CONTENTS

June 29, 2020

Proofs involving quantifiers

Theorem (1.6.1)

If $a, b, c \in \mathbb{Z}$ and $c|a$ and $c|b$, then c divides every linear combination of a and b. In particular, $c|(a+b)$ and $c|(a-b)$.

Logical form in $\mathbb{Z}$: $(\forall a)(\forall b)(\forall c)([c|a \wedge c|b] \Rightarrow (\forall x)(\forall y)[c|(ax+by)])$

Proofs by contradiction

PROOF OF $(\forall x)P(x)$ BY CONTRADICTION
Proof.
Suppose $\sim (\forall x)P(x)$.
Then $(\exists x) \sim P(x)$.
Let t be an object such that $\sim P(t)$.
$\vdots$
Therefore $Q \wedge \sim Q$.
Thus $(\exists x) \sim P(x)$ is false, so $(\forall x)P(x)$ is true. $\square$

Example

Prove that for all $x \in (0, \frac{\pi}{2}),\ \sin x + \cos x > 1$.

CONSTRUCTIVE PROOF OF $(\exists x)P(x)$

Proof: Specify one particular object a.

If necessary, verify that a is in the universe.

$\vdots$

Therefore, $P(a)$ is true.

Thus, $(\exists x)P(x)$ is true. $\square$

Example

Prove that $\exists n \in \mathbb{N}$ whose square is the sum of three other squares.

INDIRECT PROOF OF $(\exists x)P(x)$

Proof.

$\vdots$

Therefore, there must be an object a such that $P(a)$ is true.

Therefore, $(\exists x)P(x)$ is true.$\square$

Proofs by contradiction

PROOF OF $(\exists x)P(x)$ BY CONTRADICTION

Proof.

Suppose $\sim (\exists x)P(x)$.

Then $(\forall x) \sim P(x)$.

$\vdots$

Therefore, $\sim Q \wedge Q$, a contradiction.

Thus $\sim (\exists x)P(x)$ is false.

Therefore $(\exists x)P(x)$ is true.$\square$

Example

Let S be a set of 6 positive integers, each less than or equal to 10. Prove that there exists a pair of integers in S whose sum is 11.

Theorem (1.6.2)

Between any two rational numbers x and y there is a (different) rational number z.

Symbolized form:

Unique existence

PROOF OF $(\exists!x)P(x)$

Proof.

i) Prove that $(\exists x)P(x)$ is true. Use any method.

ii) Prove that $(\forall y)(\forall z)[P(y) \wedge P(z) \Rightarrow y = z]$.

Assume that y and z are objects in the universe such that $P(y)$ and $P(z)$ are true.

$\vdots$

Therefore, $y = z$.

From i) and ii) conclude that $(\exists!x)P(x)$ is true. $\square$

Example

Prove that every nonzero real number has a unique multiplicative inverse.

Valid deductions

1. $(\forall x)(\forall y)P(x,y) \iff (\forall y)(\forall x)P(x,y)$.
2. $(\exists x)(\exists y)P(x,y) \iff (\exists y)(\exists x)P(x,y)$.
3. $[(\forall x)P(x) \vee (\forall x)Q(x)] \Rightarrow (\forall x)[P(x) \vee Q(x)]$.
4. $(\forall x)[P(x) \Rightarrow Q(x)] \Rightarrow [(\forall x)P(x) \Rightarrow (\forall x)Q(x)]$.
5. $(\forall x)[P(x) \wedge Q(x)] \iff [(\forall x)P(x) \wedge (\forall x)Q(x)]$.
6. $(\exists x)(\forall y)P(x,y) \Rightarrow (\forall y)(\exists x)P(x,y)$.

Exercise: Check that the converses of statements 3 and 4 are not valid. For instance, the converse of 6 is not valid since

Suggestion: *Read and try to solve by yourself all Examples in the book (we have skipped some). Then do the same with the Exercises in ALL sections, start with the $\star$ stared ones.*

Example (Counterexamples)

In $\mathbb{R}$, is it true or false that $(\forall x)(\forall y)[(x+y)^2 = x^2 + y^2]$?

Example ($\sim (\exists x)P(x) \iff (\forall x) \sim P(x)$)

There is no even integer which is odd.

If you want to learn more strategies then read Section 1.7.

CONTENTS

June 29, 2020

Basic Concepts of Set Theory

Definition

Let $\varnothing = \{x : x \neq x\}$. Then $\varnothing$ is a set, called the *empty set* or *null set*.


UCDAVIS
AGGIES

Definition

DIRECT PROOF OF $A \subseteq B$

Proof.

Let x be any object.

Suppose $x \in A$.

$\vdots$

Thus $x \in B$.

Therefore $A \subseteq B$.

Theorem (2.1.1)

a) *For every set* A, $\varnothing \subseteq A$.

b) *For every set* A, $A \subseteq A$.

c) *For all sets* A, B, *and* C, *if* $A \subseteq B$ *and* $B \subseteq C$, *then* $A \subseteq C$.

Equal sets and Proper subsets

Definition

TWO PART PROOF OF $A = B$

Proof.

i) Prove that $A \subseteq B$ (by any method).

ii) Prove that $B \subseteq A$ (by any method).

Therefore $A = B$.


UCDAVIS
AGGIES

Theorem (2.1.2)

If A and B are sets with no elements, then $A = B$.

Proof: See Exercise 12. $\Diamond$

Theorem (2.1.3)

For any sets A and B, if $A \subseteq B$ and $A \neq \varnothing$, then $B \neq \varnothing$.

Venn diagrams


UCDAVIS
AGGIES

Power set

Definition

Let A be a set. The *power set* of A is the set whose elements are the subsets of A and is denoted $\mathcal{P}(A)$. Thus

$$\mathcal{P}(A) = \{B : B \subseteq A\}.$$

Theorem (2.1.4)

If A is a set with n elements, then $\mathcal{P}(A)$ is a set with 2^n elements.

Theorem (2.1.5)

Let A and B be sets. Then $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.


UCDAVIS
AGGIES