Notes on First Order Logic

September 29, 2007

1 First-Order Logic

1.1 The Syntax of a First-Order Language $\mathbb{L}$

We start with the symbols of a first-order language. There are two types of symbols: *logical symbols*, and *parameters.*

Logical Symbols:

1. The two symbols (and). The *parentheses* are used for punctuation.
2. $\longrightarrow$ and $\neg$. These are the sentential connective symbols.
3. $v_1, v_2, \ldots, v_n, \ldots$ This is an enumerable list of symbols called *variables.*
4. $\doteq$. This is the *identity* or *equality* symbol. It may, or may not be present in a particular first-order language.

Parameters

1. $\dot{\forall}$. This is the *universal quantifier* symbol.
2. For each $n > 0$ there is a set (possibly empty) of objects called n -ary (or n-place) *relation* (or *predicate* symbols.
3. For each $n > 0$ there is a set (possibly empty) of objects called n -ary (or n-place) *function* symbols.
4. A set (possibly empty) of objects called *constant* symbols.

By a *symbol* we mean, temporarily, either a logical symbol or a parameter

Further requirements.

$\doteq$ is a 2-ary relation symbol.

We require that there must be at least one relation symbol.

The symbols are distinct, and no symbol is equal to a finite sequence of other symbols. For example, no 2-ary function symbol is also a 3-ary function symbol, no function symbol is a relation symbol, etc.

Remark 1.1. We have not put any requirements on the number of function symbols, relation symbols, or constant symbols. For example, it is possible that for a given first-order language there are three constant symbols, enumerably many function symbols, and uncountably many relation symbols!

Definition 1.2. An *expression* is a finite sequence of symbols. A *term sequence* is a finite sequence $t_1, \ldots, t_n$ of expressions such that each t_i is either

1. a variable, or a constant symbol, or
2. is of the form $fs_1 \cdots s_n$, where f is an n-ary function symbol and each of $s_1, \ldots, s_n$ occurs earlier in the sequence.

Definition 1.3. An expression t is a *term* if there is a term sequence $t_1, \ldots, t_k$ such that $t = t_k$.

Example 1.4. Suppose:

f is a 2-ary function symbol;

g is a 3-ary function symbol;

c_1 and c_2 are constant symbols.

Then $gfc_1c_2v_3c_1$ is a term since

$$v_3,\ c_1,\ c_2,\ fc_1c_2,\ gfc_1c_2v_3c_1$$

is a term sequence.

Definition 1.5. An expression is an *atomic formula* if it is of the form $Pt_1 \cdots t_k$, where $t_1, \ldots, t_k$ are terms, and P is a k-ary relation symbol.

Example 1.6. The expression $\doteq v_7v_3$ (consisting of three symbols) is an atomic formula since $\doteq$ is a 2-ary relation symbol and v_7 and v_3 are terms. If c_1 and c_2 are constant symbols then $\doteq c_2c_7$ is an atomic formula.

Definition 1.7. A *well-formed sequence* is a finite sequence $\alpha_1, \ldots, \alpha_n$ of expressions such that each α_i is either

1. an atomic well-formed formula, or
2. is of the form $(\neg\beta)$ or $(\beta \longrightarrow \gamma)$, where β and γ occur earlier in the list, or
3. is of the form $\dot{\forall} v_i \beta$, where β occurs earlier in the list.

Definition 1.8. The expression α is a *well-formed formula* (wff) if there is a well-formed sequence $\alpha_1, \ldots, \alpha_k$ such that $\alpha = \alpha_k$.

Example 1.9. The expression $(\neg\dot{\forall} v_3 \doteq v_1 v_2)$ is a wff since

$$\doteq v_1 v_2,\ \dot{\forall} v_3 \doteq v_1 v_2,\ (\neg\dot{\forall} v_3 \doteq v_1 v_2)$$

is a well-formed sequence of expressions.

1.2 Examples

We give two examples involving the definition of *satisfaction* and *logical consequence*

Example 1.10 (Satisfaction)**.** Let $\mathbb{L}$ be the first-order language that has (in addition to the usual symbols),

$\doteq$,

$\dot{<}$ (a 2-ary relation symbol),

$\times$ (a 2-ary function symbol), and

$\dot{0}$ (a constant symbol).

Let φ be the wff

$$\dot{\forall} v_1\ \dot{\exists} v_2\ (v_1 \dot{<} v_2 \wedge v_3 \dot{\times} v_1 \doteq v_2))\ )$$

Let

$$\mathfrak{Z} = (\mathbb{Z}, <, \times, 0)$$

and $s\colon V \longrightarrow \mathbb{Z}$ be the assignment:

$$s(v_i) = \begin{cases} 2, & \text{if } i \text{ is even} \\ 5, & \text{if } i \text{ is odd.} \end{cases}$$

We unravel the definition of satisfaction to determine if $\models_{\mathfrak{Z}} \varphi[s]$. The following are equivalent:

$\models_{\mathfrak{Z}} \varphi[s]$;

$\models_{\mathfrak{Z}} \dot{\forall} v_1 \, \dot{\exists} v_2 \, (v_1 \dot{<} v_2 \wedge v_3 \dot{\times} v_1 \doteq v_2 \,)[s]$;

