SPASS-SATT:
a CDCL(LA) Solver

(Paper at CADE-27)

Martin Bromberger, Mathias Fleury, Simon Schwarz,
and Christoph Weidenbach

SPASS-SATT:
a CDCL(LA) Solver

(Paper at CADE-27)

Translation: fun (=SPASS) sated (=SATT)

Martin Bromberger, Mathias Fleury, Simon Schwarz,
and Christoph Weidenbach

SPASS-SATT:
a CDCL(LA) Solver

(Paper at CADE-27)

Translation: fun (=SPASS) sated (=SATT)

being sick/tired of having fun…

Martin Bromberger, Mathias Fleury, Simon Schwarz,

and Christoph Weidenbach

Quantifier-Free Linear Arithmetic

$$(x > 0 \quad \vee \quad x + y > 0) \;\wedge\; (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \;\; (y < 0) \;\; \wedge \;\; \neg(x > 0)$$

Quantifier-Free Linear Arithmetic

$$(x > 0 \quad \vee \quad x + y > 0) \ \wedge \ (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \ \ (y < 0) \ \ \wedge \ \ \neg(x > 0)$$

Signature: $\Sigma_{LA} \coloneqq \{+, -, <, \leq, \geq, >, 0, 1, 2, \ldots\}$

Quantifier-Free Linear Arithmetic

$$(x > 0 \quad \vee \quad x + y > 0) \ \wedge \ (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \ \ (y < 0) \ \ \wedge \ \ \neg(x > 0)$$

Signature: $\Sigma_{LA} \coloneqq \{+, -, <, \leq, \geq, >, 0, 1, 2, \dots\}$

Multiplication only as syntactic sugar!

E.g.: $3 \cdot x \ \mapsto x + x + x$

Quantifier-Free Linear Arithmetic

$$(x > 0 \quad \vee \quad x + y > 0) \;\wedge\; (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \;\; (y < 0) \;\; \wedge \;\; \neg(x > 0)$$

Signature: $\Sigma_{LA} := \{+, -, <, \leq, \geq, >, 0, 1, 2, \ldots\}$

Multiplication only as syntactic sugar!

E.g.: $3 \cdot x \;\mapsto x + x + x$

Goal: Quantifier-Free Linear Rational Arithmetic (QF_LRA)

$\Rightarrow$ rational solution, i.e., $x, y, \ldots \in \mathbb{Q}$

Quantifier-Free Linear Integer Arithmetic (QF_LIA)

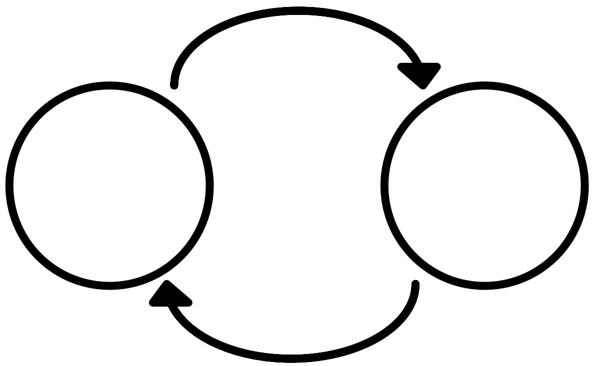
$\Rightarrow$ integer solution, i.e., $x, y, \ldots \in \mathbb{Z}$

CDCL(T)/DPLL(T)

$$(x > 0 \quad \vee \quad x + y > 0) \ \wedge \ (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \ \ (y < 0) \ \ \wedge \ \ \neg(x > 0)$$

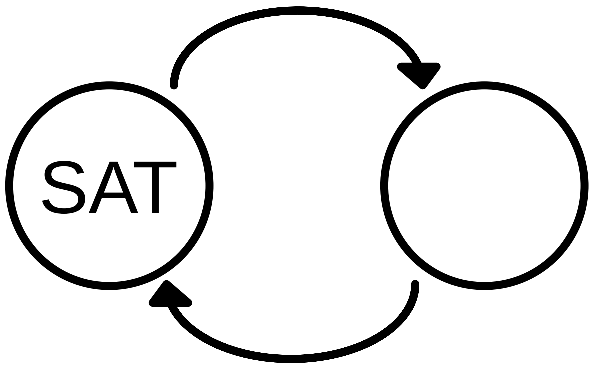
CDCL(T)/DPLL(T)

$$(x > 0 \quad \vee \quad x + y > 0) \wedge (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \quad (y < 0) \quad \wedge \quad \neg(x > 0)$$



CDCL(T)/DPLL(T)

$$(x > 0 \quad \vee \quad x + y > 0) \ \wedge \ (x < 0 \quad \vee \ \ x + y < 3)$$
$$\wedge \ \ (y < 0) \ \ \wedge \ \ \neg(x > 0)$$

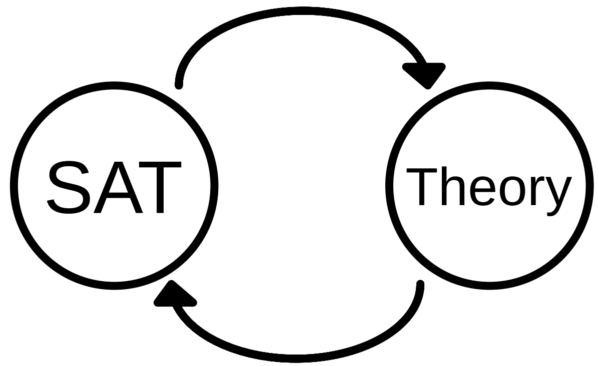


CDCL solver:

CDCL = conflict-driven clause-learning
Decision procedure for propositional CNF formulas

CDCL(T)/DPLL(T)

$$(x > 0 \quad \vee \quad x + y > 0) \;\wedge\; (x < 0 \quad \vee \quad x + y < 3)$$
$$\wedge \quad (y < 0) \quad \wedge \quad \neg(x > 0)$$



CDCL solver:

CDCL = conflict-driven clause-learning
Decision procedure for propositional CNF formulas

Theory solver:

Decision procedure for conjunctions of theory atoms
e.g. Simplex for QF_LRA & Branch-and-Bound for QF_LIA

SMT-COMP 2018

QF_LIA (Main Track)

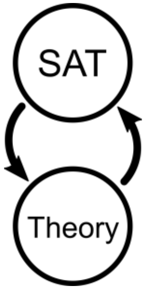
QF_LIA = quantifier-free linear integer arithmetic
Benchmarks: 6947
Time limit: 1200s

Solver	Solved Score	CPU time Score	Solved
SPASS-SATT	6587.626	72.048	6744
Ctrl-Ergo	6221.467	156.086	6259
MathSAT^n	6135.114	164.626	6528
SMTInterpol	5915.623	204.123	6286
CVC4	5891.019	194.986	6357
Yices 2.6.0	5867.976	209.452	6232
z3-4.7.1^n	5733.374	224.539	6195
SMTRAT-Rat	4049.914	515.394	3112
veriT	3155.162	295.434	2734

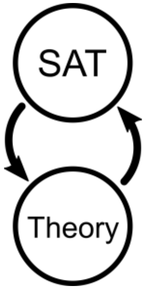
QF_LRA (Main Track)

QF_LRA = quantifier-free linear rational arithmetic
Benchmarks: 1649
Time limit: 1200s

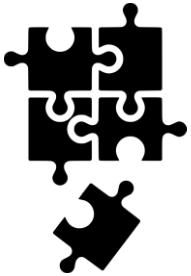
Solver	Solved Score	CPU time Score	Solved
CVC4	1586.833	69.006	1566
SPASS-SATT	1586.396	64.292	1590
Yices 2.6.0	1583.186	63.901	1567
veriT	1568.212	79.840	1527
SMTInterpol	1548.476	102.257	1521
MathSAT^n	1536.458	107.673	1461
z3-4.7.1^n	1527.249	113.154	1435
opensmt2	1498.663	131.674	1329
Ctrl-Ergo	1450.082	172.097	1354
SMTRAT-Rat	1297.891	275.918	984
SMTRAT-MCSAT	1090.526	409.015	711



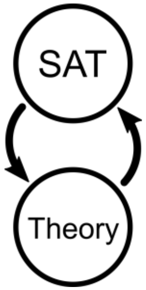
SAT and theory interaction:



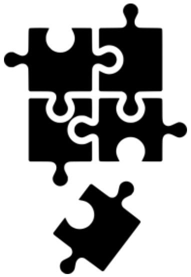
SAT and theory interaction:



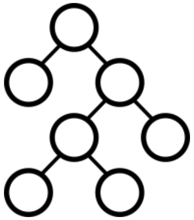
Theory solver extensions:



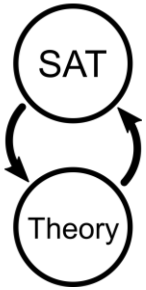
SAT and theory interaction:



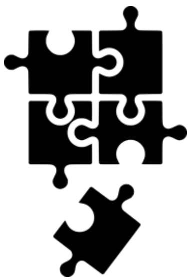
Theory solver extensions:



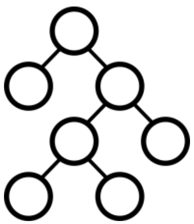
Data-structure improvements:



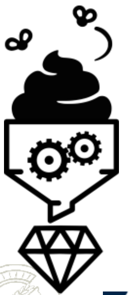
SAT and theory interaction:



Theory solver extensions:

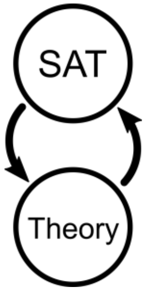


Data-structure improvements:



Preprocessing:

[…] invented by our team   […] invented & published by someone else   […] never published but implemented



SAT and theory interaction:

- weakened early pruning [Sebastiani07]
- unate propagations and bound refinements [Dutertre06]
- decision recommendations [Yices]

Theory solver extensions:

- unit cube test [Bromberger16]
- bounding transformation [Bromberger18]
- simple rounding and bound propagation [Schrijver86]

Data-structure improvements:

- priority queue for pivot selection [pretty much everyone]
- integer coefficients instead of rational coefficients [veriT]
- backup instead of recalculation [pretty much everyone]

Preprocessing:

- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]

[…] invented by our team [...] invented & published by someone else [...] never published but implemented

SAT and theory interaction:

- weakened early pruning [Sebastiani07]
- unate propagations and bound refinements [Dutertre06]
- decision recommendations [Yices]

Theory solver extensions:

- unit cube test [Bromberger16]
- bounding transformation [Bromberger18]
- simple rounding and bound propagation [Schrijver86]

Data-structure improvements:

- priority queue for pivot selection [pretty much everyone]
- integer coefficients instead of rational coefficients [veriT]
- backup instead of recalculation [pretty much everyone]

Preprocessing:

- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

$\boxed{C \Leftrightarrow y \geq 5;}$

Model: $\boxed{A}$ $\boxed{B}$

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

Use rational assignment as heuristic
(Assignment is side effect of failed weakened early pruning)

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

$\boxed{C \Leftrightarrow y \geq 5;}$

Model: $\boxed{A}$ $\boxed{B}$

Assignment: $x = 0, y = 1$

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

Use rational assignment as heuristic
(Assignment is side effect of failed weakened early pruning)

Goal: assignment should stay solution for model

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

$\boxed{C \Leftrightarrow y \geq 5;}$

Model: $\boxed{A}$ $\boxed{B}$

Assignment: $x = 0, y = 1$

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

Use rational assignment as heuristic
(Assignment is side effect of failed weakened early pruning)

Goal: assignment should stay solution for model
(Why? Might reduce time spent on theory checking)

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

$\boxed{C \Leftrightarrow y \geq 5;}$

Model: $\boxed{A}$ $\boxed{B}$

Assignment: $x = 0, y = 1$

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

Use rational assignment as heuristic
(Assignment is side effect of failed weakened early pruning)

Goal: assignment should stay solution for model
(Why? Might reduce time spent on theory checking)

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

$\boxed{C \Leftrightarrow y \geq 5;}$

$\boxed{C^\dagger \Leftrightarrow 1 \geq 5;}$

$\boxed{\neg C^\dagger \Leftrightarrow 1 < 5;}$

Model: $\boxed{A}$ $\boxed{B}$

Assignment: $x = 0, y = 1$

Decision Recommendations

How to select phase of decision literal? $\boxed{C^\dagger}$ or $\boxed{\neg C^\dagger}$

Use rational assignment as heuristic
(Assignment is side effect of failed weakened early pruning)

Goal: assignment should stay solution for model
(Why? Might reduce time spent on theory checking)

$\boxed{A \Leftrightarrow x \geq 0;}$

$\boxed{B \Leftrightarrow y \geq x + 1;}$

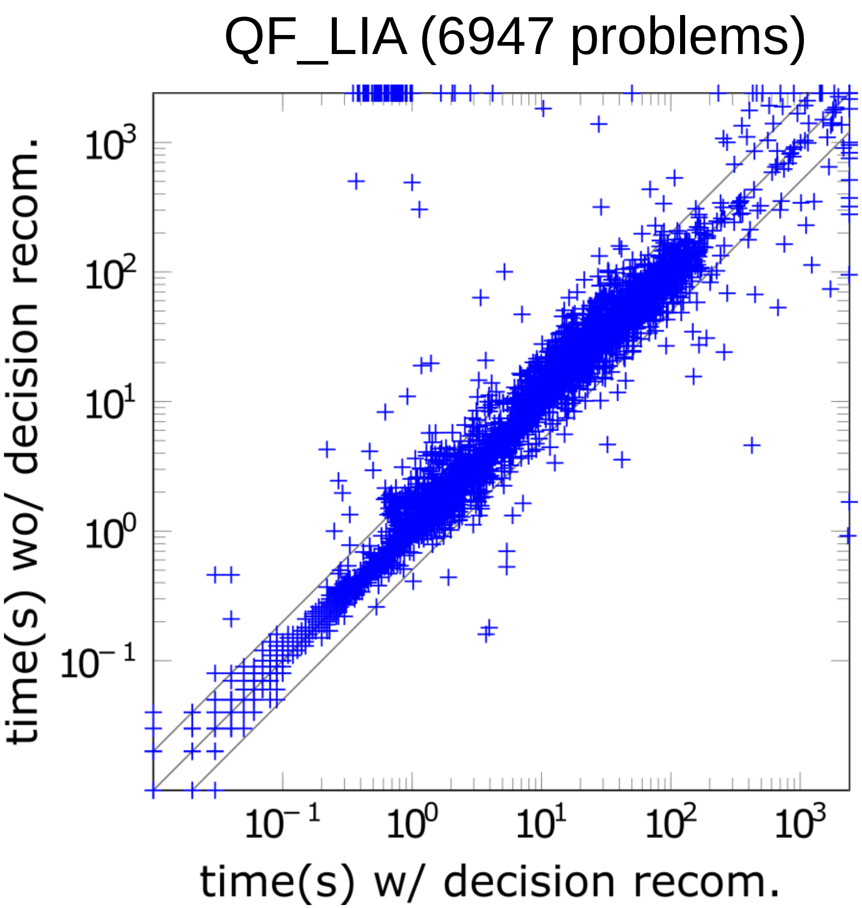
$\boxed{C \Leftrightarrow y \geq 5;}$

$\boxed{C^\dagger \Leftrightarrow 1 \geq 5;}$ $\boxed{\neg C^\dagger \Leftrightarrow 1 < 5;}$

Model: $\boxed{A}$ $\boxed{B}$ $\boxed{\neg C^\dagger}$

Assignment: $x = 0, y = 1$

Decision Recommendations

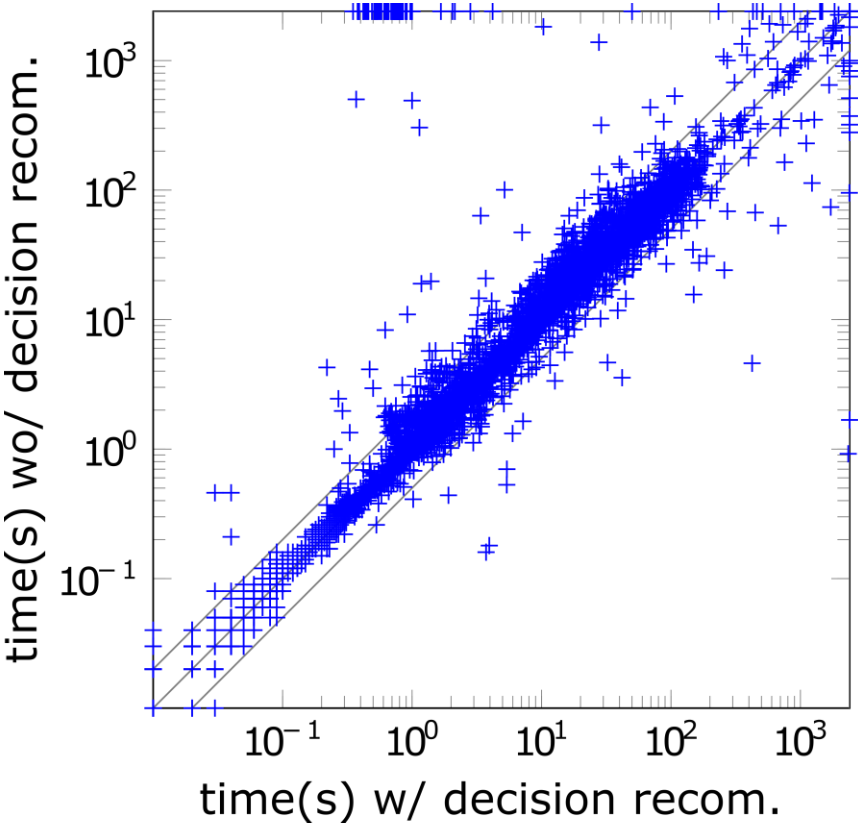


additional instances: 129

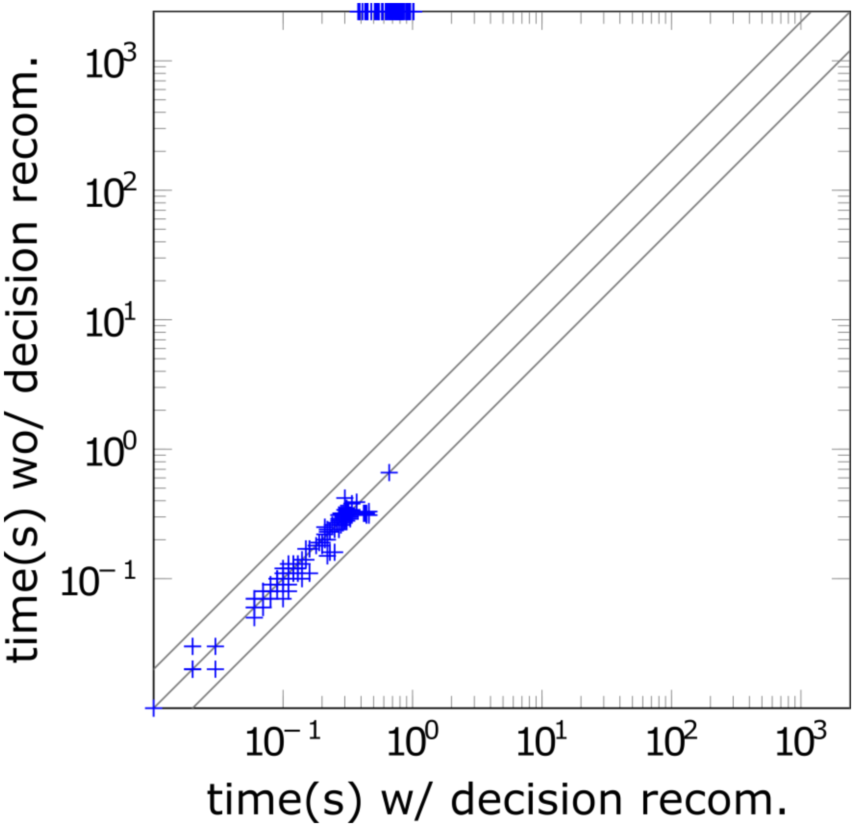
twice as fast/slow: 389/58

Decision Recommendations

QF_LIA (6947 problems)



convert (319 problems)



additional instances: 129

twice as fast/slow: 389/58

additional instances: 116

max planck institut informatik

SIC Saarland Informatics Campus

Theory Solver

Input: $\{a_i^T x \leq b_i \mid i = 1, \ldots, m\}$

Goal: QF_LRA: $x_1, \ldots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \ldots, x_n \in \mathbb{Z}$

