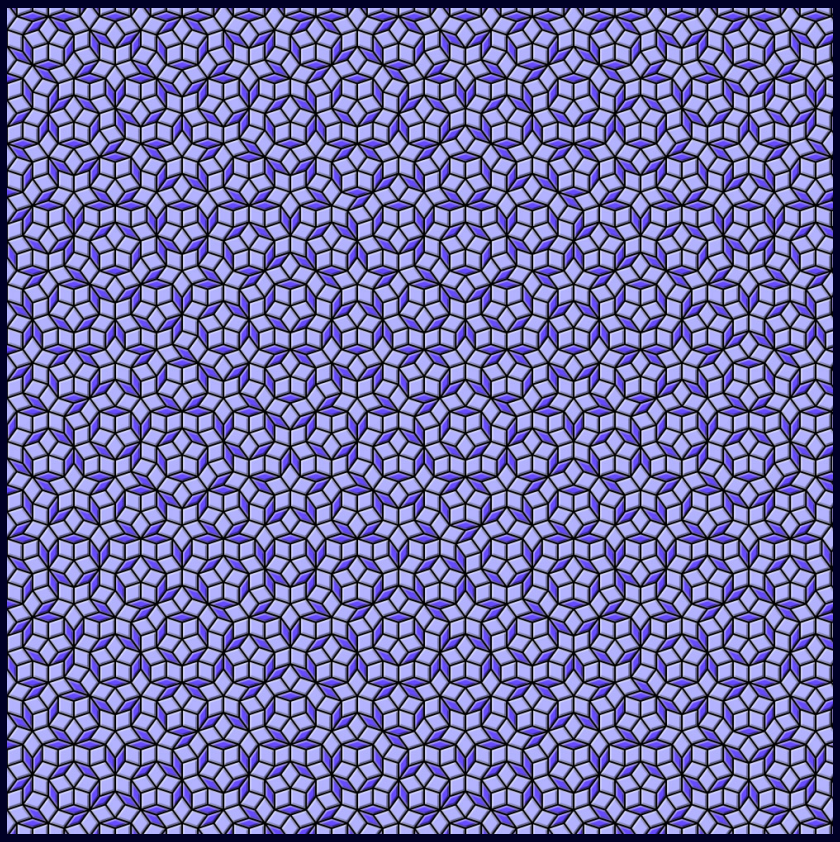
Math 2200 – Discrete Mathematics
Summer 2015



Instructor: Davar Khoshnevisan (davar@math.utah.edu)
Department of Mathematics, University of Utah
Text: *Discrete Mathematics* by K.H. Rosen,
McGraw Hill, NY, Seventh Edition, 2011

Contents

1 Introduction **2**
- 1.1 Some Questions . . . 2
- 1.2 Topics Covered . . . 3

2 Elementary Logic **3**
- 2.1 Propositional Logic . . . 3
- 2.2 Equivalences and Tautologies . . . 6
- 2.3 Predicates and Quantifiers . . . 8

3 Logic in Mathematics **10**
- 3.1 Some Terminology . . . 10
- 3.2 Proofs . . . 11
  - 3.2.1 Proof by Exhaustion . . . 11
  - 3.2.2 Proof by Contradiction . . . 12
  - 3.2.3 Proof by Induction . . . 13

4 Naive Set Theory **17**
- 4.1 Some Terminology . . . 17
- 4.2 The Calculus of Set Theory . . . 20
- 4.3 Set Identities . . . 24

5 Transformations **26**
- 5.1 Functions . . . 26
- 5.2 The Graph of a Function . . . 28
- 5.3 One-to-One Functions . . . 29
- 5.4 Onto Functions . . . 32
- 5.5 Inverse Functions . . . 32
- 5.6 Composition of Functions . . . 33
- 5.7 Back to Set Theory: Cardinality . . . 34

6 Patterns and Sequences **39**
- 6.1 Recurrence Relations . . . 40
- 6.2 Infinite Series . . . 42
- 6.3 Continued Fractions . . . 43

7 Number Theory **45**
- 7.1 Division . . . 46
- 7.2 Modular Arithmetic . . . 48

1 Introduction

> There is a story about two friends, who were classmates in high school, talking about their jobs. One of them became a statistician and was working on population trends. He showed a reprint to his former classmate. The reprint started, as usual, with the Gaussian distribution and the statistician explained to his former classmate the meaning of the symbols for the actual population, for the average population, and so on. His classmate was a bit incredulous and was not quite sure whether the statistician was pulling his leg. "*How can you know that?*" was his query. "*And what is this symbol here?*" "*Oh,*" said the statistician, "*this is π.*" "*What is that?*" "*The ratio of the circumference of the circle to its diameter.*" "*Well, now you are pushing your joke too far,*" said the classmate, "*surely the population has nothing to do with the circumference of the circle.*"
>
> ⋮ ⋮ ⋮ ⋮
>
> The preceding two stories illustrate the two main points which are the subjects of the present discourse. The first point is that mathematical concepts turn up in entirely unexpected connections. Moreover, they often permit an unexpectedly close and accurate description of the phenomena in these connections. Secondly, just because of this circumstance, and because we do not understand the reasons of their usefulness, we cannot know whether a theory formulated in terms of mathematical concepts in uniquely appropriate. We are in a position similar to that of a man who was provided with a bunch of keys and who, having to open several doors in succession, always hit on the right key on the first or second trial.
>
> –Eugene Paul Wagner[1]

1.1 Some Questions

- Is mathematics a natural science, or is it a human invention?
- Is mathematics the science of laboriously doing the same things over and over, albeit very carefully? If yes, then why is it that some people discover truly-novel mathematical ideas whereas many others do not? Or, for that matter, why can't we seem to write an algorithm that does new mathematics for us? If no, then is mathematics an art?
- Is mathematics a toolset for doing science? If so, then why is it that the same set of mathematical ideas arise in so many truly-different scientific disciplines? Is mathematics a consequence of the human condition, or is it intrinsic in the physical universe?

[1] "The unreasonable effectiveness of mathematics in the natural sciences," *Communications in Pure and Applied Mathematics (1960) vol. 13, no. 1.*

- Why is it that many people are perfectly comfortable saying something like, "I can't do mathematics," or "I can't draw," but very few are comfortable saying, "I can't read," or "I can't put on my socks in the morning"?

- Our goal, in this course, is to set forth elementary aspects of the language of mathematics. The language can be learned by most people, though perhaps with effort. Just as most people can learn to read or put on their socks in the morning. [What one does with this elaborate language then has to do with one's creativity, intellectual curiosity, and other less tangible things.]

1.2 Topics Covered

- Propositional Logic, Modus Ponens, and Set Theory [Chapters 1-2]

- Algorithms [Chapter 3]

- Number Theory and Cryptography [Chapter 4]

- Induction and Recursion [Chapter 5]

- Enumerative Combinatorics and Probability [Chapters 6–8]

- Topics from logic, graph theory, and computability.

2 Elementary Logic

2.1 Propositional Logic

According to the Merriam-Webster online dictionary, "Logic" could mean any one of the following:

- A proper or reasonable way of thinking about or understanding something;

- A particular way of thinking about something; and/or

- The science that studies the formal processes used in thinking and reasoning.

"Propositional logic" and its natural offspring, predicate logic, are early attempts to make explicit this process. Propositional logic was developed in the mid-19th century by Augustus DeMorgan, George Boole, and others, and is sometimes also referred to as "naive logic," or "informal logic." The first part of this course is concerned with the development of propositional logic.

The building blocks of propositional logic are "propositions," and "rules of logic." A *proposition* is a statement/declaration which is, by definition,

either true or false, but not both. If a proposition p is true, then its *truth value* is "true" or "T." If p is false, then its *truth value* is "false" or "F."

Example 2.1. Here are some simple examples of logical propositions:

1. "It is now 8:00 p.m." is a proposition.
2. "You are a woman," "He is a cat," and "She is a man" are all propositions.
3. "$x^2 + y^2 = z^2$" is not a proposition, but "the sum of the squares of the sides of a triangle is equal to the square of its hypotenuse" is a proposition. Notice that, in propositional logic, you do not have to represent a proposition in symbols.

The rules of logic—essentially also known as *Modus Ponens*—are an agreed-upon set of rules that we allow ourselves to use in order to build new propositions from the old. Here are some basic rules of propositional logic.

NOT. If p is a proposition, then so is the *negation* of p, denoted by $\neg p$ [in some places, not here, also $\sim p$]. The proposition $\neg p$ declares that "proposition p is not valid." By default, the truth value of $\neg p$ is the opposite of the truth value of p.

Example 2.2. If p is the proposition, "I am taking at least 3 courses this summer," then $\neg p$ is the proposition, "I am taking at most 2 courses this summer."

Here is the "truth table" for negation.

p	$\neg p$
T	F
F	T

AND. If p and q are propositions, then their *conjunction* is the proposition "p and q are both valid." The conjunction of p and q is denoted by $p \wedge q$. The truth value of $p \wedge q$ is true if p and q are both true; else, the truth value of $p \wedge q$ is false. Here is the "truth table" for conjunctive propositions.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

OR. Similarly, the *disjunction* of two propositions p and q is the proposition, "at least one of p and q is valid." The disjunction of p and q is denoted by $p \vee q$.

Example 2.3. Suppose p denotes the proposition, "I am cold," and q the proposition, "I am old." Then $p \wedge q$ denotes the proposition, "I am cold and old," and $p \vee q$ is the proposition, "I am either cold or old or both." Equivalently, $p \vee q$ denotes "p [inclusive-] or q."

Here is the "truth table" for disjunctive propositions.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

XOR. The *exclusive or* of propositions p and q is the proposition, "either p is valid, or q, but not both." The exclusive or of p and q is denoted by $p \oplus q$. Here is the "truth table" for the logical operation exclusive or.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

IF THEN. The proposition "p implies q" [also "if p then q"]—denoted by $p \to q$—is a *conditional statement*. It denotes the proposition, "if p were true, then so would be q."

Example 2.4. The following are 2 examples of conditional propositions:

1. If I were elected, then I would lower taxes;
2. If I were a dog, then I would eat dog food;
3. If you eat your meat, then you can have your pudding.

Here is the "truth table" for conditional propositions.

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

IFF. The proposition "p if and only if q"—denoted by $p \leftrightarrow q$—is a *biconditional proposition*; it is true if and only if both conditional statements $p \to q$ and $q \to p$ are valid.

Example 2.5. Let p denote the proposition, "you can have your pudding," and q the proposition, "you can eat your meat." Then, $p \leftrightarrow q$ is the assertion that "you can have your pudding if *and only if* you have your meat."

Here is the "truth table" for biconditional propositions.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

2.2 Equivalences and Tautologies

One can sometimes use known/available propositions, and combine them in order to form new, *compound*, propositions.

Example 2.6. As a simple example, consider the proposition $\neg p \vee q$, build from two propositions p and q, using both negation and conjunction. Here is the truth table for this particular compound proposition.

p	q	$\neg p \vee q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 2.7. For a second [perhaps more interesting] example, consider the truth table for the compound propositions $p \to q$ and $\neg q \to \neg p$.

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

Example 2.8. Here is the truth table for the proposition, "$p \wedge (\neg q) \to p \wedge q$."

p	q	$p \wedge (\neg q)$	$p \wedge q$	$p \wedge (\neg q) \to p \wedge q$
T	T	F	T	T
T	F	T	F	F
F	T	F	F	T
F	F	F	F	T

- We say that propositions p and q are *equivalent* if they have the same truth table. We write $p \equiv q$ when p and q are equivalent.

