Lurch validates Plato
An Application of Proof Verification Software to Philosophy

Nathan Carter    Kenneth G. Monks*

MAA MathFest, Aug 3, 2018
What is *Lurch*\textsuperscript{1}

*Proof verification software for use in a first course on mathematical proof.*

**Goals:**

- No automated theorem proving—the student should do the work
- No code—user interface must be just like books, notes, PDFs
- Highly Customizable—instructors can tailor it to their own courses

Current release: Version 0.8 for Windows, Mac (lurchmath.org)

\textsuperscript{1} *Lurch* was developed by the authors, with support in part from the National Science Foundation’s Division of Undergraduate Education (grant #0736644).
Lurch is a mathematical word processor.

It has support for math typesetting, such as $\forall x, x \neq 0 \Rightarrow (\exists y, \frac{x}{y} = 1)$.

It also supports various fonts, styles, and images:
**Lurch** is a mathematical word processor.

It has support for math typesetting, such as $\forall x, x \neq 0 \Rightarrow \left( \exists y, \frac{x}{y} = 1 \right)$.

It also supports various fonts, *styles*, and images:
Lurch is a mathematical word processor. It has support for math typesetting, such as \( \forall x, x \neq 0 \Rightarrow (\exists y, \frac{x}{y} = 1) \).

It also supports various fonts, styles, and images:
Theorem: The composition of injections is an injection.

Proof: Assume \( f:A\to B \), \( f \) is injective, \( g:B\to C \), and \( g \) is injective. Then we know both \( g\circ f:A\to C \) and \( \forall x, (g\circ f)(x) = g(f(x)) \), because that's what function composition means when \( f:A\to B \) and \( g:B\to C \).

Let \( x \) and \( y \) be arbitrary elements of \( A \). From \( \forall x, (g\circ f)(x) = g(f(x)) \), we obtain both \( (g\circ f)(x) = g(f(x)) \) and \( (g\circ f)(y) = f(f(y)) \), by the definition of the quantifier \( \forall \).
**Theorem:** The composition of injections is an injection.

**Proof:**

Assume $f:A \rightarrow B \;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;}
Teaching Mathematical Proof

Definition

A *proof* is an **explanation** of why a statement must be **objectively correct**.
Formal, Semiformal, and Traditional Proofs

Theorem. \( \forall A, VB, \forall C, A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C. \)

Proof.

1. Let \( A \) be arbitrary
2. Let \( B \) be arbitrary
3. Let \( C \) be arbitrary
4. Assume \( A \subseteq B \text{ and } B \subseteq C \)
5. \( A \subseteq B \) and \( -4 \)
6. \( B \subseteq C \) and \( -4 \)
7. \( A \subseteq B \Leftrightarrow (\forall x, x \in A \Rightarrow x \in B) \) definition of \( \subseteq \)
8. \( B \subseteq C \Leftrightarrow (\forall x, x \in B \Rightarrow x \in C) \) definition of \( \subseteq \)
9. \( A \subseteq B \Rightarrow (\forall x, x \in A \Rightarrow x \in B) \) \( \Leftrightarrow 7 \)
10. \( B \subseteq C \Rightarrow (\forall x, x \in B \Rightarrow x \in C) \) \( \Leftrightarrow 8 \)
11. \( \forall x, x \in A \Rightarrow x \in B \) \( \Leftrightarrow 5, 9 \)
12. \( \forall x, x \in B \Rightarrow x \in C \) \( \Leftrightarrow 6, 10 \)
13. Let \( a \) be arbitrary
14. Assume \( a \in A \)
15. \( a \in A \Rightarrow a \in B \) \( V+; 11 \)
16. \( a \in B \) \( \Rightarrow 14, 15 \)
17. \( a \in B \Rightarrow a \in C \) \( V+; 12 \)
18. \( a \in C \) \( \Rightarrow 16, 17 \)
19. \( \Rightarrow - \)
20. \( a \in A \Rightarrow a \in C \) \( \Rightarrow 14, 18 \)
21. \( \Rightarrow - \)
22. \( \forall x, x \in A \Rightarrow x \in C \) \( V+; 13, 20 \)
23. \( A \subseteq C \Rightarrow (\forall x, x \in A \Rightarrow x \in C) \) definition of \( \subseteq \)
24. \( (\forall x, x \in A \Rightarrow x \in C) \Rightarrow A \subseteq C \) \( \Rightarrow 23 \)
25. \( A \subseteq C \) \( \Rightarrow 22, 24 \)
26. \( \Rightarrow - \)
27. \( A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C \) \( \Rightarrow 4, 25 \)
28. \( \Rightarrow - \)
29. \( \forall C, A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C \) \( V+; 3, 27 \)
30. \( \Rightarrow - \)
31. \( \forall B, \forall C, A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C \) \( V+; 3, 29 \)
32. \( \Rightarrow - \)
33. \( \forall A, VB, \forall C, A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C \) \( V+; 3, 31 \)

Semiformal Proof

Theorem. For all \( A, B, \) and \( C, \) if \( A \subseteq B \text{ and } B \subseteq C \) then \( A \subseteq C. \)

Proof.

