29
Non-standard models of Z are not recursive

A non-standard model of arithmetic is a model that is not isomorphic to the standard model $\mathcal{N}$ but in which the same sentences are true as are true in $\mathcal{N}$. In Chapter 17 we showed the existence of non-standard models of arithmetic with a denumerable domain. Since any model with a denumerable domain is isomorphic to one whose domain is the set N of natural numbers, it follows that there are non-standard models of arithmetic with domain N. Because the domain of all models with which the present chapter is concerned is N, we shall restrict the term 'model' accordingly: From now on, a *model* is an interpretation of the language of arithmetic whose domain is N.

The model $\mathcal{N}$ is certainly a model of the theory Z, elementary Peano arithmetic. In this chapter we are going to examine non-standard models of Z, with an eye to questions of definability. A model $\mathcal{M}$ is called *recursive* if the functions s, $\oplus$, and $\otimes$ that $\mathcal{M}$ assigns to the symbols $'$, $+$, and $\cdot$ are recursive. If $\oplus$ is recursive, so is s: $s(a) = a \oplus b$, where b is the number, whatever it might be, that $\mathbf{0}'$ denotes in $\mathcal{M}$. A theorem due to Stanley Tennenbaum asserts that there are no recursive non-standard models of arithmetic. We shall demonstrate an extension of Tennenbaum's theorem due to Georg Kreisel and Kenneth McAloon: in no non-standard model of Z is either $\oplus$ (Kreisel) or $\otimes$ (McAloon) recursive. We'll also show that in no non-standard model of *arithmetic* is either $\oplus$ or $\otimes$ definable in arithmetic.

At the end of Chapter 17 we saw that the LESS THAN ordering in any model of arithmetic is isomorphic to the result of taking the rational numbers $\geqslant 0$ and < 1, replacing 0 by a copy of the natural numbers, and replacing each rational > 0 and < 1 by a copy of the integers (with no one object in any two copies, of course). Our proof made use of certain truths about the natural numbers. Because all of these truths are provable in Z, the LESS THAN ordering in any model *of Z* is isomorphic to the relation thus obtained from the rationals $\geqslant 0$ and < 1. It would be an easy exercise to define a recursive twoplace relation R on N that is isomorphic to the LESS THAN ordering in any denumerable model of Z; it would be almost as easy to construct R so that the R-successor function is also recursive. Thus there are models of Z in which LESS THAN and s are recursive. The theorem of Tennenbaum, Kreisel, and McAloon implies that we cannot do much better. In contrast, the tables in Exercise 14.2 show that there are non-standard models of Q in which both $\oplus$ and $\otimes$ are recursive.

A notational preliminary: Suppose that F is, e.g., the formula $\exists x\, y \cdot x = z$. Then we shall write $\mathscr{M} \models \exists x\, y \cdot x = z[o_1, o_2]$ to mean

$$\mathscr{M}^{a_1 a_2}_{o_1 o_2}(F_y {a_1}_z a_2) = 1.$$

Likewise for other formulas; context and alphabetical order can be expected to resolve any ambiguities over which objects are correlated with which variables. '$\mathscr{M} \models \exists x\, y \cdot x = z\,[o_1, o_2]$' may be read: o_1 and o_2, when assigned to y and z, respectively, satisfy $\exists x\, y \cdot x = z$ in $\mathscr{M}$. If S is a sentence, we shall similarly write $\mathscr{M} \models S$, instead of $\mathscr{M}(S) = 1$. (Incidentally, we shall use 'a', 'b' etc. in what follows to vary over natural numbers rather than names.)

Now let $\mathscr{M}$ be an arbitrary non-standard model of Z; s, $\oplus$, and $\otimes$ are the functions that $\mathscr{M}$ assigns to the symbols $'$, $+$, and $\cdot$. A number d is called a non-standard element of $\mathscr{M}$ if for every n, $\mathscr{M} \models \mathbf{n} < z[d]$. (If d is a non-standard element of $\mathscr{M}$, then $\mathscr{M} \models \mathbf{d} < z[d]$!) Lemma 29.1 asserts that there are non-standard elements of $\mathscr{M}$.

Lemma 29.1

For some d, for every n, $\mathscr{M} \models \mathbf{n} < z\,[d]$.

