Proofs Strategies For

PROOFS AND FUNDAMENTALS

February 9, 2017

1. Prove if P then Q — via Direct Proof

Theorem. *Let P and Q be statements. … (hypotheses) … Prove if P then Q.*

Symbols: $P \to Q$

Proof. Suppose that P is true.

$\vdots$

(argumentation)

$\vdots$

Then Q is true. □

2. Prove if P then Q — via Proof by Contrapositive

Theorem. *Let P and Q be statements. … (hypotheses) … Prove if P then Q.*

Symbols: $P \to Q$

Proof. Suppose that Q is false.

$\vdots$

(argumentation)

$\vdots$

Then P is false. □

3. Prove if P then Q — via Proof by Contradiction

Theorem. *Let P and Q be statements. … (hypotheses) … Prove if P then Q.*

Symbols: $P \to Q$

Proof. Suppose that P is true. Suppose that Q is false.

$\vdots$

(argumentation)

$\vdots$

We have reached a contradiction. Therefore Q must be true. □

4. Prove if P, then A or B

Theorem. *Let P, A and B be statements. … (hypotheses) … Prove if P, then A or B.*

Symbols: $P \to (A \vee B)$

***Proof*.** Suppose that P is true. Suppose that A is false.

⋮

(argumentation)

⋮

Then B is true. □

5. Prove if A or B, then Q

Theorem. *Let A, B and Q be statements. … (hypotheses) … Prove if A or B, then Q.*

Symbols: $(A \vee B) \to Q$

***Proof*.** Suppose that A or B are true.
Case 1: Suppose that A is true.

⋮

(argumentation)

⋮

Then Q is true.
Case 2: Suppose that B is true.

⋮

(argumentation)

⋮

Then Q is true. □

6. Prove P if and only if Q

Theorem. *Let P and Q be statements. … (hypotheses) … Prove P if and only if Q.*

Symbols: $P \longleftrightarrow Q$

***Proof*.** $\Rightarrow$ Suppose that P is true.

⋮

(argumentation)

⋮

Then Q is true.

$\Leftarrow$ Suppose that Q is true.

⋮

(argumentation)

⋮

Then P is true. □

7. Prove a Statement with a For All Quantifier

Theorem. *Let $P(x)$ be a statement with free variable x, and let U be a collection of possible values of x. … (hypotheses) … Prove that for all x in U, the statement $P(x)$ holds.*

Symbols: $(\forall x \text{ in } U) P(x)$

***Proof*.** Let c be in U.

⋮

(argumentation)

⋮

Then $P(c)$ is true. □

8. Prove a Statement with a There Exists Quantifier

Theorem. *Let $P(x)$ be a statement with free variable x, and let U be a collection of possible values of x. … (hypotheses) … Prove that there exists some x in U such that the statement $P(x)$ holds.*

Symbols: $(\exists x \text{ in } U)P(x)$

Proof. Let $c = \ldots$. *[Only one example of c is needed.]*

⋮

(argumentation)

⋮

Then c is in U.

⋮

(argumentation)

⋮

Then $P(c)$ is true. □

9. Prove an Existence and Uniqueness Statement

Theorem. *Let $P(x)$ be a statement with free variable x, and let U be a collection of possible values of x. … (hypotheses) … Prove that there exists a unique x in U such that the statement $P(x)$ holds.*

Symbols: $(\exists ! x \text{ in } U)P(x)$

Proof. Uniqueness:

Let a and b be in U. Suppose that $P(a)$ and $P(b)$ are true.

⋮

(argumentation)

⋮

Then $a = b$.

Existence:

Let $c = \ldots$. *[Only one example of c is needed.]*

⋮

(argumentation)

⋮

Then c is in U.

