

4. Symbolic Logic

In this lecture, we shall learn some of the basics of symbolic logic – ways to read and write in a commonly used symbolic language.

Just like any other languages, this one has its own vocabulary and grammatical or syntax rules. However, there are some important differences between an ordinary literary language (say, English) and this symbolic language. At the basic level, its alphabet and vocabulary list is very short. The syntax rules are fairly simple and intuitive, but are strict and precise.

Once again, in this lecture, we will encounter a small number of primitive terms (examples: if, then, or, and, unique, exist, etc.) that we can't define, but the ways in which they are used in logic will be explained. Since these terms already exist in English, important lessons can be drawn from the ways in which they are commonly used in ordinary communication. Indeed, the rules governing their use in logic are really just a precise version of some of the rules governing their use in English. That being said, it is important to keep in mind that using those terms in logic does require a bit more care than we normally exercise in our daily use of English.

4.1. Statements

There are exactly two kinds mathematical statements. Statements of the first kind are said to be *universally quantified*, and they are of the form or can be put into the *standard form*

For every member x of A , $P(x)$ is true.

Here $P : U \rightarrow \{true, false\}$ is a binary function defined on some pre-determined set U containing A as a subset. Statements of the second kind are said to be *existentially quantified*, and they are of the form or can be put into the standard form

There exist a member x of A such that $P(x)$ is true.

Again, P is a binary function defined on some pre-determined set U that contains A as a subset.

Let's consider some examples.

- i. Every real number x is such that $|x| \geq x$.
- ii. Every real number x is such that $|x| \leq x$.
- iii. We can find a real number x such that $|x| \leq x$.
- iv. We can find a real number x such that $|x| < x$.
- v. We can find a real number x such that $x^8 - x + \frac{3}{4} < 0$.
- vi. We can find a real number x such that $x^2 = y$.

All of these are considered mathematical statements, some of which are true, some false, and one is incomplete and whose truth value depends on a further input.

Statement i is universally quantified, because it is equivalent to the standard form "For every member x of \mathbf{R} , $P(x)$ is true," where $P : \mathbf{R} \rightarrow \{true, false\}$ is the function that assigns to each $x \in \mathbf{R}$ the value " $|x| \geq x$ ", which happens to be *true* for every $x \in \mathbf{R}$. (Note that we are able to see the equivalence only because we are drawing on lessons from common usage of similar sentences in English.) Thus, we say that statement i is true.

Statement ii also has the same form, but $P(x)$ in this case is the value $|x| \leq x$, which can be true or false depending on $x \in \mathbf{R}$. For instance, $P(1) = true$ but $P(-1) = false$. Thus, we say that statement ii is false, because it is *not* the case that every real number x has the property that $|x| \leq x$.

Statement iii-v are all existentially quantified, because each of them is equivalent to the standard form “There exist a member x of A such that $P(x)$ is true.” For iii, $P(x)$ is $|x| \leq x$. Since we have found that the number 1 makes $P(1) = \text{true}$, iii is true. In iv, $|x| < x$ is false for any $x \in \mathbf{R}$. So, iv is false. Even though it is not immediately clear if v is true or false (because it is not obvious how to solve the inequality appearing in v without more work,) there is no doubt that it is a bona fide statement.

Finally, vi is an *incomplete* statement because the expression $x^2 = y$ does not constitute a binary function, since it contains a symbol y whose value has never been provided in this context, hence there is no way to evaluate $x^2 = y$ even if a specific number x is given. The right way to view vi is that it is a *formula* for a binary function. Let's denote by $P(y)$. Then given a number y , $P(y) = \text{true}$ if a number x can be found to solve $x^2 = y$, and $P(y) = \text{false}$ otherwise. The next example illustrate how we can use vi as a binary function in a complete statement.

vi'. For every real number y , we can find a real number x that has the property that $x^2 = y$.

