Mathematical Skills

Logical structure of proofs

Mathematical statements and proof

Axioms (e.g. Peano axioms for natural numbers, the axioms of Euclidean geometry) are statements that are assumed to be true and from which other true statements can be derived by proof by using classical logic (a statement is either true or false, and only true statements follow from the axioms).[1] There may be statements that make sense in a theory but cannot be proved to be either true or false (undecidable statements).[2]

Definition (introduces notation, terminology).

A mathematical statement may be referred by one of the following titles:

Theorem (a significant result), *Proposition* (a small result), *Lemma* (a result used for deriving a main theorem or sevaral propositions), *Corollary* (a result that immediately follows from a previous result).

Claim (an intermediate statement in a proof – like a miniature lemma)

Conjecture (a statement not proved, but believed to be true with some partial justification).

Counterexample (an example that shows a given statement to be false – a counterexample to P serves as a proof of $\neg P$).

Truth functions

The two truth values True and False are denoted by T and F respectively.

An $n$ary *truth function* (or *Boolean function*) is a function $f : \{T, F\}^n \to \{T, F\}$.

The n variables of an $n$ary truth function are denoted by letters $P, Q, \ldots$ etc. when n is small, or $P_1, \ldots, P_n$. (The P is for "Proposition" - a statement that is either true or false.)

For each n, we use the same letter T to stand for the truth function constantly equal to T. Likewise, F denotes the truth function constantly equal to F.

Unary Negation: $\neg : \{T, F\} \to \{T, F\}$.

P	$\neg P$
T	F
F	T

Binary Conjunction $\wedge$, disjunction $\vee$, implication $\to$, equivalence $\leftrightarrow$: $\{T, F\}^2 \to \{T, F\}$.

[1] The axioms of one theory may be inconsistent with the axioms of another theory, but it is always the case that the axioms of a theory are consistent among themselves: applying logical proof to the axioms does not lead to proving both a statement P and its negation $\neg P$. Cantor's Continuum Hypothesis is an example of an axiom that is true in one theory but false in another theory, both theories being internally consistent: the hypothesis states that there is no set S with cardinality lying strictly between the cardinality of $\mathbb{N}$ and the cardinality of $\mathbb{R}$.

[2] This is part of Gödel's Incompleteness Theorem.

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

Exclusive or has the truth table of $\neg(P \leftrightarrow Q)$.(Identifying T with 1 and F with 0, the operations of exclusive or and $\wedge$ correspond to addition and multiplication in the field $\mathbb{Z}_2$.)

Nand has the truth table of $\neg(P \wedge Q)$.

Nor has the truth table of $\neg(P \vee Q)$.

Disjunctive normal form Any truth function $f : \{T, F\}^n \rightarrow \{T, F\}$ other than F (constantly false) can be expressed as a disjunction of conjunctions. A procedure for constructing this formula is best described by an example.

The ternary function $f : \{T, F\}^3 \rightarrow \{T, F\}$ with truth table

P	Q	R	$f(P, Q, R)$
T	T	T	F
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	T

(true when an even number of the three variables are true) has *disjunctive normal form* (DNF)

$$(P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R).$$

Here the first conjunction $P \wedge Q \wedge \neg R$ corresponds to the row with $(P, Q, R) = (T, T, F)$, the second conjunction $P \wedge \neg Q \wedge R$ corresponds to the row with $(P, Q, R) = (T, F, T)$, the third conjunction $\neg P \wedge \neg Q \wedge R$ corresponds to the row with $(P, Q, R) = (F, T, T)$, and the fourth conjunction $\neg P \wedge \neg Q \wedge \neg R$ to $(P, Q, R) = (F, F, F)$. These are the assignments of truth values to (P, Q, R) for which $f(P, Q, R) = T$.

