Chapter 3: Proofs

CS1231 Discrete Structures

Wong Tin Lok

National University of Singapore

2022/23 Semester 2

> [M]athematical rigor is like clothing: in its style it ought to suit the occasion, and it diminishes comfort and restricts freedom of movement if it is either too loose or too tight. Simmons (2017)

Proofs

What one can prove in computer science

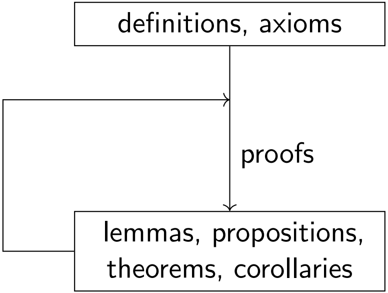
- A program or a circuit satisfies its specification.
- A machine never reaches an undesirable state.
- The resources used by a program is (or cannot be) within specific bounds.

> (i) The point of solving problems is to understand mathematics better.
>
> (ii) The point of understanding mathematics is to become better able to solve problems.
>
> Most mathematicians would say that there is truth in both (i) and (ii). Not all problems are equally interesting, and one way of distinguishing the more interesting ones is to demonstrate that they improve our understanding of mathematics as a whole. Equally, if somebody spends many years struggling to understand a difficult area of mathematics, but does not actually do anything with this understanding, then why should anybody else care? Gowers (2000)

Plan:

- mathematical theories
- proof techniques

Mathematical theories



definitions, axioms

proofs

lemmas, propositions, theorems, corollaries

Definitions: even and odd integers

Terminology 3.1.1

A *definition* is a description of what a (newly introduced) piece of terminology or notation exactly means and does not mean.

Definition 3.1.2

(1) An integer is *even* if it is $2x$ for some integer x.

(2) An integer is *odd* if it is $2x + 1$ for some integer x.

Example 3.1.3

(1) The integer 0 is even because $0 = 2 \times 0$, where 0 is an integer.

(2) The integer -1231 is odd because $-1231 = 2 \times (-616) + 1$, where -616 is an integer.

Definitions: strings

Definition 3.1.4

(1) An *alphabet* is a set of symbols.

(2) A *string* over an alphabet Γ is a finite sequence of symbols from Γ.

(3) The set of all strings over an alphabet Γ is denoted Γ^*.

(4) The *length* of a string is the number of symbols the string has (including repetition).

Example 3.1.5

Let Γ be the set that consists precisely of the symbols $\mathsf{A}, \mathsf{B}, \ldots, \mathsf{Z}, 0, 1, 2, \ldots, 9$, and let Φ be the set that consists precisely of the symbols $\mathsf{A}, \mathsf{B}, \ldots, \mathsf{Z}, \mathsf{a}, \mathsf{b}, \ldots, \mathsf{z}$.

(1) Γ and Φ are alphabets.

(2) CS1231 is a string over Γ, but it is not a string over Φ.

(3) $\text{CS1231} \in \Gamma^*$, but $\text{CS1231} \notin \Phi^*$.

(4) The length of the string CS1231 is 6.

Axioms

Terminology 3.1.6

Axioms are propositions that are taken (without proof) to be true in a theory, to specify which objects the theory is about.

Note 3.1.7

Even for the same mathematical theory, one may choose different (but equivalent) axioms in different contexts.

> [The] grand aim of all science [is] to cover the greatest number of empirical facts by logical deduction from the smallest possible number of hypotheses or axioms.
>
> Einstein, as quoted by Barnett (1957)

Axioms: inclusions and operations

$\mathbb{R}$ **includes** $\mathbb{Q}$	$\forall x \in \mathbb{Q}$	$x \in \mathbb{R}.$
$\mathbb{Q}$ **includes** $\mathbb{Z}$	$\forall x \in \mathbb{Z}$	$x \in \mathbb{Q}.$
$\mathbb{Z}$ **includes** $\mathbb{N}$	$\forall x \in \mathbb{N}$	$x \in \mathbb{Z}.$
Closure of $\mathbb{R}$ **under** $+$	$\forall x, y \in \mathbb{R}$	$x + y \in \mathbb{R}.$
Closure of $\mathbb{R}$ **under negatives**	$\forall x \in \mathbb{R}$	$-x \in \mathbb{R}.$
Definition of $-$	$\forall x, y \in \mathbb{R}$	$x - y = x + (-y).$
Closure of $\mathbb{R}$ **under** $\times$	$\forall x, y \in \mathbb{R}$	$x \cdot y \in \mathbb{R}.$
Closure of $\mathbb{R}$ **under reciprocals**	$\forall x \in \mathbb{R}$	$\left(x \neq 0 \to \frac{1}{x} \in \mathbb{R}\right).$
Definition of $/$	$\forall x, y \in \mathbb{R}$	$\left(y \neq 0 \to \frac{x}{y} = x \cdot \frac{1}{y}\right).$

