Developments in Deciding Presburger Arithmetic with Automata

Michal Hečko, Ondřej Lengál

Faculty of Information Technology
Brno University of Technology

AVM, Sep 2022

Automata-based decision procedure for $Th(\mathbb{Z}, 0, 1, +, \leq)$

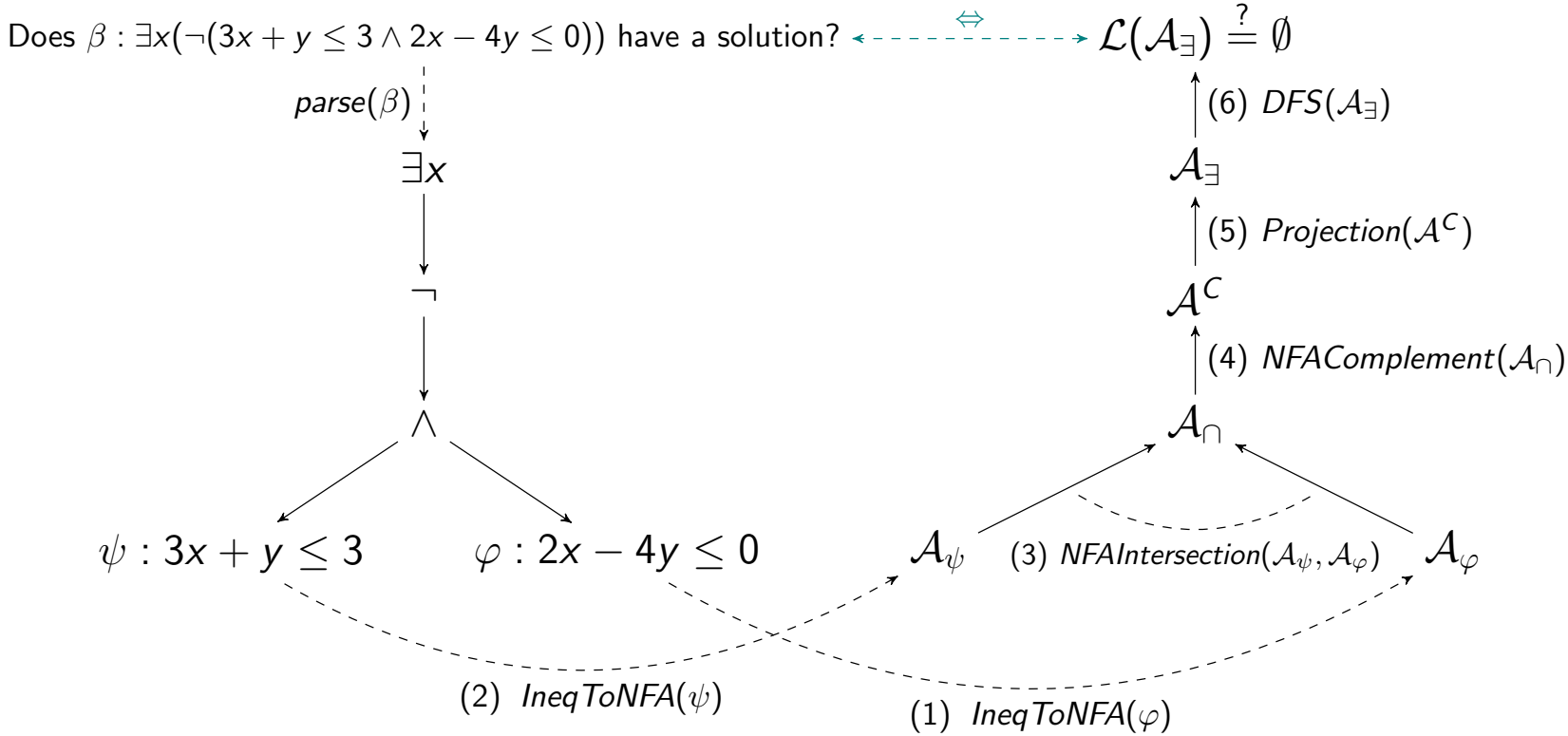


Figure: Illustration of an automata-based decision procedure

Progress made so far

- fully functional implementation (Python3)
- support for a subset of *SMTLIB2* found in LIA benchmarks
- two execution backends
  - *native* one, storing transitions explicitly
  - *MTBDD*-based one, storing transitions symbolically (implemented using the Sylvan library)
- research-oriented features, e.g., graphical output of the entire decision procedure (DOT)

