max planck institut
informatik

The Bernays–Schönfinkel–Ramsey Fragment with Bounded Difference Constraints over the Reals is Decidable

Marco Voigt

SAARLAND UNIVERSITY
SAARBRÜCKEN GRADUATE SCHOOL OF COMPUTER SCIENCE

September 29, 2017

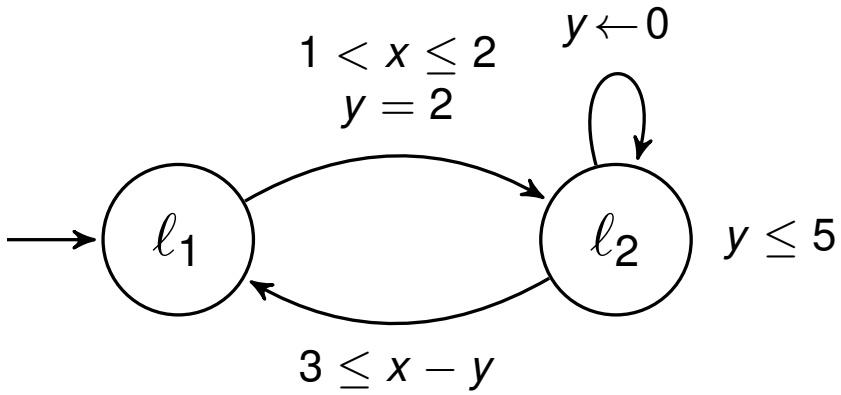
SIC Saarland Informatics Campus

International Max Planck Research School
for Computer Science

Motivation

For some formalization tasks,
we would like to have

- linear arithmetic over $\mathbb{R}$,
- uninterpreted predicates,
- universal quantification.



$\rightsquigarrow$ Convenient and powerful modeling language

$\rightsquigarrow$ Too powerful, indeed: Satisfiability is undecidable.

$\rightsquigarrow$ Remains undecidable, even when adding
only unary uninterpreted predicates.

$\rightsquigarrow$ We have to restrict the arithmetic part!

The Plan

1. Present the
   Bernays–Schönfinkel–Ramsey Fragment
   with Bounded Difference Constraints — BSR(BD)

2. Exemplary application:
   reachability for timed automata

Bernays–Schönfinkel–Ramsey with Bounded Difference Constraints — BSR(BD)

$\exists^*\forall^*$ quantifier prefix
$+$ uninterpreted predicates
$+$ linear rational arithmetic
$+$ syntactic restrictions

$=$ BSR(BD)

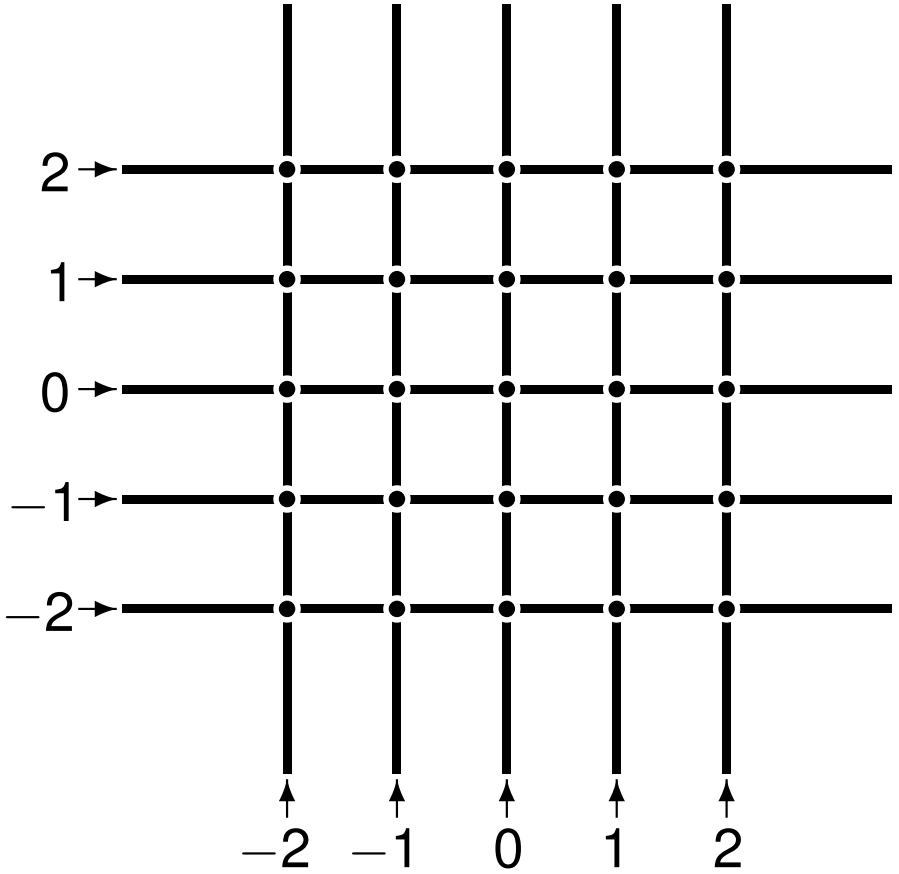
- clauses in $(\ldots) \to (\ldots)$ notation
- arithm. atoms only left of $\to$
- allowed arithm. atoms:
  - $x \triangleleft c$, $x \triangleleft y$ and
  - $x - y \triangleleft c$ conjoined with bounds $\ell \leq x, y \leq u$

where $c, \ell, u \in \mathbb{Q}$ and $\triangleleft \in \{<, \leq, =, \neq, \geq, >\}$

$$\forall xyz.\ \underbrace{x - y < \tfrac{3}{2}}_{\text{diff. constraint requires bounds}} \wedge \underbrace{-2 \leq x, y \leq 2}_{\text{diff. constraint requires bounds}} \wedge \underbrace{x < z}_{\text{no bound on } z \text{ required}} \wedge Q(x, y) \longrightarrow T(x) \vee Q(y, x)$$

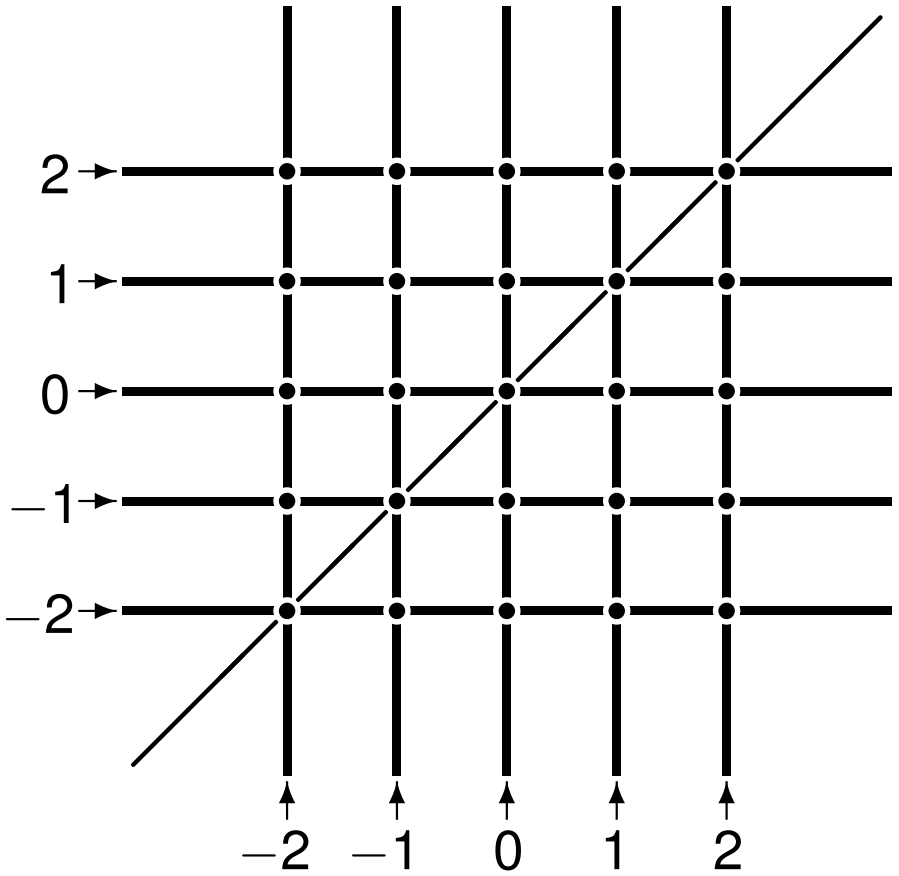
$\rightsquigarrow$ Bounds are necessary for decidability.
$\rightsquigarrow$ For convenience, we only consider integer bounds here.