$\forall a \in \mathbb{Z} \models_{\mathfrak{Z}} \dot{\exists} v_2 \, (v_1 \dot{<} v_2 \wedge v_3 \dot{\times} v_1 \doteq v_2)[s^{v_1}_{a}]$;

$\forall a \in \mathbb{Z} \, \exists b \in \mathbb{Z} \ \models_{\mathfrak{Z}} (v_1 \dot{<} v_2 \wedge v_3 \dot{\times} v_1 \doteq v_2)[s^{v_1,v_2}_{a\ ,b}]$;

$\forall a \in \mathbb{Z} \, \exists b \in \mathbb{Z} \, \big[\models_{\mathfrak{Z}} v_1 \dot{<} v_2 [s^{v_1,v_2}_{a\ ,b}] \ \& \ \models_{\mathfrak{Z}} v_3 \dot{\times} v_1 \doteq v_2 [s^{v_1,v_2}_{a\ ,b}] \big]$;

$\forall a \in \mathbb{Z} \, \exists b \in \mathbb{Z} \, \big[s^{v_1,v_2}_{a\ ,b}(v_1) < s^{v_1,v_2}_{a\ ,b}(v_2) \ \& \ s^{v_1,v_2}_{a\ ,b}(v_3) \times s^{v_1,v_2}_{a\ ,b}(v_1) = s^{v_1,v_2}_{a\ ,b}(v_2)$;

$\forall a \in \mathbb{Z} \, \exists b \in \mathbb{Z} \, \big[a < b \ \& \ 5 \times a = b \, \big]$.

The last line above is a false statement since, for example, if $a = -1$ then the only b such that $b = 5 \times a$ is -5 and so not $a < b$. Hence $\not\models_{\mathfrak{Z}} \varphi[s]$.

Note that we used written $s^{v_1,v_2}_{a\ ,b}$ for the function

$$\begin{aligned} s^{v_1,v_2}_{a\ ,b}(x) &= (s^{v_1}_{a})^{v_2}_{b}(x) \\ &= \begin{cases} s^{v_1}_{a}(x) & \text{if } x \neq v_2 \\ b, & \text{if } x = v_2 \\ & \end{cases} \\ &= \begin{cases} s(x), & \text{if } x \neq v_2 \ \& \ x \neq v_1 \\ a, & \text{if } x = v_1 \\ b, & \text{if } x = v_2 \end{cases} \end{aligned}$$

□

Remark 1.11. Suppose in Example 2.10 we replace $\mathfrak{Z}$ by $\mathfrak{N} = (\mathbb{N}, <, \times, 0)$. Then for the same wff φ, we have

$$\models_{\mathfrak{N}} \varphi[s] \ .$$

Example 1.12 (Logical Consequence)**.** We show

$$\dot{\forall} v_1 \, Q v_1 \models \dot{\exists} v_1 \, Q v_1 \ .$$

Here the language $\mathbb{L}$ has (at least) a 1-ary relation symbol Q. We must show:

for every structure $\mathfrak{A}$ for $\mathbb{L}$, and
for every assignment $s \colon V \longrightarrow |\mathfrak{A}|$,

if

$$\models_{\mathfrak{A}} \dot{\forall} v_1 \, Q v_1 [s] \tag{1}$$

then

$$\models_{\mathfrak{A}} \dot{\exists} v_1 \, Q v_1 [s] \tag{2}$$

Suppose (2) holds for a given $\mathfrak{A}$ and s. Then

$$\forall a \in |\mathfrak{A}| \; [a \in Q^{\mathfrak{A}}] \; ,$$

i.e.

$$Q^{\mathfrak{A}} = |\mathfrak{A}| \; . \tag{3}$$

Since by the definition of a structure, $|\mathfrak{A}| \neq \emptyset$, there is some $a \in |\mathfrak{A}|$. But then

$$\models_{\mathfrak{A}} \dot{\exists} v_1 \, Q v_1 \; .$$

$\square$

1.3 Models of Sentences

Definition 1.13. The structure

$\mathfrak{A}$ is *finite* if $|\mathfrak{A}|$ is finite;

$\mathfrak{A}$ is *infinite* if $|\mathfrak{A}|$ is infinite;

$\mathfrak{A}$ is *countable* if $|\mathfrak{A}|$ is countable;

$\mathfrak{A}$ is *enumerable* if $|\mathfrak{A}|$ is enumerable;

$\mathfrak{A}$ is *uncountable* if $|\mathfrak{A}|$ is uncountable.

Definition 1.14. Let τ be a sentence, and Σ be a set of sentences of some first-order language.

$\mathfrak{A}$ is a *model* of τ if $\models_{\mathfrak{A}} \tau$.

$\mathfrak{A}$ is a *model* of Σ if $\mathfrak{A}$ is a model of each σ in Σ.

$\mathrm{Mod}(\Sigma)$ is the collection of all models of Σ.

Exercise 1.15. Let P be a two place relation symbol, and Σ be the following set of sentences:

$$\begin{align}
&\dot\forall x\,\dot\forall y\,\dot\forall z\ (Pxy \wedge Pyz \longrightarrow Pxz) \tag{4}\\
&\dot\exists x\,\dot\forall y\ Pxy \tag{5}\\
&\dot\exists z\,\dot\forall y\ Pyz \tag{6}\\
&\dot\exists x\,\dot\exists y\ (\neg Pxy \wedge \neg Pyx) \tag{7}\\
&\dot\forall x\,\dot\forall y\ (Pxy \wedge Pyx \longrightarrow x \doteq y)\ . \tag{8}
\end{align}$$

Does Σ have a finite model? If it does find one. If it doesn't, explain why.

