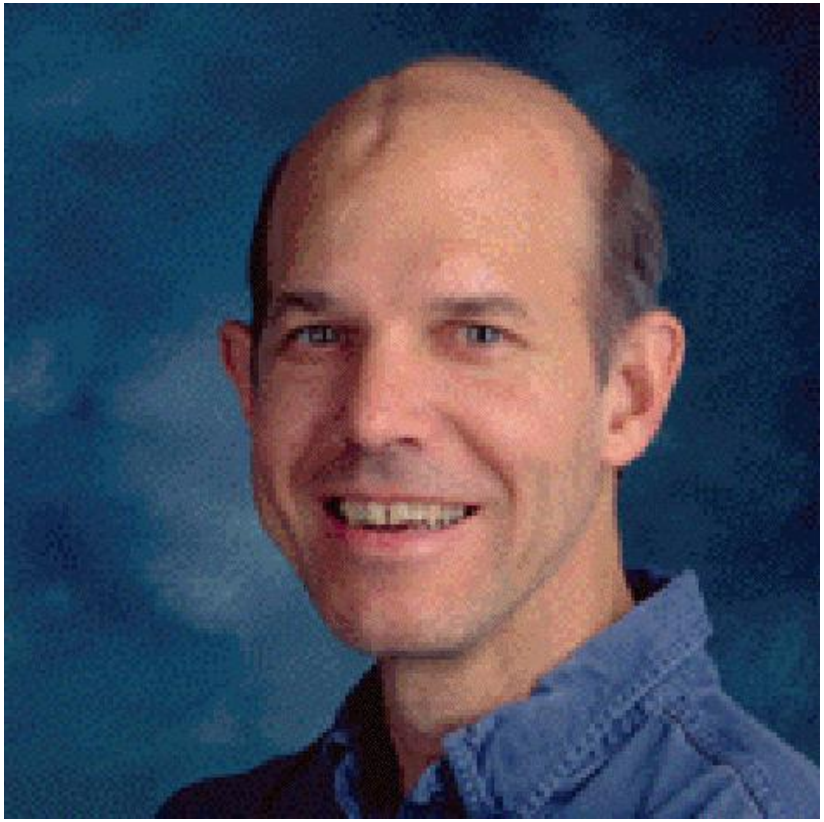
Internals of SMT Solvers

Leonardo de Moura
Microsoft Research

Acknowledgements

- Dejan Jovanovic (SRI International, NYU)
- Grant Passmore (Univ. Edinburgh)

Herbrand Award 2013



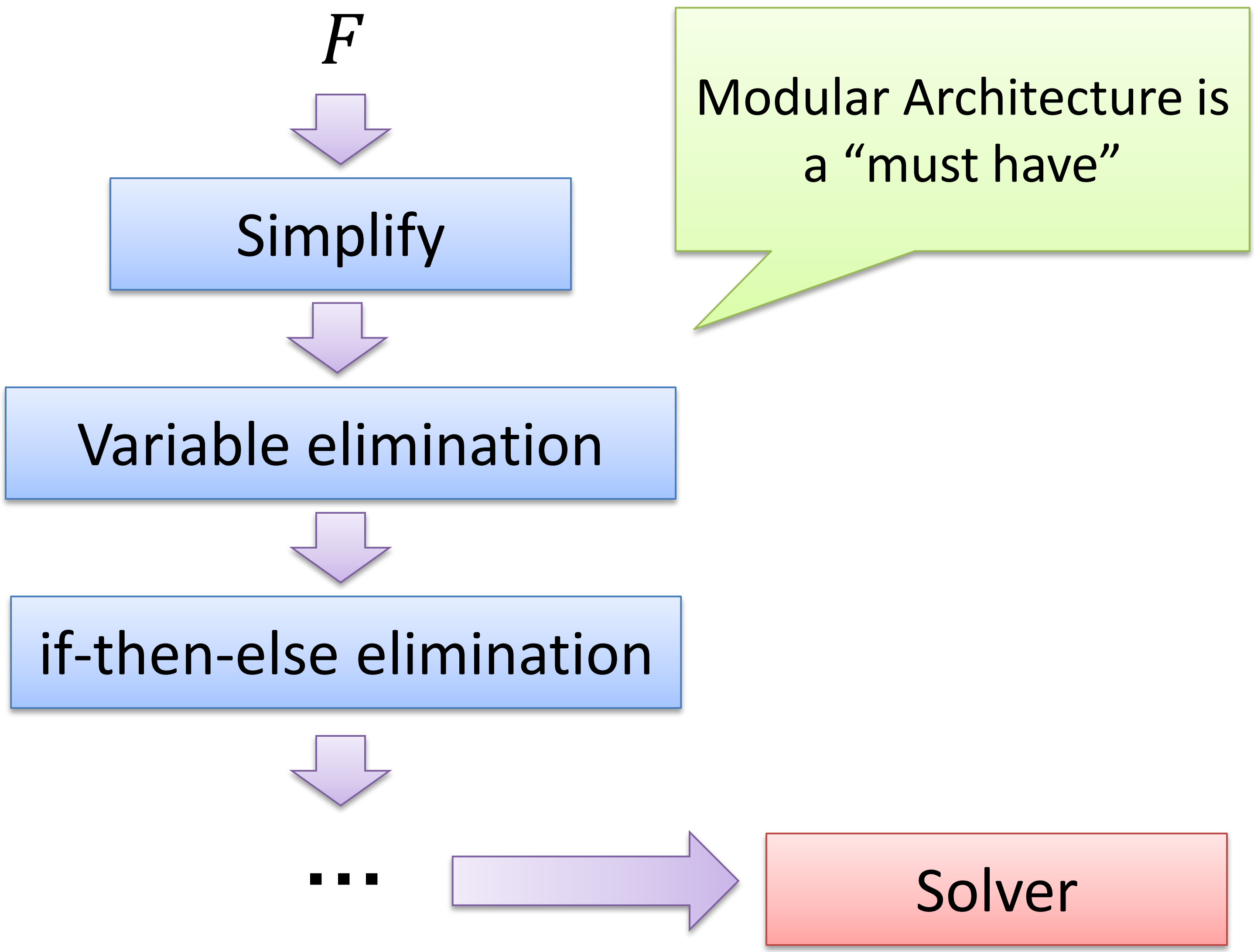
Greg Nelson

What is a SMT Solver?

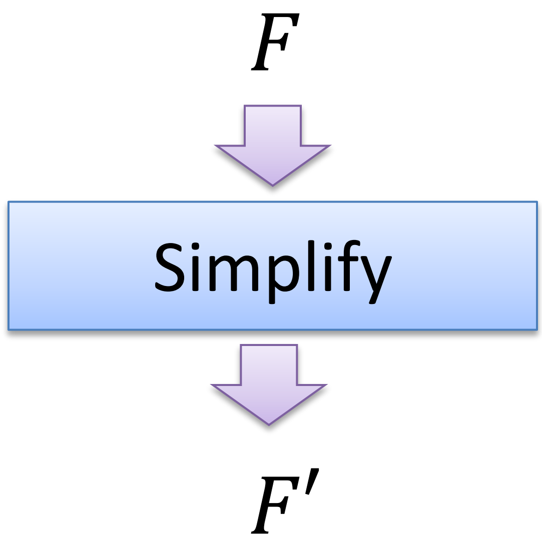
Multiple Approaches

Z3 is a portfolio of solvers

Preprocessing



Equivalence Preserving Simplifications

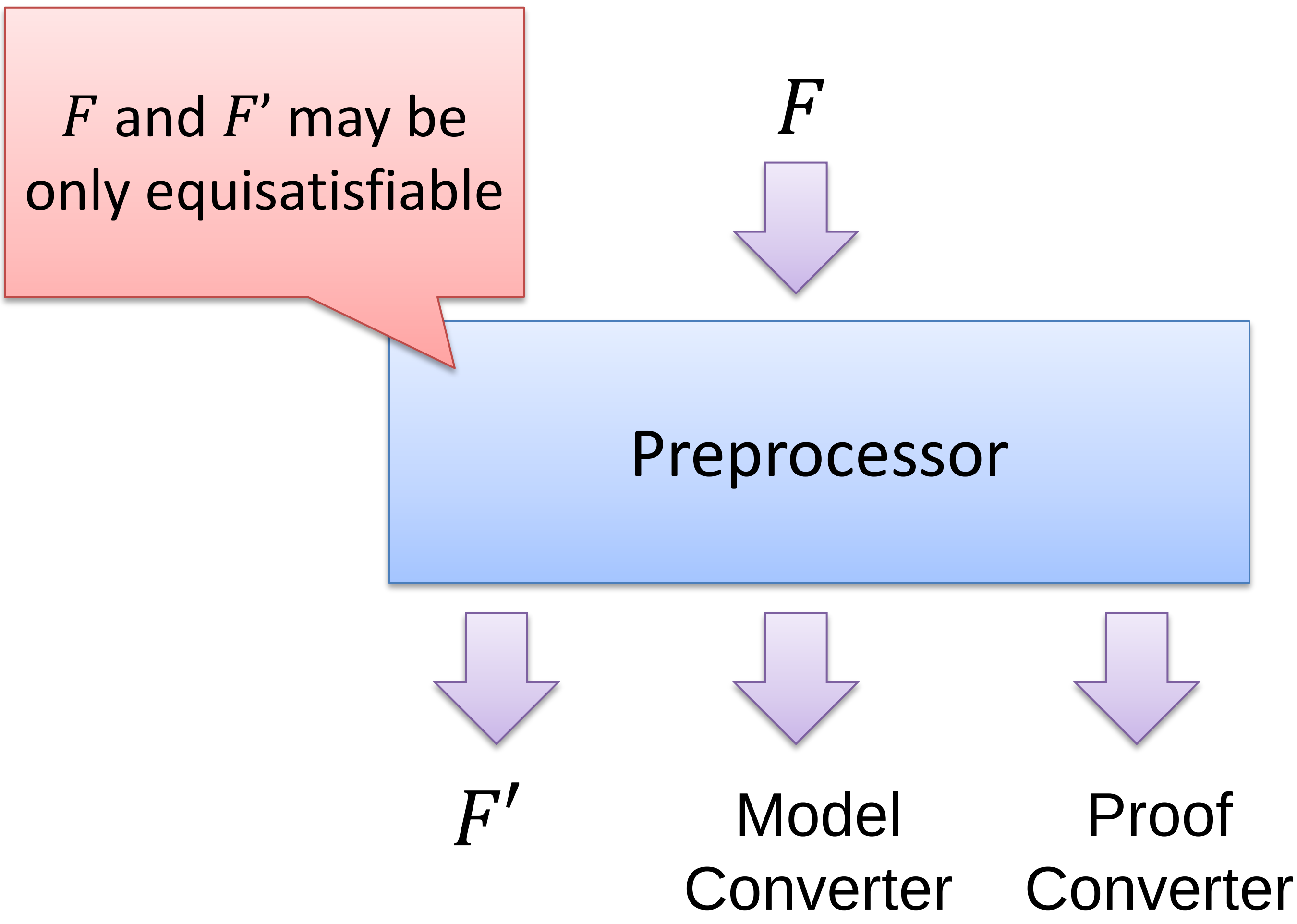


Examples:

$$x + y + 1 - x - 2 \;\mapsto\; y - 1$$

$$p \land true \land p \mapsto p$$

Preprocessor API



Example

$$[\ a = b + 1,\ (a < 0 \vee a > 0),\ b > 3\ ]$$

Variable Elimination

$$[\ (b + 1 < 0 \vee b + 1 > 0),\ b > 3\ ]$$

Proof builder

Model builder

Example

$$[\ a = b + 1,\ (a < 0 \vee a > 0),\ b > 3\ ]$$

Variable Elimination

$$M, M(a) = M(b) + 1$$

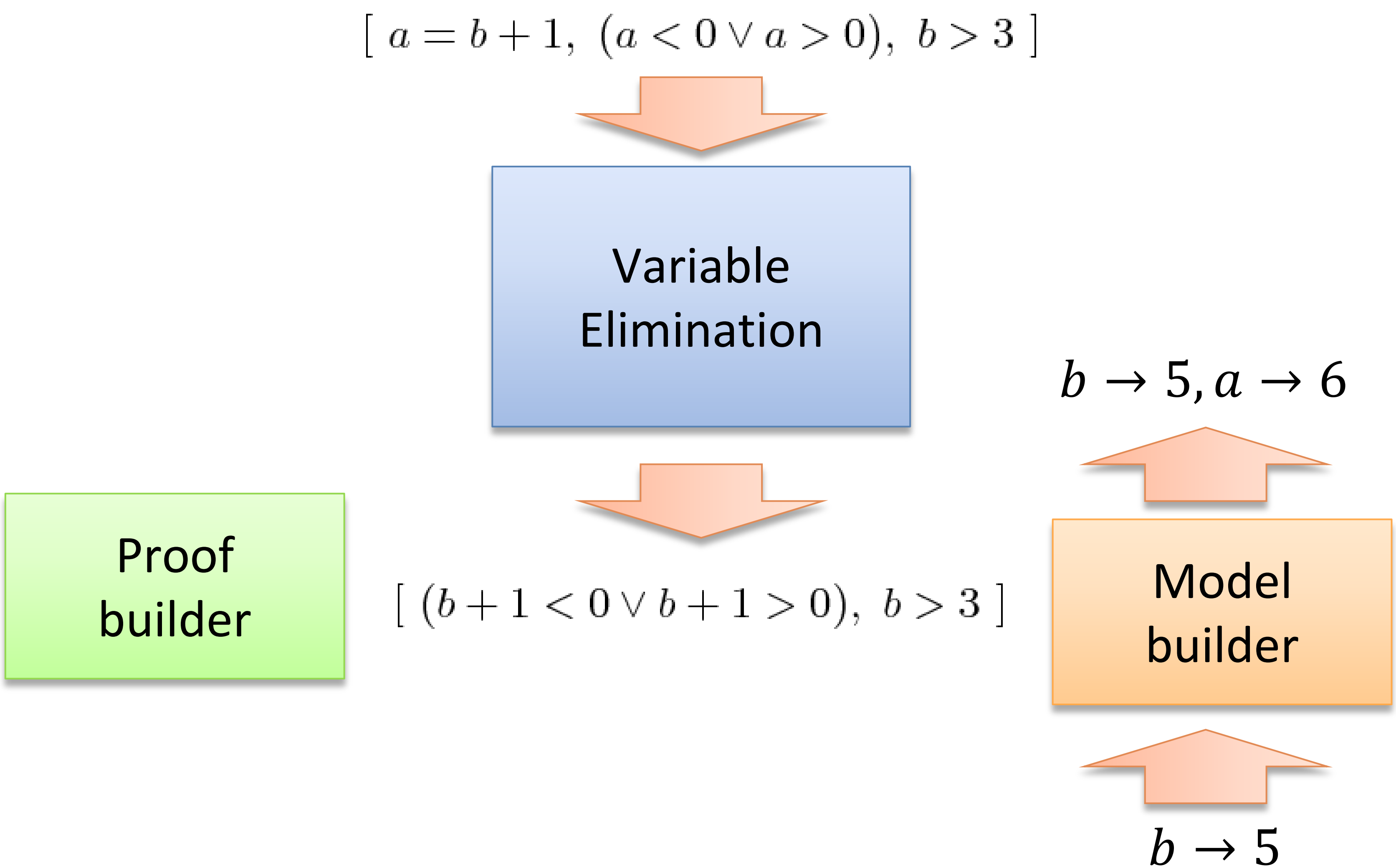
Proof builder

$$[\ (b + 1 < 0 \vee b + 1 > 0),\ b > 3\ ]$$

Model builder

$$M$$

Example

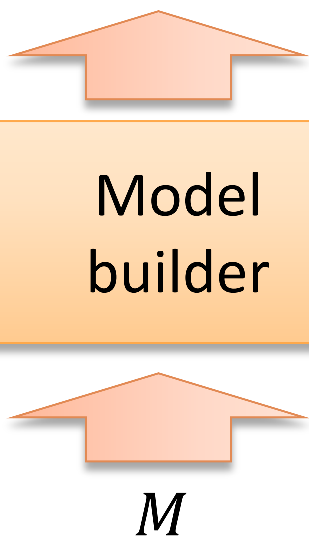

$[\ a = b + 1,\ (a < 0 \vee a > 0),\ b > 3\ ]$
Variable Elimination
$b \to 5, a \to 6$
Proof builder
$[\ (b + 1 < 0 \vee b + 1 > 0),\ b > 3\ ]$
Model builder
$b \to 5$

