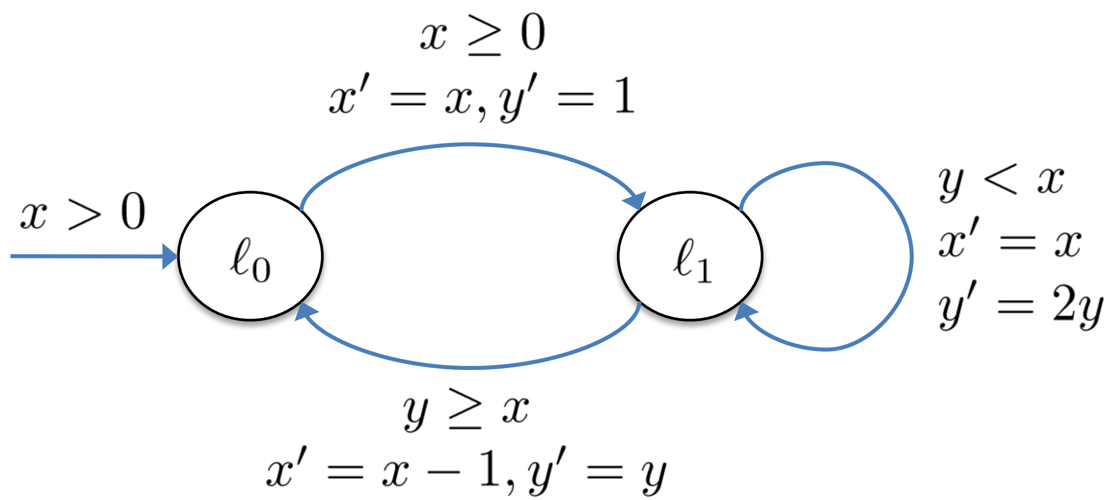
Decision Procedures for Automating Termination Proofs

Ruzica Piskac, EPFL
Thomas Wies, IST Austria

Proving Program Termination

```
assume x > 0
while x ≥ 0 do
   y := 1
   while y < x do
      y := 2y
   end
   x := x − 1
end
```



Ranking function into the natural numbers:

$$R(\langle x, y, \ell_0 \rangle) = 2x + \lceil \log(x!) \rceil$$
$$R(\langle x, y, \ell_1 \rangle) = 2x + \lceil \log(x!) - \log(y) \rceil - 1$$

Construction of global ranking functions is difficult (to automate)!

Automating Termination Proofs

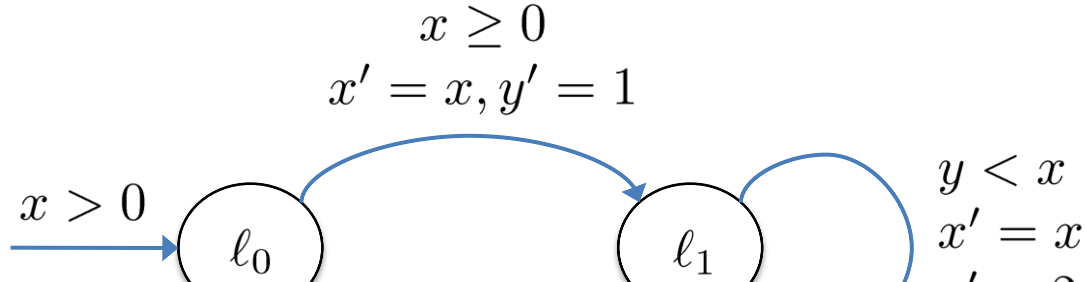
Proof techniques based on local ranking functions
- Size-change principle [Lee, Jones, Ben-Amram 2001]
- Transition invariants [Podelski, Rybalchenko 2004]

Idea
- decompose program into simpler ones
- prove each simple program terminating independently

Use decision procedures for well-founded domains
to automate these tasks
➔ Terminator [Cook, Podelski, Rybalchenko 2006]

Proving Program Termination

assume $x > 0$
while $x \geq 0$ **do**
  $y := 1$
  while $y < x$ **do**



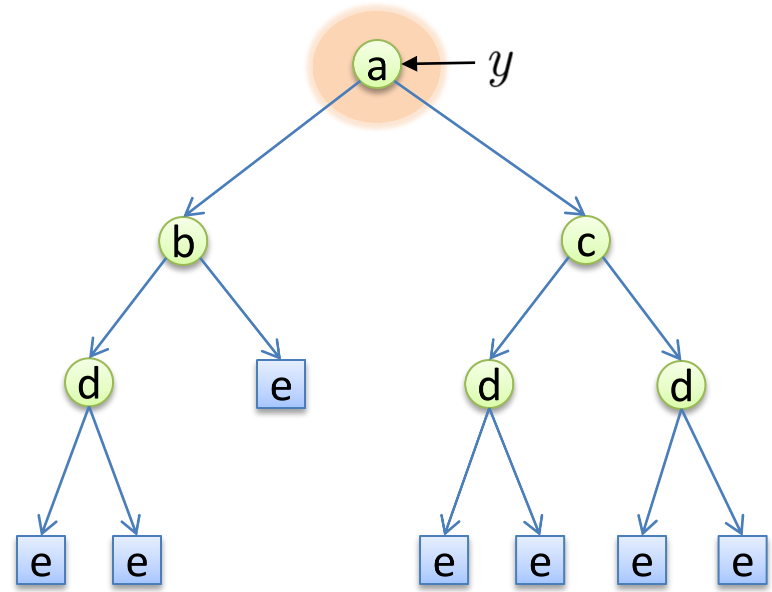
We need decision procedures for more powerful well-founded orderings.
This talk: decision procedures for **multiset orderings**

$$R(\langle x, y, \ell_0 \rangle) = (x, 1, 2x - y)$$
$$R(\langle x, y, \ell_1 \rangle) = (x, 0, 2x - y)$$

Decomposition into linear ranking functions is not always possible!

