Lecture Slides 22
Appendix: Exercises in First-Order Definability

Assaf Kfoury

7 October 2024

All the structures in this handout are over the universe $\mathbb{N}$ of natural numbers $\{0, 1, 2, \ldots\}$. The underlying predicates and functions of each structure, as specified by the signature, will be different in different exercises.

We assume throughout that the equality predicate between natural numbers is available, *i.e.*, the symbol "$\approx$" (which is always interpreted as equality between natural numbers) can be used in the syntax of first-order wff's, as a binary predicate in infix position, and will not be explicitly mentioned in the signature.

For brevity, we use the same symbol to denote a function name (or a predicate name) and the interpretation of that name. For example, we use the same symbol "+" to denote the name of a binary function (used in infix position) *and* the interpretation of that name as addition of natural numbers; *i.e.*, if addition is one of the underlying operations of the structure $\mathcal{N}$, we do not bother to write "$+^{\mathcal{N}}$" to make explicit that addition is different from the symbol "+" of which "$+^{\mathcal{N}}$" is the interpretation.

We use several common arithmetical operations and refer to them by their usual names: the binary *addition* $+$, *subtraction* $-$, and *multiplication* $\times$ (all in infix position), the *ordering* predicate $<$ (in infix position), and the unary *successor* succ. We also use:

- the *predecessor* operation, $\mathsf{pred}(n) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } n = 0, \\ n-1 & \text{if } n > 0, \end{cases}$
- the *monus* operation, $m \dot{-} n \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } m \leqslant n, \\ m-n & \text{if } m > n, \end{cases}$
- the *divisibility* predicate, $m \,|\, n \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if } m \text{ is a divisor of } n, \\ \mathit{false} & \text{if } m \text{ is not a divisor of } n, \end{cases}$
- the *least common multiple* operation, $\mathsf{lcm}(m, n)$,
- the *greatest common divisor* operation, $\mathsf{gcd}(m, n)$,
- the *perfect square* predicate, $\mathsf{perfectSq}(n) \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if there is } m \in \mathbb{N} \text{ such that } n = m^2, \\ \mathit{false} & \text{otherwise}, \end{cases}$
- the *prime* predicate, $\mathsf{prime}(n) \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if } n \text{ is a prime number} \geqslant 2, \\ \mathit{false} & \text{otherwise}, \end{cases}$
- the *coprime* predicate, $\mathsf{coprime}(m, n) \stackrel{\text{def}}{=} \begin{cases} \mathit{true} & \text{if } \mathsf{gcd}(m, n) = 1, \\ \mathit{false} & \text{otherwise}, \end{cases}$

Exercise 1. The constant 0 is first-order definable in the structure $(\mathbb{N}; <)$. □

Solution for Exercise 1: The constant "0" is first-order definable in $(\mathbb{N}; <)$ by the wff $\varphi_{\{0\}}(x)$:

$$\varphi_{\{0\}}(x) \stackrel{\text{def}}{=} \forall y\,(x \approx y \vee x < y)$$

Exercise 2. The successor function $\mathsf{succ} : \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; <)$. □

Solution for Exercise 2: "$\mathsf{succ}(x) = y$" is first-order definable in $(\mathbb{N}; <)$ by the wff $\varphi_{\mathsf{succ}}(x, y)$:

$$\varphi_{\mathsf{succ}}(x, y) \stackrel{\text{def}}{=} (x < y) \wedge \forall z\,\big(x < z \to (y \approx z \vee y < z)\big) \wedge \forall z\,\big(z < y \to (z \approx x \vee z < x)\big)$$

The wff $\varphi_{\mathsf{succ}}(x, y)$ is the conjunction of three sub-wff's. Can you simplify it to two sub-wff's?

Exercise 3. Every finite subset $X \subseteq \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; <)$.