Exercise 1.16. Let $\mathbb{L}$ be the first-order language with $\doteq$, and a 2-place relation symbol P, but no other function or relation or constant symbols. Find a sentence σ of $\mathbb{L}$ such that:

σ is true in some infinite structure, but false in every finite structure (i.e. σ has an infinite model, but no finite model).

Explain carefully why the sentence σ you have found has the desired properties.

Exercise 1.17. Choose an appropriate first-order language $\mathbb{L}$ and find a set of sentences Σ of $\mathbb{L}$ such that:

Σ has an uncountable model but no countable model.

Show that your Σ has the desired properties.

Exercise 1.18.

1. Try to find a first-order language $\mathbb{L}$ and a sentence σ of $\mathbb{L}$ such that for each n, the sentence σ is true in some structure $\mathfrak{A}$ with $|\mathfrak{A}| \geq n$, but σ is false in every infinite structure.

2. Try to find a first-order language $\mathbb{L}$ and a set Σ of sentences of $\mathbb{L}$ such that for each n, Σ has a model in some structure $\mathfrak{A}$ with $|\mathfrak{A}| \geq n$, but Σ has no infinite model.

Exercise 1.19. Let $\mathbb{L}$ be the first-order language with $\doteq$, and a binary relation symbol $\dot<$. Try to find a sentence of $\mathbb{L}$ that is true in the structure $(\mathbb{R}, <)$ but false in $(\mathbb{Q}, <)$.

Exercise 1.20. Let $\mathbb{L}$ be the first-order language with $\doteq$. Try to find a sentence σ of $\mathbb{L}$ such that for every finite structure $\mathfrak{A} = (|\mathfrak{A}|, =)$:

$$\models_{\mathfrak{A}} \sigma \quad \text{iff} \quad |\mathfrak{A}| \text{ has an even number of members.}$$

Definition 1.21. Suppose $\mathfrak{A} = (A, R)$ is a structure, where R is a binary relation on A. Let $B \subseteq A$, and $b \in A$. b is an *R-minimal member of* B, if

1. $b \in B$, and
2. $\forall a \in B\ [(a, b) \notin B]$.

Example 1.22. Let:

1. $\mathfrak{R} = (\mathbb{R}, <)$;
2. $B_1 = \{x : 0 \leq x < 3\}$;
3. $B_2 = \{x : 0 < x < 3\}$,

where $<$ is the *less than* relation on $\mathbb{R}$. Then 0 is an $<$-minimal member of B_1, but there is no $<$-minimal member of B_2.

Definition 1.23. The structure $\mathfrak{A} = (A, R)$ (where R is a binary relation on $|A|$) is

1. *wellfounded* if every non-empty subset of A has an R-minimal member;

2. *wellordered* if it is wellfounded and ordered.

Example 1.24.

1. $\mathfrak{R} = (\mathbb{R}, <)$ is not wellfounded.
2. $\mathfrak{R}_{\geq 0} = (\{x \in \mathbb{R} : x \geq 0\}, <)$ (where $<$ is the *less than* relation on $\{x \in \mathbb{R} : x \geq 0\}$) is not wellfounded.
3. $\mathfrak{N} = (\mathbb{N}, <)$ (where $<$ is the *less than* relation on $\mathbb{N}$) is wellordered.

Theorem 1.25. *The structure $\mathfrak{A} = (A, R)$ is not wellfounded iff there is an infinite sequence $a_0, a_1, \ldots, a_n, \ldots$ of members of A such that for all n, $a_{n+1} R\, a_n$.*

Proof. ($\Longleftarrow$): Suppose that for all n, $a_{n+1} R\, a_n$. Let $B = \{a_0, \ldots, a_n, \ldots\}$. Then B has no R-minimal member.

($\Longrightarrow$): Suppose $\mathfrak{A}$ is not wellfounded. Then there is some $B \neq \emptyset$ which has no R-minimal member. Choose $a_0 \in B$. a_0 is not R-minimal, and so there is some $a_1 \in B$ such that $a_1 R\, a_0$. Since a_1 is not R-minimal, there is an $a_2 \in B$ such that $a_2 R\, a_1$. Continuing, we see that for each $n \in B$, there is an $a_{n+1} \in B$ such that $a_{n+1} R\, a_n$. Thus there is an infinite sequence $a_0, \ldots, a_n, \ldots$ of members of B such that for all n, $a_{n+1} R\, a_n$. $\square$

***Question* 1.26.** Let $\mathbb{L}$ be the first-order language with $\doteq$, and a 2-place predicate symbol P, but no other function or relation or constant symbols.

1. Does there exist a sentence σ of $\mathbb{L}$ such that for every structure $\mathfrak{A} = (A, R)$,
$$\models_{\mathfrak{A}} \sigma \;\text{ iff }\; \mathfrak{A} \text{ is wellfounded?}$$
(The existence of such a sentence is equivalent to saying that the class of wellfounded structures is an EC class.)

