which include finite ones). "Incoherent" and "ontology" are philosophical notions, but I'm a mere mathematician. So I'm much more interested in actual theorems about $F$.

If these theorems are proved in a metatheory that can prove $F$ has infinitely many formulas, that's fine! — just make sure to tell me what metatheory is being used. And if someone has proved some other theorems, in a metatheory that can't prove $F$ has infinitely formulas — in other words, a metatheory that more closely resembles $F$ itself — that's fine too! All I really want to know is what's been proved, in what framework.

But I guess it all gets a bit tricky around Gödel's 2nd incompleteness theorem. What does it mean for $F$ to "prove its own consistency"? I guess it means something like this. (I haven't thought about this very much, so bear with me.) Using some chosen metatheory, you can prove

$$F \vdash \mathrm{Con}(F)$$

where Con(F) is some statement in $F$ that according to the chosen metatheory states the consistency of F. The Hilbert-Bernays provability conditions [http://en.wikipedia.org/wiki/Hilbert%E2%80%93Bernays_provability_conditions] are supposed to help us know what "states the consistency of F" means, but if you want to use some other conditions, that's okay — as long as you tell me what they are. I can then make up my mind how happy I am.

From the reference above:

> Let $T$ be a formal theory of arithmetic with a formalized provability predicate Prov($n$), which is expressed as a formula of $T$ with one free number variable. For each formula $\phi$ in the theory, let $\#(\phi)$ be the Gödel number of $\phi$. The Hilbert–Bernays provability conditions are:
>
> 1. If $T$ proves a sentence $\phi$ then $T$ proves Prov($\#(\phi)$).
> 2. For every sentence $\phi$, $T$ proves Prov($\#(\phi)$) $\implies$ Prov($\#$(Prov($\#(\phi)$))).
> 3. $T$ proves that Prov($\#(\phi \implies \Psi)$) and Prov($\#(\phi)$) imply Prov($\#(\Psi)$)

Posted by: John Baez