A Model-Constructing Satisfiability Calculus

SAT 2014

Leonardo de Moura — Microsoft Research

Dejan Jovanović — SRI International

The RISE of Model-Driven Techniques

Search x Saturation

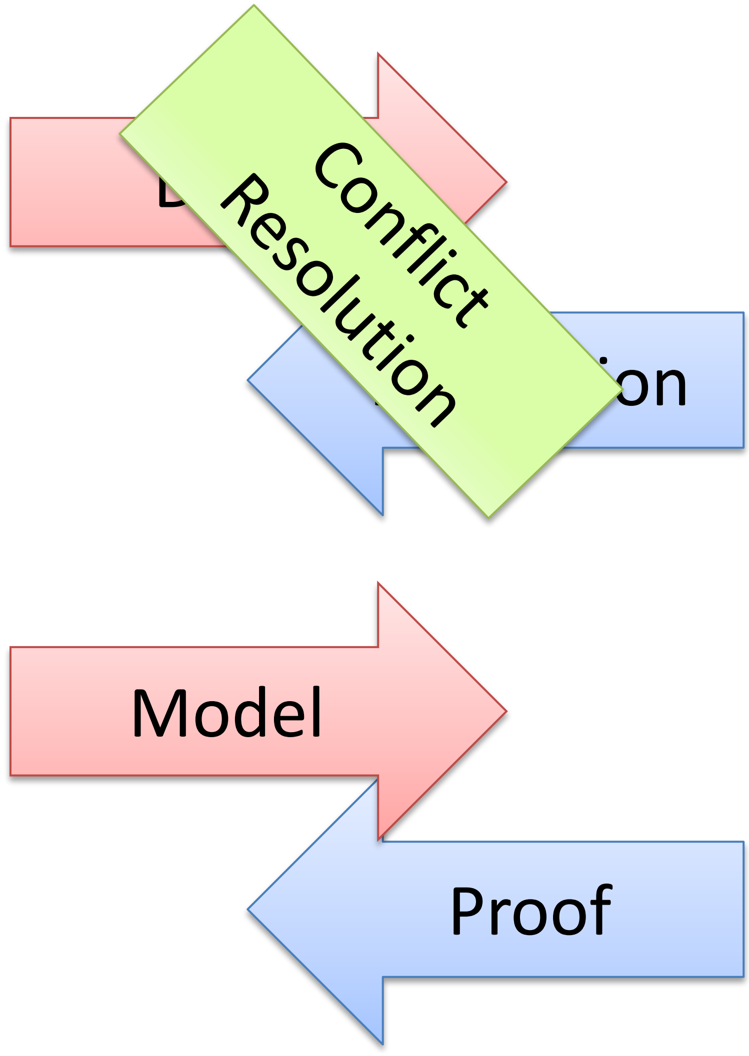
Model-finding

Proof-finding

Two procedures

Resolution	DPLL
Proof-finder	Model-finder
Saturation	Search

CDCL: Conflict Driven Clause Learning



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 $\alpha_k \in C$

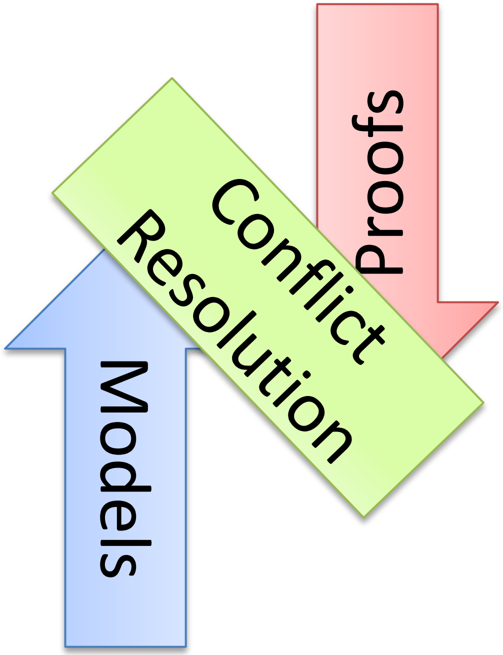
   If there is no feasible cell, then backtrack

NLSAT: Model-Based Search

Start the Search before Saturate/Project

We saturate on demand

Model guides the saturation

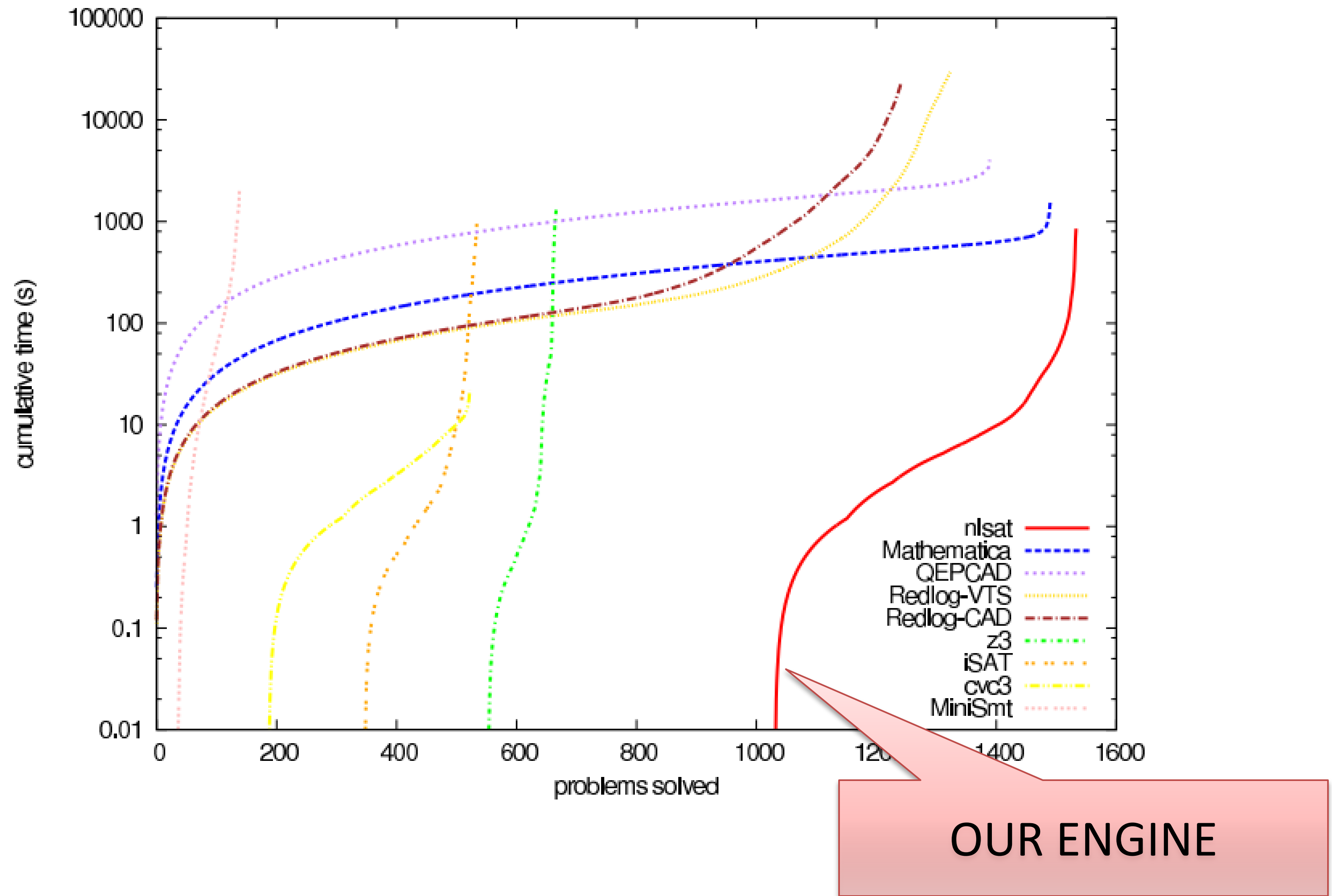


Experimental Results (1)

OUR 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)



Other examples
(for linear arithmetic)

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

Conflict Resolution [Korovin et al 2009]

Other examples

Array Theory by Axiom Instantiation

X

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

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

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

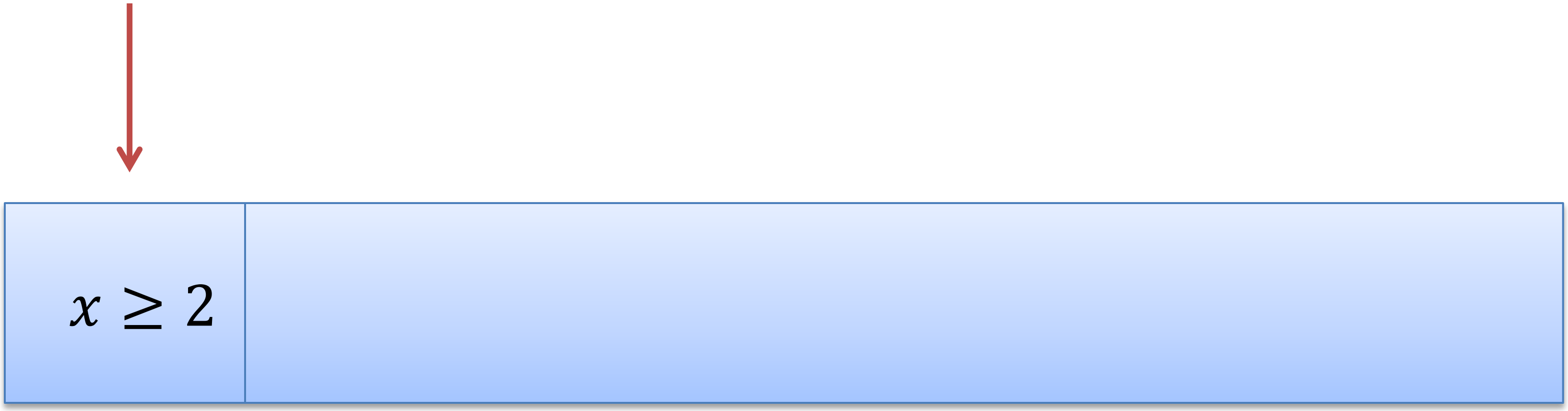
Model construction is explicit

MCSat

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

MCSat

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



Propagations

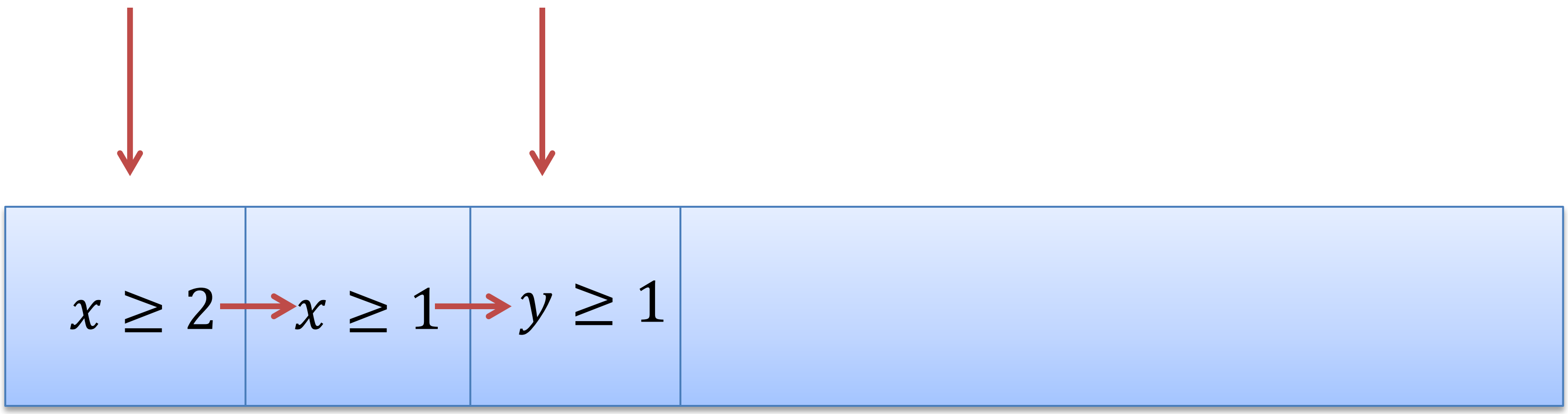
MCSat

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

Propagations

MCSat

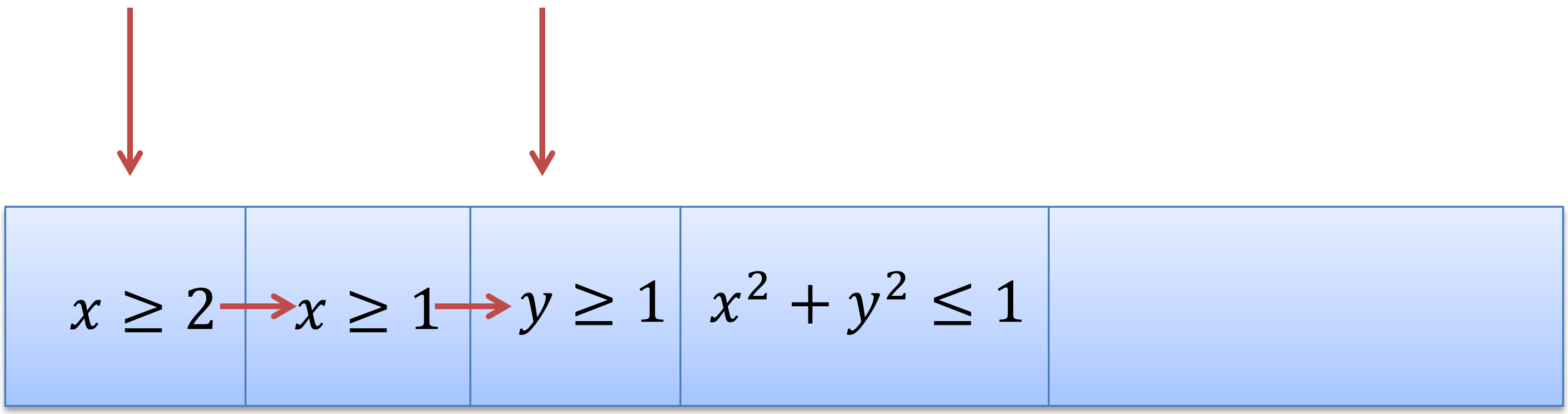
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



