1 Preliminaries

Recall the basic facts from recursion theory:
Primitive functions: $+$ (addition), $\times$ (multiplication), S (succesor), Z (null function), $\mathrm{i}^k_j : [x_1, x_2, \ldots, x_k] \mapsto x_j$ (projection), $\mathrm{e} : [x, y] \mapsto 1$ iff $x = y$ and $[x, y] \mapsto 0$ otherwise. **Operation of minimalization**: $\mu y(\varphi(y, \overline{x}) = 0))$. We say that a function f from N to N is a **partial recursive function** (FCR) if it is a composition of primitive functions and operation of minimalization. We say that a function f from N to N is **recursive function** if it is partial recursive function with $dom(f) = \mathrm{N}$. We say that a set $A \subseteq \mathrm{N}$ is **recursively enumerable** (r.e.) if its characteristic function is partial recursive. We say that a set $A \subseteq \mathrm{N}$ is **recursive** if its characteristic function is recursive.

Turing predicate a a recursive predicate T defined by: $\mathrm{T}_k(e, \overline{x}, w)$ iff "e is a code of a function, w its computation and $[x_1, x_2, \ldots, x_k]$ its input". **Universal function** is a function U such that $\forall \psi \in \mathrm{FCR} : \exists e : \forall \overline{x} \psi(\overline{x}) \simeq \mathrm{U}(\mu w(\mathrm{T}_k(e, \overline{x}, w)))$. Using the universal function we can for every e define a function $\varphi^k_e(\overline{x}) = \mathrm{U}(\mu w(\mathrm{T}_k(e, \overline{x}, w)))$ and $\mathrm{W}^k_e(\overline{x}) = dom(\varphi^k_e) = \{\overline{x} \mid \exists w \mathrm{T}_k(e, \overline{x}, w)\}$. Since every r.e. set A is a domain of some FCR (at least its characteristic function) and such a FCR has some index e, we can always write W_e instead of A for suitable e. By similar argument there exists for every FCR ψ an index e such that $\psi = \varphi_e$.

Definition. *For every index e and a number s we define a function:*

$$\varphi_{e,s}(x) \cong \varphi_e(x) \text{ if } \exists w < s : T(e, x, w) \text{ and } \varphi_{e,s}(x) \cong \uparrow \text{ otherwise.}$$

We call the function $\varphi_{e,s}$ an s-th approximation of a function φ_e.

Since w in the previous definition codes whole computation of φ_e with an input x and output y it must be the case that $x, y < w$ and whence we can understand s-th aproximation of φ_e by asking for given $x < s$ whether any of $w \leq s$ codes a computation with an input x (recursive condition) and if the answer is "no", we leave the function undefined.

Theorem. *(Second Recursion Theorem) For every $\psi \in \mathrm{FCR}$ there exists an index e such that $\varphi_e(\overline{x}) \cong \psi(e, \overline{x})$.*

Definition. *Let $A, B \subseteq \mathrm{N}$ then we say that A is m-reducible to B and write $A \leq_m B$ if there exists a recursive function g such thath $x \in A \leftrightarrow g(x) \in B$. We say further that a set A is m-complete if every r.e. set is m-reducible to A.*

Theorem. *(Post) Let A, B be r.e. sets, then A and B are recursive whenever $A \cup B = \mathrm{N}$ and $A \cap B = \emptyset$.*

Following theorem is given in [ODI] pages 258-9.

Theorem. *Complement of every m-complete set contains an infinite r.e. subset.*

2 Simple sets

Now we finally move to the main question of this paper:

Post's Problem. *(m-version) Are there r.e. sets which are nor recursive neither m-complete?*

Since both, complement of complete set and complement of recursive set, contain an infinite r.e. subset, it would be sufficient to show that there exists a r.e. set whose complement does not contains a r.e. subsets or in other words, a r.e. set which intersects every infinite r.e. set.

