Discrete Mathematics:

Lecture 4. Proof

proofs

- a proof is a valid argument that establishes the truth of a mathematical statement
- an axiom is a statement we assume to be true without proof

  ex) when x and y are real number, x + y is a real number
- a theorem is a statement that has been proven to be true (using axiom)

  ex) Pythagorean theorem
- a lemma is a small theorem, which can be used to prove theorem
- a corollary is a theorem that can be established directly from a theorem
- a conjecture is a statement whose truth value has not been proven

proofs

- direct proofs
- proof by contraposition
- vacuous proofs
- trivial proofs
- proof by contradiction
- proof by cases
- existence proofs

direct proof

for direct proof of a conditional statement $p \longrightarrow q$,

- assume that p is true in the first step.
- use rules of inference in the subsequent steps.
- show q must be true

theorem: " If n is an odd integer, then n^2 is odd"

proof: by the definition of an odd integer, $n = 2k + 1$, where k is some integer

$n^2 = (2k+1)^2 = 4k^2 + 4k +1 = 2(2k^2 + 2k) + 1$

we can conclude that n^2 is an odd integer by the definition of odd integer.

proof by contraposition

show $\neg q \longrightarrow \neg p$ to prove $p \longrightarrow q$

theorem: if n is an integer and 3n+2 is odd, then n is odd

proof: if n is even, 3n+2 is even

when $n = 2k$, $3n+2 = 3(2k)+2 = 2(3k+1)$

p	q	$p \longrightarrow q$	$\neg p$	$\neg q$	$\neg q \longrightarrow$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

vacuous proofs

$\boxed{\text{show p is false to prove } p \longrightarrow q}$

Show that the proposition P(0) is true, where P(n) is “If $n>1$, then $n^2 > n$” and the domain consists of all integers.

P(0): if $0 > 1$, then $0^2 > 0$

since premise $0>1$ is false, P(0) is true

trivial proofs

$\boxed{\text{show } q \text{ is true to prove } p \longrightarrow q}$

Let P(n) be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that P(0) is true

P(0): if $a \geq b$ $(a > 0, b > 0)$, then $a^0 \geq b^0$

Because $a^0 = b^0 = 1$, the conclusion is true

Thus, P(0) is true

proof by contradiction

to prove a statement p is true, show that $\neg p \longrightarrow (q \wedge \neg q)$ is true

prove that $\sqrt{2}$ is irrational by giving a proof by contradiction

p: $\sqrt{2}$ is irrational
$\neg$ p: $\sqrt{2}$ is rational
Let's show that assuming $\neg$ p is true leads to a contradiction

- if $\sqrt{2}$ is rational, $\sqrt{2} = a/b$, where a and b are integers, $b \neq 0$, and a and b have no common factors.
- if both sides of the equation are squared, $2 = a^2/b^2$, which can be $2b^2 = a^2$
- because a is an even number, $a=2c$ for some integer c
- since $2b^2 = 4c^2$, $b^2 = 2c^2$
- since both a and b are even numbers, they have a common factor, which lead to the contradiction
- thus, $\sqrt{2}$ is irrational

proof by cases

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \longrightarrow q] \longleftrightarrow [(p_1 \longrightarrow q) \wedge (p_2 \longrightarrow q) \wedge \ldots \wedge (p_n \longrightarrow q)]$$

prove that if n is an integer, then, $n^2 \geq n$

- case1: when $n = 0$, $0 \geq 0$, which is true
- case2: when $n \geq 1$, $n \cdot n \geq n \cdot 1$ by multiplying $n > 0$, which is true
- case3: when $n \leq -1$, $n^2 \geq n$ is true since is $n^2 \geq 0$

existence proofs

constructive existence proofs
    to prove $\exists x\, P(x)$, find a such that $P(a)$ is true

show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways

$1729 = 10^3 + 9^3 = 12^3 + 1^3$

existence proofs

nonconstructive existence proofs

show that the negation of the existential quantification implies a contradiction

show that it is not possible that all the cases are false

show that there exist irrational numbers x and y such that x^y is rational

$x = \sqrt{2}$, $y = \sqrt{2}$, which are irrational

if $x^y = \sqrt{2}^{\sqrt{2}}$ is rational, we have irrational number x, y such that x^y is rational

if $\sqrt{2}^{\sqrt{2}}$ is irrational, $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, which is rational

The Halting problem

- The halting problem was the first mathematical function proven to have no algorithm that computes it! We say, it is uncomputable.

- The function is Halts(P, I) :≡ “Program P, given input I, eventually terminates.”

- Theorem: Halts is uncomputable!

  I.e., There does not exist any algorithm A that computes Halts correctly for all possible inputs.

  Its proof is thus a non-existence proof.

- Corollary: General impossibility of predictive analysis of arbitrary computer programs.

The Halting problem

Proof

- Given any arbitrary program H(P, I),
- Consider algorithm Breaker is defined as:

procedure Breaker (P: a program)

halts := H(P, P)

if halts then while T begin end

- Note that Breaker (Breaker) halts iff H(Breaker , Breaker) = F
- So H does not compute the function Breaker !