Proof Text Evaluation and Comparison Consent Form

You are invited to participate in a research study of what constitutes a good, or bad, proof text. You were selected as a possible participant because of your response to requests for participants in this study. We ask that you read this form and ask any questions you may have before agreeing to be in the study.

Background Information: The purpose of this study is to evaluate the quality and readability of a variety of proof texts. This study is part of a research project to build an automatic system that translates formal, computer-generated proofs into natural language proofs.

Procedures: If you agree to be in this study, we will ask you to do the following: Read a series of proof texts and then answer questions about your perception of their quality. The questionnaire should take about an hour to complete.

Risks and Benefits of being in the Study: We do not anticipate any risks for you participating in this study, other than those encountered in day-to-day life.

There are no direct benefits to you, the subject, in participating, but by gathering this data, we will be able to guide our text generation system towards producing texts which are of greater use to human readers.

Voluntary Nature of Participation: Your decision whether or not to participate will not affect your current or future relations with the University. If you decide to participate, you are free to withdraw at any time without affecting those relationships.

Confidentiality: The records of this study will be kept private. In any sort of report we might publish, we will not include any information that will make it possible to identify you. Research records will be kept in a locked file; only the researchers will have access to the records. Please note that while you are welcome to contact us via e-mail, Internet transmission is neither private nor secure and there is a chance your answers could be read by a third party.

Contacts and Questions: The researcher(s) conducting this study are Amanda Holland-Minkley and Robert Constable. Please ask any questions you have now. If you have questions later, you may contact them at 255-9202, 4116 Upson Hall, hollandm@cs.cornell.edu or 255-9204, 4149 Upson Hall, rc@cs.cornell.edu. If you have an questions or concerns regarding your rights as a subject in this study, you may contact the University Committee on Human Subjects (UCHS) at 5-2943, or access their website at http://www.osp.cornell.edu/Compliance/UCHS/homepageUCHS.htm.

You will be given a copy of this form to keep for your records.

Statement of Consent: I have read the above information, and have received answers to any questions I asked. I consent to participate in the study.

Signature ______________________________ Date ________________________

This consent form was approved by the UCHS on August 27, 2002.

This page intentionally blank.

Proof Text Evaluation and Comparison Study

Return to Upson 4116
or Amanda Holland-Minkley's mailbox

Thank you for taking part in this study to evaluate the quality and readability of a variety of proof texts. This study is part of a research project to build a system that translates formal, computer-generated proofs into a natural language proofs. As part of this project, it is important to look at what readers consider to be good proof texts.

As a participant, you will be asked to read a number of proof texts and answer a variety of questions about them. In order to get an accurate evaluation of these texts, please read them all of the way through, and carefully, before proceeding to the questions. It may help you to read the texts as if you were an instructor reading and evaluating a student's assignment. The intended audience for these texts is an individual who is familiar with the mathematical concepts being used, but wishes to know how to put them together to prove the given theorem.

If you have any questions in the course of completing this survey, feel free to contact me either via e-mail at hollandm@cs.cornell.edu, or in my office at Upson 4116, phone 5-9202. In particular, you are welcome to contact me for clarifications in what you are being asked to do, or explanations of any formal math content appearing in this survey. If at any point you do not wish to continue with the study, feel free to stop, though I would appreciate receiving any portion of the study which you do complete. All materials can be returned to my office or my mailbox in the student mailroom.

Biographical Information

Answers to following questions would be appreciated but are not required. All personal information will be kept strictly confidential, though you may be contacted with follow-up information.

Name ______________________________

E-mail Address ______________________________

Cornell Status (e.g. undergrad, grad student, researcher, etc.) ____________________

What level of mathematics education have you had? ____________________

What level of experience do you have in writing math proofs? ____________________

What level of experience do you have with formal mathematics? ____________________

Part One: Proof Reading

Shown below is a proof of the theorem:

For an integer a and b, it is the case where there exists an integer y where GCD(a;b;y).

Formally: $\forall a,b{:}\mathbb{Z}.\ \exists y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y)$

Your task here is to act as a "grader" for this proof, commenting on possible flaws or improvements. Please read the proof through carefully. Then go back and mark up those aspects of the proof that you would change. Be particularly explicit as to organizational changes you would make, or information which you think was omitted, or was presented badly.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

`gcd_exists_n` == $\forall b{:}\mathbb{N}.\ \forall a{:}\mathbb{Z}.\ \exists y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y)$

`gcd_p_neg_arg_2` == $\forall a,b,y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y) \iff \mathrm{GCD}(a;-b;y)$

Proof:

There are 2 possible cases. In the first case, assume that a is an integer, b is an integer and $0 \leq b$. By the `gcd_exists_n` lemma, we have shown there exists an integer y where GCD(a;b;y). In the second case, assume that a is an integer, b is an integer and $\neg 0 \leq b$. Applying the `gcd_p_neg_arg_2` lemma, we can instead show there exists an integer y where GCD(a;$-b$;y). Applying the `gcd_exists_n` lemma, we have shown there exists an integer y where GCD(a;$-b$;y).

