Tennenbaum's Theorem*

Peter Smith, University of Cambridge

February 28, 2014

Contents

*A first version of these notes were written in 2011 for a reading group on Kaye's *Models of Peano Arithmetic*, in particular for our discussion of his Ch. 11. The notes were revised later after some discussions with Thomas Forster and Zachiri McKenzie. The basic line of proof is still essentially as in Kaye's treatment: but the stripped-down presentation here aims to be reasonably stand-alone and hence, perhaps, more accessible. The usual warning applies: just because it is prettily LaTeXed, that doesn't mean that it's right! All corrections and suggestions for improvement welcome, to ps218@cam.ac.uk.

We are going to prove a key theorem that tells us something about the structure of some of the non-standard models of first-order Peano Arithmetic *PA*. At the end, we add some remarks which *very* briefly consider whether any broadly philosophical/conceptual morals can be drawn from the technical result.

1 The headline news: stating the theorem

Take the non-logical vocabulary of the formalized theory *PA* to be: $\mathsf{0}$, $\mathsf{1}$, $+$, $\times$, $<$.[1]

Then a model $\mathcal{M}$ for *PA* specifies a domain, a 'carrier set' M, picks out two elements of M, $0^{\mathcal{M}}$ and $1^{\mathcal{M}}$, to be the denotations of '$\mathsf{0}$' and '$\mathsf{1}$', specifies a couple of two-place functions $\oplus$ and $\otimes$ defined over M to be assigned as interpretations to '$+$' and '$\times$', and specifies a two-place relation $\lessdot$ defined over M to be assigned as interpretation to '$<$'. So we can put $\mathcal{M} =_{\text{def}} (M, 0^{\mathcal{M}}, 1^{\mathcal{M}}, \oplus, \otimes, \lessdot)$.

The standard model for *PA* is of course $\mathcal{N} =_{\text{def}} (\mathbb{N}, 0, 1, +, \times, <)$, where $\mathbb{N}$ is the set of the familiar natural numbers of everyday arithmetic, 0 and 1 are the familiar zero and one, the functions $+$ and $\times$ are familiar addition and multiplication, and the order relation is the natural order relation on the natural numbers. ('Familiar' here of course papers over some issues that we will return to touch on at the end; but the issues aren't at stake in the proof of our target theorem.)

It is immediate from the Löwenheim-Skolem theorem that *PA* (assumed here to be consistent) has oodles of non-standard models too, because – like any first-order theory with a countably infinite model – it has models of any infinite cardinality. More excitingly, there are even oodles of *countable* non-standard models of *PA*, i.e. non-standard models whose carrier set M is countable. (Indeed, though it isn't especially relevant here, there are continuum-many pairwise non-isomorphic countable models of *PA*.)

Now, without loss of generality, we can take the domain of any countable model $\mathcal{M}$ to be the natural numbers again, and in that case $\oplus$ and/or $\otimes$ will be arithmetical functions. To build the model, we need to re-order the numbers by $\lessdot$ and define new arithmetic $\oplus$ and $\otimes$ functions. We know the numbers ordered by $\lessdot$ must then begin with the new zero and its 'successors' ('adding' the new unit, according to the model's $\oplus$ function), But then – because we are in a non-standard model – there will stuff coming after zero and all its successors. So far, so abstract. But when we try to *describe* a suitable non-standard $\oplus$ function (and hence corresponding order relation) on the numbers, no natural construction seems to do the job. Tennenbaum 's theorem tells us why. $\oplus$ (and $\otimes$) can't be recursive.

We can state the result like this:

Theorem 1. *Any countable model* $\mathcal{M}_{\mathbb{N}} =_{\text{def}} (\mathbb{N}, 0^{\mathcal{M}}, 1^{\mathcal{M}}, \oplus, \otimes, \lessdot)$ *of PA where* $\oplus$ *and/or* $\otimes$ *is recursive is isomorphic to* $\mathcal{N}$.

In other jargon, there is (up to isomorphism, of course) only one recursive model of *PA*.

2 Fixing notation and terminology

Let's nail down some more symbolism and terminology, and give a few reminders:

[1] If you prefer to set up *PA* without the constant '1' and without the relation '$<$' built in, and with a primitive expression 'S' for the successor function and a defined less-than relation instead, be my guest. Nothing important hangs on that kind of minor tweaking.

1. Symbolism: As we said, we'll take the non-logical vocabulary of the formalized theory *PA* to be: $\mathsf{0}$, $\mathsf{1}$, $+$, $\times$, $<$. You can't tell with the last three, but those symbols are all in sans-serif font(!), and we will adopt the nice convention of using sans-serif for all wffs and other expressions of the language of *PA* (and also for formal expressions added to the formal language by definition). By contrast, ordinary informal mathematical symbols will be in *italics* as usual. Note that n, like other mid-alphabet variables, is always a variable running over the ordinary natural numbers (i.e. over $\mathbb{N}$).