Hint: Use $\varphi_{\{0\}}$ from Exercise 1 and φ_{succ} from Exercise 2. □

Exercise 4. The order predicate $< : \mathbb{N} \times \mathbb{N} \to \{true, false\}$ is first-order definable in $(\mathbb{N}; +, 0)$. □

Solution for Exercise 4: "$x < y$" is first-order definable in $(\mathbb{N}; +, 0)$ by the wff $\varphi_{<}(x, y)$:

$$\varphi_{<}(x, y) \stackrel{\text{def}}{=} \exists z\,(\neg(z \approx 0) \wedge (x + z \approx y))$$

Exercise 5. The monus operation $\dot{-} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; +, 0)$. □

Solution for Exercise 5: "$x \dot{-} y = z$" is first-order definable in $(\mathbb{N}; +, 0)$ by the wff $\varphi_{\dot{-}}(x, y, z)$:

$$\varphi_{\dot{-}}(x, y, z) \stackrel{\text{def}}{=} (\varphi_{<}(x, y) \to z \approx 0) \wedge (\neg\varphi_{<}(x, y) \to x \approx y + z)$$

Note that $\varphi_{\dot{-}}(x, y, z)$ uses $\varphi_{<}(x, y)$ from Exercise 4.

Exercise 6. The operation $\mathsf{lcm} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; |, +, 0)$. □

Solution for Exercise 6: "$\mathsf{lcm}(x, y) = v$" is first-order definable in $(\mathbb{N}; |, +, 0)$ by the wff $\varphi_{\mathsf{lcm}}(x, y, v)$:

$$\varphi_{\mathsf{lcm}}(x, y, v) \stackrel{\text{def}}{=} (x|v) \wedge (y|v) \wedge \forall w\,\Big((x|w) \wedge (y|w) \to \big(v \approx w \vee \varphi_{<}(v, w)\big)\Big)$$

Note that $\varphi_{\mathsf{lcm}}(x, y, z)$ uses $\varphi_{<}(x, y)$ from Exercise 4, and $\varphi_{<}(x, y)$ is first-order definable using only $\{+, 0\}$ and, therefore, can be interpreted in the structure $(\mathbb{N}; |, +, 0)$. A somewhat shorter definition of $\varphi_{\mathsf{lcm}}(x, y, v)$, which does not use $\varphi_{<}(x, y)$ and uses only $\{\,|\,\}$, is the following:

$$\varphi'_{\mathsf{lcm}}(x, y, v) \stackrel{\text{def}}{=} \forall w\,\big((x|w) \wedge (y|w) \leftrightarrow (v|w)\big)$$

Exercise 7. The operation $\mathsf{gcd} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; |, +, 0)$. □

Solution for Exercise 7: Similar to the solution for Exercise 6. Details omitted.

Exercise 8. The predicate $\mathsf{perfectSq} : \mathbb{N} \to \{true, false\}$ is first-order definable in $(\mathbb{N}; |, +, 0)$.

Hint: $x = y^2$ iff $x + y = \mathsf{lcm}(y, y + 1)$.[1] □

[1] If you want to know the justification for the hint (which you do not need in order to answer the question correctly), here it is: Given an arbitrary natural number y, we have $\mathsf{gcd}(y, y + 1) = 1$, which is easy to prove (try it!). Another fact is that for every natural numbers m and n, we have that $\mathsf{gcd}(m, n) \times \mathsf{lcm}(m, n) = m \times n$ (again very easy to prove, try it!). Hence $\mathsf{lcm}(y, y + 1) = y \times (y + 1) = y^2 + y$. Hence, if $x = y^2$ then $x + y = \mathsf{lcm}(y, y + 1)$ – and conversely, if $x + y = \mathsf{lcm}(y, y + 1)$ then $x = y^2$.

Solution for Exercise 8: To take advantage of the hint, first show that "$\mathsf{perfectSq}(x)$" is first-order definable in $(\mathbb{N}; |, \mathsf{succ}, +, 0)$ by the wff $\varphi'_{\mathsf{perfectSq}}(x)$:

$$\varphi'_{\mathsf{perfectSq}}(x) \stackrel{\text{def}}{=} \exists y\, \varphi'_{\mathsf{lcm}}\big(y, \mathsf{succ}(y), x+y\big)$$

which uses $\varphi'_{\mathsf{lcm}}(x,y,z)$ from Exercise 6. Next, we remove succ in $\varphi'_{\mathsf{perfectSq}}(x)$, using $\varphi_{\mathsf{succ}}(x,y)$ from Exercise 2 to obtain $\varphi''_{\mathsf{perfectSq}}(x)$:

