UPPSALA
UNIVERSITET

Approximations for Deciding Quantified Floating-Point Constraints

Peter Backeman, Aleksandar Zeljić

Vetenskapsrådet

Motivation

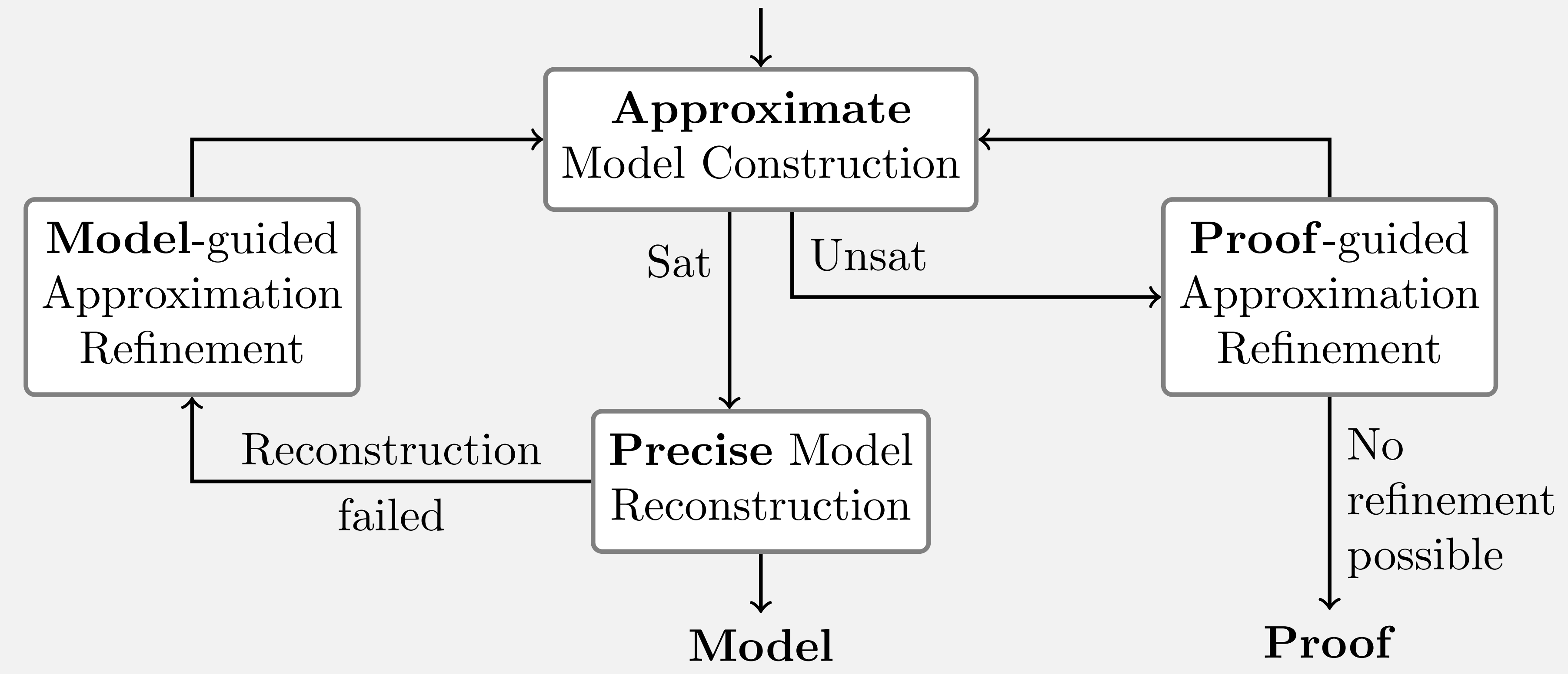
Efficient model construction of satisfiable constraints is an important challenge with applications in, for example, automatic test-case generation, synthesis of invariants, computation ranking functions, etc. Computing models for quantified constraints remains a very difficult problem. With continuous success of applying approximations in reasoning, we propose extending an approximation framework [1] with support for quantified reasoning.

Using Approximations

1. Lift ϕ to an approximated problem $\hat{\phi}$
2. Solve it in the approximation theory
3. Reconstruct the model

$$\begin{tikzcd}
\hat{m}, \hat{\beta}, \gamma \arrow[d, "\textit{model reconstruction}"'] & \models_{\hat{T}} & \hat{\phi} \\
m, \beta & \models_{T} & \phi \arrow[u, "\textit{lift}"']
\end{tikzcd}$$

Approximation Refinement Framework



Approximate Model Construction

Model-guided Approximation Refinement

Proof-guided Approximation Refinement

Sat

Unsat

Precise Model Reconstruction

Reconstruction failed

No refinement possible

Model

Proof

Lifting the constraints

- Introduce *precision* arguments for each quantifier, function and relation symbol.
- Allows control over approximations.