2. If the answer to (a) is *no*, does there exist a set Σ of sentences of $\mathbb{L}$ such that for every structure $\mathfrak{A} = (A, R)$,
$$\mathfrak{A} \text{ is a model of } \Sigma \;\text{ iff }\; \mathfrak{A} \text{ is a wellfounded structure?}$$
(The existence of such a set of sentences is equivalent to saying that the class of wellfounded structures is an EC_Δ.)

1.4 Graphs

Definition 1.27. Let $\mathbb{L}$ be a first-order language with $\doteq$ and a binary relation symbol E. A structure $\mathfrak{A} = (A, E^{\mathfrak{A}})$ for $\mathbb{L}$ is a *graph* if:

1. $E^{\mathfrak{A}}$ is *irreflexive*, i.e. $\forall a \in A\ (a, a) \notin E^{\mathfrak{A}}$, and
2. $E^{\mathfrak{A}}$ is *symmetric*, i.e. $\forall a \in A\, \forall b \in A\ [(a, b) \in E^{\mathfrak{A}} \Longrightarrow (b, a) \in E^{\mathfrak{A}}]$.

A graph is *finite* if its universe is finite.

Remark 1.28. Let σ be the sentence $\dot\forall x \neg Exx \wedge \dot\forall x \dot\forall y\ (Exy \longrightarrow Eyx)$. Then for every structure $\mathfrak{A}$,
$$\mathfrak{A} \in \mathrm{Mod}(\sigma) \text{ iff } \mathfrak{A} \text{ is a graph.}$$

Remark 1.29. If $\mathfrak{A} = (A, E^{\mathfrak{A}})$ is a finite graph we can draw a picture of it by drawing a line between each elements a and b just in case $(a, b) \in E^{\mathfrak{A}}$.

Example 1.30. Let $\mathfrak{A}_3 = (A_3, E^{\mathfrak{A}_3})$ and $\mathfrak{A}_4 = (A_4, E^{\mathfrak{A}_4})$ be the graphs, where
$$\begin{aligned} A_3 &= \{0, 1, 2, 3\}\ ; \\ E^{\mathfrak{A}_3} &= \{(0, 2), (2, 0), (1, 3), (3, 1), (1, 2), (2, 1)\}\ , \end{aligned}$$

and

$$\begin{aligned} A_4 &= \{0, 1, 2, 3, 4\}\ ; \\ E_4 &= \{(0,2), (2,0), (1,3), (3,1), (2,4), (4,2), (0,4), (4,0)\}\ . \end{aligned}$$

We can picture these graphs as follows:

Definition 1.31. Let $\mathfrak{A} = (A, E^{\mathfrak{A}})$ be a graph.

1. A *path* between elements a and b of A is a finite sequence $a_1, \ldots, a_k$ of elements of A such that
   (a) $a = a_1$ and $b = a_k$, and
   (b) for each i such that $0 < i < k$, we have $(a_i, a_{i+1}) \in E^{\mathfrak{A}}$.
2. $\mathfrak{A}$ is a *connected graph* if for every a and b in A there is some path between a and b.

Remark 1.32. The graph $\mathfrak{A}_3$ is connected, but the graph $\mathfrak{A}_4$ is not connected.

We can generalize the graphs $\mathfrak{A}_3$ and $\mathfrak{A}_4$ as follows:

Definition 1.33. For $n > 0$, let $\mathfrak{A}_n = (A_n, E^{\mathfrak{A}_n})$ be the finite structure with

$$\begin{aligned} A &= \{0, \ldots, n\}, \text{ and} \\ E^{\mathfrak{A}_n} &= \{(i,j) : 0 \leq i, j \leq n \;\&\; |i - j| = 2\} \\ &\quad \cup \{(0,n), (n,0)\} \cup \{(1, n-1), (n-1, 1)\} \;. \end{aligned}$$

Remark 1.34. The graph $\mathfrak{A}_n$ is connected iff n is odd, i.e. iff the universe of $\mathfrak{A}_n$ has an even number of members.

***Question* 1.35.** Is there a sentence σ of the language for graphs such that for every graph $\mathfrak{A}$,

$$\mathfrak{A} \text{ is connected iff } \models_{\mathfrak{A}} \sigma \text{ ?}$$

1.5 Definability Within a Structure

Let:

$$\begin{aligned} \mathfrak{N}_< &= (\mathbb{N}, <) \\ \mathfrak{N}_+ &= (\mathbb{N}, +) \\ \mathfrak{N}_\times &= (\mathbb{N}, \times) \\ \mathfrak{N}_{+,\times} &= (\mathfrak{N}, +, \times) \;, \end{aligned}$$

where $<$ is the 'less than' relation on $\mathbb{N}$, and $+$ and $\times$ are the addition and multiplication functions on $\mathbb{N}$. (The structure $\mathfrak{N}_{+,\times}$ has in its associated language the symbols $\dot{=}$, $\dot{+}$, $\dot{\times}$, but no other predicate, function, or constant symbols.)

Example 1.36.

