Foundation of proofs

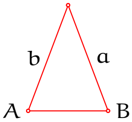
Jim Hefferon

http://joshua.smcvt.edu/proofs

The need to prove

In Mathematics we prove things

'The base angles of an isoceles triangle are equal' seems obvious to a person with mathematical aptitude.

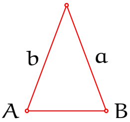


if $a \cong b$ then $\angle A \cong \angle B$

Another example that seems obvious to such a person is 'each positive integer factors into a product of primes'.

In Mathematics we prove things

'The base angles of an isoceles triangle are equal' seems obvious to a person with mathematical aptitude.



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

Another example that seems obvious to such a person is 'each positive integer factors into a product of primes'.

But is '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' perfectly clear?

A characteristic of our subject is that we show that new results follow logically from those already established.

Convincing is not enough

Convincing is not enough

- The polynomial $n^2 + n + 41$ seems 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

- The polynomial $n^2 + n + 41$ seems 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

- The polynomial $n^2 + n + 41$ seems 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 $1 + 2$ of prime factors, 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 if you fix any number $n > 1$ then among the numbers below it, the even types never outnumber the odd types.

Convincing is not enough

- The polynomial $n^2 + n + 41$ seems 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 $1 + 2$ of prime factors, 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 if you fix any number $n > 1$ then among the numbers below it, the even types 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.

'It is not the case that $3+3=5$' is true.

'It is not the case that $3+3=6$' is false.

Negation

Prefixing a proposition with not inverts its truth value.

'It is not the case that $3 + 3 = 5$' is true.

'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. We say 'not' is a unary logical operator or a unary boolean function since it takes one input, a truth value, and yields as output a truth value.

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

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

So 'and' and 'or', conjunction and disjunction, are binary logical operators.

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 of a complexity that would be awkward 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.

Sometimes we prefer using 0 for F and 1 for T. One reason for the preference is that on the left side of the tables the rows make the ascending binary numbers.

P	$\bar{P}$
0	1
1	0

P	Q	$P \cdot Q$	$P + Q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

In this context we symbolize ‘not P’ with $\bar{P}$, we symbolize ‘P and Q’ with $P \cdot Q$, and we symbolize ‘P or Q’ with $P + Q$.

Sometimes we prefer using 0 for F and 1 for T. One reason for the preference is that on the left side of the tables the rows make the ascending binary numbers.

P	$\bar{P}$
0	1
1	0

P	Q	$P \cdot Q$	$P + Q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

In this context we symbolize 'not P' with $\bar{P}$, we symbolize 'P and Q' with $P \cdot Q$, and we symbolize 'P or Q' with $P + Q$.

Note that $\bar{P} = 1 - P$. The table makes clear why for 'P and Q' we use a multiplication dot $P \cdot Q$. For 'P or Q' the plus sign is a good symbol because 'or' accumulates the truth value T.

Other operators: 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

Other operators: Implies

We model 'if P then Q' this way.

P	Q	$P \rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

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

Other operators: Bi-implication

Model ‘P if and only if Q’ with this.

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

Mathematicians often write ‘iff’.

All binary operators

This lists all of the binary logical operators.

P	Q	P α_0 Q
F	F	F
F	T	F
T	F	F
T	T	F

P	Q	P α_1 Q
F	F	F
F	T	F
T	F	F
T	T	T

...

P	Q	P α_{15} Q
F	F	T
F	T	T
T	F	T
T	T	T

All binary operators

This lists all of the binary logical operators.

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

...

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

This lists all of the binary logical operators.

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 $(P \to Q) \wedge (P \to R)$.

P	Q	R	$P \to Q$	$P \to R$	$(P \to Q) \wedge (P \to R)$
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 just consists of decomposing the statement into its components $P \to Q$, etc., and building up to the full sentence.

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 give the same input-output relationship. Check that expressions E_0 and E_1 are equivalent by using truth tables to verify that $E_0 \leftrightarrow E_1$ is a tautology.

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 give the same input-output relationship. Check that expressions E_0 and E_1 are equivalent by using truth tables to verify that $E_0 \leftrightarrow E_1$ is a tautology.

For instance, $P \wedge Q$ and $Q \wedge P$ are equivalent. Another 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: the definition of implication

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

Our definition of implies takes 'if Babe Ruth was president then $1 + 2 = 4$' to be a true statement, because its antecedent is false.

Discussion: the definition of implication

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

Our definition of implies takes ‘if Babe Ruth was president then $1 + 2 = 4$’ to be a true statement, because its antecedent is false. Similarly we take ‘if Mallory reached the summit of Everest then $1 + 2 = 3$’ to be true because its consequent is true. Why define it this way?

Discussion: the definition of implication

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

Our definition of implies takes ‘if Babe Ruth was president then $1 + 2 = 4$’ to be a true statement, because its antecedent is false. Similarly we take ‘if Mallory reached the summit of Everest then $1 + 2 = 3$’ to be true because its consequent is true. Why define it this way?

Standard mathematical practice defines implication so that statements like this one are true:

for all $n \in \mathbb{N}$, if n is a perfect square then n is not prime

(because $n = a \cdot a$ is a factorization).

