Abstract canonical inference: on fairness in theorem proving[1]

Maria Paola Bonacina

Dipartimento di Informatica
Università degli Studi di Verona
Verona, Italy, EU

Talk given at the Department of Informatics, King's College, London, England, UK
(Subsuming a talk with the same title contributed to a meeting of COST Action IC0901 Rich-model toolkit: an infrastructure for reliable computer systems, held as 4th SVARM (System Verification by Automated Reasoning Methods) and 7th VERIFY (Verification) Workshop, 6th Int. Joint Conf. on Automated Reasoning (IJCAR), Manchester, England, UK)

July 2012

[1] Joint work with Nachum Dershowitz

Fairness: what's in a word

Fairness: to be fair

- beautiful, attractive, comely, handsome, pretty
- equitable, just, candid, frank, honest, impartial, unbiased, upright (e.g., fair play)
- mediocre, middling, passable, promising, tolerable
- distinct, open, plain, unobstructed (e.g., fair view)
- bright, clear, cloudless, dry, unclouded (i.e., fair weather)
- blond, clean, clear, light, not dark, unblemished, unspotted, untarnished, white (e.g., fair complexion)

Fairness in computer science

- equitable, just, honest, impartial, unbiased
- scheduling: no starvation (e.g., of processes)
- theorem proving ?

What is theorem proving

S: set of *assumptions*
properties of the object of study
(e.g., system, circuit, program, data type, communication protocol, mathematical structure)

φ: *conjecture*
a property to be verified

Problem: does φ *follow* from S?

$$S \models^{?} \varphi$$

Theorem proving: building proofs or models

$$S \models^{?} \varphi$$

- **Refutational theorem proving:**
  find a *proof* that $S \cup \{\neg\varphi\} \vdash \bot$ and answer affirmatively
- **Model building or theorem disproving:**
  find a *model* of $S \cup \{\neg\varphi\}$, or a *counter-model* (*counter-example*) of $S \models \varphi$, and answer negatively

Some applications of theorem proving

- Analysis, verification, synthesis of SW and HW, e.g.:
  - Static analyses: e.g., test case generation, abstraction refinement, invariant generation
  - Proof of verification conditions for invariant checking
  - Synthesis, e.g.: example generation, invariant generation
- Natural language processing, question answering
- Mathematics: Proving non-trivial theorems in, e.g., Boolean algebras, theories of rings, groups, quasigroups, loops, many-valued logic

Theorem proving based on logic: Fairness in natural deduction?

An example: Smullyan analytic tableaux for PL

- Signed formulæ (e.g., $\mathbf{T}A$, $\mathbf{F}A$)
- Completeness theorem: if A is a tautology, then *every complete* tableau for $\mathbf{F}A$ must close
  where
  - closed tableau: all branches closed
  - complete tableau: all branches either closed or complete
  - *complete* branch: if α then both α_1 and α_2 (e.g., $\mathbf{T}a \wedge b$)
    if β then at least one of β_1 and β_2 (e.g., $\mathbf{T}a \vee b$)

Smullyan analytic tableaux for FOL

Completeness theorem:
if A is valid, *there exists* a closed tableau for $\mathbf{F}A$;
if A is valid, the *systematic* tableau for $\mathbf{F}A$ must close in finitely many steps, where systematic tableau:

- step 1: $\mathbf{F}A$
- step $n+1$: node Y of minimum depth not marked "used"
  for every branch through Y: if α then add α_1 and α_2
  if β then branch with β_1 and β_2
  if δ then add $\delta(a)$ (e.g., $\mathbf{T}\exists x.A$)
  if γ then add $\gamma(a)$ and γ (e.g., $\mathbf{T}\forall x.A$)
  mark Y "used"

Comparison of the examples

- PL: *every complete* tableau for **F***A* must close
  every: may proceed blindly
  (decidable problem, finite search space)
  complete tableau: do everything, neglect nothing
- FOL: *there exists* a closed tableau
  there exists: need to search for one
  (semi-decidable problem, infinite search space)
  systematic tableau: do everything, neglect nothing

First intuition about fairness

- Complete, systematic, exhaustive:
  trivial, brute force ways to be fair
- Propositional logic: finite (huge) search space
  search needed for efficiency
- First-order logic: infinite search space
  search needed for completeness and efficiency
- Fairness: reduce gap between completeness and efficiency;
  neglect nothing .... that's *really* needed!

Theorem-proving strategies

- *Inference system:*
  non-deterministic set of *inference rules*
  defines the *search space* of all possible inferences
- *Search plan:* adds determinism
  controls inference rules application
  guides the search for proof/model

Inference system + search plan = *theorem-proving strategy*
Deterministic: given $S \cup \{\neg\varphi\}$, unique *derivation*

Requirements

- On inference system: *refutational completeness*
  if $S \cup \{\neg\varphi\}$ unsatisfiable, *there exist* derivations yielding $\perp$
- On search plan: *fairness:*
  ensure that one such derivation is generated!
- Refutationally complete inference system $+$ fair search plan $=$ *complete* TP strategy

Fairness

- Exhaustive: consider *eventually* all *applicable* inferences
  trivial, brute force way to be fair
- Better: consider *eventually* all *needed* inferences
- What is needed?