1. $v_1 \dot{<} v_2$ defines the relation $<$ in $\mathfrak{N}_<$. But the same wff $v_1 \dot{<} v_2$ also defines the 3-ary relation $\{(m,n,p) : m,n,p \in \mathbb{N} \;\&\; m < n\}$, the 4-ary relation $\{(m,n,p,q) : m,n,p,q \in \mathbb{N} \;\&\; m < n\}$, etc.
2. $v_2 \dot{<} v_4$ defines the 4-ary relation $\{(m,n,p,q) : m,n,p,q \in \mathbb{N} \;\&\; n < q\}$, the 5-ary relation $\{(m,n,p,q,r) : m,n,p,q,r \in \mathbb{N} \;\&\; n < p\}$, etc.
3. $\forall v_2\,(v_2 \not\doteq v_1 \rightarrow v_1 \dot{<} v_2)$ defines the set $\{0\}$.
4. $\exists v_3\,[\forall v_2\,(v_2 \not\doteq v_3 \rightarrow v_3 \dot{<} v_2) \wedge v_1 \not\doteq v_3 \wedge \forall v_4\,(v_4 \dot{<} v_1 \rightarrow v_4 \doteq v_3)]$ defines $\{1\}$.

Definition 1.37. Let $\mathfrak{A}$ be a structure for the language $\mathbb{L}$. The n-ary function $f\colon A^n \longrightarrow A$ is *definable in* $\mathfrak{A}$ if its graph is definable in $\mathfrak{A}$. For example, the binary function $f\colon A^2 \longrightarrow A$ is definable in $\mathfrak{A}$ if the 3-ary relation

$$\{(a,b,c) : f(a,b) = c\}$$

is definable.

Proposition 1.38. *Let $\mathfrak{A}$ be a structure for the language $\mathbb{L}$ with $A = |\mathfrak{A}|$.*

1. *$\emptyset$ and A are definable.*
2. *The relation $P^{\mathfrak{A}}$ is definable for each predicate symbol P. (In particular, the equality relation $=^A$ on A is definable, assuming $\doteq$ is in the language $\mathbb{L}$.)*
3. *The function $f^{\mathfrak{A}}$ is definable, for each function symbol f.*
4. *If the relation R is definable, then so is its complement.*
5. *If each of the k-ary relations $R_1, \ldots, R_n$ is definable, then both the union, $R_1 \cup \ldots \cup R_n$, and the intersection, $R_1 \cap \ldots R_n$, are definable.*
6. *If the $n+1$-ary relation R is definable, then so are the n-ary relations Q and S, where*

$$\begin{aligned} Q(\mathbf{x}) &\iff \exists y \in A\, R(\mathbf{x}, y) \\ S(\mathbf{x}) &\iff \forall y \in A\, R(\mathbf{x}, y)\ . \end{aligned}$$

Exercise 1.39. Let $\mathfrak{A}$ be a structure for $\mathbb{L}$ and $A = |\mathfrak{A}|$.

1. Show that each projection function $Pr_i^n\colon A^n \longrightarrow A$ is definable, where $Pr_i^n(a_1, \ldots, a_n) = a_i$.
2. Show that the class of functions definable on $\mathfrak{A}$ is closed under composition. For example, show that if f and g are 1-ary functions which are definable in $\mathfrak{A}$, then h is also definable, where $h(a) = f(g(a))$.

Example 1.40.

1. $\leq$ is definable in $\mathfrak{N}_+$;
2. $<$ is definable in $\mathfrak{N}_+$;
3. $\{2n : n \in \mathbb{N}\}$ (the set of even integers in $\mathbb{N}$) is definable in $\mathfrak{N}_+$.

***Question* 1.41.**

1. Is $\times$ definable in $\mathfrak{N}_+$?
2. Is $+$ definable in $\mathfrak{N}_\times$?

Definition 1.42. The *initial* functions on $\mathbb{N}$ consist of all functions Pr_i^n, Cs_c^n, and Sc_i^n, where $k > 0$ and $i < n$ and

1. $\mathrm{Pr}_i^n(a_1, \ldots, a_n) = a_i$ (the *projection* functions);
2. $\mathrm{Cs}_c^n(a_1, \ldots, a_n) = c$ (the *constant* functions);
3. $\mathrm{Sc}_i^n(a_1, \ldots, a_n) = a_i + 1$ (the *successor* functions).

Exercise 1.43. Show that every initial function is definable in $\mathfrak{N}_{+,\times}$.

Remark 1.44. You can skip the rest of this section. We will return to it after we have defined the class of recursive functions.

Exercise 1.45. Suppose f is an $n+1$-ary function which is definable in $\mathfrak{N}_{+,\times}$ and g is defined by unbounded search from f. Show that g is definable in $\mathfrak{N}_{+,\times}$.

***Question* 1.46.** We know from the above exercises that every initial function is definable in $\mathfrak{N}_{+,\times}$, and the functions definable in $\mathfrak{N}_{+,\times}$ are closed under composition and unbounded search. Is every recursive function definable in $\mathfrak{N}_{+,\times}$?

Exercise 1.47. Assume that every recursive function is definable in $\mathfrak{N}_{+,\times}$.

1. Show that every recursively enumerable relation is definable in $\mathfrak{N}_{+,\times}$.
2. Show that there are relations definable in $\mathfrak{N}_{+,\times}$ which are not recursively enumerable.

