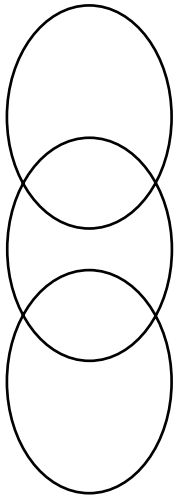
Lesson 5:

Methods of Proof

- Mathematical Reasoning
- Methods of Proofs
  - Direct / Indirect Proofs
  - Vacuous / Trivial Proofs
  - Proof by Contradiction
  - Proof by Cases
- The Halting Problem



Chapter 1.5

Mathematical Reasoning

Mathematical Reasoning

- The basis of all mathematical reasoning is the Argument (ארגומנט) or Proof (הוכחה).
- Used to validate mathematical hypothesis and assumptions.
- Used in CS :
  - Validate Programs
  - Ensure security of Operating Systems
  - Inference and learning in AI

We shall learn:
Principles of correct proofs. When is a proof in/correct.

Mathematical Reasoning

Definitions:

Theorem (משפט) - a statement that can be shown to be true.

Proof (הוכחה) or *Argument* (ארגומנט) - a series of statements that demonstrate that a theorem is true.

This series includes:

- *Axioms* (אקסיומות) - assumptions on the world
- Hypotheses of the theorem to be proved
- previously proven theorems.

Rules of inference (חוקי הסק) - laws that allow deduction of new conclusions from previous arguments.

Lemma (למה) - a (simple) theorem used in the proof of a more complex theorem.

Corollary (מסקנה) - statement or proposition that is deduced directly from a theorem.

Proofs

We want to prove statements of the following form:

"If p then q".

That is we want to prove $p \rightarrow q$ or that $p \rightarrow q \Leftrightarrow \mathbf{T}$

Remember: that $p \rightarrow q$ is always true except when p is true and q is false

Note: it is enough to prove that under the assumption of p is true, we have that q is true.

Direct Proof (הוכחה ישירה)

Direct Proof (הוכחה ישירה)

Prove $p \rightarrow q$ directly by assuming p and proving q using axioms, inference and previously proven theorems.

Direct Proof (הוכחה ישירה)

Example:

Definition: n is even iff there exists an integer k $\in \mathbb{Z}$ such that n = 2*k.

Theorem: If $\overbrace{\text{n is even}}^{p}$ then $\overbrace{n^2 \text{ is even}}^{q}$.

Proof: Assume n is even (assume p $\Leftrightarrow$ **T**),

then there exists an integer k $\in \mathbb{Z}$ such that n=2*k.

Then $n^2 = (2*k)^2 = 4*k^2 = 2*(2*k^2)$.

Since k $\in \mathbb{Z}$ then $2*k^2 \in \mathbb{Z}$

Thus n^2 equals 2 times an integer and by definition is even.

We have proven the conclusion is true (q $\Leftrightarrow$ **T**).

Indirect Proof (הוכחה בשלילה)

Indirect Proof (הוכחה בשלילה)

Since $p \to q \Leftrightarrow \neg q \to \neg p$ (contrapositive),

prove $p \to q$ by proving $\neg q \to \neg p$:

assume $\neg q$ and prove $\neg p$ using axioms, inference and previously proven theorems.

Indirect Proof (הוכחה בשלילה)

Example:

Theorem: If $\overbrace{3*n+2 \text{ is odd}}^{p}$ then $\overbrace{n \text{ is odd}}^{q}$.

Proof: Assume the conclusion is false ($\neg q \Leftrightarrow$ **F**)

i.e. assume that n is even.

Then there exists an integer $k \in \mathbb{Z}$ such that n=2*k.

However, then 3*n+2 = (3*(2*k)+2) = 6*k+2 = 2*(3*k+1).

Since $k \in \mathbb{Z}$ then $3*k+1 \in \mathbb{Z}$

Thus 3*n+2 equals 2 times an integer and by definition is even. We have proven that the premise is False ($\neg p \Leftrightarrow$ **F**) and $\neg q \rightarrow \neg p \Leftrightarrow p \rightarrow q \Leftrightarrow$ **T.**

Vacuous Proof (הוכחה ריקה)

Vacuous Proof (הוכחה ריקה)

If $p \Leftrightarrow \mathbf{F}$ then $p \rightarrow q \Leftrightarrow \mathbf{T}$ (regardless of value of q).