This is a universally quantified statement. Note that vi is playing the role of a binary function in vi'. Statement vi' is, of course, false since no solution $x \in \mathbf{R}$ to $x^2 = y$ can be found when $y < 0$. Finally, we can modify vii' to a true statement (cf. the Square Root Theorem) by adding just one word:

vi''. For every positive real number y , we can find a real number x that has the property that $x^2 = y$.

4.2. Symbolic statements

We now learn how to write a universally or an existentially quantified statement in purely symbolic form. We introduce the following symbols and how they are used:

Name	Symbol	Syntax	Meaning
Universal quantifier	\forall	$(\forall x \in U)P(x)$	For every $x \in U$, $P(x)$ is true.
Existential quantifier	\exists	$(\exists x \in U)P(x)$	There exists $x \in U$ such that $P(x)$ is true.

Here $P : U \rightarrow \{true, false\}$ is a binary function, which we shall refer to as the *primary binary function* of a statement.

Negation. We can always negate a given statement by adding the phrase “It is not true that.” For instance, we can negate the existentially quantified statement “There is a genius whose IQ score is 200” by saying “It is not true that there is a genius whose IQ score is 200.” But which of the two kinds is the latter negated statement – is it universally or existentially quantified? That negated statement is clearly equivalent to “Every genius has IQ score not equal to 200.” Thus, it is a universally quantified statement. Likewise, negating a universally quantified statement yields an existentially quantified statement. Symbolically, we have the following rules:

Negation	Standard form	Meaning
$\neg(\forall x \in U)P(x)$	$(\exists x \in U)\neg P(x)$	There exists $x \in U$ such that $P(x)$ is false.
$\neg(\exists x \in U)P(x)$	$(\forall x \in U)\neg P(x)$	For every $x \in U$, $P(x)$ is false.

For example, consider a function $f : \mathbf{R} \rightarrow \mathbf{R}$. We can give the definition of boundedness of f in symbolic form. We say that f is bounded if

$$(\exists M \in \mathbf{R})(\forall x \in \mathbf{R})(|f(x)| \leq M).$$

Note that this statement is in the standard form $(\exists M \in \mathbf{R})P(M)$, where the primary binary function in this case is given by $P(M) = (\forall x \in \mathbf{R})(|f(x)| \leq M)$, which is itself an existentially quantified statement. To say that f is not bounded or unbounded is the say that

$$\neg(\exists M \in \mathbf{R})(\forall x \in \mathbf{R})(|f(x)| \leq M).$$

This is also equivalent to

$$(\forall M \in \mathbf{R})\neg(\forall x \in \mathbf{R})(|f(x)| \leq M).$$

In turn, this is equivalent to

$$(\forall M \in \mathbf{R})(\exists x \in \mathbf{R})\neg(|f(x)| \leq M).$$

Finally, this is equivalent to

$$(\forall M \in \mathbf{R})(\exists x \in \mathbf{R})(|f(x)| > M).$$

Verbally, this says that for any given $M \in \mathbf{R}$, there is a number x such that $|f(x)|$ exceeds M .

Example. Here is the definition for surjectivity in symbolic form. We say that a function $f : A \rightarrow B$ is surjective if

$$(\forall y \in B)(\exists x \in A)(f(x) = y).$$

4.3. Logical connectives

There are a number of ways to form a compound statement – symbolic or otherwise – from simpler ones: by using words such as *not*, *and*, *or*. These operators on statements are called *logical connectives*. Without them, it would be very difficult to make even the most commonly used mathematical statements. For example, there would be no way to state the definition of injectivity of a function $f : A \rightarrow B$.

Here is a list of commonly used logical connectives and their symbolic forms:

Name	Syntax	Meaning	When is it true?
Negation	$\neg P$	not P	P is false.
Conjunction	$P \wedge Q$	P and Q	both P, Q are true.
Disjunction	$P \vee Q$	P or Q	at least one of P, Q is true.
Conditional	$P \Rightarrow Q$	if P , then Q	P implies Q .
Biconditional	$P \Leftrightarrow Q$	P if and only if Q	P and Q have the same truth value.

