# PROPOSITIONAL LOGIC: SUBPROOFS*

Ian Barland
John Greiner
Phokion Kolaitis
Moshe Vardi
Matthias Felleisen

This work is produced by The Connexions Project and licensed under the
Creative Commons Attribution License †

**Abstract**

Using subproofs, to show RAA or to aid in presentation.

## 1 Subproofs

The *reductio ad absurdum* ("RAA"), Latin for "reduction to absurdity", seems very strange: If we can prove that false is true, then we can prove the negation of our premise. Huh!?! What on Earth does it mean to prove that false is true?

This is known as **proof-by-contradiction**. We start by making a single unproven assumption. We then try to prove that false is true. Clearly, that it nonsense, so we must have done something wrong. Assuming we didn't make any mistakes in the individual inference steps, then the only thing that could be wrong is the assumption. It must not hold. Therefore, we have just proven its negation.

This form of reasoning is often expressed via **contrapositive**. Consider the slogan

*If you paid list price, you didn't buy it at SuperMegaMart.*

(This is a contrapositive, because the real statement the advertisers want to make is that if you buy it at SuperMegaMart, then you won't pay list price.), which we'll abbreviate payFull $\Rightarrow$ ¬boughtAtSMM. You know this slogan is true, and you just made a SuperMegaMart purchase (boughtAtSMM), and are suddenly wanting a **proof** that you got a good deal. Well, suppose we didn't. That is, **suppose**payFull. Then by the truth of the marketing slogan, we infer ¬boughtAtSMM. But this contradicts boughtAtSMM (that is, from ¬boughtAtSMM and boughtAtSMM together we can prove that false is true). The problem must have been our pessimistic assumption payFull; clearly that couldn't have been true, and we're happy to know that ¬payFull.

**Example 1**

Spot the proof-by-contradiction used in The Simpsons:

Bart, filing through the school records: " Hey, look at this: Skinner makes $25,000 per year! "

Other kids: "Ooooh!"

*Version 1.12: Mar 10, 2009 4:28 pm GMT-5

†http://creativecommons.org/licenses/by/1.0

Milhouse: " And he's 40 years old; that makes him a millionaire! "
Skinner, indignantly: " I wasn't a principal when I was 1!"
Milhouse: "**And,** he paints houses during the summer ... he's a billionaire! "
Skinner: " If I were a billionaire, would I still be living with my mother? " [Kids' laughter]
Skinner, to himself: " The kids just aren't responding to logic anymore! "

In the particular set of inference rules we have chosen to use, RAA is surprisingly important. It is the only way to prove formulas that begin with a single "¬". [1]

**Example 2**
We'll prove $\vdash \neg(\alpha \wedge \neg\alpha)$.

| | | | |
|---|---|---|---|
| 1 | subproof: $\alpha \wedge \neg\alpha \vdash$ false | | |
| 1.a | | $\alpha \wedge \neg\alpha$ | Premise for subproof |
| 1.b | | $\alpha$ | $\wedge$Elim (left), line 1.a, where $\phi = \alpha$, and $\psi = \neg\alpha$ |
| 1.c | | $\neg\alpha$ | $\wedge$Elim (right), line 1.a, where $\phi = \alpha$, and $\psi = \neg\alpha$ |
| 1.d | | false | falseIntro, lines 1.b,1.c, where $\phi = \alpha$ |
| 2 | $\neg(\alpha \wedge \neg\alpha)$ | | RAA, line 1, where $\phi = \alpha \wedge \neg\alpha$ |

**Table 1**

**Exercise 1** *(Solution on p. 10.)*
Here's another relatively simple example which uses RAA. Show that the **modus tollens** rule holds: $\alpha \Rightarrow \beta, \neg\beta \vdash \neg\alpha$

Another use of subproofs is to organize proofs' presentations. Many proofs naturally break down into larger subparts, each with its own intermediate conclusion. These steps between these subparts are big enough to correspond to our intuition, but too big to correspond to individual inference rules. This gives additional useful structure to a proof, aiding our understanding.

**Example 3**
Previously, we showed that $\wedge$ (AND) commutes[2]. However, that conclusion is only directly applicable when the $\wedge$ is at the "top-level", *i.e.*, not nested inside some other connective. Here, we'll show that $\wedge$ commutes inside $\neg$, or more formally, $\neg(\alpha \wedge \beta) \vdash \neg(\beta \wedge \alpha)$.