Proof. Since $\mathscr{M}$ is a model of Q, by Lemmas 14.11 and 14.13, for every n, $\mathscr{M} \models \forall z(z = \mathbf{0} \vee \ldots \vee z = \mathbf{n-1} \vee z = \mathbf{n} \vee \mathbf{n} < z)$, and therefore for every d, $\mathscr{M} \models (z = \mathbf{0} \vee \ldots \vee z = \mathbf{n-1} \vee z = \mathbf{n} \vee \mathbf{n} < z)\,[d]$. It thus suffices to show that for some d, for every n, $\mathscr{M} \models z \neq \mathbf{n}\,[d]$.

Define a function h from natural numbers to natural numbers by: $h(0) = e$; $h(n+1) = s(h(n))$. Then, with the aid of the axioms of Q, which hold in $\mathscr{M}$, it is easy to see that h is one–one and for all m, n, $h(m+n) = h(m) \oplus h(n)$ and $h(mn) = h(m) \otimes h(n)$. If also for every d, $\mathscr{M} \models z = \mathbf{n}[d]$, then h would be onto the domain of $\mathscr{M}$, and therefore an isomorphism of $\mathscr{N}$ onto $\mathscr{M}$. But then $\mathscr{M}$ would not be non-standard.

Let p_n be the nth prime number counting from 0, so that $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc. The function whose value at any n is p_n is recursive; let $\theta(x, y)$ represent it in Q.

Our first task will be to prove the following quite surprising result.

Theorem 29.1

Let $A(x)$ be an arbitrary formula of L. Then there exist b, c such that for every natural number n,
(1) $\mathscr{M} \vDash A(\mathbf{n})$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n 'a's) $= b$, and
(2) $\mathscr{M} \vDash A(\mathbf{n})$ iff for some a, $a \otimes a \otimes \ldots \otimes a$ (p_n 'a's) $= c$.

To prove Theorem 29.1, we need several lemmas concerning provability in Z and non-standard models.

Lemma 29.2

Let $m > 0$. Then $\vdash_Z \mathbf{m} \cdot x = x + x + \ldots + x$ (m 'x's).

Proof. Induction on m. Basis: $\vdash_Z \forall x\, \mathbf{1} \cdot x = x$. Induction step: $\vdash_Z \forall w \forall x\, (w + \mathbf{1}) \cdot x = w \cdot x + x$. Let $q = m + 1$. Then $\vdash_Z \mathbf{q} \cdot x = \mathbf{m} \cdot x + x = (x + x + \ldots + x$ (m 'x's)$) + x = x + x + \ldots + x$ ($m + 1$, $= q$, 'x's).

Let $w | y$ be the formula $\exists x\, w \cdot x = y$, which defines the division relation in Q.

Lemma 29.3

Let $m > 0$. Then $\mathscr{M} \vDash \mathbf{m} | y\, [b]$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (m 'a's) $= b$.

Proof. $\mathscr{M} \vDash \mathbf{m} | y\, [b]$ iff $\mathscr{M} \vDash \exists x\, \mathbf{m} \cdot x = y\, [b]$, iff by Lemma 29.2 for some a, $a \oplus a \oplus \ldots \oplus a$ (m 'a's) $= b$.

Exponentiation can be defined and its basic properties proved in Z.

Lemma 29.4

Let $m > 0$. Then $\vdash_Z x^{\mathbf{m}} = x \cdot x \cdot \ldots \cdot x$ (m 'x's).

Proof. A simple induction on m, like the one in the proof of Lemma 29.2.

Lemma 29.5

$\vdash_Z \forall w \forall y (y > \mathbf{0} \rightarrow [w \mid y \leftrightarrow \exists x (x^w = \mathbf{2}^y)])$.

Proof. Formalize in Z the following argument: Suppose y positive. Then $2^y > 1$. If w divides y, then for some v, $vw = y$. Let $x = 2^v$. Then $x^w = (2^v)^w = 2^{vw} = 2^y$. Conversely, assume that $x^w = 2^y$. Then $x \neq 0, 1$ and $w \neq 0$. No odd prime divides x; otherwise some odd prime divides 2^y. So for some v, $x = 2^v$. Then $2^y = x^w = 2^{vw}$, and so $vw = y$ and v divides y.

Lemma 29.6

Let $m > 0$. Suppose that $\mathcal{M} \models y > \mathbf{0}\, [b]$ and $\mathcal{M} \models \mathbf{2}^y = z\, [b, c]$. Then $\mathcal{M} \models \mathbf{m} \mid y\, [b]$ iff for some a, $a \otimes a \otimes \ldots \otimes a$ (m 'a's) $= c$.

