Ma 117a: Computability

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

TA: Michael Wolman
mwolman@caltech.edu
OH: TBA

Assessment = 7-8 HWs
- one 1-week extension
- one 48 hr extension

Grade cutoffs = not worse than standard 90-100 = A, 80-89 = B, etc

Textbook: none; will post class notes on Canvas

Course outline

our focus in 117a
① Concept of a computable function (aka recursive function)

② Basic theory of computable functions

(3) Relations w/ logic and number theory

(4) Undecidable problems

(8) Decidable problems + computational complexity

The big question

Q: What does it mean for a function (e.g. $f: \mathbb{N}^n \to \mathbb{N}$) to be computable?

↳ many familiar functions are intuitively computable, e.g. $\gcd(m,n)$
↳ need a rigorous def'n if we want to show a given f is/isn't computable

---

Alphabets and Strings

- an alphabet is a nonempty set A (usually finite) whose elements are called symbols
- a word or string from A is a sequence $w = a_1 a_2 \cdots a_n$ of symbols $a_i \in A$

will write as 0!

- the *empty word* $0 = \emptyset$ has no symbols
- the *length* of a word $w = a_1 \cdots a_n$ is n
write: $|w| = n$ (note: $|0| = 0$ .. bad notation alert)

- $A^n :=$ set of all words of length n on A
- $A^* := \bigcup_{n \in \mathbb{N}} A^n =$ all (finite) words on A

- the *concatenation* of $u = a_1 \cdots a_n$ and $v = b_1 \cdots b_m$ is $uv := a_1 \cdots a_n b_1 \cdots b_m$
- a word w *occurs in* v if $v = xwy$ for some $x, y \in A^*$

- we consider functions $f: (A^*)^n \to A$ called *n-ary total functions*

- if $A = \{a\}$ consists of a single symbol we think of $A^* = \{0, a, aa, aaa, \ldots\}$ as being $\mathbb{N} = \{0, 1, 2, \ldots\}$

Primitive recursive functions

- primitive recursive (pr) functions are an attempt to capture notion of "computable function"
- are built from some simple basic functions using composition and recursion
- we'll see: pr functions do not fully capture notion of "computable function"

- Sps $A = \{\sigma_1, \sigma_2, \dots, \sigma_k\}$ is our alphabet

The initial functions are the:

① Erase function: $E: A^* \to A^*$
$E(x) = 0$

② Successor functions: for $1 \le j \le k$
$S_j : A^* \to A^*$
$S_j(x) = x\sigma_j$ ("+1" when $A^* = \mathbb{N}$)

③ Projection functions: For any n and $1 \le j \le n$, $P_j^n : (A^*)^n \to A^*$
$P_j^n(w_1, \dots, w_j, \dots, w_n) = w_j$
↳ note: P_1^1 is identity

The composition rules are:

④ Substitution (generalized composition):
given $g: (A^*)^m \to A^*$ and $h_1, \dots, h_m : (A^*)^n \to A^*$
we construct $f: (A^*)^n \to A^*$ by defining:
$f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$
↳ note: when n understood write $\vec{x}$ for $(x_1, \dots, x_n)$

⑤ Primitive recursion: given $g: (A^*)^n \to A^*$ starting function
and $h_1, \dots, h_k : (A^*)^{n+2} \to A^*$, construct
one for each symbol in A
$f: (A^*)^{n+1} \to A^*$ by:
$f(0, x_1, \dots, x_n) = g(x_1, \dots, x_n)$
$f(y\sigma_j, x_1, \dots, x_n) = h_j(f(y, x_1, \dots, x_n), y, x_1, \dots, x_n)$

"compute $f(0)$ (using $\vec{x}$ parameters)
using g (@ $\vec{x}$)"
" compute $f(y\sigma_j)$ using h_j @ $f(y)$"
... so (roughly) e.g. $f(\sigma_i\sigma_j\sigma_k) =$
$h_k(h_j(h_i(g(0))))$

Note: allow $n=0$ in 5 (no parameters $\vec{x}$),
in which case convention is g is a constant
so recurs'n looks like: $f(0) =$ constant
$f(y\sigma_j) = h_j(f(y), y)$

<u>Def'n</u> (i) $f: (A^*)^n \to A^*$ is <u>primitive recursive (pr)</u> if it can be obtained from the initial functions 1–3 by applying 4–5

(ii) if $f_1, \ldots, f_m = f$
where f_i is an init. function or obtained from previous functions by applying 4, 5
then is called a pr <u>derivation</u> of f.

<u>Ex's</u> 1 Given $w \in A^*$, the constant function $C_w(x) = w$ is p.r.

