

Decision methods for arithmetic

Third summer school on formal methods

Leonardo de Moura

Microsoft Research

Symbolic Reasoning

Software analysis/verification tools
need some form of **symbolic reasoning**

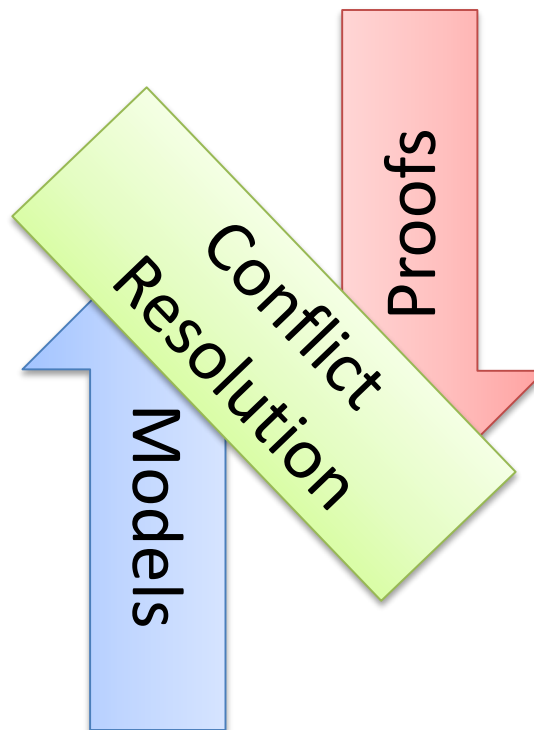
Logic is “The Calculus of Computer Science”

Zohar Manna

Saturation x Search

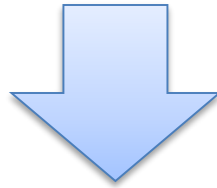
Proof-finding

Model-finding



SAT

$$p_1 \vee \neg p_2, \quad \neg p_1 \vee p_2 \vee p_3, \quad p_3$$



$$p_1 = \text{true}, \quad p_2 = \text{true}, \quad p_3 = \text{true}$$

CNF is a set (conjunction) set of clauses

Clause is a disjunction of literals

Literal is an atom or the negation of an atom

Two procedures

Resolution	DPLL
Proof-finder	Model-finder
Saturation	Search

Resolution

$$C \vee l, D \vee \neg l \Rightarrow C \vee D$$

$$l, \neg l \Rightarrow \mathbf{unsat}$$

Improvements

Delete tautologies $l \vee \neg l \vee C$

Ordered Resolution

Subsumption (delete redundant clauses)

$$C \textit{ subsumes } C \vee D$$

...

Resolution: Example

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

Resolution: Example

$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r \quad \Rightarrow$

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

Resolution: Example

$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r \quad \Rightarrow$

$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r \quad \Rightarrow$

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

Resolution: Example

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r \quad \Rightarrow$$

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r \quad \Rightarrow$$

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r, q \vee r \quad \Rightarrow$$

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

Resolution: Example

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r \quad \Rightarrow$$

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r \quad \Rightarrow$$

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r, q \vee r \quad \Rightarrow$$

$$\neg p \vee \neg q \vee r, \neg p \vee q, p \vee r, \neg r, \neg q \vee r, q \vee r, r \quad \Rightarrow$$

