On the Combination of the Bernays–Schönfinkel–Ramsey Fragment with Simple Linear Integer Arithmetic

Matthias Horbach **Marco Voigt** Christoph Weidenbach

max planck institut informatik

SAARLAND UNIVERSITY
SAARBRÜCKEN GRADUATE SCHOOL OF COMPUTER SCIENCE

SIC Saarland Informatics Campus

International Max Planck Research School for Computer Science

August 08, 2017

Motivation: Quantified Properties of Data Structures

Expressing interesting properties of data structures often requires quantification over indices.

Example: array a over characters $\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots$ and the alphabetic ordering $\prec$:

$$\begin{aligned} \exists d.\ & a[d] = \mathtt{C} \wedge a[d+1] = \mathtt{A} \wedge a[d+2] = \mathtt{D} \wedge a[d+3] = \mathtt{E} \\ & \wedge \forall ij.\ i \leq j \leq d \longrightarrow a[i] \preceq a[j] \\ & \wedge \forall ij.\ d+3 \leq i \leq j \longrightarrow a[i] \preceq a[j] \end{aligned}$$

Satisfying assignment for a:

0	1	2	3	4	5	6	7	8	9	10	11	...
A	B	B	C	A	D	E	X	Y	Z	Z	Z	...

Motivation: Quantified Properties of Data Structures

Satisfiability for the *Array Property Fragment* is decidable.

[Bradley, Manna, Sipma 2006].

⇝ Exhaustive instantiation with occurring ground index expressions suffices:

$$\exists d.\ a[d] = \mathtt{C} \wedge a[d+1] = \mathtt{A} \wedge a[d+2] = \mathtt{D} \wedge a[d+3] = \mathtt{E}$$
$$\wedge \forall ij.\ i \leq j \leq d \longrightarrow a[i] \preceq a[j]$$
$$\wedge \forall ij.\ d+3 \leq i \leq j \longrightarrow a[i] \preceq a[j]$$

⇝ Every universally quantified variable is instantiated with every index expression.

⇝ 32 ground instances

Motivation: Getting along with fewer instances

There are more economical ways of instantiation,
and they are applicable to more general formula fragments,
e.g. [Ge, de Moura 2009].

Our contribution:

- Further improved instantiation techniques
  - ⇝ Exponentially fewer instances in certain cases
  - ⇝ Inspired by quantifier elimination methods over linear *rational* arithmetic w/o uninterpreted preds. or functs.
    [Loos, Weispfenning 1993], [Dolzmann 2000]
- Our methods are applicable to
  - *Array Property Fragment* [Bradley, Manna, Sipma 2006]
  - *stratified vocabulary* fragments [Abadi et al. 2007], [Korovin 2013]
  - *Finite Essentially Uninterpreted Fragment* [Ge, de Moura 2009]

The Plan

1. Illustrate parts of our methods for the Bernays–Schönfinkel–Ramsey Fragment with Simple Linear Integer Arithmetic — BSR(SLI)

   $\rightsquigarrow$ Not yet expressive enough for array properties

2. Extend BSR(SLI) to BSR(SLI$+T$) and transfer instantiation methods

Bernays–Schönfinkel–Ramsey with Simple Linear Integer Arithmetic — BSR(SLI)

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

- clauses in ... $\to$ ... notation
- arithm. atoms only left of $\to$
- $+, -$ only in ground terms
- $x \le y$ ✓, $x = y$ ✓, ~~$x < y$~~, ~~$x \ne y$~~

$=$ BSR(SLI)

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

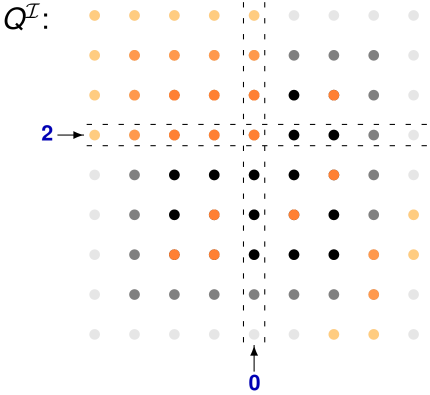
$<, \le, =, \ne, \ge, >$ allowed

only $\le, =, \ge$ allowed

$\rightsquigarrow$ We here concentrate on constraints $1 \le x$, $x \le 2$, $x \le y$