Axioms: $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$

Naturality of 0 $\qquad 0 \in \mathbb{N}.$

Closure of $\mathbb{N}$ under $+1$ $\qquad \forall x \in \mathbb{N} \quad x + 1 \in \mathbb{N}.$

Induction Every set of natural numbers that contains 0 and is closed under the successor function must contain all natural numbers, i.e., for every set A of natural numbers,

$$0 \in A \wedge (\forall x \in A \;\; x + 1 \in A) \to \forall x \in \mathbb{N} \;\; x \in A.$$

Definition of $\mathbb{Z}$ $\qquad \forall x \in \mathbb{R} \quad (x \in \mathbb{Z} \leftrightarrow x \in \mathbb{N} \vee -x \in \mathbb{N}).$

Definition of $\mathbb{Q}$ $\qquad \forall x \in \mathbb{R} \quad \left(x \in \mathbb{Q} \leftrightarrow \exists y, z \in \mathbb{Z} \;\; \left(z \neq 0 \wedge x = \frac{y}{z}\right)\right).$

Axioms: algebraic properties

Associativity of $+$	$\forall x, y, z \in \mathbb{R}$	$(x+y)+z = x+(y+z).$
Associativity of $\cdot$	$\forall x, y, z \in \mathbb{R}$	$(x \cdot y) \cdot z = x \cdot (y \cdot z).$
Identity for $+$	$\forall x \in \mathbb{R}$	$x+0 = x.$
Identity for $\cdot$	$\forall x \in \mathbb{R}$	$x \cdot 1 = x.$
Inverse for $+$	$\forall x \in \mathbb{R}$	$x+(-x) = 0.$
Inverse for $\cdot$	$\forall x \in \mathbb{R}$	$\left(x \neq 0 \rightarrow x \cdot \frac{1}{x} = 1\right).$
Commutativity of $+$	$\forall x, y \in \mathbb{R}$	$x+y = y+x.$
Commutativity of $\cdot$	$\forall x, y \in \mathbb{R}$	$x \cdot y = y \cdot x.$
Distributivity of $\cdot$ **over** $+$	$\forall x, y, z \in \mathbb{R}$	$x \cdot (y+z) = (x \cdot y)+(x \cdot z).$

Axioms: order properties

Irreflexivity of $<$	$\forall x \in \mathbb{R} \quad x \not< x.$
Trichotomy	$\forall x, y \in \mathbb{R} \quad (x < y \vee x = y \vee y < x).$
Transitivity of $<$	$\forall x, y, z \in \mathbb{R} \quad (x < y \wedge y < z \to x < z).$
$+$ respects $<$	$\forall x, y, z \in \mathbb{R} \quad (x < y \to x + z < y + z).$
Closure of $\mathbb{R}^+$ under $\cdot$	$\forall x, y \in \mathbb{R} \quad (x > 0 \wedge y > 0 \to x \cdot y > 0).$
Completeness	Every nonempty set of real numbers that has an upper bound in $\mathbb{R}$ must have a smallest upper bound in $\mathbb{R}$, i.e., for every nonempty set A of real numbers, $\exists b \in \mathbb{R}\ \forall x \in A\ x < b$ $\to \exists b^* \in \mathbb{R}\ \big(\forall x \in A\ x < b^*$ $\wedge \forall b \in \mathbb{R}\ \big((\forall x \in A\ x < b) \to b^* \leqslant b\big)\big).$

Proofs and deductions

Terminology 3.1.8

In mathematics, a *proof* of a proposition is a carefully reasoned argument, which may invoke definitions, axioms and previously established propositions, for convincing the reader/audience that the proposition is true beyond doubt.

Notation 3.1.9

quod erat demonstrandum

The end of a proof is often marked by $\square$. Some authors use ■, $\dashv$, or QED.

Terminology 3.1.10

One *(logically) deduces* a proposition q from propositions $p_1, p_2, \ldots, p_n$ if the forms of $p_1, p_2, \ldots, p_n, q$ alone (without involving the subject matter) guarantee that q is true whenever $p_1, p_2, \ldots, p_n$ are all true.

picture proofs?

Note 3.1.16

Typically, a proof in mathematics consists of a number of steps. Each step either comes from the definitions, the axioms or previously established propositions, or is deduced logically from the previous steps.

Modus ponens

Example 3.1.11

Let p, q be propositions. From $p \to q$ and p, one can deduce q.

Justification

As one can see from the following truth table, the only situation when $p \to q$ and p are both true is when q is also true.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

□

Exercise 3.1.12

Let p, q be propositions. From $p \to q$ and $\neg p$, can one deduce $\neg q$ in general? ✎ 3a

Universal instantiation

Example 3.1.13

Let $P(x)$ be a sentence and z be an object. From $\forall x\ P(x)$, one can deduce $P(z)$.

