Going backwards suffices: some reflections on proof construction for formal verification[1]

Programs, Minds and Machines 2018
IMATE UNAM Mexico City

Favio Ezequiel Miranda Perea
(joint work with Lourdes González Huesca and Selene Linares Arévalo)

Facultad de Ciencias
Universidad Nacional Autónoma de México

Mexico City, August 9th 2018

[1]supported by UNAM PAPIME PE102117

How to write proofs: a quick guide

Eugenia Cheng

1. Begin at the end and end at the beginning

This is a really, really terrible thing to do. This might be even worse than leaving out gaps in the middle. Because if you begin at the end and end at the beginning you *monumentally* haven't got where you're trying to go. Here's an example of this for Example 1 from Section 4:

$$\begin{aligned} a(b-c) &= ab-ac \\ ab+a(-c) &= ab-ac \\ a(-c) &= -ac \\ ac+a(-c) &= 0 \\ a(c+(-c)) &= 0 \\ a.0 &= 0 \\ 0 &= 0 \qquad \square \end{aligned}$$

Try comparing this with the *good* proof given in Section 4 – you'll see that all the correct steps are there, but they're all in the wrong order.

Classical and Nonclassical Logics

Erich Schechter

Working backwards is not a method of proof at all - it is a method of discovery -. However, beginners sometimes confuse it with proof, perhaps because it slightly resembles an indirect proof, or because they do not understand the difference between discovery and certification, or because working backwards often succeeeds in some lower-level math courses. It does not work in most advanced parts of math. That is because, though most of the computations in lower-level math courses are reversible, many of the reasoning steps in the higher-level math courses are not reversible.

How to Prove It. A Structured Approach. Daniel J. Velleman

Proof strategies

To prove a goal of the form $P \to Q$:
Assume P is true and then prove Q.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
P	

How to Prove It. A Structured Approach. Daniel J. Velleman

Proof strategies

Before using strategy:

Givens	*Goal*
—	$\exists x\, P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

$x =$ (the value you decided on)

How to Prove It. A Structured Approach. Daniel J. Velleman

Proof strategies

To prove a goal of the form $\neg P$:

If possible, reexpress the goal in some other form and then use one of the proof strategies for this other goal form.

To prove a goal of the form $\neg P$:

Assume P is true and try to reach a contradiction. Once you have reached a contradiction, you can conclude that P must be false.

Assumption Strategy 3.6.3. Given a diagram containing the form

Assume $P \vee Q$
Prove R

there are three approaches:

(a) Use a *proof by cases*; that is, replace the form with

Case 1: Assume P
Prove R
Case 2: Assume Q
Prove R.

(b) If you are assuming or can prove $\neg P$, then you can deduce Q. Now prove R.
(c) If you are assuming or can prove $\neg Q$, then you can infer P. Now prove R.

Proof Strategy 3.4.1. Given a diagram containing one of the forms

Prove $\forall x P(x)$	Prove $(\forall x \in A)P(x)$

replace the form with the corresponding lower diagram, as follows:

Let x be arbitrary. Prove $P(x)$	Let $x \in A$ be arbitrary. Prove $P(x)$

If the letter x is already being used in the proof, then use another letter, say y, in the lower diagram.

Relevancy of proofs

Mathematics vs. Computer Science

Proving theorems = Formal verification

- The value of a proof is that it warrants the truth of the theorem.
- Mathematics: proofs and not only theorems are relevant. New proofs of a known theorem provide new insights into the theory.
- Formal verification: proofs are irrelevant, once a proof succeeds we dispose of it. We are only interested in the verified property.
- Mathematics: proof strategies are only heuristics related to backward reasoning, only forward proof is valid.
- Formal verification: backward proof suffices. Why bother to construct the forward proof?

Mind the gap!

Formal proofs

- Formal proof construction is a process related to backward heuristics and human creativity.
- Formal logic, in particular deductive systems, are supossed to help in proof formalization.
- Proof assistants are sophisticated implementations of deductive systems.
- Mind the gap: there is no explicit connection between the formal deductive systems and their operational implementation in proof assistants.
- This is an important problem in the teaching of computational logic and formal verification.

