A compact linear translation for bounded model checking

Paul B. Jackson[1] Daniel Sheridan[2]

[1]University of Edinburgh

[2]Adelard LLP

BMC '06

Aim of translation

- Assume given
  - Kripke structure $\hat{M} = \langle \hat{I}, \hat{T} \rangle$ over set of Boolean variables V
    $\hat{I} = \hat{I}(V)$ describes initial states
    $\hat{T} = \hat{T}(V, V')$ describes transition relation
  - LTL formula ϕ in negation normal form
  - bound $k > 0$

  Variables V used for atomic propositions in ϕ
- A state s of $\hat{M}$ is a valuation of V (function $V \longrightarrow \mathbb{B}$)
- A path $s_0, s_1, \ldots$ is an infinite sequence of states such that
  s_0 satisfies $\hat{I}$, and
  every pair $\langle s_i, s_{i+1} \rangle$ satisfies $\hat{T}$
- Translation produces Boolean formula satisfiable in two cases

  prefix case: all paths of $\hat{M}$ with some common prefix $s_0, \ldots s_{k-1}$ satisfy ϕ

  loop case: some loop path of form $s_0, \ldots s_{l-1}(s_l, \ldots, s_{k-1})^\omega$ for some l satisfies ϕ

Sketch of translation

- For every subformula ψ of ϕ and each timestep $i < k$, introduce a new Boolean variable $(\psi)_i$
- Create constraints relating variables. Constraints for **F**, **G**, **U**, **R** are based on fixpoint characterisations. $\mathbf{G}\,\theta$ is greatest solution to

$$\mathbf{G}\,\theta = \theta \wedge \mathbf{X}\,\mathbf{G}\,\theta$$

  and get constraints of form

$$(\mathbf{G}\,\theta)_i \Rightarrow (\theta)_i \wedge (\mathbf{G}\,\theta)_{i+1}$$

- Could use $\Leftrightarrow$ too. $\Rightarrow$ is sufficient and more concise
- Strong similarity with automata-based LTL translations and Helsinki work
- For least-fixpoint operators (**F**, **U**), additional constraints are necessary (cf Büchi acceptance conditions)

Structure of translation result

- Boolean formula produced is equivalent to

$$[\hat{M}]_k \wedge \left([\psi]_k^0 \vee \bigvee_{l=0}^{k-1} \left({}_lL_k(\hat{M}) \wedge {}_l[\psi]_k^0 \right) \right)$$

where

$$[\hat{M}]_k \doteq \hat{I}(V^0) \wedge \bigwedge_{i=0}^{k-2} \hat{T}(V^i, V^{i+1})$$

$${}_lL_k(\hat{M}) \doteq \hat{T}(V^{k-1}, V^l)$$

- Size of formula translations $[\psi]_k^0$ and ${}_l[\psi]_k^0$ is linear in k. Formulae very similar. Can factor so overall size is linear in k.

Approach to deriving and verifying translation

- Bulk of translation expressed as series of equational transformations on LTL syntax.
- Most important transformation steps are:
  - Conversion of temporal operators **F**, **G**, **U**, **R** into explicit fixpoint versions. Syntax added: $\mu\alpha.\phi$ and $\nu\alpha.\phi$.

$$\mathbf{G}\,\phi \longrightarrow \nu\alpha.\ \phi \wedge \mathbf{X}\,\alpha$$

  - Replacement of fixpoint expressions by suitably constrained existentially quantified variables. Syntax added: $\exists\alpha.\phi$.
- Advantages of approach
  - Aids understanding and justification of translation
  - Simplifies consideration of alternate translations

  In literature, translations usually given in monolithic form

Outline

Denotational semantics

- Equational transformations justified using denotational semantics
- Each equational step justified by asserting equality of denotations of formulae before and after
- Denotational approach well-suited for giving semantics of fixpoint operators
- 3 semantics
  - Infinite semantics
  - Finite prefix-case semantics
  - Finite loop-case semantics
- Finite semantics also guide generation of Boolean formulae from LTL formulae produced by equational transformations

Infinite denotation function

- LTL semantics commonly given using satisfaction relation $\pi \models^i \phi$ for path π and position i on path.

$$\pi \models^i \mathbf{G}\,\phi \quad \Leftrightarrow \quad \forall j \geq i.\ \pi \models^j \phi$$