Part One: Proof Reading

Shown below is a proof of the theorem:

For a natural number b and an integer a, it is the case where there exists an integer u and v where GCD(a;b;$u \cdot a + v \cdot b$).

Formally: $\forall b{:}\mathbb{N}.\ \forall a{:}\mathbb{Z}.\ \exists u,v{:}\mathbb{Z}.$ GCD(a;b;$u \cdot a + v \cdot b$)

Your task here is to act as a "grader" for this proof, commenting on possible flaws or improvements. Please read the proof through carefully. Then go back and mark up those aspects of the proof that you would change. Be particularly explicit as to organizational changes you would make, or information which you think was omitted, or was presented badly.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

`comb_for_gcd_p_wf` == $(\boldsymbol{\lambda} a,b,y,z.\mathrm{GCD}(a;b;y)) \in a{:}\mathbb{Z} \to b{:}\mathbb{Z} \to y{:}\mathbb{Z} \to \downarrow\mathrm{True} \to \mathbb{P}_1$

== GCD(a;b;y) is a well-formed proposition over a, b, and y

`gcd_p_zero` == $\forall a{:}\mathbb{Z}.$ GCD(a;0;a)

`quot_rem_exists` == $\forall a{:}\mathbb{Z}.\ \forall b{:}\mathbb{N}^{+}.\ \exists q{:}\ \mathbb{Z}.\ \exists r{:}\mathbb{N}b.\ a = q \cdot b + r$

`gcd_p_sym` == $\forall a,b,y{:}\mathbb{Z}.$ GCD(a;b;y) $\Rightarrow$ GCD(b;a;y)

`gcd_p_shift` == $\forall a,b,y,k{:}\mathbb{Z}.$ GCD(a;b;y) $\Rightarrow$ GCD(a;$b + k \cdot a$;y)

Proof:

We proceed by induction over b. There are 2 possible cases. In the first case, assume $b = 0$. Applying the `comb_for_gcd_p_wf` lemma, we can instead show GCD(a;0;a). From the `gcd_p_zero` lemma, we have shown GCD(a;0;a). In the second case, assume $\neg b = 0$. By applying the `quot_rem_exists` lemma, we know that q is an integer, r is an integer segment and $a = q \cdot b + r$. By simplification, we know that u is an integer, v is an integer and GCD(b;r;$u \cdot b + v \cdot r$). From the `comb_for_gcd_p_wf` lemma, we know GCD(b;r;$b \cdot u + r \cdot v$) and we must show GCD($r + b \cdot q$;b;$b \cdot u + r \cdot v$). Using the `gcd_p_sym` lemma, we can instead show GCD(b;$r + b \cdot q$;$b \cdot u + r \cdot v$). By applying the `gcd_p_shift` lemma, we have shown GCD(b;$r + b \cdot q$;$b \cdot u + r \cdot v$).

Part One: Proof Reading

Shown below is a proof of the theorem:

For the positive natural number r and s, it is the case where

CoPrime(r,s) $\Rightarrow$ ($\forall a$,b:$\mathbb{Z}$. $\exists x$:$\mathbb{Z}$. ($x = a$ mod r) $\wedge$ ($x = b$ mod s)).

Formally: $\forall r$,s:$\mathbb{N}^{+}$. CoPrime(r,s) $\Rightarrow$ ($\forall a$,b:$\mathbb{Z}$. $\exists x$:$\mathbb{Z}$. $x = a$ mod r $\wedge$ $x = b$ mod s)

Your task here is to act as a "grader" for this proof, commenting on possible flaws or improvements. Please read the proof through carefully. Then go back and mark up those aspects of the proof that you would change. Be particularly explicit as to organizational changes you would make, or information which you think was omitted, or was presented badly.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

CoPrime(a,b) == GCD(a;b;1) == a and b are coprime

`gcd_p_sym` == $\forall a$,b,y:$\mathbb{Z}$. GCD(a;b;y) $\Rightarrow$ GCD(b;a;y)