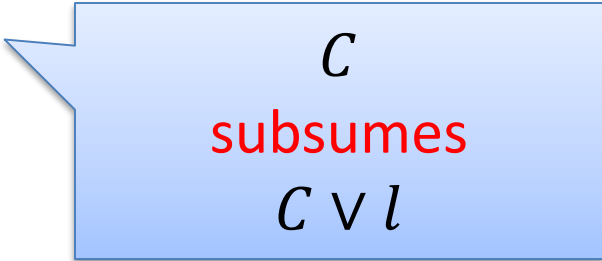
unsat

Resolution: Problem

Exponential time and space

Unit Resolution

$$C \vee l, \neg l \Rightarrow C$$

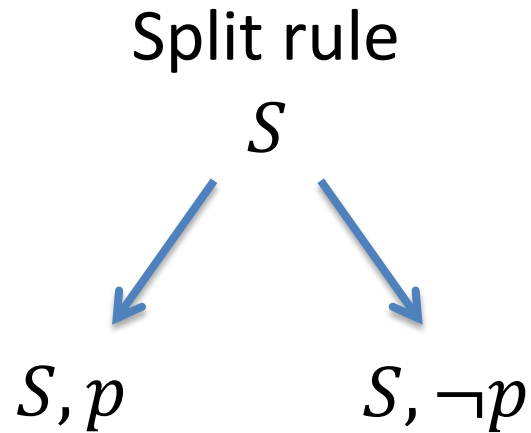


C
subsumes
 $C \vee l$

Complete for Horn Clauses

$$\neg q_1 \vee \dots \vee \neg q_n \vee p$$

DPLL



DPLL = Unit Resolution + Split rule

DPLL

$x \vee y,$ $\neg x \vee y,$ $x \vee \neg y,$ $\neg x \vee \neg y$



$x \vee y,$
 $\neg x \vee y,$
 $x \vee \neg y,$
 $\neg x \vee \neg y,$
 x

DPLL

$x \vee y,$ $\neg x \vee y,$ $x \vee \neg y,$ $\neg x \vee \neg y$



$x \vee y,$
 $\neg x \vee y,$
 $x \vee \neg y,$
 $\neg x \vee \neg y,$
 x

DPLL

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y$



$y,$

$\neg y,$

x

DPLL

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y$



$y,$

$\neg y,$

$x,$

unsat

DPLL

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y$



$y,$

$\neg y,$

$x,$

unsat

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y,$

$\neg x$

DPLL

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y$



$y,$

$\neg y,$

$x,$

unsat

$x \vee y,$

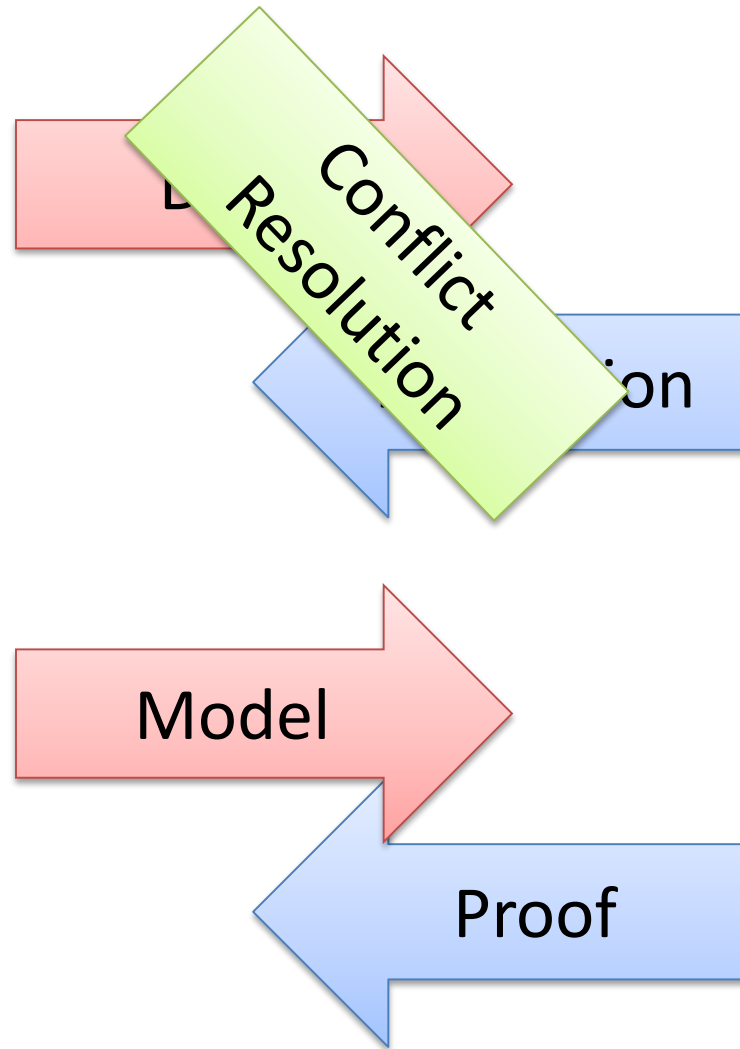
$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y,$

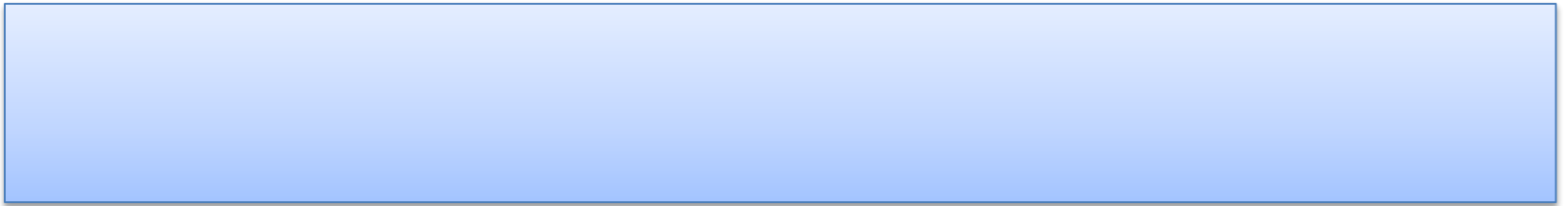
$\neg x$

CDCL: Conflict Driven Clause Learning



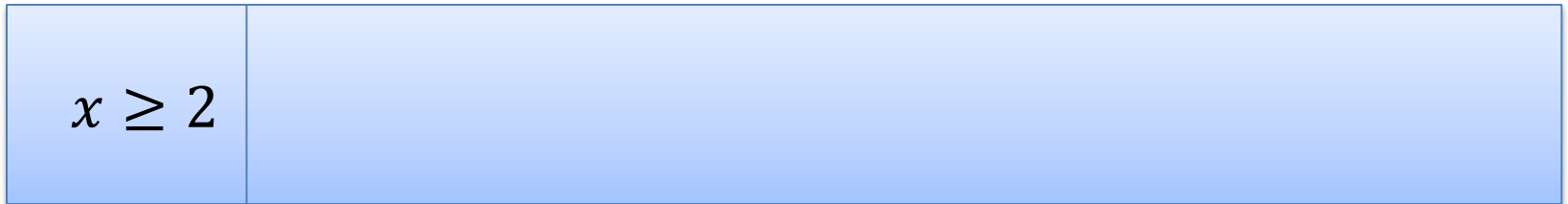
MCSat

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



MCSat

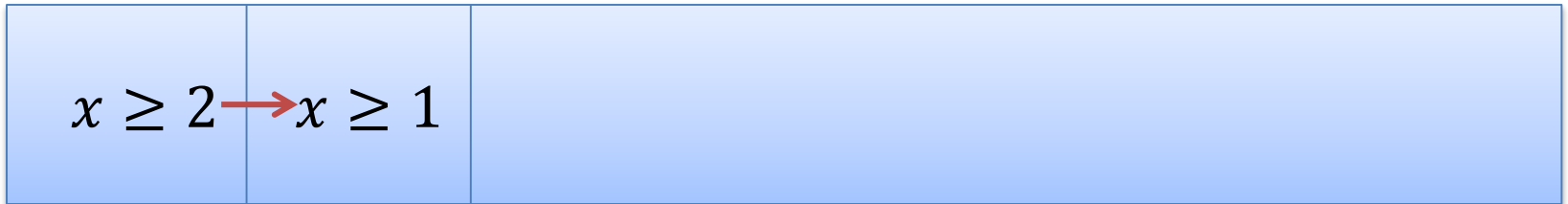
$$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$$



Propagations

MCSat

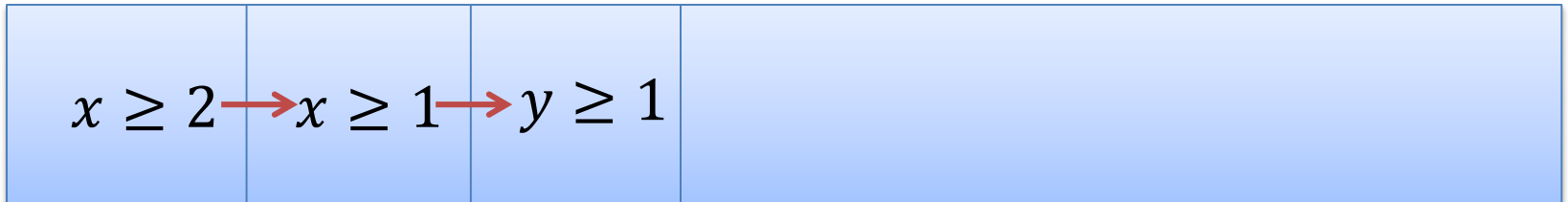
$$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$$



Propagations

MCSat

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



Propagations

MCSat

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



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

Decisions

MCSat

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

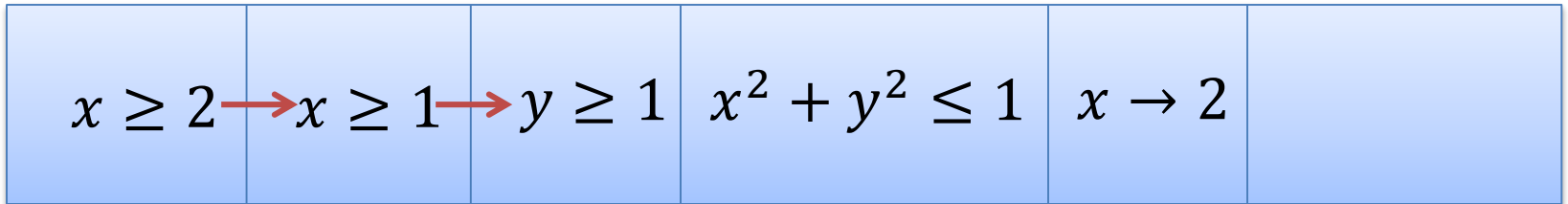


$x \geq 2$	$x \geq 1$	$y \geq 1$	$x^2 + y^2 \leq 1$	$x \rightarrow 2$	
------------	------------	------------	--------------------	-------------------	--

Model Assignments

MCSat

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



Model Assignments

We can't falsify any fact in the trail.