- The infinite denotation ${}^{\pi}[\![\phi]\!]$ of formula ϕ is an element of $\mathbb{B}^\omega$. Has property

$${}^{\pi}[\![\phi]\!](i) \quad \Leftrightarrow \quad \pi \models^i \phi$$

- Example

	0	1	2	3	4 . . .
${}^{\pi}[\![\phi]\!]$	$\bot$	$\top$	$\bot$	$\top$	$\top^\omega$
${}^{\pi}[\![\mathbf{G}\,\phi]\!]$	$\bot$	$\bot$	$\bot$	$\top$	$\top^\omega$

Finite loop-case representations

- Finite loop-case denotation function works with finite representations of infinite loop paths and denotations
- Assume given bound k and loop start $l < k$.

  finite path $s_0, \ldots, s_{k-1}$ such that $T(s_{k-1}, s_l)$ represents
  infinite loop path $s_0 \ldots s_{l-1}(s_l \ldots s_{k-1})^\omega$

  finite denotation $a_0, \ldots, a_{k-1}$ where $a_i \in \mathbb{B}$ represents
  infinite denotation $a_0 \ldots a_{l-1}(a_l \ldots a_{k-1})^\omega$

- A loop-case inflation function $\uparrow_\circ^\infty$ maps finite paths and denotations to the corresponding infinite paths and denotations.

The finite loop-case denotation function

- Written as $\dot{\pi}\,{}^{\mathrm{F}}_{l}[\![\phi]\!]_k$. $\dot{\pi}$ is a k-bounded path representing a (k, l) loop path. Maps ϕ to element of $\mathbb{B}^k$
- Constructed from auxiliary function on LTL operators

$$
\begin{aligned}
\dot{\pi}\,{}^{\mathrm{F}}_{l}[\![\mathbf{O}\,\phi]\!]_k &\doteq {}_{l}{}^{\mathrm{F}}[\![\mathbf{O}]\!]_k(\dot{\pi}\,{}^{\mathrm{F}}_{l}[\![\phi]\!]_k) && \text{for } \mathbf{O} \in \{\mathbf{X}, \mathbf{F}, \mathbf{G}\} \\
{}_{l}{}^{\mathrm{F}}[\![\mathbf{X}]\!]_k(\dot{a})(i) &\doteq \begin{cases} \dot{a}(i+1) & \text{if } i < k-1 \\ \dot{a}(l) & \text{if } i = k-1 \end{cases} \\
{}_{l}{}^{\mathrm{F}}[\![\mathbf{G}]\!]_k(\dot{a})(i) &\doteq \forall j \in \{\min(i, l) \mathinner{..} k-1\}.\ \dot{a}(j)
\end{aligned}
$$

where $\dot{a} \in \mathbb{B}^k$ is a finite denotation, position $i \in \{0 \mathinner{..} k-1\}$

- Finite denotation exactly mimics infinite denotation

$$
\dot{\pi}{\uparrow}^{\infty}_{\circ}[\![\phi]\!] \;=\; \dot{\pi}\,{}^{\mathrm{F}}_{l}[\![\phi]\!]_k \uparrow^{\infty}_{\circ}
$$

Correctness of loop-case equational transformations

- Correctness statement

$$\dot{\pi}\uparrow_{\circ}^{\infty}[\![\phi]\!] \;=\; \dot{\pi}_{l}^{\mathrm{F}}[\![\mathcal{N}(\phi)]\!]_{k}\uparrow_{\circ}^{\infty}$$

  where $\mathcal{N}()$ carries out equational transformations

- Proof involves justifying
  1. initial equational steps with ${}^{\pi}[\![\cdot]\!]$ semantics
  2. switch to $\dot{\pi}_{l}^{\mathrm{F}}[\![\cdot]\!]_{k}$ semantics
  3. subsequent equational steps with $\dot{\pi}_{l}^{\mathrm{F}}[\![\cdot]\!]_{k}$ semantics

Semantics of fixpoint operators

- Infinite semantics is standard Tarski-Knaster construction

$$\begin{aligned} {}^{\pi}[\![\nu\alpha.\phi]\!]^{\rho} &= \mathrm{gfp}\big({}^{\pi}[\![\lambda\alpha.\phi]\!]^{\rho}\big) \\ &= \bigsqcup\{a \in \mathbb{B}^{\omega} \mid a \sqsubseteq {}^{\pi}[\![\phi]\!]^{\rho[\alpha \mapsto a]}\} \end{aligned}$$

