Automating inductive proof

Citation for published version:
Bundy, A 2014, Automating inductive proof. in M Baaz & S Hetzl (eds), Perspectives on Induction: Special session of the Logic Colloquium at the Vienna Summer of Logic. Vienna Summer of Logic, Vienna, Austria, pp. 19.

Automating Inductive Proof

Alan Bundy
School of Informatics
University of Edinburgh

Perspectives on Induction

18^{th} July 2014

Practical Importance of Inductive Proof

Needed for reasoning about repetition, e.g.:

- recursive data stuctures;
- recursion and interative programs & plans;
- parameterised hardware,
  e.g., n-bit adder;
- traces of programs,
  e.g., microprocessor, security protocol;

Theoretical Impediments

- Gödel's incompleteness theorems.
- Undecidability of halting problem.
- Lack of cut elimination.

Lack of Cut Elimination

Gentzen's Cut Rule:

$$\frac{\boldsymbol{A}, \Gamma \vdash \Delta, \quad \Gamma \vdash \boldsymbol{A}}{\Gamma \vdash \Delta}$$

lacks subformula property.

Cut Elimination Theorem:

Gentzen showed Cut Rule redundant in FOL.

But necessary in inductive theories.

Practical Consequences:

Need to generalise conjectures.

Need to introduce intermediate lemmas.

Need for non-standard induction rules.

Need for Intermediate Lemmas

Conjecture:

$$\forall l{:}list(\tau).\ rev(rev(l)) = l$$

Rewrite Rules:

$$(nil) <> L \Rightarrow L$$
$$(H :: T) <> L \Rightarrow H :: (T <> L)$$

$$rev(nil) \Rightarrow nil$$
$$rev(H :: T) \Rightarrow rev(T) <> (H :: nil)$$

Upper case indicates meta-variable.

Step Case:

$$rev(rev(t)) = t \vdash rev(\boldsymbol{rev(h :: t)}) = h :: t$$
$$\vdash \underbrace{\boldsymbol{rev(rev(t) <> (h :: nil))}}_{\textbf{blocked}} = h :: t$$

Introducing an Intermediate Lemma

Lemma Required:

$$rev(X <> Y) \Rightarrow rev(Y) <> rev(X)$$

Cut Rule: introduces this:

Original: $\Gamma \vdash rev(rev(l)) = l$

New:

$$\Gamma, \boldsymbol{rev(X <> Y) \Rightarrow rev(Y) <> rev(X)}$$
$$\vdash rev(rev(l)) = l$$

Justification:

$$\Gamma \vdash \boldsymbol{rev(X <> Y) \Rightarrow rev(Y) <> rev(X)}$$

Heuristics needed: to speculate lemma.

Step Case Unblocked

$rev(rev(t)) = t$

$\vdash rev(\boldsymbol{rev(h :: t)}) = h :: t$

$\vdash \boldsymbol{rev(rev(t) <> (h :: nil))} = h :: t$

$\vdash \boldsymbol{rev(h :: nil)} <> rev(rev(t)) = h :: t$

$\vdash (\boldsymbol{rev(nil)} <> (h :: nil)) <> rev(rev(t)) = h :: t$

$\vdash (\boldsymbol{nil <> (h :: nil)}) <> rev(rev(t)) = h :: t$

$\vdash \boldsymbol{(h :: nil) <> rev(rev(t))} = h :: t$

$\vdash h :: (\boldsymbol{nil <> rev(rev(t))}) = h :: t$

$\vdash \boldsymbol{h :: rev(rev(t)) = h :: t}$

$\vdash h = h \wedge \boldsymbol{rev(rev(t)) = t}$

Now possible to use induction hypothesis.

