On Global Induction Mechanisms in a \( \mu \)-Calculus with Explicit Approximations

Christoph Sprenger
Swedish Institute of Computer Science, Kista, Sweden
sprenger@sics.se

Mads Dam
Royal Institute of Technology, Kista, Sweden
mfd@it.kth.se

FICS ’02 Workshop, Copenhagen
July 20, 2002
## Motivation

<table>
<thead>
<tr>
<th></th>
<th>Local Induction</th>
<th>Global Induction</th>
</tr>
</thead>
<tbody>
<tr>
<td>derivations</td>
<td>trees</td>
<td>graphs</td>
</tr>
<tr>
<td>soundness</td>
<td>internal, local induction rules</td>
<td>external, discharge condition</td>
</tr>
<tr>
<td>tradition</td>
<td>“classical“ logics</td>
<td>modal/temporal logics</td>
</tr>
<tr>
<td>$\mu$-calculi</td>
<td>Park’s induction [Kozen]</td>
<td>sequent calculus [Dam/Gurov]</td>
</tr>
<tr>
<td></td>
<td>fixed point tagging [Winskel]</td>
<td>model checking [Sti/Wal,Bra]</td>
</tr>
</tbody>
</table>

**Programme:** relate local and global inductive reasoning (proof translations)

**This work:** compare global discharge conditions in context of $\mu$-calculi
Overview

1. Gentzen-style proof system for first-order $\mu$-calculus
   
   (a) $\mu$-Calculus with explicit approximations
   
   (b) Local proof rules and graph-shaped derivations (pre-proofs)

2. Induction discharge conditions:
   
   (A) semantical: runs [Dam/Gurov]
   
   (B) syntactical: traces
   
   (C) automata-theoretic

**Theorem** For a given pre-proof (A), (B) and (C) are equivalent.
\( \mu \)-Calculus with Explicit Approximations (1)

Syntax first-order logic + (approximated) fixed points

\[ \phi ::= \text{FOL formula} \mid \Phi_X(t) \quad \text{formulas} \]
\[ \Phi_X ::= X \mid \mu X(\overline{x}).\phi \mid \mu^\kappa X(\overline{x}).\phi \quad \text{abstractions} \]

Remarks

☞ individual, predicate and ordinal variables

☞ both \( X \) and \( \overline{x} \) are bound in \( \mu X(\overline{x}).\phi \) and \( \mu^\kappa X(\overline{x}).\phi \)

☞ usual syntactic monotonicity condition restricts fixed point formation
\( \mu \)-Calculus with Explicit Approximations (2)

Models \( \mathcal{M} = (\mathcal{A}, \rho) \) \( \mathcal{A} \) a first-order structure, \( \rho \) a valuation

Semantics interpretation in lattice of predicates with point-wise ordering

\[
\| \mu X(\overline{x}).\phi \|_{\rho}^A = \mu \Psi \\
\| \mu^\kappa X(\overline{x}).\phi \|_{\rho}^A = \mu^{\rho(\kappa)} \Psi
\]

where \( \Psi = \lambda P. \lambda \overline{a}. \| \phi \|_{\rho[P/X, \overline{a}/\overline{x}]}^A \) monotone predicate transformer

Proposition

1. \( \mu \Psi = \bigvee_\alpha \mu^\alpha \Psi \)
2. \( \mu^\alpha \Psi = \bigvee_{\beta < \alpha} \Psi(\mu^\beta \Psi) \)
Sequents and Validity

**Sequents** are of the form

\[ \Gamma \vdash \mathcal{O} \Delta \]

where \( \mathcal{O} = (|\mathcal{O}|, \leq_{\mathcal{O}}) \) is a finite partial order on ordinal variables recording ordinal constraints