As we shall see, these logical connectives are not all independent. In fact, each of the last three can be expressed as some combination of negation and conjunction.

The following *truth table* summarizes the truth values of a negative, a conjunctive and a disjunctive statements depending on the truth values of their constituents statements P, Q .

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$
T	T	F	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	F

Exercise. Using this truth table, work out the truth tables for $\neg(P \vee Q)$ and for $\neg P \wedge \neg Q$, and see that they are the same. In other words, those two statements are equal. Likewise,

verify that the statement $\neg(P \wedge Q)$ is equal to $\neg P \vee \neg Q$. The two equalities are called de Morgan's rules in logic.

Here is a common English sentence that illustrates the first de Morgan's rule. "It is *not true* that John is both Canadian *and* American." This is saying that John lacks at least one of those two citizenships. So, the statement has the same truth value as "John is *not* a Canadian *or* he is *not* an American."

When is a conditional $P \Rightarrow Q$ false? Imagine that your boss says that "If you finish your work by 3pm, then you can go home early." The one and *only* scenario in which you can claim that he lies is when you actually finish your work by 3pm, but he doesn't let you go home early. Similarly, the one and only case in which we can say that the conditional statement "If P , then Q " is *false* is when P is true and Q is false. The following *truth table* summarizes all truth values of a conditional statement, and compares it with another compound statement.

P	Q	$P \Rightarrow Q$	$(\neg P) \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

This table shows that the two compound statements $P \Rightarrow Q$ and $(\neg P) \vee Q$ are equal. The last two rows of the table has the following important implication in logic: *you can prove any conclusion, if you allow yourself to make a false assumption.*

Exercise. Work out the truth tables for $P \Leftrightarrow Q$ and for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, and see that they are equal.

Exercise. Verify that the statement $P \Rightarrow Q$ is equal to $(\neg Q) \Rightarrow (\neg P)$. Therefore, to prove a statement of the form $P \Rightarrow Q$, it is equally valid to prove $(\neg Q) \Rightarrow (\neg P)$.

Example. Let $f : A \rightarrow B$ be a function. We can now state the definition for injectivity of f in symbolic form. We say that f is injective if and only if

$$(\forall x \in A)(\forall y \in A)(x \neq y \Rightarrow f(x) \neq f(y)).$$

Note that $x \neq y$ is the same as $\neg(x = y)$. By the preceding exercise, we can also say that f is injective if and only if

$$(\forall x \in A)(\forall y \in A)(f(x) = f(y) \Rightarrow x = y).$$

Example. Let's translate to symbolic form the statement: "There is a unique positive number x such that $x^2 = 2$." It helps to put this verbal statement into a standard form first. It says: "There exists $x \in \mathbf{R}$ such that $x > 0$ and $x^2 = 2$, and that if y is any other number with these two properties then $y = x$." Here is a symbolic translation:

$$(\exists x \in \mathbf{R})[(x > 0 \wedge x^2 = 2) \wedge (\forall y \in \mathbf{R})((y > 0 \wedge y^2 = 2) \Rightarrow y = x)].$$

Exercise. State the Square Root Theorem in symbolic form.

4.4. Useful tips for translations

Multiple variants. When translating a verbal statement to a symbolic one and back, it is important to keep in mind that there can be many different variants of verbal equivalents of the same symbolic form.

For example, the existential quantification $\exists x$ can be translated into any of the following phrases: we have x , we can find x , there exist(s) x , there is x . The universal quantification $\forall x$ can be translated into any of the following phrases: for every x , for each x , for any given x , for any fixed x , for any arbitrary x , for any fixed but arbitrary x , every x . Note that extra words like "fixed" and "arbitrary" in some of these variants are used for the purpose of emphasis only and are not meant to modify the meaning of universal quantification in any way. The symbolic statement $P \Leftrightarrow Q$ can be translated into any of the following (and back):

- i. P if and only if Q .
- ii. P is necessary and sufficient for Q .
- iii. P is equivalent to Q .

