PROOF TEMPLATES

1. Basic form of a proof of an existential statement using the method of constructive proof.
2. Proving an existential statement without a domain using the method of constructive proof.
3. Basic form of proofs using the method of direct proof.
4. Proofs using the method of direct proof in other situations.
5. Basic form of proofs using the method of division into cases.
6. Basic form of proofs using the method of argument by contradiction.
7. Basic form of proofs using the method of argument by contraposition.
8. The form of proofs using the principle of mathematical induction.
9. The form of proofs using the principle of strong mathematical induction.

BASIC FORM OF A PROOF OF AN EXISTENTIAL STATEMENT USING THE METHOD OF CONSTRUCTIVE PROOF

Suppose you are trying to prove a statement which has the following logical form

$$\exists x \in D \ s.t. \ P(x)$$

Before beginning your proof, take out some scratch paper and find some particular a in D with the property that $P(a)$ is true. You can now give a dirct proof of the statement which looks like (instructions and comments are written in italics):

Proof. Let $x = a$.

write out a proof that $x \in D$ here

*
*
*

write out a proof that $P(x)$ here

*
*
*

We have established that there exists an x in D such that $P(x)$.

QED

You might prefer the following alternative.

Proof.

write out a proof that $a \in D$ here

*
*
*

write out a proof that $P(a)$ here

*
*
*

Since $a \in D$ and $P(a)$, there exists an x in D such that $P(x)$.

QED

PROVING AN EXISTENTIAL STATEMENT WITHOUT A DOMAIN USING THE METHOD OF CONSTRUCTIVE PROOF

Suppose the statement you are trying to prove is like that on the previous page but is missing the domain D:

$$\exists x \ s.t. \ P(x)$$

As on the previous template, before beginning your proof, take out some scratch paper and find some particular a with the property that $P(a)$ is true. You can now give a dirct proof of the statement which looks like (instructions and comments are written in italics):

Proof. Let $x = a$.

write out a proof that $P(x)$ here

*
*
*

We have established that there exists an x such that $P(x)$.

QED

You might prefer the following alternative.

Proof.

write out a proof that $P(a)$ here

*
*
*

Since $P(a)$, there exists an x such that $P(x)$.

QED

BASIC FORM OF PROOFS USING THE METHOD OF DIRECT PROOF

Suppose you are trying to prove a statement which has the following logical form

$$\forall x \in D,\ if\ P(x)\ then\ Q(x)$$

Here is what a direct proof of that statement should look like. Instructions and comments are written in italics.

Proof. Assume x is an arbitrary element of D such that $P(x)$. We will show that $Q(x)$.

*
*
*

your proof of $Q(x)$ *using assumptions* $x \in D$ *and* $P(x)$

*
*
*

Since x was an arbitrary element of D such that $P(x)$, for every element x of D, if $P(x)$ then $Q(x)$.

QED

PROOFS USING
THE METHOD OF DIRECT PROOF IN OTHER SITUATIONS

The method of direct proof on the basic template is for proving statements with logical form

$$\forall x \in D,\ if\ P(x)\ then\ Q(x)$$

Here we will consider the method of direct proof for statements with the following logical forms (remember, these arguements work for predicates too so there may be other variables in the predicates than those indicated e.g. $P(x)$ may be replaced by a predicate with another variable y as in $P(x, y)$).
The other logical forms we consider are

1. $\forall x,\ if\ P(x)\ then\ Q(x)$
2. $\forall x \in D,\ Q(x)$
3. $\forall x,\ Q(x)$
4. $if\ P\ then\ Q$
5. Versions of the basic form, 1, 2 and 3 with more than one quantifier e.g. $\forall x \in D, \forall y \in E,\ if\ P(x, y)\ then\ Q(x, y)$

1. Suppose you are trying to prove a statement with the logical form on the basic template BUT D is missing:

$$\forall x,\ if\ P(x)\ then\ Q(x)$$

What should the proof look like?

