Arithmetic and Optimization @ MCSat

Leonardo de Moura
Joint work with
Dejan Jovanović and Grant Passmore

Arithmetic and Optimization @ MCSat (random remarks)

Leonardo de Moura
Joint work with
Dejan Jovanović and Grant Passmore

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"

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

$x\,y - 1 > 0$

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	-

CONFLICT

$x \rightarrow -2$

2. Search

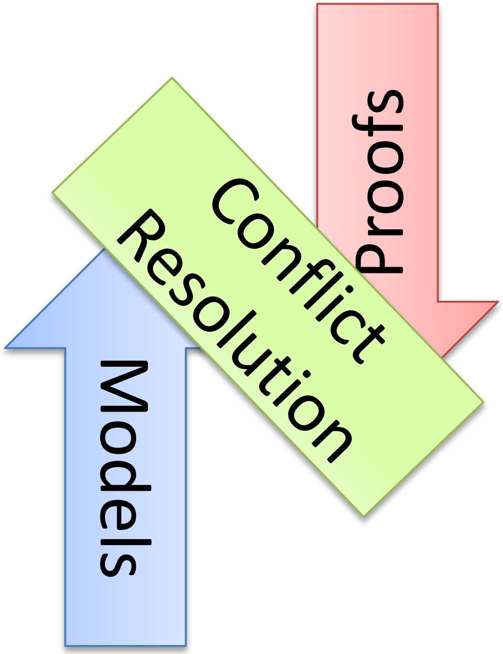
	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

NLSAT: MCSAT for Nonlinear Arithmetic

Static x Dynamic

Optimistic approach

Key ideas



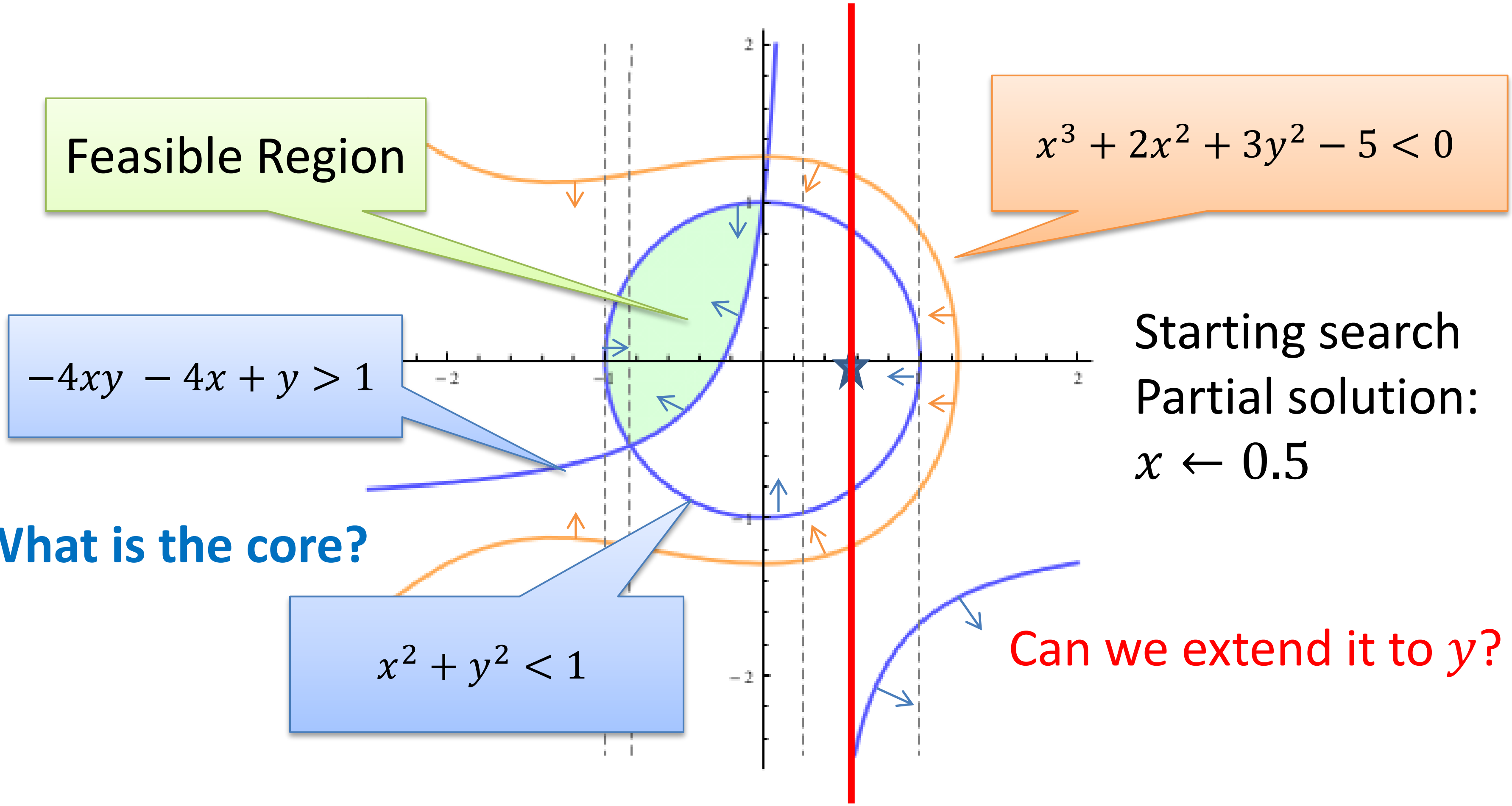
Start the Search before Saturate/Project