Satisfiability for BSR(SLI)

An interpretation $\mathcal{I}$ of $Q : \mathbb{Z} \times \mathbb{Z}$ is a coloring of the integer lattice:



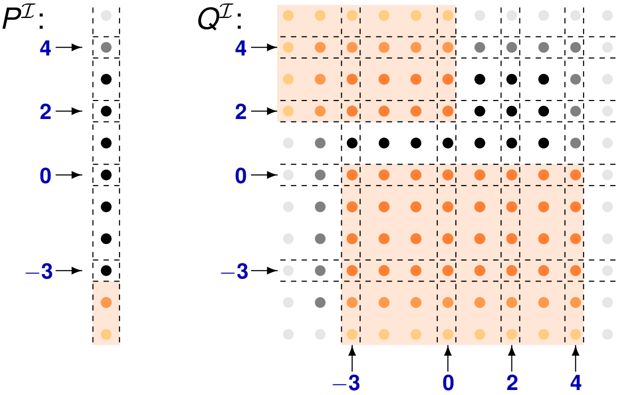
- ⇝ There are infinitely many colorings
- ⇝ Fortunately, we can concentrate on a special kind: *interval-uniform*
- ⇝ Similar to *finite model property*

$\forall xy.\ x \leq 0 \wedge 2 \leq y \longrightarrow Q(x, y)$ is satisfied by $\mathcal{I}$

Interval-Uniform Models

$$x \le 4 \;\wedge\; y \le 0 \;\wedge\; y \le x \;\rightarrow\; P(x) \vee Q(x, y)\,,$$
$$x \le 0 \;\wedge\; 2 \le y \;\rightarrow\; Q(x, y)\,,$$
$$-3 \le x \;\rightarrow\; \neg P(x)$$

$\leadsto$ If satisfiable, then we find a model $\mathcal{I}$ of the form

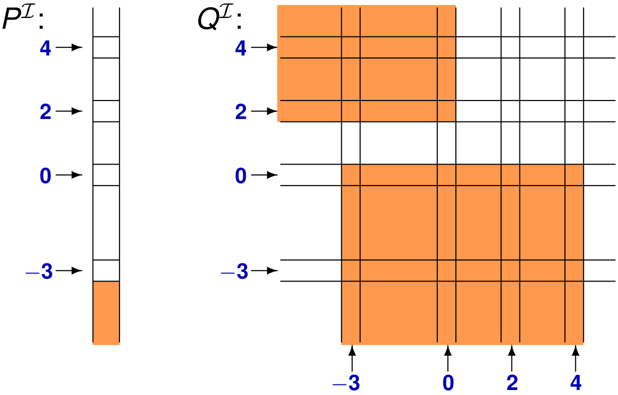


$\leadsto$ $P^{\mathcal{I}}$ and $Q^{\mathcal{I}}$ need not distinguish what arithmetic constraints cannot distinguish

Interval-Uniform Models

$$
\begin{aligned}
x \le 4 \wedge y \le 0 \wedge y \le x &\rightarrow P(x) \vee Q(x,y)\,, \\
x \le 0 \wedge 2 \le y &\rightarrow Q(x,y)\,, \\
-3 \le x &\rightarrow \neg P(x)
\end{aligned}
$$

$\rightsquigarrow$ If satisfiable, then we find a model $\mathcal{I}$ of the form



- $\rightsquigarrow$ $P^{\mathcal{I}}$ and $Q^{\mathcal{I}}$ need not distinguish what arithmetic constraints cannot distinguish
- $\rightsquigarrow$ Color only finitely many regions

Key Insight about BSR(SLI) Satisfiability

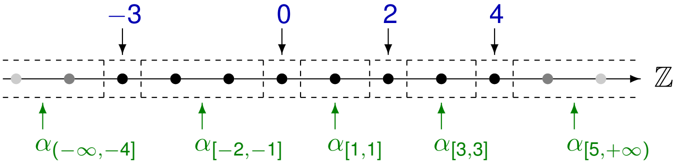
Theorem

Satisfiability for finite BSR(SLI) clause sets is decidable.