Definition. *We say that a r.e. set S is simple if its complement $\overline{S}$ is infinite and does not contain an infinite r.e. subset.*

There might be an idea to enumerate all infinite r.e sets and construct S inductively but unfortunately this would not ensure S being r.e. since a set of infinite r.e. sets is not r.e. To show there exists a simple set, we use an argument of Kolmogorov:

Definition. *We define a function* K *called Kolmogorov complexity by*

$$\mathrm{K}(x) = \mu e(\varphi_e(0) \cong x),$$

we say further that $\mathrm{K}(x)$ *is a complexity of* x *and that a number* x *is random if* $x \leq \mathrm{K}(x)$ *otherwise we say it is nonrandom.*

Lemma. *There exists infinitely many random numbers.*

Proof. We show that for every n there exists a random number whose complexity is bigger than n: Let n be given, then we have following sequence $\varphi_0(0), \varphi_1(0), \ldots, \varphi_n(0)$ (note that every $i \in \omega$ can be always considered as an index of some function, at least an empty function). Let x be the least number which is not in the sequence. Then $x \leq n+1$ and from x not being a value of a function with index $\leq n$ and input 0 we have $n+1 \leq \mathrm{K}(x)$, whence x is random with complexity bigger than n and we are done. □

Theorem. *The set of nonrandom numbers is simple.*

Proof. Let $A = \{x \mid \mathrm{K}(x) < x\}$ then A is r.e. by

$$x \in A \text{ iff } \exists e < n : \varphi_e(0) \cong x.$$

To show that $\overline{A}$ does not contains any infinite r.e. set, it is sufficient to prove that every infinite set of random numbers is not r.e.

Assume for a contradiction that R is an infinite r.e. set of random numbers and ρ is recursive function such that $rng(\rho) = R$. Assume without lost of generality that ρ is injective. We define a function f by $f(e, 0) =$"the smallest $x \in R$ such that there is $i \le e + 1$ with $\rho(i) = x$ and $\rho(i) > e$", formally:

$$f(e, 0) = \mu x((\exists i \le e + 1)(\rho(i) = x \ \wedge \ x > e))$$

Note that the definition of $f(e, 0)$ is correct for every e. Indeed, since $\rho(0), \rho(1), \ldots, \rho(e+1)$ is a sequence of $e + 2$ pairwise different numbers, there always exists a number between $\rho(0), \rho(1), \ldots, \rho(e+1)$ bigger than e. By *Second Recursion Theorem* there exists an index e such that $\varphi_e(x) \cong f(e, x)$ and whence $\varphi_e(0) > e$ i.e. $x > e \ge \mathrm{K}(x)$ by definition of f, however, this contradicts $x \in R$. □

Corollary. *Let T be a consistent theory extending* PA *(maybe* PA *can be replaced by* Q*?), then $T \vdash \overline{n} \le \mathrm{K}(\overline{n})$ for at most finitely many n's.*

Proof. Since 'being provable in T' is a r.e. condition, the set $\{\overline{n} \mid T \vdash \overline{n} \le \mathrm{K}(\overline{n})\}$ is r.e. and hence finite by previous theorem. □

Note that Corollary of Kolmogorov's Theorem mention only that randomness is provable for at most finitely many numerals, however since Kolmogorov's Lemma can be formalised within PA (or maybe Q), it holds that $T \vdash (\forall n)(\exists x)(x \le n + 1 \le \mathrm{K}(x))$ i.e. "PA knows" there exist infinitely many random numbers, but "PA does not know" (except finitely many cases) their concrete values. Whence there exists infinitely many independent sentences of the form $\overline{n} \le \mathrm{K}(\overline{n})$.

3 Hypersimple Sets

Now we move to another use of simple sets. Since the m-degrees (sets A, B have the same m-degree iff $A \le_m B$ and $B \le_m A$) can be (in some sense) understood as a measure of complexity of r.e. problems in the way that recursive sets corresponds to the easiest problems and m-complete sets corresponds to the hardest problems, we can rephrase some questions in equivalence of existence of some concrete set of some concrete m-degree and so obtain an intuition of “how complicated the problem is”. In this section we show that a question whether some first-order axiomatizable theory is independently axiomatizable (see below) is equivalent to existence of concrete set which is hypersimple (see below).

Definition. *We say that a number z is a canonical index of a finite set $\{x_1, \ldots, x_n\}$ if $z = 2^{x_1} + 2^{x_2} + \ldots + 2^{x_n}$ and by D_z we denote a finite set with canonical index z.*

Before we state a definition of hypersimple sets, we recall a definition of s-th aproximation and show its menaning by an example: Assume φ_e is a function with domain $\mathrm{W}_e = \{code(\{n, n+1\}) \mid n = 2k\}$ then for some s the domain of s-th aproximation of φ_e might be for example $\mathrm{W}_{e,s} = \{code(\{1,2\}), code(\{3,4\}), code(\{5,6\})\}$.

