117b: Computability

Garrett Ervin
gervin @ caltech.edu
OH: TBA
Office: 204 Kellogg

Class overview:
- evaluation: 5 - 8 HW sets
- grading cutoffs: not more harsh than standard cutoffs 90 - 100 = A
80 - 89 = B, etc.

- content: a big goal: prove Gödel's Incompleteness Theorems
  - ↳ before that:
    - relative computability
    - Turing degrees
    - some complexity theory

Recursion relative to an oracle:

- 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. (i.e. $\mathrm{dom}(f) \subsetneq \mathbb{N}^n$)

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

"basic functions"
1. constant-0 functions $c_n : \mathbb{N}^n \to \mathbb{N}$
   $c_n(x_1, \ldots, x_n) = 0$
2. successor function $s : \mathbb{N} \to \mathbb{N}$ $s(x) = x+1$
3. projections: $\pi^n_j : \mathbb{N}^n \to \mathbb{N}$
   $\pi^n_j(x_1, \ldots, x_j, \ldots, x_n) = x_j$

and closed under

(i) composition: if $f : \mathbb{N}^n \to \mathbb{N}$ is p.r. and $h_1, \ldots, h_n : \mathbb{N}^k \to \mathbb{N}$ are p.r., so is $f(h_1, \ldots, h_n) : \mathbb{N}^k \to \mathbb{N}$

(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:

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

→ p.r. functions are always total

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

→ will write $\vec{x}$ for $(x_1, \ldots, x_n)$ when arity irrelevant or clear from context.

- The recursive functions R is the smallest class containing the basic functions that is closed under comp'n, prim. recurs'n, and (iii) minimalization: if $g: \mathbb{N}^{n+1} \to \mathbb{N}$ is in R then so is $f: \mathbb{N}^n \to \mathbb{N}$

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

where:

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

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

→ μ'ing leads to partial functions
→ write: $f(\vec{x})\downarrow$ if f defined @ $\vec{x}$
$f(\vec{x})\uparrow$ if not

Relative 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 R)

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

↳ turns out can get away w/ a <u>single</u> <u>unary</u> function

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

Before pf, recall:

- for every n there is a p.r. injection $\langle \cdot, \ldots, \cdot \rangle_n : \mathbb{N}^n \to \mathbb{N}$ defined by $\langle x_0, \ldots, x_{n-1} \rangle_n = \prod_{0 \le i \le n-1} p_i^{x_i+1}$ ← "code" for sequence $(x_0, \ldots, x_{n-1})$

$$= p_0^{x_0+1} p_1^{x_1+1} \cdots p_{n-1}^{x_{n-1}+1}$$

ith prime

- e.g. $\langle 2,6,1 \rangle = \underset{p_0}{2}^3 \underset{p_1}{3}^7 \underset{p_2}{5}^2$

- often drop subscript: $\langle \ldots \rangle$ instead of $\langle \ldots \rangle_n$ — but technically there are ∞ many coding functions, one for each n
- the function $\mathrm{length}(s)$ = # 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 factorization of s) -1 ← or 0 whichever greater
- then $(\cdot)_j$ is p.r. and when $s = \langle x_0, \ldots, x_{n-1} \rangle$ is a code and $j < n$ have $(s)_j = x_j$

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

<u>"pf" of Lemma</u>: - for each $F_i : \mathbb{N}^{n_i} \to \mathbb{N}$ consider the unary $F_i' : \mathbb{N} \to \mathbb{N}$ defined by $F_i'(s) = F_i((s)_0, \dots, (s)_{n_i - 1})$

- then $\alpha : \mathbb{N} \to \mathbb{N}$ defined by

$$\alpha(s) = \langle F_1'(s), \dots, F_n'(s) \rangle$$ works ✓

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

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

<u>Recall</u>: a relation $P \subseteq \mathbb{N}^n$ is called <u>(prim.) recursive</u> iff char. function χ_P is (prim.) recursive

where $\chi_P : \mathbb{N}^n \to \{0, 1\}$

$\chi_P(\vec{x}) = 1$ iff $\vec{x} \in P$

write $P(\vec{x})$

<u>Fact</u>: p.r. relations are closed under

- Boolean operations $\neg, \cap, \cup$
- bdd minimalization $(\mu y < n [\dots])$

- definitions by $\neg, \wedge, \vee, =, <$
- bdd quantification (i.e. $\exists x < n\ [\cdots]$
  $\forall y < n\ [\cdots]$)

- 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 α (roughly: $\bar{\alpha}(n+1) = \bar{\alpha}(n) * \langle \alpha(n) \rangle$ is p.r. def'n)

and α is p.r. in $\bar{\alpha}$ ($\alpha(n)$ = last nonzero exponent 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. rel'n $P \subseteq \mathbb{N}^{n+2}$ s.t.

$$(\star) \qquad f(\vec{x}) = y \quad \text{iff} \quad \exists k\, P(\vec{x}, y, \bar{\alpha}(k))$$

"f is recursive (in α) iff graph(f) is r.e. (in α)"

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

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

"search for least $s = \langle y, n, \rangle$ (if exists) s.t. $P(\vec{x}, y, \bar{\alpha}(n))$, and return y"

($\Rightarrow$) suff. to check class of f defined by $(\star)$ contains basic functions and α, and is closed under comp'n, prim. recurs'n, and minimal'n.

- for cn's, successor s, projections π_j^n (i.e. basic functions) follows from

<u>117a Fact</u>: graph's of p.r. f's are p.r.

- e.g. for s:

is p.r.

$$s(x) = y \quad \text{iff} \quad \chi_{=}(s(x), y) = 1$$

$$\text{iff} \quad s(x) = y$$ ("fmla version")

$$\text{iff} \quad \exists k\,(s(x) = y)$$ (in desired form ⊛: $P(x,y,z)$ is "$s(x) = y$")

is p.r.

dummy variable just so in desired form

- for α: $\alpha(x) = y$ 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

$P(x,y,z)$ is

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

- <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 $\exists y \exists k \exists k'\, (Q(\ldots) \wedge P(\ldots))$
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 yourself: there are p.r. functions b, c, d s.t.
$b(\bar{\alpha}(s)) = (s)_0$ $\quad c(\bar{\alpha}(s)) = \bar{\alpha}((s)_1)$ $\quad d(\bar{\alpha}(s)) = \bar{\alpha}((s)_2)$

iff $\exists s\, (Q(x, b(\bar{\alpha}(s)), c(\bar{\alpha}(s))) \wedge$
$P(b(\bar{\alpha}(s)), z, d(\bar{\alpha}(s))))$

iff $\exists s\, R(x, z, \bar{\alpha}(s))$ ← desired form
where $R(x, z, q)$ is $Q(x, b(q), c(q)) \wedge$
$P(b(q), z, d(q))$
→ is p.r.

- prim. recursion: exercise