BSR(BD): Distinguishable Regions of $\mathbb{R}^2$



Constraints $x \triangleleft c$
with $c \in \{-2, -1, 0, 1, 2\}$
can distinguish
the grid regions.

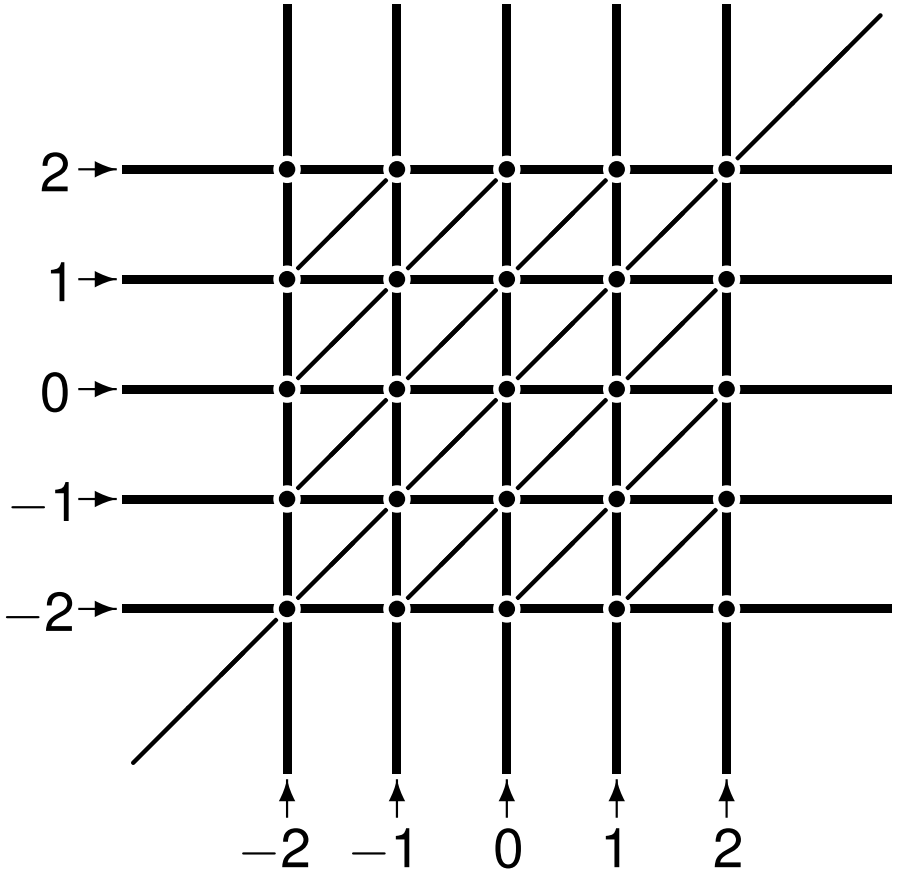
BSR(BD): Distinguishable Regions of $\mathbb{R}^2$



Constraints $x \triangleleft c$ with $c \in \{-2, -1, 0, 1, 2\}$ can distinguish the grid regions.

Constraints $x \triangleleft y$ can distinguish the simple diagonal.

BSR(BD): Distinguishable Regions of $\mathbb{R}^2$

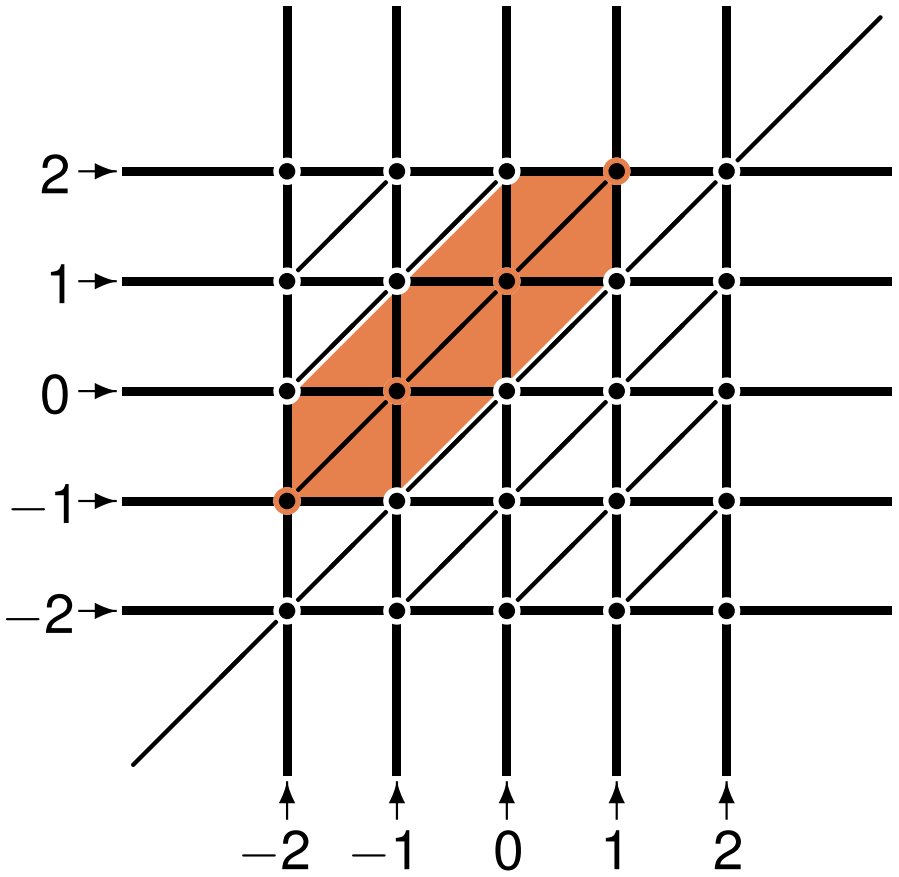


Constraints $x \triangleleft c$
with $c \in \{-2, -1, 0, 1, 2\}$
can distinguish
the grid regions.

Constraints $x \triangleleft y$
can distinguish
the simple diagonal.

Difference constraints
$x - y \triangleleft c$
with bounds
$-2 \leq x, y \leq 2$
can distinguish
more triangles.