- $\rightsquigarrow$ Theoretically, via coloring a finite partition of the integer lattice
  - $\rightsquigarrow$ BSR(SLI)-Sat is NEXPTIME-complete
- $\rightsquigarrow$ Practically, via finite (ground) instantiation
  - $\rightsquigarrow$ Use constants to represent regions

Constants as Representatives

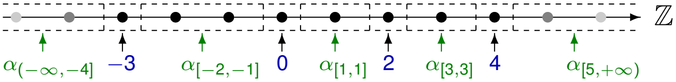
$$
\begin{aligned}
x \le 4 \wedge \quad y \le 0 \wedge y \le x &\rightarrow P(x) \vee Q(x,y)\ ,\\
x \le 0 \wedge 2 \le y &\rightarrow Q(x,y)\ ,\\
-3 \le x &\rightarrow \neg P(x)
\end{aligned}
$$



⇝ To construct interval-uniform models it suffices to probe one representative per interval!

⇝ We can derive an equisatisfiable finite clause set via instantiation with these representatives

<u>Idea:</u> Pick one representative from each interval.



The clause $\quad -3 \leq x \longrightarrow \neg P(x)$

can be instantiated to

$$
\begin{aligned}
x &= \alpha_{(-\infty,-4]} && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= -3 && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= \alpha_{[-2,-1]} && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= 0 && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= \alpha_{[1,1]} && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= 2 && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= \alpha_{[3,3]} && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= 4 && \wedge -3 \leq x \longrightarrow \neg P(x)\,,\\
x &= \alpha_{[5,+\infty)} && \wedge -3 \leq x \longrightarrow \neg P(x)\,.
\end{aligned}
$$

How to Get Along with Fewer Instances

(1) Filter wrt. argument position (similar to [Ge, de Moura 2009])

$$\boxed{x \le 4} \;\wedge\; y \le 0 \;\wedge\; y \le x \;\rightarrow\; P(x) \;\vee\; Q(x, y)$$

⇝ Not all bounds are relevant for x

(2) Filter wrt. bound direction

⇝ Instantiation points are exclusively derived from lower bounds or from upper bounds

⇝ Next slide

(3) Independent selection of bound directions

⇝ E.g. lower bounds for x and upper bounds for y

How to Get Along with Fewer Instances

(1) Filter wrt. argument position (similar to [Ge, de Moura 2009])

$$\boxed{x \leq 4} \land y \leq 0 \land y \leq x \rightarrow P(x) \lor Q(x, y)$$

$\rightsquigarrow$ Not all bounds are relevant for x

(2) Filter wrt. bound direction

$\rightsquigarrow$ Instantiation points are exclusively derived from lower bounds or from upper bounds

$\rightsquigarrow$ Next slide

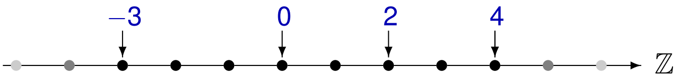
(3) Independent selection of bound directions

$\rightsquigarrow$ E.g. lower bounds for x and upper bounds for y

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y) \,,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y) \,,$$
$$-3 \leq x \rightarrow \neg P(x)$$

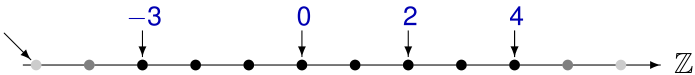


Instantiation points for x:

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y) ,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y) ,$$
$$-3 \leq x \rightarrow \neg P(x)$$

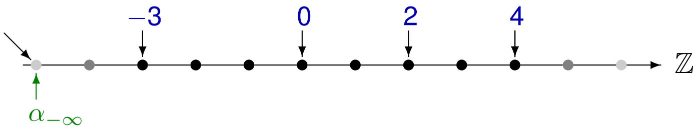


Instantiation points for x:

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y) ,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y) ,$$
$$-3 \leq x \rightarrow \neg P(x)$$