`comb_for_eqmod_wf` == ($\boldsymbol{\lambda} m$,a,b,z.$a = b$ mod m) $\in$ m:$\mathbb{Z} \rightarrow a$:$\mathbb{Z} \rightarrow b$:$\mathbb{Z} \rightarrow \downarrow$True $\rightarrow \mathbb{P}_{\mathbf{1}}$

== $a = b$ mod m is a well-formed proposition over a, b, and m

`eqmod_weakening` == $\forall a$,b:$\mathbb{Z}$. $a = b \Rightarrow$ ($a = b$ mod m)

Proof:

By simplification, we know that r is the positive natural number, s is the positive natural number, a is an integer, b is an integer and CoPrime(r,s) and we must show where $x = a$ mod r and $x = b$ mod s, there exists an integer x where $x = a$ mod r and $x = b$ mod s, There are 2 possible cases. In the first case, assume there exists an integer x where $x = 1$ mod r and $x = 0$ mod s. By simplification, we know GCD(r;s;1) and we must show GCD(s;r;1). From the `gcd_p_sym` lemma, we have shown GCD(s;r;1). In the second case, assume that there exists an integer x where $x = 1$ mod r and $x = 0$ mod s and there exists an integer x where $x = 1$ mod s and $x = 0$ mod r. By simplification, we know that p is an integer, q is an integer, $p = 1$ mod r, $p = 0$ mod s, $q = 1$ mod s and $q = 0$ mod r. There are 2 possible cases. In the first case, we need to show $(a \cdot p + b \cdot q) = a$ mod r. Using the `comb_for_eqmod_wf` lemma, we can instead show $a = a$ mod r. Using the `eqmod_weakening` lemma, we have shown $a = a$ mod r. In the second case, we need to show $(a \cdot p + b \cdot q) = b$ mod s. By the `comb_for_eqmod_wf` lemma, we can instead show $b = b$ mod s. From the `eqmod_weakening` lemma, we have shown $b = b$ mod s.

Part Two: Proof Comparison

Shown below are two accounts of the same approach to the proof of the theorem:

For a natural number b and an integer a, it is the case where there exists an integer y where GCD(a;b;y).

Formally: $\forall b{:}\mathbb{N}.\ \forall a{:}\mathbb{Z}.\ \exists y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y)$

Please read both of the proofs carefully and then answer the questions given below.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

gcd(a;b) == the greatest common divisor of a and b

`comb_for_gcd_p_wf` == $(\boldsymbol{\lambda} a,b,y,z.\mathrm{GCD}(a;b;y)) \in a{:}\mathbb{Z} \to b{:}\mathbb{Z} \to y{:}\mathbb{Z} \to \downarrow\mathrm{True} \to \mathbb{P}_1$

== GCD(a;b;y) is a well-formed proposition over a, b, and y

`gcd_p_zero` == $\forall a{:}\mathbb{Z}.\ \mathrm{GCD}(a;0;a)$

`quot_rem_exists` == $\forall a{:}\mathbb{Z}.\ \forall b{:}\mathbb{N}^{+}.\ \exists q{:}\ \mathbb{Z}.\ \exists r{:}\mathbb{N}b.\ a = q \cdot b + r$

`gcd_p_sym` == $\forall a,b,y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y) \Rightarrow \mathrm{GCD}(b;a;y)$

`add_com` == $\forall a,b{:}\mathbb{Z}.\ a + b = b + a$

`gcd_p_shift` == $\forall a,b,y,k{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y) \Rightarrow \mathrm{GCD}(a;b + k \cdot a;y)$

Proof A: We proceed by induction over b. There are 2 possible cases. In the first case, assume $b = 0$. By the `comb_for_gcd_p_wf` lemma, we can instead show GCD(a;0;a). By the `gcd_p_zero` lemma, we have shown GCD(a;0;a). In the second case, assume $\neg b = 0$. From the `quot_rem_exists` lemma, we know that q is an integer, r is an integer segment and $a = q \cdot b + r$. By simplification, we know there exists an integer y where GCD(b;r;y). By simplification, we know that y is an integer and GCD(b;r;y) and we must show GCD(a;b;y). Using the `gcd_p_sym` lemma, we can instead show GCD(b;$q \cdot b + r$;y). By the `add_com` lemma, we can instead show GCD(b;$r + q \cdot q$;y). Applying the `gcd_p_shift` lemma, we have shown GCD(b;$r + q \cdot b$;y).