1.6 Substructures and Reducts

Definition 1.48. Substructure] Let $\mathfrak{A} = (A, \ldots)$ and $\mathfrak{B} = (B, \ldots)$ be structures for the first-order language $\mathbb{L}$.

1. $\mathfrak{A}$ is a *substructure* of $\mathfrak{B}$ (written $\mathfrak{A} \subseteq \mathfrak{B}$) if
    (a) $A \subseteq B$;
    (b) for every k-ary relation symbol P and every k-tuple $\bar{a} = (a_1, \ldots, a_k)$ of elements of A,
    $$\bar{a} \in P^{\mathfrak{A}} \iff \bar{a} \in P^{\mathfrak{B}}$$
    (Note that this is not the same as saying that $P^{\mathfrak{A}} \subseteq P^{\mathfrak{B}}$);
    (c) for every k-ary function symbol f and every k-tuple $\bar{a} = (a_1, \ldots, a_k)$ of elements of A,
    $$f^{\mathfrak{A}}(\bar{a}) = f^{\mathfrak{B}}(\bar{a}) \; ;$$
    (d) for each constant symbol c of $\mathbb{L}$,
    $$c^{\mathfrak{A}} = c^{\mathfrak{B}} \; .$$

If $\mathfrak{A}$ is a substructure of $\mathfrak{B}$ we also say that $\mathfrak{B}$ is an *extension* of $\mathfrak{A}$.

The notion of substructure is defined on page 95 of Enderton.

Example 1.49. Let

$$\mathfrak{N} = (\mathbb{N}, <^{\mathbb{N}}, +^{\mathbb{N}}, \times^{\mathbb{N}}) \tag{9}$$
$$\mathfrak{E} = (\mathbb{E}, <^{\mathbb{E}}, +^{\mathbb{N}}, \times^{\mathbb{E}}) \; . \tag{10}$$

Then $\mathfrak{E}$ is a substructure of $\mathfrak{N}$.

Exercise 1.50. Let

$$\begin{aligned} \mathfrak{B} &= (B, P^{\mathfrak{B}}) \; , \text{ and} \\ \mathfrak{A} &= (A, P^{\mathfrak{A}}) \; , \end{aligned}$$

where

$$\begin{aligned} &B = \mathbb{N} \text{ and } P^{\mathfrak{B}} = \mathbb{E} \\ &A = \{0, 1, 2, 3\} \text{ and } P^{\mathfrak{A}} = \{0, 1\} \; . \end{aligned}$$

Is $\mathfrak{A}$ a substructure of $\mathfrak{B}$?

Definition 1.51 (Reduct)**.** Let $\mathbb{L}$ be a first-order language and let $\mathbb{L}'$ be the first-order language obtained from $\mathbb{L}$ by eliminating from $\mathbb{L}$ some of the relation symbols, function symbols, or constant symbols. Let $\mathfrak{A} = (A, \ldots)$ be a structure for $\mathbb{L}$ and $\mathfrak{B} = (B, \ldots)$ be a structure for $\mathbb{L}'$. $\mathfrak{B}$ is a *reduct* of $\mathfrak{A}$ if

1. $A = B$ (so $\mathfrak{A}$ and $\mathfrak{B}$ have the same universe);
2. For each relation symbol P, function symbol f, and constant symbol c of $\mathbb{L}'$,

$$\begin{aligned} P^{\mathfrak{A}} &= P^{\mathfrak{B}} \ ; \\ f^{\mathfrak{A}} &= f^{\mathfrak{B}} \ ; \\ c^{\mathfrak{A}} &= c^{\mathfrak{B}} \ . \end{aligned}$$

Example 1.52. Let

$$\begin{aligned} \mathfrak{N} &= (\mathbb{N}, <^{\mathbb{N}}, +^{\mathbb{N}}, \times^{\mathbb{N}}, 0, 1) \ ; \\ \mathfrak{B} &= (\mathbb{N}, +^{\mathbb{N}}) \ . \end{aligned}$$

So $\mathfrak{N}$ is a structure for the language $\mathbb{L}$ which has symbols $\doteq$, $<$, $+$, $\times$, $\mathbf{0}$, and $\mathbf{1}$. And $\mathfrak{B}$ is a structure for the language $\mathbb{L}'$ which has $\doteq$, and $+$. $\mathfrak{B}$ is a reduct of $\mathfrak{N}$. Note that the numbers 0 and 1 are still in the universe of $\mathfrak{B}$ even though the constant symbols $\mathbf{0}$ and $\mathbf{1}$ are not part of the language $\mathbb{L}'$.

1.7 Homomorphisms

Definition 1.53. Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures for the same language $\mathbb{L}$. A function $h \colon |\mathfrak{A}| \longrightarrow |\mathfrak{A}|$ is a *homomorphism* from $\mathfrak{A}$ to $\mathfrak{B}$, if:

1. for every n-ary relation symbol P, every n-ary function symbol f, and every n-tuple $a_1, \ldots, a_n$ of elements of $|\mathfrak{A}|$, and every constant symbol c:
2. $(a_1, \ldots, a_n) \in P^{\mathfrak{A}} \iff (h(a_1), \ldots, h(a_n)) \in P^{\mathfrak{B}}$.
3. $h(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_n))$.
4. $h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$.

Definition 1.54.

