Invariants for One-Counter Automata with Disequality Tests

Dmitry Chistikov
University of Warwick
United Kingdom

Jérôme Leroux
LaBRI, CNRS, Bordeaux
France

Henry Sinclair-Banks
University of Warwick
United Kingdom

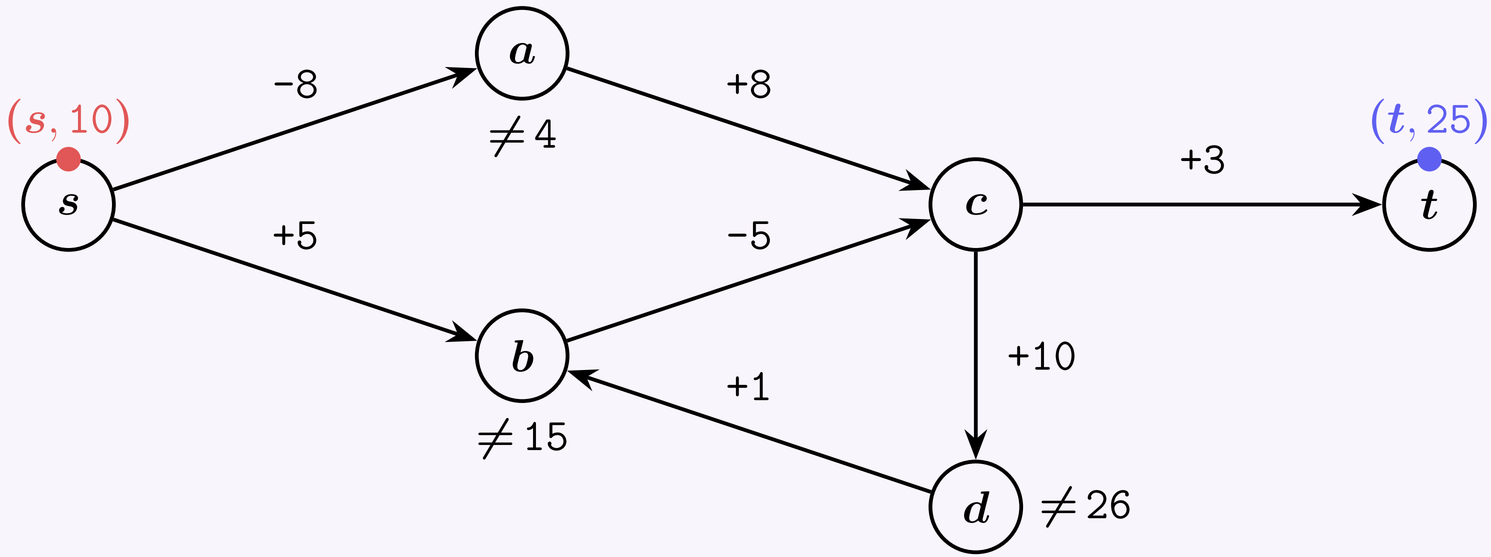
Nicolas Waldburger
IRISA, Université de Rennes
France

CONCUR'24: Automata and Logic I

12th September 2024

Best Western Plus Village Park Inn, Calgary, Canada

One-Counter Automata with Disequality Tests



A **configuration** consists of current state and counter value that respects the disequality tests.

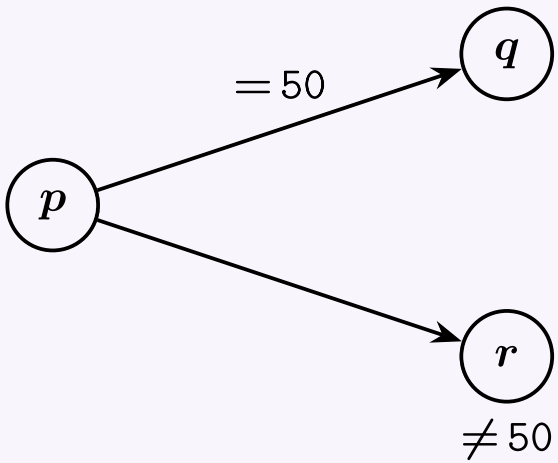
A **run** is a sequence of configurations.

Reachability: is there a run from **the initial configuration** to **the target configuration** ?

Motivation

Original motivation. Reachability in one-counter automata with disequality tests can be used for model checking in LTL extended with *flat freeze operators*. [Demri and Sangnier '10]
[Lechner, Mayr, Ouaknine, Pouly, and Worrell '18]

Standalone motivation. Equality and disequality tests allow for *if–then–else* conditionals.