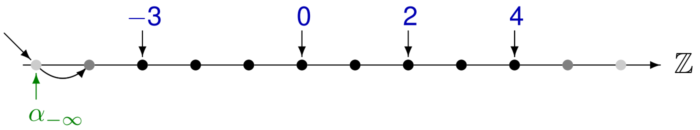


Instantiation points for x: $\alpha_{-\infty}$

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

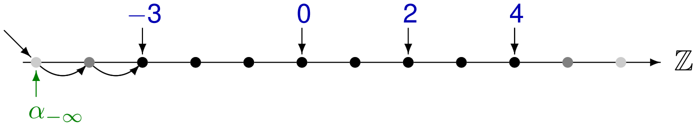


Instantiation points for x: $\alpha_{-\infty}$

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y)\ ,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y)\ ,$$
$$-3 \leq x \rightarrow \neg P(x)$$

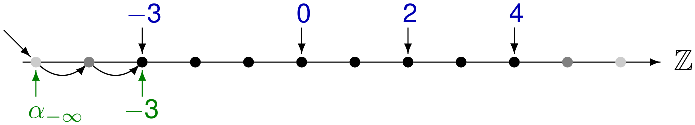


Instantiation points for x: $\alpha_{-\infty}$

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y)\ ,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y)\ ,$$
$$-3 \leq x \rightarrow \neg P(x)$$

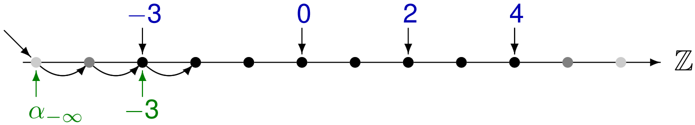


Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

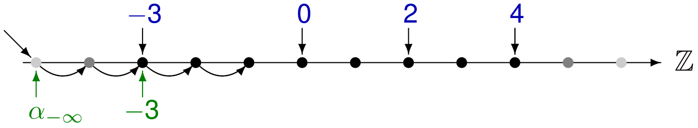


Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

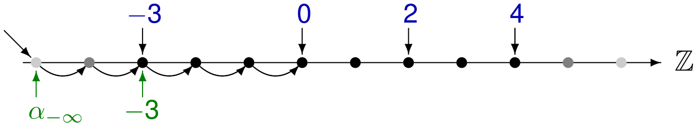


Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \;\wedge\; y \leq 0 \;\wedge\; y \leq x \;\rightarrow\; P(x) \vee Q(x,y)\,,$$
$$x \leq 0 \;\wedge\; 2 \leq y \;\rightarrow\; Q(x,y)\,,$$
$$-3 \leq x \;\rightarrow\; \neg P(x)$$

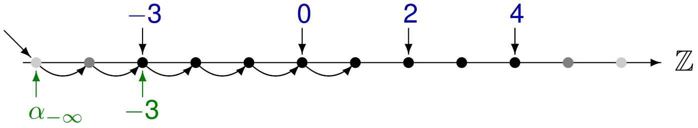


Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

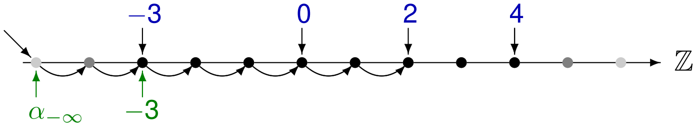


Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$



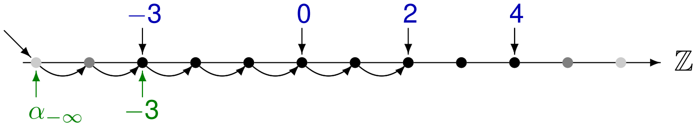
Instantiation points for x: $\alpha_{-\infty}$, -3

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \;\wedge\; y \leq 0 \;\wedge\; y \leq x \;\rightarrow\; P(x) \vee Q(x,y)\,,$$
$$x \leq 0 \;\wedge\; 2 \leq y \;\rightarrow\; Q(x,y)\,,$$
$$-3 \leq x \;\rightarrow\; \neg P(x)$$

bound propagation !