Theory Solver

Input: $\{a_i^T x \leq b_i \mid i = 1, \ldots, m\}$

Goal: QF_LRA: $x_1, \ldots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \ldots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \quad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

max planck institut informatik

SIC Saarland Informatics Campus

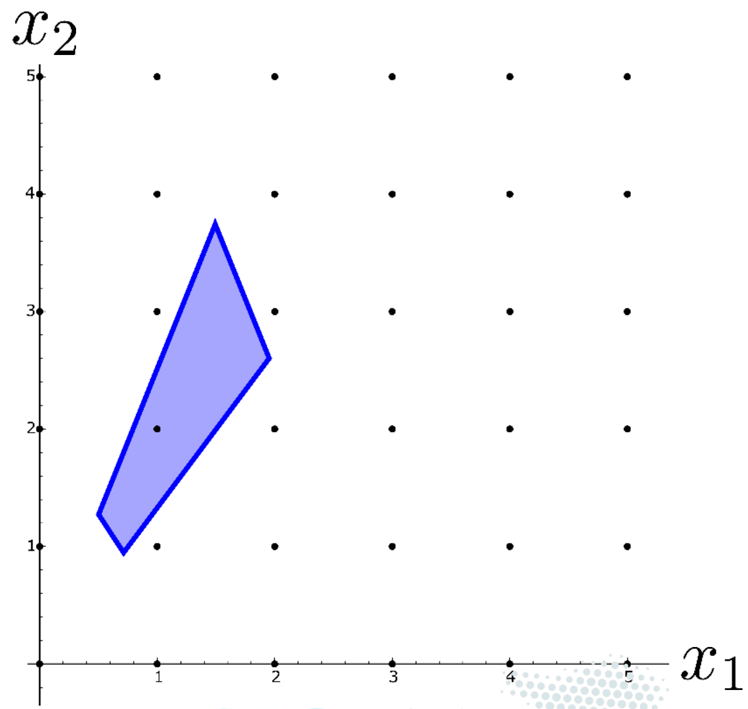
Theory Solver

Input: $\{a_i^T x \leq b_i \mid i = 1, \ldots, m\}$

Goal: QF_LRA: $x_1, \ldots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \ldots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \quad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$



Theory Solver

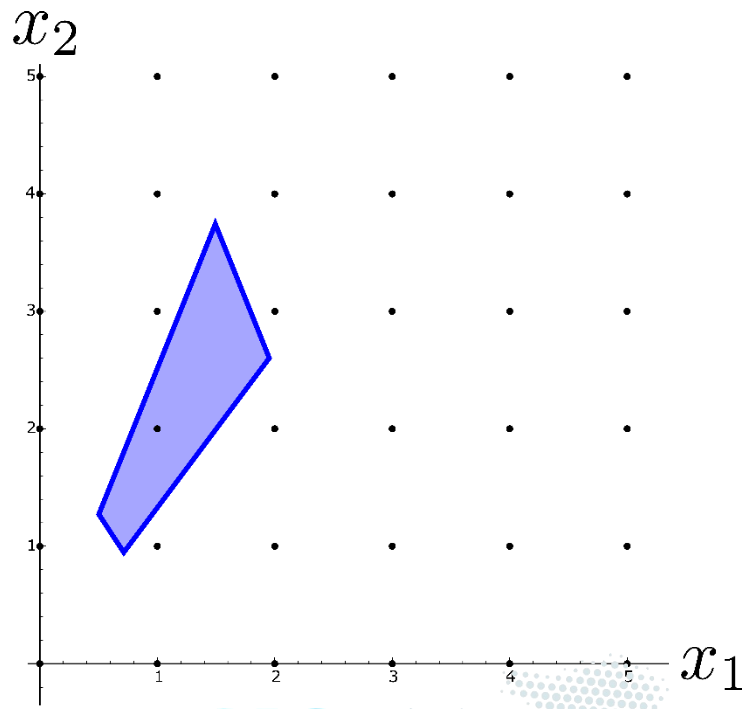
Input: $\{a_i^T x \leq b_i \mid i = 1, \dots, m\}$

Goal: QF_LRA: $x_1, \dots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \dots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \qquad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

$x_1, x_2 \in \mathbb{Q}$ QF_LRA



max planck institut informatik

SIC Saarland Informatics Campus

Theory Solver

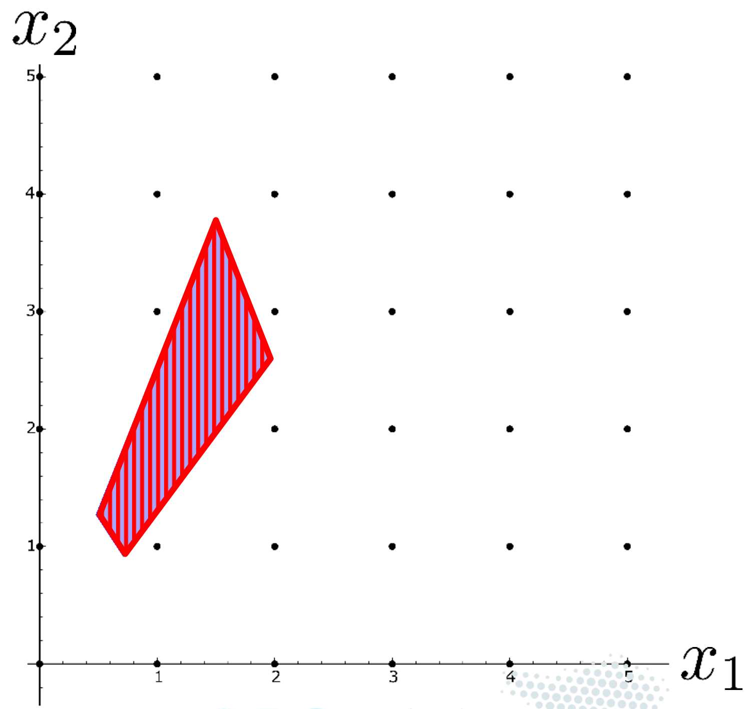
Input: $\{a_i^T x \leq b_i \mid i = 1, \dots, m\}$

Goal: QF_LRA: $x_1, \dots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \dots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \qquad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

$x_1, x_2 \in \mathbb{Q}$ QF_LRA



Theory Solver

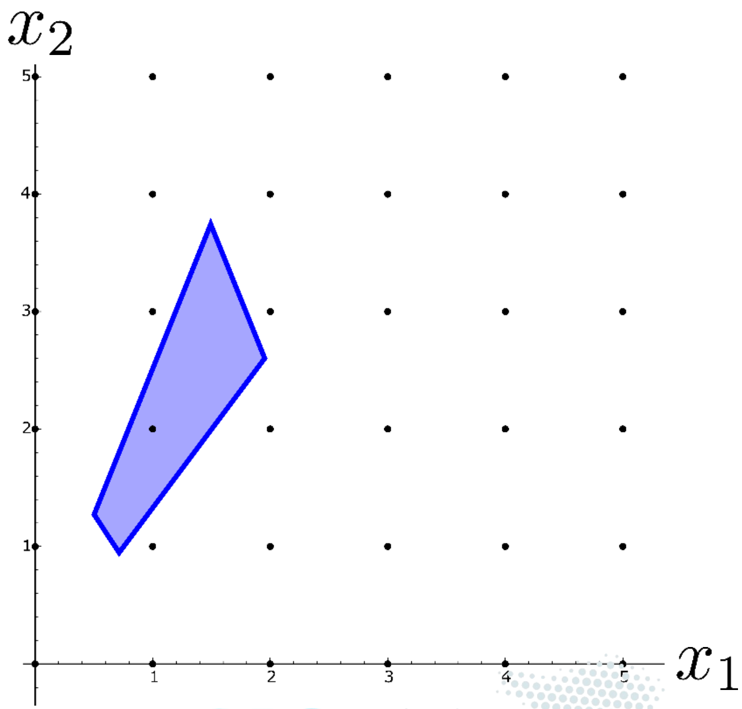
Input: $\{a_i^T x \leq b_i \mid i = 1, \dots, m\}$

Goal: QF_LRA: $x_1, \dots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \dots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \qquad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

$x_1, x_2 \in \mathbb{Z}$ QF_LIA



Theory Solver

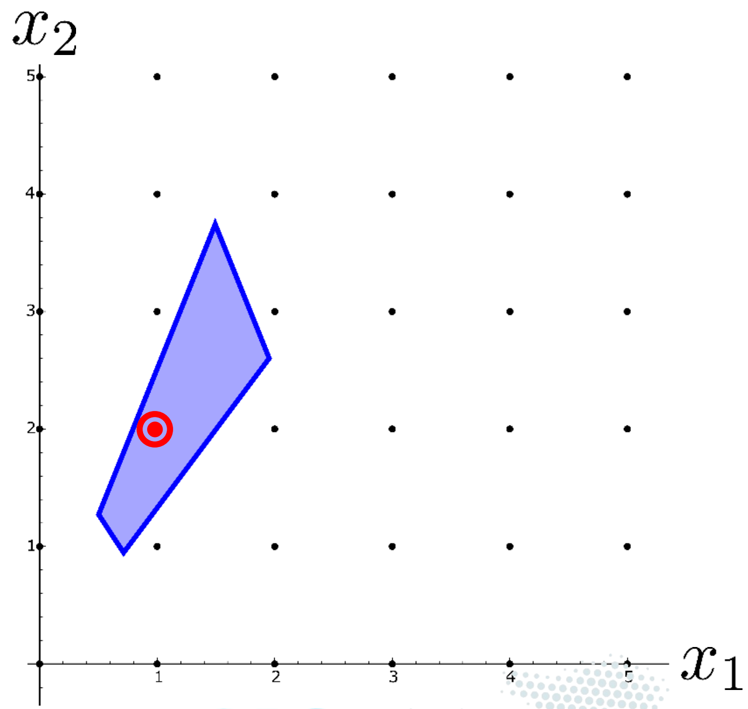
Input: $\{a_i^T x \leq b_i \mid i = 1, \dots, m\}$

Goal: QF_LRA: $x_1, \dots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \dots, x_n \in \mathbb{Z}$

Example:

$$2x_2 \leq 5x_1, \qquad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

$x_1, x_2 \in \mathbb{Z}$ QF_LIA



Theory Solver

Input: $\{a_i^T x \leq b_i \mid i = 1, \dots, m\}$

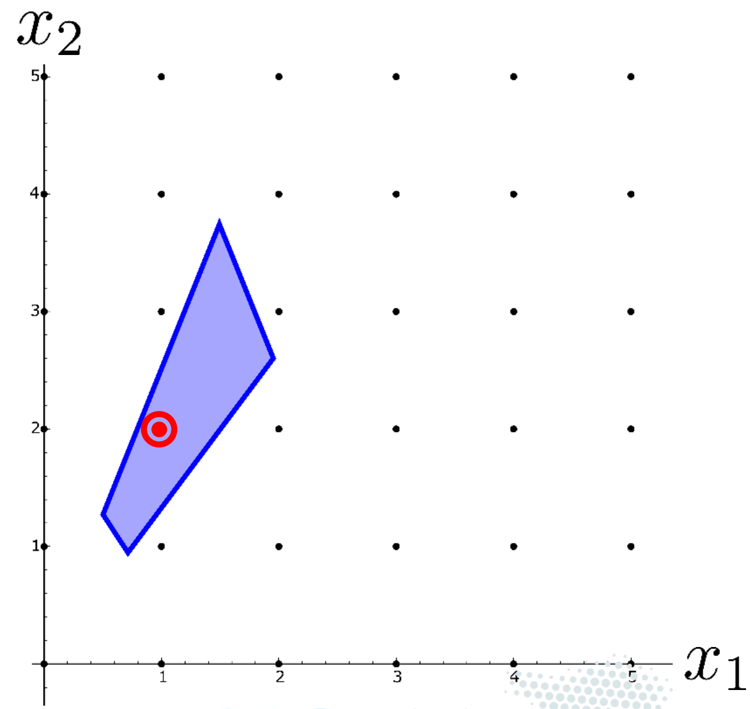
Goal: QF_LRA: $x_1, \dots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \dots, x_n \in \mathbb{Z}$

Solver: QF_LRA: dual simplex
QF_LIA: branch and bound

Example:

$2x_2 \leq 5x_1,$	$3x_2 \geq 4x_1,$
$2x_2 \leq -5x_1 + 15,$	$2x_2 \geq -3x_1 + 4,$

$x_1, x_2 \in \mathbb{Z}$ QF_LIA



Theory Solver

Input: $\{a_i^T x \leq b_i \mid i = 1, \ldots, m\}$

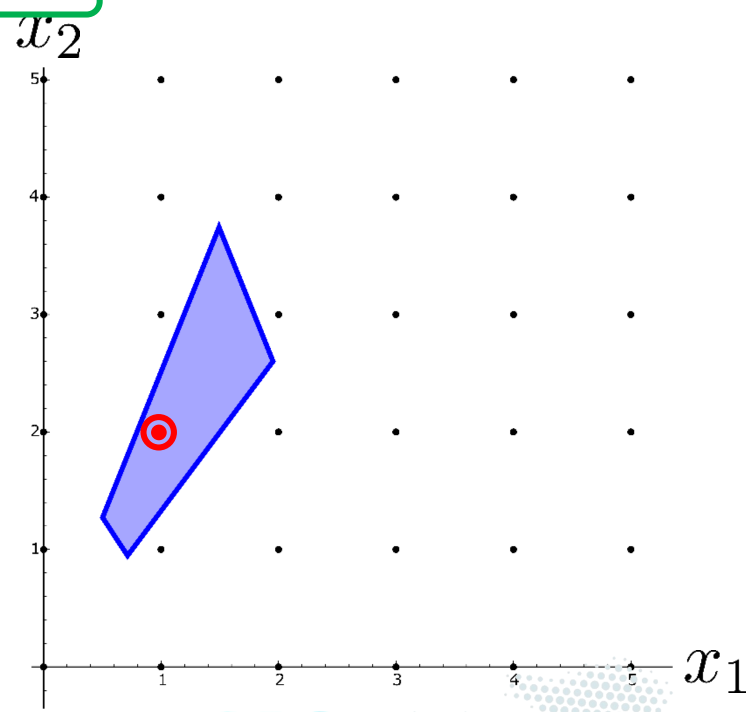
Goal: QF_LRA: $x_1, \ldots, x_n \in \mathbb{Q}$ or QF_LIA: $x_1, \ldots, x_n \in \mathbb{Z}$

Solver: QF_LRA: dual simplex
QF_LIA: branch and bound

Example:

$$2x_2 \leq 5x_1, \qquad 3x_2 \geq 4x_1,$$
$$2x_2 \leq -5x_1 + 15, \quad 2x_2 \geq -3x_1 + 4,$$

