Issues in Machine-checking the Decidability of Implicational Ticket Entailment

Jeremy Dawson, Rajeev Goré

Logic and Computation Group
Research School of Computer Science
The Australian National University
jeremy.dawson@anu.edu.au

September 29, 2017

Overview

The logics, and their calculi

Modelling derivations in Isabelle (sample!)

Admissibility results confirmed

Relations between the calculi

The decidability argument

Axiomatisations of various logics

Name	Axioms	Logic			
		$T_{\to}$	$T^{\mathbf{t}}_{\to}$	$R_{\to}$	$R^{\mathbf{t}}_{\to}$
(A1)	$A \to A$	✓	✓	✓	✓
(A2)	$(A \to B) \to (C \to A) \to (C \to B)$	✓	✓	✓	✓
(A3)	$(A \to B \to C) \to (B \to A \to C)$			✓	✓
(A4)	$(A \to A \to B) \to (A \to B)$	✓	✓	✓	✓
(A5)	$(A \to B) \to (B \to C) \to (A \to C)$	✓	✓		
Name	Rules of Inference				
(R1)	from $A \to B$ and A, deduce B	✓	✓	✓	✓
(R2)	$\vdash A \,//\, \vdash \mathbf{t} \to A$		✓		✓

(Multiset) Sequent Rules and Calculi

$$(\mathrm{id})\ \frac{}{A \vdash A} \qquad (\to\vdash)\ \frac{\Gamma_1 \vdash A \qquad B, \Gamma_2 \vdash C}{\Gamma_1, A \to B, \Gamma_2 \vdash C} \qquad (\vdash\to)\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

$$(\mathrm{W}\vdash)\ \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C} \qquad (\mathbf{t}\vdash)\ \frac{\Gamma \vdash C}{\mathbf{t}, \Gamma \vdash C} \qquad (\vdash \mathbf{t})\ \frac{}{\vdash \mathbf{t}}$$

$$[\to\vdash]\ \frac{\Gamma_1 \vdash A \qquad B, \Gamma_2 \vdash C}{[\Gamma_1, A \to B, \Gamma_2] \vdash C}\ \dagger$$

In the $[\to\vdash]$ rule, $[\Gamma_1, A \to B, \Gamma_2] \vdash C$ means $\Gamma_1, A \to B, \Gamma_2 \vdash C$, then *some* contraction

	(id)	$(\to\vdash)$	$(\vdash\to)$	$(\mathrm{W}\vdash)$	$(\mathbf{t}\vdash)$	$(\vdash\mathbf{t})$	$[\to\vdash]$
$LR_\to$	✓	✓	✓	✓			
$LR^{\mathbf{t}}_\to$	✓	✓	✓	✓	✓	✓	
$[LR_\to]$	✓	✓	✓				✓
$[LR^{\mathbf{t}}_\to]$	✓	✓	✓		✓	✓	✓

(Structure) Consecution Rules and Calculi

$$LT^{\mathbf{t}}_{\rightarrow}$$

$$(\mathrm{id};)\ \frac{}{A \vdash A} \qquad (\mathrm{W}\vdash;)\ \frac{U\{X\ ;\ Y\ ;\ Y\} \vdash C}{U\{X\ ;\ Y\} \vdash C}$$

$$(\rightarrow\vdash;)\ \frac{V \vdash A \qquad U\{B\} \vdash C}{U\{A \rightarrow B\ ;\ V\} \vdash C} \qquad (\vdash\rightarrow;)\ \frac{U\ ;\ A \vdash B}{U \vdash A \rightarrow B}$$

$$(\mathrm{B}\vdash;)\ \frac{U\{X\ ;\ (Y\ ;\ Z)\} \vdash C}{U\{X\ ;\ Y\ ;\ Z\} \vdash C} \qquad (\mathrm{B}'\vdash;)\ \frac{U\{X\ ;\ (Z\ ;\ Y)\} \vdash C}{U\{Z\ ;\ X\ ;\ Y\} \vdash C}$$

$$(\mathrm{KI}_{\mathbf{t}}\vdash;)\ \frac{U\{Y\} \vdash C}{U\{\mathbf{t}\ ;\ Y\} \vdash C} \qquad (\mathrm{M}_{\mathbf{t}}\vdash;)\ \frac{U\{\mathbf{t}\ ;\ \mathbf{t}\} \vdash C}{U\{\mathbf{t}\} \vdash C}$$

$$LT^{ⓣ}_{\rightarrow} \ :=\ LT^{\mathbf{t}}_{\rightarrow} \ +\ (\mathrm{K}_{\mathbf{t}}\vdash;)\ +\ (\mathrm{T}_{\mathbf{t}}\vdash;)$$

$$(\mathrm{K}_{\mathbf{t}}\vdash;)\ \frac{U\{Y\} \vdash C}{U\{Y\ ;\ \mathbf{t}\} \vdash C} \qquad (\mathrm{T}_{\mathbf{t}}\vdash;)\ \frac{U\{Y\ ;\ \mathbf{t}\} \vdash C}{U\{\mathbf{t}\ ;\ Y\} \vdash C}$$

