On Interpolation and Symbol Elimination in Theory Extensions

Viorica Sofronie-Stokkermans

University Koblenz-Landau, Koblenz, Germany

IJCAR 2016, Coimbra, 28.06.2016

Motivation

SMT solvers: check satisfiability/unsatisfiability

Application: Verification (e.g. Invariant checking, BMC)

Motivation

SMT solvers: check satisfiability/unsatisfiability

> **Application:** Verification (e.g. Invariant checking, BMC)

More interesting: Beyond yes/no answers

- Consider parametric systems

- Infer constraints on parameters (which can be values or functions) which guarantee that certain properties are met.

  (e.g. guarantee the unsatisfiability of clauses in theory extensions)

> **Application:** Verification/synthesis of parametric systems
>   [VSS 2010, 2013] use hierarchical reasoning + quantifier elimination

Goals

Symbol elimination

$\mapsto$ **Synthesis of constraints**

$\mapsto$ **Ground Interpolation**

Main idea:

- Use quantifier elimination (QE)

- If theory does not allow QE, but its model completion does

  then use QE in the model completion.

- For theory extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$

  Instantiation + Hierarchical reduction to reasoning in $\mathcal{T}_0$

  $\qquad\qquad$ + QE in $\mathcal{T}_0$ or its model completion.

Overview

- **Definitions** (QE, model completions, AP, ...)

- **Ground Interpolation** (w.r.t. a theory $\mathcal{T}$ / its model completion $\mathcal{T}^*$)

- **Theory Extensions, Locality**

- **Symbol Elimination in Theory Extensions**

- **Ground Interpolation in Theory Extensions**

Overview

- **Definitions** (QE, model completions, AP, ...)

- **Ground Interpolation** (w.r.t. a theory $\mathcal{T}$ / its model completion $\mathcal{T}^*$)

- **Theory Extensions, Locality**

- **Symbol Elimination in Theory Extensions**

- **Ground Interpolation in Theory Extensions**

Definitions

$\mathcal{T}$ allows quantifier elimination (QE)

if for every formula ϕ there exists a quantifier-free formula ϕ^* with
$$\phi \equiv_{\mathcal{T}} \phi^*.$$

Definitions

$\mathcal{T}$ allows quantifier elimination (QE)
if for every formula ϕ there exists a quantifier-free formula ϕ^* with
$$\phi \equiv_{\mathcal{T}} \phi^*.$$

$\mathcal{T}$ is model complete if all embeddings between its models are elementary
(i.e. preserve the truth of all first-order formulae).
$\mathcal{T}$ allows QE $\Rightarrow$ $\mathcal{T}$ is model complete.

Definitions

$\mathcal{T}$ allows quantifier elimination (QE)
if for every formula ϕ there exists a quantifier-free formula ϕ^* with
$$\phi \equiv_{\mathcal{T}} \phi^*.$$

$\mathcal{T}$ is model complete if all embeddings between its models are elementary
(i.e. preserve the truth of all first-order formulae).
$\mathcal{T}$ allows QE $\Rightarrow$ $\mathcal{T}$ is model complete.

Examples: The following theories allow QE, hence are model complete.

- Presburger arithmetic with congruence mod. n,
- Rational linear arithmetic,
- The theories of real closed fields and of algebraically closed fields,
- The theory of finite fields,
- The theory of acyclic lists in the signature $\{\mathsf{car}, \mathsf{cdr}, \mathsf{cons}\}$

Definitions

$\mathcal{T}$ allows quantifier elimination (QE)
if for every formula ϕ there exists a quantifier-free formula ϕ^* with
$$\phi \equiv_{\mathcal{T}} \phi^*.$$

$\mathcal{T}$ is model complete if all embeddings between its models are elementary (i.e. preserve the truth of all first-order formulae).
$\mathcal{T}$ allows QE $\Rightarrow$ $\mathcal{T}$ is model complete.

$\mathcal{T}^*$ is a model companion of $\mathcal{T}$ if   (i) $\mathcal{T}$ and $\mathcal{T}^*$ are co-theories
      (ii) $\mathcal{T}^*$ is model complete.
$\mathcal{T}^*$ is a model completion of $\mathcal{T}$ iff (i), (ii) and (iii) hold.
 (iii)   for every model $\mathcal{A}$ of $\mathcal{T}$, $\mathcal{T}^* \cup \Delta(\mathcal{A})$ is a complete theory.
      ($\Delta(\mathcal{A})$ is the diagram of $\mathcal{A}$).

