FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

Diplomarbeitspräsentation

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 $\models A \supset B$. Then there is an interpolant I for A and B such that:*

- $\models A \supset I$
- $\models I \supset B$
- $\mathbf{Lang}(I) \subseteq \mathbf{Lang}(A) \cap \mathbf{Lang}(B)$

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

$\Rightarrow$ 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 of program

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_B be theories extending A and B
- Build model from maximal consistent intersection of T_A and T_B

Reduction to first-order logic without equality [1]

Translate equality and function symbols:

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

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]

- Extract structure from proof
- Replace colored terms by quantified variables

[redacted]

[redacted] $\ldots Q(f(c), c) \ldots$

[redacted] $\exists x_3 \forall x_5 \ldots Q(x_5, x_3) \ldots$

Interpolant extraction from proofs in one phase

- Replace colored terms during extraction

[redacted]

[redacted] $\ldots Q(f(c), c) \ldots$

[redacted] $\ldots \forall x_5 \ldots Q(x_5, c) \ldots$

[redacted] $\exists x_3 \ldots \forall x_5 \ldots Q(x_5, x_3) \ldots$

Contributions

- We introduced the one phase-approach.
- We showed that the number of quantifier alternations in the interpolant essentially 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 Formulas.
In *Proc COCOON '95*, p. 181–190, 1995.

Kontakt: b.mallinger@gmx.at