ITB8832 Mathematics for Computer Science
Lecture 2: 9 September 2024

Contents

Next section

The Law of Non-Contradiction

Law of Non-Contradiction

It is impossible that something and its negation
are both true at the same time.

In formula:

$$\overline{\text{not}(P \text{ and } \text{not}(P))}$$

This could be the most important principle of logic.

The Law of the Excluded Middle

Law of the Excluded Middle

Given anything and its negation, one of the two is true.

In formula:

$$\frac{}{P \text{ or } \text{not}(P)}$$

This is another fundamental principle of *classical* logic.

- However, there are other logics where the Law of the Excluded Middle is not valid.
- This happens, for example, in *intuitionistic logic*, where a proof of P is a *witness* that P is true.
- In this context, a witness of "P implies Q" is a "black box" that transforms any witness of P, however chosen, into some witness of Q: that is, a *function* from P to Q.
- Then $\text{not}(P)$ is *defined* as P implies $\bot$, where $\bot$ (read "bottom") is a proposition that has no witnesses.
- It is *always* possible to construct a witness of $\text{not}(\text{not}(P))$ from a witness of P.
- But in general, it is *not* possible to construct a witness of P starting from a witness of $\text{not}(\text{not}(P))$.

Proof by Contradiction

Suppose we have a proposition P, of which we don't know whether it is true or false.

1. Assume the contrary, that is, suppose P is *false*.
2. Taking not(P) as a hypothesis, construct a proof of not(Q), where Q is a proposition which we know to be *true*.
3. Since *it is impossible to prove a false statement by starting from true hypotheses and reasoning correctly*, P cannot be false:
   By the law of excluded middle, it must be true.

Example: The square root of 2 is irrational

Claim

$\sqrt{2}$ is irrational.

Example: The square root of 2 is irrational

Claim

$\sqrt{2}$ is irrational.

Step 1: Assume the contrary.

- Suppose integers m and n exist such that $\sqrt{2} = \frac{m}{n}$.

Example: The square root of 2 is irrational

Claim

$\sqrt{2}$ is irrational.

Step 2: Construct a proof of a false statement.

- We may suppose that m, n are positive and have no common positive factors except 1.
- By squaring and multiplying by n^2 we get $m^2 = 2n^2$.
- As m^2 is even, so must be m.
- Let $m = 2k$. Then $4k^2 = 2n^2$, hence $2k^2 = n^2$.
- As n^2 is even, so must be n.
- So *m and n are two integers, without common positive factors except 1, both even...*

Example: The square root of 2 is irrational

Claim

$\sqrt{2}$ is irrational.

Step 3: Conclude that the original proposition is true.

- We have proved that if the square root of 2 is rational, then there are two *relatively prime* integers which are both even.
- But two relatively prime integers cannot be both even.
- Therefore, the square root of 2 cannot be rational: it must be irrational.

Proof by Contradiction vs Proof by Negation

Suppose we have a proposition P, of which we don't know whether it is true or false.

1. Suppose P is *true*.
2. Taking P as a hypothesis, construct a proof of not(Q), where Q is a predicate which we know to be true.
3. Since it is impossible to prove a false statement by starting from true hypotheses and reasoning correctly, P cannot be true: it must be false.

Proof by Contradiction vs Proof by Negation

Suppose we have a proposition P, of which we don't know whether it is true or false.

1. Suppose P is *true*.
2. Taking P as a hypothesis, construct a proof of not(Q), where Q is a predicate which we know to be true.
3. Since it is impossible to prove a false statement by starting from true hypotheses and reasoning correctly, P cannot be true: it must be false.

Is this the same kind of argument as proof by contradiction?

Proof by Contradiction vs Proof by Negation

Suppose we have a proposition P, of which we don't know whether it is true or false.

1. Suppose P is *true*.
2. Taking P as a hypothesis, construct a proof of not(Q), where Q is a predicate which we know to be true.
3. Since it is impossible to prove a false statement by starting from true hypotheses and reasoning correctly, P cannot be true: it must be false.

Is this the same kind of argument as proof by contradiction?

Yes and no:

- An argument by *contradiction* has the form:

  If not(P), then contradiction; thus, P.

