Lessons of Mathematical Logic

Antonino Salibra
26 September 2011, h.15:00

1. Notations

$\overline{x}, \overline{y}, \ldots$ denote sequences of indeterminate length.
$\overline{x_n}$ denotes the sequence $x_1, \ldots, x_n$; and similarly, for $\overline{x_k}, \overline{x_m}, \overline{y_n}, \overline{y_k}, \overline{y_m}$.
$z \in \overline{x}$ means that z is an element of the sequence $\overline{x}$.
$\overline{x} \cap \overline{y} = \emptyset$ means that the two sequences $\overline{x}$ and $\overline{y}$ do not have common elements.
$X \subseteq_{\mathrm{f}} Y$ means X is a finite subset of Y.
Sometimes "1" represents the truth value "true" and "0" represents the truth value "false".

2. The language of mathematics

In mathematics we prove *sentences* (= theorems or propositions or lemmas) expressing properties of mathematical objects. The sentences are usually expressed in the natural language. The mathematical objects can be of different type: integers, reals, matrices, sequences, continuous functions, groups, etc.. When we provide a proof of a sentence ϕ, we express a judgment of truth: the sentence ϕ is true because of its proof. In such a case, the sentence $\neg\phi$ is false. No other truth value is allowed in classic mathematics. In the real life the situation is different.

Mathematical logic is a branch of mathematics, where sentences and proofs are formalized in a formal language. In this way sentences, proofs, and theories become mathematical objects as integers or groups, so that we can prove sentences expressing properties of formal sentences, proofs and theories.

2.1. Predicate symbols, terms and atomic formulas

In the language of mathematics *atomic sentences* are constructed by relating mathematical objects. Mathematical objects are denoted by *terms* (or expressions), where variables may occur. For example, in algebra the terms may denote the elements of a group (or a ring, vector space, etc.), while in analysis they may denote reals or continuous functions. It is also possible to consider terms for sets of objects (for example, subgroups, vector subspaces, etc.).

- Terms or expressions without variables (denoting mathematical objects):
    - 3 denotes (= is a name for) the natural number three
    - $5 + 6$ denotes (= is a name for) the natural number eleven
    - 0.3147 denotes (= is a name for) the real number 3/10+1/100+4/1000+7/10000
    - $\{3, 6, 7\}$ denotes (= is a name for) the set whose elements are 3, 6, 7
    - "The author of Romeo and Juliet" is a term denoting (= a name for) Shakespeare
    - "The father of Antonino Salibra" is a term denoting (= a name for) Luigi Salibra

- Terms or expressions with variables (denoting mathematical objects after interpretation of the variables in the universe):
  - x denotes a generic element
  - $5+x$, where x ranges in the set of natural numbers, denotes a generic natural number greater than 5
  - $0.3xy7$ denotes a generic real number of the form 3/10+x/100+y/1000+7/10000
  - $\{x, y, z\}$ denotes a generic set of at most three elements
  - "The author of x" denotes a generic writer
- An atomic sentence (without occurrences of variables) denotes a truth value:
  - 3 divides 21
  - 121 is a multiple of 11
  - $3 = 5 + 6$
  - $11 + 6$ is a prime number
  - 5 is odd
  - $3 \in \{3, 6, 7\}$
  - $\{3\} \subseteq \{3, 6, 7\}$
  - John loves Mary
  - John is father of Mary
  - $P(5)$
  - $Q(dog, cat, dogcat)$

The words "divides", "is a multiple of", "=", "⊆", "loves" and "is a father of" are binary relations (or predicates). They relate pairs of elements of the universe of elements we are speaking or writing about. The words "is odd", "is a prime number" and "P" are unary predicates (or "properties" of the elements of the universe we are writing about). The binary predicate "∈" relates elements and sets. The ternary predicate "Q" relates triple of elements of the universe.

- An atomic formula (possibly with occurrences of variables) denotes a truth value after the interpretation of the variables:
  - x divides 122
  - $x + y = y + x$
  - $3 + 5 = 5 + 3$ (it is a particular instance of the atomic formula $x + y = y + x$, where $x = 3$ and $y = 5$)
  - x is a prime number
  - x is odd
  - $3 \in X$
  - $X \subseteq Y$
  - $\{3\} \subseteq \{3, 6, 7\}$ (it is a particular instance of the atomic formula $X \subseteq Y$, where $X = \{3\}$ and $Y = \{3, 6, 7\}$)
  - John loves X

- $P(x)$
- $Q(dog, x, y)$
- A

The symbol "A" represents a predicate of arity 0, in other words a propositional variable. "A" can be only either true or false.

2.2. Models

Before giving a judgment of truth for a sentence, we must fix a *model* $\mathcal{M}$, which is given by a set M of elements (called the universe of the model), plus suitable operations $f^{\mathcal{M}}, g^{\mathcal{M}}, \ldots$ and relations $P^{\mathcal{M}}, R^{\mathcal{M}}, \ldots$ among these elements.

A unary predicate P is interpreted in a model as a subset $P^{\mathcal{M}} \subseteq M$ of the universe M, a binary predicate R as a binary relation $R^{\mathcal{M}} \subseteq M \times M$, i.e. a set of pairs of elements of M, etc.

If $a \in P^{\mathcal{M}}$ then the sentence $P(a)$ is true in the model; If $a \notin P^{\mathcal{M}}$ then the sentence $P(a)$ is false in the model. If $(a, b) \in R^{\mathcal{M}}$ then the sentence $R(a, b)$ is true in the model; If $(a, b) \notin R^{\mathcal{M}}$ then the sentence $R(a, b)$ is false in the model.

Example 2.1. (The model $\mathbb{N}_{Ar}$ of arithmetics) *The universe of the model is the set* $\mathbb{N}$ *of natural numbers. The operations are the usual arithmetical operations of sum* $+^{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *and product* $*^{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. *We have a primitive predicate of equality* $=^{\mathbb{N}} =_{\text{def}} \{(x, x) : x \in \mathbb{N}\}$.

We can express the truth values of the following sentences:

(i) *"3 divides 21" is true in the model because* $21 = 3 \times 7$.

