Discrete Mathematics

Predicates and Proofs

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2015

License

Topics

Predicates

Definition

predicate (or open statement): a declarative sentence which

- contains one or more variables, and
- is not a proposition, but
- becomes a proposition when the variables in it are replaced by certain allowable choices

- set of allowable choices: universe of discourse ($\mathcal{U}$)

Sets

- explicit notation: $\{a_1, a_2, \dots, a_n\}$
- $a \in S$: a is an element of S
- $a \notin S$: a is not an element of S

- $\mathbb{Z}$: integers
- $\mathbb{N}$: natural numbers
- $\mathbb{Z}^+$: positive integers
- $\mathbb{Q}$: rational numbers
- $\mathbb{R}$: real numbers
- $\mathbb{C}$: complex numbers

Predicate Examples

$\mathcal{U} = \mathbb{N}$
$p(x)$: $x + 2$ is an even integer.
$p(5)$: F
$p(8)$: T

$\neg p(x)$: $x + 2$ is not an even integer.

$\mathcal{U} = \mathbb{N}$
$q(x, y)$: $x + y$ and $x - 2y$ are even integers.
$q(11, 3)$: F, $q(14, 4)$: T

Quantifiers

Definition
existential quantifier: $\exists$
predicate is true for some values

- read: *there exists*
- one and only one: $\exists!$

Definition
universal quantifier: $\forall$
predicate is true for all values

- read: *for all*

$$\mathcal{U} = \{x_1, x_2, \dots, x_n\}$$
$$\exists x\ p(x) \Leftrightarrow p(x_1) \vee p(x_2) \vee \cdots \vee p(x_n)$$
$$\forall x\ p(x) \Leftrightarrow p(x_1) \wedge p(x_2) \wedge \cdots \wedge p(x_n)$$

Quantifier Examples

$\mathcal{U} = \mathbb{R}$

- $p(x) : x \geq 0$
- $q(x) : x^2 \geq 0$
- $r(x) : (x - 4)(x + 1) = 0$
- $s(x) : x^2 - 3 > 0$

are the following expressions true?

- $\exists x\ [p(x) \wedge r(x)]$
- $\forall x\ [p(x) \rightarrow q(x)]$
- $\forall x\ [q(x) \rightarrow s(x)]$
- $\forall x\ [r(x) \vee s(x)]$
- $\forall x\ [r(x) \rightarrow p(x)]$

Negating Quantifiers

- replace $\forall$ with $\exists$, and $\exists$ with $\forall$
- negate the predicate

$$\begin{aligned}
\neg\exists x\ p(x) &\Leftrightarrow \forall x\ \neg p(x)\\
\neg\exists x\ \neg p(x) &\Leftrightarrow \forall x\ p(x)\\
\neg\forall x\ p(x) &\Leftrightarrow \exists x\ \neg p(x)\\
\neg\forall x\ \neg p(x) &\Leftrightarrow \exists x\ p(x)
\end{aligned}$$

Negating Quantifiers

Theorem
$\neg\exists x\ p(x) \Leftrightarrow \forall x\ \neg p(x)$

Proof.

$$\begin{aligned}
\neg\exists x\ p(x) &\Leftrightarrow \neg[p(x_1) \vee p(x_2) \vee \cdots \vee p(x_n)]\\
&\Leftrightarrow \neg p(x_1) \wedge \neg p(x_2) \wedge \cdots \wedge \neg p(x_n)\\
&\Leftrightarrow \forall x\ \neg p(x)
\end{aligned}$$

□

Predicate Theorems

- $\exists x\ [p(x) \vee q(x)] \Leftrightarrow \exists x\ p(x) \vee \exists x\ q(x)$
- $\forall x\ [p(x) \wedge q(x)] \Leftrightarrow \forall x\ p(x) \wedge \forall x\ q(x)$
- $\forall x\ p(x) \Rightarrow \exists x\ p(x)$
- $\exists x\ [p(x) \wedge q(x)] \Rightarrow \exists x\ p(x) \wedge \exists x\ q(x)$
- $\forall x\ p(x) \vee \forall x\ q(x) \Rightarrow \forall x\ [p(x) \vee q(x)]$

Multiple Quantifiers

- quantifiers can be combined
- $\exists x \exists y\ p(x, y)$
- $\forall x \exists y\ p(x, y)$
- $\exists x \forall y\ p(x, y)$
- $\forall x \forall y\ p(x, y)$
- order of quantifiers is significant

Multiple Quantifier Example

$\mathcal{U} = \mathbb{Z}$
$p(x, y) : x + y = 17$

- $\forall x \exists y \; p(x, y)$:
  for every x there exists a y such that $x + y = 17$
- $\exists y \forall x \; p(x, y)$:
  there exists a y so that for all x, $x + y = 17$
- what changes if $\mathcal{U} = \mathbb{N}$?

