Discrete Mathematics
Theorem Proving

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2012

License

Topics

Brute Force Method

- examining all possible cases one by one

Theorem

Every number from the set $\{2, 4, 6, \ldots, 26\}$ can be written as the sum of at most 3 square numbers.

Proof.

$2 = 1+1$	$10 = 9+1$	$20 = 16+4$
$4 = 4$	$12 = 4+4+4$	$22 = 9+9+4$
$6 = 4+1+1$	$14 = 9+4+1$	$24 = 16+4+4$
$8 = 4+4$	$16 = 16$	$26 = 25+1$
	$18 = 9+9$	

□

Basic Rules

Universal Specification (US)

$\forall x\ p(x) \Rightarrow p(a)$

Universal Generalization (UG)

$p(a)$ for an arbitrarily chosen $a \Rightarrow \forall x\ p(x)$

Universal Specification Example

Example

All humans are mortal. Socrates is human.
Therefore, Socrates is mortal.

- $\mathcal{U}$: all humans
- $p(x)$: x is mortal
- $\forall x\ p(x)$: All humans are mortal.
- a: Socrates, $a \in \mathcal{U}$: Socrates is human.
- therefore, $p(a)$: Socrates is mortal.

Universal Specification Example

Example

$$\frac{\begin{array}{c}\forall x\ [j(x) \vee s(x) \rightarrow \neg p(x)] \\ p(m)\end{array}}{\therefore \neg s(m)}$$

1.	$\forall x\ [j(x) \vee s(x) \rightarrow \neg p(x)]$	A
2.	$p(m)$	A
3.	$j(m) \vee s(m) \rightarrow \neg p(m)$	$US : 1$
4.	$\neg(j(m) \vee s(m))$	$MT : 3, 2$
5.	$\neg j(m) \wedge \neg s(m)$	$DM : 4$
6.	$\neg s(m)$	$AndE : 5$

Universal Generalization Example

Example

$$\frac{\begin{array}{c}\forall x\ [p(x) \rightarrow q(x)] \\ \forall x\ [q(x) \rightarrow r(x)]\end{array}}{\therefore \forall x\ [p(x) \rightarrow r(x)]}$$

1.	$\forall x\ [p(x) \rightarrow q(x)]$	A
2.	$p(c) \rightarrow q(c)$	$US : 1$
3.	$\forall x\ [q(x) \rightarrow r(x)]$	A
4.	$q(c) \rightarrow r(c)$	$US : 3$
5.	$p(c) \rightarrow r(c)$	$HS : 2, 4$
6.	$\forall x\ [p(x) \rightarrow r(x)]$	$UG : 5$

Vacuous Proof

vacuous proof

to prove $P \Rightarrow Q$, show that P is false

Vacuous Proof Example

Theorem

$\forall S\ [\emptyset \subseteq S]$

Proof.

$\emptyset \subseteq S \Leftrightarrow \forall x\ [x \in \emptyset \rightarrow x \in S]$

$\forall x\ [x \notin \emptyset]$ □

Trivial Proof

trivial proof

to prove $P \Rightarrow Q$, show that Q is true

Trivial Proof Example

Theorem

$\forall x \in \mathbb{R}\ [x \geq 0 \Rightarrow x^2 \geq 0]$

Proof.

$\forall x \in \mathbb{R}\ [x^2 \geq 0]$ □

Direct Proof

direct proof

to prove $P \Rightarrow Q$, show that $P \vdash Q$

Direct Proof Example

Theorem

$\forall a \in \mathbb{Z}\ [3|(a-2) \Rightarrow 3|(a^2-1)]$

Proof.

$$
\begin{aligned}
3|(a-2) &\Rightarrow a-2 = 3k \\
&\Rightarrow a+1 = a-2+3 = 3k+3 = 3(k+1) \\
&\Rightarrow a^2-1 = (a+1)(a-1) = 3(k+1)(a-1)
\end{aligned}
$$

□

Indirect Proof

indirect proof

to prove $P \Rightarrow Q$, show that $\neg Q \vdash \neg P$

Indirect Proof Example

Theorem

$\forall x, y \in \mathbb{N}\ [x \cdot y > 25 \Rightarrow (x > 5) \vee (y > 5)]$

Proof.