Rippling in the Step Case

$$t <> (Y <> Z) = (t <> Y) <> Z$$

$$\vdash \boxed{h :: \underline{t}}^{\uparrow} <> (y <> z) = (\boxed{h :: \underline{t}}^{\uparrow} <> y) <> z$$

$$\vdash \boxed{h :: \underline{t <> (y <> z)}}^{\uparrow} = \boxed{h :: \underline{t <> y}}^{\uparrow} <> z$$

$$\vdash \boxed{h :: \underline{t <> (y <> z)}}^{\uparrow} = \boxed{h :: \underline{(t <> y) <> z}}^{\uparrow}$$

$$\vdash \boxed{h = h \wedge \underline{t <> (y <> z) = (t <> y) <> z}}^{\uparrow}$$

- Changing bits in $\boxed{\textit{orange boxes}}^{\uparrow}$ (wave-fronts).
- Unchanging bits in ***red*** (skeleton).
- Shows embedding of induction hypothesis in induction conclusion.

Wave-Rules

$$\boxed{H :: \underline{\boldsymbol{T}}}^{\uparrow} <> \boldsymbol{L} \Rightarrow \boxed{H :: \underline{\boldsymbol{T} <> \boldsymbol{L}}}^{\uparrow}$$

$$\boldsymbol{rev}(\boxed{H :: \underline{\boldsymbol{T}}}^{\uparrow}) \Rightarrow \boxed{\underline{\boldsymbol{rev}(\boldsymbol{T})} <> (H :: nil)}^{\uparrow}$$

$$\boxed{X_1 :: \underline{\boldsymbol{X_2}}}^{\uparrow} = \boxed{Y_1 :: \underline{\boldsymbol{Y_2}}}^{\uparrow} \Rightarrow \boxed{X_1 = Y_1 \wedge \underline{\boldsymbol{X_2} = \boldsymbol{Y_2}}}^{\uparrow}$$

$$\boldsymbol{X} <> \boxed{(\underline{\boldsymbol{Y}} <> Z)}^{\uparrow} \Rightarrow \boxed{(\underline{\boldsymbol{X} <> \boldsymbol{Y}}) <> Z}^{\uparrow}$$

- Note preservation of skeleton and
- outward movement of wave-fronts.

Rippling Sideways and In

$$rev(t) <> L = qrev(t, L)$$

$$\vdash rev(\boxed{h :: \boxed{t}}^{\uparrow}) <> \lfloor l \rfloor = qrev(\boxed{h :: \boxed{t}}^{\uparrow}, \lfloor l \rfloor)$$

$$\vdash (\boxed{\boxed{rev(t)} <> (h :: nil)}^{\uparrow}) <> \lfloor l \rfloor = qrev(t, \boxed{h :: \boxed{\lfloor l \rfloor}}^{\downarrow})$$

$$\vdash rev(t) <> (\boxed{(h :: nil) <> \boxed{\lfloor l \rfloor}}^{\downarrow}) = qrev(t, \lfloor h :: l \rfloor)$$

$$\vdash rev(t) <> (\lfloor (h :: nil) <> l \rfloor) = qrev(t, \lfloor h :: l \rfloor)$$

$$\vdash rev(t) <> (\lfloor h :: l \rfloor) = qrev(t, \lfloor h :: l \rfloor)$$

- Using induction hypothesis unifies L with $\lfloor h :: l \rfloor$.
- $\lfloor Sinks \rfloor$ provide alternative wave-front destination, available when free variables are in hypothesis.
- Wave-fronts have directions: $\boxed{out}^{\uparrow}$ / $\boxed{in}^{\downarrow}$.
- Note that sinks and wave-fronts may need to be simplified, but this is skeleton preserving.

Sideways and Inwards Wave-rules

$$qrev(\boxed{H :: \underline{T}}^{\uparrow}, L) \Rightarrow qrev(T, \boxed{H :: \underline{L}}^{\downarrow})$$

$$\boxed{H :: \underline{T <> L}}^{\downarrow} \Rightarrow \boxed{H :: \underline{T}}^{\downarrow} <> L$$

$$(\boxed{\underline{X} <> Y}^{\uparrow}) <> Z \Rightarrow X <> (\boxed{Y <> \underline{Z}}^{\downarrow})$$

- Note that some equations can be annotated in both directions.

$$\boxed{H :: \underline{T}}^{\uparrow} <> L \Rightarrow \boxed{H :: \underline{T <> L}}^{\uparrow}$$

$$H :: \boxed{\underline{T} <> L}^{\uparrow} \Rightarrow \boxed{\underline{H :: T} <> L}^{\uparrow}$$

$$X <> (\boxed{Y <> \underline{Z}}^{\uparrow}) \Rightarrow (\boxed{\underline{X} <> Y}^{\downarrow}) <> Z$$

Preconditions of the Wave Method

1. The induction conclusion contains a wave-front,

   e.g. $\ldots = qrev(\boxed{h :: \underline{t}}^{\uparrow}, \lfloor l \rfloor)$.

