The Foundations: Logic and Proofs

Friday 22nd September, 2023

Outline

1. Simple Direct Proof
   - Proof w/o Quantifiers
   - Inference with Quantifiers

2. Proofs
   - Getting Started
   - Terminology
   - Direct Proofs
   - Proof by Contrapositive
   - Proof by Contradiction

Example

Convert English to Logic

Example

If Jimmy moves to Anchorage, then he will freeze in winter; but if he moves to Augusta, then he will burn up in summer. Either he will move to Anchorage or Augusta. Therefore, he will either freeze this winter or burn up next summer.

Propositions

Example

Convert English to Logic

Example

If Jimmy moves to Anchorage, then he will freeze in winter; but if he moves to Augusta, then he will burn up in summer. Either he will move to Anchorage or Augusta. Therefore, he will either freeze this winter or burn up next summer.

Propositions

a - Jimmy moves to Anchorage.

g - Jimmy moves to Augusta.

f - Jimmy freezes next winter.

b - Jimmy burns up next summer.

Example

Convert English to Logic

Example

If Jimmy moves to Anchorage, then he will freeze in winter; but if he moves to Augusta, then he will burn up in summer. Either he will move to Anchorage or Augusta. Therefore, he will either freeze this winter or burn up next summer.

Propositions

a - Jimmy moves to Anchorage.

g - Jimmy moves to Augusta.

f - Jimmy freezes next winter.

b - Jimmy burns up next summer.

Given:

$a \Rightarrow f$

$g \Rightarrow b$

$a \vee g$

Example

Convert English to Logic

Example

Propositions

a - Jimmy moves to Anchorage.

g - Jimmy moves to Augusta.

f - Jimmy freezes next winter.

b - Jimmy burns up next summer.

Given:

$a \Rightarrow f$

$g \Rightarrow b$

$a \vee g$

Prove:

$f \vee b$

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \land (g \Rightarrow b) \land (a \lor g) \Rightarrow (f \lor b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \lor g$	Premise

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \vee g$	Premise
$\neg a \Rightarrow g$	Material implication, 3

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \vee g$	Premise
$\neg a \Rightarrow g$	Material implication, 3
$\neg a \Rightarrow b$	Hypothetical Syllogism 2, 4

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \vee g$	Premise
$\neg a \Rightarrow g$	Material implication, 3
$\neg a \Rightarrow b$	Hypothetical Syllogism 2, 4
$\neg b \Rightarrow a$	Contrapositive and Double Negative 5

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \vee g$	Premise
$\neg a \Rightarrow g$	Material implication, 3
$\neg a \Rightarrow b$	Hypothetical Syllogism 2, 4
$\neg b \Rightarrow a$	Contrapositive and Double Negative 5
$\neg b \Rightarrow f$	HS 1,6

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \land (g \Rightarrow b) \land (a \lor g) \Rightarrow (f \lor b)$

Proof.

$a \Rightarrow f$	Premise
$g \Rightarrow b$	Premise
$a \lor g$	Premise
$\neg a \Rightarrow g$	Material implication, 3
$\neg a \Rightarrow b$	Hypothetical Syllogism 2, 4
$\neg b \Rightarrow a$	Contrapositive and Double Negative 5
$\neg b \Rightarrow f$	HS 1,6
$b \lor f$	MI, DN 7

Example

Proof w/o Quantifiers

To be proven: $(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$

Proof.

	$a \Rightarrow f$	Premise
	$g \Rightarrow b$	Premise
	$a \vee g$	Premise
	$\neg a \Rightarrow g$	Material implication, 3
	$\neg a \Rightarrow b$	Hypothetical Syllogism 2, 4
	$\neg b \Rightarrow a$	Contrapositive and Double Negative 5
	$\neg b \Rightarrow f$	HS 1,6
	$b \vee f$	MI, DN 7
$\therefore$	$f \vee b$	Commutation of $\vee$ 8
$\therefore$	$(a \Rightarrow f) \wedge (g \Rightarrow b) \wedge (a \vee g) \Rightarrow (f \vee b)$	

□

Fallacies

Affirming the Conclusion

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are disappointed with the subtitles in *Avatar*.
Therefore, you are a font geek.

Fallacies

Affirming the Conclusion

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are disappointed with the subtitles in *Avatar*.
Therefore, you are a font geek.
g - you are a font geek
d - you are disappointed with the subtitles
Is this a tautology?

$$((g \Rightarrow d) \land d) \Rightarrow g$$

Fallacies

Affirming the Conclusion

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are disappointed with the subtitles in *Avatar*.
Therefore, you are a font geek.
g - you are a font geek
d - you are disappointed with the subtitles
Is this a tautology?

$$((g \Rightarrow d) \wedge d) \Rightarrow g$$

No, not true for $\neg g$ and d. Exactly the case that the "proof" is wrong.