- This new argument, however, has the form:

  If P, then contradiction; thus, not(P).

  This is more appropriately called a *proof by negation*.

- We *could* apply proof by negation to not(P), but we would get:

  If not(P), then contradiction; thus, not(not(P)).

- To conclude with P, we still need "if not(not(P)), then P": which is (another form of) the law of the excluded middle!

Next section

The Well Ordering Principle

Every *nonempty* set
of *nonnegative* integers
has a *smallest* element.

Next section

Revisiting an old example

We saw a proof of the following:

Theorem

$\sqrt{2}$ is irrational.

At one point, the proof went:

- We may suppose $m, n \geq 1$ and $\gcd(m, n) = 1$.

Revisiting an old example

We saw a proof of the following:

Theorem

$\sqrt{2}$ is irrational.

At one point, the proof went:

- We may suppose $m, n \geq 1$ and $\gcd(m, n) = 1$.

Question: *why* could we suppose so?

Revisiting an old example

We saw a proof of the following:

Theorem

$\sqrt{2}$ is irrational.

At one point, the proof went:

- We may suppose $m, n \geq 1$ and $\gcd(m, n) = 1$.

Question: *why* could we suppose so?

Answer: because of the well ordering principle!

Every fraction can be written in lowest terms.

Suppose that there exist positive integers m, n such that the fraction $\frac{m}{n}$ *cannot* be written in *lowest terms*, that is, so that the numerator and denominator have no prime factors in common.
(A *prime number* is an integer $p > 1$ which is only divisible by 1 and itself.)

- Let C be the set of those positive integers that are *numerators* of fractions which cannot be written in lowest terms.

Every fraction can be written in lowest terms.

Suppose that there exist positive integers m, n such that the fraction $\frac{m}{n}$ *cannot* be written in *lowest terms*, that is, so that the numerator and denominator have no prime factors in common.
(A *prime number* is an integer $p > 1$ which is only divisible by 1 and itself.)

- Let C be the set of those positive integers that are *numerators* of fractions which cannot be written in lowest terms.
- Then C is nonempty, because it contains m.
- Let m_0 be the smallest element of C.
- Correspondingly, let n_0 be such that $\frac{m_0}{n_0}$ cannot be written in lowest terms.
- Then m_0 and n_0 must have a *common prime factor* p:
  Otherwise, $\frac{m_0}{n_0}$ would be a writing in lower terms.

Every fraction can be written in lowest terms.

Suppose that there exist positive integers m, n such that the fraction $\frac{m}{n}$ *cannot* be written in *lowest terms*, that is, so that the numerator and denominator have no prime factors in common.
(A *prime number* is an integer $p > 1$ which is only divisible by 1 and itself.)

- Let C be the set of those positive integers that are *numerators* of fractions which cannot be written in lowest terms.
- We have established the following:

$$\begin{gathered}\text{If } m_0 \text{ is the smallest element of } C,\\ \text{and } \frac{m_0}{n_0} \text{ cannot be written in lowest terms,}\\ \text{then } m_0 \text{ and } n_0 \text{ have a common prime factor } p.\end{gathered}$$

- But $\frac{m_0/p}{n_0/p} = \frac{m_0}{n_0}$, so $\frac{m_0}{p}$ must also belong to C.
- But this is impossible, because $\frac{m_0}{p} < m_0$, and m_0 is the smallest element of C.

Notation for sets

Let $P(x)$ be a predicate whose truth value depends on the value of variable x.

- If an object x is in a set S, we write: $x \in S$.
- We denote by:

  $$\{x \in S \mid P(x)\}$$

  the set of *all and only* those elements x of S for which $P(x)$ is true.
  - We read: "the set of the x in S such that $P(x)$".
  - We may omit S if irrelevant or clear from the context.
- Assume now that the sets S and T are clear from the context.
  If $E(x)$ is an expression dependent on a parameter x such that, for each value of $x \in S$, the expression $E(x)$ describes some object in the set T, we can use the shorthand:

  $$\{E(x) \mid P(x)\} ::= \{y \in T \mid \text{there exists } x \in S \text{ such that } P(x) \text{ and } y = E(x)\}$$

  We read: "the set of the $E(x)$ such that $P(x)$".
- The *empty set* which has no elements at all is denoted by $\emptyset$.
- The set of *natural numbers* (that is, *nonnegative* integers) is denoted by $\mathbb{N}$.