Proof B: Proof by strong natural number induction on b. Base: Assume $b = 0$. Show $\forall a{:}\mathbb{Z}.\ \exists y{:}\mathbb{Z}$ such that gcd(a,0) = y by theorem $\forall a{:}\mathbb{Z}.$ gcd(a,0) = a so $y = a$. Induction: Assume $b \in \mathbb{N}$; $b \neq 0$, $a \in \mathbb{Z}$, I.H.: $\forall b_1 < b \Rightarrow (\forall a{:}\mathbb{Z}.\exists y{:}\mathbb{Z}.\ \mathrm{gcd}(a,b_1) = y)$. Then let $q \in \mathbb{Z}$, $r \in \mathbb{N}$ ($r < b$) such that $a = q \cdot b + r$. Since $b \in \mathbb{N} \Rightarrow b \in \mathbb{Z}$, and $r < b$ by the I.H. we have $\exists y{:}\mathbb{Z}.\ \mathrm{gcd}(b,r) = y$. So y = gcd(b,r) = gcd(b,$r + q \cdot b$) [by `gcd_p_shift`] = gcd(b, $q \cdot b + r$) [by additive com.] = gcd(b,a) [since $a = q \cdot b + r$] = gcd(a,b) [by `gcd_p_sym`]. Therefore y exists such that y = gcd(a,b) $\forall a{:}\mathbb{Z}, \forall b{:}\mathbb{N}$.

Questions:

How do these proofs compare on general readability?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on organizational quality?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on ability to express the central proof idea?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

Part Two: Proof Comparison

Shown below are two accounts of the same approach to the proof of the theorem:

For an integer p, it is the case where prime(p) $\Rightarrow$ ($\forall a_1$,a_2:$\mathbb{Z}$. $p \mid a_1 \cdot a_2 \Rightarrow p \mid a_1 \vee p \mid a_2$).

Formally: $\forall p$:$\mathbb{Z}$. prime(p) $\Rightarrow$ ($\forall a_1$,a_2:$\mathbb{Z}$. $p \mid a_1 \cdot a_2 \Rightarrow p \mid a_1 \vee p \mid a_2$)

Please read both of the proofs carefully and then answer the questions given below.

The constructs and lemmas referred to in this proof are:

$b \mid a$ == $\exists c$:$\mathbb{Z}$. $a = b \cdot c$ == b divides a

$a \sim b$ == $a \mid b \wedge b \mid a$

prime(a) == $\neg(a = 0) \wedge \neg(a \sim 1) \wedge (\forall b,c{:}\mathbb{Z}.\ a \mid b \cdot c \Rightarrow a \mid b \vee a \mid c)$ == a is prime

GCD(a;b;c) == the greatest common divisor of a and b is c

CoPrime(a,b) == GCD(a;b;1) == a and b are coprime

`decidable__divides` == $\forall a$,b:$\mathbb{Z}$. Decidable($a \mid b$) == it is decidable if a divides b

`coprime_iff_ndivides` == $\forall a$,p:$\mathbb{Z}$. prime(p) $\Rightarrow$ (CoPrime(p,a) $\iff \neg(p \mid a)$)

Proof A: Assume we have a prime integer p and two integers a_1 and a_2 such that p divides ($a_1 \cdot a_2$). Assume p doesn't divide a_1 or a_2. Then `coprime_iff_ndivides` implies that p and a_1 are coprime and p and a_2 are coprime. But then, by `coprime_prod`, p and $a_1 \cdot a_2$ are coprime so p does not divide $a_1 \cdot a_2$ and we have reached a contradiction. So p must divide one of a_1 or a_2.

Proof B: By simplification, we know that p is an integer, a_1 is an integer, a_2 is an integer, prime(p) and $p \mid a_1 \cdot a_2$ and we must show $p \mid a_1$ or $p \mid a_2$. There are 2 possible cases. In the first case, assume $p \mid a_1$. Therefore, we have shown $p \mid a_1$ or $p \mid a_2$. In the second case, assume $\neg p \mid a_1$. By applying the `decidable__divides` lemma, we know $\neg p \mid a_2$ and we must show $p \mid a_2$. Applying the `coprime_iff_ndivides` lemma, we know that CoPrime(p,a_1) and CoPrime(p,a_2). Using the `coprime_iff_ndivides` lemma, we know that CoPrime(p,$a_1 \cdot a_2$) and $\neg p \mid a_1 \cdot a_2$. Therefore, we have shown $p \mid a_2$.

Questions:

How do these proofs compare on general readability?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on organizational quality?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on ability to express the central proof idea?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

Part Two: Proof Comparison

Shown below are two accounts of the same approach to the proof of the theorem:

For an integer a, b_1 and b_2, it is the case where if CoPrime(a,b_1) then if CoPrime(a,b_2) then CoPrime(a,$b_1 \cdot b_2$).