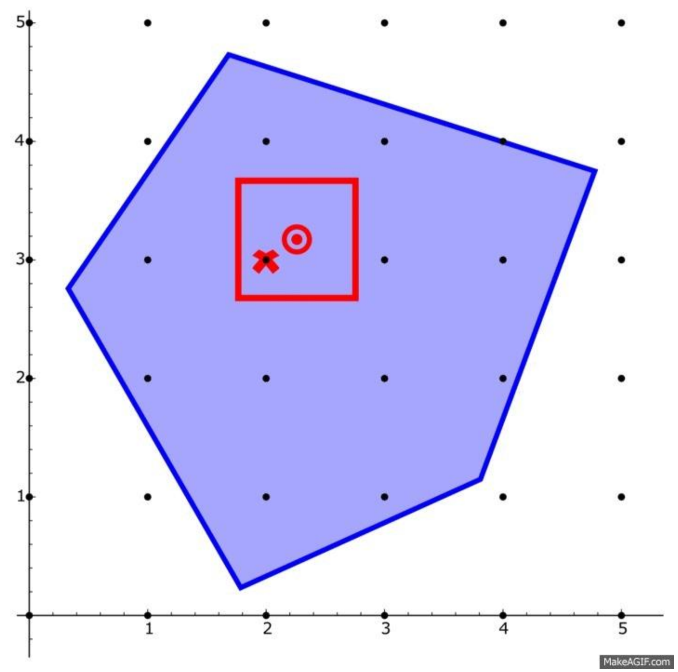
$x_1, x_2 \in \mathbb{Z}$ QF_LIA



Theory Solver Extensions

Unit Cube Test

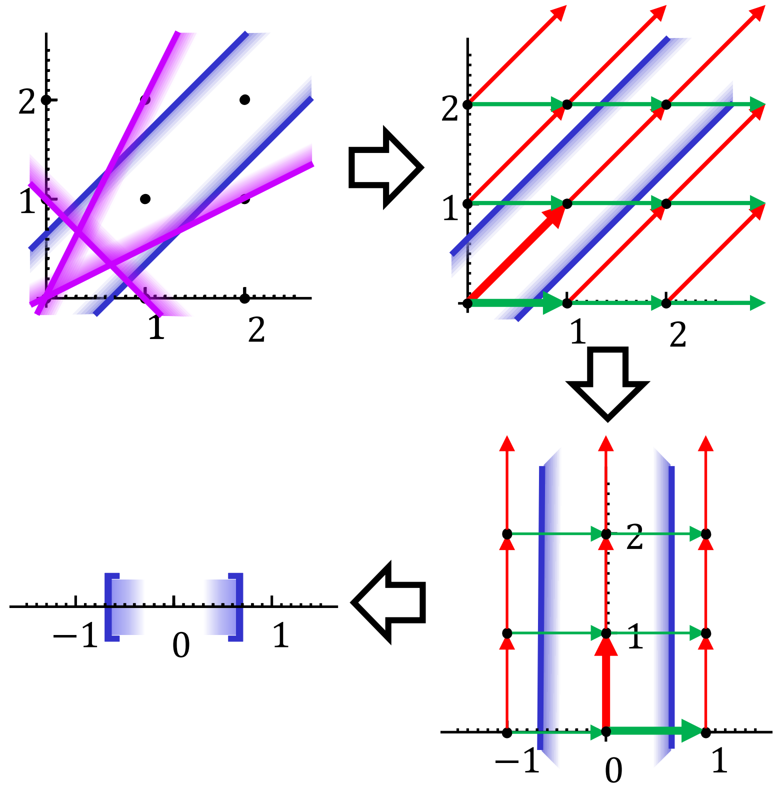
(IJCAR 2016)



for absolutely unbounded problems

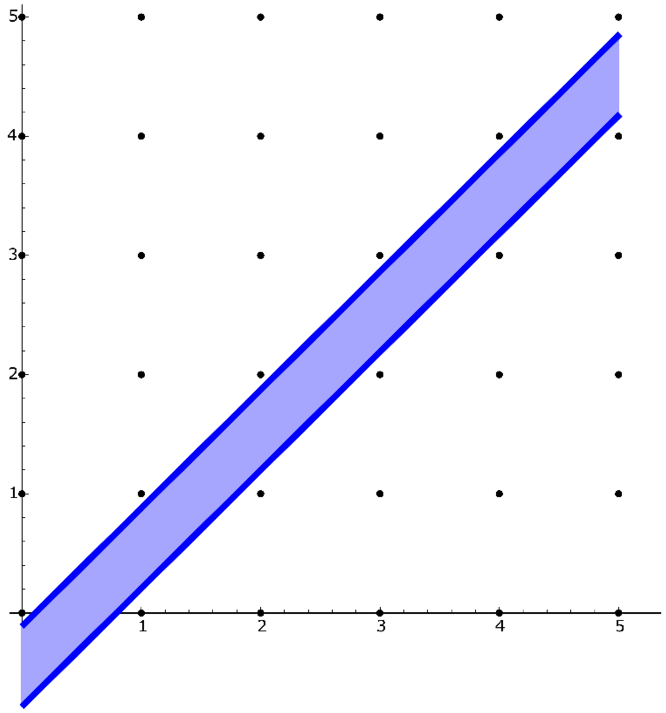
Bounding Transformation

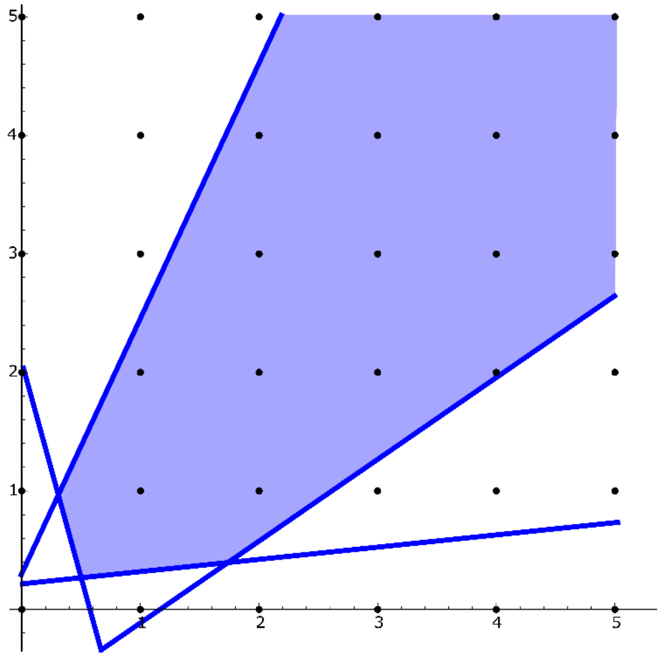
(IJCAR 2018)



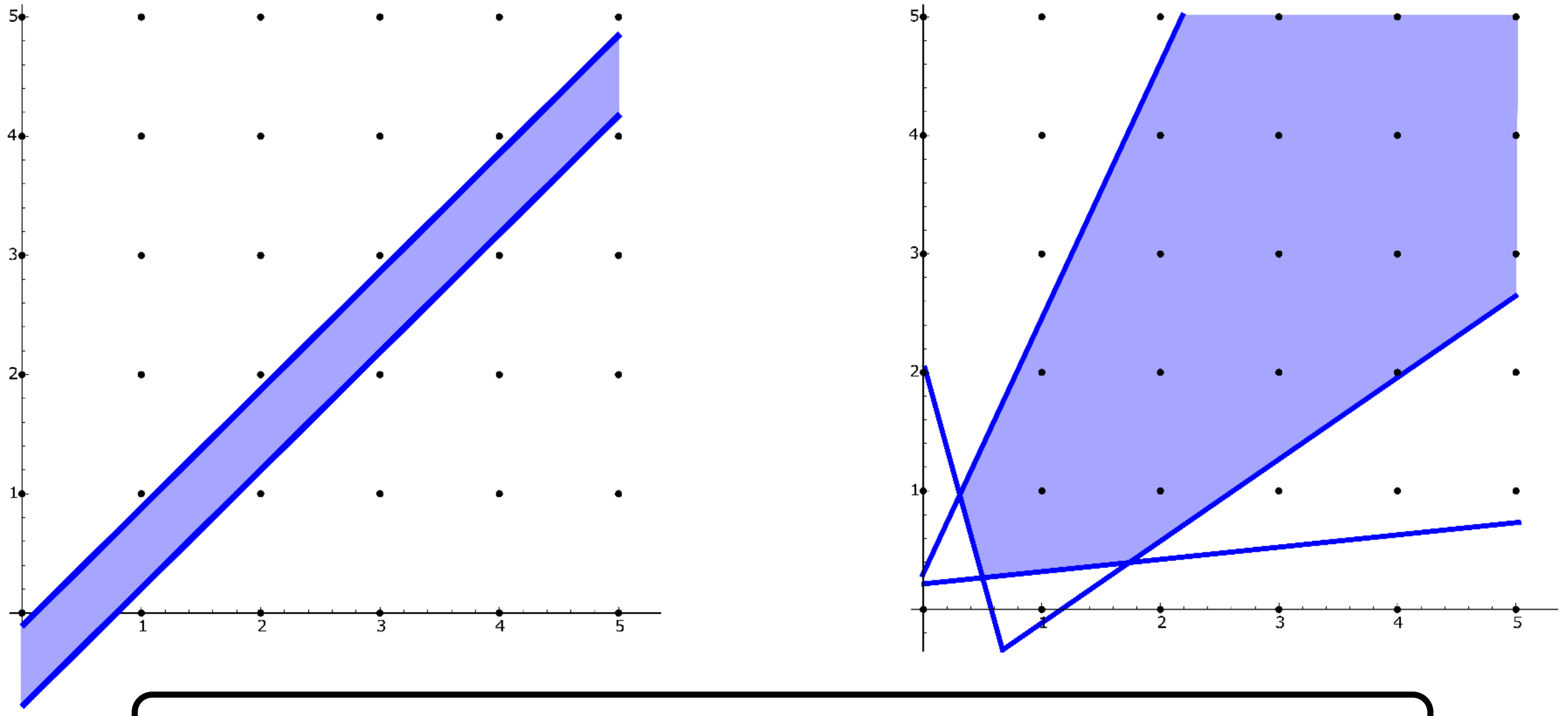
for partially unbounded problems

Unbounded Problems



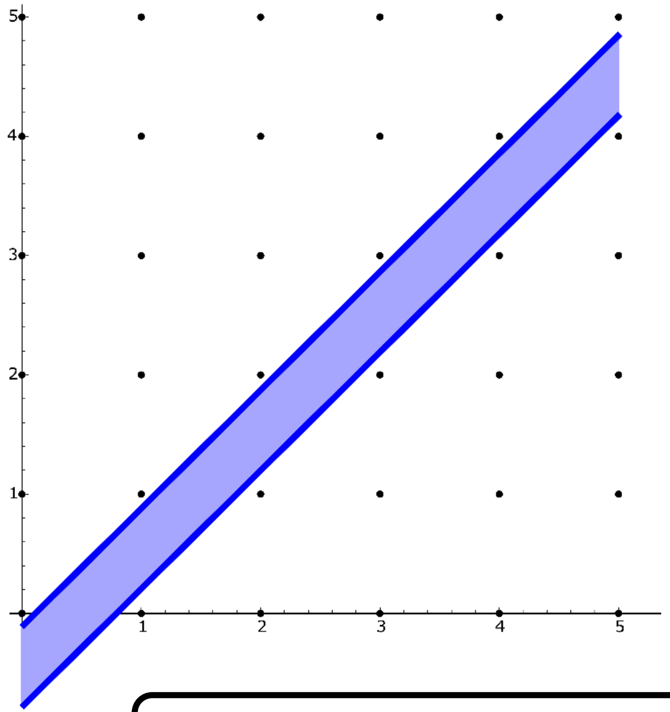


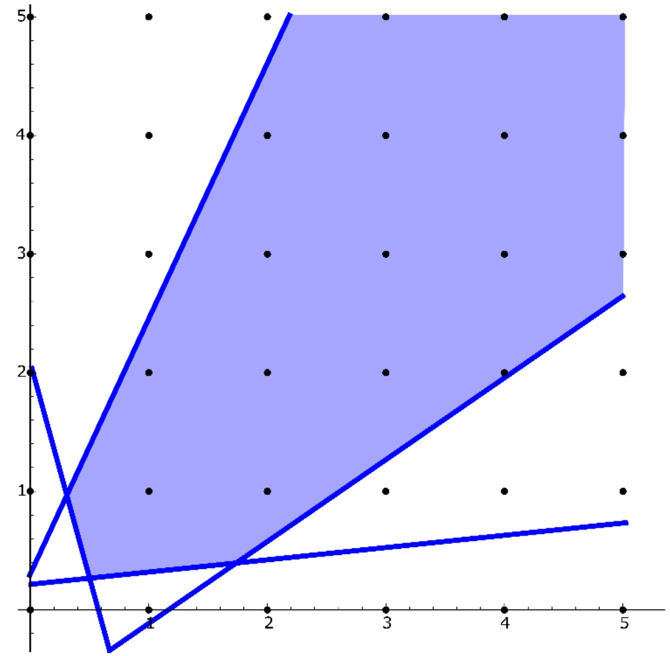
Unbounded Problems



Requirement: unbounded direction

Unbounded Problems





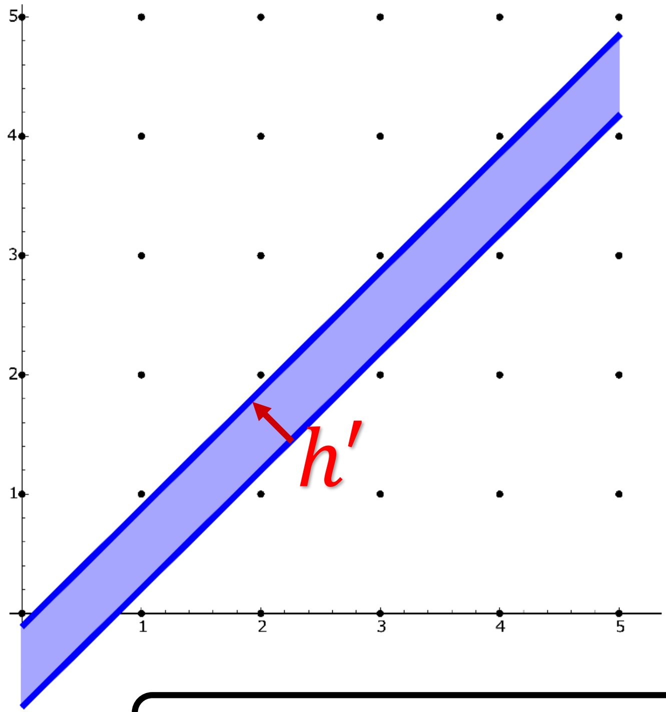
Requirement: unbounded direction

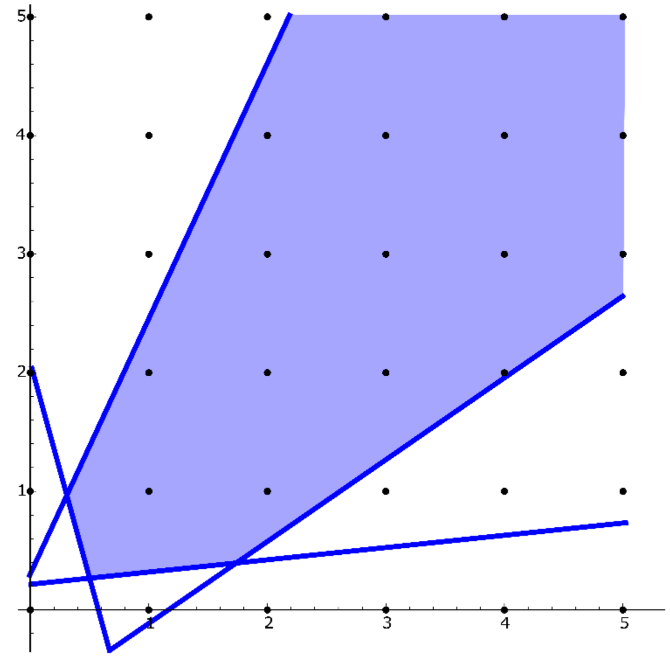
$h \in \mathbb{Q}^n$ is bounded iff

$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n. \left\{a_i^T x \le b_i \,\middle|\, i = 1, \dots, m\right\} \to \boxed{l \le} h^T x \boxed{\le u}$$

lower bound upper bound

Unbounded Problems





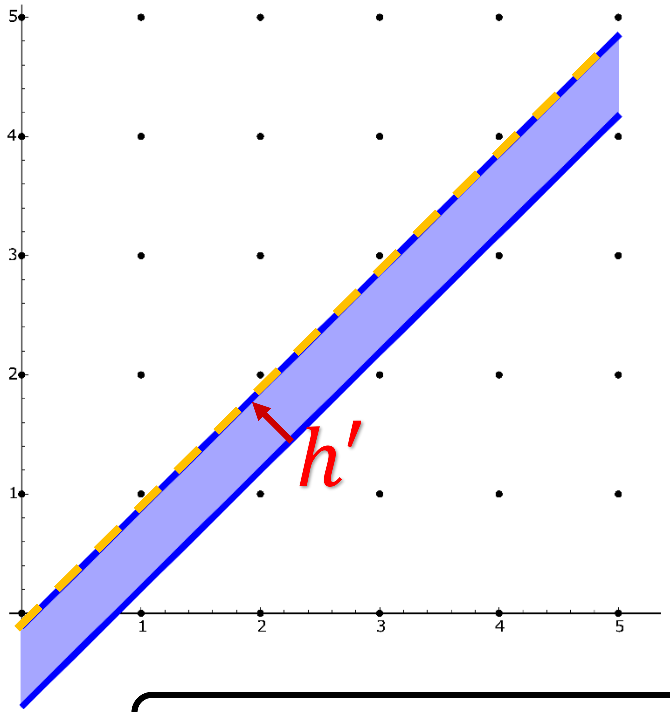
Requirement: unbounded direction

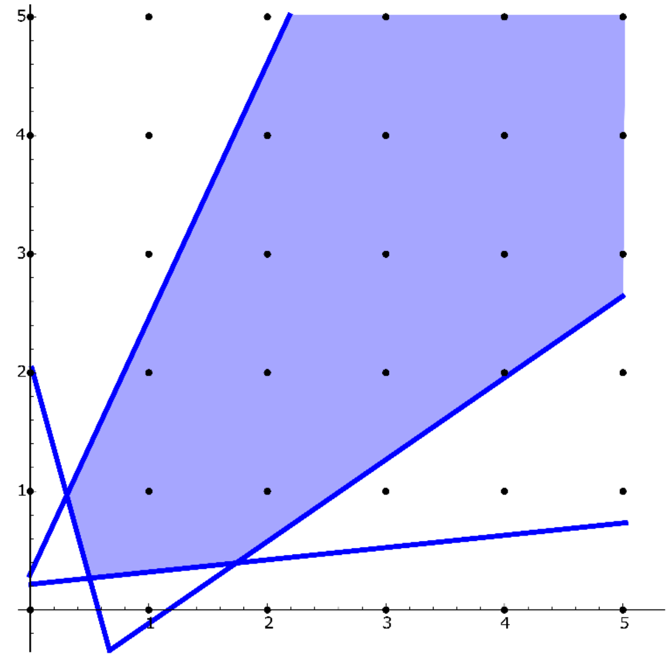
$h \in \mathbb{Q}^n$ is bounded iff

$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n. \{a_i^T x \le b_i \mid i = 1, \ldots, m\} \rightarrow \boxed{l \le} h^T x \boxed{\le u}$$

lower bound upper bound

Unbounded Problems





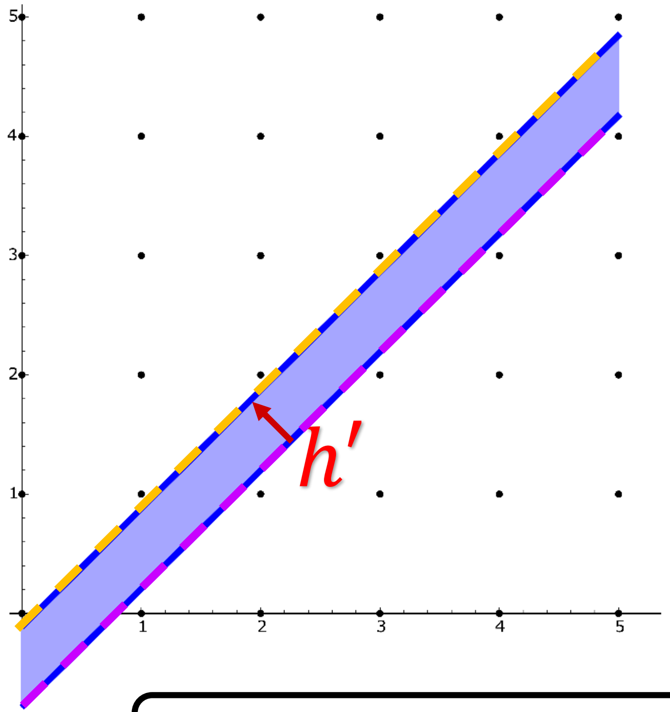
Requirement: unbounded direction

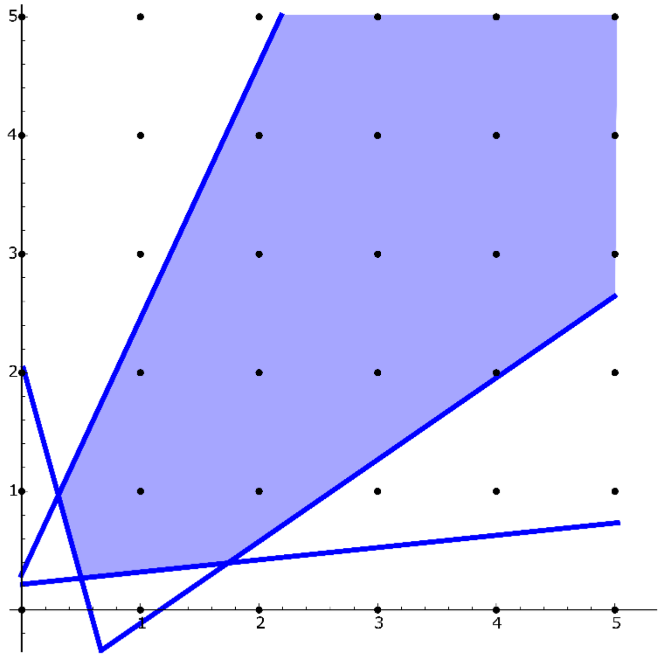
$h \in \mathbb{Q}^n$ is bounded iff

$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n. \{a_i^T x \le b_i \mid i = 1, \dots, m\} \rightarrow \boxed{l \le} h^T x \boxed{\le u}$$