Lifting the formula:

$$\exists x \forall a \exists y . \phi(x, a, y)$$

results in:

$$\exists_{\gamma_x} x \forall_{\gamma_a} a \exists_{\gamma_y} y . \phi_{\gamma}(x, a, y)$$

Eliminating the Existential Quantifier

- By Skolemization
- Alternating quantifiers introduce functions

Applied to:

$$\exists_{\gamma_x} x \forall_{\gamma_a} a \exists_{\gamma_y} y . \phi_{\gamma}(x, a, y)$$

becomes:

$$\forall_{\gamma_a} a . \phi_{\gamma}(f_x, a, f_y(a))$$

Approximating the Universal Quantifier

- Precision regulates domain size of the bound variable.
- Quantifier is replaced by a finite conjuction

Let $D(a) = \{a_0, a_1, \ldots, a_n\}$. The formula:

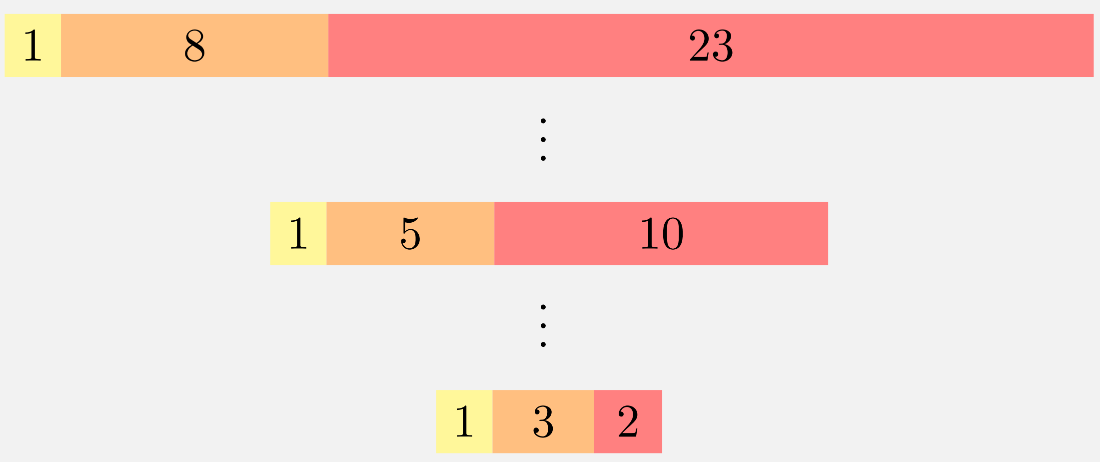
$$\forall_{\gamma_a} a . \phi_{\gamma}(f_x, a, f_y(a))$$

becomes the following:

$$\phi(f_x, a_0, f_y(a_0)) \wedge \ \ldots \ \wedge \phi(f_x, a_n, f_y(a_n))$$

Reducing the Domain

- Consider theory-specific solutions
- FPA is parametrized by design
- Domains of FPA are scaled based on precision
- The framework aims to exploit the domain reduction
- For universally bound variables, model reconstruction can depend on the choice of the reduced domain.



Reducing the range and precision of the floating-point sorts

Representing Skolem Functions

Consider the following formula and several candidate models:

$$\exists x \forall a \exists y . a - x = a$$

$$\begin{array}{cc|c|c|c|c}
D(a) & = & \{0\} & \{0,1\} & \{0,1,2\} & \{0,1,2,\ldots\} \\
f_x & = & 0 & 0 & 0 & 0 \\
f_y(a) & = & 0 & \begin{cases} 1 & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases} & \begin{cases} 2 & \text{if } a \neq 2 \\ 1 & \text{if } a = 1 \\ 0 & \text{if } a = 0 \end{cases} & a \\
\text{CEx} & & 0 - 0 \neq 1 & 1 - 0 \neq 2 & 2 - 0 \neq 3 & \text{None}
\end{array}$$

- Representation of Skolem functions needs to be compact and allow generalization
- Reconstruction can attempt to obtain various classes of functions.

Future Work and Challenges

- Compact Skolem-function representation
- Finding useful function templates
- Generalizing Skolem functions
- Informed reduction of the quantified domain
- Expanding the reduced domain in a meaningful way
- Balancing domain reduction with function generalization

[1]: Approximations For Model Construction — A. Zeljić, C. M. Wintersteiger, P. Rümmer, IJCAR 2014

Department of Information Technology, Uppsala University http://it.uu.se/