Discussion: the definition of implication

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

Our definition of implies takes 'if Babe Ruth was president then $1+2=4$' to be a true statement, because its antecedent is false. Similarly we take 'if Mallory reached the summit of Everest then $1+2=3$' to be true because its consequent is true. Why define it this way?

Standard mathematical practice defines implication so that statements like this one are true:

$$\text{for all } n \in \mathbb{N}, \text{ if } n \text{ is a perfect square then } n \text{ is not prime}$$

(because $n = a \cdot a$ is a factorization). Then taking $n = 6$ shows that we need $F \to T$ to evaluate to T.

Discussion: the definition of implication

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

Our definition of implies takes 'if Babe Ruth was president then $1 + 2 = 4$' to be a true statement, because its antecedent is false. Similarly we take 'if Mallory reached the summit of Everest then $1 + 2 = 3$' to be true because its consequent is true. Why define it this way?

Standard mathematical practice defines implication so that statements like this one are true:

$$\text{for all } n \in \mathbb{N}, \text{ if } n \text{ is a perfect square then } n \text{ is not prime}$$

(because $n = a \cdot a$ is a factorization). Then taking $n = 6$ shows that we need $F \to T$ to evaluate to T. Use $n = 3$ to see that we need $F \to F$ to yield T.

Discussion: the definition of implication

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

Our definition of implies takes 'if Babe Ruth was president then $1+2=4$' to be a true statement, because its antecedent is false. Similarly we take 'if Mallory reached the summit of Everest then $1+2=3$' to be true because its consequent is true. Why define it this way?

Standard mathematical practice defines implication so that statements like this one are true:

$$\text{for all } n \in \mathbb{N}\text{, if } n \text{ is a perfect square then } n \text{ is not prime}$$

(because $n = a \cdot a$ is a factorization). Then taking $n = 6$ shows that we need $F \to T$ to evaluate to T. Use $n = 3$ to see that we need $F \to F$ to yield T. For $T \to T$ take $n = 4$.

Points about implication

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

- As noted on the prior slide, the antecedent P need not be materially 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

- As noted on the prior slide, the antecedent P need not be materially connected to the consequent Q.
- Also noted there are: (1) if the antecedent P is false then the statement as a whole is true, said to be vacuously true, and (2) 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

- As noted on the prior slide, the antecedent P need not be materially connected to the consequent Q.
- Also noted there are: (1) if the antecedent P is false then the statement as a whole is true, said to be vacuously true, and (2) if the consequent Q is true then the statement as a whole is true.
- 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 $\neg Q \to \neg P$.

Points about implication

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

- As noted on the prior slide, the antecedent P need not be materially connected to the consequent Q.
- Also noted there are: (1) if the antecedent P is false then the statement as a whole is true, said to be vacuously true, and (2) if the consequent Q is true then the statement as a whole is true.
- 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 $\neg Q \to \neg P$.
- On a table in front of you are four cards, marked 'A', 'B', '0', and '1'. You must verify the truth of the implication, 'if a card has a vowel on the one side then it has an even number on the other.' How to do it, turning over the fewest cards? (This is the *Wason test*; fewer than 10% of Americans get it right.)

Predicates, Quantifiers

Here is a typical mathematical statement.

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

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

Here is a typical mathematical statement.

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

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 stating $(*)$ would mean that it holds for all n. We denote 'for all' by $\forall$ so the statement is formally written $\forall n \in \mathbb{N}\big[Odd(n) \to Square(n)\big]$. (It is, of course, a false statement.)

Predicates, Quantifiers

Here is a typical mathematical statement.

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

It involves two clauses, 'n is odd' and 'n is square'. For each, the truth value depend on the variable n. 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 stating $(*)$ would mean that it holds for all n. We denote 'for all' by $\forall$ so the statement is formally written $\forall n \in \mathbb{N}\big[Odd(n) \to Square(n)\big]$. (It is, of course, a false statement.)

A quantifier describes 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' the other common quantifier is 'there exists', denoted $\exists$. The statement $\exists n \in \mathbb{N}\big[Odd(n) \to Square(n)\big]$ is true.

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

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

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

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

- There are five different powers n where the equation $2^n - 7 = a^2$ has a solution.

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

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

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

- There are five different powers n where the equation $2^n - 7 = a^2$ has a solution.

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

- Any two integers have a common multiple.

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

Examples of statements written formally, with explicit quantifiers.

- Every number is divisible by 1.

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

- There are five different powers n where the equation $2^n - 7 = a^2$ has a solution.

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

- Any two integers have a common multiple.

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

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

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

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'.

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'

$$\forall n \in \mathbb{N}\left[\mathit{Odd}(n) \rightarrow \mathit{Square}(n)\right]$$

is

$$\exists n \in \mathbb{N}\neg\left[\mathit{Odd}(n) \rightarrow \mathit{Square}(n)\right]$$

which is equivalent to this.

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

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.

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'

$$\forall n \in \mathbb{N} \left[\mathit{Odd}(n) \rightarrow \mathit{Square}(n) \right]$$

is

$$\exists n \in \mathbb{N} \neg \left[\mathit{Odd}(n) \rightarrow \mathit{Square}(n) \right]$$

which is equivalent to this.

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

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.

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