We saturate on demand

Model guides the saturation

NLSAT/MCSAT

Key ideas: Use partial solution to guide the search



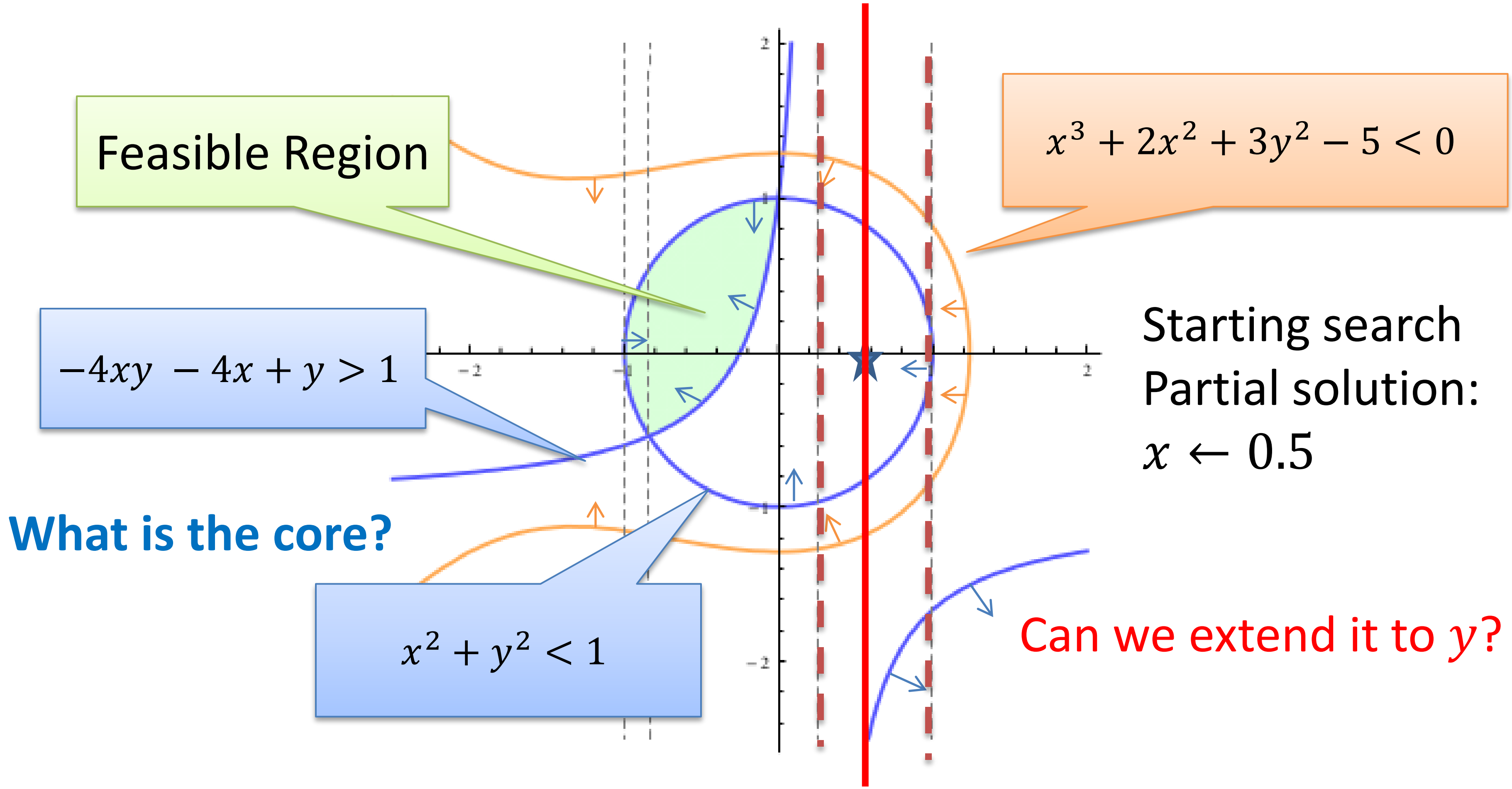
Starting search
Partial solution:
$x \leftarrow 0.5$

What is the core?

Can we extend it to y?

NLSAT/MCSAT

Key ideas: Use partial solution to guide the search



NLSAT/MCSAT

Key ideas: Solution based Project/Saturate

$$\mathsf{P}_c(A, x) = \bigcup_{f \in A} \mathsf{coeff}(f, x) \cup \bigcup_{\substack{f \in A \\ g \in \mathsf{R}(f,x)}} \mathsf{psc}(g, g'_x, x) \cup \bigcup_{\substack{i<j \\ g_i \in \mathsf{R}(f_i,x) \\ g_j \in \mathsf{R}(f_j,x)}} \mathsf{psc}(g_i, g_j, x)$$

Standard project operators are pessimistic.
Coefficients can vanish!