Prove $p \rightarrow q$ by proving $p \Leftrightarrow \mathbf{F}$ always.

Example:

Theorem: For natural numbers if n<0 then 2*n is even.

Proof: For all natural numbers $n<0 \Leftrightarrow \mathbf{F}$

Thus premise is always **F**alse regardless of the conclusion and theorem is proven.

Trivial Proof (הוכחה טריביאלית)

Trivial Proof (הוכחה טריביאלית)

If $q \Leftrightarrow \mathbf{T}$ then $p \rightarrow q \Leftrightarrow \mathbf{T}$ (regardless of value of p).

Prove $p \rightarrow q$ by proving $p \Leftrightarrow \mathbf{F}$ always.

Example:

Theorem: For integers, if n is prime then 2*n is even.

Proof: For all integers 2*n is even by definition.

Thus conclusion is always **T**rue regardless of the premise value and theorem is proven.

Proof Strategy

Example:

Theorem: For integers, if n^2 is odd then n is odd.

Proof: 1) Try Direct Proof:

If n^2 is odd then there exists $k \in \mathbb{Z}$ such that $n^2 = 2*k + 1$.

Then $n = \sqrt{2*k + 1}$ .....

2) Try Indirect Proof:

Assume n is even, then $n = 2*k$.

Then $n^2 = (2*k)^2 = 4*k^2 = 2*(2*k^2)$.

If $k \in \mathbb{Z}$ then $2*k^2 \in \mathbb{Z}$ and n^2 is even.

Thus theorem is proven.

Proof by Contradiction (הוכחה ע"י סתירה)

We want to prove general statements p
(possibly $p \Leftrightarrow (s \rightarrow t)$ but not necessarily)

Find a Contradiction q ($q \Leftrightarrow \mathbf{F}$) and prove $\neg p \rightarrow q$.
i.e. $\neg p \rightarrow \mathbf{F}$. However this implies $\neg p \Leftrightarrow \mathbf{F}$ and $p \Leftrightarrow \mathbf{T}$.

We assume $\neg p$ and prove a contradiction, indicating that the initial assumption is not true and that $p \Leftrightarrow \mathbf{T}$.

Proof by Contradiction (הוכחה ע"י סתירה)

Example:

Theorem: out of 15 randomly chosen days, at least 3 are the same day of the week.

Proof: Assume by contradiction that no 3 are the same day of the week. Thus at most 2 days are the same day of the week. The week has 7 days thus at most 2*7 = 14 days were randomly chosen.
Contradiction to the fact that 15 days were chosen.
Due to contradiction we deduce that at least 3 days are the same day of the week.

Proof by Contradiction (הוכחה ע"י סתירה)

Example:

Definition: n is *Rational* (מספר רציונלי) if there exist integers a,b with $b \neq 0$ such that $n = a/b$.
If n is not rational it is *Irrational* (אי-רציונלי).

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume by contradiction that $\sqrt{2}$ is rational.

1. $\sqrt{2}$ is rational
2. $\sqrt{2} = a/b$ $a,b \in \mathbb{Z}$ with no common factors (definition of rational)
3. $2 = a^2/b^2$ (arithmetic)
4. $2*b^2 = a^2$ (arithmetic)
5. a^2 is even (definition of even)

Proof by Contradiction (הוכחה ע"י סתירה)

Proof cont.:

5. a^2 is even (definition of even)
6. a is even (Theorem: if n^2 is even then n is even)
7. $a = 2*k \quad k \in \mathbb{Z}$ (definition of even)
8. $a^2 = 4* k^2$ (arithmetic)
9. $2*b^2 = 4* k^2$ (from 4. and 8.)
10. $b^2 = 2*k^2$ (arithmetic)
11. b^2 is even (definition of even)
12. b is even (Theorem: if n^2 is even then n is even)
13. 2|a and 2|b (from 6. and 12.) **Contradicts 2.**
14. 2. and 13. $\Leftrightarrow$ **F**

Thus we showed "$\sqrt{2}$ is rational" $\rightarrow$ **F** so "$\sqrt{2}$ is rational" $\Leftrightarrow$ **F** and we have "$\sqrt{2}$ is irrational" .