**Validity** subsequent \( \Gamma \vdash \mathcal{O} \Delta \) is valid if

\[ \bigwedge \Gamma \rightarrow \bigvee \Delta \]

true in all models \((\mathcal{A}, \rho)\) where \( \rho \) respects \( \mathcal{O} \), i.e. \( \rho(\kappa) \leq \rho(\kappa') \) whenever \( \kappa \leq_{\mathcal{O}} \kappa' \)
Local Proof Rules for Fixed Points

\[\begin{align*}
\text{(\(\mu - L\))} & \quad \frac{\Gamma, (\mu X(x).\phi)(\bar{t}) \vdash_{\Theta} \Delta}{\Gamma, (\mu^\kappa X(x).\phi)(\bar{t}) \vdash_{\Theta'} \Delta} \\
\text{(\(\mu - R\))} & \quad \frac{\Gamma \vdash_{\Theta} (\mu X(x).\phi)(\bar{t}), \Delta}{\Gamma \vdash_{\Theta} \phi[\mu X(x).\phi/X, \bar{t}/x], \Delta} \\
\text{(\(\mu^\kappa - L\))} & \quad \frac{\Gamma, (\mu^\kappa X(x).\phi)(\bar{t}) \vdash_{\Theta} \Delta}{\Gamma, \phi[\mu^{\kappa'} X(x).\phi/X, \bar{t}/x] \vdash_{\Theta'} \Delta} \\
\text{(\(\mu^\kappa - R\))} & \quad \frac{\Gamma \vdash_{\Theta} (\mu^\kappa X(x).\phi)(\bar{t}), \Delta}{\Gamma \vdash_{\Theta} \phi[\mu^{\kappa'} X(x).\phi/X, \bar{t}/x], \Delta}
\end{align*}\]

\[\Theta' = \Theta \cup \{\kappa\}\]

\[\Theta' = \Theta \cup \{(\kappa', \kappa)\}\]

\[\kappa' <_{\Theta} \kappa\]
Derivation Trees and Pre-Proofs

Derivation tree $\mathcal{D} = (\mathcal{N}, \mathcal{E}, \mathcal{L})$ sequent-labeled, consistent with proof rules

Repeat $R = (M, N, \sigma)$ leaf $N(\Gamma' \vdash \mathcal{O}, \Delta')$, $\sigma$-instance of $M(\Gamma \vdash \mathcal{O}, \Delta)$

☞ more precisely: $\Gamma \sigma \subseteq \Gamma'$, $\Delta \sigma \subseteq \Delta'$ and $\mathcal{O} \sigma \subseteq \mathcal{O}'$

☞ $N$ called repeat node and $M$ its companion

Pre-proof $\mathcal{P} = (\mathcal{D}, \mathcal{R})$ pair of derivation tree $\mathcal{D}$ and set of repeats $\mathcal{R}$

☞ every non-axiom leaf appears in exactly one repeat of $\mathcal{R}$

☞ pre-proof graph: $\mathcal{G}(\mathcal{P}) = \mathcal{D} +$ repeat edges
Runs – Semantic Discharge (1)

Run of Pre-Proof $\mathcal{P}$ (rooted) path of $\mathcal{G}(\mathcal{P})$, labeled by valuations:

$$\Pi = (N_0, \rho_0) \cdots (N_i, \rho_i) \cdots$$

labels: $\rho_i$ respects $\mathcal{O}_i$, and

tree edge: $(N_i, N_{i+1}) \in \mathcal{E}$ implies $\rho_{i+1}$ agrees with $\rho_i$ on all free variable common to $N_{i+1}$ and $N_i$, and

repeat: $(N_{i+1}, N_i, \sigma) \in \mathcal{R}$ implies $\rho_{i+1} = \rho_i \circ \sigma$
Proofs – Semantic Discharge (2)

Proof  pre-proof $\mathcal{P}$ such that all runs of $\mathcal{P}$ are finite

$\Rightarrow$ proof = pre-proof + well-foundedness

$\Rightarrow$ reference discharge condition to which we compare others

Theorem (Soundness)  If there is a proof for $\Gamma \vdash \Delta$ then $\Gamma \vdash \Delta$ is valid.
Traces – Syntactic Discharge (1)