A general procedure for constructing a DNF for a truth function $f(P_1, \ldots, P_n)$ is for each of the n-tuples of truth values assigned to $(P_1, P_2, \ldots, P_n)$ for which f takes the value T, associate the conjunction $\mathscr{P}_1 \wedge \mathscr{P}_2 \wedge \cdots \wedge \mathscr{P}_n$, where

$$\mathscr{P}_i = \begin{cases} P_i & \text{if } P_i \text{ is assigned value } T, \\ \neg P_i & \text{if } P_i \text{ is assigned value } F. \end{cases}$$

Then take the disjunction of all these conjunctions to obtain a truth function with the same truth table as f.

Conjunctive normal form Suppose instead of taking the rows in which a truth function f takes the value T we take those rows where it takes value F and make the DNF as above. Then we have represented the *negation* of f in DNF. By then negating this formula and applying DeMorgan's Laws we move from a disjunction of conjunctions to a conjunction of disjunctions (known as , *conjunctive normal form* (CNF)).

For the parity function f as above we first form

$$(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$$

to represent its negation, and then negate *this* formula to obtain

$$(\neg P \vee \neg Q \vee R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee \neg R)$$

as the CNF for f.

Any truth function not constantly T has a CNF formed in this way.

Propositional calculus

An *atomic proposition* is a statement that is either true or false and cannot be broken down into simpler statements. Atomic propositions are contingent (not necessarily true or necessarily false). Atomic propositions can be viewed as Boolean variables that take either True or False as values (which of these they take depends on the the possible world they say something about).

Formally speaking, an atomic proposition is one of a given countable set of symbols (containing $P, Q, R, \dots, P_1, P_2, P_3, \dots$). Each symbol stands for a variable that takes a truth value T or F.

A *compound proposition* $\mathscr{P}$ is composed of constituent atomic propositions combined together by logical connectives (e.g. negation, disjunction, conjunction). A compound proposition is either true or false. The variables of a truth function may be substituted by propositions, since the latter take values T or F. It is possible to formalize compound propositions axiomatically as *well-formed formulas*:

(i) An atomic proposition is a well-formed formula.

(ii) If $\mathscr{P}$ is a well-formed formula then so is $(\neg\mathscr{P})$.

(iii) If $\mathscr{P}$ and $\mathscr{Q}$ are well-formed formulas then so are $(\mathscr{P} \wedge \mathscr{Q})$, $(\mathscr{P} \vee \mathscr{Q})$, $(\mathscr{P} \rightarrow \mathscr{Q})$ and $(\mathscr{P} \leftrightarrow \mathscr{Q})$.

In order to reduce the number of parentheses in a well-formed formula the convention is to apply precedence rules (cf. multiplication applied before addition in arithmetic), making some operators more binding than others. Usually, the order is $\neg, \rightarrow, \wedge, \vee$ (from most binding to least binding). Thus $\neg P \wedge Q \vee R$ is short for $((\neg P) \wedge Q) \vee R)$. Further simplifications can be made using the fact that $\vee$ and $\wedge$ are both associative in order to reduce for example $((P \vee Q) \vee R)$ unambiguously to $P \vee Q \vee R$.

Logical equivalence Two compound propositions $\mathscr{P}$ and $\mathscr{Q}$ are *logically equivalent* if the truth table for $\mathscr{P}$ is the same as the truth table for $\mathscr{Q}$. Alternatively stated, $\mathscr{P}$ and $\mathscr{Q}$ are logically equivalent if the compound proposition $\mathscr{P} \leftrightarrow \mathscr{Q}$ is constantly true, and we then write $\mathscr{P} \Leftrightarrow \mathscr{Q}$. If $\mathscr{P} \Leftrightarrow \mathscr{Q}$ then proving $\mathscr{P}$ is equivalent to proving $\mathscr{Q}$. For example, $\neg\neg\mathscr{P} \Leftrightarrow \mathscr{P}$ (showing $\mathscr{P}$ is true is equivalent to showing the negation of $\mathscr{P}$ is false). Logical equivalence is used to recast a statement into a form that may be more amenable to proof (for example, replacing $\mathscr{P} \Rightarrow \mathscr{Q}$ by the logically equivalent contrapositive form $\neg\mathscr{Q} \Rightarrow \neg\mathscr{P}$).