Proof. By Lemma 29.5, $\mathcal{M} \models \mathbf{m} \mid y\, [b]$ iff for some a, $\mathcal{M} \models x^{\mathbf{m}} = \mathbf{2}^y\, [a, b]$, iff for some a, $\mathcal{M} \models x^{\mathbf{m}} = z\, [a, c]$, iff by Lemma 29.4 for some a, $\mathcal{M} \models x \cdot x \cdot \ldots \cdot x$ (m 'x's) $= z\, [a, c]$, iff for some a, $a \otimes a \otimes \ldots \otimes a$ (m 'a's) $= c$.

Lemma 29.7

For any formula $A(x)$ of L, the following sentence is a theorem of Z: (*) $\forall z \exists y > \mathbf{0} \forall x (\exists w (\theta(x, w) \,\&\, w \mid y) \leftrightarrow (x < z \,\&\, A(x)))$.

(*) says that for every z, there is a positive integer y such that for all x, the xth prime divides y if and only if x is less than z and $A(x)$ holds.

Proof. To prove (*) in Z, formalize in Z the following induction on z: Basis: If $z = 0$, let $y = 1$. Then done, for no prime divides 1 and no natural number is less than 0.

Induction step: Suppose that for all x, the xth prime divides the positive integer y if and only if $x < z$ and $A(x)$ holds. Let p be the zth prime. If $A(z)$ holds, let $v = y \cdot p$; otherwise let $v = y$. Then v is positive and for all x the xth prime divides v if and only if $x < z + 1$ and $A(x)$ holds.

Before getting down to the details of the proof of Theorem 29.1, let us briefly indicate its main idea, which is due to Tennenbaum. Lemma 29.7 can be regarded as saying that for every z there is a y that encodes the answers to all questions: $A(x)$? for x less than z. Lemma 29.7 is provable in Z and therefore holds in any non-standard model of Z. A non-standard model $\mathscr{M}$ contains a non-standard element d. Therefore in the domain of $\mathscr{M}$ there is a b that encodes the answers to all questions: $\mathscr{M} \models A(x)\,[i]$? for i LESS THAN d. In a non-standard model, however, the standard elements, i.e. the denotations of numerals, are all LESS THAN the non-standard elements. Thus $\mathscr{M}$ contains an element b that encodes the answers to all of the infinitely many questions: $\mathscr{M} \models A(\mathbf{n})$?.

Proof of Theorem 29.1. All theorems of Z are true in $\mathscr{M}$. Thus by Lemma 29.7, $\mathscr{M} \models \forall z \exists y > \mathbf{0} \forall x(\exists w(\theta(x,w) \,\&\, w \mid y) \leftrightarrow (x < z \,\&\, A(x)))$. By Lemma 29.1, for some d, for every n, $\mathscr{M} \models \mathbf{n} < z\,[d]$, and therefore $\mathscr{M} \models \exists y > \mathbf{0} \forall x(\exists w(\theta(x,w) \,\&\, w \mid y) \leftrightarrow (x < z \,\&\, A(x)))\,[d]$. We thus let b be such that $\mathscr{M} \models y > \mathbf{0}\,[b]$ and $\mathscr{M} \models \forall x(\exists w(\theta(x,w) \,\&\, w \mid y) \leftrightarrow (x < z \,\&\, A(x)))\,[b,d]$. Then for every n, $\mathscr{M} \models (\exists w(\theta(\mathbf{n},w) \,\&\, w \mid y) \leftrightarrow (\mathbf{n} < z \,\&\, A(\mathbf{n})))\,[b,d]$, and therefore $\mathscr{M} \models (\exists w(\theta(\mathbf{n},w) \,\&\, w \mid y) \leftrightarrow A(\mathbf{n}))\,[b]$. Since θ defines in Q the function whose value at every n is p_n, $\mathscr{M} \models \forall w(\theta(\mathbf{n},w) \leftrightarrow w = \mathbf{p_n})$. Thus for every n, $\mathscr{M} \models (\mathbf{p_n} \mid y \leftrightarrow A(\mathbf{n}))\,[b]$, and $\mathscr{M} \models (\exists x(\mathbf{p_n} \cdot x = y) \leftrightarrow A(\mathbf{n}))\,[b]$. It follows that for every n, $\mathscr{M} \models A(\mathbf{n})$ if and only if for some a, $\mathscr{M} \models \mathbf{p_n} \cdot x = y\,[a,b]$. But by Lemma 29.3, $\mathscr{M} \models \mathbf{p_n} \cdot x = y\,[a,b]$ if and only if $a \oplus a \oplus \ldots \oplus a$ (p_n 'a's) $= b$. So $\mathscr{M} \models A(\mathbf{n})$ if and only if for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n 'a's) $= b$. Thus (1) holds.