Example 2.9. Check the following from first principles:

- $\neg(\neg p) \equiv p$. Another way to say this is that the compound proposition "$-(\neg p) \leftrightarrow p$" is always true;
- $(p \wedge q) \equiv (q \wedge p)$. Another way to say this is that the compound proposition "$(p \wedge q) \leftrightarrow (q \wedge p)$" is always true;
- $(p \vee q) \equiv (q \vee p)$. Another way to say this is that the compound proposition "$(p \vee q) \leftrightarrow (q \vee p)$" is always true.

- A proposition is a *tautology* if it is always true, and a *fallacy* if it is always false. Thus, $p \equiv q$ is the same proposition as "$p \leftrightarrow q$ is a tautology."

  Example 2.10. If p is a proposition, then $\neg p \vee p$ is a tautology and $\neg p \wedge p$ is a fallacy. One checks these by computing truth tables:

p	$\neg p$	$\neg p \vee p$	$\neg p \wedge p$
T	F	T	F
T	F	T	F
F	T	T	F
F	T	T	F

  In casual conversation, the word "tautology" is sometimes equated with other words such as "self-evident," "obvious," or even sometimes "trivial." In propositional logic, tautologies are not always obvious. All theorems of mathematics and computer science qualify as logical tautologies, but many are far from obvious and the like. If "$p \equiv q$," then we may think of p and q as the same proposition.

- There are infinitely-many tautologies in logic; one cannot memorize them. Rather, one learns the subject. Still, some tautologies arise more often than others, and some have historical importance and have names. So, educated folk will want to know and/or learn them. Here are two examples of the latter type.

  Example 2.11 (De Morgan's Laws)**.** The following two tautologies are known as *De Morgan's Laws*: If p and q are propositions, then:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q;$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q.$$

  You can prove them by doing the only possible thing: You write down and compare the truth tables. [Check!]

2.3 Predicates and Quantifiers

It was recognized very early, in the 19th century, that one needs a more flexible, more complex, set of logical rules in order to proceed with more involved logical tasks. For instance, we cannot use propositional logic to ascertain whether or not "$y = 2x + 1$." In order to do that, we also need to know the numerical values of the "variables" x and y, not to mention some of the basic rules of addition and multiplication [i.e., tables]. "Predicate logic" partly overcomes this definiciency by: (i) including the rules of propositional logic; and (ii) including "variables" and "[propositional] functions."

- A *propositional function* $P(x)$ is a proposition for every possible choice of the *variable* x; P is referred to as a *predicate*.

  Example 2.12. Let $P(x)$ denote "$x \geq -1/8$ for every real number x. Then, $P(1)$ is a true proposition, whereas $P(-1)$ is a false one.

  Example 2.13. The variable of a proposition need not be a real number. For instance, $P(x\,,y)$ could denote the proposition, "$x + y = 1$." In this case, the variable of P is a 2-vector $(x\,,y)$ for every possible real number x and y. Here, for instance, $P(1\,,1)$ is false, whereas $P(5.1\,,-4.1)$ is true. You can think of the predicate P, in English terms and informally, as the statement that the point $(x\,,y)$ falls on a certain straight line in the plane.

Predicate logic has a number of rules and operations that allow us to create propositions from predicates. Here are two notable operations:

FOR ALL. If P is a predicate, then $\forall x P(x)$ designates the proposition, "$P(x)$ for all x" within a set of possible choices for x. The "for all" operation $\forall$ is a *quantifier* for $P(x)$, and that set of possible choices of x is the *domain* of the quantifier $\forall$ here. If the domain D is not universal ["for all real numbers x" and the like], then one includes the domain by saying, more carefully, something like $\forall x P(x)[x \geq 0]$, or $\forall x P(x)[(x \geq -2) \vee (x \leq 5)]$, etc.

Example 2.14. Suppose $P(x)$ if the proposition that "$x > 2$," for every real number x. Then $\forall x P(x)$ is false; for example, that is because $P(0)$ is false. But $\forall x P(x)[x \geq 8]$ is true.

FOR SOME. If P is a predicate, then $\exists x P(x)$ designates the proposition, "$P(x)$ for some x" within a set of possible choices for x. The "there exits" operation $\exists$ is a *quantifier* for $P(x)$, and that set of possible choices of x is the *domain* of the quantifier $\exists$ here.

Example 2.15. Suppose $P(x)$ if the same proposition as before for every real number x: That "$x > 2$." Then $\exists x P(x)$ is true; for example, that is because $P(3)$ is true. But $\exists x P(x)[x \leq 0]$ is false.

- (De Morgan's Laws for Quantifiers) We have the following tautologies:

$$\neg\exists x P(x) \equiv \forall x \neg P(x);$$
$$\neg\forall x P(x) \equiv \exists x \neg P(x).$$

One proves these De Morgan laws by simply being careful. For instance, let us verify the first one. Our ask is two fold:

1. We need to show that if $\neg\exists x P(x)$ is true then so is $\forall x \neg P(x)$; and
2. We need to show that if $\forall x \neg P(x)$ is true then so is $\neg\exists x P(x)$.

We verify (1) as follows: If $\neg\exists x P(x)$ were true, then $\exists x P(x)$ is false. Equivalently, $P(x)$ is false for all x [in the domain of the quantifier] and hence $\neg P(x)$ is true for all x [also in the domain of the quantifier]. This yields $\forall x \neg P(x)$ as true and completes the proof of (1). I will leave the proof of (2) up to you.

Example 2.16. The negation of "Everyone is smelly" is "someone is not smelly." In order to demonstrate this using predicate logic, let $P(x)$ denote "x is smelly." Then, "everyone is smelly" is codified as $\forall x P(x)$; its negation is $\exists x \neg P(x)$, thanks to the De Morgan laws. I will leave it up to you to do the rest.

ex:smelly

Example 2.17. The negation of "Someone will one day win the jackpot" is "no one will ever win the jackpot." In order to demonstrate this using predicate logic, let $P(x\,, y)$ denote "x will win the jackpot on day y." Then, "someone will win the jackpot one day" is codified as $\exists(x\,, y)P(x\,, y)$, whose negation is—thanks to De Morgan's laws—the proposition $\forall(x\,, y)\neg P(x\,, y)$. As an important afterthought, I ask, "What are the respective domains of these quantifiers?"

- Predicate logic allows us to define new predicates from old. For instance, suppose $P(x\,, y)$ is a predicate with two variables x and y. Then, $\forall x P(x\,, y)$, $\exists y P(x\,, y)$, ... are themselves propositional functions [the first is a function of y and the second of x].

- Some times, if the expressions become too complicated, one separates the quantifiers from the predicates by a colon. For instance,

$$\forall x \forall y \forall z \forall \alpha \exists \beta P(x\,, y\,, z\,, \alpha\,, \beta)$$

can also be written as

$$\forall x \forall y \forall z \forall \alpha \exists \beta : \; P(x\,, y\,, z\,, \alpha\,, \beta),$$

in order to ease our reading of the logical "formula."

Example 2.18. See if you can prove [and understand the meaning of] the tautologies:

$$\forall(x\,,y)P(x\,,y) \equiv \forall x\forall y P(x\,,y) \equiv \forall y\forall x P(x\,,y);$$
$$\exists(x\,,y)P(x\,,y) \equiv \exists x\exists y P(x\,,y) \equiv \exists y\exists x P(x\,,y);$$
$$\neg\Big(\forall x\exists y P(x\,,y) \equiv \exists y\forall x P(x\,,y)\Big).$$

ex:sqrt:2

Example 2.19. A real number x is said to be *rational* if we can write $x = a/b$ where a and b are integers. An important discovery of the mathematics of antiquity—generally ascribed to a Pythagorean named Hippasus of Metapontum (5th Century B.C.)—is that $\sqrt{2}$ is *irrational*; that is, it is not rational. We can write this statement, using predicate logic, as the following tautology:

$$\neg\exists a, b:\ \sqrt{2} = \frac{a}{b}\ [a, b \in \mathbb{Z}],$$

where $\mathbb{Z} := \{0\,, \pm 1\,, \pm 2\,, \cdots\}$ denotes the collection of all integers, ":=" is shorthand for "is defined as," and "$\in$" is shorthand for "is an element of."

ex:fermat:last:thm

Example 2.20. *Fermat's last theorem*, as conjectured by Pierre de Fermat (1637) and later proved by Andrew Wiles (1994/1995), is the tautology,

$$\neg\Big(\exists a\exists b\exists c\exists n\, P(a\,, b\,, c\,, n)\Big)\ [(a, b, c \in \mathbb{N}) \wedge (n \in \{3\,, 4\,, \ldots\})]\,,$$

where every $P(a\,, b\,, c\,, n)$ denotes the proposition, "$a^n + b^n = c^n$."

ex:continuity

Example 2.21. In calculus, one learns that a function f of a real variable x is *continuous* if, and only if, for every $\varepsilon > 0$ there exists $\delta > 0$ such that $|f(x) - f(y)| \leq \varepsilon$ whenever $|x - y| \leq \delta$. We can state this definition, as a proposition in predicate logic as

$$\forall\varepsilon\exists\delta P(\varepsilon\,, \delta)\ [\varepsilon > 0 \wedge \delta > 0],$$

where each $P(\varepsilon\,, \delta)$ denotes the following proposition:

$$\forall x, y Q(x\,, y\,, \varepsilon)\ [-\infty < x < \infty \wedge x - \delta < y < x + \delta],$$

and every $Q(x\,, y\,, \varepsilon)$ denotes the event that $|f(x) - f(y)| \leq \varepsilon$.

3 Logic in Mathematics

3.1 Some Terminology

- In mathematics [and related fields such as theoretical computer science and theoretical economics], a *theorem* is an assertion that:

1. Can be stated carefully in the language of logic [for instance, the logical systems of this course, or more involved ones]; and
2. Is always <u>true</u> [i.e., a tautology, in the language of predicate logic].

- Note that, in the preceding, "true" is underlined to emphasize that it is meant in the sense of the logical system being used [explicitly], and therefore can be demonstrated [in that same logical system] explicitly.
- Officially speaking, *Propositions*, *lemmas*, *fact*, etc. are also theorems. However, in the culture of mathematical writing, theorems are deemed as the "important" assertions, propositions as less "important," and lemmas as "technical" results en route establishing theorems. I have put quotations around "important" and "technical" because these are subjective annotations [usually decided upon by whoever is writing the mathematics].
- Officially speaking, a *Corollary* is also a theorem. But we call a proposition a "corollary" when it is a "simple" or "direct" consequence of another fact.
- A *conjecture* is an assertion that is believed to be true, but does not yet have a logical proof.
- Frequently, one writes the domain of the variables of a mathematical proposition together with the quantifiers, rather than at the end of the proposition. For instance, consider the tautology,

$$\forall x, y : \frac{x}{y} > 0 \ [x > 0 \wedge y > 0].$$

Stated in English, the preceding merely says that if you divide two [strictly] positive numbers then you obtain a positive number. In mathematics, we prefer to write instead of the preceding symbolism the following:

$$\forall x, y > 0 : \frac{x}{y} > 0; \quad \text{or sometimes} \quad \forall x > 0, \forall y > 0 : \frac{x}{y} > 0.$$

3.2 Proofs

There is no known algorithm for proving things just as there is no known algorithm for living one's life and/or for having favorite foods. Still, one can identify some recurring themes in various proofs of well-understood mathematical theorems.

3.2.1 Proof by Exhaustion

Perhaps the simplest technique of proof is *proof by exhaustion*. Instead of writing a silly general definition, I invite you to consider the following example.

