Foolproof Proof-writing

Nicolas Schank, Nathan Malimban

April 18, 2016
Introduction: High School Lied to You

Who remembers writing proofs like this?

Prove the identity

\[
\cot(x) + \tan(x) = \cos(x) \csc(x)
\]

\[
(\sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x))
\]

\[
= \cot(x) \left( \sin^2(x) \cos^2(x) + \sin^2(x) \sin^2(x) \right)
\]

\[
= \cot(x) (\tan^2(x) + \cos^2(x) + \sin^2(x))
\]

\[
= \tan(x) + \cot(x)
\]

Can you spot any mistakes in this proof?
Who remembers writing proofs like this?

Prove the identity
\[ \cot(x) + \tan(x) = \cos(x) \csc(x) \]
\[ \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right) \]
\[ \cos(x) \csc(x) \]
\[ \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right) \]
\[ (1) \]
\[ \cot(x) \]
\[ \left( \sin^2(x) \cos^2(x) + \sin^2(x) \sin^2(x) \right) \]
\[ \tan(x) + \cot(x) \]
\[ (2) \]
\[ \tan(x) + \cot(x) \]
\[ (3) \]
\[ \tan(x) + \cot(x) \]
\[ (4) \]
Who remembers writing proofs like this?
Prove the identity
$$\cot(x) + \tan(x) = \cos(x) \csc(x) \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right).$$
Who remembers writing proofs like this?

Prove the identity

\[
cot(x) + \tan(x) = \cos(x) \csc(x) \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right).
\]

\[
\begin{align*}
\cos(x) \csc(x) \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right) &\quad (1) \\
= \cot(x) \left( \frac{\sin^2(x)}{\cos^2(x)} + \frac{\sin^2(x)}{\sin^2(x)} \right) &\quad (2) \\
= \cot(x) (\tan^2(x) + \cos^2(x) + \sin^2(x)) &\quad (3) \\
= \tan(x) + \cot(x) &\quad (4)
\end{align*}
\]
Who remembers writing proofs like this?
Prove the identity
\[
cot(x) + \tan(x) = \cos(x) \csc(x) \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right).
\]
\[
cos(x) \csc(x) \left( \sin^2(x) \sec^2(x) + \sin^2(x) \csc^2(x) \right) \quad (1)
\]
\[
= \cot(x) \left( \frac{\sin^2(x)}{\cos^2(x)} + \frac{\sin^2(x)}{\sin^2(x)} \right) \quad (2)
\]
\[
= \cot(x) (\tan^2(x) + \cos^2(x) + \sin^2(x)) \quad (3)
\]
\[
= \tan(x) + \cot(x) \quad (4)
\]
Can you spot any mistakes in this proof?
Introduction: High School Lied to You

Of course you can’t!
Of course you can’t!

Because this isn’t a good proof.
What is a good proof?

Any ideas?
What is a good proof?

Here are some of ours:
What is a good proof?

Here are some of ours:

1. It has to be *clear*. 
What is a good proof?

Here are some of ours:

1. It has to be clear.
2. It has to have good structure.
What is a good proof?

Here are some of ours:

1. It has to be *clear*.
2. It has to have good *structure*.
3. It has to *flow*. 
Outline

1. Structure
2. Clarity
3. Flow
4. One-on-One Feedback
Outline

1. Structure
2. Clarity
3. Flow
4. One-on-One Feedback
Structure: Proofs as Essays

- Start with an outline.
- Group connected ideas into paragraphs.
- Write a first draft, using complete sentences.
- Proofread. (Literally)
Structure: Proofs as Essays

- Start with an outline.
Structure: Proofs as Essays

- Start with an outline.
- Group connected ideas into paragraphs.
Structure: Proofs as Essays

- Start with an outline.
- Group connected ideas into paragraphs.
- Write a first draft, using complete sentences.
Structure: Proofs as Essays

- Start with an outline.
- Group connected ideas into paragraphs.
- Write a first draft, using complete sentences.
- Proofread. (Literally)
Structure: Sentence Structure

