# 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

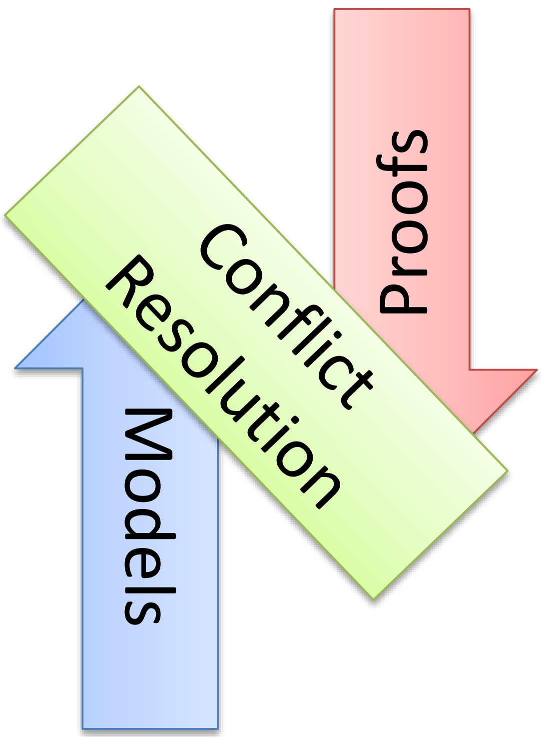
Logic is "The Calculus of Computer Science"

Zohar Manna

# Saturation x Search

Proof-finding

Model-finding



# SAT

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

$$p_1 = true, \qquad p_2 = true, \qquad p_3 = true$$

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

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

$$l, \neg l \quad \Rightarrow \quad \textbf{unsat}$$

Improvements

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

Ordered Resolution

Subsumption (delete redundant clauses)

$C$ *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

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

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

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

# Resolution: Example

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

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

$$\neg p \vee \neg q \vee r,\ \neg p \vee q,\ p \vee r,\ \neg r,\ {\color{red}\neg q} \vee r,\ {\color{red}q} \vee r \qquad \Rightarrow$$

$$\neg p \vee \neg q \vee r,\ \neg p \vee q,\ p \vee r,\ \neg r,\ \neg q \vee r,\ q \vee r,\ {\color{red}r}$$

# Resolution: Example

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

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

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

$\neg p \vee \neg q \vee r,\ \neg p \vee q,\ p \vee r,\ \color{red}{\neg r},\ \neg q \vee r,\ q \vee r,\ \color{red}{r} \quad \Rightarrow$

**unsat**

# Resolution: Problem

Exponential time and space

# Unit Resolution

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

$C$
subsumes
$C \vee l$

Complete for Horn Clauses

$$\neg q_1 \vee\ \ldots \vee \neg qn \vee p$$

# DPLL

Split rule

$$
\begin{tikzcd}
 & S \arrow[dl] \arrow[dr] & \\
S, p & & S, \neg p
\end{tikzcd}
$$

DPLL = Unit Resolution + Split rule

# DPLL

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

$$\begin{gathered} x \vee y, \\ \neg x \vee y, \\ x \vee \neg y, \\ \neg x \vee \neg y, \\ x \end{gathered}$$

