

Interpolation in First-Order Logic with Equality

Master Thesis Presentation

Bernhard Mallinger

Advisor: Stefan Hetzl

Institute of Discrete Mathematics and Geometry
TU Wien

13. Oktober 2014

Agenda

- ➊ Introduction (10 min)
- ➋ Proof by Reduction (6 min)
- ➌ Interpolant Extraction from Resolution Proofs (12 min)
- ➍ Semantic Proof (6 min)
- ➎ Conclusion
 - References

Agenda

- 1 Introduction (10 min)
- 2 Proof by Reduction (6 min)
- 3 Interpolant Extraction from Resolution Proofs (12 min)
- 4 Semantic Proof (6 min)
- 5 Conclusion
 - References

Craig Interpolation (1/2)

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

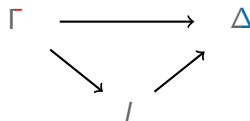
- Γ contains *red* and *mygray* symbols and
- Δ contains *blue* and *mygray* symbols

such that:

- $\Gamma \models \Delta$

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

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



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

- 1 Introduction (10 min)
- 2 Proof by Reduction (6 min)
- 3 Interpolant Extraction from Resolution Proofs (12 min)
- 4 Semantic Proof (6 min)
- 5 Conclusion
 - References

Proof by Reduction

Reduction to FOL without equality and function symbols:

Translate equality and function symbols:

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

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

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

Add axioms for equality and new predicate symbols:

$$(\varphi)^* \equiv \left(T_E \wedge \bigwedge_{f \in FS} T_F \right) \supset \varphi^*$$

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 $L(I) \subseteq L(\Gamma_1, \Delta_1) \cap L(\Gamma_2, \Delta_2)$

[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 $L(I) \subseteq L(\Gamma_1, \Delta_1) \cap L(\Gamma_2, \Delta_2)$

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

Open question: Can it be extended to include equality?

Agenda

- 1 Introduction (10 min)
- 2 Proof by Reduction (6 min)
- 3 Interpolant Extraction from Resolution Proofs (12 min)**
- 4 Semantic Proof (6 min)
- 5 Conclusion
 - References

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 not alter the set of interpolants
- Have to use “reverse” (but equivalent) formulation of interpolation

Interpolant Extraction

Motivation

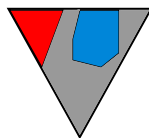
- Proof by reduction is impractical
- Goal: Compute interpolants from proof
- The following is based on [Huang, 1995]

Interpolant extraction from resolution proofs

- Skolemisation and clausal form transformation do not alter the set of interpolants
- Have to use “reverse” (but equivalent) formulation of interpolation

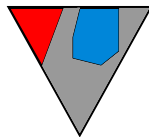
Huang's Algorithm (1/3)

Proof:



\Downarrow *Extract propositional interpolant structure from proof*

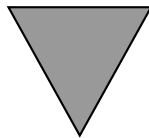
Propositional Interpolant:



$\dots Q(\textcolor{red}{f}(\textcolor{blue}{c}), \textcolor{blue}{c}) \dots$

\Downarrow *Replace colored function and constant symbols*

Prenex First-Order Interpolant:



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

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)

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

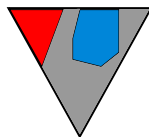
- The second phase replaces the remaining colored terms by quantified variables
- The ordering of the lifting variables is crucial
- The type of the quantifier is determined by the coloring of the symbol

Theorem

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

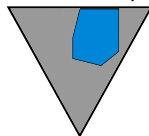
Interpolation Extraction in one Phase

Proof:



Combined structure extraction and replacing of colored symbols

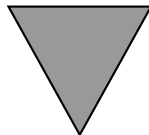
Interpolant
modulo
current clause:



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

Recursively applied to all inferences of the proof results in:

Non-Prenex
First-Order
Interpolant:



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

Agenda

- 1 Introduction (10 min)
- 2 Proof by Reduction (6 min)
- 3 Interpolant Extraction from Resolution Proofs (12 min)
- 4 Semantic Proof (6 min)**
- 5 Conclusion
 - References

Semantic Proof

TODO

Agenda

- 1 Introduction (10 min)
- 2 Proof by Reduction (6 min)
- 3 Interpolant Extraction from Resolution Proofs (12 min)
- 4 Semantic Proof (6 min)
- 5 Conclusion
 - References

Conclusion

- Craig's and Huang's proof based interpolant extraction from proofs
⇒ differ in applicability
- Craig shows that the interpolation theorem holds also in FOL/EQ
- Huang shows that interpolants can efficiently be extracted in FOL/EQ
 - Does not require different methods
 - Little attention so far in research
- Interpolation also allows for a model theoretic approach



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.