Examples of logical equivalences include:

commutativity	$\mathscr{P} \wedge \mathscr{Q} \Leftrightarrow \mathscr{Q} \wedge \mathscr{P}$ $\mathscr{P} \vee \mathscr{Q} \Leftrightarrow \mathscr{Q} \vee \mathscr{P}$	identity for $\vee$	$\mathscr{P} \wedge F \Leftrightarrow F$ $\mathscr{P} \vee F \Leftrightarrow \mathscr{P}$
associativity	$(\mathscr{P} \wedge \mathscr{Q}) \wedge \mathscr{R} \Leftrightarrow \mathscr{P} \wedge (\mathscr{Q} \wedge \mathscr{R})$ $(\mathscr{P} \vee \mathscr{Q}) \vee \mathscr{R} \Leftrightarrow \mathscr{P} \vee (\mathscr{Q} \vee \mathscr{R})$	identity for $\wedge$	$\mathscr{P} \vee T \Leftrightarrow T$ $\mathscr{P} \wedge T \Leftrightarrow \mathscr{P}$
distributivity	$\mathscr{P} \wedge (\mathscr{Q} \vee \mathscr{R}) \Leftrightarrow (\mathscr{P} \wedge \mathscr{Q}) \vee (\mathscr{P} \wedge \mathscr{R})$ $\mathscr{P} \vee (\mathscr{Q} \wedge \mathscr{R}) \Leftrightarrow (\mathscr{P} \vee \mathscr{Q}) \wedge (\mathscr{P} \vee \mathscr{R})$	complement	$\mathscr{P} \wedge \neg\mathscr{P} \Leftrightarrow F$ $\mathscr{P} \vee \neg\mathscr{P} \Leftrightarrow T$
DeMorgan's laws	$\neg(\mathscr{P} \vee \mathscr{Q}) \Leftrightarrow \neg\mathscr{P} \wedge \neg\mathscr{Q}$ $\neg(\mathscr{P} \wedge \mathscr{Q}) \Leftrightarrow \neg\mathscr{P} \vee \neg\mathscr{Q}$	idempotence	$\mathscr{P} \vee \mathscr{P} \Leftrightarrow \mathscr{P}$ $\mathscr{P} \wedge \mathscr{P} \Leftrightarrow \mathscr{P}$

If $\mathscr{P}$ appears as part of the hypothesis and as part of the conclusion, then its appearance in the conclusion may be dropped:

$$(\mathscr{P} \wedge \mathscr{Q}) \to (\mathscr{P} \wedge \mathscr{R}) \;\Leftrightarrow\; (\mathscr{P} \wedge \mathscr{Q}) \to \mathscr{R}.$$

(In other words, you do not need to prove $\mathscr{P}$ if it is already assumed as part of the hypothesis.)

Logical implication If $\mathscr{P} \to \mathscr{Q}$ is constantly true then we say $\mathscr{P}$ logically implies $\mathscr{Q}$ and we write $\mathscr{P} \Rightarrow \mathscr{Q}$. Given that $\mathscr{P} \Rightarrow \mathscr{Q}$, if $\mathscr{P}$ is true (such as an axiom) then we deduce that $\mathscr{Q}$ is true. This "transmission of truth" is what drives the engine of proof: proof relies on logical implication in order to pass from one true statement to another, beginning from axioms (propositions declared to be true). Together with logical equivalence (which allows you to move freely around a related set of truths), logical implication grows out truth from its beginnings in the axioms to a larger and larger set of truths (as new theorems are discovered).