Simple sentence structure is generally easier to read. Don't worry about sounding a little formulaic. Use the active voice. Example: It will be proved via contradic... We now prove via contradiction...
Simple sentence structure is generally easier to read.
Structure: Sentence Structure

- Simple sentence structure is generally easier to read.
- Don’t worry about sounding a little formulaic.
Structure: Sentence Structure

- Simple sentence structure is generally easier to read.
- Don’t worry about sounding a little formulaic.
- Use the active voice.
Structure: Sentence Structure

- Simple sentence structure is generally easier to read.
- Don’t worry about sounding a little formulaic.
- Use the active voice.

Example

It will be proved via contradiction...
We now prove via contradiction...
Structure: Sentence Structure

- Simple sentence structure is generally easier to read.
- Don’t worry about sounding a little formulaic.
- Use the active voice.
- Try to only justify one thing per sentence.
Structure: Overall Structure

Some proof types have structure that you can use to your advantage!

- Induction
- Element Method
- Bijections
- Bidirectional Proofs (If and Only If)
Structure: Overall Structure

- Some proof types have structure that you can use to your advantage!
Structure: Overall Structure

- Some proof types have structure that you can use to your advantage!
  - Induction
  - Element Method
  - Bijections
  - Bidirectional Proofs (If and Only If)
Structure: Overall Structure

- Some proof types have structure that you can use to your advantage!
- Avoid using lists inside a proof.
Structure: Overall Structure

- Some proof types have structure that you can use to your advantage!
- Avoid using lists inside a proof.
  The description environment looks nice though!

  **Injectivity**  Proof of the injectivity of $f$ would go here. It nicely aligns the paragraphs within the proof.

  **Surjectivity**  Proof of the surjectivity of $f$ would go here.
Example Proof 1: Problem Statement

Consider the function $f : \mathbb{Z} \rightarrow \mathbb{E}$, $f(x) = 2x$. Prove that $f$ is a bijection.
Example Proof 1: Rough Draft

Proof.
It is necessary to show that \( f \) is surjective and injective, or that \( f(x) \neq f(y) \implies x \neq y \) \( \forall x, y \in \mathbb{Z} \) and that \( \forall y \in \mathbb{E}, \exists x \in \mathbb{Z} \) where \( f(x) = y \). For any \( y \in \mathbb{E} \) that you can think of, by definition of an even number, \( y = 2x \) for some \( x \in \mathbb{Z} \), since every even number can be divided by 2, no matter what. And if \( f(x) \neq f(y) \), then \( 2x \neq 2y \) which would suggest that \( x \neq y \). \( \square \)
Example Proof 1: Polished

Proof.
To prove that $f$ is a bijection, we must show injectivity and surjectivity.

**Injectivity**  Suppose we have $x, y \in \mathbb{Z}$ such that $f(x) \neq f(y)$. Then $2x \neq 2y$, which means $x \neq y$, as needed.

**Surjectivity**  Consider an arbitrary $y \in \mathbb{E}$. By definition of an even number, $y = 2x$ for some $x \in \mathbb{Z}$, as needed.

Thus, $f$ is a bijection.  \qed
Outline

1. Structure
2. Clarity
3. Flow
4. One-on-One Feedback
Introduction: What are you about to do?

Example

To prove a function is odd, we must show...

In order to prove that $R$ is an equivalence relation, we need...
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?

Example

To prove a function is odd, we must show...
Clarity: Keeping the Reader Informed

▶ Introduction: What are you about to do?

**Example**
To prove a function is odd, we must show...
In order to prove that $R$ is an equivalence relation, we need...
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
Introduction: What are you about to do?
Use transitions to indicate your next move.

Example
Thus, we have...
But we recall from earlier that...
Combining this with our result from case 1...
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
- If you use a theorem or nontrivial property to make a step, say so.
Clarity: Keeping the Reader Informed

▶ Introduction: What are you about to do?
▶ Use transitions to indicate your next move.
▶ If you use a theorem or nontrivial property to make a step, say so.