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

Conflict

We can't find a value of y

s.t. $4 + y^2 \leq 1$

MCSat

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



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

Conflict

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

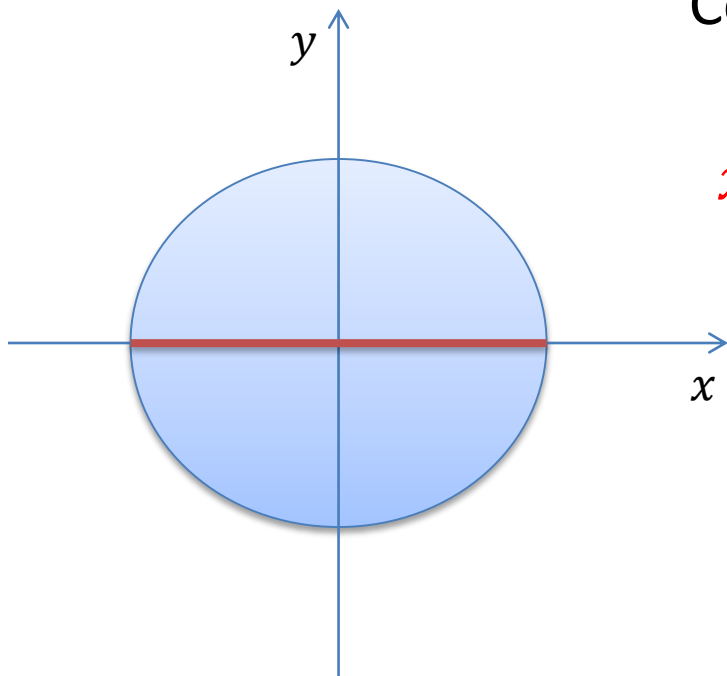
Learning that
 $\neg(x^2 + y^2 \leq 1) \vee \neg(x=2)$
is not productive

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



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

Conflict

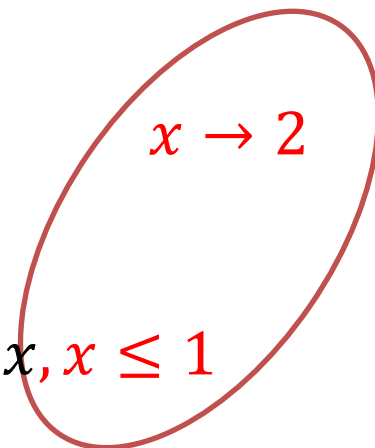


$$x^2 + y^2 \leq 1$$



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

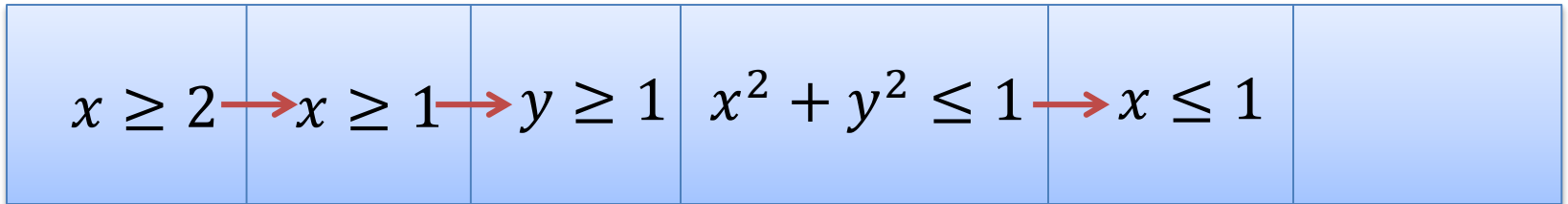
$$x \rightarrow 2$$



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

MCSat

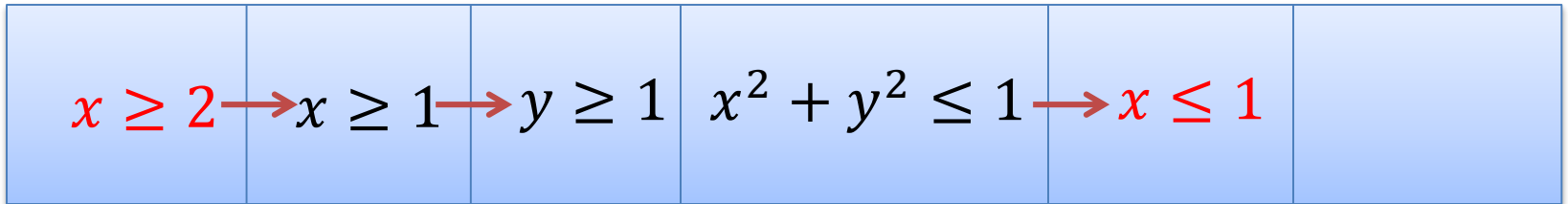
$$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$$



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

MCSat

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



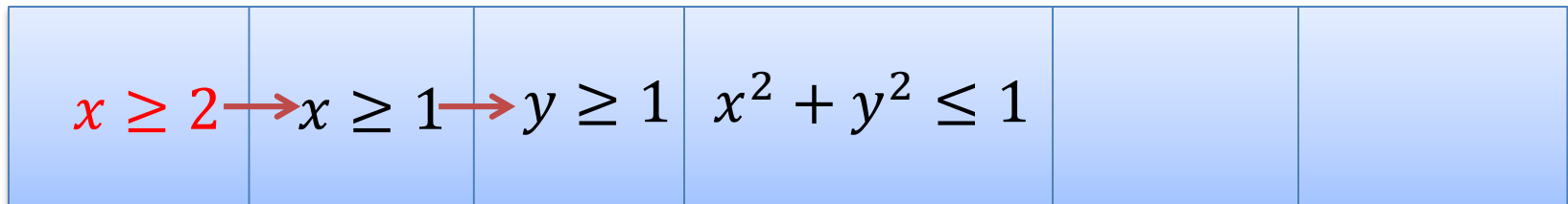
$$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$$