Performance problems of the decision procedure

- exponential time complexity w.r.t. #variables
  - alleviated by using MTBDDs
- big coefficients in atomic formulae: $\vec{a} \cdot \vec{x} \leq K \rightsquigarrow \|\vec{a}\|$ states
  - automata for such atoms are already minimal
  - a single NFA for such an atom hinders the performance of the entire solver
  - the *20190429-UltimateAutomizerSvcomp2019* benchmark from the SMT competition contains such atoms:

$$(y \ mod \ 299993) \leq z + 300007$$

  - negation forces determinization of such automata $\rightsquigarrow$ even bigger NFAs

Handling large atoms with modulo terms

Fragment of a problematic formula

$$\overbrace{\exists y(x \leq y \wedge (y \bmod 299993) \leq z + 600000 \wedge (y \bmod 299993) \neq 0 \wedge y < 0)}$$

rewritten as

$$\exists y, m(x \leq y \wedge m \leq z + 600000 \wedge m \neq 0 \wedge y < 0 \wedge 0 \leq m \leq 299992 \wedge m \equiv_{299993} y)$$

simplified into

$$\psi : \exists y, m(x \leq y \wedge m \leq z + 600000 \wedge y < 0 \wedge 1 \leq m \leq 299992 \wedge m \equiv_{299993} y)$$

Handling large atoms with modulo terms

- experiments with smaller moduli show that the minimal DFA $\hat{\mathcal{A}}_\psi$ is very small compared to $\mathcal{A}_\psi$ resulting from the standard subset construction
- a simulation preorder $\preceq$ could be used to produce smaller states during determinization of a lazily constr. automaton
  - When computing $M' = \mathit{Post}(M, \sigma)$ in the subset construction, check for any $q \in M'$ such that $\exists r \in M'(r \neq q \wedge q \preceq r)$ and remove such q from M' [1]
- straightforward computation of the simulation requires constructing the automaton $\rightsquigarrow$ search for *implicit* simulations

[1] Glabbeek, R. van and Ploeger, B. Five Determinisation Algorithms. In: Ibarra, B., ed. Implementation and Applications of Automata. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, p. 161–170. ISBN 978-3-540-70844-5.

Implicit simulations

$$\psi : \exists y, m(x \leq y \wedge m \leq z + 600000 \wedge y < 0 \wedge 1 \leq m \wedge m \leq 299992 \wedge m \equiv_{299993} y)$$

- six atoms in $\psi \rightsquigarrow$ states of $\mathcal{A}_\psi$ will be sets of 6-tuples
- every 6-tuple represents a formula related to the atoms in ψ

$$(-1, -1, -1, 0, 0, 303)$$

$$\vdots \text{ represents}$$

$$x - y \leq -1 \wedge m - z \leq -1 \wedge y \leq -1 \wedge -m \leq 0 \wedge m \leq 0 \wedge m - y \equiv_{299993} 303$$

Implicit simulations

Therefore $(-1,-1,-1,0,0,303) \preceq (0,-1,-1,0,0,303)$ as

$$Sol(x - y \leq -1 \cdots \equiv_{299993} 303) \subseteq Sol(x - y \leq 0 \cdots \equiv_{299993} 303)^2$$

[2] $Sol(\varphi)$ denotes the solution space of φ

Implicit simulations - going further

- states of $\mathcal{A}_\psi$ are sets of 6-tuples $\Leftrightarrow$ disjunctions of formulae
- one can push existential quantifiers deeper into the disjunction and simplify if suitable/possible

$$\{\dots(-1,-1,-1,0,0,303)\dots\}$$

represents

$$\exists y, m(x - y \leq -1 \wedge m - z \leq -1 \wedge y \leq -1 \wedge -m \leq 0 \wedge m \leq 0 \wedge m - y \equiv_{299993} 303)$$

infer fixed value $m = 0$

$$\exists y(x - y \leq -1 \wedge -z \leq -1 \wedge y \leq -1 \wedge -y \equiv_{299993} 303)$$