Indirect Proof vs Proof by Contradiction
(והוכחה בסתירה והוכחה בשלילה)

For theorems of the form $p \rightarrow q$, Indirect Proof and Proof by Contradiction is the same.

Indirect proof

assume $\neg q$
prove $\neg p$
deduce $\neg q \rightarrow \neg p$
equal to $p \rightarrow q$

Proof by Contradiction

assume $\neg(p \rightarrow q)$
i.e. assume p
assume $\neg q$
prove $\neg p$
deduce $\neg p \wedge p \Leftrightarrow F$
deduce $\neg(p \rightarrow q) \rightarrow F$
deduce $(p \rightarrow q) \Leftrightarrow T$

Generalizing Proofs

Theorem of the form $p \wedge q$, prove p and q separately.

Example:

Theorem: if n is divisible by 6 (6|n) then n is divisible by 2 (2|n) and n is divisible by 3 (3|n).

$$6|n \rightarrow (2|n \wedge 3|n)$$

Proof: $6|n \rightarrow (2|n \wedge 3|n) \Leftrightarrow$

$(6|n \rightarrow 2|n) \wedge (6|n \rightarrow 3|n)$ (distributive)

prove $(6|n \rightarrow 2|n)$

prove $(6|n \rightarrow 3|n)$

Generalizing Proofs

Theorem of the form $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$

$\Leftrightarrow (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$

Prove every $(p_i \rightarrow q)$ separately

Example:

Theorem: if n is divisible by 6 (6|n) or n is divisible by 8 (8|n) then n is divisible by 2 (2|n).

$(6|n \vee 8|n) \rightarrow 2|n$

Proof: prove $(6|n \rightarrow 2|n)$

prove $(8|n \rightarrow 2|n)$

Proof By Cases (הוכחה בחלקים)

To prove a theorem of the form $p \rightarrow q$, replace it with $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$ where $p \Leftrightarrow (p_1 \vee p_2 \vee \ldots \vee p_n)$ and prove each $p_i \rightarrow q$ separately.

Example:

Theorem: if $\overbrace{n \in \mathbb{Z} \text{ is not divisible by } 3}^{p}$ then $\overbrace{n^2 \equiv 1 \pmod 3}^{q}$.

Proof: $p \Leftrightarrow p_1 \vee p_2$ where p_1 = "$n \equiv 1 \pmod 3$"

p_2 = "$n \equiv 2 \pmod 3$"

Case 1: prove $p_1 \rightarrow q$

Case 2: prove $p_2 \rightarrow q$

Proof By Cases (הוכחה בחלקים)

Proof cont.:

Case 1: prove $p_1 \rightarrow q$ (“$n \equiv 1 \pmod 3$” $\rightarrow$ “$n^2 \equiv 1 \pmod 3$”)

(Direct Proof) assume “$n \equiv 1 \pmod 3$”

$n = 3*k + 1 \quad k \in \mathbb{Z}$ (definition of mod)

$n^2 = (3*k+1)^2 =$

$= 9k^2 + 6k + 1$

$= 3*(3k^2 + 2k) + 1$ (math)

$\underbrace{\qquad}_{\in \mathbb{Z}}$

$n^2 \equiv 1 \pmod 3$” (definition of mod)

Proof By Cases (הוכחה בחלקים)

Proof cont.:

Case 2: prove $p_2 \rightarrow q$ (“$n \equiv 2 \pmod 3$” $\rightarrow$ “$n^2 \equiv 1 \pmod 3$”)

(Direct Proof) assume “$n \equiv 2 \pmod 3$”

$n = 3*k + 2 \quad k \in \mathbb{Z}$ (definition of mod)

$n^2 = (3*k+2)^2 =$

$= 9k^2 + 12k + 4$

$= 3*(3k^2 + 4k + 1) + 1$ (math)

$\in \mathbb{Z}$

$n^2 \equiv 1 \pmod 3$” (definition of mod)

Generalizing Proofs

Theorem of the form $p \leftrightarrow q$

$\Leftrightarrow \ (p \rightarrow q) \wedge (q \rightarrow p)$

Prove every $(p \rightarrow q)$ and $(q \rightarrow p)$ separately.