Exercise. Let $g : X \rightarrow Y$ be a given function. Write the Bijectivity Test in symbolic form. First, introduce the following notations. Let $F(X, Y)$ denote the set of functions from X to Y . For $g \in F(X, Y)$, let $Q(g)$ denote the statement that g is bijective.

Sentence helpers. In writing verbal statements, we often use words help use smooth out the English. These words, called *helpers*, often have no symbolic equivalents. Here are some helper phrases: has the property that, is such that, satisfies. Thus, $(\exists x \in A)P(x)$ can be translated into “There is a member x of A that has the property that $P(x)$ is true.” Likewise, “There exists x in A such that $P(x)$,” is just as good. We can also say “We can find x in A such that $P(x)$ holds.”

Order of quantifiers. To avoid one of the most common mistakes in logic, we must keep in mind that the order of certain words is crucial to the meaning of a statement. Consider the statements:

i. $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(y > x)$.

ii. $(\exists y \in \mathbf{R})(\forall x \in \mathbf{R})(y > x)$.

One of them is true, while the other is false. Which one is which? Statement i is true because for every given $x \in \mathbf{R}$, the number $y = x + 1$ makes $y > x$ true. But ii is false, since it says that we can find a single number y that exceeds *all* other numbers. Thus, when a universal and an existential quantifier are next to each other, their order matters!

Fortunately, when two universal quantifiers are right next to each other, their order does not matter. Thus the following two statements are equal:

i. $(\forall x \in A)(\forall y \in B)P(x, y)$.

ii. $(\forall y \in B)(\forall x \in A)P(x, y)$.

Likewise, when two existential quantifiers are right next to each other, their order does not matter.

4.5. Some proof strategies

We have seen that the statement $P \Rightarrow Q$ is equal to $\neg Q \Rightarrow \neg P$. The second

statement is called the *contrapositive* of the first statement. Thus, if we wish to prove a statement of the form $P \Rightarrow Q$, the equality gives us two possible strategies.

A *direct proof method* would be to first assume that P is true, and then use whatever the truth of P tells us to try to derive the truth of Q . A *contrapositive proof method* would be to first assume that Q is false (i.e. $\neg Q$ is true,) and then from this try to show that P is also false.

We have seen several examples of the direct proof method. For example, we have been given two sets A, B and asked to prove $A \subset B$. That means proving

$$x \in A \Rightarrow x \in B.$$

A direct proof approach to this would be to use the assumption that x passes the membership test for A to show that x also passes the membership test for B .

Here is a simple example of the contrapositive argument. Let's prove that $\sqrt{2}$ is not a fraction. This can be stated as the conditional that for $x > 0$,

$$x^2 = 2 \implies x \notin \mathbf{Q}.$$

We assume that $\neg(x \notin \mathbf{Q})$, and we will show that $x^2 \neq 2$. We have $x \in \mathbf{Q}$. Since $x > 0$, we have $x = u/v$ for some positive integers u, v . The Prime Factorization Theorem from arithmetic says that each positive integer n can be expressed as the product of a list of prime number factors, and that if arranged in increasing order the prime factors are uniquely determined by n . Thus, we can express u and v as products of primes, and by canceling out all their common prime factors we can write $x = \frac{u}{v} = \frac{p_1 \cdots p_i}{q_1 \cdots q_j}$, where the p 's and q 's are the remaining prime factors after cancelation, so none of the p 's is equal to any of the q 's. Clearing denominator and squaring yield

$$(*) \quad x^2 q_1^2 \cdots q_j^2 = p_1^2 \cdots p_i^2.$$

This shows that x^2 cannot be 2. For $x^2 = 2$ would imply that 2 is a prime factor of the left side, forcing one of the p 's to be 2 on the right side, by the Prime Factorization Theorem. In this case, canceling out a 2 on both sides would still leave a 2 on the right side, forcing one of the q 's to be 2, and contradicting the fact that none of the p 's is equal to any of the q 's. Thus, we have proved $\neg(x \notin \mathbf{Q}) \Rightarrow \neg(x^2 = 2)$, which is the contrapositive of our original conditional statement.