BSR(BD): Distinguishable Regions of $\mathbb{R}^2$



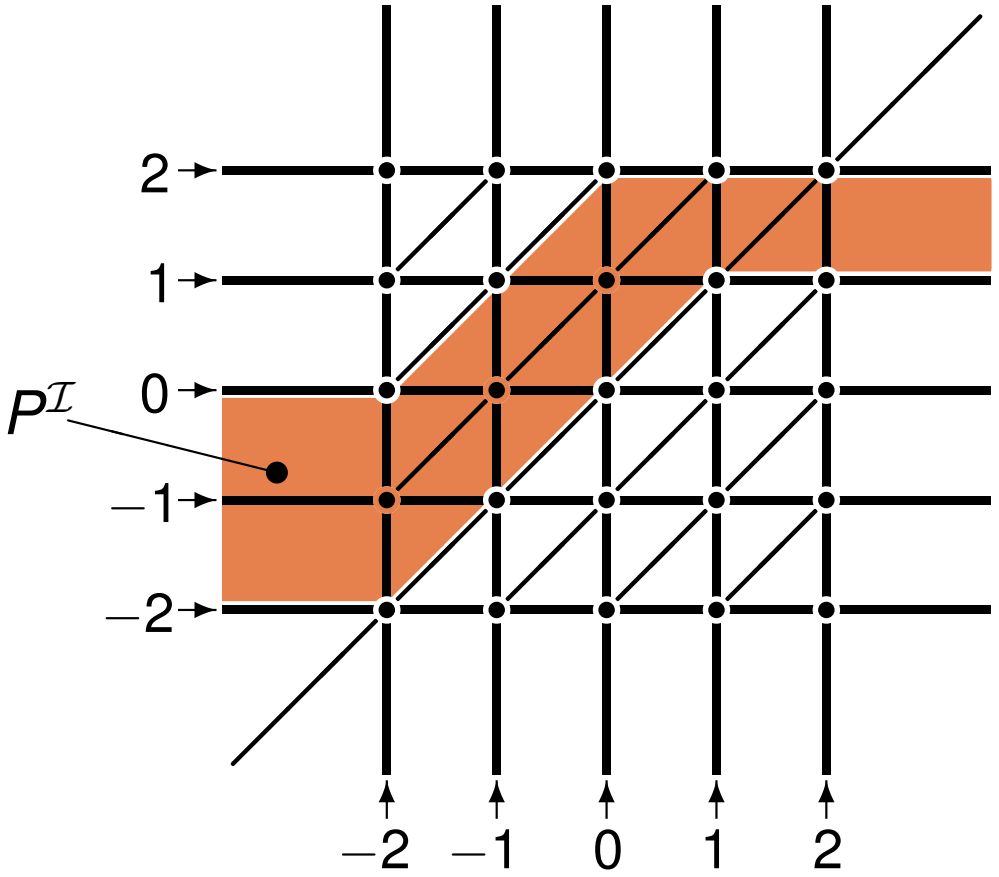
$$-2 < x - y < 0 \quad \wedge \quad -2 \leq x, y \leq 2 \quad \wedge \quad x \leq 1 \quad \wedge \quad -1 \leq y$$

Constraints $x \triangleleft c$ with $c \in \{-2, -1, 0, 1, 2\}$ can distinguish the grid regions.

Constraints $x \triangleleft y$ can distinguish the simple diagonal.

Difference constraints $x - y \triangleleft c$ with bounds $-2 \leq x, y \leq 2$ can distinguish more triangles.

BSR(BD): Interpretation of Predicates $P^{\mathcal{I}} \subseteq \mathbb{R}^2$



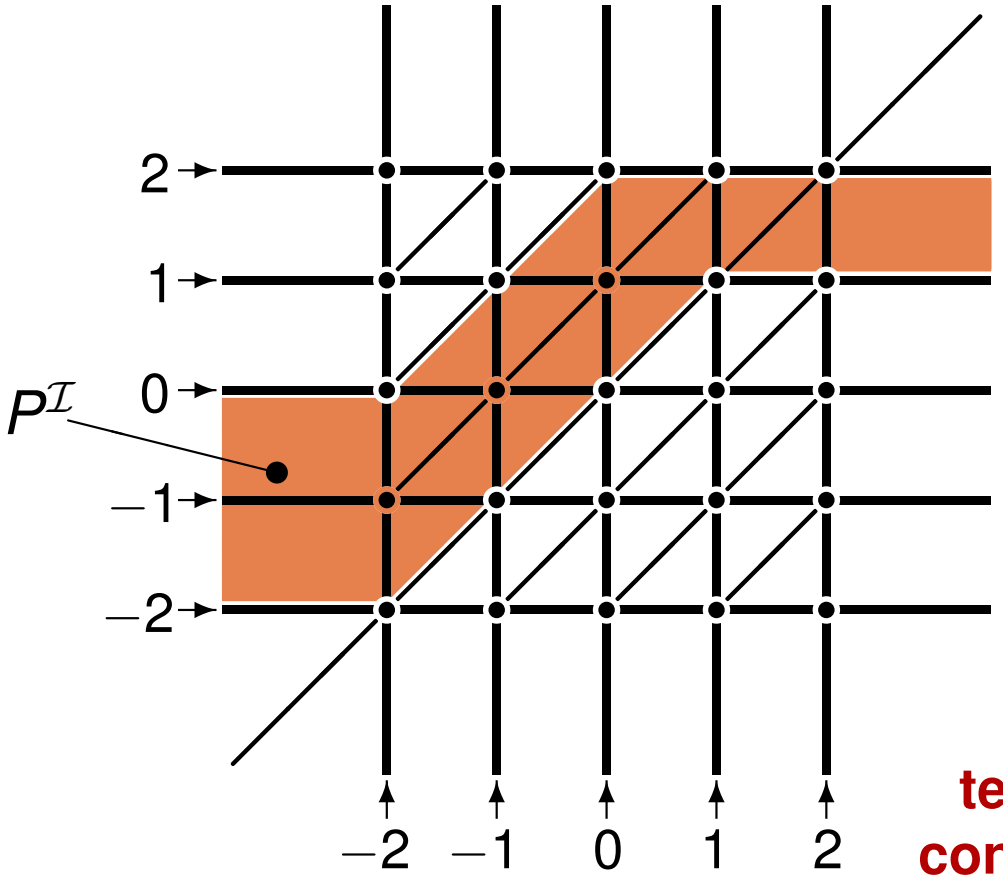
$$
\begin{array}{rcrcl}
-2 < x - y < 0 & \wedge & -2 \leq x, y \leq 2 & \rightarrow & P(x, y) \\
x \leq -2 & \wedge & -2 < y < 0 & \rightarrow & P(x, y) \\
1 \leq x & \wedge & 1 < y < 2 & \rightarrow & P(x, y)
\end{array}
$$

Key insight:

Predicates needn't distinguish what arithmetic constraints can't distinguish.

$\rightsquigarrow$ Only a finite number of interpretations need to be checked to decide satisfiability.

BSR(BD): Interpretation of Predicates $P^{\mathcal{I}} \subseteq \mathbb{R}^2$



Key insight:

Predicates needn't distinguish what arithmetic constraints can't distinguish.

main technical contribution

$\rightsquigarrow$ Only a finite number of interpretations need to be checked to decide satisfiability.