Definition. *We say that a set W is an infinite strong disjoint array (ISDA) if it is an infinite r.e. set whose elements are canonical indexes and $\forall x, y \in W : D_x \cap D_y = \emptyset$.*

Definition. *We say that a r.e. set H is hypersimple if $\overline{H}$ is infinite and there is no ISDA intersecting $\overline{H}$ by every element.*

The following proof use a kind construction called Priority Argument construction which works as follows: At the beginning we state a positive and a negative condition (there might be of course more than one pair and in fact it must not be always a pair positive-negative). These conditions have an instances with some order of priority (in our case they will be ordered by size of e). Durning the construction at every stage s, we can try to satisfy a condition with the highest priority by doing some action with an element that seems to be appropriate for this, however we can always recall this action at some higher stage whenever this element seems to be appropriate for satisfying the negative condition. At the end we show that all of the instances were satisfied.

Theorem. *(Post 1944) There exists a hypersimple set.*

Proof. I'm going to follow the proof given in [ODI] p.275-276 and comment (in italic) what was added by me.

We build a hypersimple set A by stages. At stage s we will have A_s, and we will let $A_s = \{a_0^s < a_s^1 < a_2^s < \ldots\}$. In the end we let $\overline{A} = \{a_0 < a_1 < a_2 < \ldots\}$ where $a_n = lim_{s\to\infty} a_n^s$. We want to satisfy the following requirements:

$$P_e : \text{if } \mathrm{W}_e \text{ is an ISDA then } (\exists z \in \mathrm{W}_e)(D_z \subseteq A)$$

$$N_e : \overline{A} \text{ has at least } e \text{ elements, or } lim_{s\to\infty} a_e^s < \infty$$

(I think "$\overline{A}$ has at least e elements" is not needed since we show "$lim_{s\to\infty} a_e^s < \infty$" for every n in second part of this proof.)
(The meaning for P_e should be "a positive action on A with e" since to satisfy P_e we are going to add elements into A. The meaning of N_e is "a negative action on A with e" since to satisfy N_e we are going to (give back) an elements from A to $\overline{A}$.)
The construction is as follows. We start with $A_0 = \emptyset$ and $\overline{A}_0 = \{0 < 1 < 2 < 3 < \ldots\}$ i.e. $a_n^0 = n$. At stage $s+1$ we search for the smallest $e \leq s$ such that:

(i) $z \in \mathrm{W}_{e,s} \to D_z \cap \overline{A}_s \neq \emptyset$
(ii) for some $z \in \mathrm{W}_{e,s}, D_z \subseteq [a_e^s, +\infty)$.

Note that both, A_s and $\mathrm{W}_{e,s}$, are finite and we assume only $e \leq s$, so the search is effective (recursive).
If such e does not exist, we move to the next stage.Otherwise, P_e is the condition with smallest index which looks unsatisfied and with a chance to be satisfied. Then put all of D_z into A, where z is the smallest one such that $z \in \mathrm{W}_{e,s}$ and $D_z \subseteq [a_e^s, +\infty)$. *(in other words, define $A_{s+1} = A_s \cup D_z$ or equivalently, for every n let $m = n + |\{a_0^s, \ldots, a_{n-1}^s\} \cap D_z|$ and $a_n^{s+1} = a_m^s$).* Since the construction is effective, $A = \bigcup_{s\in\omega} A_s$ is r.e. Moreover:

$\overline{A}$ is infinite:
It is enough to prove that $lim_{s\to\infty} a_n^s$ exists. Indeed, a_n^s may move at a certain stage $s+1$ only if it happens that $a_n^s \in D_z$ for some $z \in \mathrm{W}_e$, $e \leq n$ (indeed, if $e > n$ then by (ii) D_z is not relevant since $D_z \nsubseteq [a_e^s, +\infty)$). Since for every e, W_e contributes at most one such a finite set and there are only finitely many $e \leq n$, a_n^s moves only finitely many times. So all N_e's are satisfied.
(Note that this argument is in fact inductive: since a_0^s moves at a certain stage $s+1$ only if it happens that $a_0^s \in D_z$ for some $z \in \mathrm{W}_e$, $e \leq n$ i.e. it moves at most once as $n = 0$. Now assume a_n^s since the limit exists for $a_0, \ldots, a_{n-1}$, there is some stage s such that $a_0^s, \ldots, a_{n-1}^s$ does not move anymore and hence (since a_n^s moves iff a_i^s for $i \leq n$ moves, but a_i^s for $i < n$ does not move anymore) a_n^s can move at a stage $s+1$ only if it happens that $a_n^s \in D_z$ for some $z \in \mathrm{W}_e$, $e \leq n$.)