Actually, the last step of our proof illustrates yet another proof method (embedded within the contrapositive proof method.) From (*), where none of the p 's is equal to any of the q 's, we asserted that $x^2 \neq 2$. We proved this assertion by *first assuming* the contrary $x^2 = 2$, and then we derived a conclusion that contradicts a previously established fact. This method is called the *proof-by-contradiction* method.

4.6. Russell's paradox: a lesson in logic

Bertrand Russell was one of the founders of modern theory of logic and axiomatic set theory. He gave an ingenious argument to demonstrate the need for a solid foundation of set theory, as a basis for any meaningful mathematical discussions. He argued that the notion of sets, while is primitive, must be used with care by laying out appropriate restrictions for it in order to avoid certain contradictions or paradoxes in mathematics. Here was one of his famous examples.

Suppose we declare U to be the set "defined" by the membership test that $x \in U$ if and only if x is a set. So, we call U "the set of all sets." Now define S to be the set consisting of all $x \in U$ such that $x \notin x$. In other words, a set is a member of S if and only if x does not have x itself as a member. Now, since S is a set, a member of U , we can apply the membership test for S to S itself. *Is S a member of S or not?*

It turns out that neither is possible, hence the statement " $S \in S$ " is neither true nor false – a paradox. Let's prove this. If $S \in S$ is true, then S must pass the membership test for S , implying that $S \notin S$ is true, contradicting the supposition that $S \in S$ is true. On the other hand, if $S \in S$ is false, then S must fails the membership test for S , implying that $S \in S$ is true, again a contradiction.

The paradox here was a result of the flaw in our "definition" of U . It was the self-referential nature of its declaration that was getting us into trouble. We did not really specify a good membership test for U . In fact, doing so would require declaring another set (a universe) and defining a binary function on it. Such a universal *set* has no place in mathematics, for allowing it would result in irreparable logical inconsistency.

This is not to say that "the collection of all sets" has no place in mathematics. It is just that Russell's example shows that we must avoid using the term *set* as an attribute for

this collection. Such a collection is called a category, a notion that is essential in modern mathematics.

Exercise. *Self-referential definition can be dangerous.* A liar is a person who lies to you. John says to you “I am a liar.” Is John a liar?

5. Induction

5.1. What is it?

Let's prove the following assertion:

$$(*) \quad \text{For every positive integer } n, \text{ we have } 1 + 2 + \cdots + n = \frac{1}{2}n(n + 1).$$

(A famous anecdote has it that J.C.F. Gauss, the most prodigious mathematician ever lived, discovered this formula in grade school, when his teacher J.G. Büttner told him to add 1 to 100 as a punishment for being too chatty in class.) We can think of the assertion (*) as an infinite list of assertions, indexed by the set of positive integers \mathbf{N} . Let's denote these assertions by $P(1), P(2), P(3), \dots$. Thus, the n th assertion is

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

For example,

$$P(1) : 1 = \frac{1}{2}1(1 + 1),$$

which is true. Similarly, we can verify $P(2), P(3)$, etc. on a case-by-case basis, by numerically computing and comparing both sides of the equation $P(n)$ in each case. While such numerical verifications provide further evidence to support the truth of (*), they by no means constitute a *proof*.

On the other hand, let's say that somehow we can prove the *conditional* statement:

$$(I) \quad (\forall n \in \mathbf{N})[P(n) \Rightarrow P(n + 1)].$$

In other words, for any given n , by *assuming* that and only that

$$P(n) : 1 + 2 + \cdots + n = \frac{1}{2}n(n + 1)$$

is true, we have somehow logically derived from it the equality

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

Is this enough for a proof of ()?* The answer is yes. But before getting into that, let's address one issue that is often troubling to a reader.

