Natural Typesetting of $\mathbb{N}$aproche Formalizations (Un)hiding Information in a proof of Euclid's Theorem

Tim Lichtnau

31.07.2021

Situation

Goals:

1. Verifiability: Use the same `*.ftl.tex`-code for LaTeX and $\mathbb{N}$aproche
2. Legibility: clear, readable PDF-File

Problem:

$\mathbb{N}$aproche can't reconstruct parameters from the context.
Example: $x \cdot y$ indicates the multiplication of the group (monoid, magma etc.), that contains x and y. Obvious parameters distract the reader:

$$\begin{aligned} 0_R &= (0_R \cdot_R x) \text{-}_R\, (0_R \cdot_R x) \\ &= ((0_R +_R 0_R) \cdot_R x) \text{-}_R\, (0_R \cdot_R x) \\ &= ((0_R \cdot_R x) +_R (0_R \cdot_R x)) \text{-}_R\, (0_R \cdot_R x) \\ &= (0_R \cdot_R x) +_R ((0_R \cdot_R x) \text{-}_R\, (0_R \cdot_R x)) \\ &= (0_R \cdot_R x) +_R 0_R. \end{aligned}$$

Binary operation on a magma M

- in LaTeX:

```
\newcommand{\gdot}[1]{\cdot_{#1}}
```

- In $\mathbb{N}$aproche:

  Signature

  Let $x, y \in |M|$. $x \cdot_M y$ is an element of $|M|$.

In the source code:

```
x \gdot{M} y
```

Hiding the obvious variable M

- in LaTeX:

```
\newcommand{\gdot}[1]{\cdot}
```

  (Still a unary function!)

- In $\mathbb{N}$aproche:

  Signature

  Let $x, y \in |M|$. $x{\cdot}y$ *is an element of* $|M|$.

Other Information to omit

- Forgetting Structure
  $\mathbb{N}$aproche internally distinguishes between a structure M and its underlying set $|M|$.

  Definition
  M is associative iff $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in M$.

Other Information to omit

- Forgetting Structure
  $\mathbb{N}$aproche internally distinguishes between a structure M and its underlying set $|M|$.

  Definition
  M is associative iff $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in M$.

  Domain and target have to be clear from the context!

Other Information to omit

- Forgetting Structure
  $\mathbb{N}$aproche internally distinguishes between a structure M and its underlying set $|M|$.

  Definition
  M is associative iff $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in M$.

  Domain and target have to be clear from the context!

- Relations

  Let O denote a order.

  Definition
  Let $N \subseteq O$. An upper bound of N by O is an element x of O such that $n \leq x$ for all $n \in N$.

Unhide the Information?

ambiguity while reading?
$\rightarrow$ No need to look up the `*.ftl.tex`-file! Tooltips can help.

Unhide the Information?

ambiguity while reading?
$\rightarrow$ No need to look up the `*.ftl.tex`-file! Tooltips can help.
Example:

Definition
$|$ is an order on M such that for any $x, y \in M$ we have $x|y$ iff x divides y in M .

...

Signature
$\mathbb{N}_{>0}$ *is a submonoid of* $\mathrm{Mu}(\mathbb{Z})$.

...

Lemma
$|$ *is a partial order.*

An Order-theoretic approach to Euclid's Theorem

Theorem

Let O be a wellfounded partial order. Assume for every element x of O there exists a $y \in O$ such that x and y have no common predecessors by O. Then

$$\{m \in O \mid m \text{ is a minimum of } O\}$$

has no upper bound by O.

Thanks for your attention!

Complete Formalization:
https://github.com/naproche/FLib/tree/master/NumberTheory
(Also in the paper-references)

Contact:

- Peter Koepke : koepke@math.uni-bonn.de
- Jonas Lippert : jlippert@uni-bonn.de
- Tim Lichtnau: s6tilich@uni-bonn.de

Questions?