Proof and Logic

Table of contents

1. Mathematical Proofs.

"Mathematics is nothing more, nothing less, than the exact part of our thinking."
— L. E. J. Brouwer (1881 – 1966)

"... if you do not take care to prove what you say, then you run the risk of saying something that is wrong. ... if you do try to prove statements, then you will understand them in a completely different and much more interesting way."
— Timothy Gowers (1963 –) ([Gow02])

"But a proof is a device of communication. The creator or discoverer of this new mathematical result wants others to believe it and accept it. In the physical sciences – chemistry, biology, or physics for example – the method for achieving this end is the *reproducible experiment*. For the mathematician, the reproducible experiment is a proof that others can read and understand and validate."
— Steven G. Krantz (1951 –) ([Kra11])

Exercise 1. ([Bur07]) Some coins are spread out on a table. They lie either heads up or tails up. You are blindfolded and wear thick gloves and thus can only count the coins but cannot tell which face is up. Someone tells you the number of coins that are heads up. Now you can turn any of the coins over and move them around. Can you divide the coins into two collections so that they have the same number of heads up coins?

Prove that your strategy always works.

1.1. What is a mathematical proof.

A proof is a *convincing* argument establishing the truth or falsehood of a *mathematical statement*.

- *Mathematical statement*: A *mathematical statement* is "a declarative sentence that is either true or false but not both." ([Bur07])

  Exercise 2. ([Bur07]) Determine which of the following sentences are mathematical statements:

  - My e-mail password is "swordfish."
  - I don't understand.
  - Are you really taking that math course? Are you crazy?
  - This sentence is false.
  - $\frac{310}{0} = 31$.

- *Convincing*:
  - The standard for "convincing" changes as mathematics evolves.[1] In particular, "visual" proofs are **not** convincing anymore by today's standard, as it can easily lead to (very hard to detect) mistakes. The current standard for "convincing" in mathematics is "logically necessary".

Remark 1. Note that what a mathematical proof can do is to guarantee the implication "If statement A is true then statement B is true." It can say nothing about the absolute truth values of A or B. One example is the following.

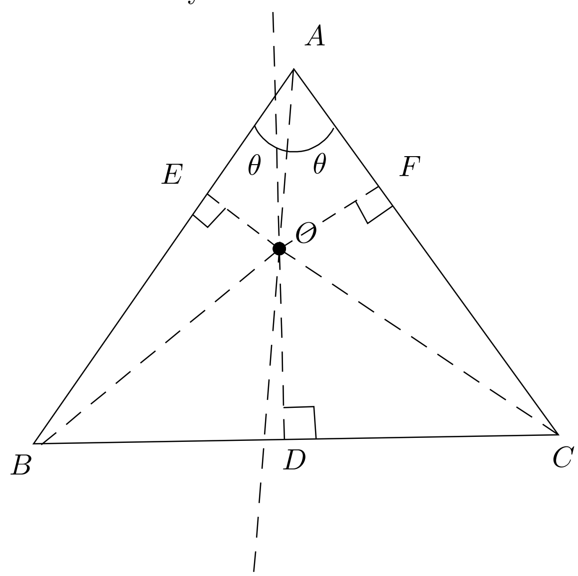
In Analysis there is a so-called "Axiom of Choice" which claims there is a way to pick one object from each set in an arbitrary collection of sets. Sounds very natural. However, it can be proved that, if Axiom of Choice is true, then the following Banach-Tarski paradox is true:

1. See [Kra11] for the history of mathematical proof.

> Given a ball in the three-dimensional space. There is a way to break it into finitely many pieces, and then reassemble to form two balls, each identical to the original one.

Example 2. ([Bin80]) Let ABC be an arbitrary triangle. The following "proof" argues that it is equilateral. Can you spot the mistake?

Proof. Let's show AB = AC. Similarly BC = BA can be shown.



Now we draw auxiliary lines as above, in particular D is the middle point of BC. Clearly the two triangles AOE and AOF are the same, therefore AE = AF, OE = OF. Furthermore we have OB = BC. By Pythagorean theorem we have EB = FC. As a consequence AB = AC. ☐

Remark 3. Mathematical statements generally cover infinitely many cases, therefore **no finite number of examples will be enough for a proof**. For example

> Odd numbers are $1, 3, 5, \ldots$. We have $1^2 = 1, 3^2 = 9, 5^2 = 25\ldots$ All odd.

does not qualify as "proof" for the statement

> The square of an odd number is odd.