Proving the conditional statement (I) may seem like a triviality – because it seems like we have assumed what we are trying to prove. In fact, we have not. One must not confuse (I) with

$$(\forall n \in \mathbf{N})P(n) \Rightarrow (\forall n \in \mathbf{N})P(n + 1)$$

whose proof would be a triviality, because *in this case* we would indeed be assuming what we are trying to prove.

Now, why is proving (I) enough for a proof of (*)? One way to think of (I) is, again, to think of it as an infinite list of statements, one for each $n \in \mathbf{N}$. Thus, (I) can be thought of as the following conjunction of an infinite list of statements

$$P(1) \Rightarrow P(2) \text{ and } P(2) \Rightarrow P(3) \text{ and } \cdots.$$

Since we have verified that $P(1)$ is true, the truth of the conjunction would imply that $P(2)$ is true, which in turn would imply that $P(3)$ is true, and so on. Thus, that (I) is true implies that (*) is true, provided we accept the idea of conjunction of an *infinite* list of statements.

The idea that we can prove (*) by proving $P(1)$ and (I) is known as *the Principle of Induction* (or induction for short,) which we shall accept as an axiom. In symbolic form, this general axiom states that for any given infinite list of statements $P(1), P(2), P(3), \dots$, the statement

$$(\forall n \in \mathbf{N})P(n)$$

is equal to

$$P(1) \wedge (\forall n \in \mathbf{N})[P(n) \Rightarrow P(n + 1)]$$

Verifying the first component $P(1)$ of this compound statement is called the basic step. Proving the second component, i.e. the conditional, is called the inductive step. In this

conditional, $P(n)$ is called the inductive assumption (or hypothesis,) and $P(n + 1)$ the inductive conclusion.

We now apply induction to prove Gauss' theorem (*). We have verified that $P(1)$ is true. Next, our inductive assumption is $P(n)$:

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

Adding $n + 1$ to both sides, we get

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

which is our desired inductive conclusion $P(n + 1)$. Thus by the Principle of Induction, we have proved

$$(\forall n \in \mathbf{N})P(n)$$

which is just the symbolic form of (*).

Incidentally, Gauss probably did not use induction in grade school. It was said that he had the following clever idea: he wrote the sum $1 + 2 + \cdots + n$ (which we will denote by S_n) in two different ways – backward and forward. Thus he got

$$\begin{array}{ccccccc} 1 & + & 2 & + & \cdots & + & n \\ n & + & n - 1 & + & \cdots & + & 1. \end{array}$$

Adding up both rows of numbers would give $2S_n$. But, he noticed that he could also add them by first adding each term in the top row with the term right below it, giving the result

$$(n + 1) + (n + 1) + \cdots + (n + 1)$$

with a total of n parathesized terms, each being $n + 1$. So, this way of adding yields $n(n + 1)$, which must be equal to $2S_n$, proving that

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

5.2. The basic step is essential

In an induction proof, the basic step is typically the easiest step. But we must always verify it.

Here is an example. Consider the assertion

$$(\forall n \in \mathbf{N})(n = n + 1)$$

which is obviously false. Yet, we can carry out the inductive step, since for each $n \in \mathbf{N}$ the conditional

$$n = n + 1 \Rightarrow n + 1 = n + 2$$

is true. The falsity of the original assertion would only be detected in this case by verifying the basic step: $1 = 2$, which is false.

5.3. Some examples of induction proofs

We will prove by induction some elementary inequalities and equalities involving certain products and sums of real numbers. First some notations: for $a_1, \dots, a_n \in \mathbf{R}$, we write $\sum_{i=1}^n a_i$ to mean the sum $a_1 + \dots + a_n$, and $\prod_{i=1}^n a_i$ to mean the product $a_1 \cdots a_n$.