Redundancy

- Dually: what is *not needed*, that is: what is *redundant*?
- Fairness and redundancy are related

Research challenge

- Non-trivial definitions of fairness for theorem proving
- Non-trivially fair search plans

Ordering-based strategies

- *Expansion inference rule:*

$$\frac{S}{S'} \quad S \subset S'$$

(e.g., *resolution* and *paramodulation/superposition*)

- *Contraction inference rule:*

$$\frac{S}{S'} \quad S \not\subseteq S' \quad S' \prec S$$

$\prec$: well-founded ordering
(e.g., *subsumption* and *simplification*)

Resolution and subsumption

Well-founded ordering $\prec$ on terms and literals
(e.g., Complete Simplification Ordering)

- *Resolution*: generate resolvents by resolving away complementary literals (maximal after mgu)
- *Subsumption*: eliminate less general clauses

- *Redundancy*: φ redundant in S ($\varphi \in \mathit{Red}(S)$) if there exists $\psi \in S$ that subsumes φ [Michäel Rusinowitch]

Add Paramodulation/Superposition and Simplification

- *Paramodulation/Superposition*: resolution with equality built-in: superpose maximal side of maximal equation into maximal literal/side (maximal after mgu)
- *Simplification*: by well-founded rewriting

- *Redundancy*: ground φ redundant in S if for ground instances $\psi_1, \ldots \psi_n$ of clauses in S, $\psi_1, \ldots \psi_n \prec \varphi$ and $\psi_1, \ldots \psi_n \models \varphi$; φ redundant in S ($\varphi \in Red(S)$) if all its ground instances are [Leo Bachmair and Harald Ganzinger]

Derivation and limit

Derivation:

$$S_0 \vdash S_1 \vdash \ldots S_i \vdash S_{i+1} \ldots$$

where $S_0 = S \cup \{\neg\varphi\}$

Limit: set of *persistent clauses* [Gérard Huet]

$$S_\infty = \bigcup_{j \geq 0} \bigcap_{i \geq j} S_i$$

Soundness and adequacy

$Th(S)$: set of all theorems of S

- *Soundness:* if $S \vdash S'$ then $S' \subseteq Th(S)$
- *Adequacy:* if $S \vdash S'$ then $S \subseteq Th(S')$

Adequacy implies *monotonicity*:

$S \vdash S'$ implies $Th(S) \subseteq Th(S')$

Uniform fairness

$\varphi \in I_E(S)$: φ generated from S by expansion
$S_0 \vdash S_1 \vdash \ldots S_i \vdash S_{i+1} \ldots$

1. For all $\varphi \in I_E(S_\infty)$ exists j such that $\varphi \in S_j \cup Red(S_j)$
2. For all $\varphi \in I_E(S_\infty \setminus Red(S_\infty))$ exists j such that $\varphi \in S_j$
3. Redundant inference: uses or generates redundant clause
   Irredundant: not redundant
   All irredundant expansion inferences done eventually

[Michäel Rusinowitch] [Leo Bachmair and Harald Ganzinger]

Abstract canonical inference

- S presentation of $Th(S)$
- *Proof orderings* take center stage
- Inference as *presentation tranformation* and *proof reduction*
  [Leo Bachmair and Nachum Dershowitz] [MPB and Jieh Hsiang]
- Properties of presentations
  [Nachum Dershowitz and Claude Kirchner]
- Properties of derivations: fairness
  [MPB and Nachum Dershowitz]

Proof orderings

- Well-founded proof ordering $<$
- Proofs with premises in S: $Pf(S)$
- Justification: set of proofs P
- Minimal proofs in a justification: $\mu(P)$

Proof reduction

- Comparing justifications:
  Q *better* than P: $P \sqsupseteq Q$: $\forall p \in P. \exists q \in Q.\ p \geq q$
- Comparing presentations:
  S' *simpler* than S: $S \succsim S'$: $S \equiv S'$ and $Pf(S) \sqsupseteq Pf(S')$
- *Normal-form* proofs of S: $Nf(S) = \mu(Pf(Th(S)))$
  the minimal proofs in the set of proofs with premises in $Th(S)$

Properties of presentations I

- *Contracted*: contains all and only the premises of its minimal proofs
- *Canonical*: contains all and only the premises of normal-form proofs: $S^\sharp$
- *Saturated*: provides all normal-form proofs: $\mu(Pf(S)) = Nf(S)$
- *Complete*: provides a normal-form proof for every theorem

Properties of presentations II

- *Saturated* and *complete* coincide if minimal proofs are *unique* (e.g., total proof ordering)
- *Canonical* presentation: *smallest saturated* presentation
- *Canonical* if and only if *saturated* and *contracted*

