CSC165
Mathematical Expression and Reasoning for Computer Science

Module 11

Proof by Contradiction

Proof by Contradiction

- To prove something by contradiction:
  - We assume that what we want to prove is not true
  - We show the consequences of this assumption are not possible
  - That is, the consequences contradict either what we have just assumed, or something we already know to be true
- Proof Process:
  - Assume that the statement is not true (i.e., false)
  - Show that this assumption leads to a contradiction
  - Thereby conclude the original statement is true
- When the assumptions are implicit, try assuming the statement is false, and see whether it leads somewhere, hunting for a contradiction

Proof by Contradiction: Note

- Remember that negating a universal statement leads to an extensional one
  - $\neg(\forall x \in D: A(x)): \exists x \in D: \neg A(x)$
  - $\neg(\forall x \in D: P(x) \rightarrow Q(x)): \exists x \in D: P(x) \wedge \neg Q(x)$
- When you assume the negated form, you have to work with a generic value in the domain (you cannot specify the value of x)
  - Assume $\exists x \in D: \neg A(x)$
  - Let $x_0 \in D$ such that : $A(x_0)$
  - …

Proof Structure

- Prove $\forall x \in D: A(x)$
- Generic Proof:

\# proof by contradiction
Assume $\exists x \in D: \neg A(x)$. # assume statement (to be proven) as false
Let $x_0 \in D$ such that $\neg A(x_0)$. # x_0 is generic
Then $C_1(x_0)$. # find the chain
Then $C_2(x_0)$. # find the chain
$\vdots$
Then $\neg P(x_0)$. # contradiction, since P is known to be true
Then $A(x_0)$. # since assuming $\neg A(x)$ leads to contradiction prove $A(x)$ is true for the generic x

Therefore, $\forall x \in D: A(x)$. # introduce universal quantifier

Example

- Prove no integer can be both even and odd
- Thoughts:
  - To use proof by contradiction, we assume the statement to be false
  - We assume the negation of the statement (to be true)
  - Then we look for a contradiction
  - If we find a contradiction, we declare our assumption is wrong (i.e., the statement is not false)
  - We conclude that the statement is true

Prove: no integer can be both even and odd

- First we assume there exists an integer that can be both even and odd
- Then $\exists z \in \mathbb{Z}$: (z is even) $\wedge$ (z is odd)
- z is even $\leftrightarrow \exists k \in \mathbb{Z}: z = 2k$
- z is odd $\leftrightarrow \exists j \in \mathbb{Z}: z = 2j + 1$
- $z = z \rightarrow 2k = 2j + 1$
- $k - j = \frac{1}{2}$
- The difference of two integers (k and j) must be an integer
- However, $k - j = \frac{1}{2}$ … a fraction!
- Contradiction
- Then, no integer can be both even and odd

 7

Proof: no integer can be both even and odd

\# proof by contradiction

Assume there exists an integer that can be both even and odd. # assuming $\neg A$

Then $\exists z \in \mathbb{Z}$: (z is even) $\wedge$ (z is odd).

Let $z_0 \in \mathbb{Z}$ such that (z_0 is even) $\wedge$ (z_0 is odd).

Then $\exists k \in \mathbb{Z}: z_0 = 2k$.

Let $k_0 \in \mathbb{N}$ such that $z_0 = 2k_0$.

Also $\exists j \in \mathbb{Z}: z_0 = 2j + 1$.

Let $j_0 \in \mathbb{Z}$ such that $z_0 = 2j_0 + 1$.

Since $(k_0 \in \mathbb{Z}) \wedge (j_0 \in \mathbb{Z})$, then $(k_0 - j_0 \in \mathbb{Z})$.

Then $2k_0 = 2j_0 + 1$.

Then $2k_0 - 2j_0 = 1$.

Then $k_0 - j_0 = \frac{1}{2}$.

However, since $(k_0 \in \mathbb{Z}) \wedge (j_0 \in \mathbb{Z}) \wedge (k_0 - j_0 \notin \mathbb{Z})$, then contradiction.

Therefore, no integer can be both even and odd.