Formally: $\forall a,b_1,b_2{:}\mathbb{Z}.\ \text{CoPrime}(a,b_1) \Rightarrow \text{CoPrime}(a,b_2) \Rightarrow \text{CoPrime}(a,b_1 \cdot b_2)$

Please read both of the proofs carefully and then answer the questions given below.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

CoPrime(a,b) == GCD(a;b;1) == a and b are coprime

`coprime_bezout_id` == $\forall a,b{:}\mathbb{Z}.\ \text{CoPrime}(a,b) \iff (\exists x,y{:}\mathbb{Z}.\ a \cdot x + b \cdot y = 1)$

`add_mono_wrt_eq` == $\forall a,b,n{:}\mathbb{Z}.\ a = b \iff a + n = b + n$

`mul_functionality_wrt_eq` == $\forall i_1,i_2,j_1,j_2{:}\mathbb{Z}.\ i_1 = j_1 \Rightarrow i_2 = j_2 \ \Rightarrow i_1 \cdot i_2 = j_1 \cdot j_2$

Proof A: Application of the lemma `coprime_bezout_id` to the assumptions and conclusion reduces our task to showing that for some x,y, $a \cdot x + (b_1 \cdot b_2) \cdot y = 1$ assuming that for some x,y, $a \cdot x + b_1 \cdot y = 1$ and that for some x,y, $a \cdot x + b_2 \cdot y = 1$ So by our assumptions there are x_1,y_1,x_2,y_2 such that $a \cdot x_1 + b_1 \cdot y_1 = 1$ and $a \cdot x_2 + b_2 \cdot y_2 = 1$ Adding $(-a \cdot x_1)$ to both sides of the first equation, and adding $(-a \cdot x_2)$ to both sides of the second, then simplifying, gives us **(A)** $b_1 \cdot y_1 = 1 + -a \cdot x_1$ and $b_2 \cdot y_2 = 1 + -a \cdot x_2$ Taking $x_1 + x_2 - a \cdot x_1 \cdot x_2$ and $y_1 \cdot y_2$ as witnesses for x,y of our goal, it is enough to show that $a \cdot (x_1 + x_2 - a \cdot x_1 \cdot x_2) + b_1 \cdot b_2 \cdot y_1 \cdot y_2 = 1$ which, by adding $((1 - a \cdot x_1) \cdot (1 - a \cdot x_2) - 1)$ to both sides and simplifying, further reduces to showing $b_1 \cdot b_2 \cdot y_1 \cdot y_2 = 1 + a \cdot a \cdot x_1 \cdot x_2 + -a \cdot x_1 + -a \cdot x_2$ But this equality is equivalent to multiplying the left-hand sides of the equations of **(A)** above and equating them to the product of the right hand sides, i.e. it follows from **(A)** by the general fact that $i_1 = j_1$ and $i_2 = j_2$ imply $i_1 \cdot i_2 = j_1 \cdot j_2$.

Proof B: By simplification, we know that a is an integer, b_1 is an integer, b_2 is an integer, CoPrime(a,b_1) and CoPrime(a,b_2) and we must show CoPrime(a,$b_1 \cdot b_2$). From the `coprime_bezout_id` lemma, we know that there exists an integer x and y where $a \cdot x + b_1 \cdot y = 1$ and there exists an integer x and y where $a \cdot x + b_2 \cdot y = 1$ and we must show when $a \cdot x + b_1 \cdot b_2 \cdot y = 1$, there exists an integer x and y where $a \cdot x + b_1 \cdot b_2 \cdot y = 1$, By simplification, we know that x_1 is an integer, y_1 is an integer, x_2 is an integer, y_2 is an integer, $a \cdot x_1 + b_1 \cdot y_1 = 1$ and $a \cdot x_2 + b_1 \cdot b_2 \cdot y = 1$. By applying the `add_mono_wrt_eq` lemma, we know that $b_1 \cdot y_1 = 1 + -a \cdot x_1$ and $b_2 \cdot y_2 = 1 + -a \cdot x_2$. By simplification, we can instead show $a \cdot (x_1 + x_2 - a \cdot x_1 \cdot x_2) + b_1 \cdot b_2 \cdot y_1 \cdot y_2 = 1$. By the `add_mono_wrt_eq` lemma, we can instead show $b_1 \cdot b_2 \cdot y_1 \cdot y_2 = 1 + a \cdot a \cdot x_1 \cdot x_2 + -a \cdot x_1 + -a \cdot x_2$. By the `mul_functionality_wrt_eq` lemma, we have shown $b_1 \cdot b_2 \cdot y_1 \cdot y_2 = 1 + a \cdot a \cdot x_1 \cdot x_2 + -a \cdot x_1 + -a \cdot x_2$.