Propagations

MCSat

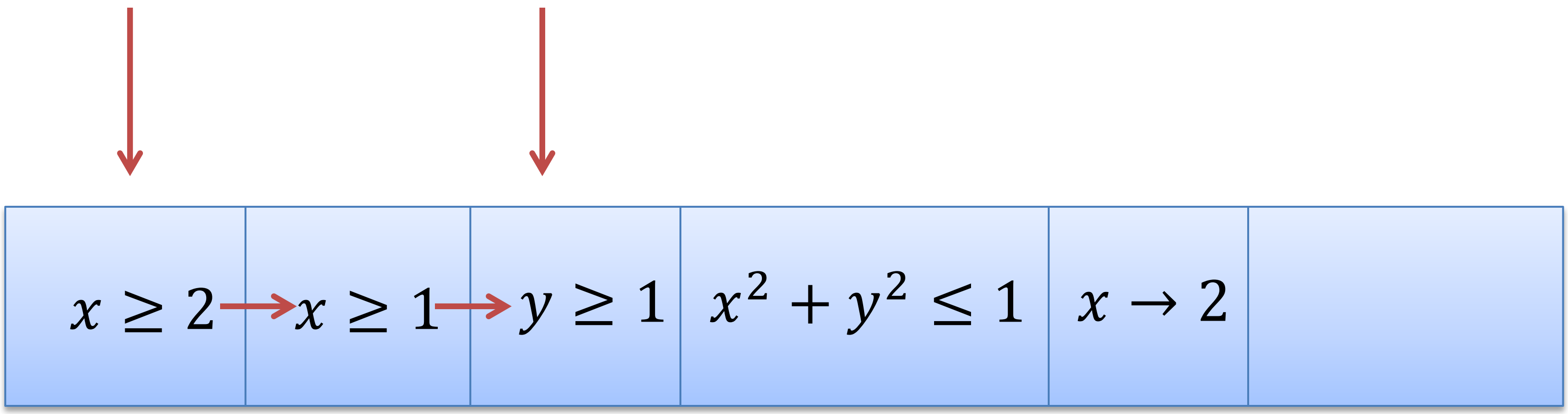
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



Boolean Decisions

MCSat

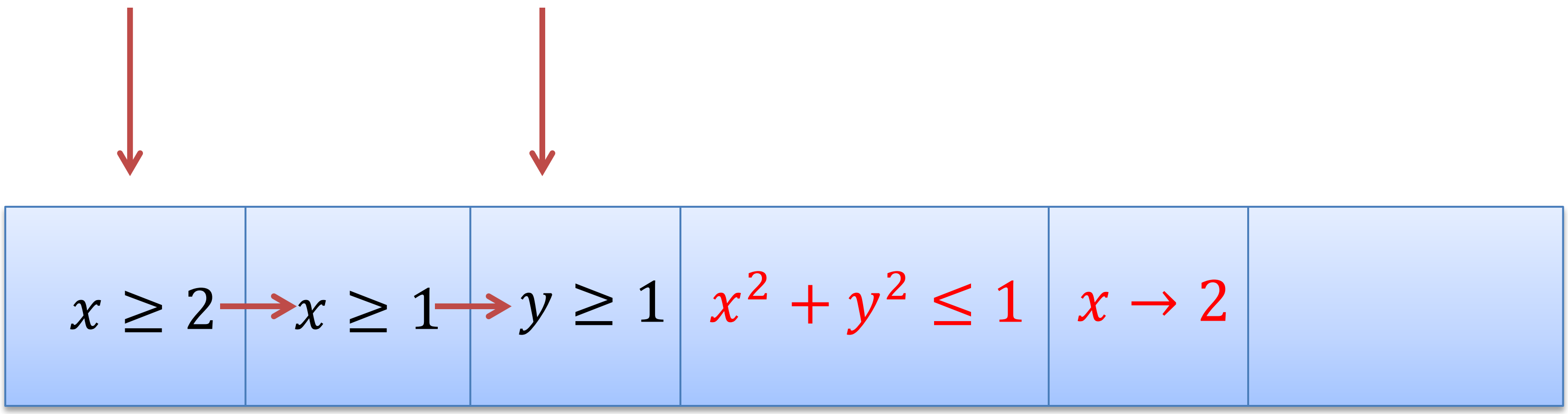
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