- $\neg Q \Leftrightarrow (0 \leq x \leq 5) \wedge (0 \leq y \leq 5)$
- $0 = 0 \cdot 0 \leq x \cdot y \leq 5 \cdot 5 = 25$

□

Indirect Proof Example

Theorem

$(\exists k\ a, b, k \in \mathbb{N}\ [ab = 2k]) \Rightarrow (\exists i \in \mathbb{N}\ [a = 2i]) \vee (\exists j \in \mathbb{N}\ [b = 2j])$

Proof.

- $\neg Q \Leftrightarrow (\neg\exists i \in \mathbb{N}\ [a = 2i]) \wedge (\neg\exists j \in \mathbb{N}\ [b = 2j])$

$$
\begin{aligned}
&\Rightarrow (\exists x \in \mathbb{N}\ [a = 2x+1]) \wedge (\exists y \in \mathbb{N}\ [b = 2y+1]) \\
&\Rightarrow ab = (2x+1)(2y+1) \\
&\Rightarrow ab = 4xy + 2(x+y) + 1 \\
&\Rightarrow \neg(\exists a, b, k \in \mathbb{N}\ [ab = 2k])
\end{aligned}
$$

□

Proof by Contradiction

proof by contradiction

to prove P, show that $\neg P \vdash Q \wedge \neg Q$

Proof by Contradiction Example

Theorem

There is no largest prime number.

Proof.

- $\neg P$: There is a largest prime number.
- Q: The largest prime number is S.
- prime numbers: $2, 3, 5, 7, 11, \ldots, S$
- $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots S + 1$ is not divisible by a prime number between $2..S$
  1. either it is prime itself: $\neg Q$
  2. or it is divisible by a prime number greater than S: $\neg Q$

$\square$

Proof by Contradiction Example

Theorem

$\neg \exists a, b \in \mathbb{Z}^+ \; [\sqrt{2} = \frac{a}{b}]$

Proof.

- $\neg P$: $\exists a, b \in \mathbb{Z}^+ \; [\sqrt{2} = \frac{a}{b}]$
- Q: $gcd(a, b) = 1$

$$\begin{aligned} &\Rightarrow \; 2 = \frac{a^2}{b^2} \\ &\Rightarrow \; a^2 = 2b^2 \\ &\Rightarrow \; \exists i \in \mathbb{Z}^+ \; [a^2 = 2i] \\ &\Rightarrow \; \exists j \in \mathbb{Z}^+ \; [a = 2j] \end{aligned}$$

$$\begin{aligned} &\Rightarrow \; 4j^2 = 2b^2 \\ &\Rightarrow \; b^2 = 2j^2 \\ &\Rightarrow \; \exists k \in \mathbb{Z}^+ \; [b^2 = 2k] \\ &\Rightarrow \; \exists l \in \mathbb{Z}^+ \; [b = 2l] \\ &\Rightarrow \; gcd(a, b) \geq 2 : \neg Q \end{aligned}$$

$\square$

Equivalence Proofs

- to prove $P \Leftrightarrow Q$, both $P \Rightarrow Q$ and $Q \Rightarrow P$ must be proven
- a method to prove $P_1 \Leftrightarrow P_2 \Leftrightarrow \cdots \Leftrightarrow P_n$:
  $P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_n \Rightarrow P_1$

Equivalence Proof Example

Theorem

$a, b, n, q_1, r_1, q_2, r_2 \in \mathbb{Z}^+$

$a = q_1 \cdot n + r_1$

$b = q_2 \cdot n + r_2$

$r_1 = r_2 \Leftrightarrow n | (a - b)$

Equivalence Proof Example

$r_1 = r_2 \Rightarrow n | (a - b)$.

$$\begin{aligned} a - b &= (q_1 \cdot n + r_1) \\ &\quad -(q_2 \cdot n + r_2) \\ &= (q_1 - q_2) \cdot n \\ &\quad +(r_1 - r_2) \\ r_1 = r_2 &\Rightarrow r_1 - r_2 = 0 \\ &\Rightarrow a - b = (q_1 - q_2) \cdot n \end{aligned}$$

$\square$

$n | (a - b) \Rightarrow r_1 = r_2$.

$$\begin{aligned} a - b &= (q_1 \cdot n + r_1) \\ &\quad -(q_2 \cdot n + r_2) \\ &= (q_1 - q_2) \cdot n \\ &\quad +(r_1 - r_2) \\ n | (a - b) &\Rightarrow r_1 - r_2 = 0 \\ &\Rightarrow r_1 = r_2 \end{aligned}$$