Model Converters

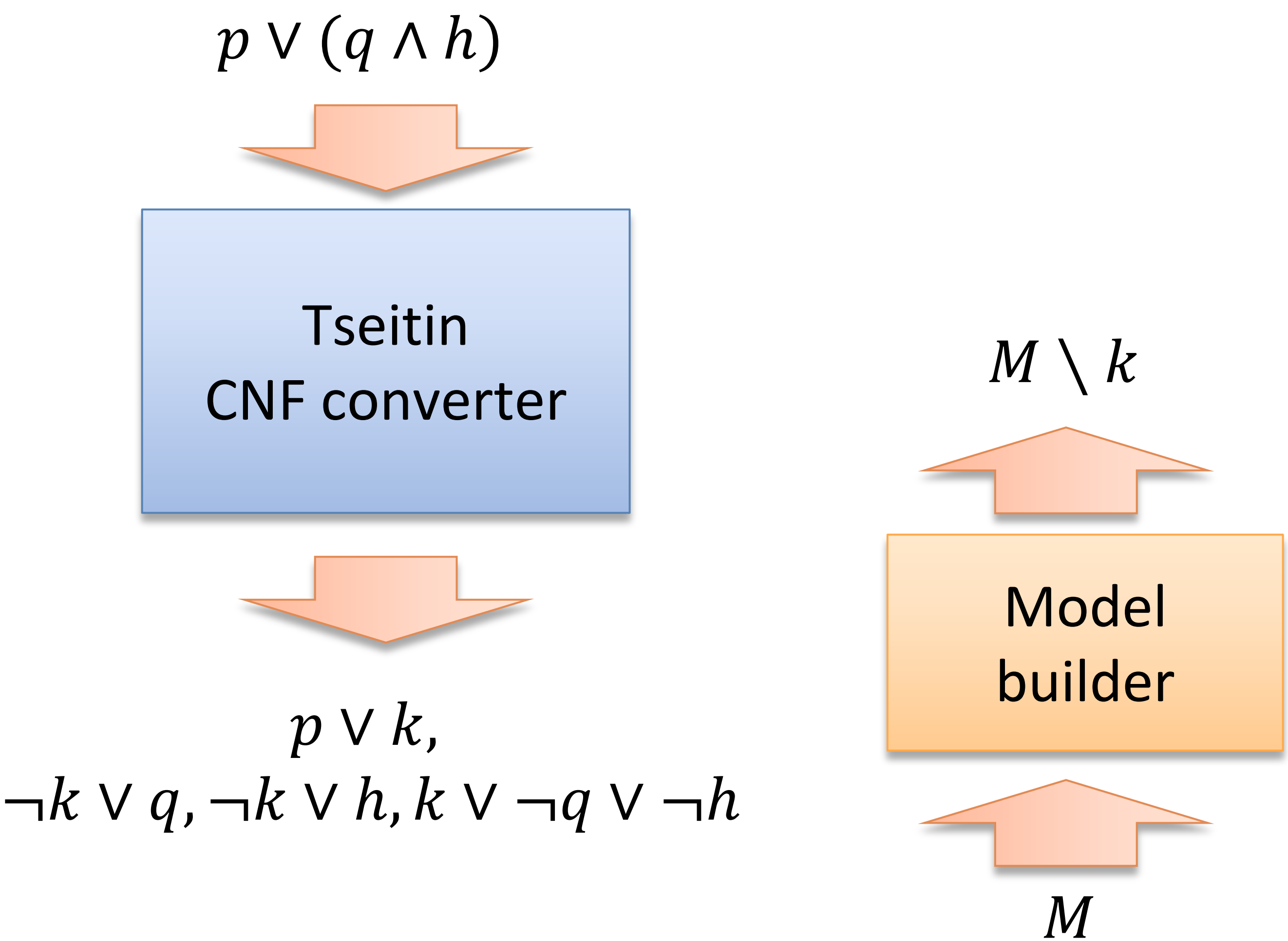
Extension

Filter

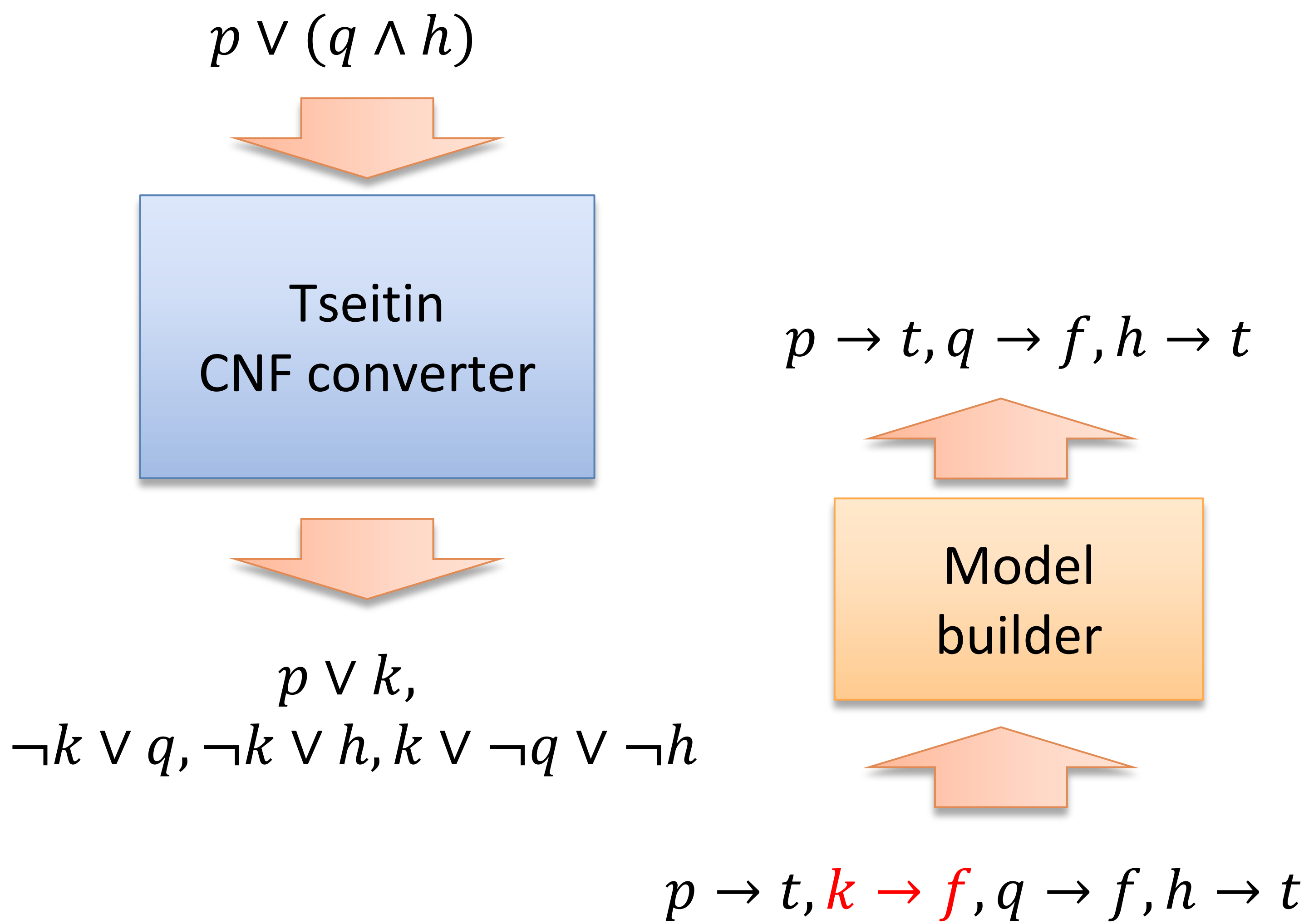
$$M, M(a) = M(b) + 1$$



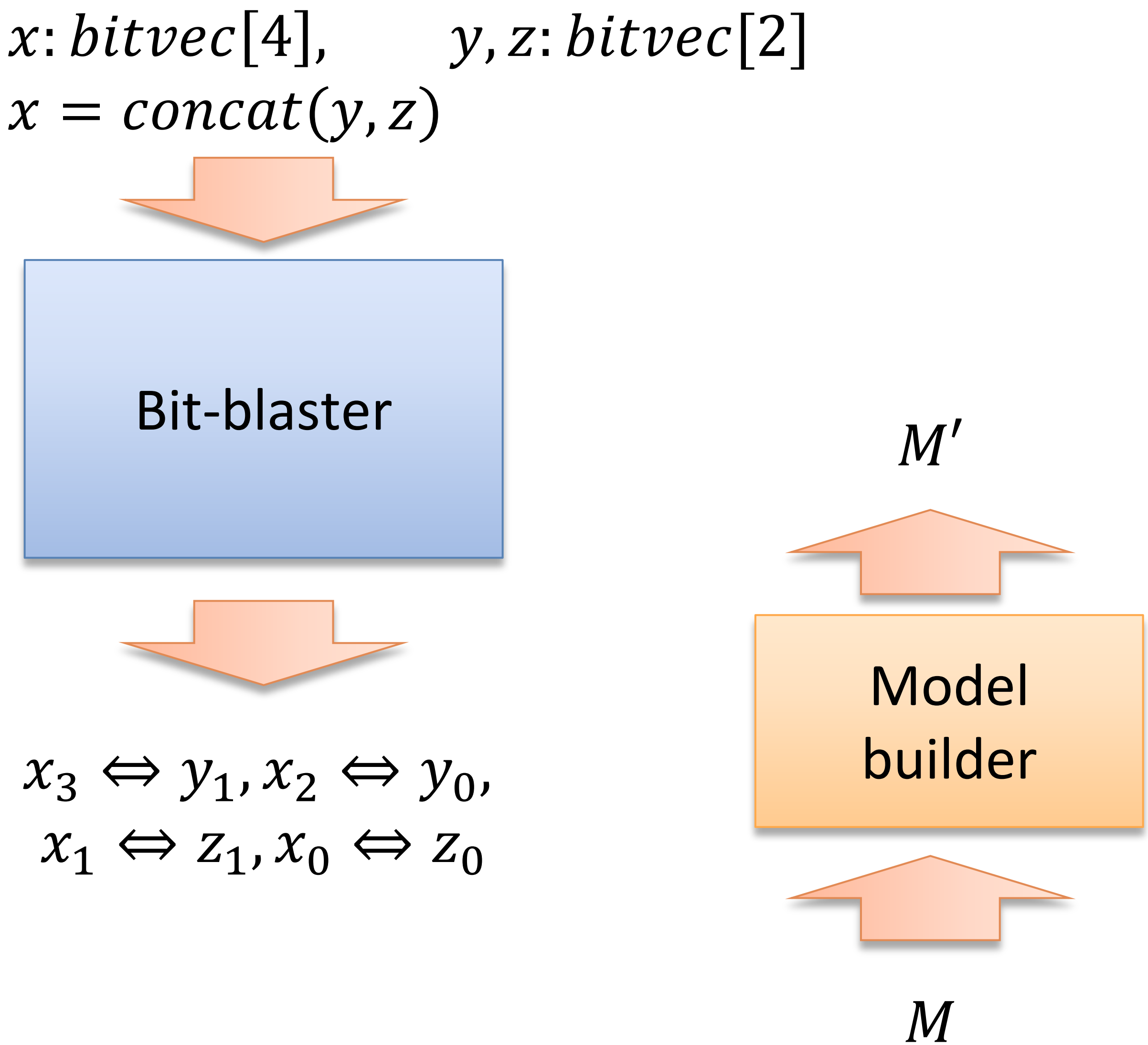
Model Converter: Filter



Model Converter: Filter



Model Converter: Extension + Filter

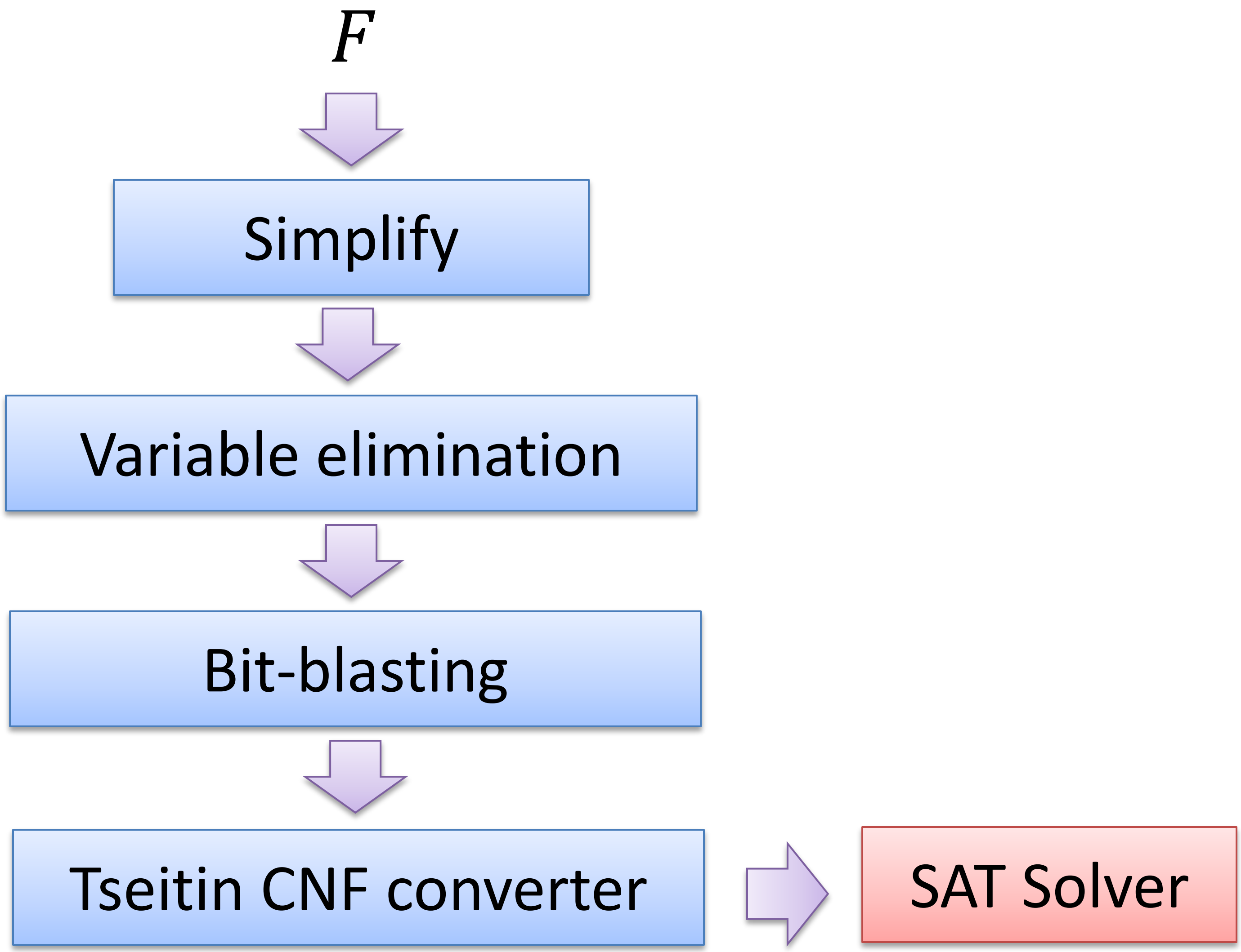


Preprocessors

1. Produce Equivalent Formula
2. Produce Equisatisfiable Formula
3. Assume "closed world" (non-incremental)

Example: symmetry reduction

Simple QF_BV (bit-vector) solver



Under/Over-Approximations

Under-approximation

unsat answers cannot be trusted

Over-approximation

sat answers cannot be trusted

Under/Over-Approximations

Under-approximation

model finders

Over-approximation

proof finders

Under/Over-Approximations

Under-approximation

$S \to S \cup S'$

Over-approximation

$S \to S \setminus S'$

Under/Over-Approximations

Under-approximation

Example: QF_NIA model finders

add bounds to unbounded variables (and blast)

Over-approximation

Example: Boolean abstraction

Under/Over-Approximations

Combining under and over is bad!

sat and unsat answers cannot be trusted.

Tracking: under/over-approximations

Proof and Model converters can check if the resultant models and proofs are valid.