# DPLL

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

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y,$

$x$

# DPLL

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

$y$,

$\neg y$,

$x$

# DPLL

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

$y,$

$\neg y,$

$x,$

$unsat$

# DPLL

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

$y,$

$\neg y,$

$x,$

$unsat$

$x \vee y,$

$\neg x \vee y,$

$x \vee \neg y,$

$\neg x \vee \neg y,$

$\neg x$

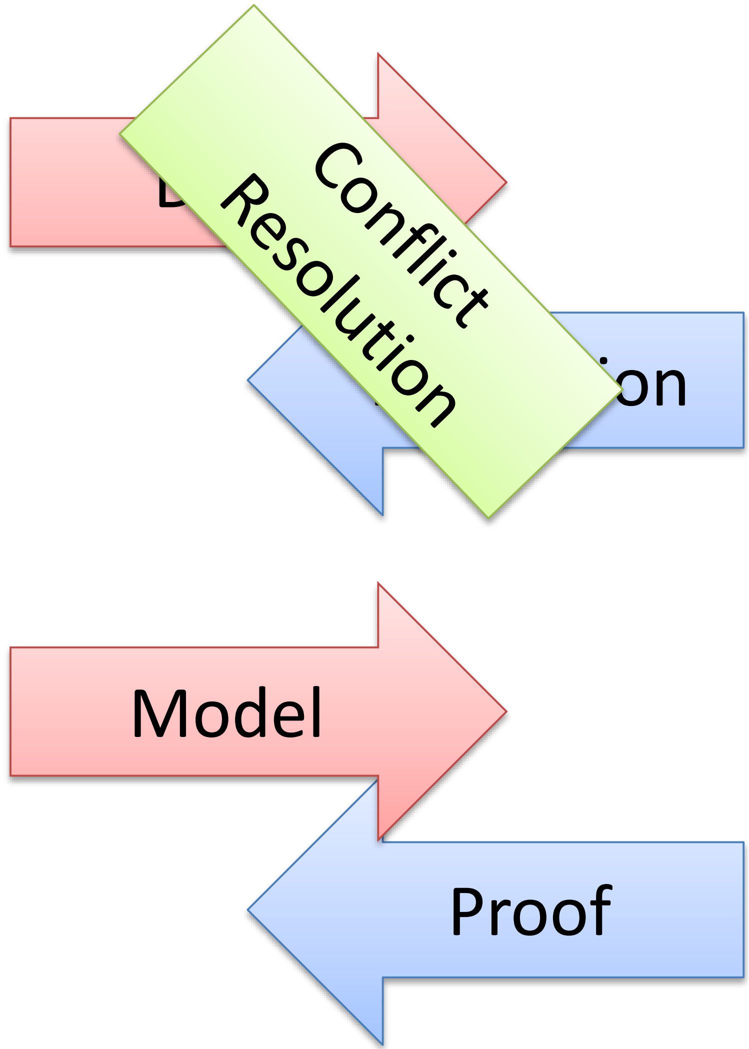
# DPLL

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

$y,$
$\neg y,$
$x,$
$unsat$

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

# CDCL: Conflict Driven Clause Learning



# MCSat

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

# 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

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

| | | |
|---|---|---|
| $x \geq 2$ | $\rightarrow x \geq 1$ | |

Propagations

# MCSat

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

| | | | |
|---|---|---|---|
| $x \geq 2$ → | $x \geq 1$ → | $y \geq 1$ | |

Propagations

# MCSat

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

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

Decisions

# MCSat

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

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

Model Assignments

# MCSat

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

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

Model Assignments

We can't falsify any fact in the trail.

# MCSat

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

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

Conflict

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

# MCSat

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

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

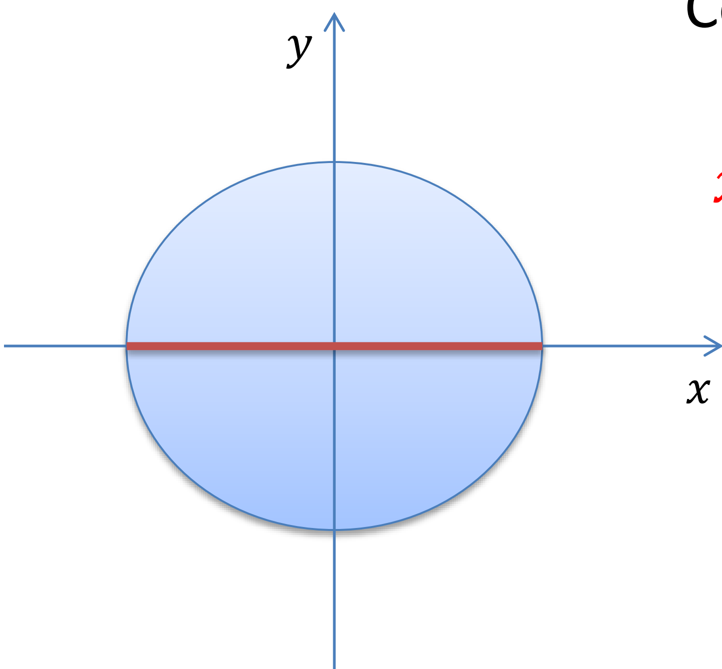
Conflict

We can't find a value 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

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

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




Conflict

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

$x \rightarrow 2$

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

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

# MCSat

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

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

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

# MCSat

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

$\color{red}{x \geq 2} \rightarrow x \geq 1 \rightarrow y \geq 1 \quad x^2 + y^2 \leq 1 \rightarrow \color{red}{x \leq 1}$

$\neg(x^2 + y^2 \leq 1) \vee \color{red}{x \leq 1}$

Conflict

$\neg(x \geq 2) \vee \color{red}{\neg(x \leq 1)}$

# MCSat

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

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

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

Learned by resolution

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

# MCSat

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

| | | | | |
|---|---|---|---|---|
| $\color{red}{x \geq 2}$ $\rightarrow$ | $x \geq 1$ $\rightarrow$ | $y \geq 1$ | $\neg(x^2 + y^2 \leq 1)$ | |

