Why We Need Structured Proofs in Mathematics

Mauricio Ayala-Rincón[†,‡] **Gabriel Silva**[‡]

ayala@unb.br

gabrielfsilva1995@gmail.com

Departments of [†] Mathematics and [‡] Computer Science
Universidade de Brasília

July 30, 2020

Overview

Goal

Making Proofs More Readable

Avoid Writing Wrong Proofs

Additional Considerations and Conclusion

How can I start?

Goal

To present **structured proofs** and argue that they are a **necessary tool** in the toolbox of the 21st century mathematician.

A Tale of Three Mathematicians

Once upon a time, Camilo was writing a proof for two mathematicians:

- Fê - An experienced mathematician who is more interested in "getting the big picture".
- Armandinho - A novice math student who wants to check every detail in a proof.

Camilo, Fê and Armandinho

Figure 1: Camilo*

Figure 2: Fê*

Figure 3: Armandinho*

(*) *Armandinho and his friends*

Characters of the Brazilian cartoonist Alexandre Beck[1]

[1] https://tirasarmandinho.tumblr.com

Can Camilo Please Everyone?

Can Camilo please everyone?

The Traditional Way

If Camilo writes a standard proof (henceforth called a **prose proof**):

- If Camilo writes a **prose proof** and explains only the main steps of it, Armandinho **may not be able to fill the details** by himself.
- If Camilo writes a **prose proof** and provides every tiny detail of it, these **excessive details can cloud** (for Fê and Armandinho) what are the main steps that make the proof work.

Camilo's Theorem

Camilo is writing a proof of the Schroeder-Bernstein Theorem:

Definition (Equipollent Sets)

Two sets A and B are said to be **equipollent** iff there is a one-to-one function on A with range B.

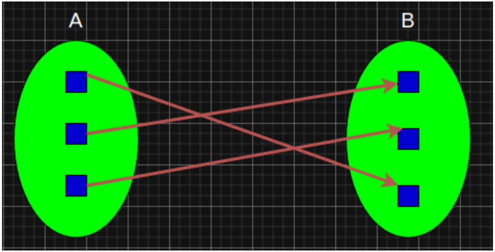

Figure 4: A and B are equipollent

Camilo's Theorem (cont.)

Theorem (Schroeder-Bernstein Theorem)

If there is a one-to-one function on a set A to a subset of a set B and there is also a one-to-one function on B to a subset of A, then A and B are equipollent.

An Example of a Prose Proof

This **prose proof** is from Kelley's book "General Topology" [1]:

> *"PROOF Suppose that f is a one-to-one map of A into B and g is one-to-one on B to A. It may be supposed that A and B are distinct. The proof of the theorem is accomplished by decomposing A and B into classes which are most easily described in terms of parthenogenesis. A point x (of either A or B) is an ancestor of a point y iff y can be obtained from x by successive application of f and g (or g and f). Now decompose A into three sets: let A_E consist of all points of A which have an even number of ancestors, let A_O consists of points which have an odd number of ancestors, and let A_I consist of points with infinitely many ancestors. Decompose B similarly and observe: f maps A_E onto B_O and A_I onto B_I, and g^{-1} maps A_O onto B_E. Hence, the function which agrees with f on $A_E \cup A_I$ and agrees with g^{-1} on A_O is a one-to-one map of A onto B. $\square$"*

Fê and Armandinho's opinion

If Camilo wrote this proof he would not please everyone:

- Fê may be satisfied.
- Armandinho would not be satisfied. He wanted to know why "f maps A_E onto B_O".

Structured Proofs to the Rescue!

Camilo decides to use a **structured proof** as described by Leslie Lamport in [2], [3].

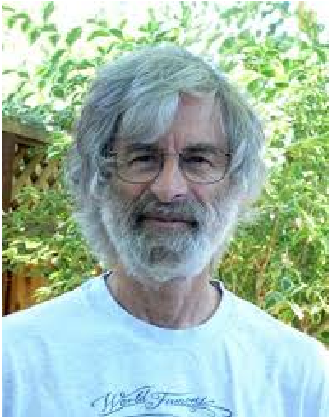

Figure 5: Leslie Lamport

Camilo's Structured Proof

$\langle 1 \rangle 1.$ **Let:** f be a one-to-one map of A into B and g be a one-to-one map of B into A.

$\langle 1 \rangle 2.$ **Case:** A and B are disjoint.