Fallacies

Denying the Hypothesis

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are not a font geek.
Therefore, you are happy with the subtitles.

Fallacies

Denying the Hypothesis

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are not a font geek.
Therefore, you are happy with the subtitles.
g - you are a font geek
d - you are disappointed with the subtitles
Is this a tautology?

$$((g \Rightarrow d) \wedge \neg g) \Rightarrow \neg d$$

Fallacies

Denying the Hypothesis

If you are a font geek, then you are disappointed with the subtitles in *Avatar*. You are not a font geek.
Therefore, you are happy with the subtitles.
g - you are a font geek
d - you are disappointed with the subtitles
Is this a tautology?

$$((g \Rightarrow d) \wedge \neg g) \Rightarrow \neg d$$

No, not true for $\neg g$ and d. Exactly the case that the "proof" is wrong.

Example: Superman

Superman [1.6 35]

Is the following argument valid?

Example

If Superman were able and willing to prevent evil, he would do so. If Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent. Superman does not prevent evil. If Superman exists, he is neither impotent nor malevolent. Therefore, Superman does not exist.

Example: Superman

Extracting the Propositions

Example

If Superman were (a)ble and (w)illing to prevent (e)vil, he would do so. If Superman were unable to prevent evil ($\neg a$), he would be (i)mpotent; if he were unwilling to prevent evil ($\neg w$), he would be (m)alevolent. Superman does not prevent evil ($\neg e$). If Superman e(x)ists, he is neither impotent nor malevolent ($\neg i \wedge \neg m$). Therefore, Superman does not exist ($\neg x$).

Example: Superman

Extracting the Propositions

Example

a - Superman is able to prevent evil
w - Superman is willing to prevent evil
e - Superman prevents evil
i - Superman is impotent
m - Superman is malevolent
x - Superman exists

Example: Superman

To Be Proven

Example

a - Superman is able to prevent evil
w - Superman is willing to prevent evil
e - Superman prevents evil
i - Superman is impotent
m - Superman is malevolent
x - Superman exists

To be proven:

$(a \land w) \Rightarrow e$	1	Premise
$\neg a \Rightarrow i$	2	Premise
$\neg w \Rightarrow m$	3	Premise
$\neg e$	4	Premise
$x \Rightarrow (\neg i \land \neg m)$	5	Premise
$\neg x$		

Example: Superman

Proof

Example

	$(a \wedge w) \Rightarrow e$	1	Premise
	$\neg a \Rightarrow i$	2	Premise
	$\neg w \Rightarrow m$	3	Premise
	$\neg e$	4	Premise
	$x \Rightarrow (\neg i \wedge \neg m)$	5	Premise
	$\neg e \Rightarrow (\neg a \vee \neg w)$	6	Contrapositive 1
	$\neg a \vee \neg w$	7	Modus Ponens 4, 6
	$a \vee i$	8	Material Implication 2
	$w \vee m$	9	MI 3
	$\neg a \vee m$	10	Resolution 7, 9
	$i \vee m$	11	Resolution 8, 10
	$\neg\neg(i \vee m)$	12	Double Negative 11
	$\neg(\neg i \wedge \neg m)$	13	DeMorgan's 12
$\therefore$	$\neg x$	14	Modus Tolens 5, 13

Example: Superman

Conclusion

Example

$$
\begin{array}{rl}
 & (a \land w) \Rightarrow e \land \\
 & \neg a \Rightarrow i \land \\
 & \neg w \Rightarrow m \land \\
 & \neg e \land \\
 & x \Rightarrow (\neg i \land \neg m) \\
\hline
\therefore & \neg x
\end{array}
$$

Inference with Quantifiers

Example

John is a lawyer. All lawyers are rich. Every person has a house. If a person is rich and they have a house, the house is big. If a person lives in a big house, they have a mortgage. Everyone with a mortgage has to work. $\therefore$ John has to work.

Inference with Quantifiers

Example

$L(p)$ - person p is a lawyer
$R(p)$ - person p is rich
$H(p, h)$ - person p owns house h
$B(h)$ - house h is big
$M(p)$ - person p has a mortgage
$W(p)$ - person p must work

Inference with Quantifiers

Example

John is a lawyer.
All lawyers are rich.
Every person has a house.
If a person is rich and they have a house, the house is big.
If a person lives in a big house, they have a mortgage.
Everyone with a mortgage has to work.