Goal is decidability of $T^{\mathbf{t}}_{\rightarrow}$

- There is a decidable sequent calculus $[LR^{\mathbf{t}}_{\rightarrow}]$ for $R^{\mathbf{t}}_{\rightarrow}$
- There is a consecution calculus $LT^{ⓣ}_{\rightarrow}$ for $R^{\mathbf{t}}_{\rightarrow}$
- There is a consecution calculus $LT^{\mathbf{t}}_{\rightarrow}$ for $T^{\mathbf{t}}_{\rightarrow}$
-
- $LT^{ⓣ}_{\rightarrow}$ is $LT^{\mathbf{t}}_{\rightarrow}$ plus two more rules
-
- Aim is decidability of $T^{\mathbf{t}}_{\rightarrow}$ by
  - look at all proofs in $[LR^{\mathbf{t}}_{\rightarrow}]$
  - translate them to proofs in consecution calculus $LT^{ⓣ}_{\rightarrow}$
  - if any is in $LT^{\mathbf{t}}_{\rightarrow}$, then theorem of $T^{\mathbf{t}}_{\rightarrow}$, else non-theorem

Derivability in Isabelle

- Capture the implicit fact of derivability

```
 'a psc = "'a list * 'a" (* single inference *)
derl ::  "'a psc set => 'a psc set"
derrec ::  "'a psc set => 'a set => 'a set"
```

- Neat example theorems

```
"derrec ?rls (derrec ?rls ?ps) = derrec ?rls ?ps"
"derl (derl ?rls) = derl ?rls"
"derrec (derl ?rls) ?prems = derrec ?rls ?prems"
```

- Alternatively, concrete structure representing explicit derivation tree

```
 datatype 'a dertree = Der 'a ('a dertree list)
          | Unf 'a (* unfinished, unproved leaf *)
```

- Link these implicit and explicit concepts

Theorem

$c \in \mathtt{derrec}\ \mathtt{rls}\ \{\}$ *iff* $\exists\, dt.\ \mathtt{valid}\, dt\ \&\ \mathtt{conclDT}\, dt = c$

c is $\mathtt{rls}$*-derivable iff there is a valid derivation tree* $\mathtt{dt}$ *with conclusion c*

Substitution in a hole in a structure

- Example: $(X; (Y; Z),\ \ X; Y; Z) \in rls$
- We build the structure around the required substitution

```
 inductive "sctxt r"
intrs
scL "(a, b) :  sctxt r ==> (C;a, C;b) :  sctxt r"
scR "(a, b) :  sctxt r ==> (a;C, b;C) : sctxt r"
scid "(a, b) :  r ==> (a, b) :  sctxt r"
```

- $(U\{X; (Y; Z)\},\ \ U\{X; Y; Z\}) \in \texttt{sctxt}\ rls$
- We turn this into a one-premise rule which does this substitution in the antecedent

```
 inductive "lctxt r"
  intrs
   I "(As, Bs) :  sctxt r ==>
         ([As |- E], Bs |- E) : lctxt r"
```

- $([U\{X; (Y; Z)\} \vdash C],\ \ U\{X; Y; Z\} \vdash C) \in \texttt{lctxt}\ rls$

The complexity this adds to cut-admissibility proofs

- Cut-admissibility proofs require re-ordering rule applications
- Define: $(u, v) \in \texttt{strrep}\ S$, u and v same except may differ at (several) subterms u' and v', where $(u', v') \in S$

```
 inductive "strrep S"
  intrs
  same "(s, s) :  strrep S"
  repl "p :  S ==> p :  strrep S"
  sc "(u, v) :  strrep S ==> (x, y) :  strrep S
     ==> (u; x, v; y) :  strrep S"
```