 8

Example

- Prove there are infinitely many even natural numbers
- Thoughts:
  - There is an infinite number of even numbers
  - That means there is no largest even number
  - First we assume there is a finite number of even numbers
  - There must be a largest even number, call it m
  - If we multiply m by 2: we get a larger number, a larger even number
  - So m is NOT the largest even number
  - Contradiction!
  - We conclude there are infinitely many even numbers

Proof: there are infinitely many even natural numbers

proof by contradiction

Assume there are a finite number of even numbers. # assuming $\neg A$

Then there exists a largest even number, call it $m > 0$.

Let $m' = 2m$.

Then m' is an even number.

Since m is assumed the largest even number, then $m' < m$.

Since $m' = 2m$, then $m' > m$.

However, since m is assumed the largest even number and $m' > m$, then contradiction.

Therefore, there are infinitely many even numbers. # assuming $\neg A$ leads to contradiction, so A

Example

- Prove there is no smallest positive rational number
- Thoughts:
  - There is no positive rational number that is smallest than all other rational numbers
  - First we assume there is a smallest rational number, call it r
  - $\exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: r = \frac{p}{q}\right]$
  - All other positive rational numbers should be greater than r
  - Now $r/2$ is a positive rational number and smaller than r
  - Contradiction!
  - We conclude there is no smallest positive rational number

Proof: there is no smallest positive rational number

\# proof by contradiction

Assume there is a smallest positive rational number, $r > 0$. # assuming $\neg A$

Then $\exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: r = \frac{p}{q}\right]$.

Let $(p_0 \in \mathbb{Z}) \wedge (q_0 \in \mathbb{Z}^*)$ such that $r = \frac{p_0}{q_0}$.

Then $\forall n \in \mathbb{R}^+: R(n) \rightarrow n \geq r$.   # $R(n)$ means n is rational

Let $q_1 = 2q_0$. Then $q_1 \in \mathbb{Z}^*$.

Let $r' = r/2$.

Since r is assumed the smallest positive rational number, then r' has to be $> r$.

Then $r' = \frac{p_0}{2q_0} = p_0/q_1$.

Then $\exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: r' = \frac{p}{q}\right]$.

Then r' is a rational number.

Then $r' > 0$.

Since, $r' = \frac{r}{2}$, then $r' < r$.

However, since r is assumed to be the smallest positive rational number and $r' < r$, then contradiction.

Therefore, there is no smallest positive rational number. # assuming $\neg A$ leads to contradiction, so A

Examples

Example

- Prove $\sqrt{2}$ is irrational number
- Thoughts:
  - A real number x is rational $\leftrightarrow \exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: x = \frac{p}{q}\right]$
  - Need to prove that $\sqrt{2}$ is irrational (i.e., cannot be written as above)
  - First we assume $\sqrt{2}$ is rational
  - That means we assume $\exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: \sqrt{2} = \frac{p}{q}\right]$
  - Note that it is implicitly assumed that p and q have no common factors (i.e., co-primes)
  - If p and q have common factors, we can divide the common factor out to get co-prime p' and q'.

Prove: $\sqrt{2}$ is irrational

- Assume $\sqrt{2}$ is rational
- $\sqrt{2} = \frac{p}{q}$
- q and p are co-primes
- $\sqrt{2}\, q = p$
- $2q^2 = p^2$
- p^2 is even, then p is even
- $\exists k \in \mathbb{Z}: p = 2k$
- $2q^2 = p^2 = (2k)^2 = 4k^2$
- $q^2 = 2k^2$
- q^2 is even, then q is even
- $\exists l \in \mathbb{Z}: q = 2l$
- Both q and p are even, then both have 2 as a factor
- q and p are not co-primes
- Contradiction
- $\sqrt{2}$ is irrational

Proof: $\sqrt{2}$ is irrational

proof by contradiction

Assume $\sqrt{2}$ is rational. # assuming $\neg A$

Then $\exists p \in \mathbb{Z}: \left[\exists q \in \mathbb{Z}^*: \sqrt{2} = \frac{p}{q}\right]$. # p, q *are assumed to be co-primes*

Let $(p_0 \in \mathbb{Z}) \wedge (q_0 \in \mathbb{Z}^*)$ such that $\sqrt{2} = \frac{p_0}{q_0}$. # p_0, q_0 *are assumed to be co-primes*

Then $\sqrt{2}\, q_0 = p_0$.