2. In this version of *PA*, the *standard numerals* are simply the expressions '$\mathsf{0}$', '$\mathsf{1}$', '$\mathsf{1+1}$', '$\mathsf{1+1+1}$', '$\mathsf{1+1+1+1}$', ... We will use $\overline{\mathsf{n}}$ to abbreviate the n-th such numeral (counting from zero). According to the standard model $\mathcal{N}$, $\overline{\mathsf{n}}$ denotes n.

3. Any model $\mathcal{M}$ of *PA* must supply elements to be the denotations for the standard numerals i.e. for '$\mathsf{0}$', '$\mathsf{1}$', '$\overline{\mathsf{2}}$' (i.e. '$\mathsf{1+1}$'), '$\overline{\mathsf{3}}$' (i.e. '$\mathsf{1+1+1}$'), etc. These denotations will be respectively the elements $0^{\mathcal{M}}$, $1^{\mathcal{M}}$, $2^{\mathcal{M}}$ (i.e. $1^{\mathcal{M}} \oplus 1^{\mathcal{M}}$), $3^{\mathcal{M}}$ (i.e. $2^{\mathcal{M}} \oplus 1^{\mathcal{M}}$), etc.. We'll say $\overline{\mathsf{n}}$ denotes $n^{\mathcal{M}}$ in $\mathcal{M}$.

   These $n^{\mathcal{M}}$ can be called $\mathcal{M}$'s *standard elements*. Only in models isomorphic to the standard model, however, are all the elements in the carrier set standard elements. (In fact, as we noted, in non-standard models the standard elements form a proper initial segment of the domain under the ordering $\otimes$.)

4. Suppose model $\mathcal{M}$, together with the assignment of the element e to the variable 'x', satisfies the open wff $\varphi(\mathsf{x})$. Then, for brevity, we'll write $\mathcal{M} \vDash \varphi([e])$. This is simply shorthand for what might also (in some ways, more perspicuously) be written e.g. $\mathcal{M}, e \vDash \varphi(\mathsf{x})$. But for ease of comparison, I'm mostly adopting the brisker notation here.

5. Finally, for future use, let π_n be the n-th prime (again, we count from zero, so $\pi_0 = 2, \pi_1 = 3, \pi_2 = 5, \ \ldots$). The function $\pi : \ n \to \pi_n$ is primitive recursive, and it can in fact be (strongly) represented in the language of *PA* by a Δ_0 wff $\mathsf{P(x,y)}$, so that for any n, $\mathcal{N} \vDash \mathsf{P}(\overline{\mathsf{n}}, \overline{\pi_n})$ and $PA \vdash \mathsf{P}(\overline{\mathsf{n}}, \overline{\pi_n})$, where of course $\overline{\pi_n}$ is the formal numeral '$\mathsf{1+1+\ldots+1}$' with π_n summands.

   Suppose we want to say in *PA* that the k-th prime multiplied by l equals m. Then we'd officially need to write (i) $\exists\mathsf{y}(\mathsf{P}(\overline{\mathsf{k}}, \mathsf{y}) \wedge \mathsf{y} \times \overline{\mathsf{l}} = \overline{\mathsf{m}})$ – or better, we can keep things Δ_0 by writing restricting the initial quantifier and using $(\exists\mathsf{y} \leq \overline{\mathsf{m}})$. For ease of notation, however, we'll suppose that – as will be permissible, since P will be functional – we've definitionally added to *PA* a function expression 'p' defined in the terms of P so that '$\mathsf{p(x) = y}$' is equivalent to '$\mathsf{P(x,y)}$'. Then we can write (ii) $\mathsf{p}(\overline{\mathsf{k}}) \times \overline{\mathsf{l}} = \overline{\mathsf{m}}$.

   Suppose we want to say in the language of *PA* that the n-th prime divides m: then we can write (iii) $(\exists\mathsf{y} \leq \overline{\mathsf{m}})(\mathsf{p}(\overline{\mathsf{n}}) \times \mathsf{y} = \overline{\mathsf{m}})$. But for convenience it will be useful to introduce shorthand to express divisibility, and abbreviate (iii) as (iv), $\mathsf{p}(\overline{\mathsf{n}}) \,/\, \overline{\mathsf{m}}$.[2]

[2] I use '$a \,/\, b$' rather than '$a \mid b$' because the latter occurring between set-former braces can give rise to expressions of the form '$\{\ldots a \mid b \ldots\}$' which long habit might make you misread.

3 A result about recursive inseparability

Before getting to the meat of the proof of (part of) Tennenbaum's Theorem, we need a few very quick background results (which could well be just reminders). We start by recalling a standard definition from computability theory.

Two sets of numbers $A \subseteq \mathbb{N}$ and $B \subseteq \mathbb{N}$ are recursively inseparable if and only if (i) they are disjoint but (ii) there is no recursive set $S \subseteq \mathbb{N}$ such that $A \subseteq S$ and $B \subseteq \overline{S}$. In other words, A and B are disjoint, but you can't separate them by throwing a recursively-defined lasso S around all of A (and maybe more) while capturing none of B.

