

Turing machines

Computable functions

Recall:

Definition. $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ is (**register machine**) **computable** if there is a register machine M with at least $n + 1$ registers R_0, R_1, \dots, R_n (and maybe more)

such that for all $(x_1, \dots, x_n) \in \mathbb{N}^n$ and all $y \in \mathbb{N}$,

the computation of M starting with $R_0 = 0, R_1 = x_1, \dots, R_n = x_n$ and all other registers set to 0, halts with $R_0 = y$

if and only if $f(x_1, \dots, x_n) = y$.

Turing computable function

Definition. $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ is **Turing computable** if and only if there is a Turing machine M with the following property:

Starting M from its initial state with tape head on the left endmarker of a tape coding $[0, x_1, \dots, x_n]$, M halts if and only if $f(x_1, \dots, x_n) \downarrow$, and in that case the final tape codes a list (of length ≥ 1) whose first element is y where $f(x_1, \dots, x_n) = y$.

Theorem. A partial function is Turing computable if and only if it is register machine computable.

Proof (sketch). We've seen how to implement any TM by a RM. Hence

f TM computable implies f RM computable.

For the converse, one has to implement the computation of a RM in terms of a TM operating on a tape coding RM configurations. To do this, one has to show how to carry out the action of each type of RM instruction on the tape. It should be reasonably clear that this is possible in principle, even if the details (omitted) are tedious.

Notions of computability

- Church (1936): λ -calculus [see later]
- Turing (1936): Turing machines.

Turing showed that the two very different approaches determine the same class of computable functions. Hence:

Church-Turing Thesis. Every algorithm [in intuitive sense of Lect. 1] can be realized as a Turing machine.

Notions of computability

Church-Turing Thesis. Every algorithm [in intuitive sense of Lect. 1] can be realized as a Turing machine.

Further evidence for the thesis:

- Gödel and Kleene (1936): **partial recursive functions**
- Post (1943) and Markov (1951): **canonical systems** for generating the theorems of a formal system
- Lambek (1961) and Minsky (1961): **register machines**
- Variations on all of the above (e.g. **multiple tapes**, non-determinism, **parallel execution**...)

All have turned out to determine the same collection of computable functions.

Notions of computability

Church-Turing Thesis. Every algorithm [in intuitive sense of Lect. 1] can be realized as a Turing machine.

In rest of the course we'll look at

- Gödel and Kleene (1936): **partial recursive functions**
(\leadsto branch of mathematics called **recursion theory**)
- Church (1936): **λ -calculus**
(\leadsto branch of CS called **functional programming**)

Partial recursive functions

Aim

A more abstract, machine-independent description of the collection of computable partial functions than provided by register/Turing machines:

*they form the smallest collection of partial functions containing some **basic** functions and closed under some fundamental operations for forming new functions from old—**composition, primitive recursion and minimization.***

The characterization is due to Kleene (1936), building on work of Gödel and Herbrand.

Basic functions

- **Projection** functions, $\text{proj}_i^n \in \mathbb{N}^n \rightarrow \mathbb{N}$:

$$\text{proj}_i^n(x_1, \dots, x_n) \triangleq x_i$$

- **Constant** functions with value 0, $\text{zero}^n \in \mathbb{N}^n \rightarrow \mathbb{N}$:

$$\text{zero}^n(x_1, \dots, x_n) \triangleq 0$$

- **Successor** function, $\text{succ} \in \mathbb{N} \rightarrow \mathbb{N}$:

$$\text{succ}(x) \triangleq x + 1$$

Basic functions

are all RM computable:

- Projection proj_i^n is computed by

$$\text{START} \rightarrow \boxed{R_0 ::= R_i} \rightarrow \text{HALT}$$

- Constant zero^n is computed by

$$\text{START} \rightarrow \text{HALT}$$

- Successor succ is computed by

$$\text{START} \rightarrow R_1^+ \rightarrow \boxed{R_0 ::= R_1} \rightarrow \text{HALT}$$