  Here $\bigsqcup$ is least upper bound operator on complete lattice

$$\langle \mathbb{B}^{\omega}, \sqsubseteq \rangle$$

  where

$$a \sqsubseteq b \doteq \forall i \in \mathbb{N}.\ a(i) \Rightarrow b(i)$$

- finite loop-case and prefix-case semantics are similar

Translation of greatest-fixpoint operators (loop-case)

1. Introduce gfp operator ν

$$^{\pi}[\![\mathbf{G}\,\beta]\!] \;=\; ^{\pi}[\![\nu\alpha.\ \beta \wedge \mathbf{X}\,\alpha]\!]$$

where π is any infinite path

2. Switch to finite semantics

$$^{\dot{\pi}\uparrow^{\infty}_{\circ}}[\![\nu\alpha.\ \beta \wedge \mathbf{X}\,\alpha]\!] \;=\; ^{\dot{\pi}}_{l}[\![\nu\alpha.\ \beta \wedge \mathbf{X}\,\alpha]\!]^{\mathrm{F}}_{k}\uparrow^{\infty}_{\circ}$$

where $\dot{\pi}$ is a length k path representing a (k, l) loop path

Introduction of the existential quantification

- Translation is

$$\dot{\pi}_l^{\mathrm{F}}[\![\ \Psi[\nu\alpha.\ \phi]\ ]\!]_k^{\dot{\rho}} \quad = \quad \dot{\pi}_l^{\mathrm{F}}[\![\ \exists\alpha.\ \mathbf{G}_0\,(\alpha \Rightarrow \phi) \wedge \Psi[\alpha]\ ]\!]_k^{\dot{\rho}}$$

where $\Psi[\cdot]$ is a monotone context and

$$\begin{aligned}
\dot{\pi}_l^{\mathrm{F}}[\![\exists\alpha.\ \phi]\!]_k^{\dot{\rho}}(i) &\doteq \exists \dot{a} \in \mathbb{B}^k.\ \dot{\pi}_l^{\mathrm{F}}[\![\phi]\!]_k^{\dot{\rho}[\alpha \mapsto \dot{a}]}(i) \\
{}_l^{\mathrm{F}}[\![\mathbf{G}_0]\!]_k(\dot{a})(i) &\doteq \forall j \in \{0\,..\,k-1\}.\ \dot{a}(j)
\end{aligned}$$

- Intuition is from semantics of $\nu\alpha.\phi$:

$$\dot{\pi}_l^{\mathrm{F}}[\![\nu\alpha.\phi]\!]_k^{\dot{\rho}} \quad = \quad \bigsqcup\{\dot{a} \in \mathbb{B}^k \mid \dot{a} \sqsubseteq \dot{\pi}_l^{\mathrm{F}}[\![\phi]\!]_k^{\dot{\rho}[\alpha \mapsto \dot{a}]}\}$$

  - $\exists$ derives from $\bigsqcup$ operator
  - $\mathbf{G}_0\,(\alpha \Rightarrow \phi)$ expresses in syntax the constraint $\dot{a} \sqsubseteq \dot{\pi}_l^{\mathrm{F}}[\![\phi]\!]_k^{\dot{\rho}[\alpha \mapsto \dot{a}]}$
  - Both pulled through context Ψ

Example of translation

- Translation yielding Boolean formula satisfiable by finite path $\dot{\pi}$ just when $\dot{\pi}^{\mathrm{F}}_{l}[\![p \wedge \mathbf{G}\, q]\!]_k(0) = \top$

- Equational transformations are

$$p \wedge \mathbf{G}\, q \quad \longrightarrow \quad p \wedge \nu\alpha.\ q \wedge \mathbf{X}\, \alpha$$

$$\longrightarrow \quad \exists\alpha.\ \mathbf{G}_0\, (\alpha \Rightarrow q \wedge \mathbf{X}\, \alpha) \wedge p \wedge \alpha$$