(ii) *"121 is a multiple of 11" is true because* $121 = 11 \times 11$

(iii) *"*$3 = 5 + 6$*" is false because* $5 + 6 = 11$ *and* $3 \neq 11$

(iv) *"*$3 \leq 5 + 6$*" is true because* $5 + 6 = 11$ *and* $11 = 3 + 8$

Notice that the predicates "divides", " is a multiple of " and 'less or equal"'are not primitive in the model. They can be defined in terms $+, *$ *and equality:*

$$x \textit{ divides } y \textit{ iff there exists } z \textit{ such that } y = z * x$$

Formally,

$$x \textit{ divides } y \textit{ iff } \exists z(y = z * x).$$

The symbol $\exists$ *means "there exists". For the other predicates we have:*

$$x \textit{ is a multiple of } y \textit{ iff there exists } z \textit{ such that } x = y * z \textit{ iff } \exists z(x = y * z)$$

$$x \leq y \textit{ iff there exists } z \textit{ such that } y = x + z \textit{ iff } \exists z(y = x + z).$$

The atomic formula "x *divides 122" is neither true neither false in the model. Before giving a judgment of truth we need to give a value to the variable* x. *The same for the formulas "*x *is a prime number" and "*x *is odd".*

Example 2.2. (The model $\mathcal{B}_{Ar}$ of truth values) *The universe of the model is the set* $\{\mathrm{tt}, \mathrm{ff}\}$ *of truth values. The symbols of operation are interpreted as follows:* $+^{\mathcal{B}}$ *= the propositional connective or;* $*^{\mathcal{B}}$ *= the propositional connective and;* $0^{\mathcal{B}} = \mathrm{ff}$*;* $1^{\mathcal{B}} = \mathrm{tt}$. *Then the sentence* $1 + 1 = 1$ *is true in* $\mathcal{B}_{Ar}$ *but not in* $\mathbb{N}_{Ar}$.

Example 2.3. (Model of sets) *The universe of the model $\mathcal{M}$ is the class SET of all sets and elements. We have the usual primitive predicate of equality and the binary relation of "to belong" $\in^{\mathcal{M}}= \{(x, y) :\ x \text{ is an element of set } y\}$.*

- $3 \in \{3, 6, 7\}$ *is trivially true*
- *"*$\{3\} \subseteq \{3, 6, 7\}$*" is true because the unique element of set* $\{3\}$ *is also element of* $\{3, 6, 7\}$. *However, the predicate* $\subseteq$ *is not primitive. It must be defined:*

  $$x \subseteq y \textit{ iff } \forall z(z \in x \to z \in y).$$

  The symbol $\forall$ *means "for every", while the symbol* $\to$ *represents the logical connective of implication. Then,* $z \in x \to z \in y$ *means "If* $z \in x$ *then* $z \in y$*".*
- $\{3\} \in x$ *can be formalized as follows:* $\exists z(z \in x \land \forall y(y \in z \to y = 3))$. *The symbol* $\land$ *represents the logical connective of conjunction.*
- *"There exists the empty set" can be written as follows:* $\exists x \forall z(\neg(z \in x))$, *that is, there is a set without elements. The symbol* $\neg$ *is the logical connective of negation.*
- *"There is an infinite set" can be expressed as follows:* $\exists x(\exists z(z \in x) \land \forall y(y \in x \to \{y\} \in x$. *Why is* x *infinite? if* $z \in x$ *then* $\{z\}, \{\{z\}\}, \{\{\{z\}\}\}, \dots$ *are infinite elements of* x.

2.3. Logical connectives, quantifiers and formulas

Starting from atomic formulas, more complex formulas can be written by using the propositional connectives

$$\land \text{ (AND)}; \quad \lor \text{ (OR)}; \quad \neg \text{ (NOT)}; \quad \to \text{ (IF THEN)}; \quad \leftrightarrow \text{ (IF AND ONLY IF)},$$

the universal quantifier

$$\forall \quad \text{(Every)}$$

and the existential quantifier

$$\exists \quad \text{(Some)}.$$

Another idiomatic expression for the universal quantifier is "for all" and for the existential quantifier is "there exists".

2.3.1. Notation

To save parenthesis, we define the following priorities among the logical symbols:

$$1 :\ \neg, \forall, \exists; \qquad 2 :\ \land, \lor; \qquad 3 : \to .$$

For example, we write

$$\forall x A(x) \land B \to C \lor \neg D \quad \text{for} \quad ((\forall x A(x)) \land B) \to (C \lor (\neg D)),$$

where A, B, C, D are arbitrary formulas. We also write

$$A \to B \to C \to D \quad \text{for} \quad A \to (B \to (C \to D)).$$

2.3.2. Semantics of the propositional connectives

It is well known the semantics of the propositional connectives in classical logic:

1. $A \wedge B$ is true if, and only if, A is true and B is true;
2. $A \vee B$ is false if, and only if, A is false and B is false;
3. $\neg A$ is true if, and only if, A is false;
4. $A \to B$ is false if, and only if, A is true and B is false.

To know the truth value of the propositional formula $A \wedge B \to C$, we need to know the truth values of the propositional variables A, B, C. For example, if A, C are true and B is false, then $A \wedge B \to C$ is true. The formula $A \wedge B$ is false because B is false, and any implication, whose premises is false, is true.

Then a model for a propositional language is just an interpretation of the propositional variables into the set of truth values. We compute the truth value of more complex propositional formulas by using the above semantics of the connectives.

A propositional formula is a *tautology* if it true for every interpretation of the propositional variables. For example, $A \to A$ is a tautology, because an implication is false only if the premise and the conclusion have different truth values (false and true, respectively).

2.3.3. Semantics of the quantifiers

The semantics of the quantifiers is more complex. We need a model with a universe $M = \{a_1, a_2, \dots, a_n, \dots\}$.

5. $\forall x P(x)$ is true in the universe M if, and only if, the following formula (of length infinite if M is infinite) is true:
$$P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n) \wedge \dots$$
6. $\exists x P(x)$ is true in the universe M if, and only if, the following formula (of length infinite if M is infinite) is true:
$$P(a_1) \vee P(a_2) \vee \dots \vee P(a_n) \vee \dots$$

If the universe M is infinite, the check that $\forall x P(x)$ is true cannot be done in a finite time, because we have to check that each formula in the infinite sequence $P(a_1), P(a_2), \dots, P(a_n), \dots$ is true. Similarly, the check that $\exists x P(x)$ is false cannot be done in a finite time, because we have to check that each formula in the infinite sequence $P(a_1), P(a_2), \dots, P(a_n), \dots$ is false. This is the reason why we need proofs. A proof of the formula $\forall x P(x)$ gives us the information that $\forall x P(x)$ is true in a finite time. We pay a price: to find the right proof in the infinite universe of all possible proofs.