⋮

(argumentation)

⋮

Then $P(c)$ is true. □

10. Prove a Statement with Two Quantifiers — For All and There Exists

Theorem. *Let $P(x, y)$ be a statement with free variables x and y, let U be a collection of possible values of x and let V be a collection of possible values of y. … (hypotheses) … Prove that for each x in U there exists some y in V such that the statement $P(x, y)$ holds.*

Symbols: $(\forall x \text{ in } U)(\exists y \text{ in } V)P(x, y)$

Proof. Let c be in U.

⋮

(argumentation)

⋮

Let $d = \ldots$. *[Note that d can depend upon c.]*

⋮

(argumentation)

⋮

Then d is in V.

⋮

(argumentation)

⋮

Then $P(c, d)$ is true. □

11. Prove a Statement with Two Quantifiers — There Exists and For All

Theorem. *Let $P(x, y)$ be a statement with free variables x and y, let U be a collection of possible values of x and let V be a collection of possible values of y. … (hypotheses) … Prove that there is some x in U such that for each y in V, the statement $P(x, y)$ holds.*

Symbols: $(\exists x \text{ in } U)(\forall y \text{ in } V)P(x, y)$

Proof. Let $c = \ldots$. *[Only one example of c is needed.]*

⋮

(argumentation)

⋮

Then c is in U.

⋮

(argumentation)

⋮

Let d be in V. *[Note that d is independent of c.]*

⋮

(argumentation)

⋮

Then $P(c, d)$ is true. □

12. Prove that One Set is a Subset of Another Set

Theorem. *Let A and B be sets. … (hypotheses) … Prove that* $A \subseteq B$.

Symbols: $(\forall x \in A)(x \in B)$

***Proof*.** Let $x \in A$.

$\vdots$

(argumentation)

$\vdots$

Then $x \in B$. Hence $A \subseteq B$. □

13. Prove that Two Sets are Equal

Theorem. *Let A and B be sets. … (hypotheses) … Prove that* $A = B$.

Symbols: $(\forall x \in A)(x \in B) \ \wedge \ (\forall x \in B)(x \in A)$

***Proof*.** Let $x \in A$.

$\vdots$

(argumentation)

$\vdots$

Then $x \in B$. Hence $A \subseteq B$.
Next, Let $y \in B$.

$\vdots$

(argumentation)

$\vdots$

Then $y \in A$. Hence $B \subseteq A$.
We conclude that $A = B$. □

14. Prove that Two Functions are Equal

Theorem. *Let $f : A \to B$ and $g : C \to D$ be functions. … (hypotheses) … Prove that $f = g$.*

Symbols: $A = C \ \wedge \ B = D \ \wedge \ (\forall x \in A)(f(x) = g(x))$

Proof. (Argumentation)

$\vdots$

Therefore $A = C$. Hence f and g have the same domain.

$\vdots$

(argumentation)

$\vdots$

Therefore $B = D$. Hence f and g have the same codomain.
Let $a \in A = C$.

$\vdots$

(argumentation)

$\vdots$

Then $f(a) = g(a)$.
Therefore $f = g$. □

15. Prove that a Functions has a Right Inverse.

Theorem. *Let $f : A \to B$ be a function. … (hypotheses) … Prove that f has a right inverse.*

Symbols: $(\exists g : B \to A)(\forall x \in B)(f(g(x)) = x)$

Proof. Let $g : B \to A$ be defined by …. *[Only one example of g is needed.]*
Let $y \in B$.

$\vdots$

(Argumentation)

$\vdots$

Then $f(g(y)) = y$. Hence $f \circ g = 1_B$.
Therefore g is a right inverse of f. □

16. Prove that a Functions has a Left Inverse.

Theorem. *Let $f : A \to B$ be a function. ... (hypotheses) ... Prove that f has a left inverse.*

Symbols: $(\exists g : B \to A)(\forall x \in A)(g(f(x)) = x)$

Proof. Let $g : B \to A$ be defined by .... *[Only one example of g is needed.]*
Let $x \in A$.
⋮
(Argumentation)
⋮
Then $g(f(x)) = x$. Hence $g \circ f = 1_A$.
Therefore g is a left inverse of f. □

