Chapter IX

APPENDIX
Why mathematicians need not lose sleep over automatic theorem provers

This appendix presents the technical fact that any *creative* set L has trivially describable (hence trivially recognizable) infinite recursive[†] subsets such that any "verifier" for L—i.e., a ϕ_i such that $L = W_i$—takes an unreasonably-horrendously-outrageously humongous amount of time to verify membership in such subsets.

More precisely, we will define a particular creative set L and show that for *any* choice of a *recursive* ϕ_{j_0}—e.g., one with a horrendously big run time, see Chapter 7—and for ***any*** ϕ_{i_0} such that $L = W_{i_0}$ there is a "trivially recognizable" *infinite* subset $T \subseteq L$ such that, *for every* $x \in T$, the computation of $\phi_{i_0}(x)$ will take at least as many steps as that of $\phi_{j_0}(x)$.

We will then offer an interpretation of this fact in the context of recursively axiomatized theories such as Peano arithmetic and Set Theory.

1. *A creative set*

1.1 Definition. We define the set L as follows:

$$L = \Big\{ \langle i, j, x\rangle : \big(\phi_i(\langle i, j, x\rangle) \downarrow \vee \phi_j(\langle i, j, x\rangle) \downarrow \big) \wedge \\ \phi_i(\langle i, j, x\rangle) \text{ needs at least as many steps as } \phi_j(\langle i, j, x\rangle) \Big\}$$

$\square$

1.2 Theorem. *L defined above is creative.*

Proof. (1) L is semi-recursive (r.e.). Indeed, let

$$g(i, j, x) \stackrel{\text{def}}{=} (\mu y)\big(T(i, \langle i, j, x\rangle, y) \vee T(j, \langle i, j, x\rangle, y)\big)$$

[†]Indeed under some mild assumptions, *regular*.

Then,

$$\langle i,j,x\rangle \in L \leftrightarrow (\exists y)\big(T(i,\langle i,j,x\rangle,y) \vee T(j,\langle i,j,x\rangle,y)\big) \wedge \\ T\big(j,\langle i,j,x\rangle,g(i,j,x)\big)$$

and we are done by strong projection, closure properties of $\mathcal{P}_*$, including the fact that $\mathcal{P}_*$ is closed under substitution of $\mathcal{P}$-functions into variables.†

(2) Next we prove that $\overline{L}$ is productive. We will argue that $f = \lambda i.\langle i,i,0\rangle$ is a productive function for $\overline{L}$.‡

Let then

$$W_i \subseteq \overline{L} \tag{2.1}$$

Question. Can it be $\langle i,i,0\rangle \in L$? Well, if yes, then, in particular, $\phi_i(\langle i,i,0\rangle)\downarrow$, that is,§ $\langle i,i,0\rangle \in W_i$ contradicting (2.1).

We conclude that $\langle i,i,0\rangle \in \overline{L}$.

Question. Can it be $\langle i,i,0\rangle \in W_i$? Well, if yes, then $\phi_i(\langle i,i,0\rangle)\downarrow$. Moreover $\phi_i(\langle i,i,0\rangle)$ takes no more time to compute than $\phi_i(\langle i,i,0\rangle)$ (i.e., itself). Thus, the entrance requirement for L is met: $\langle i,i,0\rangle \in L$, contradicting (2.1) once more. Thus, $\langle i,i,0\rangle \notin W_i$ and we are done. □

With the theorem out of the way—for now—let us choose and fix ***any recursive*** ϕ_{j_0} ***whatsoever***. Next, let us choose <u>any verifier whatsoever</u>¶ ϕ_{i_0} for L. That is

$$L = W_{i_0} \tag{3}$$

Let also

$$T \stackrel{\text{def}}{=} \Big\{\langle i_0,j_0,x\rangle : x \in \mathbb{N}\Big\} \tag{4}$$

We will argue two things:

(I) $T \subseteq L$

(II) For all $x \in \mathbb{N}$, $\phi_{i_0}(\langle i_0,j_0,x\rangle)$ takes at least as much time as $\phi_{j_0}(\langle i_0,j_0,x\rangle)$ to compute.