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

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

# MCSat – Finite Basis

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

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

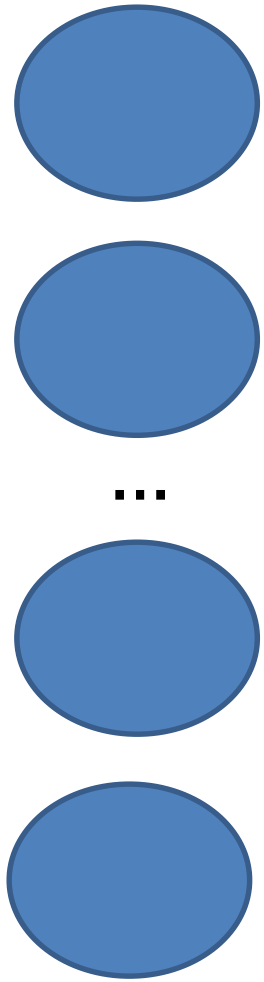
$$y_1 \to \alpha_1, \dots, y_m \to \alpha_m$$

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

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

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

# MCSat – Finite Basis



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

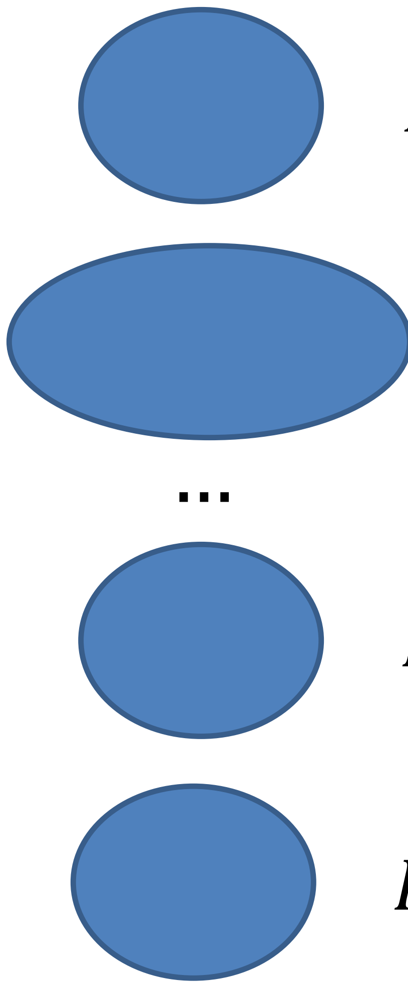
$F_{n-1}[x_{1,} x_2, \ldots, x_{n-1}]$

…

$F_2[x_{1,} x_2]$

$F_1[x_1]$

# MCSat – Finite Basis



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

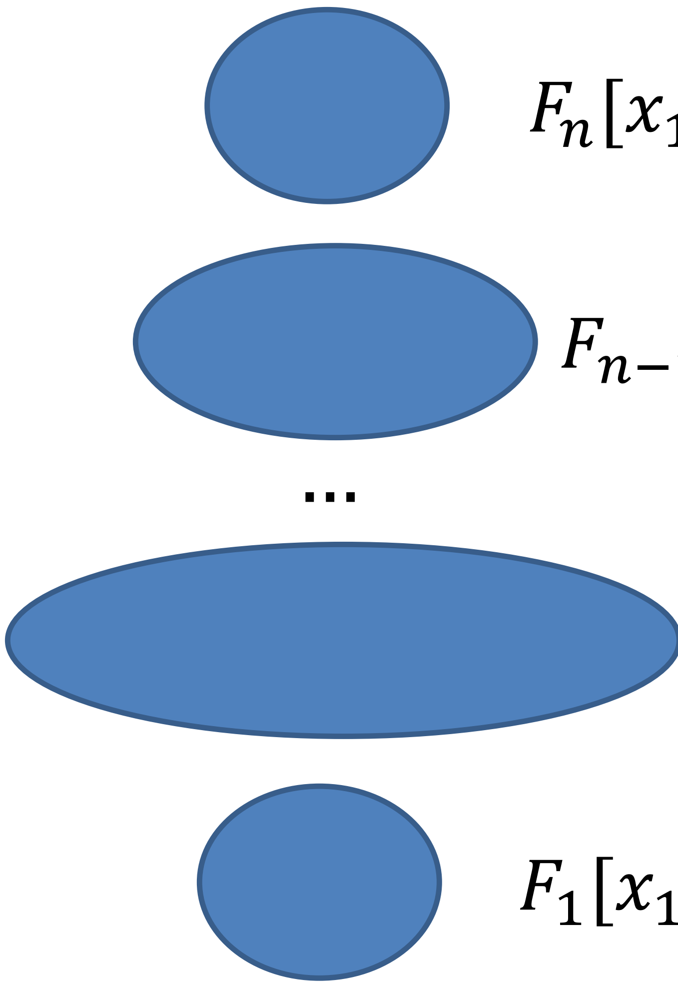
$F_{n-1}[x_{1,}x_2, \dots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