NLSAT/MCSAT

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

NLSAT/MCSAT

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

Propagations

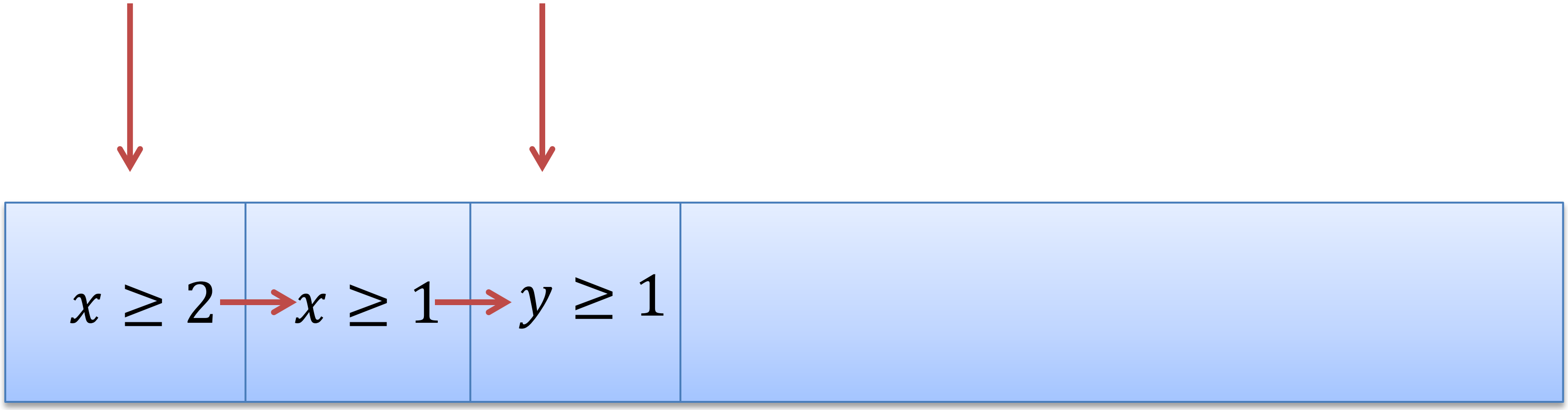
NLSAT/MCSAT

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

Propagations

NLSAT/MCSAT

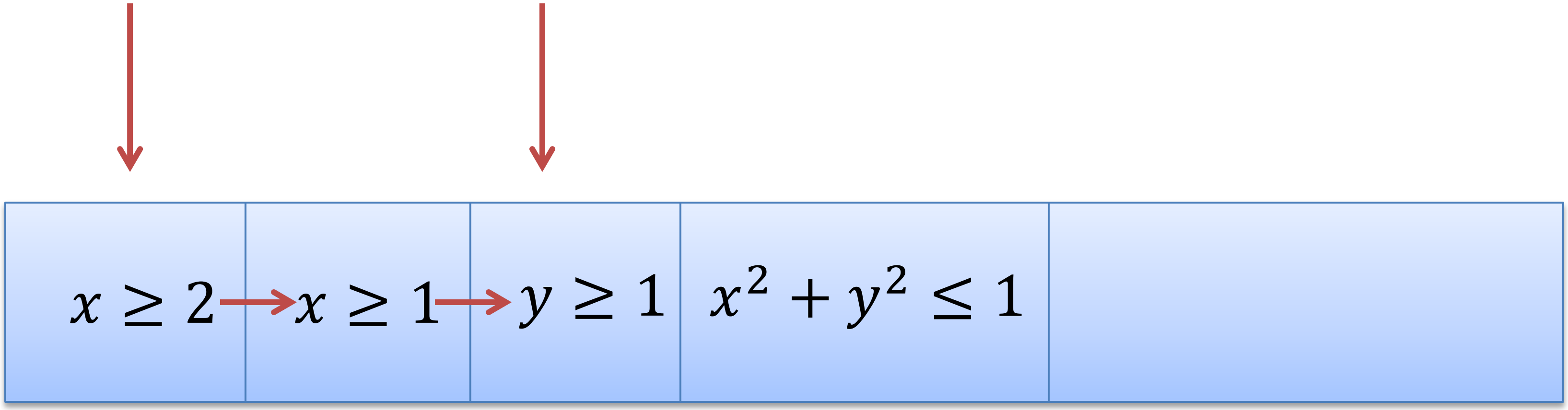
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



Propagations

NLSAT/MCSAT

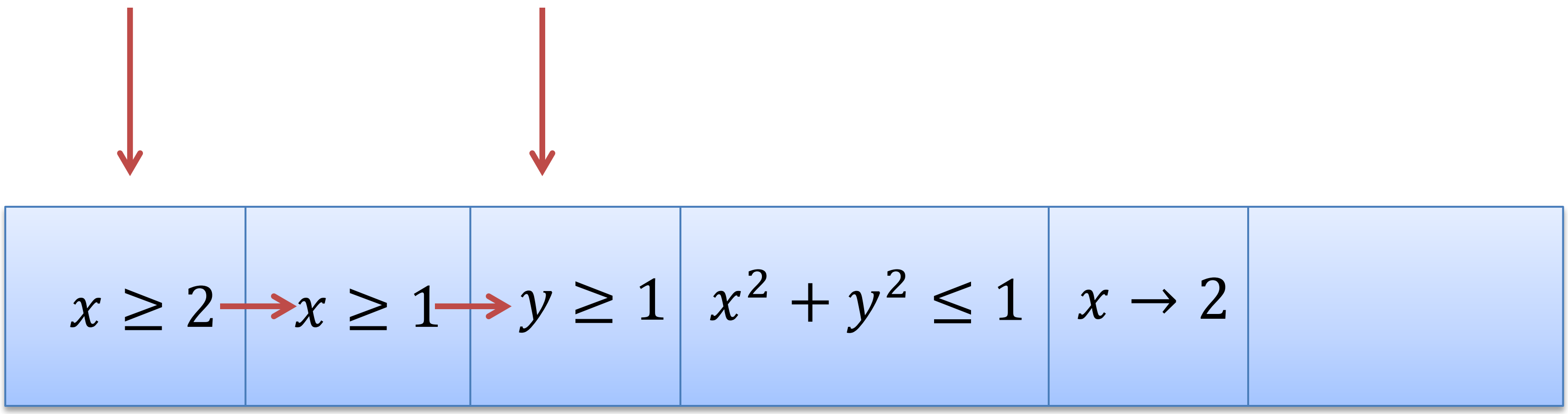
$x \geq 2, \quad (\neg x \geq 1 \lor y \geq 1), \quad (x^2 + y^2 \leq 1 \lor xy > 1)$



