Efficient Convex Zone Merging in Parametric Timed Automata

Étienne André[1], Dylan Marinho[1], Laure Petrucci[2], Jaco van de Pol[3]

[1] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
[2] LIPN, CNRS UMR 7030, Université Sorbonne Paris Nord, Villetaneuse, France

[3] Aarhus University, Aarhus, Denmark

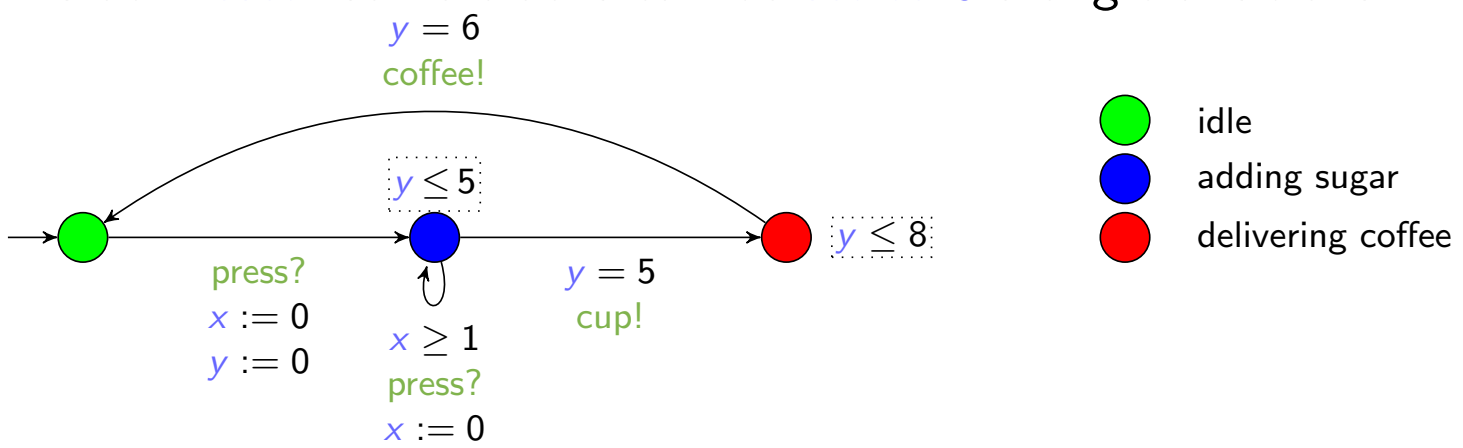
14 September 2022
FORMATS 2022, Warsaw, Poland

Supported by the ANR-NRF French-Singaporean research program ProMiS (ANR-19-CE25-0015) and CNRS-INS2I project TrAVAIL.

Timed Automaton (TA)

- Finite state automaton (sets of locations and actions) augmented with
  - a set X of clocks [AD94]
    - Real-valued variables evolving linearly at the same rate
    - Can be compared to integer constants in invariants and guards

- Features
  - Location invariant: property to be verified to stay at a location
  - Transition guard: property to be verified to enable a transition
  - Clock reset: some clocks can be set to 0 along transitions



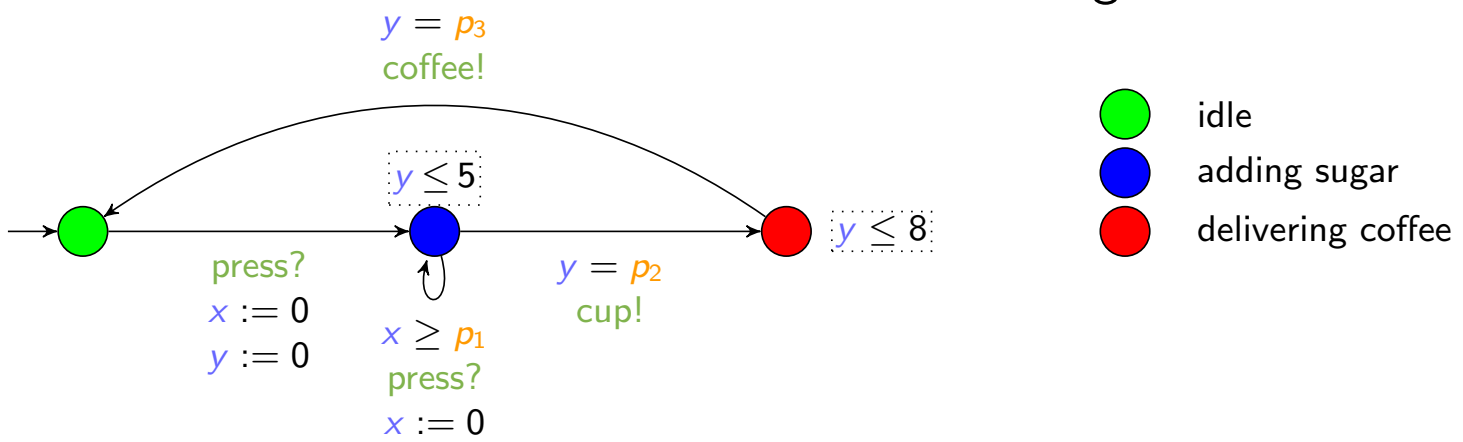
[AD94] Rajeev Alur and David L. Dill. "A theory of timed automata". In: *Theoretical Computer Science* 126.2 (Apr. 1994), pp. 183–235. ISSN: 0304-3975. DOI: 10.1016/0304-3975(94)90010-8

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. "Parametric real-time reasoning". In: *STOC* (May 16–18, 1993). Ed. by S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal. San Diego, California, United States: ACM, 1993, pp. 592–601. DOI: 10.1145/167088.167242

Parametric Timed Automaton (PTA)

- Finite state automaton (sets of locations and actions) augmented with
  - a set X of clocks [AD94]
    - Real-valued variables evolving linearly at the same rate
    - Can be compared to integer constants in invariants and guards
  - a set P of parameters (unknown constants) [AHV93]

- Features
  - Location invariant: property to be verified to stay at a location
  - Transition guard: property to be verified to enable a transition
  - Clock reset: some clocks can be set to 0 along transitions



[AD94] Rajeev Alur and David L. Dill. "A theory of timed automata". In: *Theoretical Computer Science* 126.2 (Apr. 1994), pp. 183–235. ISSN: 0304-3975. DOI: 10.1016/0304-3975(94)90010-8

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. "Parametric real-time reasoning". In: *STOC* (May 16–18, 1993). Ed. by S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal. San Diego, California, United States: ACM, 1993, pp. 592–601. DOI: 10.1145/167088.167242

Parametric Zone Graph (PZG)

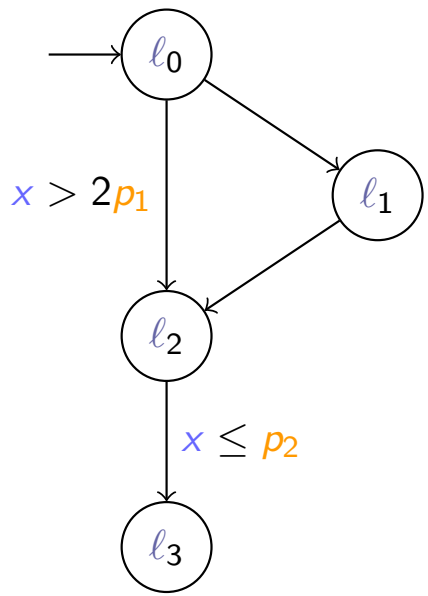
- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters

---

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters

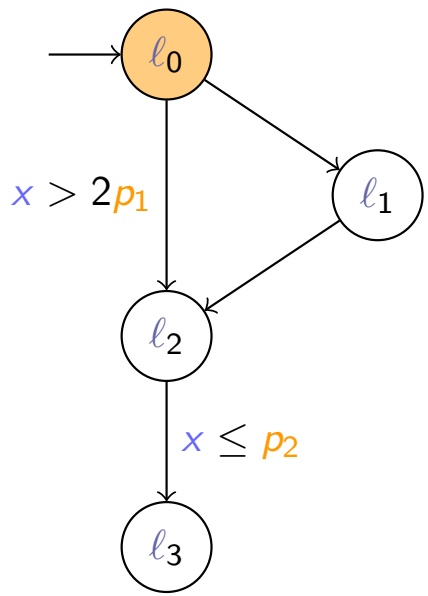


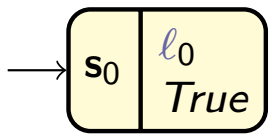
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



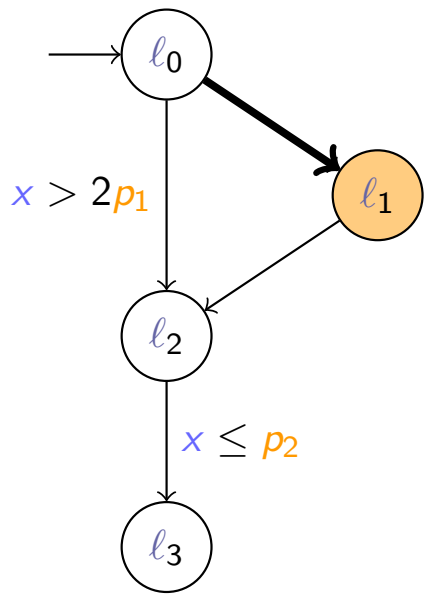


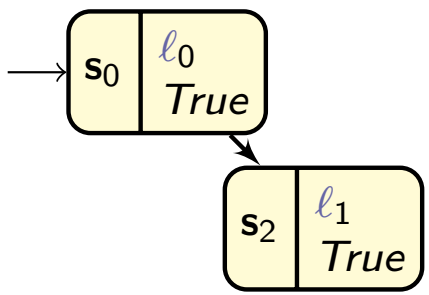
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