WARNING: When doing inference-style proofs, we will **not** use the Boolean algebra laws nor replace subformulas with equivalent formulas. Conversely, when doing algebraic proofs, don't use inference rules! While theoretically it's acceptable to mix the two methods, for homeworks we want to make sure you can do the problems using either method alone, so keep the two approaches separate!

[1] This is an example of reasoning **about** our logic system. It shows us that while we might have some redundant inference rules, RAA isn't one of them. The only other rule which produces formulas starting with an initial "¬" is ¬Intro. Is this also essential, or could we still prove all the same things even without ¬Intro?
[2] "Propositional Logic: inference rules", Example 4 <http://cnx.org/content/m10718/latest/#commutativity>

We'll do two proofs of this to illustrate that there's always more than one way to prove something!

In our first proof, we'll use RAA. Why? Looking at our desired conclusion, what could be the last inference rule used in the proof to reach the conclusion? By the shape of the formula, the last step can't use any of the "introduction" inference rules (∧Intro, ∨Intro, ⇒Intro, falseIntro, or ¬Intro). We could potentially use any of the "elimination" inference rules. But, for ∧Elim, ∨Elim, ⇒Elim, ¬Elim, or CaseElim, we would first have to prove some more complicated formula to obtain our desired conclusion. That seems somewhat unlikely or unnecessary. For falseElim, we'd have to first prove false, *i.e.*, obtain a contradiction, but our only premise isn't self-contradictory. The only remaining option is RAA.

| | | | |
|---|---|---|---|
| 1 | $\neg(\alpha \wedge \beta)$ | | Premise |
| 2 | subproof: $\beta \wedge \alpha \vdash$ false | | |
| 2.a | | $\beta \wedge \alpha$ | Premise for subproof |
| 2.b | | $\alpha \wedge \beta$ | Theorem: ∧ commutes[3], line 2a |
| 2.c | | false | falseIntro, lines 1,2.b |
| 3 | $\neg(\alpha \wedge \beta)$ | | RAA, line 2 |

**Table 2**

The proof above uses a subproof because it is necessary for the use of RAA. In contrast, the proof below uses two subproofs simply for organization.

For our second proof, let's not use RAA directly. Our plan is as follows:

- Assume the premise $\neg(\alpha \wedge \beta)$.
- Again, use commutativity to show that $\beta \wedge \alpha \Rightarrow \alpha \wedge \beta$
- Use modus tollens (Exercise 1) to obtain the conclusion.

We can organize the proof into corresponding subparts:

| | | | |
|---|---|---|---|
| 1 | $\neg(\alpha \wedge \beta)$ | | Premise |
| 2 | subproof: $\beta \wedge \alpha \Rightarrow \alpha \wedge \beta$ | | |
| 2.a | | $\beta \wedge \alpha \vdash \alpha \wedge \beta$ | Theorem statement: ∧ commutes[4] |
| 2.b | | $\beta \wedge \alpha \Rightarrow \alpha \wedge \beta$ | ⇒Intro, line 2.a |
| 3 | subproof: $\neg(\beta \wedge \alpha)$ | | |
| 3.a | | $\beta \wedge \alpha \Rightarrow \alpha \wedge \beta, \neg(\alpha \wedge \beta) \vdash \neg(\beta \wedge \alpha)$ | Theorem statement: modus tollens (Exercise 1) |
| | | | *continued on next page* |

[3]"Propositional Logic: inference rules", Example 4 <http://cnx.org/content/m10718/latest/#commutativity>

| | | | |
|---|---|---|---|
| 3.b | | $(\beta \wedge \alpha \Rightarrow \alpha \wedge \beta) \wedge \neg(\alpha \wedge \beta) \Rightarrow \neg(\beta \wedge \alpha)$ | $\Rightarrow$Intro, line 3.a |
| 3.c | | $(\beta \wedge \alpha \Rightarrow \alpha \wedge \beta) \wedge \neg(\alpha \wedge \beta)$ | $\wedge$Intro, lines 2,1 |
| 3.d | | $\neg(\beta \wedge \alpha)$ | $\Rightarrow$Elim, lines 3.b,3.c |

**Table 3**

## 2 More examples

Now let's use these rules in a couple larger proofs, to show some more interesting results.