Trace path of $\mathcal{G}(\mathcal{P})$ labeled by ordinal constraints:

$$\tau = (N_0, (\kappa_0, \kappa'_0)) \cdots (N_i, (\kappa_i, \kappa'_i)) \cdots$$

labels: $\kappa'_i \leq \mathcal{O}_i \kappa_i$ where $N_i(\Gamma_i \vdash \mathcal{O}_i \Delta_i)$, and

tree edge: $(N_i, N_{i+1}) \in \mathcal{E}$ implies $\kappa'_i = \kappa_{i+1}$, and

repeat: $(N_{i+1}, N_i, \sigma) \in \mathcal{R}$ implies $\kappa'_i = \sigma(\kappa_{i+1})$
Example – Syntactic Discharge (2)

\[ (N_0, (\delta, \varepsilon)) \quad (N_1, (\alpha, \beta)) \quad (N_2, (\beta, \gamma)) \quad (N_3, (\gamma, \gamma)) \quad (N_4, (\kappa, \kappa)) \]

repeat \quad companion \quad repeat \quad companion
Progress – Syntactic Discharge (3)

**Progress**

- **trace** $\tau$ progresses at $i$ if $\kappa'_i \prec_{\mathcal{O}_i} \kappa_i$ (strict decrease),

  *is progressive* if it progresses at infinitely many positions

- **path** $\pi$ is *progressive* if there is a progressive trace along a suffix of $\pi$

**Condition (T-DC):** all infinite paths of $\mathcal{G}(\mathcal{P})$ are progressive

**Theorem** A pre-proof $\mathcal{P}$ satisfies (T-DC) iff it is a proof.
Normal Traces – Automata-Theoretic DC (1)

**Observation** any trace $\tau$ can be transformed into a normal trace $\hat{\tau}$ progressing at most at repeat nodes and with equivalent progress characteristics

\[
(N_0, (\delta, \varepsilon)) \quad (N_1, (\alpha, \alpha)) \quad (N_2, (\alpha, \alpha)) \quad (N_3, (\alpha, \gamma)) \quad (N_4, (\kappa, \kappa))
\]

repeat \hspace{1cm} companion \hspace{1cm} repeat \hspace{1cm} companion
Automata-Theoretic Discharge (2)

Idea construct two Buechi automata, $B_1$ and $B_2$, over the alphabet $\mathcal{R}$ s.t.

- $B_1$ recognises sequences of repeats as traversed by paths of $G(\mathcal{P})$,
- $B_2$ recognises a sequences of repeats potentially connected through a normal trace (provided the sequence is also accepted by $B_1$)
- $L(B_1) \subseteq L(B_2)$ characterises previous discharge conditions
Automata-Theoretic Discharge (3)

Automaton $B_2$ Details

States \[ \{ (\kappa, R, \lambda) \mid R = (M, N, \sigma) \text{ and } \sigma(\lambda) \leq_{\mathcal{O}_N} \kappa \} \cup \{ \spadesuit \} \]

Accepting \((\kappa, R, \lambda)\) with \(\sigma(\lambda) <_{\mathcal{O}_N} \kappa\) (progress)

Transitions \((\kappa, R, \lambda) \xrightarrow{R} (\lambda, R', \iota)\)

Example $B_2$ Transition
Main Result and Summary

**Theorem** Let $\mathcal{P}$ be a pre-proof. Are equivalent:

1. $\mathcal{P}$ is a proof (all runs of $\mathcal{P}$ are finite)
2. $\mathcal{P}$ satisfies (T-DC) (all infinite paths of $\mathcal{G}(\mathcal{P})$ are progressive)
3. $L(B_1) \subseteq L(B_2)$ (ditto, using normal traces)

The latter can be checked in time $2^{O(n^3 \log n)}$, where $n = |\mathcal{N}|$. 
Related and Future Work

Gentzen-style proof systems

☞ subsume Rabin-like syntactic conditions by [Sch/Sim] and [Dam et al.]:
  - obtained by restricting $B_2$ to states $(\kappa, R, \kappa)$ (no renaming)
  - complexity drops to $2^{O(n^2 \log n)}$ (time vs. space)

☞ but: do the new conditions provide more proof power?

Games (modal $\mu$-calculus)

☞ generalisation of $\mu$-$\nu$-traces [Walukiewicz]