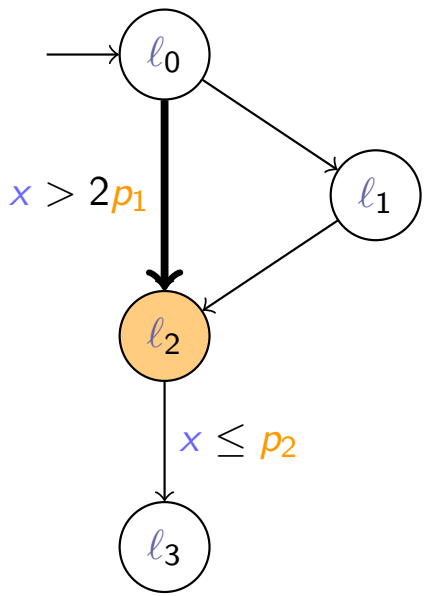


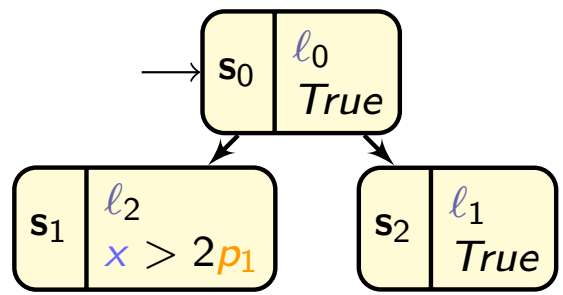
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



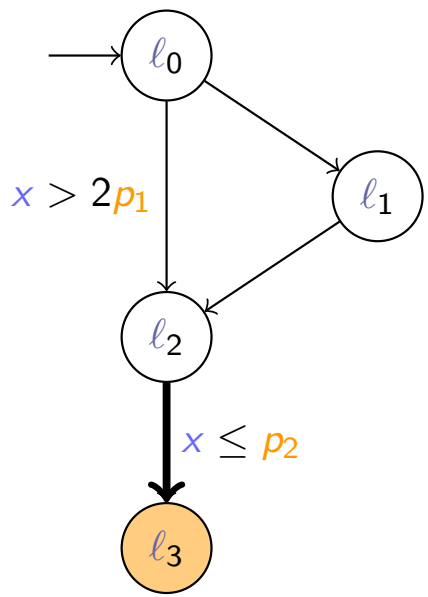


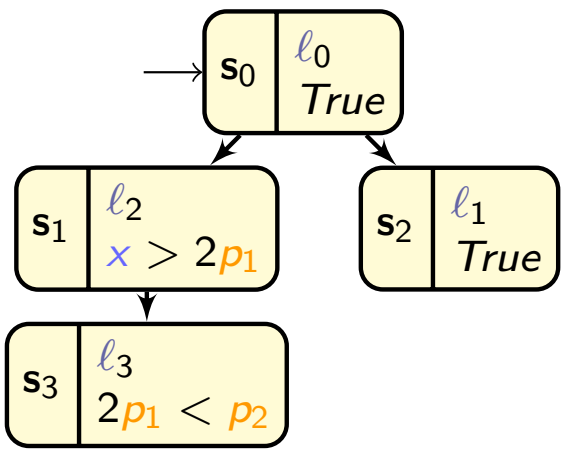
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



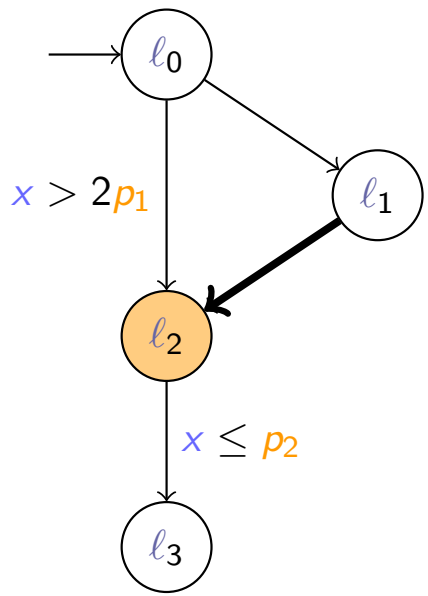


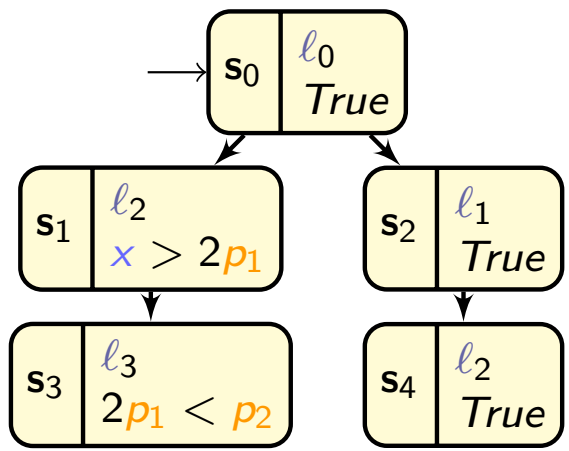
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



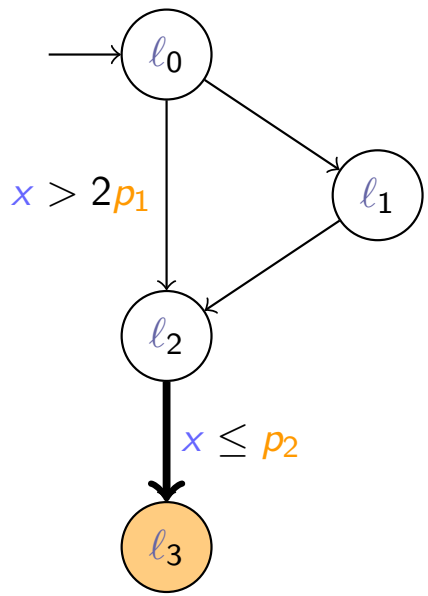


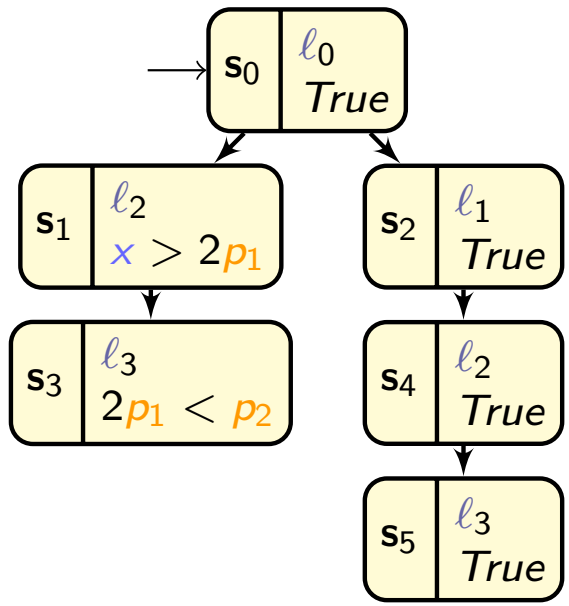
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



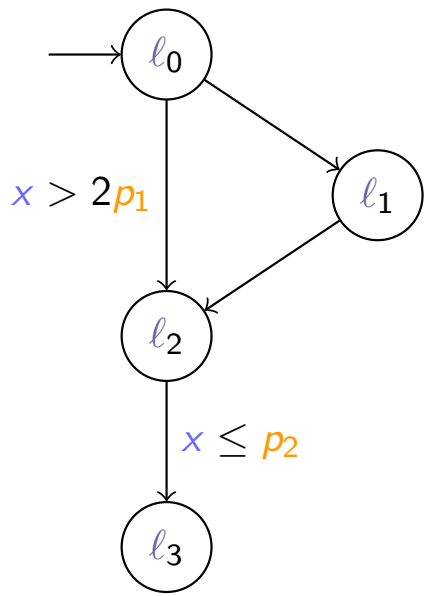


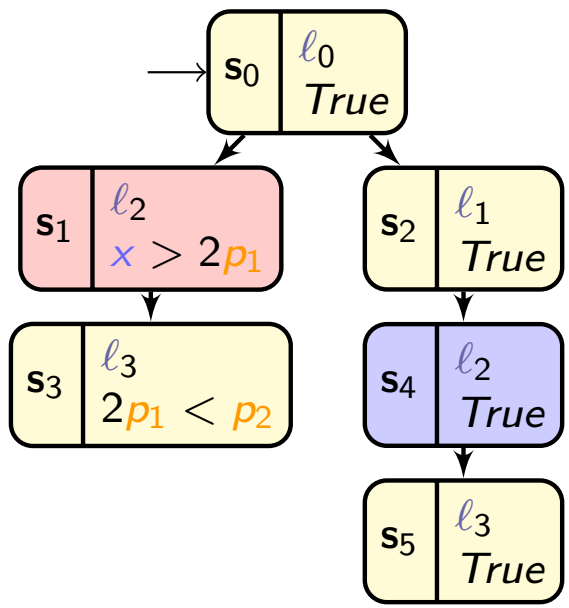
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters



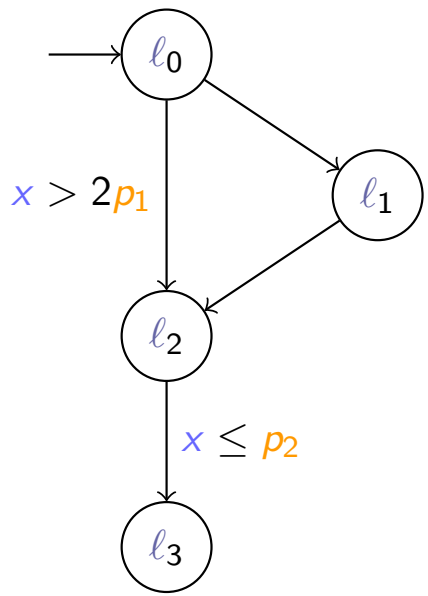


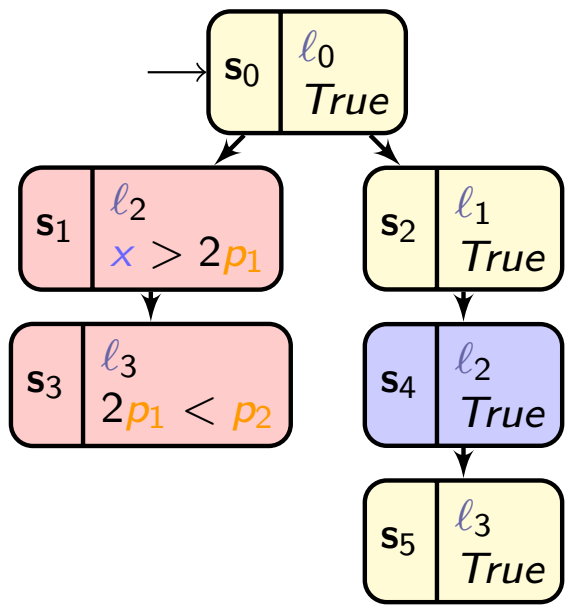
[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Parametric Zone Graph (PZG)

- Symbolic state: a pair with a location and an attached parametric zone (constraint)
- Parametric zone: a set of valuations defined by conjunctions of constraints on clocks and parameters





[HT15]

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9

Merging states

Definition

Two states (●, $\mathbf{C}_1$) and (●, $\mathbf{C}_2$) are mergeable if:

- ● = ●
- $\mathbf{C}_1 \cup \mathbf{C}_2$ is convex

Their merging is defined by (●, $\mathbf{C}_1 \cup \mathbf{C}_2$)

[Dav05] Alexandre David. "Merging DBMs Efficiently". In: *NWPT* (Oct. 19–21, 2005). DIKU, University of Copenhagen, 2005, pp. 54–56

[AFS13] Étienne André, Laurent Fribourg, and Romain Soulat. "Merge and Conquer: State Merging in Parametric Timed Automata". In: *ATVA* (Oct. 15–18, 2013). Ed. by Dang-Van Hung and Mizuhito Ogawa. Vol. 8172. LNCS. Ha Noi, Viet Nam: Springer, Oct. 2013, pp. 381–396. DOI: 10.1007/978-3-319-02444-8_27

Merging states

Definition

Two states $(\bullet, \mathbf{C}_1)$ and $(\bullet, \mathbf{C}_2)$ are mergeable if:

- $\bullet = \bullet$
- $\mathbf{C}_1 \cup \mathbf{C}_2$ is convex

Their merging is defined by $(\bullet, \mathbf{C}_1 \cup \mathbf{C}_2)$

State merging techniques were introduced:

- in TA [Dav05]
- in PTA for Inverse Method [AFS13]

[Dav05] Alexandre David. "Merging DBMs Efficiently". In: *NWPT* (Oct. 19–21, 2005). DIKU, University of Copenhagen, 2005, pp. 54–56

[AFS13] Étienne André, Laurent Fribourg, and Romain Soulat. "Merge and Conquer: State Merging in Parametric Timed Automata". In: *ATVA* (Oct. 15–18, 2013). Ed. by Dang-Van Hung and Mizuhito Ogawa. Vol. 8172. LNCS. Ha Noi, Viet Nam: Springer, Oct. 2013, pp. 381–396. DOI: 10.1007/978-3-319-02444-8_27

Merging states

Definition

Two states $(\bullet, \mathbf{C}_1)$ and $(\bullet, \mathbf{C}_2)$ are mergeable if:

- $\bullet = \bullet$
- $\mathbf{C}_1 \cup \mathbf{C}_2$ is convex

Their merging is defined by $(\bullet, \mathbf{C}_1 \cup \mathbf{C}_2)$

State merging techniques were introduced:

- in TA [Dav05]
- in PTA for Inverse Method [AFS13]

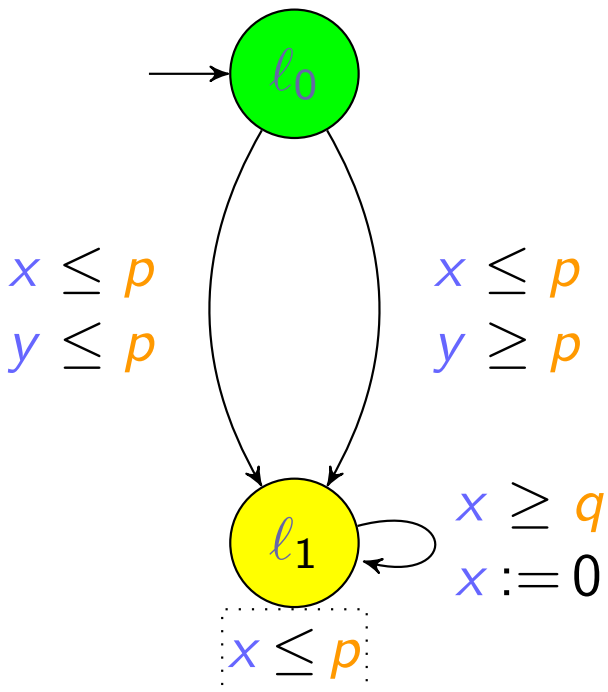
Merging preserves reachability

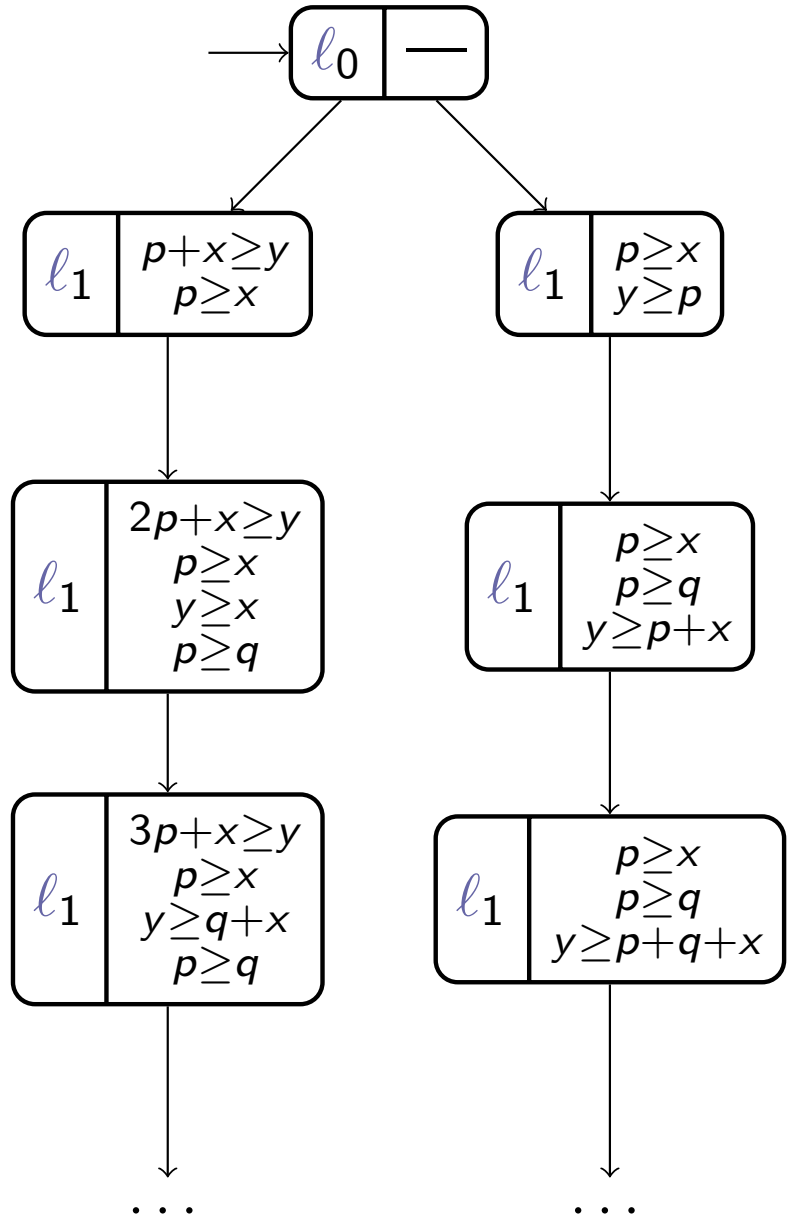
[Dav05] Alexandre David. "Merging DBMs Efficiently". In: *NWPT* (Oct. 19–21, 2005). DIKU, University of Copenhagen, 2005, pp. 54–56

[AFS13] Étienne André, Laurent Fribourg, and Romain Soulat. "Merge and Conquer: State Merging in Parametric Timed Automata". In: *ATVA* (Oct. 15–18, 2013). Ed. by Dang-Van Hung and Mizuhito Ogawa. Vol. 8172. LNCS. Ha Noi, Viet Nam: Springer, Oct. 2013, pp. 381–396. DOI: 10.1007/978-3-319-02444-8_27

Merging can make difference for termination!