Conflict

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

MCSat

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



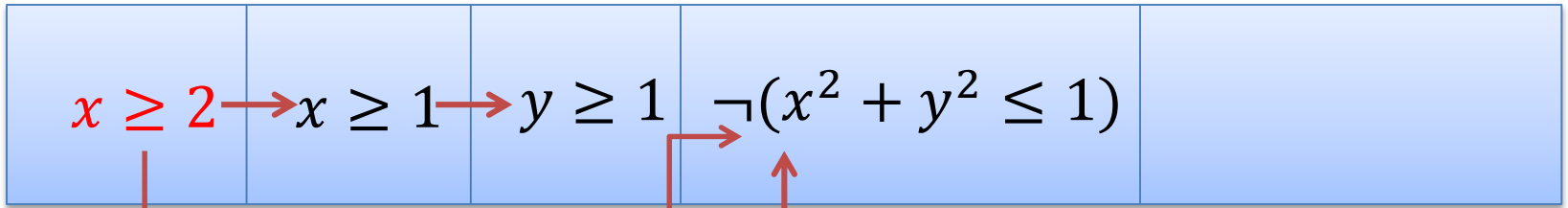
$$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$$

Learned by resolution

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

MCSat

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



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

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

MCSat – Finite Basis

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

$$F[x_1, \dots, x_n, y_1, \dots, y_m]$$

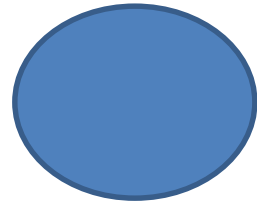
$$\exists x_1, \dots, x_n: F[x_1, \dots, x_n, y]$$

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

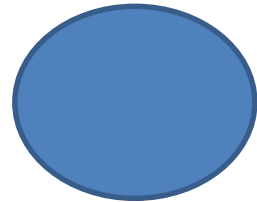
$$\neg F[x_1, \dots, x_n, y_1, \dots, y_m] \vee C_k[y_1, \dots, y_m]$$

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

MCSat – Finite Basis

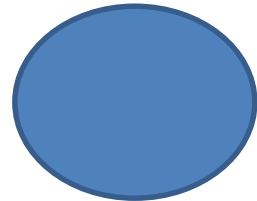


$$F_n[x_1, x_2, \dots, x_{n-1}, x_n]$$

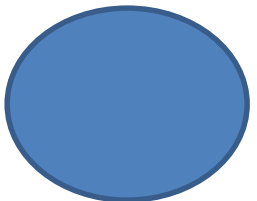


$$F_{n-1}[x_1, x_2, \dots, x_{n-1}]$$

...