Questions:

How do these proofs compare on general readability?

_______ Proof A is much better than Proof B.
_______ Proof A is slightly better than Proof B.
_______ Proof A and Proof B are about the same.
_______ Proof A is slightly worse than Proof B.
_______ Proof A is much worse than Proof B.

How do these proofs compare on organizational quality?

_______ Proof A is much better than Proof B.
_______ Proof A is slightly better than Proof B.
_______ Proof A and Proof B are about the same.
_______ Proof A is slightly worse than Proof B.
_______ Proof A is much worse than Proof B.

How do these proofs compare on ability to express the central proof idea?

_______ Proof A is much better than Proof B.
_______ Proof A is slightly better than Proof B.
_______ Proof A and Proof B are about the same.
_______ Proof A is slightly worse than Proof B.
_______ Proof A is much worse than Proof B.

Part Two: Proof Comparison

Shown below are two accounts of the same approach to the proof of the theorem:

For a natural number n, it is the case where CoPrime(fib(n),fib($n+1$)).

Formally: $\forall n{:}\mathbb{N}.$ CoPrime(fib(n),fib($n+1$))

Please read both of the proofs carefully and then answer the questions given below.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c

CoPrime(a,b) == GCD(a;b;1) == a and b are coprime

$\text{fib}(n) == \text{the } n^{th} \text{ Fibonacci number} == \begin{cases} 1 & \text{if } n = 0 \text{ or } n = 1 \\ \text{fib}(n-1) + \text{fib}(n-2) & \text{otherwise} \end{cases}$

`gcd_p_one` == $\forall a{:}\mathbb{Z}.$ GCD(a;1;1)

`comb_for_fib_wf` == $(\boldsymbol{\lambda} n,z.\text{fib}(n)) \in n{:}\mathbb{N} \longrightarrow \downarrow\text{True} \longrightarrow \mathbb{N}$

== fib(n) is a well-formed function over n

`comb_for_coprime_wf` == $(\boldsymbol{\lambda} a,b,z.\text{CoPrime}(a,b)) \in a{:}\mathbb{Z} \longrightarrow b{:}\mathbb{Z} \longrightarrow \downarrow\text{True} \longrightarrow \mathbb{P}_{\mathbf{1}}$

== CoPrime(a,b) is a well-formed proposition over a and b

`gcd_p_sym` == $\forall a,b,y{:}\mathbb{Z}.$ GCD(a;b;y) $\Rightarrow$ GCD(b;a;y)

`gcd_p_shift` == $\forall a,b,y,k{:}\mathbb{Z}.$ GCD(a;b;y) $\Rightarrow$ GCD(a;$b + k \cdot a$;y)

Proof A: We proceed by induction over n. Consider the base case. By simplification, we can instead show CoPrime(1,1). By the `gcd_p_one` lemma, we have shown CoPrime(1,1). In the step case, assume the inductive hypothesis that CoPrime(fib($n-1$),fib($n-1+1$)). By the `comb_for_fib_wf` lemma, we know CoPrime(fib($-1+n$),fib(n)) and we must show CoPrime(fib(n),fib($1+n$)). There are 2 possible cases. In the first case, assume $1+n=0$ or $1+n=1$. Therefore, we have shown CoPrime(fib(n),1). In the second case, assume $\neg 1+n=0$ and $\neg 1+n=1$. By applying the `comb_for_coprime_wf` lemma, we can instead show CoPrime(fib(n),fib($1+n-1$)+fib($1+n-2$)). By the `gcd_p_shift` lemma, we have shown CoPrime(fib(n),fib($-1+n$)+fib(n)).

Proof B: By induction on n we are going to prove that fib(n) and fib($n+1$) are coprime. Base case: ($n=0$) We compute fib(0) and fib($0+1$) (both are equal to 1) and by `gcd_p_one` lemma they are indeed co-prime. Induction step: ($n>0$): We know that fib($n-1$) and fib(n) are co-prime, and we want to show that fib(n) and fib($n+1$) are co-prime. We know that it is not the case that $n+1=0$ or $n+1=1$, so fib($n+1$) = fib(n) + fib($n-1$). But from `gcd_p_sym` and `gcd_p_shift` lemma, we know that this sum is co-prime with fib($n-1$) iff fib($n-1$) and fib(n) are co-prime.

Questions:

How do these proofs compare on general readability?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on organizational quality?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

How do these proofs compare on ability to express the central proof idea?

________ Proof A is much better than Proof B.
________ Proof A is slightly better than Proof B.
________ Proof A and Proof B are about the same.
________ Proof A is slightly worse than Proof B.
________ Proof A is much worse than Proof B.