- "Closing the loop" lemma: if

$$\frac{\mathcal{C}[p]}{\mathcal{C}[c_A]} \xrightarrow{A \to X} C_X$$

then there exist $\mathcal{C}'$ and c_X st $C_X = \mathcal{C}'[c_X]$ where

$$\frac{\mathcal{C}[p] \xrightarrow{A \to X} \mathcal{C}'[p]}{\mathcal{C}[c_A] \xrightarrow{A \to X} \mathcal{C}'[c_X]} \quad \text{and} \quad c_A \xrightarrow{A \to X} c_X$$

Inductive Multi-cut Admissibility via gen_step2

Suppose the conclusions cl and cr have respective derivations as shown below:

$$\dfrac{\dfrac{\mathtt{pl}_1 \ \ldots \ \mathtt{pl}_n}{\mathtt{cl}}\,\rho_l \qquad \dfrac{\mathtt{pr}_1 \ \ldots \ \mathtt{pr}_m}{\mathtt{cr}}\,\rho_r}{?}\,(cut\ ?)$$

- We want to prove an arbitrary property P of these derivations, eg (multi)cut-admissibility for a cut-formula A
- Proof is first, by induction on A, then on "stage in the proof"
- Induction on "stage in the proof" assumes P holds for each $\mathtt{pl}_i$ with cr, and for cl with each $\mathtt{pr}_j$
- gen_step2 expresses a single case of the inductive argument
- we have a lemma that this is enough for P to hold generally

Results for $LR_{\rightarrow}$, $LR^{\mathbf{t}}_{\rightarrow}$, $[LR_{\rightarrow}]$, and $[LR^{\mathbf{t}}_{\rightarrow}]$ in Isabelle

Theorem

$LR_{\rightarrow}$ and $LR^{\mathbf{t}}_{\rightarrow}$ enjoy multi-cut admissibility.

Theorem

$[LR_{\rightarrow}]$ and $[LR^{\mathbf{t}}_{\rightarrow}]$ enjoy contraction admissibility.

Corollary

$[LR_{\rightarrow}]$ and $[LR^{\mathbf{t}}_{\rightarrow}]$ enjoy multi-cut admissibility.

- Proved in a different order from the paper (we couldn't reproduce the proof indicated briefly in B&D)
- OOPS! We actually needed

Theorem

$[LR_{\rightarrow}]$ and $[LR^{\mathbf{t}}_{\rightarrow}]$ enjoy height-preserving contraction admissibility.

This one uses the analogue, for concrete derivation trees, of the `gen_step2` definition and lemmas

Multi-cut admissibility for $LT^{\mathbf{t}}_{\to}$ and $LT^{\textcircled{t}}_{\to}$

- For (multiset) sequents, "multi-cut" meant this:

$$\frac{X \vdash A \qquad A^n, Y \vdash B}{X, Y \vdash B}$$

(just one 'X' in the consequent)

- For (structure) consecutions, we have to define what we mean by multi-cut admissibility.

$$(\text{multicut})\ \frac{X \vdash A \qquad Y\{A\}\{A\}\cdots\{A\} \vdash B}{Y\{X\}\{X\}\cdots\{X\} \vdash B}$$

(multiple occurrences of 'X' in the consequent)

Theorem

$LT^{\mathbf{t}}_{\to}$ and $LT^{\textcircled{t}}_{\to}$ enjoy multi-cut admissibility.

Soundness and Completeness

Theorem

$LT^{\mathbf{t}}_{\rightarrow}$ is complete for $T^{\mathbf{t}}_{\rightarrow}$
$LT^{\textcircled{\mathbf{t}}}_{\rightarrow}$ is complete for $R^{\mathbf{t}}_{\rightarrow}$

For the sequent systems, we have proved

Lemma

for each rule of $LR_{\rightarrow}$ there is a "corresponding" proof in $R_{\rightarrow}$ (for some ordering of antecedents)

We still need to prove that any re-ordering of antecedents in $A_1 \rightarrow A_2 \rightarrow \ldots \rightarrow A_n \rightarrow B$ is provable in $R_{\rightarrow}$

Linking the sequent and consecution systems

Theorem

Given a derivation in $LT^{\textcircled{t}}_{\rightarrow}$, we can, by turning structures into multi-sets, obtain an "equivalent" derivation in $LR^{\mathbf{t}}_{\rightarrow}$. ("equivalent" means "same" premises and conclusion, not necessarily same proof steps)

- This is the transformation π, which we have not actually defined, we have just shown it exists.
- For the converse (using the τ transformation), we need to prove that the rules of $LT^{\textcircled{t}}_{\rightarrow}$ permit any permutation and grouping, into a structure, of any multiset of formulae.
- Lemmas 8,9 and 10 do this for up to 3 formulae (proved in Isabelle, but not in that order!)
- Need to extend this to any number of formulae (we have worked out argument, not proved)

