

Interpolation in First-Order Logic with Equality

Masterstudium:
Computational Intelligence

Bernhard Mallinger

Technische Universität Wien
Institut für diskrete Mathematik und Geometrie
Betreuer: Ass.Prof. Stefan Hetzl

Craig Interpolation

Theorem (Craig). Let A and B be first-order formulas where

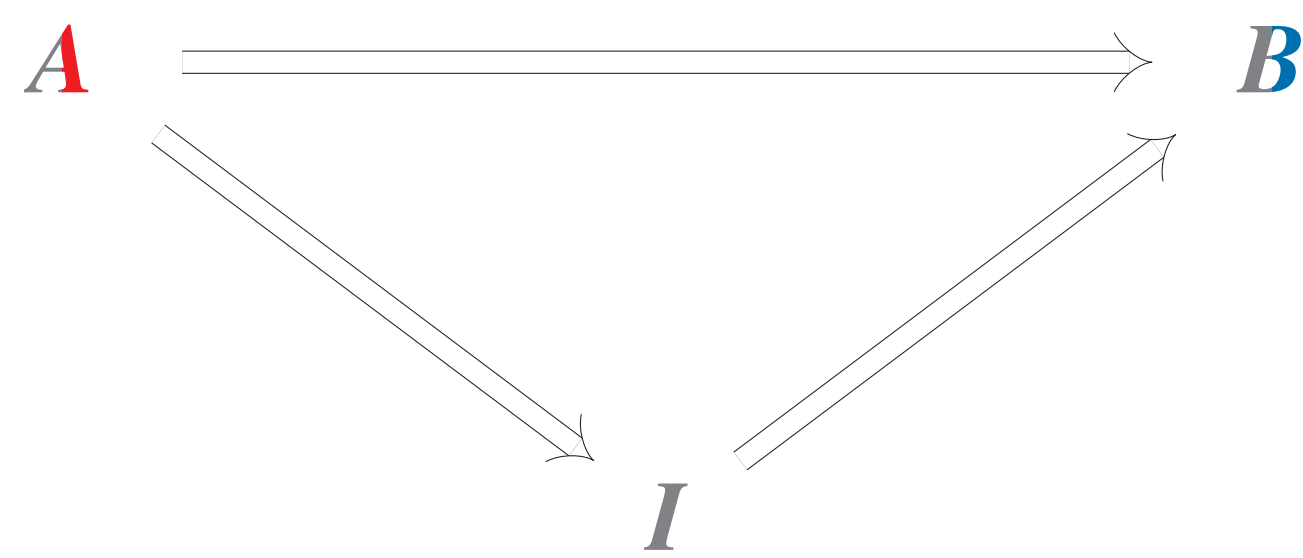
- ▶ A contains *red* and *gray* symbols and
- ▶ B contains *blue* and *gray* symbols

such that:

- ▶ $\models A \supset B$

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

- ▶ $\models A \supset I$
- ▶ $\models I \supset B$



⇒ Interpolants give a concise logical summary of the implication

Applications of Craig Interpolation

Theoretical:

- ▶ Proof of Beth's Definability Theorem

Practical:

- ▶ Program analysis: Detect loop invariants
- ▶ Model checking: Overapproximate set of reachable states

Aim and Scope of the Thesis

Provide overview of existing techniques and extend them:

- ▶ Model-theoretic proof
- ▶ Reduction to first-order logic without equality
- ▶ Interpolant extraction from resolution proofs

Model-theoretic proof

- ▶ Non-constructive proof by contradiction:
 - ▶ Let T_A and $T_{\neg B}$ be theories extending A and $\neg B$ respectively
 - ▶ Build a model from maximal consistent intersection of T_A and $T_{\neg B}$ (assuming the non-existence of interpolants)
 - ⇒ $A \wedge \neg B$ satisfiable
- ▶ Related to Robinson's Joint Consistency Theorem

Reduction to first-order logic without equality [1]

Translate equality and function symbols:

$$\begin{aligned} (P(c))^* &\equiv \exists x (C(x) \wedge P(x)) \\ (P(f(c)))^* &\equiv \exists x (\exists y (C(y) \wedge F(y, x)) \wedge P(x)) \\ (s = t)^* &\equiv E(s, t) \end{aligned}$$

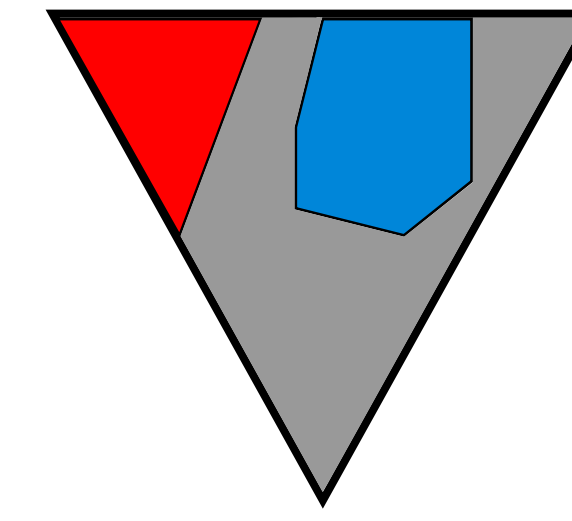
Add theory of equality:

$$\varphi \rightarrow T_E \supset \varphi^*$$

⇒ Then calculate interpolant in reduced logic

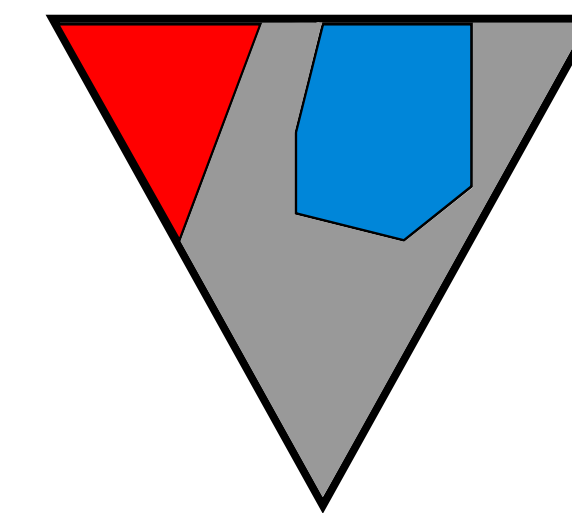
Interpolant extraction from proofs in two phases [2]