Example: Equational theories

- *Contracted*: inter-reduced
- *Saturated*: convergent (confluent and terminating)
- *Canonical*: convergent and inter-reduced
- *Normal-form proof* of $\forall\bar{x}\ s \simeq t$:
  valley proof $\hat{s} \xrightarrow{*} \circ \xleftarrow{*} \hat{t}$ by rewriting where $\hat{s}$ and $\hat{t}$ are s and t with variables replaced by Skolem constants

Proof-ordering based redundancy

- φ redundant in S ($\varphi \in Red(S)$) if adding it does not improve minimal proofs:
  $\mu(Pf(S)) = \mu(Pf(S \cup \{\varphi\}))$
- φ redundant in S ($\varphi \in Red(S)$) if removing it does not worsen proofs:
  $S \succsim S \setminus \{\varphi\}$ or $Pf(S) \sqsupseteq Pf(S \setminus \{\varphi\})$

Properties of derivations

$S_0 \vdash S_1 \vdash \ldots S_i \vdash S_{i+1} \ldots$

- *Good*: $S_i \succsim S_{i+1}$ for all i
- *Completing*: S_∞ is complete
- *Saturating*: S_∞ is saturated
- *Contracting*: S_∞ is contracted
- *Canonical*: saturating and contracting

Ordering-based strategies

- *Expansion:* $A \vdash A \cup B$ with $B \subseteq Th(A)$
- *Contraction:* $A \cup B \vdash A$ with $A \cup B \succsim A$
- Expansions and contractions are *good*

Proof-ordering based fairness I

$$(S_0; \varphi_0) \vdash (S_1; \varphi_1) \vdash \ldots (S_i; \varphi_i) \vdash (S_{i+1}; \varphi_{i+1}) \ldots$$

- Whenever a minimal proof of the target theorem is reducible by inferences, it is reduced eventually
- For all $i \geq 0$ and $p \in \mu(Pf(S_i, \varphi_i))$, if there are inferences $(S_i; \varphi_i) \vdash \ldots \vdash (S'; \varphi')$ such that $p > q$, for some $q \in \mu(Pf(S', \varphi'))$, then there exist $(S_j; \varphi_j)$, for $j > i$, and $r \in \mu(Pf(S_j, \varphi_j))$ such that $q \geq r$

Proof-ordering based fairness II

$S_0 \vdash S_1 \vdash \ldots S_i \vdash S_{i+1} \ldots$

- *Critical proof*: minimal proof, not in normal form, all proper subproofs in normal form
  (E.g.: peak $\hat{s} \leftarrow \circ \rightarrow \hat{t}$ yielding critical pair)
- $C(S)$: critical proofs of S
- Persistent critical proofs: $C(S_\infty)$
- All persistent critical proofs reduced eventually:
  $C(S_\infty) \sqsupset Pf(\bigcup_{i \geq 0} S_i)$

Uniform fairness

- *Trivial proof*: made of the theorem itself
- $\widehat{S}$: trivial proofs of S
- Persistent trivial proofs: $\widehat{S_\infty}$
- All persistent trivial proofs reduced eventually: $\widehat{S_\infty} \setminus \widehat{S^\sharp} \sqsupset Pf(\bigcup_{i\geq 0} S_i)$

Results about derivations

- Fairness is sufficient to yield complete theorem-proving strategy
- Fair derivation yields complete limit
- Uniformly fair derivation yields saturated limit

Properties of the search plan

- Schedule enough expansion to be *fair* (in the limit)
- Schedule enough contraction to be *contracting* (in the limit)
- Schedule contraction *before* expansion: *eager contraction* (during the derivation)

Eager contraction

- *Forward contraction*: contract new φ wrt already existing ones: φ'
- *Backward contraction*: contract already existing ones wrt φ'
- $Red(S_i) = \emptyset$ for all i: not feasible if every step is a single inference
- $Red(S_i) = \emptyset$ for some i: given-clause loop with $active \cup passive$ inter-reduced
- $Red(B_i) = \emptyset$ for some $B_i \subseteq S_i$ and some i: given-clause loop with *active* inter-reduced

Discussion

- Fairness should earn something weaker than saturation
- Proof orderings vs. formula orderings
- Non-trivially fair and eager contraction search plans

References

- Maria Paola Bonacina and Nachum Dershowitz. Abstract canonical inference. *ACM Transactions on Computational Logic*, 8(1):180-208, January 2007.
- Maria Paola Bonacina and Nachum Dershowitz. Canonical ground Horn theories. In Andrei Voronkov and Christoph Weidenbach (Eds.) *In Memory of Harald Ganzinger*. Springer, Lecture Notes in Artificial Intelligence, 1–37, to appear, accepted February 2011.
- Maria Paola Bonacina and Jieh Hsiang. Towards a foundation of completion procedures as semidecision procedures. *Theoretical Computer Science*, 146:199-242, July 1995.
- Maria Paola Bonacina. Distributed Automated Deduction. PhD Thesis, Dept. of CS, SUNY Stony Brook, December 1992.