A is hypersimple:
By induction, suppose that s_0 is such that $s_0 \geq e$, all P_i with $i < e$ have been satisfied at stage s_0, and no finite set with index in W_i, $i < e$ goes into A after stage s_0. if W_e is a disjoint strong array intersecting $\overline{A}$, there are $s \geq s_0$ and $z \in \mathrm{W}_{e,s}$ such that $D_z \subseteq [a_e^s, +\infty)$.

Then, for one of these z, D_z goes into A at stage $s+1$ because e is the smallest index for which P_e looks unsatisfied and with chance to be satisfied, contradiction.
(This is again an inductive argument: suppose $e = 1$ then there is some s_0 such that P_0 is satisfied. Indeed, otherwise if there were no such a stage s_0 then $\forall s \forall z{\in}\mathrm{W}_{0,s} : D_z \not\subseteq [a_0^s, +\infty)$ but since $lim_{s\to+\infty} a_0^s$ exists it must be the case that $\forall z{\in}\mathrm{W}_{0,s}$, D_z contains an element $< \lim_{s\to+\infty} a_0^s$, but as W_e contains only disjoint elements and there is only finitely many such D_z's, W_e must be finite – contradiction. For $e+1$ use the induction argument that there is some stage s_0 such that all P_i's with $i \leq e$ are satisfied and proceed as in the previous case. Whence as P_e is satisfied for every e and so A is hypersimple by definition of P_e.)

□

Definition. *A set of formulas in a given language is called a first-order theory if it is closed under logical consequence. A theory is:*

1 ***axiomatizable*** *if it is the closure under logical consequence of an recursively enumerable set of formulas $\{\alpha_i\}_{i\in\omega}$*
2 ***independently axiomatizable*** *if it is axiomatizable and moreover for every i the formula α_i is not a logical consequence of the remaining formulas*
3 ***finitely axiomatizable*** *if it has a finite set of axioms*

Theorem (Kreisler, Pour-El 60's). *The following are equivalent for an axiomatizable first-order theory F:*

1 F is independently axiomatizable
2 for any axiomatization $\{\alpha_i\}_{i\in\omega}$ of F the set $A = \{n \mid \alpha_0 \wedge \ldots \wedge \alpha_n \vdash \alpha_{n+1}\}$ is not hypersimple
3 for some axiomatization $\{\alpha_i\}_{i\in\omega}$ of F the set $A = \{n \mid \alpha_0 \wedge \ldots \wedge \alpha_n \vdash \alpha_{n+1}\}$ is not hypersimple

Proof. Note that if F is finitely axiomatizable it is trivial. Hence we can assume F is not finitely axiomatizable in the whole proof.

1 $\to$ 2: Let $\{\beta_i\}_{i\in\omega}$ be an independent axiomatization of F and let $\{\alpha_i\}_{i\in\omega}$ be a given axiomatization of F. We would like to show that there exists an ISDA W_e such that $\forall z \in \mathrm{W}_e : D_z \cap \overline{A} \neq \emptyset$. Note that it is sufficient to show that there exists an algorithm which for every $n \in \omega$ find $m \in \omega$ such that $\{n, n+1, \ldots, m-1\} \cap \overline{A} \neq \emptyset$. Then whenever f is such an algorithm, $W = \{code(\{i, i+1, \ldots, f(i)-1\}) \mid i \in \{0, f(0), f(f(0)), f(f(f(0))), \ldots\}\}$ is an ISDA intersecting $\overline{A}$ by every element.

We show there exist such an algorithm:

Let $n \in \omega$ be given, then

$$\exists p \in \omega : \beta_0 \wedge \ldots \wedge \beta_p \vdash \alpha_0 \wedge \ldots \wedge \alpha_n$$

and since $\{\alpha_i\}_{i\in\omega}$ is an axiomatization of F also

$$\exists m \in \omega : \alpha_0 \wedge \ldots \wedge \alpha_m \vdash \beta_{p+1}.$$

Note that $m > n$. Indeed, otherwise if $m \leq n$ then $\beta_0 \wedge \ldots \wedge \beta_p \vdash \alpha_0 \wedge \ldots \wedge \alpha_n \vdash \alpha_0 \wedge \ldots \wedge \alpha_m \vdash \beta_{p+1}$ hence $\beta_0 \wedge \ldots \wedge \beta_p \vdash \beta_{p+1}$ which is a contradiction since $\{\beta_i\}_{i\in\omega}$ is an independent axiomatization.