Proof:



↓ Extract propositional
interpolant structure from proof

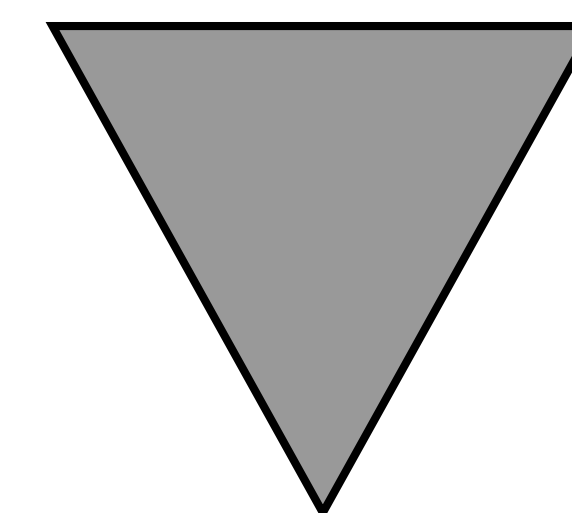
Propositional
Interpolant:



... $Q(f(c), c)$...

↓ Replace colored function
and constant symbols

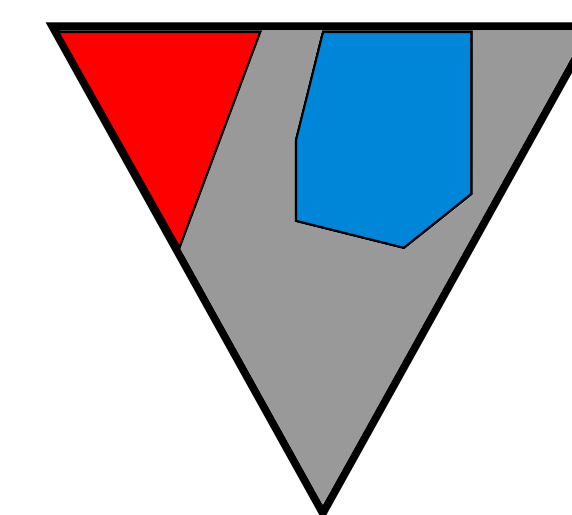
Prenex
First-Order
Interpolant:



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

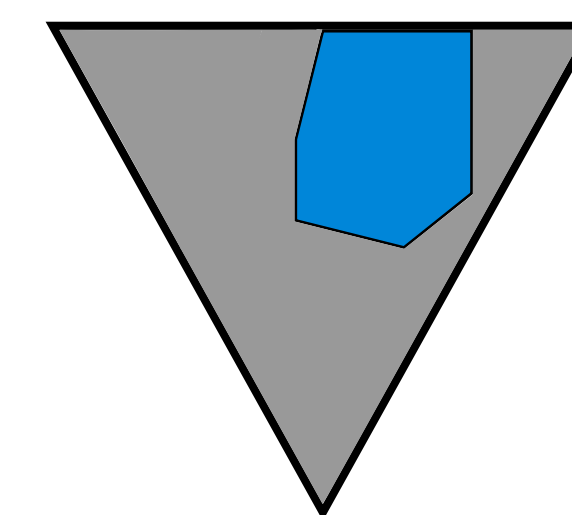
Interpolant extraction from proofs in one phase

Proof:



↓ Combined structure extraction
and replacing of colored symbols

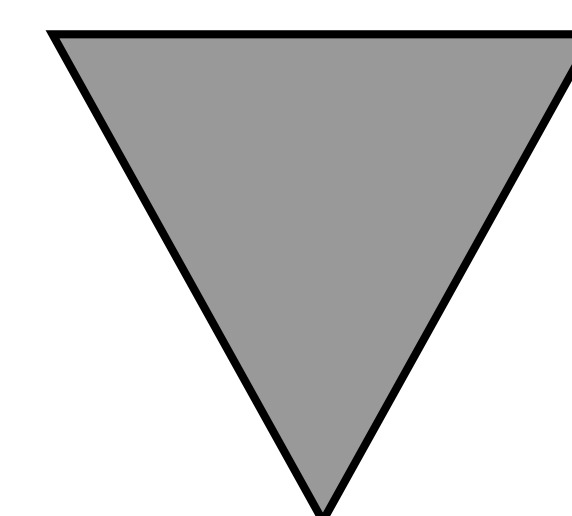
Interpolant
modulo
current clause:



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

Recursively applied to all infer-
ences of the proof results in:

Non-Prenex
First-Order
Interpolant:



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

Contributions

- ▶ We introduced the one phase extraction approach.
- ▶ We showed that the number of *quantifier alternations* in the extracted interpolant essentially corresponds to the number of *color alternations* in the terms of the proof.

References

- [1] William Craig. Linear Reasoning. A New Form of the Herbrand-Gentzen Theorem. *Journal of Symbolic Logic*, 22(3):250–268, 1957.
- [2] Guoxiang Huang. Constructing Craig Interpolation Formulas. In *Proc COCOON '95*, p. 181–190, 1995.