**Example 4**

Let's redo the first example[5]'s proof formally and show $\mathrm{H-has-2} \wedge \mathrm{J-safe} \vdash \mathrm{G-unsafe}$. The inference rules we used informally above don't correspond exactly to those in our definition, so the formal proof is more complicated.

| | | | |
|---|---|---|---|
| 1 | $\mathrm{H-has-2} \Rightarrow \mathrm{P-unsafe} \wedge \mathrm{G-unsafe} \vee \mathrm{J-unsafe} \wedge \mathrm{P-unsafe} \vee \mathrm{G-unsafe} \wedge \mathrm{J-unsafe}$ | | WaterWorld axiom, choosing a grouping of the ternary $\vee$, as justified by $\vee$ commutativity[6] |
| 2 | $\mathrm{H-has-2} \wedge \mathrm{J-safe}$ | | Premise |
| 3 | $\mathrm{H-has-2}$ | | $\wedge$Elim (left), line 2 |
| 4 | $\mathrm{P-unsafe} \wedge \mathrm{G-unsafe} \vee \mathrm{J-unsafe} \wedge \mathrm{P-unsafe} \vee \mathrm{G-unsafe} \wedge \mathrm{J-unsafe}$ | | $\Rightarrow$Elim, lines 1,3 |
| 5 | $\mathrm{J-safe}$ | | $\wedge$Elim (right), line 2 |
| 6 | $\mathrm{J-safe} \Rightarrow \neg\mathrm{J-unsafe}$ | | WaterWorld axiom |
| 7 | $\neg\mathrm{J-unsafe}$ | | $\Rightarrow$Elim, lines 5,6 |
| 8 | subproof:$\mathrm{G-unsafe} \wedge \mathrm{J-unsafe} \vdash \mathrm{false}$ | | |
| 8.a | | $\mathrm{G-unsafe} \wedge \mathrm{J-unsafe}$ | Premise for subproof |
| 8.b | | $\mathrm{J-unsafe}$ | $\wedge$Elim (right), line 8.a |
| 8.c | | false | falseIntro, lines 7,8.b |
| | | | *continued on next page* |

[4]"Propositional Logic: inference rules", Example 4 <http://cnx.org/content/m10718/latest/#commutativity>
[5]"Propositional Logic: inference rules", Example 1 <http://cnx.org/content/m10718/latest/#running-example1>

| | | | |
|---|---|---|---|
| 9 | $\neg (G - unsafe \wedge J - unsafe)$ | | RAA, line 8 |
| 10 | $P - unsafe \wedge G - unsafe \vee J - unsafe \wedge P - unsafe$ | | CaseElim (right), lines 4,9 |
| 11 | subproof:$J - unsafe \wedge P - unsafe \vdash false$ | | |
| 11.a | | $J - unsafe \wedge P - unsafe$ | Premise for subproof |
| 11.b | | $J - unsafe$ | $\wedge$Elim (left), line 11.a |
| 11.c | | false | falseIntro, lines 7,11.b |
| 12 | $\neg (J - unsafe \wedge P - unsafe)$ | | RAA, line 11 |
| 13 | $P - unsafe \wedge G - unsafe$ | | CaseElim (right), lines 10,12 |
| 14 | $G - unsafe$ | | $\wedge$Elim (right), line 13 |

**Table 4**

Wow! This formalization is a lot longer than the original informal proof. That's a result of the particular set of inference rules we are using, that we can only make inferences in small steps. Also, here we were pickier about the distinction between "not safe" and "unsafe".

**Example 5**

The previous example (Example 4) is a perfect candidate for adding structure to the proof by using additional subproofs. The following is more similar to the original informal proof[7].