Examples of logical implications include:

	$\mathscr{P} \wedge \mathscr{Q} \Rightarrow \mathscr{P}$
	$\mathscr{P} \Rightarrow \mathscr{P} \vee \mathscr{Q}$
modus ponens	$\mathscr{P} \wedge (\mathscr{P} \to \mathscr{Q}) \Rightarrow \mathscr{Q}$
modus tollens	$(\mathscr{P} \to \mathscr{Q}) \wedge \neg\mathscr{Q} \Rightarrow \neg\mathscr{P}$

Tautologies and contradictions A *tautology* is a compound proposition that is logically equivalent to T.

An atomic proposition other than the constant T is never a tautology: it can either be true or false. A compound proposition can be constantly true on account of its logical form: for example, $\mathscr{P} \vee \neg\mathscr{P}$ is a tautology.

A *contradiction* is a compound proposition that is logically equivalent to F.

A *contingent* or *satisfiable* proposition is one that is neither a tautology nor a contradiction: in some assigment of truth values to its constituent atomic propositions it is true, while in others it is false.

The *law of the excluded middle* is that $\mathscr{P} \vee \neg\mathscr{P}$ is a tautology, for any well-formed formula $\mathscr{P}$: a proposition is either true or false, and nothing in between.

First order logic and quantification A free variable x in a proposition $\mathscr{P} = \mathscr{P}(x)$ ranges over a given domain (set) when the proposition is interpreted in some model (such as the natural numbers, or the real numbers). In Propositional Logic $\mathscr{P}(x)$ becomes a proposition upon assigning a value to x, when it becomes either True or False.

First Order Logic allows quantification over the elements of a domain. (Second Order Logic allows quantification over subsets of a domain.) All that is needed at this stage is familiarity with how to formulate mathematical statements using quantification (for example, $\forall\, \epsilon > 0\; \exists N \in \mathbb{N}\; \forall\, n \geq N\; |x_n - x| < \epsilon$ for the convergence of the sequence (x_n) to limit x) and how to negate these statements by taking the negation through the quantifiers and switching $\forall$ and $\exists$ (for example, $\exists\, \epsilon > 0\; \forall N \in \mathbb{N}\; \exists\, n \geq N\; |x_n - x| \geq \epsilon$ for the statement that (x_n) diverges).

Universal quantification: $\forall\, x \in X\; \mathscr{P}(x)$, declared to be true when $\mathscr{P}(x)$ is true for all x in the given domain X.

Existential quantification: $\exists\, x \in X\; \mathscr{P}(x)$, declared to be true when $\mathscr{P}(x)$ is true for at least one x in the domain X.

Negation of quantifiers: $\neg\forall\, x \in X\; \mathscr{P}(x)$ is logically equivalent to $\exists x \in X\; \neg\mathscr{P}(x)$ ($\mathscr{P}(x)$ fails to be true for all x if and only if there is some x for which $\mathscr{P}(x)$ is false).

$\neg\exists\, x \in X\; \mathscr{P}(x)$ is logically equivalent to $\forall\, x \in X\; \neg\mathscr{P}(x)$ (there is no x for which $\mathscr{P}(x)$ is true if and only if $\mathscr{P}(x)$ is false for all x).

We then have

$$\begin{aligned} \neg\forall\, x \in X\, \neg\mathscr{P}(x) \quad &\Leftrightarrow \quad \exists\, x \in X\ \mathscr{P}(x), \\ \neg\exists\, x \in X\, \neg\mathscr{P}(x) \quad &\Leftrightarrow \quad \forall\, x \in X\ \mathscr{P}(x). \end{aligned}$$

The order in which quantifiers appear can change the meaning of a statement. For example, $\forall\, x\ \exists y\ (x+y=0)$ says that each x has an additive inverse, while $\exists\, y\ \forall x\ (x+y=0)$ says that there is an element y which added to every element x makes 0 (a different statement, and one that is false in the usual interpretation of arithmetic addition).

