Computing Linear Arithmetic Representation of Reachability Relation of One-counter Automata

Authors: **Xie Li**, Taolue Chen, Zhilin Wu and Mingji Xia

SETTA 2020: Guangzhou, China, November 24-28, 2020

Overview

- Introduction to One-counter Automata(OCA) and its Reachability Problem.

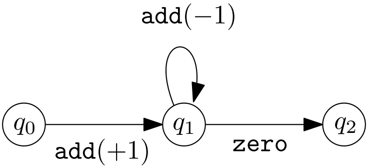
Overview

- Introduction to One-counter Automata(OCA) and its Reachability Problem.
- Computing the Reachability Relation of OCA.
- Introduction to Tool ORAREACH.
- Experimental Results of our Tool OCAREACH.

What is One-counter Automata(OCA)

- DFA with a **counter** where counter value is **non-negative**.
- Transitions: $q \xrightarrow{\texttt{Op}} q'$ where $\texttt{Op} \in \{\texttt{add}(+1), \texttt{add}(-1), \texttt{zero}\}$

Example (OCA)



Semantic of OCA: A transition system where the configuration is of the form (q, c) and counter changes corresponds to OCA.

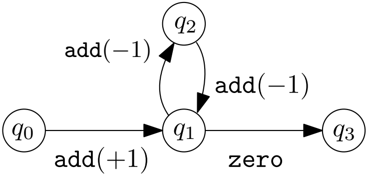
$$(q_1, c_1) \rightarrow_{\mathcal{A}} (q_2, c_2)$$

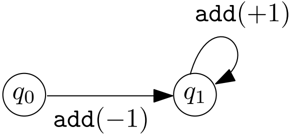
if $q_1 \xrightarrow{\texttt{add}(+1)} q_2$ in the OCA and $c_1 + 1 = c2$, or
if $q_1 \xrightarrow{\texttt{zero}} q_2$ and $c_1 = c_2 = 0$.

Reachability

Reachability Problem of OCA: whether $(q_s, c_s) \rightarrow^*_{\mathcal{A}} (q_t, c_t)$

Example





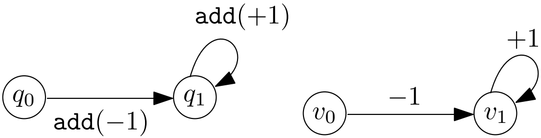
- $(q_3, 0)$ is reachable from $(q_0, 1)$.
- $(q_3, 0)$ is not reachable from $(q_0, 0)$

Due to the non-negative requirement, $(q_1, 1)$ is not reachable from $(q_0, 0)$

Weighted Directed Graph, Path Flow and Support

- An OCA can be regarded as a weighted directed graph $G_{\mathcal{A}} = (V, E, \eta)$.
- **Path**: a sequence of vertices $v_0 \cdot v_1 \cdots v_k$ where $(v_i, v_{i+1}) \in E$.
  - Weight of path
  - Drop of path
- **Flow**: a function $f : E \to \mathbb{N}$.

Example

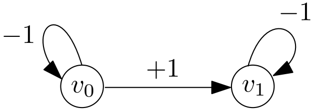


- path: $v_0 \cdot v_1 \cdot v_1$
- weight: $+1$
- drop: -1

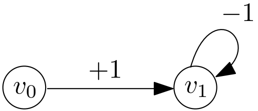
Path Flow and Support

- s-t **path flow**: the flow corresponds to a path.
- Support: edge-induced subgraph of path.

Example



- Support:



- Path: $v_0 \cdot v_1 \cdot v_1$
- Pathflow: $f(v_0, v_0) = 0$
  $f(v_0, v_1) = 1$
  $f(v_1, v_1) = 2$
- Weight:
  $w = \Sigma_{e \in E} f(e) \cdot \eta(e)$

The Difficulty of the Reachability Problem

NON-NEGATIVE

If we do not require the non-negative of counter.

- Flow is a path flow $\Leftrightarrow$ Requirements on flow.
  - $v_s \cdots v_t$ where $s \neq t$
  - $v_s \cdots v_s$
- Weight equals to the value change.

Non-negative implies the constraint: everywhere along the path, the counter need to be non-negative.

Certificate of the Reachability

Use **path flow** as certificate of OCA reachability problem.

- Type 1 Certificate
- Type 2 Certificate
- Type 3 Certificate

Edge Decomposition

Reachability Relation of OCA

Reachability Relation of OCA:

$$\phi_{\mathcal{A},q_s,q_t}(x_s, x_t)$$

How we Reduce the Reachability Relation to QFPA Formula

OCAREACH: Architecture

Experimental Evaluation