The following example from [Hua02] illustrates this point more dramatically. Consider the factorizations

$$
\begin{aligned}
x - 1 &= x - 1 && (1)\\
x^2 - 1 &= (x - 1)(x + 1) && (2)\\
x^3 - 1 &= (x - 1)(x^2 + x + 1) && (3)\\
x^4 - 1 &= (x - 1)(x + 1)(x^2 + 1) && (4)\\
x^5 - 1 &= (x - 1)(x^4 + x^3 + x^2 + x + 1) && (5)\\
x^6 - 1 &= (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) && (6)\\
&\vdots
\end{aligned}
$$

Any reasonable person would spot the pattern and conjecture that the factorization of $x^n - 1$ gives polynomials with coefficients $0, 1, -1$.[2] Turned out that this holds all the way from $n = 1$ to $n = 104$, but is false for $n = 105$.

2. According to the book this conjecture is named after someone with name sounds like "Chibatanov". However I don't understand Russian and could not figure out the correct English spelling.

Exercise 3. ([Hua02]) Consider the formula n^2+n+17.

a) Show that for $n=1,\ldots,15$ the results are all prime numbers.

b) Show that when $n=16$ the result is not prime.

c) Consider in general $f(n):=n^2+n+p$. Prove that no matter what p is, there is $n<p$ such that n^2+n+p is not prime.

1.2. How to prove.

General procedure.

1. Check the definitions of all the mathematical concepts involved. Make sure you know the precise meaning of each terminology in the statement.
2. Identify the logical structure of the statement.
3. Convince yourself through examples.
4. Apply appropriate proof strategy.

We discuss Steps 2, 4 below. But before that it should be emphasized that Step 1 is very important and shouldn't be skipped in any circumstances. Step 3 is not necessary when the proof is relatively simple.

Step 2. Identify logical structure.

The following are common logical structures of mathematical statements (they will be made precise in the next section).

- Hypothesis - conclusion.

  This is the most common type of problems.

- Disproof.

  Show that a mathematical statement is false.

Step 4. Common proof strategies.

- For "Hypothesis - Conclusion" type statements. First we need to identify the hypotheses and the conclusion(s). Then apply one of the following method.

  - *Direct proof*.

    A direct proof starts from the hypothesis and see what it leads to, hopefully to the conclusion.

    Example 4. Prove that the square of an even number is even.

    Proof. First check definition: A number m is even if and only if there is an integer k such that $m=2k$.

    Now identify:

    - Hypothesis: m is even.
    - Conclusion: m^2 is even.

    We start from the hypothesis: m is even.

    1. By definition $m=2k$ for some integer k;
    2. Calculate $m^2=4k^2$;
    3. Notice $4k^2=2(2k^2)$;
    4. Use the fact: k is an integer $\Longrightarrow 2k^2$ is an integer;

Remark 5. To justify this, we need precise definition of "integers". Turns out in the definition of integers there is a property: If m, n are integers, so is $m\,n$.

Exercise 4. Using the above remark, prove: k is an integer $\Longrightarrow$ $2\,k^2$ is an integer.

5. By definition m^2 is even. □

- *Forward-backward proof*.

  When the relation between the hypothesis and conclusion is more involved, we need to start from both ends and try to meet in the middle.

Example 6. ([Lie06]) Let x, y, z be real numbers, satisfying $x + y + z = 0$. Prove that $x\,y + y\,z + z\,x \leqslant 0$.

Follow the procedure:

1. First make sure we know the definitions;
2. Hypothesis: x, y, z real numbers; $x + y + z = 0$; Conclusion: $x\,y + y\,z + z\,x \leqslant 0$.
3. Convince: A few examples;
4. Proof:
   - Forward: $x + y + z = 0$ implies $x = -(y + z)$;
   - Backward: $x\,y + y\,z + z\,x \leqslant 0$ **is implied by** $x\,(y + z) + y\,z \leqslant 0$.
   - Meet in the middle: since $-(y+z)^2 + y\,z = -\frac{y^2+z^2}{2} - \frac{(y+z)^2}{2} \leqslant 0$, $x = -(y + z)$ implies $x\,(y + z) + y\,z \leqslant 0$.