17. Prove that a Functions has an Inverse.

Theorem. *Let $f : A \to B$ be a function. ... (hypotheses) ... Prove that f has an inverse.*

Symbols: $(\exists g : B \to A)[(\forall x \in A)(g(f(x)) = x) \land (\forall x \in B)(f(g(x)) = x)]$

Proof. Let $g : B \to A$ be defined by ....
Let $x \in B$.
⋮
(Argumentation)
⋮
Then $f(g(x)) = x$. Hence $f \circ g = 1_B$.
Therefore g is a right inverse of f.
Let $x \in A$.
⋮
(Argumentation)
⋮
Then $g(f(x)) = x$. Hence $g \circ f = 1_A$.
Therefore g is a left inverse of f.
We conclude that g is an inverse of f. □

18. Prove that a Function is Injective

Theorem. *Let A and B be sets, and let $f : A \to B$ be a function. ... (hypotheses) ... Prove that f is injective.*

Symbols: $(\forall x, y \in A)(f(x) = f(y) \to x = y)$

Proof. Let $x, y \in A$. Suppose that $f(x) = f(y)$.

$\vdots$

(argumentation)

$\vdots$

Then $x = y$. Hence f is injective. □

19. Prove that a Function is Surjective

Theorem. *Let A and B be sets, and let $f : A \to B$ be a function. ... (hypotheses) ... Prove that f is surjective.*

Symbols: $(\forall b \in B)(\exists a \in A)(f(a) = b)$

Proof. Let $b \in B$.

$\vdots$

Let $a = \ldots$.

$\vdots$

(argumentation)

$\vdots$

Then $f(a) = b$. Hence f is surjective. □

20. Prove that a Function is Bijective

Theorem. *Let A and B be sets, and let $f : A \to B$ be a function. … (hypotheses) … Prove that f is injective.*

Symbols: $(\forall x, y \in A)(f(x) = f(y) \to x = y) \;\wedge\; (\forall b \in B)(\exists a \in A)(f(a) = b)$

Proof. Let $x, y \in A$. Suppose that $f(x) = f(y)$.
⋮
(argumentation)
⋮
Then $x = y$. Hence f is injective.
Let $b \in B$.
⋮
Let $a = \dots$.
⋮
(argumentation)
⋮
Then $f(a) = b$. Hence f is surjective.
We conclude that f is bijective. □

21. Prove that Two Relations are Equal

Theorem. *Let A and B be sets, and let R and S be relations from A to B. … (hypotheses) … Prove that $R = S$.*

Symbols: $(\forall x, y \in A)(x \; R \; y \longleftrightarrow x \; S \; y)$

Proof. Let $x \in A$ and $y \in B$. First, suppose that $x \; R \; y$.
⋮
(argumentation)
⋮
Then $x \; S \; y$.
Second, suppose that $x \; S \; y$.
⋮
(argumentation)
⋮
Then $x \; R \; y$.
Therefore $R = S$. □

22. Prove that a Relation is Reflexive

Theorem. *Let A be a set, and let R be a relation on A. … (hypotheses) … Prove that R is reflexive.*

Symbols: $(\forall x \in A)(x \ R \ x)$

Proof. Let $x \in A$.

⋮

(argumentation)

⋮

Then $x \ R \ x$. Hence R is reflexive. □

23. Prove that a Relation is Symmetric

Theorem. *Let A be a set, and let R be a relation on A. … (hypotheses) … Prove that R is symmetric.*

Symbols: $(\forall x, y \in A)(x \ R \ y \to y \ R \ x)$

Proof. Let $x, y \in A$. Suppose that $x \ R \ y$.