instantiate $\exists y$ with $y = -303$

$$(x + 303 \leq -1 \wedge -z \leq -1)$$

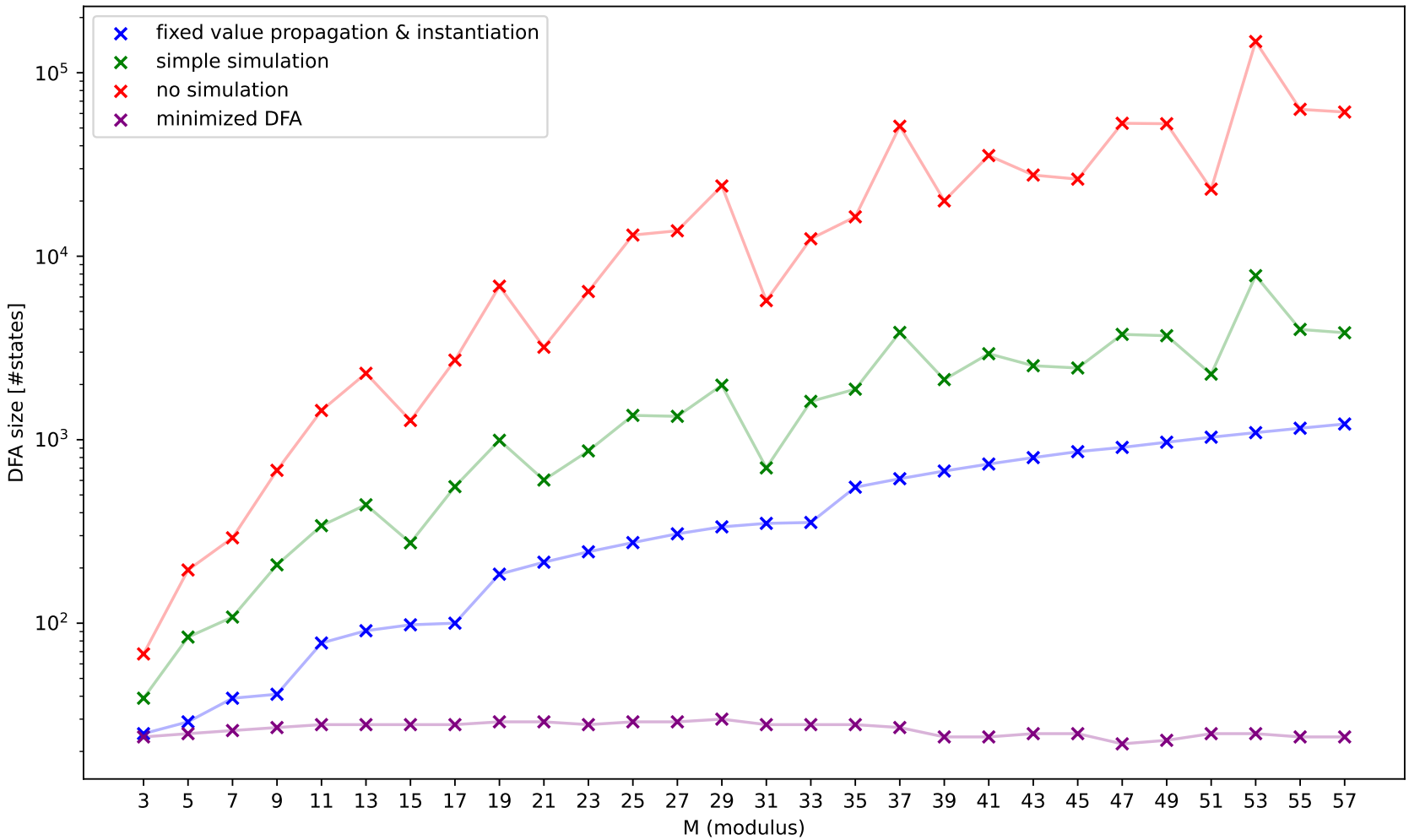
simplify

$$(x \leq -304 \wedge -z \leq -1)$$

- performing this simplification as preprocessing of the input formula?