Proposition 5.1. *For $x_1, \dots, x_n \in \mathbf{R}$ and $0 \leq x_i \leq 1$, $i = 1, \dots, n$, we have*

$$\prod_{i=1}^n (1 - x_i) \geq 1 - \sum_{i=1}^n x_i.$$

Proof: Note that it is implicitly understood that the assertion here is that the statement in the proposition is true *for every* $n \in \mathbf{N}$. Thus, the assertion is of the form $(\forall n \in \mathbf{N})P(n)$, where $P(n)$ denotes the statement in the proposition. We will prove this by induction.

Let's begin with the basic step: $P(1)$, which is the statement that for $x_1 \in \mathbf{R}$ and $0 \leq x_1 \leq 1$,

$$1 - x_1 \geq 1 - x_1,$$

which is true. For the inductive step, we take $n \in \mathbf{N}$. Assume that $P(n)$ is true, which is to say that

$$\prod_{i=1}^n (1 - x_i) \geq 1 - \sum_{i=1}^n x_i.$$

To derive $P(n + 1)$, we start from its left side:

$$\prod_{i=1}^{n+1} (1 - x_i) = (1 - x_{n+1}) \prod_{i=1}^n (1 - x_i) \geq (1 - x_{n+1}) \left(1 - \sum_{i=1}^n x_i \right).$$

The last inequality follows from multiplying both sides of the inequality $P(n)$ by the number $1 - x_{n+1} \geq 0$. Expanding, we get

$$(1 - x_{n+1}) \left(1 - \sum_{i=1}^n x_i \right) = 1 - x_{n+1} - \sum_{i=1}^n x_i + x_{n+1} \sum_{i=1}^n x_i \geq 1 - \sum_{i=1}^{n+1} x_i.$$

The last inequality follows from the fact that $x_{n+1} \sum_{i=1}^n x_i \geq 0$ and the Translation Law. Finally, by the Transitive Law, we get

$$\prod_{i=1}^{n+1} (1 - x_i) \geq 1 - \sum_{i=1}^{n+1} x_i.$$

This proves $P(n+1)$, hence completing the induction proof. \square

Corollary 5.2. *If $1 \leq a \leq 1$ and $n \in \mathbf{N}$, then $(1 - a)^n \geq 1 - na$.*

Proof: Specializing the preceding proposition to the case $x_1 = \dots = x_n = a$ yields the corollary. \square

Every induction proof is about proving an infinite list of statements, indexed by $n \in \mathbf{N}$. It is acceptable to write an induction proof without explicitly introducing a notation like $P(n)$ to label those statements, provided that it is clear to the reader which statement in the text is indexed by $n \in \mathbf{N}$. However, for novice, it is a good practice to use explicit labels to guard against confusion (for both the writer and the reader.)

Exercise. Use induction to prove that for $n \in \mathbf{N}$, $\sum_{i=1}^n i^2 = n(n+1)(2n+1)/6$.

5.4. Shifting the index

Let's prove by induction the assertion:

$$(*) \text{ For } n \geq 3, \sum_{i=1}^n (i-1)(n-i) = \binom{n}{3}.$$

The right side of the equation is the binomial coefficient $\frac{n!}{(n-3)!3!} = \frac{1}{6}n(n-1)(n-2)$.

Note that (*) is a list of statements indexed by an integer $n \geq 3$, rather than the usual $n \in \mathbf{N}$. Thus, labeling the equation in (*) by $P(n)$, our appropriate basic step of

induction is to verify $P(3) : 0 \cdot 2 + 1 \cdot 1 + 2 \cdot 0 = \frac{1}{6} \cdot 3 \cdot 2 \cdot 1$, which is true. For the inductive step, we take $n \geq 3$. Assume that $P(n)$ is true, which is to say that

$$\sum_{i=1}^n (i-1)(n-i) = \frac{1}{6}n(n-1)(n-2).$$

To derive $P(n+1)$, we start from its left side:

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

By $P(n)$, the first sum on the right side is $\frac{1}{6}n(n-1)(n-2)$. The second sum is $1 + 2 + \dots + (n-1) = \frac{1}{2}(n-1)n$, by Gauss' formula. Thus, the two sums add up to

$$\frac{1}{6}n(n-1)(n-2) + \frac{1}{2}(n-1)n = \frac{1}{6}(n+1)n(n-1).$$

This yields $P(n+1)$, completing the induction proof of (*).