$\square$

Equivalence Proof Example

Theorem

$$\begin{aligned} & A \subseteq B \\ \Leftrightarrow \; & A \cup B = B \\ \Leftrightarrow \; & A \cap B = A \\ \Leftrightarrow \; & \overline{B} \subseteq \overline{A} \end{aligned}$$

Equivalence Proof Example

$A \subseteq B \Rightarrow A \cup B = B.$

$A \cup B = B \Leftrightarrow A \cup B \subseteq B \wedge B \subseteq A \cup B$

$B \subseteq A \cup B$

$$\begin{aligned} x \in A \cup B &\Rightarrow x \in A \vee x \in B \\ A \subseteq B &\Rightarrow x \in B \\ &\Rightarrow A \cup B \subseteq B \end{aligned}$$

□

Equivalence Proof Example

$A \cup B = B \Rightarrow A \cap B = A.$

$A \cap B = A \Leftrightarrow A \cap B \subseteq A \wedge A \subseteq A \cap B$

$A \cap B \subseteq A$

$$\begin{aligned} y \in A &\Rightarrow y \in A \cup B \\ A \cup B = B &\Rightarrow y \in B \\ &\Rightarrow y \in A \cap B \\ &\Rightarrow A \subseteq A \cap B \end{aligned}$$

□

Equivalence Proof Example

$A \cap B = A \Rightarrow \overline{B} \subseteq \overline{A}.$

$$\begin{aligned} z \in \overline{B} &\Rightarrow z \notin B \\ &\Rightarrow z \notin A \cap B \\ A \cap B = A &\Rightarrow z \notin A \\ &\Rightarrow z \in \overline{A} \\ &\Rightarrow \overline{B} \subseteq \overline{A} \end{aligned}$$

□

Equivalence Proof Example

$\overline{B} \subseteq \overline{A} \Rightarrow A \subseteq B.$

$$\begin{aligned} \neg(A \subseteq B) &\Rightarrow \exists w \; [w \in A \wedge w \notin B] \\ &\Rightarrow \exists w \; [w \notin \overline{A} \wedge w \in \overline{B}] \\ &\Rightarrow \neg(\overline{B} \subseteq \overline{A}) \end{aligned}$$

□

Induction

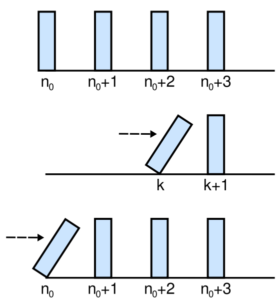
Definition

$S(n)$: a predicate defined on $n \in \mathbb{Z}^+$

$S(n_0) \wedge (\forall k \geq n_0 \; [S(k) \Rightarrow S(k+1)]) \Rightarrow \forall n \geq n_0 \; S(n)$

- $S(n_0)$: *base step*
- $\forall k \geq n_0 \; [S(k) \Rightarrow S(k+1)]$: *induction step*

Induction



Induction Example

Theorem
$\forall n \in \mathbb{Z}^+ \; [1 + 3 + 5 + \cdots + (2n-1) = n^2]$

Proof.

- $n = 1$: $1 = 1^2$
- $n = k$: assume $1 + 3 + 5 + \cdots + (2k-1) = k^2$
- $n = k+1$:

$$\begin{aligned} & 1 + 3 + 5 + \cdots + (2k-1) + (2k+1) \\ = \; & k^2 + 2k + 1 \\ = \; & (k+1)^2 \end{aligned}$$

$\square$

Induction Example

Theorem
$\forall n \in \mathbb{Z}^+, n \geq 4 \; [2^n < n!]$

Proof.

- $n = 4$: $2^4 = 16 < 24 = 4!$
- $n = k$: assume $2^k < k!$
- $n = k+1$:
  $2^{k+1} = 2 \cdot 2^k < 2 \cdot k! < (k+1) \cdot k! = (k+1)!$

$\square$

Induction Example

Theorem
$\forall n \in \mathbb{Z}^+, n \geq 14 \; \exists i, j \in \mathbb{N} \; [n = 3i + 8j]$

Proof.