Proposition 3.1. *There are 2 even integers between 3 and 7.*

Proof. Proof by exhaustion does what it sounds like it should: In this case, you list, exhaustively, all even integers between 3 and 7. They are 4 and 6. □

Or you can try to prove the following on your own, using the method of exhaustion.

Proposition 3.2. $2n < 2^n$ *for every integer* n *between 3 and 1000.*

Enough said.

3.2.2 Proof by Contradiction

Recall that $p \to q$ is equivalent to $\neg q \to \neg p$. The idea of *proof by contradiction*—also known as *proof by contraposition*—is that, sometimes, it is easier to prove $\neg q \to \neg p$ rather than $p \to q$. I will cite a number of examples. The first is a variation of the socalled *pigeonhole principle* to which we might return later on.

Proposition 3.3. *If* x_1 *and* x_2 *are two real numbers and* $x_1 + x_2 \geq 10$*, then at least one of* x_1 *and* x_2 *is* ≥ 5*. More generally, if* $x_1 + \cdots + x_k \geq y$*, all real numbers, then* $x_j \geq y/k$ *for some* $1 \leq j \leq k$*.*

Proof. The second statement reduces to the first when you specialize to $k = 2$. Therefore, it suffices to prove the second statement. We will prove its contrapositive statement. That is, we will prove that $x_1 + \cdots + x_k < y$ whenever $x_j < y/k$ for all $1 \leq j \leq k$. Indeed, suppose $x_j < y/k$ for all $1 \leq j \leq k$. Then,

$$x_1 + \cdots + x_k < \frac{y}{k} + \cdots + \frac{y}{k} = y.$$

This proves the contrapositive of the second assertion of the proposition. □

Our next two examples are from elementary number theory.

Proposition 3.4. *Suppose* $x^2 - x + 1$ *is an even integer for some* $x \in \mathbb{N}$*. Then,* x *is odd.*

Proof. If x were even, then we would be able to write $x = 2w$ for some positive integer w. In particular,

$$x^2 - x + 1 = 4w^2 - 2w + 1 = \underbrace{2w(2w-1)}_{\text{an even integer}} + 1$$

would have to be an odd integer. □

pr:xy:even

Proposition 3.5. *Suppose* x, y *are positive integers and* xy *is even. Then, at least one of* x *and* y *must be even.*

Proof. If x and y were both odd, then we would be able to write $x = 2a + 1$ and $y = 2b + 1$ for two non-negative integers a and b. In that case, we would also have to have

$$xy = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = \underbrace{2(2ab + a + b)}_{\text{even integer}} + 1$$

be an odd number. Therefore, we have proved by contraposition that if xy is even then at least one of x or y must be even. □

The preceding also has a converse. Namely,

pr:xy:odd

Proposition 3.6. *Suppose x, y are positive integers and xy is odd. Then, x and y must both be odd.*

Proof. If x were even, then we would be able to write $x = 2a$ for some integer $a \geq 1$, whence $xy = 2ay$ is necessarily an even number. Similarly, if y were even, then we would be able to write $y = 2b$ for some integer $b \geq 1$, and hence $xy = 2xb$ is even. This proves the result in its contrapositive form. □

We can combine Propositions 3.5 and 3.6 in order to deduce the following.

cor:xy:parity

Corollary 3.7. *Let x and y be two positive integers. Then, xy is odd if and only if x and y are both odd.*

3.2.3 Proof by Induction

Consider a propositional function P, whose variable $n \geq 1$ is an integer, and suppose that we wanted to prove that $P(n)$ is valid for all $n \geq 1$. "Mathematical induction" is one method of proof that we could try. The method can be explained quite quickly as follows: First prove, however you can, that $P(1)$ is true. Then prove the following assertion:

$$\forall n \geq 1 : \ P(1) \wedge \cdots \wedge P(n) \to P(n + 1). \tag{1}$$

eq:induction

It is easy to see why the method works when it does: $P(1)$ is true by our *ad hoc* reasoning. Since $P(1)$ and (1) are true, we may appeal to (1) [specialized to $n = 1$] in order to see that $P(2)$ is true. Now that we know that $P(1)$ and $P(2)$ are true, we apply (1) to deduce the truth of $P(3)$, then $P(4)$, etc. We see, in n steps, that $P(n)$ is true for every $n \geq 1$. This does the job.

The term "mathematical induction" is sometimes used in order to not mix things up with "induction," which is a rather different idea from logic [and, to a lesser extent, philosophy]. We will used both terms interchangeably since we will not discuss the second notion of induction in this course.

The idea of using induction in mathematical proofs is quite old, dating back at least as far back as some of the writings of Plato ($\approx$ 370 B.C.) do, and most likely much farther back still.

Here are some examples of induction in proofs. These are all examples from antiquity.

pr:1+...+n

Proposition 3.8. *For every positive integer n,*

$$1 + \cdots + n = \frac{n(n+1)}{2}. \tag{2}$$

eq:1+...+n

Definition 3.9 (Summation Notation)**.** If $x_1, x_2, \ldots, x_n$ are n real numbers, then we define,

$$\sum_{i=1}^{n} x_i := x_1 + \cdots + x_n.$$

Note that "there is no i" anywhere on the right-hand side of the preceding display. Therefore, the same is true of the quantity on the left. In other words, $\sum_{z=1}^{n} x_z$, $\sum_{\theta=1}^{n} x_\theta$, $\sum_{v=1}^{n} x_v$, $\sum_{p=1}^{n} x_p$, etc. all designate the same quantity, "$x_1 + \cdots + x_n$." However, "$\sum_{n=1}^{n} x_n$" is simply nonesense [why?].

With these remarks in mind, we can rewrite Proposition 3.8 in the following equivalent form: For every positive integer n,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. The assertion is clearly true when $n = 1$. Suppose (2) holds. We will prove that it holds also when n is replaced by $n + 1$. Since

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1),$$

our *induction hypothesis*, if (2) were valid for n, then

$$\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + n + 1 = (n+1)\left[\frac{n}{2} + 1\right] = \frac{(n+1)(n+2)}{2}.$$

This proves that (2) holds with n replaced by $n + 1$, and completes our induction proof. □

pr:1+...+n:odd

Proposition 3.10. *For every positive integer n,*

$$\sum_{i=1}^{n} (2i-1) = \underbrace{1 + 3 + \cdots (2n-1)}_{\text{the sum of all odd integers} < 2n} = n^2.$$

Proof. The assertion holds true for $n = 1$. To proceed with induction, we suppose that $\sum_{i=1}^{n} (2i-1) = n^2$, and use that induction hypothesis in order

to conclude that $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$ [sort this out!]. This will do the job. But the induction hypothesis shows that

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + (2n+1) = n^2 + (2n+1),$$

which is equal to $(n+1)^2$. Therefore, the preceding concludes the proof. □

We should pause to appreciate one of the many added benefits of having introduced good notation: Proposition 3.10 is a direct corollary of Proposition 3.8 and elementary properties of addition, without need for an elaborate induction proof. Simply note that

$$\sum_{i=1}^{n}(2i-1) = \sum_{i=1}^{n}(2i) - \sum_{i=1}^{n}1 = 2\sum_{i=1}^{n} i - n = n(n+1) - n,$$

where the last equality is deduced from Proposition 3.8. This does the job because $n(n+1) - n = n^2$.

Exercise. Find the numerical value of $1 + 2 + 4 + \cdots + 2n$ [the sum of all even integers between 1 and $2n$, inclusive] for every positive integer n.

The following result is perhaps a little more interesting.

Proposition 3.11. *For every positive integer n,*

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3}$$ eq:1^2+...+n^2

Proof. Let $P(n)$ designate the proposition implied by (3). Since $1 = 1$, $P(1)$ is valid. Suppose $P(n)$ is valid for some integer $n \geq 1$; we aim to prove [conditionally] that $P(n+1)$ is valid. By the induction hypothesis,

$$\begin{aligned}\sum_{i=1}^{n+1} i^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = (n+1)\left[\frac{n(2n+1)}{6} + n + 1\right] \\ &= (n+1)\left[\frac{2n^2+7n+6}{6}\right] = (n+1)\left[\frac{(n+2)(2n+3)}{6}\right].\end{aligned}$$

Since $(n+2)(2n+3) = ([n+1]+1)(2[n+1]+1)$, the preceding completes the *induction step* [that is, the process of proving $P(n) \to P(n+1)$], and hence the proof. □

Let us use this opportunity to introduce one more piece of good notation.

Definition 3.12 (Multiplication Notation)**.** If $x_1, \ldots, x_n$ are real numbers, then we sometimes denote their product as

$$\prod_{i=1}^{n} x_i := x_1 x_2 \cdots x_n.$$

Proposition 3.13. *For every integer $n \geq 2$,*

$$\prod_{i=2}^{n} \left(1 - \frac{1}{i}\right) = \frac{1}{n}.$$

Proof. The statement is clear for $n = 2$. Suppose the displayed formula of the proposition is valid for some integer n; we will use it conditionally to prove it is valid with n replaced by $n + 1$. Indeed, the induction hypothesis implies that

$$\prod_{i=1}^{n+1} \left(1 - \frac{1}{i}\right) = \prod_{i=1}^{n} \left(1 - \frac{1}{i}\right) \times \left(1 - \frac{1}{n+1}\right) = \frac{1}{n} \times \frac{n}{n+1},$$

which is manifestly equal to $(n + 1)^{-1}$. This completes the induction step of the proof. □

Interestingly enough, the preceding proposition shows that too much reliance on notation [without relying on one's own thought processes] can obfusciate the truth as well. Indeed, note that

$$\prod_{i=2}^{n} \left(1 - \frac{1}{i}\right) = \frac{1}{2} \times \frac{2}{3} \times \cdots \times \frac{n-2}{n-1} \times \frac{n-1}{n}.$$

Therefore, we obtain the result by cancelling terms [in the only way that is meaningful and possible here]. Still, a completely logical proof requires induction because n is arbitrary. [Sort this out!]

With the preceding remarks in mind, the following can be seen to be a more interesting example.

