# 117b: Computability



Garrett Ervin
gervin@caltech.edu
OH (tentative): Tu/Th 2:30–4:00 pm
Office: Kellogg 204

The class:

- Eval: approx 8 HW sets
- focus on: undecidability + incompleteness results
- a big goal: prove Gödel's Incompleteness theorems
- before that: relative computability + Turing degrees + some complexity theory

---

Recursion relative to an oracle

PR and R:

~~[illegible]~~ – all functions of form $f: \mathbb{N}^n \to \mathbb{N}$ for some $n$; e.g. $f: \mathbb{N}^2 \to \mathbb{N}$
$f(x, y) = x + y$

– $f$ can be partial.

Recall: the class PR of primitive recursive functions is the smallest class containing the

"basic functions"
(1) constant-0 functions $c_n : \mathbb{N}^n \to \mathbb{N}$
$c_n(x_1, \dots, x_n) = 0$
(2) successor $S : \mathbb{N} \to \mathbb{N}$, $S(x) = x+1$
(3) projections $\pi_j^n : \mathbb{N}^n \to \mathbb{N}$
$\pi_j^n(x_1, \dots, x_j, \dots, x_n) = x_j$

and closed under
(i) composition: if $f : \mathbb{N}^n \to \mathbb{N}$ is pr and $h_1, h_2, \dots, h_n : \mathbb{N}^k \to \mathbb{N}$ are pr. then so is $f(h_1, \dots, h_n) : \mathbb{N}^k \to \mathbb{N}$

(ii) primitive recursion. if $h : \mathbb{N}^{n+2} \to \mathbb{N}$ and $g : \mathbb{N}^n \to \mathbb{N}$ are p.r. then so is: $f : \mathbb{N}^{n+1} \to \mathbb{N}$ defined by:

$$f(0, x_1, \dots, x_n) = g(x_1, \dots, x_n)$$
$$f(y+1, x_1, \dots, x_n) = h(f(y, x_1, \dots, x_n), y, x_1, \dots, x_n)$$

↳ p.r. functions always total
↳ $x+y$, $xy$, $x^y$, the function $f(p) = 1$ iff $p$ is prime, etc. etc. .. all p.r.

write $\vec{x}$ for $(x_1, \dots x_n)$ when parity is clear.

The recursive functions $\mathcal{R}$ is the smallest class containing the basic functions, closed under comp'n, prim. recurs'n and:

(iii) minimalization: if $g: \mathbb{N}^{n+1} \to \mathbb{N}$ is in $\mathcal{R}$ then so is $f: \mathbb{N}^n \to \mathbb{N}$

$$f(\vec{x}) = \mu y\, [g(y, \vec{x}) = 0]$$

where:

$$\mu y [g(y, \vec{x}) = 0] = k \quad \text{iff} \quad g(k, \vec{x}) = 0 \text{ and } \forall k' < k \;\; g(k', \vec{x}) \neq 0 \text{ and } g(k', \vec{x}) \text{ defined}$$

Fact: p.r. functions closed under bounded $\mu$ i.e. $\mu y < n[\ldots]$

↳ $\mu$'ing leads to partial functions

↳ write: $f(\vec{x})\downarrow$ if $f$ defined @ $\vec{x}$

o.w. $f(\vec{x})\uparrow$

## Relative $\mathcal{R}$

- Sps $F_1, \ldots, F_n$ are total functions $F_i : \mathbb{N}^{n_i} \to \mathbb{N}$ (think: $F_i$ are not in $\mathcal{R}$)

**Def'n** a function $f: \mathbb{N}^k \to \mathbb{N}$ is recursive in the functions $F_1, \ldots, F_n$ (write: $f \in \mathcal{R}(F_1, \ldots, F_n)$) iff $f$ belongs to smallest class containing basic functions and the $F_i$, and closed under (i), (ii), (iii) turns out:

↳ can get away w/ a single unary function:

Lemma. there is a unary $\alpha: \mathbb{N} \to \mathbb{N}$ s.t. $R(\alpha) = R(F_1, \dots, F_n)$

Before pf, recall:

- for every $n$ there is a p.r. (prim. recursive) injection $\langle \cdot, \dots, \cdot \rangle_n : \mathbb{N}^n \to \mathbb{N}$ defined by
$$\langle x_0, \dots, x_{n-1} \rangle_n = \prod_{0 \le i \le n-1} p_i^{x_i + 1}$$
"code" for sequence $(x_0, \dots, x_{n-1})$
- e.g. $\langle 2, 6, 1 \rangle = 2^3 3^7 5^2$
- often drop subscript as above - but there are technically $\infty$ many coding functions, one for each $n$.
- the function length(s) = # of primes in factorization of s (= length of sequence coded by s when s is a code) is p.r.
- for $s \in \mathbb{N}$ write $(s)_j$ for (exponent of $p_j$ in decomp. of s) − 1 (or 0 when this is −1)
- then $(\,)_j$ is pr and when $s = \langle x_0, \dots, x_j, \dots, x_{n-1} \rangle$ is a code we have $(s)_j = x_j$

