APPLICATION OF FIRST ORDER LOGIC: DIVISIBILITY, v.2

Let us take a brief look into an application of FOL in arithmetic, considering divisibility as an example.

Divisibility relation on the set of integers, denoted $\mathbb{Z}$, is defined, in the traditional textbook style, as follows:

> Let x and y be integers with $x \neq 0$. We say that x divides y if there is an integer z such that $y = x \cdot z$.

We can formalize the *divides* relation as a binary predicate. Instead of using prefix notation, e.g. $Divides(x, y)$, we prefer the customary infix notation, $x|y$, read "x divides y".

$$x|y \equiv_{def} \exists u\ (y = x \cdot u)$$

where the domain for x is $\mathbb{Z} - \{0\}$, for y and u, $\mathbb{Z}$.

A basic property of divisibility is stated as follows:

> Let x, y, and z be integers, where $x \neq 0$. Then, if $x|y$ and $x|z$ then $x|(y + z)$.

A typical proof goes like this:

Suppose that $x|y$ and $x|z$. Then, from the definition of divisibility, there are integers s and t such that $y = x \cdot s$ and $z = x \cdot t$. By doing arithmetic, $y + z = x \cdot s + x \cdot t = x \cdot (s + t)$. Hence, $x|(y + z)$.

We can formalize this proposition as follows:

$$\forall x \forall y \forall z \, (x|y \wedge x|z \longrightarrow x|(y+z))$$

Let us rewrite the proof in the style of natural deduction.

a, b, c fresh names

1. $a|b \wedge a|c$ assumption
2. $a|b$ $1, \wedge e$
3. $\exists u \, (b = a \cdot u)$ 2, definition
4. $a|c$ $1, \wedge e$
5. $\exists u \, (c = a \cdot u)$ 4, definition

s, t fresh names

6. $b = a \cdot s$ assumption, 3
7. $c = a \cdot t$ assumption, 5
8. $b + c = a \cdot s + a \cdot t$ 6,7, arithmetic
9. $b + c = a \cdot (s + t)$ 8, arithmetic
10. $\exists u(b + c = a \cdot u)$ $9, \exists i$

11. $\exists u(b + c = a \cdot u)$ $3,5,6-10, \exists e(2)$
12. $a|(b + c)$ 11, definition
13. $a|b \wedge a|c \rightarrow a|(b + c)$ $1-12, \rightarrow i$
14. $\forall x \forall y \forall z\big(x|y \wedge x|z \rightarrow x|(y + z)\big)$ $1-13, \forall i(3)$

Regarding the proof above, please, be aware of

- Abbreviated style (combining similar steps)
- Equational reasoning (use of the predicate =)
- Use of terms (with arithmetic function symbols)

For combining steps (as indicated in lines 11 and 14), we took the advantage of following equivalences:

$$\exists x \exists y \varphi(x, y) \equiv \exists y \exists x \varphi(x, y)$$

$$\forall x \forall y \varphi(x, y) \equiv \forall y \forall x \varphi(x, y)$$

Verify these two equivalences as an exercise.

Using area knowledge, e.g. arithmetic facts, is necessary for any application of Logic in that particular area. Terms constructed by $using\ t$he functions symbols, e.g. addition and multiplication symbols, are essential to compute objects in the domain.

The equality predicate, designated, as usual, =, has a special place in FOL. It is interpreted by the identity relation on the domain it is applied. The given proof uses equational reasoning (e.g. substituting equal terms for each other) without making fuss about it.

Thanks to the equality predicate we can express the notion of uniqueness:

$$\exists!\, x \varphi(x) \equiv_{def} \exists x \varphi(x) \wedge \forall x \forall y (\varphi(x) \wedge \varphi(y) \longrightarrow x = y)$$

We read $\exists!\, x \varphi(x)$ as “there is a unique x such that $\varphi(x)$ holds”.

For example, $\forall x \forall y \exists!\, u\ (y = x \cdot u)$