2. A wave-rule applies to this wave-front.

   e.g. $qrev(\boxed{H :: \underline{T}}^{\uparrow}, L) \Rightarrow qrev(T, \boxed{H :: \underline{L}}^{\downarrow})$.

3. Any condition is provable.

   e.g. $X \neq H \rightarrow X \in \boxed{H :: \underline{T}}^{\uparrow} \Rightarrow X \in T$.

4. Inserted inwards wave-fronts contain a sink or an outwards wave-front.

   e.g. $\ldots = qrev(t, \boxed{h :: \underline{\lfloor l \rfloor}}^{\downarrow})$.

Advantages of Rippling

Selective: not exhaustive rewriting.

skeleton preserving and measure decreasing.

Bi-directional: rewriting.

different annotations in each direction.

Termination: of any set of wave-rules,

despite bi-directionality.

Heuristic basis: for choosing lemmas,

generalisations, case splits and inductions.

Ripple-Based Heuristics

Induction Rules: choose induction which best supports rippling.

Lemmas: design wave-rule to unblock ripple.

Generalisation: generalise goal to allow wave-rule to apply.

Critic: Lemma Speculation

Conjecture:

$$rev(rev(L)) = L$$

Wave-Rule:

$$rev(\boxed{H :: \underline{T}}^{\uparrow}) \Rightarrow \boxed{\underline{rev(T)} <> H :: nil}^{\uparrow}$$

Induction Conclusion:

$$rev(rev(\boxed{h :: \underline{t}}^{\uparrow})) = \boxed{h :: \underline{t}}^{\uparrow}$$

$$\underbrace{rev(\boxed{\underline{rev(t)} <> (h :: nil)}^{\uparrow})}_{\textbf{blocked}} = \boxed{h :: \underline{t}}^{\uparrow}$$

Pattern Sought:

$$rev(\boxed{\underline{X} <> Y}^{\uparrow}) \Rightarrow \boxed{F(\underline{rev(X)}, X, Y)}^{\uparrow}$$

Lemma Discovered:

$$rev(\boxed{\underline{X} <> Y}^{\uparrow}) \Rightarrow \boxed{rev(Y) <> \underline{rev(X)}}^{\uparrow}$$

Failure of Ripple Precondition

- Precondition 1 is true:

1. The induction conclusion contains a wave-front.

$$\boldsymbol{rev}(\boxed{\boldsymbol{rev(t)} <> (h :: nil)}^{\uparrow}) = \boxed{h :: \boldsymbol{t}}^{\uparrow}$$

(in fact, two)

- Precondition 2 is false:

2. A wave-rule applies to this wave-front.
(to neither of them)

- Preconditions 3 and 4 are inapplicable.

3. Any condition is provable.
4. Inserted inwards wave-fronts contain a sink or an outwards wave-front.

Rippling Failure: Missing Sink

Conjecture:

$$\forall t{:}list(\tau).\ rev(t) = qrev(t, nil)$$

Wave-Rules:

$$rev(\boxed{H :: \underline{T}}^{\uparrow}) \Rightarrow \boxed{\underline{rev(T)} <> H :: nil}^{\uparrow}$$

$$qrev(\boxed{H :: \underline{T}}^{\uparrow}, L) \Rightarrow qrev(T, \boxed{H :: \underline{L}}^{\downarrow})$$

Induction Conclusion:

$$rev(\boxed{h :: \underline{t}}^{\uparrow}) = qrev(\boxed{h :: \underline{t}}^{\uparrow}, nil)$$

$$\boxed{\underline{rev(t)} <> h :: nil}^{\uparrow} = \underbrace{qrev(\boxed{h :: \underline{t}}^{\uparrow}, nil)}_{\text{missing sink}}$$