Finally we show that $\{n, n+1, \ldots, m-1\} \cap \overline{A} \neq \emptyset$:

Suppose for a contradiction $\forall k \in \{n, n+1, \ldots, m-1\} : k \in A$, then $\alpha_0 \wedge \ldots \wedge \alpha_n \vdash \alpha_{n+1}$ and hence by induction $\alpha_0 \wedge \ldots \wedge \alpha_n \vdash \alpha_0 \wedge \ldots \wedge \alpha_m \vdash \beta_{p+1}$. However from $\beta_0 \wedge \ldots \wedge \beta_p \vdash \alpha_0 \wedge \ldots \wedge \alpha_n$ we derive $\beta_0 \wedge \ldots \wedge \beta_p \vdash \beta_{p+1}$ which is the contradiction and we are done.

$3 \to 1$: Suppose $\{\alpha_i\}_{i\in\omega}$ is an axiomatization of F and W_e ISDA intersecting $\overline{A}$ by every element. We split the construction of an independent axiomtization S into two steps, at first we show there is a procedure which for any formula γ finds a formula γ' such that $\gamma \nvdash \gamma'$ and using this procedure we construct a r.e. independent subset of formulas from F. In second step we refine this independent subset into an independent axiomatization of F by ensuring that $S \vdash \alpha_i$ for every $i \in \omega$.

Let γ be a formula provable in F. Then there exists $n \in \omega$ such that $\alpha_0 \wedge \ldots \wedge \alpha_n \vdash \gamma$. Since W_e is infinite there is some $z \in \mathrm{W}_e$ with $\forall j \in D_z : j > n$. Using D_z we define γ' to be a formula $\bigwedge_{j\in D_z} \alpha_{j+1} \wedge \bigwedge_{j\leq min(D_z)} \alpha_j$. To show $\gamma \nvdash \gamma'$ argue as follows: let $k \in D_z \cap \overline{A}$, then $\alpha_0 \wedge \ldots \wedge \alpha_k \nvdash \alpha_{k+1}$ i.e $\alpha_0 \wedge \ldots \wedge \alpha_k \nvdash \gamma'$ but since $k > n$, $\alpha_0 \wedge \ldots \wedge \alpha_k \vdash \gamma$ and whence $\gamma \nvdash \gamma'$.

Now assume formulas defined by: $\delta_0 : \alpha_0 \wedge \alpha_0'$ and $\delta_{n+1} : \delta_n \wedge \alpha_{n+1} \wedge (\delta_n \wedge \alpha_{n+1})'$ then

$$S \;:\; \delta_0, \delta_0 \to \delta_1, \delta_1 \to \delta_2, \ldots$$

forms an independent axiomatization of F. Since α_n is provable from the first n axioms of S, it remains to show it is independent.

It is clear that for any $j \in \omega$: (i) $\forall i < j : \delta_i \nvdash \delta_j$ and (ii) $\forall i \leq j : \delta_j \vdash \delta_i$.

We show δ_0 is not provable from $S - \{\delta_0\}$ at first: By (i) $\delta_0 \nvdash \delta_i$, $T_0 = \{\neg\delta_0\} \cup \{\neg\delta_1\}$ has a model and $T_0 \nvdash \delta_2$ (otherwise $T \vdash \delta_1$ by (ii), but this is not possible) and whence

$T_1 = T_0 \cup \{\neg\delta_2\}$ has model and so on inductively $T = \bigcup_{i\in\omega} T_i$ has a model by compactness and $T \vdash \delta_i \to \delta_{i+1}$ for all $i \in \omega$.

To show $\delta_j \to \delta_{j+1}$ is not provable from $S - \{\delta_j \to \delta_{j+1}\}$ argue as follows: Let $j \in \omega$ be given, then we construct a model for $\neg(\delta_j \to \delta_{j+1})$ where $\delta_i \to \delta_{i+1}$ holds for every $i \neq j$, which proves the independence of $\delta_j \to \delta_{j+1}$. Assume $T = \{\delta_j \wedge \neg\delta_{j+1}\}$ then by (i), T has a model and by (ii), $T \vdash \delta_0$ and $T \vdash \delta_i \to \delta_{i+1}$ for $i < j$. Note further that $T \not\vdash \delta_{j+2}$ (otherwise $T \vdash \delta_{j+1}$ by (ii), but this is not possible) and whence $T' = T \cup \{\neg\delta_{j+2}\}$ has a model. By induction and compactness as in the previous case there exists a model witnessing an independence of $\delta_j \to \delta_{j+1}$ and we are done.

□

References

[ODI] P.G. Odifreddi. *Classical Recursion Theory.* North-Holland, Amsterdam, 1992