1. An *isomorphism* is a homomorphism that is one-to-one.

2. Two structures $\mathfrak{A}$ and $\mathfrak{B}$ are *isomorphic* is there is an isomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$.

3. $\mathfrak{A} \simeq \mathfrak{B}$ means $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic.

4. An *automorphism* of $\mathfrak{A}$ is an isomorphism of $\mathfrak{A}$ onto itself.

Theorem 1.55 (Homomorphism Theorem). *Let:*

> *h be a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$;*
>
> *$s\colon V \longrightarrow |\mathfrak{A}|$ be an assignment;*
>
> *α be a wff.*

The statement

$$\models_{\mathfrak{A}} \alpha[s] \iff \models_{\mathfrak{B}} \alpha[h \circ s]$$

1. *is true for every quantifier-free wff that does not contain $\doteq$;*

2. *is true for every quantifier-free wff if h is one-to-one;*

3. *is true for every wff that does not contain $\doteq$, if h maps onto $|\mathfrak{B}|$.*

4. *is true for every wff if h is one-to-one and maps onto $|\mathfrak{B}|$ (i.e. if h is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$).*

Corollary 1.56. *If $\mathfrak{A} \simeq \mathfrak{B}$ then $\mathfrak{A} \equiv \mathfrak{B}$.*

Corollary 1.57 (Automorphism Theorem). *For every n-ary relation R that is definable in $\mathfrak{A}$, and every automorphism h of $\mathfrak{A}$, and every n-tuple $a_1, \ldots, a_n$ of elements of $\mathfrak{A}$,*

$$(a_1, \ldots, a_n) \in R \iff (h(a_1), \ldots, h(a_n)) \in R\,.$$

1.8 Congruence Relations

Recall that if R is a binary relation then $(a, b) \in R$, $R(a, b)$, and aRb all have the same meaning.

Definition 1.58. An *equivalence relation* on a set A is a binary relation R on A (i.e. a subset of $A \times A$) such that for all a,b, and c in A:

1. aRb and bRc implies aRC (R is *transitive*);

2. aRb implies bRa (R is *symmetric*);

3. aRa (R is *reflexive*)

We often use $\equiv$ to stand for an equivalence relation.

Definition 1.59. Let $\equiv$ be an equivalence relation on A. For $a \in A$,

$$[a] = \{b : b \equiv a\} \ .$$

$[a]$ is called the *equivalence class* of a. It consists of all things 'equivalent' to a.

Theorem 1.60. *Let $\equiv$ be an equivalence relation on A. Then for all a and b in A:*

1. *If $a \equiv b$ then $[a] = [b]$;*
2. *If $a \not\equiv b$ then $[a] \cap [b] = \emptyset$;*
3. *$a \in [a]$.*

It follows that the equivalence classes form a *partition* of A.

Example 1.61. For a and b in $\mathbb{N}$, let

$$a \equiv_2 b \iff a - b \text{ is even} \ .$$

Then $\equiv_2$ is an equivalence relation on $\mathbb{N}$. There are only two equivalence classes:

$$\begin{aligned} [0] &= \text{the set of even integers, and} \\ [1] &= \text{the set of odd integers.} \end{aligned}$$

Example 1.62. Let m be a positive integer. For a and b in $\mathbb{N}$, let

$$a \equiv_m b \iff b - a \text{ is divisible by } m \ .$$

Then $\equiv_m$ is an equivalence relation on $\mathbb{N}$. There are m equivalence classes:

$$\begin{aligned} [0] &= \{a : a \text{ is divisible by } m\} \ ; \\ [1] &= \{a : a - 1 \text{ is divisible by } m\} \ ; \\ &\vdots \\ [m-1] &= \{a : a - (m-1) \text{ is divisible by } m\} \ . \end{aligned}$$

Thus

$$\begin{aligned}
[0] &= \{0, m, 2m, 3m, \ldots\} \\
[1] &= \{1, m+1, 2m+1, \ldots\} \\
[2] &= \{2, m+2, 2m+2, \ldots\} \\
&\vdots
\end{aligned}$$

Definition 1.63. Let $\mathfrak{A}$ be a structure for $\mathbb{L}$. The binary relation $\equiv$ on $|\mathfrak{A}|$ is a *congruence relation for* $\mathfrak{A}$ if

1. $\equiv$ is an equivalence relation on $|\mathfrak{A}|$;
2. for every pair $a_1, \ldots, a_n$ and $a'_1, \ldots, a'_n$ of n-tuples of elements of $|\mathfrak{A}|$, every n-ary relation symbol P, and n-ary function symbol f, if

$$a_1 \equiv a'_1, \ldots, a_n \equiv a'_n$$

   then

   (a) $(a_1, \ldots, a_n) \in P^{\mathfrak{A}} \iff (a'_1, \ldots, a'_n) \in P^{\mathfrak{A}}$, and

   (b) $f^{\mathfrak{A}}(a_1, \ldots, a_n) \equiv f^{\mathfrak{A}}(a'_1, \ldots, a'_n)$.

Exercise 1.64. Let $\mathbb{L}$ have the binary function symbols $\dot{+}$ and $\dot{\times}$. $\equiv_2$ is a congruence relation for the structure $(\mathbb{N}, +, \times)$. In fact, show that $\equiv_m$ is a congruence relation for this structure, for each positive integer m.