OK, <u>fix an arbitrary x</u> and let us pose and answer some questions:

Question. Can it be $\phi_{i_0}(\langle i_0,j_0,x\rangle)\uparrow$? If yes, then surely $\phi_{i_0}(\langle i_0,j_0,x\rangle)$ takes at least as much time as $\phi_{j_0}(\langle i_0,j_0,x\rangle)$ since the former is undefined and the latter is *defined* (recall that $\phi_{j_0} \in \mathcal{R}$). Thus the entrance conditions for L are met:

$$\langle i_0,j_0,x\rangle \in L$$

But $\phi_{i_0}(\langle i_0,j_0,x\rangle)\uparrow$ means

$$\langle i_0,j_0,x\rangle \notin W_{i_0}$$

†If $Q(y,\vec{x}) \in \mathcal{P}_*$ and $\lambda\vec{z}.f(\vec{z}) \in \mathcal{P}$, then $Q(f(\vec{z}),\vec{x}) \in \mathcal{P}_*$ since $Q(f(\vec{z}),\vec{x}) \leftrightarrow (\exists y)(y = f(\vec{z}) \wedge Q(y,\vec{x}))$. Now use the fact that the graph of f is in $\mathcal{P}_*$, and closure under $\wedge$ and $\exists$.

‡So is $\lambda i.\langle i,i,k\rangle$ for any $k \in \mathbb{N}$.

§Recall the definition: $W_i = \mathrm{dom}(\phi_i)$.

¶Recall the terminology "verifier". It means that if $z \in L$ then $\phi_{i_0}(z)\downarrow$—i.e., "program" i_0 verifies membership—else $\phi_{i_0}(z)\uparrow$, i.e., program i_0 runs forever.

contradicting (3). Thus,

$$\phi_{i_0}(\langle i_0, j_0, x\rangle)\downarrow \tag{5}$$

By (3), $\langle i_0, j_0, x\rangle \in L$, establishing (I).

Now for (II):

Question. Can it be that $\phi_{i_0}(\langle i_0, j_0, x\rangle)\downarrow$ in *strictly fewer steps* than $\phi_{j_0}(\langle i_0, j_0, x\rangle)\downarrow$?

NO. Otherwise, we have the entrance sub-condition (for L) to the left of "$\wedge$" true, but the sub-condition to the right **false**. Hence $\langle i_0, j_0, x\rangle \notin L$ (yet $\langle i_0, j_0, x\rangle \in W_{i_0}$) contradicting (3) again. Thus, (II) is proved.

Since we can arrange to pick a ϕ_{j_0} that runs horrendously-outrageously-humongously slowly (Ch.7), what we have proved is that for any such ϕ_{j_0} and ***any choice of verifier "program"*** i_0 for L, we can build an infinite subset T (see (4)) of L that, despite being *trivially recognizable* on its own, ***the verifier*** i_0 ***for*** L ***will be horrendously-impractically-slow on*** ***<u>every</u>*** ***input in*** T.

Let us now bring into the discussion the fact that L is creative. We cite two facts without proof (for proofs see Ch.9 of "Computability").

By the way, we can hope for no more than a verifier for a creative set. We can have ***no*** yes/no recognizer (that is, decider) since such a set is not recursive (its complement is productive, i.e., *effectively non-r.e.*).

Fact 1. The set of theorems of each of Peano arithmetic and (axiomatic) Set Theory is creative.

Fact 2. Any two creative sets, A and B are recursively isomorphic. This means that there is a recursive 1-1 and onto function $f : \mathbb{N} \to \mathbb{N}$ such that $f[A] = B$.

Thus, there is, essentially, only *one* creative set. In particular, L can be thought (within two-way 1-1 recursive encoding) that it ***is*** the set of all theorems of Peano arithmetic.

Select now, as above, a very-very-very slowly computable total ϕ_{j_0} and pick ***any*** verifier ϕ_{i_0} for L.

Consider the associated set T. This is a (sub)set of theorems (an infinite one at that) of Peano arithmetic, since $T \subseteq L$. Now, "humanly" speaking, the T-theorems are trivial to recognize, since we can tell at a glance if a number has the form $\langle i_0, j_0, x\rangle$—i.e., $2^{i_0+1}3^{j_0+1}5^{x+1}$—or not.

On the other hand, our arbitrary verifier ϕ_{i_0} will have loads of trouble on ***every theorem*** in T: it will take more time on each such than what ϕ_{j_0} needs.

Mathematicians (and computer scientists who prove theorems) will sleep easy tonight.

If we think of natural numbers as strings over $\{0, 1\}$, that is, if we identify $\mathbb{N}$ with $\{0, 1\}^*$, then the set of theorems T is a regular language over the alphabet $\{0, 1, (,), ;\}$ where ";" represents ",". I mean, we can think of "$\langle i_0, j_0, x\rangle$" as the string "$(i_0; j_0; x)$", $x \in \{0, 1\}^*$.