Proof. Assume x is arbitrary such that $P(x)$. We will show that $Q(x)$.

$$*$$
$$*$$
$$*$$

your proof of $Q(x)$ using the assumption $P(x)$

$$*$$
$$*$$
$$*$$

Since x was arbitrary such that $P(x)$, for every x, if $P(x)$ then $Q(x)$.

QED

2. Now suppose $P(x)$ is missing:

$$\forall x \in D, Q(x)$$

What should the proof look like?

Proof. Assume x is an arbitrary element of D. We will show that $Q(x)$.

*
*
*

your proof of $Q(x)$ *using the assumption* $x \in D$

*
*
*

Since x was an arbitrary element of D, for every element x of D, $Q(x)$.

QED

3. Now suppose both D and $P(x)$ is missing:

$$\forall x, Q(x)$$

What should the proof look like?

Proof. Assume x is arbitrary. We will show that $Q(x)$.

*
*
*

your proof of $Q(x)$

*
*
*

Since x was an arbitrary, for every x, $Q(x)$.

QED

4. Suppose $\forall x \in D$ is missing:

$$if\ P\ then\ Q$$

What should the proof look like?

Proof. Assume P. We will show that Q.

*
*
*

your proof of Q using the assumption P

*
*
*

We have established that P implies Q.

QED

5. Suppose you are trying to prove a statement with the logical form on the basic template but there is a second universal quantifier:

$$\forall x \in D, \forall y \in E,\ if\ P(x,y)\ then\ Q(x,y)$$

What should the proof look like?

Proof. Assume x is an arbitrary element of D and y is an arbitrary element of E such that $P(x,y)$. We will show that $Q(x,y)$.

*
*
*

your proof of $Q(x,y)$ using the assumptions $x \in D$, $y \in E$ and $P(x,y)$

*
*
*

Since x was an arbitary element of D and y was arbitary and arbitary element of E such that $P(x,y)$, for every x in D and every y in E, if $P(x,y)$ then $Q(x,y)$.

QED

Similar extensions can be made to statements of forms 1, 2 and 3 if there is more than one universal quantifier.

BASIC FORM OF PROOFS USING THE METHOD OF DIVISION INTO CASES

Suppose you are trying to prove a statement S. If you first prove P **or** Q you can then divide your argument into cases depending on whether P is true or Q is true. Here is how such a proof would look. Instructions and comments are written in italics.

Proof.

*
*
*

*your proof of P **or** Q ending with the statement of P **or** Q below*

*
*
*

P **or** Q.
We will argue by cases depending on whether P or Q.
Case 1: Assume P.

*
*
*

your proof of S using the assumption P

*
*
*

Case 2: Assume Q.

*
*
*

your proof of S using the assumption Q

*
*
*

In every case, S.

QED

BASIC FORM OF A PROOF USING THE METHOD ARGUMENT BY CONTRADICTION

Suppose you are trying to prove a statement A. A proof of A by contradiciton looks like (instructions and comments are written in italics):

Proof. We will argue by contradiction. Assume that $\sim A$ *(you should simplify the form of* $\sim A$ *by the usual rules for rewriting a negation).*

write out a proof of a contradiction here –
usually this means proving q *and* $\sim q$ *for some statement* q

*
*
*

Since assuming A is false leads to a contradiction, A. *QED*

BASIC FORM OF A PROOF USING THE METHOD ARGUMENT BY CONTRAPOSITION

This method uses the logical equivalent of a conditional or universal conditional with it's contrapositive:

$$p \to q \;\equiv \sim p \to \sim q$$

$$\forall x \in D, if\; P(x)\; then\; Q(x) \quad \equiv \quad \forall x \in D, if\; \sim Q(x)\; then\; \sim P(x)$$

A proof by contraposition of a conditional or universal conditional A consists of trying to prove the contrapositive.

Proof. We will prove the contrapositive of A i.e. *write out the contrapositive here.*

write out a proof of the contrapositive here –
for example, use a direct proof

*
*
*

Since we have established the contrapositive of A, A. QED

THE FORM OF PROOFS USING THE PRINCIPLE OF MATHEMATICAL INDUCTION

Here is what a proof by mathematical induction should look like. Instructions and comments are written in italics.