Kanger's definition

Provability in Logic. Stockholm Studies in Philosophy I. 1957

A sequence Π of sequents (with repetitions allowed) is called a *quasi-deduction* (in LC) of S from the class Φ of assumption sequents, if

(1) Π begins with an occurrence of S and
(2) each member T of Π is either
  (i) an instance of postulate *1 or
  (ii) a member of Φ or
  (iii) directly inferrable by an application of a rule of inference (of LC) from succeeding members, one or two, of Π.

Kanger's definition

Provability in Logic. Stockholm Studies in Philosophy I. 1957

$$\forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P$$

The rules of inference applied are specified to the right. The easiest way to obtain the proof is to start from below with the sequent to be proved.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{F^x_c, \sim \forall x Fx, F^x_d, \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P, F^x_d}\,*5}{F^x_c, (\sim \forall x Fx \;\&\; F^x_d), \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P, F^x_d}\,*11}{F^x_c, \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P, F^x_d}\,*10}{F^x_c, \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P, \forall x Fx}\,*9}{\sim \forall x Fx, F^x_c, \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P}\,*5}{(\sim \forall x Fx \;\&\; F^x_c), \forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P}\,*11}{\forall x(\sim \forall x Fx \;\&\; Fx) \longrightarrow P}$$

Proof example

Natural deduction in sequent style

Let $\Gamma = \{p \to q \vee r\ ,\ q \to r\ ,\ r \to s\}$. The following is a derivation of $\Gamma \vdash p \to s$

1	$\Gamma,\ p \vdash p$	(Hyp)
2	$\Gamma,\ p \vdash p \to q \vee r$	(Hyp)
3	$\Gamma,\ p \vdash q \vee r$	$(\to E)\ 1, 2$
4	$\Gamma,\ p,\ q \vdash q$	(Hyp)
5	$\Gamma,\ p,\ q \vdash q \to r$	(Hyp)
6	$\Gamma,\ p,\ q \vdash r$	$(\to E)\ 4, 5$
7	$\Gamma,\ p,\ r \vdash r$	(Hyp)
8	$\Gamma,\ p \vdash r$	$(\vee E)\ 3, 6, 7$
9	$\Gamma,\ p \vdash r \to s$	(Hyp)
10	$\Gamma,\ p \vdash s$	$(\to E)\ 8, 9$
11	$\Gamma \vdash p \to s$	$(\to I)\ 10$

Proof example

Natural deduction in sequent style

Let $\Gamma = \{p \to q \vee r\ ,\ q \to r\ ,\ r \to s\}$. The following is a derivation of $\Gamma \vdash p \to s$

1	$\Gamma,\ p \vdash p$	(Hyp)
2	$\Gamma,\ p \vdash p \to q \vee r$	(Hyp)
3	$\Gamma,\ p \vdash q \vee r$	$(\to E)\ 1, 2$
4	$\Gamma,\ p,\ q \vdash q$	(Hyp)
5	$\Gamma,\ p,\ q \vdash q \to r$	(Hyp)
6	$\Gamma,\ p,\ q \vdash r$	$(\to E)\ 4, 5$
7	$\Gamma,\ p,\ r \vdash r$	(Hyp)
8	$\Gamma,\ p \vdash r$	$(\vee E)\ 3, 6, 7$
9	$\Gamma,\ p \vdash r \to s$	(Hyp)
10	$\Gamma,\ p \vdash s$	$(\to E)\ 8, 9$
11	$\Gamma \vdash p \to s$	$(\to I)\ 10$

Proof example

Practical logic

Let $\Gamma = \{p \to q \vee r\ ,\ q \to r\ ,\ r \to s\}$. The following is a derivation of $\Gamma \vdash p \to s$