However, two universal quantifiers next to each other can be swapped, and likewise two existential quantifiers:

$$\forall\, x \forall\, y\ \mathscr{P}(x,y) \quad \Leftrightarrow \forall\, y \forall\, x\ \mathscr{P}(x,y)$$

and

$$\exists\, x \exists\, y\ \mathscr{P}(x,y) \quad \Leftrightarrow \exists\, y \exists\, x\ \mathscr{P}(x,y)$$

Logical equivalences and implications underlying proof techniques

Direct proof

$$(\mathscr{P} \to \mathscr{R}) \wedge (\mathscr{R} \to \mathscr{Q}) \quad \Rightarrow \quad (\mathscr{P} \to \mathscr{Q})$$

Chain of implications pieced together to get from the initial hypothesis $\mathscr{P}$ to the final conclusion $\mathscr{Q}$. Many statements of the form $\mathscr{P} \to \mathscr{Q}$ can be proved after a number of such intermediate steps.

Example: "If $n \in \mathbb{N}$ is odd then n^2 is odd" has a direct proof: $n = 2m+1$ (definition), $n^2 = (2m+1)(2m+1) = 4m^2+4m+1$ (definition of square, distributivity of multiplication over addition, commutativity of addition and multiplication) and $4m^2+4m+1 = 2(2m^2+2m)+1 = 2m'+1$ for $m' = 2m^2+2m \in \mathbb{N}$.

Proof by cases

$$(\mathscr{P} \vee \mathscr{Q}) \to \mathscr{R} \quad \Leftrightarrow \quad (\mathscr{P} \to \mathscr{R}) \wedge (\mathscr{Q} \to \mathscr{R}).$$

In particular, if $(\mathscr{P} \vee \mathscr{Q}) \Leftrightarrow T$ ($\mathscr{P}$ and $\mathscr{Q}$ exhaust all cases) then since

$$T \to \mathscr{R} \quad \Leftrightarrow \quad \mathscr{R}$$

we have

$$\mathscr{R} \quad \Leftrightarrow \quad (\mathscr{P} \to \mathscr{R}) \wedge (\mathscr{Q} \to \mathscr{R}) \quad \text{when } (\mathscr{P} \vee \mathscr{Q}) \leftrightarrow T.$$

Example: Let $\mathscr{R}(n)$ be"If $n \in \mathbb{N}$ then $n^2 \equiv 0$ or $1 \pmod 4$." If $\mathscr{P}(n)$ is "$n \in \mathbb{N}$ is even" and $\mathscr{Q}(n)$ is "$n \in \mathbb{N}$ is odd", then $\mathscr{P}(n) \vee \mathscr{Q}(n) = T$ for each $n \in \mathbb{N}$. To prove $\mathscr{R}(n)$ it is equivalent to prove "If $\mathscr{P}(n)$ then $\mathscr{R}(n)$" and "If $\mathscr{Q}(n)$ then $\mathscr{R}(n)$." In other words, split into the cases n is even and n is odd (if $n = 2m$ then $n^2 = 4m^2$ is $0 \pmod 4$ and if $n = 2m+1$ then $n^2 = 4m(m+1)+1$ is $1 \pmod 4$)).

Proof by cases is useful for proving statements the domain of which can be partitioned into subsets: for example to show that $|x+y| \le |x|+|y|$ in $\mathbb{R}$ there are four cases according as $x \ge 0, x < 0$ and $y \ge 0, y < 0$.

Indirect proof: contrapositive

$$\mathscr{P} \to \mathscr{Q} \quad \Leftrightarrow \quad \neg\mathscr{Q} \to \neg\mathscr{P}$$

Example:"If n^2 is odd then n is odd" has contrapositive "If n is even then n^2 is even"

Indirect proof: by contradiction (i) Statements $\mathscr{P}$ not necessarily of the form "If... then..." (for example, "There are infinitely many primes."):

$$\mathscr{P} \Leftrightarrow (\neg\mathscr{P} \to F)$$

To prove $\mathscr{P}$ we prove that if we suppose $\mathscr{P}$ to be false (i.e. $\neg\mathscr{P}$) then we derive a contradiction (i.e., F). For F we may substitute any contradiction (proposition logically equivalent to F).