An elementary theorem concerning this notion is

Theorem 2. *There are disjoint recursively enumerable sets of numbers A and B which are not recursively separable.*

Proof. Let φ_e be the one-place partial function computed by the e-th Turing machine. Put $A = \{e : \varphi_e(e) = 0\}$ and $B = \{e : \varphi_e(e) = 1\}$. Plainly, A and B are disjoint. They are also both recursively enumerable (just start doing a zigzag though steps of the computations of $\varphi_0(0)$, $\varphi_1(1)$, $\varphi_2(2)$ ... and eventually every computation of a $\varphi_e(e)$ which terminates will indeed deliver an output: put the values of e where $\varphi_e(e) = 0$ into A, and the values of e where $\varphi_e(e) = 1$ into B, and there are our desired enumerations).

Suppose S is a recursive set separating A from B, so $A \subseteq S$ and $B \subseteq \overline{S}$. Then some total computable function φ_s is S's characteristic function, which is to say $S = \{n : \varphi_s(n) = 1\}$, $\overline{S} = \{n : \varphi_s(n) = 0\}$. But then we have either $s \in S$ or $s \in \overline{S}$, yet each disjunct immediately leads to contradiction. □

4 A result about overspill and Δ_0-absoluteness

Now back to a couple of results PA and its models. We note a simple form of 'overspill' theorem:

Theorem 3. *Suppose that $\mathcal{M}$ is a non-standard model of PA such that, for all n, $\mathcal{M} \vDash \varphi(\overline{\mathsf{n}})$. Then there is a non-standard element e which also satisfies $\varphi(\mathsf{x})$, i.e. such that $\mathcal{M} \vDash \varphi([e])$.*

Proof. Suppose that all but *only* standard elements satisfy $\varphi(\mathsf{x})$. Then, trivially, we have $\mathcal{M} \vDash \varphi(\mathsf{0})$. And consider the wff $\varphi(\mathsf{x}) \to \varphi(\mathsf{x}+1)$. If the antecedent is true of an element, the element must be standard, then that element's successor will be standard and must satisfy φ too. Hence $\mathcal{M} \vDash \forall\mathsf{x}(\varphi(\mathsf{x}) \to \varphi(\mathsf{x}+1))$. But $\mathcal{M}$ must also satisfy PA's induction axiom for φ. So we can conclude $\mathcal{M} \vDash \forall\mathsf{x}\varphi(\mathsf{x})$, so φ is satisfied by the non-standard elements after all. Contradiction. □

Look at it this way: there's no φ such $\mathcal{M}$ 'knows' that its standard elements are just that things which satisfy φ.

Next, a reminder of the very basic fact that non-standard models of PA are well-behaved with respect to Δ_0 truths: that is to say.

Theorem 4. *If φ is a Δ_0 sentence and $\mathcal{N} \vDash \varphi$, then for any model $\mathcal{M}$ of PA, $\mathcal{M} \vDash \varphi$.*

Proof. If φ is a Δ_0 truth of arithmetic, i.e. $\mathcal{N} \vDash \varphi$, then $PA \vdash \varphi$ because PA is Δ_0 complete. Therefore any model of PA, standard or non-standard, must make φ true. □

5 Coding sets of numbers – the basics

Think informally for a moment. Fix on a monadic property C. Then the following is true for any natural number bound m: there is a number c such that, for all $k < m$, k has property C if and only if π_k divides c. Why? Well, we can just set c to be a product of the primes π_k such that both $k < m$ and k has C. In an obvious sense, we can treat c as a code for numbers with property C which are less than m: we decode by prime factorization – k has C iff $\pi_k \,/\, c$, i.e. iff the k-th prime divides c.

Trading in properties for their extensions and going formal, we have the following. Let S be some set of numbers bounded by the number m. Then there is a code number c for the set such that $S = \{n : \mathcal{N} \vDash \mathsf{p}(\overline{\mathsf{n}}) \,/\, \overline{\mathsf{c}}\}$. Or equivalently, of course, we could write $S = \{n : \mathcal{N} \vDash \mathsf{p}(\overline{\mathsf{n}}) \,/\, [c]\}$.[3]

So far so elementary. But of course in $\mathcal{N}$, elements c – being finite, and having only a finite number of prime divisors – can only be used to code up finite sets in this way. However, now let's generalize and think about what can happen in non-standard models. We will say that $S \subseteq \mathbb{N}$ is *canonically coded* by c in the model $\mathcal{M}$ just if $S = \{n : \mathcal{M} \vDash \mathsf{p}(\overline{\mathsf{n}}) \,/\, [c]\}$. So a number n is in S just in case, when we look at the denotation d of $\mathsf{p}(\overline{\mathsf{n}})$ according to $\mathcal{M}$ (so $d = \pi_n^{\mathcal{M}}$), we can find some element $e \in M$ such that $d \otimes e = c$. Note: A non-standard element c inside $\mathcal{M}$ might have an infinite number of 'prime divisors' according to $\mathcal{M}$, and so the coded set S can now be infinite.

6 Other codings?

Having got the basic idea of coding a (possibly infinite) set of numbers by an element in a model, we might now wonder about liberalizing the idea beyond coding-by-primes. We could use instead e.g. the trick of coding using the relation E where mEn when the m-th bit of the binary representation of n is 1, and again this is easily formalized.