Counting Leaves in a Tree

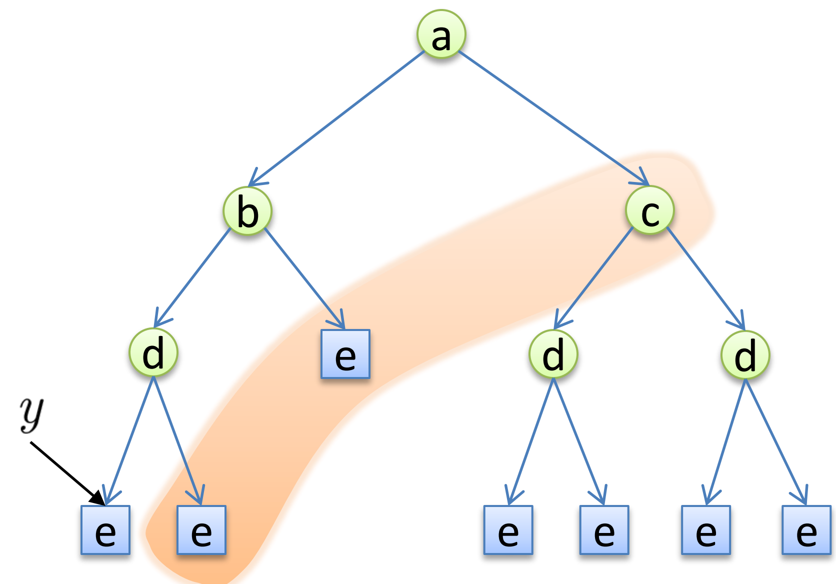
$$
\begin{array}{l}
\textbf{prog}\ \mathit{CountLeaves}(\mathit{root} : \mathsf{Tree}) : \mathsf{int} = \\
\quad \textbf{var}\ S : \mathsf{Stack}[\mathsf{Tree}] = \mathit{root} \\
\quad \textbf{var}\ c : \mathsf{int} = 0 \\
\quad \textbf{do} \\
\quad\quad y := \mathit{head}(S) \\
\quad\quad \textbf{if}\ \mathit{leaf}(y)\ \textbf{then} \\
\quad\quad\quad S := \mathit{tail}(S) \\
\quad\quad\quad c := c + 1 \\
\quad\quad \textbf{else}\ S := \mathit{left}(y) \cdot \mathit{right}(y) \cdot \mathit{tail}(S) \\
\quad \textbf{until}\ S = \epsilon \\
\quad \textbf{return}\ c
\end{array}
$$



S : a

Counting Leaves in a Tree

prog $\mathit{CountLeaves}(\mathit{root} : \mathsf{Tree}) : \mathsf{int} =$
    var $S : \mathsf{Stack}[\mathsf{Tree}] = \mathit{root}$
    var $c : \mathsf{int} = 0$
    do
        $y := \mathit{head}(S)$
        if $\mathit{leaf}(y)$ **then**
            $S := \mathit{tail}(S)$
            $c := c + 1$
        else $S := \mathit{left}(y) \cdot \mathit{right}(y) \cdot \mathit{tail}(S)$
    until $S = \epsilon$
    return c

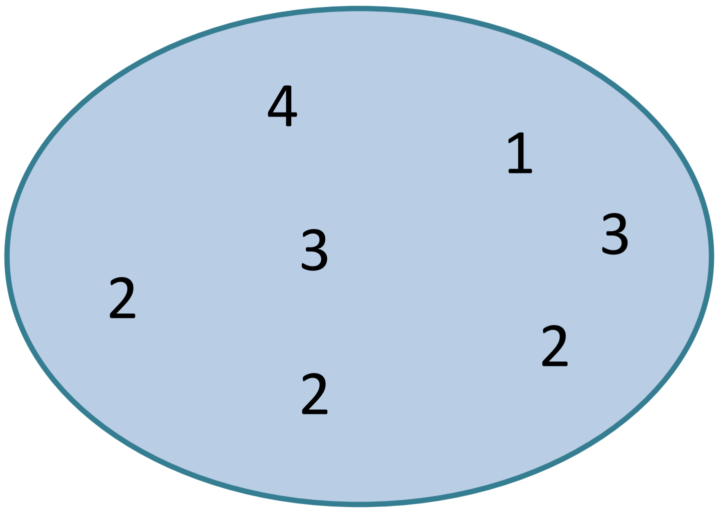


$S : \mathsf{e} \cdot \mathsf{e} \cdot \mathsf{c}$

Ranking function for loop: $R(\langle S, c\rangle) = \sum_{t \in S} |\mathit{nodes}(t)|$

Consider S as a multiset of trees with subtree ordering.

Multisets



X

base set

$$X : \mathbb{N} \to \mathbb{N}$$

$$X(0) = 0$$ multiplicity

$$\begin{array}{rl} & X(1) = 1 \\ & X(2) = 3 \\ & X(3) = 2 \\ & X(4) = 1 \\ & X(5) = 0 \\ + & \ldots \\ \hline & 7 \end{array}$$

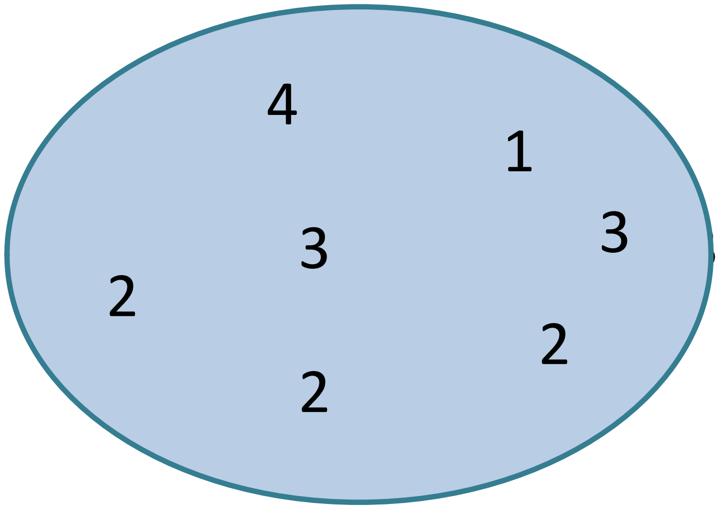
finite multisets

Operations are defined point-wise:

