Foundation of proofs

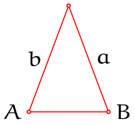
Jim Hefferon

http://joshua.smcvt.edu/proofs

The need to prove

In Mathematics we prove things

To a person with a mathematical turn of mind, 'the base angles of an isoceles triangle are equal' seems obvious.

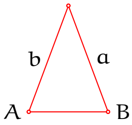


if $a \cong b$ then $\angle A \cong \angle B$

Another example that comes naturally to someone with aptitude is, 'each positive integer factors into a product of primes'.

In Mathematics we prove things

To a person with a mathematical turn of mind, 'the base angles of an isoceles triangle are equal' seems obvious.



if $a \cong b$ then $\angle A \cong \angle B$

Another example that comes naturally to someone with aptitude is, 'each positive integer factors into a product of primes'.

But what about: 'in a right triangle the square of the length of the hypoteneuse is equal to the sum of the squares of the other two sides'? Is that obvious, or does it require justification?

A characteristic of our subject is that we are completely sure of new results because we show that they follow logically from things we've already established.

Convincing is not enough

These assertions seem convincing but turn out to be false.

Convincing is not enough

These assertions seem convincing but turn out to be false.

- The polynomial $n^2 + n + 41$ appears to outputs only primes.

n	0	1	2	3	4	5	6	7
$n^2 + n + 41$	41	43	47	53	61	71	83	97

Convincing is not enough

These assertions seem convincing but turn out to be false.

- The polynomial $n^2 + n + 41$ appears to outputs only primes.

n	0	1	2	3	4	5	6	7
$n^2 + n + 41$	41	43	47	53	61	71	83	97

  However, that pattern eventually fails: for $n = 41$ the output $41^2 + 41 + 41$ is divisible by 41.

Convincing is not enough

These assertions seem convincing but turn out to be false.

- The polynomial $n^2 + n + 41$ appears to outputs only primes.

n	0	1	2	3	4	5	6	7
$n^2 + n + 41$	41	43	47	53	61	71	83	97

  However, that pattern eventually fails: for $n = 41$ the output $41^2 + 41 + 41$ is divisible by 41.

- When decomposed, $18 = 2^1 \cdot 3^2$ has an odd number of prime factors ($1 + 2$ of them), while $24 = 2^3 \cdot 3^1$ has an even number ($3 + 1$ of them). We say that 18 is of *odd* type while 24 is of *even* type.

n	1	2	3	4	5	6	7	8	9
type	even	odd	odd	even	odd	even	odd	odd	even

  Pòlya conjectured that for any $n > 1$, the even types below it never outnumber the odd types.

Convincing is not enough

These assertions seem convincing but turn out to be false.

- The polynomial $n^2 + n + 41$ appears to outputs only primes.

n	0	1	2	3	4	5	6	7
$n^2 + n + 41$	41	43	47	53	61	71	83	97

  However, that pattern eventually fails: for $n = 41$ the output $41^2 + 41 + 41$ is divisible by 41.

- When decomposed, $18 = 2^1 \cdot 3^2$ has an odd number of prime factors ($1 + 2$ of them), while $24 = 2^3 \cdot 3^1$ has an even number ($3 + 1$ of them). We say that 18 is of *odd* type while 24 is of *even* type.

n	1	2	3	4	5	6	7	8	9
type	even	odd	odd	even	odd	even	odd	odd	even

  Pòlya conjectured that for any $n > 1$, the even types below it never outnumber the odd types. The first counterexample is $906\,150\,257$.

Elements of logic

Propositions

A proposition is an assertion that has a truth value, either 'true' or 'false'.

Propositions

A proposition is an assertion that has a truth value, either ‘true’ or ‘false’.

These are propositions: ‘$2 + 2 = 4$’ and ‘Two circles in the plane intersect in either zero points, one point, two points, or all of their points.’

Propositions

A proposition is an assertion that has a truth value, either 'true' or 'false'.

These are propositions: '$2 + 2 = 4$' and 'Two circles in the plane intersect in either zero points, one point, two points, or all of their points.'

These are not propositions: '$3 + 5$' and 'x is not prime'.

Negation

Prefixing a proposition with not inverts its truth value.

The statement ‘it is not the case that $3 + 3 = 5$’ is true, while ‘it is not the case that $3 + 3 = 6$’ is false.

Negation

Prefixing a proposition with not inverts its truth value.

The statement ‘it is not the case that $3 + 3 = 5$’ is true, while ‘it is not the case that $3 + 3 = 6$’ is false.

So the truth value of ‘not P’ depends only on the truth of P.