Proposition 3.14. *For every integer $n \geq 2$,*

$$\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}.$$

Proof. The statement is clear for $n = 2$. Suppose the displayed formula of the proposition is valid for some integer n; we will use it conditionally to prove it is valid with n replaced by $n+1$. Indeed, by the induction hypothesis,

$$\prod_{i=1}^{n+1} \left(1 - \frac{1}{i^2}\right) = \prod_{i=1}^{n} \left(1 - \frac{1}{i^2}\right) \times \left(1 - \frac{1}{(n+1)^2}\right) = \frac{n+1}{2n} \times \frac{n^2+2n}{(n+1)^2} = \frac{n+2}{2(n+1)}.$$

This completes the induction step of the proof. □

Let us finish this section with perhaps our most historically-interesting example thus far. The proof is a blend of induction and proof by contradiction.

pr:Hippasus **Proposition 3.15** (Ascribed to Hippasus, 5th Century B.C.). *$\sqrt{2}$ is irrational.*

Proof. Suppose not. Then we would be able to find positive integers a_0 and b_0 such that $\sqrt{2} = a_0/b_0$. Since $a_0^2 = 2b_0^2$, it follows that a_0^2 is even, whence also a_0 is even by Proposition 3.5. Therefore we can find a positive integer a_1 such that $a_0 = 2a_1$. Because $4a_1^2 = (2a_1)^2 = a_0^2 = 2b_0^2$, it follows that $b_0^2 = 2a_1^2$, whence b_0^2 is even, whence also b_0 is even. Therefore, we can write $b_0 := 2b_1$ for some positive integer b_1. Now we can observe that $\sqrt{2} = a_0/b_0 = a_1/b_1$. By induction [work out the details!], we can in fact deduce the existence of a sequence of positive integers $a_0 = 2a_1 = 4a_2 = \cdots$ and $b_0 = 2b_1 = 4b_2 = \cdots$ such that $\sqrt{2} = a_n/b_n$ for all $n \geq 0$. Now a second round of induction [check!] shows that

$$b_n = \frac{b_{n-1}}{2} = \frac{b_{n-2}}{4} = \cdots = \frac{b_0}{2^n} \qquad \text{for all } n \geq 0.$$

In particular, $b_n < 1$ as soon as n is large enough to ensure that $b_0/2^n < 1$—that is, for all positive integers $n > \log_2(b_0)$. This shows that b_n cannot be a positive integer when $n > \log_2(b_0)$, in contrary to what we had deduced, and yields the desired contradiction. □

4 Naive Set Theory

4.1 Some Terminology

- A *set* is a collection of objects. Those objects are referred to as the *elements* of the set. If A is a set, then we often write "$a \in A$" when we mean to say that "a is an element of A." Sometimes we also say that "a is in A" when we mean "$a \in A$." If and when we can write all of the elements of A, then we denote A by $\{a_1, a_2, \ldots, a_n\}$, where $a_1, \ldots, a_n$ are the elements of A. Note the use of curly brackets! We write "$a \notin A$," when we mean to say that "a is not an element of A." More precisely,
$$a \notin A \leftrightarrow \neg(a \in A).$$

  Example 4.1. The collection of all vowels in English is a set. We can write that collection as $\{a, e, i, o, u\}$.

  Example 4.2. $\{1, 2\}$ and $\{2, 1\}$ are the same set.

  Example 4.3. $\{1, 1, 1\}$, $\{1, 1\}$, and $\{1\}$ are all the same set.

  Example 4.4. We have already seen the set $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$ of all integers, and the set $\mathbb{N} := \{1, 2, \ldots\}$ of all positive integers [also known as numerals, or natural numbers]. We will sometimes also refer to $\mathbb{Q}$ as the set of all rational numbers, and $\mathbb{R}$ as the set of all real numbers.

Example 4.5. 1 is not a set, it is a number. However, $\{1\}$ is a set, and has one element; namely, 1. You should make sure that you understand clearly that $\{1\}$ is not an element of $\{1\}$. This can be a subtle issue. Read on only after you have completely digested it.

Example 4.6. The ordered pair $(1,2)$ is not a set; it is, just like it says, an ordered pair [or a vector, or a point in the plane, ...]. However, $\{(1,2)\}$ is a set with one element. That element is the point $(1,2)$.

Example 4.7. The collection of all straight lines in the plane is a set [sometimes denoted by the impressive-looking symbol, $\mathrm{Gr}(1,\mathbb{R})$]. Every element of that set is a straight line in the plane, and every such straight line is an element of that set.

Example 4.8. Very often, mathematicians and computer scientists build sets with elements that are themselves sets. For instance, $\{\{1\}\}$ is a set with one element; namely, $\{1\}$. Of $\{\{1\},\{1,2\}\}$ is a set with two elements: $\{1\}$ and $\{1,2\}$.

- By the *empty set* we mean the [unique] set that has no elements. The empty set is often denoted by $\varnothing$, sometimes also $\{\}$.
- Our definition of a set is naive in part because "collection" and "object" are ill-defined terms. Our definition has some undesirable consequences as well, as it allows some very nasty objects to be sets. For example, we could define, using the preceding, A to be the collection of all sets. Since every set is an "object," whatever that means, A would itself have to be a set. In particular, A would have to have the extremely unpleasant property that A is an element of itself! Bertrand Russel (1902) tried to correct this deficiency, and discovered that all of naive set theory and naive logic is [somewhat] irrational; see Example 4.14.
- One can build a set by looking at all objects x that have a certain property Π. Such a set is written as $\{x : x \text{ has property } \Pi\}$, or sometimes [as is done in your textbook, for example], $\{x \mid x \text{ has property } \Pi\}$. And by $B := \{x \in A : x \text{ has property } \Pi\}$ we mean the obvious thing: "B is defined as the set of all elements of A that have property Π."

Example 4.9. $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 1\}$.

Example 4.10. $\mathbb{Q} = \{x \in \mathbb{R} : x = a/b \text{ for some } a, b \in \mathbb{Z}\}$.

Example 4.11. *Complex numbers* are, by definition, elements of the following set:

$$\mathbb{C} := \{x \mid x = a + ib \text{ for some } a, b \in \mathbb{R}\},$$

where $i := \sqrt{-1}$.

Example 4.12 (intervals)**.** Suppose a and b are real numbers. If $a \leq b$, then we may define

$$[a\,,b] := \{x \in \mathbb{R} :\ a \leq x \leq b\}\,.$$

This is called the *closed interval from a to b*. If, in addition, $a < b$, then we may define

$$\begin{aligned}(a\,,b) &:= \{x \in \mathbb{R} :\ a < x < b\}\,,\\ (a\,,b] &:= \{x \in \mathbb{R} :\ a < x \leq b\}\,,\\ [a\,,b) &:= \{a \in \mathbb{R} :\ a \leq x < b\}\,.\end{aligned}$$

The first of these three is called the *open interval from a to b*; the other two are *half-open, half-closed intervals*.

- Two sets A and B are said to be *equal* if they have exactly the same elements. In that case, we may write $A = B$. In other words,

$$(A = B) \leftrightarrow \forall x \Big[(x \in A) \leftrightarrow (x \in B)\Big].$$

The preceding is useful because frequently this is how one checks to see whether or not $A = B$.

Example 4.13. Suppose f is a strictly-increasing function of a real variable. Let f^{-1} denote the inverse function to f. Then

$$\{x : f(x) \leq 1\} = (-\infty\,, f^{-1}(1)].$$

Here is the proof: Let A denote the left-hand side and B the right-hand side. If $x \in A$ then $f(x) \leq 1$; because f^{-1} is increasing, $x = f^{-1}(f(x)) \leq f^{-1}(1)$ and hence $x \in B$. Conversely, if $x \in B$ then $x \leq f^{-1}(1)$. Since f is increasing, $f(x) \leq f(f^{-1}(1)) = 1$ and hence $x \in A$. We have shown that $x \in A$ if and only if $x \in B$; therefore, $A = B$.

ex:Russel

Example 4.14 (Russel's Paradox)**.** Here is an example that was concocted by Bertrand Russel (1902) in order to show that naive set theory—and propositional and/or predicate logic, for that matter—are flawed.[2] Let $\mathcal{B}$ denote the collection of all sets x that are not elements of themselves. That is,

$$\mathcal{B} := \{x :\ x \notin x\}.$$

[Note that we really want "$x \notin x$" and not "$x \notin \{x\}$," the latter being a tautology for any object x.] Russel's set $\mathcal{B}$ is nonempty; for example, $\{1\} \in \mathcal{B}$. At the same time, the definition of $\mathcal{B}$ immediately ensures the tautology,

$$(\mathcal{B} \in \mathcal{B}) \leftrightarrow (\mathcal{B} \notin \mathcal{B}),$$

Thus, we must conclude that our definition of a "set" is flawed.

[2]The remedy is twentieth-century *axiomatic set theory* and *axiomatic logic*. There is good news and bad news for us. The bad news is that both axiomatic theories lie well beyond the scope of this course. The good news is that the naive set theory and logic of this course are good enough for most elementary applications in other areas of mathematics.

4.2 The Calculus of Set Theory

- Let A and B be two sets. We say that B is a *subset* of A, and denote it by "$B \subseteq A$," if every element of B is an element of A. In other words,

$$B \subseteq A \leftrightarrow \forall x \Big[x \in B \to x \in A \Big].$$

- $\varnothing \subseteq A$ for every set A, since the following is a tautology:

$$x \in \varnothing \to x \in A.$$

- $A \subseteq A$ for every set A, by default $[x \in A \to x \in A]$.

- $A = B$ if and only if both of the following propositions are true: $A \subseteq B$; and $B \subseteq A$. In other words,

$$A = B \leftrightarrow [(A \subseteq B) \wedge (B \subseteq A)].$$

- If A and B are two sets, then their *intersection*—denoted by $A \cap B$—is the set whose elements are all common elements of A and B. More precisely,

$$A \cap B := \{x : (x \in A) \wedge (x \in B)\}.$$

  In other words, $x \in A \cap B$ if and only if $x \in A$ and $x \in B$. For this reason, some people refer to $A \cap B$ as A *and* B. The similarity between the symbols "$\cap$" and "$\wedge$" is by design and serves as a mnemonic.

- If A and B are two sets, then their *union*—denoted by $A \cup B$—is the set whose elements are all common elements of A and B. More precisely,

$$A \cup B := \{x : (x \in A) \vee (x \in B)\}.$$

  In other words, $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. For this reason, some people refer to $A \cup B$ as A *or* B. The similarity between the symbols "$\cup$" and "$\vee$" is by design and serves as a mnemonic.

- If A and B are sets, then $A \setminus B$ denotes the elements of A that are not elements of B; that is,

$$A \setminus B := \{x \in A : x \notin B\}.$$

  The set $A \setminus B$ is called A *set minus* B; it is also sometimes called the *complement of* B *in* A.[3]

[3] Your textbook writes this as $A - B$. We will not do that in this course, because in most of mathematics that notation is reserved for something else.

- In some contexts, we have a large ["universal"] set U and are interested in subsets of U only. In such a context, we write A^c—read as "A complement"—in place of $U \setminus A$. For instance, if we are studying the real numbers, then $U := \mathbb{R}$, and $[a\,,b]^c$ denotes $(-\infty\,,a) \cup (b\,,\infty)$ whenever $a \le b$ are two real numbers.[4]

- The collection of all subsets of a set A is a set; it is called the *power set* of A and denoted by $\mathcal{P}(A)$. That is,

$$\mathcal{P}(A) := \{B : B \subseteq A\}.$$

Example 4.15. The power set of $\{0\,,1\}$ is

$$\mathcal{P}(\{0\,,1\}) = \Big\{\varnothing\,,\{0\}\,,\{1\}\,,\{0\,,1\}\Big\}.$$

Example 4.16. The set $\{\varnothing\,,0\,,1\,,\{0\,,1\}\}$ is not the power set of any set.

Example 4.17. The power set of $\{0\,,1\,,2\}$ is

$$\mathcal{P}(\{0\,,1\,,2\}) = \Big\{\varnothing\,,\{0\}\,,\{1\}\,,\{2\}\,,\{0\,,1\}\,,\{0\,,2\}\,,\{1\,,2\}\,,\{0\,,1\,,2\}\Big\}.$$

- If A has many elements, then how can we be sure that we listed all of its subsets correctly? The following gives us a quick and easy test.

pr:count:card

Proposition 4.18. *Choose and fix an integer $n \ge 0$. If a set A has n distinct elements, then $\mathcal{P}(A)$ has 2^n distinct elements.*

I will prove this fact in due time.