CEGAR is your friend

Counter-Example Guided Abstract Refinement

Using over-approximation

procedure Solver(F)

F_p := Abstract(F)

loop

(R, M) := Solve(F_p)

if R = UNSAT **then return** UNSAT

R' := Check(F, M)

if R' = SAT **then return** SAT

F_p := Refine(F, F_p, M)

Model

CEGAR is your friend

Counter-Example Guided Abstract Refinement

Using under-approximation

Proof

procedure Solver(F)

  F_p := Abstract(F)

  loop

    (R, Pr) := Solve(F_p)

    if R = SAT **then return** SAT

    R’ := Check(F, Pr)

    if R’ = UNSAT **then return** UNSAT

    F_p := Refine(F, F_p, M)

CEGAR is your friend

Counter-Example Guided Abstract Refinement

Refinements:

Incremental Solver

Run over and under-approximation is parallel

Uninterpreted Functions by CEGAR

Suppose we have a Solver that does not support uninterpreted functions (example: QF_BV solver)

Congruence Rule:

$$x_1 = y_1, \ldots, x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

Uninterpreted Functions by CEGAR

Congruence Rule:

$$x_1 = y_1, \dots, xn = yn \Rightarrow f(x_1, \dots, xn)$$

Abstract: replace each f-application with a fresh variable (over-approximation)

$$a = b + 1, f(a-1) = c, f(b) \neq c$$

$$k_1 \equiv f(a-1),$$
$$k_2 \equiv f(b)$$

$$a = b + 1, k_1 = c, k_2 \neq c$$

Uninterpreted Functions by CEGAR

Congruence Rule:

$$x_1 = y_1, \ldots, xn = yn \Rightarrow f(x_1, \ldots, xn)$$

Check: check if congruence rule is satisfied

$$a = b + 1, k_1 = c, k_2 \neq c$$

$$k_1 \equiv f(a - 1),$$
$$k_2 \equiv f(b)$$

$$a \rightarrow 1, b \rightarrow 0, c \rightarrow 0, k_1 \rightarrow 0, k_2 \rightarrow 1$$

Uninterpreted Functions by CEGAR

Congruence Rule:

$$x_1 = y_1, \ldots, xn = yn \Rightarrow f(x_1, \ldots, xn)$$

Refine: expand congruence axiom $a - 1 = b \Rightarrow k_1 = k_2$

$$a = b + 1, k_1 = c, k_2 \neq c$$

$$k_1 \equiv f(a - 1),$$
$$k_2 \equiv f(b)$$

$$a \to 1, b \to 0, c \to 0, k_1 \to 0, k_2 \to 1$$

Uninterpreted Functions by CEGAR

Congruence Rule:

$$x_1 = y_1, \dots, xn = yn \Rightarrow f(x_1, \dots, xn)$$

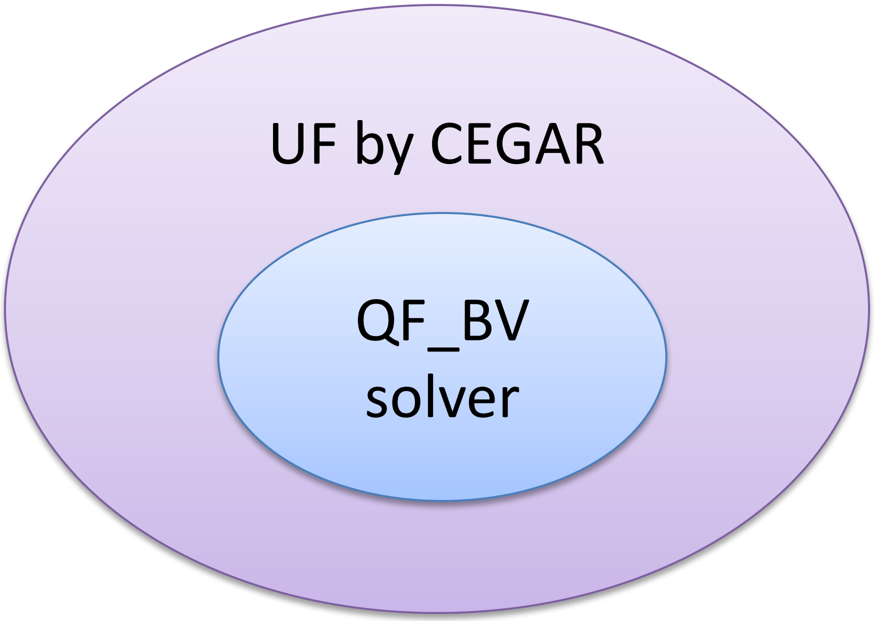
Refine: expand congruence axiom $a - 1 = b \Rightarrow k_1 = k_2$

$$a = b + 1, k_1 = c, k_2 \neq c, (a - 1 = b \Rightarrow k_1 = k_2)$$

unsat

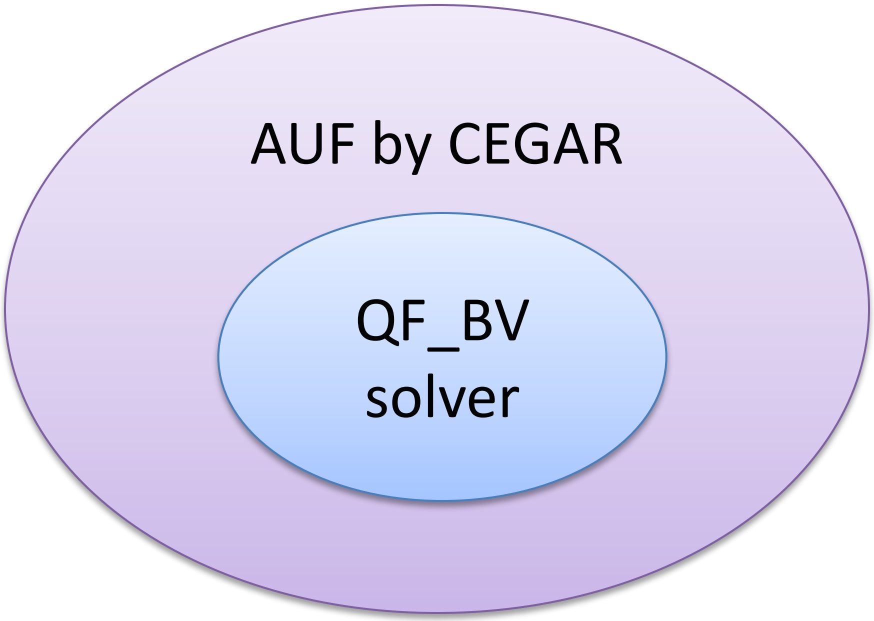
$$a - 1 \neq b \vee k_1 = k_2$$

Simple QF_UFBV Solver



Simple QF_AUFBV Solver

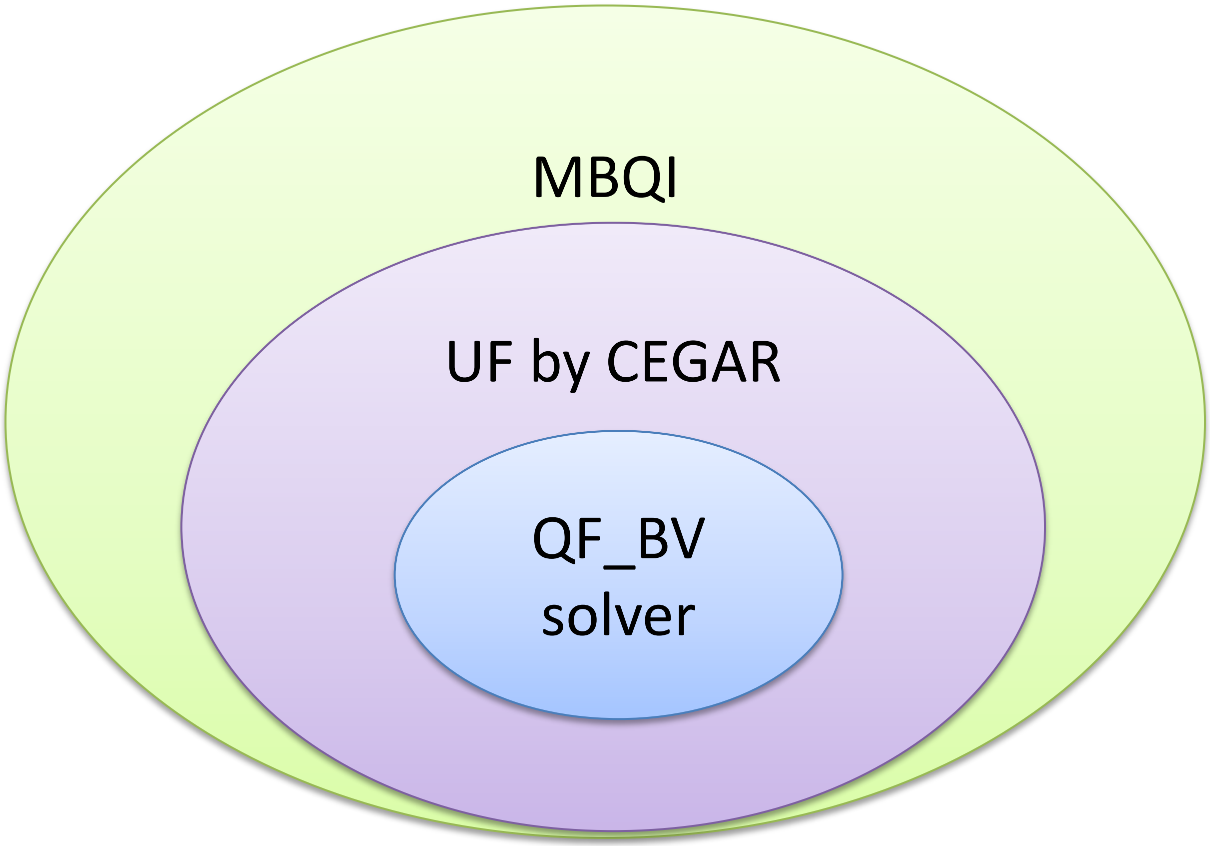
arrays on top of UF



Lemmas on Demand For Theory of Arrays [Brummayer-Biere 2009]

Simple UFBV Solver

model-based quantifier instantiation



Efficiently solving quantified bit-vector formulas [Wintersteiger at al 2010]

Simple QF_NIA "solver" by CEGAR

nonlinear integer arithmetic

Hilbert's 10^{th} Problem

DPRM theorem: QF_NIA is undecidable

Idea: use (under-approximation) CEGAR

1. Add lower/upper bounds to all variables, and convert into QF_BV
2. If SAT → done
3. Otherwise, refine: increase lower/upper bounds

Lazy SMT as CEGAR

Suppose we have a Solver that can only process a conjunction of literals.

Examples:

Congurence Closure (UF),

Simplex (Linear Real Arithmetic)

Lazy SMT as CEGAR: 1. Abstract

Basic Idea

$x \geq 0,\ y = x + 1,\ (y > 2 \vee y < 1)$

$\Downarrow$

$p_1,\ p_2,\ (p_3 \vee p_4)$ $\quad$ $p_1 \equiv (x \geq 0),\ p_2 \equiv (y = x + 1),$
$p_3 \equiv (y > 2),\ p_4 \equiv (y < 1)$

[Audemard et al - 2002], [Barrett et al - 2002], [de Moura et al - 2002]
[Flanagan et al - 2003], …

Lazy SMT as CEGAR: 2. Solve

Basic Idea

$x \geq 0,\ y = x + 1,\ (y > 2 \vee y < 1)$

$p_1,\ \ p_2,\ (p_3 \vee p_4)$

$p_1 \equiv (x \geq 0),\ p_2 \equiv (y = x + 1),$
$p_3 \equiv (y > 2),\ p_4 \equiv (y < 1)$

SAT
Solver

Lazy SMT as CEGAR: 2. Solve

Basic Idea

$x \geq 0,\ y = x + 1,\ (y > 2 \vee y < 1)$

$p_1,\ p_2,\ (p_3 \vee p_4)$

$p_1 \equiv (x \geq 0),\ p_2 \equiv (y = x + 1),$
$p_3 \equiv (y > 2),\ p_4 \equiv (y < 1)$

SAT
Solver

Assignment
$p_1,\ p_2,\ \neg p_3,\ p_4$

Lazy SMT as CEGAR: 3. Check

Basic Idea

$x \geq 0,\ y = x + 1,\ (y > 2 \vee y < 1)$

$p_1,\ p_2,\ (p_3 \vee p_4)$

$p_1 \equiv (x \geq 0),\ p_2 \equiv (y = x + 1),$
$p_3 \equiv (y > 2),\ p_4 \equiv (y < 1)$

