Rewriting Induction + Linear Arithmetic = Decision Procedure

Stephan Falke and Deepak Kapur
(by: Cynthia Kop)

September 14, 2023

$\mathbb{Z}$-Term Rewriting Systems

Terms: term rewriting systems that may include all integers and linear integer operations
Rules: pairs $l \to r\ [\varphi]$ of two terms and a constraint

$\mathbb{Z}$-Term Rewriting Systems

Terms: term rewriting systems that may include all integers and linear integer operations

Rules: pairs $l \to r\ [\varphi]$ of two terms and a constraint

Example:

$$\begin{array}{lcll}
\texttt{Divides}(x, y) & \to & \texttt{Divides}(-x, y) & [x < 0] \\
\texttt{Divides}(x, y) & \to & \texttt{Divides}(x, -y) & [y < 0] \\
\texttt{Divides}(x, y) & \to & \texttt{True} & [y = 0] \\
\texttt{Divides}(x, y) & \to & \texttt{False} & [x > y \land y > 0] \\
\texttt{Divides}(x, y) & \to & \texttt{Divides}(x, y - x) & [y \geq x \land x > 0]
\end{array}$$

Rewriting induction

Given: an equation $s \approx t \; [\varphi]$

Rewriting induction

Given: an equation $s \approx t \; [\varphi]$
Provides: a number of rules to prove either:

Rewriting induction

Given: an equation $s \approx t\ [\varphi]$

Provides: a number of rules to prove either:

- for all substitutions γ so that $\varphi\gamma$ is satisfied we have $s\gamma \leftrightarrow^* t\gamma$;

Rewriting induction

Given: an equation $s \approx t \; [\varphi]$
Provides: a number of rules to prove either:

- for all substitutions γ so that $\varphi\gamma$ is satisfied we have $s\gamma \leftrightarrow^* t\gamma$;
- there exists substitution γ so that $\varphi\gamma$ is satisfied and not $s\gamma \leftrightarrow^* t\gamma$.

Rewriting induction

Given: an equation $s \approx t\ [\varphi]$

Provides: a number of rules to prove either:

- for all substitutions γ so that $\varphi\gamma$ is satisfied we have $s\gamma \leftrightarrow^* t\gamma$;
- there exists substitution γ so that $\varphi\gamma$ is satisfied and not $s\gamma \leftrightarrow^* t\gamma$.

Example equations:

- $\texttt{Divides}(x, y) \approx \texttt{Divides}(\texttt{Times}(z, x), \texttt{Times}(y, z))\ [z > 0]$
- $\texttt{Divides}(x + 1, y) \approx \texttt{Divides}(x, y - 1)\ [x \neq y]$

Paper claim

We can use the rules of rewriting induction to
decide
whether or not an equation is satisfied.