But let's go for generality: let's say that $S \subseteq \mathbb{N}$ can be *simply coded* in $\mathcal{M}$ just if there is a Δ_0 wff *PA*-formula $\varphi(\mathsf{x}, \mathsf{y})$ and element b in the model such that $S = \{n : \mathcal{M} \vDash \varphi(\overline{\mathsf{n}}, [b])\}$. We now remark that

Theorem 5. *If φ is Δ_0, and $\mathcal{M}$ is a non-standard model of PA, then for any element $b \in M$ there is a $c \in M$ such that for any natural number n,*

$$\mathcal{M} \vDash \varphi(\overline{\mathsf{n}}, [b]) \leftrightarrow \mathsf{p}(\overline{\mathsf{n}}) \,/\, [c],$$

so any set simply coded using φ can be canonically coded using prime divisors.

In other words, as long as we keep to 'simple' codings that can be handled by Δ_0 wffs, it isn't going to matter which coding we choose.

For the record, here's a proof (which illustrates how the overspill lemma can be used):

Proof. Temporarily fix a number m. Then consider the *PA*-wff

$$\forall \mathsf{b} \exists \mathsf{c} (\forall \mathsf{u} < \overline{\mathsf{m}})\{\varphi(\mathsf{u}, \mathsf{b}) \leftrightarrow \mathsf{p}(\mathsf{u}) \,/\, \mathsf{c}\,\}.$$

Given what we've said before, this is very elementarily seen to be true on the standard interpretation. For it just says: take any number b, then there is a code number c such

[3]Reality check: the condition on the right is just short hand for saying that in the model $\mathcal{N}$, c satisfies the open wff $(\exists \mathsf{y} \leq \mathsf{x})(\mathsf{p}(\overline{\mathsf{n}}) \times \mathsf{y} = \mathsf{x})$.

that – for numbers u below the bound m – the pair (u, b) satisfies φ just in case π_u divides c. (Which is trivial, since we can just put c equal to the product of the π_u for u such that (u, b) satisfies φ.)

Since this is such a very elementary truth (given φ is Δ_0), and *PA* is so very powerful, we can cheerfully assume

$$PA \vdash \forall \mathsf{b} \exists \mathsf{c} (\forall \mathsf{u} < \overline{\mathsf{m}}) \{\varphi(\mathsf{u}, \mathsf{b}) \leftrightarrow \mathsf{p}(\mathsf{u}) \,/\, \mathsf{c}\},$$

and hence for any arbitrary non-standard model $\mathcal{M}$,

$$\mathcal{M} \vDash \forall \mathsf{b} \exists \mathsf{c} (\forall \mathsf{u} < \overline{\mathsf{m}}) \{\varphi(\mathsf{u}, \mathsf{b}) \leftrightarrow \mathsf{p}(\mathsf{u}) \,/\, \mathsf{c}\}.$$

Since this holds for any m, we can apply the overspill Theorem 2, so for some non-standard element $e \in M$:

$$\mathcal{M} \vDash \forall \mathsf{b} \exists \mathsf{c} (\forall \mathsf{u} < [e]) \{\varphi(\mathsf{u}, \mathsf{b}) \leftrightarrow \mathsf{p}(\mathsf{u}) \,/\, \mathsf{c}\}.$$

This means for any $b \in M$ there will be an element $c \in M$ such that

$$\mathcal{M} \vDash (\forall \mathsf{u} < [e]) \{\varphi(\mathsf{u}, [b]) \leftrightarrow \mathsf{p}(\mathsf{u}) \,/\, [c]\}.$$

However, every standard element $n^{\mathcal{M}}$ is 'less than' a non-standard element in $\mathcal{M}$ (i.e. $n^{\mathcal{M}} \otimes e$). So for any element b there is an c such that we certainly have for all n

$$\mathcal{M} \vDash \varphi(\overline{\mathsf{n}}, [b]) \leftrightarrow \mathsf{p}(\overline{\mathsf{n}}) \,/\, [c].$$

Which is just what we set out to prove. □

7 Non-standard models can code non-recursive sets

Recall the standard theorem that the only sets straightforwardly definable in *PA* are recursive. We are now going to show that, in contrast, coding-by-non-standard-elements-in-non-standard-models can pick out non-recursive sets, by giving an example which proves:

Theorem 6. *For any non-standard model $\mathcal{M}$ of PA, there is a corresponding non-recursive set $X \subset \mathbb{N}$ which is canonically coded in $\mathcal{M}$ by an element c. Moreover, $n \in X$ iff there is an element e in the model such that $c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e$ (for π_n summands).*

Proof of first part. Suppose A and B are recursively enumerable yet recursively inseparable subsets of $\mathbb{N}$.

Being recursively enumerable, there will be Σ_1 wffs $\exists \mathsf{u} \mathsf{A}(\mathsf{u}, \mathsf{x})$ and $\exists \mathsf{u} \mathsf{B}(\mathsf{u}, \mathsf{x})$ that define these sets, where the kernels A and B are Δ_0.