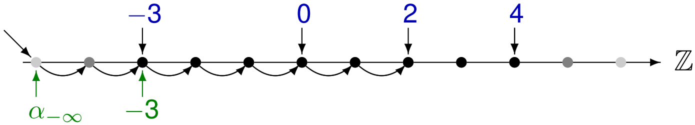


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow \neg Q(x, y),$$
$$-3 \leq x \rightarrow \neg P(x)$$



Instantiation points for x: $\alpha_{-\infty}$, -3, 2

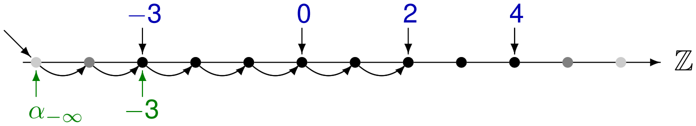
Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \le 4 \;\wedge\; y \le 0 \;\wedge\; y \le x \;\rightarrow\; P(x) \vee Q(x, y)\,,$$
$$x \le 0 \;\wedge\; 2 \le y \;\rightarrow\; \neg Q(x, y)\,,$$
$$-3 \le x \;\rightarrow\; \neg P(x)$$

$\models \bot$

at $[x \mapsto 2, y \mapsto 2]$



Instantiation points for x: $\alpha_{-\infty}$, -3, 2

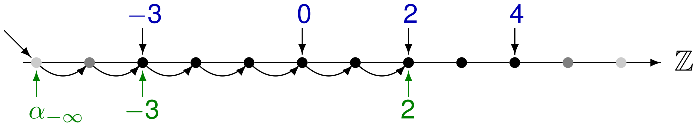
Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y)\ ,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow \neg Q(x, y)\ ,$$
$$-3 \leq x \rightarrow \neg P(x)$$

$\models \bot$

at $[x \mapsto 2, y \mapsto 2]$

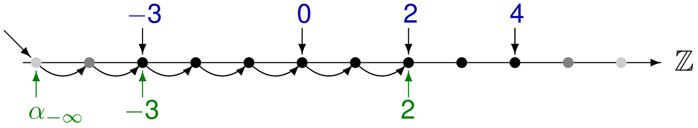


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

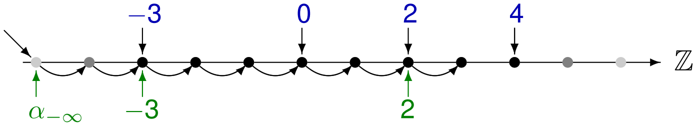


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x, y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x, y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

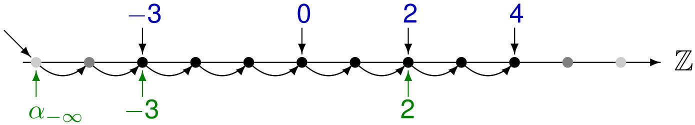


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

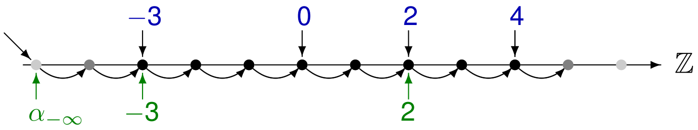


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

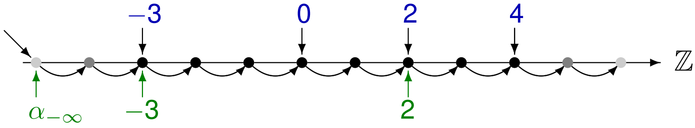


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y),$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y),$$
$$-3 \leq x \rightarrow \neg P(x)$$

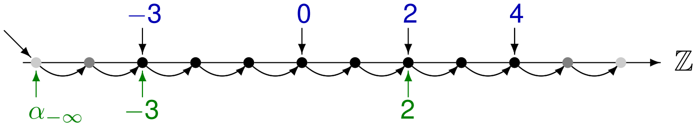


Instantiation points for x: $\alpha_{-\infty}$, -3, 2

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$
\begin{array}{lcr}
x \leq 4 \wedge y \leq 0 \wedge y \leq x & \rightarrow & P(x) \vee Q(x, y)\,, \\
x \leq 0 \wedge 2 \leq y & \rightarrow & Q(x, y)\,, \\
-3 \leq x & \rightarrow & \neg P(x)
\end{array}
$$