Justification

This follows directly from Definition 2.2.1(3), in which we defined exactly when $\forall x\ P(x)$ is true. □

Transitivity of the conditional and the biconditional

Example 3.1.14

Let p, q, r be propositions. From $p \to q$ and $q \to r$, one can deduce $p \to r$.

$$\begin{array}{rl} & p \to q \\ & q \to r \\ \therefore & p \to r \end{array}$$

Justification

This is based on the tautology from Tutorial Exercise 1.5. □

Example 3.1.15

Let p, q, r be propositions. From $p \leftrightarrow q$ and $q \leftrightarrow r$, one can deduce $p \leftrightarrow r$.

$$\begin{array}{rl} & p \leftrightarrow q \\ & q \leftrightarrow r \\ \therefore & p \leftrightarrow r \end{array}$$

Justification

This is based on Tutorial Exercise 1.4 and the transitivity of the conditional. □

Notation 3.1.17

In a proof, one sometimes write $\therefore\ p$ in the case when p is a proposition to indicate that p is deduced logically from the immediately preceding step(s). One may read $\therefore$ as "therefore".

Chains of equivalences

Notation 3.1.18

Many proofs use the transitivity of the biconditional in the form

$$\begin{array}{rl} & p_1 \leftrightarrow p_2. \\ & p_2 \leftrightarrow p_3. \\ & \vdots \\ & p_{n-1} \leftrightarrow p_n. \\ \therefore & p_1 \leftrightarrow p_n. \end{array}$$

One may write this more succinctly as

$$\begin{aligned} p_1 &\Leftrightarrow p_2 \\ &\Leftrightarrow p_3 \\ &\vdots \\ &\Leftrightarrow p_n. \end{aligned}$$

Note 3.1.19

(1) One may use $\Leftrightarrow$ for $\leftrightarrow$, but not vice versa, because their meanings are essentially the same between two propositions.

(2) In fact, it is common practice to use $\Leftrightarrow$ exclusively in mathematical contexts where logic is not the subject matter. We will follow this common practice.

Chains of implications

Notation 3.1.18

Many proofs use the transitivity of the conditional in the form

$$\begin{aligned} p_1 &\to p_2. \\ p_2 &\to p_3. \\ &\vdots \\ p_{n-1} &\to p_n. \\ \therefore\ \ p_1 &\to p_n. \end{aligned}$$

One may write this more succinctly as

$$\begin{aligned} p_1 &\Rightarrow p_2 \\ &\Rightarrow p_3 \\ &\vdots \\ &\Rightarrow p_n. \end{aligned}$$

Note 3.1.19

(1) One may use ⇒ for →, but not vice versa, because their meanings are essentially the same between two propositions.

(2) In fact, it is common practice to use ⇒ exclusively in mathematical contexts where logic is not the subject matter. We will follow this common practice.

Bootstrapping (1/3)

Base clause for exp	$\forall x \in \mathbb{R}$	$x^0 = 1.$
Recursion clause for exp	$\forall x \in \mathbb{R}\ \forall y \in \mathbb{N}$	$x^{y+1} = x^y \cdot x.$
Definition of $\leqslant$	$\forall x, y \in \mathbb{R}$	$(x \leqslant y \leftrightarrow x < y \vee x = y).$
Closure of $\mathbb{Z}$ under $+$	$\forall x, y \in \mathbb{Z}$	$x + y \in \mathbb{Z}.$
Closure of $\mathbb{Z}$ under $-$	$\forall x, y \in \mathbb{Z}$	$x - y \in \mathbb{Z}.$
Closure of $\mathbb{Z}$ under $\times$	$\forall x, y \in \mathbb{Z}$	$x \cdot y \in \mathbb{Z}.$
Closure of $\mathbb{Q}$ under $+$	$\forall x, y \in \mathbb{Q}$	$x + y \in \mathbb{Q}.$
Closure of $\mathbb{Q}$ under $-$	$\forall x, y \in \mathbb{Q}$	$x - y \in \mathbb{Q}.$
Closure of $\mathbb{Q}$ under $\times$	$\forall x, y \in \mathbb{Q}$	$x \cdot y \in \mathbb{Q}.$
Closure of $\mathbb{Q}$ under $/$	$\forall x, y \in \mathbb{Q}$	$\left(y \neq 0 \rightarrow \dfrac{x}{y} \in \mathbb{Q}\right).$
$\mathbb{N} = \mathbb{Z}_{\geqslant 0}$	$\forall x \in \mathbb{R}$	$(x \in \mathbb{N} \leftrightarrow x \in \mathbb{Z} \wedge x \geqslant 0)$
Discreteness of $\mathbb{N}$	$\forall x \in \mathbb{N}$	$(x > 0 \rightarrow x \geqslant 1).$
Cancellation Law for $+$	$\forall x, y_1, y_2 \in \mathbb{R}$	$(x + y_1 = x + y_2 \rightarrow y_1 = y_2).$
Differences	$\forall x, z \in \mathbb{R}$	$x + (z - x) = z.$
Differences and negatives	$\forall x, z \in \mathbb{R}$	$z - x = z + (-x).$
Double negatives	$\forall x \in \mathbb{R}$	$-(-x) = x.$
Distributivity of $\cdot$ over $-$	$\forall x, y, z \in \mathbb{R}$	$x \cdot (y - z) = (x \cdot y) - (x \cdot z).$
Annihilator for $\times$	$\forall x \in \mathbb{R}$	$x \cdot 0 = 0.$
Cancellation Law for $\cdot$	$\forall x, y_1, y_2 \in \mathbb{R}$	$(x \neq 0 \wedge x \cdot y_1 = x \cdot y_2 \rightarrow y_1 = y_2).$