Proof. $x + y + z = 0$ implies $x = -(y + z)$. Therefore

$$x\,y + y\,z + z\,x = x\,(y + z) + y\,z = -(y + z)^2 + y\,z = -\frac{y^2 + z^2}{2} - \frac{(y + z)^2}{2} \leqslant 0 \tag{7}$$

Thus ends the proof. □

- *Proof by contradiction*.

  The proof by contradiction assumes that the conclusion is false, treat it as a new hypothesis and try to either show that the hypothesis must be false, or something absurd happends.

Example 7. Let m be an integer. Prove that if m^2 is even, then m is even.

Proof. Assume m is not even. Then m is odd, that is $m = 2\,k + 1$ with some integer k. Taking square we have

$$m^2 = 2\,(2\,k^2 + 2\,k) + 1 \tag{8}$$

so m^2 is odd. Contradiction. □

Example 8. Prove that $\sqrt{2}$ is irrational, that is cannot be written as p/q with integers p, q.

Proof. Here clearly the conclusion is "$\sqrt{2}$ is irrational", while the hypothesis is not explicitly given. Rigorously speaking, The hypothesis consists of all true statements about rational numbers. Thus to prove by contradiction is to show that

$$\text{If "}\sqrt{2}\text{ is irrational" is not true, then some true statement about rational numbers is false.} \tag{9}$$

or equivalently,

If $\sqrt{2}$ is rational, then some true statement about rational numbers has to be false. (10)

Therefore, to start our proof, we assume $\sqrt{2} = p/q$ with p, q integers. It is clear that we can assume p, q to be natural numbers, and at least one of them is odd. Now taking square of the equation we have

$$2 = p^2/q^2 \Longrightarrow p^2 = 2\,q^2. \tag{11}$$

If p is odd, we have already reached a contradiction; On the other hand, if p is even, by our assumption q must be odd. Write $p = 2\,k$ we have

$$(2\,k)^2 = 2\,q^2 \Longrightarrow q^2 = 2\,k^2 \tag{12}$$

and reach contradiction again. □

Remark 9. In both examples it is difficult to do a direct or forward-backward proof. For the first example, if we start from m^2 it is hard to proceed as we do not have explicit formula for taking squareroot, while on the other hand taking square is much more explicit; For the second example, we do not have a constructive definition for irrationals, but we have such a definition for rationals, that is "not-irrationals".

- Disproof.

  Usually the statement to be disproved takes the form "for all ..., something holds". In this case all we need to do is to find a "*counterexample*".

Example 10. ([Sib09]) Decide which of the following are true and which are false. Justify.

a) For all natural numbers x, $x^2 + 3\,x + 2 \geqslant 0$.

b) For all integers x, $x^2 + 3\,x + 2 \geqslant 0$.

c) For all rationals x, $x^2 + 3\,x + 2 \geqslant 0$.

d) For all real numbers x, $x^2 + 3\,x + 2 \geqslant 0$.

Example 11. (Fermat primes) A formula producing prime numbers has always been dreamt by mathematicians. In 1650, Pierre de Fermat observed the following:

$$2^{2^0} + 1 = 3,\;\; 2^{2^1} + 1 = 5,\;\; 2^{2^2} + 1 = 17,\;\; 2^{2^3} + 1 = 257 \tag{13}$$

All primes. He conjectured that

for all integers $n \geqslant 0$, $2^{2^n} + 1$ is prime.

To convince himself, he checked one more example:

$$2^{2^4} + 1 = 65537 \tag{14}$$

which indeed is a prime number. However he could not prove his conjecture.

Later in 1732 Leonhard Euler found a counterexample:[3]

$$2^{2^5} + 1 = 4294967297 = 641 \times 6700417. \tag{15}$$

3. According to http://en.wikipedia.org/wiki/Fermat_number, "It is widely believed that Fermat was aware of the form of the factors later proved by Euler, so it seems curious why he failed to follow through on the straightforward calculation to find the factor.[1] One common explanation is that Fermat made a computational mistake and was so convinced of the correctness of his claim that he failed to double-check his work."

Mathematical induction.

Principle of Mathematical Induction. Suppose for every positive integer n there is associated as statement $S(n)$. If $S(1)$ is true, and if the truth of $S(n)$ always implies the truth of $S(n+1)$, then $S(n)$ is true for every n.

Remark 12. (Variants) The following are two useful variants.