- Final (existentially quantified) Boolean formula is

$$\exists a_0, \ldots, a_{k-1}.\ \bigwedge_{i=0}^{k-2} (a_i \Rightarrow q^i \wedge a_{i+1}) \wedge (a_{k-1} \Rightarrow q^{k-1} \wedge a_l) \wedge p^0 \wedge a_0$$

Translation of least-fixpoint operators (loop case)

1. Introduce lfp operator μ

$$^{\pi}[\![\mathbf{F}\,\beta]\!] \;=\; ^{\pi}[\![\mu\alpha.\ \beta \vee \mathbf{X}\,\alpha]\!]$$

   where π is any infinite path

2. Switch to finite semantics

$$^{\dot{\pi}\uparrow^{\infty}_{\circ}}[\![\mu\alpha.\ \beta \vee \mathbf{X}\,\alpha]\!] \;=\; ^{\mathrm{F}}_{\dot{\pi}_{l}}[\![\mu\alpha.\ \beta \vee \mathbf{X}\,\alpha]\!]_{k}\uparrow^{\infty}_{\circ}$$

   where $\dot{\pi}$ is a length k path representing a (k, l) loop path.

3. Eliminate gfp operator μ

$$^{\mathrm{F}}_{\dot{\pi}_{l}}[\![\ \Psi[\mu\alpha.\ \phi]\ ]\!]^{\dot{\rho}}_{k} \quad = \quad ^{\mathrm{F}}_{\dot{\pi}_{l}}[\![\ \forall\alpha.\ \mathbf{G}_0\,(\phi \Rightarrow \alpha) \wedge \Psi[\alpha]\ ]\!]^{\dot{\rho}}_{k}$$

4. Translation yields QBF problems, not SAT problems
5. Way out: enable switch to gfp by making fixpoint unique

Approach to least fixpoints using single loop unroll

- Want alternate expression of finite loop-case semantics for **F** that involves fixpoint characterisation where fixpoint is unique
- Let $\dot{a} \in \mathbb{B}^k$ represent infinite (k, l) loop denotation $a = \dot{a} \uparrow^{\infty}_{\circ}$. Consider $i \in \{0 \,..\, k-1\}$. Have that

$$
\begin{aligned}
{}^{\mathrm{F}}_{l}[\![\mathbf{F}]\!]_k(\dot{a})(i) &= [\![\mathbf{F}]\!](a)(i) \\
&= \exists j \geq i.\ a(j) \\
&= \exists j \in \{i \,..\, k'-1\}.\ a(j) \qquad *** \\
&= {}^{\mathrm{F}}_{l}[\![\tilde{\mathbf{F}}^{\perp}]\!]_{k'}(a|_{k'})(i)
\end{aligned}
$$

  where $k' = k + (k - l)$ (1 loop unroll)

- Step *** valid since sufficient to visit distinct values of a once
- Similar argument explains **F**, **U** treatment in original TACAS '99 paper and **F**, **U**, **G**, **R** treatment in Helsinki FMCAD '04 paper

Alternate $\mathbf{F}$ using a greatest fixpoint

- Definitions are

$$
\begin{array}{lcl}
{}^{\mathrm{F}}_{I}[\![\mathbf{X}^{\perp}]\!]_k(\dot{a})(i) & \doteq & \begin{cases} \dot{a}(i+1) & \text{if } i < k-1 \\ \perp & \text{if } i = k-1 \end{cases} \\
\tilde{\mathbf{F}}^{\perp}\,\alpha & \doteq & \nu\beta.\ \alpha \vee \mathbf{X}^{\perp}\,\beta
\end{array}
$$

- $\tilde{\mathbf{F}}^{\perp}$ has property ${}^{\mathrm{F}}_{I}[\![\tilde{\mathbf{F}}^{\perp}]\!]_k(\dot{a})(i) \;=\; \exists j \in \{i \,..\, k-1\}.\ \dot{a}(j)$
- ${}^{\mathrm{F}}_{I}[\![\tilde{\mathbf{F}}^{\perp}]\!]_k(\dot{a})$ is greatest $\dot{b}$ such that

$$
\begin{array}{rcll}
\dot{b}(j) & \Leftrightarrow & \dot{a}(j) \vee \dot{b}(j+1) & \forall j < k-1 \\
\dot{b}(k-1) & \Leftrightarrow & \dot{a}(k-1) \vee \perp &
\end{array}
$$