Ground Interpolation

$\mathcal{T}$ has the **ground interpolation** property if for every ground formulae

$$A(\overline{c}, \overline{a}) \quad \text{and} \quad B(\overline{c}, \overline{b}) \quad \text{with } A(\overline{c}, \overline{a}) \wedge B(\overline{c}, \overline{b}) \models_{\mathcal{T}} \perp$$

there exists a ground formula $I(\overline{c})$ such that

$$A(\overline{c}, \overline{a}) \models_{\mathcal{T}} I(\overline{c}) \quad \text{and} \quad B(\overline{c}, \overline{b}) \wedge I(\overline{c}) \models_{\mathcal{T}} \perp \ .$$

Ground Interpolation

$\mathcal{T}$ has the **ground interpolation** property if for every ground formulae
$$A(\overline{c}, \overline{a}) \qquad \text{and} \qquad B(\overline{c}, \overline{b}) \qquad \text{with } A(\overline{c}, \overline{a}) \wedge B(\overline{c}, \overline{b}) \models_{\mathcal{T}} \bot$$
there exists a ground formula $I(\overline{c})$ such that
$$A(\overline{c}, \overline{a}) \models_{\mathcal{T}} I(\overline{c}) \qquad \text{and} \qquad B(\overline{c}, \overline{b}) \wedge I(\overline{c}) \models_{\mathcal{T}} \bot .$$

$\mathcal{T}$ (with signature Σ) has the **general ground interpolation** property if for every signature Σ' disjoint from Σ and every ground $\Sigma \cup \Sigma'$-formulae
$$A(\overline{c}, \overline{h}, \overline{a}, \overline{f}) \qquad \text{and} \qquad B(\overline{c}, \overline{h}, \overline{b}, \overline{g}) , \qquad \text{with} \qquad A \wedge B \models_{\mathcal{T} \cup \mathsf{UIF}_{\Sigma'}} \bot$$
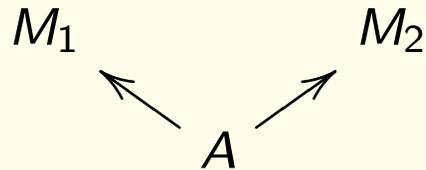there exists a ground formula $I(\overline{c}, \overline{h})$, such that:

(i) all predicate, constants and function symbols from Σ' occurring in I also occur in A and B;

(ii) $A(\overline{c}, \overline{h}, \overline{a}, \overline{f}) \models_{\mathcal{T} \cup \mathsf{UIF}_{\Sigma'}} I(\overline{c}, \overline{h})$ and $B(\overline{c}, \overline{h}, \overline{b}, \overline{g}) \wedge I(\overline{c}, \overline{h}) \models_{\mathcal{T} \cup \mathsf{UIF}_{\Sigma'}} \bot$

Amalgamation

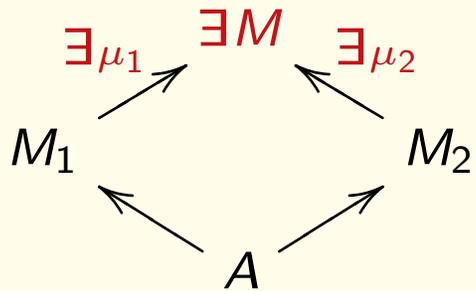A theory $\mathcal{T}$ has the sub-amalgamation property (SAP) iff

$$M_1 \qquad M_2$$
$$\nwarrow \qquad \nearrow$$
$$A$$

A substructure of M_1, M_2

Amalgamation

A theory $\mathcal{T}$ has the sub-amalgamation property (SAP) iff

$$\begin{array}{ccc} & \exists M & \\ {}^{\exists\mu_1}\nearrow & & \nwarrow {}^{\exists\mu_2} \\ M_1 & & M_2 \\ \nwarrow & & \nearrow \\ & A & \end{array}$$
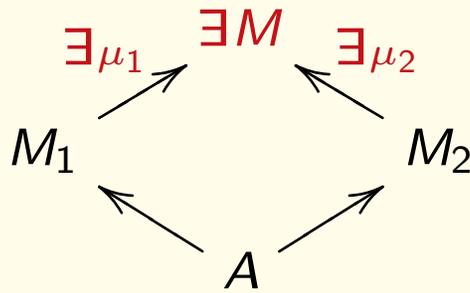
A substructure of M_1, M_2

such that μ_1, μ_2 embeddings and $\mu_{1|A} = \mu_{2|A}$.

Amalgamation

A theory $\mathcal{T}$ has the sub-amalgamation property (SAP) iff

$$
\begin{array}{ccc}
 & \exists M & \\
{}^{\exists \mu_1}\nearrow & & \nwarrow{}^{\exists \mu_2} \\
M_1 & & M_2 \\
\nwarrow & & \nearrow \\
 & A &
\end{array}
$$

A substructure of M_1, M_2

such that μ_1, μ_2 embeddings and $\mu_{1|A} = \mu_{2|A}$.

and the strong sub-amalgamation property (strong SAP) if μ_1, μ_2, M can be chosen s.t.:

if $\mu_1(m_1) = \mu_2(m_2)$, then there exists an element $a \in A$ s.t. $m_1 = m_2 = a$.