- If A and B are two sets, then $A \times B$ is their *Cartesian product*, and is defined as the collection of all ordered pairs $(a\,,b)$ such that $a \in A$ and $b \in B$; that is,[5]

$$A \times B := \{(a\,,b) : a \in A,\, b \in B\}.$$

More generally, if $A_1, \ldots, A_n$ are n sets, then their *Cartesian product* is the collection of all ordered n-tuples $(a_1\,,\ldots,a_n)$ such that $a_i \in A_i$ for all $1 \le i \le n$. That is,

$$A_1 \times \cdots \times A_n := \{(a_1\,,\ldots,a_n) : a_i \in A_i \text{ for all } 1 \le i \le n\}.$$

Example 4.19. Since $[1\,,2] \times [0\,,1] = \{(x\,,y) : 1 \le x \le 2,\, 0 \le y \le 1\}$, we can think of this set geometrically as a planar square with vertices at the points $(1\,,0)$, $(1\,,1)$, $(2\,,0)$, and $(2\,,1)$.

[4] Your textbook writes $\bar{B}$ instead of B^c. We will not do that in this course because $\bar{B}$ means something else in most of mathematics.

[5] More precisely still, $A \times B = \{(a\,,b) : (a \in A) \wedge (b \in B)\}$.

- Let A be a set and n a positive integer. We frequently write A^n in place of the Cartesian-product set $A \times \cdots \times A$ [n times].

  Example 4.20. Choose and fix positive integers n and p. Then, $\mathbb{R}^n$ denotes the collection of all n-tuples of real numbers, and $\mathbb{N}^p$ denotes the collection of all p-tuples of positive integers. For another example consider the set,

  $$A := \{\text{⚽}, \text{👦}\}.$$

  Then,

  $$A^2 = \{(\text{⚽}, \text{⚽}),\ (\text{👦}, \text{👦}),\ (\text{⚽}, \text{👦}),\ (\text{👦}, \text{⚽})\}.$$

  The following is a sophisticated [and useful] way to restate "multiplication tables" that we learn in second grade.

pr:|A x B|

Proposition 4.21. *If A has n distinct elements and B has m distinct elements, then $A \times B$ has nm distinct elements.*

Remark 4.22. I am making some fuss about the word "distinct" because otherwise it is not clear what we mean when we say that "a set A has n elements." For example, the set $A := \{\text{🐦}, \text{🐦}\}$ should really only have one element because $\{\text{🐦}, \text{🐦}\}$ is the same set as $\{\text{🐦}\}$, even though visual inspection might suggest that $\{\text{🐦}, \text{🐦}\}$ ought to have 2 elements.

We can draw a multiplication table in order to convince oneself of the verasity of Proposition 4.21. But is it really true? The answer is, "yes."

Proof. We proceed by applying induction. First consider the case that $n = 1$, in which case we can write $A = \{a\}$ for some a. If B is a set with m elements, say $B = \{b_1, \ldots, b_m\}$, then $A \times B$ is the collection of all pairs (a, b_i) for $i = 1, \ldots, m$. There are m such points. Therefore, $A \times B$ has $nm = m$ elements in this case. In other words, the proposition is true when $n = 1$ [regardless of the numerical value of m].

Choose and fix a positive integer n, and let $P(n)$ denote the proposition that "$A \times B$ has nm elements for all integers $m \geq 1$ and all sets A and B with n and m elements respectively." We just verified that $P(1)$ is true. It suffice to suppose that $P(1), \ldots, P(n)$ are true [this is our induction hypothesis], and prove conditionally that $P(n+1)$ is true.

If A has $n+1$ elements, then we can write $A = \{a_1, \ldots, a_n, a_{n+1}\}$. If B is any set of m elements, for any integer $m \geq 1$, then we can also write $B := \{b_1, \ldots, b_m\}$, in which case, $A \times B$ is the collection of all pairs (a_i, b_j) for $1 \leq i \leq n+1$ and $1 \leq j \leq m$. We can divide this collection of pairs into two disjoint parts: Those with index $1 \leq i \leq n$ and those with index $i = n+1$. The induction hypothesis ensures that there are nm-many such pairs that are of the first type; and there are m such pairs of the second type. Therefore, altogether there are $nm + m = (n+1)m$-many such pairs. This completes the proof of the induction step, whence also that of the proposition. □

cor:multiply

Corollary 4.23. *Suppose $A_1, \dots, A_k$ respectively have $n_1, \dots, n_k$ distinct elements. Then, $A_1 \times \cdots \times A_k$ has $n_1 \times \cdots \times n_k$ distinct elements. In particular, if A has n distinct elements then A^k has n^k distinct elements for every positive integer k.*

Proof. We will prove the first assertion; the second follows from the first, after we specialize the latter to the case that $A_1 = \cdots = A_k = A$ and $n_1 = \cdots = n_k = n$.

Let $P(k)$ denote the assertion that "if $A_1, \dots, A_k$ are sets that respectively have $n_1, \dots, n_k$-many distinct elements, then $A_1 \times \cdots \times A_k$ has $n_1 \times \cdots n_k$-many distinct elements." Proposition 4.21 ensures that $P(2)$ is true. Now suppose, as our induction hypothesis, that $P(1), \dots, P(k)$ are true for some integer $k \geq 1$. We plan to prove that $P(k+1)$ is true; this and the method of mathematical induction together imply that $P(n)$ is true for all positive integers n. But

$$A_1 \times \cdots \times A_{k+1} = \underbrace{(A_1 \times \cdots \times A_k)}_{:=A} \times A_{k+1}.$$

By the induction hypothesis, A has $N := n_1 \times \cdots \times n_k$-many distinct elements. A second appeal to the induction hypothesis [using the validity of $P(2)$] shows us then that $A \times A_{k+1}$ has Nn_{k+1}-many distinct elements. This completes the proof that $P(k)$ is true for all $k \geq 1$. □

Let us close this section with the following.

Proof of Proposition 4.18. We first need to think of a good way to list all of the subsets of a finite set $A := \{1, \dots, n\}$ with n elements, say. List the elements of A, and then underneath your list assign a checkmark (✓) or an xmark (✗) to every element. Every time you see an ✗ the element is ignored; elements that correspond to ✓ are put into the subset. For example,

1	2	3	⋯	$n-1$	n
✗	✗	✓	⋯	✓	✗

is a way to code the subset $\{3, \dots, n-1\}$,

1	2	3	⋯	$n-1$	n
✓	✗	✓	⋯	✓	✓

is another way to write $\{1, 3, \dots, n-1, n\}$, and

1	2	3	⋯	$n-1$	n
✗	✗	✗	⋯	✗	✗

[all with xmarks] designates the empty subset $\varnothing$. Every distinct ✗/✓code creates a distinct subset of A. Conversely, every subset of A has an ✗/✓assignment.

In summary, the total number of subsets of A is equal to the total number of different ways we can create a list of n xmarks and checkmarks. The set of all lists of n xmarks and checkmarks is simply $\{✗, ✓\}^n$. Corollary 4.23 tells us that there are 2^n-many such lists. □

Example 4.24. This is a natural time to stop and re-examine the preceding proof by considering an example. Suppose $A = \{1, 2, 3\}$ is a set with 3 elements. There are $2^3 = 8$ subsets of A which we can write, together with their ✗/✓ code as follows:

Subset	Code
$\varnothing$	$\{✗, ✗, ✗\}$
$\{1\}$	$\{✓, ✗, ✗\}$
$\{2\}$	$\{✗, ✓, ✗\}$
$\{3\}$	$\{✗, ✗, ✓\}$
$\{1, 2\}$	$\{✓, ✓, ✗\}$
$\{1, 3\}$	$\{✓, ✗, ✓\}$
$\{2, 3\}$	$\{✗, ✓, ✓\}$
$\{1, 2, 3\}$	$\{✓, ✓, ✓\}$

4.3 Set Identities

The calculus of sets implies countless relations between sets, just as the calculus of functions does for functions. The latter topic fills a year of freshman "calculus." Here are some examples of the former. Throughout this discussion, A, B, C, ... denote a collection of sets. Whenever we write U, then we imply that U is a universal set.

1. $A \cap B = B \cap A$.

   Proof. The *only* way to prove this, and the following assertions, is to follow the definition of equality for sets carefully. For this reason, I will prove this first assertion only. You should check a few more in order to ensure that you understand this method.

   According to the definition of equality for sets, we need to prove two thing: (1) If $x \in A \cap B$ then $x \in B \cap A$; and (2) If $x \in B \cap A$ then $x \in A \cap B$.

   Now that we understand that we have to prove both (1) and (2), the rest is pedantic: If $x \in A \cap B$, then x is both in A and B. Equivalently, x is both in B and A. Hence, $x \in B \cap A$. Conversely, if $x \in B \cap A$, then x is both in A and B, whence $x \in A \cap B$. □

2. $A \cup \varnothing = A$.

3. $A \cap \varnothing = \varnothing$.

4. $A \cup (B \cup C) = (A \cup B) \cup C$. Therefore, we may—and often will—omit the parentheses.

5. $A \cap (B \cap C) = (A \cap B) \cap C$. Therefore, we may—and often will—omit the parentheses.
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Therefore, we may—and often will—omit the parentheses.
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Therefore, we may—and often will—omit the parentheses.
8. $A = (A^c)^c$ [when A is a subset of a universal set U].
9. $A \cup A^c = U$ [when A is a subset of a universal set U].
10. $A \cap A^c = \varnothing$ [when A is a subset of a universal set U].
11. $(A \cup B)^c = A^c \cap B^c$ [when A and B are subsets of a universal set U]. Therefore, we may not omit the parentheses.
12. $(A \cap B)^c = A^c \cup B^c$ [when A and B are subsets of a universal set U]. Therefore, we may not omit the parentheses.
13. $(A \cup B \cup C)^c = A^c \cap B^c \cap B^c$ [when A, B, C are subsets of a universal set U]. Therefore, we may not omit the parentheses.
14. $(A \cap B \cap C)^c = A^c \cup B^c \cup B^c$ [when A, B, C are subsets of a universal set U]. Therefore, we may not omit the parentheses.
15. Etc.

Definition 4.25. We often write $\cup_{i=1}^n A_i$ in place of $A_1 \cup \cdots \cup A_n$, and $\cap_{i=1}^n A_i$ in place of $A_1 \cap \cdots \cap A_n$, whenever $A_1, \ldots, A_n$ are sets. More generally, if $A_1, A_2, \ldots$ are sets, then $\cup_{i=1}^\infty A_i := A_1 \cup A_2 \cup \cdots$ denotes the set of all points that are in at least one of the A_i's, and $\cap_{i=1}^n A_i := A_1 \cap A_2 \cap \cdots$ denotes the set of all points that are in every A_i. More generally still, if A_i is a set for all i in some index set I, then $\cup_{i \in I} A_i$ denotes the set of all points that are in at least one A_i and $\cap_{i \in I} A_i$ denotes the set of all points that are in every A_i.

Example 4.26. If n is a positive integer, then

$$\bigcup_{i=1}^{n-1} [i\,,i+1] = [1\,,n], \quad \bigcap_{i=1}^{n} [i\,,n] = \{n\}, \quad \text{and} \quad \bigcap_{i=1}^{n} [i\,,i+1] = \varnothing.$$

Example 4.27. $\mathbb{R} = \cup_{i=-\infty}^{\infty} [-i\,,-i+1]$. Moreover,

$$\{1\} = \bigcap_{i=1}^{\infty} \left[1\,,1+i^{-1}\right) \quad \text{and} \quad \varnothing = \bigcap_{i=1}^{\infty} \left(1\,,1+i^{-1}\right),$$

whereas

$$[1\,,2) = \bigcup_{i=1}^{\infty} \left[1\,,1+i^{-1}\right) \quad \text{and} \quad (1\,,2) = \bigcup_{i=1}^{\infty} \left(1\,,1+i^{-1}\right).$$

Example 4.28. Here is a final example to work on:

$$\bigcap_{i=1}^{\infty} \left[1\,,1+i^{-1}\right)^{c} = (-\infty\,,1) \cup [2\,,\infty).$$

5 Transformations

5.1 Functions

- Let A and B denote two sets. A *function f from A to B* assigns to every element $a \in A$ one element $f(a) \in B$. In this case, we sometimes say that *f maps A into B*, or sometimes even *f maps A to B*.