# MCSat – Finite Basis



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

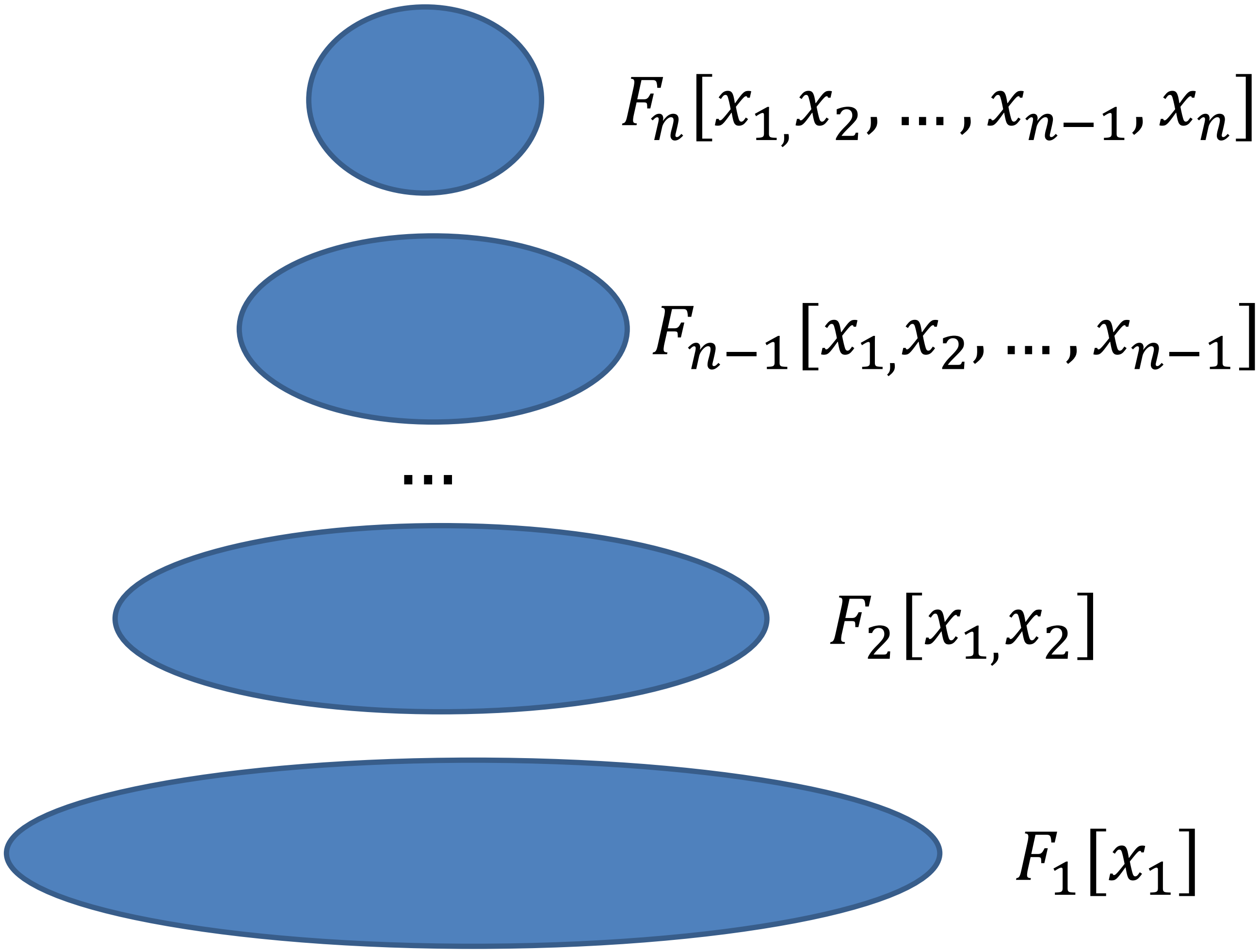
$F_{n-1}[x_{1,} x_2, \ldots, x_{n-1}]$

…

$F_2[x_{1,} x_2]$

$F_1[x_1]$

# MCSat – Finite Basis



# MCSat – Finite Basis

Every “finite” theory has a finite basis

$$F[x_1, \ldots, x_n, y_1, \ldots, y_m] \qquad\qquad y_1 \to \alpha_1, \ldots, y_m \to \alpha_m$$