Equality Interpolating

Definition [Brutomesso, Ghilardi, Ranise 2014]

A theory $\mathcal{T}$ is equality interpolating iff it has the ground interpolation property and has the property that

for all tuples $x = x_1, \ldots, x_n$, $y^1 = y_1^1, \ldots, y_{n_1}^1$, $z^1 = z_1^1, \ldots, z_{m_1}^1$, $y^2 = y_1^2, \ldots, y_{n_2}^2$, $z^2 = z_1^2, \ldots, z_{m_2}^2$ of constants,

and for every pair of ground formulae $A(x, z^1, y^1)$ and $B(x, z^2, y^2)$ s.t.:

$$A(x, z^1, y^1) \wedge B(x, z^2, y^2) \models_{\mathcal{T}} \bigvee_{i=1}^{n_1} \bigvee_{j=1}^{n_2} y_i^1 = y_j^2$$

there exists a tuple of terms containing only the constants in x, $v(x) = v_1, \ldots, v_k$ such that

$$A(x, z^1, y^1) \wedge B(x, z^2, y^2) \models_{\mathcal{T}} \bigvee_{i=1}^{n_1} \bigvee_{u=1}^{k} y_i^1 = v_k \vee \bigvee_{j=1}^{n_2} \bigvee_{u=1}^{k} v_k = y_j^2$$

Ground Interpolation and Quantifier Elimination

Theorem [Brutomesso, Ghilardi, Ranise 2014]

$\mathcal{T}$ SAP $\qquad\qquad\Leftrightarrow\quad$ ground interpolation

$\qquad\qquad\qquad\qquad\quad\Leftrightarrow\ (\ \text{Strong SAP}\ \ \text{iff}\ \ \text{equality interpolating})$

$\mathcal{T}$ Strong SAP $\qquad\Leftrightarrow\quad$ general ground interpolation

$\mathcal{T}$ universal $+$ QE $\ \Rightarrow\quad$ equality interpolating

Theorem

$\mathcal{T}$ universal and allows QE $\Rightarrow$ $\mathcal{T}$ has general ground interpolation.

Proof: $\mathcal{T}$ allows QE $\Rightarrow$ $\mathcal{T}$ has ground interpolation

$\mathcal{T}$ universal and allows QE $\Rightarrow$ $\mathcal{T}$ equality interpolating

Then $\mathcal{T}$ has strong SAP, hence general ground interpolation.

Model Companions and Ground Interpolation

Theorem [Bacsich75, ChangKeisler]

$\mathcal{T}$ universal. Then $\mathcal{T}$ has AP $\Leftrightarrow$ $\mathcal{T}$ has ground interpolation

$\mathcal{T}^*$ model companion of $\mathcal{T}$ $\quad\Leftrightarrow$ $(i)\mathcal{T}$ has AP iff $(ii)\mathcal{T}^*$ model completion of $\mathcal{T}$

$+\mathcal{T}$ universal $\quad\Rightarrow$ $(i),(ii)$ equiv to $\mathcal{T}^*$ allows QE

Theorem. Let $\mathcal{T}$ be a theory and $\mathcal{T}^*$ a model companion of $\mathcal{T}$.

1. $\mathcal{T}$ universal and has ground interpolation $\Rightarrow \mathcal{T}^*$ allows QE.

2. $\mathcal{T}^*$ has ground interpolation $\Rightarrow \mathcal{T}$ has ground interpolation; ground interpolants computed w.r.t. $\mathcal{T}^*$ are interpolants w.r.t. $\mathcal{T}$.

3. $\mathcal{T}$ universal. $\mathcal{T}$ has ground interpolation $\Leftrightarrow \mathcal{T}^*$ has ground interpolation.

4. $\mathcal{T}^*$ allows QE $\Rightarrow \mathcal{T}$ has ground interpolation.

Proof: Follows from $\mathcal{T}_\forall = \mathcal{T}^*_\forall$.

Model Companions and Ground Interpolation

Theorem [Bac...

$\mathcal{T}$ universal. T...

$\mathcal{T}^*$ model com... of $\mathcal{T}$

$+\mathcal{T}$ universal

Examples of theories with ground interpolation

- The pure theory of equality (model completion: the theory of an infinite set, which allows QE).

- The theory of total orderings (model completion: the theory of dense total orders without endpoints, which allows QE).

- The theory of Boolean algebras (model completion: the theory of atomless Boolean algebras, which allows QE).

- The theory of fields (model completion: the theory of algebraically closed fields, which allows QE).

Theorem. Let

1. If $\mathcal{T}$ is un...

2. If $\mathcal{T}^*$ has ground interpolation then so does $\mathcal{T}$;
   ground interpolants computed w.r.t. $\mathcal{T}^*$ are interpolants w.r.t. $\mathcal{T}$.

3. $\mathcal{T}$ universal. $\mathcal{T}$ has ground interpolation iff $\mathcal{T}^*$ has ground interpolation.

4. If $\mathcal{T}^*$ allows QE then $\mathcal{T}$ has ground interpolation.

Proof: Follows from $\mathcal{T}_\forall = \mathcal{T}^*_\forall$.

Model Companions and Ground Interpolation

Theorem [Bac...

$\mathcal{T}$ universal. T...