Size reductions when using implicit simulation preorders

$$\psi : \exists y, m(x \leq y \wedge m \leq z + 30 \wedge y < 0 \wedge 1 \leq m \wedge m \leq M \wedge m \equiv_M y)$$



Thank you for your attention.

Questions?

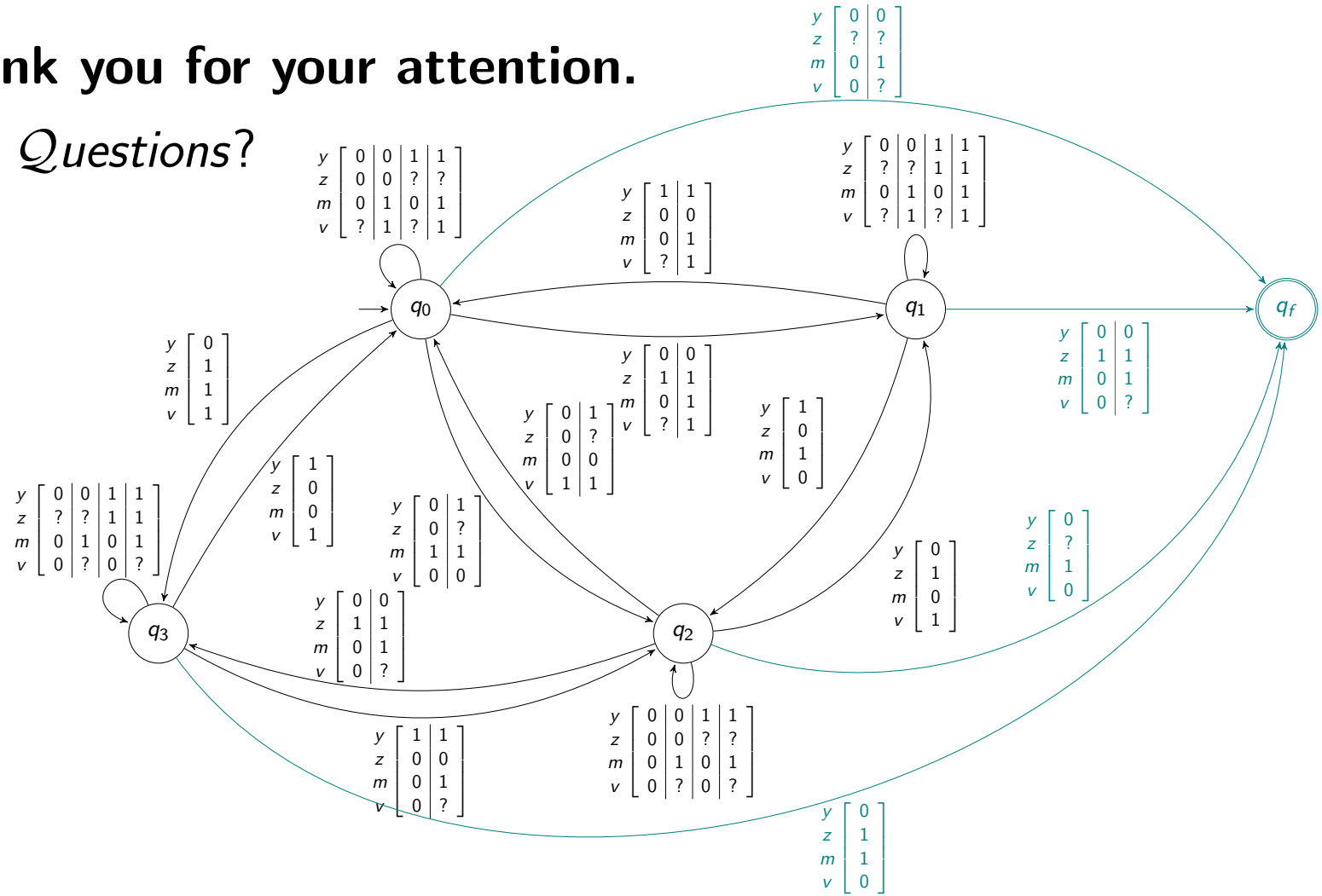


Figure: SCC of $\mathcal{A}$ for $z \leq y \wedge 0 \leq y \wedge m \leq v + 300007$