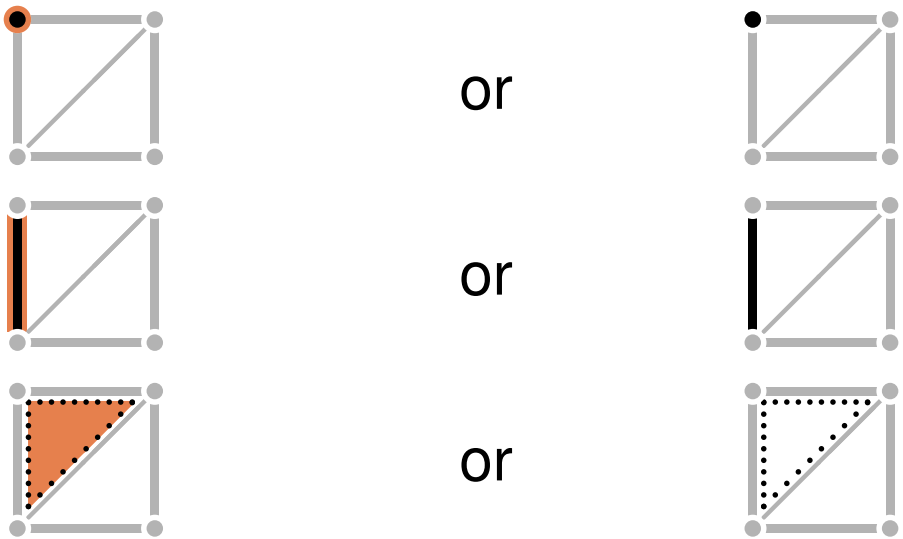
$$
\begin{array}{rcl}
-2 < x - y < 0 \ \wedge \ -2 \leq x, y \leq 2 & \rightarrow & P(x,y) \\
x \leq -2 \ \wedge \ -2 < y < 0 & \rightarrow & P(x,y) \\
1 \leq x \ \wedge \ 1 < y < 2 & \rightarrow & P(x,y)
\end{array}
$$

BSR(BD): Region-Uniform Interpretations of $P^{\mathcal{I}}$

Region-uniform interpretation $P^{\mathcal{I}} \subseteq \mathbb{R}^2$:

Every region is either

fully contained in $P^{\mathcal{I}}$ or disjoint from $P^{\mathcal{I}}$.



Key lemma: For satisfiable BSR(BD) clause sets region-uniform models always exist.

BSR(BD): Region-Uniform Interpretations of $P^{\mathcal{I}}$

Given:
- a satisfiable BSR(BD) clause set N in which the arity of predicates is $\leq m$,
- some model $\mathcal{A}$ of N.

Frank P. Ramsey

There is a sufficiently large but finite subset S of $\mathbb{R}$ that covers all regions in $\mathbb{R}^m$ and over which $\mathcal{A}$ is region-uniform.

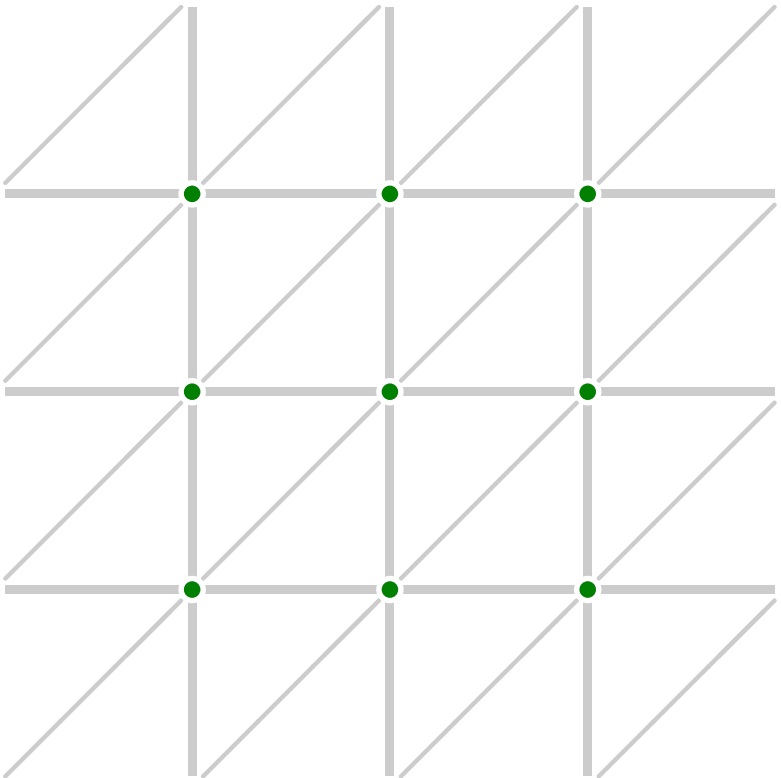
$\rightsquigarrow$ We extend $\mathcal{A}|_S$ to a model $\mathcal{B}$ of N that is region-uniform over $\mathbb{R}^m$.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

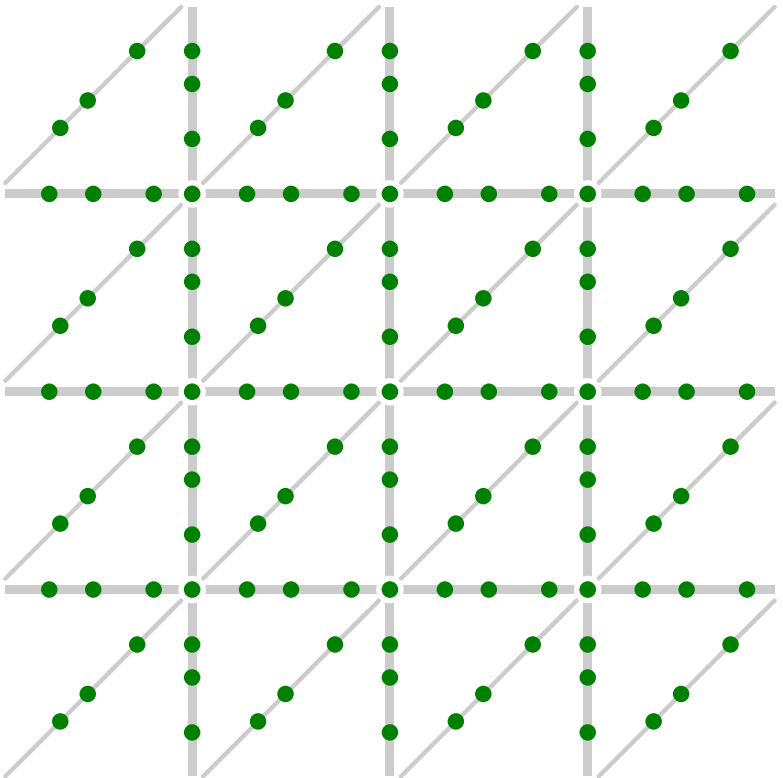
Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



$\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

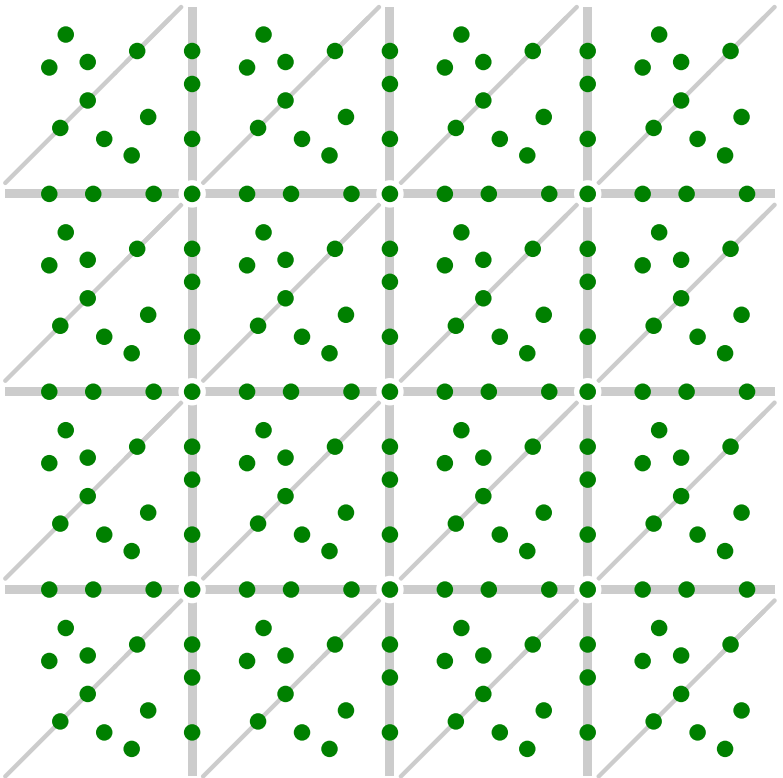
Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