Example 2.4. *Consider the sentence $\phi(x) \equiv A(x) \to \neg\exists y B(x,y)$ and a model $\mathcal{M}$ of universe $\{0,1,2,3\}$ such that $A(0)$, $A(2)$, $B(0,3)$ and $B(2,1)$ are true; in all other cases $A(x)$ and $B(x,y)$ are false. We now evaluate the sentence $\forall x \phi(x)$:*

1. *$\forall x \phi(x)$ is true in $\mathcal{M}$ iff the formulas $\phi(0), \phi(1), \phi(2), \phi(3)$ are all true in $\mathcal{M}$.*
2. *$\phi(0) \equiv A(0) \to \neg\exists y B(0,y)$ is false iff $A(0)$ is true and $\neg\exists y B(0,y)$ is false iff $A(0)$ is true and $\exists y B(0,y)$ is true. Since $B(0,3)$ is true, then $\exists y B(0,y)$ is also true. Thus we conclude that $\phi(0)$ is false.*
3. *Since $\phi(0)$ is false in the model $\mathcal{M}$, then $\forall x \phi(x)$ is also false in the model $\mathcal{M}$.*

We were able to prove that the sentence $\forall x \phi(x)$ is true in $\mathcal{M}$ by semantical methods (without a proof) because the universe of $\mathcal{M}$ is finite.

3. Examples of formalization

In algebra we may write formulas to express that a binary operation is commutative or that a vector sub-space has dimension 3; in analysis, formulas to express that a sequence is convergent or that a function is continuous; in set theory, formulas to express the inclusion of two sets. We now provide examples of sentences and formulas.

Remark 3.1. *Notice that, the phrases "Every professor is...", "Every multiple of* 3 *is...", in general, "Every P is..." are translated formally as follows:*

$$\forall x(P(x) \to ....)$$

Notice that, the phrases "Some professor is ...", "There is a multiple of 3 *such that...", in general, "Some P is..." are translated as follows:*

$$\exists x(Px \land \dots)$$

We have many examples below.

Example 3.1. Every multiple of 6 is a multiple of 3. *Formally:*

1. x *multiple-of* y *iff* $\exists k(x = y * k)$
2. y *divides* x *iff* $\exists k(x = y * k)$
3. $\forall x(x \text{ multiple-of } 6 \to x \text{ multiple-of } 3)$.

Example 3.2. The predecessor of a multiple of 4 is a prime number. *Formally:*

1. $Prime(z) \equiv \neg(z = 0) \land \neg(z = 1) \land \forall x(x \text{ divides } z \to x = 1 \lor x = z)$
2. $\forall x(x \text{ multiple-of } 4 \to \exists z(Prime(z) \land x - 1 = z))$.

Example 3.3. The binary operation + is commutative. *Formally:* $\forall x \forall y(x + y = y + x)$.

Example 3.4. *Consider a binary predicate A, a unary predicate P and a constant m, with the following intuitive meaning:*

$$A(x, y) \equiv x \text{ likes } y; \quad P(x) \equiv x \text{ is a professor}; \quad m \equiv \text{Mary}$$

1. Mary likes every professor: $\forall x(Px \to A(m, x))$.
2. Mary likes only the professors. *The above sentence is logicalle equivalent to: Mary likes all professors and does not like the other people. Formally,*

   $$\forall x(Px \to A(m, x)) \land \forall x(\neg Px \to \neg A(m, x)),$$

   which is logically equivalent to

   $$\forall x((Px \to A(m, x)) \land (\neg Px \to \neg A(m, x))).$$

   because it holds the following logical equivalence (Q ed R are arbitrary unary predicates):

   $$\forall x(Qx \land Rx) \leftrightarrow (\forall x Qx \land \forall x Rx)$$

3. Only one *professor likes Mary:* $\exists x(Px \wedge A(x,m) \wedge \forall z(Pz \wedge A(z,m) \to z = x))$.

   We have the following logical equivalences:

   - $\neg\forall x Rx \leftrightarrow \exists x\neg Rx$;
   - $\neg\exists x Rx \leftrightarrow \forall x\neg Rx$;
   - $(A \to B) \leftrightarrow (\neg A \vee B)$;
   - $(\neg A \vee \neg B) \leftrightarrow \neg(A \wedge B)$.

   Then,

$$\begin{array}{rcl} \forall z(Pz \wedge A(z,m) \to z = x) & \leftrightarrow & \forall z(\neg(Pz \wedge A(z,m)) \vee z = x) \\ & \leftrightarrow & \forall z(\neg(Pz \wedge A(z,m)) \vee \neg\neg(z = x)) \\ & \leftrightarrow & \forall z\neg(Pz \wedge A(z,m) \wedge \neg(z = x)) \\ & \leftrightarrow & \neg\exists z(Pz \wedge A(z,m) \wedge \neg(z = x)) \end{array}$$

   Then the formula formalizing "Only one professor likes Mary" can be written as follows:

$$\exists x(Px \wedge A(x,m) \wedge \neg\exists z(Pz \wedge A(z,m) \wedge \neg(z = x)).$$

4. Two *professors like Mary:* $\exists xy(Px \wedge Py \wedge x \neq y \wedge A(x,m) \wedge A(y,m))$, *where* $x \neq y$ *stands for* $\neg(x = y)$.

5. Only two *professors like Mary:* $\exists xy(Px \wedge Py \wedge x \neq y \wedge A(x,m) \wedge A(y,m) \wedge \neg\exists z(Pz \wedge z \neq x \wedge z \neq y \wedge A(z,m)))$.