Let \( A, B, \) and \( C \) be arbitrary.

Assume \( A \subseteq B \text{ and } B \subseteq C \)

Let \( a \in A \) be arbitrary.

\( a \in B \) since \( a \in A \text{ and } A \subseteq B \)

\( a \in C \) since \( a \in B \text{ and } B \subseteq C \)

\( A \subseteq C \) since every \( a \in A \) is in \( C \)

If \( A \subseteq B \text{ and } B \subseteq C \) then \( A \subseteq C. \)

Traditional Proof

Theorem. The subset relation is transitive.

Proof. By the definition of transitivity, we wish to show that for any sets \( A, B, \) and \( C, \) if \( A \subseteq B \text{ and } B \subseteq C \) then \( A \subseteq C. \)

To do so, suppose \( A, B, \) and \( C \) are sets for which \( A \subseteq B \text{ and } B \subseteq C. \) Let \( a \) be an arbitrary element of \( A. \) Then since \( A \subseteq B \) we have \( a \in B. \) Therefore, since \( B \subseteq C \) we also have \( a \in C. \)

Since \( a \in A \) was chosen to be arbitrary, it follows that every element in \( A \) is an element of \( C, \) and hence \( A \subseteq C, \) as desired.
**Theorem.** \( \forall A, \forall B, \forall C, A \subseteq B \) and \( B \subseteq C \) \( \Rightarrow \) \( A \subseteq C \).

**Proof.**

1. Let \( A \) be arbitrary
2. Let \( B \) be arbitrary
3. Let \( C \) be arbitrary
4. Assume \( A \subseteq B \) and \( B \subseteq C \)
5. \( A \subseteq B \) and -; 4
6. \( B \subseteq C \) and -; 4
7. \( A \subseteq B \leftrightarrow (\forall x, x \in A \Rightarrow x \in B) \) definition of \( \subseteq \)
8. \( B \subseteq C \leftrightarrow (\forall x, x \in B \Rightarrow x \in C) \) definition of \( \subseteq \)
9. \( A \subseteq B \Rightarrow (\forall x, x \in A \Rightarrow x \in B) \leftrightarrow-; 7 

Formal Proof
Theorem. For all $A$, $B$, and $C$, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.  

Proof. 

Let $A$, $B$, and $C$ be arbitrary. 

Assume $A \subseteq B$ and $B \subseteq C$ 

Let $a \in A$ be arbitrary. 

$a \in B$ since $a \in A$ and $A \subseteq B$  

$a \in C$ since $a \in B$ and $B \subseteq C$  

$A \subseteq C$ since every $a \in A$ is in $C$  

If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. 

Semiformal Proof
**Theorem.** The subset relation is transitive.

**Proof.** By the definition of transitivity, we wish to show that for any sets $A$, $B$, and $C$, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

To do so, suppose $A$, $B$, and $C$ are sets for which $A \subseteq B$ and $B \subseteq C$. Let $a$ be an arbitrary element of $A$. Then since $A \subseteq B$ we have $a \in B$. Therefore, since $B \subseteq C$ we also have $a \in C$.

Since $a \in A$ was chosen to be arbitrary, it follows that every element in $A$ is an element of $C$, and hence $A \subseteq C$, as desired. \(\square\)
An Unexpected Email

“Dr. Monks,

I have to give a philosophy presentation on Thursday, and I wanted to write up something close to a formalization of an argument in a Platonic dialogue. Naturally, I turned to Lurch. I have the first one attached. (It’s a little rough around the edges.)

Be proud.

-Don Vispi”
Proof that the parts of virtue have at least one similar quality

1. Assume \((\forall x)(\forall y)((x \text{ is a part of virtue } \land y \text{ is a part of virtue } \land x \neq y) \Rightarrow \neg(\exists z)(x \text{ is } z \land y \text{ is } z))\)
2. Piety is a part of virtue.
3. Justice is a part of virtue.
4. Piety is justice.
5. (Piety is a part of virtue \land justice is a part of virtue \land piety \neq justice) \Rightarrow \neg(\exists z)(\text{piety is } z \land \text{justice is } z)
6. \neg(\exists z)(\text{piety is } z \land \text{justice is } z)
7. Piety is pious.
8. Justice is just.
9. Justice is pious \lor \neg(\text{justice is pious}).
10. Justice is pious.
11. Piety is pious and justice is pious.
12. (\exists z)(\text{piety is } z \land \text{justice is } z)
13. \neg\neg
14. (\forall x)(\forall y)((x \text{ is a part of virtue } \land y \text{ is a part of virtue } \land x \neq y) \Rightarrow \neg(\exists z)(x \text{ is } z \land y \text{ is } z))
“... And suppose that some one were to ask us, saying, ”O Protagoras, and you, Socrates, what about this thing which you were calling justice, is it just or unjust?”-and I were to answer, just: would you vote with me or against me?

With you, he said.

Thereupon I should answer to him who asked me, that justice is of the nature of the just: would not you?