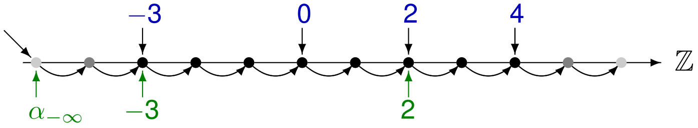


Instantiation points for x: $\alpha_{-\infty}, \; -3, \; 2$

Fewer Instances: Filter wrt. bound direction

Idea: Consider exclusively lower bounds [Dolzmann 2000]

$$x \le 4 \wedge y \le 0 \wedge y \le x \rightarrow P(x) \vee Q(x,y) \,,$$
$$x \le 0 \wedge 2 \le y \rightarrow Q(x,y) \,,$$
$$-3 \le x \rightarrow \neg P(x)$$

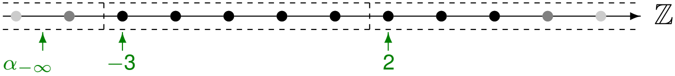


Instantiation points for x: $\alpha_{-\infty},\ -3,\ 2$

$\rightsquigarrow$ Dually, upper bounds would suffice: $\alpha_{+\infty},\ 4,\ 0$

Fewer Instances: Filter wrt. bound direction

Induced partition:



The clause $-3 \leq x \longrightarrow \neg P(x)$

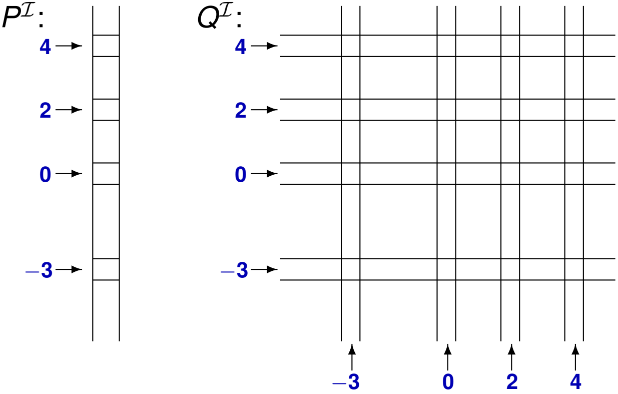
s is *equisatisfiable* to

$$x = \alpha_{-\infty} \wedge x \leq -3 \longrightarrow \neg P(x),$$
$$x = -3 \wedge x \leq -3 \longrightarrow \neg P(x),$$
$$x = 2 \wedge x \leq -3 \longrightarrow \neg P(x),$$
$$\alpha_{-\infty} < -3$$

⇝ 3 instances plus 1 unit clause instead of 9 instances

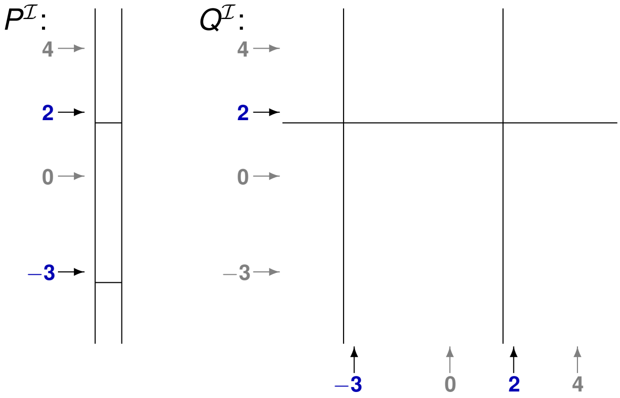
Naive Partition of $\mathbb{Z}$

$$
\begin{array}{rcl}
x \le 4 \;\wedge\; y \le 0 \;\wedge\; y \le x & \rightarrow & P(x) \vee Q(x,y)\,, \\
x \le 0 \;\wedge\; 2 \le y & \rightarrow & Q(x,y)\,, \\
-3 \le x & \rightarrow & \neg P(x)
\end{array}
$$