Conjunction, disjunction

A proposition consisting of the word and between two sub-propositions is true if the two halves are true.

'$3 + 1 = 4$ and $3 - 1 = 2$' is true

'$3 + 1 = 4$ and $3 - 1 = 1$' is false

'$3 + 1 = 5$ and $3 - 1 = 2$' is false

Conjunction, disjunction

A proposition consisting of the word and between two sub-propositions is true if the two halves are true.

'$3 + 1 = 4$ and $3 - 1 = 2$' is true

'$3 + 1 = 4$ and $3 - 1 = 1$' is false

'$3 + 1 = 5$ and $3 - 1 = 2$' is false

A compound proposition constructed with or between two sub-propositions is true if at least one half is true.

'$2 \cdot 2 = 4$ or $2 \cdot 2 \neq 4$' is true

'$2 \cdot 2 = 3$ or $2 \cdot 2 \neq 4$' is false

'$2 \cdot 2 = 4$ or $3 + 1 = 4$' is true

Truth Tables

Write $\neg P$ for 'not P', $P \wedge Q$ for 'P and Q', and $P \vee Q$ for 'P or Q'. We can describe the action of these operators using truth tables.

P	$\neg P$
F	T
T	F

P	Q	$P \wedge Q$	$P \vee Q$
F	F	F	F
F	T	F	T
T	F	F	T
T	T	T	T

Truth Tables

Write $\neg P$ for 'not P', $P \wedge Q$ for 'P and Q', and $P \vee Q$ for 'P or Q'. We can describe the action of these operators using truth tables.

P	$\neg P$
F	T
T	F

P	Q	$P \wedge Q$	$P \vee Q$
F	F	F	F
F	T	F	T
T	F	F	T
T	T	T	T

One advantage of this notation is that it allows formulas more complex than you could say in a natural language. For instance, $(P \vee Q) \wedge \neg(P \wedge Q)$ is hard to express in English.

Another advantage is that a natural language such as English has ambiguities but a formal language does not.

Exclusive or

Disjunction models sentences meaning ‘and/or’ such as ‘sweep the floor or do the laundry’. We would say that someone who has done both has satisfied the admonition.

In contrast, ‘Eat your dinner or no dessert’, and ‘Give me the money or the hostage gets it’, and ‘Live free or die’, all mean one or the other, but not both.

P	Q	P XOR Q
F	F	F
F	T	T
T	F	T
T	T	F

Implication

We model 'if P then Q' this way.

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

(We will speak to some subtle aspects of this definition below.) Here, P is the antecedent while Q is the consequent.

Bi-implication

We take 'P if and only if Q' to mean the two have the same values, 'a number n is divisible by 5' if and only if 'the number n ends in 0 or 5'.

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Mathematicians often write 'iff'.

All binary operators

We can list all of the binary logical functions.

P	Q	$P\ \alpha_0\ Q$
F	F	F
F	T	F
T	F	F
T	T	F

P	Q	$P\ \alpha_1\ Q$
F	F	F
F	T	F
T	F	F
T	T	T

$\ldots$

P	Q	$P\ \alpha_{15}\ Q$
F	F	T
F	T	T
T	F	T
T	T	T

All binary operators

We can list all of the binary logical functions.

P	Q	$P\ \alpha_0\ Q$
F	F	F
F	T	F
T	F	F
T	T	F

P	Q	$P\ \alpha_1\ Q$
F	F	F
F	T	F
T	F	F
T	T	T

$\ldots$

P	Q	$P\ \alpha_{15}\ Q$
F	F	T
F	T	T
T	F	T
T	T	T

These are the unary ones.

P	$\beta_0 P$
F	F
T	F

P	$\beta_1 P$
F	F
T	T

P	$\beta_2 P$
F	T
T	F

P	$\beta_3 P$
F	T
T	T

All binary operators

We can list all of the binary logical functions.

P	Q	$P\ \alpha_0\ Q$
F	F	F
F	T	F
T	F	F
T	T	F

P	Q	$P\ \alpha_1\ Q$
F	F	F
F	T	F
T	F	F
T	T	T

$\ldots$

P	Q	$P\ \alpha_{15}\ Q$
F	F	T
F	T	T
T	F	T
T	T	T

These are the unary ones.

P	$\beta_0 P$
F	F
T	F

P	$\beta_1 P$
F	F
T	T

P	$\beta_2 P$
F	T
T	F

P	$\beta_3 P$
F	T
T	T

A zero-ary operator is constant so there are two: T and F.