- If $S(n_0)$ is true, and if when $n \geqslant n_0$ the truth of $S(n)$ always implies the truth of $S(n+1)$, then $S(n)$ is true for every $n \geqslant n_0$.
- If $S(n_0)$ is true, and if when $n \geqslant n_0$ the truth of $S(n_0), S(n_0+1), \ldots, S(n)$ together always implies the truth of $S(n+1)$, then $S(n)$ is true for every $n \geqslant n_0$.

Remark 13. ([Gow02]) "Put less formally, if you have an infinite list of statements that you wish to prove, then one way to do it is to show that the first one is true and that each one implies the next."

Example 14. Prove the following using induction.

A) For any integer $n \geqslant 1$, $1+3+5+\cdots+(2\,n-1)=n^2$.[4]

B) For any integer $n \geqslant 1$, $\frac{1}{2}+\cdots+\frac{1}{2^n}=1-\frac{1}{2^n}$.

C) For any $r \neq 1$, $1+r+r^2+\cdots+r^n=\frac{r^{n+1}-1}{r-1}$. What happens at $r=1$?

Exercise 5. For any integer $n \geqslant 1$, $1^2+2^2+\cdots+n^2=\frac{n\,(n+1)\,(2\,n+1)}{6}$.

Exercise 6. ([Lie06]) Prove the following:

a) For all $n \geqslant 1$, 2^{4n-1} ends with 8.

b) For all $n \geqslant 1$, $n^3+(n+1)^3+(n+2)^3$ is a multiple of 9.

c) For all $x \geqslant 2, n \geqslant 1$, $x^n \geqslant n\,x$.

d) For all $n \geqslant 3$, $5^n > 4^n+3^n+2^n$.

Example 15. Find out what is wrong with the following proof of the claim:

Any $a, b \in \mathbb{N}$, $a=b$.

Proof. We prove by induction. Let $P(n)$ be the statement:

$$a, b \in \mathbb{N},\ \max(a,b)=n, \qquad \text{then}\, a=b.$$

- $P(1)$ is clearly true.
- We assume $P(n)$ is true. To prove $P(n+1)$, consider arbitrary $a, b \in \mathbb{N}$ with $\max(a,b)=n+1$. Then $\max(a-1,b-1)=n$ and we have $a-1=b-1$ thanks to $P(n)$ being true. This gives $a=b$. □

How to write proofs.

Keep in mind the following insight from Andrew Gleason (1921 – 2008): The purpose of writing down a proof is not "to convince you that something is true", but "to show you why it is true."

4. It is said that Andrey Kolmogorov discovered this formula by himself at the age of 5.

2. Basic Logic.

> "Logic is the hygiene which the mathematician uses to keep his ideas healthy and strong."
> – Hermann Weyl (1885 - 1955) (Taken from [Sib09])

The basic idea is to start from simple statements and then gradually build more complicated statements using logic operations:

- "and", "or";
- "not";
- "implication": If this then that; This only if that; This if that; ...
- quantifiers: For all such this, that is true.
  - Existential quantifier $\exists$: There is A such that B is true.
  - Universal quantifier $\forall$: For every $x \in A$, $P(x)$ is true.

The key is to define precisely how the truth of these compound statements depends on the true/false of the components. We will see that sometimes the mathematical meaning will be slightly different from the meaning of these words in everyday language.

Remark 16. When we assign precise meanings, we use definition.

2.1. Logic operations.

"and", "or", "not".

Definition 17. *Let A, B be mathematical statements. Then the following are also mathematical statements:*

- *"A and B", denoted $A \wedge B$;*
- *"A or B", denoted $A \vee B$;*
- *"Not A", denoted $\neg A$.*

The true/false of these new statements are determined from that of A, B by the following "truth table":

A	B	$A \wedge B$	$A \vee B$	$\neg A$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Table 1. *Truth table of "and", "or", "not".*

Here "T" means true, "F" means false.

We see that

- "A and B" and "not A" means roughly the same thing as in everyday language. For example,

$$(5 > 3) \ \wedge \ (6 > 4) \tag{16}$$

is a true statement, while

$$(3>5)\wedge(5>2) \tag{17}$$

is false.

- On the other hand, "A or B" in everyday language has two meanings: "one or the other, but not both", and "one or the other or both". In mathematics the latter meaning is agreed upon. Thus

$$(3>5)\vee(5>2) \tag{18}$$

is a true statement while

$$(3>5)\vee(1>2) \tag{19}$$

is false.

Such formal definition may seem an overkill for simple expressions like $5>3 \, \text{and} \, 6>4$, but it helps us to unravel more complicated expressions.