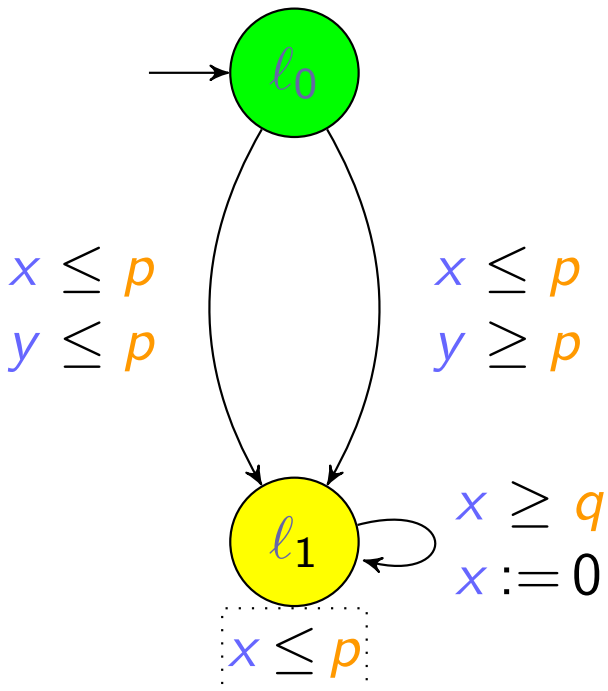
PZG without any heuristic

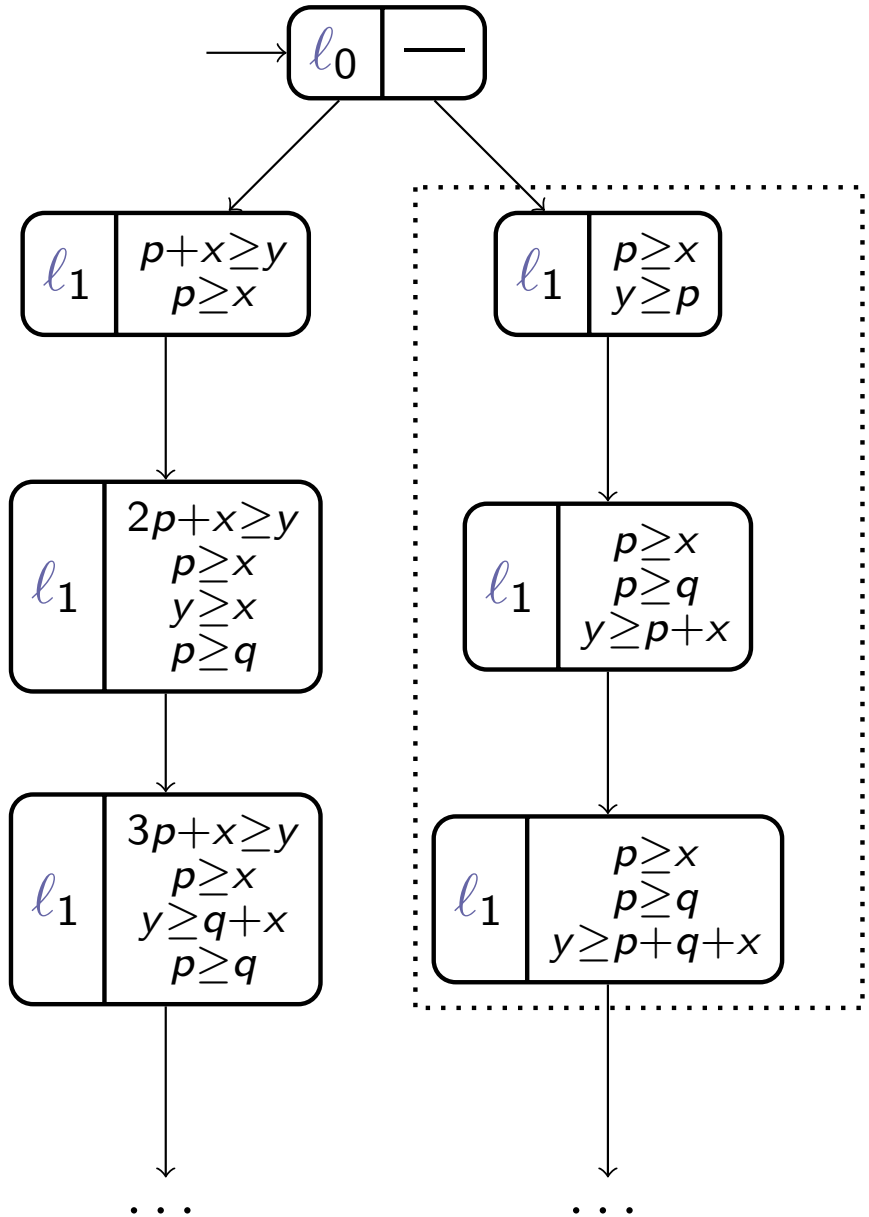




Merging can make difference for termination!

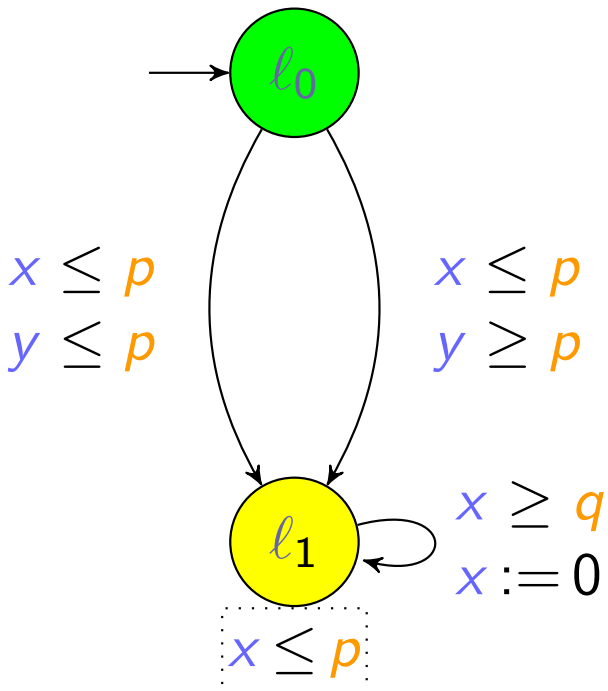
PZG with inclusion

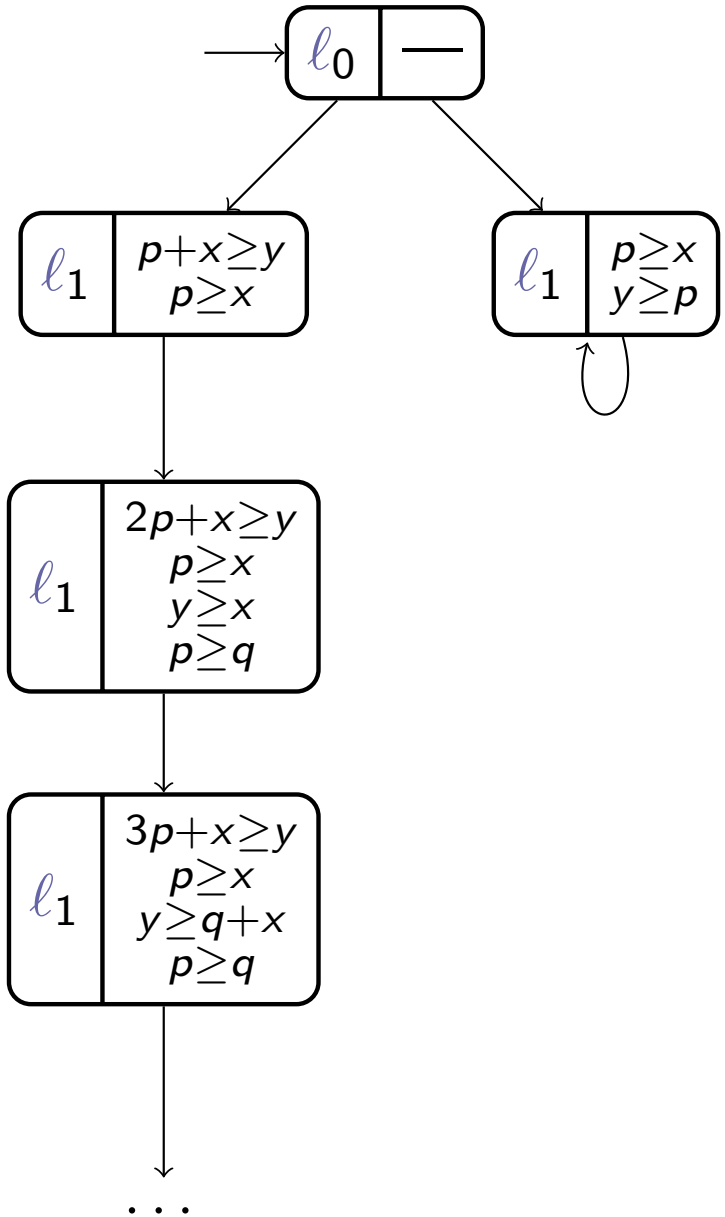




Merging can make difference for termination!