$\therefore$ John has to work.

Inference with Quantifiers

Example

$L(J)$
All lawyers are rich.
Every person has a house.
If a person is rich and they have a house, the house is big.
If a person lives in a big house, they have a mortgage.
Everyone with a mortgage has to work.

$\therefore$ John has to work.

Inference with Quantifiers

Example

$L(J)$
$\forall p \in \{\text{People}\}(L(p) \Rightarrow R(p))$
Every person has a house.
If a person is rich and they have a house, the house is big.
If a person lives in a big house, they have a mortgage.
Everyone with a mortgage has to work.

$\therefore$ John has to work.

Inference with Quantifiers

Example

$L(J)$
$\forall p \in \{\text{People}\}(L(p) \Rightarrow R(p))$
$\forall p \in \{\text{People}\}\exists h \in \{\text{Houses}\}H(p,h)$
If a person is rich and they have a house, the house is big.
If a person lives in a big house, they have a mortgage.
Everyone with a mortgage has to work.

$\therefore$ John has to work.

Inference with Quantifiers

Example

$L(J)$

$\forall p \in \{\text{People}\}(L(p) \Rightarrow R(p))$

$\forall p \in \{\text{People}\}\exists h \in \{\text{Houses}\}H(p, h)$

$\forall p \in \{\text{People}\}\forall i \in \{\text{Houses}\}(R(p) \land H(p, i) \Rightarrow B(i))$

If a person lives in a big house, they have a mortgage.

Everyone with a mortgage has to work.

$\therefore$ John has to work.

Inference with Quantifiers

Example

$$
\begin{array}{rl}
& L(J) \\
& \forall p \in \{\text{People}\}(L(p) \Rightarrow R(p)) \\
& \forall p \in \{\text{People}\}\exists h \in \{\text{Houses}\}H(p,h) \\
& \forall p \in \{\text{People}\}\forall i \in \{\text{Houses}\}(R(p) \wedge H(p,i) \Rightarrow B(i)) \\
& \forall p \in \{\text{People}\}\forall j \in \{\text{Houses}\}(H(p,j) \wedge B(j)) \Rightarrow M(p) \\
& \text{Everyone with a mortgage has to work.} \\
\hline
\therefore & \text{John has to work.}
\end{array}
$$

Inference with Quantifiers

Example

$$
\begin{array}{ll}
 & L(J) \\
 & \forall p \in \{\text{People}\}(L(p) \Rightarrow R(p)) \\
 & \forall p \in \{\text{People}\}\exists h \in \{\text{Houses}\}H(p,h) \\
 & \forall p \in \{\text{People}\}\forall i \in \{\text{Houses}\}(R(p) \wedge H(p,i) \Rightarrow B(i)) \\
 & \forall p \in \{\text{People}\}\forall j \in \{\text{Houses}\}(H(p,j) \wedge B(j)) \Rightarrow M(p) \\
 & \forall p \in \{\text{People}\}(M(p) \Rightarrow W(p)) \\
\hline
\therefore & \text{John has to work.}
\end{array}
$$

Inference with Quantifiers

Example

$$
\begin{array}{ll}
 & L(J) \\
 & \forall p \in \{\text{People}\}(L(p) \Rightarrow R(p)) \\
 & \forall p \in \{\text{People}\}\exists h \in \{\text{Houses}\}H(p,h) \\
 & \forall p \in \{\text{People}\}\forall i \in \{\text{Houses}\}(R(p) \wedge H(p,i) \Rightarrow B(i)) \\
 & \forall p \in \{\text{People}\}\forall j \in \{\text{Houses}\}(H(p,j) \wedge B(j)) \Rightarrow M(p) \\
 & \forall p \in \{\text{People}\}(M(p) \Rightarrow W(p)) \\
\hline
\therefore & \text{W(J)}
\end{array}
$$

Inference with Quantifiers

Definition (Universal Instantiation)

$$\begin{array}{rl} & \forall x P(x) \\ \hline \therefore & P(c) \text{ (for any particular } c\text{)} \end{array}$$

Inference with Quantifiers

Definition (Universal Instantiation)

$$\begin{array}{rl} & \forall x P(x) \\ \hline \therefore & P(c) \text{ (for any particular } c\text{)} \end{array}$$

Proof.

$$\begin{array}{rll} & \forall p(L(p) \Rightarrow R(p)) & \text{Premise} \\ \hline \therefore & L(J) \Rightarrow R(J) & \text{Universal Instantiation} \end{array}$$

