

The halting problem

The halting problem is an example of a problem that cannot be solved by any procedure.

Problem: determine whether there is a procedure that takes as an input a pair (P, I) , where P is a program and I is an input of P , and outputs whether P will eventually stop when run with this input.

Solution: we will show that no such procedure exists. Suppose for contradiction that it does.

Let us call it H .

Let P be a program and I be an input of P .

We have

Output of $H(P, I) = \begin{cases} \text{"halt"}, & \text{if } P \text{ stops with input } I \\ \text{"loops forever"}, & \text{otherwise.} \end{cases}$

A program can have itself as an input.

If this does not "make sense", the algorithm will output an error. H will determine if this error is obtained in a finite amount of time or if it loops forever.

Let K be the procedure defined as follows:

$K(P)$ will $\begin{cases} \text{"halt"} & \text{if output of } H(P, P) \text{ is "loops forever"} \end{cases}$

$K(K)$ will "loops forever" otherwise.

Let us provide K as input to K .

If $H(K, K)$ loops forever, then $K(K)$ halts
(by definition of K).

If $H(K, K)$ halts, then $K(K)$ loops forever
(by definition of K).

But $H(K, K)$ and $K(K)$ must have the same answers. This is a contradiction.

The growth of functions

In order to compare how long it takes for some algorithms to perform a given task, we introduce the big- O notation.

Definition: Let $f: A \rightarrow \mathbb{R}$ and $g: A \rightarrow \mathbb{R}$ be functions, where $A = \mathbb{Z}$ or $A = \mathbb{R}$.

We write $f(x) = O(g(x))$ if there are constants C and K such that

$$|f(x)| \leq C |g(x)|.$$

whenever $x \geq K$.

(read: $f(x)$ is big-oh of $g(x)$).

Meaning: f grows slower than some fixed multiple of g as x grows.

Obs: There might be many values of C and K which witness the big-oh.

Example: Let $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2 + 2x + 1$.
Show that $f(x) = O(x^2)$.

Lemma: Let $f, g, h: \mathbb{R} \rightarrow \mathbb{R}$ be functions such that $f(x) = O(g(x))$ and $g(x) = O(h(x))$.
Then, $f(x) = O(h(x))$.

Proof: $f(x) = O(g(x)) \Rightarrow \exists K_1, C_1$ such that

$$\textcircled{1} \quad |f(x)| \leq C_1 |g(x)| \quad \forall x \geq K_1$$

In the same way, $g(x) = O(h(x)) \Rightarrow \exists K_2, C_2$ such that

$$\textcircled{2} \quad |g(x)| \leq C_2 |h(x)| \quad \forall x \geq K_2$$

From $\textcircled{1}$ and $\textcircled{2}$ we obtain that

$$|f(x)| \leq C_1 |g(x)| \leq C_1 \cdot C_2 |h(x)|$$

for every $x \geq \max\{K_1, K_2\}$.

Therefore, $C_1 \cdot C_2$ and $\max\{K_1, K_2\}$ are our constants which witness that $f(x) = O(h(x))$.

Definition: Let $f, g: A \rightarrow \mathbb{R}$ be functions, where $A = \mathbb{Z}$ or $A = \mathbb{R}$. We say that f and g have the same order if $f(x) = O(g(x))$ and $g(x) = O(f(x))$.

Lemma: If $f, g: A \rightarrow \mathbb{R}$ have the same order, then there exists C and K such that

$$|f(x)| \leq C |g(x)| \text{ and } |g(x)| \leq C |f(x)|$$

for every $x \geq K$.

Proof: $f(x) = O(g(x)) \Rightarrow \exists k_1, C_1$ such that

$$\textcircled{1} \quad |f(x)| \leq C_1 |g(x)| \quad \forall x \geq k_1$$

In the same way, $g(x) = O(f(x)) \Rightarrow \exists k_2, C_2$ such that

$$\textcircled{2} \quad |g(x)| \leq C_2 |f(x)| \quad \forall x \geq k_2$$

Take $C = \max\{C_1, C_2\}$ and $K = \max\{k_1, k_2\}$.

From $\textcircled{1}$ and $\textcircled{2}$ we obtain that

$$|f(x)| \leq C |g(x)| \text{ and } |g(x)| \leq C |f(x)|$$

for every $x \geq K$.

Notation: We denote by $f(x) = \Theta(g(x))$ when f and g have the same order.

Definition : Let $f, g: A \rightarrow \mathbb{R}$ be functions, where $A = \mathbb{R}$ or \mathbb{Z} . We write $f(x) = \Omega(g(x))$ if there exists positive constants C and K such that

$$|f(x)| \geq C |g(x)|$$

whenever $x > K$.

Observation : $f(x) = \Omega(g(x))$ if and only if $g(x) = \mathcal{O}(f(x))$.