Semantic Decisions

MCSat

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

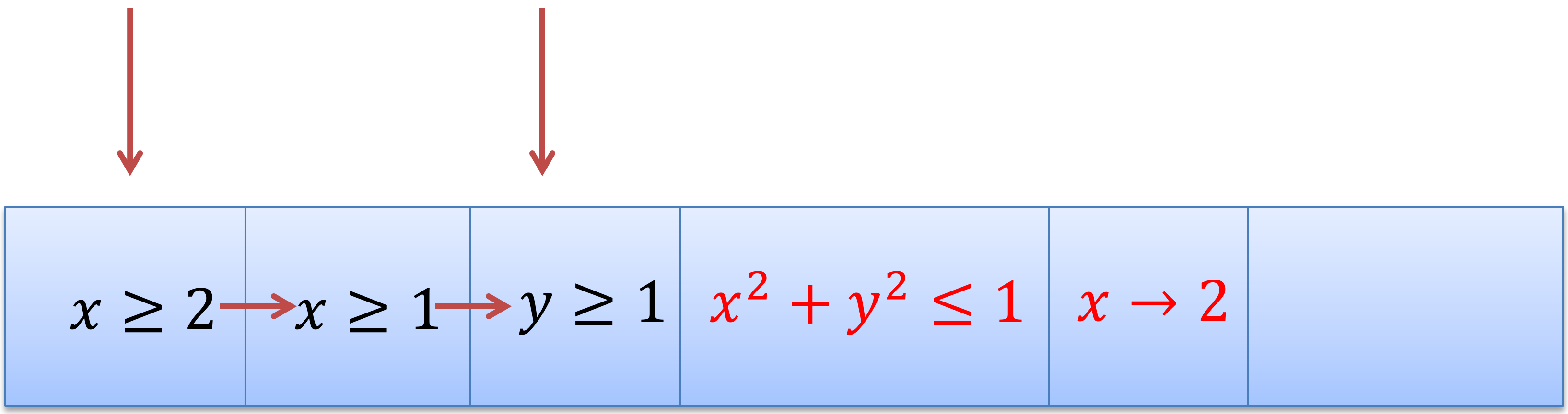


Conflict

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

MCSat

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

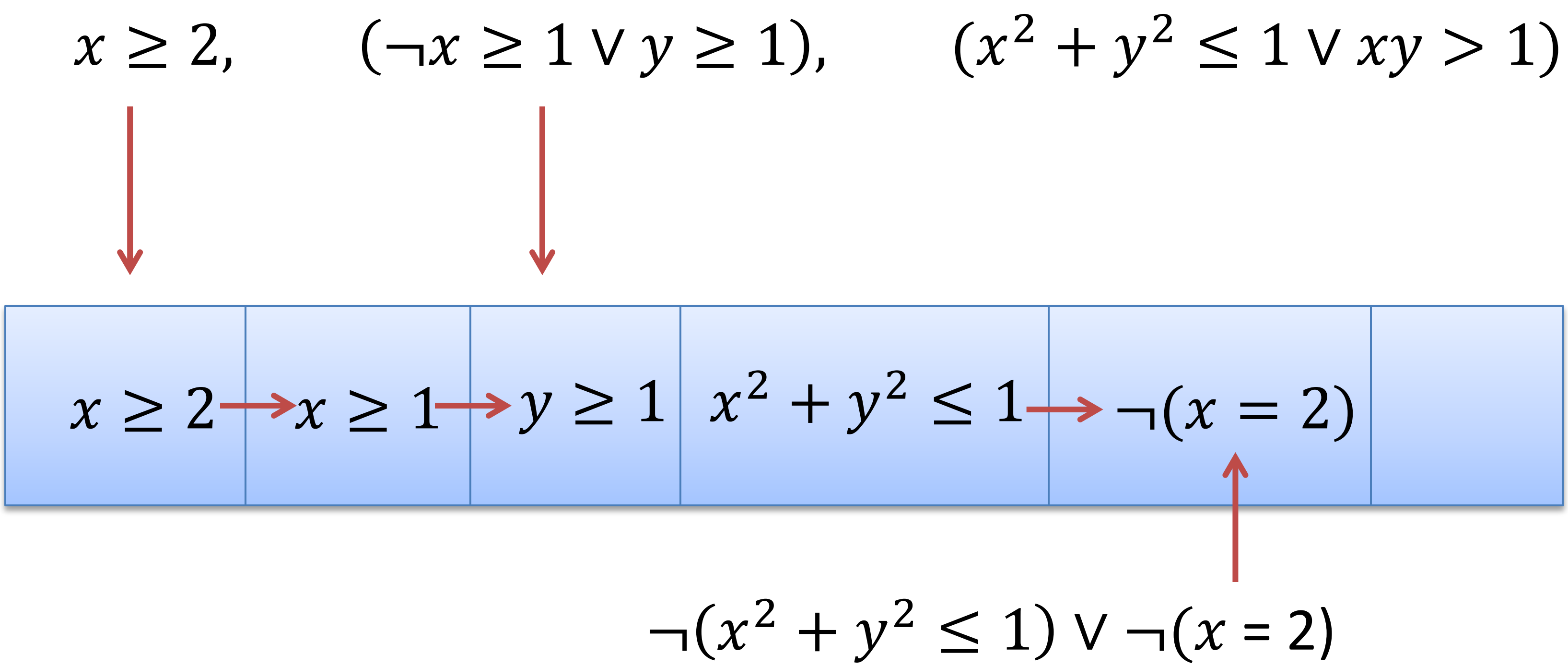


Conflict

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

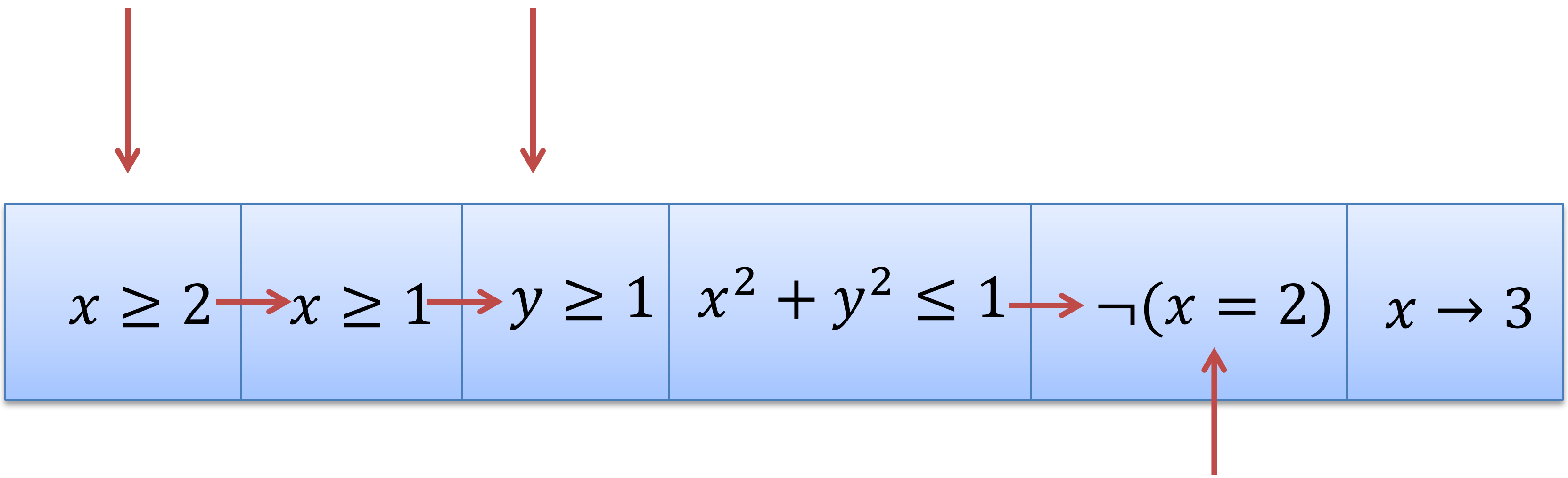
MCSat



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

MCSat

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

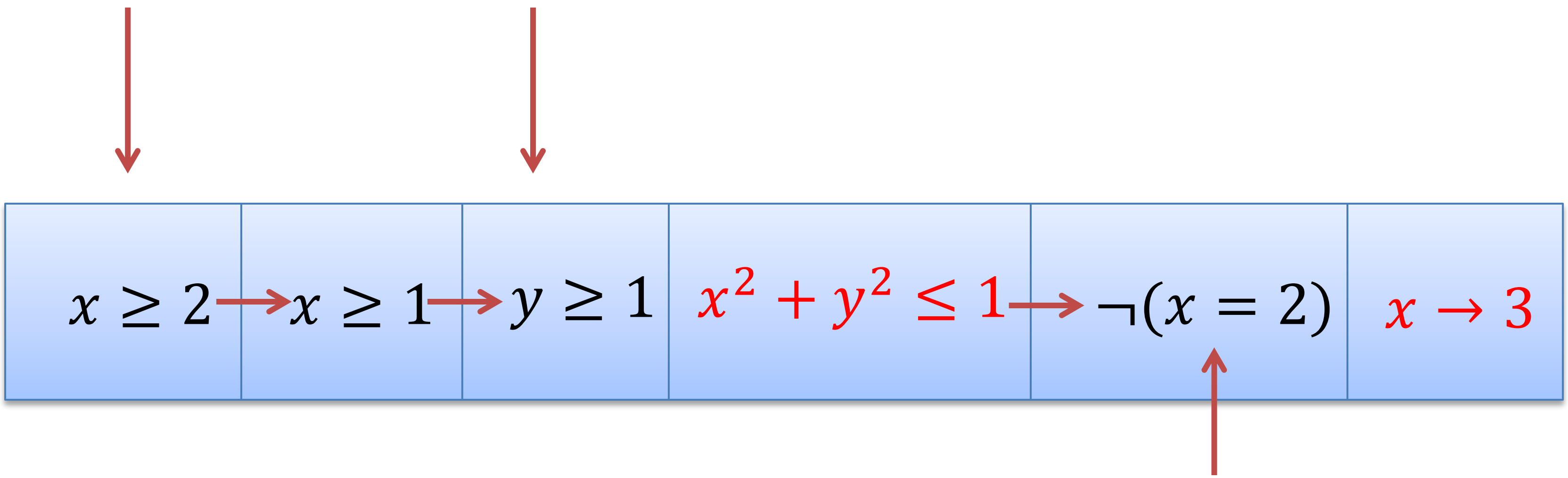


$\neg(x^2 + y^2 \leq 1) \lor \neg(x = 2)$

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

MCSat

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



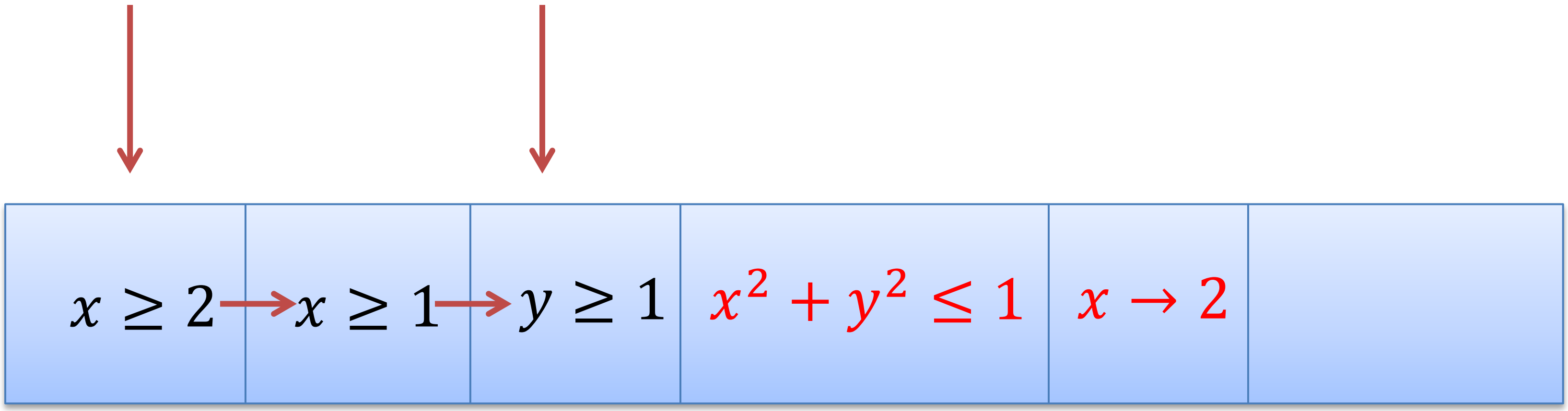
"Same" Conflict

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

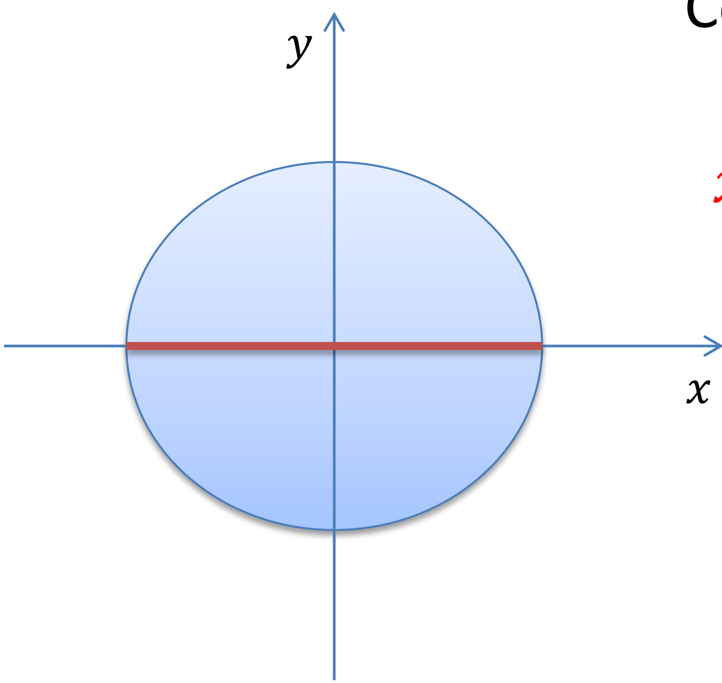
We can't find a value for y
s.t. $9 + y^2 \leq 1$

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

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



Conflict



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

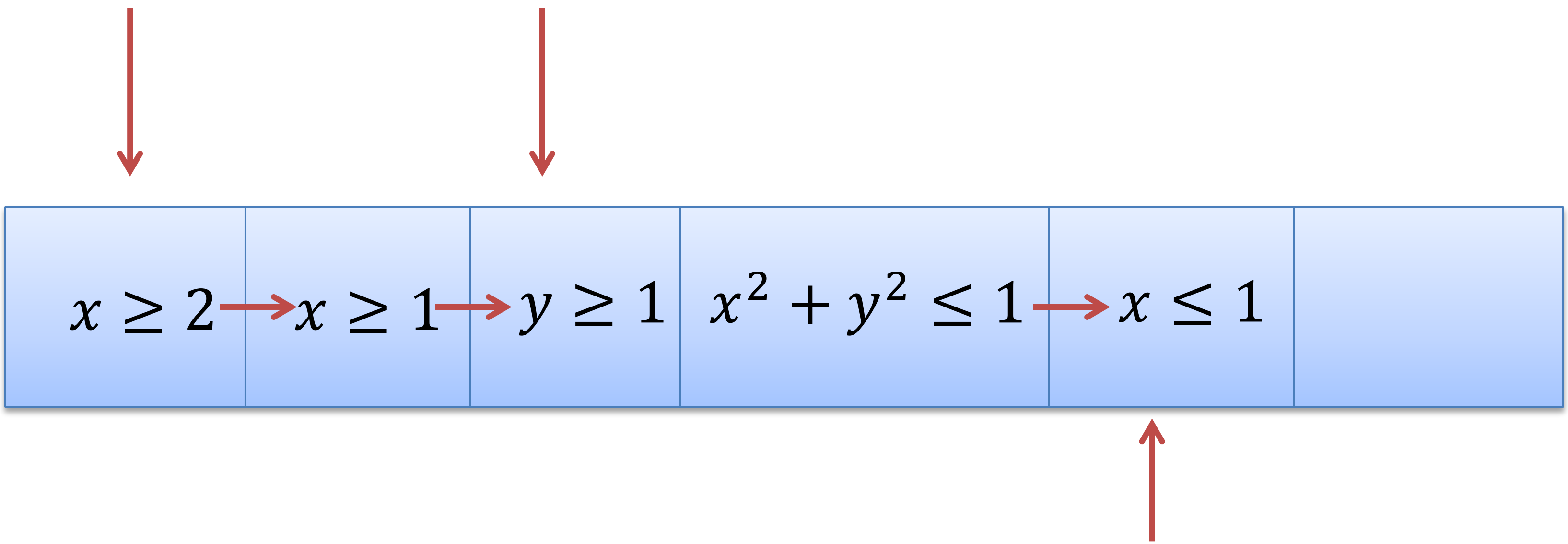
$x \to 2$

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

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

MCSat

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



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

MCSat

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

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

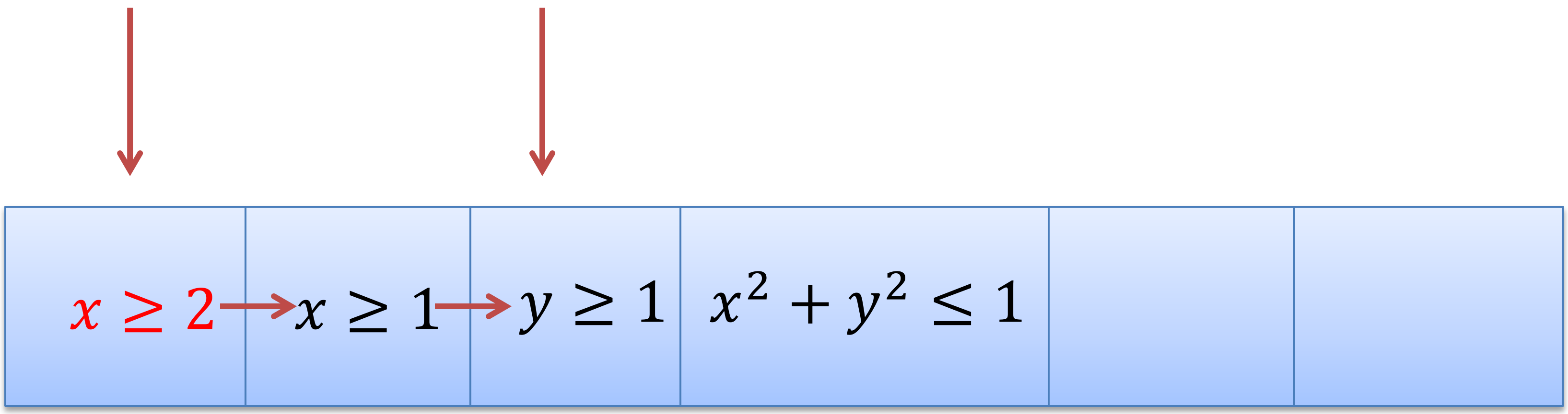
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