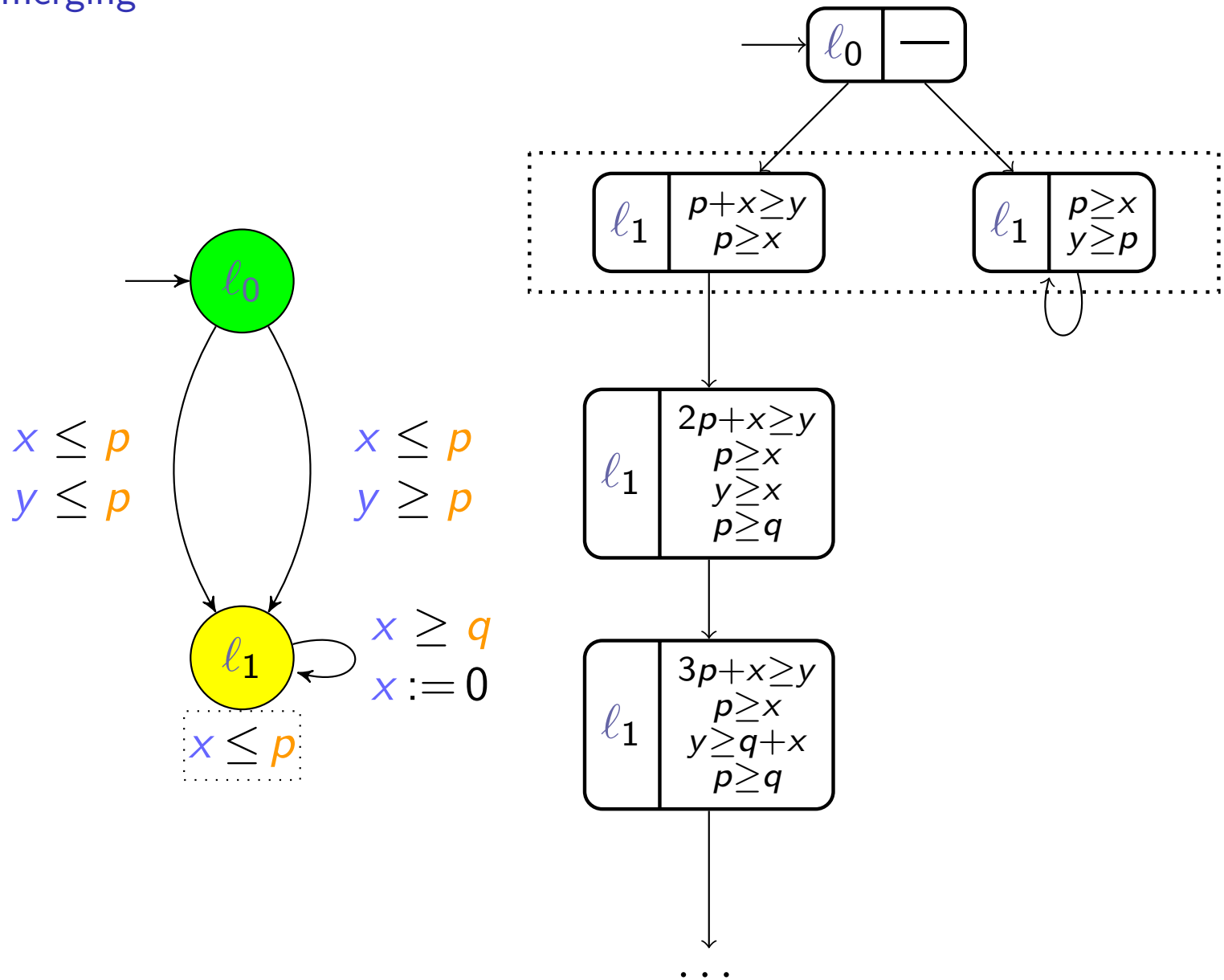
PZG with inclusion





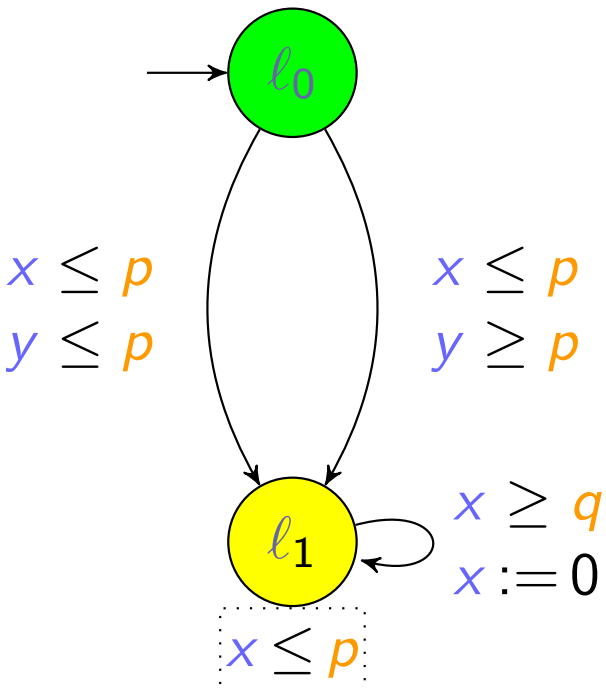
Merging can make difference for termination!

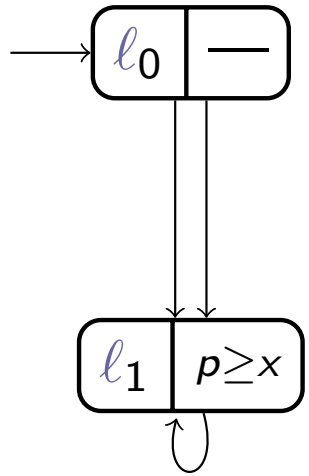
PZG with merging



Merging can make difference for termination!

PZG with merging





The construction of the PZG

Algorithm 1: BFS by layer layerBFS($\mathcal{A}$)

1 $\mathbf{Visited} \leftarrow \{\mathbf{s}_0\}$
2 $\mathbf{Queue} \leftarrow \{\mathbf{s}_0\}$
3 $\Rightarrow \leftarrow \emptyset$
4 **while** $\mathbf{Queue} \neq \emptyset$ **do**
5 $\mathbf{Q}_{new} \leftarrow \emptyset$
6 **foreach** $\mathbf{s} \in \mathbf{Queue}$ **do**
7 **foreach** $(e, \mathbf{s}') \in \mathrm{SuccE}(\mathbf{s})$ **do**
8 $\mathbf{Q}_{new} \leftarrow \mathbf{Q}_{new} \cup (\{\mathbf{s}'\} \setminus \mathbf{Visited})$
9 $\Rightarrow \leftarrow \Rightarrow \cup \{(\mathbf{s}, e, \mathbf{s}')\}$
10 $\mathbf{Visited}, \mathbf{Queue} \leftarrow \mathit{mergeSets}(\mathbf{PZG}, \mathbf{Visited}, \mathbf{Q}_{new})$

Heuristics for merging

What to merge with what? Queue, Visited, Ordered

Restart after merge?

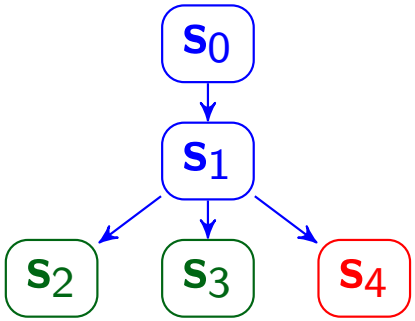
When to update the state space?

- After each merge
- After exploring the candidates list
- After exploring a BFS level

How to update the state space?

- Reconstruction of the state-space
- *In situ*

Illustration of the merging options



- visited
- in the queue
- being processed
- after merge

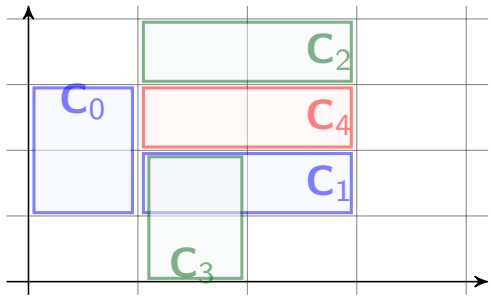
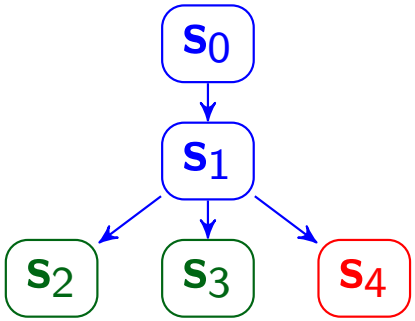
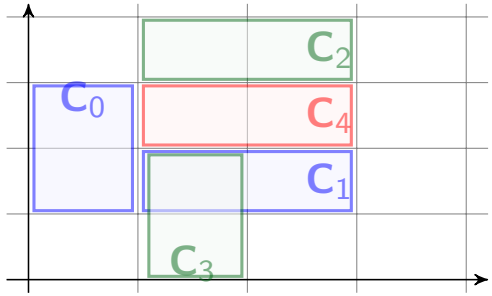