SAT Solver

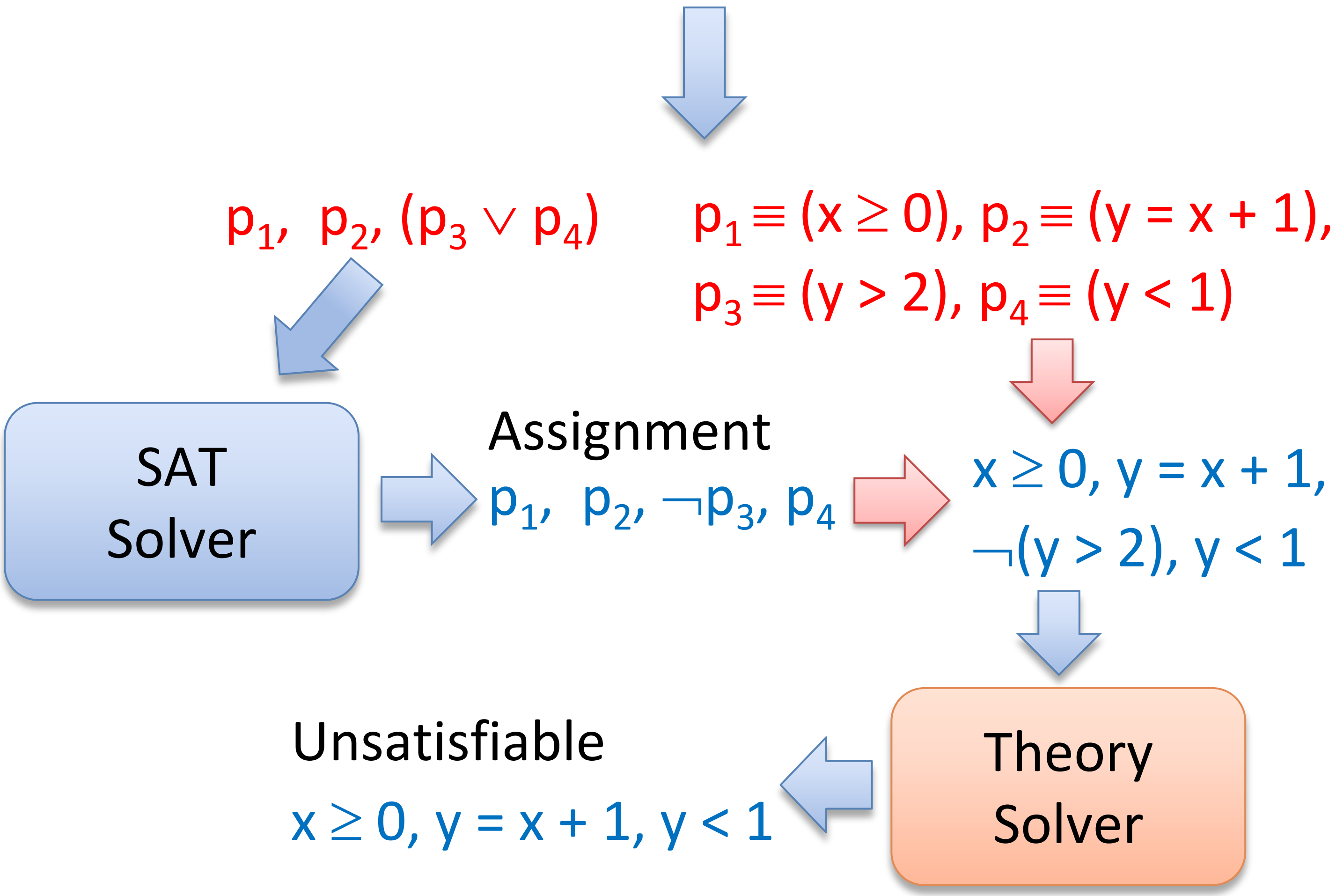
Assignment
$p_1,\ p_2,\ \neg p_3,\ p_4$

$x \geq 0,\ y = x + 1,$
$\neg(y > 2),\ y < 1$

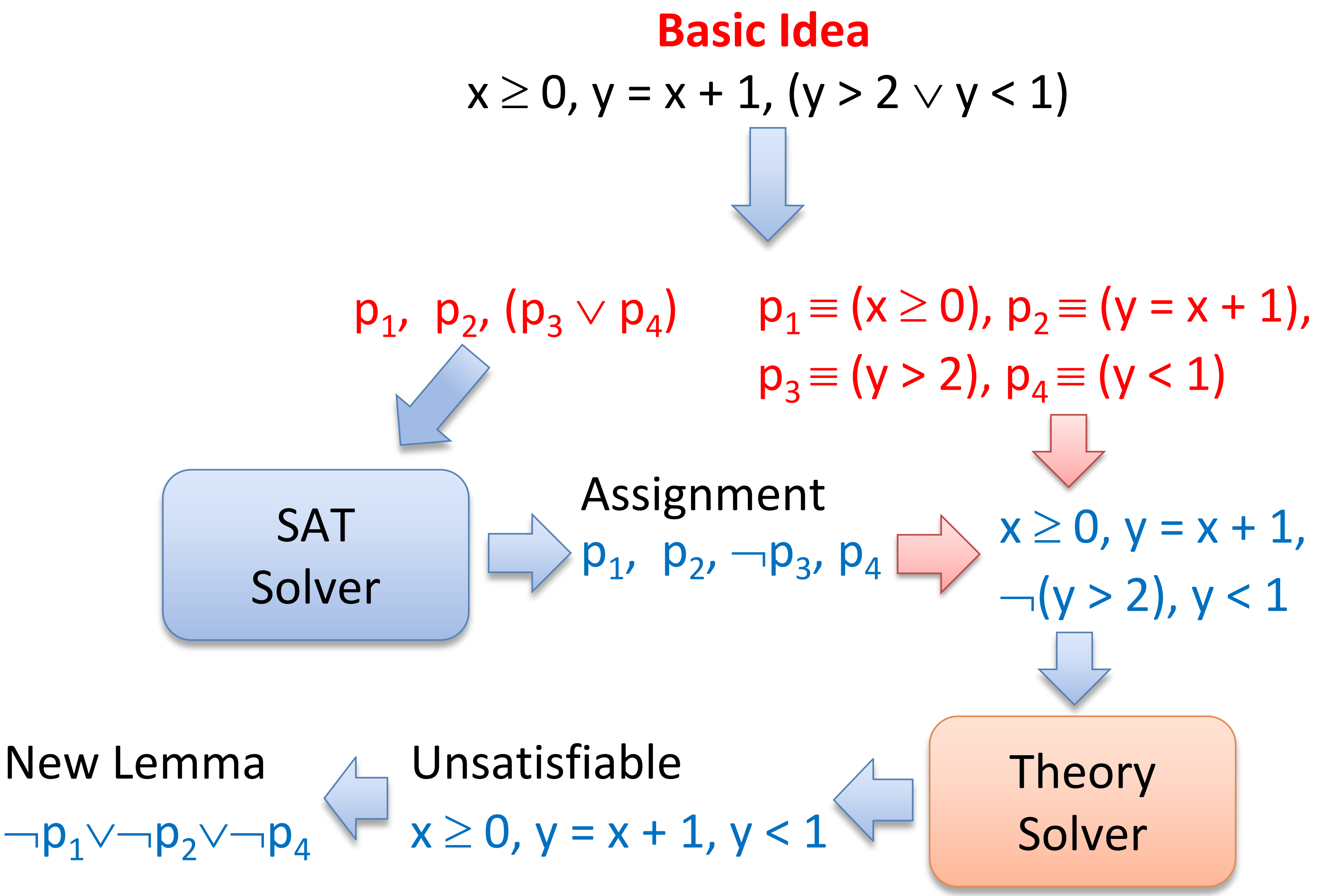
Lazy SMT as CEGAR: 3. Check

Basic Idea

$x \geq 0, y = x + 1, (y > 2 \vee y < 1)$



Lazy SMT as CEGAR: 4. Refine



Lazy SMT as CEGAR: 4. Refine

Basic Idea

New Lemma

$\neg p_1 \vee \neg p_2 \vee \neg p_4$

Unsatisfiable

$x \geq 0,\ y = x + 1,\ y < 1$

Theory Solver

AKA
Theory conflict

Lazy SMT as CEGAR: refinements

Many refinements:

Incrementality

Efficient Backtracking

Efficient Lemma Generation

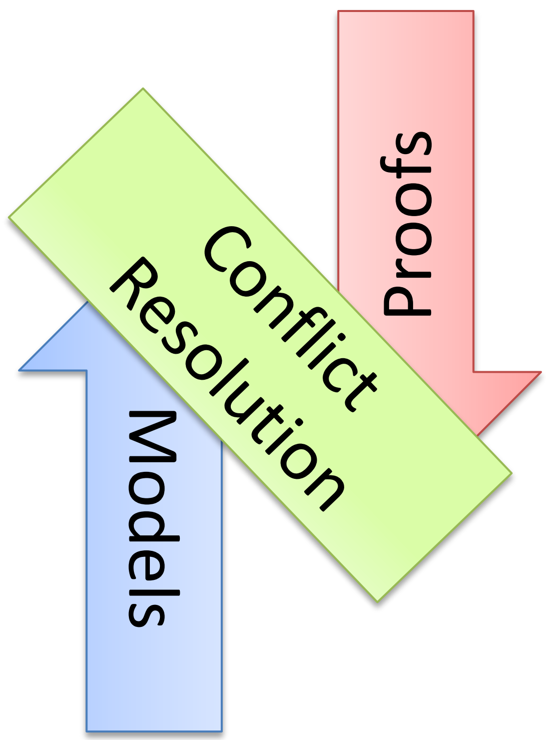
Theory propagation - DPLL(T) [Ganzinger et all – 2004]

Many SMT solvers are based on DPLL(T)

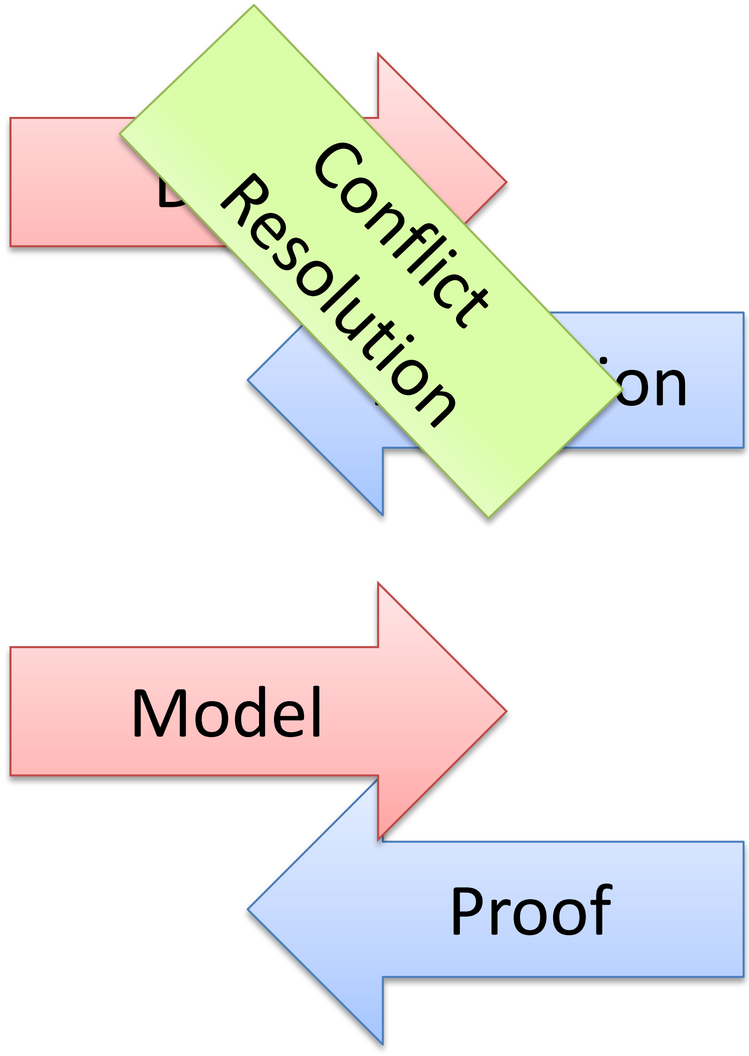
DPLL(T) weakness

Theories are “second-class citizens”.

DPLL(T) is not model-driven (key property of CDCL).



CDCL: Conflict Driven Clause Learning



DPLL(T) weakness

DPLL(T) works well only for "easy" theories.

Examples:

Uninterpreted functions

Difference logic ($x - y \leq c$)

Linear real arithmetic

"Hard theories":

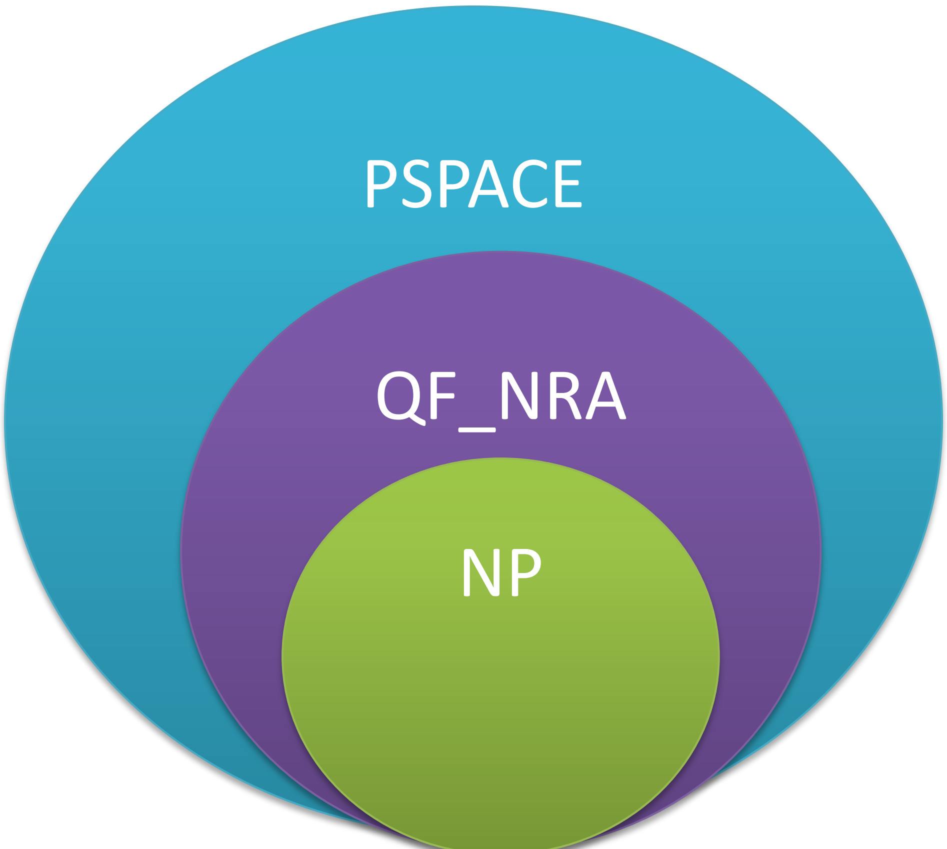
Linear integer arithmetic

Arrays

Nonlinear real arithmetic

Example: Nonlinear Real Arithmetic

$$x^2 - 4x + y^2 - y + 8 < 1$$
$$xy - 2x - 2y + 4 > 1$$



PSPACE membership

Canny – 1988,

Grigor'ev – 1988

NP-hardness

x is "Boolean" → x (x-1) = 0

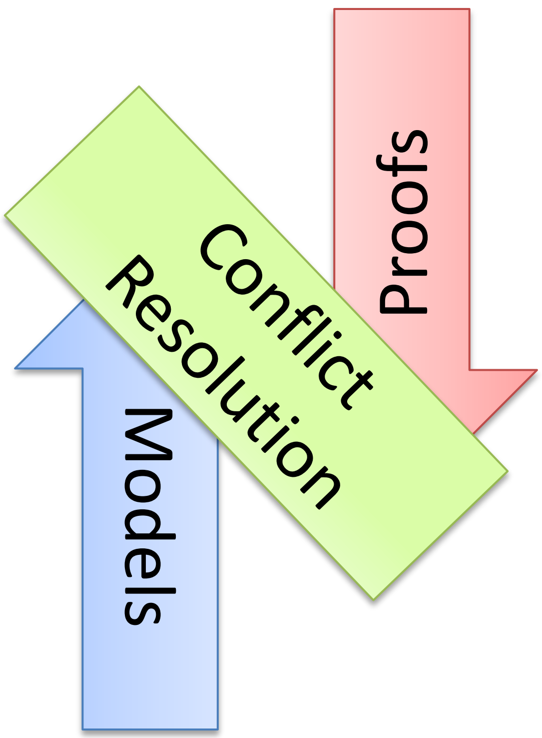
x or y or z → x + y + z > 0

The RISE of Model-Driven Techniques in SMT

Saturation x Search

Proof-finding

Model-finding



Two procedures

Resolution	DPLL
Proof-finder	Model-finder
Saturation	Search

CDCL is model-driven proof search

Linear Arithmetic

Fourier-Motzkin	Simplex
Proof-finder	Model-finder
Saturation	Search

Fourier-Motzkin

$$t_1 \leq ax, \qquad bx \leq t_2$$

$$bt_1 \leq abx, \qquad abx \leq at_2$$

$$bt_1 \leq at_2$$

Very similar to Resolution

Exponential time and space

Polynomial Constraints

AKA

Existential Theory of the Reals

∃R

$$x^2 - 4x + y^2 - y + 8 < 1$$
$$xy - 2x - 2y + 4 > 1$$

CAD "Big Picture"

1. Project/Saturate set of polynomials
2. Lift/Search: Incrementally build assignment v: $x_k \rightarrow \alpha_k$

   Isolate roots of polynomials $f_i(\boldsymbol{\alpha}, x)$

   Select a feasible cell C, and assign x_k some $\alpha_k \in C$

   If there is no feasible cell, then backtrack

CAD "Big Picture"

$$x^2 + y^2 - 1 < 0$$
$$x\,y - 1 > 0$$

1. Saturate

$$x^4 - x^2 + 1$$
$$x^2 - 1$$
$$x$$

2. Search

	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

CAD "Big Picture"

$x^2 + y^2 - 1 < 0$

$x\,y - 1 > 0$

1. Saturate

$x^4 - x^2 + 1$

$x^2 - 1$

x

	$(-\infty, -\frac{1}{2})$	$-\frac{1}{2}$	$(-\frac{1}{2}, \infty)$
$4 + y^2 - 1$	+	+	+
$-2y - 1$	+	0	-

$x \rightarrow -2$

2. Search

	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

CAD “Big Picture”

$\boldsymbol{x^2 + y^2 - 1 < 0}$

$x\,y - 1 > 0$

1. Saturate

$x^4 - x^2 + 1$

$x^2 - 1$

x

	$(-\infty, -\frac{1}{2})$	$-\frac{1}{2}$	$(-\frac{1}{2}, \infty)$
$\boldsymbol{4 + y^2 - 1}$	+	+	+
$-2y - 1$	+	0	-

CONFLICT

$\boldsymbol{x \to -2}$

2. Search

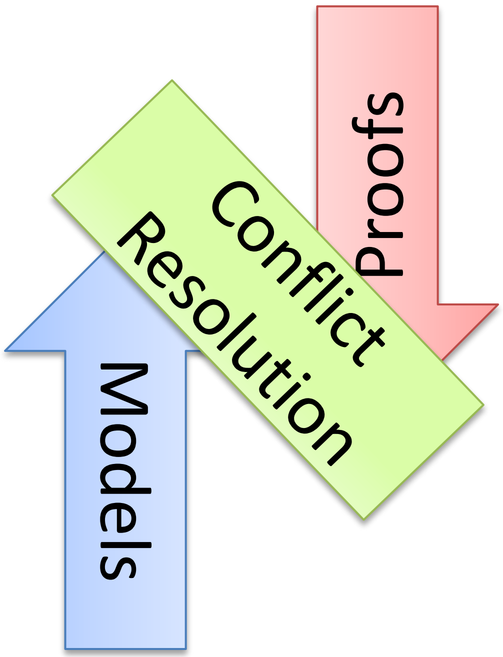
	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