Bootstrapping (2/3)

Quotients	$\forall x, z \in \mathbb{R}$	$\left(x \neq 0 \to x \cdot \frac{z}{x} = z\right).$
Double reciprocals	$\forall x \in \mathbb{R}$	$\left(x \neq 0 \to \frac{1}{1/x} = x\right).$
Zero divisors	$\forall x, y \in \mathbb{R}$	$(x \cdot y = 0 \to x = 0 \vee y = 0).$
Products and negatives	$\forall x, y \in \mathbb{R}$	$((-x) \cdot y = x \cdot (-y) \ \wedge\ x \cdot (-y) = -(x \cdot y)).$
	$\forall x, y \in \mathbb{R}$	$(-x) \cdot (-y) = x \cdot y.$
Quotients and negatives	$\forall x, y \in \mathbb{R}$	$\left(y \neq 0 \to \frac{-x}{y} = \frac{x}{-y} \ \wedge\ \frac{x}{-y} = -\frac{x}{y}\right).$
	$\forall x, y \in \mathbb{R}$	$\left(y \neq 0 \to \frac{-x}{-y} = \frac{x}{y}\right).$
Fraction equivalence	$\forall x, y, z \in \mathbb{R}$	$\left(y \neq 0 \wedge z \neq 0 \to \frac{x}{y} = \frac{x \cdot z}{y \cdot z}\right).$
Fraction addition	$\forall u, v, x, y \in \mathbb{R}$	$\left(v \neq 0 \wedge y \neq 0 \to \frac{u}{v} + \frac{x}{y} = \frac{u \cdot y + v \cdot x}{v \cdot y}\right).$
Fraction multiplication	$\forall u, v, x, y \in \mathbb{R}$	$\left(v \neq 0 \wedge y \neq 0 \to \frac{u}{v} \cdot \frac{x}{y} = \frac{u \cdot x}{v \cdot y}\right).$
Fraction division	$\forall u, v, x, y \in \mathbb{R}$	$\left(v \neq 0 \wedge x \neq 0 \wedge y \neq 0 \to \frac{u/v}{x/y} = \frac{u \cdot y}{v \cdot x}\right).$

Bootstrapping (3/3)

Closure of $\mathbb{R}^+$ under $+$	$\forall x, y \in \mathbb{R}$	$(x > 0 \land y > 0 \to x + y > 0)$.
Positivity of negatives	$\forall x \in \mathbb{R}$	$((x > 0 \lor x = 0 \lor -x > 0) \ \land \ \neg(x > 0 \land -x > 0))$.
	$\forall x \in \mathbb{R}$	$(x < 0 \to -x > 0)$.
Positivity of one		$1 > 0$.
Positivity of products	$\forall x, y \in \mathbb{R}$	$(x \cdot y > 0 \to (x > 0 \land y > 0) \lor (x < 0 \land y < 0)))$.
Positivity of squares	$\forall x \in \mathbb{R}$	$(x \neq 0 \to x^2 > 0)$.
Positivity and $<$	$\forall x, y \in \mathbb{R}$	$(x < y \leftrightarrow y - x > 0)$.
$+$ respects $<$	$\forall u, v, x, y \in \mathbb{R}$	$(u < v \land x < y \to u + x < v + y)$.
Negatives and $<$	$\forall x, y \in \mathbb{R}$	$(x < y \to -y < -x)$.
$\cdot$ and $<$	$\forall x, y, z \in \mathbb{R}$	$(x < y \land z > 0 \to x \cdot z < y \cdot z)$.
	$\forall x, y, z \in \mathbb{R}$	$(x < y \land z < 0 \to x \cdot z > y \cdot z)$.
	$\forall u, v, x, y \in \mathbb{R}$ $(u > 0 \land x > 0 \land u < v \land x < y \to u \cdot x > 0 \land u \cdot x < v \cdot y)$.	
Strict trichotomy	$\forall x, y \in \mathbb{R}$	$(\neg(x < y \land x = y) \land \neg(x = y \ \land \ y < x) \land \neg(y < x \land x < y))$.
Archimedean property of $\mathbb{R}$	$\forall x \in \mathbb{R} \ \exists y \in \mathbb{N}$	$y > x$.