Evaluating complex statements

No matter how intricate the propositional logic sentence, with patience we can calculate how the output truth values depend on the inputs. Here is the work for $(P \to Q) \land (P \to R)$.

P	Q	R	$P \to Q$	$P \to R$	$(P \to Q) \land (P \to R)$
F	F	F	T	T	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	T	T
T	F	F	F	F	F
T	F	T	F	T	F
T	T	F	T	F	F
T	T	T	T	T	T

The calculation decomposes the statement into its components $P \to Q$, etc., and then builds the truth table up from the simpler components.

Tautology, Satisfiability, Equivalence

A formula is a tautology if it evaluates to T for every value of the variables. A formula is satisfiable if it evaluates to T for at least one value of the variables.

Tautology, Satisfiability, Equivalence

A formula is a tautology if it evaluates to T for every value of the variables. A formula is satisfiable if it evaluates to T for at least one value of the variables.

Two propositional expressions are logically equivalent if they have the same final column in their truth tables. For instance, $P \wedge Q$ and $Q \wedge P$ are equivalent.

Tautology, Satisfiability, Equivalence

A formula is a tautology if it evaluates to T for every value of the variables. A formula is satisfiable if it evaluates to T for at least one value of the variables.

Two propositional expressions are logically equivalent if they have the same final column in their truth tables. For instance, $P \wedge Q$ and $Q \wedge P$ are equivalent.

An important example is that $P \to Q$ and $\neg Q \to \neg P$ are equivalent.

P	Q	$P \to Q$	$\neg Q$	$\neg P$	$\neg Q \to \neg P$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	T	F	F	T

Discussion: our definition of 'implies'

For $P \to Q$ everyone expects when P is true then Q will follow, so that if P is T but Q is F then the statement as a whole is F. What about the other cases?

P	Q	$P \to Q$
F	F	
F	T	
T	F	F
T	T	

Standard mathematical practice defines implication so that, for instance, this statement is true for all real numbers:

if x is rational then x^2 is rational

(because $x = p/q$ gives $x^2 = p^2/q^2$).

Discussion: our definition of 'implies'

For $P \to Q$ everyone expects when P is true then Q will follow, so that if P is T but Q is F then the statement as a whole is F. What about the other cases?

P	Q	$P \to Q$
F	F	
F	T	T
T	F	F
T	T	

Standard mathematical practice defines implication so that, for instance, this statement is true for all real numbers:

if x is rational then x^2 is rational

(because $x = p/q$ gives $x^2 = p^2/q^2$). Taking $x = \sqrt{2}$ shows that we need $F \to T$ to evaluate to T.

Discussion: our definition of ‘implies’

For $P \to Q$ everyone expects when P is true then Q will follow, so that if P is T but Q is F then the statement as a whole is F. What about the other cases?

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	

Standard mathematical practice defines implication so that, for instance, this statement is true for all real numbers:

if x is rational then x^2 is rational

(because $x = p/q$ gives $x^2 = p^2/q^2$). Taking $x = \sqrt{2}$ shows that we need $F \to T$ to evaluate to T. Take $x = \pi$ to see that we need $F \to F$ to yield T.

Discussion: our definition of ‘implies’

For $P \to Q$ everyone expects when P is true then Q will follow, so that if P is T but Q is F then the statement as a whole is F. What about the other cases?

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

Standard mathematical practice defines implication so that, for instance, this statement is true for all real numbers:

if x is rational then x^2 is rational

(because $x = p/q$ gives $x^2 = p^2/q^2$). Taking $x = \sqrt{2}$ shows that we need $F \to T$ to evaluate to T. Take $x = \pi$ to see that we need $F \to F$ to yield T. For $T \to T$ take $x = 1/2$.

Discussion: our definition of 'implies'

For $P \to Q$ everyone expects when P is true then Q will follow, so that if P is T but Q is F then the statement as a whole is F. What about the other cases?

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

Standard mathematical practice defines implication so that, for instance, this statement is true for all real numbers:

$$\text{if } x \text{ is rational then } x^2 \text{ is rational}$$

(because $x = p/q$ gives $x^2 = p^2/q^2$). Taking $x = \sqrt{2}$ shows that we need $F \to T$ to evaluate to T. Take $x = \pi$ to see that we need $F \to F$ to yield T. For $T \to T$ take $x = 1/2$.

The intuition is that $P \to Q$ is a promise that if P holds then Q must hold also. If P doesn't hold, that is not a counterexample to the promise. If Q does hold, that is also not a counterexample.

Points about implication

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

- If the antecedent P is false then the statement as a whole is true, said to be vacuously true. If the consequent Q is true then the statement as a whole is true.