lower bound upper bound

Unbounded Problems





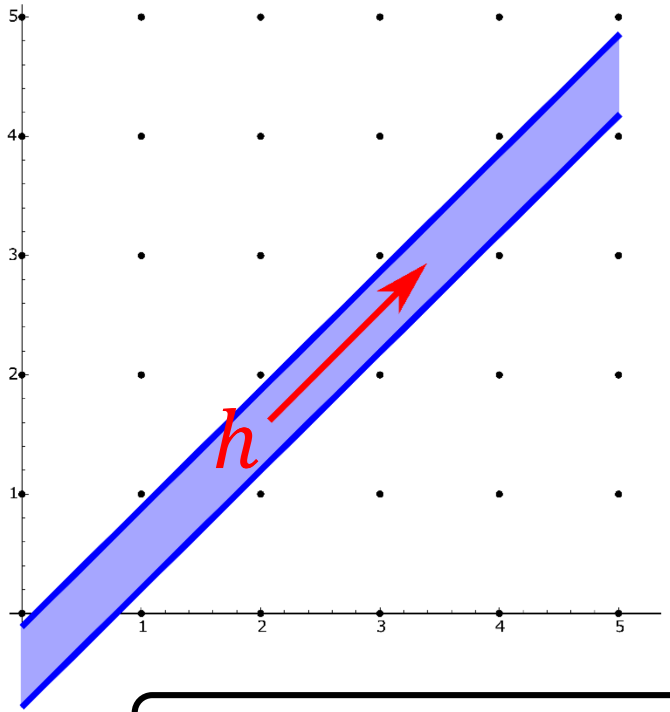
Requirement: unbounded direction

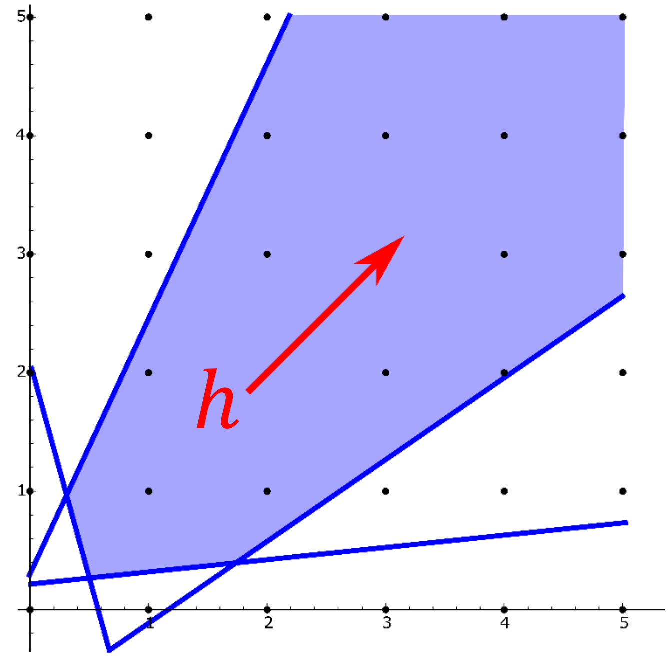
$h \in \mathbb{Q}^n$ is bounded iff

$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n. \{a_i^T x \le b_i \mid i = 1, \dots, m\} \rightarrow \boxed{l \le} h^T x \boxed{\le u}$$

lower bound upper bound

Unbounded Problems





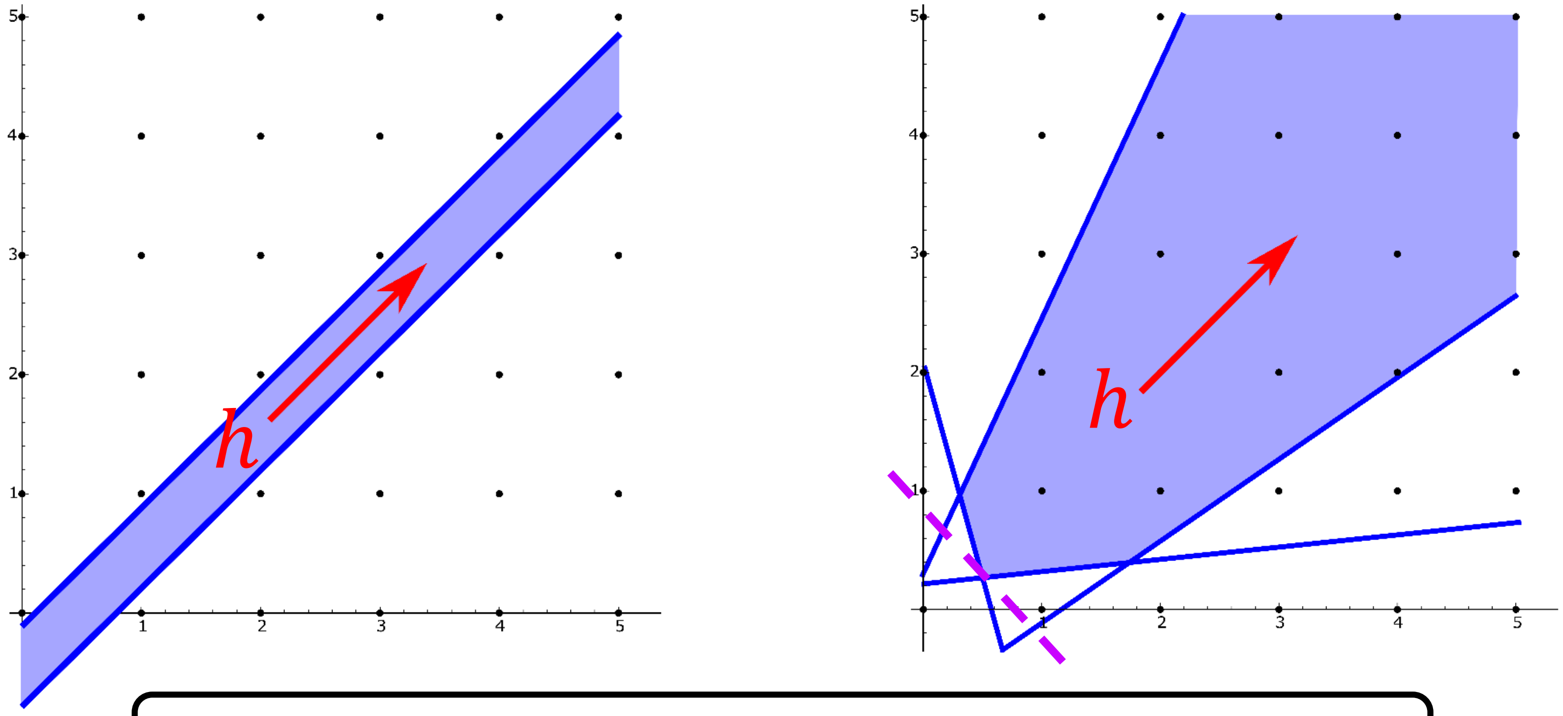
Requirement: unbounded direction

$h \in \mathbb{Q}^n$ is bounded iff

$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n. \{a_i^T x \leq b_i \mid i = 1, \dots, m\} \rightarrow \boxed{l \leq} h^T x \boxed{\leq u}$$

lower bound upper bound

Unbounded Problems



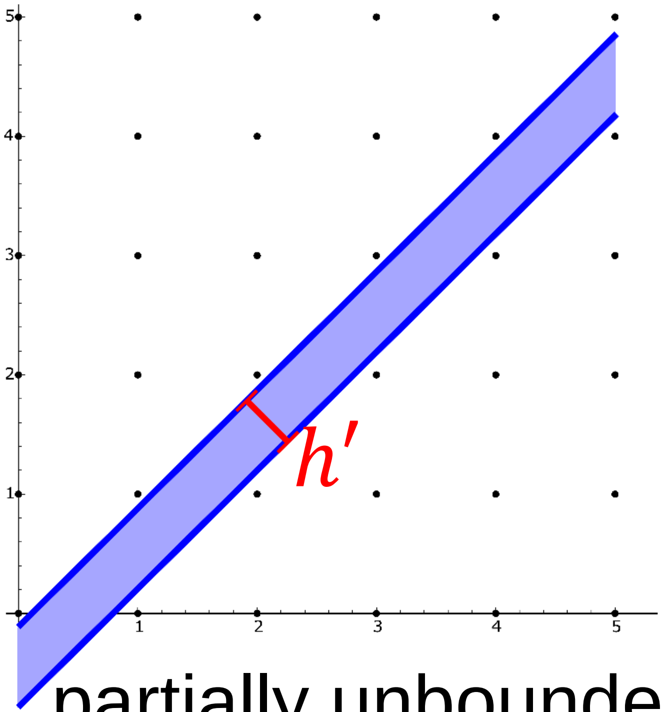
Requirement: unbounded direction

$h \in \mathbb{Q}^n$ is bounded iff

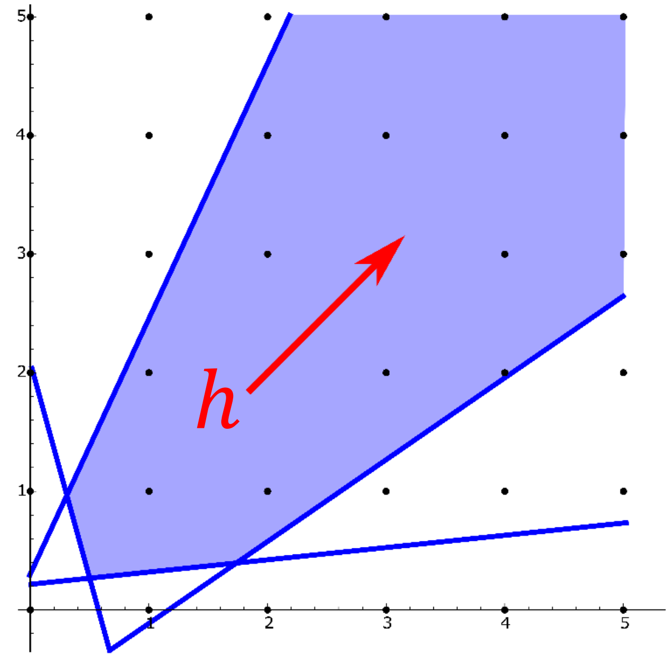
$$\exists l, u \in \mathbb{Z}.\ \forall x \in \mathbb{Q}^n.\ \{a_i^T x \leq b_i \mid i = 1, \ldots, m\} \rightarrow \boxed{l \leq} h^T x \boxed{\leq u}$$

lower bound upper bound

Unbounded Problems

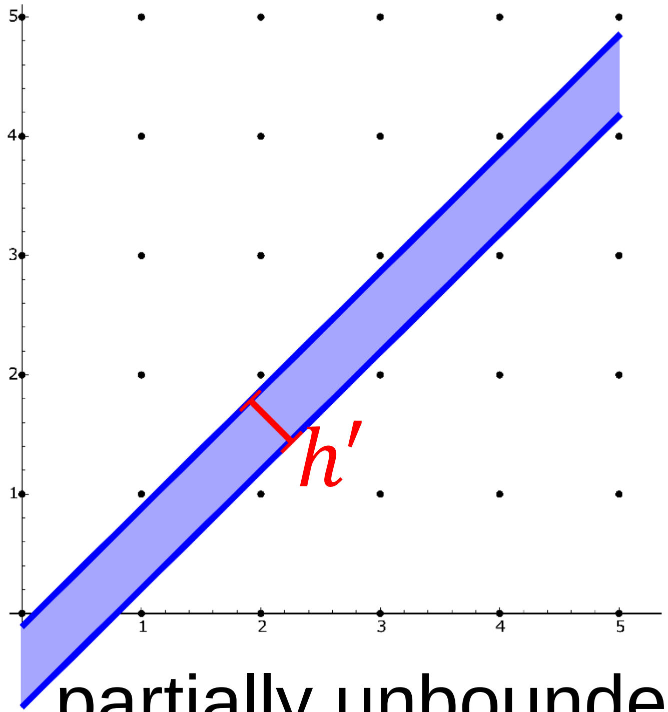


partially unbounded

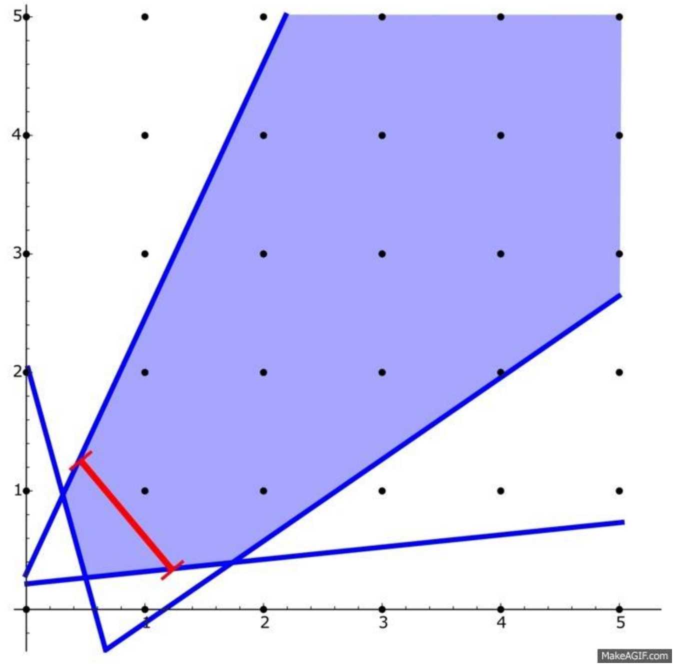


partially unbounded:
both bounded and unbounded directions

Unbounded Problems



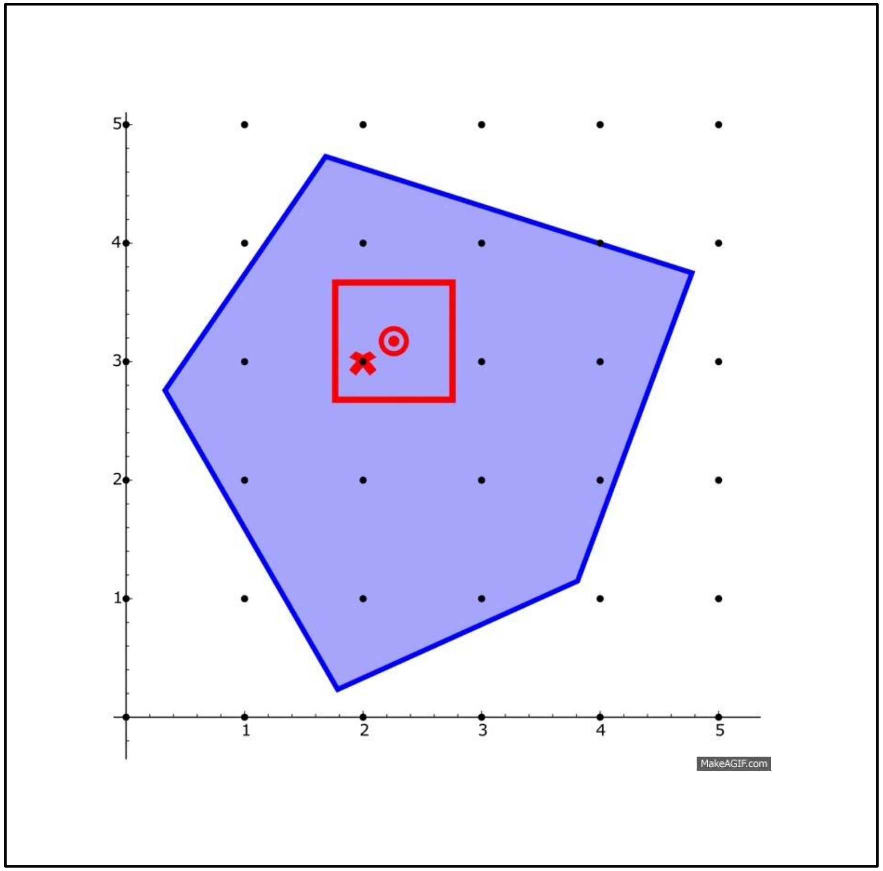
partially unbounded



absolutely unbounded

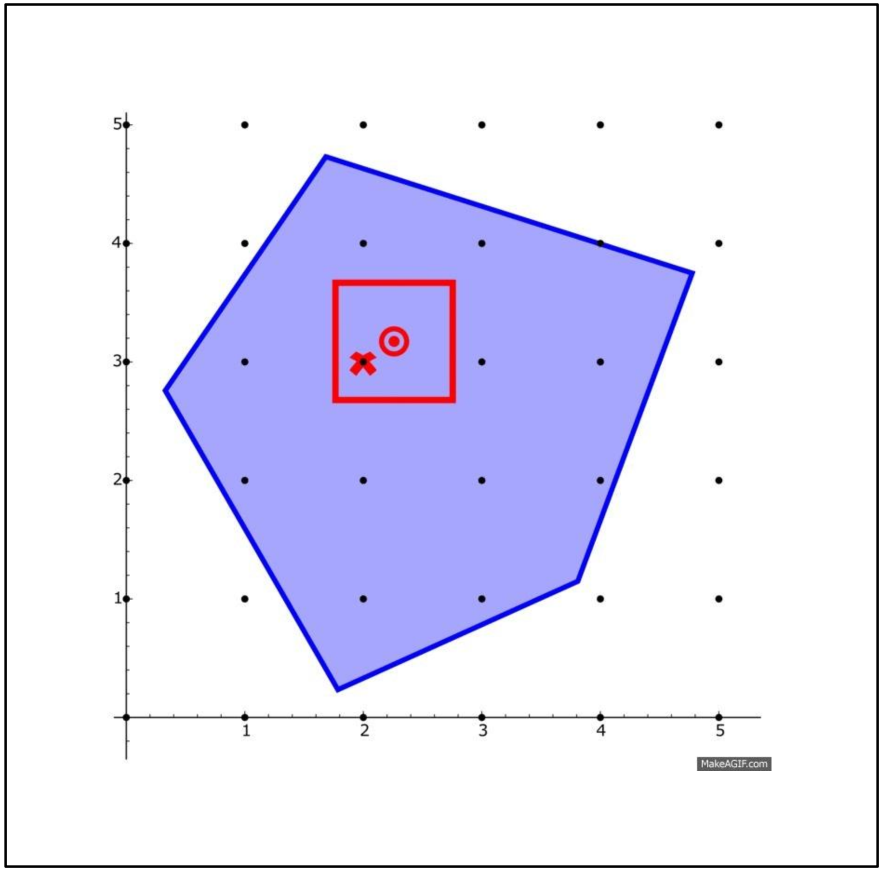
absolutely unbounded:
only unbounded directions