1	$p \to q \vee r, q \to r, r \to s, p, q \vdash q$	(Hyp)
2	$p \to q \vee r, q \to r, r \to s, p, q \vdash r$	$(\to L)$ 1
3	$p \to q \vee r, q \to r, r \to s, p, r \vdash r$	(Hyp)
4	$p \to q \vee r, q \to r, r \to s, p \vdash p$	(Hyp)
5	$p \to q \vee r, q \to r, r \to s, p, q \vee r \vdash r$	$(\vee L)$ 2, 3
6	$p \to q \vee r, q \to r, r \to s, p \vdash q \vee r$	$(\to L)$ 4
7	$p \to q \vee r, q \to r, r \to s, p \vdash r$	(Cut) 5, 6
8	$p \to q \vee r, q \to r, r \to s, p \vdash s$	$(\to L)$ 7
9	$p \to q \vee r, q \to r, r \to s \vdash p \to s$	$(\to R)$ 8

Proof example

Practical logic

Let $\Gamma = \{p \to q \vee r\ ,\ q \to r\ ,\ r \to s\}$. The following is a derivation of $\Gamma \vdash p \to s$

1	$p \to q \vee r, q \to r, r \to s, p, q \vdash q$	(Hyp)
2	$p \to q \vee r, q \to r, r \to s, p, q \vdash r$	$(\to L)$ 1
3	$p \to q \vee r, q \to r, r \to s, p, r \vdash r$	(Hyp)
4	$p \to q \vee r, q \to r, r \to s, p \vdash p$	(Hyp)
5	$p \to q \vee r, q \to r, r \to s, p, q \vee r \vdash r$	$(\vee L)$ 2, 3
6	$p \to q \vee r, q \to r, r \to s, p \vdash q \vee r$	$(\to L)$ 4
7	$p \to q \vee r, q \to r, r \to s, p \vdash r$	(Cut) 5, 6
8	$p \to q \vee r, q \to r, r \to s, p \vdash s$	$(\to L)$ 7
9	$p \to q \vee r, q \to r, r \to s \vdash p \to s$	$(\to R)$ 8

Proof example

Practical logic

Let $\Gamma = \{p \to q \vee r\ ,\ q \to r\ ,\ r \to s\}$. The following is a derivation of $\Gamma \vdash p \to s$

1	$p \to q \vee r, q \to r, r \to s, p, q \vdash q$	(Hyp)
2	$p \to q \vee r, q \to r, r \to s, p, q \vdash r$	$(\to L)$ 1
3	$p \to q \vee r, q \to r, r \to s, p, r \vdash r$	(Hyp)
4	$p \to q \vee r, q \to r, r \to s, p \vdash p$	(Hyp)
5	$p \to q \vee r, q \to r, r \to s, p, q \vee r \vdash r$	$(\vee L)$ 2, 3
6	$p \to q \vee r, q \to r, r \to s, p \vdash q \vee r$	$(\to L)$ 4
7	$p \to q \vee r, q \to r, r \to s, p \vdash r$	(Cut) 5, 6
8	$p \to q \vee r, q \to r, r \to s, p \vdash s$	$(\to L)$ 7
9	$p \to q \vee r, q \to r, r \to s \vdash p \to s$	$(\to R)$ 8

Backwards reading of a rule

$$\frac{\Gamma_1 \vdash A_1 \ldots \Gamma_n \vdash A_n}{\Gamma \vdash B}$$

- To prove $\Gamma \vdash B$ it suffices to show $\Gamma_1 \vdash A_1 \ldots \Gamma_n \vdash A_n$
- This property is formalized by means of a transition rule:

$$\Gamma \vdash B \ \rhd \ \Gamma_1 \vdash A_1 \ ; \ \ldots \ ; \ \Gamma_n \vdash A_n$$

- Read $\rhd$ as "it suffices to show"
- Any such transition rule is called a tactic. (Edinburgh LCF)
- The transition system corresponds to interactive backward proof-search