Part Three: Proof Recreation

Shown below is a partial proof of the theorem:
For an integer a and b, it is the case where $\gcd(a;b) \sim \gcd(b;a)$.
Formally: $\forall$a,b:$\mathbb{Z}$. gcd(a;b) $\sim$ gcd(b;a)

A line has been omitted from the proof, as indicated by the blank. Please read the proof through carefully, and then fill in on the blank the content needed to make the proof complete. Be sure to look over the lemmas provided, as the step omitted may requiring using one of them.

The constructs and lemmas referred to in this proof are:
$b \mid a == \exists c{:}\mathbb{Z}.\ a = b \cdot c == b$ divides a
$a \sim b == a \mid b \land b \mid a$
$\gcd(a;b) ==$ the greatest common divisor of a and b
$\mathrm{GCD}(a;b;c) ==$ the greatest common divisor of a and b is c
`gcd_elim` $== \forall a,b{:}\mathbb{Z}.\ \exists y{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y) \land \gcd(a;b) = y$
`gcd_unique` $== \forall a,b,y_1,y_2{:}\mathbb{Z}.\ \mathrm{GCD}(a;b;y_1) \Rightarrow \mathrm{GCD}(a;b;y_2) \Rightarrow y_1 \sim y_2$
`assoced_weakening` $== \forall a,b{:}\mathbb{Z}.\ a = b \Rightarrow a \sim b$

Proof:

By simplification, we know that a is an integer and b is an integer and we must show $\gcd(a;b) \sim \gcd(b;a)$. By applying the `gcd_elim` lemma, we know that there exists an integer y where $\mathrm{GCD}(a;b;y)$ and $\gcd(a;b) = y$ and there exists an integer y where $\mathrm{GCD}(b;a;y)$ and $\gcd(b;a) = y$. ______________________________

____

From the `gcd_unique` lemma, we know that $\mathrm{GCD}(a;b;y_2)$ and $y_1 \sim y_2$. Applying the `assoced_weakening` lemma, we have shown $\gcd(a;b) \sim \gcd(b;a)$.

Part Three: Proof Recreation

Shown below is a partial proof of the theorem:

For an integer a and b, it is the case where there exists an integer u and v where GCD(a;b;$u \cdot a + v \cdot b$).
Formally: $\forall a,b{:}\mathbb{Z}.\ \exists u,v{:}\mathbb{Z}.$ GCD(a;b;$u \cdot a + v \cdot b$)

A line has been omitted from the proof, as indicated by the blank. Please read the proof through carefully, and then fill in on the blank the content needed to make the proof complete. Be sure to look over the lemmas provided, as the step omitted may requiring using one of them.

The constructs and lemmas referred to in this proof are:

GCD(a;b;c) == the greatest common divisor of a and b is c
CoPrime(a,b) == GCD(a;b;1) == a and b are coprime
`bezout_ident_n` == $\forall b{:}\mathbb{N}.\ \forall a{:}\mathbb{Z}.\ \exists u,v{:}\mathbb{Z}.$ GCD(a;b;$u \cdot a + v \cdot b$)
`gcd_p_neg_arg` == $\forall a,b,y{:}\mathbb{Z}.$ GCD(a;b;y) $\Rightarrow$ GCD(a;$-b$;y)

Proof:

There are 2 possible cases. In the first case, assume that a is an integer, b is an integer and $0 \leq b$. Applying the `bezout_ident_n` lemma, we have shown there exists an integer u and v where GCD(a;b;$u \cdot a + v \cdot b$). In the second case, assume that a is an integer, b is an integer and $\neg 0 \leq b$. ______________________________

____

Applying the `gcd_p_neg_arg` lemma, we have shown there exists an integer u and v where GCD(a;b;$u \cdot a + v \cdot b$).

Part Three: Proof Recreation

Shown below is a partial proof of the theorem:

For any integers a_1, a_2, and b, if a_1 and a_2 are coprime and a_1 and a_2 both divide b, then $a_1 \cdot a_2$ divides b.
Formally: $\forall a_1,a_2,b{:}\mathbb{Z}.\ \mathrm{CoPrime}(a_1,a_2) \Rightarrow a_1 \mid b \Rightarrow a_2 \mid b \Rightarrow a_1 \cdot a_2 \mid b$

A line has been omitted from the proof, as indicated by the blank. Please read the proof through carefully, and then fill in on the blank the content needed to make the proof complete. Be sure to look over the lemmas provided, as the step omitted may requiring using one of them.