Motivation

Original motivation. Reachability in one-counter automata with disequality tests can be used for model checking in LTL extended with *flat freeze operators*. [Demri and Sangnier '10]

[Lechner, Mayr, Ouaknine, Pouly, and Worrell '18]

Standalone motivation. Equality and disequality tests allow for *if − then − else* conditionals.

Theorem. Reachability in one-counter automata (with equality tests) is NP-complete.

[Haase, Kreutzer, Ouaknine, and Worrell '09]

Simulating disequality tests with equality tests is inefficient.

Theorem. Reachability in one-counter automata with $\leq$ tests is PSPACE-complete.

[Fearnley and Jurdziński '13]

Our Main Contribution and Prior Work

Theorem. Reachability in one-counter automata (with equality tests) is NP-complete

[Haase, Kreutzer, Ouaknine, and Worrell '09]

Theorem. Coverability (and boundedness) in one-counter automata with disequality tests is in P.

[Almagor, Cohen, Pérez, Shirmohammadi, and Worrell '20]

"*The complexity of reaching a given configuration in this model is open, lying between* NP *and* PSPACE"

Theorem. Reachability in one-counter automata with disequality tests is in $\mathsf{coNP}^{\mathsf{NP}}$. [This paper]

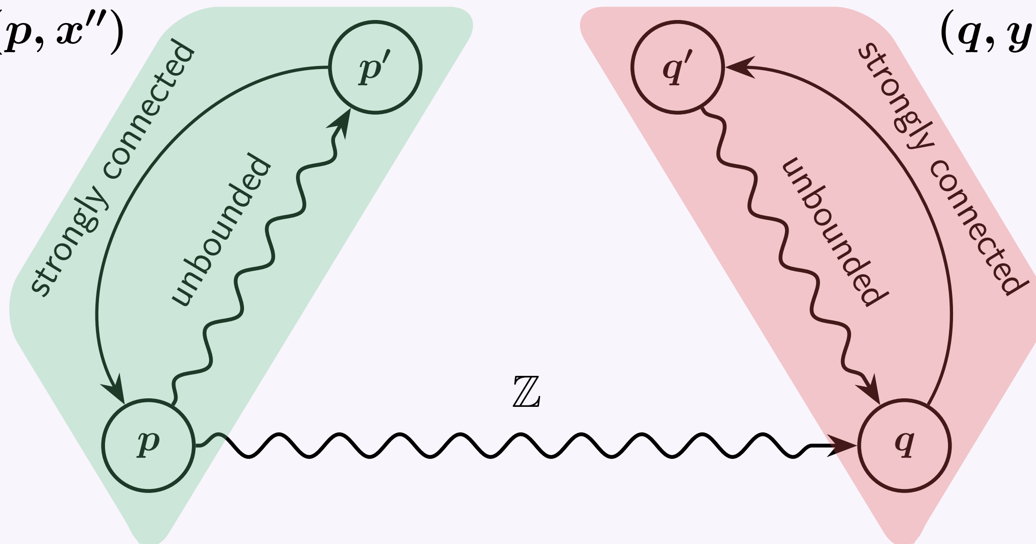
Reachability in Strongly Connected OCA with Disequality Tests

Case 1: (p, x) is unbounded and (q, y) is "reverse unbounded".

Claim: There is a run from (p, x) to (q, y) if and only if there is a $\mathbb{Z}$-run from (p, x) to (q, y).

$(p, x) \xrightarrow{*} (p', x') \xrightarrow{*} (p, x'')$

Positive cycle α.



$(q, y) \xleftarrow{*} (q', y') \xleftarrow{*} (q, y'')$

Negative cycle β.

$$(p, x) \xrightarrow{\alpha\,\alpha\,\cdots\,\alpha} (p, x + L) \xrightarrow[\mathbb{Z}]{*} (q, y + L) \xrightarrow{\beta\,\beta\,\cdots\,\beta} (q, y)$$

Reachability in Strongly Connected OCA with Disequality Tests

Case 1: (p, x) is unbounded and (q, y) is "reverse unbounded".

Claim: There is a run from (p, x) to (q, y) if and only if there is a $\mathbb{Z}$-run from (p, x) to (q, y).