$\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

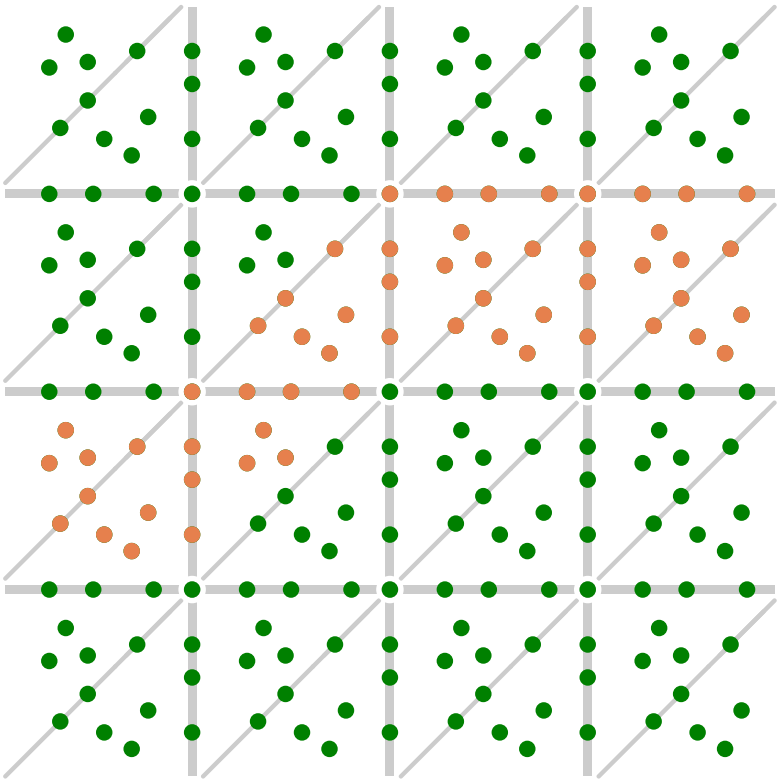
Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



$\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

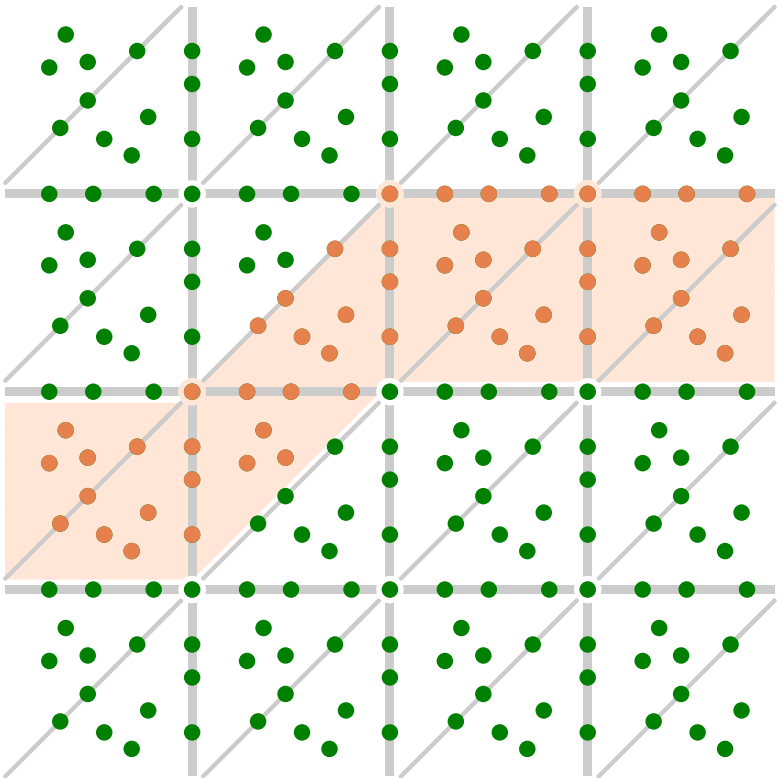
Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



- $\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.
- $\rightsquigarrow$ The regions over S^2 are interpreted uniformly by $\mathcal{A}$.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

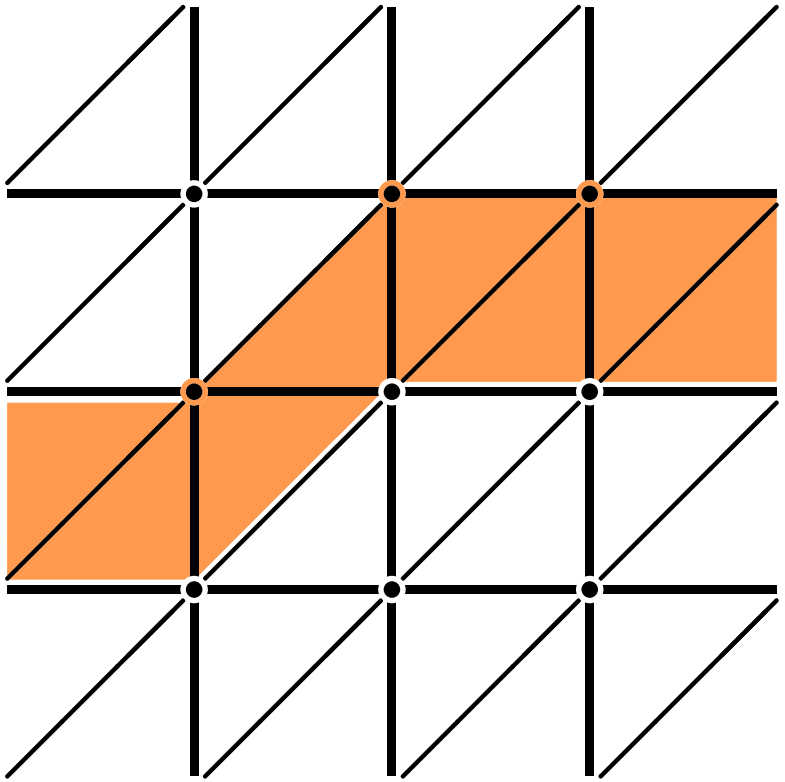
Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



- $\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.
- $\rightsquigarrow$ The regions over S^2 are interpreted uniformly by $\mathcal{A}$.
- $\rightsquigarrow$ This induces $\mathcal{B}$.

BSR(BD): Region-uniformity for a finite subset of $\mathbb{R}^2$

Every model $\mathcal{A}$ is region-uniform on some sufficiently large but finite subset $S \subseteq \mathbb{R}$.



- $\rightsquigarrow$ The finite subset $S^2 \subseteq \mathbb{R}^2$ must cover all regions.
- $\rightsquigarrow$ The regions over S^2 are interpreted uniformly by $\mathcal{A}$.
- $\rightsquigarrow$ This induces $\mathcal{B}$.

BSR(BD): Satisfiability is Decidable

Theorem

Satisfiability for finite BSR(BD) clause sets N is decidable.

Proof:

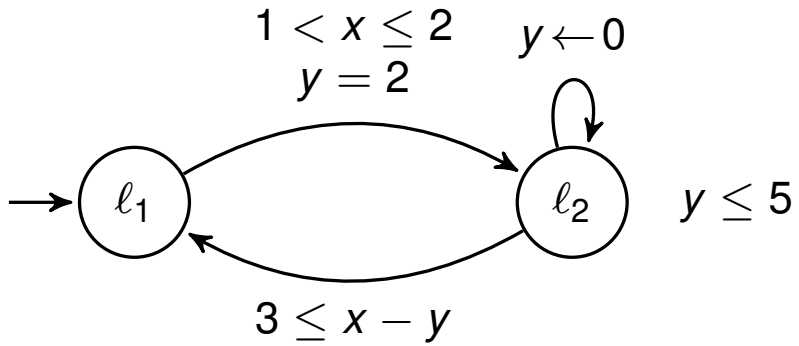
- If any model exists, then a region-uniform model exists.
- There are only finitely many region-uniform interpretations.
- We can guess one and check whether it is a model of N.