$\mathcal{T}^*$ model comp... of $\mathcal{T}$

$+\mathcal{T}$ universal

Examples of theories with ground interpolation

- The pure theory of equality (model completion: the theory of an infinite set, which allows QE).

- The theory of total orderings (model completion: the theory of dense total orders without endpoints, which allows QE).

- A : $\quad d \leq a_1 \wedge a \leq c \wedge d_1 \leq a \qquad\qquad \mathcal{T} = \text{TOrd}$
  B : $\quad b \leq d \wedge b_1 \not\leq c \wedge b_1 \leq d_1$

- $I = d_1 \leq c$ obtained by QE in TOrd^*
  $\qquad$ from $\exists x, x_1 (d \leq x_1 \wedge x \leq c \wedge d_1 \leq x)$

Theorem. Let ...

1. If $\mathcal{T}$ is un...

2. If $\mathcal{T}^*$ has ground interpolation then so does $\mathcal{T}$;
   ground interpolants computed w.r.t. $\mathcal{T}^*$ are interpolants w.r.t. $\mathcal{T}$.

3. $\mathcal{T}$ universal. $\mathcal{T}$ has ground interpolation iff $\mathcal{T}^*$ has ground interpolation.

4. If $\mathcal{T}^*$ allows QE then $\mathcal{T}$ has ground interpolation.

Proof: Follows from $\mathcal{T}_\forall = \mathcal{T}_\forall^*$.

Overview

- **Definitions** (QE, model completions, AP, ...)

- **Ground Interpolation** (w.r.t. a theory $\mathcal{T}$ / its model completion $\mathcal{T}^*$)

- **Theory Extensions, Locality**

- **Symbol Elimination in Theory Extensions**

- **Ground Interpolation in Theory Extensions**

Local Theory Extensions

Theory extension: $\mathcal{T}_0 \subseteq \mathcal{T} = \mathcal{T}_0 \cup \mathcal{K}$

$\mathcal{K}$ set of clauses axiomatizing properties of extension functions.

> (Loc) $\mathcal{T}_0 \subseteq \mathcal{T}$ is local, if for ground clauses G,
> $\mathcal{T}_0 \cup \mathcal{K} \cup G \models \bot$ iff $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G \models \bot$

Extension to Ψ-locality, where Ψ is a closure operator telling which instances $\mathcal{K}[\Psi(G)]$ to consider.

Local Theory Extensions

Theory extension: $\mathcal{T}_0 \subseteq \mathcal{T} = \mathcal{T}_0 \cup \mathcal{K}$

$\mathcal{K}$ set of clauses axiomatizing properties of extension functions.

(Loc) $\mathcal{T}_0 \subseteq \mathcal{T}$ is local, if for ground clauses G,

$\mathcal{T}_0 \cup \mathcal{K} \cup G \models \perp$ iff $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G \models \perp$

Extension to Ψ-locality, where Ψ is a closure operator telling which instances $\mathcal{K}[\Psi(G)]$ to consider.

Hierarchical reasoning: [VS 2005]

 – purify $\mathcal{K}[G]$ and G $\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge \mathsf{Def}$

  $\mapsto$ definitions for terms starting with extension functions

 – reduce to satisfiability in $\mathcal{T}_0$ $\Rightarrow \mathcal{K}_0 \wedge G_0 \wedge \mathsf{Con}[G]_0$

Symbol Elimination in Theory Extensions

$\Pi_0 = (\Sigma_0, \text{Pred})$, $\quad \mathcal{T}_0$ Π_0-theory, $\quad$ Σ_P parameters, $\quad$ $\Sigma \cap (\Sigma_0 \cup \Sigma_P) = \emptyset$

- $\mathcal{K}$ $\Pi_0 \cup \Sigma_P \cup \Sigma$-clauses, all variables also below functions in $\Sigma_1 = \Sigma_P \cup \Sigma$.

- G ground clauses, T ground terms over $\Pi_0 \cup \Sigma_P \cup \Sigma \cup C$ (finite)

Step 1: $\mathcal{K}[T] \cup G \;\rightsquigarrow\; \mathcal{K}_0 \cup G_0 \cup \text{Con}[G]_0 =: G_1$ (purification, Π_0^C clauses).

Step 2: $G_1(\overline{c}_p, \overline{c}_f, \overline{c}) \;\rightsquigarrow\; \exists \overline{x} G_1(\overline{c}_p, \overline{c}_f, \overline{x})$

  - $\overline{c}_f$, $f \in \Sigma_P$, where $c_f = f \in \Sigma_P$ or introduced by $c_f := f(c_1, \ldots, c_k)$
  - $\overline{c}_p$ occurring as arguments of functions in Σ_P in such definitions.
  - $\overline{c}$ be the remaining variables.