Multiple Quantifiers

$$\mathcal{U}_x = \{1, 2\} \wedge \mathcal{U}_y = \{A, B\}$$

$$\begin{array}{lcl}
\exists x \exists y \; p(x, y) & \Leftrightarrow & [p(1, A) \vee p(1, B)] \vee [p(2, A) \vee p(2, B)] \\
\exists x \forall y \; p(x, y) & \Leftrightarrow & [p(1, A) \wedge p(1, B)] \vee [p(2, A) \wedge p(2, B)] \\
\forall x \exists y \; p(x, y) & \Leftrightarrow & [p(1, A) \vee p(1, B)] \wedge [p(2, A) \vee p(2, B)] \\
\forall x \forall y \; p(x, y) & \Leftrightarrow & [p(1, A) \wedge p(1, B)] \wedge [p(2, A) \wedge p(2, B)]
\end{array}$$

Method of Exhaustion

- examining all possible cases one by one

Theorem
Every even number between 2 and 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

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

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

1.	$\forall x\ [j(x) \vee s(x) \to \neg p(x)]$	A
2.	$p(m)$	A
3.	$j(m) \vee s(m) \to \neg p(m)$	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

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

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

Trivial Proofs

vacuous proof
to prove: $\forall x\ [p(x) \to q(x)]$
show: $\forall x\ \neg p(x)$

trivial proof
to prove: $\forall x\ [p(x) \to q(x)]$
show: $\forall x\ q(x)$

Trivial Proof Examples

Theorem

$\forall x \in \mathbb{N}\ [x < 0 \rightarrow \sqrt{x} < 0]$

Proof.

$\forall x \in \mathbb{N}\ [x \not< 0]$ □

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: $\forall x\ [p(x) \rightarrow q(x)]$

show: $\forall x\ [p(x) \vdash q(x)]$

Direct Proof Example

Theorem

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

$x \mid y$: $y \ mod \ x = 0$

Proof.

- assume: $3 \mid (a-2)$

$$\Rightarrow \exists k \in \mathbb{Z}\ [a - 2 = 3k]$$
$$\Rightarrow a + 1 = a - 2 + 3 = 3k + 3 = 3(k+1)$$
$$\Rightarrow a^2 - 1 = (a+1)(a-1) = 3(k+1)(a-1)$$

□

Indirect Proof

indirect proof

to prove: $\forall x\ [p(x) \rightarrow q(x)]$

show: $\forall x\ [\neg q(x) \vdash \neg p(x)]$

Indirect Proof Example

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

Proof.

- assume: $\neg((x > 5) \vee (y > 5))$

$$\Rightarrow \quad (0 \leq x \leq 5) \wedge (0 \leq y \leq 5)$$
$$\Rightarrow \quad x \cdot y \leq 5 \cdot 5 = 25$$

□

Indirect Proof Example

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

Proof.

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

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

□

Proof by Contradiction

proof by contradiction
to prove: P
show: $\neg P \vdash Q \wedge \neg Q$

Proof by Contradiction Example

Theorem
There is no largest prime number.

Proof.

- assume: There is a largest prime number.
- Q: The largest prime number is s.
- prime numbers: $2, 3, 5, 7, 11, \ldots, s$
- let $z = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots s + 1$
- z is not divisible by any prime number in the range $[2, s]$

1. either z is a prime number (note that $z > s$): $\neg Q$
2. or z is divisible by a prime number t ($t > s$): $\neg Q$

□

Proof by Contradiction Example

Theorem

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

Proof.

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

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

□

Proof by Contradiction Example

Theorem

$0.\overline{9} = 1$

Proof.

- assume: $0.\overline{9} < 1$
- let $x = \frac{0.\overline{9}+1}{2}$
- Q: $0.\overline{9} < x < 1$
- what digit other than 9 can x contain?

□

Induction

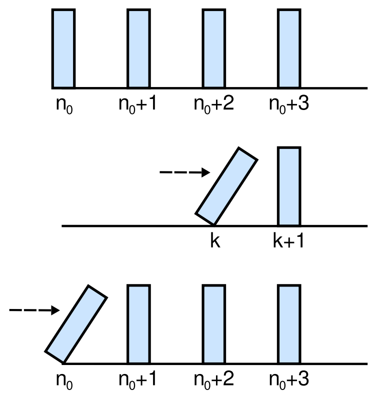
Definition

$S(n)$: 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 n is prime: $n = n$
    2. if n is not prime: $n = u \cdot v$

       $u \leq k \Rightarrow u = u_1 \cdot u_2 \cdots$ where $u_1, u_2, \ldots$ are prime

       $v \leq k \Rightarrow v = v_1 \cdot v_2 \cdots$ where $v_1, v_2, \ldots$ are prime

       $n = u_1 \cdot u_2 \cdots v_1 \cdot v_2 \cdots$

□

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 $k = 3i + 8j$
- $n = k + 1$: $k + 1 = (k - 2) + 3$

□

References

Required Reading: Grimaldi

- Chapter 2: Fundamentals of Logic
    - 2.4. The Use of Quantifiers
    - 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 Reading: O'Donnell, Hall, Page

- Chapter 7: Predicate Logic
- Chapter 4: Induction