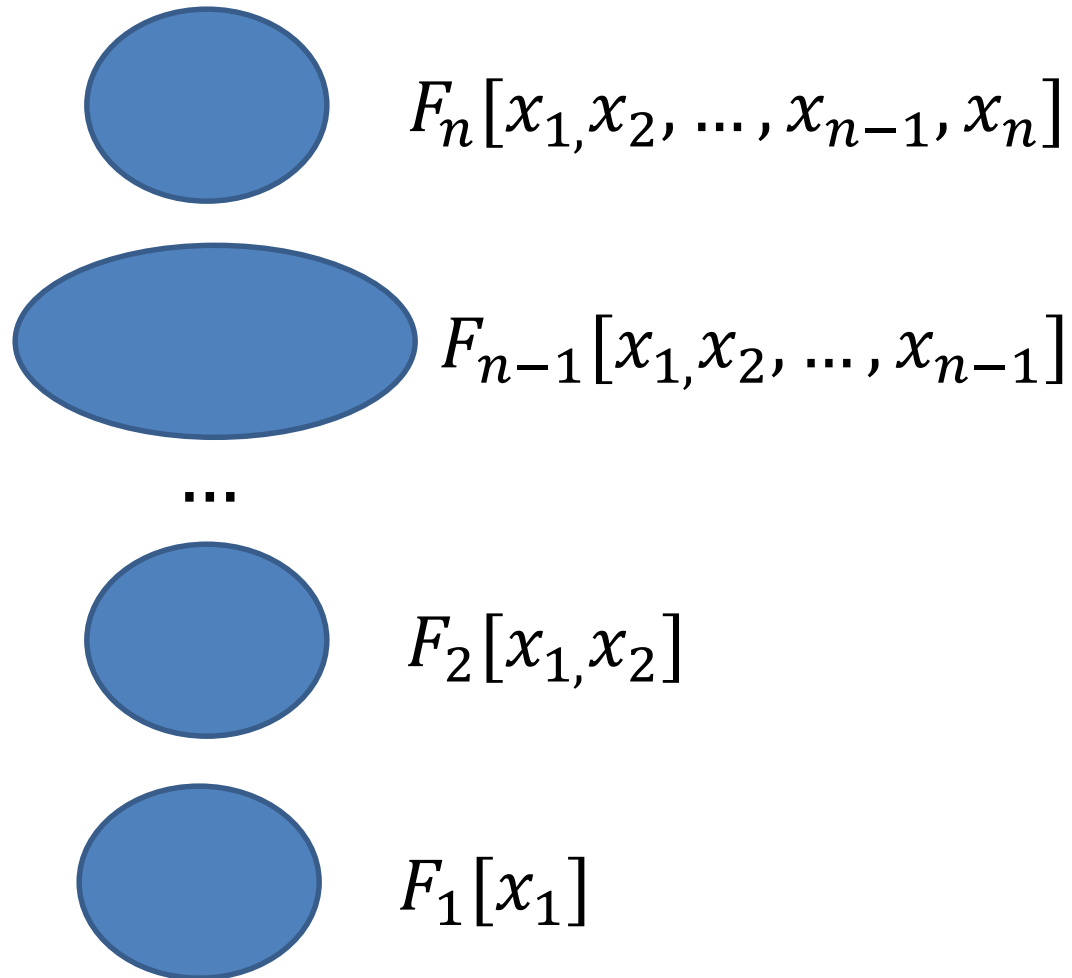


$$F_2[x_1, x_2]$$

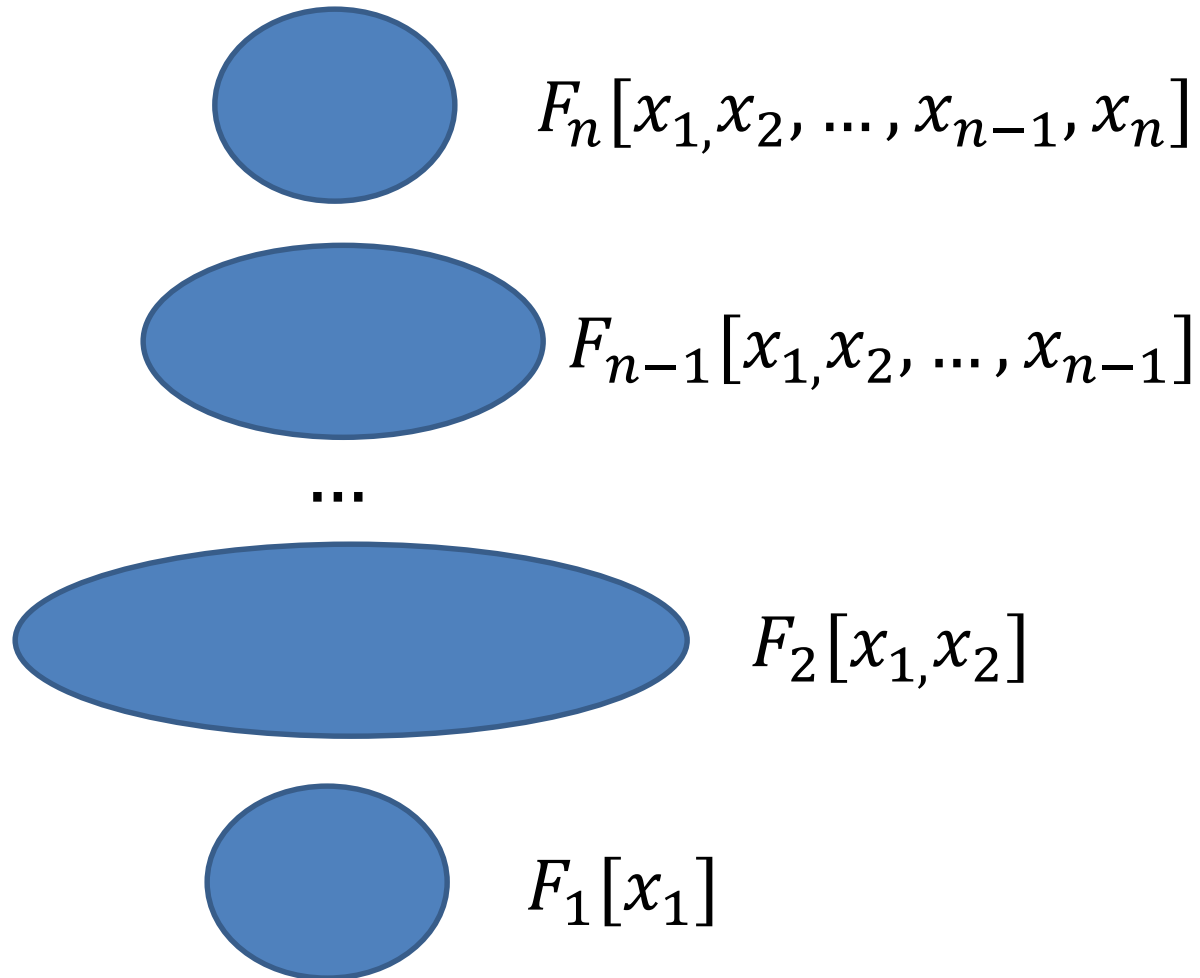


$$F_1[x_1]$$

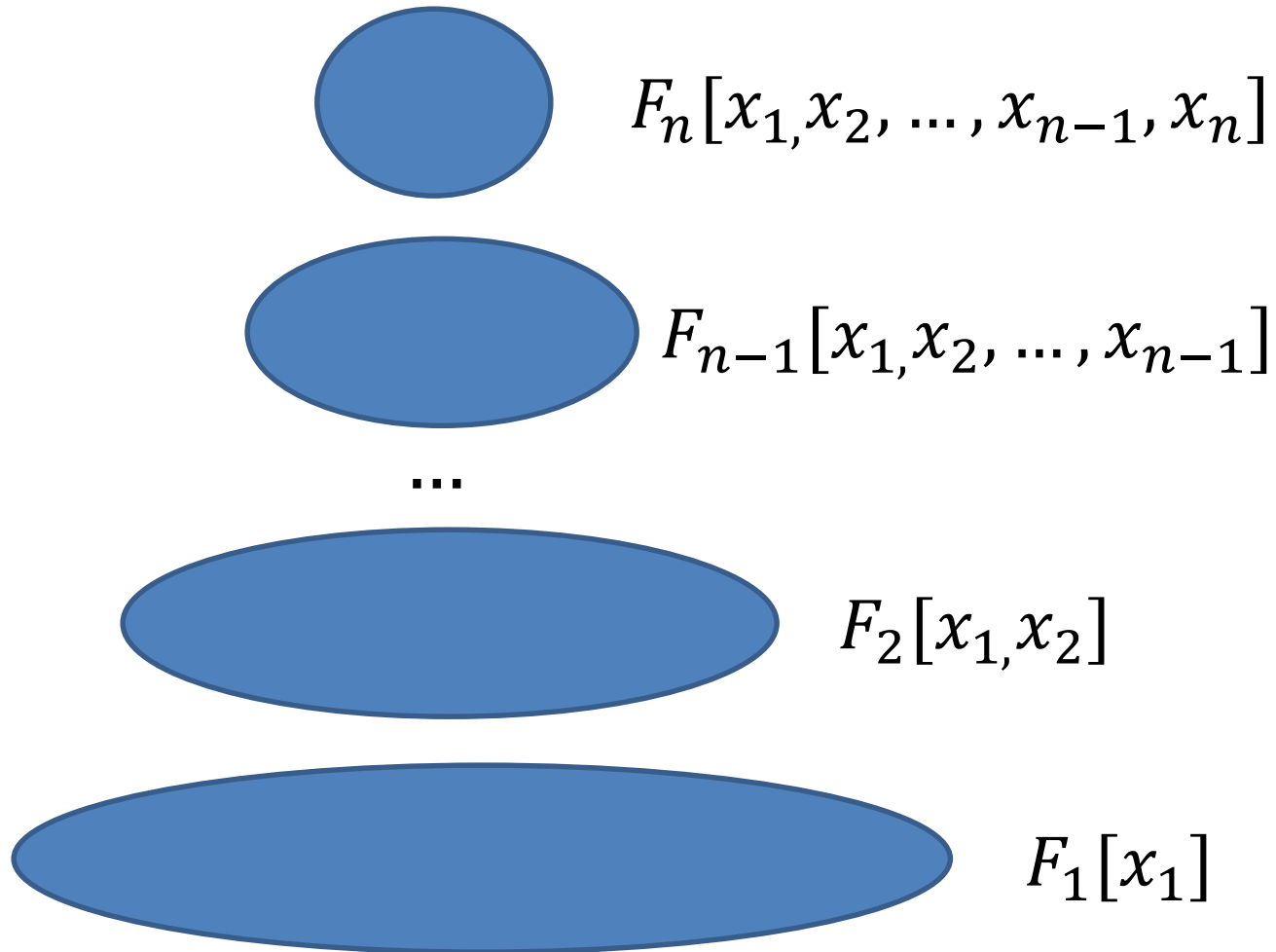
MCSat – Finite Basis



MCSat – Finite Basis



MCSat – Finite Basis



MCSat – Finite Basis

Every “finite” theory has a finite basis

$$F[x_1, \dots, x_n, y_1, \dots, y_m] \quad y_1 \rightarrow \alpha_1, \dots, y_m \rightarrow \alpha_m$$