Propositions that have proofs

Terminology 3.1.20

(1) A *theorem* is a proposition that has a proof and is often of considerable significance (in the particular context).

(2) A *proposition* sometimes refers to a proposition in the sense of Definition 1.1.1 that has a proof and is of medium significance (in the particular context).

(3) A *lemma* is a proposition that has a proof and helps in the proofs of other propositions, but on its own is of little significance (in the particular context).

(4) A *corollary* is a proposition that can be deduced easily from other previously established propositions.

Witnesses

Technique 3.2.1

To prove $\exists x \; P(x)$, where $P(x)$ is a sentence, produce a witness, i.e., an object z for which $P(z)$ is true.

Proposition 3.2.2

Some even integer n satisfies $n^2 = 2n$.

Proof

The integer 2 is even because $2 = 2 \times 1$ where 1 is an integer. Also $2^2 = 4 = 2 \times 2$. □

To prove a conditional directly

Technique 3.2.3

One way to prove $p \to q$, where p, q are propositions, is to assume p is true, then prove (from this assumption) that q must also be true.

Proposition 3.2.4

The square of any even integer is even.

If n is an even integer, then n^2 is an even integer.

Proof

Let n be an even integer. Use the definition of even integers to find an integer x such that $n = 2x$. Then $n^2 = (2x)^2 = 2(2x^2)$, where $2x^2$ is an integer. So n^2 is even by the definition of even integers. □

Convention 3.2.5

In proofs, when there is no risk of ambiguity, it is sometimes convenient and instructive to use the same letter for both a variable and an object to be substituted into that variable.

Exercise about negatives

Exercise 3.2.6

Let n be an integer. Prove that ✎ 3b

(1) if n is even, then $-n$ is even;

(2) if n is odd, then $-n$ is odd.

Proofs by contraposition

Technique 3.2.7

One way to prove $p \to q$, where p, q are propositions, is to assume q is false, then prove (from this assumption) that p must also be false.

Justification

This is based on the equivalence of a conditional proposition $p \to q$ and its contrapositive $\neg q \to \neg p$ from Theorem 1.4.12(1). □

Proposition 3.2.8

Any integer whose square is even must itself be even.

For every integer n,
if n^2 is even,
then n is even.

Proof

Let n be an integer that is not even. Then n is odd. Use the definition of odd integers to find an integer x such that $n = 2x + 1$. Then $n^2 = (2x+1)^2 = 4x^2 + 4x + 1 = 2(x^2 + 2x) + 1$, where $x^2 + 2x$ is an integer. So n^2 is odd by the definition of odd integers. This implies n^2 is not even, as required. □

Equivalences

Technique 3.2.9

One way to prove $p \leftrightarrow q$, where p, q are propositions, is to prove both $p \rightarrow q$ and $q \rightarrow p$.

Justification

This is based on the equivalence of $p \leftrightarrow q$ and $(p \rightarrow q) \wedge (q \rightarrow p)$ from Tutorial Exercise 1.4. □

Corollary 3.2.10

An integer is even if and only if its square is even.

Proof

The "$\leftarrow$" part is given by Proposition 3.2.8. The "$\rightarrow$" part is given by Proposition 3.2.4. □

Splitting into cases

Technique 3.2.11

One way to prove a proposition r is to first find two propositions p and q such that either p or q is true, and then prove r from each of p and q.

Proposition 3.2.12

If n is an integer, then $n(n+1)$ is even.

Tautology involved:
$(p \vee q) \wedge (p \to r) \wedge (q \to r) \to r$.

Proof

We split into two cases.

Case 1: suppose n is even. Use the definition of even integers to find an integer x such that $n = 2x$. Then $n(n+1) = (2x)(2x+1) = 2(x(2x+1))$, where $x(2x+1)$ is an integer. So $n(n+1)$ is even.

Case 2: suppose n is odd. Use the definition of odd integers to find an integer x such that $n = 2x+1$. Then $n(n+1) = (2x+1)((2x+1)+1) = 2((2x+1)(x+1))$, where $(2x+1)(x+1)$ is an integer. So $n(n+1)$ is even.

So $n(n+1)$ is even in all cases. □

Exhaust all the cases!