Note also that subproofs can have their own subproofs.

| | | | |
|---|---|---|---|
| 1 | $H - has - 2 \Rightarrow P - unsafe \wedge G - unsafe \vee J - unsafe \wedge P - unsafe \vee G - unsafe \wedge J - unsafe$ | | WaterWorld axiom, choosing a grouping of the ternary $\vee$, as justified by $\vee$ commutativity[8] |
| 2 | subproof:$\vdash H - has - 2$ | | |
| 2.a | | $H - has - 2 \wedge J - safe$ | Premise |
| 2.b | | $H - has - 2$ | $\wedge$Elim (left), line 2.a |
| 3 | $P - unsafe \wedge G - unsafe \vee J - unsafe \wedge P - unsafe \vee G - unsafe \wedge J - unsafe$ | | $\Rightarrow$Elim, lines 1,3 |
| 4 | subproof:$\vdash \neg J - unsafe$ | | |
| 4.a | | $H - has - 2 \wedge J - safe$ | Premise |
| | | *continued on next page* | |

[6]"Propositional Logic: inference rules", Example 4 <http://cnx.org/content/m10718/latest/#commutativity>
[7]"Propositional Logic: inference rules", Example 1 <http://cnx.org/content/m10718/latest/#running-example1>

| | | | | |
|---|---|---|---|---|
| 4.b | | J – safe | | ∧Elim (right), line 4.a |
| 4.c | | J – safe ⇒ ¬J – unsafe | | WaterWorld axiom |
| 4.d | | ¬J – unsafe | | ⇒Elim, lines 4.b,4.c |
| 5 | subproof:⊢ P – unsafe ∧ G – unsafe | | | |
| 5.a | | subproof:G – unsafe ∧ J – unsafe ⊢ false | | |
| 5.a.i | | | G – unsafe ∧ J – unsafe | Premise for subproof |
| 5.a.ii | | | J – unsafe | ∧Elim (right), line 5.a.1 |
| 5.a.iii | | | false | falseIntro, lines 4,5.a.2 |
| 5.b | | ¬ (G – unsafe ∧ J – unsafe) | | RAA, line 5.a |
| 5.c | | P – unsafe ∧ G – unsafe ∨ J – unsafe ∧ P – unsafe | | CaseElim (right), lines 3,5.b |
| 5.d | | subproof:J – unsafe ∧ P – unsafe ⊢ false | | |
| 5.d.i | | | J – unsafe ∧ P – unsafe | Premise for subproof |
| 5.d.ii | | | J – unsafe | ∧Elim (left), line 5.d.1 |
| 5.d.iii | | | false | falseIntro, lines 4,5.d.2 |
| 5.e | | ¬ (J – unsafe ∧ P – unsafe) | | RAA, line 5.d |
| 5.f | | P – unsafe ∧ G – unsafe | | CaseElim (right), lines 5.c,5.e |
| 6 | G – unsafe | | | ∧Elim (right), line 5 |

**Table 5**

A standard way of presenting proofs is by using **lemmas** to show parts of the proofs. Lemmas are simply formulas which we prove not as an end result, but as intermediate steps in a larger proof. So, they are simply another way of presenting subproofs.

**Example 6**

[8]"Propositional Logic: inference rules", Example 4 <http://cnx.org/content/m10718/latest/#commutativity>