- concatenation function $*: \mathbb{N}^2 \to \mathbb{N}$ which when $s = \langle x_0, .., x_{n-1} \rangle$
$t = \langle y_0, .., y_{m-1} \rangle$
returns $s * t = \langle x_0, .., x_{n-1}, y_0, .., y_{m-1} \rangle$
is p.r.

"Pf" of lemma: - for each $F_i : \mathbb{N}^{n_i} \to \mathbb{N}$ consider unary $F_i' : \mathbb{N} \to \mathbb{N}$ defined by $F_i'(s) = F_i((s)_0, .., (s)_{n_i - 1})$

- then $\alpha : \mathbb{N} \to \mathbb{N}$ defined by
$\alpha(s) = \langle F_1'(s), .., F_n'(s) \rangle$ works

(point: values $F_i(\vec{x})$ can be extracted from values $\alpha(s)$ in a (prim) recursive way and vice versa
so $R(\alpha) = R(F_1, .., F_n)$ ) ✓

Def'n An oracle is a total function $\alpha : \mathbb{N} \to \mathbb{N}$ (think: non-recursive)

Recall: a relation $P \subseteq \mathbb{N}^n$ is called (prim) recursive iff char. function $\chi_p$ is (prim) rec. where $\chi_p : \mathbb{N}^n \to \{0,1\}$ defined by $\chi_p(x_1, .., x_n) = 1$ iff $(x_1, .., x_n) \in P$ ← write $P(x_1, .., x_n)$

<u>Fact</u>: p.r. sets are closed under Boolean operations and <u>bounded</u> min (i.e. $\mu y < n \ldots$) and definitions by $\neg, \wedge, \vee, =, <$, and <u>bounded</u> quantification (i.e. $\exists x < n \ldots$ $\forall x < n \ldots$)

Given $\alpha : \mathbb{N} \to \mathbb{N}$ define $\bar{\alpha} : \mathbb{N} \to \mathbb{N}$ by $\bar{\alpha}(n) = \langle \alpha(0), \ldots, \alpha(n-1) \rangle$

<u>Fact</u>: $\bar{\alpha}$ is p.r. in $\alpha$ (roughly: $\bar{\alpha}(n+1) = \bar{\alpha}(n) * \langle \alpha(n) \rangle$ is rec. defn)

and $\alpha$ is p.r. in $\bar{\alpha}$ ($\alpha(n)$ = last exp in $\bar{\alpha}(n+1)$)

So: $R(\alpha) = R(\bar{\alpha})$

<u>Theorem</u> Sps $f : \mathbb{N}^n \to \mathbb{N}$ is a partial function.

Then $f \in R(\alpha)$ iff there is a p.r. relation $P \subseteq \mathbb{N}^{n+2}$ s.t.

(*) $$f(\vec{x}) = y \Leftrightarrow \exists k \, P(\vec{x}, y, \bar{\alpha}(k))$$

<u>Pf</u> ($\Leftarrow$) Given such a $P$ can compute $f$ as follows.

$$f(\vec{x}) = \left(\mu s\left[\chi_P(\vec{x}, (s)_0, \bar{\alpha}((s)_1)) = 1\right]\right)_0$$

which is in $R(\bar{\alpha}) = R(\alpha)$

"Search over codes of pairs $s = \langle y, n\rangle$ until we find least one (if exists) s.t. $P(\vec{x}, y, \bar{\alpha}(n))$ true, and return $y$"

($\Rightarrow$) Suff. to check class of $f$ defined as in ✱ contains basic functions and $\alpha$, closed under comp'n, prim. recurs'n, minimal'n

For $c_n$'s, successor $S$, projections $\pi^n_i$ — follows from fact: graphs of p.r. $f$'s are p.r.

e.g. for $S$:

is p.r.!

$S(x) = y$ iff $\chi_=(S(x), y) = 1$

iff $S(x) = y$ "fmla" version

iff $\exists k\,(S(x) = y)$ in desired form $P(x, y, z)$ is "$S(x) = y$"

For $\alpha$: $\alpha(x) = y$ iff $(\bar{\alpha}(x+1))_x = y$

iff $\exists k(\text{length}(\bar{\alpha}(k)) = x+1$

$\wedge\ y = (\bar{\alpha}(k))_x)$

in desired form: $P(x,y,z)$

$\Downarrow$ $\text{length}(z) = x+1 \wedge$

p.r. $\rightarrow$ $y = (z)_x$ $\Leftarrow$

<u>Composition</u>: for simplicity – but sufficient – why?