Reminder: Timed Automata [Alur&Dill 1994], [Henzinger et al. 1994]

Finite state machines equipped with *real*-valued clocks x, y, ...

Constraints: $x \triangleleft d$, $x - y \triangleleft d$, $\triangleleft \in \{<, \leq, =, \geq, >\}$, $d \in \mathbb{N}$

Operations: $x \leftarrow 0$

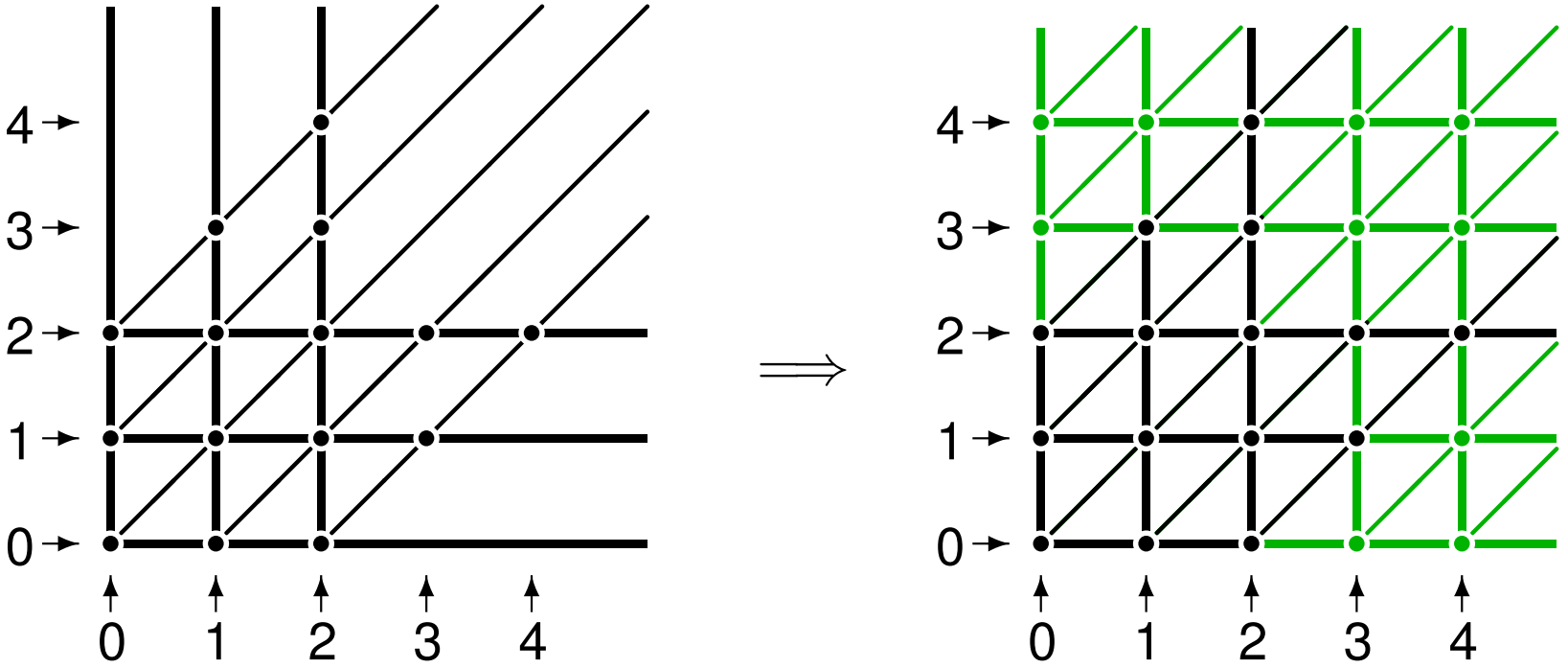


Semantics:
- states $\left\langle \ell, \begin{array}{l} x \mapsto r_1 \\ y \mapsto r_2 \end{array} \right\rangle$ with $r_1, r_2 \in \mathbb{R}$,
- transitions between locations (instantaneous), and
- progress of time (for all clocks simultaneously).

$\rightsquigarrow$ Reachability is PSPACE-complete.

TA Constraints: Distinguishable Regions of $\mathbb{R}^2$

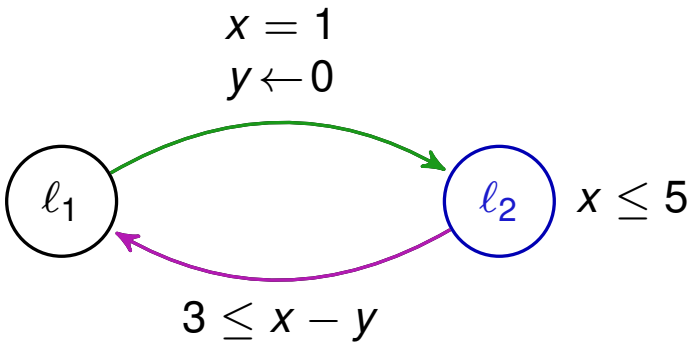
For two clocks x, y, TA constraints with constants $d \leq 2$ can distinguish regions as follows:



$\rightsquigarrow$ The BSR(BD) regions for constraints with constants from $\{-4, \ldots, 0, \ldots, 4\}$ are a refinement of the TA regions.

Encoding Reachability for a Timed Automaton

[Fietzke, Weidenbach 2012]



$$x = 1 \wedge y' = 0 \wedge x \leq 5 \wedge \mathrm{Reach}(\ell_1, x, y) \rightarrow \mathrm{Reach}(\ell_2, x, y')$$

$$(\exists t.\, t \geq 0 \wedge x' = x + t \wedge y' = y + t) \wedge x' \leq 5 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_2, x', y')$$

$$3 \leq x - y \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_1, x, y)$$

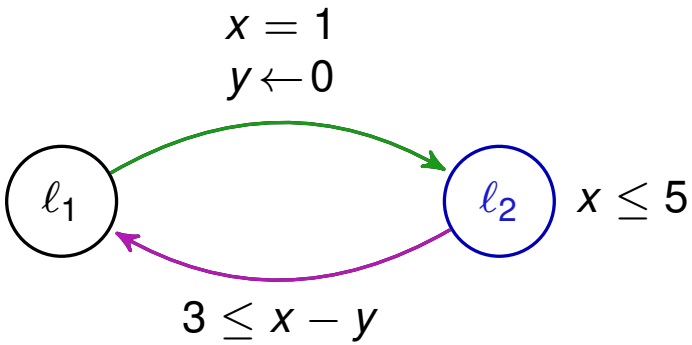
Start clause: $x = 0 \wedge y = 0 \wedge \rightarrow \mathrm{Reach}(\ell_1, x, y)$

Query clause: $y = 4 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \square$

$\rightsquigarrow$ Saturation leads to $\square$ if the answer to the query is *YES*.