Conflict

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

MCSat

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

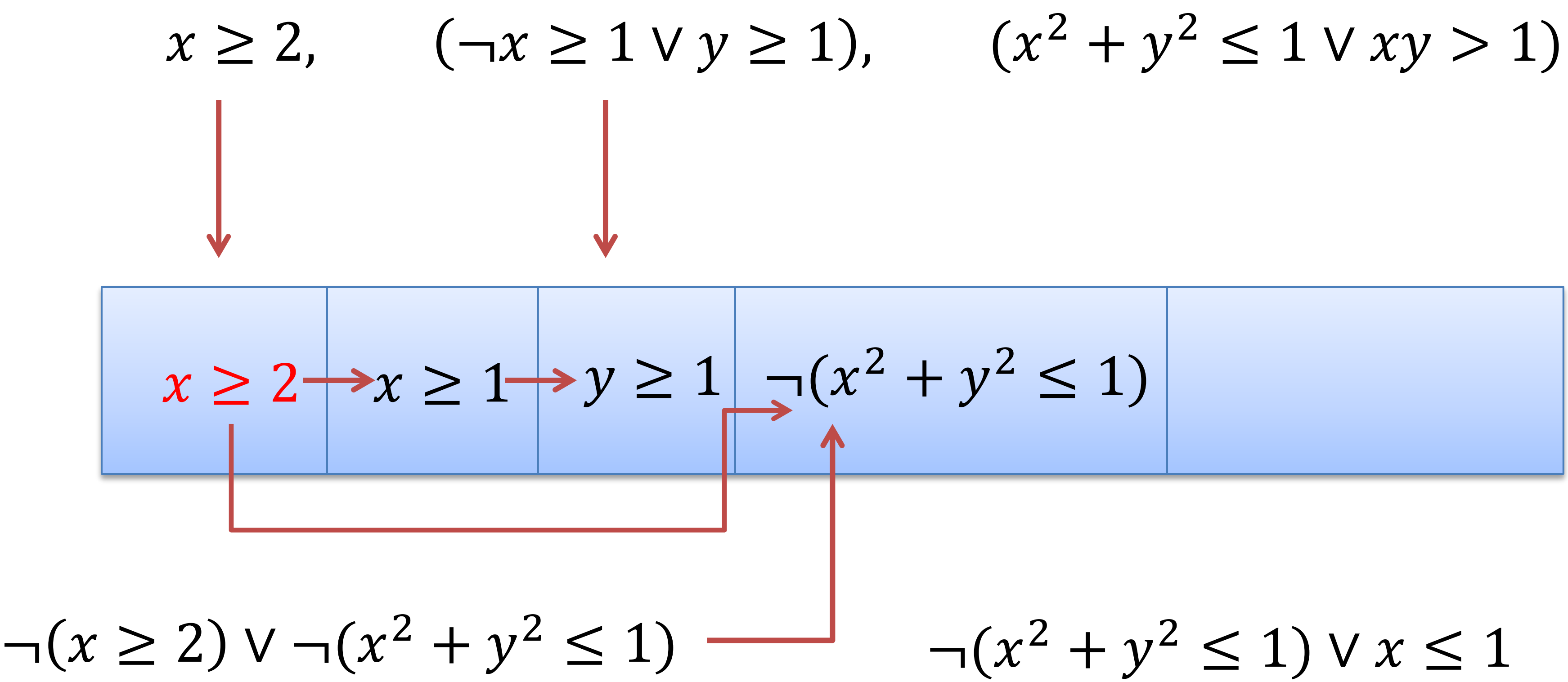


$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

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

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

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

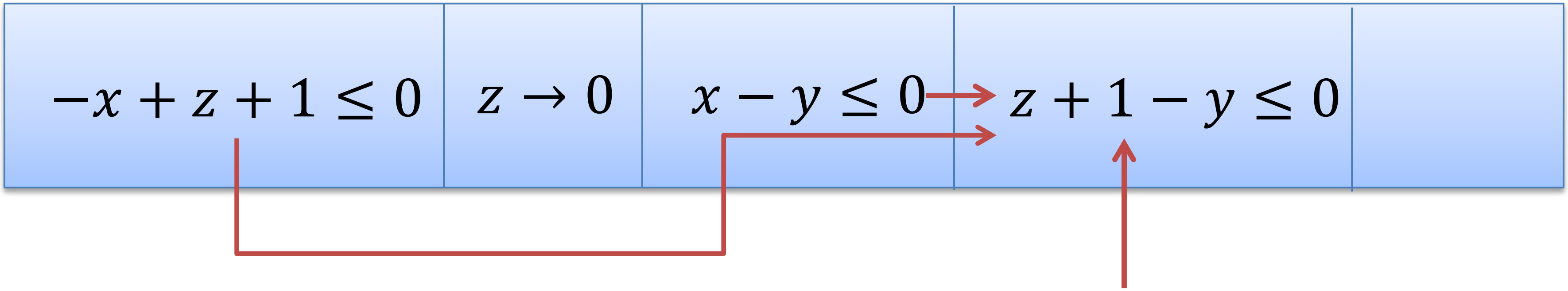
$$\exists x: -x + z + 1 \leq 0 \land x - y \leq 0$$

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

Fourier-Motzkin

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

MCSat: FM Example



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

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

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

$$\neg(-x + z + 1 \le 0) \lor \neg(x - y \le 0) \lor z + 1 - y \le 0$$

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

$$\equiv$$

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

$$1 \le x, \quad x \le 1$$

MCSat – Finite Basis

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

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

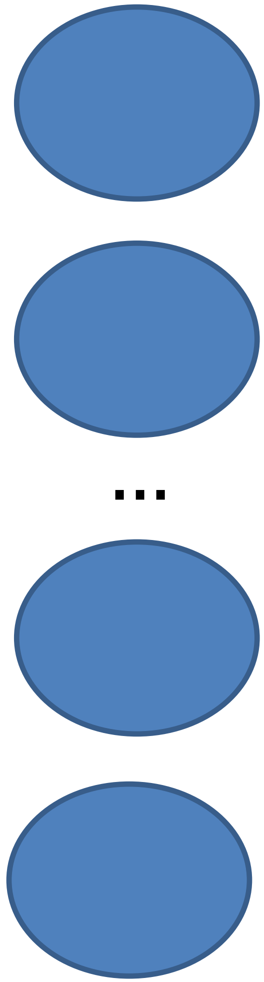
$y_1 \to \alpha_1, \dots, y_m \to \alpha_m$

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

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

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

MCSat – Finite Basis



$F_n[x_1, x_2, \ldots, x_{n-1}, x_n]$

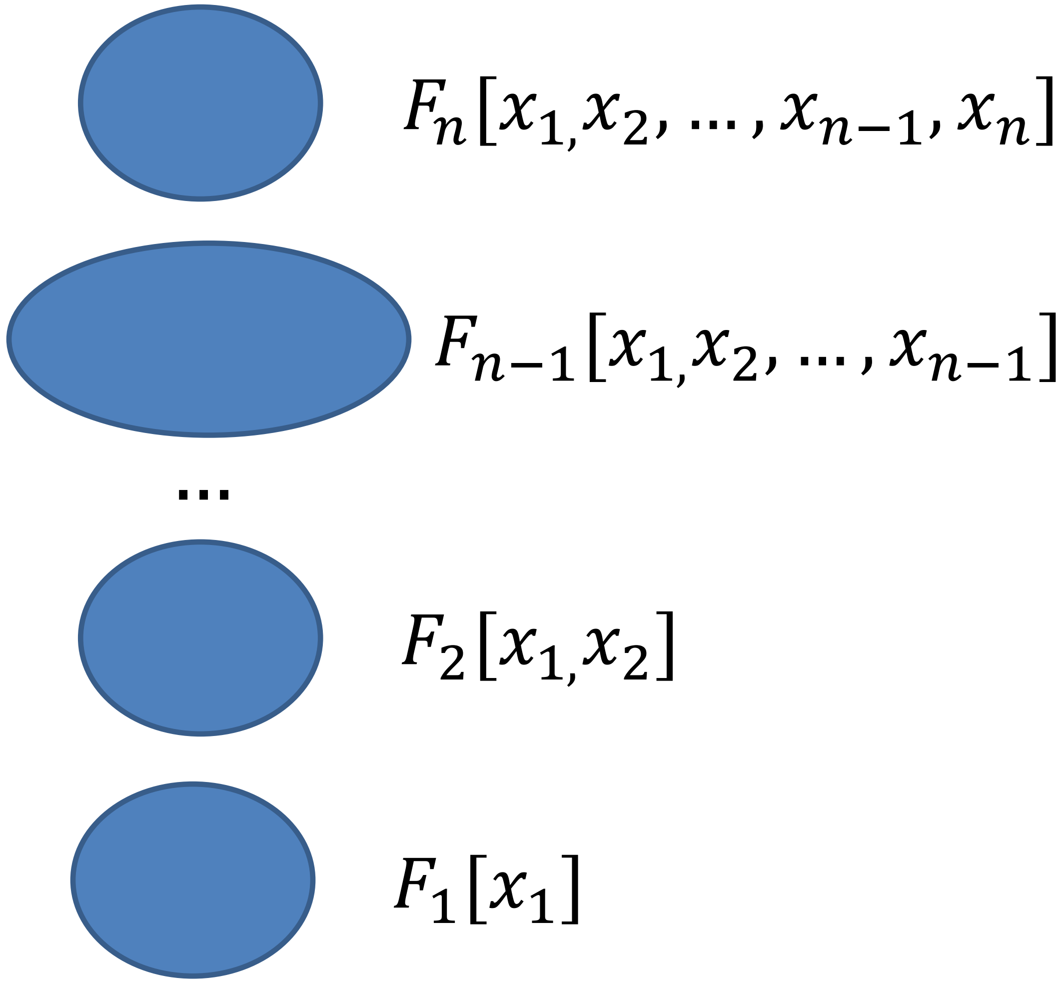
$F_{n-1}[x_1, x_2, \ldots, x_{n-1}]$

...