<u>Pf</u>: we induct on $n = |w|$
– if $w = 0$ is empty word, $C_w = E$ is erase function
– if $w = y\sigma_j$ and C_y is p.r.
then $C_w(x) = C_y(x)\sigma_j$
$= S_j(C_y(x))$
which is p.r. (using 4)

2. Given n, and $x_1, \ldots, x_n \in A^*$, define $con_n(x_1, \ldots, x_n) = x_1 \cdots x_n$ be n-wise concatenation function.

<u>Claim</u>: con_n is pr.

<u>Pf</u>: - induct on n

- con_1 is P^1_1
- we define con_2 using (S)
- by convention we recurse on first coord, so we first show $con_2^*(y,x) = xy$ is p.r.

$$con_2^*(0, y) = y = P^1_1(y) \quad (\text{so } g = P^1_1)$$

$$\begin{aligned} con_2^*(x\sigma_j, y) &= yx\sigma_j \\ &= con_2^*(x,y)\sigma_j \\ &= S_j(P^3_1(con_2^*(x,y), x, y)) \end{aligned}$$

(so h_j is $S_j(P^3_1(x_1, x_2, x_3))$ which is p.r. by (C))

$\Rightarrow con_2^*$ is pr by (S)

- now note: $con_2(x,y) = xy = con_2^*(y,x)$
$$= con_2^*(P^2_2(x,y), P^2_1(x,y))$$
which is pr by (C)

- now note: $con_3(x,y,z) = con_2(con_2(x,y), z)$
$$= con_2(con_2(P^3_1(x,y,z), P^3_2(x,y,z)), P^3_3(x,y,z))$$
which is pr by (C)

- etc. for $n > 3$

3. Given n and $x \in A^*$, define $F_n(x) = xx \cdots x$ (n-times) (write x^n)

Then F_n is p.r. Pf: you try

4 Define $Del_r : A^* \to A^*$ by:

$Delr(x) = 0$ if $x = 0$

$= y$ if $x = y\sigma_j$.

Then Del_r is p.r.

pf: $Del_r(0) = 0$ (so gis constant 0)

$Del_r(y\sigma_j) = y = P_2^2(Del_r(y), y)$ ✓

5 For a word x, write x^* for reverse of x, if $x = a_1 a_2 \ldots a_n$, $x^* = a_n \ldots a_2 a_1$

Define $Rev : A^* \to A^*$ by

$Rev(x) = x^*$

abuse of notation different use of * than A^*

Then Rev is p.r.

pf: $Rev(0) = 0$

$Rev(x\sigma_j) = \sigma_j Rev(x)$

$= Con_2^*(Rev(x), \sigma_j)$

hence Rev is pr by 8

(being informal here — can you formalize? use projections and C_{σ_j})

6 Define $Del_e(x) = Rev(Del_r(Rev(x)))$

is p.r. ✓

7 Given $x, y \in A^*$, let $x - y$ denote x minus first $|y|$ symbols

(e.g. $\sigma_1\sigma_2\sigma_1 - \sigma_3\sigma_3 = \sigma_1$)

Then: $x - y$ is p.r. (i.e. $f(x,y) = x - y$ is p.r.)

pf: $x - 0 = x$

$x - (y\sigma_j) = \mathrm{Pel}_e(x - y)$ ✓

(can you formalize?)

8. Define $\mathrm{Lev}: A^* \to A^*$ by

$\mathrm{Lev}(x) = 0$ if $x = 0$

$= \sigma_1$ if $x \neq 0$

← think of σ_1 as "1"

Then Lev is p.r.

pf: $\mathrm{Lev}(0) = 0$

$\mathrm{Lev}(x\sigma_j) = \sigma_1 \Leftarrow C_{\sigma_1}(P_1^2(\mathrm{Lev}(z), \cancel{x}))$

9. Define $\mathrm{Lev}'(x) = 0$ if $x \neq 0$

$= \sigma_1$ if $x = 0$

is p.r. (Why?)

10. Define $\mathrm{End}_j(x) = 0$ if $x = y\sigma_j$

$= \sigma_1$ o/w

Then End_j is p.r.

pf. $\mathrm{End}_j(0) = \sigma_1$

$\mathrm{End}_j(y\sigma_k) = 0$ if $k = j$

$= \sigma_1$ if $k \neq j$

(Let $h_k = E$ for $k = j$

$= S_1(E)$ for $k \neq j$)

(11) For $x, y \in A^*$, define $Ex'(x,y) := x^{|y|} = xx\ldots x$ ($|y|$ times)

(note $x^0 = \sigma_1$)

Then Ex' is pr

pf: $Ex'(x,0) = \sigma_1$

$Ex'(x, y\sigma_j) = con_2(Ex'(x,y), x)$

(12) define $Ex(x) = x^{|x|}$

Then Ex is p.r. (why?)