Inference with Quantifiers

Definition (Universal Instantiation)

$$\begin{array}{rl} & \forall x P(x) \\ \hline \therefore & P(c) \text{ (for any particular } c\text{)} \end{array}$$

Proof.

$$\begin{array}{rll} & \forall p(L(p) \Rightarrow R(p)) & \text{Premise} \\ \hline \therefore & L(J) \Rightarrow R(J) & \text{Universal Instantiation} \end{array}$$

$$\begin{array}{rll} & L(J) & \text{Premise} \\ \hline \therefore & R(J) & \text{Modus Ponens with conclusion} \end{array}$$

□

Inference with Quantifiers

Definition (Existential Instantiation)

$$\begin{array}{rl} & \exists x P(x) \\ \hline \therefore & P(c) \text{ (for some element } c\text{)} \end{array}$$

Inference with Quantifiers

Definition (Existential Instantiation)

$$\begin{array}{ll} & \exists x P(x) \\ \hline \therefore & P(c) \text{ (for some element } c\text{)} \end{array}$$

Proof.

$$\begin{array}{lll} & \forall p \exists h H(p,h) & \text{Premise} \\ & \exists h H(J,h) & \text{UI} \\ \hline & H(J,Q) & \text{Existential Instantiation} \end{array}$$

□

$$\begin{array}{lll} & \forall p \forall i (R(p) \land H(p,i) \Rightarrow B(i)) & \\ & R(J) \land H(J,Q) \Rightarrow B(Q) & 2 \times \text{UI} \\ \hline \therefore & B(Q) & \end{array}$$

Inference with Quantifiers

Proof.

$L(J)$	1
$\forall p(L(p) \Rightarrow R(p))$	2
$\forall p \exists h H(p,h)$	3
$\forall p \forall i(R(p) \wedge H(p,i) \Rightarrow B(i))$	4
$\forall p \forall j(H(p,j) \wedge B(j)) \Rightarrow M(p)$	5
$\forall p(M(p) \Rightarrow W(p))$	6

Inference with Quantifiers

Proof.

$L(J)$	1	
$\forall p(L(p) \Rightarrow R(p))$	2	
$\forall p \exists h H(p, h)$	3	
$\forall p \forall i(R(p) \wedge H(p, i) \Rightarrow B(i))$	4	
$\forall p \forall j(H(p, j) \wedge B(j)) \Rightarrow M(p)$	5	
$\forall p(M(p) \Rightarrow W(p))$	6	
$L(J) \Rightarrow R(J)$	7	Univ Instan 2

Inference with Quantifiers

Proof.

$L(J)$	1	
$\forall p(L(p) \Rightarrow R(p))$	2	
$\forall p \exists h H(p,h)$	3	
$\forall p \forall i(R(p) \wedge H(p,i) \Rightarrow B(i))$	4	
$\forall p \forall j(H(p,j) \wedge B(j)) \Rightarrow M(p)$	5	
$\forall p(M(p) \Rightarrow W(p))$	6	
$L(J) \Rightarrow R(J)$	7	Univ Instan 2
$R(J)$	8	MP 1, 7

Inference with Quantifiers

Proof.

$L(J)$	1	
$\forall p(L(p) \Rightarrow R(p))$	2	
$\forall p \exists h H(p, h)$	3	
$\forall p \forall i(R(p) \wedge H(p, i) \Rightarrow B(i))$	4	
$\forall p \forall j(H(p, j) \wedge B(j)) \Rightarrow M(p)$	5	
$\forall p(M(p) \Rightarrow W(p))$	6	
$L(J) \Rightarrow R(J)$	7	Univ Instan 2
$R(J)$	8	MP 1, 7
$H(J, Q)$	9	Exist Instan 3

Inference with Quantifiers

Proof.

$L(J)$	1	
$\forall p(L(p) \Rightarrow R(p))$	2	
$\forall p \exists h H(p, h)$	3	
$\forall p \forall i(R(p) \land H(p, i) \Rightarrow B(i))$	4	
$\forall p \forall j(H(p, j) \land B(j)) \Rightarrow M(p)$	5	
$\forall p(M(p) \Rightarrow W(p))$	6	
$L(J) \Rightarrow R(J)$	7	Univ Instan 2
$R(J)$	8	MP 1, 7
$H(J, Q)$	9	Exist Instan 3
$B(Q)$	10	UI + MP 8, 9 and 4

Inference with Quantifiers

Proof.