Encoding Reachability for a Timed Automaton

[Fietzke, Weidenbach 2012]



$$x = 1 \wedge y' = 0 \wedge x \leq 5 \wedge \mathrm{Reach}(\ell_1, x, y) \rightarrow \mathrm{Reach}(\ell_2, x, y')$$

$$(\exists t.\, t \geq 0 \wedge x' = x + t \wedge y' = y + t) \wedge x' \leq 5 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_2, x', y')$$

$$3 \leq x - y \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_1, x, y)$$

Start clause: $x = 0 \wedge y = 0 \wedge \rightarrow \mathrm{Reach}(\ell_1, x, y)$

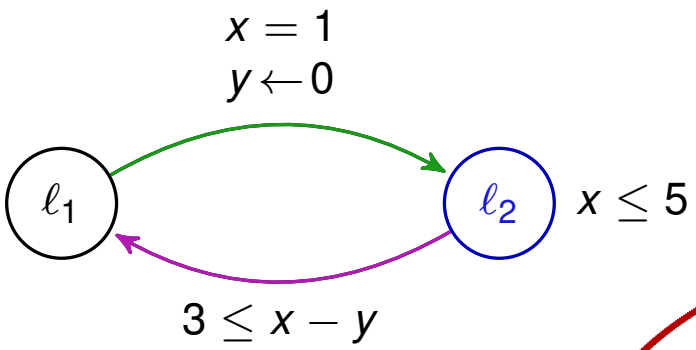
Query clause: $y = 4 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \square$

$\rightsquigarrow$ Saturation leads to $\square$ if the answer to the query is *YES*.

$\rightsquigarrow$ Syntax restrictions of BSR(BD) are not met.

Encoding Reachability for a Timed Automaton

[Fietzke, Weidenbach 2012]



$$x = 1 \wedge y' = 0 \wedge x \leq 5 \wedge \mathrm{Reach}(\ell_1, x, y) \rightarrow \mathrm{Reach}(\ell_2, x, y')$$

$$(\exists t.\, t \geq 0 \wedge x' = x + t \wedge y' = y + t) \wedge x' \leq 5 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_2, x', y')$$

$$3 \leq x - y \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_1, x, y)$$

$\exists t.\, t \geq 0 \wedge x' = x + t \wedge y' = y + t$

is equivalent to

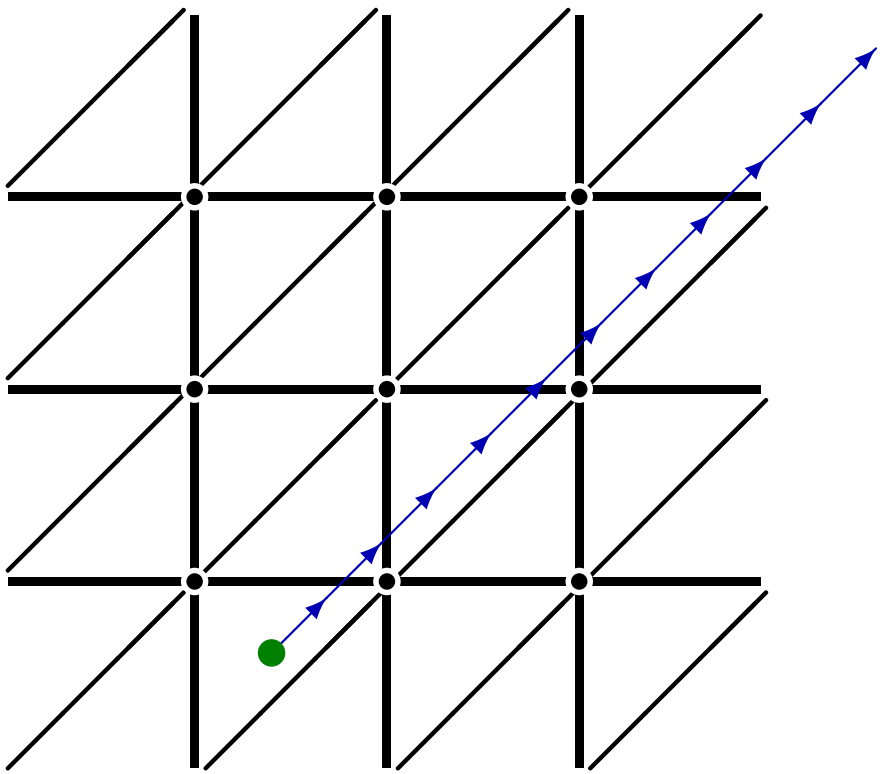
$x' \geq x \wedge y' \geq y \wedge x' - x = y' - y$

$\rightsquigarrow$ Syntax restrictions of BSR(BD) are not met.

De-Synchronizing Progression of Time

The constraint $x' \geq x \ \wedge \ y' \geq y \ \wedge \ x' - x = y' - y$

enforces *synchronous* progression of time.

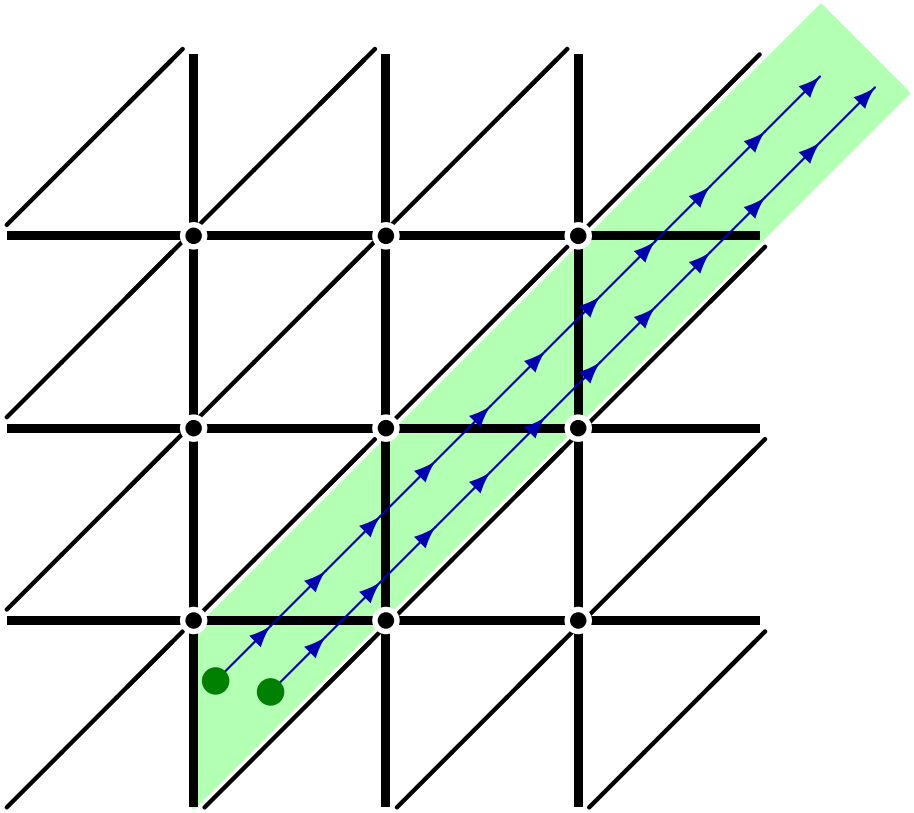


$\rightsquigarrow$ Synchronous time progression from a reachable point yields a one-dimensional reachable area.

De-Synchronizing Progression of Time

The constraint $x' \geq x \ \wedge \ y' \geq y \ \wedge \ x' - x = y' - y$

enforces *synchronous* progression of time.