As for (2), let c be such that $\mathscr{M} \models \mathbf{2}^y = z\,[b,c]$. By Lemma 29.6, $\mathscr{M} \models \mathbf{p_n} \mid y\,[b]$ iff for some a, $a \otimes a \otimes \ldots \otimes a$ (p_n 'a's) $= c$. So $\mathscr{M} \models A(\mathbf{n})$ if and only if for some a, $a \otimes a \otimes \ldots \otimes a$ (p_n 'a's) $= c$, and (2) also holds.

To prove that neither $\oplus$ nor $\otimes$ is recursive, we need the notions of recursive enumerability and recursive inseparability.

A set W of natural numbers is called *recursively enumerable* (r.e. for short) if for some recursive relation R, $W = \{n\text{: for some } k, Rnk\}$. If W is a recursive set, then W is automatically r.e.: Let Rnk iff $n \in W$ and $k = k$; then R is recursive and $W = \{n\text{: for some } k, Rnk\}$.

We shall shortly give examples of r.e. sets that are not recursive. We want now to show that a set W is recursive if and only if both W and $N-W$, the set of natural numbers not in W, are r.e. The left–right implication is clear: If W is recursive, so is $N-W$, and therefore both W and $N-W$ are r.e. For the converse, suppose W and $N-W$ r.e. Then for some recursive relations R and S, $W = \{n$: for some k, $Rnk\}$, and $N-W = \{n$: for some k, $Snk\}$. Let Qnk iff either Rnk or Snk. Q is recursive and *regular*: For every n there is a k such that Qnk. Thus the function f obtained from Q by minimization is recursive, as then is $\{n\text{:} Rnf(n)\}$. But $W = \{n$: $Rnf(n)\}$: If $n \in W$, Rnk for some k; let k be least. Since $n \notin N-W$, Snj for no j. Thus k is the least i such that Qni, $f(n) = k$, and $Rnf(n)$. Conversely, if $Rnf(n)$, then for some k, Rnk, and $n \in W$.

Sets W and X of natural numbers are called *recursively inseparable* if they are disjoint, i.e., have no common member, and there is no recursive set Y such that $W \subseteq Y$ and $X \subseteq N-Y$. If W and X are recursively inseparable, neither is recursive, for if W were recursive, then $W \subseteq W$ and $X \subseteq N-W$, contra inseparability; similarly for X. We now exhibit a pair of recursively inseparable r.e. sets.

Let Rnk iff the Turing machine with gödel number n, when started with input n, halts at the kth stage of its computation, with output 0. Similarly, let Snk iff the Turing machine with gödel number n, when started with input n, halts at stage k, with output 1. R and S are recursive relations. Let $A = \{n\text{: for some } k, Rnk\}$ and $B = \{n\text{: for some } k, Snk\}$. A and B are r.e. Since a Turing machine produces at most one output, A and B are also disjoint. To show that they are recursively inseparable, suppose that Y is a recursive set, $A \subseteq Y$, and $B \subseteq N-Y$. Let f be the characteristic function of Y. Then f is recursive. Let e be the gödel number of a Turing machine that computes f.

Then $e \in Y, \rightarrow f(e) = 1$,

→ the Turing machine with gödel number e generates 1 when started with input e,

→ for some k, Sek,

→ $e \in B$,

$\rightarrow e \notin Y$,
$\rightarrow f(e) = 0$,
$\rightarrow$ the Turing machine with gödel number e generates 0 when started with input e,
$\rightarrow$ for some k, Rek,
$\rightarrow e \in A$,
$\rightarrow e \in Y$, contradiction.

A and B are therefore recursively inseparable.

Let $\rho(x, y)$ and $\sigma(x, y)$ be formulas defining R and S in Q. We suppose that ρ and σ are defined in a reasonable manner, so that $\forall x \forall y \forall z - (\rho(x, y) \,\&\, \sigma(x, z))$ is a theorem of Z. Let $\alpha(x)$ be the formula $\exists y \rho(x, y)$ and let $\beta(x)$ be $\exists y \sigma(x, y)$. Then

(1) $\vdash_Z \forall x - (\alpha(x) \,\&\, \beta(x))$ and

(2) for all n, if $n \in A$, $\vdash_Z \alpha(\mathbf{n})$ and if $n \in B$, $\vdash_Z \beta(\mathbf{n})$.