$L(J)$	1	
$\forall p(L(p) \Rightarrow R(p))$	2	
$\forall p \exists h H(p,h)$	3	
$\forall p \forall i(R(p) \land H(p,i) \Rightarrow B(i))$	4	
$\forall p \forall j(H(p,j) \land B(j)) \Rightarrow M(p)$	5	
$\forall p(M(p) \Rightarrow W(p))$	6	
$L(J) \Rightarrow R(J)$	7	Univ Instan 2
$R(J)$	8	MP 1, 7
$H(J,Q)$	9	Exist Instan 3
$B(Q)$	10	UI + MP 8, 9 and 4
$M(J)$	11	UI + MP 9, 10, and 5

Inference with Quantifiers

Proof.

	$L(J)$	1	
	$\forall p(L(p) \Rightarrow R(p))$	2	
	$\forall p \exists h H(p,h)$	3	
	$\forall p \forall i(R(p) \wedge H(p,i) \Rightarrow B(i))$	4	
	$\forall p \forall j(H(p,j) \wedge B(j)) \Rightarrow M(p)$	5	
	$\forall p(M(p) \Rightarrow W(p))$	6	
	$L(J) \Rightarrow R(J)$	7	Univ Instan 2
	$R(J)$	8	MP 1, 7
	$H(J,Q)$	9	Exist Instan 3
	$B(Q)$	10	UI + MP 8, 9 and 4
	$M(J)$	11	UI + MP 9, 10, and 5
$\therefore$	$W(J)$		UI + MP 11, 6

□

Inference with Quantifiers

Table

Rule of Inference	*Name*
$\dfrac{\forall x P(x)}{\therefore\; P(c) \text{ (for any } c\text{)}}$	Universal Instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\; \forall x P(x)}$	Universal Generalization
$\dfrac{\exists x P(x)}{\therefore\; P(c) \text{ (for some element } c\text{)}}$	Existential Instantiation
$\dfrac{P(c) \text{ for some } c}{\therefore\; \exists x P(x)}$	Existential Generalization

Transitivity of Implication

Poof

Justify the rule of **universal transitivity**, which states that if $\forall x(P(x) \Rightarrow Q(x))$ and $\forall x(Q(x) \Rightarrow R(x))$ are true, then $\forall x(P(x) \Rightarrow R(x))$ is true, where the domains of all quantifiers are the same.

Transitivity of Implication

Poof

Justify the rule of **universal transitivity**, which states that if $\forall x(P(x) \Rightarrow Q(x))$ and $\forall x(Q(x) \Rightarrow R(x))$ are true, then $\forall x(P(x) \Rightarrow R(x))$ is true, where the domains of all quantifiers are the same.

To be proven: $(\forall x(P(x) \Rightarrow Q(x)) \wedge \forall(Q(x) \Rightarrow R(x))) \Rightarrow \forall x(P(x) \Rightarrow R(x))$

	$\forall x(P(x) \Rightarrow Q(x))$	1	Premise
	$P(c) \Rightarrow Q(c)$ for arbitrary c	2	UI 1
	$\forall x(Q(x) \Rightarrow R(x))$	3	Premise
	$Q(c) \Rightarrow R(c)$ for same c	4	UI 3
	$P(c) \Rightarrow R(c)$	5	HS 2, 4
$\therefore$	$\forall x(P(x) \Rightarrow R(x))$	6	U Gen 5

$\therefore (\forall x(P(x) \Rightarrow Q(x)) \wedge \forall(Q(x) \Rightarrow R(x))) \Rightarrow \forall x(P(x) \Rightarrow R(x))$

Proofs

Terminology

Definitions

A theorem

A premise

A proof
An axiom

A lemma

Proofs

Terminology

Definitions

A **theorem** is a statement that can be proved to be true. Synonyms: **proposition**, **fact**, **result**

A premise

A proof

An axiom

A lemma

Proofs

Terminology

Definitions

A theorem is a statement that can be proved to be true. Synonyms: proposition, fact, result

A **premise** is a proposition given as true as part of the statement of a theorem. Synonyms: **given**

A proof

An axiom

A lemma

Proofs

Terminology

Definitions

A theorem is a statement that can be proved to be true. Synonyms: proposition, fact, result

A premise is a proposition given as true as part of the statement of a theorem. Synonyms: given

A **proof** is a valid argument that establishes the truth of a theorem.

An axiom

A lemma

Proofs

Terminology

Definitions

A theorem is a statement that can be proved to be true. Synonyms: proposition, fact, result

A premise is a proposition given as true as part of the statement of a theorem. Synonyms: given

A proof is a valid argument that establishes the truth of a theorem.