⋮

(argumentation)

⋮

Then $y \ R \ x$. Hence R is symmetric. □

24. Prove that a Relation is Transitive

Theorem. *Let A be a set, and let R be a relation on A. … (hypotheses) … Prove that R is transitive.*

Symbols: $(\forall x, y, z \in A)([x \ R \ y \ \wedge \ y \ R \ z] \to x \ R \ z)$

Proof. Let $x, y, z \in A$. Suppose that $x \ R \ y$ and $y \ R \ z$.

⋮

(argumentation)

⋮

Then $x \ R \ z$. Hence R is transitive. □

25. Prove that a Relation is an Equivalence Relation

Theorem. *Let A be a set, and let R be a relation on A. … (hypotheses) … Prove that R is an equivalence relation.*

Symbols: $(\forall x, y, z \in A)([x \ R \ x] \ \wedge \ [x \ R \ y \to y \ R \ x] \ \wedge \ [(x \ R \ y \ \wedge \ y \ R \ z) \to x \ R \ z])$

Proof. Let $x, y, z \in A$.

$\vdots$

(argumentation)

$\vdots$

Then $x \ R \ x$. Hence R is reflexive.
Suppose that $x \ R \ y$.

$\vdots$

(argumentation)

$\vdots$

Then $y \ R \ x$. Hence R is symmetric.
Suppose that $x \ R \ y$ and $y \ R \ z$.

$\vdots$

(argumentation)

$\vdots$

Then $x \ R \ z$. Hence R is transitive.
We conclude that R is an equivalence relation. □

26. Prove a Statement Using Mathematical Induction.

Theorem. *Let $P(n)$ be a statement with free variable n, where n is a natural number. … (hypotheses) … Prove that for all n in $\mathbb{N}$, the statement $P(n)$ holds.*

Symbols: $P(1) \ \wedge \ (\forall n \in \mathbb{N})(P(n) \to P(n+1))$

Proof. (Argumentation)

$\vdots$

Then $P(1)$ is true.
Let $n \in \mathbb{N}$. Suppose that $P(n)$ is true.

$\vdots$

(argumentation)

$\vdots$

Then $P(n+1)$ is true. □

27. Prove that Two Sets Have the Same Cardinality — via Bijectivity.

Theorem. *Let A and B be sets. … (hypotheses) … Prove that $A \sim B$.*

Symbols: $(\exists f : A \to B)[(\forall x, y \in A)(f(x) = f(y) \to x = y) \wedge (\forall b \in B)(\exists a \in A)(f(a) = b)]$

Proof. Let $f : A \to B$ be defined by …. *[Only one example of f is needed.]*
Let $x, y \in A$. Suppose that $f(x) = f(y)$.
$\vdots$
(argumentation)
$\vdots$
Then $x = y$. Hence f is injective.
Let $b \in B$.
$\vdots$
Let $a = \ldots$.
$\vdots$
(argumentation)
$\vdots$
Then $f(a) = b$. Hence f is surjective.
We conclude that f is bijective. It follows that $A \sim B$. □

28. Prove that Two Sets Have the Same Cardinality — via Inverse Functions.

Theorem. *Let A and B be sets. … (hypotheses) … Prove that $A \sim B$.*

Symbols: $(\exists f : A \to B)(\exists g : B \to A)[(\forall x \in A)(g(f(x)) = x) \wedge (\forall x \in B)(f(g(x)) = x)]$

Proof. Let $f : A \to B$ be defined by …. *[Only one example of f is needed.]*
Let $g : B \to A$ be defined by ….
Let $y \in B$.
$\vdots$
(Argumentation)
$\vdots$
Then $f(g(y)) = y$. Hence $f \circ g = 1_B$.
Therefore g is a right inverse of f.
Let $x \in A$.
$\vdots$
(Argumentation)
$\vdots$
Then $g(f(x)) = x$. Hence $g \circ f = 1_A$.
Therefore g is a left inverse of f.
We conclude that g is an inverse of f. Therefore f is bijective. It follows that $A \sim B$. □