Step 3: Construct $\Gamma_1(\overline{c}_p, \overline{c}_f) \equiv_{\mathcal{T}_0} \exists \overline{x} G_1(\overline{c}_p, \overline{c}_f, \overline{x})$ (use QE in $\mathcal{T}_0$)

Step 4: $\Gamma_1(\overline{c}_p, \overline{c}_f) \;\rightsquigarrow\; \Gamma_2(\overline{c}_p) \rightsquigarrow \exists \overline{y} \Gamma_2(\overline{y})$ ($c_f \rightsquigarrow f(c_1, \ldots, c_k), c_p \rightsquigarrow y$).

Step 5: Negate: $\forall \overline{y} \Gamma_T(\overline{y}) := \neg(\exists \overline{y} \Gamma_2(\overline{y})) = \forall \overline{y} \neg \Gamma_2(\overline{y})$.

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

> **Task:** Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\mathrm{Mon}(g): \quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\mathrm{Mon}(g)$.

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

Task: Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\text{Mon}(g) : \quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

---

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\text{Mon}(g)$.

Step 1: $\mathcal{T}_0 \cup \mathcal{K}[G] \cup G \rightsquigarrow \mathcal{T}_0 \cup \mathcal{K}_0 \cup \text{Con}_0 \cup G_0$ (purification)

$\text{Def} = \{g_1 = g(c_1), g_2 = g(c_2), f_1 = f(c_1), f_2 = f(c_2), h_1 = h(c_1), h_2 = h(c_2)\}$

$$\mathcal{K}_0 \cup \text{Con}_0 \cup G_0 := \{ \quad c_1 \leq c \rightarrow g_1 = f_1, c_2 \leq c \rightarrow g_2 = f_2, c < c_1 \rightarrow g_1 = h_1,$$
$$c < c_2 \rightarrow g_2 = h_2, c_1 = c_2 \rightarrow g_1 = g_2, c_1 = c_2 \rightarrow f_1 = f_2,$$
$$c_1 = c_2 \rightarrow h_1 = h_2, c_1 \leq c_2, g_1 > g_2\}$$

13

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

Task: Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\mathrm{Mon}(g): \quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

---

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\mathrm{Mon}(g)$.

Step 2: $\Sigma_P = \{f, h, c\}$. To eliminate g we replace g_1, g_2 with existentially quantified variables z_1, z_2.

We obtain $\exists z_1, z_2\, G_1(c_1, c_2, c, f_1, f_2, h_1, h_2, z_1, z_2) =$

$$\exists z_1, z_2(c_1 \leq c \rightarrow z_1{=}f_1 \wedge c_2 \leq c \rightarrow z_2{=}f_2 \wedge c_1{=}c_2 \rightarrow f_1{=}f_2 \wedge c_1 = c_2 \rightarrow h_1{=}h_2$$

$$c < c_1 \rightarrow z_1{=}h_1 \wedge c < c_2 \rightarrow z_2{=}h_2 \wedge c_1{=}c_2 \rightarrow z_1{=}z_2 \wedge c_1 \leq c_2 \wedge z_1 > z_2)$$

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

Task: Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\text{Mon}(g) : \quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\text{Mon}(g)$.

Step 3: After simplification followed by QE for dense total orderings without endpoints we obtain the formula $\Gamma_1(c_1, c_2, c, f_1, f_2, h_1, h_2)$

$$
\begin{aligned}
(\quad & (c_1 \leq c \;\wedge\; c_2 \leq c \;\wedge\; c_1 \leq c_2 \;\wedge\; f_1 > f_2 \;\wedge\; c_1 \neq c_2) \;\vee \\
& (c_1 \leq c \;\wedge\; c < c_2 \;\wedge\; c_1 \leq c_2 \;\wedge\; f_1 > h_2 \;\wedge\; c_1 \neq c_2) \;\vee \\
& (c < c_1 \;\wedge\; c_2 \leq c \;\wedge\; c_1 \leq c_2 \;\wedge\; h_1 > f_2 \;\wedge\; c_1 \neq c_2) \;\vee \\
& (c < c_1 \;\wedge\; c < c_2 \;\wedge\; c_1 \leq c_2 \;\wedge\; h_1 > h_2 \;\wedge\; c_1 \neq c_2))
\end{aligned}
$$

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

Task: Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\mathrm{Mon}(g):\quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\mathrm{Mon}(g)$.

Step 4: We construct the formula $\Gamma_2(c_1, c_2, c)$ from Γ_1 by replacing f_i by $f(c_i)$ and h_i by $h(c_i)$, $i = 1, 2$.

We obtain (after minor simplification/rearrangement for facilitating reading):

$((c_1 < c_2 \leq c \wedge f(c_1) > f(c_2)) \vee (c_1 \leq c < c_2 \wedge f(c_1) > h(c_2)) \vee$

$(c < c_1 < c_2 \wedge h(c_1) > h(c_2)))$

Example

$\mathcal{T}_0$: dense total orderings without endpoints. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \to g(x) = f(x)), \forall x(c < x \to g(x) = h(x))\}$.

> **Task:** Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\text{Mon}(g): \quad \forall x, y(x \leq y \to g(x) \leq g(y))$,

$G = \{c_1 \leq c_2, g(c_1) > g(c_2)\}$ is the negation of $\text{Mon}(g)$.