Illustration of the merging options



- visited
- in the queue
- being processed
- after merge



Merge with Queue

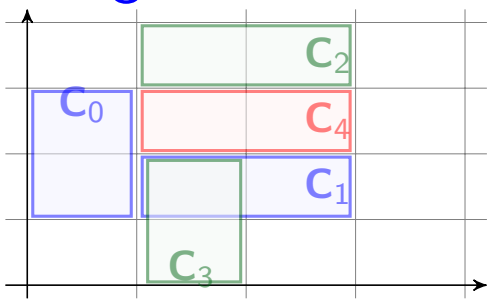
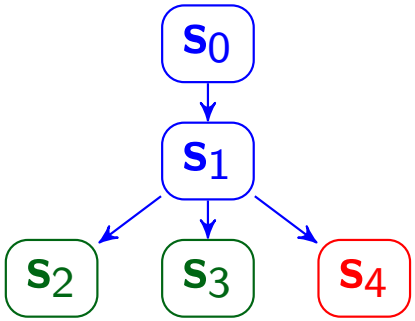
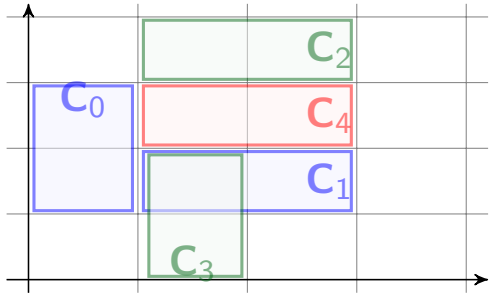


Illustration of the merging options



- visited
- in the queue
- being processed
- after merge



Merge with Queue

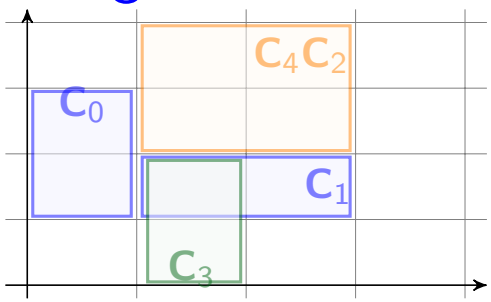
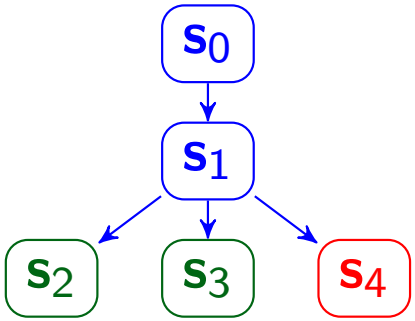
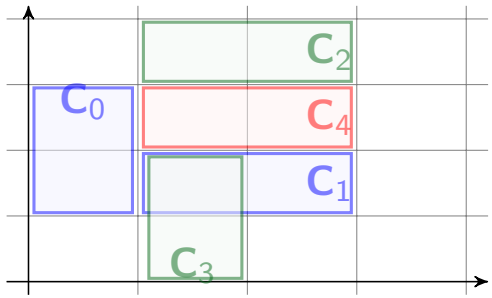


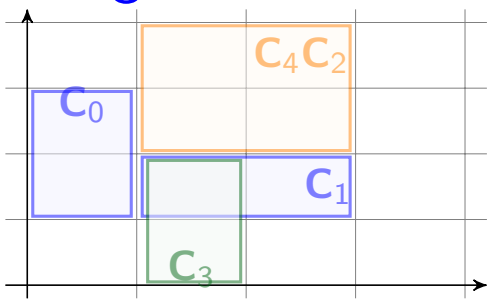
Illustration of the merging options



visited
in the queue
being processed
after merge



Merge with Queue



Merge with Visited

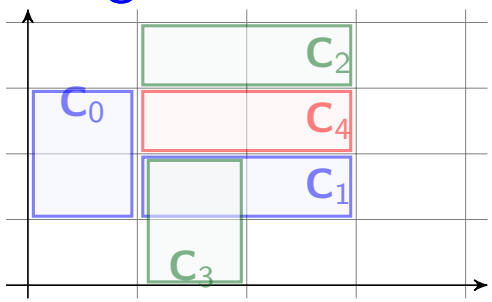
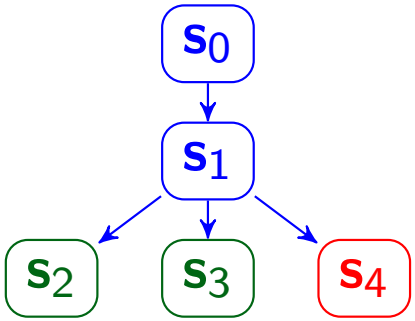
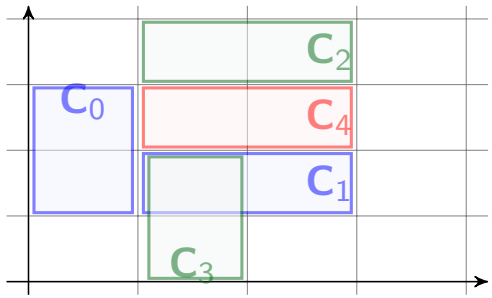


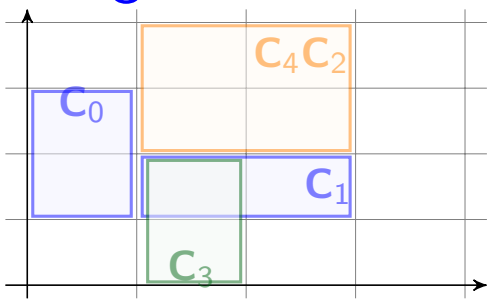
Illustration of the merging options



- visited
- in the queue
- being processed
- after merge



Merge with Queue



Merge with Visited

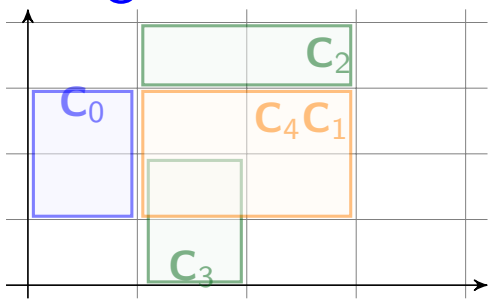
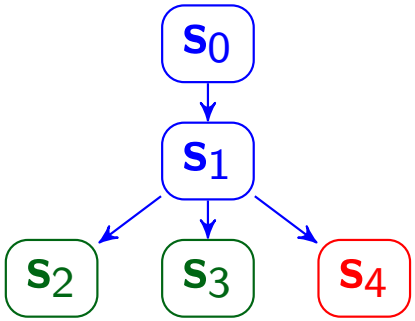
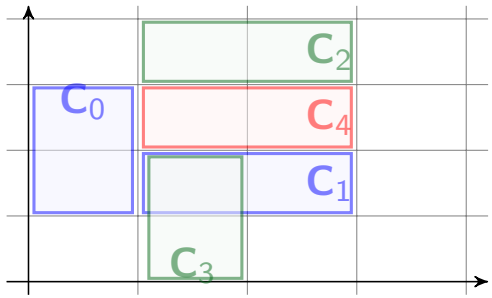


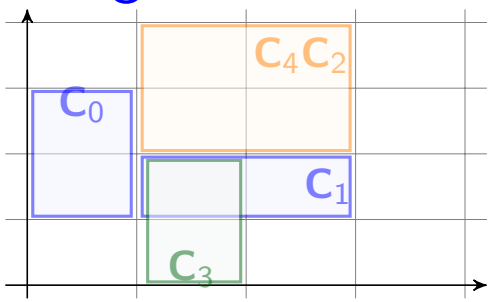
Illustration of the merging options



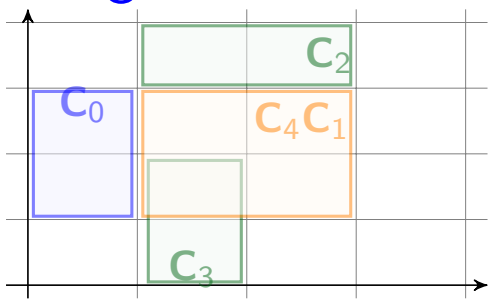
visited
in the queue
being processed
after merge



Merge with Queue



Merge with Visited



and Restart

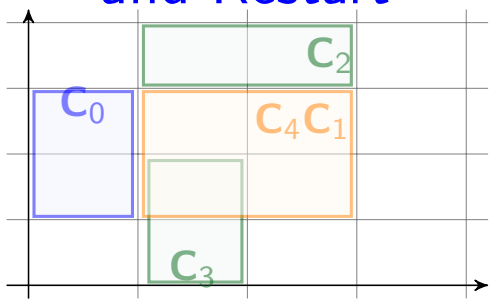
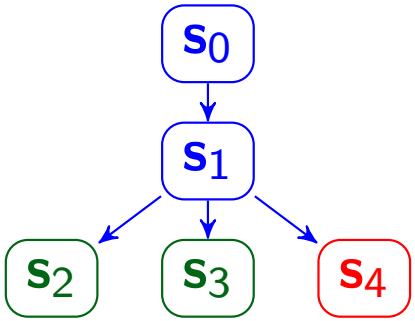
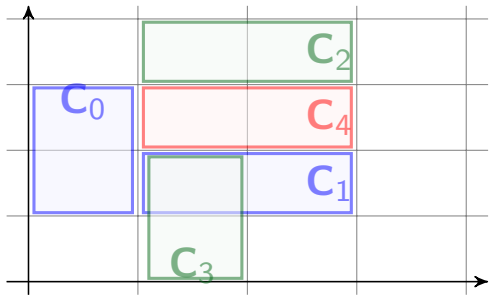