Overview: Unit Cube Test
(IJCAR 2016)



for absolutely unbounded problems

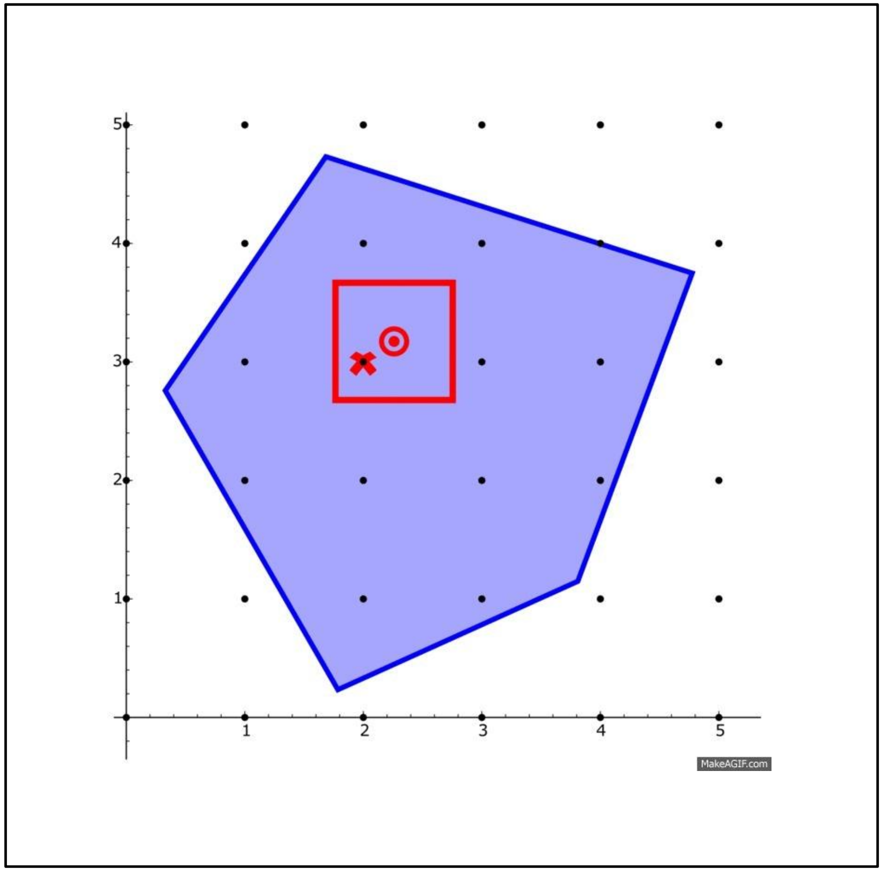
Overview: Unit Cube Test
(IJCAR 2016)



for absolutely unbounded problems

- **unit cube** guarantees integer solution

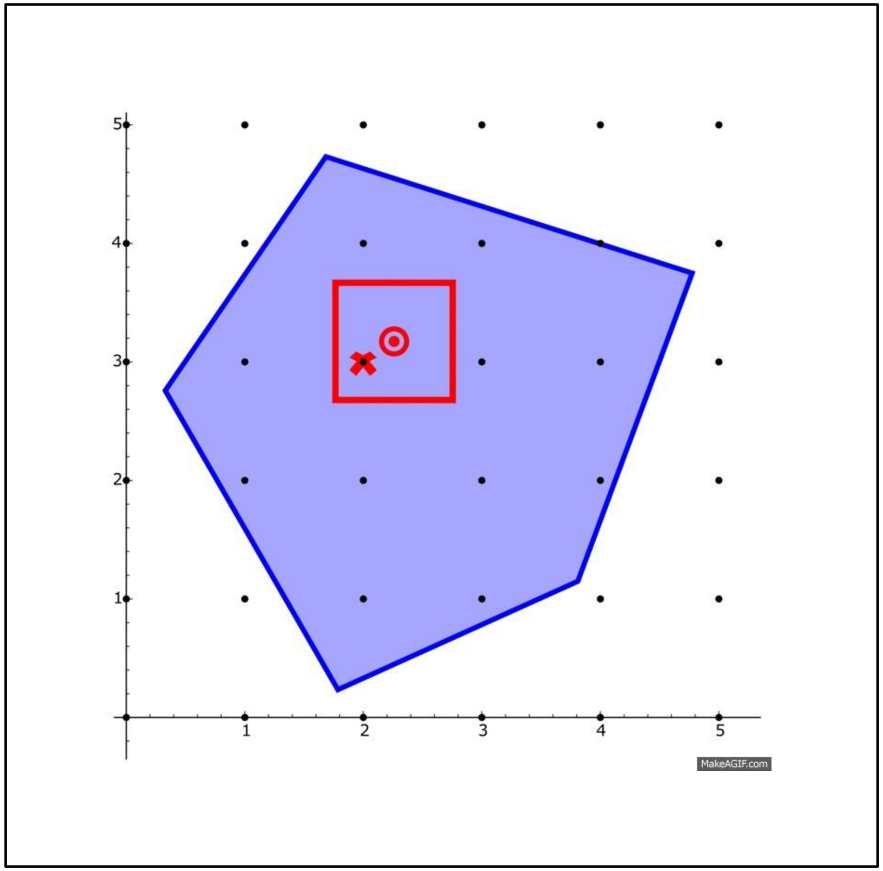
Overview: Unit Cube Test
(IJCAR 2016)



for absolutely unbounded problems

- **unit cube** guarantees integer solution
- computable in **polynomial time**

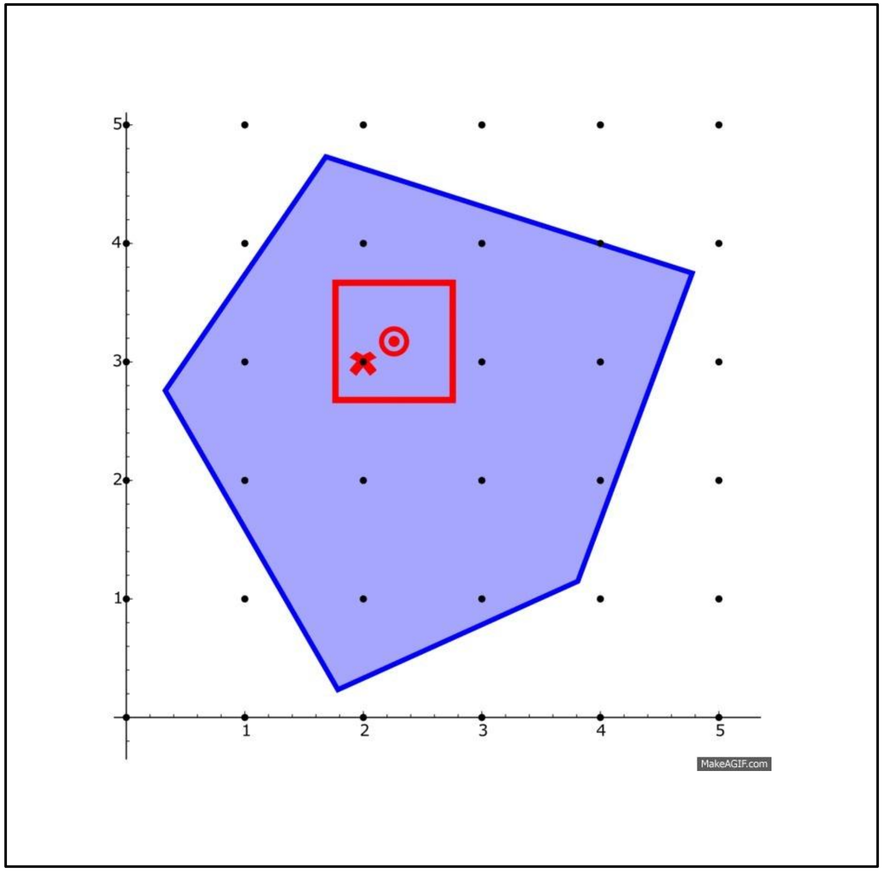
Overview: Unit Cube Test
(IJCAR 2016)



- **unit cube** guarantees integer solution
- computable in **polynomial time**
- **incremental**

for absolutely unbounded problems

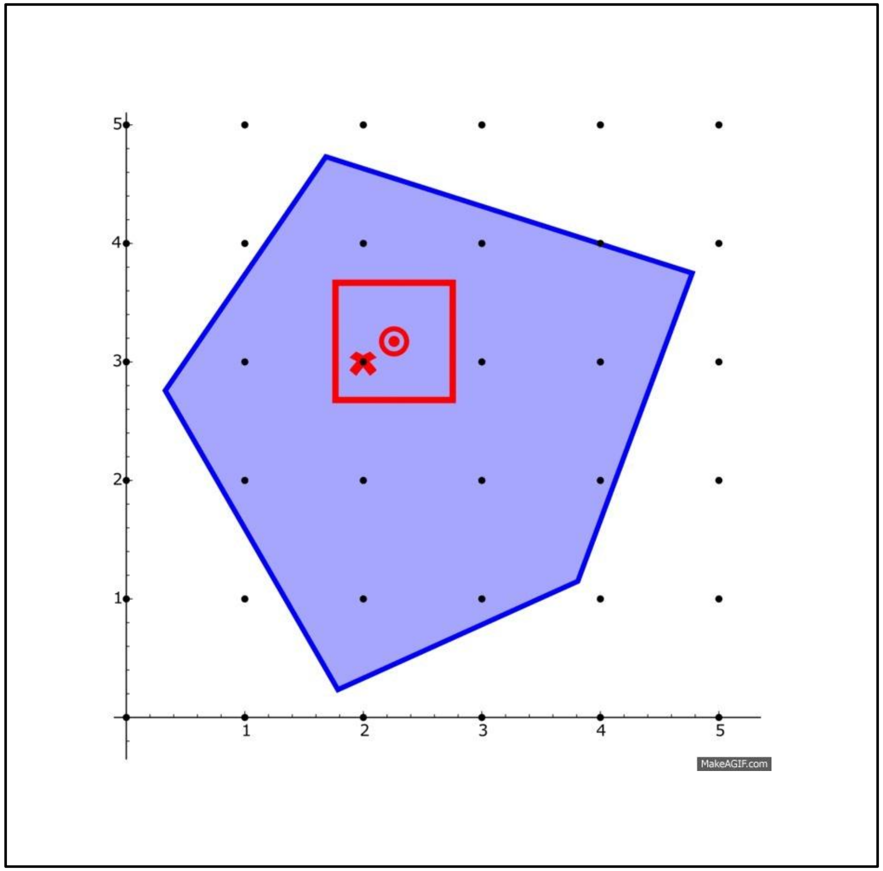
Overview: Unit Cube Test
(IJCAR 2016)



for absolutely unbounded problems

- **unit cube** guarantees integer solution
- computable in **polynomial time**
- **incremental**
- **not complete** in general

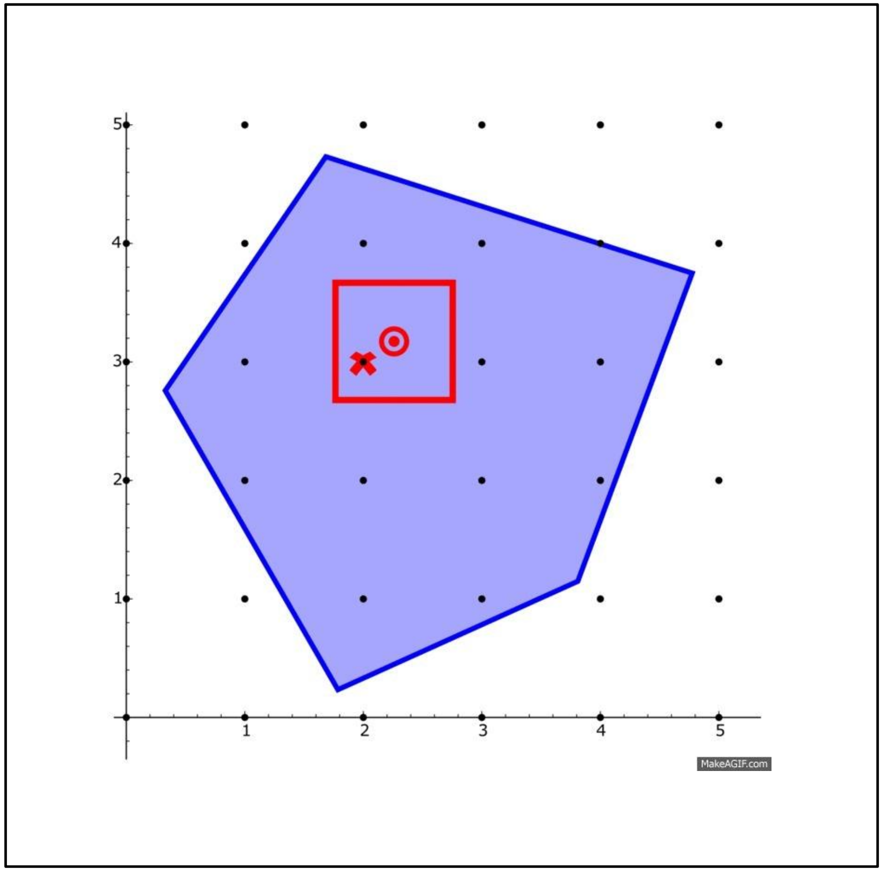
Overview: Unit Cube Test
(IJCAR 2016)



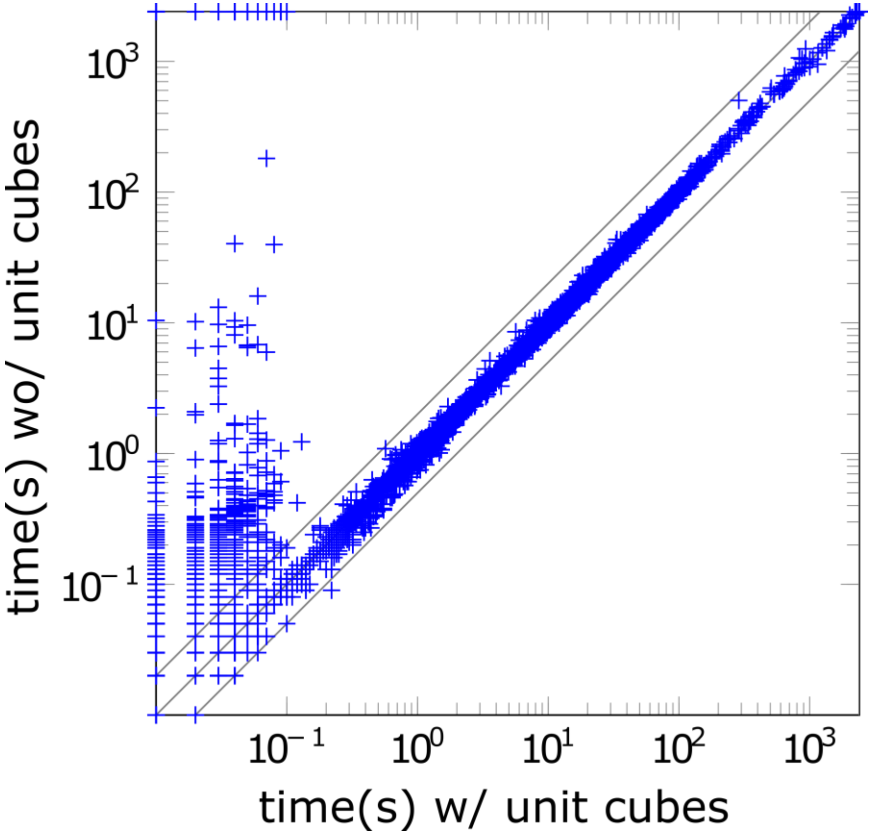
for absolutely unbounded problems

- **unit cube** guarantees integer solution
- computable in **polynomial time**
- **incremental**
- **not complete** in general
- always succeeds on abs. unbd. problems

Results: Unit Cube Test
(IJCAR 2016)



QF_LIA (6947 problems)