- Functions are also known as *mappings* or *transformations*.

ex:cowdog

Example 5.1. Sometimes it is more convenient to write "formulas," as one does in school Calculus. For instance, $f(x) := x^2$ for $x \in \mathbb{R}$ describes a mapping that yields the value x^2 upon input $x \in \mathbb{R}$. Note that "there is no x" in this formula; just the mapping $x \to x^2$. But you should not identify functions with such formulas because that can lead to non sense. Rather, you should think of a function f as an algorithm: "f accepts as input a point $a \in A$, and returns a point $f(a) \in B$." For example, the following describes a function f from the set $A := \{\text{cow}\,,\text{dog}\}$ to the set $B := \{$ $\}$:

$$f(\text{cow}) := \text{  }, \qquad f(\text{dog}) := \text{  }.$$

Question. Does it matter that the displayed description of f does not make a reference to the computer-mouse symbol  which is one of the elements of the set B?

Example 5.2. All assignments tables are in fact functions. And we do not always label functions as f, g, etc. For instance, consider the first truth table that we saw in this course:

p	$\neg p$
T	F
F	T

This table in fact describes a function—which we denoted by "$\neg$"—from the set of all possible truth assignments for p to the corresponding truth assignments for $\neg p$. Namely, $\neg(\text{T}) := \text{F}$; and $\neg(\text{F}) := \text{T}$.

- The preceding remark motivates the notation "$f : A \to B$" which is short hand for "let f be a function from A to B." We use this notation from now on.

- In discrete mathematics, one often considers functions $f : A \to B$ where A and B are a finite collection of objects. The preceding 2 examples are of course of this type. One can think about such functions not so much via formulas such as "$f(x) = x^2$," rather as mappings from A to B and draw a representing picture such as the one in Figure 1.

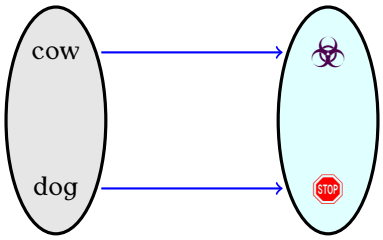


Figure 1: A graphical representation of the function in Example 5.1 fig:cowdog

- One can imagine all sorts of functions in this way. For example, consider 2 abstract sets $A := \{a_1, \ldots, a_3\}$ and $B := \{b_1, b_2\}$, together with the function $f : A \to B$ that is defined as $f(a_1) = f(a_3) = b_2$ and $f(a_2) = b_1$. We can think of this function, pictorially, as is shown in Figure 2

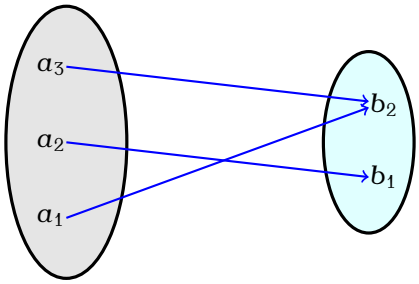


Figure 2: A graphical representation of the function in Example 5.1 fig:ab

- A function f is said to be *real valued* when it maps some set A to a subset of $\mathbb{R}$ [possibly $\mathbb{R}$ itself]. Most functions that one sees in a standard calculus course are real-valued functions.

  Example 5.3. We can use the relation $f(x) := x^2$ to define a real-valued function from $[0, 1]$ to $\mathbb{R}$. We can use it also to define a [real-valued] function from $\mathbb{R}$ to $[0, \infty)$, as well a [real-valued] function from $\mathbb{N}$ to $[0, \infty)$. However, $f(x) = x^2$ does not define a function from any subset of $\mathbb{R}$ to $(-\infty, 0)$.

  Example 5.4 (Floor and Ceiling Functions)**.** Two functions of import in discrete mathematics are the floor and the ceiling. The *floor* of any

real number x—denoted by $\lfloor x \rfloor$—is the largest integer that is $\leq x$. The *ceiling* of x—denoted by $\lceil x \rceil$ is the smallest integer $\geq x$. For instance,

$$\lfloor 1.5 \rfloor = \lfloor 1.99 \rfloor = 1, \quad \text{and} \quad \lceil 1.5 \rceil = \lceil 1.99 \rceil = 2.$$

Similarly,

$$\lfloor -1.5 \rfloor = \lfloor -1.99 \rfloor = -2, \quad \text{and} \quad \lceil -1.5 \rceil = \lceil -1.99 \rceil = -1,$$

etc.

Example 5.5 (The Factorial Function)**.** The *factorial* function is the function $f : \mathbb{Z}_+ := \{0, 1, 2, \ldots\} \to \mathbb{Z}_+$, defined as $f(n) := n!$, where

$$0! := 1, \quad 1! := 1,$$

and

$$\forall n \geq 2 : \ n! := n \times (n-1)!.$$

Therefore, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, $4! = 4 \times 3 \times 2 \times 1 = 24$, etc. It is often better to write $n!$ than to evaluate it numerically, in part because $n!$ is a huge number even when n is modestly large. For instance:

$$10! \approx 3.6 \times 10^6; \ 15! \approx 1.3 \times 10^{12}; \ \text{ and } \ 20! \approx 2.4 \times 10^{18}.$$

Abraham de Moivre (1728) proved that there exists a number $B \approx 2.5$ such that $n!(n/e)^{-n} n^{-1/2} \to B \qquad \text{as } n \to \infty$. A few years later (1730), James Stirling proved that $B = \sqrt{2\pi}$. In other words, the formula of de Moivre, and later Stirling, tells us that

$$n! \approx \sqrt{2\pi} n^{n+(1/2)} e^{-n} \qquad \text{for } n \text{ large.}$$

This approximation is nowadays called *Sitrling's formula*, though the ascription is admittedly inaccurate. Stirling's formula yield good results even when n is modestly large. For instance, it yields $10! \approx 3.5987 \times 10^6$, when in fact $10! = 3,628,800$.

5.2 The Graph of a Function

- The *graph* of a function $f : A \to B$ is the set

$$\{(a, f(a)) : a \in A\} = \{(a, b) : \ [a \in A] \vee [b = f(a)]\}.$$

Example 5.6. You have encountered graphs of functions many times already in this and your other mathematics courses. For instance, in Figure 3 you can seea plot of the graph $f(x) := x^3$ that maps $A := [-1, 1]$ to $B := [-5, 8]$ (say). Of course, we could also think of this function f as a map from $A := [-1, 1]$ to $B := [-1, 1]$, etc.

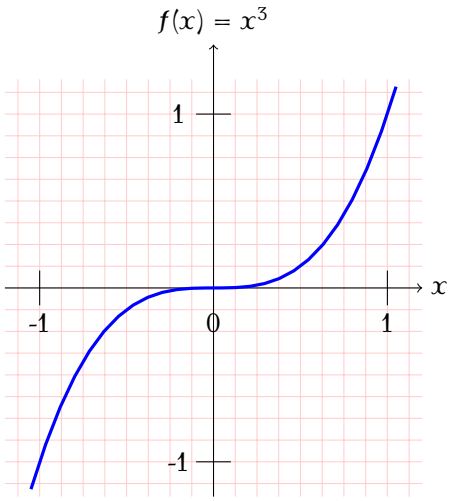


Figure 3: The function $f(x) = x^3$ plotted over the region $-1 \leq x \leq 1$ fig:x^3

Example 5.7. Consider the function f that is defined on the domain

$$A := \{-2, -1.5, -1, 0, 1, 2\}$$

as follows:

x	-2	-1.5	-1	0	1	2
$f(x)$	0.5	1.5	-1.5	2	1	0

We can think of f as a function from $A := \{-2, -1.5, -1, 0, 1, 2\}$ to $B := [-2, 2]$ (say), or from A to $B := \{-1.5, 0, 0.5, 1, 1.5, 2\}$, etc. The graph of the function f is plotted in Figure 4. Note that the graph is "discrete"; that is, it constitutes a finite collection of singletons. In this sense, the graph of the function of this example appears to be different from the graph of a function such as $f(x) = x^3$ in the previous example. Note, however, that the graph of $f(x) = x^3$ is also a collection of singletons; it is just not a finite collection.

Example 5.8. In Figure 5 you can find a plot of the floor function $f(x) = \lfloor x \rfloor$ from $A := [-3, 3]$ to $B := [3, 3]$ (say). Can you plot the ceiling function $g(x) = \lceil x \rceil$ from $A := [-3, 3]$ to $B := [-3, 3]$?

5.3 One-to-One Functions

- Consider a function $f : A \to B$ from a set A to a set B. If $S \subseteq A$ is a subset of A, then the *image* of S under f is the set

  $$f(S) := \{f(x) : x \in S\}.$$

  I emphasize the fact that $f(S) \subseteq B$.

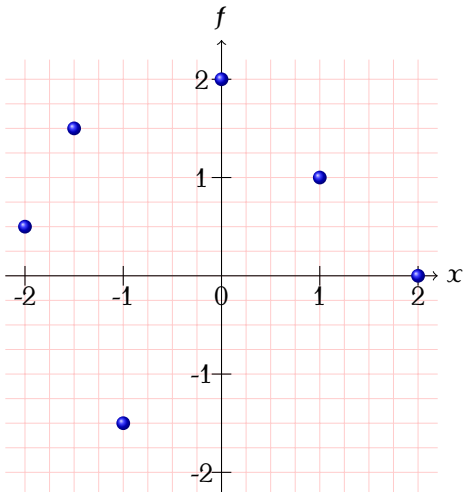


Figure 4: A discrete function

fig:discrete:f

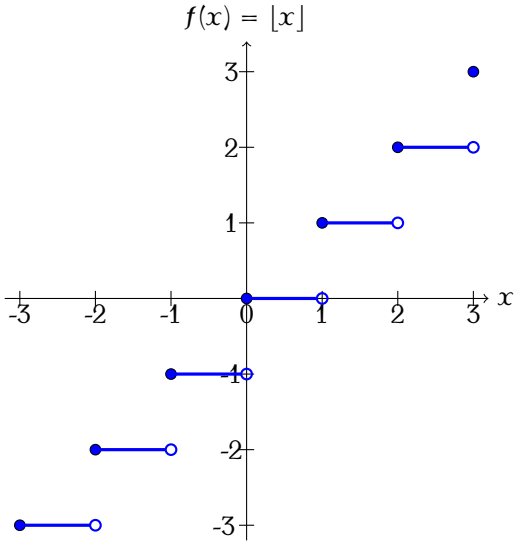


Figure 5: The floor function

fig:floor

Example 5.9. Consider the function $f : \{a_1, a_2, a_3\} \to \{b_1, b_2, b_3\}$, depicted in the following graphical representation:

Then, $f(\{a_2, a_3\}) = \{b_2\}$ and $f(\{a_1\}) = \{b_1\}$.

Example 5.10. Consider the function $f : [0, 2\pi] \to \mathbb{R}$ that is defined by $f(x) := \sin(x)$ for all $x \in [0, 1]$. Then, $f([0, \pi/2]) = f([0, \pi]) = [0, 1]$, $f([\pi, 2\pi]) = [-\pi, 0]$, and $f([0, 2\pi]) = [-1, 1]$.