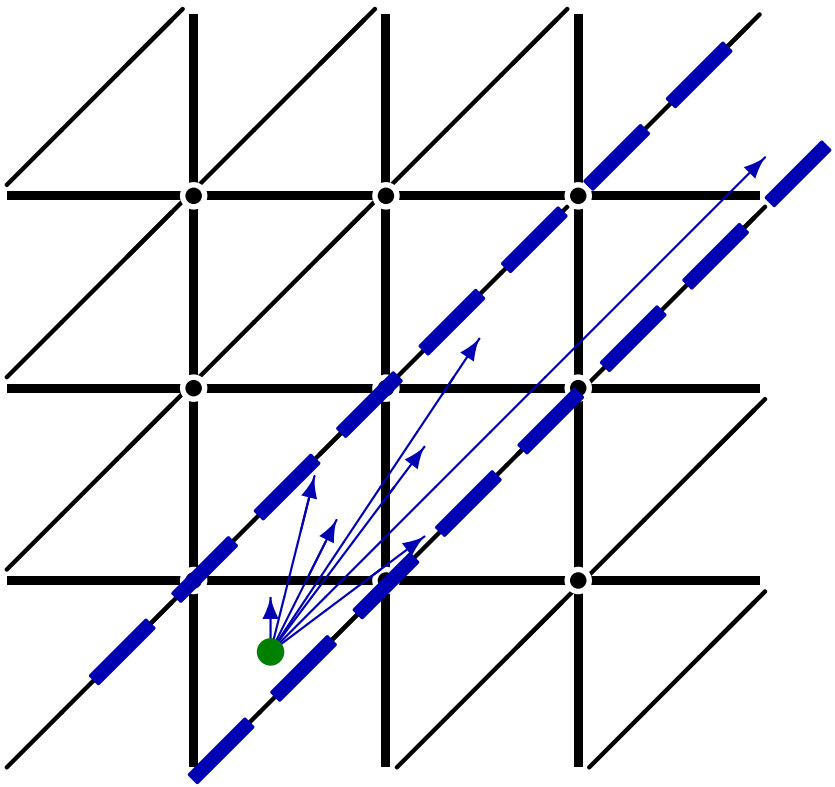


- $\rightsquigarrow$ Synchronous time progression from a reachable point yields a one-dimensional reachable area.
- $\rightsquigarrow$ Since other points in the same region are reachable, we obtain a whole reachable corridor.

De-Synchronizing Progression of Time

The constraint $x' \geq x \ \wedge \ y' \geq y \ \wedge \ x' - x = y' - y$

enforces *synchronous* progression of time.

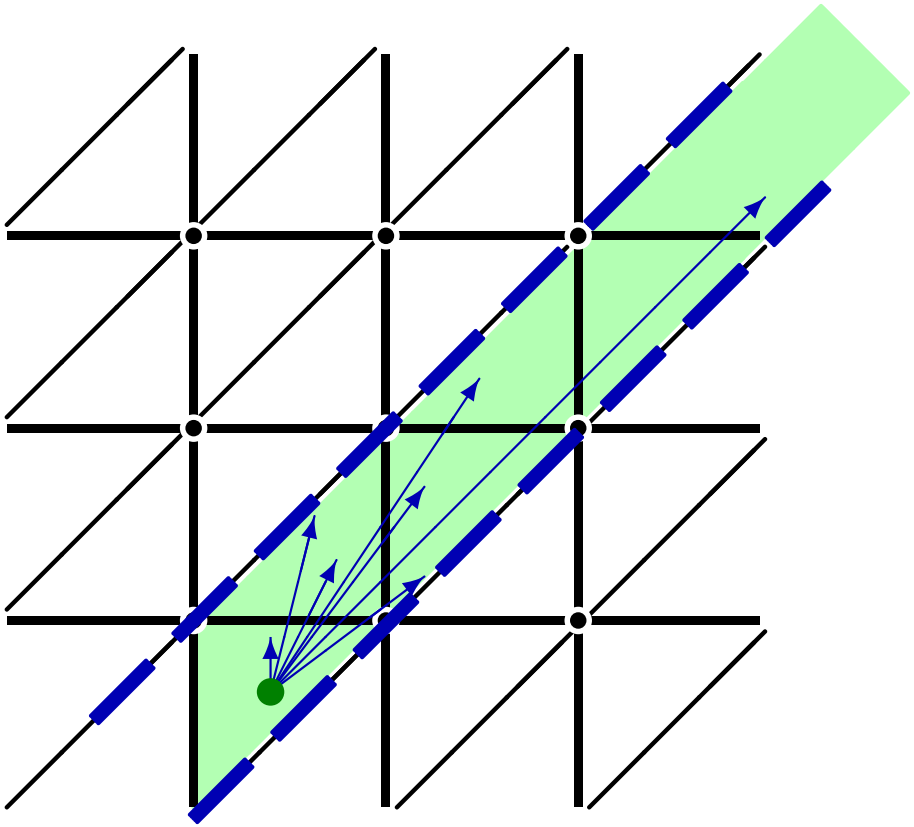


- ⇝ Synchronous time progression from a reachable point yields a one-dimensional reachable area.
- ⇝ Since other points in the same region are reachable, we obtain a whole reachable corridor.
- ⇝ We can weaken the the synchronicity requirement

De-Synchronizing Progression of Time

The constraint $x' \geq x \ \wedge \ y' \geq y \ \wedge \ x' - x = y' - y$

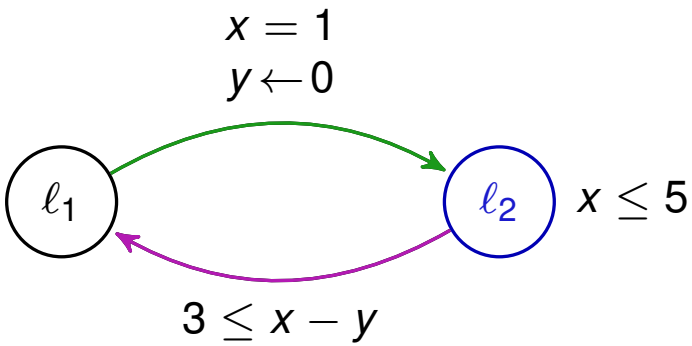
enforces *synchronous* progression of time.



- $\rightsquigarrow$ Synchronous time progression from a reachable point yields a one-dimensional reachable area.
- $\rightsquigarrow$ Since other points in the same region are reachable, we obtain a whole reachable corridor.
- $\rightsquigarrow$ We can weaken the the synchronicity requirement to

$$\bigwedge_{k \in \{-\lambda,\ldots,\lambda\}} \big(x - y \leq k \leftrightarrow x' - y' \leq k\big) \wedge \big(x - y \geq k \leftrightarrow x' - y' \geq k\big).$$

Encoding Reachability for a Timed Automaton



$$x = 1 \wedge y' = 0 \wedge x \leq 5 \wedge 0 \leq x, y, y' < 11 \wedge \mathrm{Reach}(\ell_1, x, y) \rightarrow \mathrm{Reach}(\ell_2, x, y')$$

$$\bigwedge_{k \in \{-10,\ldots,10\}} \Big((x - y \leq k \leftrightarrow x' - y' \leq k) \wedge (x - y \geq k \leftrightarrow x' - y' \geq k) \Big) \wedge 0 \leq x, y, x', y' \leq 11 \wedge x' \leq 5 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_2, x', y')$$

$$3 \leq x - y \wedge 0 \leq x, y, y' < 11 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \mathrm{Reach}(\ell_1, x, y)$$

Start clause: $x = 0 \wedge y = 0 \wedge \rightarrow \mathrm{Reach}(\ell_1, x, y)$

Query clause: $y = 4 \wedge \mathrm{Reach}(\ell_2, x, y) \rightarrow \square$

⇝ Syntax restrictions of BSR(BD) are met.

⇝ Reachability for TA can be expressed with BSR(BD).

Conclusion

We have seen BSR with *bounded* difference constraints — BSR(BD).

- BSR(BD)-Sat is decidable
- BSR(BD) can express reachability for timed automata

We have not seen BSR with *simple* linear rational arithmetic.

$$\exists cd\, \forall xy.\ c \neq d \ \wedge\ x > c + 2d - 3 \ \wedge\ x < y \ \wedge Q(x, y) \longrightarrow T(x) \ \vee\ Q(y, x)$$

- Satisfiability is decidable, too.

Future work

- Instantiation methods for BSR(BD) and for BSR(SLR) as for BSR with *simple* LIA [Horbach, V., Weidenbach. CADE'17]

- More applications of BSR(BD) and BSR(SLR)

Thank You!