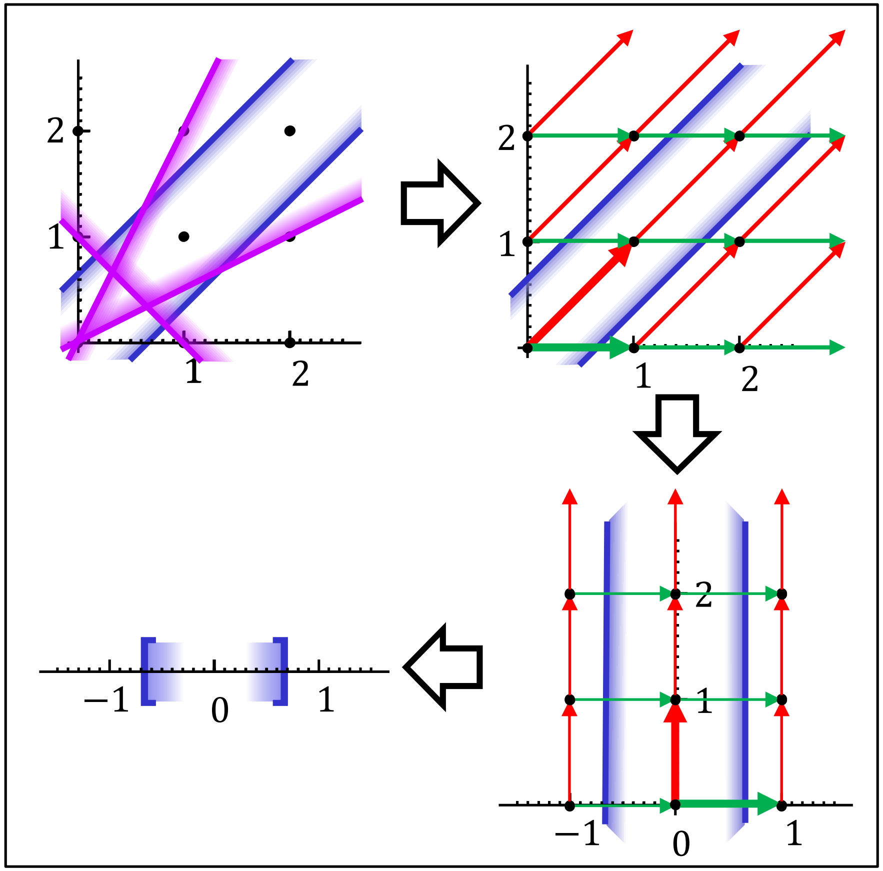


for absolutely unbounded problems

additional instances: 56

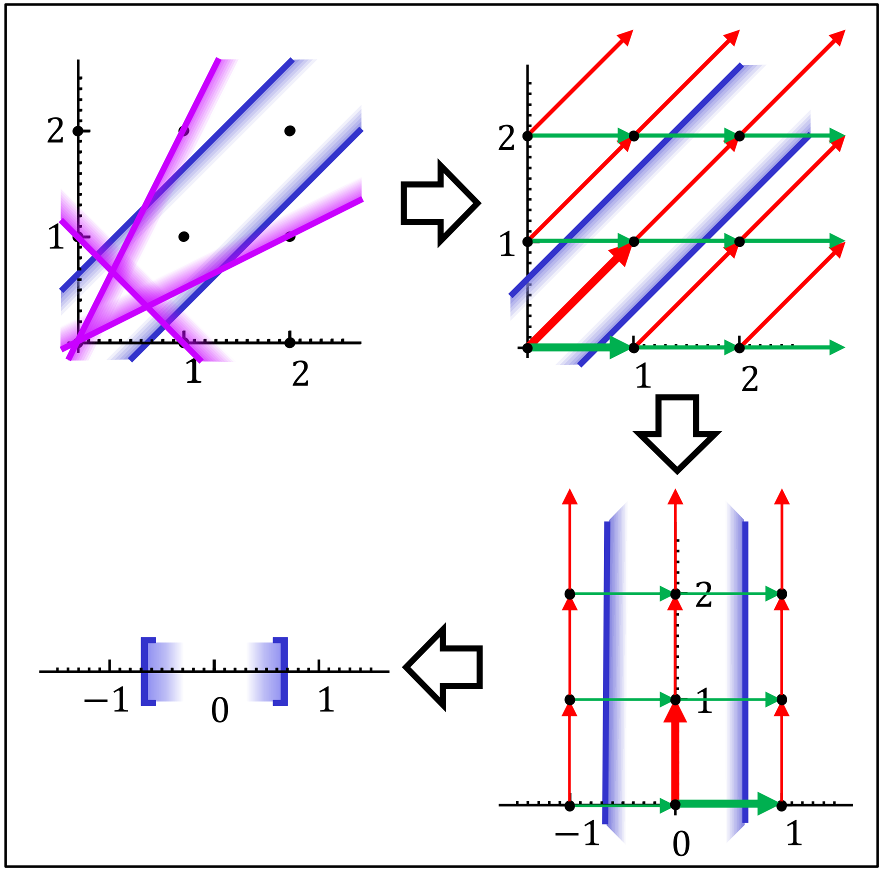
more than twice as fast: 705

Overview: Bounding Transformation
(IJCAR 2018)



for partially unbounded problems

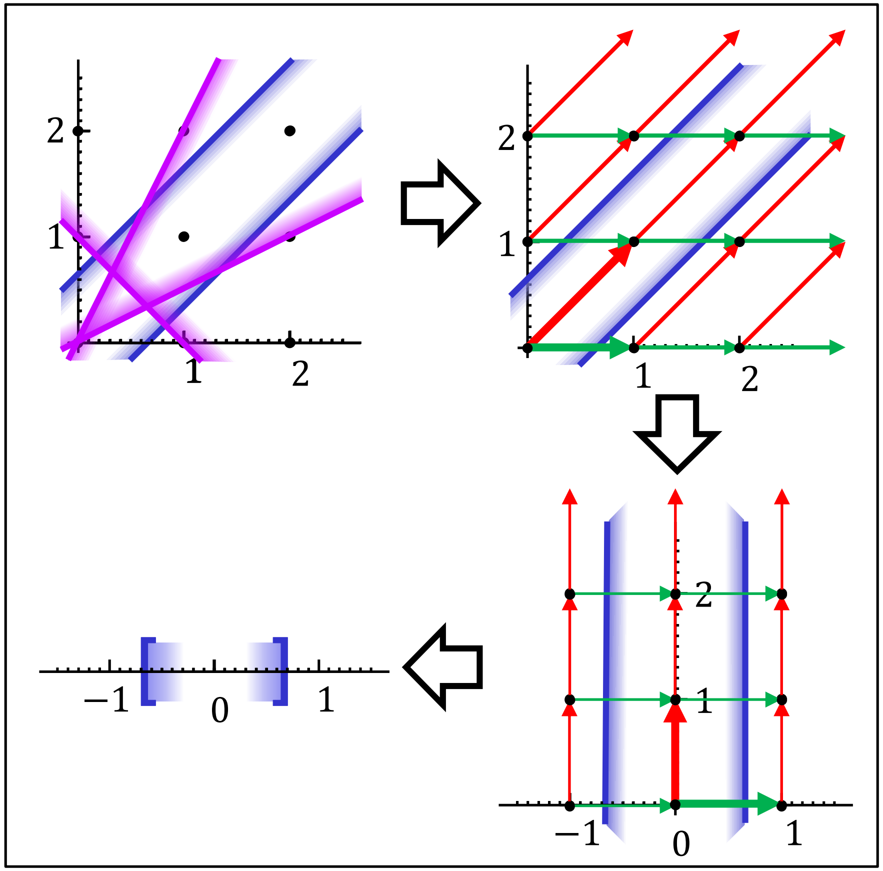
Overview: Bounding Transformation
(IJCAR 2018)



for partially unbounded problems

- transforms **unbounded into bounded** problems

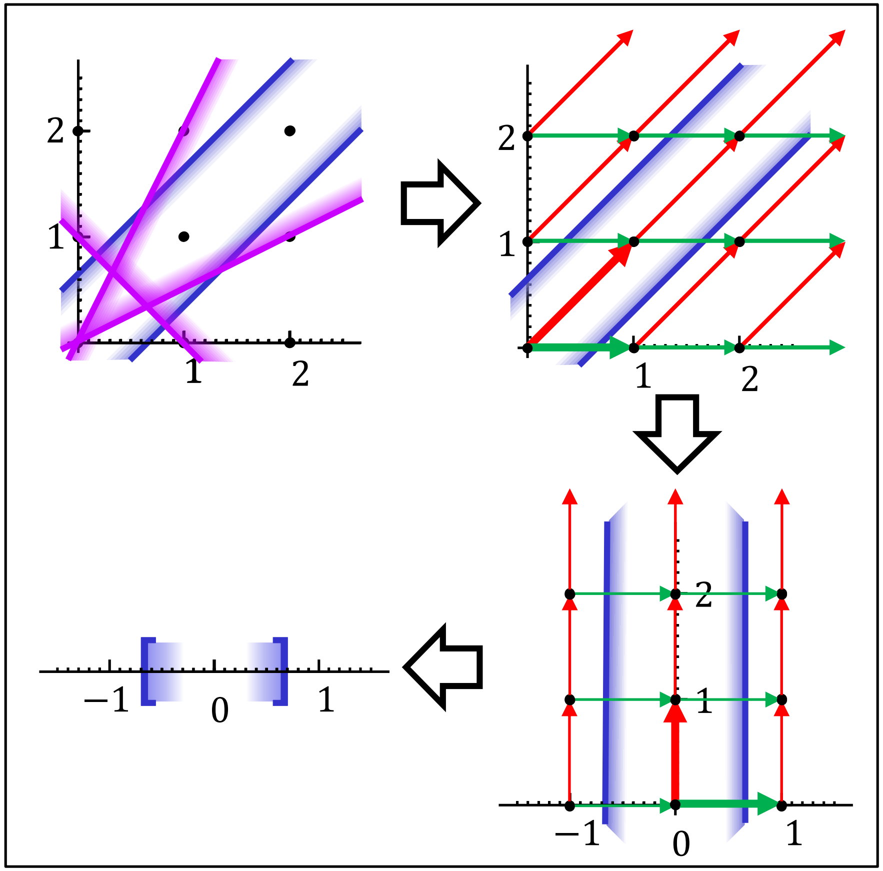
Overview: Bounding Transformation
(IJCAR 2018)



for partially unbounded problems

- transforms **unbounded into bounded** problems
- computable in **polynomial time**

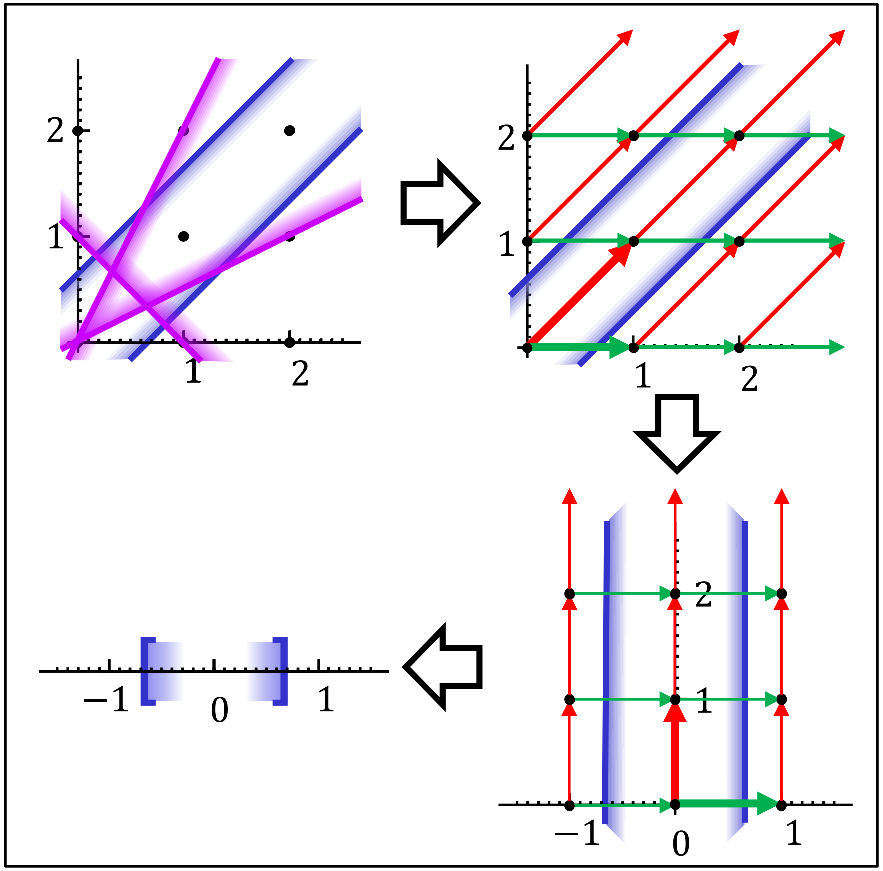
Overview: Bounding Transformation
(IJCAR 2018)



for partially unbounded problems

- transforms **unbounded into bounded** problems
- computable in **polynomial time**
- **solution & conflict conversion** (polynomial time)

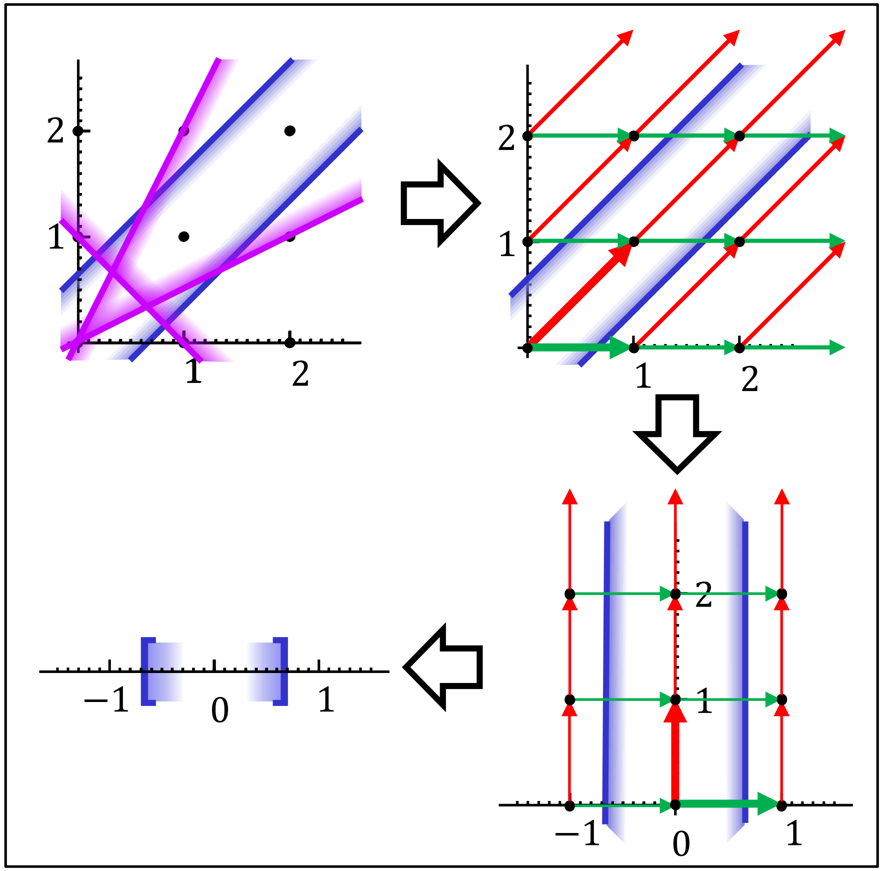
Overview: Bounding Transformation
(IJCAR 2018)

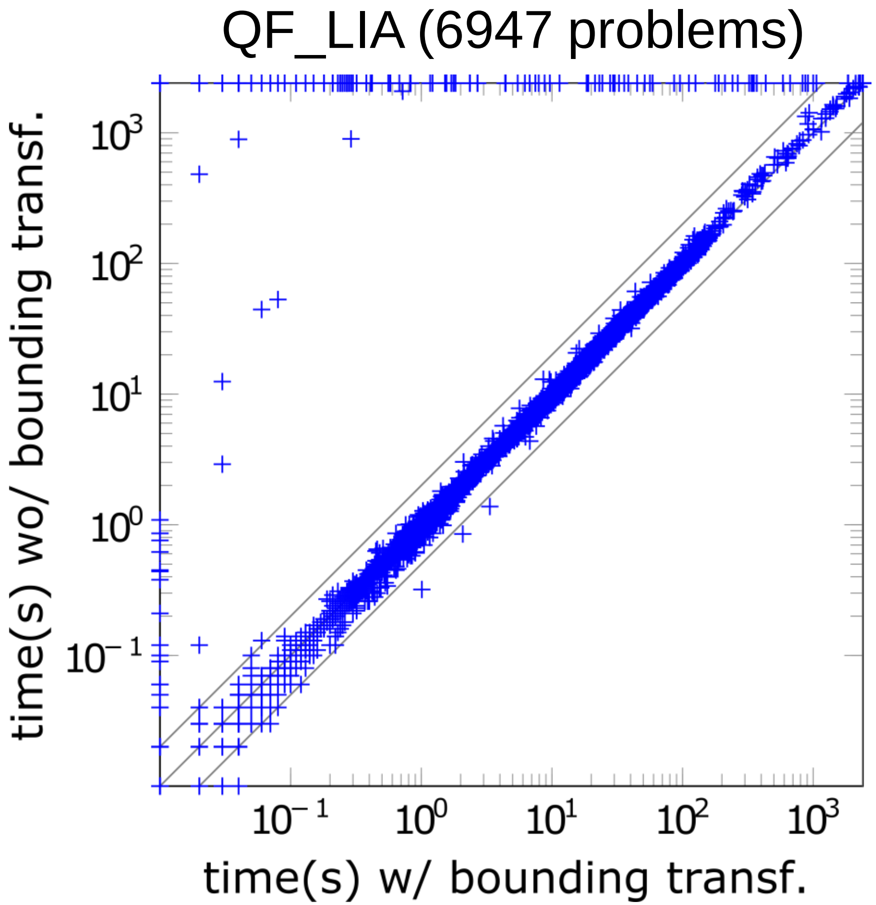


for partially unbounded problems

- transforms **unbounded into bounded** problems
- computable in **polynomial time**
- **solution & conflict conversion** (polynomial time)
- **incremental**

Results: Bounding Transformation
(IJCAR 2018)





for partially unbounded problems

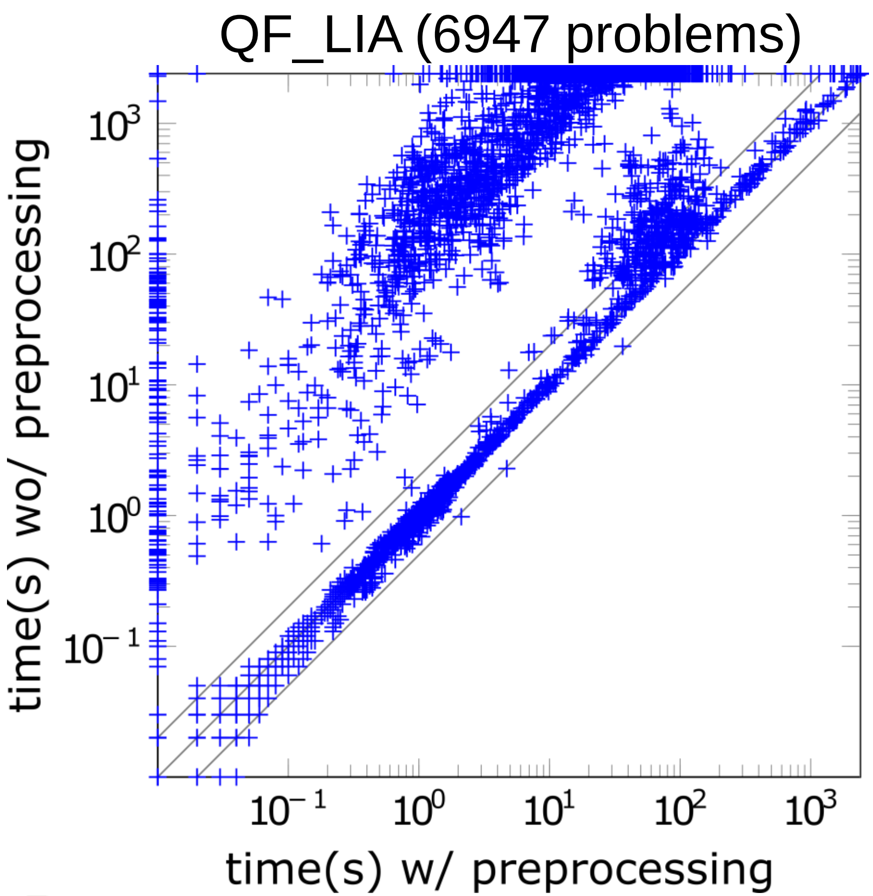
additional instances: 169
more than twice as fast: 167