Boolean Decisions

NLSAT/MCSAT

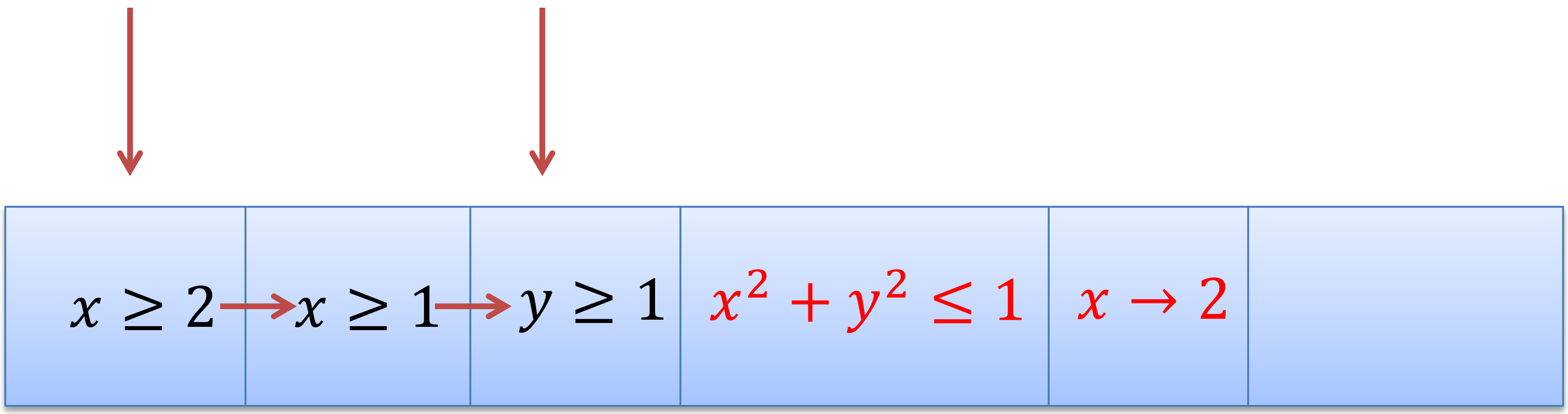
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



