Interpolation in First-Order Logic with Equality

Master Thesis Presentation

Bernhard Mallinger

Advisor: Stefan Hetzl

Institute of Discrete Mathematics and Geometry
TU Wien

October 13, 2014

Agenda

Agenda

Craig Interpolation (1/2)

Theorem ([Craig, 1957]).
Let Γ and Δ be sets of first-order formulas where

- Γ *contains red and gray symbols and*
- Δ *contains blue and gray symbols*

such that:

- $\Gamma \models \Delta$

Then there is a interpolant I containing only gray symbols such that:

- $\Gamma \models I$
- $I \models \Delta$

$$\begin{tikzcd} \Gamma \arrow[rr] \arrow[dr] & & \Delta \\ & I \arrow[ur] & \end{tikzcd}$$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a)\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a))\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a)\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a))\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a)\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Craig Interpolation (2/2)

Example

- Let $\Gamma = \{P(a)\}$ and $\Delta = \{\forall x(P(x) \supset Q(x)), \exists y Q(y)\}$.
- Interpolant: $\exists z\, P(z)$

Example

- Let $\Gamma = \{P(a), \neg P(b)\}$ and $\Delta = \{a \neq b\}$.
- Only possible interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Only possible interpolant: $\perp$

Applications and Motivation

Applications

- Proof of Beth's Definability Theorem
- Model checking
- Detecting loop invariants
- Reasoning with large knowledge bases

Motivation

- Craig interpolation in full first-order logic with equality has received little attention so far
- Interest for constructive proofs giving rise to interpolant extraction algorithms

Applications and Motivation

Applications

- Proof of Beth's Definability Theorem
- Model checking
- Detecting loop invariants
- Reasoning with large knowledge bases

Motivation

- Craig interpolation in full first-order logic with equality has received little attention so far
- Interest for constructive proofs giving rise to interpolant extraction algorithms

Agenda

Proof by Reduction

Reduction to FOL without equality and function symbols:

Translate equality and function symbols:

$$\Big(P(c)\Big)^* \equiv \exists x(C(x) \land P(x))$$

$$\Big(P(f(c))\Big)^* \equiv \exists x(\exists y(C(y) \land F(y,x)) \land P(x))$$

$$\Big(s = t\Big)^* \equiv E(s,t)$$

Add axioms for equality and new predicate symbols:

$$\Big(\varphi\Big)^* \equiv \Big(\mathsf{T}_E \land \bigwedge_{f \in \mathsf{FS}} \mathsf{T}_F\Big) \supset \varphi^*$$

Clearly φ and φ^* are equisatisfiable.

Proof in FOL without Equality and Function Symbols

Lemma (Maehara)

Let Γ and Δ be sets of first-order formulas without equality and function symbols such that $\Gamma \vdash \Delta$ is provable in ***sequent calculus****. Then for any partition $\langle(\Gamma_1;\Delta_1),(\Gamma_2;\Delta_2)\rangle$ there is an interpolant I such that*

1. $\Gamma_1 \vdash \Delta_1, I$ *is provable*
2. $\Gamma_2, I \vdash \Delta_2$ *is provable*
3. $\mathrm{L}(I) \subseteq \mathrm{L}(\Gamma_1,\Delta_1) \cap \mathrm{L}(\Gamma_2,\Delta_2)$

[Baaz and Leitsch, 2011] presents a strengthening which includes function symbols.

Open question: Can it be extended to include equality?

Proof in FOL without Equality and Function Symbols

Lemma (Maehara)

Let Γ and Δ be sets of first-order formulas without equality and function symbols such that $\Gamma \vdash \Delta$ is provable in ***sequent calculus****. Then for any partition $\langle(\Gamma_1; \Delta_1), (\Gamma_2; \Delta_2)\rangle$ there is an interpolant I such that*

1. $\Gamma_1 \vdash \Delta_1, I$ *is provable*
2. $\Gamma_2, I \vdash \Delta_2$ *is provable*
3. $\mathsf{L}(I) \subseteq \mathsf{L}(\Gamma_1, \Delta_1) \cap \mathsf{L}(\Gamma_2, \Delta_2)$

[Baaz and Leitsch, 2011] presents a strengthening which includes function symbols.

Open question: Can it be extended to include equality?

Agenda

Interpolant Extraction

Motivation

- Proof by reduction is impractical
- Goal: Compute interpolants from proof
- The following is based on [Huang, 1995]

Interpolant extraction from resolution proofs

- Skolemisation and clausal form transformation do no alter the set of interpolants
- Have to use "reverse" (but equivalent) formulation of interpolation

Interpolant Extraction

Motivation

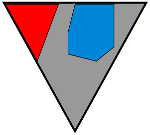
- Proof by reduction is impractical
- Goal: Compute interpolants from proof
- The following is based on [Huang, 1995]

Interpolant extraction from resolution proofs

- Skolemisation and clausal form transformation do no alter the set of interpolants
- Have to use "reverse" (but equivalent) formulation of interpolation

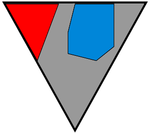
Huang's Algorithm (1/3)

Proof:



$\Downarrow$ *Extract propositional interpolant structure from proof*

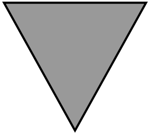
Propositional Interpolant:



$\ldots Q(f(c), c) \ldots$

$\Downarrow$ *Replace colored function and constant symbols*

Prenex First-Order Interpolant:



$\exists x_3 \forall x_5 \ldots Q(x_5, x_3) \ldots$

Huang's Algorithm (2/3)

First phase

- Propositional interpolant is extracted inductively, is boolean combination of PIs of clauses and resolved literals or equations of paramodulation inferences.
- Propositional interpolant is interpolant modulo function and constant symbols (only grey predicate symbols) (this strategy already gives rise to a complete procedure for propositional logic)
- Rule for paramodulation somewhat more complex but still same approach as for resolution and factorisation

Huang's Algorithm (3/3)

Second phase

- The second phase replaces the remaining colored terms by quantified variables
- The ordering of the lifting variables is crucial
- The type of the quantifier is determined by the coloring of the symbol

Theorem

The number of quantifier alternations in the resulting interpolant directly corresponds to the number of color alternations of terms in the resolution proof.

Huang's Algorithm (3/3)

Second phase

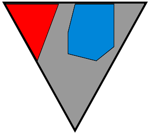
- The second phase replaces the remaining colored terms by quantified variables
- The ordering of the lifting variables is crucial
- The type of the quantifier is determined by the coloring of the symbol

Theorem

The number of quantifier alternations in the resulting interpolant directly corresponds to the number of color alternations of terms in the resolution proof.

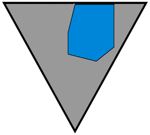
Interpolation Extraction in one Phase

Proof:



$\Downarrow$ *Combined structure extraction and replacing of colored symbols*

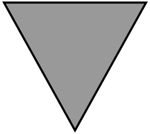
Interpolant modulo current clause:



$\forall x_5 \ldots Q(x_5, c) \ldots$

Recursively applied to all inferences of the proof results in:

Non-Prenex First-Order Interpolant:



$\exists x_3 \ldots \forall x_5 \ldots Q(x_5, x_3) \ldots$

Agenda

Semantic Proof

Indirect and model-theoretic proof of the interpolation theorem
$\Rightarrow$ non-constructive

Definition (Separation)

A formula A in the language $L(\Gamma) \cap L(\Delta)$ separates Γ and Δ if

- $\Gamma \models A$
- $\Delta \models \neg A$.

Theorem (Robinson's joint consistency theorem)

$\Gamma \cup \Delta$ is consistent iff there is no formula which separates Γ and Δ.

$\Rightarrow$ Separating formula corresponds to interpolant.

Semantic Proof

Indirect and model-theoretic proof of the interpolation theorem
$\Rightarrow$ non-constructive

Definition (Separation)

A formula A in the language $\mathrm{L}(\Gamma) \cap \mathrm{L}(\Delta)$ separates Γ and Δ if

- $\Gamma \models A$
- $\Delta \models \neg A$.

Theorem (Robinson's joint consistency theorem)

$\Gamma \cup \Delta$ *is consistent iff there is no formula which separates* Γ *and* Δ.

$\Rightarrow$ Separating formula corresponds to interpolant.

Semantic Proof

Proof (sketch, $\Leftarrow$ direction).

- Suppose Γ and Δ inseparable.
- Set $T_0 = \Gamma$ and $T_0' = \Delta$.
- Add to T_i the ith formula of $\mathsf{L}(\Gamma)$ if this does not make T_i and T_i' separable (similar for T_i').
- Let $T = \bigcup_{i \leq 0} T_i$ and $T' = \bigcup_{i \leq 0} T_i'$.
- Can show that:
  - T and T' inseparable
  - T and T' each consistent
  - T and T' each maximal consistent w.r.t. to $\mathsf{L}(\Gamma)$ and $\mathsf{L}(\Delta)$ respectively
  - $T \cap T'$ maximal consistent w.r.t. to $\mathsf{L}(\Gamma) \cap \mathsf{L}(\Delta)$
- Hence $T \cup T'$ is satisfiable. $\square$

Agenda

Conclusion

- Craig's and Huang's proof based interpolant extraction from proofs
  $\Rightarrow$ but differ in practical applicability
- Craig shows that the interpolation theorem holds also in FOL with equality
- Huang shows that interpolants can efficiently be extracted in FOL with equality
  - Handling of equality does not require a different approach
  - Little attention so far in research
- Huang's two-stage approach can be changed to a one-stage approach yielding non-prenex interpolants
- Interpolation also allows for a model theoretic approach

References

Baaz, M. and Leitsch, A. (2011).
Methods of Cut-Elimination.
Trends in Logic. Springer.

Craig, W. (1957).
Linear Reasoning. A New Form of the Herbrand-Gentzen Theorem.
Journal of Symbolic Logic, 22(3):250–268.

Huang, G. (1995).
Constructing Craig Interpolation Formulas.
In *Proceedings of the First Annual International Conference on Computing and Combinatorics*, COCOON '95, pages 181–190, London, UK, UK. Springer-Verlag.