Example 18. Is the claim

$$[(5\,\text{is prime})\wedge(5>7)]\vee[\neg(4>5)] \tag{20}$$

true or false?

Solution. After judging the truth value of each inner-most claim, we reach

$$\begin{aligned}[(5\,\text{is prime})\wedge(5>7)]\vee[\neg(4>5)] &= (T\wedge F)\vee(\neg F)\\ &= F\vee T\\ &= T. \end{aligned} \tag{21}$$

So the statement is true.

Such formality also helps discovering equivalent statements.

Example 19. Show that $\neg(A\vee B)$ is equivalent to $(\neg A)\wedge(\neg B)$.

Proof. All we need to do is to show that the two statements have the same truth table. To construct such a table we need to replace A, B by all four cases $T, T; T, F; F, T; F, F$ and calculate the truth values. For example, in the case T, T, we have

$$\neg(A\vee B)=\neg(T\vee T)=\neg T=F; \tag{22}$$

$$(\neg A)\wedge(\neg B)=(\neg T)\wedge(\neg T)=F\wedge F=F. \tag{23}$$

After some calculation we conclude

A	B	$\neg(A\vee B)$	$(\neg A)\wedge(\neg B)$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

We see that both statements have exactly the same truth values and the proof ends. □

Exercise 7. Prove $\neg(\neg P)=P$.

Exercise 8. Compare $P\wedge(Q\vee R)$, $(P\wedge Q)\vee R$, $(P\wedge Q)\vee(P\wedge R)$. Which two of the three are equivalent?

2.2. Logic relations.

Implication.

As we have discussed, we need rules to show that one statement is the logical conclusion of the other. This is fulfilled in logic through "implication".

Definition 20. *Let A, B be mathematical statements. Then a new statement $A \Longrightarrow B$ is defined through the following truth table*

A	B	$A \Longrightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

and we define $A \Longleftarrow B$ to be $B \Longrightarrow A$.

Exercise 9. ([Sol10]) Jack: "If I do not get my car fixed, I will miss my job interview." We know that Jack's car is fixed and he missed the interview. Is his claim false?

Exercise 10. Prove that $A \Longrightarrow B$ is the same as $(\neg A) \vee B$.

Exercise 11. (Modus ponendo ponens)

a) Prove that for formula

$$((A \Longrightarrow B) \wedge A) \Longrightarrow B \tag{24}$$

is a tautology, that is always true.

b) Consider the following argument:

All dogs have four legs;
My table has four legs;
Therefore my table is a dog.

Show that such argument can be formalized as

$$((A \Longrightarrow B) \wedge B) \Longrightarrow A \tag{25}$$

c) Prove that the formula

$$((A \Longrightarrow B) \wedge (\neg B)) \Longrightarrow \neg A \tag{26}$$

(modus tollendo tollens).

Exercise 12. ([Bin80]) Let P be a statement. If $(\neg P) \Longrightarrow P$ is true, what can we say about P? Justify your answer.

Exercise 13. (Converse and contrapositive)

- Prove that $A \Longrightarrow B$ and its *converse* $B \Longrightarrow A$ are not equivalent.
- Prove that $A \Longrightarrow B$ and its *contrapositive* $\neg B \Longrightarrow \neg A$ are equivalent. Note that this is the foundation of an important proof strategy: Proof by contradiction.

Exercise 14. ([Sib09]) Write down the converse and contrapositive of the following statements.

a) If you don't study, your grade will suffer.

b) If I am worried, I don't sleep well.

c) If $x^2 - 4x + 4 = 0$, then $x = 2$.

d) I think therefore I am.

Exercise 15. ([Sol10]) If you want to show $A \Longrightarrow B$, and you can prove B is false. Then should you try to show A is true or false? Justify your answer.

Remark 21. "If" and "only if". As proofs are for humans instead of computers, people sometimes choose not to use $\Longrightarrow$ but use "if", "only if" instead. We agree that

- If P then Q means $P \Longrightarrow Q$;
- Q only if P means $Q \Longrightarrow P$.

The following all means $P \Longrightarrow Q$:

- P implies Q;
- Q is implied by P;

- Q if P;
- Q whenever P;
- P is sufficient for Q;
- Q is necessary for P;
- P only if Q.