Example 3.5. *Consider a binary predicate B and two unary predicates C and S with the following intuitive meaning:*

$$B(x,y) \equiv x \text{ likes } y; \quad Px \equiv x \text{ is a university course;} \quad Sx \equiv x \text{ is a student}$$

1. No student likes every course*:* $\neg\exists x(Sx \wedge \forall y(Cy \to B(x,y)))$
2. No course is loved by all students*:* $\neg\exists x(Cx \wedge \forall y(Sy \to B(y,x)))$

Example 3.6. *We formalize the sentence* "There exists infinite elements" *with the binary predicate of equality "=". The predicate of equality is always interpreted in a model of universe M as $\{(x,x) : x \in M\}$. This implies that every sentence including only the predicate of equality describes properties of the set M.*

We remark the following properties of the universal and existential sentences:

- *An existential sentence $\exists x Rx$ is* true *in a model if we can find an element a in the universe of the model such that Ra is true.*
- *A universal sentence $\forall x Rx$ is* false *in a model if we can find an element a in the universe of the model such that Ra is false.*
- There exists at least one element*:* $\exists x(x = x)$.
- There exist at least two elements*:* $\exists xy(x \neq y)$
- There exist at least three elements*:* $\exists xyz(x \neq y \wedge x \neq z \wedge y \neq z)$

- There exists at least n elements*:* $\exists x_1 \dots x_n(x_1 \neq x_2 \wedge \dots \wedge x_i \neq x_j \wedge \dots \wedge x_{n-1} \neq x_n)$ *(for $i \neq j$).*
- There exists at most one element*. It is equivalent to the negation of* There exist at least two elements*:*
  - *(a)* $\neg\exists xy(x \neq y)$
  - *(b)* $\forall xy(\neg x \neq y)$
  - *(c)* $\forall xy(x = y)$
- There exist at most two elements*:*
  - *(d)* $\neg\exists xyz(x \neq y \wedge x \neq z \wedge y \neq z)$
  - *(e)* $\forall xyz\neg(x \neq y \wedge x \neq z \wedge y \neq z)$
  - *(f)* $\forall xyz(\neg x \neq y \vee \neg x \neq z \vee \neg y \neq z)$
  - *(g)* $\forall xyz(x = y \vee x = z \vee y = z)$
- The universe is empty*:* $\phi_0 \equiv_{def} \neg\exists x(x = x)$
- The universe has exactly one element*:* $\phi_1 \equiv_{def} \exists x(x = x) \wedge \forall xy(x = y)$
- The universe has exactly two elements*:* $\phi_2 \equiv_{def} \exists xy(x \neq y) \wedge \forall xyz(x = y \vee x = z \vee y = z)$
- The universe has exactly three elements*:*
  $\phi_3 \equiv_{def} \exists xyz(x \neq y \wedge x \neq z \wedge y \neq z) \wedge \forall xyzu(x = y \vee x = z \vee x = u \vee y = z \vee y = u \vee z = u)$

The sentence "The universe has infinite elements" is equivalent to the satisfiability of the following infinite set of sentences:i $\neg\phi_0, \neg\phi_1, \neg\phi_2, \dots, \neg\phi_n, \dots$

Example 3.7. *If we want to express the sentence "The universe has infinite elements" with a unique sentence, we need a richer language. We introduce a binary predicate B and we formalize the sentence "B is an injective but not surjective function".*

- B is a function*:* $\forall xyz(B(x, y) \wedge B(x, z) \rightarrow y = z)$
- B is a total function*:* $\forall xyz(B(x, y) \wedge B(x, z) \rightarrow y = z) \wedge \forall x\exists yB(x, y)$
- B is a total injective function*:*
  B is a total function $\wedge \forall xyz(B(x, z) \wedge B(y, z) \rightarrow x = y)$
- B is an injective but not surjective function*:*
  B is a total injective function $\wedge \exists y\forall x\neg B(x, y)$

Example 3.8. Every nonempty upper bounded set of real numbers has least upper bound*. Formally:*

1. *X non-empty iff* $\exists x(x \in X)$*;*
2. *y upper-bound-of X iff* $\forall x(x \in X \rightarrow x \leq y)$*;*
3. *X upper-bounded iff* $\exists y$*(y upper-bound-of X) iff* $\exists y\forall x(x \in X \rightarrow x \leq y)$*;*
4. *X has-lub iff* $\exists z$*(z upper-bound-of X* $\wedge \forall y$*(y upper-bound-of X* $\rightarrow z \leq y$*)*

5. $\forall X(X \text{ non-empty} \land X \text{ upper-bounded} \to X \text{ has-lub})$.

Example 3.9. Every nonempty subset of natural numbers has minimum element. *Formally:*

1. X *has-minimum iff* $\exists x(x \in X \land \forall z(z \in X \to x \leq z))$
2. $\forall X(X \text{non-empty} \to X \text{has-minimum})$.

Example 3.10. Every Cauchy succession is convergent. *Formally:*

1. *Let* $\phi(x)$ *be an arbitrary formula.*
   $\exists! x\phi(x) \Leftrightarrow$ *there exists a unique* x *such that* $\phi(x) \Leftrightarrow \exists x\phi(x) \land \forall z(\phi(z) \to z = x)$.
2. $f : X \to Y$ *(read:* f *is a function from* X *into* Y*)* $\Leftrightarrow f \subseteq X \times Y \land \forall x(x \in X \to \exists! y(y \in Y \land (x, y) \in f)$
3. $Fun(f) \Leftrightarrow \exists X, Y(f : X \to Y)$
4. $f(x) = y \Leftrightarrow Fun(f) \land (x, y) \in f$
5. $Succ(a) \Leftrightarrow a : \mathbb{N} \to \mathbb{R}$, *where* $\mathbb{N}$ *is the set of natural numbers and* $\mathbb{R}$ *is the set of real numbers*
6. $n, m > k \Leftrightarrow n > k \land m > k$
7. $|a_n - a_m| < \epsilon \Leftrightarrow Succ(a) \land \exists z \exists u(z = a(n) \land u = a(m) \land |z - u| < \epsilon)$
8. *Cauchy(a)* $\Leftrightarrow Succ(a) \land \forall \epsilon \exists k(n, m > k \to |a_n - a_m| < \epsilon)$
9. $\forall a(Cauchy(a) \to \exists x \forall \epsilon \exists k(n > k \to |x - a_n| < \epsilon))$.