Example:

Theorem: n is odd **iff** n^2 is odd.

Proof: 1. prove (n is odd $\rightarrow$ n^2 is odd)

2. prove (n^2 is odd $\rightarrow$ n is odd)

1. (Direct proof) assume n is odd

n = 2*k + 1 (definition of odd)

$n^2 = 4*k^2 + 4*k + 1$

$= 2*(2k^2 + 2k) + 1$ } (math)

n^2 is odd (definition of odd)

Generalizing Proofs

Proof cont.:

2. prove (n2 is odd $\rightarrow$ n is odd)

(Indirect proof) assume $\neg$(n is odd) i.e. n is even

n = 2*k (definition of even)

$n^2 = 4*k^2$

$= 2*(2k^2)$ } (math)

n^2 is even (definition of even)

From 1. and 2. we have (n is odd $\leftrightarrow$ n^2 is odd)

Generalizing Proofs

Theorem of the form show that $p_1, p_2, \ldots, p_n$ are equivalent

use tautology:

$(p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n) \Leftrightarrow (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)$

and prove every $(p_i \rightarrow p_{i+1})$ separately.

Example:

Theorem: Show that the following statements are equivalent:

p1 = "n is an even integer"

p2 = "n+1 is an odd integer"

p3 = "n^2 is an even integer"

Proof: 1. prove (n is even $\rightarrow$ n+1 is odd)

2. prove (n+1 is odd $\rightarrow$ n^2 is even)

3. prove (n^2 is even $\rightarrow$ n is even)

Proofs of Theorems with Quantifiers

Prove theorems of the form $\exists x\, P(x)$ or $\forall x\, P(x)$

Existence Proofs

- Constructive
- Non-constructive
- Uniqueness

Counterexamples

Existence Proofs (הוכחת קיום)

Prove theorems of the form $\exists x\, P(x)$.

Method 1: *Constructive Proofs* (הוכחת קיום ע"י בניה)

Find a singled example a of assignment to x for which P(a) is True.

Example:

Theorem: There exists a prime number greater than 10.

$\exists x\, P(x) = \exists x\, (x>10 \wedge$ "x is prime")

Proof: We show that P(11) = **T**.

11>10 and 11 is prime: $2 \nmid 11$ ... $10 \nmid 11$

Existence Proofs (הוכחת קיום)

Example:

Theorem: For every number n there exists a number greater than n with the same parity.

Proof: We show that the specific case of n+2 has the same parity as n.

Case 1: n is even

n = 2*k (definition of even)

n+2 = 2*k + 2 = 2 * (k+1) (math)

n +2 is even (definition of even)

Case 2: n is odd

n = 2*k +1 (definition of odd)

n+2 = 2*k + 3 = 2 * (k+1) +1 (math)

n +2 is odd (definition of odd)

Existence Proofs (הוכחת קיום)

Prove theorems of the form $\exists x\, P(x)$.

Method 2: *Nonconstructive Proofs* (הוכחת קיום שלא ע"י בניה)

Without finding a specific, prove that there must be such a case P(x). e.g. directly or prove by contradiction.

Example: The example requires the following Lemma.

Lemma: Every natural number has at least 1 prime factor.

Proof: n is a natural number then either n can be factored into prime factors, or it is prime and then n | n and n is its own prime factor.

Existence Proofs (הוכחת קיום)

Example:

Theorem: For every natural n there exists a prime greater than n.

Proof: Assume n is natural. Consider (n! + 1).

n!+1 = (1*2*...*n) + 1 by the Lemma it has a prime factor.

However for all m<=n $m \nmid (n!+1)$ since m | n! and

$1 \equiv n!+1 \pmod{m}$.

Thus the prime factor of (n!+1) must be greater than n.

And so there exists a prime greater than n.

Uniqueness Proofs (הוכחת קיום יחיד)

Prove theorems of the form:

" there exists a unique x such that P(x)" .

Prove existence and then prove uniqueness;

$\exists x\, P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y))$

Example:

Theorem: Every integer has a unique additive inverse.