Since A and B are disjoint, then in particular, for any m,

$$\mathcal{N} \vDash (\forall \mathsf{x} < \overline{\mathsf{m}})(\forall \mathsf{v} < \overline{\mathsf{m}})(\forall \mathsf{w} < \overline{\mathsf{m}}) \neg(\mathsf{A}(\mathsf{v}, \mathsf{x}) \wedge \mathsf{B}(\mathsf{w}, \mathsf{x})).$$

But now remark that the wff we've just constructed out of the Δ_0 kernels is still Δ_0, so by the Δ_0-absoluteness Theorem 4, for any non-standard $\mathcal{M}$ and any m,

$$\mathcal{M} \vDash (\forall \mathsf{x} < \overline{\mathsf{m}})(\forall \mathsf{w} < \overline{\mathsf{m}})(\forall \mathsf{v} < \overline{\mathsf{m}}) \neg(\mathsf{A}(\mathsf{v}, \mathsf{x}) \wedge \mathsf{B}(\mathsf{w}, \mathsf{x})).$$

So by the overspill Theorem 3, for some non-standard element e belonging to M, we get

$$\mathcal{M} \vDash (\forall \mathsf{x} < [e])(\forall \mathsf{v} < [e])(\forall \mathsf{w} < [e])\neg(\mathsf{A}(\mathsf{v},\mathsf{x}) \wedge \mathsf{B}(\mathsf{w},\mathsf{x})).$$

Hence, but since for any n, $\mathcal{M} \vDash \overline{\mathsf{n}} < [e]$ for non-standard e, we get the *exclusion principle* that for any n,

$$\mathcal{M} \vDash (\forall \mathsf{v} < [e])(\forall \mathsf{w} < [e])\neg(\mathsf{A}(\mathsf{v},\overline{\mathsf{n}}) \wedge \mathsf{B}(\mathsf{w},\overline{\mathsf{n}})).$$

Let's now define $X \subseteq \mathbb{N}$ to be the set $\{n : \mathcal{M} \vDash (\exists \mathsf{v} < [e])\mathsf{A}(\mathsf{v},\overline{\mathsf{n}})\}$. And note the following two easy facts about X:

1. $A \subseteq X$. For if $n \in A$, then for some m, $\mathcal{N} \vDash \mathsf{A}(\overline{\mathsf{m}},\overline{\mathsf{n}})$. So by Theorem 4, $\mathcal{M} \vDash \mathsf{A}(\overline{\mathsf{m}},\overline{\mathsf{n}})$, whence $\mathcal{M} \vDash (\exists \mathsf{v} < [e])\mathsf{A}(\mathsf{v},\overline{\mathsf{n}})$, since the standard element denoted by $\overline{\mathsf{m}}$ stands in the relation $\otimes$ to any non-standard element.

2. $B \cap X = \emptyset$. For if $n \in B$, then for some m, $\mathcal{N} \vDash \mathsf{B}(\overline{\mathsf{m}},\overline{\mathsf{n}})$. So, arguing similarly, $\mathcal{M} \vDash (\exists \mathsf{w} < [e])\mathsf{B}(\mathsf{w},\overline{\mathsf{n}})$. Whence $\mathcal{M} \vDash \neg(\exists \mathsf{v} < [e])\mathsf{A}(\mathsf{v},\overline{\mathsf{n}})\}$, by the exclusion principle, so $n \notin X$.

Hence X can't be recursive, else A and B would be recursively separable, contrary to hypothesis. But now note that X is defined by a Δ_0 wff (formed by applying a bounded quantifier to a Δ_0 wff) so Theorem 5 applies, and hence X can serve as the desired example of a set of natural numbers which can be canonically coded by an element c in $\mathcal{M}$ but which is not recursive. □

Proof of second part. We have just shown that is an element c in the model such that $X = \{n : \mathcal{M} \vDash \mathsf{p}(\overline{\mathsf{n}}) \,/\, [c]\}$, i.e. $n \in X$ iff $\mathcal{M} \vDash \exists \mathsf{y}(\mathsf{p}(\overline{\mathsf{n}}) \times \mathsf{y} = [c])$, i.e. $n \in X$ iff for some element e, $\mathcal{M} \vDash (\mathsf{p}(\overline{\mathsf{n}}) \times [e] = [c])$.

We now remark that for any m, $PA \vdash \forall \mathsf{y}(\overline{\mathsf{m}} \times \mathsf{y} = \mathsf{y} + \mathsf{y} + \ldots + \mathsf{y})$ where we have m summands on the right, so in particular $PA \vdash \forall \mathsf{y}(\mathsf{p}(\overline{\mathsf{n}}) \times \mathsf{y} = \mathsf{y} + \mathsf{y} + \ldots + \mathsf{y})$ where we have π_n summands on the right. Whence $\mathcal{M} \vDash \forall \mathsf{y}(\mathsf{p}(\overline{\mathsf{n}}) \times \mathsf{y} = \mathsf{y} + \mathsf{y} + \ldots + \mathsf{y})$ with π_n summands. Hence we must have in particular $\pi_n^{\mathcal{M}} \otimes e = e \oplus e \oplus e \oplus \cdots \oplus e$ with π_n summands. Which gives us the target result: $n \in X$ iff there is a e in the model $\mathcal{M}$ such that $c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e$ (for π_n summands). □

8 And so, at last, to Tennenbaum's Theorem

Now suppose that (in fact for the first time!) we start concentrating on *countable* models $\mathcal{M}_{\mathbb{N}} =_{\text{def}} (\mathbb{N}, 0^{\mathcal{M}}, 1^{\mathcal{M}}, \oplus, \otimes, \otimes)$.[4] So now the two-place functions $\oplus$ and $\otimes$ are themselves *numerical* functions, hence it makes sense to wonder whether they are recursive. We'll show that $\oplus$ can't be.

