Discrete Mathematics\textsuperscript{1}
http://iscasmc.ios.ac.cn/DM2016

Lijun Zhang

March 17, 2016

\textsuperscript{1}Materials about the axiomatization are provided by Dr. Wanwei Liu.
Contents

1. The Foundations: Logic and Proofs
2. Basic Structures: Sets, Functions, Sequences, Sums, and Matrices
3. Algorithms
4. Number Theory and Cryptography
5. Induction and Recursion
6. Counting
7. Discrete Probability
8. Advanced Counting Techniques
9. Relations
10. Graphs
11. Trees
12. Boolean Algebra
13. Modeling Computation
Chapter 3
First Order Logic (FOL)

3.1 Syntax of FOL

Propositional logic is a coarse language, which only concerns about propositions and boolean connectives. Practically, this logic is not powerful enough to describe important properties we are interested in.

Example 3.1.1 (Syllogism of Aristotle). Consider the following assertions:

1. All men are mortal.
2. Socrates is a man.
3. So Socrates would die.

\[ \forall x (\text{Man}(x) \rightarrow \text{Mortal}(x)) \]

Definition 3.1.2. First order logic is an extension of proposition logic:

1. To accept parameters, it generalized propositions to predicates.
2. To designate elements in the domain, it is equipped with functions and constants.

3. It also involves quantifiers to capture infinite conjunction and disjunction.

\[ \forall \exists \neg \rightarrow \]

**Definition 3.1.3.** We are given:

- an arbitrary set of variable symbols \( VS = \{ x, y, x_1, \ldots \} \);
- an arbitrary set (maybe empty) of function symbols \( FS = \{ f, g, f_1, \ldots \} \), where each symbol has an arity; 
- an arbitrary set (maybe empty) of predicate symbols \( PS = \{ P, Q, P_1, \ldots \} \), where each symbol has an arity; 
- an equality symbol set \( ES \) which is either empty or one element set containing \( \{ \approx \} \).

Let \( L = VS \cup \{ (,)\to,\neg,\forall \} \cup FS \cup PS \cup ES \). Here \( VS \cup \{ (,)\to,\neg,\forall \} \) are referred to as logical symbols, and \( FS \cup PS \cup ES \) are referred to as non-logical symbols.

We often make use of the 

- set of constant symbols, denoted by \( CS = \{ a, b, a_1, \ldots \} \subseteq FS \), which consist of function symbols with arity 0;
• set of propositional symbols, denoted by \( PS = \{ p, q, p_1, \ldots \} \subseteq FS \), which consist of predicate symbols with arity 0.

**Definition 3.1.4** (FOL terms). The terms of the first order logic are constructed according to the following grammar:

\[
t ::= x \mid ft_1 \ldots t_n
\]

where \( x \in VS \), and \( f \in FS \) has arity \( n \).

Accordingly, the set \( T \) of terms is the smallest set satisfying the following conditions:

- each variable \( x \in VS \) is a term.
- Compound terms: \( ft_1 \ldots t_n \) is a term (thus in \( T \)), provided that \( f \) is a \( n \)-arity function symbol, and \( t_1, \ldots, t_n \in T \). Particularly, \( a \in CS \) is a term.

We often write \( f(t_1, \ldots, t_n) \) for the compound terms.
Definition 3.1.5 (FOL formulas). The well-formed formulas of the first order logic are constructed according to the following grammar:

$$\varphi ::= Pt_1 \ldots t_n | \neg \varphi | \varphi \rightarrow \varphi | \forall x \varphi$$

where $t_1, \ldots, t_n$ are terms, $P \in PS$ has arity $n$, and $x \in VS$.

We often write $P(t_1, \ldots, t_n)$ for clarity. Accordingly, the set $\text{FOF}$ of first order formulas is the smallest set satisfying:

- $P(t_1, \ldots, t_n) \in \text{FOF}$ is a formula, referred to as the atomic formula.

- Compound formulas: $(\neg \varphi)$ (negation), $(\varphi \rightarrow \psi)$ (implication), and $(\forall x \varphi)$ (universal quantification) are formulas (thus in $\text{FOF}$), provided that $\varphi, \psi \in \text{FOF}$.

We omit parentheses if it is clear from the context.

As syntactic sugar, we can define $\exists x \varphi$ as $\exists x \varphi ::= \neg \forall x \neg \varphi$.