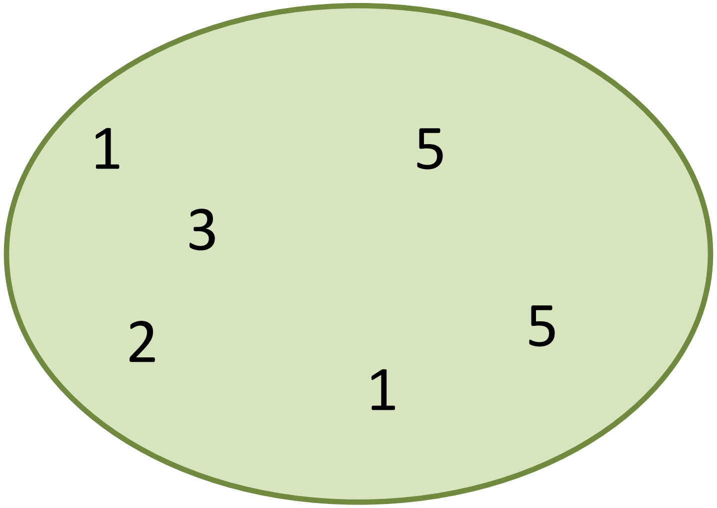
$$X = Y \uplus Z \iff \forall x. X(x) = Y(x) + Z(x)$$

Multiset Orderings

Extend ordering $\preceq$ on base set to ordering $\preceq_m$ on multisets



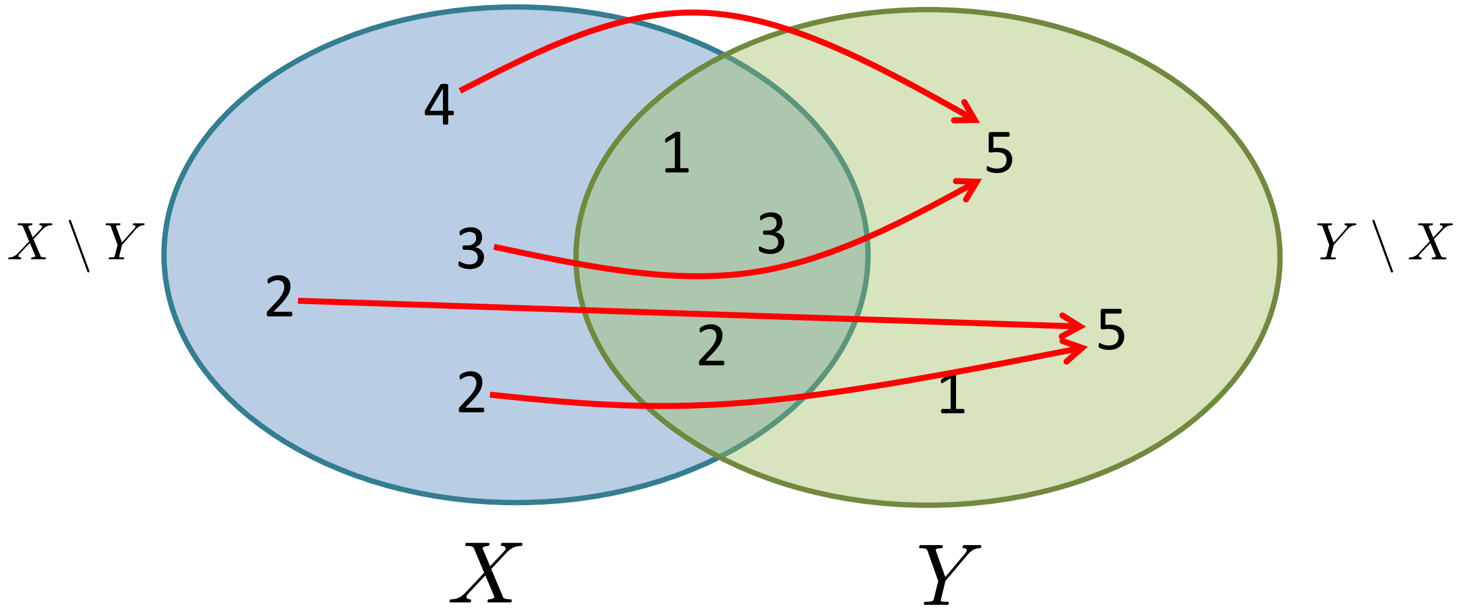
$\preceq_m$



X Y

Multiset Orderings

Extend ordering $\preceq$ on base set to ordering $\preceq_{\text{m}}$ on multisets

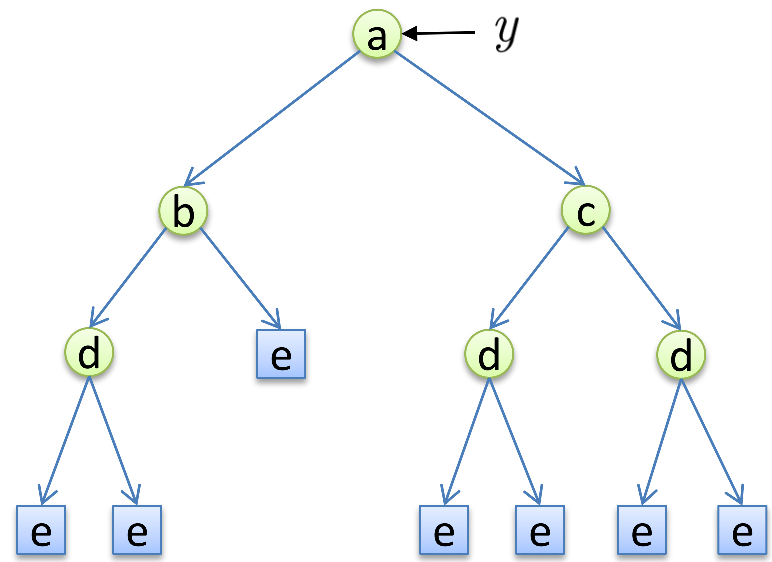


$$X \preceq_{\text{m}} Y \iff \forall x. X(x) > Y(x) \rightarrow \exists y. Y(y) > X(y) \wedge x \preceq y$$