Remark 3.2.13

One can split into more than two cases in a proof, say $p_1, p_2, \ldots, p_n$ where each p_i is a proposition, but one must make sure that these p_i's cover all possibilities, i.e., that $p_1 \vee p_2 \vee \cdots \vee p_n$ must be true.

Note 3.2.14

(1) We used implicitly in the proof of Proposition 3.2.12 that *every integer is either even or odd*, i.e., Proposition 3.2.21.

(2) In addition to Proposition 3.2.21, we used implicitly in the proof of Proposition 3.2.8 that *no integer is both even and odd*, i.e., Proposition 3.2.17.

(3) Formally Propositions 3.2.17 and 3.2.21 should appear before Propositions 3.2.12 and 3.2.8, and we should not use Propositions 3.2.12 and 3.2.8 in our proofs of Propositions 3.2.17 and 3.2.21.

Any integer whose square is even must itself be even.

Proof

1. Let n be an integer that is not even.
2. Then n is odd.
3. Use the definition of odd integers to find an integer x such that $n = 2x + 1$.
4. Then $n^2 = (2x+1)^2 = 4x^2 + 4x + 1 = 2(x^2 + 2x) + 1$, where $x^2 + 2x$ is an integer.
5. So n^2 is odd by the definition of odd integers.
6. This implies n^2 is not even, as required. □

Exercise 3.2.15

(1) In which step did we use the fact that every integer is either even or odd?

(2) In which step did we use the fact that no integer is both even and odd? ✐ 3c

Proof by contradiction, also known as *reductio ad absurdum*

Technique 3.2.16

One way to prove a proposition p is to assume that p is false, then prove (from this assumption) a contradiction.

Tautology involved: $(\neg p \to c) \to p$.

Proposition 3.2.17

No integer is both even and odd.

Proof

Suppose some integer, say n, is both even and odd. Use the definition of even and odd integers to find integers x, y such that $n = 2x$ and $n = 2y + 1$. As x and y are both integers, so is $x - y$, but

$$x - y = \frac{n}{2} - \frac{n-1}{2} = \frac{1}{2},$$

which is not an integer. So we have a contradiction. It follows that no integer can be both even and odd. □

(Extra) Explain why. ✏ 3d

Induction

Technique 3.2.19 (Mathematical Induction (MI))

Let b be an integer and $P(n)$ be a predicate over $\mathbb{Z}_{\geqslant b}$. To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to:

(base step) show that $P(b)$ is true; and

(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant b}\ \ \big(P(k) \to P(k+1)\big)$ is true.

induction hypothesis

Justification

The two steps ensure the following are true:

$$\begin{array}{ll}
P(b) & \text{by the base step;} \\
P(b) \to P(b+1) & \text{by the induction step with } k = b; \\
P(b+1) \to P(b+2) & \text{by the induction step with } k = b+1; \\
P(b+2) \to P(b+3) & \text{by the induction step with } k = b+2; \\
\vdots &
\end{array}$$

One by one, we deduce that $P(b), P(b+1), P(b+2), \ldots$ are all true. □

Induction: example

Proposition 3.2.21

Every integer is either even or odd.

Proof

In view of Exercise 3.2.6, it suffices to show that every non-negative integer is either even or odd. We prove this by MI.

induction *on n*

Let $P(n)$ be the predicate "n is either even or odd" over $\mathbb{Z}_{\geqslant 0}$.

(Base step) We know $0 = 2 \times 0$, where 0 is an integer. So 0 is even. Thus $P(0)$ is true.

(Induction step) Let k be a non-negative integer such that $P(k)$ is true, i.e., that k is either even or odd.

- If k is even, say $k = 2x$ where x is an integer, then $k + 1 = 2x + 1$, which is odd.
- If k is odd, say $k = 2x + 1$ where x is an integer, then $k + 1 = 2x + 2 = 2(x + 1)$, which is even.

So $k + 1$ is either even or odd in all cases. This shows $P(k + 1)$ is true.

Hence $\forall n \in \mathbb{Z}_{\geqslant 0}\ \ P(n)$ is true by MI. □

Strong MI

Technique 3.2.23 (Strong Mathematical Induction (Strong MI))

Let b be an integer and $P(n)$ be a predicate over $\mathbb{Z}_{\geqslant b}$. To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to choose some integer $c \geqslant b$ and:

(base step) show that $P(b), P(b+1), \ldots, P(c)$ are true;

(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant c}\ \ \big(P(b) \wedge P(b+1) \wedge \cdots \wedge P(k) \rightarrow P(k+1)\big)$ is true.