Points about implication

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

- If the antecedent P is false then the statement as a whole is true, said to be vacuously true. If the consequent Q is true then the statement as a whole is true.
- Thus, we take 'if Babe Ruth was president then $1 + 2 = 4$' to be true, vacuously true. Similarly, we take 'if Mallory reached the summit of Everest then $1 + 2 = 3$' to be true.

Points about implication

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

- If the antecedent P is false then the statement as a whole is true, said to be vacuously true. If the consequent Q is true then the statement as a whole is true.
- Thus, we take 'if Babe Ruth was president then $1 + 2 = 4$' to be true, vacuously true. Similarly, we take 'if Mallory reached the summit of Everest then $1 + 2 = 3$' to be true.
- In particular, our definition does not require that the antecedent P causes, or is in any way connected to, the consequent Q.

Points about implication

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

- If the antecedent P is false then the statement as a whole is true, said to be vacuously true. If the consequent Q is true then the statement as a whole is true.
- Thus, we take 'if Babe Ruth was president then $1 + 2 = 4$' to be true, vacuously true. Similarly, we take 'if Mallory reached the summit of Everest then $1 + 2 = 3$' to be true.
- In particular, our definition does not require that the antecedent P causes, or is in any way connected to, the consequent Q.

Points about implication

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

- If the antecedent P is false then the statement as a whole is true, said to be vacuously true. If the consequent Q is true then the statement as a whole is true.
- Thus, we take 'if Babe Ruth was president then $1 + 2 = 4$' to be true, vacuously true. Similarly, we take 'if Mallory reached the summit of Everest then $1 + 2 = 3$' to be true.
- In particular, our definition does not require that the antecedent P causes, or is in any way connected to, the consequent Q.
- Truth tables show that $P \to Q$ is logically equivalent to $\neg(P \wedge \neg Q)$, to $\neg P \vee Q$, and also to the contrapositive $\neg Q \to \neg P$.

Predicates, Quantifiers; complete statements

Here is a typical mathematical statement (it happens to be false).

$$\text{If } n \text{ is odd then } n \text{ is a perfect square.} \qquad (*)$$

It involves two clauses, 'n is odd' and 'n is square'. For each, the truth value depend on the variable n.

Predicates, Quantifiers; complete statements

Here is a typical mathematical statement (it happens to be false).

$$\text{If } n \text{ is odd then } n \text{ is a perfect square.} \tag{$*$}$$

It involves two clauses, 'n is odd' and 'n is square'. For each, the truth value depend on the variable n.

A predicate is a truth-valued function. An example is the function *Odd* that takes an integer as input and yields either T or F, as in *Odd*$(5) = T$. Another example is *Square*, as in *Square*$(5) = F$, that tells if the input is a perfect square.

Predicates, Quantifiers; complete statements

Here is a typical mathematical statement (it happens to be false).

$$\text{If } n \text{ is odd then } n \text{ is a perfect square.} \tag{$*$}$$

It involves two clauses, 'n is odd' and 'n is square'. For each, the truth value depend on the variable n.

A predicate is a truth-valued function. An example is the function *Odd* that takes an integer as input and yields either T or F, as in *Odd*$(5) = T$. Another example is *Square*, as in *Square*$(5) = F$, that tells if the input is a perfect square.

A mathematician saying $(*)$ would mean that it holds for all n. We denote 'for all' by the symbol $\forall$, so the statement is written formally $\forall n \in \mathbb{N}\big[\mathit{Odd}(n) \rightarrow \mathit{Square}(n)\big]$.

Predicates, Quantifiers; complete statements

Here is a typical mathematical statement (it happens to be false).

If n is odd then n is a perfect square. $(*)$

It involves two clauses, 'n is odd' and 'n is square'. For each, the truth value depend on the variable n.

A predicate is a truth-valued function. An example is the function *Odd* that takes an integer as input and yields either T or F, as in *Odd*$(5) = T$. Another example is *Square*, as in *Square*$(5) = F$, that tells if the input is a perfect square.

A mathematician saying $(*)$ would mean that it holds for all n. We denote 'for all' by the symbol $\forall$, so the statement is written formally $\forall n \in \mathbb{N}\big[\mathit{Odd}(n) \to \mathit{Square}(n)\big]$.

A quantifier delimits for how many values of the variable the clause must be true, in order for the statement as a whole to be true.

Besides 'for all' we will also use 'there exists', denoted $\exists$. The statement $\exists n \in \mathbb{N}\big[\mathit{Odd}(n) \to \mathit{Square}(n)\big]$ is true.