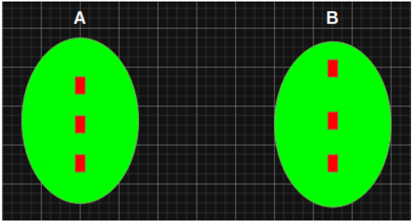

Figure 6: A and B are disjoint

Camilo's Structured Proof (cont.)

$\langle 2 \rangle 1.$ Since f and g are one-to-one we can use without ambiguity the mapping f^{-1} for elements $b \in f(A) \subseteq B$ and the mapping g^{-1} for elements $a \in g(B) \subseteq A$.

$\langle 2 \rangle 2.$ **Let:** $a \in A$. **Define:** $x_0 = a$ as the zeroth ancestor of a. If $x_0 \in g(B)$, **Define:** $x_1 = g^{-1}(x_0)$ as the first ancestor of a. If $x_0 \notin g(B)$, the sequence of ancestors of a is just $\langle x_0 \rangle$. If $x_1 \in f(A)$, **Define:** $x_2 = f^{-1}(x_1)$ as the second ancestor of a. If $x_1 \notin f(A)$, the sequence of ancestors of a is just $\langle x_0, x_1 \rangle$. **Define:** $Anc(a)$ to be the sequence (possibly infinite) of ancestors of a obtained by continuing this process for as long as we can. **Define:** $|Anc(a)|$ as the number of elements (including x_0) in $Anc(a)$.

Camilo's Structured Proof (cont.)

$\langle 2 \rangle 3$. We adapt Step $\langle 2 \rangle 2$ to an element $b \in B$. **Define:** $x_0 = b$ as the zeroth ancestor of b. If $x_0 \in f(A)$, **Define:** $x_1 = f^{-1}(x_0)$ as the first ancestor of b. If $x_0 \notin f(A)$, the sequence of ancestors of b is just $\langle x_0 \rangle$. If $x_1 \in g(B)$, **Define:** $x_2 = g^{-1}(x_1)$ as the second ancestor of b. If $x_1 \notin g(B)$, the sequence of ancestors of b is just $\langle x_0, x_1 \rangle$. **Define:** $Anc(b)$ to be the sequence (possibly infinite) of ancestors of b obtained by continuing this process for as long as we can. **Define:** $|Anc(b)|$ as the number of elements (including x_0) in $Anc(b)$. Since A and B are disjoint (see Step $\langle 1 \rangle 2$), there is no danger of Step $\langle 2 \rangle 2$ and this Step simultaneously defininig, for some $x \in A \cup B$, $Anc(x)$.

Camilo's Structured Proof (cont.)

$\langle 2 \rangle 4.$ **Let:** $A_E = \{a \mid a \in A \text{ and } |Anc(a)| \text{ is even } \}$. **Let:** $A_O = \{a \mid a \in A \text{ and } |Anc(a)| \text{ is odd } \}$. **Let:** $A_I = \{a \mid a \in A \text{ and } |Anc(a)| = \infty\}$. We have $A = A_E \uplus A_O \uplus A_I$.

$\langle 2 \rangle 5.$ Similar to Step $\langle 2 \rangle 4$, we partition B conveniently. **Let:** $B_E = \{b \mid b \in B \text{ and } |Anc(b)| \text{ is even } \}$. **Let:** $B_O = \{b \mid b \in B \text{ and } |Anc(b)| \text{ is odd } \}$. **Let:** $B_I = \{b \mid b \in B \text{ and } |Anc(b)| = \infty\}$. We have $B = B_E \uplus B_O \uplus B_I$.

Camilo's Structured Proof (cont.)

$\langle 2\rangle$6. f maps A_I onto B_I and A_O onto B_E. g^{-1} maps A_E onto B_O.

$\langle 3\rangle$1. f maps A_I onto B_I.

$\langle 4\rangle$1. **Let:** $a \in A_I$. Then, $Anc(a) = \langle x_0 = a, x_1, \ldots\rangle$ is an infinite sequence. By definition, $Anc(f(a)) = \langle f(a), f^{-1}(f(a)) = a = x_0, x_1, \ldots\rangle$, which is also an infinite sequence. Therefore we have $f(a) \in B_I$. We conclude that f maps A_I in B_I.

$\langle 4\rangle$2. **Let:** $b \in B_I$. Then, $Anc(b) = \langle x_0 = b, x_1 = f^{-1}(b), x_2, \ldots\rangle$ is an infinite sequence. **Pick** $a = f^{-1}(b)$. We have $Anc(a) = \langle a = f^{-1}(b) = x_1, x_2, \ldots\rangle$, which is also an infinite sequence. Therefore, $a \in A_I$ with $f(a) = b$. We conclude that the function f maps A_I onto B_I.