Tactics

Examples

- Or introduction:

$$\Gamma \vdash A \vee B \quad \rhd \quad \Gamma \vdash A$$

- Classical Or introduction:

$$\Gamma \vdash A \vee B \quad \rhd \quad \Gamma, \neg A \vdash B$$

- Conditional introduction:

$$\Gamma \vdash A \to B \quad \rhd \quad \Gamma, A \vdash B$$

- Classical conditional introduction by contrapositive:

$$\Gamma \vdash A \to B \quad \rhd \quad \Gamma, \neg B \vdash \neg A$$

Tactics

examples

- Proof by contradiction:

$$\Gamma \vdash B \ \rhd \ \Gamma, \neg B \vdash A \quad ; \quad \Gamma, \neg B \vdash \neg A$$

- Proof by dichotomy:

$$\Gamma \vdash B \ \rhd \ \Gamma, A \vdash B \quad ; \quad \Gamma, \neg A \vdash B$$

- Proof by transitivity:

$$\Gamma \vdash s = t \ \rhd \ \Gamma \vdash s = r \quad ; \quad \Gamma \vdash r = t$$

The cut rule

One inference rule but two tactics

$$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \textsc{Cut}$$

- This rule generates two operationally different tactics:

  Assert A:

  $$\Gamma, B \vdash A \ \rhd\ \Gamma \vdash A\ ;\ \Gamma, A \vdash B$$

  Cut A:

  $$\Gamma, B \vdash A \ \rhd\ \Gamma, A \vdash B\ ;\ \Gamma \vdash A$$

- The user needs to propose the specific A. Automation is difficult here.
- We prefer *interaction* between the human and the machine.

The transition system $\mathcal{T}$

$$\mathcal{T} = \langle \mathbb{S},\ \mathcal{I},\ \mathcal{F},\ \rhd \rangle$$

- $\mathbb{S}$ is the set of states. A state $\mathcal{S} \in \mathbb{S}$ is a finite sequence of goals (sequents).
- $\mathcal{I} = \mathit{Seq}$ is the set of initial states. An initial state is just a sequent.
- $\mathcal{F} = \{\Box\}$ is the set of final states, where $\Box$ denotes the empty list of goals.
- $\rhd \subseteq \mathbb{S} \times \mathbb{S}$ is the transition relation, inductively defined by

$$\frac{}{\mathcal{S} \rhd \mathcal{S}'}\ \textsc{Basic} \qquad \frac{\mathcal{S}_1 \rhd \mathcal{S}_2}{\mathcal{S}_1; \mathcal{S} \ \rhd\ \mathcal{S}_2; \mathcal{S}}\ \textsc{append}$$

Conclusion Analysis (Right rules)

Tactics

- `intro` $\mathcal{H}$:

$$\Gamma \vdash A \to B \quad \rhd \quad \Gamma, \mathcal{H} : A \vdash B$$

- `split`:

$$\Gamma \vdash A \wedge B \quad \rhd \quad \Gamma \vdash A \ ; \ \Gamma \vdash B$$

- `left`:

$$\Gamma \vdash A \vee B \quad \rhd \quad \Gamma \vdash A$$

- `classical right`:

$$\Gamma \vdash A \vee B \quad \rhd \quad \Gamma, \mathcal{H} : \neg A \vdash B$$

Premise Analysis (Left rules)

Tactics

- `apply` $\mathcal{H}$:

$$\Gamma, \mathcal{H} : A \to B; \Gamma' \vdash B \quad \rhd \quad \Gamma, \mathcal{H} : A \to B; \Gamma' \vdash A$$

- `destruct` $\mathcal{H}$:

$$\Gamma, \mathcal{H} : A \wedge B; \Gamma' \vdash C \quad \rhd \quad \Gamma, \mathcal{H}_1 : A, \mathcal{H}_2 : B; \Gamma' \vdash C$$

- `destruct` $\mathcal{H}$:

$$\Gamma, \mathcal{H} : A \vee B; \Gamma' \vdash C \ \rhd \ \Gamma, \mathcal{H} : A \vdash C; \Gamma', \mathcal{H} : B \vdash C$$

Lemma Assertion (Cut rule)