Definition 1.65 (Quotient Structure)**.** Let $\mathfrak{A}$ be a structure for the language $\mathbb{L}$, and $\equiv$ be a congruence relation for $\mathfrak{A}$. We define a new structure $\mathfrak{A}/_{\equiv}$, called the *quotient structure* for $\mathbb{L}$ as follows:

1. $|\mathfrak{A}/_{\equiv}| = \{[a] : a \in |\mathfrak{A}|\}$,
   i.e. the members of the universe are the equivalence classes;
2. for each n-ary relation symbol P, and elements $a_1, \ldots, a_n$ of $\mathfrak{A}$,

$$([a_1], \ldots, [a_n]) \in P^{\mathfrak{A}/\equiv} \iff (a_1, \ldots, a_n) \in P^{\mathfrak{A}} \; ;$$

3. for each n-ary function symbol f, and elements $a_1, \ldots, a_n$ of $|\mathfrak{A}|$,

$$f^{\mathfrak{A}/\equiv}([a_1], \ldots, [a_n]) = [f^{\mathfrak{A}}(a_1, \ldots, a_n)] \; ;$$

4. for each constant symbol c,
$$c^{\mathfrak{A}/\equiv} = [c^{\mathfrak{A}}] \; .$$

Proposition 1.66. *Let* $\equiv$ *be a congruence relation for* $\mathfrak{A}$ *and* $\mathfrak{A}_\equiv$ *be the associated quotient structure. Let* $h\colon |\mathfrak{A}| \longrightarrow |\mathfrak{A}|$ *be the mapping such that for* $a \in |\mathfrak{A}|$,
$$h(a) = [a] \; .$$
Then h *is a homomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{A}$.

Proof. Every member of $|\mathfrak{A}|$, is $[a]$ for some $a \in |\mathfrak{A}|$. Since $h(a) = [a]$, it follows that h maps $|\mathfrak{A}|$ onto $|\mathfrak{A}|_\equiv$. To see that h is a homomorphism, suppose P is an n-ary relation symbol. (Verifying the rest of the properties of a homomorphism is left as an exercise.) Then

$$\begin{aligned}(a_1, \ldots, a_n) \in P^{\mathfrak{A}} &\iff ([a_1], \ldots, [a_n]) \in P^{\mathfrak{A}_\equiv} \\ &\iff (h(a_1), \ldots, h(a_n)) \in P^{\mathfrak{A}_\equiv} \; .\end{aligned}$$

$\square$

Exercise 1.67. Let $\mathbb{L}$ be the first-order language with function symbols $\dot{+}$ and $\dot{\times}$, and a 2-place relation symbol $\dot{\equiv}$. Let $\mathfrak{N}$ be the structure

$$\mathfrak{N} = (\mathbb{N}, +, \times, \equiv_m)$$

for $\mathbb{L}$, where $\dot{\equiv}^{\mathfrak{N}} = \equiv_m$.

Show that if

$$\begin{aligned}&a_1 \equiv_m b_1 , \text{ and} \\ &a_2 \equiv_m b_2 \; ,\end{aligned}$$

then

$$\begin{aligned}&a_1 + a_2 \equiv_m b_1 + b_2 \; , \text{ and} \\ &a_1 \times a_2 \equiv_m b_1 \times b_2 \; .\end{aligned}$$

Conclude that $\equiv_m$ is a congruence relation for $\mathfrak{N}$.

Theorem 1.68. *Let* $\mathfrak{A}$ *be a structure for a language* $\mathbb{L}$ *that includes a binary relation symbol* $\dot{\equiv}$ *(plus perhaps other relation, function, and constant symbols).*

Let $\equiv$ *be the binary relation that* $\dot{\equiv}$ *denotes in* $\mathfrak{A}$, *i.e.*

$$\equiv = \dot{\equiv}^{\mathfrak{A}} .$$

Suppose that $\equiv$ *is a congruence relation for* $\mathfrak{A}$ *with associated quotient structure* $\mathfrak{A}_{\equiv}$.

Let $h\colon |\mathfrak{A}| \longrightarrow \mathfrak{A}_{\equiv}$, *where for* $a \in |\mathfrak{A}|$ $h(a) = [a]$ *Then*

1. h *is a homomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{A}_{\equiv}$;
2. $\dot{\equiv}^{\mathfrak{A}/\equiv} ==$, *i.e.* $\dot{\equiv}$ *denotes the identity relation on the quotient structure.*

To see 2, we have for a *and* b *in* $|\mathfrak{A}|$:

$$\begin{aligned} [a]\dot{\equiv}^{\mathfrak{A}_{\equiv}}[b] &\iff a \equiv b \\ &\iff [a] = [b] \end{aligned}$$

Exercise 1.69. Let $\mathbb{L}$ be the first-order language with binary function symbols $\dot{+}$ and $\dot{\times}$, and a binary relation symbol $\dot{\equiv}$. Let $\mathfrak{N} = (\mathbb{N}, +\times, \equiv_2)$, where $\equiv_2$ is from Example 1.62.

Is there a sentence σ that does not contain $\dot{=}$ that is true in $\mathfrak{N}$ but false in the quotient structure $\mathfrak{N}_{\equiv_2}$? If there is one, find it. If there isn't explain why.