- Existence of upper bound on position at which fixpoint constraint calculated forces uniqueness of fixpoint
- Hence ν is adequate

Optimisation of alternate **F** handling

- With $k' = k + (k - l)$

$$
\begin{aligned}
& {}^{\mathrm{F}}_{l}[\![\mathbf{F}]\!]_k(\dot{a})(i) \\
&\quad = \quad \exists j \in \{i \,..\, k'-1\}.\ a(j) \\
&\quad = \quad (\exists j \in \{i \,..\, k-1\}.\ \dot{a}(j)) \ \vee \ (\exists j \in \{k \,..\, k'-1\}.\ \dot{a}(j)) \\
&\quad = \quad (\exists j \in \{i \,..\, k-1\}.\ \dot{a}(j)) \ \vee \ (\exists j \in \{l \,..\, k-1\}.\ \dot{a}(j)) \\
&\left[\quad = \quad \exists j \in \{\min(i,l) \,..\, k-1\}.\ \dot{a}(j) \quad \right] \qquad\qquad *** \\
\end{aligned}
$$

- With ${}^{\mathrm{F}}_{l}[\![\mathbf{loopstart}]\!]_k(\dot{a})(i) \doteq \dot{a}(l)$ have that

$$
{}^{\dot{\pi}}_{l}{}^{\mathrm{F}}[\![\ \mathbf{F}\,\alpha\ ]\!]^{\dot{\rho}}_{k} \quad = \quad {}^{\dot{\pi}}_{l}{}^{\mathrm{F}}[\![\ \tilde{\mathbf{F}}^{\perp}\,\alpha \ \vee\ \mathbf{loopstart}\,\tilde{\mathbf{F}}^{\perp}\,\alpha\ ]\!]^{\dot{\rho}}_{k}
$$

- Only need fixpoint constraints up to k, not $2k$ worst case
- Step *** corresponds to treatment of **F** in TACAS '99

Semantic functions vs translation functions

- Distinction blurred in literature
- Are very similar – translation derived from finite denotation

$$\dot{\pi}_l^{\mathrm{F}}[\![\mathbf{F}\,\psi]\!]_k(i) \quad \doteq \quad \exists j \in \{\min(i,l) \mathinner{..} k-1\}.\ \dot{\pi}_l^{\mathrm{F}}[\![\mathbf{F}\,\psi]\!]_k(i)$$

$$_l[\mathbf{F}\,\phi]_k^i \quad \doteq \quad \bigvee_{j=\min(i,l)}^{k-1} {}_l[\phi]_k^j$$

- Not the same thing

$$\dot{\pi}_l^{\mathrm{F}}[\![v]\!]_k(i) \doteq s_i(v) \qquad\qquad {}_l[v]_k^i \doteq v^i$$

- Literature includes awkward hybrid statements similar to

$${}_l[v]_k^i \doteq v(s_i)$$

- Relationship is

$$\dot{\pi}_l^{\mathrm{F}}[\![\phi]\!]_k(i) \quad \Leftrightarrow \quad \dot{\pi} \models {}_l[\phi]_k^i$$

Semantic vs symbolic Kripke structures

- Symbolic Kripke structure $\langle \hat{I}, \hat{T} \rangle$ over variables V induces semantic Kripke structure $\langle S, I, T \rangle$ where
  - $S = V \to \mathbb{B}$
  - $I \subseteq S$
  - $T \subseteq S \times S$
- With symbolic Kripke structure, can write translation of path constraint more accurately as

$$\hat{I}(V^0) \wedge \bigwedge_{i=0}^{k-2} \hat{T}(V^i, V^{i+1})$$

rather than

$$I(s_0) \wedge \forall i \in \{0 \,..\, k-2\}.\ T(s_i, s_{i+1})$$

Conclusions

Contributions:

- new BMC translation for LTL linear in bound k
  - Appears to be more compact
  - Experimental evaluation needed
- Rigorous framework for reasoning about translations
  - Helps exploration of alternatives
  - Applicable to other translations
  - Addresses need for improved confidence
    - Published papers have errors
    - Correctness arguments subtle (particularly with past time)
    - Industry needs correctness

Future work:

- Implement and evaluate
- Complete tech report
- Extend to past time