NLSat: Model-Driven Search

Static x Dynamic

Optimistic approach

Key ideas



Start the Search before Saturate/Project

We saturate on demand

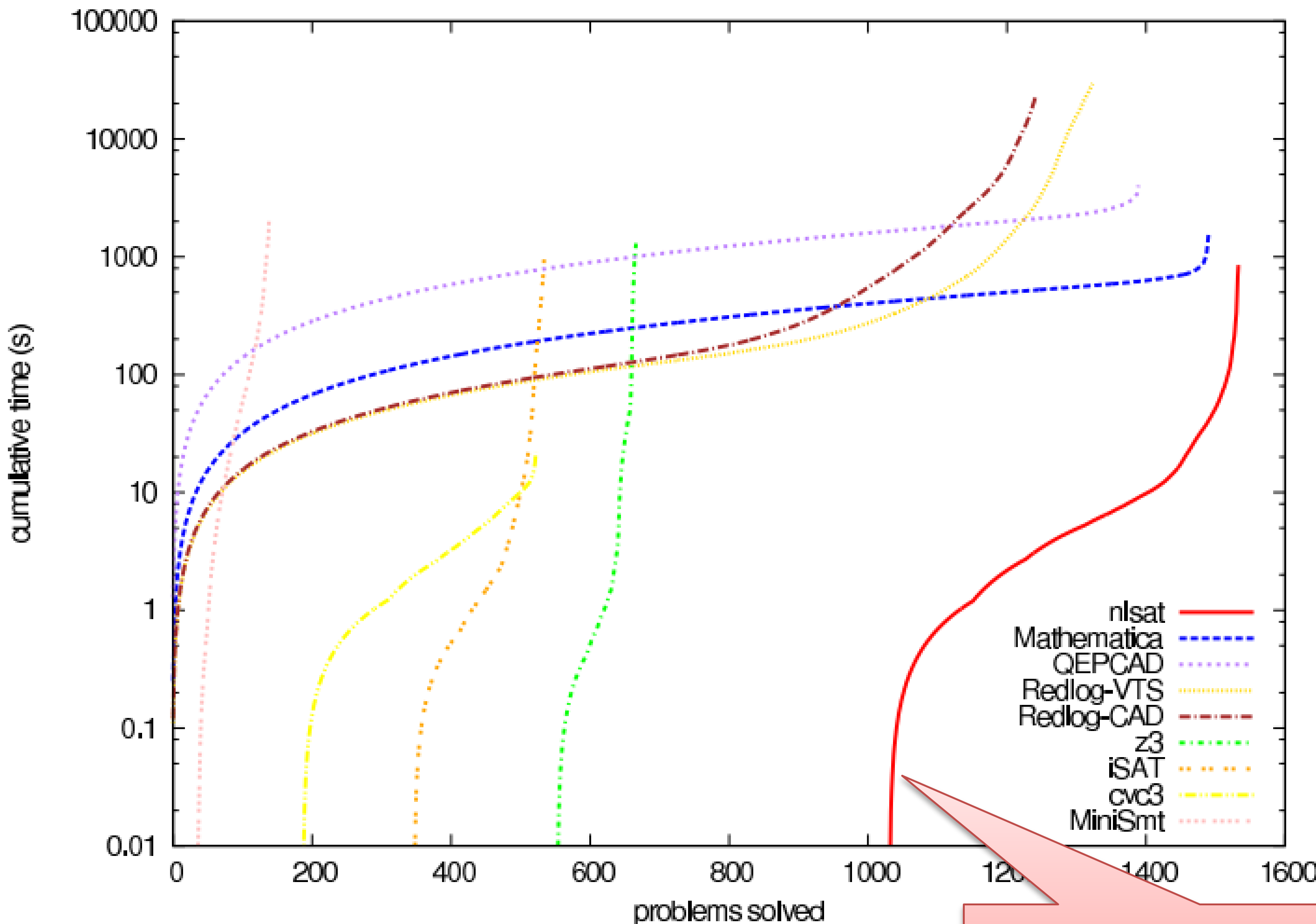
Model guides the saturation

Experimental Results (1)

OUR NEW ENGINE

	meti-tarski (1006)		keymaera (421)		zankl (166)		hong (20)		kissing (45)		all (1658)	
solver	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
nlsat	1002	343	**420**	**5**	**89**	**234**	10	170	13	95	**1534**	**849**
Mathematica	**1006**	**796**	420	171	50	366	9	208	6	29	1491	1572
QEPCAD	991	2616	368	1331	21	38	6	43	4	5	1390	4036
Redlog-VTS	847	28640	419	78	42	490	6	3	10	275	1324	29488
Redlog-CAD	848	21706	363	730	21	173	6	2	4	0	1242	22613
z3	266	83	379	1216	21	0	1	0	0	0	667	1299
iSAT	203	122	291	16	21	24	**20**	**822**	0	0	535	986
cvc3	150	13	361	5	12	3	0	0	0	0	523	22
MiniSmt	40	697	35	0	46	1370	0	0	**18**	**44**	139	2112

Experimental Results (2)



OUR NEW ENGINE

Other examples

Delayed
Theory Combination
[Bruttomesso et al 2006]

X

Model-Based
Theory Combination

Other examples

Array Theory by Axiom Instantiation

X

Lemmas on Demand For Theory of Array [Brummayer-Biere 2009]

$$\forall a, i, v: \quad a[i \coloneqq v][i] = v$$
$$\forall a, i, j, v: \; i = j \lor a[i \coloneqq v][j] = a[j]$$

Other examples
(for linear arithmetic)

Fourier-Motzkin X Generalizing DPLL to richer logics [McMillan et al 2009]

Conflict Resolution [Korovin et al 2009]

Saturation: successful instances

Polynomial time procedures

Gaussian Elimination

Congruence Closure

MCSat

Model-Driven SMT

Lift ideas from CDCL to SMT

Generalize ideas found in model-driven approaches

Easier to implement

Model construction is explicit

MCSat

$x \geq 2, \qquad (\neg x \geq 1 \vee y \geq 1), \qquad (x^2 + y^2 \leq 1 \vee xy > 1)$

MCSat

$x \geq 2,\qquad (\neg x \geq 1 \vee y \geq 1),\qquad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$

Propagations

MCSat

$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$\rightarrow x \geq 1$	

Propagations

MCSat

$x \geq 2, \qquad (\neg x \geq 1 \vee y \geq 1), \qquad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2 \rightarrow x \geq 1 \rightarrow y \geq 1$

Propagations

MCSat

$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$\rightarrow x \geq 1$	$\rightarrow y \geq 1$	$x^2 + y^2 \leq 1$	

Boolean Decisions

MCSat

$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$x \geq 1$	$y \geq 1$	$x^2 + y^2 \leq 1$	$x \to 2$	

Semantic Decisions

MCSat

$x \geq 2,\quad (\neg x \geq 1 \vee y \geq 1),\quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$x \geq 1$	$y \geq 1$	$x^2 + y^2 \leq 1$	$x \to 2$	

Conflict

We can't find a value for y
s.t. $4 + y^2 \leq 1$

MCSat

$x \geq 2$, $(\neg x \geq 1 \vee y \geq 1)$, $(x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$ →	$x \geq 1$ →	$y \geq 1$	$x^2 + y^2 \leq 1$	$x \to 2$	

Conflict

We can't find a value for y s.t. $4 + y^2 \leq 1$

Learning that $\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$ is not productive

MCSat

$x \geq 2,\quad (\neg x \geq 1 \vee y \geq 1),\quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2 \to$	$x \geq 1 \to$	$y \geq 1$	$x^2 + y^2 \leq 1 \to$	$\neg(x = 2)$	

$\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$

Learning that
$\neg(x^2 + y^2 \leq 1) \vee \neg(x= 2)$
is not productive

MCSat

$x \geq 2,\quad (\neg x \geq 1 \vee y \geq 1),\quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$x \geq 1$	$y \geq 1$	$x^2 + y^2 \leq 1$	$\neg(x = 2)$	$x \rightarrow 3$

$\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$

Learning that
$\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$
is not productive

MCSat

$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2 \rightarrow x \geq 1 \rightarrow y \geq 1$ | $x^2 + y^2 \leq 1 \rightarrow \neg(x = 2)$ | $x \rightarrow 3$

"Same" Conflict

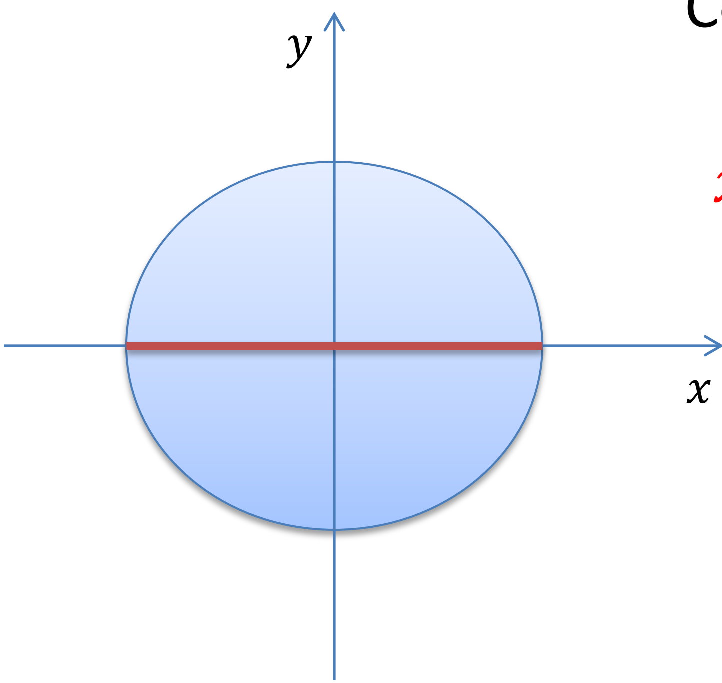
$\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$

We can't find a value for y
s.t. $9 + y^2 \leq 1$

Learning that
$\neg(x^2 + y^2 \leq 1) \vee \neg(x = 2)$
is not productive

$$x \geq 2, \qquad (\neg x \geq 1 \lor y \geq 1), \qquad (x^2 + y^2 \leq 1 \lor xy > 1)$$

$x \geq 2$ →	$x \geq 1$ →	$y \geq 1$	$x^2 + y^2 \leq 1$	$x \to 2$	



Conflict

$x^2 + y^2 \leq 1$

$x \to 2$

$-1 \leq x, x \leq 1$

$\neg(x^2 + y^2 \leq 1) \lor x \leq 1$

MCSat

$x \geq 2, \qquad (\neg x \geq 1 \vee y \geq 1), \qquad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$\rightarrow x \geq 1$	$\rightarrow y \geq 1$	$x^2 + y^2 \leq 1$	$\rightarrow x \leq 1$	

$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

MCSat

$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$\to x \geq 1$	$\to y \geq 1$	$x^2 + y^2 \leq 1$	$\to x \leq 1$	

$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

Conflict

$\neg(x \geq 2) \vee \neg(x \leq 1)$

MCSat

$x \geq 2, \qquad (\neg x \geq 1 \vee y \geq 1), \qquad (x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$\rightarrow x \geq 1$	$\rightarrow y \geq 1$	$x^2 + y^2 \leq 1$		