(Extra) $c = b - 1$? ✎ 3e

Justification

The two steps ensure the following are true:

$P(b) \wedge \cdots \wedge P(c)$ by the base step;

$P(b) \wedge \cdots \wedge P(c) \rightarrow P(c+1)$ by the indn step with $k = c$;

$P(b) \wedge \cdots \wedge P(c) \wedge P(c+1) \rightarrow P(c+2)$ by the indn step with $k = c+1$;

$P(b) \wedge \cdots \wedge P(c) \wedge P(c+1) \wedge P(c+2) \rightarrow P(c+3)$ by the indn step with $k = c+2$;

$\vdots$

One by one, we deduce that $P(b), P(b+1), P(b+2), P(b+3), \ldots$ are all true. □

Strong MI: example (1/2)

Proposition 3.2.24

For every positive integer n, $\underbrace{\text{there exist a non-negative integer } a \text{ and an odd integer } b \text{ such that } n = 2^a b.}_{P(n)}$

Proof

(Base step) $P(1)$ is true because $1 = 2^0 \times 1$, where 0 is a non-negative integer and 1 is an odd integer.

(Induction step) Let k be a positive integer such that $P(1), P(2), \ldots, P(k)$ are all true. Proposition 3.2.21 tells us that $k+1$ is either even or odd.

Case 1: suppose $k+1$ is even. [. . .]

Case 2: suppose $k+1$ is odd. Then $k+1 = 2^0(k+1)$, where 0 is a non-negative integer.

So $P(k+1)$ is true in all cases.

Hence $\forall n \in \mathbb{Z}_{\geqslant 1}$ $P(n)$ is true by Strong MI.

Strong MI: example (2/2)

Proposition 3.2.24

For every positive integer n, $\underbrace{\text{there exist a non-negative integer } a \text{ and an odd integer } b \text{ such that } n = 2^a b.}_{P(n)}$

Proof

(Base step) $P(1)$ is true [. . .]

(Induction step) Let k be a positive integer such that $P(1), P(2), \ldots, P(k)$ are all true. Proposition 3.2.21 tells us that $k+1$ is either even or odd.

Case 1: suppose $k+1$ is even. Use the definition of even integers to find an integer x such that $k+1 = 2x$. As $k \geqslant 1$,

$$x = \frac{k+1}{2} \geqslant \frac{1+1}{2} = 1 \quad \text{and} \quad 2k = k + k \geqslant k + 1 = 2x.$$

Thus $1 \leqslant x \leqslant k$ and so $P(x)$ is true by the induction hypothesis. Find a non-negative integer a and an odd integer b such that $x = 2^a b$. Then $k + 1 = 2x = 2(2^a b) = 2^{a+1} b$, where $a + 1$ is a non-negative integer.

Case 2: suppose $k+1$ is odd. [. . .]

So $P(k+1)$ is true in all cases. [. . .]

Are a and b unique? ✏ 3f

□

Unique existence

Definition 3.2.26

Let $P(x)$ be a sentence. Then "there exists a unique x such that $P(x)$", sometimes denoted $\exists! x\ P(x)$, means the conjunction of the two propositions below.

(existence) "There is at least one x such that $P(x)$", or symbolically $\exists x\ P(x)$.

(uniqueness) "There is at most one x such that $P(x)$", or symbolically

$$\forall x_1, x_2\ \big(P(x_1) \wedge P(x_2) \to x_1 = x_2\big).$$

Unique existence: example

Proposition 3.2.27

For all odd numbers m, n, there exists a unique integer a such that $m^2 + n^2 = 4a + 2$.

Proof

(Existence) Use the definition of odd numbers to find integers x, y such that $m = 2x + 1$ and $n = 2y + 1$. Then

$$m^2+n^2 = (2x+1)^2+(2y+1)^2 = 4x^2+4x+1+4y^2+4y+1 = 4(x^2+x+y^2+y)+2,$$

where $x^2 + x + y^2 + y$ is an integer.

(Uniqueness) Suppose a_1, a_2 are integers such that $m^2 + n^2 = 4a_1 + 2$ and $m^2 + n^2 = 4a_2 + 2$. Then $4a_1 + 2 = 4a_2 + 2$. Subtract 2 from both sides, then divide both sides by 4. Then we see that $a_1 = a_2$. □

Common proof techniques

Technique 3.2.1. To prove $\exists x\ P(x)$, where $P(x)$ is a sentence, produce a witness, i.e., an object z for which $P(z)$ is true.

Technique 3.2.3. One way to prove $p \to q$, where p, q are propositions, is to assume p is true, then prove (from this assumption) that q must also be true.

Technique 3.2.7 (proof by contraposition). One way to prove $p \to q$, where p, q are propositions, is to assume q is false, then prove (from this assumption) that p must also be false.

Technique 3.2.9. One way to prove $p \leftrightarrow q$, where p, q are propositions, is to prove both $p \to q$ and $q \to p$.

Technique 3.2.11 (splitting into cases). One way to prove a proposition r is to first find two propositions p and q such that either p or q is true, and then prove r from each of p and q.