A template for well ordering proofs

Let $P(n)$ be a predicate which depends on a variable n taking values in $\mathbb{N}$.
We want to prove that $P(n)$ is true for *every* $n \in \mathbb{N}$.

1. Let C be the set of the *counterexamples*:

$$C = \{c \in \mathbb{N} \mid P(c) \text{ is false}\}$$

2. By contradiction, assume that C is nonempty.
3. By the Well Ordering Principle, C has a smallest element c_0:
   This c_0 is the *smallest counterexample*.
4. Derive a contradiction. Some ways to do so:
   - Show that $P(c_0)$ is true: that is, c_0 is *not a counterexample*.
   - Show that C has an element c_1 smaller than c_0:
     that is, c_0 is *not the smallest* counterexample.
   - Use c_0 to construct a proof of not(Q) where Q is a proposition which is known to be true.
5. Conclude that C is empty, hence $P(n)$ is true for every $n \in \mathbb{N}$.

Notation for sums

Let $a \in \mathbb{N}$ be fixed and, for an integer $n \geq a$ and all integers k such that $a \leq k \leq n$, let x_k be a number.

The *sum, for k from a to n, of the x_k* is the number $\sum_{k=a}^{n} x_k$ defined as follows:

- If $n = a$, then $\sum_{k=a}^{a} x_k = x_a$.
- If $n > a$, then $\sum_{k=a}^{n} x_k = \left(\sum_{k=a}^{n-1} x_k \right) + x_n$.

This is our first example of a *recursive definition*, where a *base case* is given, and every next object can be obtained from the previous one by applying a *constructor*.

Example: The sum of the first n positive integers

Theorem 2.2.1.

For every positive integer n, $\sum_{k=1}^{n} k = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$.

Proof:

- Let $C = \left\{ c \in \mathbb{N} \mid c > 0 \text{ and } 1+2+\cdots+c \neq \frac{c(c+1)}{2} \right\}$.
- If C is nonempty, then it has a smallest element c_0.
- We observe that c_0 cannot be 1, because $1 = \frac{1 \cdot 2}{2}$.
- Then $c_0 - 1$ is still a positive integer, and as it is smaller than c_0,

$$1+2+\cdots+(c_0-1) = \frac{(c_0-1)c_0}{2}.$$

- But then,

$$1+2+\cdots+c_0 = \frac{(c_0-1)c_0}{2} + c_0 = \frac{c_0^2 - c_0 + 2c_0}{2} = \frac{c_0(c_0+1)}{2} :$$

contradiction.

Next section

The Prime Factorization Theorem

Theorem 2.3.1.

Every integer $n \geq 2$ can be factored as a product of primes.

The Prime Factorization Theorem

Theorem 2.3.1.

Every integer $n \geq 2$ can be factored as a product of primes.

Proof: by the Well Ordering Principle.

- Let C be the set of counterexamples to Theorem 2.3.1, that is, the integers $n \geq 2$ which *cannot* be factored as a product of primes.
- By contradiction, assume that C is nonempty.
- By the Well Ordering Principle, C has a smallest element c_0.
- c_0 cannot be prime, because a *product of one prime* is still a product of primes.
- Then c_0 has a positive divisor a such that $1 < a < c_0$.
- But then, $b = c_0/a$ is also such that $1 < b < c_0$.

The Prime Factorization Theorem

Theorem 2.3.1.

Every integer $n \geq 2$ can be factored as a product of primes.

Proof: by the Well Ordering Principle.

- Let C be the set of counterexamples to Theorem 2.3.1, that is, the integers $n \geq 2$ which *cannot* be factored as a product of primes.
- By contradiction, assume that C is nonempty.
- Then the smallest element c_0 of C satisfies $c_0 = a \cdot b$ where $1 < a < c_0$ and $1 < b < c_0$.
- But as a and b are smaller than c_0, and c_0 is the smallest counterexample, a and b *can* be written as products of primes!
- So let $a = p_1 p_2 \cdots p_m$ and $b = q_1 q_2 \cdots q_n$ be writings of a and b as products of primes.
- Then $ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$ is a writing of c_0 as a product of primes!