Camilo's Structured Proof (cont.)

$\langle 3 \rangle$2. f maps A_O onto B_E.

$\langle 4 \rangle$1. **Let:** $a \in A_O$. Then, $|Anc(a)| = 2k+1$, with $k \in \mathbb{N}$ and $Anc(a)$ is of the form: $\langle x_0 = a, \ldots, x_{2k} \rangle$. By definition, $Anc(f(a)) = \langle f(a), f^{-1}(f(a)) = x_0 = a, \ldots, x_{2k} \rangle$ and we have $|Anc(f(a))| = 2k+2$. Hence, $f(a) \in B_E$ and we conclude that f maps A_O in B_E.

$\langle 4 \rangle$2. **Let:** $b \in B_E$. Then $|Anc(b)| = 2k$, with $k \in \mathbb{N}^*$ and $Anc(b)$ is of the form: $\langle x_0 = b, x_1 = f^{-1}(b), \ldots, x_{2k-1} \rangle$. **Pick** $a = f^{-1}(b)$. Then, $Anc(a) = \langle x_1 = a = f^{-1}(b), \ldots, x_{2k-1} \rangle$, $|Anc(a)| = 2k-1$ and hence $a \in A_O$ with $f(a) = b$. We conclude that f maps A_O onto B_E.

Camilo's Structured Proof (cont.)

$\langle 3\rangle 3.$ g^{-1} maps A_E onto B_O.

$\langle 4\rangle 1.$ We can apply g^{-1} to every element a of A_E. That's because $|Anc(a)|$ is even and therefore, a has at least a first ancestor. According to $\langle 2\rangle 2$, this is only the case if $a \in g(B)$ and in this case we can apply g^{-1} to a.

$\langle 4\rangle 2.$ **Let:** $a \in A_E$. We have $|Anc(a)| = 2k$, with $k \in \mathbb{N}^*$ and $Anc(a)$ is of the form: $\langle x_0 = a, x_1 = g^{-1}(a), \ldots, x_{2k-1}\rangle$. By definition, $Anc(g^{-1}(a)) = \langle g^{-1}(a) = x_1, \ldots, x_{2k-1}\rangle$ and we have $|Anc(g^{-1}(a))| = 2k - 1$. Hence, $g^{-1}(a) \in B_O$. We conclude that the function g^{-1} maps A_E in B_O.

$\langle 4\rangle 3.$ **Let:** $b \in B_O$. Then $Anc(b) = \langle x_0 = b, \ldots, x_{2k}\rangle$, with $k \in \mathbb{N}$. **Pick** $a = g(b)$. By definition, $Anc(a) = \langle a, g^{-1}(a) = b = x_0, \ldots, x_{2k}\rangle$, $|Anc(a)| = 2k + 2$ and hence $a \in A_E$ with $g^{-1}(a) = b$. We conclude that the function g^{-1} maps A_E onto B_O.

Camilo's Structured Proof (cont.)

$\langle 2\rangle 7$. **Define:**

$$\phi(x) = \begin{cases} f(x) & \text{if } x \in A_I \cup A_0 \\ g^{-1}(x) & \text{if } x \in A_E \end{cases}$$

Then, ϕ is a one-to-one function on A with range B.

That's because of Step $\langle 2\rangle 6$ and the fact that $A = A_E \uplus A_O \uplus A_I$ and $B = B_E \uplus B_O \uplus B_I$.

$\langle 2\rangle 8$. A and B are equipollent.

By Step $\langle 2\rangle 7$ and the definition of equipollent sets.

Camilo's Structured Proof (cont.)

$\langle 1 \rangle 3.$ **Case:** A and B are not disjoint.

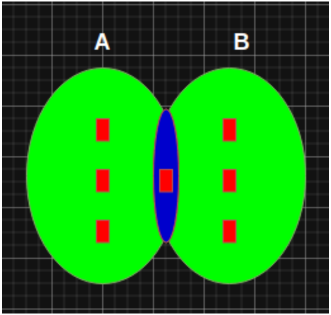

Figure 7: A and B are not disjoint

Camilo's Structured Proof (cont.)

$\langle 2\rangle 1.$ If A and B are not disjoint, **Let:** $B' = \{A\} \times B$. B' is disjoint from A.

$\langle 2\rangle 2.$ There is a one-to-one function ϕ_1 on A with range B'.