(ii) Statements $\mathscr{P} \to \mathscr{Q}$ in "If ... then ..." form. Since

$$\neg(\mathscr{P} \to \mathscr{Q}) \Leftrightarrow \mathscr{P} \wedge \neg\mathscr{Q}$$

to show $\mathscr{P} \to \mathscr{Q}$ it is equivalent to show that $(\mathscr{P} \wedge \neg\mathscr{Q}) \to F$.

For our contradiction F we could take $\mathscr{P} \wedge \neg\mathscr{P}$. Then

$$(\mathscr{P} \wedge \neg\mathscr{Q}) \to (\mathscr{P} \wedge \neg\mathscr{P}) \quad \Leftrightarrow \quad (\mathscr{P} \wedge \neg\mathscr{Q}) \to \neg\mathscr{P}$$

since $\mathscr{P}$ appears in the hypothesis as well as the conclusion. Hence proving $\mathscr{P} \to \mathscr{Q}$ by contradiction here is equivalent to supposing $\mathscr{P} \wedge \neg\mathscr{Q}$ and reaching the conclusion that $\neg\mathscr{P}$:

$$\mathscr{P} \to \mathscr{Q} \quad \Leftrightarrow \quad (\mathscr{P} \wedge \neg\mathscr{Q}) \to \neg\mathscr{P}.$$

[Examples:]

Moreover, if we just suppose $\neg\mathscr{Q}$ and reach the conclusion that $\neg\mathscr{P}$ (i.e. without having to use $\mathscr{P}$ in our hypothesis $\mathscr{P} \to \mathscr{Q}$) then we have proved $\neg\mathscr{Q} \to \neg\mathscr{P}$, which is the *contrapositive* of the statement $\mathscr{P} \to \mathscr{Q}$.

Converse The *converse* to $\mathscr{P} \to \mathscr{Q}$ is the statement $\mathscr{Q} \to \mathscr{P}$: we do *not* have any logical equivalence (or implication) between these two statements, as can be checked by looking at the truth tables for each of $P \to Q$ and $Q \to P$. For example, "If I am sleeping then I am breathing" is a true statement, but its converse "If I am breathing then I am sleeping" is not. More mathematically, "If $n > 2$ is prime then n is odd" is true, but the converse "If $n > 2$ is odd then n is prime" is false.

When asked to prove a statement of the form $\mathscr{P} \to \mathscr{Q}$ and its converse $\mathscr{Q} \to \mathscr{P}$ you are being asked to prove the statement $\mathscr{P} \leftrightarrow \mathscr{Q}$. In other words,

$$(\mathscr{P} \to \mathscr{Q}) \wedge (\mathscr{Q} \to \mathscr{P}) \quad \Leftrightarrow \quad \mathscr{P} \leftrightarrow \mathscr{Q}.$$

Equivalence

$$\mathscr{P} \leftrightarrow \mathscr{Q} \quad \Leftrightarrow \quad (\mathscr{P} \to \mathscr{Q}) \wedge (\mathscr{Q} \to \mathscr{P})$$

Transitivity of $\leftrightarrow$:

$$(\mathscr{P} \leftrightarrow \mathscr{Q}) \wedge (\mathscr{Q} \leftrightarrow \mathscr{R}) \wedge (\mathscr{R} \leftrightarrow \mathscr{P}) \quad \Leftrightarrow \quad (\mathscr{P} \leftrightarrow \mathscr{Q}) \wedge (\mathscr{Q} \leftrightarrow \mathscr{R})$$

To prove three statements are pairwise equivalent it suffices to show two pairs are equivalent.