The Prime Factorization Theorem

Theorem 2.3.1.

Every integer $n \geq 2$ can be factored as a product of primes.

Proof: by the Well Ordering Principle.

- We can summarize our findings as follows:

  If there are any counterexamples to Theorem 2.3.1,
  then the smallest such counterexample is not a counterexample.

- This is impossible, so there was no counterexample in the first place, and Theorem 2.3.1 is true.

Next section

Well ordered sets

Definition

A set S of numbers is *well ordered* if every nonempty subset of S has a minimum element.

Well ordered sets

Definition

A set S of numbers is *well ordered* if every nonempty subset of S has a minimum element.

The Well Ordering Principle can then be restated as follows:

The set of nonnegative integers is well ordered.

Are there other well ordered sets? Indeed:

Every *nonempty* subset of a well ordered set is well ordered.

A small, but useful, generalization

Denote by $\mathbb{Z}$ the set of the integer numbers.[1]

Theorem 2.4.1.

For every $n \in \mathbb{N}$, the set $\{k \in \mathbb{Z} \mid k \geq -n\}$ is well ordered.

[1] The letter is a zed because the German word for "number" is "Zahl".

A small, but useful, generalization

Denote by $\mathbb{Z}$ the set of the integer numbers.[1]

Theorem 2.4.1.

For every $n \in \mathbb{N}$, the set $\{k \in \mathbb{Z} \mid k \geq -n\}$ is well ordered.

We give an argument which does not depend on the *specific* value of n, hence holds for *every* n.

- Let S be a nonempty set of integers, none of which is smaller than $-n$.
- Then every integer of the form $k+n$ with $k \in S$ is nonnegative.
- Let $T = \{k+n \mid k \in S\} \subseteq \mathbb{N}$.
- By the Well Ordering Principle, T has a minimum m.
- Then $s_0 = m - n$ is the minimum of S.

[1] The letter is a zed because the German word for "number" is "Zahl".

Two quick corollaries

Definition 2.4.2.

A *lower bound* (resp., *upper bound*) for a set S of real numbers is a real number b such that $b \leq s$ (resp., $b \geq s$) for every $s \in S$.

Corollary 2.4.3.

Any nonempty set of integers (that is, subset of $\mathbb{Z}$) with a lower bound is well ordered.

Proof:

- If b is a lower bound for S, then so is its *floor:*

$$\lfloor b \rfloor = \max\{k \in \mathbb{Z} \mid k \leq b\}.$$

  For example, $\lfloor \pi \rfloor = 3$, and $\lfloor -\pi \rfloor = -4$.
- Then S is also a nonempty subset of $\{k \in \mathbb{Z} \mid k \geq \lfloor b \rfloor\}$, which is well ordered by Theorem 2.4.2.

Two quick corollaries

Definition 2.4.2.

A *lower bound* (resp., *upper bound*) for a set S of real numbers is a real number b such that $b \leq s$ (resp., $b \geq s$) for every $s \in S$.

Corollary 2.4.4.

Any nonempty set of integers with an upper bound has a greatest element.

Proof:

- If b is an *upper* bound for S, then $-b$ is a *lower* bound for $-S = \{-s \mid s \in S\}$.
- If m is the smallest element of $-S$, then $-m$ is the greatest element of S.

Another important principle

Lemma 2.4.5.

Every nonempty *finite* set of real numbers is well ordered.

As every subset of a finite set is finite, this is equivalent to:

Every nonempty finite set of real numbers has a smallest element.

Another important principle

Lemma 2.4.5.

Every nonempty *finite* set of real numbers is well ordered.

As every subset of a finite set is finite, this is equivalent to:

Every nonempty finite set of real numbers has a smallest element.

Proof:

- Let C be the set of those positive integers n such that there exists a finite set of exactly n real numbers which has no smallest element.
- By contradiction, assume C is nonempty.
- Let m be the smallest element of C.
- It must be $m \geq 2$, because the *unique* element of a set with exactly one element, is also its *smallest* element.

Another important principle

Lemma 2.4.5.

Every nonempty *finite* set of real numbers is well ordered.