We assume that $\forall$ and $\exists$ have higher precedence than all logical operators.
**Definition 3.1.6** (Sub-formulas). For a formula \( \varphi \), we define the sub-formula function \( S_f : \text{FOF} \to 2^{\text{FOF}} \) as follows:

\[
S_f(P(t_1, \ldots, t_n)) = \{ P(t_1, \ldots, t_n) \}
\]
\[
S_f(\neg \varphi) = \neg \forall x \in S_f(\varphi)
\]
\[
S_f(\varphi \rightarrow \psi) = \forall x \in S_f(\varphi) \cup S_f(\psi)
\]
\[
S_f(\forall x \varphi) = \forall x \in S_f(\varphi)
\]
\[
S_f(\exists x \varphi) =
\]

**Definition 3.1.7** (Scope). The part of a logical expression to which a quantifier is applied is called the scope of this quantifier. Formally, each sub-formula of the form \( Qx \psi \in S_f(\varphi) \), the scope of the corresponding quantifier \( Qx \) is \( \psi \). Here \( Q \in \{ \forall, \exists \} \).
Definition 3.1.8 (Sentence). We say an occurrence of $x$ in $\varphi$ is free if it is not in scope of any quantifiers $\forall x$ (or $\exists x$). Otherwise, we say that this occurrence is a bound occurrence. If a variable $\varphi$ has no free variables, it is called a closed formula, or a sentence.

$$\text{OCC}\left( x \right) = \{ x \}$$
$$\text{OCC}\left( \neg \phi_t \ldots \phi_n \right) = \cup \text{OCC}\left( \phi_i \right)$$
$$\text{OCC}\left( \phi_t \ldots \phi_n \right) = \cup \text{OCC}\left( \phi_i \right)$$
$$\text{OCC}\left( \forall \phi \right) = \text{OCC}\left( \phi \right)$$
$$\varphi \rightarrow \phi \quad = \quad \forall x \exists \phi \cup \text{OCC}\left( \phi \right)$$

Substitution for Terms

Definition 3.1.9 (Substitution). The substitution of $x$ with $t$ within $\varphi$, denoted as $S^x_t \varphi$, is obtained from $\varphi$ by replacing each free occurrence of $x$ with $t$.
We would extend this notation to $S_{t_1,\ldots,t_n}^{x_1,\ldots,x_n} \phi$.

**Remark 3.1.10.** It is important to remark that $S_{t_1,\ldots,t_n}^{x_1,\ldots,x_n} \phi$ is not the same as $S_{t_1}^{x_1} \ldots S_{t_n}^{x_n} \phi$: the former performs a simultaneous substitution.

For example, consider the formula $P(x,y)$: the substitution $S_{x/y}^{x,y} P(x,y)$ gives $S_{x/y}^{x,y} P(x,y) = P(y,x)$ while the substitutions $S_{y/x}^{x,y} S_{x}^{y} P(x,y)$ give $S_{y/x}^{x,y} S_{x}^{y} P(x,y) = S_{y}^{x} P(x,x) = P(y,y)$.

$$\left( S_{t_1}^{x_1} \circ S_{t_2}^{x_2} \circ \ldots \circ S_{t_n}^{x_n} \right)(\phi)$$

$$S_{x}^{x} \phi = \exists y (t < y) \quad S_{y}^{x} \phi = \exists y (y < y)$$

**Remark 3.1.11.** Consider $\phi = \exists y (x < y)$ in the number theory. What is $S_{t}^{x} \phi$ for the special case of $t = y$?

**Definition 3.1.12** (Substitutable on Terms). We say that $t$ is substitutable for $x$ within $\phi$ iff for each variable $y$ occurring in $t$, there is no free occurrence of $x$ in scope of $\forall y / \exists y$ in $\phi$. 

![Diagram](image)
Definition 3.1.13 (α-β condition). If the formula \( \varphi \) and the variables \( x \) and \( y \) fulfill:

1. \( y \) has no free occurrence in \( \varphi \), and
2. \( y \) is substitutable for \( x \) within \( \varphi \),

then we say that \( \varphi, x \) and \( y \) meet the \( \alpha-\beta \) condition, denoted as \( C(\varphi, x, y) \).

Lemma 3.1.14. If \( C(\varphi, x, y) \), then \( S_x^y S_y^x \varphi = \varphi \).
3.2 The Axiom System: the Hilbert’s System

As for propositional logic, also FOL can be axiomatized.