$\preceq_{\text{m}}$ well-founded iff $\preceq$ well-founded [Dershowitz, Manna 1979]

Counting Leaves in a Tree

prog $CountLeaves(root : \mathsf{Tree}) : \mathsf{int} =$
 var $S : \mathsf{Multiset}[\mathsf{Tree}] = root$
 var $c : \mathsf{int} = 0$
 do
  $y := choose(S)$
  if $leaf(y)$ **then**
   $S := S \setminus \{y\}$
   $c := c + 1$
  else $S := (S \setminus \{y\}) \uplus \{left(y), right(y)\}$
 until $S = \emptyset$
 return c



Termination Condition for Loop:

extension of subtree relation to Multisets

$$S(y) > 0 \ \wedge (S' = S \setminus \{y\} \vee S' = (S \setminus \{y\}) \uplus \{left(y), right(y)\}) \rightarrow S' \prec_{\mathsf{m}} S$$

Is satisfiability of multiset ordering constraints decidable?

Main Results

Let $\mathcal{T}_0$ be a base theory of a preordered set.

Examples for $\mathcal{T}_0$

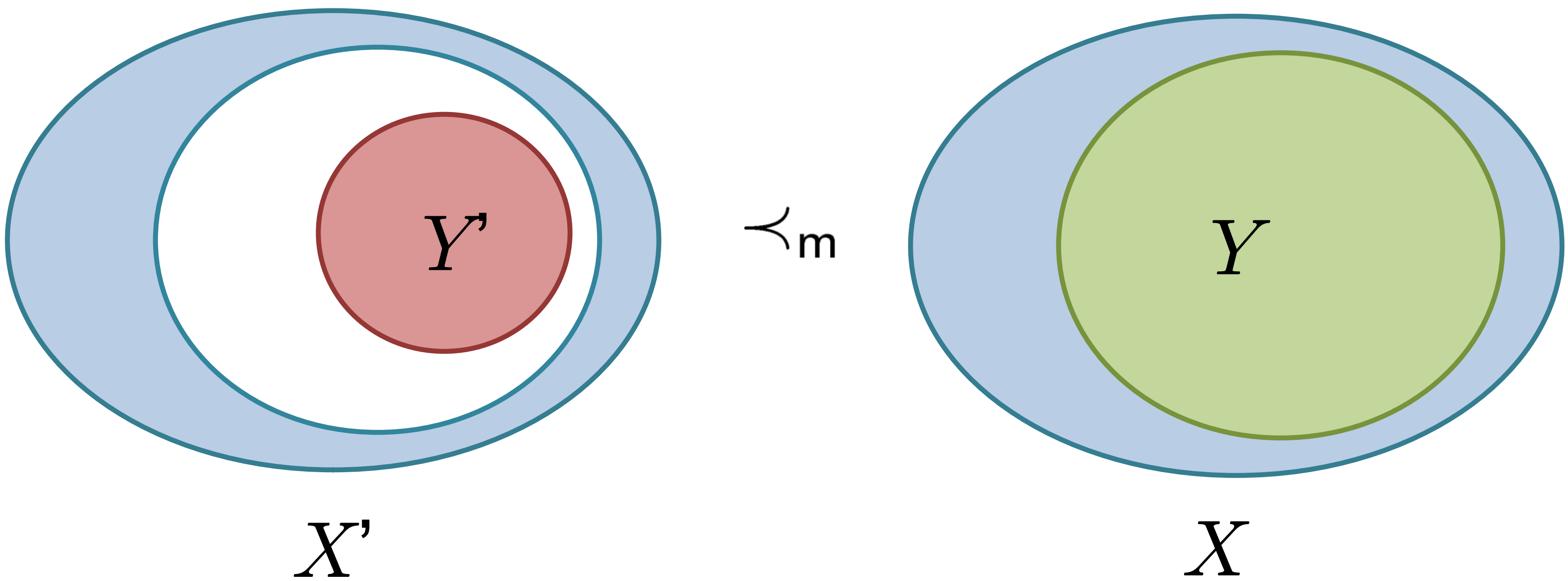
- theory of all preordered sets
- theory of linear integer arithmetic
- theory of a term algebra (trees) with subterm relation

1. If $\mathcal{T}_0$ is decidable then so is its multiset extension.
2. If $\mathcal{T}_0$ is decidable in NP then so is its multiset extension.
3. Decision procedure is easily implementable using off-the-shelf SMT solvers.

Decision Procedure through an Example

$$X' = (X \setminus Y) \uplus Y' \land Y \subseteq X \land Y' \prec_{\mathsf{m}} Y \land \neg(X' \prec_{\mathsf{m}} X)$$

Unsatisfiable!



Step 1: Flattening

Introduce fresh variables for all non-variable subterms

$$\frac{X' = (X \setminus Y) \uplus Y' \land Y \subseteq X \land Y' \prec_{\mathsf{m}} Y \land \neg(X' \prec_{\mathsf{m}} X)}{X' = X_1 \uplus Y' \land X_1 = X \setminus Y \land Y \subseteq X \land Y' \prec_{\mathsf{m}} Y \land \neg(X' \prec_{\mathsf{m}} X)} \; 1$$

Step 2: Reduction

Replace multiset operations by their pointwise definitions

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

1

$$\boxed{X' = X_1 \uplus Y'} \wedge \boxed{X_1 = X \setminus Y} \wedge \boxed{Y \subseteq X} \wedge \boxed{Y' \prec_{\mathsf{m}} Y} \wedge \boxed{\neg(X' \prec_{\mathsf{m}} X)}$$