5.5. Variants of induction

Intuitively, it seems utterly obvious that every nonempty subset S of \mathbf{N} should also have a least member, if we “line up” all the numbers in S in increasing order. But it is in fact impossible to prove this without accepting the Principle of Induction.

Lemma 5.3. *1 is the least member of \mathbf{N} .*

Proof: We prove this by induction. We have $1 \geq 1$. Take $n \in \mathbf{N}$. Assume that $n \geq 1$. Then

$$n+1 \geq 1+1 \geq 1+0$$

proving that $n+1 \geq 1$. This proves that $(\forall n \in \mathbf{N})(n \geq 1)$. In other words, 1 is the least member of \mathbf{N} . \square

Proposition 5.4. *(Well-Ordering Property) If S is a nonempty subset of \mathbf{N} , then S has a least member.*

Proof: For $n \in \mathbf{N}$, let $P(n)$ be the statement that *if $S \subset \mathbf{N}$ and $S \cap \{1, \dots, n\} \neq \emptyset$, then S has a least member*. To prove the proposition, we will prove by induction that $P(n)$ is true

for every $n \in \mathbf{N}$. For the basic step, we prove $P(1)$. Suppose that $S \subset \mathbf{N}$ and $S \cap \{1\} \neq \emptyset$. Then $1 \in S$. Then 1 is the least member of S , by the lemma. So, S has a least member.

For the inductive step, we take $n \in \mathbf{N}$. Assume that $P(n)$ is true. We will prove

$P(n+1)$: *If $S \subset \mathbf{N}$ and $S \cap \{1, \dots, n+1\} \neq \emptyset$, then S has a least member.*

So, suppose that $S \subset \mathbf{N}$ and $S \cap \{1, \dots, n+1\} \neq \emptyset$. We consider two cases. If $n+1$ is the least member of S , then S has a least member. If $n+1$ is not the least member of S , then $S \cap \{1, \dots, n\} \neq \emptyset$. Now $P(n)$ implies that S has a least element. This completes the induction. \square

Method of descent. One strategy to prove the statement $(\forall n \in \mathbf{N})P(n)$, is by assuming that it is false and then using this assumption to derive a contradiction (i.e. a false statement.) Assuming $(\forall n \in \mathbf{N})P(n)$ is false implies $P(n)$ is false for some $n \in \mathbf{N}$. By the Well-Ordering Property, there is a *least* number a such that $P(a)$ is false. The goal of this strategy is to find a smaller number $b < a$ such that $P(b)$ is also false, resulting in a contradiction.

Example. To illustrate this strategy, here we give another proof that $\sqrt{2}$ is not fraction, without using the Prime Factorization Theorem. Suppose $\sqrt{2}$ is a fraction. We will show that this leads to a contradiction. Write $\sqrt{2} = m/n$ for some $m, n \in \mathbf{N}$. Since $1 < \sqrt{2} < 2$, we have $n < m < 2n$. Thus $0 < m - n < n$. Using $2n^2 = m^2$, we do the following calculations:

$$\frac{2n - m}{m - n} = \frac{n(2n - m)}{n(m - n)} = \frac{2n^2 - mn}{n(m - n)} = \frac{m^2 - mn}{n(m - n)} = \frac{m}{n}.$$

The left side has denominator $m - n < n$. This shows that we can represent $\sqrt{2}$ by a fraction with arbitrarily small positive integer denominator. This contradicts the Well-Ordering Property.