- $n = 14$: $14 = 3 \cdot 2 + 8 \cdot 1$
- $n = k$: assume $k = 3i + 8j$
- $n = k+1$:
  - $k = 3i + 8j, j > 0 \Rightarrow k + 1 = k - 8 + 3 \cdot 3$
    $\Rightarrow k + 1 = 3(i+3) + 8(j-1)$
  - $k = 3i + 8j, j = 0, i \geq 5 \Rightarrow k + 1 = k - 5 \cdot 3 + 2 \cdot 8$
    $\Rightarrow k + 1 = 3(i-5) + 8(j+2)$

$\square$

Strong Induction

Definition
$S(n_0) \wedge (\forall k \geq n_0 \; [(\forall i \leq k \; S(i)) \Rightarrow S(k+1)]) \Rightarrow \forall n \geq n_0 \; S(n)$

Strong Induction Example

Theorem
$\forall n \in \mathbb{Z}^+, n \geq 2$
n can be written as the product of prime numbers

Proof.

- $n = 2$: $2 = 2$
- assume that the theorem is true for $\forall i \leq k$
- $n = k+1$:
  1. if prime: $n = n$
  2. if not prime: $n = u \cdot v$
     $u < k \wedge v < k \Rightarrow$ both u and v can be written as the product of prime numbers

$\square$

Strong Induction Example

Theorem
$\forall n \in \mathbb{Z}^+, n \geq 14 \; \exists i, j \in \mathbb{N} \; [n = 3i + 8j]$

Proof.

- $n = 14$: $14 = 3 \cdot 2 + 8 \cdot 1$
  $n = 15$: $15 = 3 \cdot 5 + 8 \cdot 0$
  $n = 16$: $16 = 3 \cdot 0 + 8 \cdot 2$
- $n \leq k$: assume $k = 3i + 8j$
- $n = k+1$: $k + 1 = (k-2) + 3$

$\square$

Flawed Induction Examples

Theorem

$\forall n \in \mathbb{Z}^+ \ [1 + 2 + 3 + \cdots + n = \frac{n^2+n+2}{2}]$

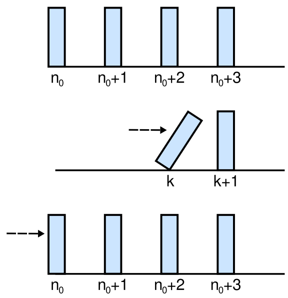
invalid base step

- $n = k$: assume $1 + 2 + 3 + \cdots + k = \frac{k^2+k+2}{2}$
- $n = k + 1$:

$$\begin{aligned} & 1 + 2 + 3 + \cdots + k + (k+1) \\ = \ & \frac{k^2 + k + 2}{2} + k + 1 = \frac{k^2 + k + 2}{2} + \frac{2k + 2}{2} \\ = \ & \frac{k^2 + 3k + 4}{2} = \frac{(k+1)^2 + (k+1) + 2}{2} \end{aligned}$$

- $n = 1$: $1 \neq \frac{1^2+1+2}{2} = 2$

Flawed Induction Examples



Flawed Induction Examples

Theorem

All horses are of the same color.

$A(n)$: *All horses in sets of n cardinality are of the same color.*

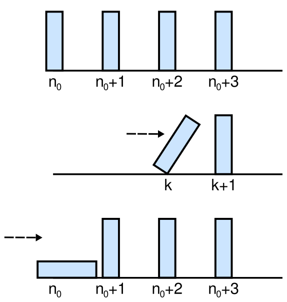
$\forall n \in \mathbb{N}^+ \ A(n)$

Flawed Induction Examples

Flawed induction over n

- $n = 1$: $A(1)$
  All horses in sets of 1 horse are of the same color.
- $n = k$: assume $A(k)$ is true
  All horses in sets of k horses are of the same color.
- $A(k+1) = \{a_1, a_2, \ldots, a_k\} \cup \{a_2, a_3, \ldots, a_{k+1}\}$
  - All horses in set $\{a_1, a_2, \ldots, a_k\}$ are of the same color (a_2)
  - All horses in set $\{a_2, a_3, \ldots, a_{k+1}\}$ are of the same color (a_2)

Flawed Induction Examples



References

Required Text: Grimaldi

- Chapter 2: Fundamentals of Logic
  - 2.5. Quantifiers, Definitions, and the Proofs of Theorems
- Chapter 4: Properties of Integers: Mathematical Induction
  - 4.1. The Well-Ordering Principle: Mathematical Induction

Supplementary Text: O'Donnell, Hall, Page

- Chapter 4: Induction