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

$$\forall n \in \mathbb{N}\, [1|n]$$

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

$$\forall n \in \mathbb{N}\left[1|n\right]$$

- There are five different powers n where $2^n - 7$ is a perfect square.

$$\exists n_0, \ldots, n_4 \in \mathbb{N}\big[(n_0 \neq n_1) \wedge (n_0 \neq n_2) \wedge \cdots \wedge (n_3 \neq n_4)$$
$$\wedge\ \exists a_0 \in \mathbb{N}(2^{n_0} - 7 = a_0^2) \wedge \cdots \wedge \exists a_4 \in \mathbb{N}(2^{n_4} - 7 = a_4^2)\big]$$

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

$$\forall n \in \mathbb{N}\left[1|n\right]$$

- There are five different powers n where $2^n - 7$ is a perfect square.

$$\begin{aligned}\exists n_0, \ldots, n_4 \in \mathbb{N}\big[&(n_0 \neq n_1) \wedge (n_0 \neq n_2) \wedge \cdots \wedge (n_3 \neq n_4) \\ &\wedge \exists a_0 \in \mathbb{N}(2^{n_0} - 7 = a_0^2) \wedge \cdots \wedge \exists a_4 \in \mathbb{N}(2^{n_4} - 7 = a_4^2)\big]\end{aligned}$$

- Any two integers have a common multiple.

$$\forall n_0, n_1 \in \mathbb{N}\ \exists m \in \mathbb{N}\left[(n_0|m) \wedge (n_1|m)\right]$$

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

$$\forall n \in \mathbb{N}\left[1|n\right]$$

- There are five different powers n where $2^n - 7$ is a perfect square.

$$\exists n_0, \ldots, n_4 \in \mathbb{N}\left[(n_0 \neq n_1) \wedge (n_0 \neq n_2) \wedge \cdots \wedge (n_3 \neq n_4)\right.$$
$$\left.\wedge\, \exists a_0 \in \mathbb{N}(2^{n_0} - 7 = a_0^2) \wedge \cdots \wedge \exists a_4 \in \mathbb{N}(2^{n_4} - 7 = a_4^2)\right]$$

- Any two integers have a common multiple.

$$\forall n_0, n_1 \in \mathbb{N}\ \exists m \in \mathbb{N}\left[(n_0|m) \wedge (n_1|m)\right]$$

- The function $f\colon \mathbb{R} \to \mathbb{R}$ is continuous at $a \in \mathbb{R}$.

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ \left[(\,|x-a| < \delta) \to (|f(x) - f(a)| < \varepsilon)\,\right]$$

Relation between $\forall$ and $\exists$

The negation of a '$\forall$' statement is a '$\exists\,\neg$' statement. For instance, the negation of 'every raven is black' is 'there is a raven that is not black'.

Relation between $\forall$ and $\exists$

The negation of a '$\forall$' statement is a '$\exists\,\neg$' statement. For instance, the negation of 'every raven is black' is 'there is a raven that is not black'.

A mathematical example is that the negation of 'every odd number is a perfect square'

$$\neg\,\forall n \in \mathbb{N}\,\bigl[\mathit{Odd}(n) \to \mathit{Square}(n)\bigr]$$

is

$$\exists n \in \mathbb{N}\,\neg\bigl[\mathit{Odd}(n) \to \mathit{Square}(n)\bigr]$$

which is equivalent to this.

$$\exists n \in \mathbb{N}\,\bigl[\mathit{Odd}(n) \wedge \neg\mathit{Square}(n)\bigr]$$

Thus a person could show that 'every odd number is a perfect square' is false by finding a number that is both odd and not a square.

Relation between $\forall$ and $\exists$

The negation of a '$\forall$' statement is a '$\exists\,\neg$' statement. For instance, the negation of 'every raven is black' is 'there is a raven that is not black'.

A mathematical example is that the negation of 'every odd number is a perfect square'

$$\neg\,\forall n \in \mathbb{N}\,\big[\mathit{Odd}(n) \to \mathit{Square}(n)\big]$$

is

$$\exists n \in \mathbb{N}\,\neg\big[\mathit{Odd}(n) \to \mathit{Square}(n)\big]$$

which is equivalent to this.

$$\exists n \in \mathbb{N}\,\big[\mathit{Odd}(n) \wedge \neg\mathit{Square}(n)\big]$$

Thus a person could show that 'every odd number is a perfect square' is false by finding a number that is both odd and not a square.

Similarly the negation of a '$\exists$' statement is a '$\forall\,\neg$' statement.