2

Step 3: Skolemization

Skolemize all existential quantifiers

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

1

$$X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

2,3

$$\begin{array}{l}
(\forall x.\, X'(x) = X_1(x) + Y'(x)) \wedge \\
(\forall x.\, X_1(x) = \max\{X(x) - Y(x), 0\}) \wedge \\
(\forall x.\, Y(x) \cdot \quad X(x)) \wedge \\
(\exists y. Y'(y) \neq Y(y)) \wedge \\
(\forall y'.\, Y(y') < Y'(y') \to \exists y.\, Y'(y) < Y(y) \wedge y' \preceq y) \wedge \\
((\forall x. X'(x) = X(x)) \vee \\
\;(\exists x'.\, X(x') < X'(x') \wedge \forall x.\, X'(x) < X'(x) \to \neg(x' \preceq x)))
\end{array}$$

Step 3: Skolemization

Skolemize all existential quantifiers

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

1

$$X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

2,3

$$
\begin{array}{l}
(\forall x.\, X'(x) = X_1(x) + Y'(x)) \wedge \\
(\forall x.\, X_1(x) = \max\{X(x) - Y(x), 0\}) \wedge \\
(\forall x.\, Y(x) \cdot \;\; X(x)) \wedge \\
(Y'(c_1) \neq Y(c_1)) \wedge \\
(\forall y'.\, Y(y') < Y'(y') \rightarrow Y'(w(y')) < Y(w(y')) \wedge y' \preceq w(y')) \wedge \\
((\forall x. X'(x) = X(x)) \vee \\
\;(X(c_2) < X'(c_2) \wedge \forall x.\, X'(x) < X'(x) \rightarrow \neg(c_2 \preceq x)))
\end{array}
$$

witness function

Step 4: Strengthening

Add additional axioms constraining the witness functions

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

1

$$X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

2,3,4

$$\begin{array}{l}
(\forall x.\, X'(x) = X_1(x) + Y'(x)) \wedge \\
(\forall x.\, X_1(x) = \max\{X(x) - Y(x), 0\}) \wedge \\
(\forall x.\, Y(x) \cdot \quad X(x)) \wedge \\
(Y'(c_1) \neq Y(c_1)) \wedge \\
(\forall y'.\, Y(y') < Y'(y') \to Y'(w(y')) < Y(w(y')) \wedge y' \preceq w(y')) \wedge \\
((\forall x. X'(x) = X(x)) \vee \\
\;(X(c_2) < X'(c_2) \wedge \forall x.\, X'(x) < X'(x) \to \neg(c_2 \preceq x))) \\
\wedge\, F(Y, Y', w)
\end{array}$$

Step 5: Instantiation

Instantiate universal quantifiers with ground terms

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

1

$$X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

2,3,4

$$\begin{aligned}
&(\forall x.\, X'(x) = X_1(x) + Y'(x)) \wedge \\
&(\forall x.\, X_1(x) = \max\{X(x) - Y(x), 0\}) \wedge \\
&(\forall x.\, Y(x) \cdot \quad X(x)) \wedge \\
&(Y'(c_1) \neq Y(c_1)) \wedge \\
&(\forall y'.\, Y(y') < Y'(y') \to Y'(w(y')) < Y(w(y')) \wedge y' \preceq w(y')) \wedge \\
&((\forall x. X'(x) = X(x)) \vee \\
&\ (X(c_2) < X'(c_2) \wedge \forall x.\, X'(x) < X'(x) \to \neg(c_2 \preceq x))) \\
&\wedge F(Y, Y', w)
\end{aligned}$$

Instantiate with $c_1, c_2, w(c_1), w(c_2)$

Step 5: Instantiation

Instantiate universal quantifiers with ground terms

$$\frac{X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)}{X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)}\;1$$

2,3,4,5

$$\begin{aligned}
&Y'(c_1) \neq Y(c_1) \wedge X'(c_1) = X(c_1) \wedge \\
&\quad X'(c_1) = X(c_1) - Y(c_1) + Y'(c_1) \vee \\
&X'(c_2) = X(c_2) - Y(c_2) + Y'(c_2) \wedge \\
&\quad X(c_2) < X'(c_2) \wedge Y(c_2) \geq Y'(c_2) \vee \\
&X'(w(c_2)) = X(w(c_2)) - Y(w(c_2)) + Y'(w(c_2)) \wedge \\
&\quad Y'(w(c_2)) < Y(w(c_2)) \wedge X'(w(c_2)) \geq X(w(c_2)) \vee \\
&c_2 \preceq w(c_2) \wedge \neg(c_2 \preceq w(c_2))
\end{aligned}$$

Step 6: Check Satisfiability

Call decision procedure for base theory + LIA + EUF

$$X' = (X \setminus Y) \uplus Y' \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$ *Unsatisfiable!*

1

$$X' = X_1 \uplus Y' \wedge X_1 = X \setminus Y \wedge Y \subseteq X \wedge Y' \prec_{\mathsf{m}} Y \wedge \neg(X' \prec_{\mathsf{m}} X)$$

2,3,4,5

$$Y'(c_1) \neq Y(c_1) \wedge X'(c_1) = X(c_1) \wedge$$
$$X'(c_1) = X(c_1) - Y(c_1) + Y'(c_1) \vee$$

Unsatisfiable!

$$X'(c_2) = X(c_2) - Y(c_2) + Y'(c_2) \wedge$$
$$X(c_2) < X'(c_2) \wedge Y(c_2) \geq Y'(c_2) \vee$$

Unsatisfiable!

$$X'(w(c_2)) = X(w(c_2)) - Y(w(c_2)) + Y'(w(c_2)) \wedge$$
$$Y'(w(c_2)) < Y(w(c_2)) \wedge X'(w(c_2)) \geq X(w(c_2)) \vee$$

Unsatisfiable!