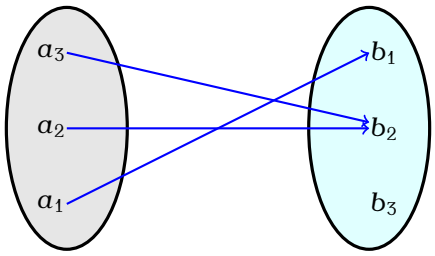


Figure 6: A function on three points. fig:ab:1

Example 5.11. If x is a real number, then there is a unique largest integer that is to the left of x; that integer is usuall denoted by $\lfloor x \rfloor$, and function $f := \lfloor \bullet \rfloor$ is usually called the *floor*, or the *greatest integer*, function. It is a good exercise to check that, if f denotes the floor function, then $f[1/2, 2] = \{0, 1, 2\}$.

- Let $f : A \to B$ denote a function from a set A to a set B. We say that f is *one-to-one* [or 1-1, or *injective*] if

$$\forall x, y \in A : \ [f(x) = f(y)] \to [x = y].$$

- Easy exercise: $f : A \to B$ is 1-1 if and only if

$$\forall x, y \in A : \ [f(x) = f(y)] \leftrightarrow [x = y].$$

Proposition 5.12. *Consider a function $f : A \to B$, where $A \subseteq \mathbb{R}$ and $B \subseteq \mathbb{R}$, and suppose that f is* strictly increasing*; that is,*

$$\forall x, y \in A : \ [x < y] \to [f(x) < f(y)].$$

Then f is one-to-one.

Proof. It suffices to prove that

$$\forall x, y \in A : \ [x \neq y] \to [f(x) \neq f(y)].$$

Suppose $x, y \in A$ are not equal. Then either $x < y$ or $y < x$. In the first case, $f(x) < f(y)$ and in the second case, $f(y) < f(x)$. In either case, we find that $f(x) \neq f(y)$. □

Example 5.13. Define a function $f : [0, 1] \to \mathbb{R}$ via $f(x) := x^2$. Then f is one-to-one.

Example 5.14. Define a function $f : [\pi/2, 3\pi/2] \to \mathbb{R}$ via $f(x) := \sin(x)$. Then f is one-to-one.

In order to show that a function is not 1-1, we need to construct, using whatever means we have, two points x, y such that $x \neq y$ and yet $f(x) = f(y)$. Depending on the function, this process can, or cannot, be very easy. Here are two very easy examples.

Example 5.15. Define a function $f : [-1, 1] \to \mathbb{R}$ via $f(x) := x^2$. Then f is not one-to-one.

Example 5.16. Define a function $f : [\pi/2, 2\pi] \to \mathbb{R}$ via $f(x) := \sin(x)$. Then f is not one-to-one.

Example 5.17. The function depicted in Figure 1 is 1-1, whereas the ones in Figures 2 and 6 are not.

5.4 Onto Functions

- A function $f : A \to B$ is said to be *onto* [or *surjective*] if

$$\forall b \in B \, \exists a \in A : f(a) = b.$$

  In other words, f is onto if and only if $f(A) = B$.

- In order to prove that a certain function $f : A \to B$ is not onto we need to find, using whatever means we have, a point $b \in B$ such that $b \neq f(a)$ for any $a \in A$.

  Example 5.18. The functions depicted in Figures 1 and 2 are onto, whereas the one in Figure 6 is not.

  Example 5.19. Being onto can have to do with our choice of the range set B, and there in fact can be different choices for B. As an example consider the function f in Figure 4, and define three sets, $A := \{-2, -1.5, -1, 0, 1, 2\}$, $B_1 := [-2, 2]$, and $B_2 := \{-1.5, 0, 0.5, 1, 1.5, 2\}$. We can view f either as a function from A to B_1, or as a function from A to B_2. In the former case, f is one-to-one but not onto. In the latter case, f is one-to-one, and onto.

  Example 5.20. Define a function $f : [0, 1] \to [0, 1]$ via $f(x) := x^2$. Then f is onto. So is the function $f : [-1, 1] \to [0, 1]$, defined via $f(x) := x^2$. See Figure 7. On the other hand, the function $f : [0, 1] \to [-1, 1]$, defined via $f(x) := x^2$, is not onto.

5.5 Inverse Functions

- If $f : A \to B$ is both 1-1 and onto, then we say that f is *invertible*.

- The definitions of one-to-one and onto functions together teach us that if f is invertible, then to every point $b \in B$ we can associate a unique point $a \in A$ such that $f(a) = b$. We define $f^{-1}(b) := a$ in this case. Then, $f^{-1} : B \to A$ is a function, and referred to as the *inverse function* to f [or the *inverse of* f].

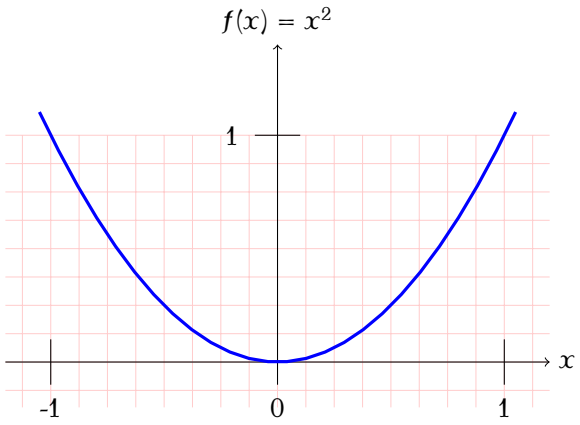


Figure 7: The function $f(x) = x^2$ plotted over the region $-1 \leq x \leq 1$ fig:x^2

Example 5.21. The function f that was depicted in Figure 1 is both 1-1 and onto. Therefore, it has an inverse f^{-1}. One can explicitly write that inverse as follows:

$$f^{-1}(\text{STOP}) = \text{dog} \quad \text{and} \quad f^{-1}(\text{☣}) = \text{cow}.$$

This function can be depicted pictorially as in Figure 8 below.

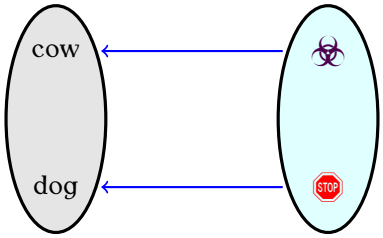


Figure 8: The inverse of the function in Example 5.1 fig:inverse:cowdog

Example 5.22. The functions in Figures 2 and 6 are not invertible.

5.6 Composition of Functions

- Choose and fix three sets, A, B, and C. If we have a function $f : A \to B$ and a function $g : B \to C$, then we can *compose* them in order to obtain a new function $g \circ f : A \to C$ as follows:

$$\forall x \in A : (g \circ f)(x) := g(f(x)).$$

The function $g \circ f$ is called the *composition of g with f*.

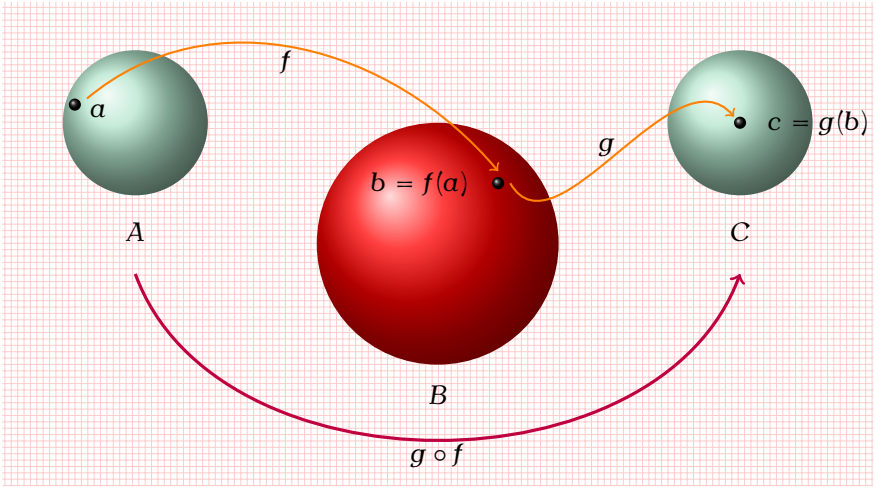


Figure 9: The composition $g \circ f$ of $g : B \to C$ with $f : A \to B$ fig:compose

Figure 9 depicts graphically how the point $a \in A$ gets mapped to $b = f(a) \in B$ by the function f, and in turn to the point $c = g(b) = g(f(a)) = (g \circ f)(a) \in C$ by the function g. We can think of the resulting mapping $g \circ f$ directly as a function that maps $a \in A$ to $c = (g \circ f)(a) \in C$.

Example 5.23. Suppose $f(a) := a^2$ for every positive integer a, and $g(b) := 1 + b$ for every positive integer b. Then, in this example, $A = B = C = \mathbb{N}$, and $(g \circ f)(a) = 1 + a^2$ for every positive integer a. Because here we have $A = B = C$, we could also consider the composed function $(f \circ g)(x) = (1 + x)^2$ for every positive integer x.

- The following follows immediately from the definitions by merely reversing the arrows in Figure 9. Can you turn this "arrow reversal" into a rigorous proof?.

  Proposition 5.24. *Suppose $f : A \to B$ and $g : B \to C$ are as above. Suppose, in addition, that f and g are invertible. Then, $g \circ f : A \to C$ is invertible and*

$$\forall c \in C : (g \circ f)^{-1}(c) = f^{-1}\left(g^{-1}(c)\right) = \left(f^{-1} \circ g^{-1}\right)(c).$$

5.7 Back to Set Theory: Cardinality

- For every integer $n \geq 1$, the *cardinality* of $\{1, \ldots, n\}$ is defined as $|\{1, \ldots, n\}| := n$.
- We say that A and B have the same *cardinality* if and only if there exists a 1-1 onto function $f : A \to B$. In this case, we write $|A| = |B|$.

Lemma 5.25. *If A has n elements, where $n \geq 1$ is an integer, then $|A| = n$.*

Proof. We can write A as $\{a_1, \ldots, a_n\}$ for some distinct $a_1, \ldots, a_n$. The function $f(x) := a_x$ $[x = 1, \ldots, x]$ is 1-1 onto from $\{1, \ldots, n\}$ to A. Therefore, $|A| = |\{1, \ldots, n\}| = n$. □

- The *cardinality* of $\mathbb{N}$ is defined as $|\mathbb{N}| := \aleph_0$ [read as "aleph-naught," after the Hebrew letter "aleph," which is written as $\aleph$].
- We say that a set A is *countable* if $|A| = \aleph_0$. We say that A is *denumerable* when A is either countable or finite. If A is not countable nor finite, then we say that A is *uncountable*.

Proposition 5.26. *The set of all even integers, the set of all odd integers, and the collection $\mathbb{Z}$ of all integers are all countable sets.*

Proof. Let $\mathbb{E}$ denote the set of all even integers. Define $f(x) := x/2$ for all $x \in \mathbb{E}$; thus, for example, $f(2) = 1$, $f(4) = 2$, $f(6) = 3$, etc. You should check that $f : \mathbb{E} \to \mathbb{N}$ is 1-1 onto (induction). It follows that $|\mathbb{E}| = \aleph_0$.

Similarly, let $\mathbb{O}$ denote the set of all odd integers. Define $g(x) := (x + 1)/2$ for all $x \in \mathbb{O}$; thus, for example, $g(1) = 1$, $g(3) = 2$, $g(5) = 3$, etc. You should check that $g : \mathbb{O} \to \mathbb{N}$ is 1-1 onto (induction). It follows that $|\mathbb{O}| = \aleph_0$.