**Definition 3.2.1 (Axioms).**

1. \( \varphi \to (\psi \to \varphi) \)

2. \( (\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta)) \)

3. \( (\neg \varphi \to \neg \psi) \to (\psi \to \varphi) \)

4. \( \forall x \varphi \to S^x_t \varphi \)  
   if \( t \) is substitutable for \( x \) within \( \varphi \)

5. \( \forall x (\varphi \to \psi) \to (\forall x \varphi \to \forall x \psi) \)  
   全称-分配

6. \( \varphi \to \forall x \varphi \)  
   \( x \) 不自由

   if \( x \) is not free in \( \varphi \)

7. \( \forall x_1 \ldots \forall x_n \varphi \)  
   全称-合取

   if \( \varphi \) is an instance of (one of) the above axioms

**MP Rule:** \( \frac{\varphi \to \psi \ \varphi}{\psi} \)
Definition 3.2.2 (Syntactical Equivalence). We say $\varphi$ and $\psi$ are syntactical equivalent iff $\varphi \vdash \psi$ and $\psi \vdash \varphi$.

Theorem 3.2.3. (Gen): If $x$ has no free occurrence in $\Gamma$, then $\Gamma \vdash \varphi$ implies $\Gamma \vdash \forall x \varphi$.

Solution. Suppose that $\varphi_0, \varphi_1, \ldots, \varphi_n = \varphi$ is the deductive sequence of $\varphi$ from $\Gamma$.

- If $\varphi_i$ is an instance of some axiom, then according to (AS7), $\forall x \varphi_i$ is also an axiom.

- If $\varphi_i \in \Gamma$, since $x$ is not free in $\Gamma$, we have $\vdash \varphi_i \rightarrow \forall x \varphi_i$ according to (AS6). Therefore, we have $\Gamma \vdash \forall x \varphi_i$ in this case.

- If $\varphi_i$ is obtained by applying (MP) to some $\varphi_j$ and $\varphi_k = \varphi_j \rightarrow \varphi_i$. By induction, we have $\Gamma \vdash \forall x \varphi_j$ and $\Gamma \vdash \forall x (\varphi_j \rightarrow \varphi_i)$. With (AS5) and (MP), we also have $\Gamma \vdash \forall x \varphi_i$ in this case.

Thus, we have $\Gamma \vdash \forall x \varphi_n$, i.e., $\Gamma \vdash \forall x \varphi$. 

11
Exercise 3.2.4. Prove that

1. $\forall x \forall y \varphi \vdash \forall y \forall x \varphi$,
2. $\exists x \forall y \varphi \vdash \forall y \exists x \varphi$.

Exercise 3.2.5. Prove that

1. $\forall x (\varphi \rightarrow \psi) \vdash \forall x (\neg \psi \rightarrow \neg \varphi)$,
2. $\forall x (\varphi \rightarrow \psi) \vdash \exists x \varphi \rightarrow \exists x \psi$. 
Exercise 3.2.6. Prove that

1. If $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg \psi$, then $\Gamma \vdash \neg (\varphi \rightarrow \psi)$,

2. $\forall x \neg (\varphi \rightarrow \psi) \vdash \neg (\varphi \rightarrow \exists x \psi)$.

Lemma 3.2.7. (Ren): If $C(\varphi, x, y)$, then $\forall x \varphi$ and $\forall y S^x_y \varphi$ are syntactical equivalent. That is,

1. $\forall x \varphi \vdash \forall y S^x_y \varphi$.

2. $\forall y S^x_y \varphi \vdash \forall x \varphi$. 

13
Lemma 3.2.8. (RS): Let $\eta_\psi$ denote the formula obtained by replacing (some or all) $\varphi$ inside $\eta$ by $\psi$.

If $\varphi \vdash \psi$ and $\psi \vdash \varphi$ then $\eta \vdash \eta_\psi$ and $\eta_\psi \vdash \eta$.

Solution. By induction on the structure of $\eta$.

Lemma 3.2.9. If $C(\varphi, x, y)$ and $\Gamma \vdash \psi$, then $\Gamma \vdash \psi^{\forall x \varphi}_{\forall y S_y \varphi}$.

Solution. An immediate result of (Ren) and (RS).
Theorem 3.2.10. (GenC) If $\Gamma \vdash S^a_\xi \varphi$ where $a$ does not occur in $\Gamma \cup \{\varphi\}$, then $\Gamma \vdash \forall x \varphi$. 