Interpolation in First-Order Logic with Equality

Master Thesis Presentation

Bernhard Mallinger

Advisor: Stefan Hetzl

Institute of Discrete Mathematics and Geometry
TU Wien

October 29, 2014

Agenda

Agenda

Craig Interpolation (1/2)

Theorem ([Craig, 1957]).
Let Γ and Δ be finite 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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Interpolant: $\bot$

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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Interpolant: $\bot$

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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- 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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Interpolant: $\bot$

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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- 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 $\Delta = \{a \neq b\}$.
- Interpolant: $a \neq b$

Example

- Let $\Gamma = \{P(a), \neg P(a)\}$, $\Delta = \emptyset$.
- Interpolant: $\bot$

Applications and Motivation

Applications

- Proof of Beth's Definability Theorem
- Model checking
- 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

Applications and Motivation

Applications

- Proof of Beth's Definability Theorem
- Model checking
- 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

Agenda

Proof by Reduction due to Craig

Reduction to FOL without equality and function symbols:

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

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

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

$$\Big(\varphi\Big)^* \equiv \Big(\top_E \wedge \bigwedge_{f \in FS} \top_F\Big) \supset \varphi^*$$

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 $\langle(\Gamma_1;\Delta_1),(\Gamma_2;\Delta_2)\rangle$ with $\Gamma_1 \uplus \Gamma_2 = \Gamma$ and $\Delta_1 \uplus \Delta_2 = \Delta$ 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 rules for LK?

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 $\langle(\Gamma_1; \Delta_1), (\Gamma_2; \Delta_2)\rangle$ with $\Gamma_1 \uplus \Gamma_2 = \Gamma$ and $\Delta_1 \uplus \Delta_2 = \Delta$ 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 rules for LK?

Agenda

Interpolant Extraction from Resolution Proofs

Motivation

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

Interpolant Extraction from Resolution Proofs

Motivation

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

The Resolution Calculus

Resolution: $$\frac{C \vee l \qquad D \vee \neg l'}{(C \vee D)\sigma}\,\text{res} \qquad \sigma = \text{mgu}(l, l')$$

Factorization: $$\frac{C \vee l \vee l'}{(C \vee l)\sigma}\,\text{fac} \qquad \sigma = \text{mgu}(l, l')$$

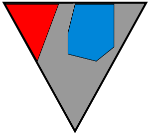
Paramodulation: $$\frac{D \vee s = t \qquad E[r]_p}{(D \vee E[t]_p)\sigma}\,\text{par} \qquad \sigma = \text{mgu}(s, r)$$

Interpolation and Resolution

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

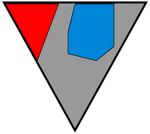
Huang's Algorithm

Proof:



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

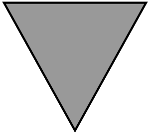
Propositional Interpolant:



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

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

Prenex First-Order Interpolant:



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

Propositional Interpolant Extraction Example

Paramodulation rule:

$$\frac{C_1 : D \vee s = t \qquad C_2 : E[r]_p}{C : (D \vee E[t]_p)\sigma} \text{ par} \qquad \sigma = \mathrm{mgu}(s, r)$$

Propositional interpolant[1]:

$$\mathrm{PI}(C) \stackrel{\mathrm{def}}{=} [(s = t \wedge \mathrm{PI}(C_2)) \vee (s \neq t \wedge \mathrm{PI}(C_1))]\sigma$$

[1] Provided that r is not contained in a colored term

Huang's Algorithm (2/3)

TODO: remove from here as soon as it's clear if it's being said at the image slide

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)

TODO: remove from here as soon as it's clear if it's being said at the image slide

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

KEEP THIS:

- Number of quantifier alternations $\sim$ number of color alternations in terms of the resolution proof

Huang's Algorithm (3/3)

TODO: remove from here as soon as it's clear if it's being said at the image slide

Second phase

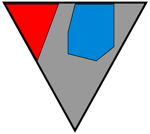
- The second phase replaces the remaining colored terms by quantified variables
- The ordering of the lifting variables is crucial
- The type of the quantifier is determined by the coloring of the symbol

KEEP THIS:

- Number of quantifier alternations $\sim$ number of color alternations in terms of the resolution proof

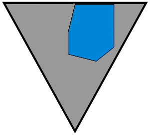
Interpolation Extraction in One Phase

Proof:



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

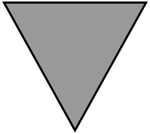
Interpolant modulo current clause:



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

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
- Inherently non-constructive
- Equality does not require explicit handling
- Interpolation in FOL with equality equivalent to Robinson's joint consistency theorem

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 adapted 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.