Yes, he said. ...”
Proof that the parts of virtue have at least one similar quality

1. Assume $(\forall x)(\forall y)((x \text{ is a part of virtue } \land y \text{ is a part of virtue } \land x \neq y) \Rightarrow \neg(\exists z)(x \text{ is } z \land y \text{ is } z))$
2. Piety is a part of virtue.
3. Justice is a part of virtue.
4. Piety$\Rightarrow$Justice.
5. $(\text{piety is a part of virtue } \land \text{ justice is a part of virtue } \land \text{ piety} \neq \text{ justice}) \Rightarrow \neg(\exists z)(\text{piety is } z \land \text{ justice is } z)$
6. $\neg(\exists z)(\text{piety is } z \land \text{ justice is } z)$
7. Piety is pious.
8. Justice is just.
9. Justice is pious $\lor$ $\neg$(justice is pious).
10. Justice is pious.
11. Piety is pious and justice is pious.
12. $(\exists z)(\text{piety is } z \land \text{ justice is } z)$
13. $\equiv$
14. $(\forall x)(\forall y)((x \text{ is a part of virtue } \land y \text{ is a part of virtue } \land x \neq y) \Rightarrow \neg(\exists z)(x \text{ is } z \land y \text{ is } z))$

Admitted by Protagoras
Admitted by Protagoras
Admitted by Protagoras
By universal instantiation and substitution (1, 2, 3, 4)
By modus ponens (5, 2, 3, 4)
Admitted by Protagoras
Admitted by Protagoras
By law of the excluded middle
Admitted by Protagoras
By conjunction
By existential generalization
By contradiction (6, 12)
By reductio ad absurdum
Preliminary Definitions

We declare the following concepts as logical constants:

- PartOfVirtue
- Piety
- Justice
- pious
- just

In addition to the usual rules of inference for logic we define one additional rule of inference as follows.

Admitted by Protagoras Rule:
- Conclude: Piety is PartOfVirtue
- Conclude: Justice is PartOfVirtue
- Conclude: not (Piety = Justice)
- Conclude: Justice is pious
- Conclude: Piety is pious
- Conclude: Justice is just
And the proof is ...

**Theorem:** It is not the case that all distinct parts of virtue have no similar quality.

**Proof.**
1. Assume $\forall x, \forall y, ((x \text{ is a PartOfVirtue}) \text{ and } (y \text{ is a PartOfVirtue})) \text{ and } x = y \Rightarrow \neg \exists z, (x \text{ is } z) \text{ and } (y \text{ is } z)$
2. Piety is a PartOfVirtue.
3. Justice is a PartOfVirtue.
4. $(\neg \text{ Piety is a PartOfVirtue}) \text{ and } (\neg \text{ Justice is a PartOfVirtue})$
5. $\neg \text{ Piety = Justice}.$
6. $(\neg \text{ Piety is a PartOfVirtue}) \text{ and } (\neg \text{ Justice is a PartOfVirtue}) \text{ and } \neg \text{ Piety = Justice}$
7. $\forall y, ((\neg \text{ Piety is a PartOfVirtue}) \text{ and } (\neg \text{ Justice is a PartOfVirtue}) \text{ and } \neg \text{ Piety = y} \Rightarrow \neg \exists z, (\neg \text{ Piety is } z) \text{ and } (\neg \text{ Justice is } z)$
8. Justice is just.
9. $(\neg \text{ Piety is a PartOfVirtue}) \text{ and } (\neg \text{ Justice is a PartOfVirtue}) \text{ and } \neg \text{ Piety = Justice} \Rightarrow \neg \exists z, (\neg \text{ Piety is } z) \text{ and } (\neg \text{ Justice is } z)$
10. $\neg \exists z, (\neg \text{ Piety is } z) \text{ and } (\neg \text{ Justice is } z)$
11. Piety is pious.
12. Justice is pious.
13. $(\neg \text{ Piety is pious}) \text{ and } (\neg \text{ Justice is pious})$
14. $\exists z, (\neg \text{ Piety is } z) \text{ and } (\neg \text{ Justice is } z)$
15. $\neg \exists z, (\neg \text{ Piety is } z) \text{ and } (\neg \text{ Justice is } z)$
16. $\forall x, \forall y, ((x \text{ is a PartOfVirtue}) \text{ and } (y \text{ is a PartOfVirtue}) \text{ and } x = y \Rightarrow \neg \exists z, (x \text{ is } z) \text{ and } (y \text{ is } z)$

Admitted by Protagoras
Admitted by Protagoras
By and+ (2, 3)
Admitted by Protagoras
By and+ (4, 5)
By $\forall$- (1)
Admitted by Protagoras
By $\forall$- (7)
By modus ponens (6, 9)
Admitted by Protagoras
Admitted by Protagoras
By and+ (11, 12)
By $\exists$- (13)
By contradiction (10, 14)
By not+ (1, 15)
Conclusions and Lessons Learned

- **Motivation:** "Will I ever use this?"
  Perhaps ... if you have sufficient background.
- **Pedagogy:** don’t ignore walking backwards across the bridge.
For further information:

**Lurch (desktop version):** lurchmath.org

**Lurch (web version):** lurchmath.github.io