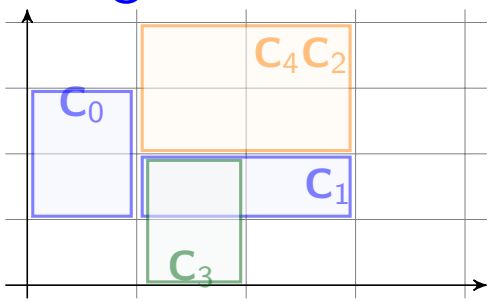
Illustration of the merging options



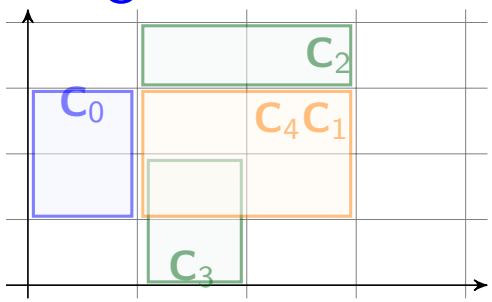
visited
in the queue
being processed
after merge



Merge with Queue



Merge with Visited



and Restart

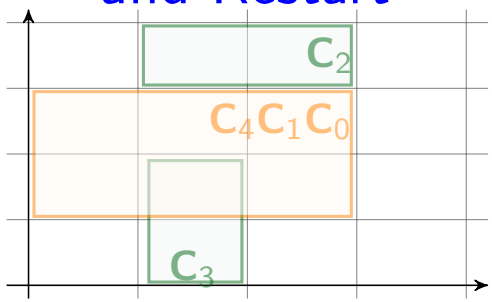
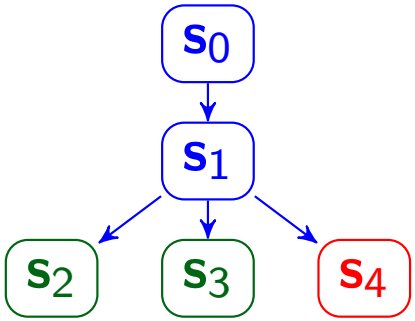
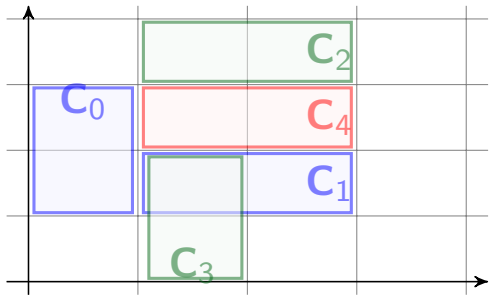


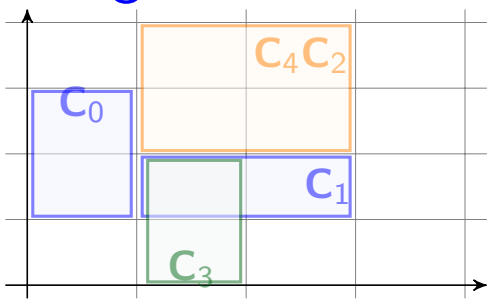
Illustration of the merging options



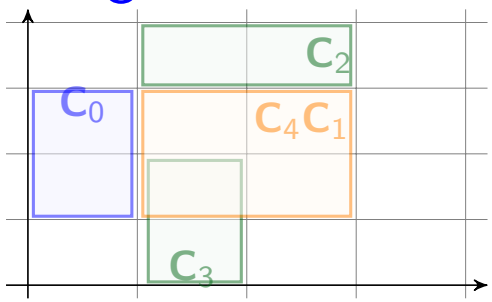
visited
in the queue
being processed
after merge



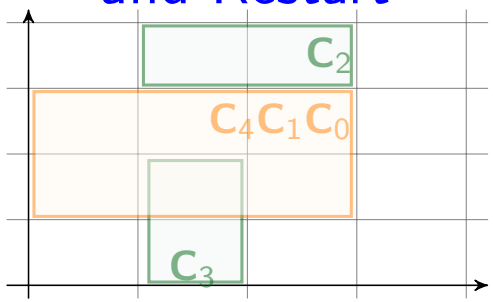
Merge with Queue



Merge with Visited



and Restart



Queue ; Visited

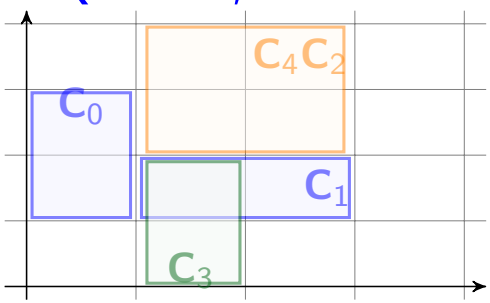
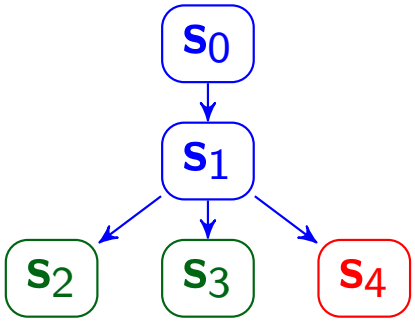
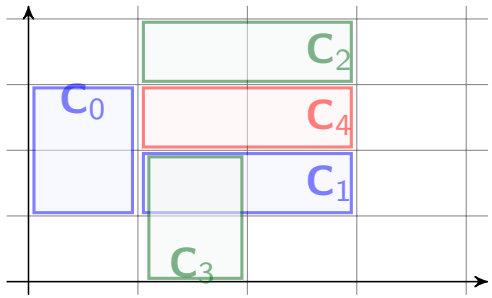


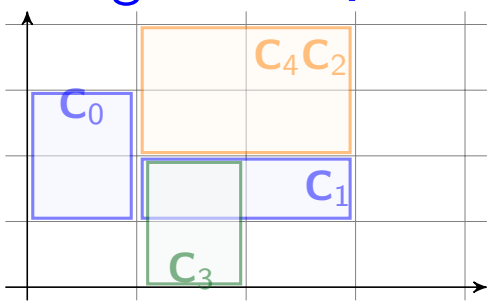
Illustration of the merging options



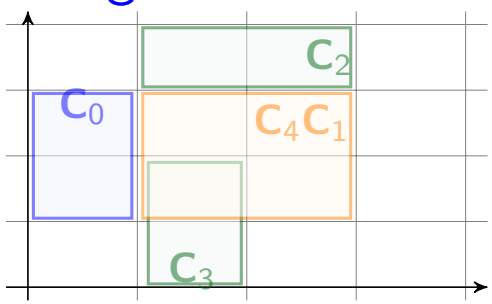
visited
in the queue
being processed
after merge



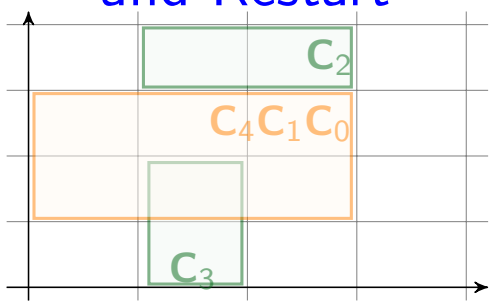
Merge with Queue



Merge with Visited



and Restart



Queue ; Visited

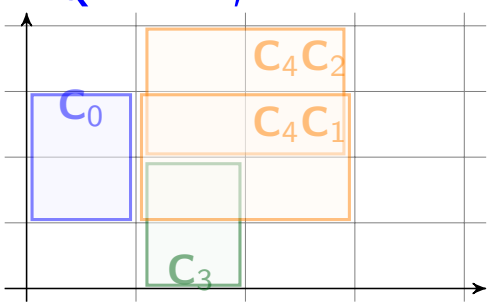
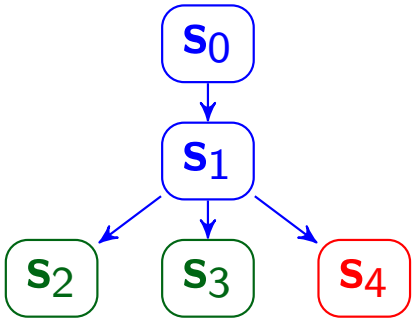
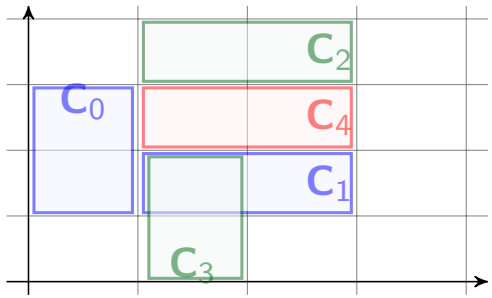


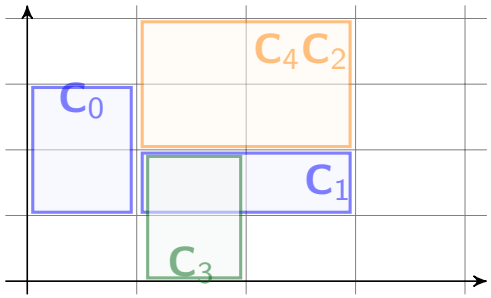
Illustration of the merging options



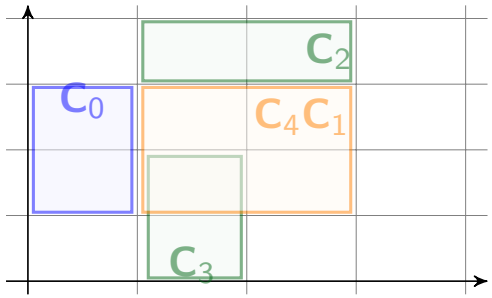
visited
in the queue
being processed
after merge