Composition

Composition of $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ with $g_1, \dots, g_n \in \mathbb{N}^m \rightarrow \mathbb{N}$ is the partial function $f \circ [g_1, \dots, g_n] \in \mathbb{N}^m \rightarrow \mathbb{N}$ satisfying for all $x_1, \dots, x_m \in \mathbb{N}$

$$f \circ [g_1, \dots, g_n](x_1, \dots, x_m) \equiv f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$$

where \equiv is “Kleene equivalence” of possibly-undefined expressions: **LHS \equiv RHS** means “either both **LHS** and **RHS** are undefined, or they are both defined and are equal.”

Composition

Composition of $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ with $g_1, \dots, g_n \in \mathbb{N}^m \rightarrow \mathbb{N}$ is the partial function $f \circ [g_1, \dots, g_n] \in \mathbb{N}^m \rightarrow \mathbb{N}$ satisfying for all $x_1, \dots, x_m \in \mathbb{N}$

$$f \circ [g_1, \dots, g_n](x_1, \dots, x_m) \equiv f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$$

So $f \circ [g_1, \dots, g_n](x_1, \dots, x_m) = z$ iff there exist y_1, \dots, y_n with $g_i(x_1, \dots, x_m) = y_i$ (for $i \in \{1 \dots n\}$) and $f(y_1, \dots, y_n) = z$.

Composition

Composition of $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ with $g_1, \dots, g_n \in \mathbb{N}^m \rightarrow \mathbb{N}$ is the partial function $f \circ [g_1, \dots, g_n] \in \mathbb{N}^m \rightarrow \mathbb{N}$ satisfying for all $x_1, \dots, x_m \in \mathbb{N}$

$$f \circ [g_1, \dots, g_n](x_1, \dots, x_m) \equiv f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$$

So $f \circ [g_1, \dots, g_n](x_1, \dots, x_m) = z$ iff there exist y_1, \dots, y_n with $g_i(x_1, \dots, x_m) = y_i$ (for $i \in \{1 \dots n\}$) and $f(y_1, \dots, y_n) = z$.

N.B. in case $n = 1$, we write $f \circ g_1$ for $f \circ [g_1]$.