$$c_2 \preceq w(c_2) \wedge \neg(c_2 \preceq w(c_2))$$

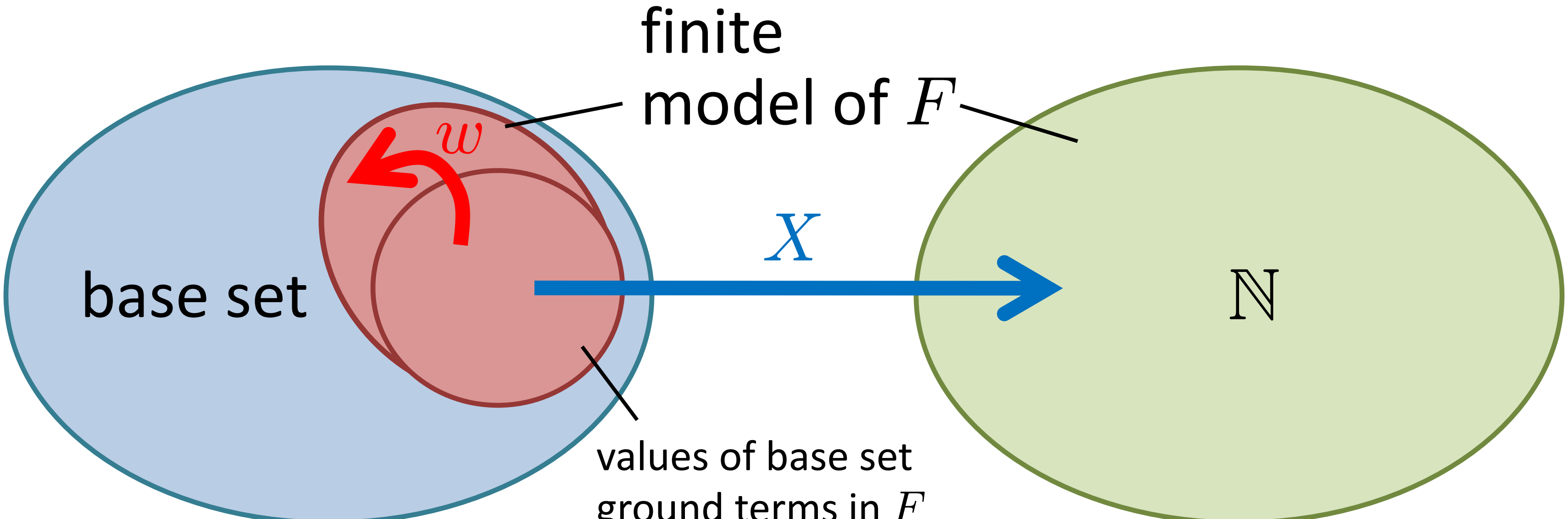
Unsatisfiable!

Completeness of Finite Instantiation

F: multiset ordering constraint after Skolemization

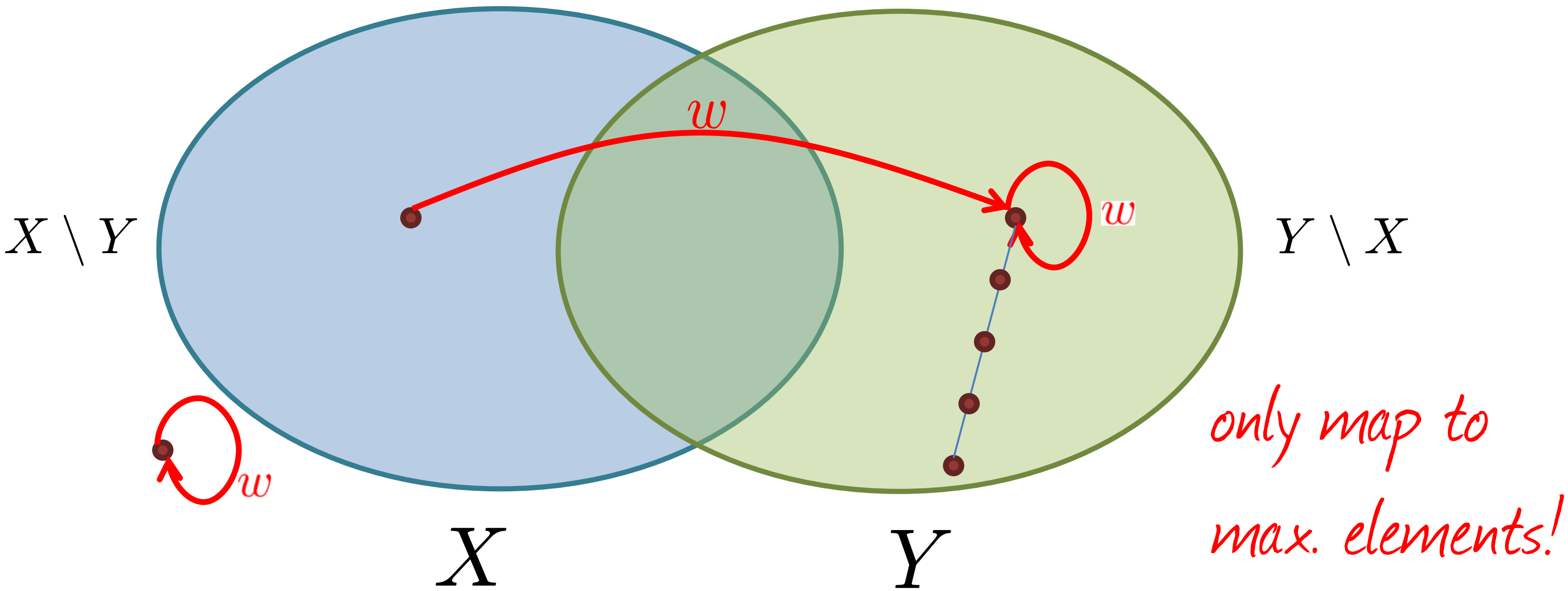
Functions representing multisets are sort restricted

but witness functions are not!



Additional axioms bound witness functions!