Semantic Decisions

NLSAT/MCSAT

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

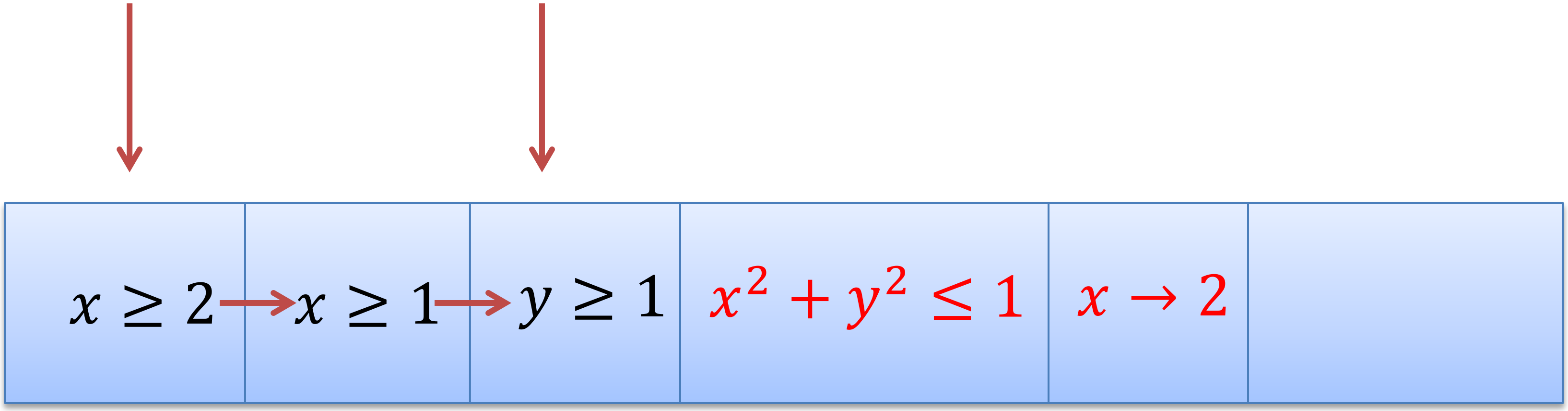


Conflict

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

NLSAT/MCSAT

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



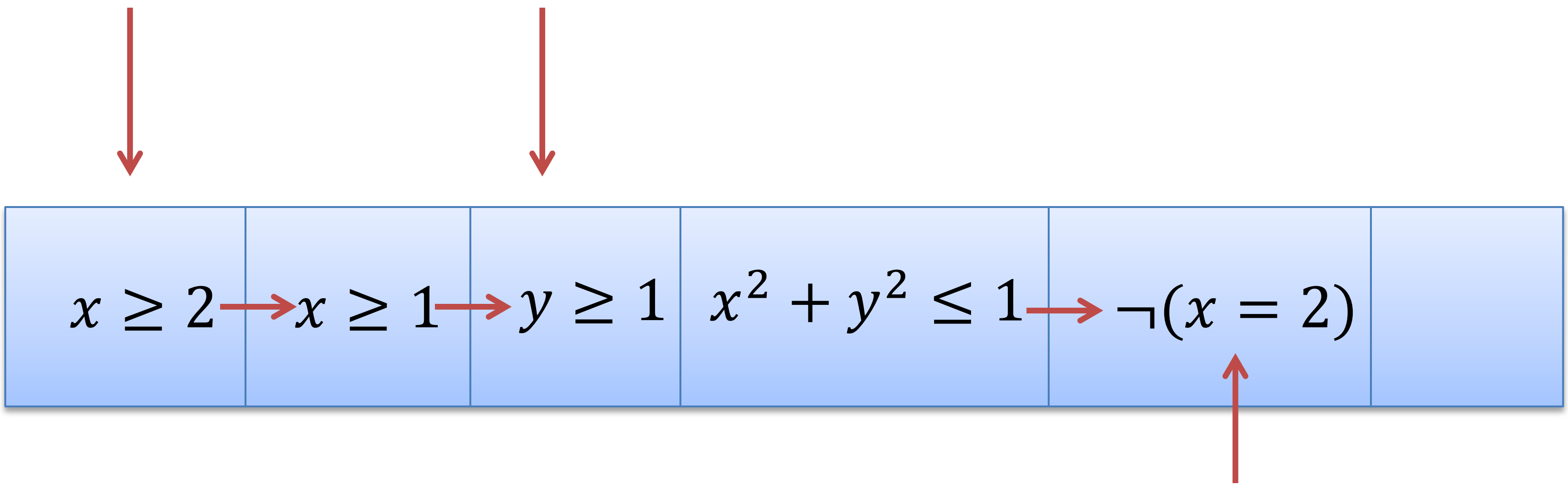
Conflict

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

NLSAT/MCSAT

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

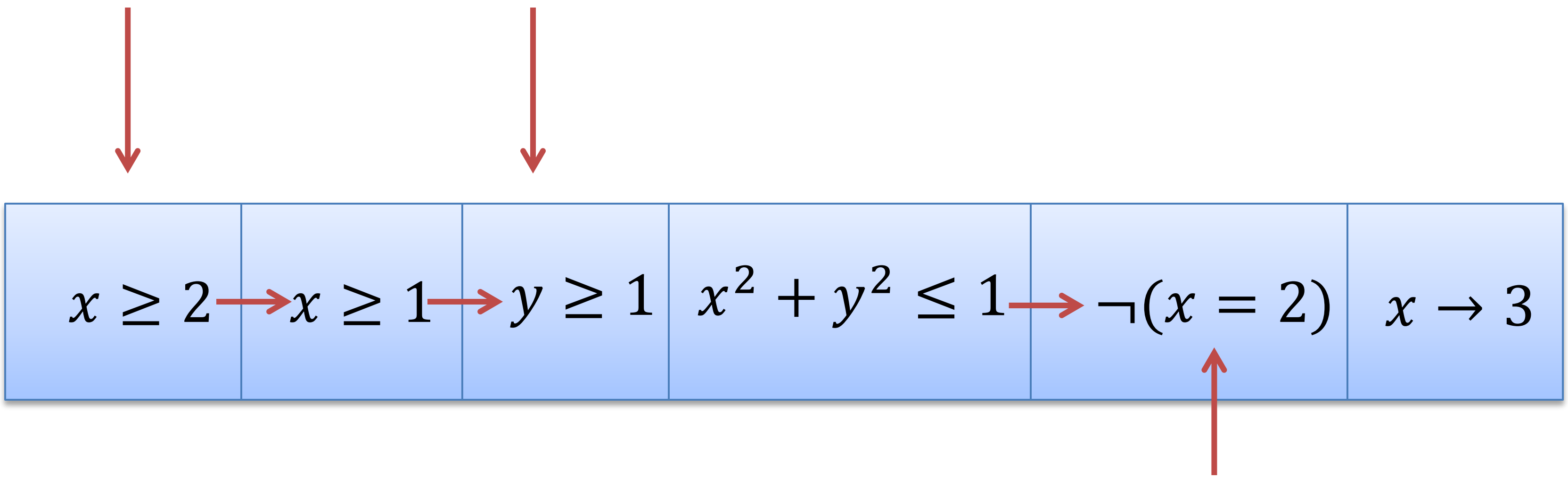