Then $2q_0^2 = p_0^2$.

Then p_0^2 is even.

Then p_0 is even.

Then $\exists k \in \mathbb{Z}: p_0 = 2k$.

Let $k_1 \in \mathbb{Z}$ such that $p_0 = 2k_1$.

…

Proof: $\sqrt{2}$ is irrational

....

Then $2q_0^2 = p_0^2 = (2k_1)^2 = 4k_1^2$.

Then $q_0^2 = 2k_1^2$.

Then q_0^2 is even.

Then q_0 is even.

Then $\exists l \in \mathbb{Z}: q_0 = 2l$.

Let $l_1 \in \mathbb{Z}$ such that $q_0 = 2l_1$.

Then both q_0 and p_0 are even.

Then q_0 and p_0 have 2 as a factor.

Then q_0 and p_0 are not co-primes.

However, since q and p are assumed to be co-primes and both q and p have 2 as a factor, then contradiction.

Therefore, $\sqrt{2}$ is irrational number.

Prime Numbers

- A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself
- A natural number greater than 1 that is not a prime number is called a composite number
- All composite numbers (that are larger than 2) can be divided by a prime
- Examples of prime numbers:
  - 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47…
- Primality of one:
  - Most early Greeks did not even consider 1 to be a number, so they could not consider it to be a prime
  - Furthermore, the prime numbers have several properties that the number 1 lacks

Example

- Prove there are infinitely many prime numbers
- Thoughts:
  - The size of the set of prime numbers is infinite
  - Define P: set of prime numbers
  - Define: $|P|$: size of P
  - Prove: $\forall n \in \mathbb{N}: |P| > n$
  - Suppose there is a finite set of prime numbers
  - Let this set $\{P_1, P_2, \dots, P_k\}$
  - Define $q' = P_1 \times P_2 \times \cdots \times P_k$
  - Also define $q = q' + 1 = P_1 \times P_2 \times \cdots \times P_k + 1$
  - Since $q \notin \{P_1, P_2, \dots, P_k\}$, then we assume q is not a prime

Prove: there are infinitely many prime numbers

- Thoughts…:
  - Then q can be divided by a prime, called $P_x \in \{P_1, P_2, \dots, P_k\}$
  - Then $\exists m \in \mathbb{N}: q = mP_x$
  - But P_x divides $q' = P_1 \times P_2 \times \cdots \times P_k$ since $P_x \in \{P_1, P_2, \dots, P_k\}$
  - $q' = P_x(P_1 \times \cdots \times P_{x-1} \times P_{x+1} \times \cdots \times P_k)$
  - $q = mP_x = P_1 \times P_2 \times \cdots \times P_k + 1$
  - $q - q' = 1 = mP_x - P_x(P_1 \times \cdots \times P_{x-1} \times P_{x+1} \times \cdots \times P_k)$
  - $1 = P_x(m - P_1 \times \cdots \times P_{x-1} \times P_{x+1} \times \cdots \times P_k)$
  - 1 divides P_x
  - Then $P_x = 1$ since only 1 divides 1
  - Since P_x is a prime then 1 should be a prime number… contradiction
  - We conclude there are infinitely many prime numbers

Proof: there are infinitely many prime numbers

proof by contradiction

Assume there is a finite set of prime numbers. # assuming $\neg A$

Then $P_1, P_2, \ldots, P_k$ are the elements of the set of prime numbers.

Let $q' = P_1 \times P_2 \times \cdots \times P_k$.

Then $q' > 1$.

Let $q = q' + 1$. # q is not prime since it is not in the set of prime numbers

Then $q > 2$.

Then $\exists P_x$ from the set of prime numbers such that P_x divides q. # every integer > 2 has a prime divider

Then P_x divides q'. # since q' is a multiplication of all the prime numbers, including P_x

Then P_x divides $q - q' = 1$.

Then $P_x = 1$. # only 1 divides 1

Then 1 is a prime number.

However, since 1 is not a prime, then contradiction. # 1 is not a prime number

Therefore, there are infinitely many prime numbers.