An **axiom** is a statement that is assumed to be true; used for definitional conditions of mathematics. Synonyms: **postulate**

A lemma

Proofs

Terminology

Definitions

A theorem is a statement that can be proved to be true. Synonyms: proposition, fact, result

A premise is a proposition given as true as part of the statement of a theorem. Synonyms: given

A proof is a valid argument that establishes the truth of a theorem.

An axiom is a statement that is assumed to be true; used for definitional conditions of mathematics. Synonyms: postulate

A **lemma** is a less important proof useful in proving other results (typically not interesting on its own).

Proofs

More Terminology

Definitions

A corollary

A conjecture

Proofs

More Terminology

Definitions

A **corollary** is a theorem that can be established directly from the theorem just proved.

A conjecture

Proofs

More Terminology

Definitions

A corollary is a theorem that can be established directly from the theorem just proved.

A **conjecture** is a statement that is **proposed** to be true but which lacks a valid proof.

Formatting

How Proofs are Stated

Remember: **All** proofs begin with a statement of what is being proved and end by concluding that that thing has been proved:

Proof.
To be proved: $\forall x \in D \forall y \in D\ P_1(x) \wedge P_2(x) \ldots P_n(x) \Rightarrow Q(x)$
<Proof of statement goes here>
$\therefore \forall x \in D \forall y \in D\ P_1(x) \wedge P_2(x) \ldots P_n(x) \Rightarrow Q(x)$

□

Formatting

How Proofs are Stated

Example

If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$.

What does this really mean?

Formatting

How Proofs are Stated

Example

If $x > y$, *where* x *and* y *are positive real numbers, then* $x^2 > y^2$.

What does this really mean?

For all positive real numbers x *and* y, *if* $x > y$, *then* $x^2 > y^2$.

Or, in logical notation

Formatting

How Proofs are Stated

Example

If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$.

What does this really mean?

For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$.

Or, in logical notation

$$\forall x \forall y \; x, y \in \mathbb{R}^+ (x > y) \Rightarrow (x^2 > y^2)$$

Definition

Definition (Direct Proof)
A proof of $p \Rightarrow q$ where p is given to be true and a sequence of logical steps leads to q being equivalently true.

Theorem
Every odd integer is the difference of two squares.
Which means:

Definition

Definition (Direct Proof)

A proof of $p \Rightarrow q$ where p is given to be true and a sequence of logical steps leads to q being equivalently true.

Theorem

Every odd integer is the difference of two squares.

Which means:

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z} \ni n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z} \ni n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI
$\exists y \in \mathbb{Z} \ni x = (2y + 1)$	3	Definition of *odd*

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z} \ni n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z} \ni n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI
$\exists y \in \mathbb{Z} \ni x = (2y + 1)$	3	Definition of *odd*
$x = (2y + 1)$	3	Existential Inst.

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI
$\exists y \in \mathbb{Z} \ni x = (2y + 1)$	3	Definition of *odd*
$x = (2y + 1)$	3	Existential Inst.
$y^2 = y^2$	4	Definition of =

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI
$\exists y \in \mathbb{Z} \ni x = (2y + 1)$	3	Definition of *odd*
$x = (2y + 1)$	3	Existential Inst.
$y^2 = y^2$	4	Definition of =
$y^2 + x = y^2 + 2y + 1$	5	Sub equality 4 - 3

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

$\forall n\ odd(n)$	1	Premise
$odd(x)$	2	UI
$\exists y \in \mathbb{Z} \ni x = (2y + 1)$	3	Definition of *odd*
$x = (2y + 1)$	3	Existential Inst.
$y^2 = y^2$	4	Definition of =
$y^2 + x = y^2 + 2y + 1$	5	Sub equality 4 - 3
$y^2 + x = (y + 1)^2$	6	Factoring

Difference of Squares

Two-column Proof

Theorem

Every odd integer is the difference of two squares.

$\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$

	$\forall n\ odd(n)$	1	Premise
	$odd(x)$	2	UI
	$\exists y \in \mathbb{Z} \ni x = (2y+1)$	3	Definition of *odd*
	$x = (2y+1)$	3	Existential Inst.
	$y^2 = y^2$	4	Definition of =
	$y^2 + x = y^2 + 2y + 1$	5	Sub equality 4 - 3
	$y^2 + x = (y+1)^2$	6	Factoring
$\therefore$	$x = (y+1)^2 - y^2$	7	Subtract equality
$\therefore$	$\forall n\ odd(n) \Rightarrow \exists a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \ni\ n = a^2 - b^2$	8	Generalization

□

Defining

Proof by Contraposition

Definition (Proof by Contrapositive)
Assume the **negation** of the conclusion as given; prove, “directly,” that the **negation** of the hypothesis follows.