$\neg(x^2 + y^2 \leq 1) \lor \neg(x = 2)$

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

NLSAT/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

NLSAT/MCSAT

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

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

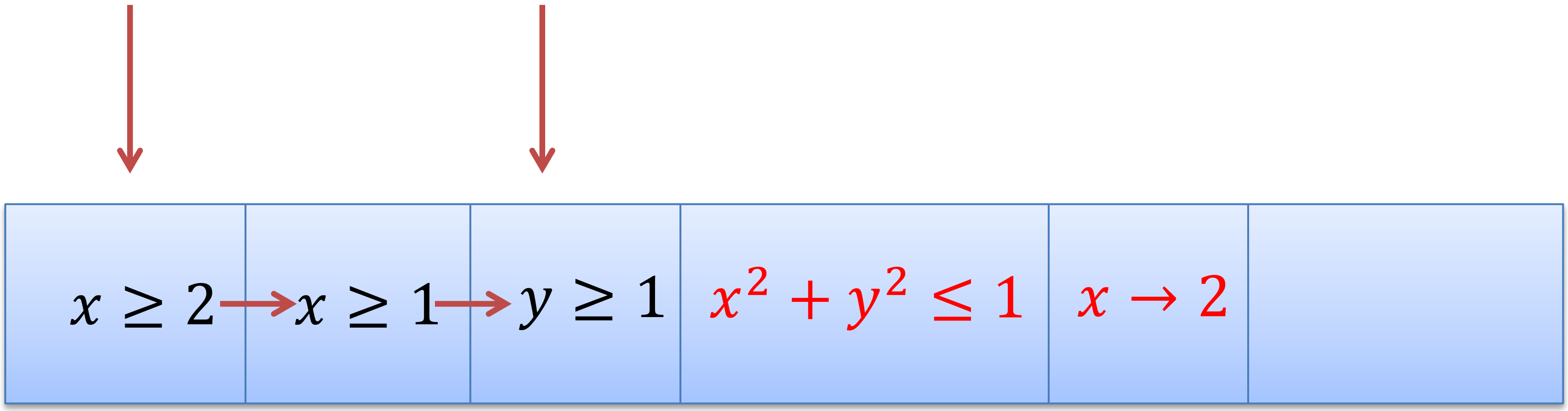
"Same" Conflict

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

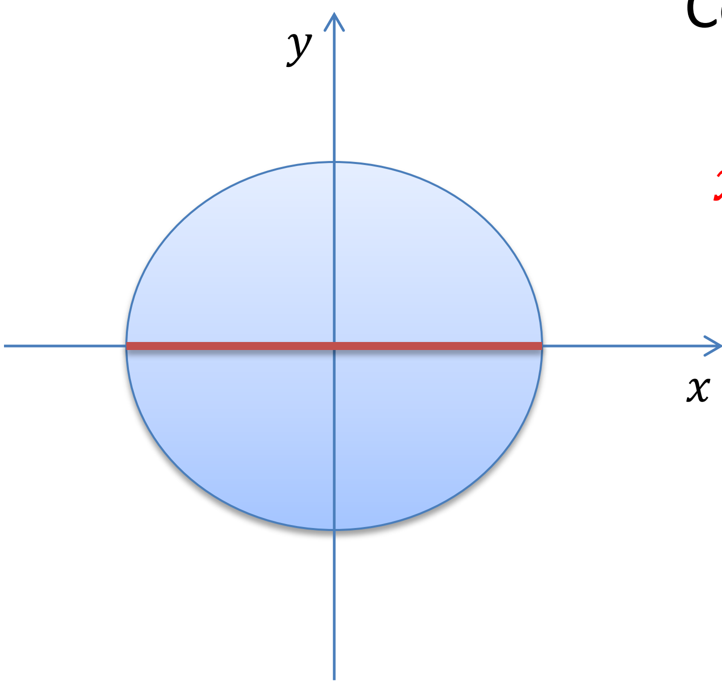
We can't find a value for y s.t. $9 + y^2 \leq 1$