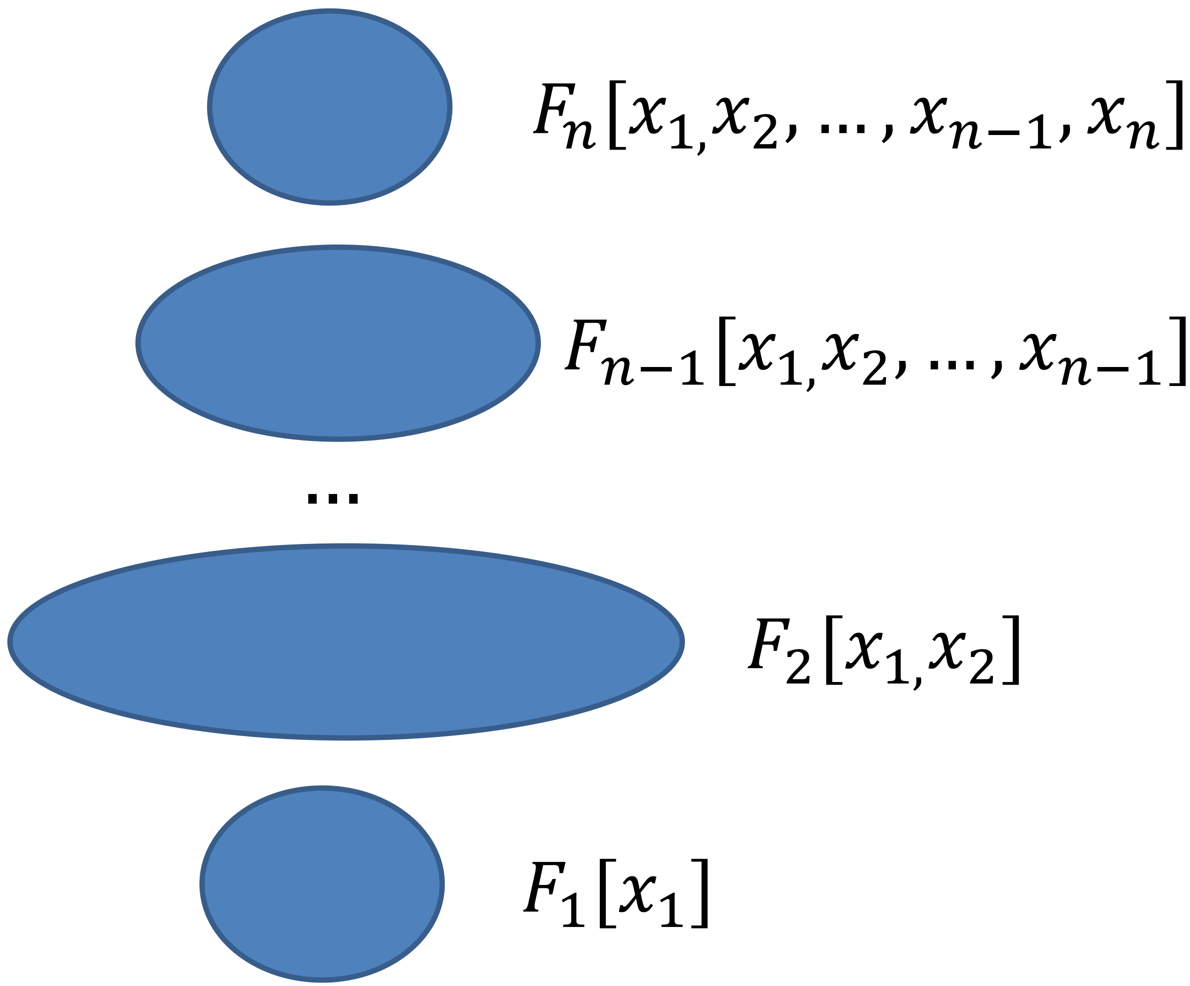
$F_2[x_1, x_2]$

$F_1[x_1]$

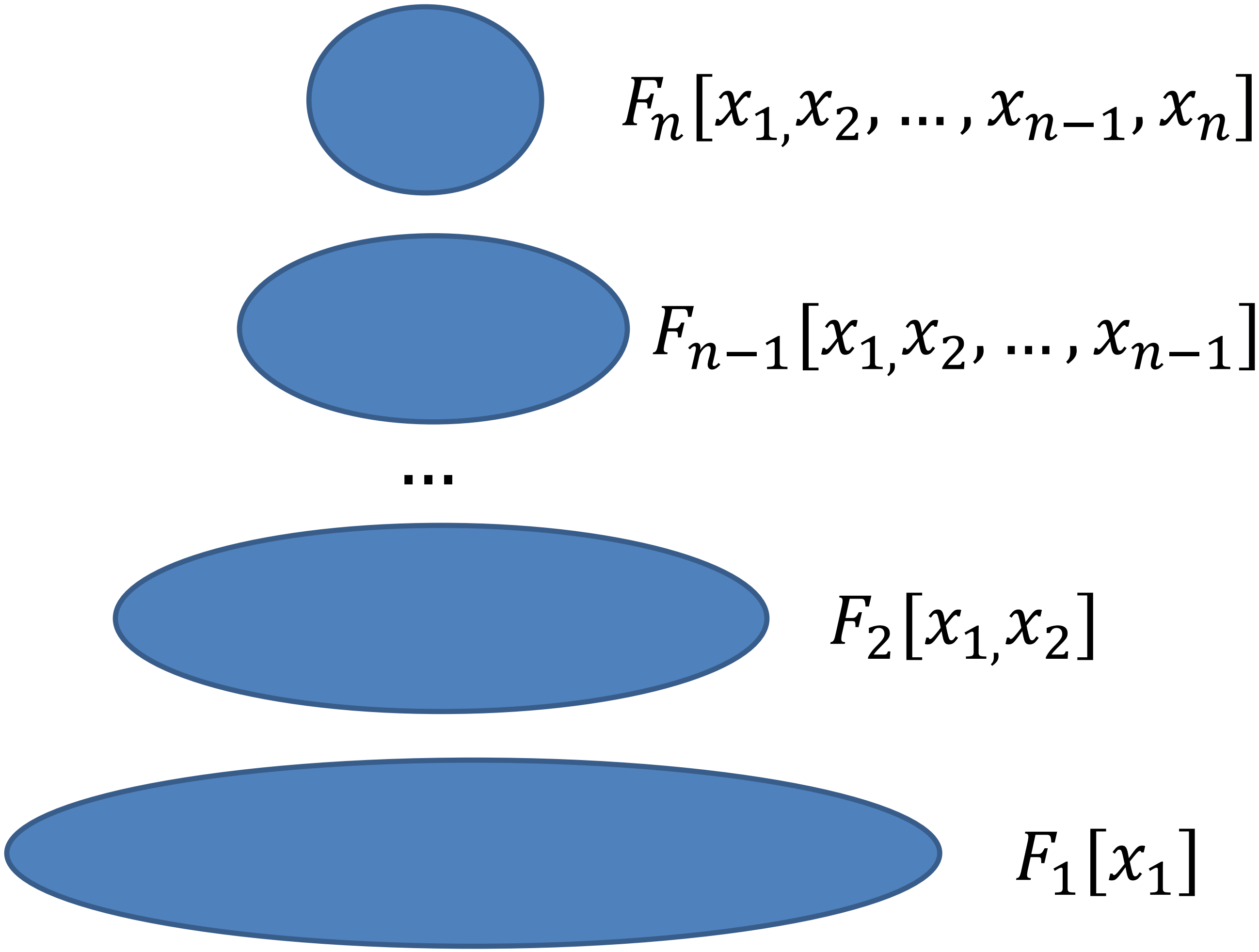
MCSat – Finite Basis



MCSat – Finite Basis



MCSat – Finite Basis



MCSat – Finite Basis

Every "finite" theory has a finite basis

Example: Fixed size Bit-vectors

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

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

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

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

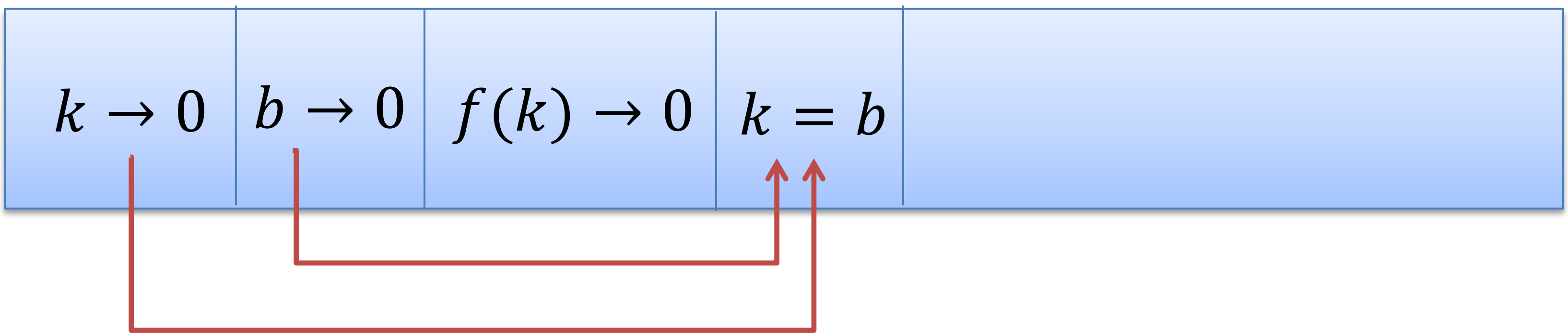
$k \to 0$	$b \to 0$	$f(k) \to 0$	$f(b) \to 2$	