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

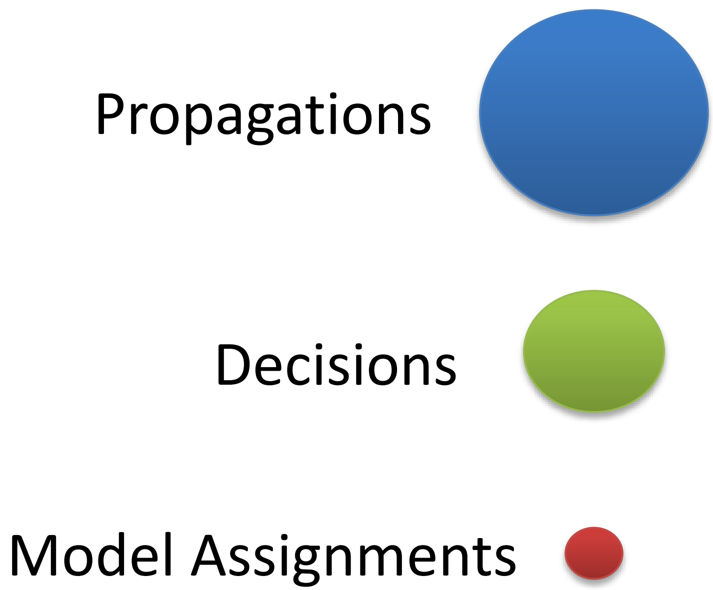
# MCSat – Finite Basis

Theory of uninterpreted functions has a finite basis

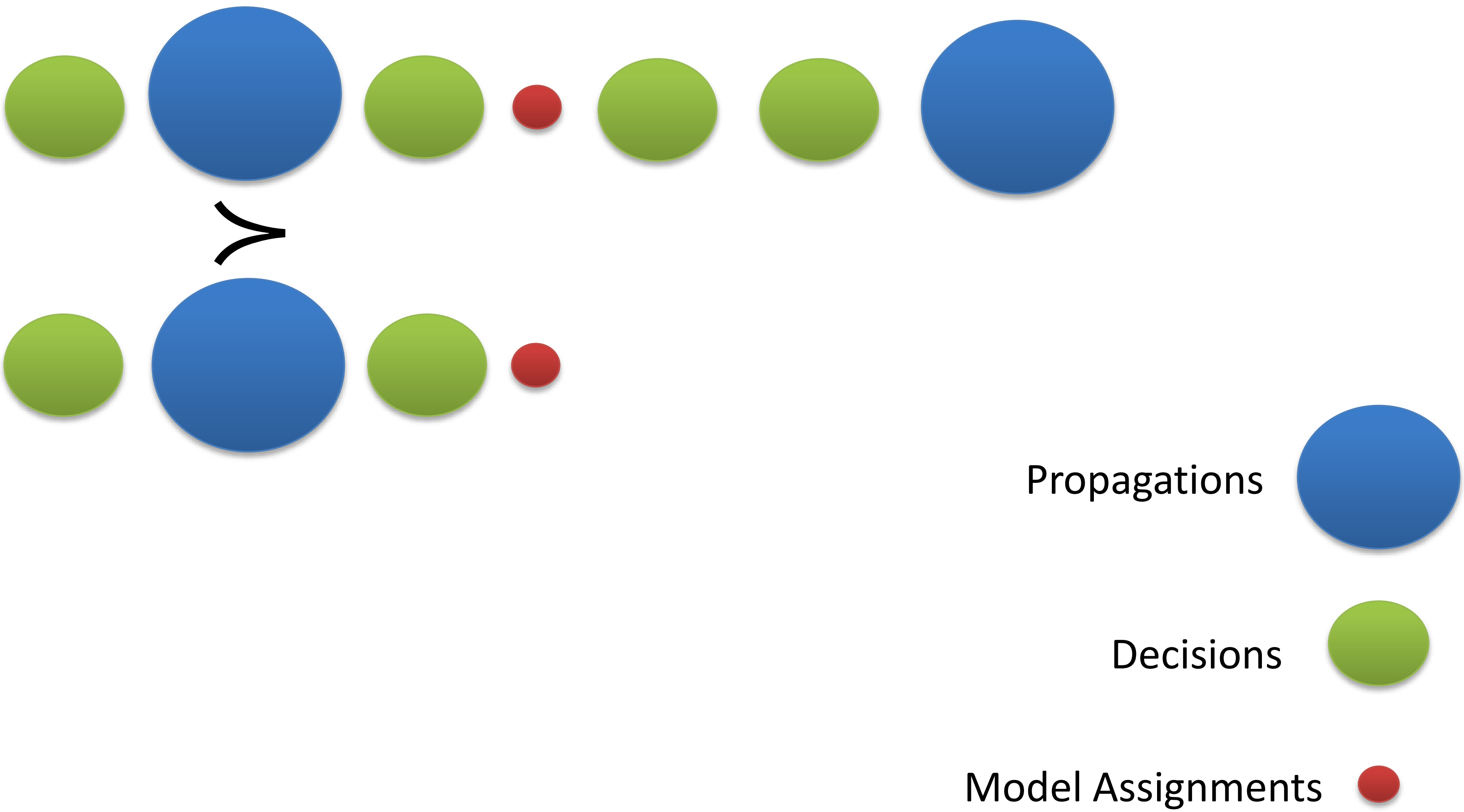
Theory of arrays has a finite basis [Brummayer- Biere 2009]