Tactics

- `assert` A:

$$\Gamma \vdash C \quad \rhd \quad \Gamma \vdash A \;;\; \Gamma, \mathcal{H} : A \vdash C$$

- `cut` A:

$$\Gamma \vdash C \quad \rhd \quad \Gamma, \mathcal{H} : A \vdash C \;;\; \Gamma \vdash A$$

Trivial proofs

Tactics

- `assumption`:

$$\Gamma, \mathcal{H} : A; \Gamma' \vdash A \quad \triangleright \quad \square$$

- `apply` $\mathcal{H}$:

$$\Gamma, \mathcal{H} : \forall x A \vdash A[x := t] \quad \triangleright \quad \square$$

- `explosion`:

$$\Gamma; \mathcal{H} : A; \Gamma', \mathcal{H}_1 : \neg A; \Gamma'' \vdash B \quad \triangleright \quad \square$$

- `reflexivity`:

$$\Gamma \vdash t = t \quad \triangleright \quad \square$$

A backward proof

Proving with tactics

Let $\Gamma = \{\mathcal{H}_1 : p \to q \vee r,\ \mathcal{H}_2 : q \to r,\ \mathcal{H}_3 : r \to s\}$. The following is a backward proof of $\Gamma \vdash p \to s$

1	$\Gamma \vdash p \to s$	original goal
2	$\Gamma,\ \mathcal{H}_4 : p \vdash s$	intro $\mathcal{H}_4$
3	$\Gamma,\ \mathcal{H}_4 : p \vdash r$	apply $\mathcal{H}_3$
4	$\Gamma,\ \mathcal{H}_4 : p \vdash q \vee r \quad ; \quad \Gamma,\ \mathcal{H}_4 : p,\ \mathcal{H}_5 : q \vee r \vdash r$	assert $\mathcal{H}_5 : q \vee r$
5	$\Gamma,\ \mathcal{H}_4 : p \vdash p \quad ; \quad \Gamma,\ \mathcal{H}_4 : p,\ \mathcal{H}_5 : q \vee r \vdash r$	apply $\mathcal{H}_1$
6	$\Gamma,\ \mathcal{H}_4 : p,\ \mathcal{H}_5 : q \vee r \vdash r$	assumption
7	$\Gamma,\ p,\ \mathcal{H}_5 : q \vdash r \quad ; \quad \Gamma,\ p,\ \mathcal{H}_6 : r \vdash r$	destruct $\mathcal{H}_5$
8	$\Gamma,\ p,\ \mathcal{H}_5 : q \vdash q \quad ; \quad \Gamma,\ p,\ \mathcal{H}_6 : r \vdash r$	apply $\mathcal{H}_2$
9	$\Gamma,\ p,\ \mathcal{H}_6 : r \vdash r$	assumption
10	$\square$	assumption

Working backwards is a valid proof method

Theorem (Equivalence of $\vdash$ and $\rhd^+$)

Let $\Gamma \vdash A$ be any sequent and $\rhd^+$ be the transitive closure of $\rhd$. The following conditions are equivalent:

(i). $\Gamma \vdash A \quad \rhd^+ \quad \square$

(ii). $\Gamma \vdash A$ *is derivable.*

- A direct consequence is that there is no need to pursue (ii) once we have (i). That is, the backward proof suffices. This is what formal verification tasks need.
- This fills the gap between deductive systems and operational proof mechanisms of computer-assisted proofs.

Final remarks

- Our notion of backward proof with tactics puts Kanger's definition at work and is applicable to other logics (e.g. Modal logic S4) or even to any formalism defined by inference rules.
- Structural rules: provide low-level tactics needed in the mechanization of structural proof-theory (cut-elimination)
- Teaching related: The transition sytem of tactics allows to learn the basic operational mechanisms of a state-of-the-art proof assistant, and provides a smooth migration from pure deductive systems to a practical use of logic.
- Goal-oriented proof theory: connections to Gabbay/Olivetti work. What can the theory of transition systems say about deductive systems?.

Thank you very much!