Now let us prove that $|\mathbb{Z}| = \aleph_0$. Define a function f on $\mathbb{Z}$ as follows: For all integers x,

$$f(x) := \begin{cases} 2x & \text{if } x \geq 0, \\ -2x - 1 & \text{if } x < 0. \end{cases}$$

Thus, for example, $f(0) = 2$, $f(1) = 4$, $f(2) = 6$, ...and $f(-1) = 1$, $f(-2) = 3$, $f(-3) = 5$, ... You should check that f is 1-1 onto from $\mathbb{Z}$ to $\mathbb{N}$ [it maps nonnegative elements of $\mathbb{Z}$ to $\mathbb{E}$ and negative elements of $\mathbb{Z}$ to $\mathbb{O}$]. This proves that $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$. □

There are obvious, or at least nearly-obvious, variations on the preceding which one can work out as basic exercises. For instance, you should check that the set $\{2, 3, \ldots\}$ of integers ≥ 2 is countable. And so is $\{\cdots, -7, -6, -5\}$, the set of integers ≤ -5. The following novel departure from the obvious should not be missed.

th:Cantor

Theorem 5.27 (Cantor)**.** *If A is a bounded open interval, then $|A| = |\mathbb{R}|$.*

Proof. We can write $A := (a\,,b)$, where $a < b$ are real numbers. Define

$$f(x) := \frac{x-a}{b-a} \qquad \text{for } a < x < b.$$

Because $f : (a\,,b) \to (0\,,1)$ is 1-1 onto, it follows that $|(a\,,b)| = |(0\,,1)|$. In particular, $|(a\,,b)|$ does not depend on the numerical value of $a < b$; therefore, we may—and will—assume without loss of generality that $a = -\pi/2$ and $b = \pi/2$. Now consider the function

$$g(x) := \tan(x) \qquad \text{for } -\frac{\pi}{2} < x < \frac{\pi}{2}.$$

Because $g : (-\pi/2\,,\pi/2) \to \mathbb{R}$ is 1-1 onto, it follows that $|(-\pi/2\,,\pi/2)| = |\mathbb{R}|$, which concludes the proof. □

- Suppose there exists a one-to-one function $f : A \to B$. Then we say that the *cardinality* of B is greater than that of A, and write it as $|A| \le |B|$.

  The following might seem obvious, but is not when we pay close attention to the definitions [as we should!!].

th:SB

Theorem 5.28 (Cantor, Schröder, and Bernstein). *If $|A| \le |B|$ and $|B| \le |A|$ then $|A| = |B|$.*

The proof is elementary but a little involved. You can find all of the details on pp. 103–105 of the lovely book, *Sets: Naïve, Axiomatic, and Applied* by D. van Dalen, H. C. Doets, and H. de Swart [Pergamon Press, Oxford, 1978], though this book refers to Theorem 5.28 as the "Cantor–Bernstein theorem," as is also sometimes done. Instead of proving Theorem 5.28, let us use it in a few examples.

Example 5.29. Let us prove that $|(0\,,1)| = |(0\,,1]|$. Because

$$(0\,,1) \subseteq (0\,,1] \subseteq \mathbb{R},$$

Theorem 5.27 shows that $|(0\,,1)| \le |(0\,,1]| \le |\mathbb{R}| = |(0\,,1)|$. Now appeal to Theorem 5.28 in order to conclude that $|(0\,,1)| = |(0\,,1]|$.

The following is another novel departure from the obvious.

th:Cantor:Q

Theorem 5.30 (Cantor). *$\mathbb{Q}$ is countable.*

Proof. Because $\mathbb{Z}$ is countable, it suffices to find a 1-1 onto function $f : \mathbb{Z} \to \mathbb{Q}$. In other words, we plan to list the elements of $\mathbb{Q}$ as a sequence $\cdots, x_{-3}, x_{-2}, x_{-1}, x_0, x_1, x_2, x_3, \ldots$ that is indexed by all integers.

We start by writing all strictly-positive rationals as follows:

Then we create a series of arrows as follows:

$$\begin{array}{cccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \cdots \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \cdots \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Figure 10: A way to list all strictly-positive elements of $\mathbb{Q}$

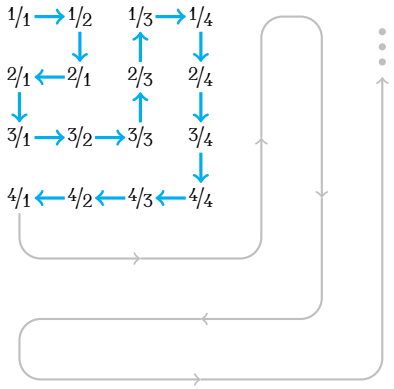


Figure 11: Navigation through strictly-positive elements of $\mathbb{Q}$

Now we define a function f by "following the arrows," except every time we encounter a value that we have seen before, we suppress the value and proceed to the next arrow:

$$\begin{array}{llllll} & f(1) := 1/1 & \to & f(2) := 1/2 & \to & f(3) := 2/1 \\ \to & f(4) := 3/1 & \to & f(5) := 3/2 & \to & [3/3 \text{ suppressed}] \\ \to & f(6) := 2/3 & \to & f(7) := 1/3 & \to & f(8) := 1/4 \\ \to & [2/4 \text{ suppressed}] & \to & f(9) := 3/4 & \to & [4/4 \text{ suppressed}] \\ \to & f(10) := 4/3 & \to & [4/2 \text{ suppressed}] & \to & f(11) := 4/1 \\ \to & \text{etc.} & & & & \end{array}$$

Also, define $f(0) := 0$ and $f(x) := -f(-x)$ for all strictly-negative integers x. Then $f : \mathbb{Z} \to \mathbb{Q}$ is 1-1 onto, whence $|\mathbb{Z}| = |\mathbb{Q}|$. Since $\mathbb{Z}$ is countable, the existence of such a function f proves that $\mathbb{Q}$ is also countable. □

And here is an even more dramatic departure from the obvious:

th:Cantor:1

Theorem 5.31 (Cantor). $\mathbb{R}$ *is uncountable.*

Proof. Thanks to Theorem 5.27, Theorem 5.31 is equivalent to the assertion that $(0,1)$—or $(e\pi^2, \pi^3)$ for that matter—is uncountable. I will prove that $(0,1)$ is uncountable. Te proof hinges on a small preamble from classical number theory.

Every number $x \in (0,1)$ has a decimal representation,

$$x = 0.x_1x_2\cdots = \frac{x_1}{10} + \frac{x_2}{100} + \frac{x_3}{1000} + \cdots = \sum_{i=1}^{\infty} \frac{x_i}{10^i},$$

where $x_1, x_2, \ldots \in \{0, \ldots, 9\}$ are the respective digits in the decimal expansion of x. Note, for example, that we can write $1/2$ either as 0.5 or as $0.4\bar{9}$. That is, we can write, for $x = 1/2$, either $x_1 = 5$, $x_2 = x_3 = \cdots = 0$, or $x_1 = 4$, and $x_2 = x_3 = \cdots = 9$. This example shows that the choice of $x_1, x_2, \ldots$ is not always unique. From now on, we compute the x_i's such that whenever we have a choice of an infinite decimal expansion that ends in all 9's from some point on or an expansion that terminates in 0's from some point on, then we opt for the 0's case. In this way we can see that the x_i's are defined uniquely; that is, if $x, y \in (0,1)$, then $x_i = y_i$ for all $i \geq 1$; and conversely, if $x_i = y_i$ for all $i \geq 1$ then $x = y$.

The preceding shows that $(0,1)$ is in 1-1, onto correspondence with the collection S of all infinite sequences of the form $(x_1, x_2, \ldots)$ where $x_i \in \{0, \cdots, 9\}$ for all $i \geq 1$. In particular, it suffices to prove that S is not countable.

Suppose, to the contrary, that S is countable. If this were so, then we could enumerate its elements as $s_1, s_2, \ldots$; that is, $S = \{s_1, s_2, \ldots\}$, where the s_i's are distinct and

$$\begin{aligned} s_1 &= (x_{1,1}, x_{1,2}, x_{1,3}, \ldots), \\ s_2 &= (x_{2,1}, x_{2,2}, x_{2,3}, \ldots), \\ s_3 &= (x_{3,1}, x_{3,2}, x_{3,3}, \ldots), \ \ldots \end{aligned}$$

and $x_{i,j} \in \{0, \ldots, 9\}$ for all $i, j \geq 1$. In order to derive a contradiction we will prove that there exists an infinite sequence $y := (y_1, y_2, \ldots)$ such that $y \notin S$, and yet $y_i \in \{0, \ldots, 9\}$ for all $i \geq 1$. This yields a contradiction since we know already that S is the collection of all sequences of the form $x_1, x_2, \ldots$ where $x_i \in \{0, \ldots, 9\}$. In particular, it will follow that S cannot be enumerated.

To construct the point y, we consider the "diagonal subsequence," $x_{1,1}, x_{2,2}, x_{3,3}, \ldots$ and define, for all $j \geq 1$,

$$y_j := \begin{cases} 0 & \text{if } x_{j,j} \neq 0, \\ 1 & \text{if } x_{j,j} = 0. \end{cases}$$

Then the sequence $(y_1, y_2, \ldots)$ is different from the sequence s_i, for every $i \geq 1$, since y_i and $x_{i,i}$ are different. In particular, $y \notin S$. □

- The preceding argument is called "Cantor's diagonalization argument."
- One can learn a good deal from studying very carefully the proof of Theorem 5.31. For instance, let us proceed as we did there, but expand every $x \in (0,1)$ in "base two," rather than in "base ten." In other words, we can associate to every $x \in (0,1)$ a sequence $x_1, x_2, \ldots$ of digits in $\{0,1\}$ such that

$$x = 0.x_1x_2\cdots = \sum_{i=1}^{\infty} \frac{x_i}{2^i}.$$

In order to make the choice of the x_i's unique, we always opt for a sequence that terminates in 0's rather than 1's, if that ever happens. [Think this through.] This expansion shows the existence of a 1-1 and onto function $f : (0,1) \to \mathcal{B}$, where $\mathcal{B}$ is the collection of all infinite sequences of 0's and 1's. In other words, $|(0,1)| = |\mathcal{B}|$, and hence $|\mathcal{B}| = |\mathbb{R}|$, thanks to Theorem 5.27. Now let us consider the following function $g : \mathcal{B} \to \mathcal{P}(\mathbb{Z}_+)$, where I recall $\mathcal{P}(\cdots)$ denotes the power set of whatever is in the parentheses: For every sequence $(s_1, s_2, \ldots) \in \mathcal{B}$ of 0's and 1's, $g(s_1, s_2, \cdots) := \cup\{k\}$, where the union is taken over all nonnegative integers k such that $s_1 = 1$. For instance,

$$\begin{aligned} g(0,0,\cdots) &= \varnothing, \\ g(1,0,0,\cdots) &= \{0\}, \\ g(0,1,0,0,\ldots) &= \{1\}, \\ g(1,1,0,0,0,\ldots) &= \{0,1\}, \\ g(1,1,1,\cdots) &= \mathbb{Z}_+, \cdots. \end{aligned}$$

A little work implies that $g : \mathcal{B} \to \mathcal{P}(\mathbb{Z}_+)$ is 1-1 and onto, and hence $|\mathcal{B}| = |\mathcal{P}(\mathbb{Z}_+)|$, which we saw earlier is equal to $|\mathbb{R}|$. We have shown most of the proof of the following theorem [the rest can be patched up with a little work].

Theorem 5.32. $|\mathbb{R}| = |\mathcal{P}(\mathbb{Z}_+)|$.