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

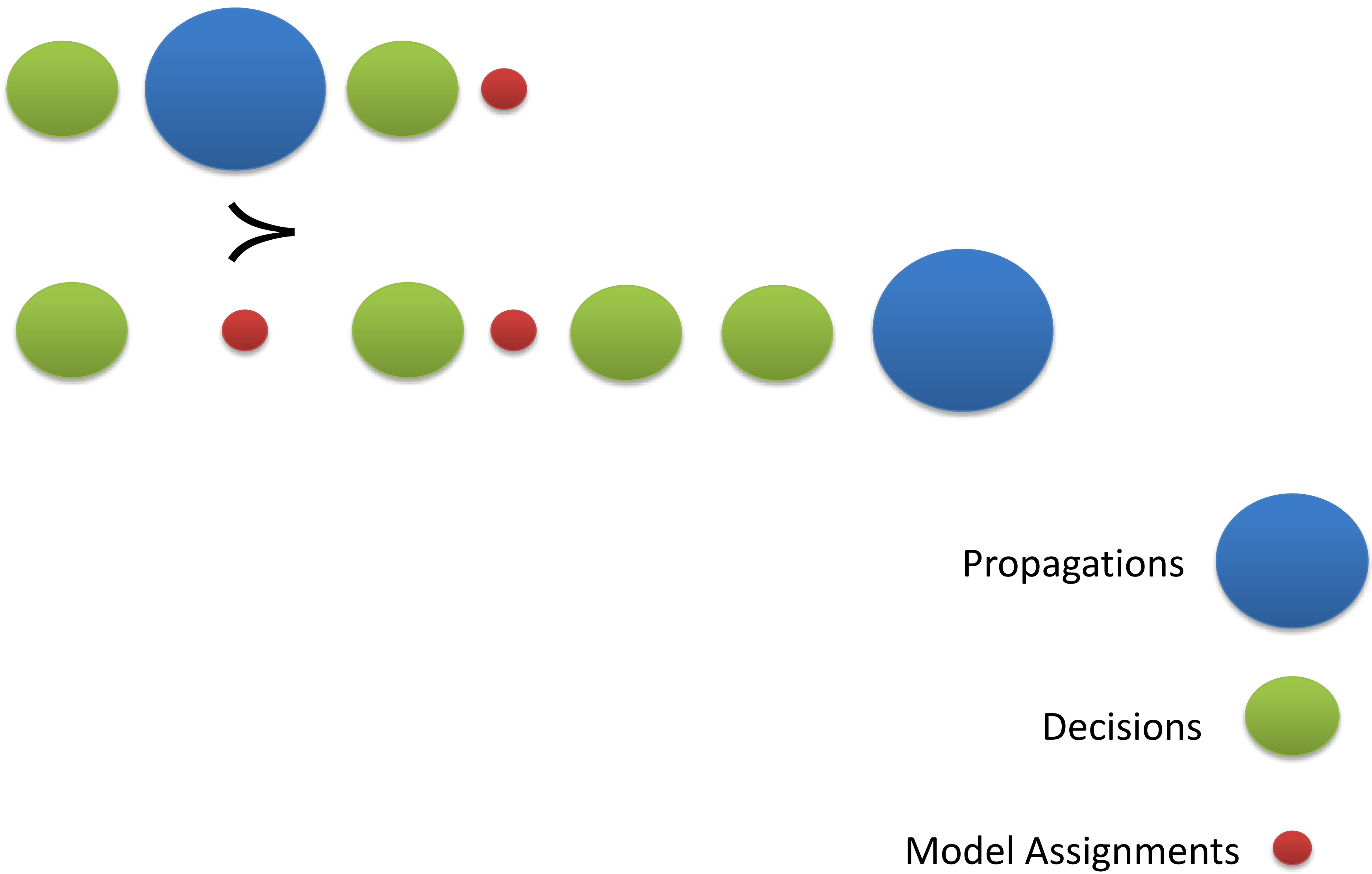
# MCSat: Termination



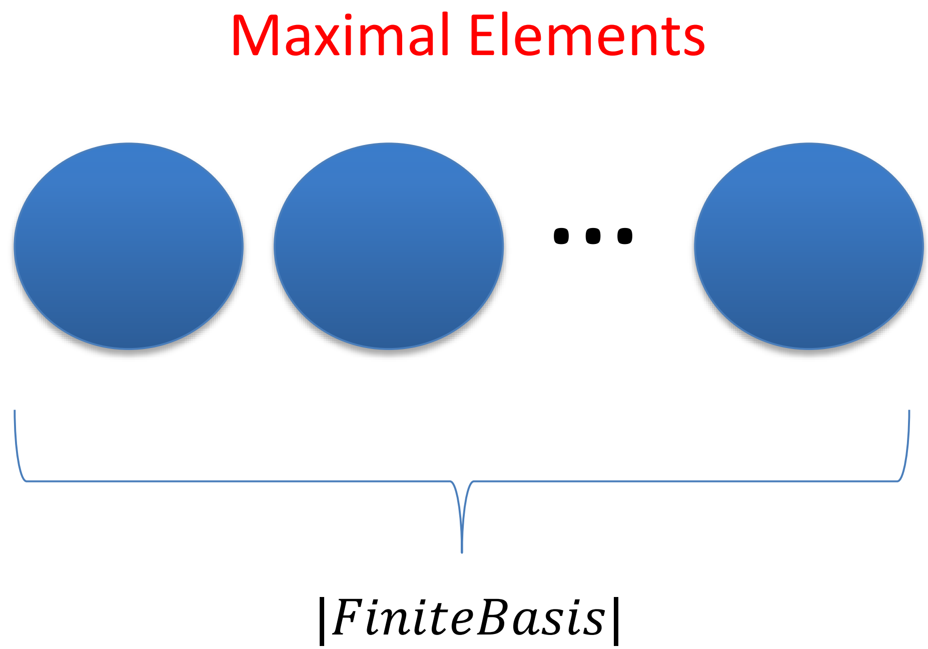
# MCSat



# MCSat



# MCSat



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

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

Conflict

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