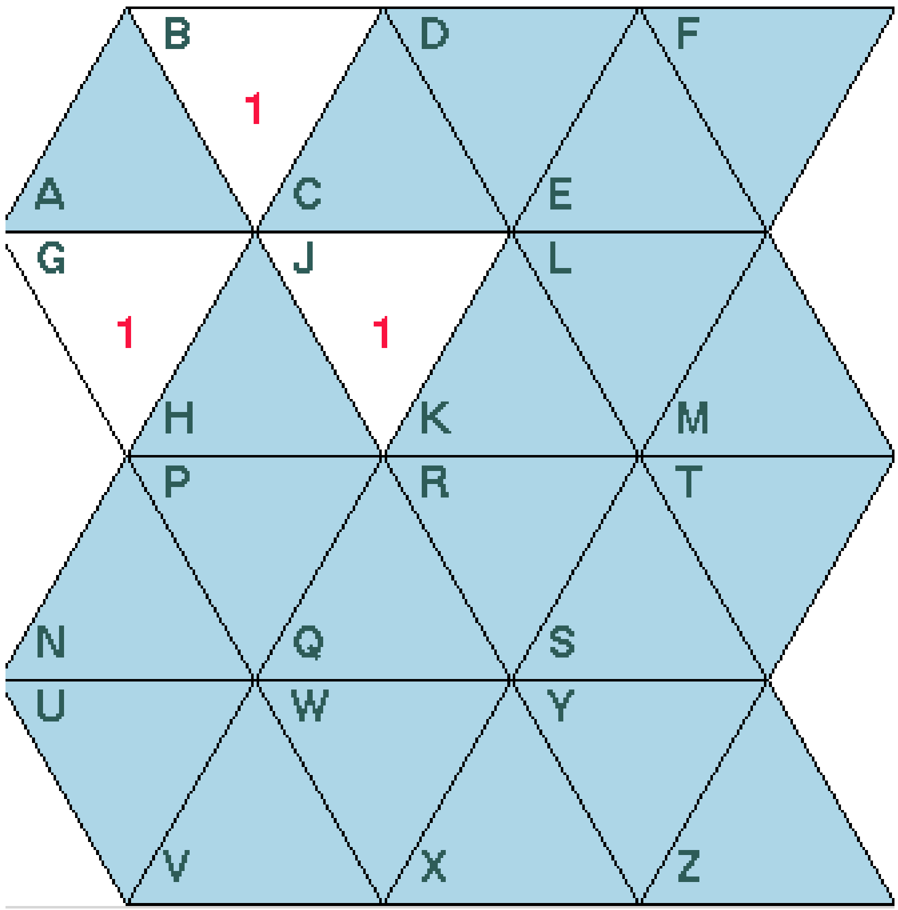


**Figure 1:** Example WaterWorld board

Consider the above figure (Figure 1). We'll show $\text{B} - \text{has} - 1 \ \wedge \ \text{G} - \text{has} - 1 \ \wedge \ \text{J} - \text{has} - 1 \vdash \text{K} - \text{unsafe}$. We'll do this through the following series of lemmas:

- Lemma A: $\neg \text{A} - \text{unsafe}, \text{G} - \text{has} - 1 \vdash \text{H} - \text{unsafe}$
- Lemma B: $\neg \text{A} - \text{unsafe}, \text{B} - \text{has} - 1 \vdash \text{C} - \text{unsafe}$
- Lemma C: $\text{H} - \text{unsafe}, \text{C} - \text{unsafe}, \text{J} - \text{has} - 1 \vdash \text{false}$
- Lemma D: $\text{A} - \text{unsafe}, \text{B} - \text{has} - 1 \vdash \text{C} - \text{safe}$
- Lemma E: $\text{A} - \text{unsafe}, \text{G} - \text{has} - 1 \vdash \text{H} - \text{safe}$
- Lemma F: $\text{C} - \text{safe}, \text{H} - \text{safe}, \text{J} - \text{has} - 1 \vdash \text{K} - \text{unsafe}$

First, we'll show the main proof, assuming each of the lemmas. Then, proofs of each of the lemmas will follow.

| | | | |
|---|---|---|---|
| 1 | $B - has - 1 \wedge G - has - 1 \wedge J - has - 1$ | | Premise |
| 2 | $B - has - 1$ | | $\wedge$Elim (left), line 1 |
| 3 | $G - has - 1 \wedge J - has - 1$ | | $\wedge$Elim (right), line 1 |
| 4 | $G - has - 1$ | | $\wedge$Elim (left), line 3 |
| 5 | $J - has - 1$ | | $\wedge$Elim (right), line 3 |
| 6 | subproof:$\neg A - unsafe \vdash false$ | | |
| 6.a | | $\neg A - unsafe$ | Premise for subproof |
| 6.b | | $H - unsafe$ | Lemma A, lines 6.a,4 |
| 6.c | | $C - unsafe$ | Lemma B, lines 6.a,2 |
| 6.d | | false | Lemma C, lines 6.b,6.c,5 |
| 7 | $A - unsafe$ | | RAA, line 6 |
| 8 | $C - safe$ | | Lemma D, lines 7,2 |
| 9 | $H - safe$ | | Lemma E, lines 7,3 |
| 10 | $K - unsafe$ | | Lemma F, lines 8,9,5 |