Proof: x is an integer. we prove $\exists y\ x+y = 0$.

(by construction) Set y = -x and then x + y = 0.

Uniqueness: Assume by contradiction that there exists integer $z \neq y$ s.t. $x+z = 0$.

Then x+z = x+y and subtracting x from both sides we get z=y contradiction.

Counterexample Proofs (שלילה ע"י דוגמא נגדית)

Proving theorems of the form $\forall x\, P(x)$ may be difficult.

Proving the falsity of $\forall x\, P(x)$ is easier:
provide counter example a such that $\neg P(a) \Leftrightarrow \mathbf{F}$

$$\forall x\, P(x) = \exists x \neg P(x)$$

Example:

Theorem: Every prime number is odd.

Proof: 2 is prime and yet 2 | 2 so that it is even.

2 is a counter example.

Counterexample Proofs (שלילה ע"י דוגמא נגדית)

Proving theorems of the form $\forall x\, P(x)$ may be difficult. It is not enough to test a few/many cases. All cases must be tested.

Example:

Is $n^2 - n + 41$ prime for every positive integer n?

Answer: True for n = 0,1,2 ...

What about n = 41?

Computer Proofs?

Christian Goldbach (1690-1764)

Goldbach's Conjecture (השארת גולדבאך) -
Every even integer greater than 2 is the sum of 2 primes.

Shown to be true:
Up to millions by hand (4 = 2+2, 6 = 3+ 3,...)
With computers proven to be true for all positive integers up to $4*10^{14}$!!

Not proven till this day!

p. 220-223

Fermat's Conjecture

Pierre de Fermat (1601-1665)

Fermat's Conjecture (השארת פרמה\ המשפט האחרון של פרמה) -
There are no positive integers x,y,z such that

$$x^n + y^n = z^n$$

for n > 2.

Fermat's Theorem - Milestones

1630 - Fermat's Theorem presented the theorem

1630 - Fermat - proven for n =4

1700 - Euler prooved for n=3

1825 - Germain, Dirichlet & Legendre proved for n=5

1832 - Dirichlet proved for n=14 (failed atempt at n=7)

1839 - Lamé proved for n=7

1847 - Lamé, Louville & Kummer proved for all primes n up to 37

1847 - Lamé, Louville & Kummer proved for al prime up to 100 except 37, 59, 67

1908 - 1912 - over 1000 false proofs published!!

Fermat's Theorem - Milestones

1937 - The calculating machines and computers come into play:

1937 - Using computers proven up to n = 617

1955 - Using computers proven up to n = 4001

1976 - Using computers proven up to n = 125,000

1993 - Using computers & based on Kummer's theory proven up to n=4,000,000

1955 - Taniyama et.al. Develop Theory of Elliptic Curves

1986 - Frey connected between Eliptic Curves & Fermat's Theorem

Beginning of the end:

1993 - Andrew Wiles concluded a talk with a corollary: "...and this proves

$x^n + y^n = z^n$ and here I'll stop!"

1993 - Wiles withdraws his proof due to an error found.

1994 - Wiles corrects the proof and completes the proof of Fermat's Theorem.

1995 - Paper with proof published = a book of hundreds of pages.

The Halting Problem

The Halting Problem (בעית העצירה) -

Is there a procedure/program that receives as input:

1) a computer program 2) input to the computer program

and determines whether the computer program will eventually stop when run with the input ?

This is not trivial: one can not simply run the program since if it does not stop in a given time is not proved that wont stop in the future.

The Halting Problem

1936 - Alan Turing proved that such a program does not exist.