$\forall n \in \mathbf{Z}$, if $n \geq a$ then *some property of* n.

Proof. We will use mathematical induction. Let $P(n)$ be the property of integers n such that

> $P(n)$ iff *write down the property of* n *from what you are trying to prove*

(basis step) We will prove $P(a)$ i.e. *write out what* $P(a)$ *means here.*

Write out a proof of $P(a)$ *here*

(inductive step) Assume $n \in \mathbf{Z}$, $n \geq a$, and $P(n)$ i.e. *write out what* $P(n)$ *means here.* We will show that $P(n+1)$ i.e. *write out what* $P(n+1)$ *means here.*

> *Write out a proof of* $P(n+1)$ *here. You can use the assumptions* $n \in \mathbf{Z}$, $n \geq a$, *and* $P(n)$ *(called the "inductive hypothesis").*

By mathematical induction, for every integer n, if $n \geq a$ then *write out* $P(n)$ *here.* *QED*

Notice that a will usually be a fixed integer like -1, 0, or 1, but sometimes a can be a variable or a complex expression.

$\forall n \in \mathbf{Z}$, if $n \geq$ then

Proof. We will use mathematical induction. Let $P(n)$ be the property of integers n such that

$P(n)$ iff

(basis step) We will prove $P(\ )$ i.e.

(inductive step) Assume $n \in \mathbf{Z}$, $n \geq$ and $P(n)$ holds i.e.

We will show that $P(n+1)$ i.e.

By mathematical induction, for every integer n, if $n \geq$ then

QED

THE FORM OF PROOFS USING THE PRINCIPLE OF STRONG MATHEMATICAL INDUCTION

Here is what a proof by strong mathematical induction should look like. Instructions and comments are written in italics.

$\forall n \in \mathbf{Z}$, if $n \geq a$ then *some property of* n.

Proof. We will use strong mathematical induction. Let $P(n)$ be the property of integers n such that

> $P(n)$ iff *write down the property of* n *from what you are trying to prove*

(basis step) We will prove $P(a), P(a+1), \ldots, P(b)$ i.e. *write out what* $P(a), P(a+1), \ldots, P(b-1)$ *and* $P(b)$ *mean here.*

Write out a proof of $P(a), P(a+1), \ldots, P(b-1)$ *and* $P(b)$ *here*

(inductive step) Assume $n \in \mathbf{Z}$, $n > b$, and $P(i)$ holds for all integers i with $a \leq i < n$ i.e. *write out what* $P(i)$ *means here* for all integers i with $a \leq i < n$. We will show that $P(n)$ i.e. *write out what* $P(n)$ *means here.*

> *Write out a proof of* $P(n)$ *here. You can use the assumptions* $n \in \mathbf{Z}$, $n > b$, *and* $P(i)$ *for all integers* i *with* $a \leq i < n$ *(called the "inductive hypothesis").*

By strong mathematical induction, for every integer n, if $n \geq a$ then *write out* $P(n)$ *here. QED*

Notice that a will usually be a fixed integer like -1, 0, or 1, but sometimes a can be a variable or a complex expression. Also, it's up to you to determine what b should be ahead of time (in your scratchwork).

To find the value for b, try to prove the indutive step and determine the least n for which your argument "works". The smaller values of n for which it doesn't work will be $a, a+1, \ldots, b$.

$\forall n \in \mathbf{Z}$, if $n \geq$ then

Proof. We will use strong mathematical induction. Let $P(n)$ be the property of integers n such that

$P(n)$ iff

(basis step) We will prove $P(\ )$ i.e.

(inductive step) Assume $n \in \mathbf{Z}$, $n >$ and $P(i)$ holds for all integers i with $\leq i < n$ i.e.

We will show that $P(n)$ i.e.

By strong mathematical induction, for every integer n, if $n \geq$ then

QED