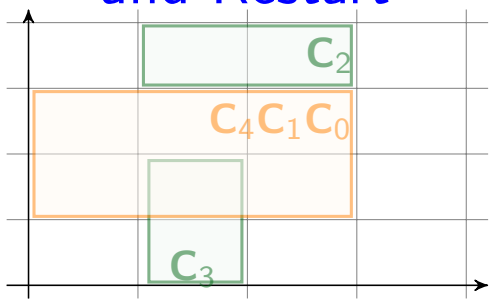
Merge with Queue



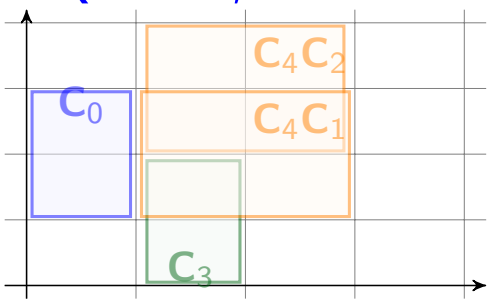
Merge with Visited



and Restart



Queue ; Visited



Update after Merge

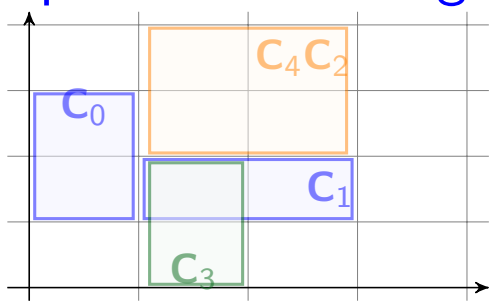
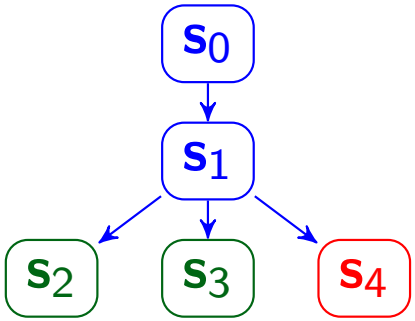
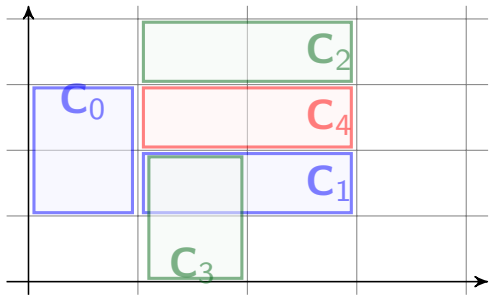


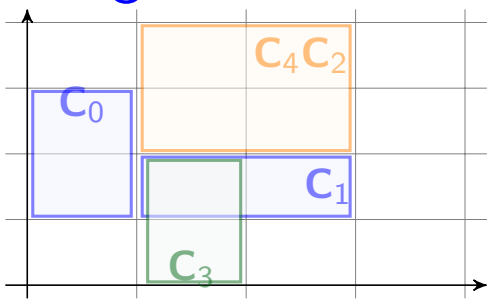
Illustration of the merging options



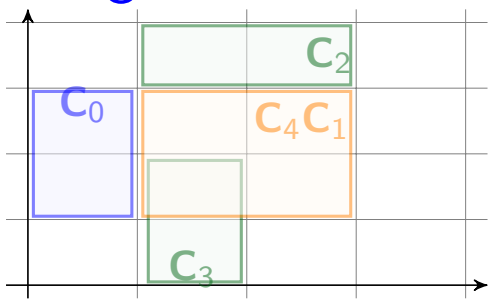
visited
in the queue
being processed
after merge



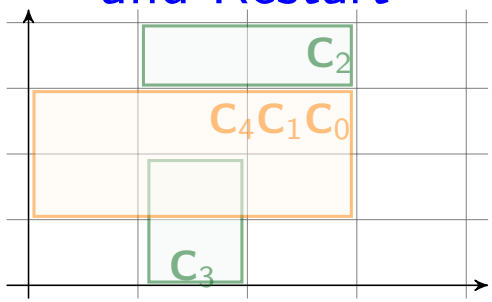
Merge with Queue



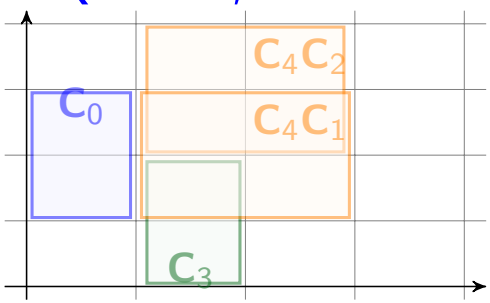
Merge with Visited



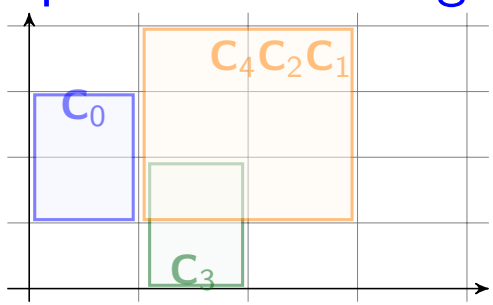
and Restart



Queue ; Visited



Update after Merge



Experiments

- Comparison of all the combinations of heuristics
- Use of the IMITATOR library, restricted to reachability-based properties [AMP21]:
  - 124 executions (model, reachability property)
  - 42 executions perform at least one merge

[AMP21] Étienne André, Dylan Marinho, and Jaco van de Pol. "A Benchmarks Library for Extended Timed Automata". In: *TAP* (June 21–25, 2021). Ed. by Frédéric Loulergue and Franz Wotawa. Vol. 12740. LNCS. virtual: Springer, 2021, pp. 39–50. DOI: 10.1007/978-3-030-79379-1_3

Results

		Nomerge	M2.12	RVMr	OQM
Time	# wins	24	20	22	**42**
	Avg (s)	10.0	5.47	4.56	**3.77**
	Avg (merge) (s)	18.8	7.83	5.57	**3.63**
	Avg (no merge) (s)	3.83	**3.82**	3.85	3.88
	Median (s)	1.39	1.2	1.14	**1.12**
	Norm. avg	1.0	0.91	0.91	**0.87**
	Norm. avg (merge)	1.0	0.75	0.74	**0.64**
	Norm. avg (no merge)	**1.0**	1.02	1.03	1.03
States	# wins	0	19	**37**	16
	Avg	11443.08	11096.54	**11064.37**	11120.79
	Avg (merge)	1512.02	670.43	**592.31**	729.33
	Median	2389.5	703.5	**604.5**	905.0
	Norm. avg	1.0	0.86	**0.84**	0.88

Conclusion and Perspectives

- investigated the merge operation for reachability analysis in PTAs
- proposed several heuristics
- shown they are sound
- extensive experiments to compare these approaches

Conclusion and Perspectives

- investigated the merge operation for reachability analysis in PTAs
- proposed several heuristics
- shown they are sound
- extensive experiments to compare these approaches

- tackle the handling of merged states:
  - pruning away
  - separate collection of potential mergers
- merge more than 2 states
- canonical merge representatives
- compatibility of merging and liveness properties

References I

[AD94] Rajeev Alur and David L. Dill. "A theory of timed automata". In: *Theoretical Computer Science* 126.2 (Apr. 1994), pp. 183–235. ISSN: 0304-3975. DOI: 10.1016/0304-3975(94)90010-8.

[AFS13] Étienne André, Laurent Fribourg, and Romain Soulat. "Merge and Conquer: State Merging in Parametric Timed Automata". In: *ATVA* (Oct. 15–18, 2013). Ed. by Dang-Van Hung and Mizuhito Ogawa. Vol. 8172. LNCS. Ha Noi, Viet Nam: Springer, Oct. 2013, pp. 381–396. DOI: 10.1007/978-3-319-02444-8_27.

References II

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. "Parametric real-time reasoning". In: *STOC* (May 16–18, 1993). Ed. by S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal. San Diego, California, United States: ACM, 1993, pp. 592–601. DOI: 10.1145/167088.167242.

[AMP21] Étienne André, Dylan Marinho, and Jaco van de Pol. "A Benchmarks Library for Extended Timed Automata". In: *TAP* (June 21–25, 2021). Ed. by Frédéric Loulergue and Franz Wotawa. Vol. 12740. LNCS. virtual: Springer, 2021, pp. 39–50. DOI: 10.1007/978-3-030-79379-1_3.

[Dav05] Alexandre David. "Merging DBMs Efficiently". In: *NWPT* (Oct. 19–21, 2005). DIKU, University of Copenhagen, 2005, pp. 54–56.

References III

[HT15] Frédéric Herbreteau and Thanh-Tung Tran. "Improving Search Order for Reachability Testing in Timed Automata". In: *FORMATS* (Sept. 2–4, 2015). Ed. by Sriram Sankaranarayanan and Enrico Vicario. Vol. 9268. LNCS. Madrid, Spain: Springer, 2015, pp. 124–139. DOI: 10.1007/978-3-319-22975-1_9.