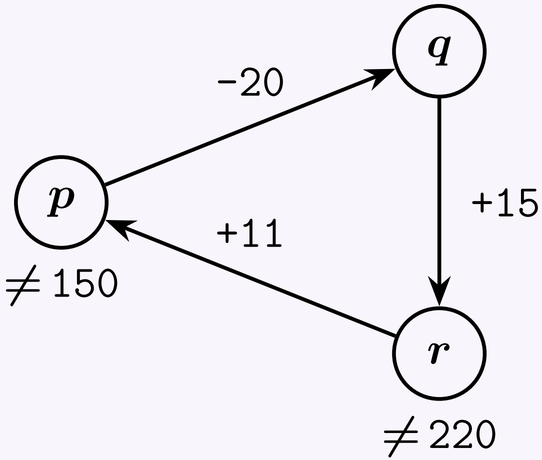
$\implies$ Case 1 is in NP.

Case 2: (p, x) is bounded (symmetric to (q, y) is "reverse bounded").

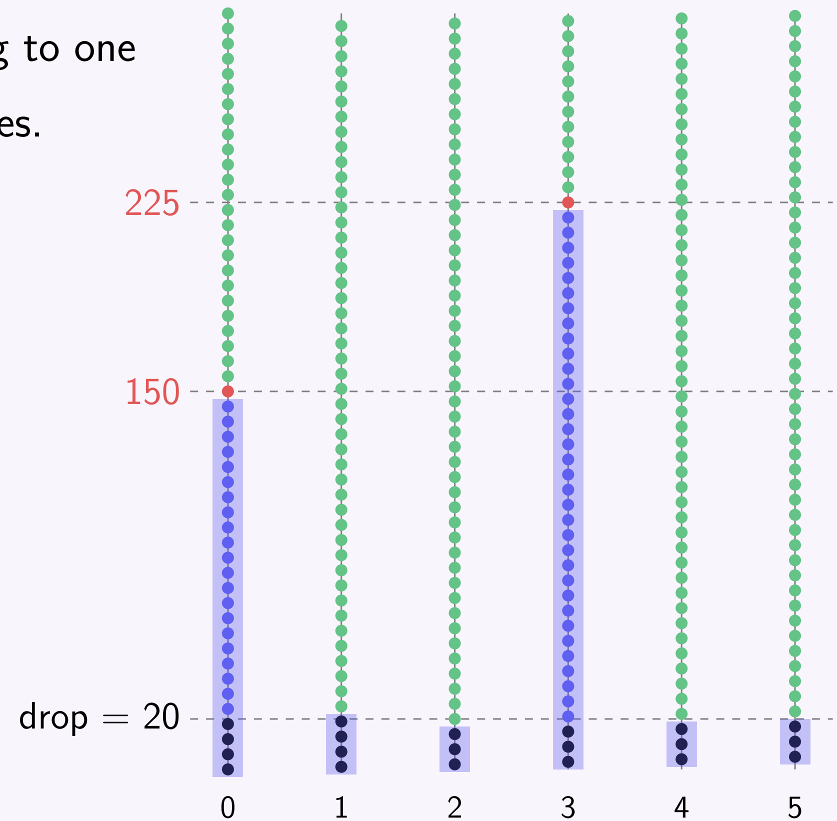
Mission for the remainder of this presentation: Case 2 is in $\mathsf{coNP}^{\mathsf{NP}}$.

Setting up an Invariant for Reachability

For each state, pick a cycle* with effect $e > 0$. In the example, for state p, $e = 6$.



Configurations belong to one of $e = 6$ many classes.



Key: Black = cannot afford cycle.

Red = violate disequality test.