For assume $n \in A$. Then for some k, Rnk. Since ρ defines R in Q, $\vdash_Q \rho(\mathbf{n}, \mathbf{k})$. Then $\vdash_Q \exists y \rho(\mathbf{n}, y)$, i.e. $\vdash_Q \alpha(\mathbf{n})$, and $\vdash_Z \alpha(\mathbf{n})$. Similarly for B and β.

We now prove that neither $\oplus$ nor $\otimes$ is recursive. According to Theorem 29.1, there exist b, b^*, c, and c^* such that for every natural number n,

$\mathscr{M} \models \alpha(\mathbf{n})$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= b$,
$\mathscr{M} \models -\alpha(\mathbf{n})$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= b^*$,
$\mathscr{M} \models \alpha(\mathbf{n})$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= c$, and
$\mathscr{M} \models -\alpha(\mathbf{n})$ iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= c^*$.

Now let $Y = \{n : \mathscr{M} \models \alpha(\mathbf{n})\}$. Then $Y = \{n$: for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= b\}$ and $N - Y = \{n : \mathscr{M} \models -\alpha(\mathbf{n})\} = \{n$: for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= b^*\}$.

If $n \in A$, then by (2), $\vdash_Z \alpha(\mathbf{n})$; so $\mathscr{M} \models \alpha(\mathbf{n})$, and $n \in Y$. Thus $A \subseteq Y$. If $n \in B$, then by (2), $\vdash_Z \beta(\mathbf{n})$; by (1), $\vdash_Z -\alpha(\mathbf{n})$, $\mathscr{M} \models -\alpha(\mathbf{n})$, and $n \in N - Y$. Thus $B \subseteq N - Y$. By the recursive inseparability of A and B, Y is not recursive, and therefore either Y is not r.e. or $N - Y$ is not r.e.

Let Rna iff $a \oplus a \oplus \ldots \oplus a$ (p_n ‘a’s) $= b$, and let Sna iff $a \oplus a \oplus \ldots \oplus a$ (p_n *‘a’s*) $= b^*$. Then $Y = \{n$: for some a, $Rna\}$, and $N - Y = \{n$: for some a, $Sna\}$. Observe that R is recursive if $\oplus$ is: To determine whether or not Rna, first calculate p_n from n. Then successively compute $a \oplus a$, $a \oplus a \oplus a$, ..., and, finally, $a \oplus a \oplus \ldots \oplus a$, with p_n 'a's. *Rna* iff the final result is b. Similarly, S is recursive if $\oplus$ is. Thus Y and $N-Y$ are r.e. if $\oplus$ is recursive. Therefore $\oplus$ is not recursive.

Replacing '$\oplus$', 'b', and 'c' in the previous paragraph by '$\otimes$', 'b', and 'c' shows that $\otimes$ is not recursive. In no non-standard model of Z is either $\oplus$ or $\otimes$ recursive.

We now let $\mathscr{M}$ be a non-standard model of *arithmetic*. We shall show that neither $\oplus$ nor $\otimes$ is definable in arithmetic. We'll consider $\oplus$; to treat $\otimes$, merely replace '$\oplus$' by '$\otimes$' in what follows. Suppose then that $\oplus$ is definable in arithmetic; we shall obtain a contradiction.

Let *Hbn* iff for some a, $a \oplus a \oplus \ldots \oplus a$ (p_n 'a's) $= b$. By the definability of $\oplus$, H is definable in arithmetic: Use the β-function to express 'there is a finite sequence $s_0, \ldots, s_k$ of length at least p_n such that for some a, $s_0 = a$, for every $i < p_n - 1$, $s_{i+1} = s_i \oplus a$, and $s_{p_n - 1} = b$'.

Let $B(x, y)$ define H in arithmetic. Then for all b, n, *Hbn* iff $\mathscr{N} \vDash B(\mathbf{b}, \mathbf{n})$. Let $A(x)$ be the formula $-B(x, x)$. By Theorem 1, there is a number b such that for every n, $\mathscr{M} \vDash A(\mathbf{n})$ iff *Hbn*. $\mathscr{M}$ is a model of arithmetic. Therefore the same sentences are true in $\mathscr{M}$ and $\mathscr{N}$, and for every n, $\mathscr{N} \vDash A(\mathbf{n})$ iff *Hbn*. But then $\mathscr{N} \vDash B(\mathbf{b}, \mathbf{b})$ iff *Hbb*, iff $\mathscr{N} \vDash A(\mathbf{b})$, iff $\mathscr{N} \vDash -B(\mathbf{b}, \mathbf{b})$, contradiction.