The constructs and lemmas referred to in this proof are:

$b \mid a == \exists c{:}\mathbb{Z}.\ a = b \cdot c == b$ divides a
$\mathrm{GCD}(a;b;c) ==$ the greatest common divisor of a and b is c
$\mathrm{CoPrime}(a,b) == \mathrm{GCD}(a;b;1) == a$ and b are coprime
$\mathrm{prime}(a) == \neg(a = 0) \wedge \neg(a \sim 1) \wedge (\forall b,c{:}\mathbb{Z}.\ a \mid b \cdot c \Rightarrow a \mid b \vee a \mid c) == a$ is prime
`coprime_bezout_id` $== \forall a,b{:}\mathbb{Z}.\ \mathrm{CoPrime}(a,b) \iff (\exists x,y{:}\mathbb{Z}.\ a \cdot x + b \cdot y = 1)$
`coprime_iff_ndivides` $== \forall a,p{:}\mathbb{Z}.\ \mathrm{prime}(p) \Rightarrow (\mathrm{CoPrime}(p,a) \iff \neg(p \mid a))$
`quot_rem_exists` $== \forall a{:}\mathbb{Z}.\ \forall b{:}\mathbb{N}^{+}.\ \exists q{:}\ \mathbb{Z}.\ \exists r{:}\mathbb{N}b.\ a = q \cdot b + r$

Proof:

Assume we have coprime integers a_1 and a_2, and a_1 and a_2 both divide the integer b. By `coprime_bezout_id`, $\mathrm{CoPrime}(a_1,a_2)$ implies that there are integers x and y such that $a_1 \cdot x + a_2 \cdot y = 1$. To show that $a_1 \cdot a_2$ divides b, we will construct c such that $b = (a_1 \cdot a_2) \cdot c$. We know there are integers c_1 and c_2 such that $b = a_1 \cdot c_1$ and $b = a_2 \cdot c_2$. ____

____

We can rewrite this as $a_1 \cdot (a_2 \cdot c_2) \cdot x + a_2 \cdot (a_1 \cdot c_1) \cdot y = b$, so our c is $c_2 \cdot x + c_1 \cdot y$ and we are done.

Part Three: Proof Recreation

Shown below is a partial proof of the theorem:

For an integer a and nonzero integer n, it is the case when $n \mid a$ if and only if $(a \div n) \cdot n = a$.
Formally: $\forall a{:}\mathbb{Z}.\ \forall n{:}\mathbb{Z}^{-\mathbf{0}}.\ n \mid a \iff (a \div n) \cdot n = a$

A line has been omitted from the proof, as indicated by the blank. Please read the proof through carefully, and then fill in on the blank the content needed to make the proof complete. Be sure to look over the lemmas provided, as the step omitted may requiring using one of them.

The constructs and lemmas referred to in this proof are:

$b \mid a == \exists c{:}\mathbb{Z}.\ a = b \cdot c ==$ b divides a
`divides_iff_rem_zero` $== \forall a{:}\mathbb{Z}.\ \forall b{:}\mathbb{Z}^{-\mathbf{0}}.\ b \mid a \iff a \text{ rem } b = 0$
`add_mono_wrt_eq` $== \forall a,b,n{:}\mathbb{Z}.\ a = b \iff a + n = b + n$
`add_com` $== \forall a,b{:}\mathbb{Z}.\ a + b = b + a$
`div_rem_sum` $== \forall a{:}\mathbb{Z}.\ \forall n{:}\mathbb{Z}^{-\mathbf{0}}.\ a = (a \div n) \cdot n + a \text{ rem } n$
`divisor_of_minus` $== \forall a,b{:}\mathbb{Z}.\ a \mid b \Rightarrow a \mid -b$
`quot_rem_exists` $== \forall a{:}\mathbb{Z}.\ \forall b{:}\mathbb{N}^{+}.\ \exists q{:}\ \mathbb{Z}.\ \exists r{:}\mathbb{N}b.\ a = q \cdot b + r$

Proof:

There are 2 possible cases. In the first case, assume that a is an integer, n is nonzero integer and $n \mid a$. By applying the `divides_iff_rem_zero` lemma, we know $(a \text{ rem } n) = 0$. ____

____

By simplification, we know $(a \div n) \cdot n + (a \text{ rem } n) = (a \div n) \cdot n$. From the `div_rem_sum` lemma, we have shown $(a \div n) \cdot n = a$. In the second case, assume that a is an integer, n is nonzero integer and $(a \div n) \cdot n = a$. By simplification, we can instead show there exists an integer c when $a = n \cdot c$. Therefore, we have shown there exists an integer c when $a = n \cdot c$.