Equivalence: circle of implications

$$(\mathscr{P} \leftrightarrow \mathscr{Q}) \wedge (\mathscr{Q} \leftrightarrow \mathscr{R}) \wedge (\mathscr{R} \leftrightarrow \mathscr{P}) \quad \Leftrightarrow \quad (\mathscr{P} \to \mathscr{Q}) \wedge (\mathscr{Q} \to \mathscr{R}) \wedge (\mathscr{R} \to \mathscr{P})$$

Definition. *A set is* countable *if S is finite or there is a bijection from $\mathbb{N}$ to S. (In the latter case S is* denumerable.

Lemma. *A subset of a countable set is countable.*

Theorem. *The following are equivalent:*

(a) S is a countable set.

(b) There exists a surjection from $\mathbb{N}$ onto S.

(c) There exists an injection from S into $\mathbb{N}$.

Proof. (a) $\Rightarrow$ (b) If S is finite there is a bijection g from $[n]$ onto S and define the function $f : \mathbb{N} \to S$ by $f(k) = g(k)$ for $k \in [n]$ and $f(k) = n$ otherwise. This defines a surjection onto S.

If S is denumerable then there is a bjiection $\mathbb{N} \to S$, which in particular is a surjection.

(b) $\Rightarrow$ (c) If $f : \mathbb{N} \to S$ is a surjection define $g : S \to \mathbb{N}$ by setting $g(s)$ to be the least element in the inverse image $f^{-1}(s) = \{n \in \mathbb{N} : f(n) = s\}$. This defines an injection, because if $g(s) = g(t) = n$ then $s = f(n) = t$.

(c) $\Rightarrow$ (a) If f is an injection from S into $\mathbb{N}$ then it is a bijection onto $f(S) = \{f(s) : s \in S\} \subseteq \mathbb{N}$.

Using the Lemma, the image set $f(S)$ is countable, and by the bijection of f from S to its image $f(S)$ the set S is by definition coutnable. □

Counterexamples

Natural numbers

Peano Axioms

(i) 0 is a natural number.

(ii) Every natural number has a successor.

(iii) 0 is not the successor of any natural number.

(iv) If the successor of x equals the successor of y, then x equals y.

(v) (Induction). If a statement is true of 0, and if the truth of that statement for a number implies its truth for the successor of that number, then the statement is true for every natural number.

In ordinary arithmetic, the successor of x is $x + 1$.

Recursive definitions Recurrence formula together with boundary values specify operations and functions with domain natural numbers.
Addition:

$$m + (n + 1) = (m + n) + 1, \quad m + 0 = m.$$

Multiplication:

$$m \cdot (n + 1) = m \cdot n + m, \quad m \cdot 0 = 0.$$

Exponentiation:

$$m^{n+1} = m^n \cdot m, \quad m^0 = 1.$$

Factorial:

$$(n + 1)! = n! \cdot (n + 1), \quad 0! = 1.$$

Binomial coefficient $\binom{n}{k}$ (number of subsets of $[n]$ of size k):

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}, \quad \binom{n}{0} = \binom{n}{n} = 1 \text{ for } n \geq 1, \ \binom{0}{0} = 0.$$

Stirling number of the second kind $\left\{ {n \atop k} \right\}$ (number of partitions of $[n]$ into k non-empty subsets):

$$\left\{ {n+1 \atop k} \right\} = k\left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\}, \quad \left\{ {n \atop 0} \right\} = \left\{ {0 \atop n} \right\} = 0 \text{ for } n \geq 1, \; \left\{ {0 \atop 0} \right\} = 1.$$

Fibonacci numbers F_n (number of compositions of 1 and 2 that sum to $n-1$):

$$F_{n+1} = F_n + F_{n-1}, \qquad F_0 = 0, F_1 = 1.$$

Proving a property of a recursively defined sequence almost invariably uses induction.

Principle of Mathematical Induction

Strong Principle of Mathematical Induction

Well-ordering of $\mathbb{N}$

Minimum counterexample

Counting

Inclusion-Exclusion [A topic in Discrete Mathematics I.]

Counting in two ways (double counting)

Pigeonhole Principle