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

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

MCSat: Uninterpreted Functions

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

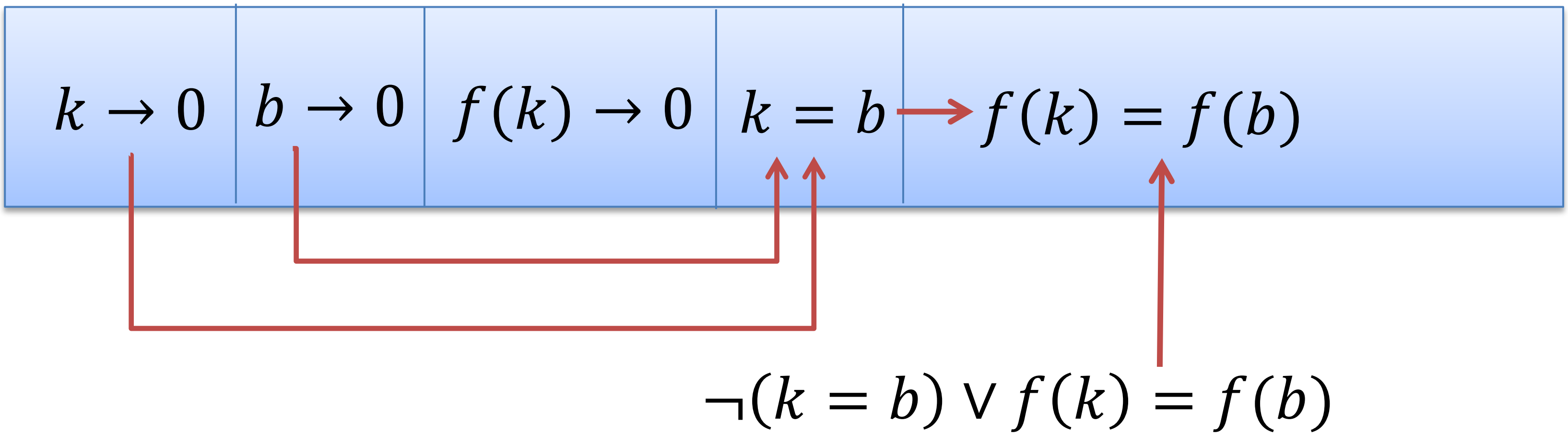


(Semantic) Propagation

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

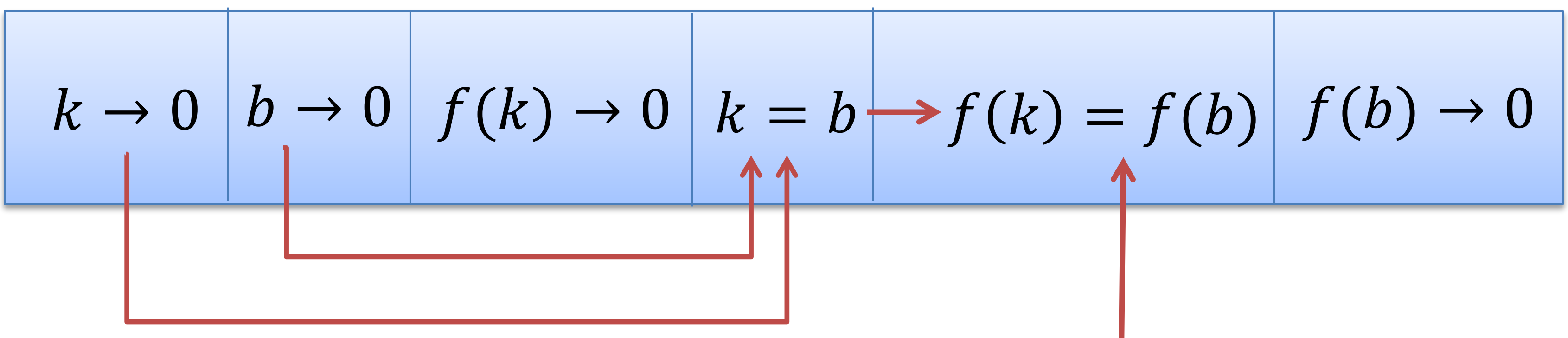
MCSat: Uninterpreted Functions

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



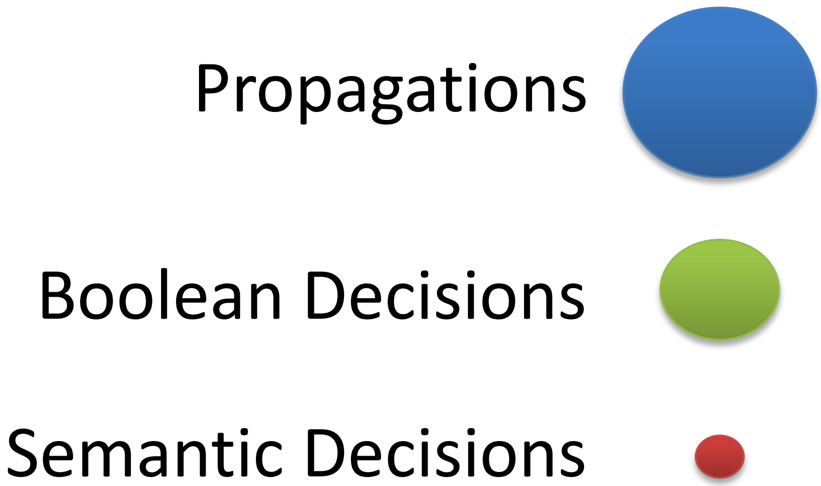
MCSat: Uninterpreted Functions

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

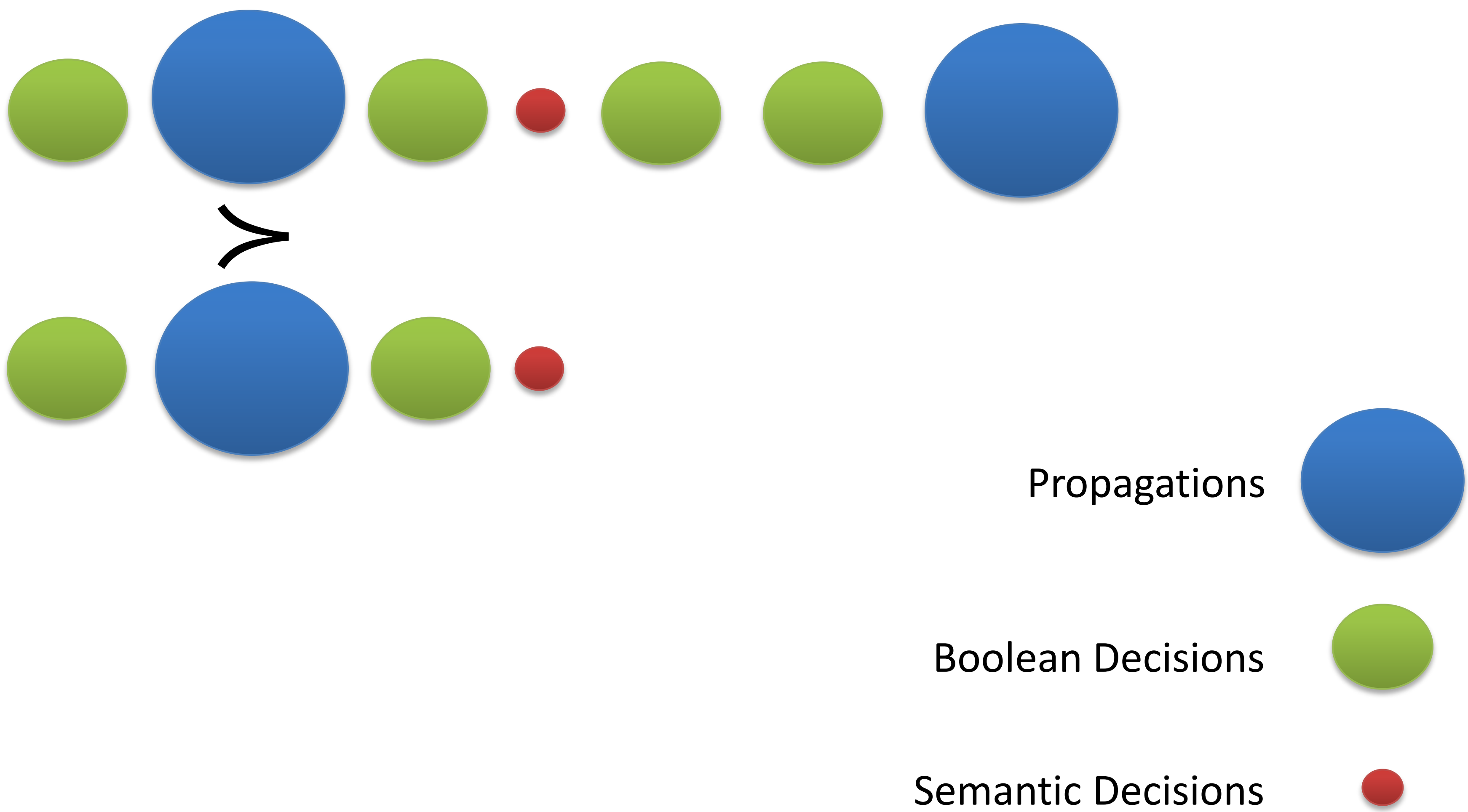


$$\neg(k = b) \vee f(k) = f(b)$$

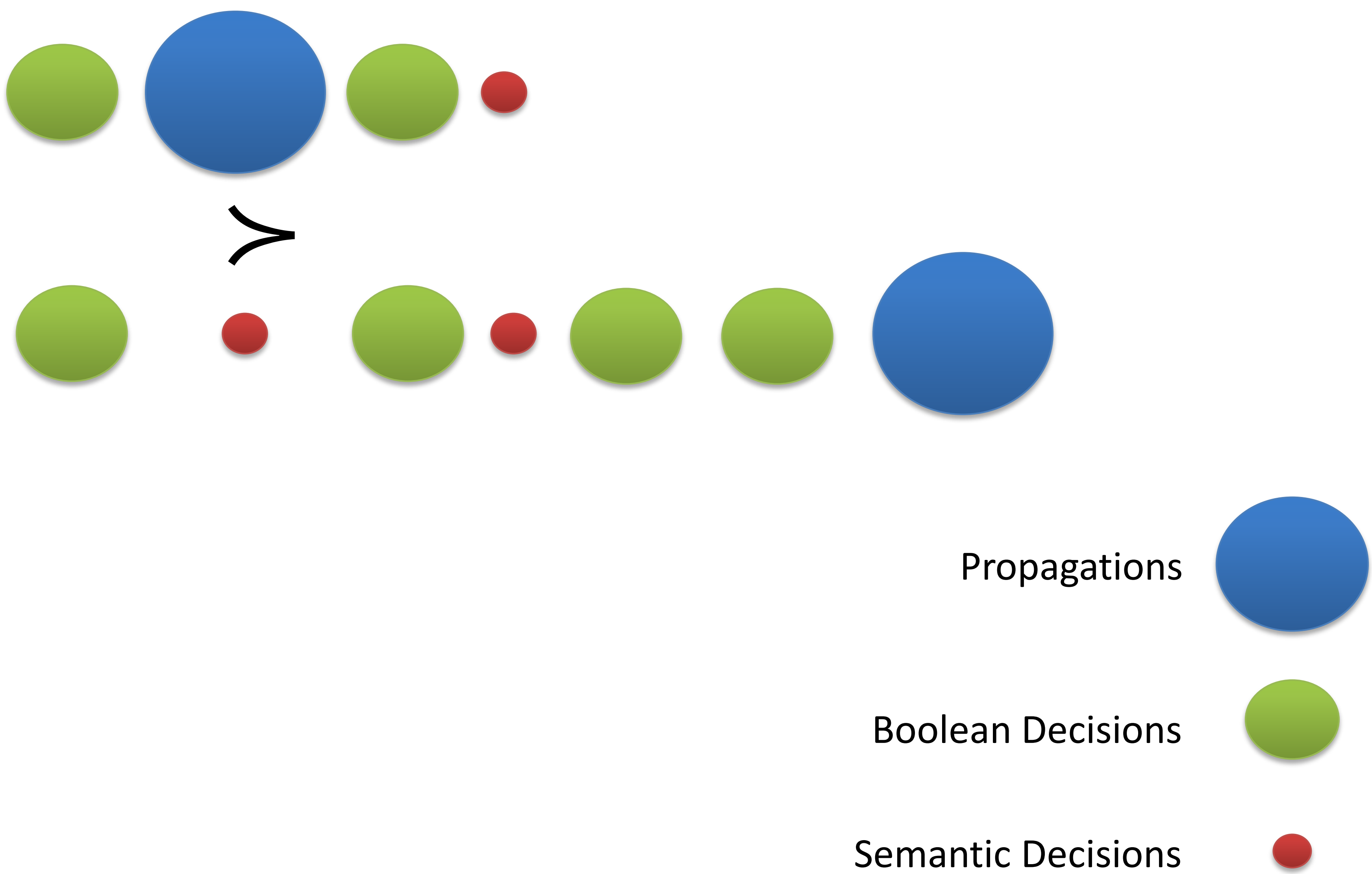
MCSat: Termination



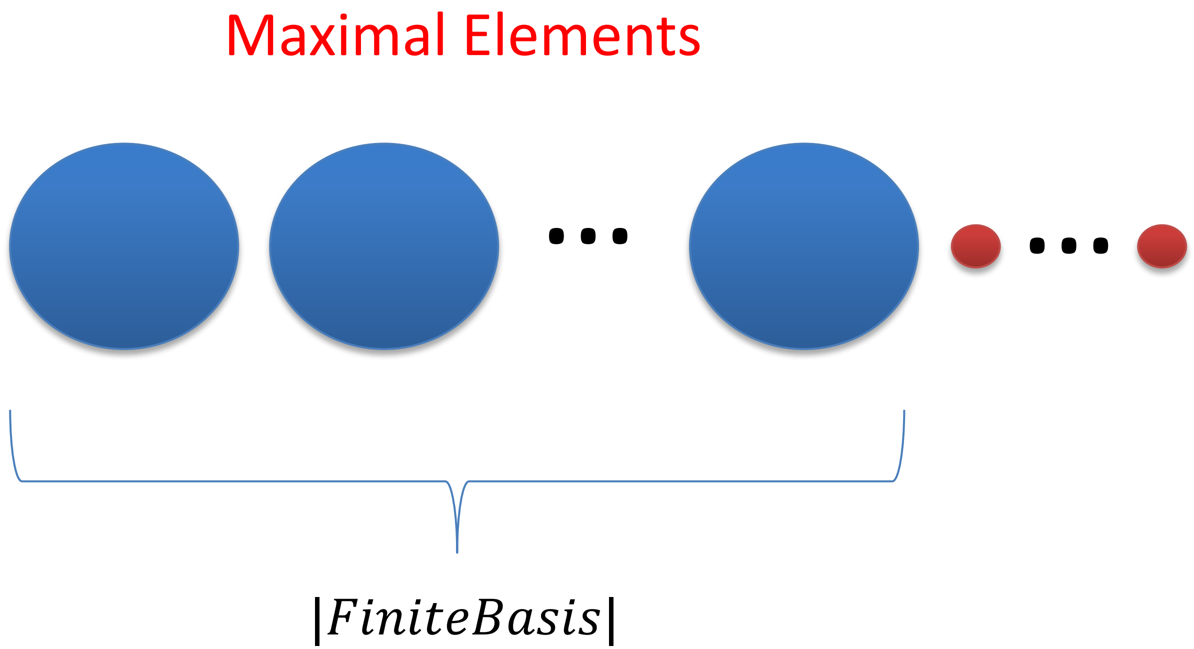
MCSat



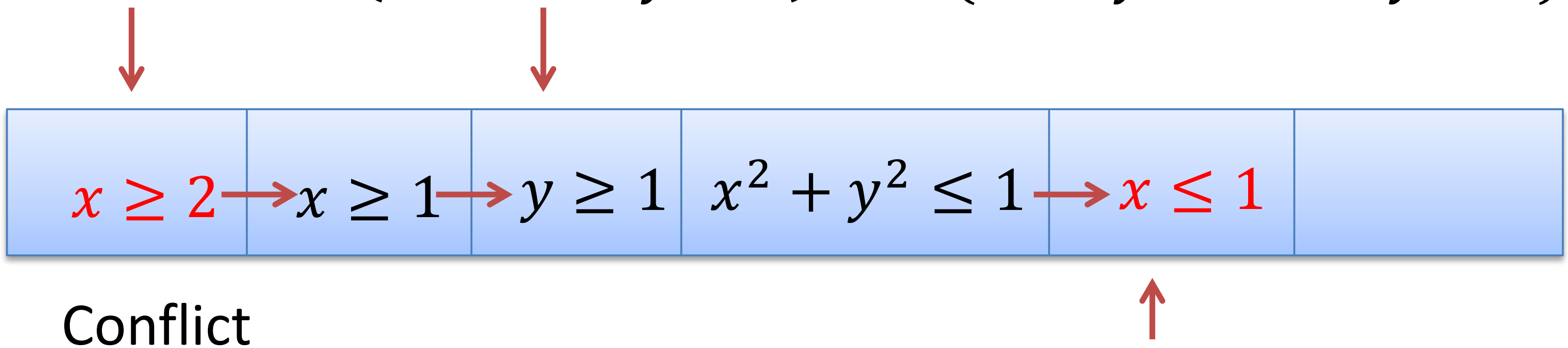
MCSat



MCSat



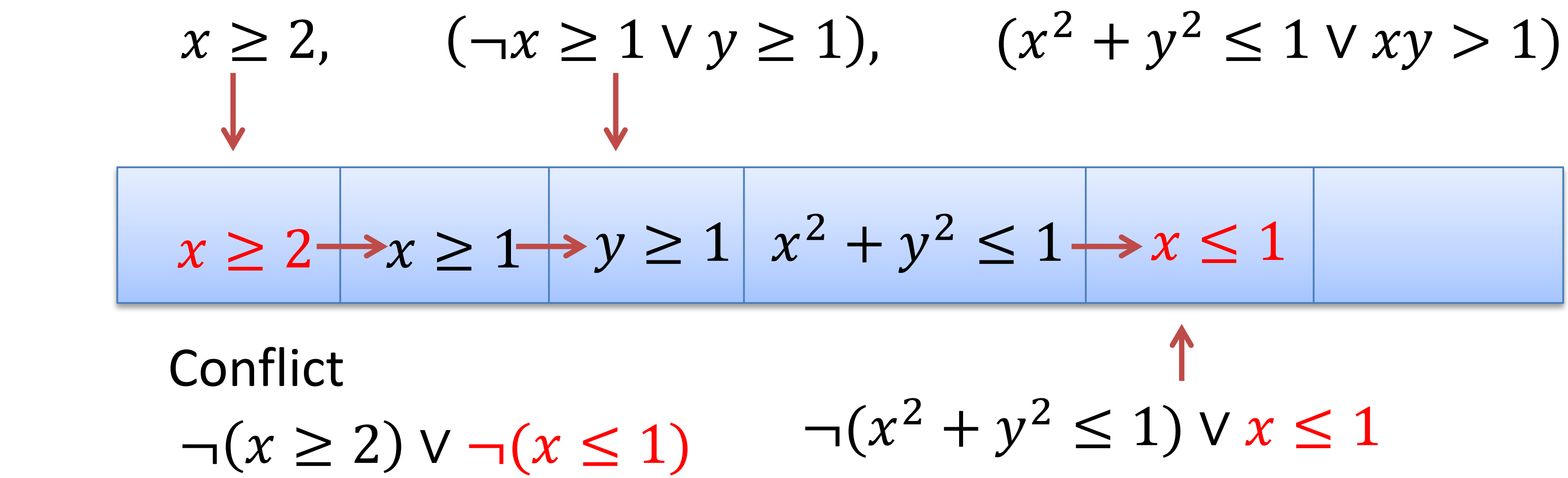
$x \geq 2,\quad (\neg x \geq 1 \lor y \geq 1),\quad (x^2 + y^2 \leq 1 \lor xy > 1)$