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

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

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

Conflict

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

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

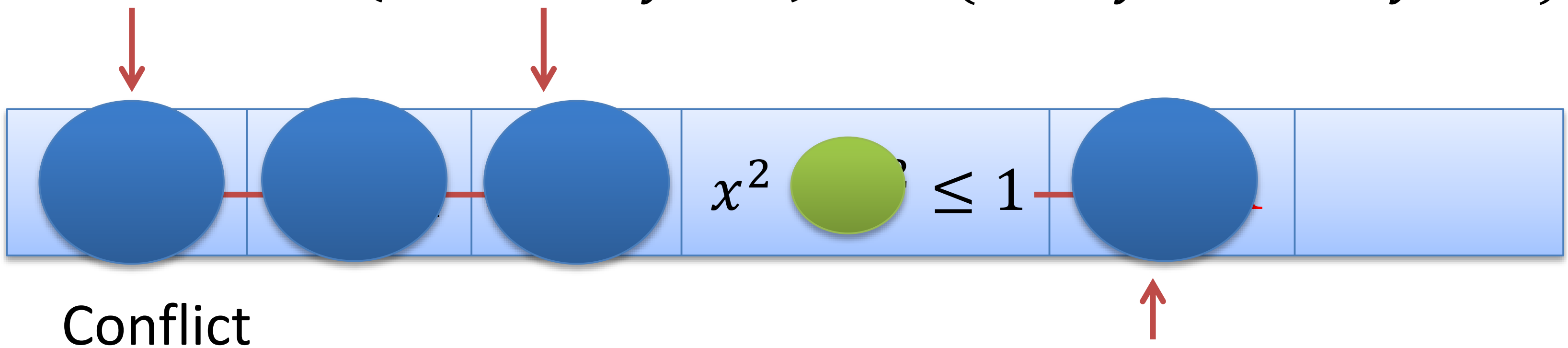
$x \geq 2, \qquad (\neg x \geq 1 \lor y \geq 1), \qquad (x^2 + y^2 \leq 1 \lor xy > 1)$