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

MCSat – Finite Basis

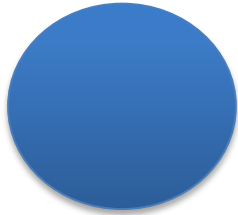
Theory of uninterpreted functions has a finite basis

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: Termination

Propagations



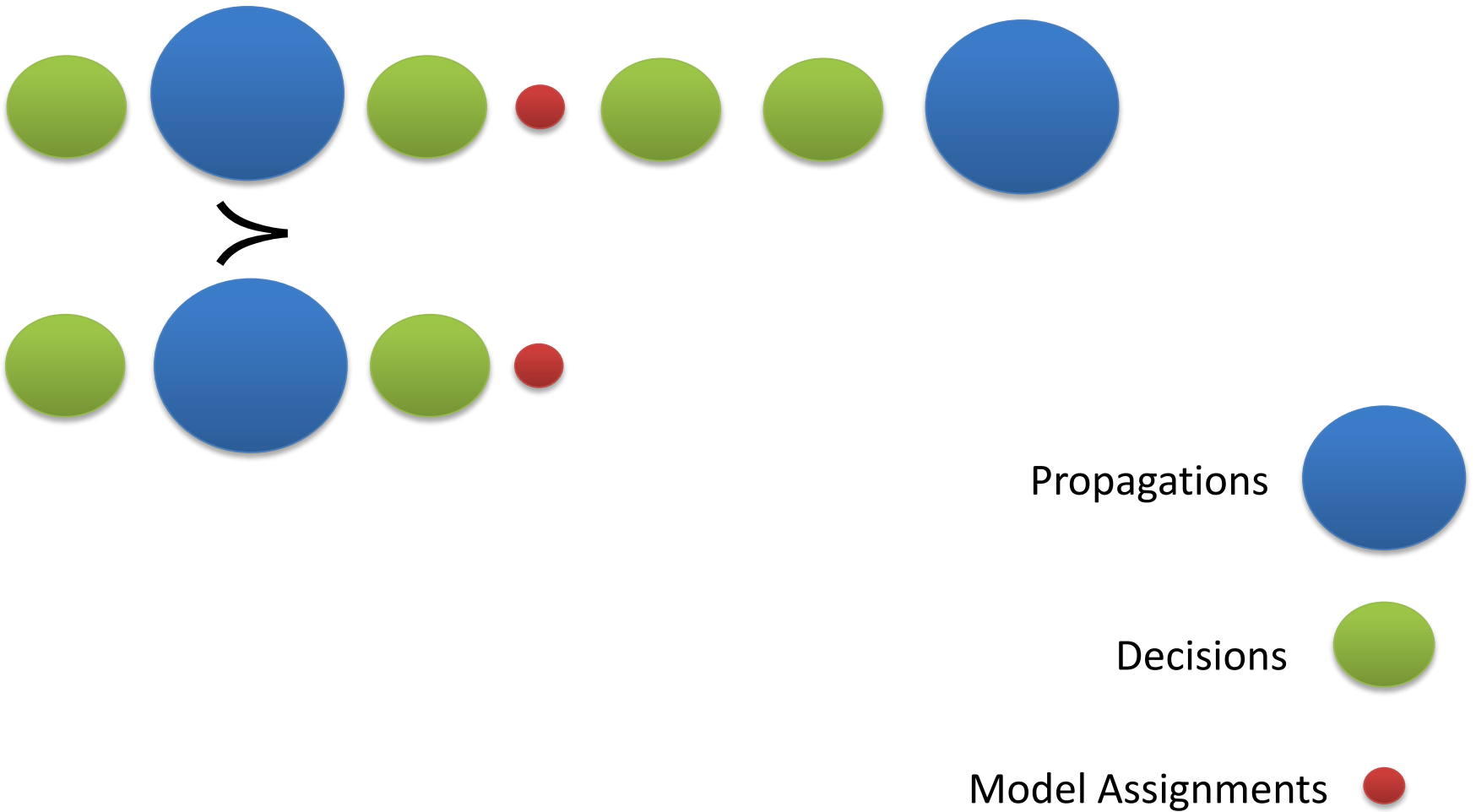
Decisions



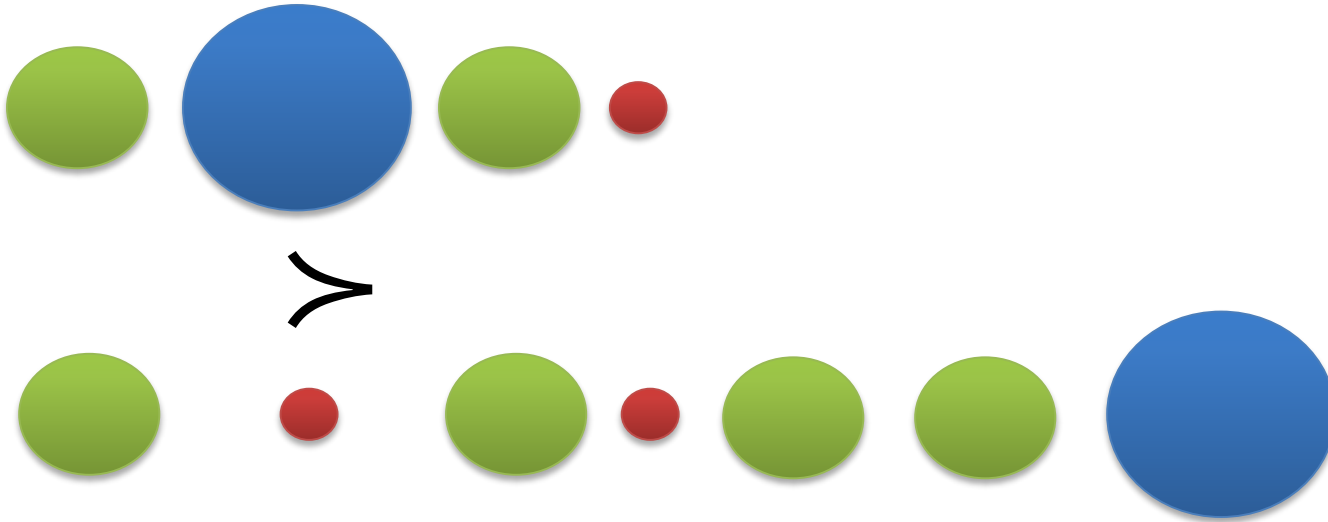
Model Assignments



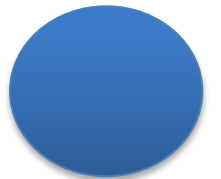
MCSat



MCSat



Propagations



Decisions

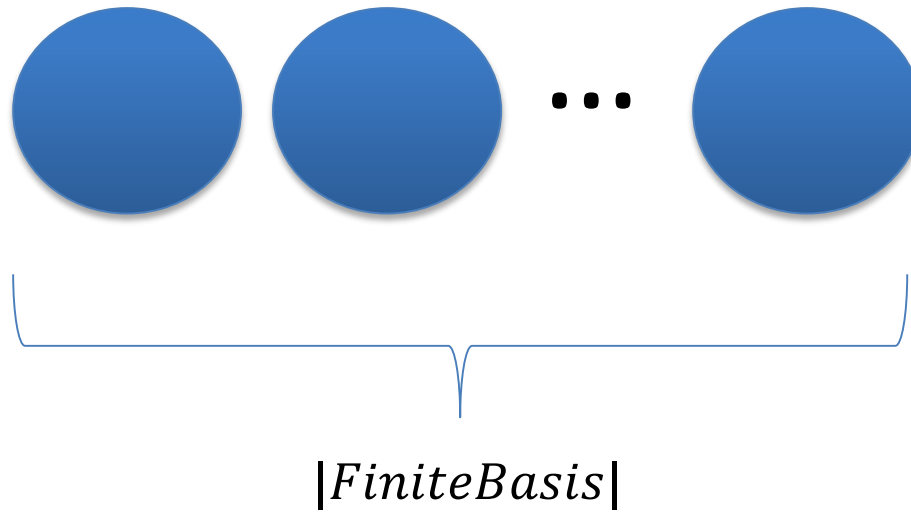


Model Assignments

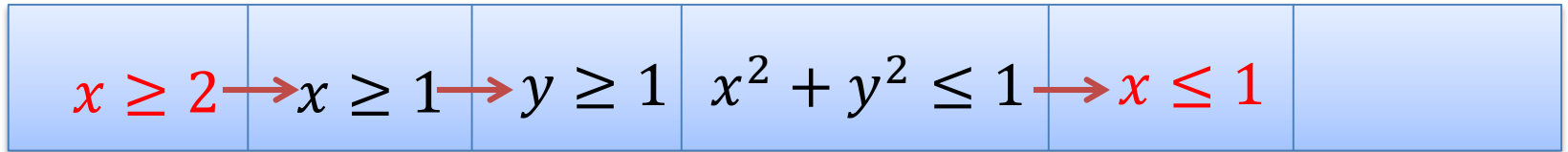


MCSat

Maximal Elements



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



Conflict

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

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

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

Conflict

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

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