Alan Mathison Turing (1912 - 1954)

Turing Machine

Turing Test

Turing Prize

The Enigma Code

The Halting Problem - Proof

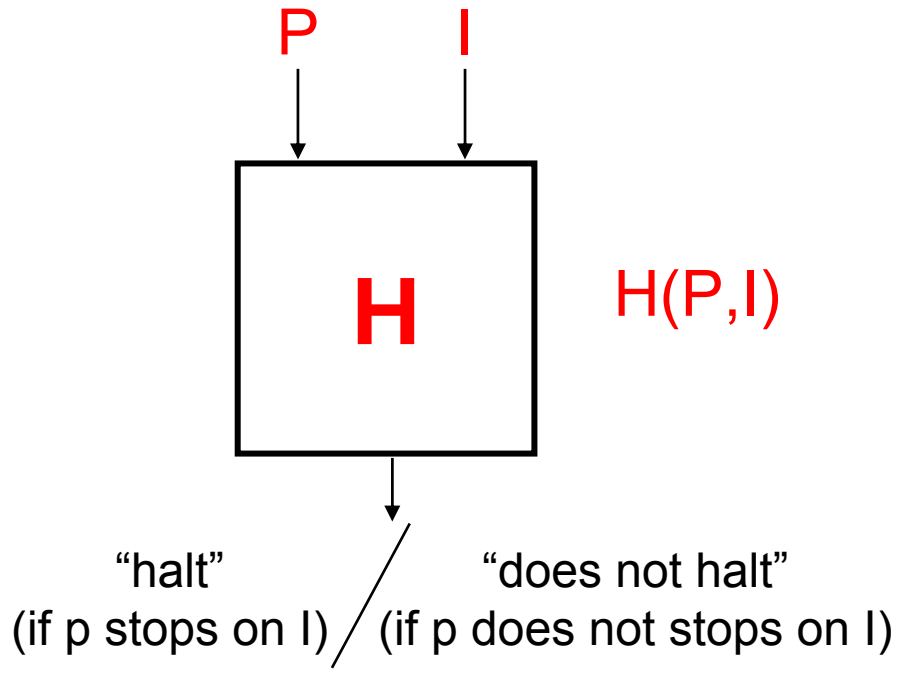
Proof of Non-existence: (proof by contradiction)

Assume that there exists a program H that receives as input:

1) a program P 2) input I

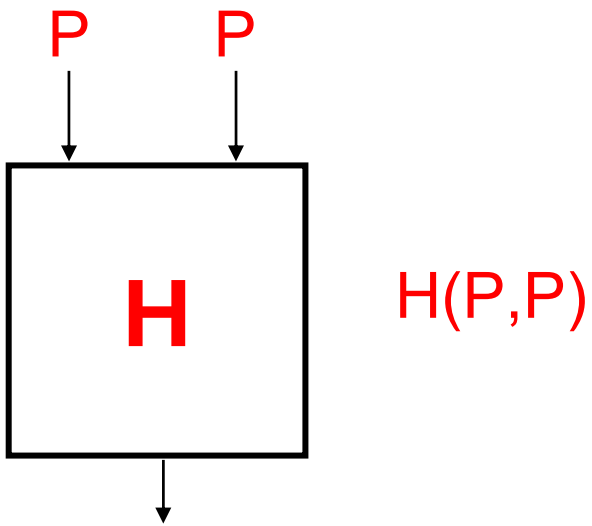
and returns "halt" if P stops when given I

and returns "does not halt" if P does not stop on input I.