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

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



Conflict



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

$x \to 2$

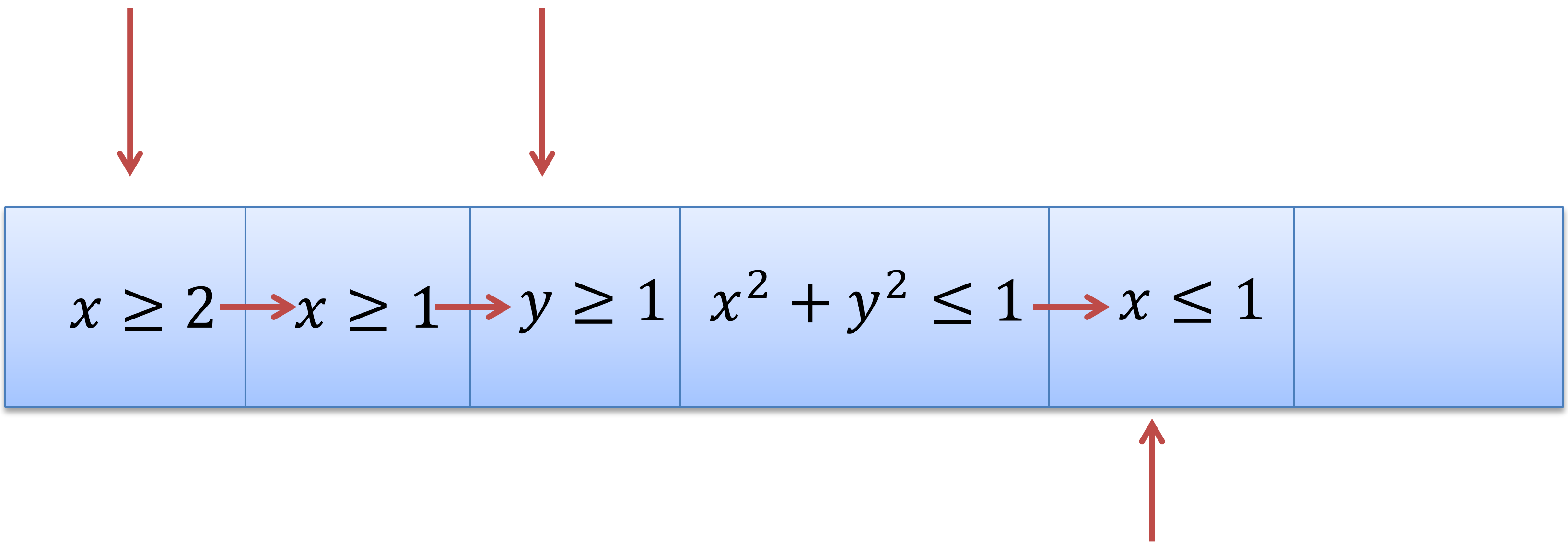
THIS IS AN INTERPOLANT

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

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

NLSAT/MCSAT

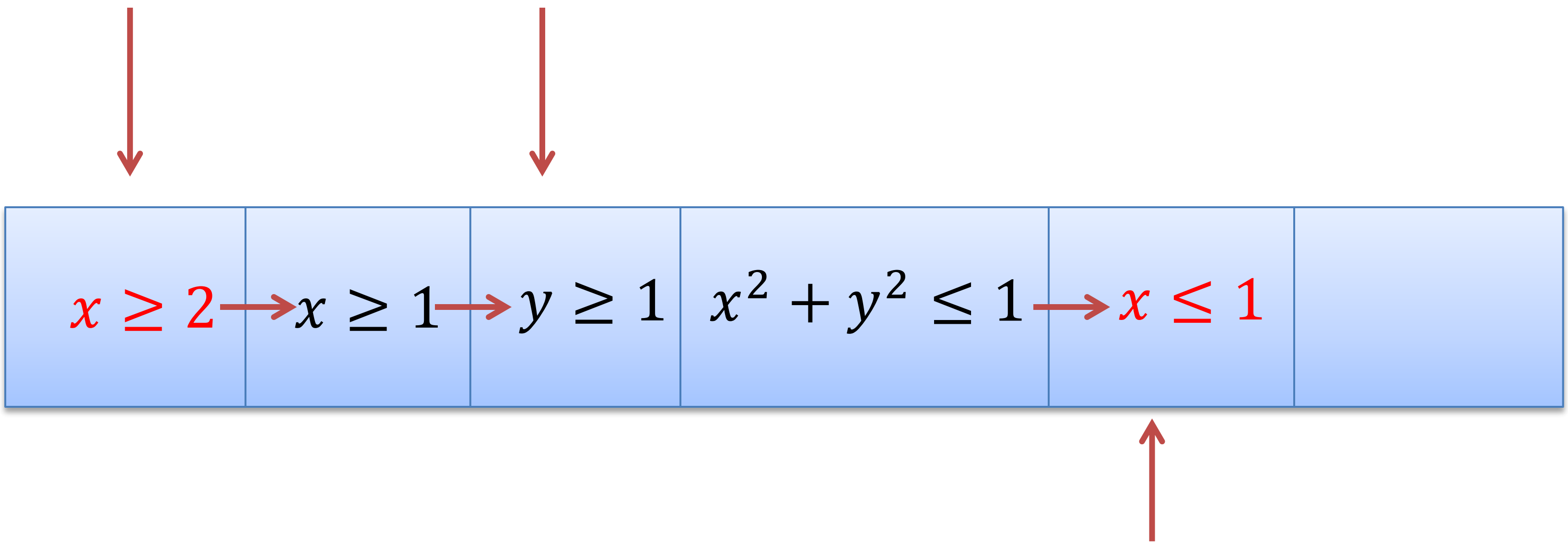
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$