- $\langle 3\rangle 1.$ There is a one-to-one function f' on A to a subset of B'. There is a one-to-one function g' on B' to a subset of A.
  - $\langle 4\rangle 1.$ **Define:** $f' : A \to B'$ by $f'(a) \mapsto A \times f(a)$.
  - $\langle 4\rangle 2.$ **Define:** $g' : B' \to A$, by $g'(A \times b) \mapsto g(b)$.
- $\langle 3\rangle 2.$ Since A and B' are disjoint, with the mentioned functions f' and g' we can use the proof of Step $\langle 1\rangle 2$ to construct a one-to-one function ϕ_1 on A with range B'.

Camilo's Structured Proof (cont.)

$\langle 2 \rangle 3$. There is a one-to-one function ϕ_2 on B' with range B.
Define: $\phi_2 : B' \to B$ by $\phi_2(A \times b) \mapsto b$.

$\langle 2 \rangle 4$. **Define:** $\phi = \phi_2 \circ \phi_1$. Then ϕ is a one-to-one function from A with range B.

$\langle 2 \rangle 5$. A and B are equipollent
By Step $\langle 2 \rangle 4$ and the definition of equipollent sets.

Fê and Armandinho's opinion

Camilo pleased everyone!

- Fê is satisfied. She just read the main steps of the proof (the ones of the form $\langle 1 \rangle x.$ and $\langle 2 \rangle x.$) and got the idea.
- Armandinho is also satisfied. He, like Fê, initially read the main steps of the proof to get the idea. Then, he read the substeps and justifications to fully understand every detail that makes the proof work.

Avoid Writing Wrong Proofs

Structured proofs, when combined with the discipline of **justifying carefully** and in detail every step of the proof, **makes it harder to prove things that are not true**.

Even Great Mathematicians Can Get It Wrong

In [3], Leslie Lamport notes that **Kelley's proof contains an error**.

Kelley (see [1]) attributes the form of the proof to G.Birkhoff and S. MacLane:

> *"The intuitively elegant form of the proof of theorem 0.20 is due to G.Birkhoff and S. MacLane".*

The Error in Kelley's Proof

The error in the proof is in the affirmation:

> *"f maps A_E onto B_O"*

since **it does not take into account the possibility of cycles**. For instance, if we have a such that its ancestors are $f(a)$ and $g(f(a)) = a$, the ancestors of $f(a)$ are also just a and $f(a)$.

There is a similar error in the affirmation:

> *"g^{-1} maps A_O onto B_E."*

Additional Considerations

Check Appendix.

Conclusion

Structured Proofs are a **better** way of writing mathematical proofs than **prose proofs**. If the writer mantains a discipline of carefully justifying each step, they also **make it harder to prove things that are not true**.

We believe structured proofs are a **necessary tool** in the toolbox of the mathematician of the 21st century.

How can I start?

1. Read **Leslie Lamport's articles** on the topic: [2] and [3].
2. No need to begin with a computer program, start with the **pf2** LaTeX package.

Thank You

Thank you! Any doubts? [2]

[2] If you want, check other works from us at: https://www.mat.unb.br/ayala/ and https://github.com/gabriel951/my_work

Bibliography

[1] J. L. Kelley, *General topology*. 1975.

[2] L. Lamport, “How to write a 21st century proof,” *J. of Fixed Point Theory and Applications*, vol. 11, no. 1, pp. 43–63, 2012.

[3] L. Lamport, “How to write a proof,” *The American math. monthly*, vol. 102, no. 7, pp. 600–608, 1995.

Pros And Cons

Pros:

1. Makes the **proof more readable**, as it is possible to add the necessary details without "clouding" what are the main steps of the proof.
2. If combined with the discipline of providing justification in detail, makes it **harder to produce wrong proofs**. The hierarchical structure makes it **easier to spot if you missed a corner case**.
3. Make it **easier for the reviewer** to check if the demonstration is correct.

Pros And Cons (cont.)

Cons:

1. Takes more space.
    - If space is an issue, maybe make the structured proof available in an extended version of the paper.
2. Takes more time to write.
    - Although a carefully constructed structured proof takes more time to write than a sloppy prose proof, the time difference between a writing a good structured proof and writing a good prose proof is not huge.

Structured Proofs vs Interactive Theorem Provers?

- Structured Proofs are **faster to write** and **more readable**.
- The probability of obtaining a wrong proof with an interactive theorem prover (ITP) is **significantly smaller** than obtaining a wrong proof by writing a structured proof.

Structured proofs and ITPs **should not be seen as rivals, but as different tools,** to be used according to the task.