Example 3.11. Existential sentences*:*

- *There is a number* n *such that* $n^2 = 543$. *Formally:* $\exists n(n^2 = 543)$.
- *There are natural numbers* a, b, c *such that* $a^2 + b^2 = c^2$. *Formally:* $\exists a \exists b \exists c(a^2 + b^2 = c^2)$.

3.0.4. An important remark

What is the difference among the following sentences?

- Every natural number is the sum of two prime numbers: $\forall n \exists x \exists y(n = x + y \land \text{Prime}(x) \land \text{Prime}(y))$.
- Every set of natural numbers has minimum element: $\forall X(X\text{non-empty} \to X\text{has-minimum})$.
- The induction principle: $\forall P(P(0) \land \forall n(P(n) \to P(n + 1)) \to \forall n P(n))$.
- Every continuous function is derivable.

The variable n ranges over "atomic" elements (in this case, natural numbers) which do not have an "inner" structure. Each natural number has meaning thanks to the relations connecting it to the other natural numbers. These relations are created by the operations of addition and multiplication and the predicate of equality.

Subsets, continuous functions and properties have an inner structure. For example, we can apply the induction principle to an arbitrary predicate expressed in an arbitrary language. There is no linguistic restriction to the ways to describe predicates, continuous functions and subsets.

4. Proofs in mathematics

Proof theory, in contraposition to truth value interpretation of logic, gives a new interpretation to the formulas. To assert the formula A means "there is a proof of A", while to assert the formula $\neg A$ means "A is contradictory (= from A it follows a contradiction)".

Classical logic believes that the Boolean logic of truth values "not true = false" and "not false = true" is the same of the logic of proofs: "not provable = contradictory" and "not contradictory = provable". Every sentence A is either "true = provable" or "false = contradictory". This explains the law of excluded middle: for any sentence A, either there exists a proof of A, or a proof of $\neg A$.

Intuitionistic logic refutes the law of excluded middle: may be, there are sentence B such that neither B is provable nor B is contradictory.

Classical logic is completely symmetric. If we consider the following map * from propositional formulas into propositional formulas:

- $A^* = \neg A$ for every propositional variable A
- $(\neg A)^* = A$
- $(A \wedge B)^* = A^* \vee B^*$
- $(A \vee B)^* = A^* \wedge B^*$
- $\bot^* = \top$ ($\bot, \top$ denote respectively false and true)
- $\top^* = \bot$

we exchange truth with false, $\wedge$ with $\vee$, etc. For example, the tautology $A \vee \neg A$ becomes $(A \vee \neg A)^* = \neg A \wedge A$, which is a logical falsehood.

Proof theory is not symmetric because we prove only true sentences. We use logical rules of deducibility. These rules must be sound (meaning: from true formulas we only prove true formulas). We use the new symbol $\vdash$ with the following interpretation:

$$A_1, \dots, A_k \vdash B$$

iff from the assumption (that proofs of) $A_1, \dots, A_k$ (exist) we prove B (by applying the logical rules of deducibility). "$A_1, \dots, A_k \vdash B$" is called a *sequent*.

4.1. Logical connectives

We introduce the simple rules of deduction of propositional logic. We start with an example of proof.

Example 4.1. *This example is from [?]. Consider the following sentence:*

$$(A \to B) \to (A \to (B \to C)) \to A \to C.$$

It can be shown a tautology by the truth values interpretation of the propositional variables. However, in mathematics the above sentence would be proven as follows: Assume $A \to B$, $A \to (B \to C)$ and A. We would like to show C. From A and $A \to B$ we deduce B. From A and $A \to (B \to C)$ we obtain $B \to C$. Finally, from B and $B \to C$ we get C.

($\wedge_e$) (read: and elimination) From a proof of $A \wedge B$ we can construct a proof of A and a proof of B. Formally,

$$A \wedge B \vdash A; \qquad A \wedge B \vdash B.$$

($\wedge_i$) (read: and introduction) From a proof of A and a proof of B we construct a proof of $A \wedge B$. Formally,

$$A, B \vdash A \wedge B.$$

($\rightarrow_i$) (read: arrow introduction) $A \rightarrow B$ is provable if from the assumption A we construct a proof of B. Formally,

$$\text{If } A \vdash B \text{ then } \vdash A \rightarrow B$$

($\rightarrow_e$) (read: arrow elimination or Modus Ponens (MP))

$$A, A \rightarrow B \vdash B$$

($\vee_i$)

$$A \vdash A \vee B; \qquad B \vdash A \vee B$$

Remark 4.1. *(See [?]) The meaning of the rules $\vee_i$ is not evident, because nobody seems to have an interest to prove $A \vee B$, when we already have, for example, a proof of A. However, in some cases we need to prove $A \vee B$. For example, assume that we have shown the following sentence: $\forall x(A(x) \vee B(x) \rightarrow C(x))$ concerning natural numbers, and we would like to prove $\forall x C(x)$. Then it is sufficient to prove $A(n) \vee B(n)$ for every natural number n, that is, to prove $A(n)$ or $B(n)$ for every n; may be, we are able to prove $A(n)$ for every even n, and $B(k)$ for every odd k.*

Example 4.2. *(See [?, Example 2.1]) We prove $A \wedge B, B \wedge A \rightarrow C \vdash C \vee D$. We write the proof as a tree (written bottom-up) whose root is labeled by $C \vee D$ and whose leaves are labeled by the assumptions.*

$$\dfrac{\dfrac{\dfrac{\dfrac{A \wedge B}{B}[\wedge_e] \qquad \dfrac{A \wedge B}{A}[\wedge_e]}{B \wedge A}[\wedge_i] \qquad B \wedge A \rightarrow C}{C}[\rightarrow_e]}{C \vee D}[\vee_i]$$

We now analyze the other logical rules.