**Table 6**

And that's the desired proof! Now it just remains to show each of the six lemmas.
**Lemma A:** $\neg A - unsafe, G - has - 1 \vdash H - unsafe$

| | | | |
|---|---|---|---|
| 1 | $\neg A - unsafe$ | | Premise |
| 2 | $G - has - 1$ | | Premise |
| 3 | subproof:$A - unsafe \wedge H - safe \vdash false$ | | |
| 3.a | | $A - unsafe \wedge H - safe$ | Premise for subproof |
| 3.b | | $A - unsafe$ | $\wedge$Elim |
| 3.c | | false | falseIntro, lines 1,3b |
| 4 | $\neg (A - unsafe \wedge H - safe)$ | | RAA, line 3 |
| 5 | $G - has - 1 \Rightarrow A - safe \wedge H - unsafe \vee A - unsafe \wedge H - safe$ | | WaterWorld axiom |
| 6 | $A - safe \wedge H - unsafe \vee A - unsafe \wedge H - safe$ | | $\Rightarrow$Elim, lines 5,2 |
| 7 | $A - unsafe \wedge H - safe \vee A - safe \wedge H - unsafe$ | | Theorem: $\vee$ commutes, line 6 |
| *continued on next page* | | | |

| | | |
|---|---|---|
| 8 | $A-\text{safe} \wedge H-\text{unsafe}$ | CaseElim, lines 4,7 |
| 9 | $H-\text{unsafe}$ | ∧Elim (right), line 8 |

**Table 7**

**Lemma B:** $\neg A-\text{unsafe}, B-\text{has}-1 \vdash C-\text{unsafe}$

| | | | |
|---|---|---|---|
| 1 | $\neg A-\text{unsafe}$ | | Premise |
| 2 | $B-\text{has}-1$ | | Premise |
| 3 | subproof:$A-\text{unsafe} \wedge C-\text{safe} \vdash \text{false}$ | | |
| 3.a | | $A-\text{unsafe} \wedge C-\text{safe}$ | Premise for subproof |
| 3.b | | $A-\text{unsafe}$ | ∧Elim (left), line 3a |
| 3.c | | false | falseIntro, lines 1,3b |
| 4 | $\neg(A-\text{unsafe} \wedge C-\text{safe})$ | | RAA, line 3 |
| 5 | $B-\text{has}-1 \Rightarrow A-\text{safe} \wedge C-\text{unsafe} \vee A-\text{unsafe} \wedge C-\text{safe}$ | | WaterWorld axiom |
| 6 | $A-\text{safe} \wedge C-\text{unsafe} \vee A-\text{unsafe} \wedge C-\text{safe}$ | | ⇒Elim, lines 5,2 |
| 7 | $A-\text{unsafe} \wedge C-\text{safe} \vee A-\text{safe} \wedge C-\text{unsafe}$ | | Theorem: ∨ commutes, line 6 |
| 8 | $A-\text{safe} \wedge C-\text{unsafe}$ | | CaseElim, lines 4,7 |
| 9 | $C-\text{unsafe}$ | | ∧Elim (right), line 8 |

**Table 8**

Proving the other lemmas is left as an exercise to the reader.

Note that we took a little shortcut: we used the lemmas as if they were inference rules. According to our previous definition of proofs, we technically should present the lemma as a subproof and then use an inference rule or two to show how that applies, as we've done in previous examples. This shorter form is common practice and much easier to read.

In summary, we must state one of the following four possible reasons for each step in a proof, allowing subproofs.

- This step's WFF is a premise.
- This step's WFF is an axiom.
- This step's WFF follows from a inference rule applied to previous steps' WFFs. The reason includes a statement of which inference rule is used and how.
- This step's WFF follows from a subproof, where that subproof may temporarily introduces additional premises. The reason includes the entire subproof. When that subproof has been shown elsewhere, such as in class or another exercise, it may simply be cited, for brevity. Of course, subproofs may have additional embedded subproofs, in turn.

Technically, when using subproofs, one must be careful to rename variables, to avoid clashes. Rather than formalize this notion, we'll leave it as "obvious".

# Solutions to Exercises in this Module

### Solution to Exercise 1 (p. 2)

| | | | |
|---|---|---|---|
| 1 | $\alpha \Rightarrow \beta$ | | Premise |
| 2 | $\neg\beta$ | | Premise |
| 3 | subproof:$\alpha \vdash$ false | | |
| 3.a | | $\alpha$ | Premise for subproof |
| 3.b | | $\beta$ | $\Rightarrow$Elim, lines 1,3.a |
| 3.c | | false | falseIntro, lines 2,3.b |
| 4 | $\neg\alpha$ | | RAA, line 3 |

**Table 9**