> **Step 5:** Negate the formula obtained after Step 4.

$$\forall z_1, z_2 \Gamma_T(z_1, z_2) = \forall z_1, z_2[(z_1 < z_2 \leq c \to f(z_1) \leq f(z_2)) \ \wedge$$
$$(z_1 \leq c < z_2 \to f(z_1) \leq h(z_2)) \ \wedge$$
$$(c < z_1 < z_2 \to h(z_1) \leq h(z_2))].$$

Symbol Elimination in Theory Extensions

Theorem. $\mathcal{T}_0$ allows QE.

After Step 5 we obtain a universal $\Pi_0 \cup \Sigma_P$-formula $\forall \overline{x} \Gamma_T(\overline{x})$ with:

- For every model $\mathcal{A}$ of $\mathcal{T}_0 \cup \mathcal{K}$ and $\forall \overline{y} \Gamma_T(\overline{y})$: $\mathcal{A} \models \neg G$.

- $\mathcal{T}_0 \cup \forall \overline{y} \Gamma_T(\overline{y}) \cup \mathcal{K} \cup G$ is unsatisfiable.

Theorem. If $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ local [$\mathcal{K}$ is flat and linear] and
partial models can be completed to total ones with same support then

$\forall y \Gamma_G(y)$ is the weakest among the univ. formulae Γ with $\mathcal{T}_0 \cup \Gamma \cup \mathcal{K} \cup G \models \perp$.
(is entailed by every such formula Γ).

Symbol Elimination in Theory Extensions

$\mathcal{T}_0$ has a model completion with $\mathcal{T}_0 \subseteq \mathcal{T}_0^*$ such that:

(i) every model of $\mathcal{T}_0 \cup \mathcal{K}$ embeds into a model of $\mathcal{T}_0^* \cup \mathcal{K}$, and

(ii) $\mathcal{T}_0^*$ allows quantifier elimination.

Theorem. After Step 5 we obtain a universal $\Pi_0 \cup \Sigma_P$-formula $\forall \overline{x} \Gamma_T(\overline{x})$ with:

- For every model $\mathcal{A}$ of $\mathcal{T}_0 \cup \mathcal{K}$ and $\forall \overline{y} \Gamma_T(\overline{y})$: $\mathcal{A} \models \neg G$.

- $\mathcal{T}_0 \cup \forall \overline{y} \Gamma_T(\overline{y}) \cup \mathcal{K} \cup G$ is unsatisfiable.

In this case we cannot guarantee that $\forall y \Gamma_G(y)$ is the weakest set of constraints in the set of all Γ with $\mathcal{T}_0 \cup \Gamma \cup \mathcal{K} \cup G \models \perp$.

Example

$\mathcal{T}_0$: theory of total orderings. $\Sigma_P = \{f, h, c\}$ and $\Sigma = \{g\}$.

$\mathcal{K} := \{\forall x(x \leq c \rightarrow g(x) = f(x)), \forall x(c < x \rightarrow g(x) = h(x))\}$.

> **Task:** Generate constraints on parameters (f, h, c) which ensure that g is monotone, e.g. satisfies $\text{Mon}(g): \quad \forall x, y(x \leq y \rightarrow g(x) \leq g(y))$,

$\mathcal{T}_0^*$ theory of dense total orders without endpoints.

(i) every model of $\mathcal{T}_0 \cup \mathcal{K}$ embeds into a model of $\mathcal{T}_0^* \cup \mathcal{K}$, and

(ii) $\mathcal{T}_0^*$ allows quantifier elimination.

The formula $\forall z_1, z_2 \Gamma_T(z_1, z_2)$ constructed before ensures that g is monotone also in this case.

Ground Interpolation in Theory Extensions

- **[VSS 2006, 2008]** Identify classes of local extensions in which ground interpolants can be computed hierarchically.

- **[Totla, Wies, 2013]** Link between hierarchical ground interpolation to an amalgamability property for partial algebras.

Restriction: convexity of base theory

Here:

- Extend these results, avoiding the restriction to convex base theories.

- Explicitly point out all conditons needed for hierarchical interpolation.

- Relate symbol elimination to computation of ground interpolants.

Example

$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$ where $\mathcal{K}$: $\forall x\ (x{\leq}g(y) \to f(x){\leq}y)$

$$\forall x\ (x \leq y \to g(x) \leq g(y))$$

$$\forall x\ (x \leq y \to f(x) \leq f(y))$$

$G = \color{red}{A} \land \color{blue}{B}$	$\mathcal{K}[G] \land \mathsf{Con}[G]$
$d{\leq}\color{red}{g(a)}\ \land\ a{\leq}c$	$b \leq \color{red}{g(a)} \to \color{blue}{f(b)} \leq a$
$b{\leq}d\ \land \color{blue}{f(b)}{\not\leq}c$	$a \lhd a \to \color{red}{g(a)} \lhd \color{red}{g(a)}$ (redundant)
	$b \lhd b \to \color{blue}{f(b)} \lhd \color{blue}{f(b)}$ $\lhd\in\{\leq,=\}$