Axioms for Witness Functions



$$\boxed{\forall x.\, (X \setminus Y)(x) > 0 \rightarrow (Y \setminus X)(w(x)) > 0 \land x \preceq w(x)}$$

$$\boxed{\forall x.\, (X \setminus Y)(x) = 0 \rightarrow w(x) = x}$$

$$\boxed{\forall x\, y.\, (X \setminus Y)(x) > 0 \land w(x) \prec y \rightarrow (Y \setminus X)(y) = 0}$$

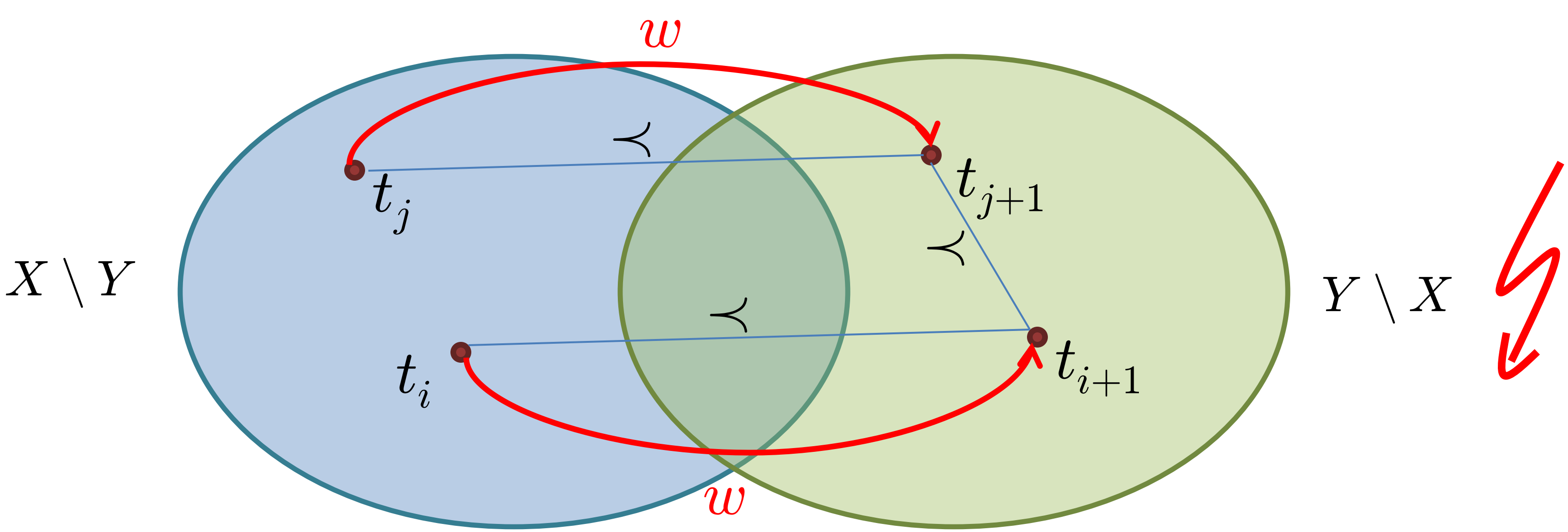
Axioms are designed specifically to guarantee NP complexity bound.

Completeness of Instantiation

F : formula obtained after strengthening, M : model of F
n : number of witness functions in F

$t_m \succ t_{m\text{-}1} \succ \ldots \succ t_0$ of length $m > n$ in M
$t_1 = w_0(t_0) \qquad t_2 = w_1(t_1) \qquad \ldots \qquad t_m = w_{m\text{-}1}(t_{m\text{-}1})$

then for some w, i, j : $0 \leq i < j < m$ and $w = w_i = w_j$

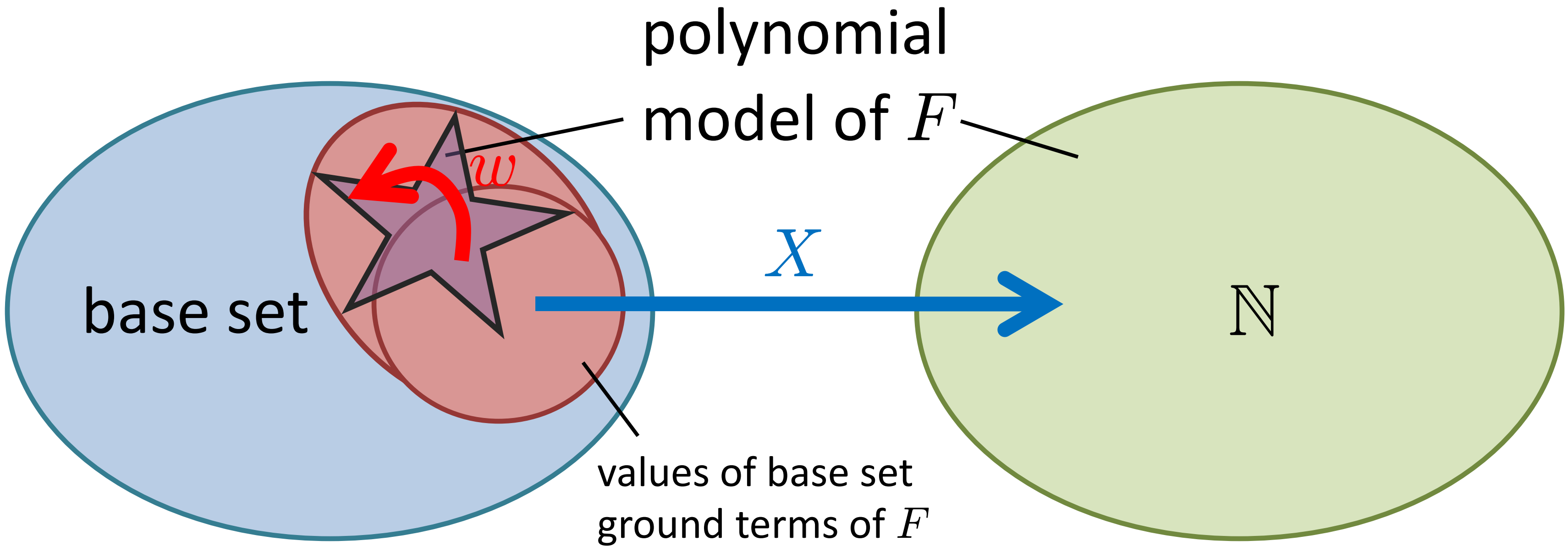


Strict chains can have at most length n!