Background to decidability argument

- multiset sequent system $LR^{\mathbf{t}}_{\rightarrow}$ for $R^{\mathbf{t}}_{\rightarrow}$, includes contraction
- $[LR^{\mathbf{t}}_{\rightarrow}]$ incorporates limited contraction into $\rightarrow\vdash$ rule, $[\rightarrow\vdash]$
- this gives height-preserving contraction admissibility, so irredundant derivations, so decidable (Kripke, König lemmas)
- likewise $LR^{\mathbf{t}}_{\rightarrow}$ and $[LR^{\mathbf{t}}_{\rightarrow}]$ for $T^{\mathbf{t}}_{\rightarrow}$
- structure sequent systems $LT^{\textcircled{t}}_{\rightarrow}$ for $R^{\mathbf{t}}_{\rightarrow}$, and $LT^{\mathbf{t}}_{\rightarrow}$ for $T^{\mathbf{t}}_{\rightarrow}$
- proof transformations:
  - π, $LT^{\textcircled{t}}_{\rightarrow}$ to $LR^{\mathbf{t}}_{\rightarrow}$ (loses ordering/grouping)
  - τ, $LR^{\mathbf{t}}_{\rightarrow}$ to $LT^{\textcircled{t}}_{\rightarrow}$ (recreates ordering/grouping)
  - difference between $T^{\mathbf{t}}_{\rightarrow}$ and $R^{\mathbf{t}}_{\rightarrow}$ (ie, between $LR^{\mathbf{t}}_{\rightarrow}$ and $LT^{\textcircled{t}}_{\rightarrow}$) is (complete) availability of re-ordering
  - τ produces several proofs in $LT^{\textcircled{t}}_{\rightarrow}$ (choice of ordering/grouping)

the decidability procedure

- get all proofs in $[LR^{\mathbf{t}}_{\rightarrow}]$
- convert these into proofs in $LR^{\mathbf{t}}_{\rightarrow}$
- transform them, using τ, to proofs in $LT^{ⓣ}_{\rightarrow}$
- examine which of these are proofs in $LT^{\mathbf{t}}_{\rightarrow}$

Issues arising:

- τ involves "all permutations and groupings": should this be "all *proofs of* all permutations and groupings"? (to find proof in $LT^{\mathbf{t}}_{\rightarrow}$, if any)
- even so, τ produces only proofs whose $\vdash\rightarrow$, $\rightarrow\vdash$ and $W\vdash$ are in the same order as the given proof in $LR^{\mathbf{t}}_{\rightarrow}$ — is this enough?
- that is, the algorithm produces only $LT^{ⓣ}_{\rightarrow}$-proofs in which contains these rules in a the same order as a proof in $[LR^{\mathbf{t}}_{\rightarrow}]$ — what if the only $LT^{\mathbf{t}}_{\rightarrow}$-proof contains them in a different order?
- (note that deriving an $[LR^{\mathbf{t}}_{\rightarrow}]$-proof from an $LR^{\mathbf{t}}_{\rightarrow}$-proof changes the order of these rules)

Lemmas supporting τ transformation

8 If $\mathcal{C}[\mathcal{A};\mathcal{B}] \vdash A$ provable in $LT^{\text{ⓣ}}_{\rightarrow}$ then so is $\mathcal{C}[t;(\mathcal{B};\mathcal{A})] \vdash A$ ($\mathcal{C}$ is any structure with a "hole")

9 If $\mathcal{C}[\mathcal{A}_1;\mathcal{A}_2;\mathcal{A}_3] \vdash A$ provable in $LT^{\text{ⓣ}}_{\rightarrow}$ then so are $\mathcal{C}[t;\mathcal{A}_i;\mathcal{A}_j;\mathcal{A}_k] \vdash A$ and $\mathcal{C}[t;\mathcal{A}_i;(\mathcal{A}_j;\mathcal{A}_k)] \vdash A$ (for all permutations i,j,k of $1,2,3$)

10 If $\mathcal{C}[\mathcal{A}_1;\mathcal{A}_2;\mathcal{A}_3] \vdash A$ provable in $LT^{\text{ⓣ}}_{\rightarrow}$ then so are $\mathcal{C}[t;(\mathcal{A}_i;\mathcal{A}_j;\mathcal{A}_k)] \vdash A$ and $\mathcal{C}[t;(\mathcal{A}_i;(\mathcal{A}_j;\mathcal{A}_k))] \vdash A$

- The proof we found for 9 actually uses 10, which we proved first: we didn't find the proof used by B&D
- We also formulated an argument to deal with four or more substructures

Do we actually need these lemmas?