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K} \qquad \text{where } \mathcal{K}: \forall x \ (x \leq g(y) \rightarrow f(x) \leq y)$$

$$\forall x \ (x \leq y \rightarrow g(x) \leq g(y))$$

$$\forall x \ (x \leq y \rightarrow f(x) \leq f(y))$$

$G = \textcolor{red}{A} \wedge \textcolor{blue}{B}$	$\mathcal{K}[G] \wedge \mathsf{Con}[G]$
$d \leq \textcolor{red}{g(a)} \ \wedge \ a \leq c$	$b \leq \textcolor{red}{g(a)} \rightarrow \textcolor{blue}{f(b)} \leq a$
$b \leq d \ \wedge \textcolor{blue}{f(b)} \not\leq c$	$a \lhd a \rightarrow g(a) \lhd g(a)$ (redundant)
	$b \lhd b \rightarrow f(b) \lhd f(b) \quad \lhd \in \{\leq, =\}$

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K} \qquad \text{where } \mathcal{K}:\ \forall x\ (x \le g(y) \to f(x) \le y)$$

$$\forall x\ (x \le y \to g(x) \le g(y))$$

$$\forall x\ (x \le y \to f(x) \le f(y))$$

Def	$G = A \wedge B$	$\mathcal{K}[G] \wedge \mathsf{Con}[G]$
$g(a) = a_1$	$d \le g(a)\ \wedge\ a \le c$	$b \le g(a) \to f(b) \le a$
$f(b) = b_1$	$b \le d\ \wedge\ f(b) \not\le c$	

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}, \qquad \text{where } \mathcal{K}: \quad \forall x \ (x \le g(y) \to f(x) \le y)$$

$$A \wedge B \models_{\mathcal{T}} \bot \qquad\qquad\qquad \forall x \ (x \le y \to g(x) \le g(y))$$

$$\forall x \ (x \le y \to f(x) \le f(y))$$

Def	$G_0 = A_0 \wedge B_0$	$\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0$
$g(a){=}a_1$	$A_0 : d \le a_1 \wedge a \le c$	$b \le a_1 \to b_1 \le a$ (unsatisfiable)
$f(b){=}b_1$	$B_0 : b \le d \wedge b_1 \not\le c$	

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$$

$$A \wedge B \models_{\mathcal{T}} \bot$$

Def	$A_0 \wedge B_0$	$\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0$
$g(a){=}a_1$	$A_0 : d \leq a_1 \wedge a \leq c$	$b \leq a_1 \rightarrow b_1 \leq a$
$f(b){=}b_1$	$B_0 : b \leq d \wedge b_1 \not\leq c$	

$A_0 \wedge B_0 \models b \leq a_1$
$B_0 \models b \leq d$
$A_0 \models d \leq a_1$

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$$

$$A \wedge B \models_{\mathcal{T}} \bot$$

Def	$A_0 \wedge B_0$	$\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0$
$g(a){=}a_1$	$A_0 : d \leq a_1 \wedge a \leq c$	$b \leq a_1 \rightarrow b_1 \leq a$
$f(b){=}b_1$	$B_0 : b \leq d \wedge b_1 \not\leq c$	

$A_0 \wedge B_0 \models b \leq a_1$	**Consider new instances of $\mathcal{K}$**
$B_0 \models b \leq d$	$b \leq d \rightarrow f(b) \leq f(d)$
$A_0 \models d \leq a_1$	$d \leq g(a) \rightarrow f(d) \leq a$

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$$

$$A \wedge B \models_{\mathcal{T}} \perp$$

Def	$A_0 \wedge B_0$	$\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0$
$g(a){=}a_1$	$A_0 : d \leq a_1 \wedge a \leq c$	$b{\leq}a_1 {\rightarrow} b_1{\leq}a$
$f(b){=}b_1$	$B_0 : b \leq d \wedge b_1 \not\leq c$	$b \leq d \rightarrow b_1 \leq d_1$
$f(d) = d_1$		$d \leq a_1 \rightarrow d_1 \leq a$

$A_0 \wedge B_0 \models b \leq a_1$	**Consider new instances of** $\mathcal{K}$
$B_0 \models b \leq d$	$b \leq d \rightarrow f(b) \leq f(d)$
$A_0 \models d \leq a_1$	$d \leq g(a) \rightarrow f(d) \leq a$

Example

$$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$$

$$A \wedge B \models_{\mathcal{T}} \bot$$

$$W(A, B) = \mathsf{st}(A) \cup \{d, f(d)\}$$
$$W(B, A) = \mathsf{st}(B) \cup \{d, f(d)\}$$

Def	$A_0 \wedge B_0$	$\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0$
$g(a) = a_1$	$A_0 : d \leq a_1 \wedge a \leq c$	$b \leq a_1 \rightarrow b_1 \leq a$
$f(b) = b_1$	$B_0 : b \leq d \wedge b_1 \not\leq c$	$b \leq d \rightarrow b_1 \leq d_1$
$f(d) = d_1$		$d \leq a_1 \rightarrow d_1 \leq a$

