Diplomarbeitspräsentation

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Interpolation in First-Order Logic with Equality

Bernhard Mallinger

Masterstudium:
Computational Intelligence

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

Craig Interpolation

Theorem (Craig). *Let A and B be first-order formulas such that* $\vDash A \supset B$ *where A contains red and gray symbols and B contains of blue and gray symbols. Then there is an interpolant I containing of gray symbols for A and B such that:*

- $\vDash A \supset I$
- $\vDash I \supset B$

$$\begin{tikzcd} A \arrow[rr, Rightarrow] \arrow[dr, Rightarrow] & & B \\ & I \arrow[ur, Rightarrow] & \end{tikzcd}$$

$\Rightarrow$ 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

Give comprehensive account 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:
  - Let T_A and $T_{\neg B}$ be theories extending A and $\neg B$
  - Build model from maximal consistent intersection of T_A and $T_{\neg B}$ (assuming the non-existence of interpolants)
    $\Rightarrow A \wedge \neg B$ satisfiable
- Related to Robinson's Joint Consistency Theorem

Reduction to first-order logic without equality [1]

Translate equality and function symbols:

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

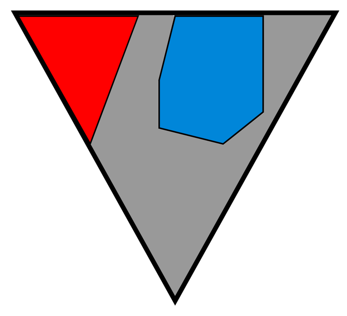
Add theory of equality:

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

$\Rightarrow$ Then calculate interpolant in reduced logic

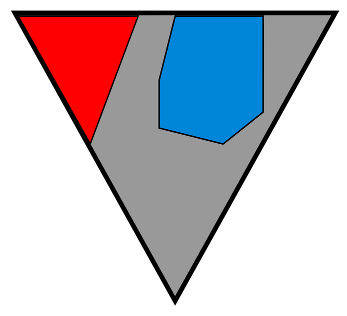
Interpolant extraction from proofs in two phases [2]

Proof:



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

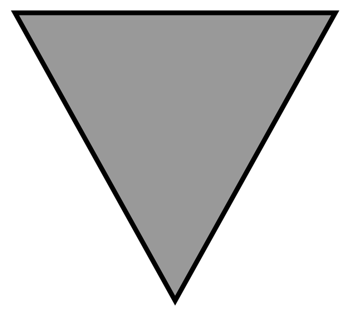
Propositional Interpolant:



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

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

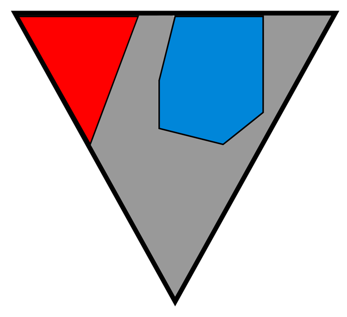
Prenex First-Order Interpolant:



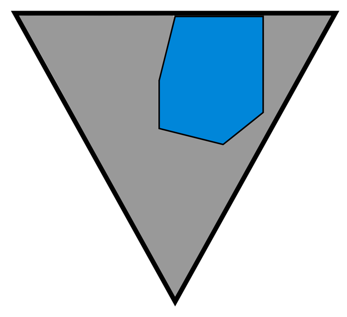
$\exists x_3 \forall x_5 \ldots Q(x_5, x_3) \ldots$

Interpolant extraction from proofs in one phase

Proof:



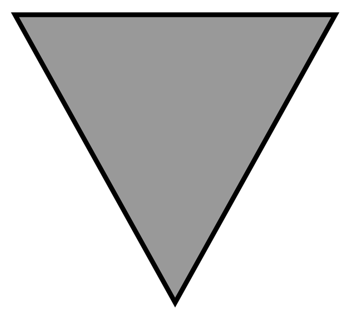
$\Downarrow \vdots \Downarrow$ *Combined extraction and replacing phases*



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

$\Downarrow \vdots \Downarrow$ *Combined extraction and replacing phases*

Non-Prenex First-Order Interpolant:



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

Contributions

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

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

Kontakt: b.mallinger@gmx.at