($\vee_e$) Consider the rule of and-introduction: $A, B \vdash A \wedge B$. If we reverse the rule by "applying" the * map introduced at the beginning of this section we get: $\neg A \vee \neg B \vdash$ either $\neg A$ or $\neg B$. If we put A for $\neg A$ and B for $\neg B$, we have:

$$A \vee B \vdash \text{ either } A \text{ or } B$$

with the obvious meaning: from the assumption that a proof of $A \vee B$ exists it follows that either a proof of A or a proof of B exists. However, this is not a deduction rule because we do not conclude with a proof of something! However, if we are able to prove a formula C by assuming either A or B then we get the right deduction rule for or-elimination:

$$(\vee_e) \text{ If } A \vdash C \text{ and } B \vdash C \text{ then } A \vee B \vdash C$$

($\bot_e$) (read: false elimination) We denote the "false" or the "absurd" with $\bot$.

$$\bot \vdash A$$

If have a proof of the absurd then we can prove anything.

($\neg_e$) (read: not elimination) The right proof-theoretical interpretation of the formula $\neg A$ is the following:

a proof of $\neg A$ iff from the assumption A we prove the absurd $\bot$

In other words,

$$\vdash \neg A \text{ iff } \vdash A \to \bot$$

Then the rule of ($\neg_e$):

$$A, \neg A \vdash \bot$$

($\neg_i$) (read: not introduction)

$$\text{If } A \vdash \bot \text{ then } \vdash \neg A$$

(RRA) (proof by contradiction) A *constructive* logic has two main properties:

- the ***disjunction property*** - $\Gamma \vdash A \vee B$ iff either $\Gamma \vdash A$ or $\Gamma \vdash B$
- the ***witness property*** - $\Gamma \vdash \exists x.A(x)$ iff $\Gamma \vdash A(t)$ for some witness t

Intuitionistic logic (IL) is constructive, but classical logic (CL) not (ex: $A \vee \neg A$ and $\exists x(Ax \to \forall y Ay)$). The rule RRA makes non constructive classical logic.

$$\text{If } \neg A \vdash \bot \text{ then } \vdash A.$$

This rule implies, for example, the tertium non datur $A \vee \neg A$ of classical logic.

Example 4.3. (Tertium non datur) *We get a proof of $A \vee \neg A$ by (RRA) if we prove $\bot$ from the assumption $\neg(A \vee \neg A)$.*

(1) *We prove $\neg(A \vee \neg A) \vdash \bot$. Assume $\neg(A \vee \neg A)$. This is the principal assumption that we can use in all steps* (1) *of the proof.*

  (1.1) *We prove $A \vdash \bot$. Assume A (this assumption can be used only in step (1.1) of the proof); then $A \vdash_{\vee_i} A \vee \neg A$. Since we can use the principal assumption $\neg(A \vee \neg A)$, then we have $A \vee \neg A, \neg(A \vee \neg A) \vdash_{\neg_e} \bot$. In conclusion, we have a proof of $\bot$ from A.*

  (1.2) $\vdash \neg A$ *by* (1.1) *and the rule* ($\neg_i$).

  (1.3) $\neg A \vdash_{\vee_i} A \vee \neg A$.

  (1.4) $A \vee \neg A, \neg(A \vee \neg A) \vdash_{\neg_e} \bot$ *(we use the proven formula $A \vee \neg A$ and again the principal assumption)*

  (1.5) *In conclusion, we have a proof $\bot$ from $\neg(A \vee \neg A) \vdash \bot$.*

(2) $\vdash A \vee \neg A$ *by* (1) *and the rule* (*RRA*).

4.2. Quantifiers

4.2.1. Proof of $\exists x P(x)$

An existential statement $\exists x P(x)$ can be proven in two different ways:

(i) The first one is a constructive method: we provides an element a satisfying $P(a)$.

(ii) The second method is not constructive: we assume that there exists a proof of $\neg\exists x P(x)$; then, we use a reasoning to get a contradiction (for example, $0 = 1$). Then there is no proof of $\neg\exists x P(x)$. In classical logic it holds the law of excluded middle: for any sentence A, either A is provable, or $\neg A$ is provable. Then in classical logic we can conclude that there exists a proof of $\exists x P(x)$, without providing an element which satisfies property P.

In intuitionist logic the fact that there is no proof of $\neg\exists x P(x)$ does not imply that there exists a proof of $\exists x P(x)$.

Example 4.4. 1. *The sentence* $\exists x Prime(x)$ *is true because* $Prime(2)$ *is true.*

2. *We would like to show by contradiction that there exist two irrational numbers* a *and* b *such that* a^b *is rational. Assume, by the way of contradiction, that the sentence is false. It is well known that* $\sqrt{2}$*, that is the length of the diagonal of the unitary square, was shown irrational by Pitagora. Then, by using our hypothesis* $\sqrt{2}^{\sqrt{2}}$ *and* $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ *are both irrational. But* $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^{2} = 2$*. Contradiction. Then the original sentence is true. By the proof we have the further information that at least one of the following pairs* $a = \sqrt{2}, b = \sqrt{2}$ *or* $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$ *is a pair of irrationals satisfying* a^b *rational.*

4.2.2. Proof of $\neg\forall x P(x)$

In order to show $\neg\forall x P(x)$ either we give a counter-example (i.e., an element a such that $P(a)$ is false) or we assume that there exists a proof of $\forall x P(x)$ and we get a contradiction. In this second case, we conclude that there is no proof of $\forall x P(x)$, which is a proof of $\neg\forall x P(x)$.

Example 4.5. *The statement* $\forall n(n^2 + 3n + 4$ *is a perfect square) is false because we have a counter-example:* $n = 1$.

4.2.3. Proof of $\forall x P(x)$

In order to show a universal statement $\forall x P(x)$ either we give a schema of proof (starting as follows: "Let x be....") by using the general properties of the variable x, or we assume that there is no proof of $\forall x P(x)$ and we get a contradiction. This second type of reasoning only holds in classical logic.

Example 4.6. *The statement* $\forall x(x^2 + 7x + 12$ *is even) is true. Let* x *be a natural number. Then we have two cases:* x *even and* x *odd. If* x *is even, then* $x^2 + 7x + 12$ *is sum of even numbers, so that it is even. If* x *is odd, then* x^2 *is odd and* $7x$ *is also odd, so that* $x^2 + 7x$ *is even. Finally,* $x^2 + 7x + 12 = (x^2 + 7x) + 12$ *is even because sum of two even numbers.*

4.2.4. Proof of $\neg\exists x P(x)$

In order to show $\neg\exists x P(x)$: give a schema of proof (starting as follows: "Let x be....") by using the general properties of the variable x.