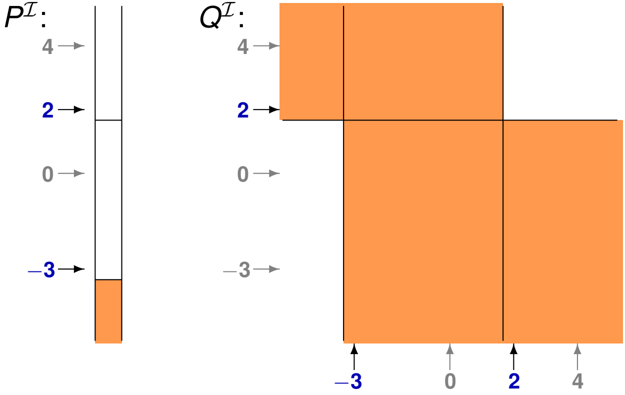
More Efficient Partition

$$x \leq 4 \wedge y \leq 0 \wedge y \leq x \rightarrow P(x) \vee Q(x,y) \,,$$
$$x \leq 0 \wedge 2 \leq y \rightarrow Q(x,y) \,,$$
$$-3 \leq x \rightarrow \neg P(x)$$



More Efficient Partition

$$x \le 4 \wedge y \le 0 \wedge y \le x \rightarrow P(x) \vee Q(x,y)\,,$$
$$x \le 0 \wedge 2 \le y \rightarrow Q(x,y)\,,$$
$$-3 \le x \rightarrow \neg P(x)$$



Enriching BSR(SLI)

$\exists^*\forall^*$ quantifier prefix
$+$ uninterpreted predicates
$+$ linear integer arithmetic
$+$ syntactic restrictions
$+$ background theory T
$+$ uninterpreted functions
$+$ further syntactic restrictions

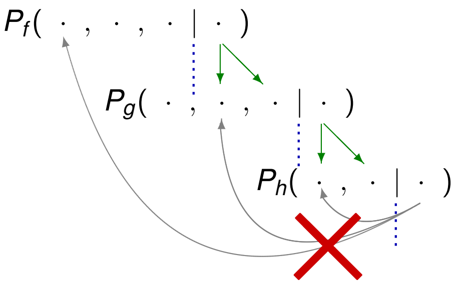
$=$ BSR(SLI $+T$)

- unint. functions represented by predicates
- unint. function application is stratified (next slide)
- $\Gamma \to \Delta, f(\ldots) \approx x$ requires $g(\ldots) \approx x$ in Γ
  $\leadsto$ similar to [Ge, de Moura 2009]
- ...

Stratified Function Application

$$f\underbrace{(\,\cdot\,,\,\cdot\,,\,\cdot\,)}_{\text{input}} \approx \underbrace{\cdot}_{\textit{output}} \qquad \Longrightarrow \qquad P_f\,(\underbrace{\,\cdot\,,\,\cdot\,,\,\cdot\,}_{\text{input}} \mid \underbrace{\,\cdot\,}_{\text{output}})$$

Stratification:



$h(\,g(\ldots f(\ldots)\ldots),\ f(\ldots)\,)$ ✓

$h(\,g(\,f(\ldots)\ldots),\ f(\,g(\ldots)\ldots)\,)$ x

$f(\ldots f(\ldots)\ldots)$ x

Results for BSR(SLI+T)

Theorem

Satisfiability for finite BSR(SLI+T) clause sets is decidable, if ground BSR(SLI+T) is decidable.

⇝ Instantiation methods for BSR(SLI) are applicable to BSR(SLI+T), too

Proposition

The *integer-indexed Array Property Fragment* [Bradley et al. 2006] with element theory *T* can be translated into BSR(SLI+T). (Un)satisfiability is preserved.

⇝ This is only one example

We have seen...

... Bernays–Schönfinkel–Ramsey Fragment with
simple linear integer arithmetic — BSR(SLI).

... BSR(SLI)-Sat is decidable via instantiation.

... improved instantiation techniques
that are applicable to other settings, too,
e.g. quantified array properties.

What else?

- Similar instantiation methods for BSR with *simple* LRA.
- Decidability results for
  - (a) BSR with *simple* LRA plus $x < y$.
  - (b) BSR with *bounded* difference constraints $x - y \triangleleft d$ where $x \in [r_1, r_2]$ and $y \in [r_3, r_4]$ and $d, r_i \in \mathbb{Q}$.
  - $\rightsquigarrow$ FroCoS'17

Thank You!