Example

...by the Fundamental Theorem of Arithmetic.
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
- If you use a theorem or nontrivial property to make a step, say so.

Example

...by the Fundamental Theorem of Arithmetic.
By definition of... (Sparingly!)
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
- If you utilize a theorem or nontrivial property to make a step, say so.
- Conclusion: What did you just do?

Example: ...thus we have reached a contradiction. Since we have proven $P(1)$ and have shown $P(k)$ implies $P(k+1)$, we have shown $P(n)$ for all $n \in \mathbb{Z}^+$. 
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
- If you utilize a theorem or nontrivial property to make a step, say so.
- Conclusion: What did you just do?

**Example**

...thus we have reached a contradiction.
Clarity: Keeping the Reader Informed

- Introduction: What are you about to do?
- Use transitions to indicate your next move.
- If you utilize a theorem or nontrivial property to make a step, say so.
- Conclusion: What did you just do?

Example

...thus we have reached a contradiction.
Since we have proven $P(1)$ and have shown $P(k)$ implies $P(k + 1)$, we have shown $P(n)$ for all $n \in \mathbb{Z}^+$. 
Clarity: Notation

▶ Use notation to make your proofs simpler.
▶ Variables (x, S, f) are like abbreviations.
▶ Do not reuse variable names.
▶ Be careful about mixing symbols and words.
▶ Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
▶ Similarly, don’t write “for an element ∈ S”. Be consistent within a given context.
▶ Look out for: ∃ ∀ ∴ ∨ ∧ = ⇒ =

Example: for all x in S ∀ x ∈ S
Use notation to make your proof *simpler*
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables ($x, S, f$) are like abbreviations.
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables \((x, S, f)\) are like abbreviations.
- Do not reuse variable names.
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables \((x, S, f)\) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables (x, S, f) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables ($x, S, f$) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write ”for an element $\in S$”. Be consistent within a given context.
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables \((x, S, f)\) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write ”for an element \(\in S\)”.
    - Be consistent within a given context.
      - Look out for: \(\exists \forall \therefore \lor \land \mid \implies \equiv\)
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables \((x, S, f)\) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write ”for an element \(\in S\). Be consistent within a given context.
    - Look out for: \(\exists \forall :. \lor \land \mid \implies =\)

**Example**

for all \(x\) in \(S\)
Clarity: Notation

- Use notation to make your proof *simpler*
- Variables \((x, S, f)\) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write ”for an element \(\in S\)”.
    - Be consistent within a given context.
      - Look out for: \(\exists \forall :. \lor \land \mid \implies =\)

**Example**

for all \(x\) in \(S\)
\(\forall x \in S\)
Clarity: Notation

- Use notation to make your proof *simpler*.
- Variables (x, S, f) are like abbreviations.
- Do not reuse variable names.
- Be careful about mixing symbols and words.
  - Don’t replace a single word with a single symbol, just like you wouldn’t write “3 + four”.
  - Similarly, don’t write ”for an element ∈ S”. Be consistent within a given context.
- Short notation tips.
Example Proof 2: Problem Statement

Prove that there are infinitely many primes.
Example Proof 2: Rough Draft

Proof.
What if there were only finitely many primes? \( p_1, p_2, \text{ through } p_n \) is the finite list of all these primes.

\[
Q = p_1 p_2 \cdots p_n + 1
\]

If \( Q \) is prime, then \( Q \) is greater than \( p_i = Q \) is not \( \in \) the list of primes. \( \Rightarrow \Leftarrow \). If \( Q \) is not prime then \( p_i \mid Q \) and \( p_i \) divides \( p_1 p_2 \cdots p_n \). \( p_i \) doesn’t divide 1. \( Q - p_1 p_2 \cdots p_n = 1 \). \( \Rightarrow \Leftarrow \) \( \square \)
Proof.
Assume for the sake of contradiction that there are finitely many primes. Let $P = \{p_1, p_2, \ldots, p_n\}$ be the set of all primes. Now, let us consider $Q = p_1 p_2 \cdots p_n + 1$. We aim to show that $Q$ can be neither prime nor composite. We consider the two cases:

**Prime** Suppose $Q$ is prime. But $Q > p_i \; \forall \; i$, meaning that $Q \notin P$. This contradicts our definition of $P$.