Failure of Ripple Precondition

- Preconditions 1, 2 and 3 are true:

1. The induction conclusion contains a wave-front.

$$\ldots = qrev(\boxed{h :: \underline{t}}^{\uparrow}, nil)$$

2. A wave-rule applies to this wave-front.

$$qrev(\boxed{H :: \underline{T}}^{\uparrow}, L) \Rightarrow qrev(T, \boxed{H :: \underline{L}}^{\downarrow})$$

3. Any condition is provable — trivially, no condition.

- Precondition 4 is false:

4. Inserted inwards wave-fronts contain a sink or an outwards wave-front.

$$\ldots = qrev(t, \boxed{h :: \underline{nil}}^{\downarrow})$$

Patch: Sink Speculation

Original Conjecture:

$$\forall t\!:\!list(\tau).\ rev(t) = qrev(t, nil)$$

Disallowed Ripple:

$$\ldots = \boldsymbol{qrev(t,}\ \boxed{h :: \boldsymbol{nil}}^{\downarrow}\ \boldsymbol{)}$$

Schematic Conjecture:

$$\forall t\!:\!list(\tau).\forall l\!:\!list(\tau).\ F(rev(t), l) = qrev(t, G(l))$$

Induction Hypothesis:

$$\boldsymbol{F(rev(t), L) = qrev(t, G(L))}$$

where F, G and L are meta-variables.

Patch: Instantiating the Meta-Variables

New Step Case:

$$F(rev(\underbrace{h :: \underline{t}}^{\uparrow}), \lfloor l \rfloor) \quad = \quad qrev(\underbrace{h :: \underline{t}}^{\uparrow}, G(\lfloor l \rfloor))$$

$$F(\underbrace{\underline{rev(t)} <> h :: nil}^{\uparrow}, \lfloor l \rfloor) \quad = \quad qrev(t, \underbrace{h :: \underline{G(\lfloor l \rfloor)}}^{\downarrow})$$

$$rev(t) <> (\underbrace{h :: nil <> \underline{F'(\underbrace{\underline{rev(t)} <> (h :: nil)}^{\uparrow}, \lfloor l \rfloor)}}^{\downarrow})$$

$$= \quad qrev(t, \underbrace{h :: \underline{G(\lfloor l \rfloor)}}^{\downarrow})$$

$$rev(t) <> (\underbrace{h :: \underline{F'(\underbrace{\underline{rev(t)} <> (h :: nil)}^{\uparrow}, \lfloor l \rfloor)}}^{\downarrow})$$

$$= \quad qrev(t, \underbrace{h :: \underline{G(\lfloor l \rfloor)}}^{\downarrow})$$

$$rev(t) <> (\lfloor h :: l \rfloor) \quad = \quad qrev(t, \lfloor h :: l \rfloor)$$

where $F = <>$, $F' = \lambda X. \lambda Y.\ Y$ and $G = \lambda X.\ X$.

Key Wave-Rule: $(\underbrace{\underline{X} <> Y}^{\uparrow}) <> Z \Rightarrow X <> (\underbrace{Y <> \underline{Z}}^{\downarrow})$

Generalised Conjecture:

$$\forall t{:}list(\tau). \forall l{:}list(\tau).\ rev(t) <> l = qrev(t, l)$$

Pattern of Failure Suggests Patch

	PC 1	PC 2	PC 3	PC 4
Generalization	$\surd$	$\surd$	$\surd$	$\times$
Case Split	$\surd$	$\surd$	$\times$	
Induction Revision	$\surd$	?		
Lemma Discovery	$\surd$	$\times$		

$\surd$ = success ? = partial success $\times$ = failure

Conclusion

- Negative theoretical results create special search problems,

  especially lack of cut elimination.

- These problems common in practice:

  induction rule choice, lemmas & generalisations.

- Inductive step case guided by rippling.

- Rippling: selective; bidirectional; terminating and

  offers heuristic choice of cut formula.

- Ripple breakdowns suggest: induction revision; lemma speculation or generalisation.

  Different patterns of proof breakdown suggest different patches.

- Implemented via proof planning with critics.