Example 4.7. *The statement* $\exists x(x^2 + 7x + 12$ *is odd) is false. Let* x *be a natural number. Then we have two cases:....*

4.2.5. Proofs by contradiction

Example 4.8. *We prove by contradiction that there exist infinite prime numbers. Assume, by contradiction, that there exists only a finite number of prime numbers:* $p_0 < p_1 < \cdots < p_n$*. Let* $n = (p_0 * \cdots * p_n) + 1$*. When we divide* n *by* p_i *we have a remainder of* 1*, so* n *is not a multiple of any of these prime numbers* p_i*. Then it must exist a prime greater than* p_n*. Contradiction.*

4.2.6. Proofs by contrapositive

Example 4.9. *We prove the following statement: If* $x \geq 4$ *is a prime number, then* $x + 1$ *is not a perfect square. It is sufficient to prove that, if* $x + 1$ *is a perfect square, then* x *is not a prime. In fact, if* $x + 1 = k^2$ *then* $x = k^2 - 1 = (k + 1)(k - 1)$ *is factorable if* $k \neq 2$ *(i.e.,* $x \geq 4$*).*

5. The Curry-Howard correspondence for intuitionistic logic: proof of formula $A =$ program of type A

Curry and Howard have established the following correspondence:

$$p \text{ is a proof of the formula } A \iff p \text{ is a (functional) program of type } A$$

In other words, formulas and types are two different interpretations of the same thing. In this section we study this correspondence. We use the notation "$p : A$" for "p is a proof of A" (or for "p is a program of type A").

5.1. Minimal logic and the functional interpretation of intuitionistic formulas

Minimal logic is the fragment of intuitionistic logic restricted to the connective of implication. The Curry-Howard correspondence becomes:

$$p \text{ is a proof of } A \to B \iff p \text{ is a function from } A \text{ into } B$$

Example 5.1. *Consider again the formula* $\phi \equiv (A \to B) \to (A \to (B \to C)) \to A \to C$ *of Example 4.1. We look for a function* $S : (C \to B \to A) \to (C \to B) \to C \to A$*. How may we give an output of type* A *from inputs* $g : A \to (B \to C)$*,* $f : A \to B$ *and* $x : A$*?*

- *Assume* $f : A \to B$*.*
  First reading: assume f *to be a proof of* $A \to B$*. Ssecond reading: assume* f *to be a function from* A *into* B*.*
- *Assume* $g : (A \to (B \to C))$*.*
  Assume g *is a function from* A *into* $(B \to C)$*; this means that, when we apply* g *to an argument of type* A *we get as result a function from* B *into* C*; in other words,* g *is a so-called higher-order function.*
- *Assume* $x : A$*. Assume* x *has type* A
  How may we give an output of type A *from inputs* $g : A \to (B \to C)$*,* $f : A \to B$ *and* $x : A$*?*
- $fx : B$*.*
  The function f *applied to the argument* x *of type* A *provides a result* fx *of type* B*; we write the application of the function* f *to the argument* x *by juxtaposition of* f *and* x*. From the point of view of logic we have applied the rule* $\to_e$ *or Modus Ponens to the formulas* $A \to B$ *and* A*.*

- $gx : B \to C$.
  gx is a function from B into C. From the point of view of logic we have applied again the rule $\to_e$ to the formulas $A \to (B \to C)$ and A.

- $(gx)(fx) : C$.
  The function gx applied to an argument of type B provides a result $(gx)(fx)$ of type C. Again $\to_e$ to the formulas $B \to C$ and B.

The program $(gx)(fx)$ is a proof of C. To get a proof of ϕ we apply three times the rule $\to_i$:

- $\lambda x.(gx)(fx) : A \to C$
  The operator λx constructs a function of x from the expression $(gx)(fx)$. The process of forming a function from the "rule" that defines it is usually formalized in mathematics according to the following schema. Given a rule or expression

  $$E$$

  which depends on a variable x, we can construct the function whose values are given by the expression E by introducing a new symbol, for example h, and defining it as

  $$h(x) = E.$$

  The new symbol h is the name of the function. Instead, the lambda calculus uses the notation

  $$\lambda x.E$$

  for the same function, where λx is the variable-binding operator of functional abstraction (with respect to the variable x). We can calculate the value of $\lambda x.E$ applied to an argument by substitution. As an informal example, consider the arithmetical expression

  $$x^2 + 3$$

  and the corresponding function

  $$\lambda x.x^2 + 3.$$

  Then we can calculate the value of this function on an argument, for example 5, by substitution:

  $$(\lambda x.x^2 + 3)5 = (x^2 + 3)[x := 5],$$

  where $(x^2 + 3)[x := 5]$ denotes the value of the expression $x^2 + 3$ when the natural number 5 is substituted for x in $x^2 + 3$, i.e.,

  $$(\lambda x.x^2 + 3)5 = 5^2 + 3 = 28.$$

- $\lambda g.\lambda x.(gx)(fx) : (A \to (B \to C)) \to A \to C$

- $\lambda f.\lambda g.\lambda x.(gx)(fx) : (A \to B) \to (A \to (B \to C)) \to A \to C$.

In conclusion, the so-called λ-term $\lambda f.\lambda g.\lambda x.(gx)(fx)$ is a proof (program) of the formula ϕ.

Example 5.2. *The formula $A \to (B \to A)$ corresponds from the computational point of view to a function $K : A \to (B \to A)$. We can give an output of type A if we have two inputs, the first of type A and the second of type B:*

$$(Kx)y = x$$

so that K is the λ-term $K \equiv \lambda xy.x$.

Example 5.3. (The Peirce formula) *The Peirce formula* $((A \to B) \to A) \to A$ *is not provable in intuitionistic logic. There is no way to construct an output of type* A *from a function* $f : (A \to B) \to A$*, because we do not have an input* s *of type* $A \to B$*.*

5.2. Typed λ-calculus and minimal logic in natural deduction

We denote by Δ a set of judgement of type $x : B$. For example, the sequent $x_1 : B_1, \ldots, x_k : B_k \vdash M : A$ has two interpretations:

- From proofs x_i of B_i $(i = 1, \ldots, n)$, we get a proof M of A.
- From inputs x_i of type B_i, we can compute an output M of type A. Then M is an expression depending on the variables $x_1, \ldots, x_k$.