$$\varphi''_{\mathsf{perfectSq}}(x) \stackrel{\text{def}}{=} \exists y\, \exists z\, \Big(\varphi_{\mathsf{succ}}(y,z) \wedge \varphi'_{\mathsf{lcm}}\big(y, z, x+y\big)\Big)$$

which defines "$\mathsf{perfectSq}(x)$" in $(\mathbb{N}; <, |, +, 0)$, which includes "$<$" among the underlying relations because φ_{succ} is written in a signature that includes "$<$" according to Exercise 2, and we need to get rid of it. Fortunately, "$<$" is definable in $(\mathbb{N}; +, 0)$ by the first-order wff $\varphi_<$ according to Exercise 4. Hence, we can write for the desired $\varphi_{\mathsf{perfectSq}}(x)$:

$$\varphi_{\mathsf{perfectSq}}(x) \stackrel{\text{def}}{=} \exists y\, \exists z\, \Big(\varphi'_{\mathsf{succ}}(y,z) \wedge \varphi'_{\mathsf{lcm}}\big(y, z, x+y\big)\Big) \qquad \text{where}$$

$$\varphi'_{\mathsf{succ}}(x) \stackrel{\text{def}}{=} \varphi_<(x,y) \wedge \forall z\, \big(\varphi_<(x,z) \to (y \approx z \vee \varphi_<(y,z))\big) \wedge \forall z\, \big(\varphi_<(z,y) \to (z \approx x \vee \varphi_<(z,x))\big)$$

which can indeed be interpreted in the stucture $(\mathbb{N}; |, +, 0)$.

Exercise 9. Show that the multiplication operation $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; |, +, 0)$.

Hint: $x \times y = z$ iff $4z = (x+y)^2 - (x-y)^2$. □

Solution for Exercise 9: First show that "$x \times y = z$" is first-order definable in $(\mathbb{N}; |, \mathsf{succ}, +, 0)$ by the wff $\varphi'_{\times}(x,y,z)$:

$$\begin{aligned}
\varphi'_{\times}(x,y,z) \stackrel{\text{def}}{=} \exists v \exists w\, \Big(& \varphi_{\dot{-}}(v, w, z+z+z+z) && (i.e.,\ 4z = v - w)\\
& \wedge\ \varphi_{\mathsf{lcm}}\big(x+y, \mathsf{succ}(x+y), x+y+v\big) && (i.e.,\ v = (x+y)^2)\\
& \wedge\ \exists u \Big(\varphi_{-}(x,y,u) \wedge \varphi_{\mathsf{lcm}}\big(u, \mathsf{succ}(u), u+w\big)\Big)\Big) && (i.e.,\ w = u^2 = (x-y)^2)
\end{aligned}$$

which uses $\varphi_{\dot{-}}(x,y,z)$ from Exercise 5 once, and $\varphi_{\mathsf{lcm}}(x,y,z)$ from Exercise 6 twice. But we are not done yet, because the desired $\varphi_{\times}(x,y,z)$ should not use succ. Fortunately, there is a first-order wff $\varphi'_{\mathsf{succ}}(x)$ which defines succ using only $\{+, 0\}$, as shown in the solution for Exercise 8 . . . . Remaining details omitted.

Exercise 10. Show that the predicate $\mathsf{prime} : \mathbb{N} \to \{true, false\}$ is first-order definable in the structure $(\mathbb{N}; |, +, 0)$. □

Exercise 11. Show the predicate $\mathsf{coprime} : \mathbb{N} \times \mathbb{N} \to \{true, false\}$ is first-order definable in the structure $(\mathbb{N}; |, +, 0)$. □

Exercise 12. Show that addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is first-order definable in the structure $(\mathbb{N}; <, \times)$.

Hint: Use the following equivalence for all $m, n, p \in \mathbb{N}$:

$$\Big((p = 0) \text{ or } (p = m+n)\Big) \quad \text{iff} \quad (m \times p + 1) \times (n \times p + 1) = p^2 \times (m \times n + 1) + 1$$

more simply written as $\Big((p = 0) \text{ or } (p = m+n)\Big)$ iff $(m \cdot p + 1) \cdot (n \cdot p + 1) = p^2 \cdot (m \cdot n + 1) + 1$. □