Composition

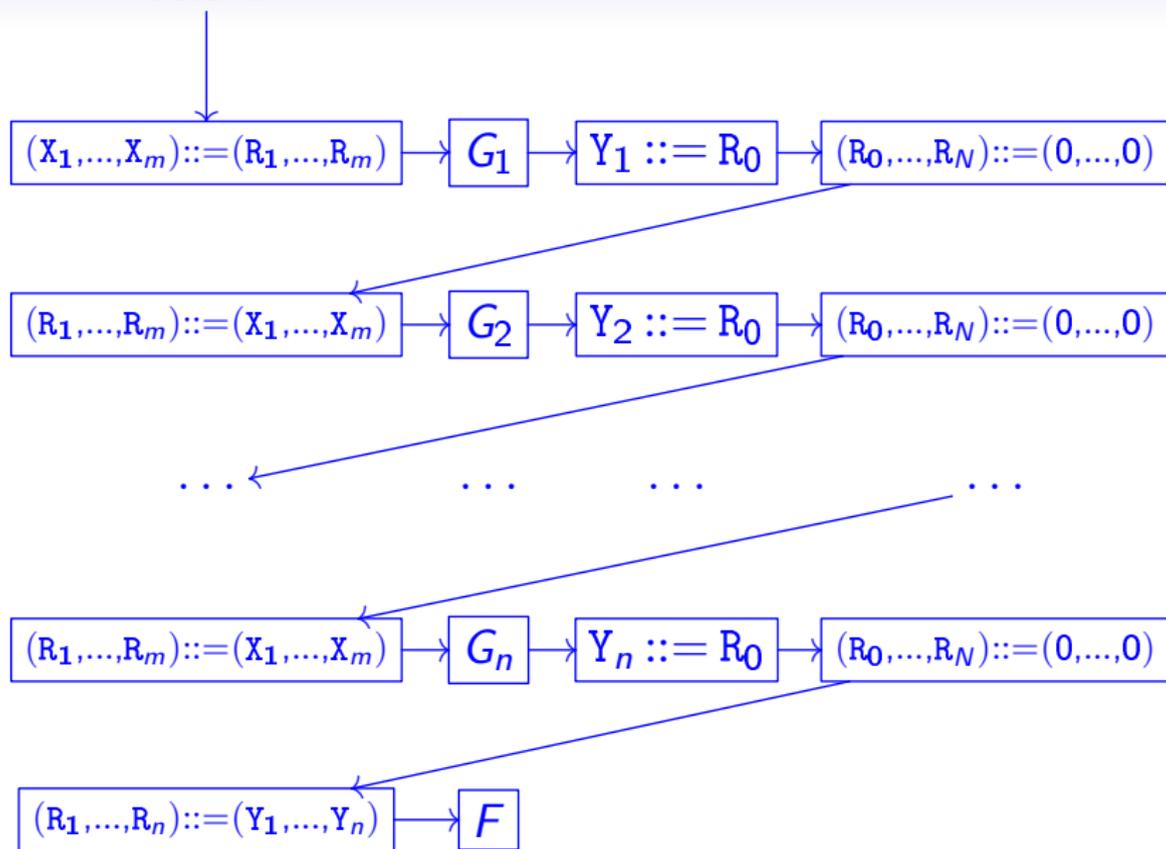
$f \circ [g_1, \dots, g_n]$ is computable if f and g_1, \dots, g_n are.

Proof. Given RM programs $\begin{cases} F \\ G_i \end{cases}$ computing $\begin{cases} f(y_1, \dots, y_n) \\ g_i(x_1, \dots, x_m) \end{cases}$ in R_0

starting with $\begin{cases} R_1, \dots, R_n \\ R_1, \dots, R_m \end{cases}$ set to $\begin{cases} y_1, \dots, y_n \\ x_1, \dots, x_m \end{cases}$, then the next slide specifies a RM program computing $f \circ [g_1, \dots, g_n](x_1, \dots, x_m)$ in R_0 starting with R_1, \dots, R_m set to x_1, \dots, x_m .

(**Hygiene** [caused by the lack of *local names* for registers in the RM model of computation]: we assume the programs F, G_1, \dots, G_n only mention registers up to R_N (where $N \geq \max\{n, m\}$) and that $X_1, \dots, X_m, Y_1, \dots, Y_n$ are some registers R_i with $i > N$.)

START



Examples of recursive definitions

$$\begin{cases} f_1(0) & \equiv 0 \\ f_1(x+1) & \equiv f_1(x) + (x+1) \end{cases}$$

$f_1(x) =$ sum of
 $0, 1, 2, \dots, x$

Examples of recursive definitions

$$\begin{cases} f_1(0) & \equiv 0 \\ f_1(x+1) & \equiv f_1(x) + (x+1) \end{cases}$$

$f_1(x)$ = sum of
 $0, 1, 2, \dots, x$

$$\begin{cases} f_2(0) & \equiv 0 \\ f_2(1) & \equiv 1 \\ f_2(x+2) & \equiv f_2(x) + f_2(x+1) \end{cases}$$

$f_2(x)$ = x th Fibonacci
number

Examples of recursive definitions

$$\begin{cases} f_1(0) & \equiv 0 \\ f_1(x+1) & \equiv f_1(x) + (x+1) \end{cases}$$

$f_1(x)$ = sum of
 $0, 1, 2, \dots, x$

$$\begin{cases} f_2(0) & \equiv 0 \\ f_2(1) & \equiv 1 \\ f_2(x+2) & \equiv f_2(x) + f_2(x+1) \end{cases}$$