As every subset of a finite set is finite, this is equivalent to:

Every nonempty finite set of real numbers has a smallest element.

Proof:

- Let C be the set of those positive integers n such that there exists a finite set of exactly n real numbers which has no smallest element.
- By contradiction, assume C is nonempty.
- Let m be the smallest element of C. We observed that $m \geq 2$.
- Consider a set F of m real numbers which has no smallest element.
- Choose an element r_0 of F, and let F' be the set made of all the elements of F except r_0.
- Then F' has $m-1 \geq 1$ elements, so it has a smallest element r_1.
- But then, every element of F is greater than or equal to *the smallest between* r_0 *and* r_1*:* contradiction.

Next subsection

The set of the fractions $n/(n+1)$

Let $\mathbb{F} = \left\{ \frac{n}{n+1} \,\middle|\, n \in \mathbb{N} \right\}$. This set is well ordered!

- We will prove this fact as an exercise.
- In the meantime: think *why* it is so.

The set of the fractions $n/(n+1)$

Let $\mathbb{F} = \left\{ \dfrac{n}{n+1} \,\middle|\, n \in \mathbb{N} \right\}$. This set is well ordered! But there's more!

Theorem

$\mathbb{N}+\mathbb{F} = \{n+f \mid n \in \mathbb{N}, f \in \mathbb{F}\}$ is well ordered.

Proof: By *two* applications of the Well Ordering Principle.

- Let S be a nonempty subset of $\mathbb{N}+\mathbb{F}$.
- Let T be the set of the nonnegative integers n such that:
  There exists $f \in \mathbb{F}$ such that $n+f \in S$.
- As S is nonempty, T must be nonempty too:
  Let n_0 be the least element *of* T.
- Let now U be the set of those $f \in \mathbb{F}$ such that $n_0 + f \in S$.
- Then U is also nonempty, and as $\mathbb{F}$ is well ordered, U has a least element f_0.

The set of the fractions $n/(n+1)$

Let $\mathbb{F} = \left\{ \frac{n}{n+1} \,\middle|\, n \in \mathbb{N} \right\}$. This set is well ordered! But there's more!

Theorem

$\mathbb{N} + \mathbb{F} = \{n + f \mid n \in \mathbb{N}, f \in \mathbb{F}\}$ is well ordered.

Proof: By *two* applications of the Well Ordering Principle.

- Let S be a nonempty subset of $\mathbb{N} + \mathbb{F}$.
- We have determined that there exist a least n_0 such that $n_0 + f \in S$ for some f, and a least f_0 such that $n_0 + f_0 \in S$.
- Then what could be the smallest element of S?
  Well: it can only be ...

The set of the fractions $n/(n+1)$

Let $\mathbb{F} = \left\{ \dfrac{n}{n+1} \,\middle|\, n \in \mathbb{N} \right\}$. This set is well ordered! But there's more!

Theorem

$\mathbb{N} + \mathbb{F} = \{n + f \mid n \in \mathbb{N}, f \in \mathbb{F}\}$ is well ordered.

Proof: By *two* applications of the Well Ordering Principle.

- Let S be a nonempty subset of $\mathbb{N} + \mathbb{F}$.
- We have determined that there exist a least n_0 such that $n_0 + f \in S$ for some f, and a least f_0 such that $n_0 + f_0 \in S$.
- Then what could be the smallest element of S?
  Well: it can only be ... $n_0 + f_0$
- Indeed, let n and f be such that $n + f \in S$.
- If $n > n_0$, then $n + f > n_0 + f_0$, because $f_0 < 1$.
- If $n = n_0$, then $n + f = n_0 + f \geq n_0 + f_0$ by our choice of f_0.
- The case $n < n_0$ is impossible by our choice of n_0.

Next section

An issue with human language

Consider these statements:

1. You can have the cake, or eat it.
2. If two and two are five, then I am the Pope.
3. If you can solve any exercise, then you will pass the test.
4. Everyone has a dream.

What do they *mean*? It might not be immediately clear.
Which is not surprising, because:

Human language is ambiguous.

This is fine: or we must renounce to poetry, humour, etc.
But it is inconvenient when we do mathematics . . .