Preprocessing:

- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]

Preprocessing:

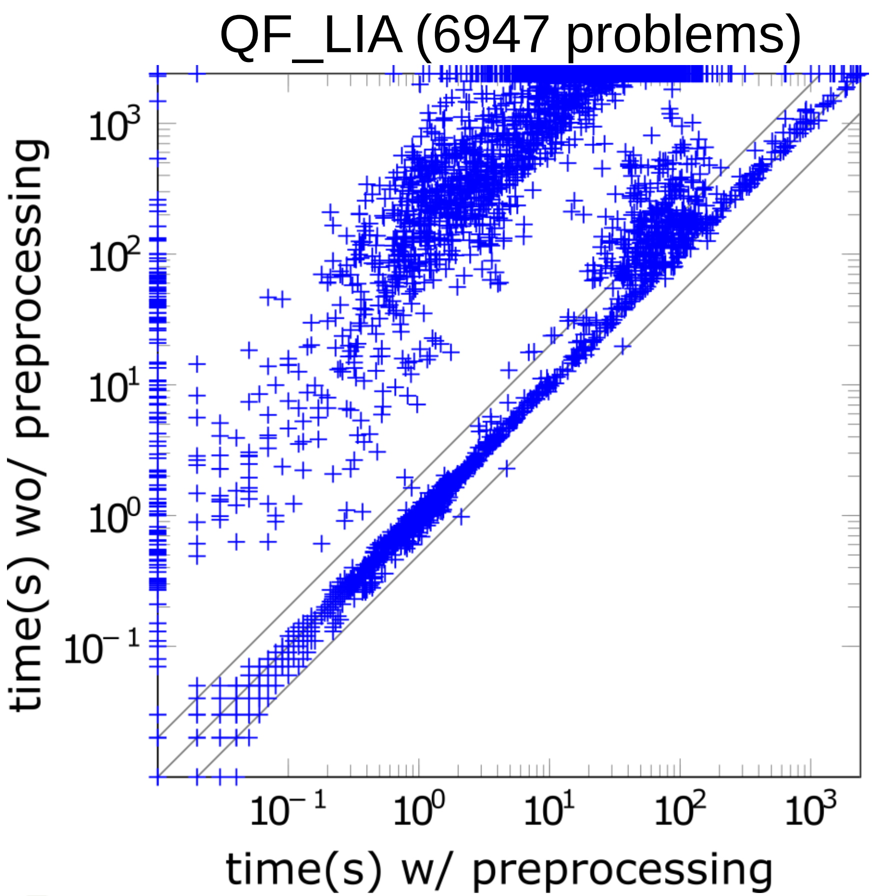
- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]



additional instances:1776

Preprocessing:

- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]



additional instances:1776

Modular Arithmetic

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

UNSAT

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

UNSAT

Proof by case distinction:

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

UNSAT

Proof by case distinction:

$x = 3 \cdot k$ for $k \in \mathbb{Z}$ $\qquad 0 \equiv_9 3 \cdot (3 \cdot k)$

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

UNSAT

Proof by case distinction:

$x = 3 \cdot k$ for $k \in \mathbb{Z}$ $\qquad 0 \equiv_9 3 \cdot (3 \cdot k)$

$x = 3 \cdot k + 1$ for $k \in \mathbb{Z}$ $\qquad 3 \equiv_9 3 \cdot (3 \cdot k + 1)$

max planck institut informatik

SIC Saarland Informatics Campus

Modular Arithmetic

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

UNSAT

Proof by case distinction:

$x = 3 \cdot k$ for $k \in \mathbb{Z}$ $\quad 0 \equiv_9 3 \cdot (3 \cdot k)$

$x = 3 \cdot k + 1$ for $k \in \mathbb{Z}$ $\quad 3 \equiv_9 3 \cdot (3 \cdot k + 1)$

$x = 3 \cdot k + 2$ for $k \in \mathbb{Z}$ $\quad 6 \equiv_9 3 \cdot (3 \cdot k + 2)$

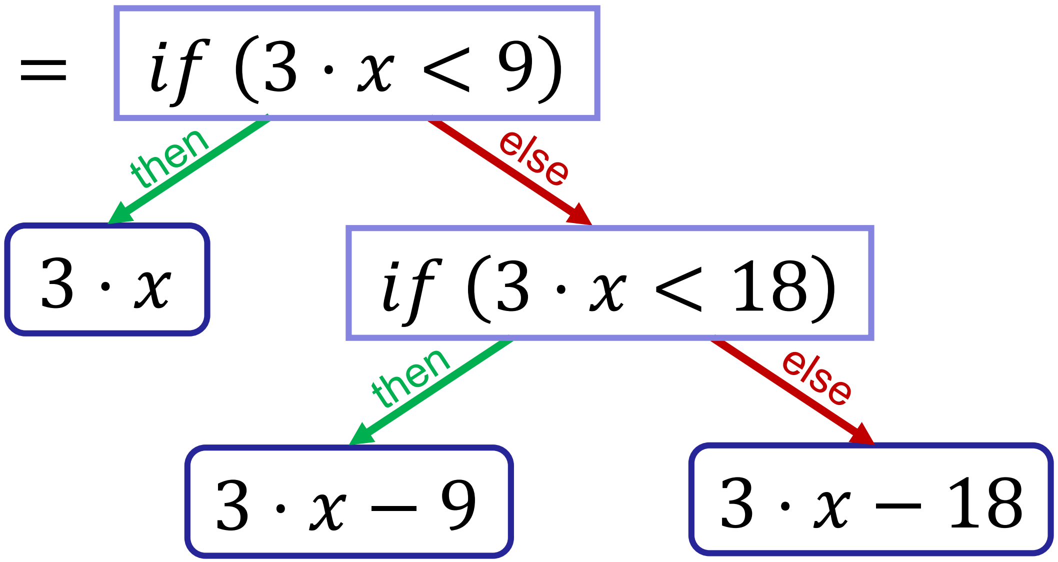
Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad \textit{for } x \in \mathbb{Z}$$

Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

$$0 \leq x < 9 \qquad \wedge \qquad 2 =$$



Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x, y \in \mathbb{Z}$$

$$0 \le x < 9 \quad \wedge \quad 2 = \boxed{if\ (3 \cdot x < 9)}$$

then: $\boxed{3 \cdot x}$

else: $\boxed{y}$

$$\wedge \quad \boxed{if\ (3 \cdot x < 18)}$$

then: $\boxed{y = 3 \cdot x - 9}$

else: $\boxed{y = 3 \cdot x - 18}$

Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad \mathit{for}\ x, y \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \wedge \quad 2 = \boxed{\mathit{if}\ (3 \cdot x < 9)}$$

$$\text{then: } \boxed{3 \cdot x} \qquad \text{else: } \boxed{y}$$

$$\wedge \quad \boxed{(\boxed{(3 \cdot x < 18)} \ \vee\ \boxed{(y = 3 \cdot x - 18)})}$$

$$\wedge \quad \boxed{(\boxed{\neg(3 \cdot x < 18)} \ \vee\ \boxed{(y = 3 \cdot x - 9)})}$$

Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x, y, z \in \mathbb{Z}$$

$$0 \leq x < 9 \qquad \wedge \qquad 2 = z$$

$$\wedge \qquad \boxed{if\ (3 \cdot x < 9)}$$

then: $\boxed{z = 3 \cdot x}$ else: $\boxed{z = y}$

$$\wedge \quad (\boxed{(3 \cdot x < 18)} \quad \vee \quad \boxed{(y = 3 \cdot x - 18)})$$

$$\wedge \quad (\boxed{\neg(3 \cdot x < 18)} \quad \vee \quad \boxed{(y = 3 \cdot x - 9)})$$

Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x, y, z \in \mathbb{Z}$$

$$0 \leq x < 9 \qquad \wedge \qquad 2 = z$$

$$\wedge \quad \boxed{(\boxed{(3 \cdot x < 9)} \quad \vee \quad \boxed{(z = 3 \cdot x)})}$$

$$\wedge \quad \boxed{(\boxed{\neg(3 \cdot x < 9)} \quad \vee \quad \boxed{(z = y)})}$$

$$\wedge \quad \boxed{(\boxed{(3 \cdot x < 18)} \quad \vee \quad \boxed{(y = 3 \cdot x - 18)})}$$

$$\wedge \quad \boxed{(\boxed{\neg(3 \cdot x < 18)} \quad \vee \quad \boxed{(y = 3 \cdot x - 9)})}$$

Modular Arithmetic via If-Then-Else

$$2 \equiv_9 3 \cdot x \qquad\qquad \mathit{for}\ x, y, z \in \mathbb{Z}$$

$$0 \leq x < 9 \qquad \land \qquad 2 = z$$

- two new variables
- suboptimally connected

$$\land\ \left(\boxed{(3 \cdot x < 9)} \lor \boxed{(z = 3 \cdot x)}\right)$$

$$\land\ \left(\boxed{\neg(3 \cdot x < 9)} \lor \boxed{(z = y)}\right)$$

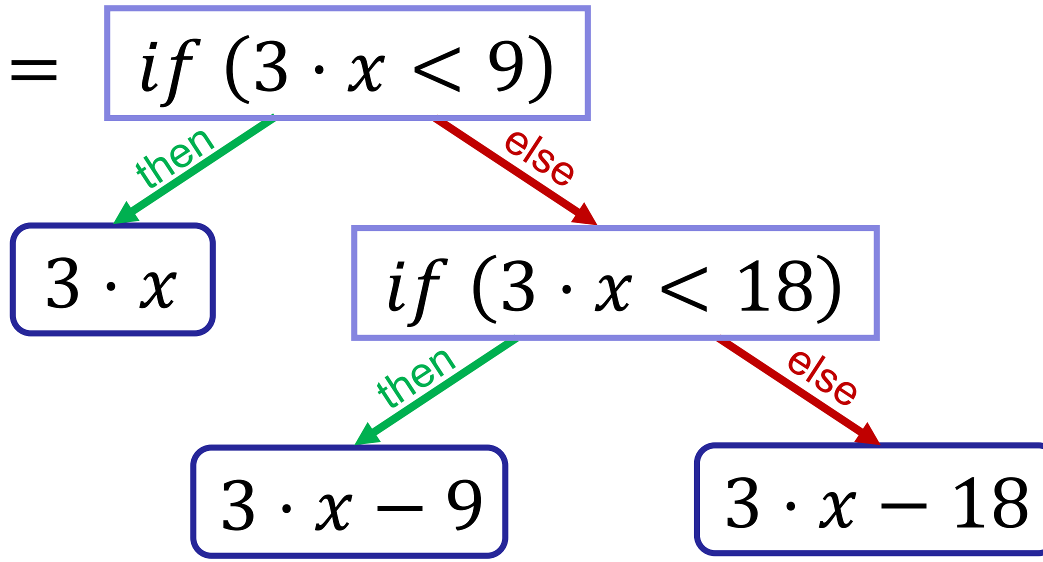
$$\land\ \left(\boxed{(3 \cdot x < 18)} \lor \boxed{(y = 3 \cdot x - 18)}\right)$$

$$\land\ \left(\boxed{\neg(3 \cdot x < 18)} \lor \boxed{(y = 3 \cdot x - 9)}\right)$$

If-Then-Else: Shared Monomial Lifting

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

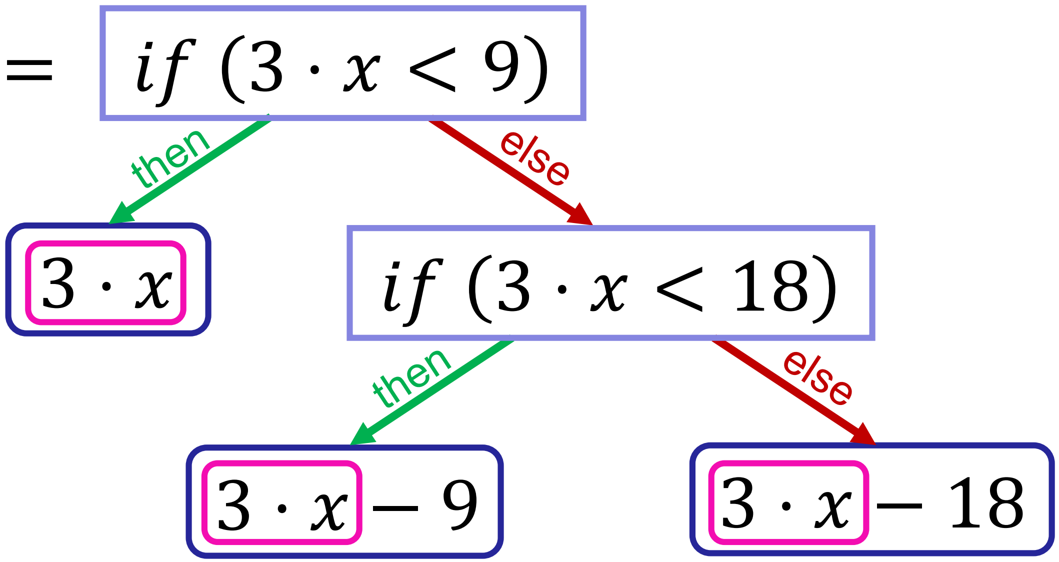
$$0 \le x < 9 \qquad \wedge \qquad 2 =$$



If-Then-Else: Shared Monomial Lifting

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \wedge \quad 2 =$$

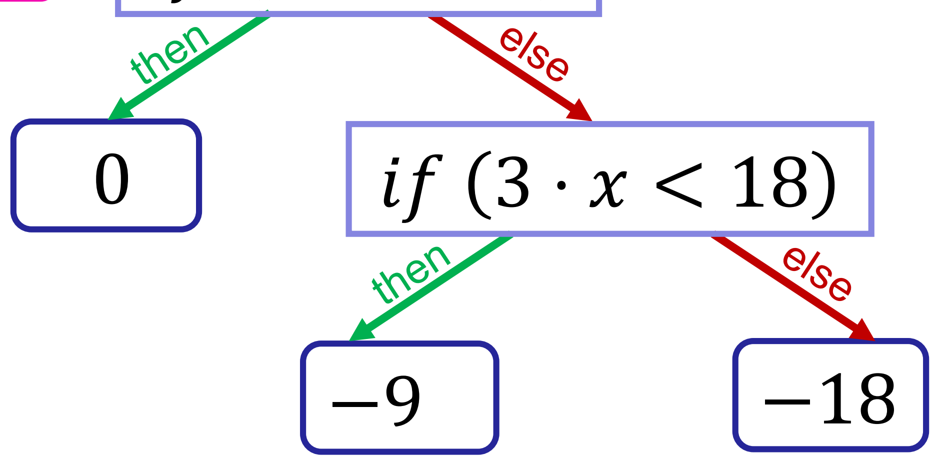


All share the monomial $\boxed{3 \cdot x}$!

If-Then-Else: Shared Monomial Lifting

$$2 \equiv_9 3 \cdot x \qquad \qquad for\ x \in \mathbb{Z}$$

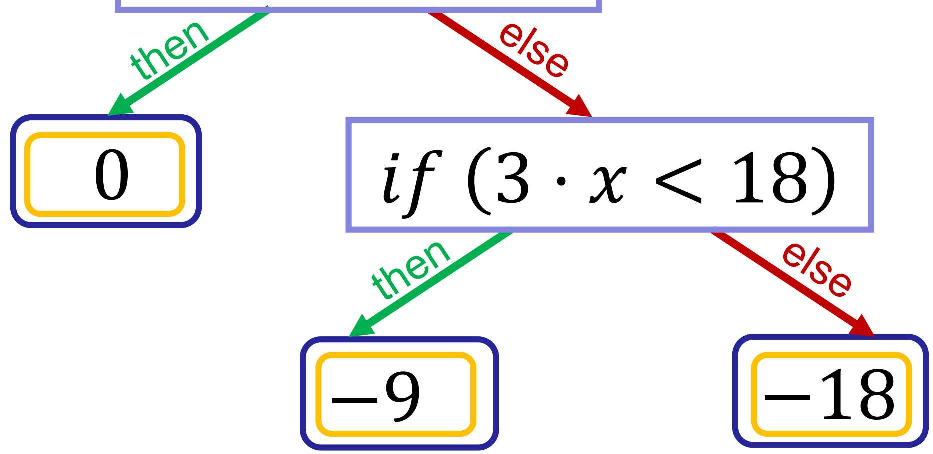
$$0 \leq x < 9 \quad \wedge \quad 2 = \boxed{3 \cdot x} + \boxed{if\ (3 \cdot x < 9)}$$



If-Then-Else: Shared Monomial Lifting

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

$$0 \le x < 9 \qquad \wedge \qquad 2 = \boxed{3 \cdot x} + \boxed{if\ (3 \cdot x < 9)}$$



All divisible by $\boxed{-9}$!