Take a non-standard countable model $\mathcal{M}_{\mathbb{N}}$. Then we have shown that there is a set $X \subset \mathbb{N}$, where

1. X is non-recursive, but

[4]Actually, we could take the interpretations of '0', '1' to be standard too: for any given countable model $\mathcal{M}$ with domain $\mathbb{N}$ that gives a deviant interpretation $0^{\mathcal{M}}$ for '0' and $1^{\mathcal{M}}$ for '1', there will be an isomorphic model $\mathcal{M}'$ which permutes $0^{\mathcal{M}}$ with 0 and $1^{\mathcal{M}}$ with 1, making compensating adjustments to the interpretations of '+', '×', '<'). But let's not fuss about this.

2. there is an element c in the model $\mathcal{M}_{\mathbb{N}}$ (which will in fact be a number, since now the carrier set M is none other than $\mathbb{N}$) which canonically codes for X, and where $n \in X$ iff there is a e in the model $\mathcal{M}_{\mathbb{N}}$ such that $c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e$ (for π_n summands).

Now suppose, for reductio, that $\oplus$ is recursive. And we set off on a search through the natural numbers taken in their *natural* order (remember, the naturals constitute the domain of $\mathcal{M}$, and c is just a particular number among them). We search until we hit a number e such the following disjunction holds,

$$\begin{aligned}
\text{either}\ \ & c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e \text{ (with } \pi_n\ e\text{s here and in each disjunct)}\\
\text{or}\ \ & c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e \oplus 1^{\mathcal{M}}\\
\text{or}\ \ & c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e \oplus 1^{\mathcal{M}} \oplus 1^{\mathcal{M}}\\
\text{or}\ \ & c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e \oplus 1^{\mathcal{M}} \oplus 1^{\mathcal{M}} \oplus 1^{\mathcal{M}}\\
& \vdots\\
\text{or}\ \ & c = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e \oplus 1^{\mathcal{M}} \oplus 1^{\mathcal{M}} \oplus 1^{\mathcal{M}} \oplus \ldots \oplus 1^{\mathcal{M}} \text{ (with } \pi_n - 1\ 1^{\mathcal{M}}\text{s).}
\end{aligned}$$

By our assumption that $\oplus$ is recursive, we can mechanically check whether the disjunction holds.

Now, our (if sensibly conducted by interleaving searches) the search for an element e which makes the disjunction true must terminate. Why? Recall: for any c, b, where $b \neq 0$, there are unique numbers, a divisor e and remainder $r < b$, such that $c = b \times e + r$. And *PA* can state and prove a formal sentence which says this. Hence our model $\mathcal{M}_{\mathbb{N}}$ must make this true, i.e. must ensure that for any c and $b \neq 0^{\mathcal{M}}$, there is an e and $r \otimes e$ such that $c = (b \otimes e) \oplus r$. Now take the particular case where b is the standard element $\pi_n^{\mathcal{M}}$. But $\pi_n^{\mathcal{M}} \otimes e = e \oplus e \oplus e \oplus e \oplus \ldots \oplus e$ with π_n summands. And if $r \otimes \pi_n^{\mathcal{M}}$, then $r = 0$ or $r = 1 \oplus 1 \oplus 1 \oplus \ldots \oplus 1$ for some number of summands less than π_n (since $PA \vdash \forall \mathsf{x}(\mathsf{x} < \overline{\pi_n} \leftrightarrow \mathsf{x} = 0 \lor \mathsf{x} = 1 \lor \mathsf{x} = 1 + 1 \lor \ldots \mathsf{x} = 1 + 1 + 1 + \ldots + 1))$.

Suppose, then, that the search terminates verifying a disjunct of the first kind (with no remainder): then $n \in X$. Otherwise, the search terminates with one of the other disjuncts verified, and then $n \notin X$.

So, in sum, if $\oplus$ recursive, we have a decision procedure for membership of X, and so X will be recursive. But by hypothesis X isn't recursive. Hence $\oplus$ is not recursive. Which proves an official version of (part of) Tennenbaum's theorem:

Theorem 7. *If $\mathcal{M}_{\mathbb{N}} = \langle \mathbb{N}, 0, 1, \oplus, \otimes, \otimes \rangle$ is a non-standard model of PA with domain the natural numbers, then $\oplus$ is not recursive.*

There's a similar proof that shows the other part of Tennenbaum's theorem in this version: if $\mathcal{M} = \langle \mathbb{N}, 0, 1, \oplus, \otimes, \otimes \rangle$ is a non-standard model of *PA* with domain the natural numbers, then $\otimes$ is not recursive. (But note, there can be non-standard models in the natural numbers where the relation $\otimes$ *is* recursive.)