**Composite** Suppose $Q$ is not prime; by the Fundamental Theorem of Arithmetic, $Q$ can be factored into primes. Consider $p_i$, one of these prime factors. Since $p_i | Q$ and $p_i | p_1 p_2 \cdots p_n$, we know that $p_i | (Q - p_1 p_2 \cdots p_n)$. But $Q - p_1 p_2 \cdots p_n = 1$, meaning that $p_i | 1$. This is a contradiction.

Thus, we have proven that there cannot be finitely many primes.
Outline

1. Structure
2. Clarity
3. Flow
4. One-on-One Feedback
You do not need to restate definitions.

Example:
We are given that $B_1, \ldots, B_k$ partitions $U$ into distinct blocks such that every element in $U$ is in some block.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.

**Example**

We are given that $B_1, \ldots, B_k$ partitions $U$ into distinct blocks such that every element in $U$ is in some block.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.

Example

...it is a bijection. Because it is surjective...
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.

**Example**

...it is a bijection. Because it is surjective...

Recall that $R$ is an equivalence relation. By the transitivity of $R$...
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.
- Level of justification depends on context.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.
- Level of justification depends on context.
- Examples are rarely very useful.
Flow: Avoiding Redundancy

- You do not need to *restate* definitions.
- Exception: Recalling an earlier proven point or citing a sub-result out of context.
- Level of justification depends on context.
- Examples are rarely very useful.
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
- Consider...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
- Consider...
- Recall...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
- Consider...
- Recall...
- In particular...
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  - In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
- Consider...
- Recall...
- In particular...
- Without loss of generality (wlog)
Flow: Using Meaningful Transitions

- Hence, thus, therefore.
- We need to show...
  In order to prove...
- It suffices to show...
- ...as needed.
- Suppose...
- Let $x$...
- Consider...
- Recall...
- In particular...
- Without loss of generality (wlog)
- Clearly, obviously, trivially
Example Proof 3: Problem Statement

Consider the following relation on the set of integers:
\( \forall a, b \in \mathbb{Z}, \ (a, b) \in R \) if and only if \( a \) and \( b \) have the same remainder when divided by 3.
Prove that \( R \) is transitive.
Proof.

We know that dividing integers by integers will yield integer remainders, by properties of division. So let \( r_a \) be the remainder when you divide \( a \) by 3. Similarly for \( r_b \) and \( r_c \) with \( b, c \).

Definition of transitivity:

\[
(a, b), (b, c) \in R \implies (a, c) \in R \quad \forall a, b, c \in \mathbb{Z}
\]

so we need this to be true to show transitivity. (e.g. \((1, 2), (2, 3) \in R \implies (1, 3) \in R\).)

Notice \((a, b) \in R \implies r_a = r_b\) and \((b, c) \subseteq R \implies r_b = r_c\) so \(r_a = r_c\).

So \( R \) is transitive because \((a, c) \in R\) for all \((a, b), (bc) \in R\). \(\Box\)
Example Proof 3: Polished

Proof.
For transitivity to hold, we need

$$(a, b), (b, c) \in R \implies (a, c) \in R \quad \forall a, b, c \in \mathbb{Z}.$$ 

Let $r_a$, $r_b$, and $r_c$ be the remainders when you divide $a$, $b$, and $c$ by 3, respectively. Since $(a, b) \in R$, we know that $r_a = r_b$. Since $(b, c) \in R$, we know that $r_b = r_c$. Thus, by the transitivity of equality, we have $r_a = r_c$. By definition of the relation $R$, $(a, c) \in R$, as needed.
Thus, we have shown that $R$ is transitive. \qed
Outline

1. Structure
2. Clarity
3. Flow
4. One-on-One Feedback