If-Then-Else: Shared Monomial Lifting

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x \in \mathbb{Z}$$

$$0 \le x < 9 \qquad \wedge \qquad 2 = \boxed{3 \cdot x}\boxed{-\,9\,\cdot}\boxed{if\ (3 \cdot x < 9)}$$

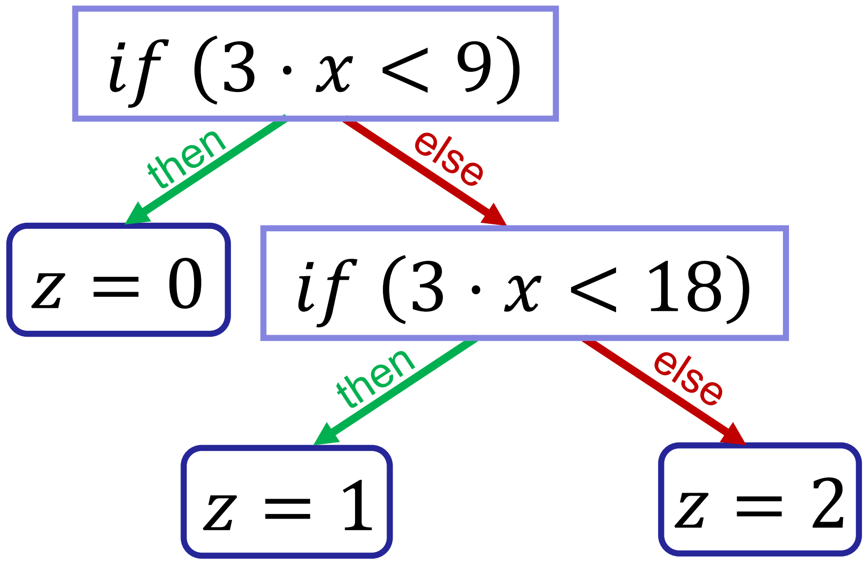
- then: $\boxed{0}$
- else: $\boxed{if\ (3 \cdot x < 18)}$
  - then: $\boxed{1}$
  - else: $\boxed{2}$

If-Then-Else: Bounding

$$2 \equiv_9 3 \cdot x \qquad\qquad \mathit{for}\ x, z \in \mathbb{Z}$$

$$0 \leq x < 9 \qquad \wedge \qquad 2 = \boxed{3 \cdot x}\boxed{- 9 \cdot} z$$

$\wedge$



max planck institut informatik

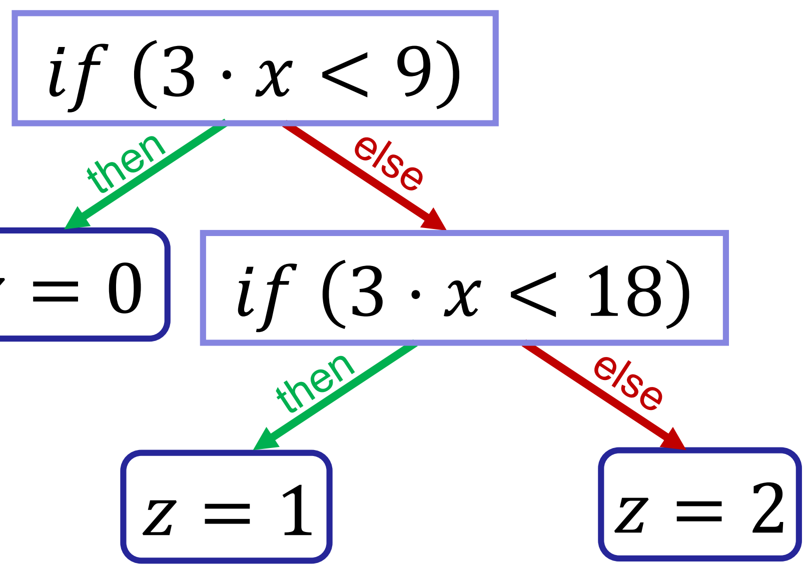
SIC Saarland Informatics Campus

If-Then-Else: Bounding

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x, z \in \mathbb{Z}$$

$$0 \le x < 9 \quad \wedge \quad 2 = \boxed{3 \cdot x}\boxed{- 9 \cdot} z \quad \wedge \quad 0 \le z \le 2$$

$\wedge$



If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad \textit{for } x, z \in \mathbb{Z}$$

$$0 \le x < 9 \quad \wedge \quad 2 = \boxed{3 \cdot x}\boxed{- 9 \cdot} z \quad \wedge \quad 0 \le z \le 2$$

$$\wedge \ (\neg(3 \cdot x < 9) \ \vee \ \boxed{z = 0})$$

$$\wedge \ \big((3 \cdot x < 9) \ \vee \neg(3 \cdot x < 18) \ \vee \ \boxed{z = 1}\big)$$

$$\wedge \ (\neg(3 \cdot x < 18) \ \vee \ \boxed{z = 2})$$

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad \textit{for } x, z \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \land \quad \boxed{2 = 3 \cdot x - 9 \cdot z} \quad \land \quad 0 \leq z \leq 2$$

$$\land\ (\neg(3 \cdot x < 9) \ \lor\ z = 0\ )$$

$$\land\ \big((3 \cdot x < 9)\ \lor \neg(3 \cdot x < 18)\ \lor\ z = 1\big)$$

$$\land\ (\neg(3 \cdot x < 18)\ \lor\ z = 2\ )$$

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad \mathit{for}\ x, z \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \wedge \quad 2 \leq 3 \cdot x - 9 \cdot z \quad \wedge \quad 0 \leq z \leq 2$$

$$\wedge \quad 2 \geq 3 \cdot x - 9 \cdot z$$

$$\wedge\ (\neg(3 \cdot x < 9)\ \vee\ z = 0\ )$$

$$\wedge\ \big((3 \cdot x < 9)\ \vee \neg(3 \cdot x < 18)\ \vee\ z = 1\big)$$

$$\wedge\ (\neg(3 \cdot x < 18)\ \vee\ z = 2\ )$$

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad for\ x, z \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \boxed{\begin{aligned} &\wedge \quad \frac{2}{3} \leq 1 \cdot x - 3 \cdot z \\ &\wedge \quad \frac{2}{3} \geq 1 \cdot x - 3 \cdot z \end{aligned}} \quad \wedge \quad 0 \leq z \leq 2$$

$$\wedge\ (\neg(3 \cdot x < 9)\ \vee\ z = 0\ )$$

$$\wedge\ \big((3 \cdot x < 9)\ \vee \neg(3 \cdot x < 18)\ \vee\ z = 1\big)$$

$$\wedge\ (\neg(3 \cdot x < 18)\ \vee\ z = 2\ )$$

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad \textit{for } x, z \in \mathbb{Z}$$

$$0 \le x < 9 \quad \wedge \left\lceil \frac{2}{3} \right\rceil \le 1 \cdot x - 3 \cdot z \quad \wedge \quad 0 \le z \le 2$$

$$\wedge \left\lfloor \frac{2}{3} \right\rfloor \ge 1 \cdot x - 3 \cdot z$$

$$\wedge \ (\neg(3 \cdot x < 9) \ \vee \ z = 0\ )$$

$$\wedge \ \big((3 \cdot x < 9) \ \vee \neg(3 \cdot x < 18) \ \vee \ z = 1\big)$$

$$\wedge \ (\neg(3 \cdot x < 18) \ \vee \ z = 2\ )$$

max planck institut informatik

SIC Saarland Informatics Campus

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad\qquad for\ x, z \in \mathbb{Z}$$

$$0 \le x < 9 \quad \boxed{\begin{array}{l} \wedge \quad 1 \le 1 \cdot x - 3 \cdot z \\ \\ \wedge \quad 0 \ge 1 \cdot x - 3 \cdot z \end{array}} \quad \wedge \quad 0 \le z \le 2$$

$$\wedge \ (\neg(3 \cdot x < 9) \ \vee \ z = 0\ )$$

$$\wedge \ \big((3 \cdot x < 9) \ \vee \neg(3 \cdot x < 18) \ \vee \ z = 1\big)$$

$$\wedge \ (\neg(3 \cdot x < 18) \ \vee \ z = 2\ )$$

If-Then-Else: Preprocessing

$$2 \equiv_9 3 \cdot x \qquad \textit{for } x, z \in \mathbb{Z}$$

$$0 \leq x < 9 \quad \land \quad 1 \leq 1 \cdot x - 3 \cdot z \quad \land \quad 0 \leq z \leq 2$$

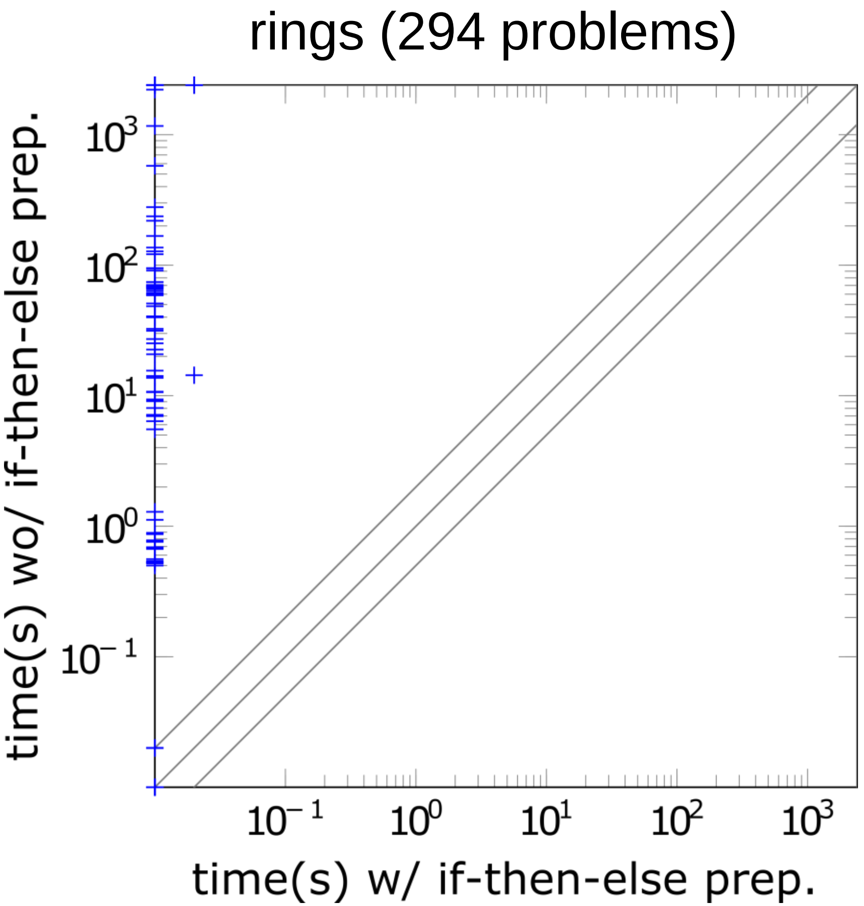
$$\land \quad 0 \geq 1 \cdot x - 3 \cdot z \qquad \Rightarrow \quad 1 \leq 0$$

$$\land \ (\neg(3 \cdot x < 9) \ \lor \ z = 0\ )$$

$$\land \ \big((3 \cdot x < 9) \ \lor \neg(3 \cdot x < 18) \ \lor \ z = 1\big)$$

$$\land \ (\neg(3 \cdot x < 18) \ \lor \ z = 2\ )$$

If-Then-Else: Preprocessing

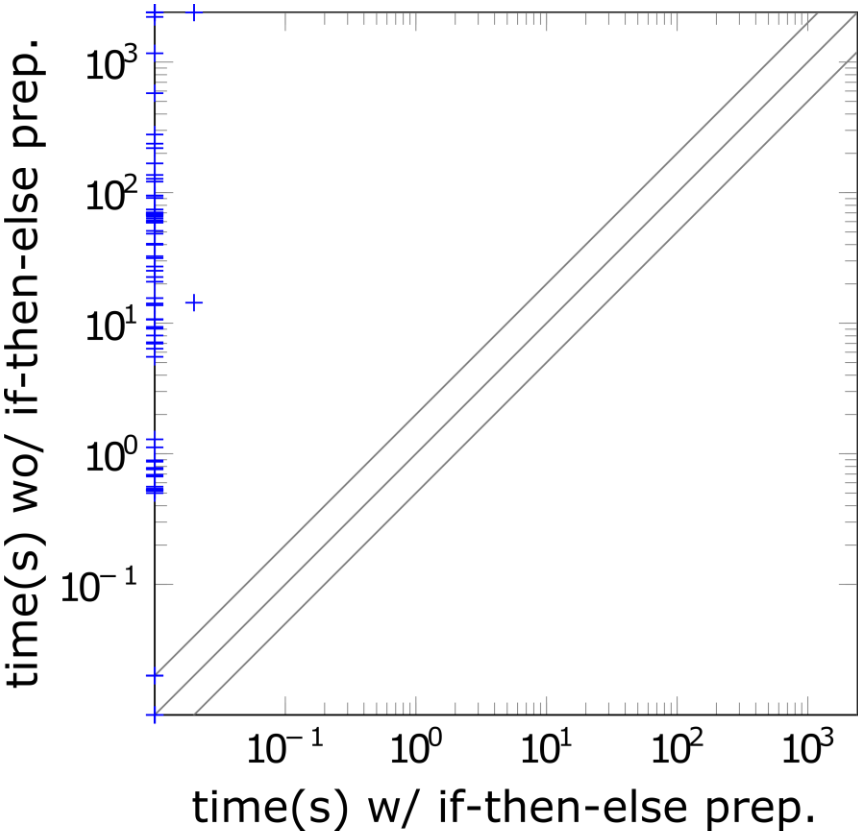


additional instances:157

Techniques: shared monomial lifting,
ite bounding, (ite reconstruction)

If-Then-Else: Preprocessing

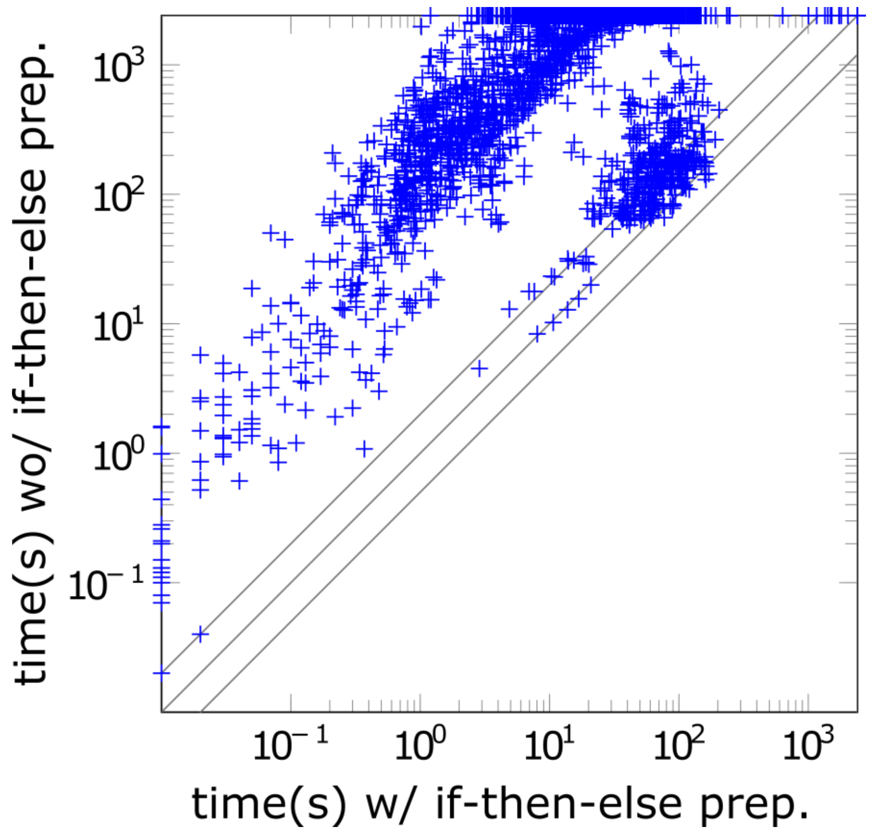
rings (294 problems)



additional instances:157

Techniques: shared monomial lifting, ite bounding, (ite reconstruction)

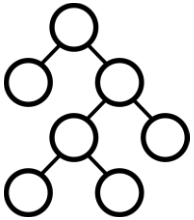
nec_smt (2800 problems)



additional instances: 1422

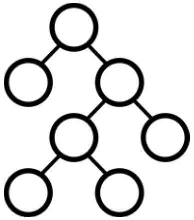
Techniques: constant-ite simplification, conjunctive-ite compression

[…] invented by our team […] invented & published by someone else […] never published but implemented



Simplex data-structure improvements:

- priority queue for pivot selection [pretty much everyone]
- integer coefficients instead of rational coefficients [veriT]
- backup instead of recalculation [pretty much everyone]



Simplex data-structure improvements:

- priority queue for pivot selection [pretty much everyone]
- integer coefficients instead of rational coefficients [veriT]
- backup instead of recalculation [pretty much everyone]

Integer Coefficients Instead of Rational Coefficient

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:

$$y = \frac{p_1}{q_1} \cdot x_1 + \cdots + \frac{p_n}{q_n} \cdot x_n$$

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:

$$y = \frac{p_1}{q_1} \cdot x_1 + \cdots + \frac{p_n}{q_n} \cdot x_n$$

Data Structure Representation:

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:

$$y = \frac{\boxed{p_1}}{\boxed{q_1}} \cdot x_1 + \cdots + \frac{\boxed{p_n}}{\boxed{q_n}} \cdot x_n$$

Data Structure Representation:

$2 \cdot n$ integers

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:

$$y = \frac{\boxed{p_1}}{\boxed{q_1}} \cdot x_1 + \cdots + \frac{\boxed{p_n}}{\boxed{q_n}} \cdot x_n$$

Data Structure Representation:

$2 \cdot n$ integers

where $q \coloneqq lcm(q_1, \dots, q_n)$

$$a_i \coloneqq \frac{p_i}{q_i} \cdot q$$

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:

$$y = \frac{\boxed{p_1}}{\boxed{q_1}} \cdot x_1 + \cdots + \frac{\boxed{p_n}}{\boxed{q_n}} \cdot x_n$$

$$\Downarrow$$

$$q \cdot y = a_1 \cdot x_1 + \cdots + a_n \cdot x_1$$

where $q \coloneqq lcm(q_1, \dots, q_n)$

$$a_i \coloneqq \frac{p_i}{q_i} \cdot q$$

Data Structure Representation:

$2 \cdot n$ integers

Integer Coefficients Instead of Rational Coefficient

Mathematical Representation:	Data Structure Representation:
$y = \frac{\boxed{p_1}}{\boxed{q_1}} \cdot x_1 + \cdots + \frac{\boxed{p_n}}{\boxed{q_n}} \cdot x_n$	$2 \cdot n$ integers
$\boxed{q} \cdot y = \boxed{a_1} \cdot x_1 + \cdots + \boxed{a_n} \cdot x_1$	$n + 1$ integers

where $q \coloneqq lcm(q_1, \ldots, q_n)$

$$a_i \coloneqq \frac{p_i}{q_i} \cdot q$$

Integer Coefficients Instead of Rational Coefficient

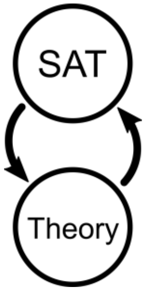
Mathematical Representation:	Data Structure Representation:
$y = \dfrac{\boxed{p_1}}{\boxed{q_1}} \cdot x_1 + \cdots + \dfrac{\boxed{p_n}}{\boxed{q_n}} \cdot x_n$	$2 \cdot n$ integers
$\Downarrow$	
$\boxed{q} \cdot y = \boxed{a_1} \cdot x_1 + \cdots + \boxed{a_n} \cdot x_1$	$n + 1$ integers

where $q \coloneqq lcm(q_1, \ldots, q_n)$

$$a_i \coloneqq \frac{p_i}{q_i} \cdot q$$

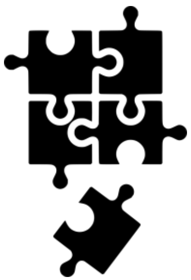
On average: x0.7 less time

[…] invented by our team   […] invented & published by someone else   […] never published but implemented



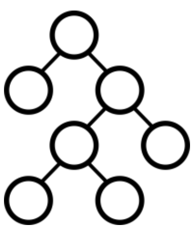
SAT and theory interaction:

- weakened early pruning [Sebastiani07]
- unate propagations and bound refinements [Dutertre06]
- decision recommendations [Yices]



Theory solver extensions:

- unit cube test [Bromberger16]
- bounding transformation [Bromberger18]
- simple rounding and bound propagation [Schrijver86]



Data-structure improvements:

- priority queue for pivot selection [pretty much everyone]
- integer coefficients instead of rational coefficients [veriT]
- backup instead of recalculation [pretty much everyone]

Preprocessing:

- if-then-else (reconstruction, lifting, simplification, bounding) [CVC4]
- pseudo-Boolean inequalities [CVC4]
- small CNF transformation [Weidenbach01]