Technique 3.2.16 (proof by contradiction). One way to prove a proposition p is to assume that p is false, then prove (from this assumption) a contradiction.

Induction

Let b be an integer and $P(n)$ be a predicate over $\mathbb{Z}_{\geqslant b}$.

Technique 3.2.19 (Mathematical Induction (MI))

To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to:

(base step) show that $P(b)$ is true; and

(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant b}\ \ \big(P(k) \to P(k+1)\big)$ is true.

Technique 3.2.23 (Strong Mathematical Induction (Strong MI))

To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to choose some integer $c \geqslant b$ and:

(base step) show that $P(b), P(b+1), \ldots, P(c)$ are true;

(induction step) show that $\forall k \in \mathbb{Z}_{\geqslant c}\ \ \big(P(b) \wedge P(b+1) \wedge \cdots \wedge P(k) \to P(k+1)\big)$ is true.

Definition 3.2.26

Let $Q(x)$ be a sentence. Then "there exists a unique x such that $Q(x)$", sometimes denoted $\exists! x\ Q(x)$, means the conjunction of the two propositions below.

(existence) "There is at least one x such that $Q(x)$", or symbolically $\exists x\ Q(x)$.

(uniqueness) "There is at most one x such that $Q(x)$", or symbolically

$$\forall x_1, x_2\ \big(Q(x_1) \wedge Q(x_2) \to x_1 = x_2\big).$$

A complete list? Natural deduction

EXTRA MATERIAL

$$\wedge\mathrm{I}\ \frac{\varphi \qquad \psi}{\varphi \wedge \psi} \qquad\qquad \frac{\varphi \wedge \psi}{\varphi}\ \wedge\mathrm{E}_1 \qquad\qquad \frac{\varphi \wedge \psi}{\psi}\ \wedge\mathrm{E}_2$$

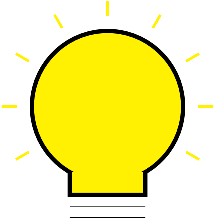
$$\vee\mathrm{I}_1\ \frac{\varphi}{\varphi \vee \psi} \qquad\qquad \vee\mathrm{I}_2\ \frac{\psi}{\varphi \vee \psi} \qquad\qquad \frac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]\\ \vdots\\ \theta\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots\\ \theta\end{array}}{\theta}\ \vee\mathrm{E}$$

$$\to\mathrm{I}\ \frac{\begin{array}{c}[\varphi]\\ \vdots\\ \psi\end{array}}{\varphi \to \psi} \qquad\qquad \frac{\varphi \qquad \varphi \to \psi}{\psi}\ \to\mathrm{E} \qquad\qquad \neg\mathrm{I}\ \frac{\begin{array}{c}[\varphi]\\ \vdots\\ \psi \wedge \neg\psi\end{array}}{\neg\varphi} \qquad\qquad \frac{\neg\neg\varphi}{\varphi}\ \neg\mathrm{E}$$

$$\forall\mathrm{I}\ \frac{\varphi(a)}{\forall x\ \varphi(x)} \qquad\qquad \frac{\forall x\ \varphi(x)}{\varphi(a)}\ \forall\mathrm{E} \qquad\qquad \exists\mathrm{I}\ \frac{\varphi(a)}{\exists x\ \varphi(x)} \qquad\qquad \frac{\exists x\ \varphi(x) \qquad \begin{array}{c}[\varphi(a)]\\ \vdots\\ \psi\end{array}}{\psi}\ \exists\mathrm{E}$$

No magic formula

In English the word "problem" has negative connotations, suggesting some unwanted and unresolved tension. [. . .] Good problems focus the mind: they challenge and frustrate; they cultivate ambition and humility; they show up the limitations of what we know, and highlight potential sources of more powerful ideas. By contrast, the word "solving" suggests a *release* of tension. The juxtaposition of these two words in the expression "problem solving" may encourage the naive to think that this unwelcome tension can be massaged away by means of some "magic formula" or process. It cannot; there is no magic formula. Gardiner (2008)



Proof-writing advice for beginners

- In general, there is no algorithm that can tell whether any given proposition has a proof or not.
- When asked to prove a proposition, understand what the proposition means, and try to see why it is true intuitively.
- One can build up some intuition by drawing some pictures, trying some small examples, studying the theory developed, etc.
- The shape of a simple proof often resembles the shape of the proposition it proves.
- Start a proof with what you have and what you want, separately. Expand them using the definitions and the known facts until the two meet.
- There is often more than one way to prove a proposition.
- Write a proof in the way you would convince the reader the truth of the proposition. This is often *not* the way you discovered the proof.
- Be prepared to give more detailed justification for almost every step you make in your proof when challenged.