Defining

Proof by Contraposition

Definition (Proof by Contrapositive)
Assume the negation of the conclusion as given; prove, “directly,” that the negation of the hypothesis follows.

Theorem
If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n} \vee b \leq \sqrt{n}$
Which means:

Defining

Proof by Contraposition

Definition (Proof by Contrapositive)
Assume the negation of the conclusion as given; prove, "directly," that the negation of the hypothesis follows.

Theorem
If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n} \vee b \leq \sqrt{n}$
Which means:
$\forall a \forall b \; a, b \in \mathbb{Z}^{+} \; let \; n = ab \; a \leq \sqrt{n} \vee b \leq \sqrt{n}$

Working Out the Contrapositive

Getting "To be proved"

Theorem

For any two positive integers, at least one of them is less than or equal to the square root of their product. $\forall a \forall b\ a, b \in \mathbb{Z}^+$ let $n = ab\ a \leq \sqrt{n} \vee b \leq \sqrt{n}$

Contrapositive:

Working Out the Contrapositive

Getting "To be proved"

Theorem

For any two positive integers, at least one of them is less than or equal to the square root of their product. $\forall a \forall b \; a, b \in \mathbb{Z}^+$ let $n = ab$ $a \leq \sqrt{n} \vee b \leq \sqrt{n}$

Contrapositive:

$\forall a \forall b \; a, b \in \mathbb{Z}^+$ *if* $\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n})$ *then* $\neg(n = ab)$

Working Out the Contrapositive

Getting "To be proved"

Theorem

For any two positive integers, at least one of them is less than or equal to the square root of their product. $\forall a \forall b\ a, b \in \mathbb{Z}^+$ let $n = ab\ a \leq \sqrt{n} \lor b \leq \sqrt{n}$

Contrapositive:

$\forall a \forall b\ a, b \in \mathbb{Z}^+$ *if* $\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n})$ *then* $\neg(n = ab)$

$\forall a \forall b\ a, b \in \mathbb{Z}^+$ *if* $a > \sqrt{n} \land b > \sqrt{n}$ *then* $n \neq ab$

Factor above/below $\sqrt{product}$

Two-column Proof

Proof.

To be proven: $\forall a \forall b \; a, b \in \mathbb{Z}^+$ let $n = ab \; a \leq \sqrt{n} \vee b \leq \sqrt{n}$

Proof proceeds by *contrapositive*

Contrapositive: $\forall a \forall b \; a, b \in \mathbb{Z}^+$ let $n = ab \; (a > \sqrt{n} \wedge b > \sqrt{n}) \Rightarrow n \neq ab$

$a > \sqrt{n}$	1	Premise and simplification
$b > \sqrt{n}$	2	Premise and simplification
$ab > n$	3	Positive Product of Inequality 1, 2
$ab \neq n$	4	Defn. of =, 3

$\therefore (a > \sqrt{n} \wedge b > \sqrt{n}) \Rightarrow n \neq$

ab

$\therefore \forall a \forall b \; a, b \in \mathbb{Z}^+ \; (a > \sqrt{n} \wedge b > \sqrt{n}) \Rightarrow n \neq ab$

$\therefore \forall a \forall b \; a, b \in \mathbb{Z}^+$ let $n = ab \; a \leq \sqrt{n} \vee b \leq \sqrt{n}$ □

Defining

Proof by Contradiction

Definition (Proof by Contradiction)

Assume we want to prove q true. If $\exists r$ such that r is a contradiction and we can show $\neg q \Rightarrow r$ then it follows that $\neg q$ must be false Why?

Defining

Proof by Contradiction

Definition (Proof by Contradiction)

Assume we want to prove q true. If $\exists r$ such that r is a contradiction and we can show $\neg q \Rightarrow r$ then it follows that $\neg q$ must be **false**

If $\neg q$ is *false*, q is **true** and we have proved our statement.