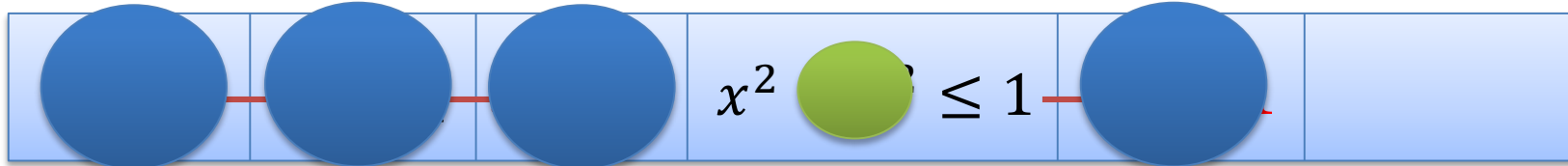
$$x \geq 2 \rightarrow x \geq 1 \rightarrow y \geq 1 \rightarrow \neg(x^2 + y^2 \leq 1)$$

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

$$x \geq 2,$$

$$(\neg x \geq 1 \vee y \geq 1),$$

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



Conflict

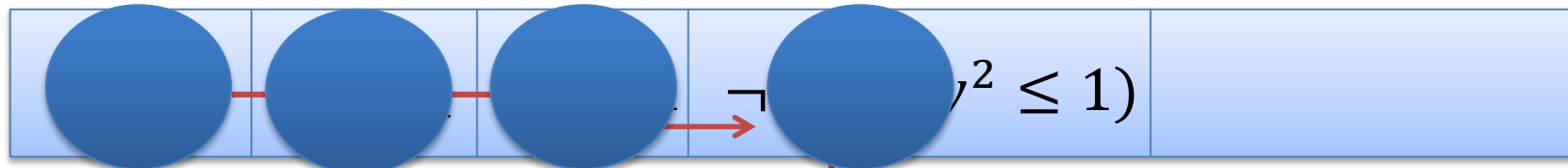
$$\neg(x \geq 2) \vee \neg(x \leq 1)$$

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

$$x \geq 2,$$

$$(\neg x \geq 1 \vee y \geq 1),$$

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



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

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

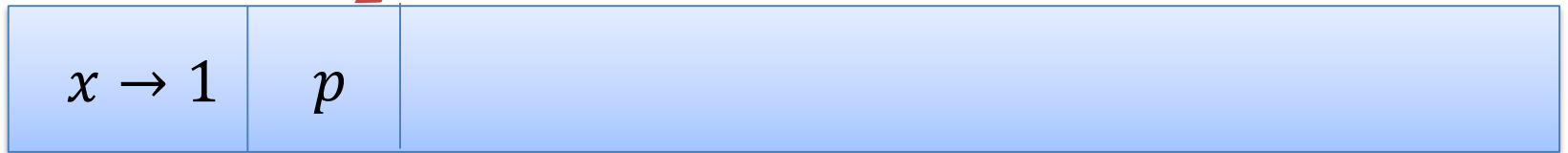
MCSat

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

$$x \rightarrow 1$$

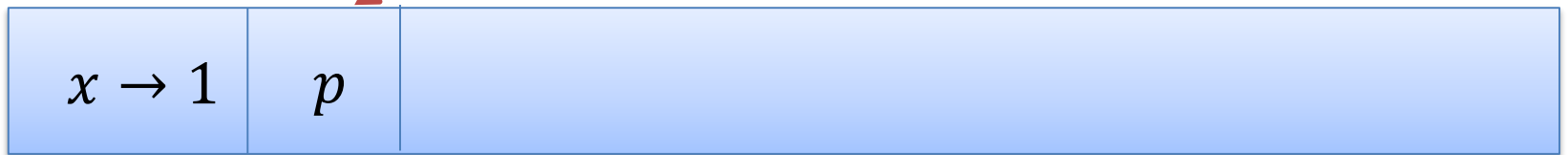
MCSat

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



MCSat

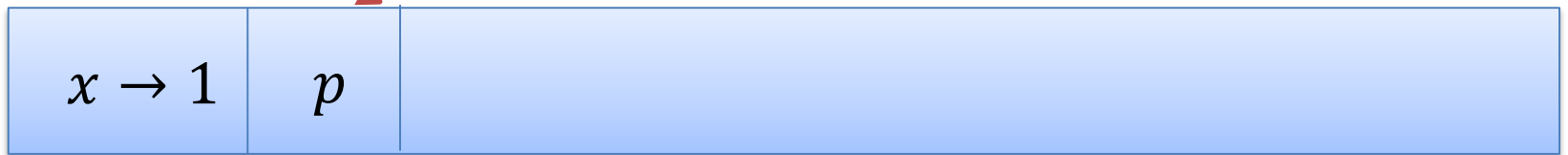
$$x < 1 \vee p, \quad \neg p \vee x = 2$$