$f_2(x)$ = x th Fibonacci
number

$$\begin{cases} f_3(0) & \equiv 0 \\ f_3(x+1) & \equiv f_3(x+2) + 1 \end{cases}$$

$f_3(x)$ undefined except
when $x = 0$

Examples of recursive definitions

$$\begin{cases} f_1(0) & \equiv 0 \\ f_1(x+1) & \equiv f_1(x) + (x+1) \end{cases}$$

$f_1(x)$ = sum of
 $0, 1, 2, \dots, x$

$$\begin{cases} f_2(0) & \equiv 0 \\ f_2(1) & \equiv 1 \\ f_2(x+2) & \equiv f_2(x) + f_2(x+1) \end{cases}$$

$f_2(x)$ = x th Fibonacci
number

$$\begin{cases} f_3(0) & \equiv 0 \\ f_3(x+1) & \equiv f_3(x+2) + 1 \end{cases}$$

$f_3(x)$ undefined except
when $x = 0$

$$f_4(x) \equiv \text{if } x > 100 \text{ then } x - 10 \\ \text{else } f_4(f_4(x + 11))$$

f_4 is McCarthy's "91
function", which maps
 x to 91 if $x \leq 100$ and
to $x - 10$ otherwise

Primitive recursion

Theorem. Given $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ and $g \in \mathbb{N}^{n+2} \rightarrow \mathbb{N}$, there is a unique $h \in \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ satisfying

$$\begin{cases} h(\vec{x}, 0) & \equiv f(\vec{x}) \\ h(\vec{x}, x + 1) & \equiv g(\vec{x}, x, h(\vec{x}, x)) \end{cases}$$

for all $\vec{x} \in \mathbb{N}^n$ and $x \in \mathbb{N}$.

We write $\rho^n(f, g)$ for h and call it the partial function **defined by primitive recursion** from f and g .

Primitive recursion

Theorem. Given $f \in \mathbb{N}^n \rightarrow \mathbb{N}$ and $g \in \mathbb{N}^{n+2} \rightarrow \mathbb{N}$, there is a unique $h \in \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ satisfying

$$(*) \begin{cases} h(\vec{x}, 0) & \equiv f(\vec{x}) \\ h(\vec{x}, x+1) & \equiv g(\vec{x}, x, h(\vec{x}, x)) \end{cases}$$

for all $\vec{x} \in \mathbb{N}^n$ and $x \in \mathbb{N}$.

Proof (sketch). *Existence:* the set

$$h \triangleq \{(\vec{x}, x, y) \in \mathbb{N}^{n+2} \mid \exists y_0, y_1, \dots, y_x \\ f(\vec{x}) = y_0 \wedge (\bigwedge_{i=0}^{x-1} g(\vec{x}, i, y_i) = y_{i+1}) \wedge y_x = y\}$$

defines a partial function satisfying (*).

Uniqueness: if h and h' both satisfy (*), then one can prove by induction on x that $\forall \vec{x} (h(\vec{x}, x) \equiv h'(\vec{x}, x))$.

Example: addition

Addition $add \in \mathbb{N}^2 \rightarrow \mathbb{N}$ satisfies:

$$\begin{cases} add(x_1, 0) & \equiv x_1 \\ add(x_1, x + 1) & \equiv add(x_1, x) + 1 \end{cases}$$

So $add = \rho^1(f, g)$ where $\begin{cases} f(x_1) & \triangleq x_1 \\ g(x_1, x_2, x_3) & \triangleq x_3 + 1 \end{cases}$

Note that $f = \text{proj}_1^1$ and $g = \text{succ} \circ \text{proj}_3^3$; so add can be built up from basic functions using composition and primitive recursion:
 $add = \rho^1(\text{proj}_1^1, \text{succ} \circ \text{proj}_3^3)$.