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

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

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

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

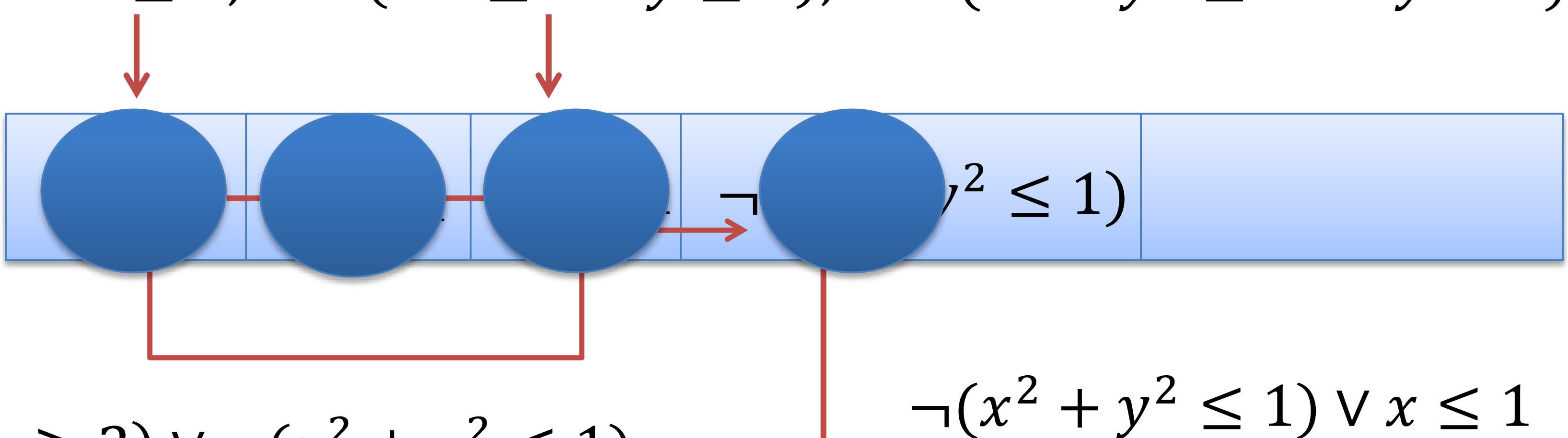


Conflict

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

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

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



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

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

# MCSat

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

| | |
|---|---|
| $x \to 1$ | |

# 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

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

| | | |
|---|---|---|
| $x \to 1$ | $p$ | |

New clause

$x < 1 \vee x = 2$

| | |
|---|---|
| $x < 1$ | |

# MCSat

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

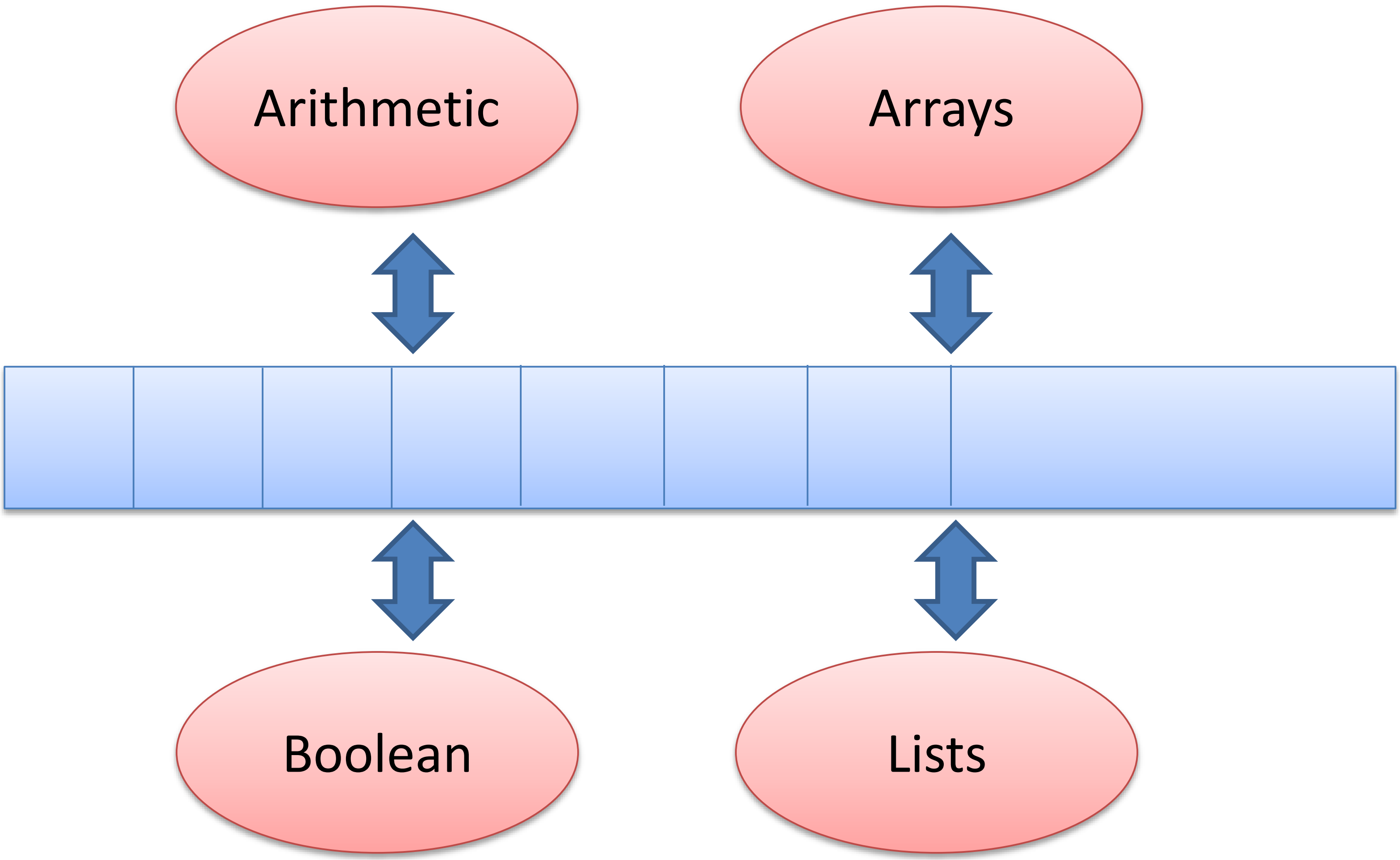
$x \to 1$

New clause

$x < 1 \vee x = 2$

1

# MCSat: Architecture



# MCSat: development