An issue with human language

Consider these statements:

1. You can have the cake, or eat it.
2. If two and two are five, then I am the Pope.
3. If you can solve any exercise, then you will pass the test.
4. Everyone has a dream.

What do they *mean*? It might not be immediately clear.
Which is not surprising, because:

Human language is ambiguous.

This is fine: or we must renounce to poetry, humour, etc.
But it is inconvenient when we do mathematics . . .

Ambiguity: inclusion and exclusion

You can have the cake, or eat it.

- Can I have the cake and also eat it?
- Must I renounce to eat the cake if I want to have it?

Ambiguity: false hypotheses, true consequences

If two and two are five, then I am the Pope.

- What if I am not the Pope?
- What if I *am* the Pope?
- What if two and two are actually five, but I am not the Pope?

Ambiguity: “some” vs “all”

If you can solve any exercise, then you will pass the test.

- Can I pass the test if I can solve only one exercise?
- Do I need to be able to solve an exercise in particular?
- Do I need to be able to solve every single exercise?

Ambiguity: “for every” vs “exists”

Everyone has a dream.

- Does every single person have a dream of their own?
- Is there a single dream that everyone has?

A non-ambiguous language for mathematics

To avoid ambiguities, mathematicians divide propositions into *atomic formulas* joined together by *logical connectives*.

The role of atomic formulas is taken by *propositional variables* which can take any of the two values T (true) and F (false).

The relation between the truth values of the variables and that of a formula can be expressed by *truth tables*.

Next section

The connective not(·)

Truth value of not(·)

If P is a proposition, then not(P) is also a proposition.
not(P) is true iff P is false.

The connective not(·) is also called *negation*.

Truth table for not(·)

P	not(P)
T	F
F	T

The connective and

Truth value of P and Q

If P and Q are propositions, then P and Q is also a proposition.
P and Q is true iff both P and Q are true.

The connective and is also called *conjunction*.

Truth table for and

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

The connective or

Truth value of P or Q

If P and Q are propositions, then P or Q is also a proposition.
P or Q is true iff either P or Q is true, or both are.

The connective or is also called *disjunction*.

Truth table for or

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

The connective xor

Truth value of P xor Q

If P and Q are propositions, then P xor Q is also a proposition.
P xor Q is true iff either P or Q is true, but not both.

xor (ex-OR) is also called *exclusive or*, or *exclusive disjunction*.

Truth table for xor

P	Q	P xor Q
T	T	F
T	F	T
F	T	T
F	F	F

You can have the cake, or eat it

Let P be the proposition "I can have the cake", and Q be the proposition "I can eat the cake".

Can I have the cake and also eat it?

This corresponds to P or Q.

Do I lose the cake if I eat it?

This corresponds to P xor Q.

The connective implies

Truth value of P implies Q

If P and Q are propositions, then P implies Q is also a proposition.
P implies Q is true iff either P is false, or Q is true.

P implies Q can be read as follows:

- If P, then Q.
- P is a *sufficient* condition for Q.
- Q is a *necessary* condition for P.

Truth table for implies

P	Q	P implies Q
T	T	T
T	F	F
F	T	T
F	F	T

The connective implies

Truth value of P implies Q

If P and Q are propositions, then P implies Q is also a proposition. P implies Q is true iff either P is false, or Q is true.

This is called the *material implication:*

"P implies Q" means "it is never the case that P without Q".

Important: it is *not* necessary that P be a *cause* for Q!

Truth table for implies

P	Q	P implies Q
T	T	T
T	F	F
F	T	T
F	F	T

If two and two are five, then I am the Pope

Let P be the proposition "two and two are five", and Q be the proposition "I am the Pope".

What if I am not the Pope?

Anyway, P implies Q has a false antecedent, so it is true.

What if I **am** the Pope?

Then P implies Q has a true consequent, so it is true.

What if two and two are actually five, but I am not the Pope?

Then P implies Q would have a true antecedent, and a false consequent: so it would be false.

The connective iff

Truth value of P iff Q

If P and Q are propositions, then P iff Q is also a proposition.
P iff Q is true iff P and Q are either both true, or both false.

That is:

"P iff Q" means "P and Q have the same truth value".

Truth table for iff

P	Q	P iff Q
T	T	T
T	F	F
F	T	F
F	F	T