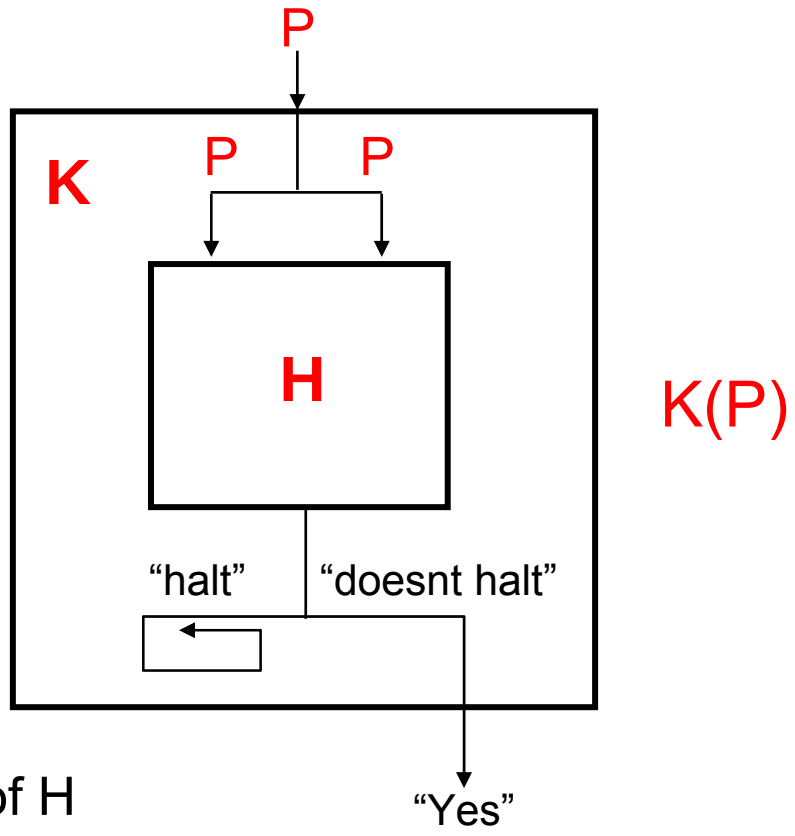
The Halting Problem - Proof

Since P is a program (= a series of letters = a series of bits) it can also serve as an input.
Thus running H(P,P) is valid:



The Halting Problem - Proof

Build a program/procedure K as follows:
K receives as input the program P and runs H(P,P).
If H(P,P) returns "halt" then K(P) goes into infinite loop.
If H(P,P) returns "does not halt" then K(P) returns "yes".

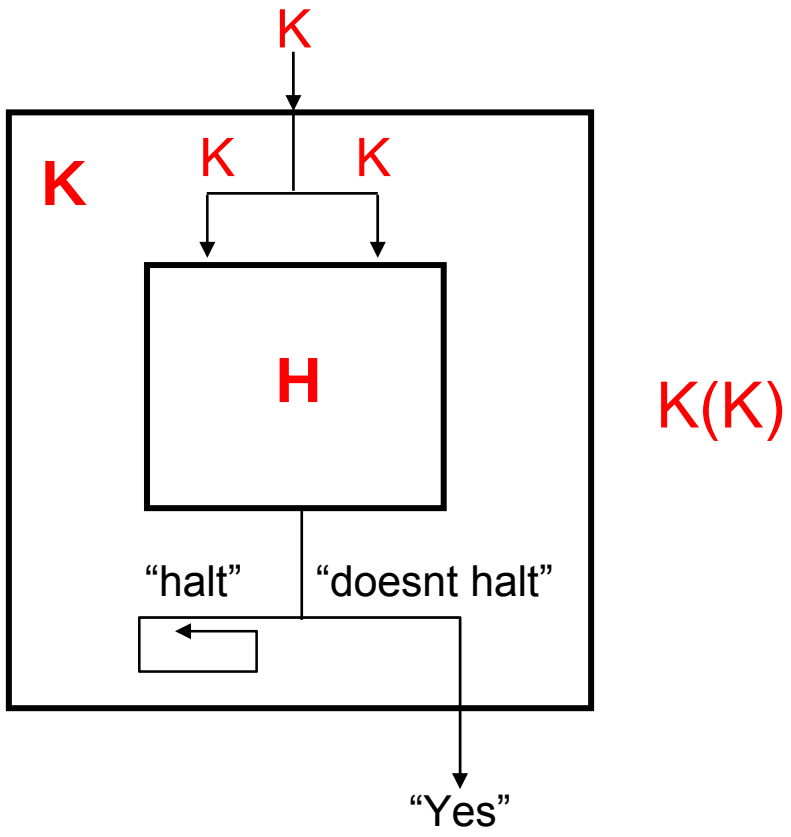


K(P)

* K does the opposite of H

The Halting Problem - Proof

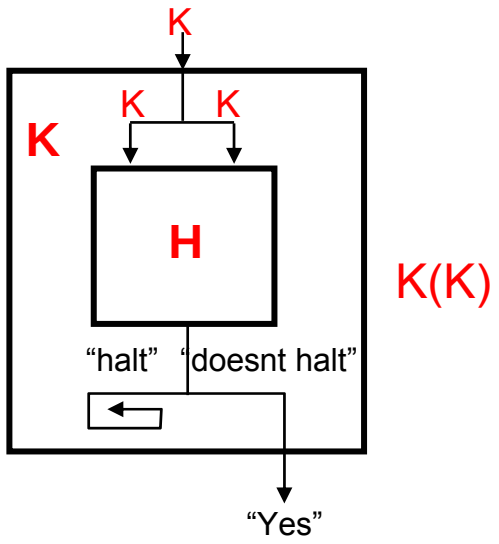
Since K is a program (= a series of letters = a series of bits) it can also serve as an input.
Thus running K(K) is valid:



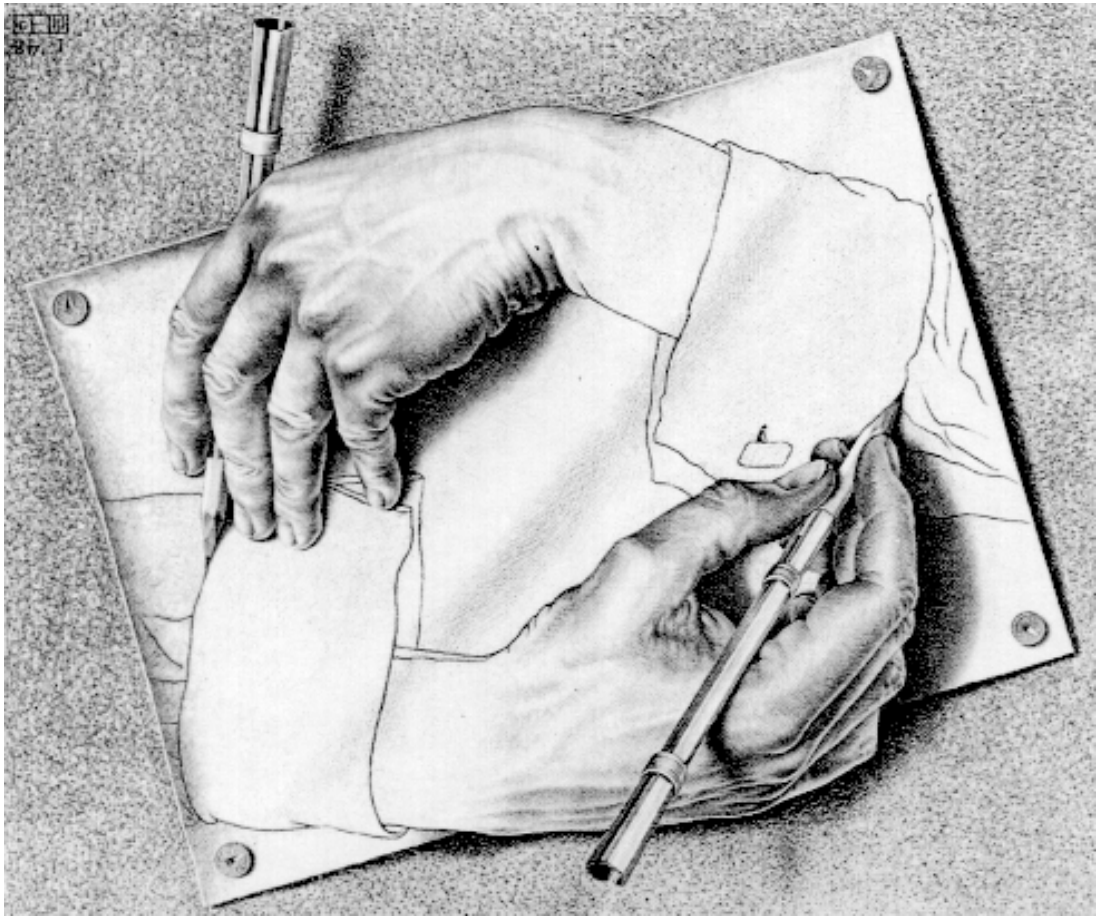
K(K)

The Halting Problem - Proof

1) If H(K,K) outputs “halt” then K(K) goes into infinite loop and does not stop BUT H(K,K) outputs that K(K) does stop - **contradiction**!
2) If H(K,K) outputs “does not halt” then K(K) stops and outputs “yes” BUT H(K,K) outputs that K(K) does not stop - **contradiction**!



Thus the assumption that procedure H exists is incorrect.



"Drawing Hands" - 1948
MC Escher