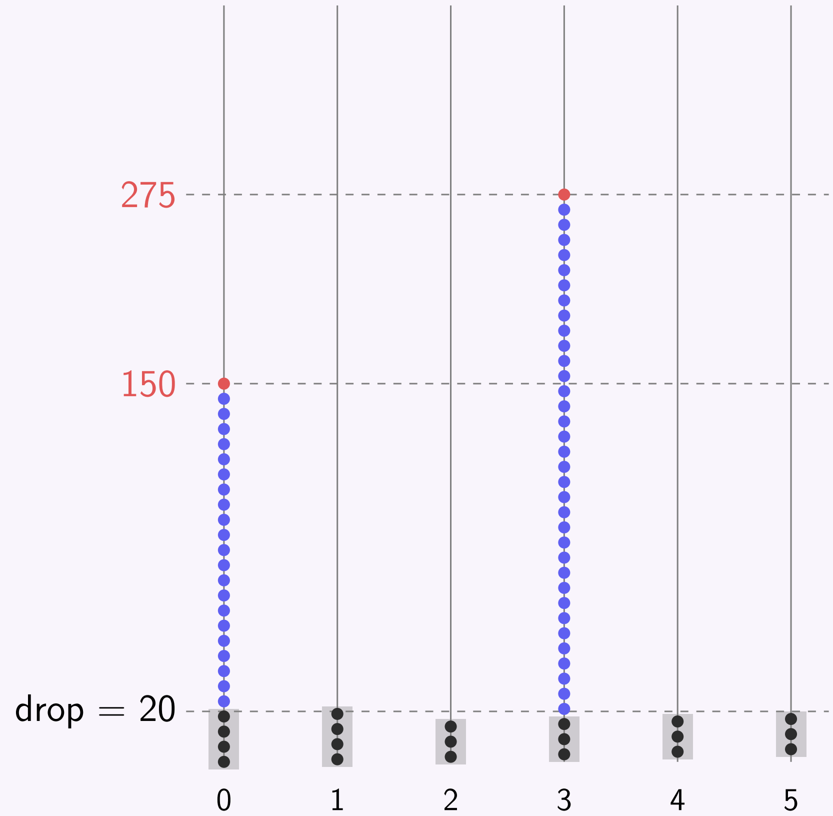
Green = unbounded.

Blue = bounded (by a disequality test).

Reachability Properties Below and in Chains

Reachability under the drop of all cycles can be checked in NP.

"Pessimistic Reachability"



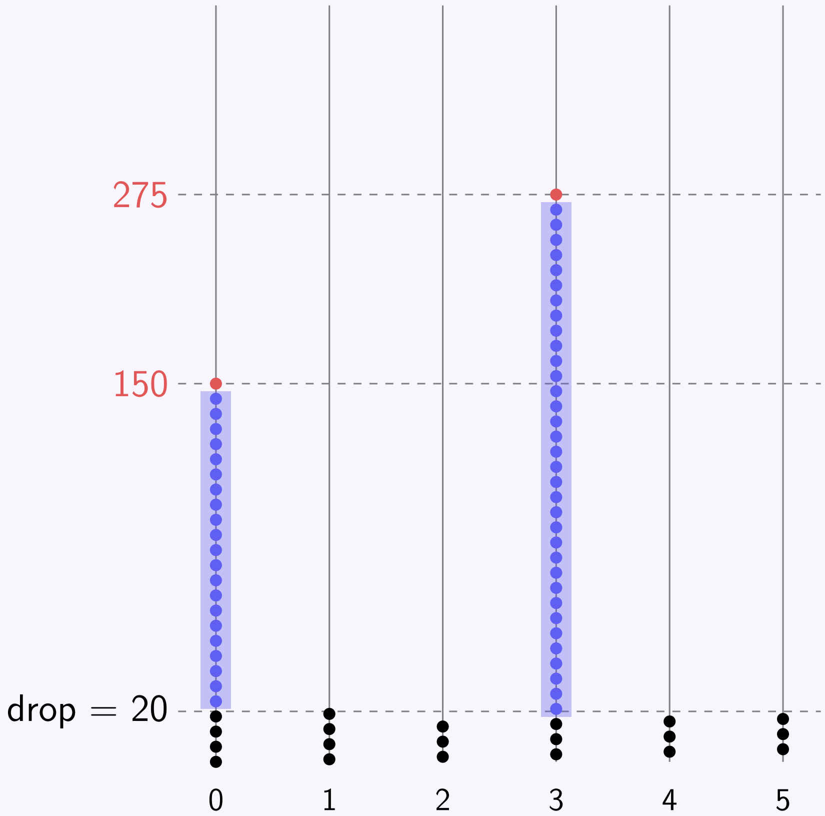
Reachability Properties Below and in Chains

Reachability under the drop of all cycles can be checked in NP.

"Pessimistic Reachability"

Bounded chains are upwards closed.

Let $\boldsymbol{R} = \{$ reachable points in bounded chains $\}$.



Reachability Properties Below and in Chains

Reachability under the drop of all cycles can be checked in NP.

"Pessimistic Reachability"

Bounded chains are upwards closed.

Let $\boldsymbol{R} = \{$ reachable points in bounded chains $\}$.