Conflict (evaluates to false)

MCSat

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

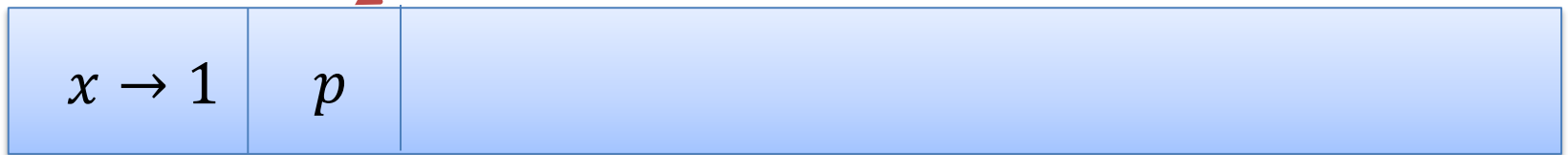


New clause

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

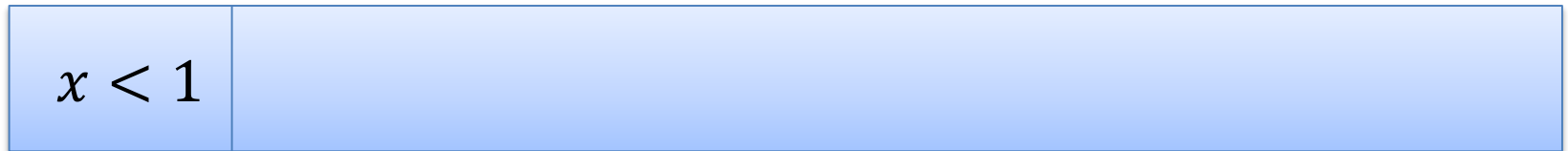
MCSat

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



New clause

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



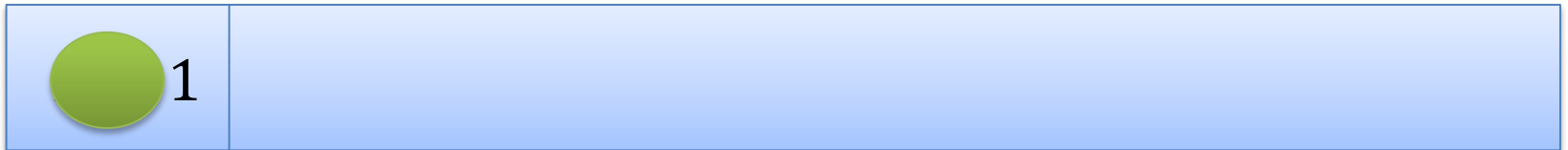
MCSat

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

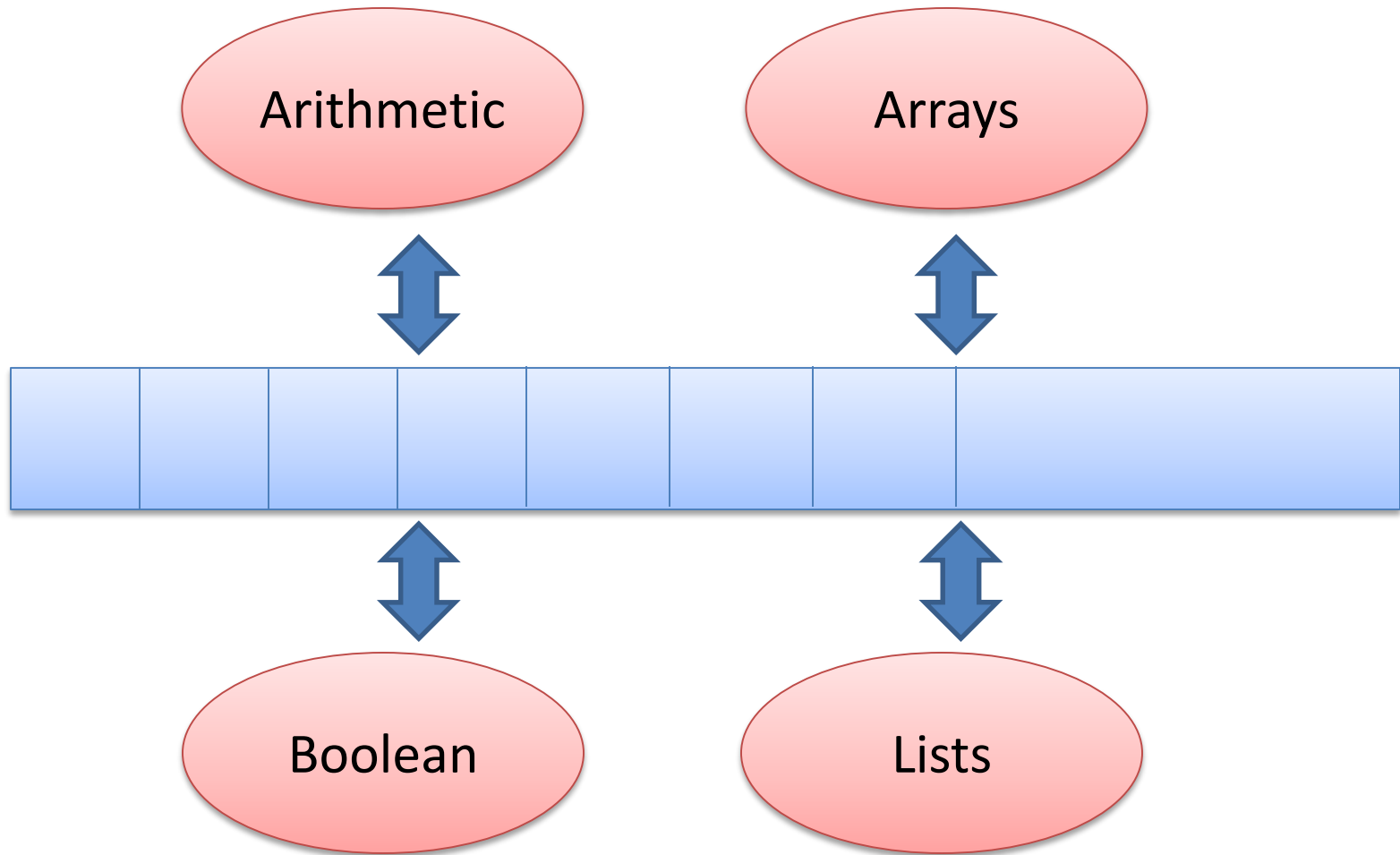


New clause

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



MCSat: Architecture



MCSat: development

Z3