9 Aside: How not to prove Tennenbaum's Theorem

It is instructive to consider why a certain simpler proof strategy doesn't work. The background thought that might tempt us astray is the observation that many familiar limitative results (Gödel's Theorem, the unsolvability of the *Entscheidungsproblem*, etc.) can be quickly derived from the unsolvability of the halting problem. So can we get Tennenbaum's Theorem the same way?

To reduce the number of variables we need to worry about, take the *self*-halting relation $H(e,t)$ which holds if and only the Turing machine numbered e in a standard enumeration, when given the numeral for e as input, has halted by the t-th tick of the computational clock. $H(e,t)$ is primitive recursive.

Let's fix an arbitrary bound m for the moment. There's evidently a finite number of j (often zero!) where $j < m$ and $\exists t H(j,t)$. So here's an elementary arithmetic proposition (of informal mathematics):

$$\exists c(\forall j < m)(\exists t H(j,t) \leftrightarrow \pi_j \,/\, c).$$

And now we do a similar trick as we've done before. *PA* knows a lot about primitive recursive stuff and elementary arithmetic, so we'll expect that for any m,

$$PA \vdash \exists \mathsf{c}(\forall \mathsf{j} < \overline{\mathsf{m}})(\exists \mathsf{t}\mathsf{H}(\mathsf{j},\mathsf{t}) \leftrightarrow \mathsf{p}(\mathsf{j}) \,/\, \mathsf{c}),$$

where H represents the relation H.

Whence for any model $\mathcal{M}$ of *PA*, and any m

$$\mathcal{M} \vDash \exists \mathsf{c}(\forall \mathsf{j} < \overline{\mathsf{m}})(\exists \mathsf{t}\mathsf{H}(\mathsf{j},\mathsf{t}) \leftrightarrow \mathsf{p}(\mathsf{j}) \,/\, \mathsf{c}).$$

We can now apply the Overspill Lemma again, which will tell us that if $\mathcal{M}$ is non-standard, there will must consequently be a non-standard element e in $\mathcal{M}$ such that

$$\mathcal{M}, e \vDash \exists \mathsf{c}(\forall \mathsf{j} < \mathsf{x})(\exists \mathsf{t}\mathsf{H}(\mathsf{j},\mathsf{t}) \leftrightarrow \mathsf{p}(\mathsf{j}) \,/\, \mathsf{c}).$$

That is to say, given non-standard $\mathcal{M}$, there must be a non-standard element e and an element c in the model (in fact it will also be non-standard) such that

$$\mathcal{M}, e, c \vDash (\forall \mathsf{j} < \mathsf{x})(\exists \mathsf{t}\mathsf{H}(\mathsf{j},\mathsf{t}) \leftrightarrow \mathsf{p}(\mathsf{j}) \,/\, \mathsf{y}).$$

But in particular, any standard element $n^{\mathcal{M}} \otimes e$, since e is non-standard. So, a fortiori, for any n

$$\mathcal{M}, c \vDash \exists \mathsf{t}\mathsf{H}(\overline{\mathsf{n}},\mathsf{t}) \leftrightarrow \mathsf{p}(\overline{\mathsf{n}}) \,/\, \mathsf{x}).$$

In other words, we've got as far as this:

Theorem 8. *Given a non-standard model $\mathcal{M}$, there must be an element c in the model such that for any n, $\mathcal{M} \vDash \exists \mathsf{t}\mathsf{H}(\overline{\mathsf{n}},\mathsf{t})$ iff inside the model, the n-th prime according to the model divides c.*

Suppose now $\mathcal{M}$ is a countable non-standard model with carrier set $\mathbb{N}$, then it makes sense to wonder whether the function $f(n,c)$ that finds the n-th prime according to the model and then determines whether it divides c according to the model might be recursive. And it might be tempting to argue that

1. If $\oplus, \otimes, \otimes$ are recursive, so is f, since stuff about primes and divisibility is definable in terms of plus, times, and less-than.

2. If f is recursive, we have a decision procedure for settling whether $\mathcal{M} \vDash \exists \mathsf{t}\mathsf{H}(\overline{\mathsf{n}},\mathsf{t})$.

3. But there can't be a decision procedure for deciding, for any n, whether $\mathcal{M} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$, for we can't decide the self-halting problem.

4. Hence, we can infer a version of Tennenbaum's theorem (the version depending on step 1): in a countable non-standard model, [some selection of] $\oplus, \otimes, \otimes$ can't all be recursive.

But unfortunately this argument limps at step 3. The unsolvability of the self-halting problem tells you that there is no way of deciding whether $\mathcal{N} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$. But $\mathcal{N} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$ is not equivalent to $\mathcal{M} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$.