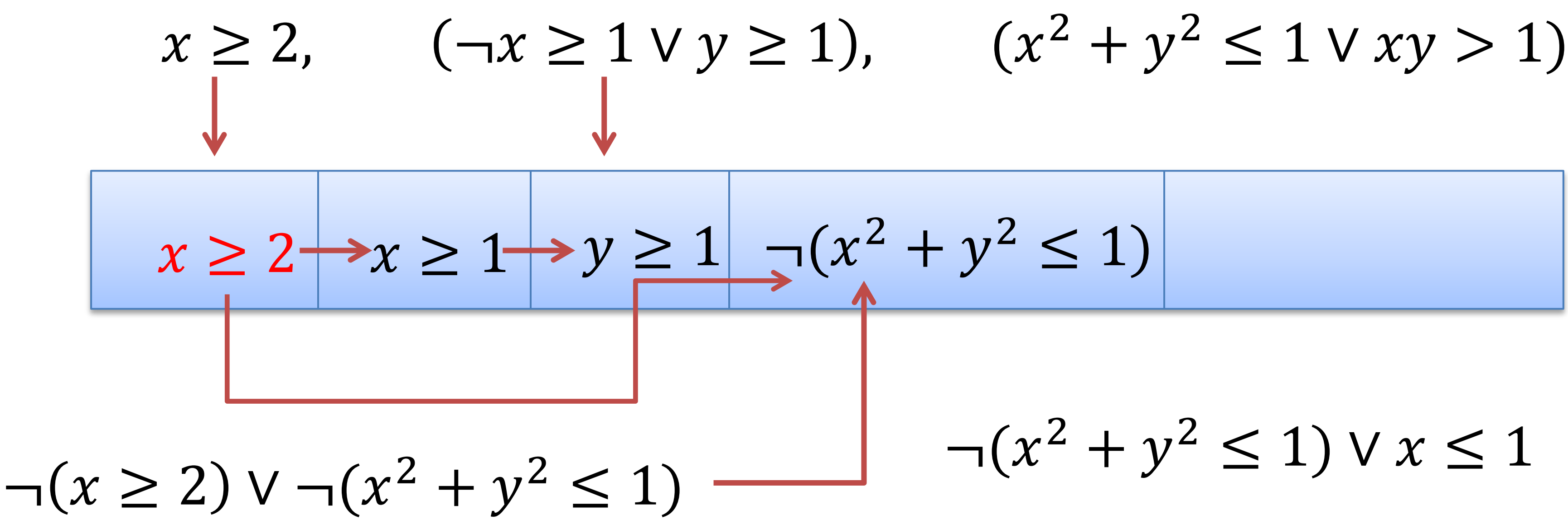


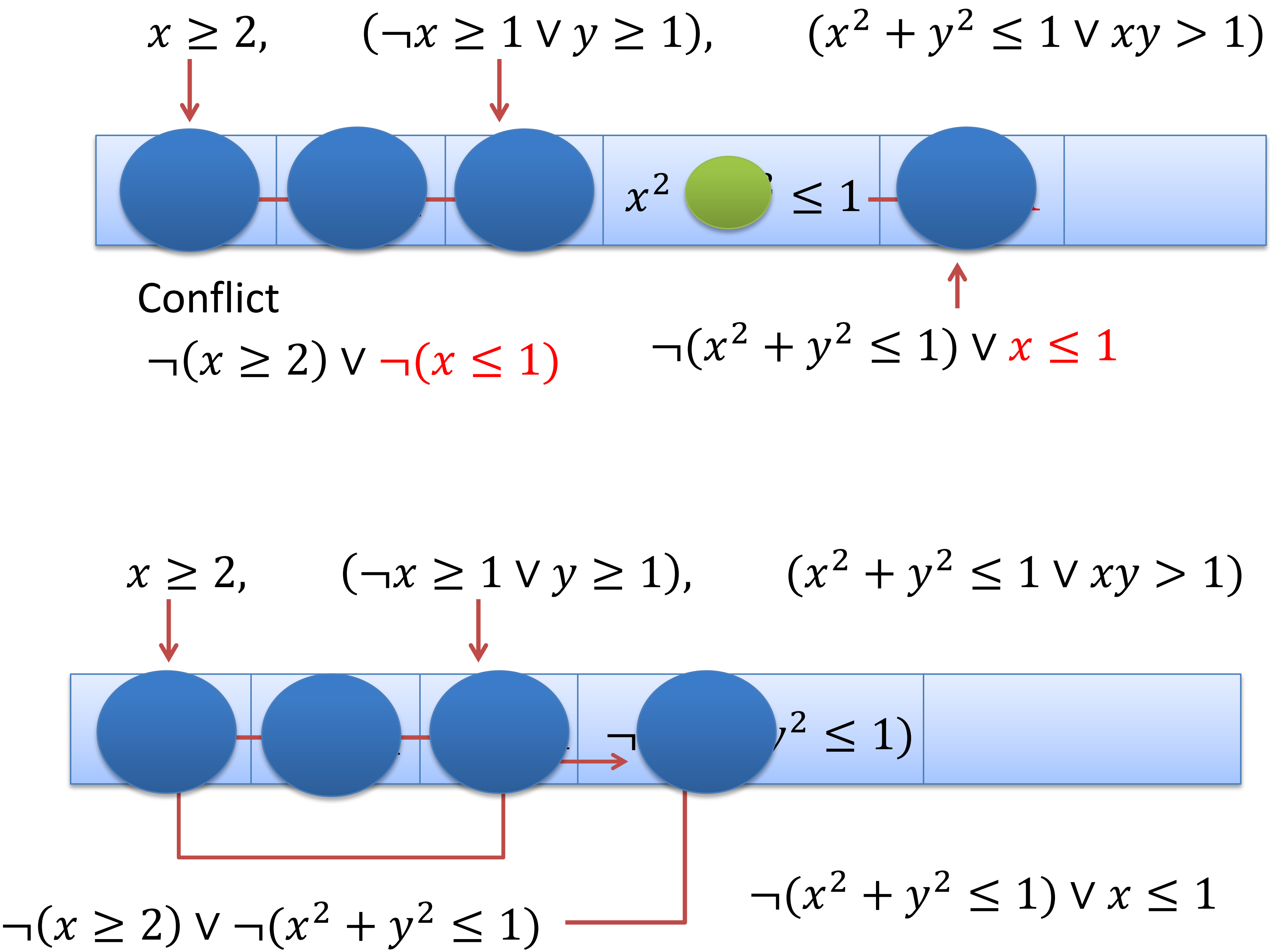
Conflict

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

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


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


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


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

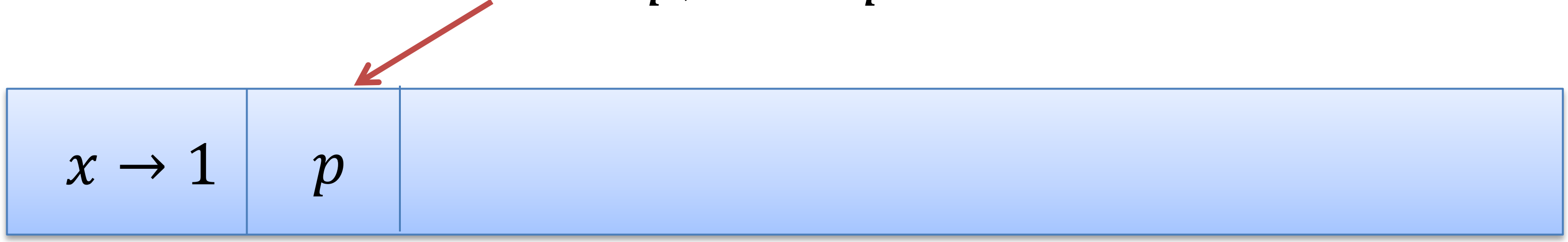
MCSat

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

$x \rightarrow 1$	

MCSat

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



MCSat

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

$x \to 1$	p	

Conflict (evaluates to false)

MCSat

$x < 1 \lor p, \quad \neg p \lor x = 2$

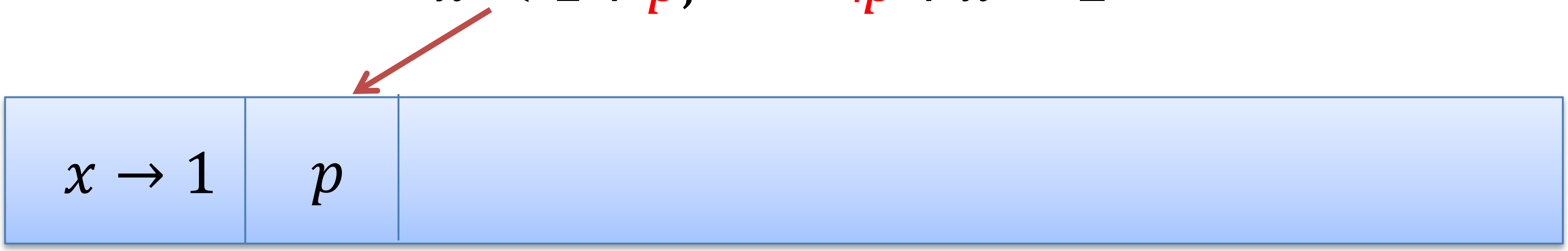
$x \to 1$	p	

New clause

$x < 1 \lor x = 2$

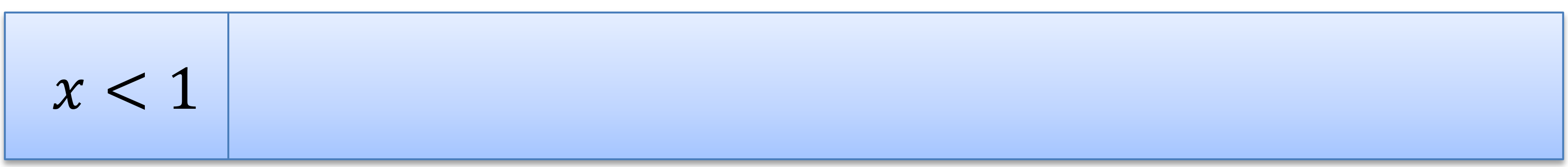
MCSat

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



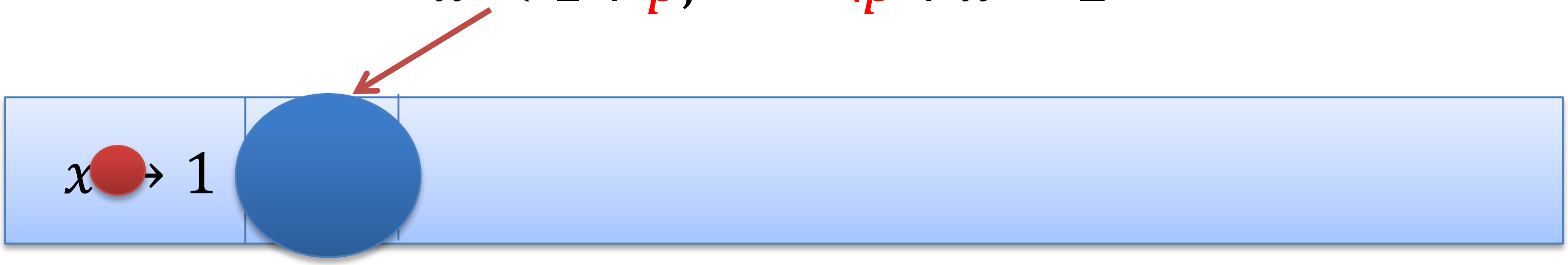
New clause

$x < 1 \vee x = 2$



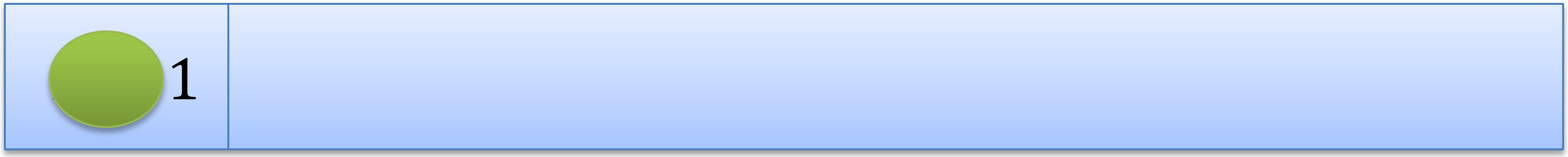
MCSat

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

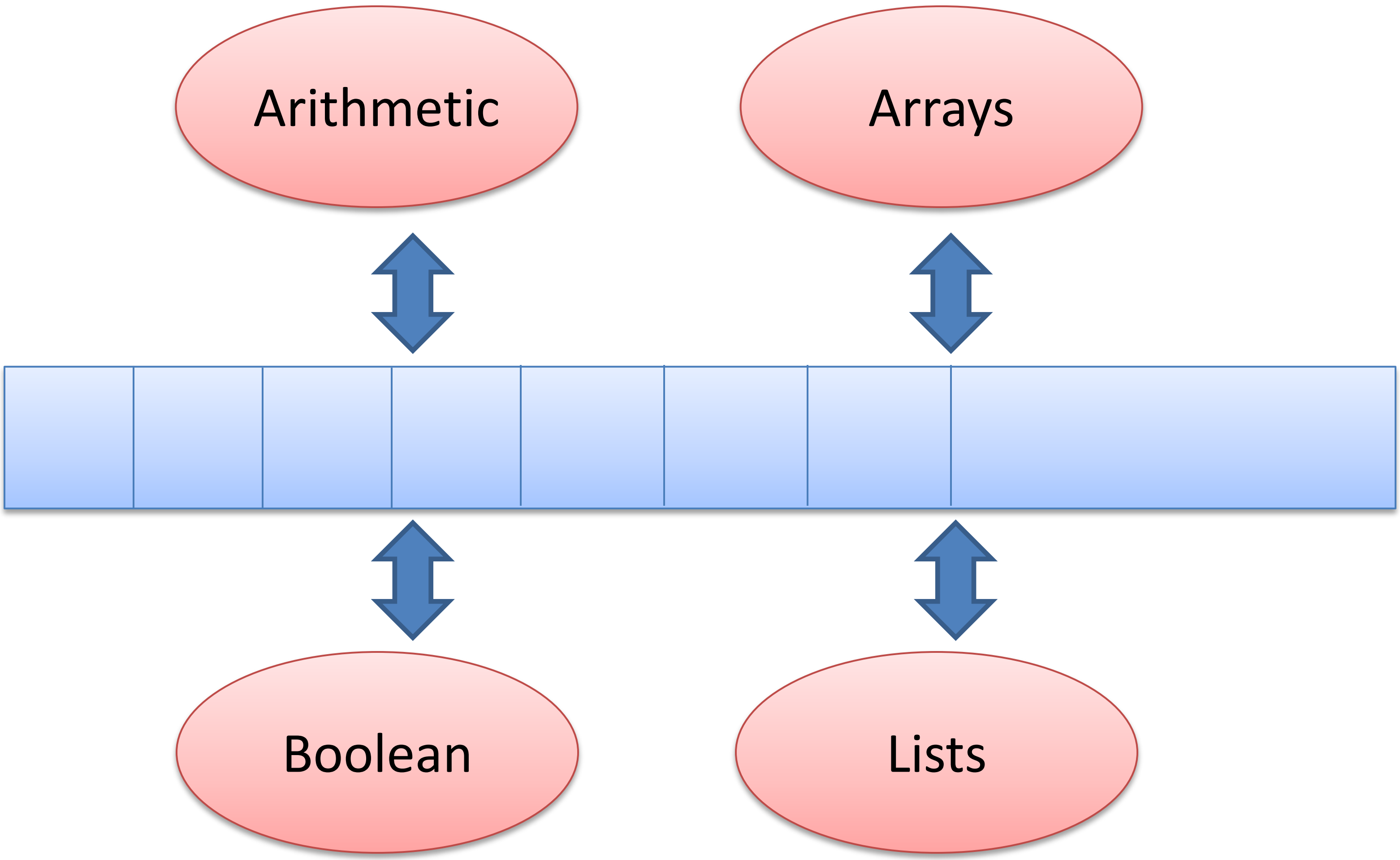


New clause

$x < 1 \vee x = 2$



MCSat: Architecture



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

Check Modulo Assignment

Given a CNF formula F and a set of literals S

$$check(F, S)$$

Check Modulo Assignment

Given a CNF formula F and a set of literals S

$$check(F, S)$$

Output:

SAT, assignment $M \supseteq S$ satisfying F

UNSAT, $\{l_1, \ldots, l_k\} \subseteq S$ s.t. $F \Rightarrow \neg l_1 \vee \cdots \vee \neg l_k$

Check Modulo Assignment

Given a CNF formula F and a set of literals S

$$check(F, S)$$

Output:

SAT, assignment $M \supseteq S$ satisfying F

UNSAT, $\{l_1, \ldots, l_k\} \subseteq S$ s.t. $F \Rightarrow \neg l_1 \vee \cdots \vee \neg l_k$

Check Modulo Assignment

$$F \equiv p \lor q \lor r, \neg p \lor q, p \lor q$$

$$check(F, \{\neg q, r\})$$

Check Modulo Assignment

$$F \equiv p \vee q \vee r, \neg p \vee q, p \vee q$$

$$check(F, \{\neg q, r\})$$

UNSAT, $\{\neg q\}$

Check Modulo Assignment

Many Applications:

- UNSAT Core generation
- MaxSAT
- Interpolant generation

Introduced in MiniSAT

Implemented in many SMT solvers

Extending Check Modulo Assignment for MCSAT

$F[\bar{x}, \bar{y}] \qquad \bar{y} \to \bar{v}$

Extending Check Modulo Assignment for MCSAT

$$F[\bar{x}, \bar{y}] \qquad \bar{y} \rightarrow \bar{v}$$

SAT, $\bar{x} \rightarrow \overline{w}, F[\overline{w}, \bar{v}]$ is true

Extending Check Modulo Assignment for MCSAT

$$F[\bar{x}, \bar{y}] \qquad \bar{y} \to \bar{v}$$

SAT, $\bar{x} \to \overline{w}$, $F[\overline{w}, \bar{v}]$ is true

UNSAT, $S[\bar{y}]$ s.t. $F[\bar{x}, \bar{y}] \Rightarrow S[\bar{y}]$, $S[\bar{v}]$ is false

NLSAT/MCSAT

$$F[\bar{x}, \bar{y}]$$

$y_1 \to w_1$	$\ldots$	$y_k \to w_k$	

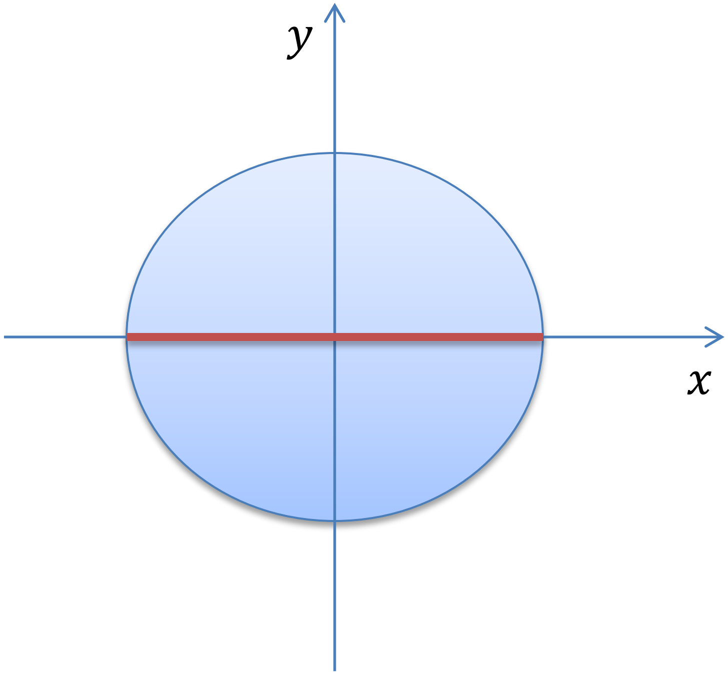
NLSAT/MCSAT

$$Check(x^2 + y^2 < 1, \{y \rightarrow -2\})$$

NLSAT/MCSAT

$$Check(x^2 + y^2 < 1, \{y \rightarrow -2\})$$

UNSAT, $y > -1$



No-good sampling

$$Check(F[\bar{x},\bar{y}],\{\, y \to \alpha_1\}) = \text{unsat}(S_1[\bar{y}]),\ \ G_1 = S_1[\bar{y}],$$

$$\alpha_2 \in G_1,\ Check(F[\bar{x},\bar{y}],\{\, y \to \alpha_2\}) = \text{unsat}(S_2[\bar{y}]),\ \ G_2 = G_1 \wedge S_2[\bar{y}],$$

$$\alpha_3 \in G_2,\ \ Check(F[\bar{x},\bar{y}],\{\, y \to \alpha_3\}) = \text{unsat}(S_3[\bar{y}]),\ G_3 = G_2 \wedge S_3[\bar{y}],$$

$\ldots$

$$\alpha_n \in G_{n-1},\ Check(F[\bar{x},\bar{y}],\{\, y \to \alpha_n\}) = \text{unsat}(S_n[\bar{y}]),\ G_n = G_{n-1} \wedge S_n[\bar{y}],$$

…

Finite decomposition property:

The sequence is finite

G_i approximates
$\exists \bar{x}, F[\bar{x},\bar{y}]$

Computing Interpolants using Extended Check Modulo Assignment

Given: $A[\bar{x}, \bar{y}] \wedge B[\bar{y}, \bar{z}]$

Ouput: $I[\bar{y}]$ s.t.

$$B[\bar{y}, \bar{z}] \Rightarrow I[\bar{y}],$$

$$A[\bar{x}, \bar{y}] \wedge I[\bar{y}] \text{ is unsat}$$

Computing Interpolants using Extended Check Modulo Assignment

$I[\bar{y}] := true$

Loop

Solve $A[\bar{x}, \bar{y}] \wedge I[\bar{y}]$

If UNSAT return $I[\bar{y}]$

Let solution be $\{\bar{x} \rightarrow \bar{w}, \bar{y} \rightarrow \bar{v}\}$

Check$(B[\bar{y}, \bar{z}], \{\bar{y} \rightarrow \bar{v}\})$

If SAT return SAT

$I[\bar{y}] := I[\bar{y}] \wedge S[\bar{y}]$

Conclusion

Model-Based techniques are very promising

MCSat is a more faithful lift of CDCL than DPLL(T)

Prototypes:

NLSAT source code is available in Z3

http://z3.codeplex.com

MCSAT (Linear arithemetic + unintepreted functions)

https://github.com/dddejan/

New versions coming soon!

Extra Slides

Lazy SMT and DPLL(T)

Abstraction Refinement Procedure

SAT + Theory Solvers

Basic Idea

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

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

$p_3 \equiv (y > 2),\ p_4 \equiv (y < 1)$

[Audemard et al - 2002], [Barrett et al - 2002], [de Moura et al - 2002]

SAT + Theory Solvers

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

SAT + Theory Solvers

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

SAT + Theory Solvers

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

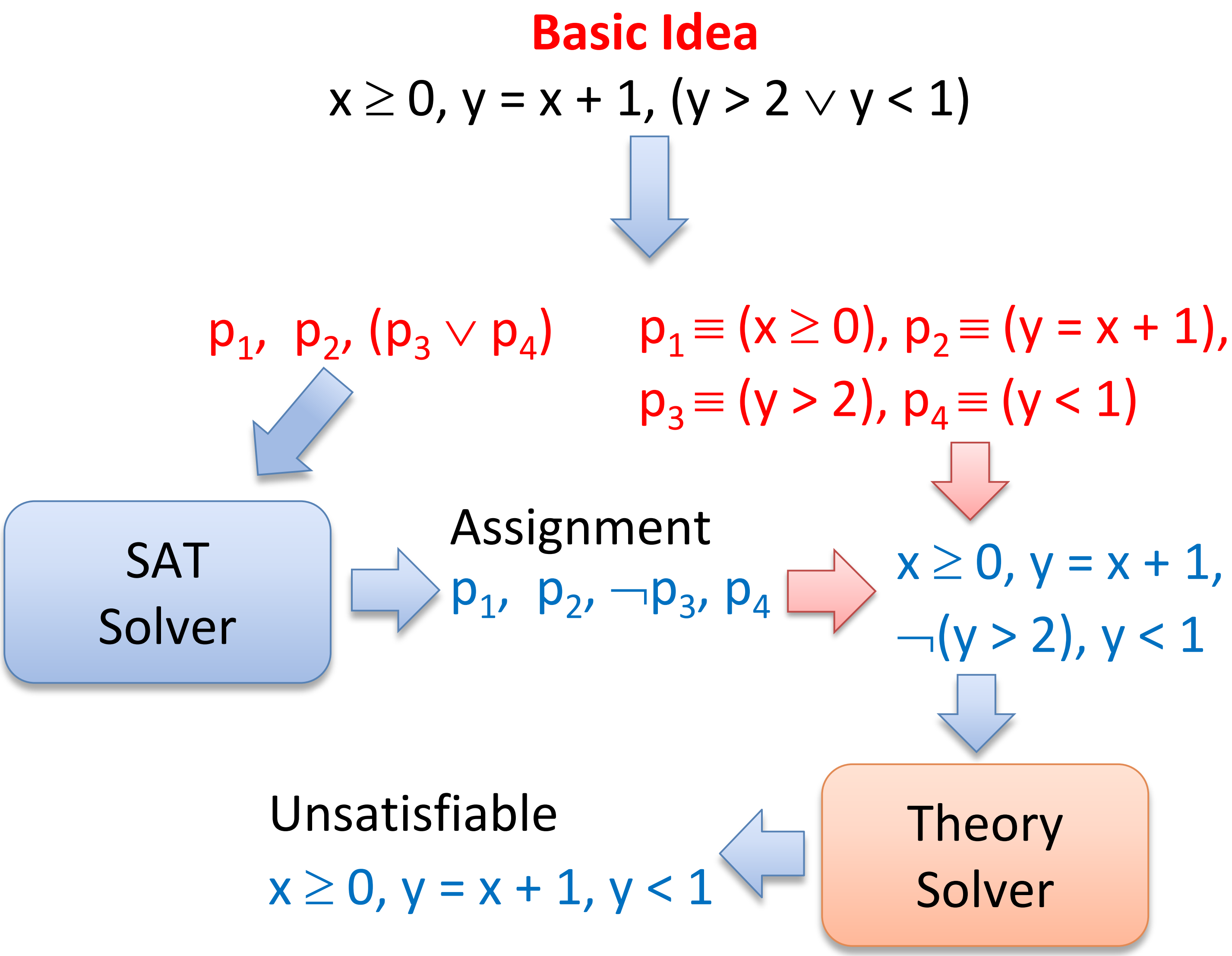
Assignment

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

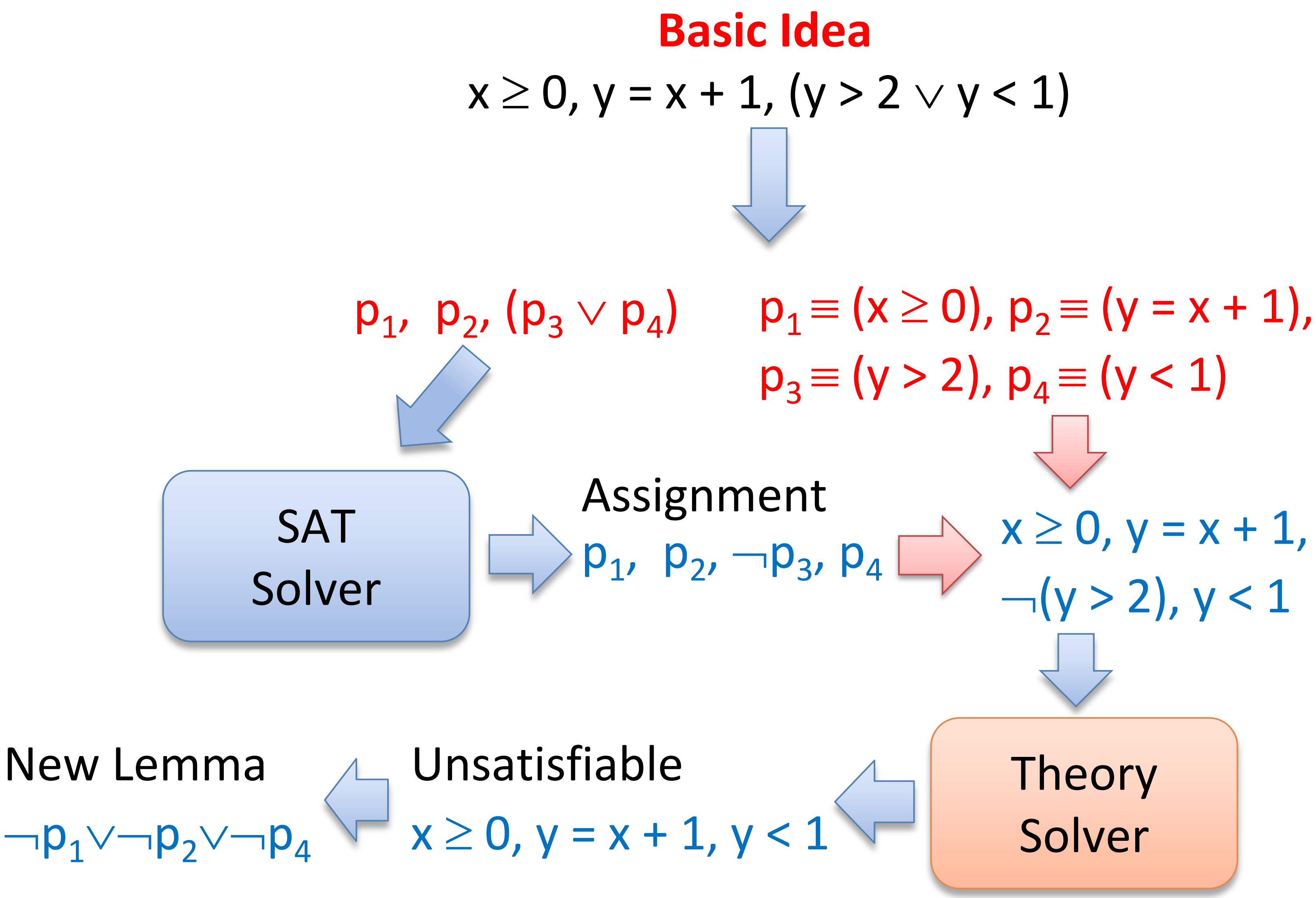
$x \geq 0,\ y = x + 1,$

$\neg(y > 2),\ y < 1$

SAT + Theory Solvers



SAT + Theory Solvers



SAT + Theory Solvers: refinements

Incrementality

Efficient Backtracking

Efficient Lemma Generation

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