Completeness of Finite Instantiation

F: multiset ordering constraint

Instantiate quantifiers with terms constructed from ground terms of F by applying each witness function at most once.



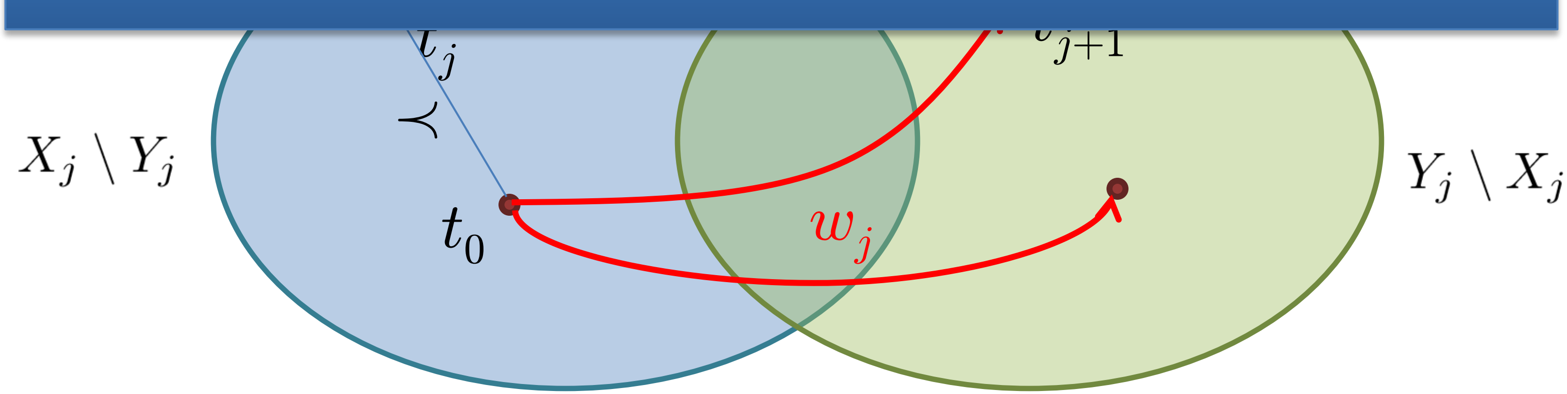
Size of the instantiated formula is exponential in number of witness functions!

Complexity

F : formula obtained after strengthening, M : model of F
n : number of witness functions, m : number of ground terms in F

$t_k \succ t_{k\text{-}1} \succ \ldots \succ t_0$: maximal strict chain of witness terms in M
$t_1 = w_0(t_0) \qquad t_2 = w_1(t_1) \qquad \ldots \qquad t_k = w_{k\text{-}1}(t_{k\text{-}1})$

If the base theory is decidable in NP then so is its multiset extension



Guess polynomially many strict chains. Then instantiate!

POSSUM

Multisets over Preordered Sets

top-level formulas:

$$\begin{array}{rcl}
F & ::= & A \mid F \wedge F \mid \neg F \\
A & ::= & M = M \mid M \subseteq M \mid M \preceq_{\mathsf{m}} M \mid A_{\mathsf{elem}} \mid K = K \mid K \cdot\ \ K \mid F^{\forall} \\
M & ::= & X \mid \emptyset \mid \{t^K\} \mid M \cap M \mid M \cup M \mid M \uplus M \mid M \setminus M \mid \mathsf{set}(M) \\
K & ::= & k \mid C \mid K + K \mid C \cdot K
\end{array}$$

restricted quantified formulas:

$$\begin{array}{rcl}
F^{\forall} & ::= & \forall x : \mathsf{elem}.F^{\forall} \mid \forall x : \mathsf{elem}.F_{\mathsf{in}} \\
F_{\mathsf{in}} & ::= & A_{\mathsf{in}} \mid F_{\mathsf{in}} \wedge F_{\mathsf{in}} \mid \neg F_{\mathsf{in}} \\
A_{\mathsf{in}} & ::= & t_{\mathsf{in}} \cdot\ \ t_{\mathsf{in}} \mid t_{\mathsf{in}} = t_{\mathsf{in}} \mid e_{\mathsf{in}} \preceq e_{\mathsf{in}} \mid e_{\mathsf{in}} = e_{\mathsf{in}} \\
t_{\mathsf{in}} & ::= & X(e_{\mathsf{in}}) \mid C \mid t_{\mathsf{in}} + t_{\mathsf{in}} \mid C \cdot t_{\mathsf{in}} \\
e_{\mathsf{in}} & ::= & x \mid t
\end{array}$$

terminals:

X - mult

t - groun

A_{elem} - g

If the base theory is decidable in NP then so is its POSSUM extension

Related Work

- Dershowitz, Manna 1979: Multiset orderings for termination proofs
- Zarba 2002: Multisets + linear integer arithmetic is decidable in NP
- Piskac, Kuncak 2008: Multisets + cardinality constraints are decidable in NP
- Kuncak, Piskac, Suter 2010: Sets over total orders + cardinality constraints are decidable in NP
- Nieuwenhuis 1993: Lexicographic path orderings decidable in NP
- Narendran, Rusinowitch, Verma 1998: Recursive path orderings decidable in NP
- Baader, Nipkow 1998: Term Rewriting and All That
- Zhang, Sipma, Manna 2005: Knuth-Bendix orderings decidable in NP
- Bradley, Manna, Sipma 2006: What's decidable about arrays?
- Sofronie-Stokkermans 2005: Local theory extensions
- Ihlemann, Jacobs, Sofronie-Stokkermans 2008: Psi-local theory extensions

Conclusion

New logic for reasoning about multisets over preordered sets (POSSUM)

- interesting applications: automating termination proofs
- parameterized by base theory
- decidable if base theory is decidable
- good complexity (NP complete for many base theories)
- implementation of decision procedure with off-the-shelf SMT-solvers possible