Because $\exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$ should be Σ_1, if $\mathcal{N} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$, then $PA \vdash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$, then $\mathcal{M} \vDash \exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$. *But the reverse conditional doesn't hold*: $\exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$ could be true-in-$\mathcal{M}$ because the model supplies a non-standard witness, without $\exists \mathsf{tH}(\bar{\mathsf{n}}, \mathsf{t})$ being really true, true in $\mathcal{N}$.

10 Concluding philosophical remarks

Tennenbaum's Theorem is very cute and has technical interest: but does it have any especial *philosophical* or *conceptual* significance?

Well, it might be suggested that we have a grip on (i) the idea of a function's being computable-by-algorithm and (ii) an understanding of addition and multiplication in particular as indeed being computable-by-algorithm. So, the thought continues, assuming Church's Thesis that computability-by-algorithm is equivalent to recursiveness, Tennenbaum's Theorem shows that our arithmetical talk must indeed be latching on to the only possible recursive model (up to isomorphism), i.e. the so-called standard model of arithmetic. And this, it might be supposed, should quiet Skolemite doubts about whether we are really talking about a particular structure (up to isomorphism) when we do arithmetic, [5]

In response to this suggested line of thought, I'll make two quick comments, one very general, one much more specific. For a little more, see my short joint paper with Tim Button, http://philmat.oxfordjournals.org/content/early/2011/11/17/philmat.nkr031.full.pdf.

(1) The general comment is that it is in fact quite unclear that there is, hereabouts, a cogent question to which an appeal to Tennenbaum's Theorem could be a cogent answer. Suppose that we are looking from the outside at aliens, so to speak, an area of whose idealized practice seems to amount to endorsing some as-yet-uninterpreted-by-us first-order theory T. Then we can ask the interpretative question: what do *their* terms refer to, and what extensions do *their* predicates have? And our mathematical knowledge of the multiplicity of models for a consistent first-order T, i.e. of the multiplicity of available interpretations that charitably make them come out speaking the truth, does raise a seemingly sensible question: is there, for all that, a determinate answer to the question of what our aliens are talking about, and if so, what determines it? If, for example, their

[5] For discussions around and about this line of thought, see Walter Dean (2002), 'Models and recursivity', http://www.walterdean.com/DEANmodelsAndRecursivity.pdf, Volker Halbach and Leon Horsten (2005) 'Computational structuralism', *Philosophia Mathematica* 13, pp. 174–186, also at http://users.ox.ac.uk/∼sfop0114/pdf/compstruct.pdf, and Paula Quinon and Konrad Zdanowski (2006), 'The Intended Model of Arithmetic. An Argument from Tennenbaum's Theorem', http://www.impan.pl/∼kz/files/PQKZ_Tenn.pdf.

theory looks rather like *PA*, what if anything fixes that they really are talking about the natural numbers *we* know and love rather than something non-standard?

So far, so good, perhaps. But it doesn't follow that it makes equal sense to start treating *ourselves* as aliens and to wonder whether *we* are really talking about the natural numbers or some non-standard model. We can work inside our own mathematical language: here we have a working understanding of talk of numbers and their natural order, and (piggy-backing on that basic understanding) we can go on to reach an understanding of – inter alia – talk about other structures built from the numbers with a deviant ordering. Alternatively, we can bracket our understanding, and try to can stand outside our practice. But we can't simultaneously do *both*: we can't understand the idea of standard vs other models because we are working *inside* maths, and at the same time treat our own mathamatical discourse as alien, awaiting radical interpretation from *outside*.

The general thought, then, is that what we need in order to sooth the itch that tempts us to Skolemite scepticism is not more technicalities to weigh against the technicalities of a non-categoricity proof, but something quite different – namely some reminders of where we are supposed to be in the story when we wonder about our own arithmetical practice. And if that is the right kind of therapy, then an appeal to a technical result like Tennenbaum's Theorem is necessarily going to be distractingly beside the point.

(2) But let's try to set aside those sorts of general concern and pretend we understand the project of explaining our own grasp of the standard model of arithmetic. There's still a special problem about appealing to Tennenbaum's Theorem in any explanation of the supposedly desired kind.

The idea, recall, was that we can appeal to our given understanding of addition and multiplication as computable-by-algorithm, and argue via Church's Thesis and Tennenbaum. But there's trouble at the very start here. For what is uncontentiously given is only that we have a practice of working out sums and products for tractably small numbers. What entitles us to project from this finite base and credit ourselves with an understanding of how 'in principle' to compute on any number-inputs at all? If there are possible divergent extensions of the finite basis – which there are! – then there are possible divergent interpretations of our original finite practice:[6] are we algorithmically computing or deviantly quomputing? I don't see how it could be legitimate, in the current context where there is supposed to be a genuine question how we grasp $+$ rather some deviant $\oplus$, to suppose that we can blithely assume that there is no similar problem about how we grasp the notion of a computation. So an appeal to the sketched argument that went via Tennenbaum's Theorem would seem to limp from the outset.

[6] I'm here consciously echoing Putnam's 'If there are possible divergent extensions of our practice, then there are possible divergent interpretations of even the natural number sequence – our practice, or our mental representations, etc., do not single out a unique 'standard model' of the natural number sequence.' (*Reason Truth and History*, p. 67)