$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

Learned by resolution

$\neg(x \geq 2) \vee \neg(x^2 + y^2 \leq 1)$

MCSat

$x \geq 2$, $(\neg x \geq 1 \vee y \geq 1)$, $(x^2 + y^2 \leq 1 \vee xy > 1)$

$x \geq 2$	$x \geq 1$	$y \geq 1$	$\neg(x^2 + y^2 \leq 1)$	

$\neg(x \geq 2) \vee \neg(x^2 + y^2 \leq 1)$

$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

MCSat: FM Example

$-x + z + 1 \leq 0$	$z \to 0$	$x - y \leq 0$	$y \to 0$	

$-x + z + 1 \leq 0, \quad x - y \leq 0$ $\qquad$ $z \to 0, \quad y \to 0$

$$\equiv$$

$z + 1 \leq x, \quad x \leq y$

$1 \leq x, \quad x \leq 0$

We can't find a value of x

MCSat: FM Example

$-x+z+1 \leq 0$	$z \to 0$	$x-y \leq 0$	$y \to 0$	

$-x+z+1 \leq 0, \quad x-y \leq 0 \qquad\qquad z \to 0, \quad y \to 0$

$$\exists x: -x+z+1 \leq 0 \ \wedge \ x-y \leq 0$$

Fourier-Motzkin

$$z+1-y \leq 0$$

$$\neg(-x+z+1 \leq 0) \vee \neg(x-y \leq 0) \vee z+1-y \leq 0$$

MCSat: FM Example

$-x+z+1 \leq 0$	$z \to 0$	$x-y \leq 0$	$z+1-y \leq 0$	

$$\neg(-x+z+1 \leq 0) \vee \neg(x-y \leq 0) \vee z+1-y \leq 0$$

MCSat: FM Example

$-x+z+1 \leq 0$	$z \to 0$	$x-y \leq 0$	$z+1-y \leq 0$	$y \to 1$

$$\neg(-x+z+1 \leq 0) \vee \neg(x-y \leq 0) \vee z+1-y \leq 0$$

$$-x+z+1 \leq 0, \quad x-y \leq 0 \qquad\qquad z \to 0, \quad y \to 1$$

$$\equiv$$

$$z+1 \leq x, \quad x \leq y$$

$$1 \leq x, \quad x \leq 1$$

MCSat: FM Example

$-x+z+1 \leq 0$	$z \to 0$	$x - y \leq 0$	$z + 1 - y \leq 0$	$y \to 1$	$x \to 1$

$$\neg(-x+z+1 \leq 0) \vee \neg(x - y \leq 0) \vee z + 1 - y \leq 0$$

$$-x+z+1 \leq 0, \quad x - y \leq 0 \qquad\qquad z \to 0, \quad y \to 1$$

$$\equiv$$

$$z + 1 \leq x, \quad x \leq y$$

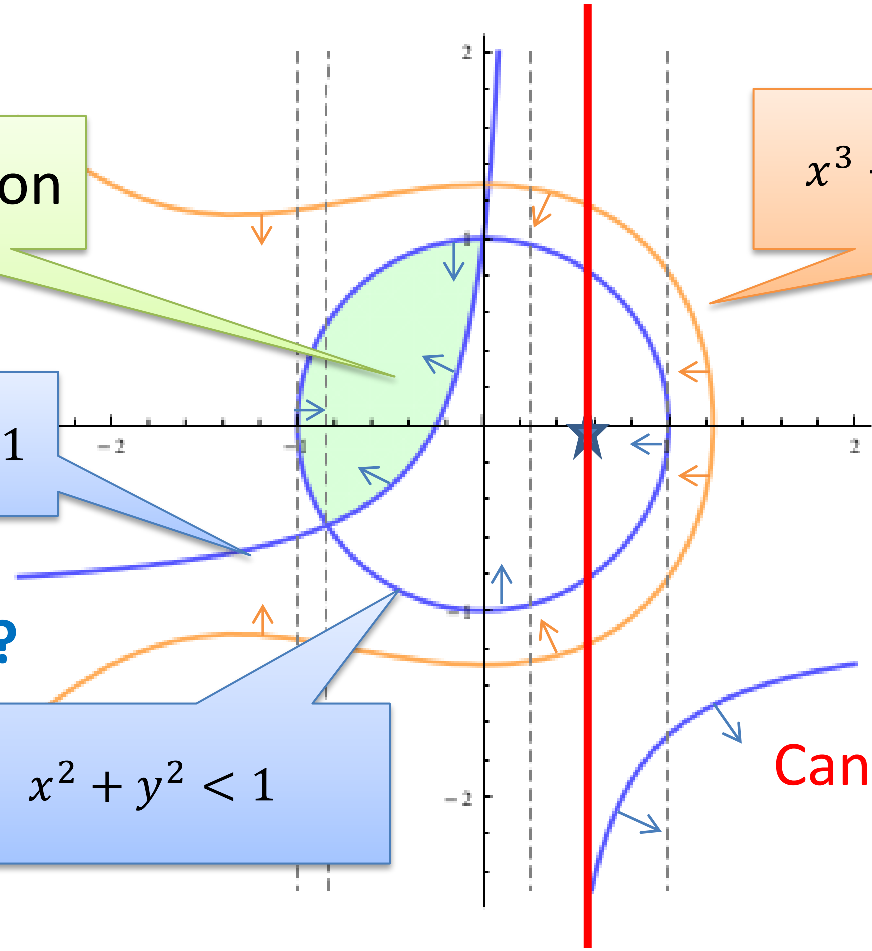
$$1 \leq x, \quad x \leq 1$$

MCSat: Another Example

$$-4xy - 4x + y > 1, \qquad x^2 + y^2 < 1, \qquad x^3 + 2x^2 + 3y^2 - 5 < 0$$

MCSat: Another Example

$$-4xy - 4x + y > 1, \qquad x^2 + y^2 < 1, \qquad x^3 + 2x^2 + 3y^2 - 5 < 0$$



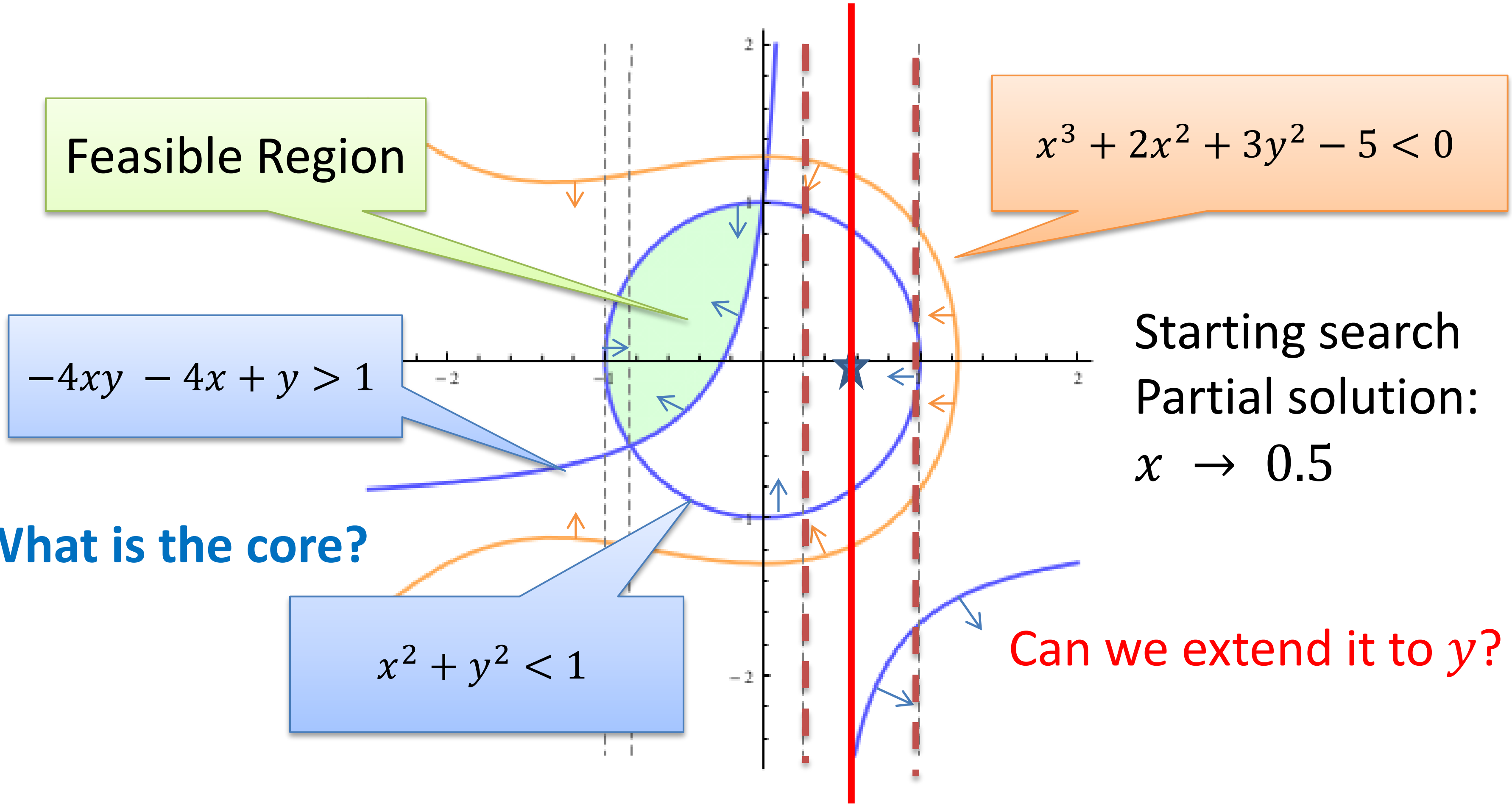
Starting search
Partial solution:
$x \to 0.5$

What is the core?

Can we extend it to y?

MCSat: Another Example

$-4xy - 4x + y > 1, \quad x^2 + y^2 < 1, \quad x^3 + 2x^2 + 3y^2 - 5 < 0$



Starting search
Partial solution:
$x \rightarrow 0.5$

What is the core?

Can we extend it to y?

MCSat – Finite Basis

Every theory that admits quantifier elimination has a finite basis (given a fixed assignment order)

$$F[x, y_1, \dots, y_m]$$

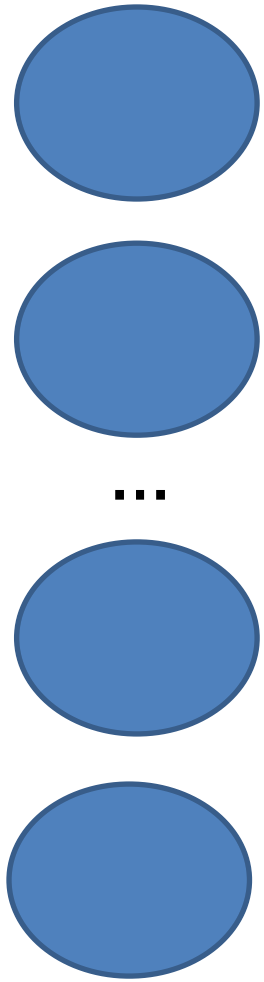
$$y_1 \to \alpha_1, \dots, y_m \to \alpha_m$$

$$\exists x: F[x, y_1, \dots, y_m]$$

$$C_1[y_1, \dots, y_m] \wedge \cdots \wedge C_k[y_1, \dots, y_m]$$

$$\neg F[x, y_1, \dots, y_m] \vee C_k[y_1, \dots, y_m]$$

MCSat – Finite Basis



$F_n[x_{1,}x_2, \dots, x_{n-1}, x_n]$

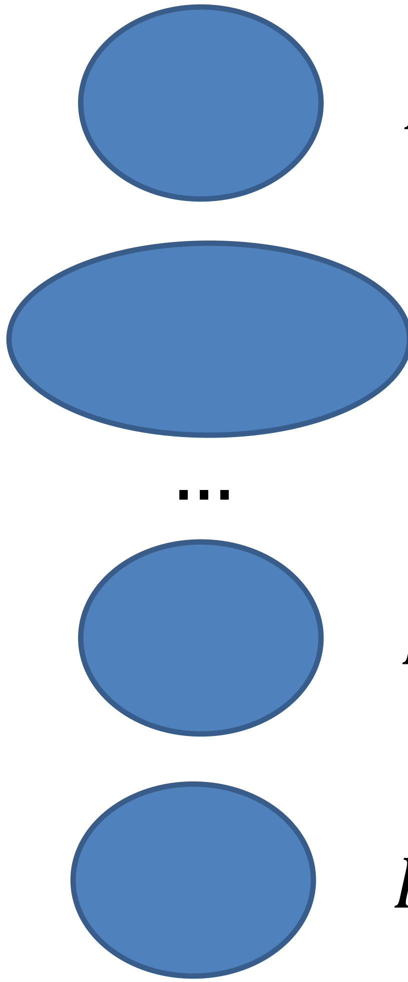
$F_{n-1}[x_{1,}x_2, \dots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

MCSat – Finite Basis



$F_n[x_{1,}x_2, \ldots, x_{n-1}, x_n]$

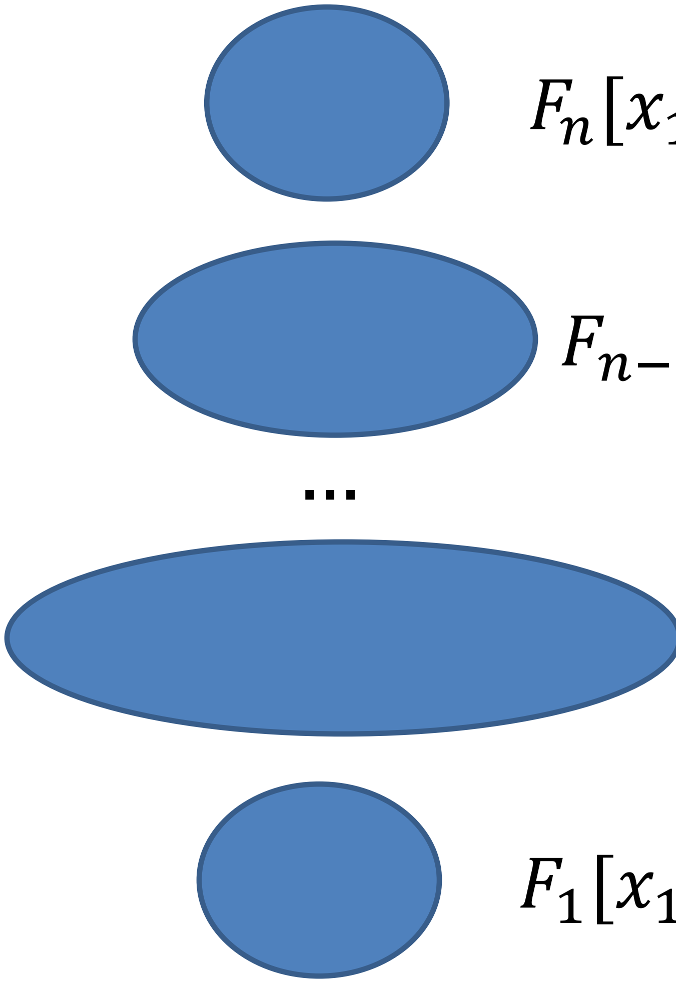
$F_{n-1}[x_{1,}x_2, \ldots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

MCSat – Finite Basis



$F_n[x_{1,}x_2, \ldots, x_{n-1}, x_n]$

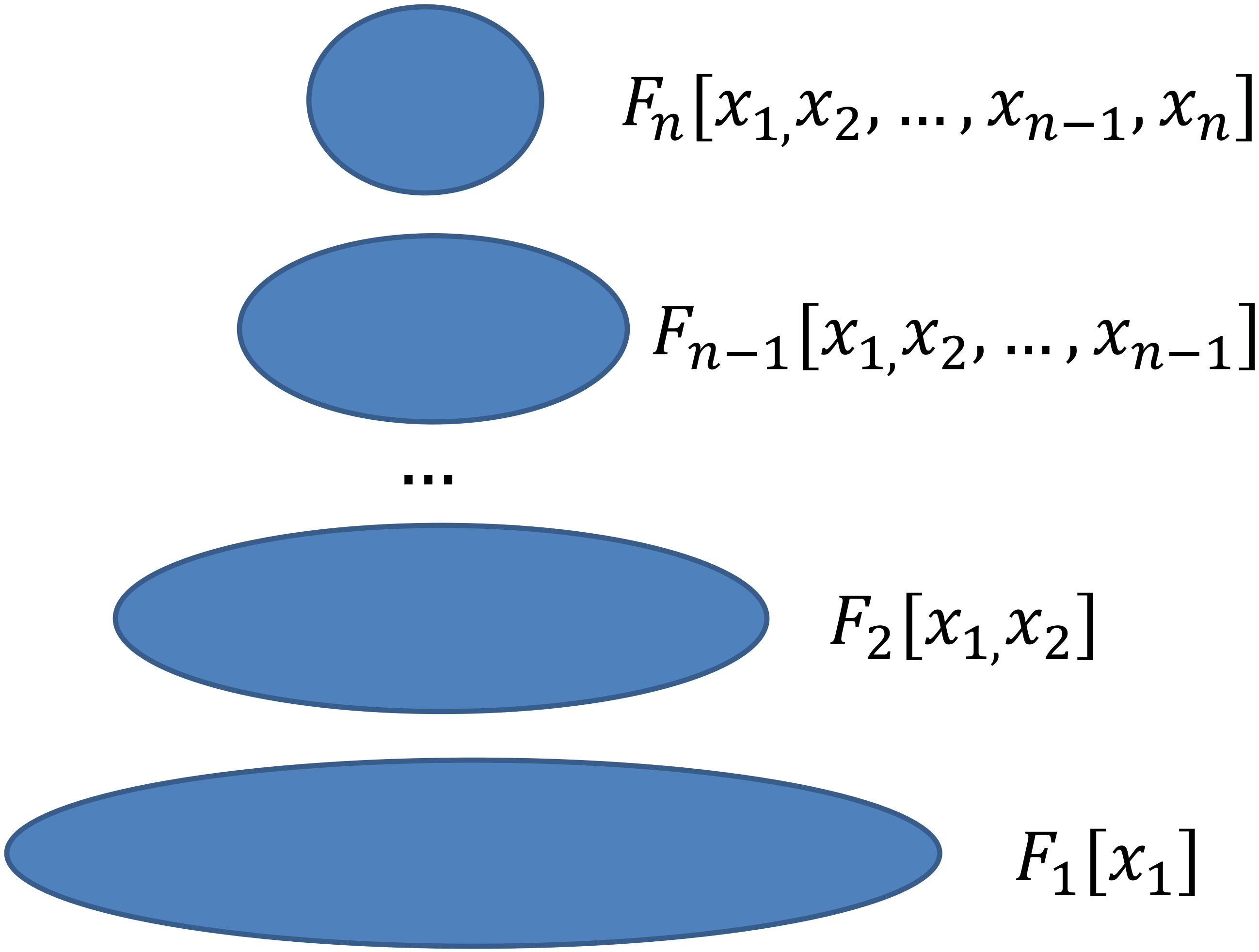
$F_{n-1}[x_{1,}x_2, \ldots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

MCSat – Finite Basis



MCSat – Finite Basis

Every "finite" theory has a finite basis

Example: Fixed size Bit-vectors

$$F[x, y_1, \ldots, y_m] \qquad\qquad y_1 \to \alpha_1, \ldots, y_m \to \alpha_m$$

$$\neg F[x, y_1, \ldots, y_m] \vee \neg(y_1 = \alpha_1) \vee \cdots \vee \neg(y_m = \alpha_m)$$

MCSat – Finite Basis

Theory of uninterpreted functions has a finite basis

Theory of arrays has a finite basis [Brummayer- Biere 2009]

In both cases the Finite Basis is essentially composed of equalities between existing terms.

MCSat: Uninterpreted Functions

$$a = b + 1, f(a - 1) < c, f(b) > a$$

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$

Treat $f(k)$ and $f(b)$ as variables
Generalized variables

MCSat: Uninterpreted Functions

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$

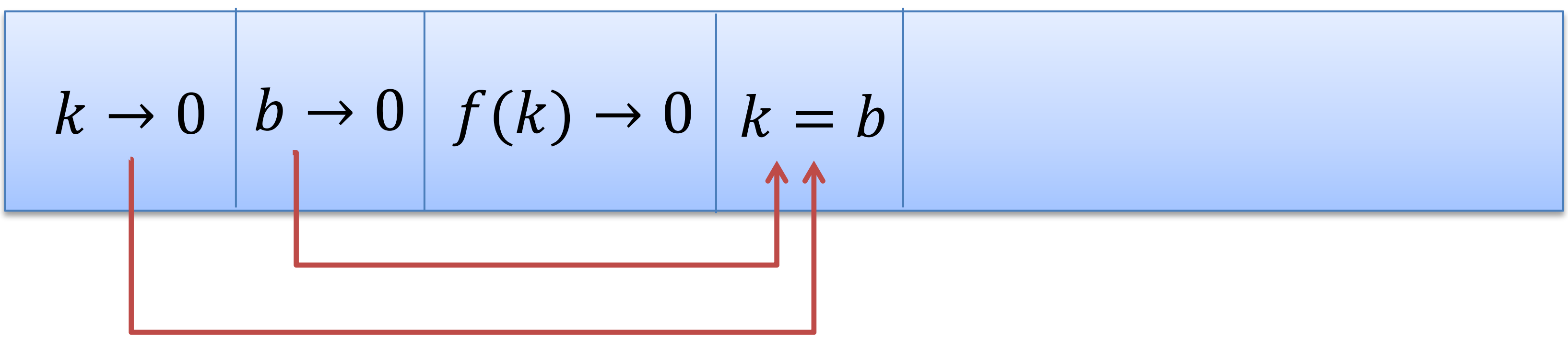
$k \to 0$	$b \to 0$	$f(k) \to 0$	$f(b) \to 2$	

Conflict: $f(k)$ and $f(b)$ must be equal

$$\neg(k = b) \vee f(k) = f(b)$$

MCSat: Uninterpreted Functions

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$



(Semantic) Propagation

$$\neg(k = b) \vee f(k) = f(b)$$

MCSat: Uninterpreted Functions

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$

$k \to 0$	$b \to 0$	$f(k) \to 0$	$k = b$	$\to f(k) = f(b)$

$$\neg(k = b) \lor f(k) = f(b)$$

MCSat: Uninterpreted Functions

$$a = b + 1, f(k) < c, f(b) > a, k = a - 1$$

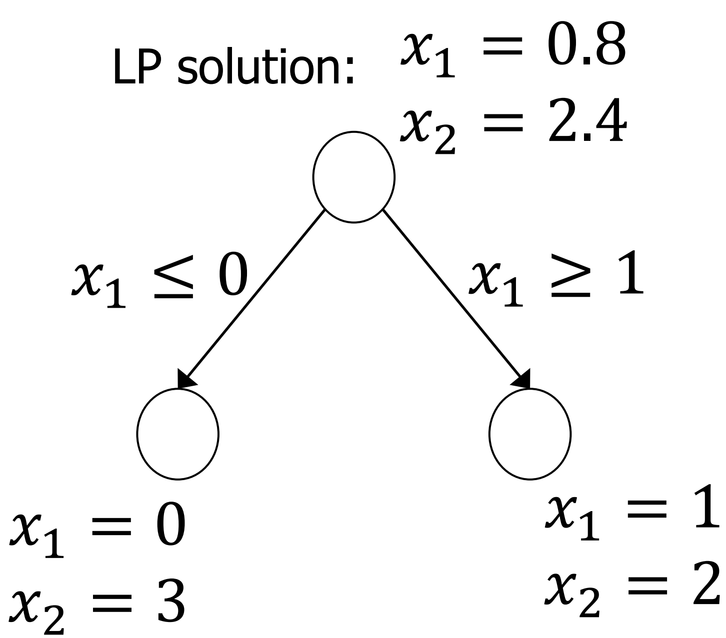
$k \to 0$	$b \to 0$	$f(k) \to 0$	$k = b$	$f(k) = f(b)$	$f(b) \to 0$