Diversion I: Definitions

Rational

Definition

A real number, q is **rational** if it can be written as a **ratio** (fraction) of two integers:

$q \in \mathbb{Q}$ if $\exists n \; \exists d \; n, d \in \mathbb{Z} \; d \neq 0 \; q = \frac{n}{d}$

Diversion I: Definitions

Rational

Definition

A real number, q is rational if it can be written as a ratio (fraction) of two integers: $q \in \mathbb{Q}$ if $\exists n\ \exists d\ n, d \in \mathbb{Z}\ d \neq 0\ q = \frac{n}{d}$

A real number r is **irrational** if it is not rational: $\neg(\exists n\ \exists d\ n, d \in \mathbb{Z}\ d \neq 0\ r = \frac{n}{d})$

Diversion II: A Lemma

Even squares come from even numbers

Lemma

$\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof by contrapositive

Contrapositive: $\forall n \in \mathbb{Z}\ 2 \nmid n \Rightarrow 2 \nmid n^2$

Diversion II: A Lemma

Even squares come from even numbers

Lemma

$\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof by contrapositive

Contrapositive: $\forall n \in \mathbb{Z}\ 2 \not| n \Rightarrow 2 \not| n^2$

Equivalently: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow odd(n^2)$

Diversion II: A Lemma

Even squares come from even numbers

Lemma

$\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof.

To be proven: $\forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

Proof by contrapositive

Contrapositive: $\forall n \in \mathbb{Z}\ 2 \not| n \Rightarrow 2 \not| n^2$

Equivalently: $\forall n \in \mathbb{Z}\ odd(n) \Rightarrow odd(n^2)$

	$odd(n)$	1	UI, Premise
	$\exists k \in \mathbb{Z} \vert n = 2k+1$	2	Defn. odd
	$n^2 = (2k+1)^2$	3	Substitution
	$n^2 = 4k^2 + 4k + 1 = 2(2k^2+2k)+1$	4	Algebra, 3
	$\exists j \in \mathbb{Z} \vert n^2 = 2j+1$	5	EG, 4
$\therefore$	$odd(n^2)$	6	Defn odd

$\therefore \forall n \in \mathbb{Z}\ odd(n) \Rightarrow odd(n^2)$

$\therefore \forall n \in \mathbb{Z}\ 2|n^2 \Rightarrow 2|n$

□

Irrational Square Root

Starting the Proof

Theorem

$\sqrt{2}$ is irrational.

Irrational Square Root

Starting the Proof

Theorem
$\sqrt{2}$ is irrational.

Proof.
To be proven: $\sqrt{2}$ is irrational.
Proof is by *contradiction*
For Sake of Contradiction: Assume $\neg(\sqrt{2}$ is irrational$)$
or

Irrational Square Root

Starting the Proof

Theorem

$\sqrt{2}$ is irrational.

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

For Sake of Contradiction: Assume $\neg(\sqrt{2} \text{ is irrational})$

or $\sqrt{2}$ is rational □

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$
$2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$	3	Square both sides

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$
$2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$	3	Square both sides
$even(a)$	4	$even(x^2) \Rightarrow even(x)$
$a = 2c$ thus $2b^2 = 4c^2$	5	Defn *even*

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$
$2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$	3	Square both sides
$even(a)$	4	$even(x^2) \Rightarrow even(x)$
$a = 2c$ thus $2b^2 = 4c^2$	5	Defn *even*
$b^2 = 2c^2$; $even(b)$	6	Algebra and as (4)

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$
$2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$	3	Square both sides
$even(a)$	4	$even(x^2) \Rightarrow even(x)$
$a = 2c$ thus $2b^2 = 4c^2$	5	Defn *even*
$b^2 = 2c^2$; $even(b)$	6	Algebra and as (4)
$2 \mid a \wedge 2 \mid b$	7	Defn divisibility
$\neg lowest(\frac{a}{b})$	8	Defn lowest terms

Irrational Square Root

Two-column Proof

Proof.

To be proven: $\sqrt{2}$ is irrational.

Proof is by *contradiction*

FSOC: $\sqrt{2}$ is rational

$\sqrt{2}$ is rational	1	Assumption
$\sqrt{2} = \frac{a}{b}$	2	Defn rational without loss of generality, $lowest(\frac{a}{b})$
$2 = \frac{a^2}{b^2}$ and $2b^2 = a^2$	3	Square both sides
$even(a)$	4	$even(x^2) \Rightarrow even(x)$
$a = 2c$ thus $2b^2 = 4c^2$	5	Defn *even*
$b^2 = 2c^2$; $even(b)$	6	Algebra and as (4)
$2 \mid a \wedge 2 \mid b$	7	Defn divisibility
$\neg lowest(\frac{a}{b})$	8	Defn lowest terms
$\neg(\sqrt{2}$ is rational$)$	9	Contradiction 2,8

$\therefore$ $\sqrt{2}$ is irrational

Proof by Contradiction

Your Turn

Prove that if you pick three marbles from an urn containing only black and white marbles, you must have a pair of white marbles or a pair of black marbles.