- Lemmas 8,9 and 10: used to prove any permutation/grouping of antecedents is provable in $LT^{\textcircled{t}}_{\rightarrow}$.
- The constructions described translate $LR^{\mathbf{t}}_{\rightarrow}$-proofs to $LT^{\textcircled{t}}_{\rightarrow}$
- We haven't yet found the result (that there exists an $LT^{\textcircled{t}}_{\rightarrow}$-proof) to be necessary.
- The constructions may be relevant to an argument that we will find a proof in $LT^{\mathbf{t}}_{\rightarrow}$, if one exists;
- BUT: if there is no proof in $LT^{\mathbf{t}}_{\rightarrow}$, does it matter if these is no proof in $LT^{\textcircled{t}}_{\rightarrow}$ either?
- We noticed this only when putting together the skeleton of a proof in Isabelle.

Proof trees and König's Lemma

- König's Lemma:
  an infinite, finitely branching, tree has an infinite branch
- When we build a proof tree, bottom (endsequent) up, the intermediate stages have leaves yet unproved.
- We call these *partial proof trees*. We represent an "infinite proof tree" by an increasing sequence of partial proof trees:
- By König's Lemma, if such a sequence is infinite, then there must be a single infinitely increasing branch
- Note: finite branching property, because each rule has finitely many premises
- And by Kripke's lemma there is no infinite irredundant branch of a (partial) proof tree in $[LR^{\mathbf{t}}_{\rightarrow}]$
- Where does this get us?

Proof search trees and König's Lemma

Now consider a *proof search tree*:

- node: partial proof tree,
  edge: extending a partial proof tree by adding one rule.
- This is a different tree!! This one is finitely branching because
  - a partial proof tree has only finitely many unproved leaves, and
  - at each leaf, only finitely many rules can be applied.
- The previous result ("no infinite proof tree") says proof search tree has no infinite branch.
- König's Lemma, again, tells us that the proof search tree is finite, that is, complete proof search is a finite process
- so this logic is decidable.
- This outline uses König's Lemma *twice*! Is this necessary?
- Literature seems to use König's Lemma just once!
  and to confuse proof trees with proof search trees

Proving decidability

- To really formalise decidability, we would need to formalise steps of computation (very low level)
- A finite proof search tree is not enough:
  - imagine a logic L, and we define a new logic L', by
    - Axioms of L': theorems of L
    - Rules of L': none
  - In L', proof search tree (for given endsequent) is tiny, but L' (may be) not decidable.
- We need further informal arguments, eg, that at any point it is straightforward to determine which rules are applicable.

Formalisation

use of Isabelle: work verified in Isabelle theorem prover

value of formal verification: detects gaps which may be overlooked in a proof

value of formalisation without verification: even planning/preparing for formal verification alerts us to problems in a proof

difficult issues: König's lemma: what is an infinite proof tree? how to formalise branch of it

Our main issue

- all $LR^{\mathbf{t}}_{\rightarrow}$-proofs $\longrightarrow$ all $LT^{\textcircled{t}}_{\rightarrow}$-proofs
  - well, let's suppose so
  - actually depends on details of "all *proofs of* all permutations and groupings"
- so all $LR^{\mathbf{t}}_{\rightarrow}$-proofs $\longrightarrow$ (including) all $LT^{\mathbf{t}}_{\rightarrow}$-proofs
- but we need: all $LR^{\mathbf{t}}_{\rightarrow}$-proofs from $[LR^{\mathbf{t}}_{\rightarrow}]$-proofs $\longrightarrow$ at least one $LT^{\mathbf{t}}_{\rightarrow}$-proof (if such exists)
- Question: are all $LR^{\mathbf{t}}_{\rightarrow}$-proofs from $[LR^{\mathbf{t}}_{\rightarrow}]$-proofs sufficiently representative of all $LR^{\mathbf{t}}_{\rightarrow}$-proofs to ensure this?
- Note: are all $LR^{\mathbf{t}}_{\rightarrow}$-proofs from $[LR^{\mathbf{t}}_{\rightarrow}]$-proofs, and the resulting $LT^{\textcircled{t}}_{\rightarrow}$-proofs, have limits on where contractions can appear