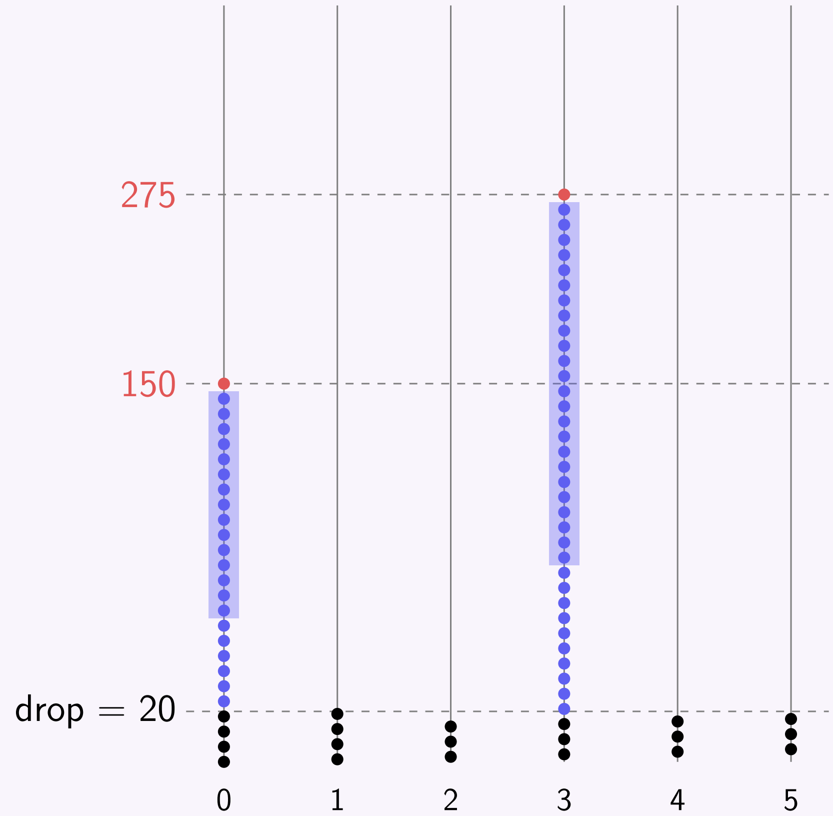
Suppose $\boldsymbol{R} = \{(\boldsymbol{p}, 60), (\boldsymbol{p}, 66), \ldots, (\boldsymbol{p}, 144)\} \cup \{(\boldsymbol{p}, 81), (\boldsymbol{p}, 89), \ldots, (\boldsymbol{p}, 219)\}$.

$\boldsymbol{R}$ has a concise description:

lowest configuration maximum cycle iteration count

$\boldsymbol{R} = \mathsf{AP}((\boldsymbol{p}, 60), \underline{+6}, 14) \cup \mathsf{AP}((\boldsymbol{p}, 81), +6, 23)$.

cycle effect



Invariants that Witness Non-reachability

Theorem. Let $\mathcal{A}$ is a strongly connected one-counter automata with disequality tests.

Let (p, x), (q, y) be two configurations and suppose (p, x) is bounded in $\mathcal{A}$.

Then, there *does not exist* a run from (p, x) to (q, y) in $\mathcal{A}$ if and only if

(Cond1) $(p, x) \in R$,

(Cond2) $(q, y) \notin \text{Post}^*_-(R)$, and

reachable via configurations under the drop of all cycles (pessimistic)

(Cond3) $\text{Post}(\text{Post}^*_-(R)) \cap \{\text{ bounded chains }\} \subseteq R$.

Theorem. Non-reachability in strongly connected one-counter automata with disequality tests is in NP^{NP}.

Proof idea. Guess R concisely. Check violation of (Cond1), or (Cond2), or (Cond3) in coNP.

Remember that $\text{NP}^{\text{coNP}} = \text{NP}^{\text{NP}}$.

Corollary. Reachability in strongly connected one-counter automata with disequality tests is in coNP^{NP}.

Invariants for One-Counter Automata with Disequality Tests

Corollary. Reachability in strongly connected one-counter automata with disequality tests is in $\mathsf{coNP}^{\mathsf{NP}}$.

[This presentation]

Theorem. Reachability in one-counter automata with disequality tests is in $\mathsf{coNP}^{\mathsf{NP}}$. [In the paper]

Theorem. Reachability in one-counter automata with *equality and disequality tests* is in $\mathsf{P}^{\mathsf{NP}^{\mathsf{NP}}}$.

[In the paper]

Thank You!

Presented by Henry Sinclair-Banks, University of Warwick, UK

CONCUR'24 in Best Western Plus Village Park Inn, Calgary, Canada