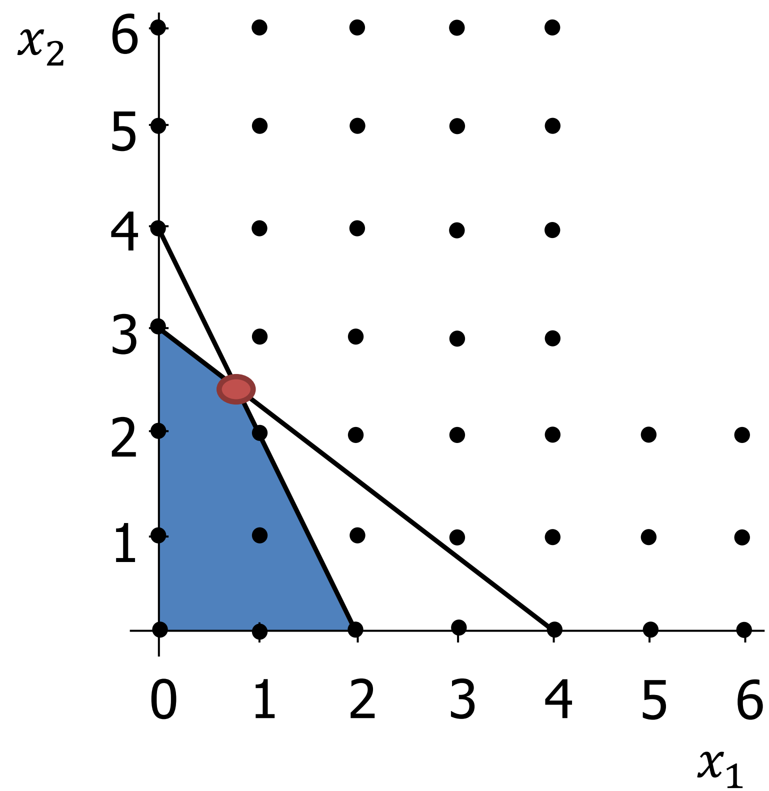
$$\neg(k = b) \vee f(k) = f(b)$$

MCSat – Finite Basis

We can also use literals from the finite basis in decisions.

Application: simulate branch&bound for bounded linear integer arithmetic



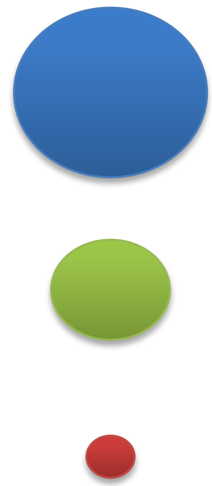


MCSat: Termination

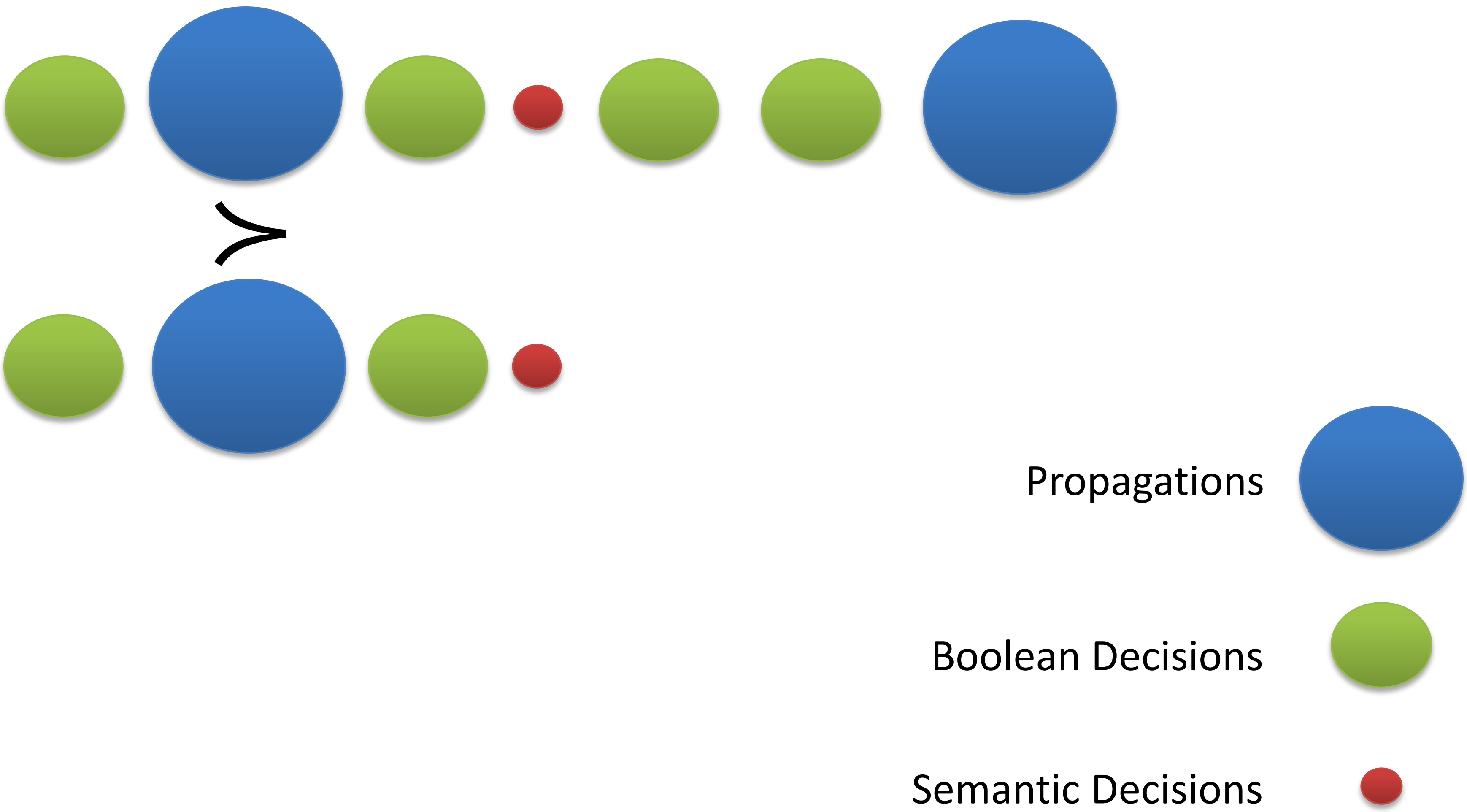
Propagations

Boolean Decisions

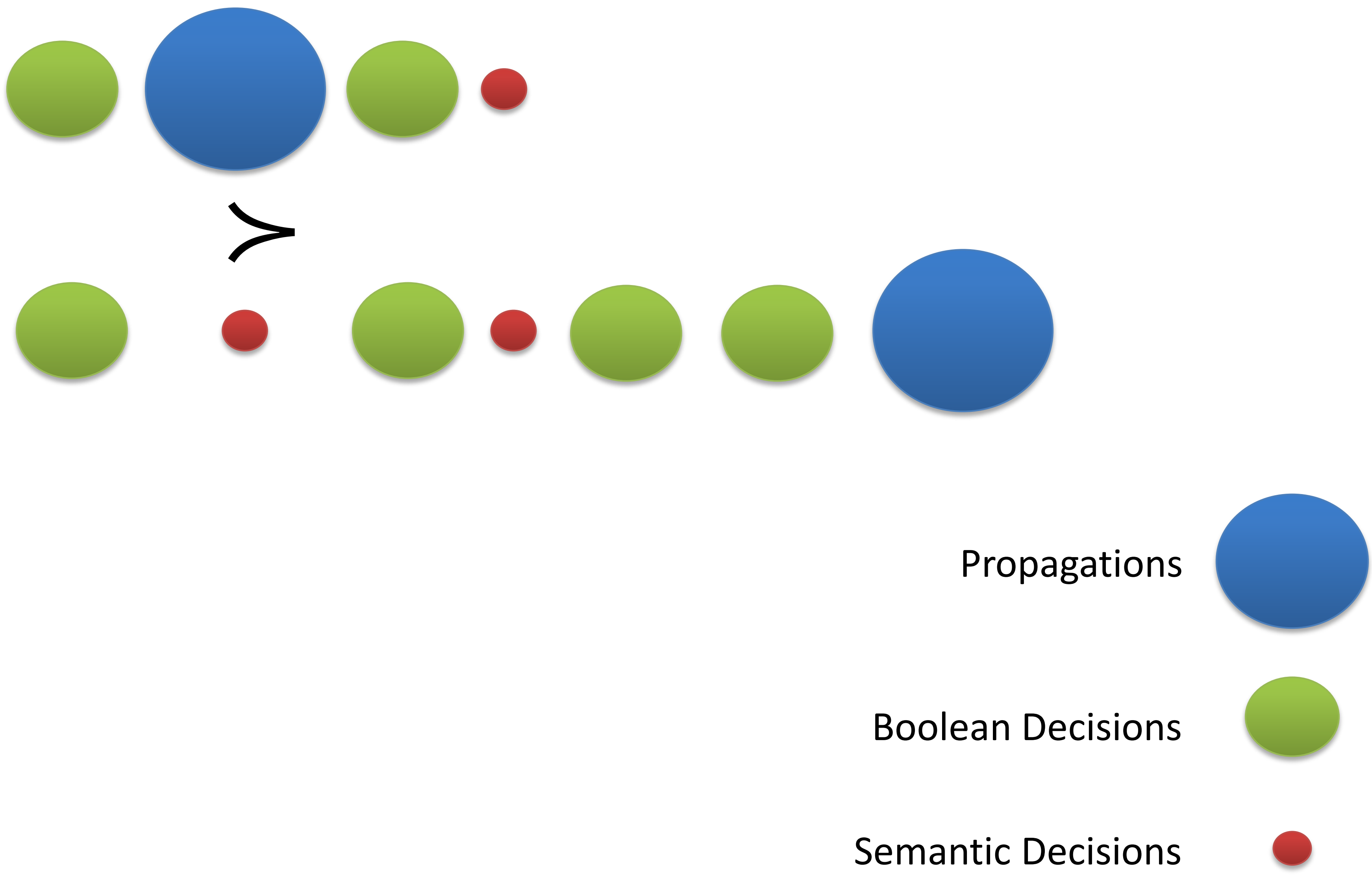
Semantic Decisions



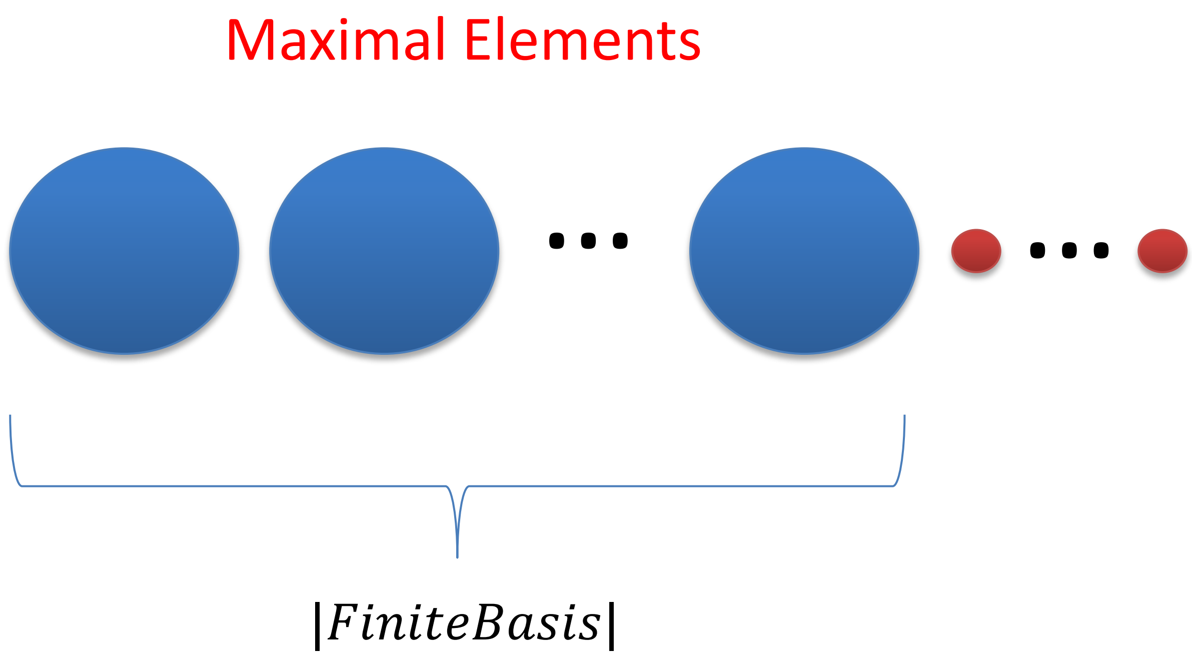
MCSat



MCSat



MCSat



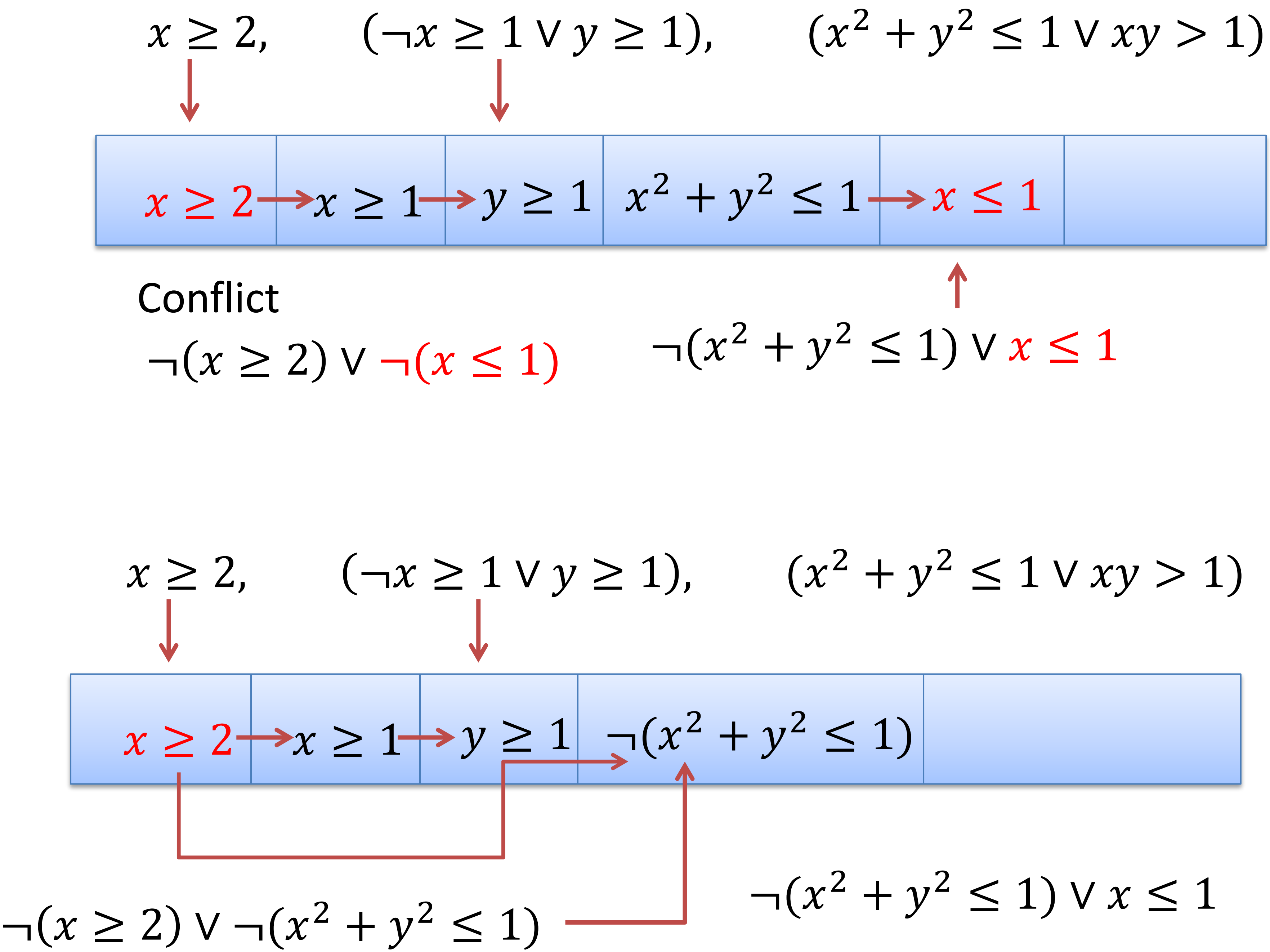
$x \geq 2, \quad (\neg x \geq 1 \lor y \geq 1), \quad (x^2 + y^2 \leq 1 \lor xy > 1)$