- Assume we are dealing w/ a unary

$h(x) = f(g(x))$

and $f, g$ defined by $P, Q$ as in ✡.

- i.e. $g(x) = y$ iff $\exists k\, Q(x,y,\bar{\alpha}(k))$

$f(y) = z$ iff $\exists k'\, P(y,z,\bar{\alpha}(k'))$

- then $h(x) = z$ iff $\exists y(g(x) = y \wedge f(y) = z)$

iff $\exists y(\exists k\, Q(x,y,\bar{\alpha}(k)) \wedge \exists k' P(y,z,\bar{\alpha}(k')))$

iff $\exists y \exists k \exists k' (\,Q(..) \wedge P(..)\,)$

iff $\exists s\,(Q(x, (s)_0, \bar{\alpha}((s)_1)) \wedge P((s)_0, z, \bar{\alpha}((s)_2))$

think $s = \langle y, k, k' \rangle$

not quite right form, but convince:

there are p.r. functions $b, c, d$ s.t.

$b(\bar{\alpha}(s)) = (s)_0$ $c(\bar{\alpha}(s)) = \bar{\alpha}((s)_1)$ $d(\bar{\alpha}(s)) = \bar{\alpha}((s)_2)$

$\rightarrow$ iff $\exists s\,\big(Q(x, b(\bar{\alpha}(s)), c(\bar{\alpha}(s))) \wedge$

$P(b(\bar{\alpha}(s)), z, d(\bar{\alpha}(s)))\big)$

p.r.

iff $\exists s\,(R(x,z,\bar{\alpha}(s)))$

For general (non unary case): exercise
(or see: unary case enough w/ coding)

prim. recursion: exercise

minimalization: Sps we have unary
$f(x) = \mu t[g(x,t)=0]$ and
$g(x,t)=y$ iff $\exists k\, P(x,t,y,\bar{\alpha}(k))$

then $f(x)=y$ iff $g(x,y)=0 \wedge \forall z<y\ g(x,z)>0$ and defined

iff $\exists k(P(x,y,0,\bar{\alpha}(k))) \wedge$
$\forall z<y\ \exists w\,(w>0 \wedge \exists l\, P(x,z,w,\bar{\alpha}(l)))$

iff $\exists k\Big(P(\ldots) \wedge \exists w\ \forall z<y\,((w)_z>0 \wedge \exists l\, P(x,z,(w)_z,\bar{\alpha}(l)))\Big)$

iff $\exists k\Big(P(..) \wedge \exists w\,\exists l\,\forall z<y\,((w)_z>0 \wedge P(x,z,(w)_z,\bar{\alpha}((l)_z)))\Big)$

iff $\exists s$ ~~[illegible]~~
$\langle k,w,l\rangle$
$(P(x,y,0,\bar{\alpha}((s)_0)) \wedge \forall z<y\,(((s)_1)_z>0 \wedge$
$P(x,z,((s)_1)_z,(\bar{\alpha}(((s)_2)_z))))$

iff $\exists s\, R(x,y,\bar{\alpha}(s))$

R p.r. using some tricks before to set R as function of $\bar{\alpha}(s)$

<u>Theorem</u> (Kleene's normal form theorem relative to $\alpha$). There is a p.r. function $U: \mathbb{N} \to \mathbb{N}$ and a p.r. relation $T \subseteq \mathbb{N}^3$ s.t. for every oracle $\alpha$,
every $f: \mathbb{N}^n \to \mathbb{N}$ that is in $R(\alpha)$
has the form

$$U(\mu k[T(e, \langle x_1, \ldots, x_n \rangle, \bar{\alpha}(k))])$$

for some $e \in \mathbb{N}$

<u>Pf</u>: Recall (117a) there is a p.r. relation $T'$ that is "universal for recursive(ly enumerable) relations"
i.e. for each rec(ly enumerable) $Q \subseteq \mathbb{N}^n$ there is $e \in \mathbb{N}$ s.t.

$$Q(x_1, \ldots, x_n) \text{ iff } \exists m\, T'(e, \langle x_1, \ldots, x_n \rangle, m)$$

($e$ codes the "computation tree" of $Q$)

<u>Now</u>: sps $f: \mathbb{N}^n \to \mathbb{N}$ is recursive in $\alpha$
- by prev thm there is p.r. $P$ s.t.

$$f(x_1, \ldots, x_n) = y \text{ iff } \exists k\, P(x_1, \ldots, x_n, y, \bar{\alpha}(k))$$

Hence for some $e$ we have