$A_0 \wedge B_0 \models b \leq a_1$
$B_0 \models b \leq d$
$A_0 \models d \leq a_1$

Consider new instances of $\mathcal{K}$

$$b \leq d \rightarrow f(b) \leq f(d)$$

$$d \leq g(a) \rightarrow f(d) \leq a$$

Example

$\mathcal{T} = \mathsf{TOrd} \cup \mathcal{K}$

$A \wedge B \models_{\mathcal{T}_1} \bot$

Def	$A_0 \wedge B_0$	$(\mathcal{K}[A, B]_0 \wedge \mathsf{Con}[A, B]_0)_{\mathsf{sep}}$
$g(a){=}a_1$	$A_0 : d \leq a_1 \wedge a \leq c$	$b {\leq} a_1 \rightarrow b_1 {\leq} a$
$f(b){=}b_1$	$B_0 : b \leq d \wedge b_1 \not\leq c$	$b \leq d \rightarrow b_1 \leq d_1$
$f(d) = d_1$		$d \leq a_1 \rightarrow d_1 {\leq} a$

Interpolant (w.r.t. TOrd): $I_0 = d_1 \leq c$

$\Downarrow$

Interpolant (w.r.t. $\mathsf{TOrd} \cup \mathcal{K}$) of $A \wedge B$: $\quad I = f(d) \leq c$

W-separability

Definition [Totla & Wies 2013]
$\mathcal{T} = \mathcal{T}_0 \cup \mathcal{K}$ is W-separable if for all sets of ground clauses A and B,

$$\mathcal{T}_0 \cup \mathcal{K} \cup A \cup B \models \perp \quad \text{iff} \quad \mathcal{T}_0 \cup \mathcal{K}[W(A, B)] \cup A \cup \mathcal{K}[W(B, A)] \cup B \models \perp.$$

Notation: $W(A, B)$ for $W(\text{st}(A), \text{st}(B))$.

$(T_A, T_B) \mapsto W(T_A, T_B)$ "amalgamation closure"

T_A and T_B finite sets of ground terms $\Rightarrow$ $W(T_A, T_B)$ finite set of T_A-pure

ground terms; contains $\text{st}_{\mathcal{K}}(T_A)$

- W is monotone and a closure operator;

- W is compatible with any map h between constants s.t. $h(c_1) \neq h(c_2)$
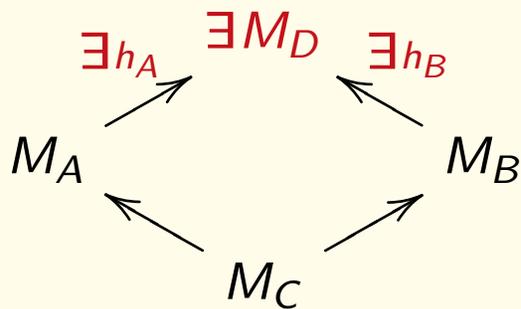 whenever $c_1 \in \text{st}(T_A)$, $c_2 \in \text{st}(T_B)$ not shared between T_A and T_B.

W-Separability and Partial Amalgamation

Theorem [Totla, Wies 2013]
W-separability $\Rightarrow$ Ψ-Locality, Ψ described with the help of *W*

Theorem [Totla,Wies2013] Partial *W*-amalgamability $\Rightarrow$ *W*-separability.

$\exists h_A$ $\exists M_D$ $\exists h_B$ total structure

M_A M_B partial structures; defined terms closed under *W*

M_C partial substructure

W-Separability and Partial Amalgamation

Theorem [Totla, Wies 2013]
W-separability $\Rightarrow$ Ψ-Locality, Ψ described with the help of *W*

Theorem [Totla,Wies2013] Partial *W*-amalgamability $\Rightarrow$ *W*-separability.

Theorems

- Implication holds if we assume *W*-amalgamability for partial structures with the same Π_0-reduct.

- *W*-separability & Interpolants contain terms in $W(A, B) \cap W(B, A)$ $\Rightarrow$ *W*-amalgamability for partial structures with the same Π_0-reduct.

- Interpolants can also be computed using QE (in $\mathcal{T}_0$ or $\mathcal{T}_0^*$) or symbol elimination

Conclusion

- **Ground Interpolation/quantifier elimination/model completions**

- **Symbol elimination in theory extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$.**

  > Given: G set of ground clauses, T set of terms.
  >
  > Task: Find constraint on parameters $\forall x \Gamma_T(x)$ s.t. $\mathcal{T}_0 \cup \mathcal{K} \cup \forall x \Gamma_T(x) \cup G \models \bot$.

  - the method uses hierarchical reasoning $+$ QE in $\mathcal{T}_0$

  - for local theory extensions obtain weakest conditions

  - the method can be used also for theories that do not allow QE

    provided they have a model completion that has QE.

- **Hierarchical interpolation in local theory extensions**