The following are the deduction rules of Minimal Logic.

$$\frac{}{\Delta, x : A \vdash x : A}\,[ax] \qquad \frac{\Delta \vdash M : A \to B \qquad \Delta \vdash N : A}{\Delta \vdash MN : B}\,[\to_e] \qquad \frac{\Delta, x : A \vdash M : B}{\Delta \vdash \lambda x.M : A \to B}\,[\to_i]$$

The rule (ax) means: if x is among the inputs then we can give x as output.

The rule $(\to_e)$ means: if M is a function from A into B and N is of type A, then the function M applied to the input N gives as result a value MN of type B.

The rule $(\to_i)$ means: if M is an expression of type B depending on variable x, then $\lambda x.M$ is the function that when applied to a value x of type A gives a value M of type B.

Example 5.4. *We show that the* λ*-term* $\lambda xy.x$ *is a proof of the formula* $A \to (B \to A)$*.*

$$\dfrac{\dfrac{\dfrac{}{x : A, y : B \vdash x : A}}{x : A \vdash \lambda y.x : B \to A}\,[\to_i]}{\vdash \lambda xy.x : A \to (B \to A)}\,[\to_i]$$

Example 5.5. *We show that* λ*-term* $\lambda xyz.(xz)(yz)$ *is a proof of the formula*

$$(C \to (B \to A)) \to (C \to B) \to C \to A.$$

Let $\Delta = x : C \to (B \to A), y : C \to B, z : C$ *and* $\phi = C \to (B \to A)$*.*

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta \vdash y : C \to B \qquad \Delta \vdash z : C}\,[ax]}{\Delta \vdash yz : B}\,[\to_e] \qquad \dfrac{\dfrac{}{\Delta \vdash x : C \to (B \to A) \qquad \Delta \vdash z : C}\,[ax]}{\Delta \vdash xz : B \to A}\,[\to_e]}{\Delta \vdash (xz)(yz) : A}\,[\to_e]}{\vdash \lambda xyz.(xz)(yz) : (C \to (B \to A)) \to (C \to B) \to C \to A}\,[\to_i \ \textit{three times}]$$

5.3. Typed λ-calculus as a programming language and proof simplification

An implicative formula A is provable iff there is a closed λ-term M such that $\vdash M : A$. However, there may be different proofs of the same formula. Some of these proofs are more simple than others. Consider the following two proofs of formula B:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta, x : A \vdash x : A}\,[ax] \qquad \dfrac{}{\Delta, x : A \vdash x : A}\,[ax] \qquad \dfrac{}{\Delta, x : A \vdash z : C}\,[ax]}{\dfrac{\cdots\cdots\cdots}{\Delta, x : A \vdash M : B}}}{\Delta \vdash \lambda x.M : A \to B}\,[\to_i] \qquad \dfrac{\cdots\cdots}{\Delta \vdash N : A}}{\Delta \vdash (\lambda x.M)N : B}\,[\to_e]$$

The second proof:

$$\dfrac{\dfrac{\cdots\cdots}{\Delta \vdash N : A} \qquad \dfrac{\cdots\cdots}{\Delta \vdash N : A} \qquad \dfrac{}{\Delta \vdash z : C}\,[ax]}{\dfrac{\cdots\cdots\cdots}{\Delta \vdash M[x := N] : B}}$$

Both the programs $(\lambda x.M)N$ and $M[x := N]$ correspond to a proof of the formula B by the assumptions Δ. However, the proof $(\lambda x.M)N$ does unuseful work because of an arrow introduction followed by an arrow elimination. Then the program $M[x := N]$ simplifies the proof $(\lambda x.M)N$ of B as follows: we take the proof M of B from the assumptions in $\Delta, x : A$ and we substitute every occurrence of the assumption $x : A$ by the proof $N : A$.

Example 5.6. (η-reduction) *Assume that $y_i : C_i$ is different from $x : A$, that is, we do not use the hypothesis $x : A$ in the proof of $M : B$.*

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta, x : A \vdash y_1 : C_1}\,[ax] \qquad \dfrac{}{\Delta, x : A \vdash y_2 : C_2}\,[ax] \qquad \ldots\; \dfrac{}{\Delta, x : A \vdash y_n : C_n}\,[ax]}{\dfrac{\cdots\cdots\cdots}{\Delta, x : A \vdash M : B}}}{\Delta \vdash \lambda x.M : A \to B}\,[\to_i] \qquad \dfrac{\cdots\cdots}{\Delta, x : A \vdash x : A}}{\Delta, x : A \vdash (\lambda x.M)x : B}\,[\to_e]$$

In the second proof we do not have anymore the hypothesis $x : A$ that we do not have used.

$$\dfrac{\dfrac{}{\Delta \vdash y_1 : C_1} \qquad \dfrac{}{\Delta \vdash y_2 : C_2} \qquad \ldots\; \dfrac{}{\Delta \vdash y_n : C_n}\,[ax]}{\dfrac{\cdots\cdots\cdots}{\Delta \vdash M : B}}$$

Example 5.7. *The proof*

$$\dfrac{\dfrac{\dfrac{}{y : B, x : A \to A \vdash y : B}\,[ax]}{y : B \vdash \lambda x.y : (A \to A) \to B}\,[\to_i] \qquad \dfrac{\dfrac{}{y : B, z : A \vdash z : A}\,[ax]}{y : B \vdash \lambda z.z : A \to A}\,[\to_i]}{y : B \vdash (\lambda x.y)(\lambda z.z) : B}\,[\to_e]$$

becomes the trivial proof $y : B \vdash y : B$.

The typed λ-calculus is a functional programming language. The following reduction rules (the way of computing in this language)
β-reduction:

$$(\lambda x.M)N \to M[x := N]$$

η-reduction:

$$(\lambda x.M)x \to M, \text{ where } x \text{ does not occur free in } M$$

correspond to proof simplifications.

Theorem 5.1. *The reduction rules of typed λ-calculus are strongly normalizable and Church-Rosser.*

Every program M of type A has a unique normal form $\mathrm{nf}(M)$ of type A. It corresponds to the simplest proof of A.