$x \geq 2 \rightarrow$	$x \geq 1 \rightarrow$	$y \geq 1$	$x^2 + y^2 \leq 1 \rightarrow$	$x \leq 1$	

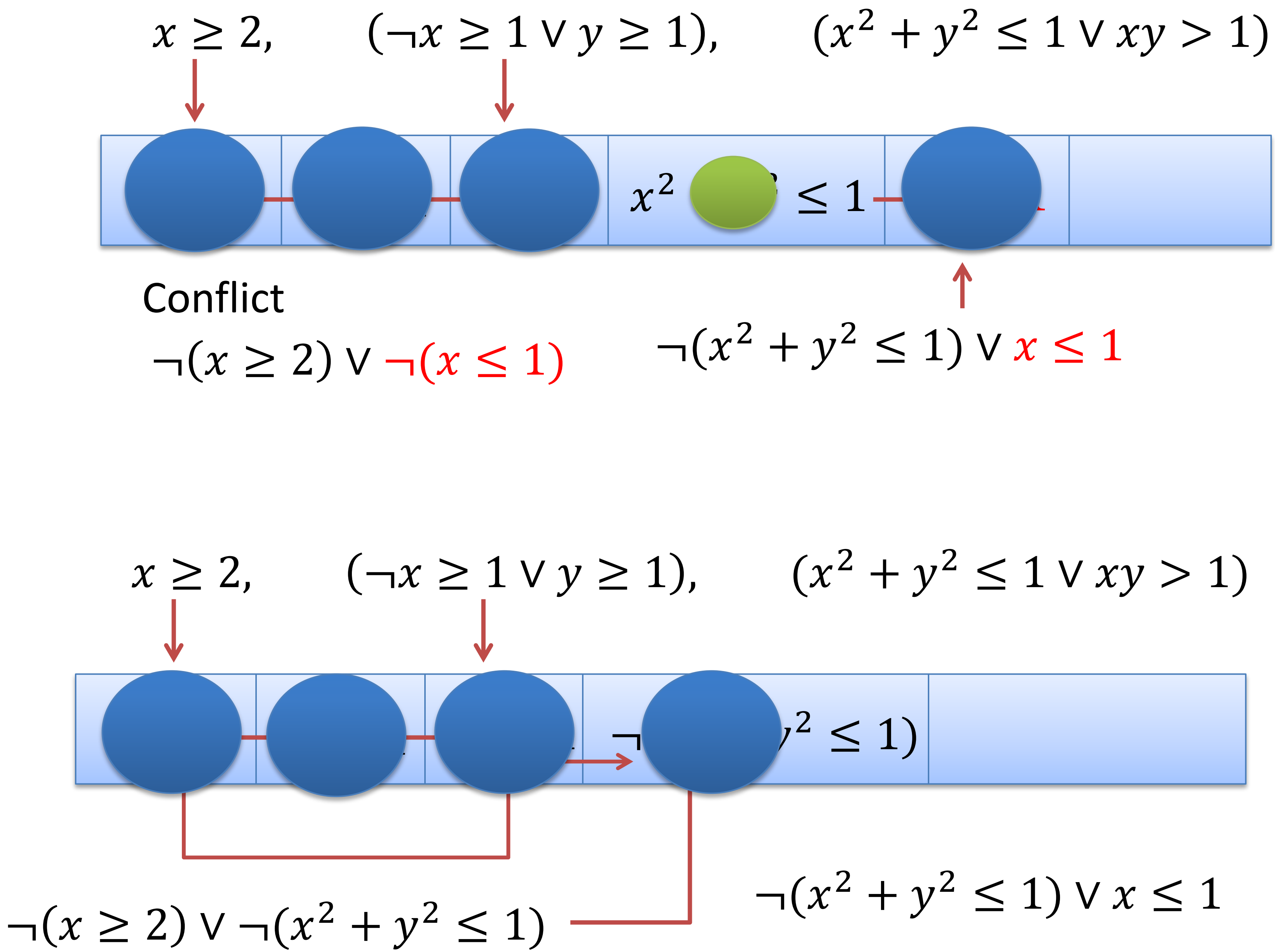
Conflict

$\neg(x \geq 2) \lor \neg(x \leq 1)$

$\neg(x^2 + y^2 \leq 1) \lor x \leq 1$



$x \geq 2,$
$(\neg x \geq 1 \vee y \geq 1),$
$(x^2 + y^2 \leq 1 \vee xy > 1)$
$x \geq 2$
$x \geq 1$
$y \geq 1$
$x^2 + y^2 \leq 1$
$x \leq 1$
Conflict
$\neg(x \geq 2) \vee \neg(x \leq 1)$
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$
$x \geq 2,$
$(\neg x \geq 1 \vee y \geq 1),$
$(x^2 + y^2 \leq 1 \vee xy > 1)$
$x \geq 2$
$x \geq 1$
$y \geq 1$
$\neg(x^2 + y^2 \leq 1)$
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$
$\neg(x \geq 2) \vee \neg(x^2 + y^2 \leq 1)$


$x \geq 2,$
$(\neg x \geq 1 \vee y \geq 1),$
$(x^2 + y^2 \leq 1 \vee xy > 1)$
x^2
≤ 1
Conflict
$\neg(x \geq 2) \vee \neg(x \leq 1)$
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$
$x \geq 2,$
$(\neg x \geq 1 \vee y \geq 1),$
$(x^2 + y^2 \leq 1 \vee xy > 1)$
$\neg$
$^2 \leq 1)$
$\neg(x \geq 2) \vee \neg(x^2 + y^2 \leq 1)$
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

MCSat

$$x < 1 \vee p, \qquad \neg p \vee x = 2$$

$x \rightarrow 1$	

MCSat

$x < 1 \vee p, \qquad \neg p \vee x = 2$

$x \to 1$	p	

MCSat

$x < 1 \vee p, \qquad \neg p \vee x = 2$

$x \to 1$	p	

Conflict (evaluates to false)

MCSat

$$x < 1 \vee p, \qquad \neg p \vee x = 2$$

$x \to 1$	p	

New clause

$$x < 1 \vee x = 2$$

MCSat

$x < 1 \vee p, \qquad \neg p \vee x = 2$

$$\boxed{x \to 1 \mid p \mid \quad}$$

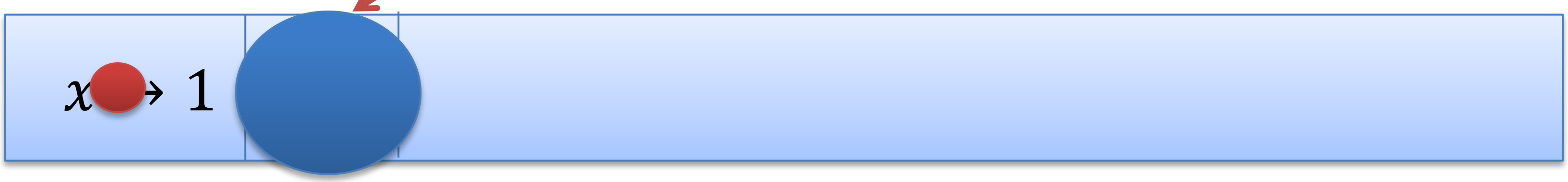
New clause

$x < 1 \vee x = 2$

$$\boxed{x < 1 \mid \quad}$$

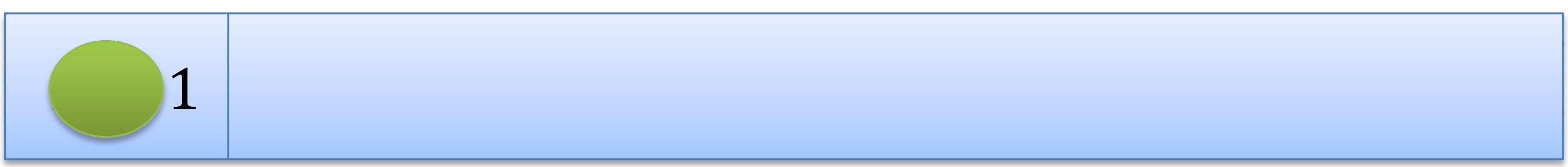
MCSat

$x < 1 \vee p, \qquad \neg p \vee x = 2$

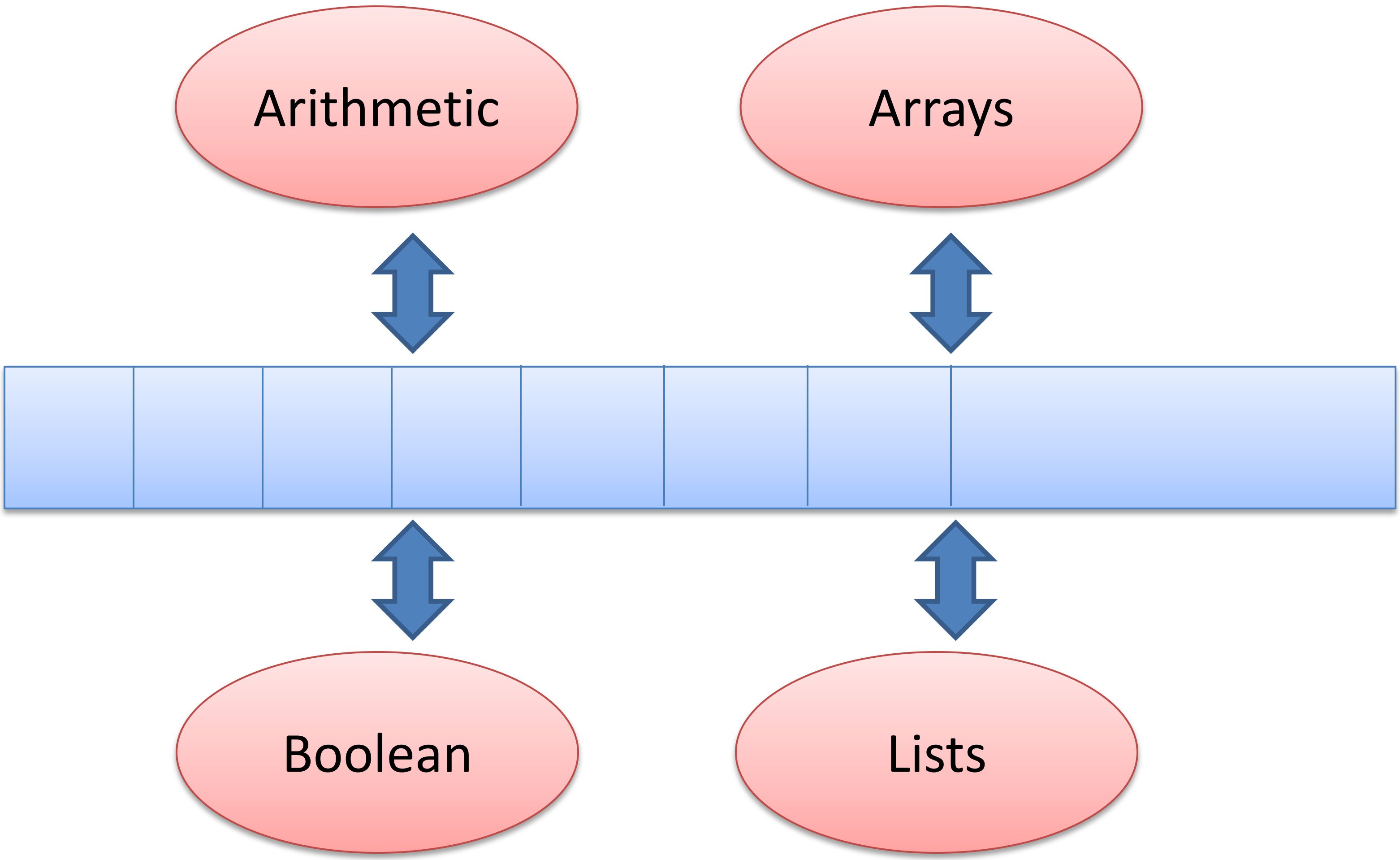


New clause

$x < 1 \vee x = 2$



MCSat: Architecture



MCSat: development

MCSat prototype: 7k lines of code

Deduction Rules

$$\frac{C \vee L \qquad \neg L \vee D}{C \vee D}$$ Boolean Resolution

$$\frac{}{\neg(p_L < x) \vee \neg(x < p_U) \vee (p_L < p_U)}$$ Fourier-Motzkin

$$\frac{}{(p = q) \vee (q < p) \vee (p < q)}$$ Equality Split

$$\frac{}{x_1 \neq y_1 \vee \cdots \vee x_k \neq y_k \vee f(x_1, \ldots, x_k) = f(y_1, \ldots, y_k)}$$ Ackermann expansion aka Congruence

$$\frac{\neg(p < q) \vee x \vee x}{(q \leq p) \vee x}$$ Normalization

MCSat: preliminary results

prototype: 7k lines of code

QF_LRA

set	mcsat		cvc4		z3		mathsat5		yices	
	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
clocksynchro (36)	**36**	**123.11**	36	1166.55	36	1828.74	36	1732.59	36	1093.80
DTPScheduling (91)	**91**	**31.33**	91	72.92	91	100.55	89	1980.96	91	926.22
miplib (42)	8	97.16	**27**	**3359.40**	23	3307.92	19	5447.46	23	466.44
sal (107)	107	12.68	107	13.46	107	6.37	107	7.99	**107**	**2.45**
sc (144)	144	1655.06	144	1389.72	144	954.42	144	880.27	**144**	**401.64**
spiderbenchmarks (42)	42	2.38	42	2.47	42	1.66	42	1.22	**42**	**0.44**
TM (25)	25	1125.21	25	82.12	**25**	**51.64**	25	1142.98	25	55.32
ttastartup (72)	70	4443.72	72	1305.93	72	1647.94	72	2607.49	**72**	**1218.68**
uart (73)	73	5244.70	73	1439.89	73	1379.90	73	1481.86	**73**	**679.54**
	596	12735.35	**617**	**8832.46**	613	9279.14	607	15282.82	613	4844.53

MCSat: preliminary results

prototype: 7k lines of code

QF_UFLRA and QF_UFLIA

	mcsat		cvc4		z3		mathsat5		yices	
set	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
EufLaArithmetic (33)	33	39.57	33	49.11	**33**	**2.53**	33	20.18	33	4.61
Hash (198)	198	34.81	198	10.60	198	7.18	198	1330.88	**198**	**2.64**
RandomCoupled (400)	400	68.04	400	35.90	400	31.44	**400**	**18.56**	384	39903.78
RandomDecoupled (500)	500	34.95	500	40.63	500	30.98	**500**	**21.86**	500	3863.79
Wisa (223)	223	9.18	223	87.35	223	10.80	223	65.27	**223**	**2.80**
wisas (108)	**108**	**40.17**	108	5221.37	108	443.36	106	1737.41	108	736.98
	1462	**226.72**	1462	5444.96	1462	526.29	1460	3194.16	1446	44514.60

Conclusion

Mode-driven techniques are very promising

Preprocessing

CEGAR

MCSat: new framework for developing SMT solvers
MCSat generalizes NLSat

Modular architecture

Resources: Papers

The Strategy Challenge in SMT Solving, L. de Moura and G. Passmore.
http://research.microsoft.com/en-us/um/people/leonardo/files/smt-strategy.pdf

Solving non-linear arithmetic, D. Jovanovic and L. de Moura
http://research.microsoft.com/en-us/um/people/leonardo/files/IJCAR2012.pdf

A Model Constructing Satisfiability Calculus, L. de Moura and D. Jovanonic
http://research.microsoft.com/en-us/um/people/leonardo/files/mcsat.pdf

The Design and Implementation of the Model Constructing Satisfiability Calculus, D. Jovanovic, C. Barrett , L. de Moura
http://research.microsoft.com/en-us/um/people/leonardo/mcsat_design.pdf

Resources: Source Code

nlsat

https://z3.codeplex.com/SourceControl/latest#src/nlsat/

mcsat

https://github.com/dddejan/CVC4/tree/mcsat

tactic/preprocessors

https://z3.codeplex.com/SourceControl/latest#src/tactic/