Remark 22. The cost of a formal, precise definition is the following: If A turns out to be false, then $A \Longrightarrow B$ is always true. For example, the statement "if 5 is even then $x^2 + 1 < 0$" is a true statement. Such implication is called "vacuously true". It turns out that when dealing with meaningful problems, this caveat does not matter. However this rule may not be as absurd as it first looks like, see the following example.

Equivalence.

Definition 23. *Let A, B be mathematical statements. Then the new statement $A \Longleftrightarrow B$ are defined through the following truth table:*

A	B	$A \Longleftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Exercise 16. Show that

$$(A \Longleftrightarrow B) \Longleftrightarrow ((A \Longrightarrow B) \wedge (B \Longrightarrow A)) \tag{27}$$

is a tautology (that is, always true).

Can we conclude that $A \Longleftrightarrow B$ is equivalent to $(A \Longrightarrow B) \wedge (B \Longrightarrow A)$?

Remark 24. The following all mean $A \Longleftrightarrow B$:

- A if and only if B (sometimes written as A iff B);
- A and B are equivalent;
- A is sufficient and necessary for B;
- B is sufficient and necessary for A.

Exercise 17. Prove that $A \Longleftrightarrow B, B \Longleftrightarrow C$ then $A \Longleftrightarrow C$.

Remark 25. When proving $A \Longleftrightarrow B$, usually one has to prove $A \Longrightarrow B$ and $B \Longrightarrow A$ separately.

Example 26. Let m be an integer. Then m^2 is even if and only if m is even.

Proof. We need to prove

1. If: m is even $\Longrightarrow$ m^2 is even;
2. Only if: m^2 is even $\Longrightarrow$ m is even. □

2.3. Quantifiers and working negation.

Quantifiers.

We often use $\forall$ to denote the *universal quantifier* "for every", and $\exists$ to denote the *existential quantifier* "there exists".[5] Thus

$$\forall x \; \exists y, \qquad y > x. \tag{28}$$

means

$$\text{For every } x, \text{ there exists } y, \text{ such that } y > x. \tag{29}$$

Example 27. The order of the quantifiers is important. For example, the statement $\forall x \exists y,\ y > x$ is true, as we can take $y = x + 1$. On the other hand $\exists y \forall x,\ y > x$ is false. Because if there is such a y, we can simply take $x = y + 1$ and reveal the absurdity of the claim.

Working negation.

As we have seen, in situations such as proof by contradiction, we need to write down the negation of some mathematical statement. Simply adding "not" to the statement doesn't work. For example, if we try to prove by contradiction the conclusion "x is rational", starting from the assumption "Not (x is rational)" would not work. We need to write one more step:

$$\neg(x \text{ is rational}) \Longleftrightarrow x \text{ is not rational} \tag{30}$$

to obtain a form of the negation that we can work on. Such is called "working negation".

Example 28. (Negation of statements with quantifiers) Find the working negation of the following statement:

$$\forall x\ \exists y,\quad y > x.$$

Solution. It is $\exists x\ \forall y,\ y \leqslant x$.

- Rules for writing working negation.

  Let $P(x, y, z, \ldots.)$ be a mathematical statement involving $x, y, z\ldots.$. Then the working negation of

  $$\forall x\ \exists y\ \forall z \ldots P(x, y, z, \ldots.) \tag{31}$$

  is

  $$\exists x\ \forall y\ \exists z \ldots. \neg P(x, y, z, \ldots) \tag{32}$$

Remark 29. To write the working negation correctly, it is important to write the statement to be negated in the following form:

$$\text{(All quantifiers in correct order) (the mathmatical statement free of quantifiers)} \tag{33}$$

Example 30. A function $f(x)$ is bounded if and only if there is $M > 0$ such that for all x, $|f(x)| < M$. Write down the working negation of the statement "$f(x)$ is bounded".

Solution. First write down "$f(x)$ is bounded":

$$\exists M > 0\ \forall x\ |f(x)| < M. \tag{34}$$

Thus its negation is

$$\forall M > 0\ \exists x\ |f(x)| \geqslant M. \tag{35}$$

Remark 31. Note that the >0 in $M > 0$ didn't change. That is, if $P_1(x)$, $P_2(y)$, $P_3(z)$ are the conditions x, y, z satisfy in the statement,

$$\forall x P_1(x) \quad \exists y P_2(y) \quad \forall z P_3(z) \qquad P(x, y, z) \tag{36}$$

then its negation is

$$\exists x P_1(x) \quad \forall y P_2(y) \quad \exists z P_3(z) \qquad \neg P(x, y, z) \tag{37}$$

Note that P_1, P_2, P_3 should not be negated.[6]

5. Clearly $\exists$ comes from the first letter "E". On the other hand $\forall$ comes from "Any", but "for any" is ambiguous.

Exercise 18. (**[Sib09]**) Write down the working negation of the following statements.

a) We will win the next game, or we won't win the tournament.

b) You are my best friend, but I won't tell you my secret.

c) $(X \vee (\neg Y)) \wedge (\neg (Z \wedge (\neg X)))$.

d) $A \Longrightarrow B$.

e) $A \Longleftrightarrow B$.

2.4. Common proof strategies revisited.

Now we gain a deeper understanding of the proof methods.

- Hypothesis-Conclusion.

  The statement takes the form $P \Longrightarrow Q$.

  - Direct:
$$P \Longrightarrow P_1 \Longrightarrow P_2 \Longrightarrow \cdots \Longrightarrow P_k \Longrightarrow Q. \tag{41}$$
  - Forward-backward:
$$P \Longrightarrow P_1 \Longrightarrow P_2 \Longrightarrow \cdots \Longrightarrow M \tag{42}$$
$$Q \Longleftarrow Q_1 \Longleftarrow \cdots \Longleftarrow M. \tag{43}$$
  - Proof by contradiction:
$$(\neg Q \Longrightarrow (\neg P \vee \neg R)) \Longrightarrow ((P \wedge R) \Longrightarrow Q) \tag{44}$$

    Remark 32. Note that in proof by contradiction, the statement R represent all the mathematical facts besides P.

- Disproof.
  - To show the falsehood of
$$\forall x \qquad P(x) \tag{45}$$
    all we need to show is
$$\exists x \qquad \neg P(x). \tag{46}$$
    Note that we have formed the working negation of the statement!

- Mathematical Induction.
  - To show that all of the countably many statements $P(1), P(2), \ldots, P(n), \ldots$ to be true, it suffices to show

    i. $P(1)$;

    ii. $\forall n \geqslant 1 \ P(n) \Longrightarrow P(n+1)$.

Exercise 19. Prove that mathematical induction works. (Hint: Prove by contradiction.)

Exercise 20. Prove that the two variants (see Remark 12) of mathematical induction work.

---

6. Intuitively, the negation to
$$\forall \text{man on earth} \qquad \text{Statement } A \text{ is true} \tag{38}$$
should not be
$$\exists \text{alien} \qquad \text{Statement } A \text{ is false} \tag{39}$$
but should be
$$\exists \text{man on earth} \qquad \text{Statement } A \text{ is false.} \tag{40}$$

Further Readings.

- A very nice informal discussion of the why, what, and how of proofs can be found in [Gow02], Chapter 2.
- More detailed discussion of various strategies of proof can be found in [Cup05], [Sol10].
- Also see Chapters 1 – 3 of [Bin80]. In particular the one-page proof of "$a=a$" in Chapter 1.[7]

BIBLIOGRAPHY

[Bin80] K. G. Binmore. *The Foundations of Analysis: A Straightforward Introduction*. Cambridge University Press, 1980.

[Bur07] Edward B. Burger. *Extending the Frontiers of Mathematics: Inquiries into proof and argumentation*. Key College Publishing, 2007.

[Cup05] Antonella Cupillari. *The Nuts and Bolts of Proofs*. Elsevier, 3 edition, 2005.

[Gow02] Timothy Gowers. *Mathematics: A Very Short Introduction*. Oxford University Press, 2002.

[Hua02] Luogeng Hua. *Shu Xue Gui Na Fa (Mathematical Induction)*. Science Press, 2002.

[Kra11] Steven G. Krantz. *The Proof is in the Pudding: The Changing Nature of Mathematical Proof*. Springer, 2011.

[Lie06] Martin Liebeck. *A Concise Introduction to Pure Mathematics*. Chapman & Hall/CRC Mathematics, 2nd edition, 2006.

[Sib09] Thomas Q. Sibley. *Foundations of Mathematics*. John Wiley & Sons, 2009.

[Sol10] Daniel Solow. *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes*. John Wiley & Sons, 5 edition, 2010.

7. In Bertrand Russell and Alfred Whitehead's masterpiece *Principia Mathematica*, the great result $2+2=4$ is finally proved after about 1200 pages.