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

NLSAT/MCSAT

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



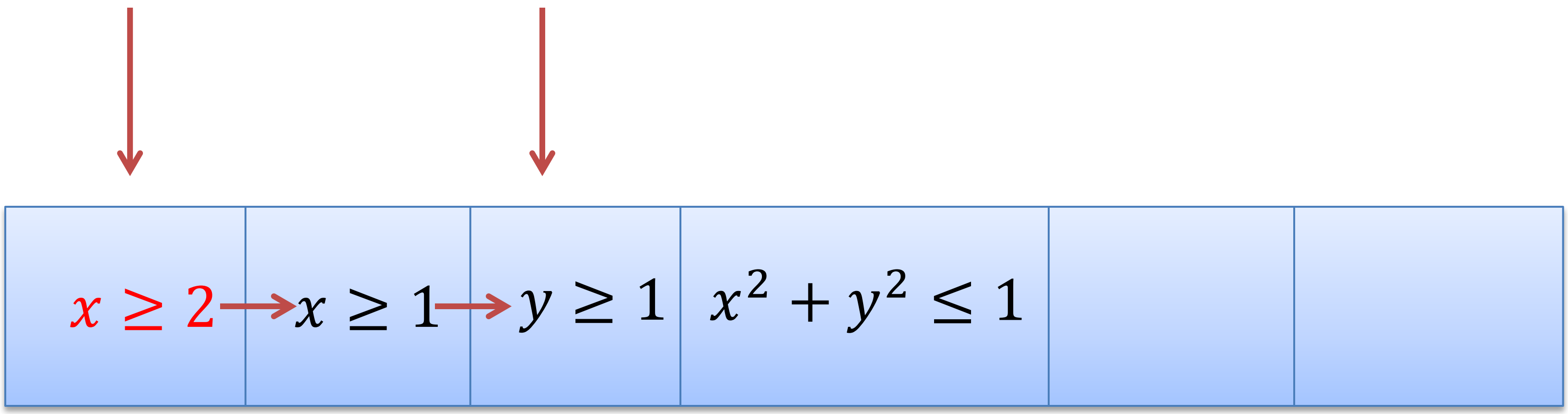
$\neg(x^2 + y^2 \leq 1) \vee x \leq 1$

Conflict

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

NLSAT/MCSAT

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



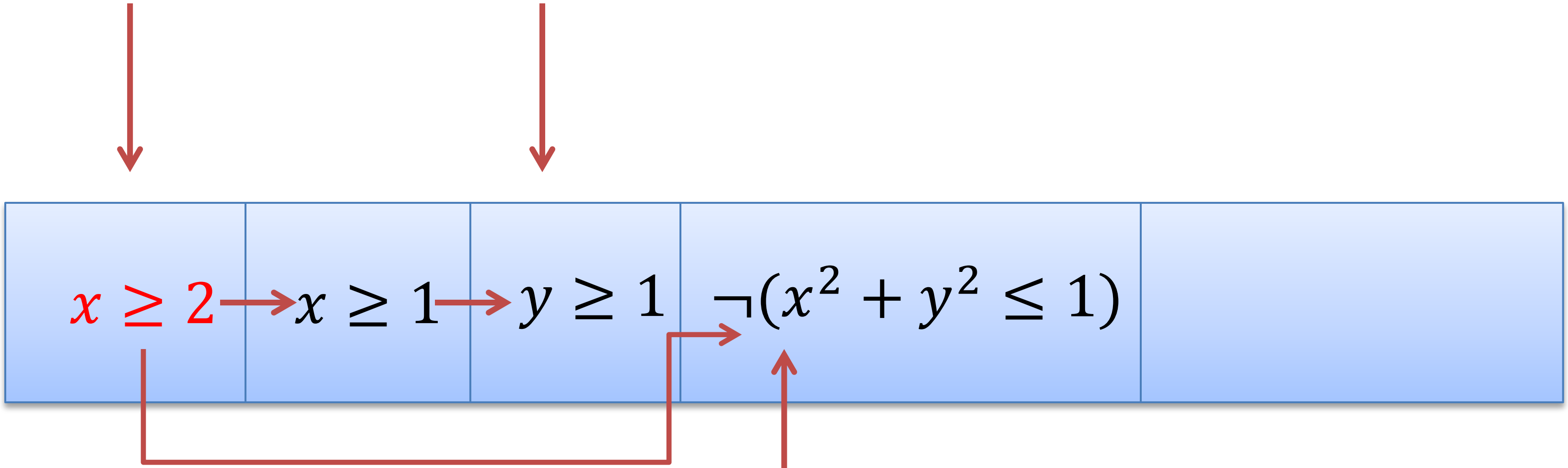
$\neg(x^2 + y^2 \leq 1) \lor x \leq 1$

Learned by resolution

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

NLSAT/MCSAT

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



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

NLSAT/MCSAT – Finite Basis

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

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

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

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

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

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

NLSAT/MCSAT – Finite Basis

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

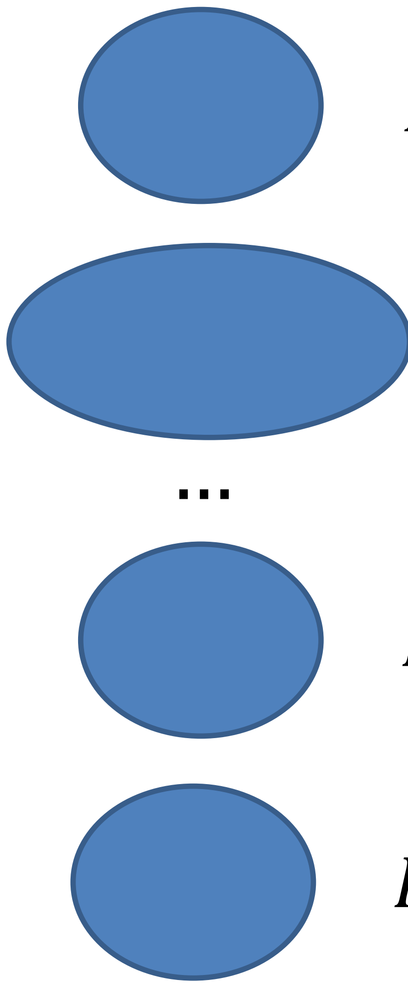
$F_{n-1}[x_{1,} x_2, \ldots, x_{n-1}]$

…

$F_2[x_{1,} x_2]$

$F_1[x_1]$

NLSAT/MCSAT – Finite Basis



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

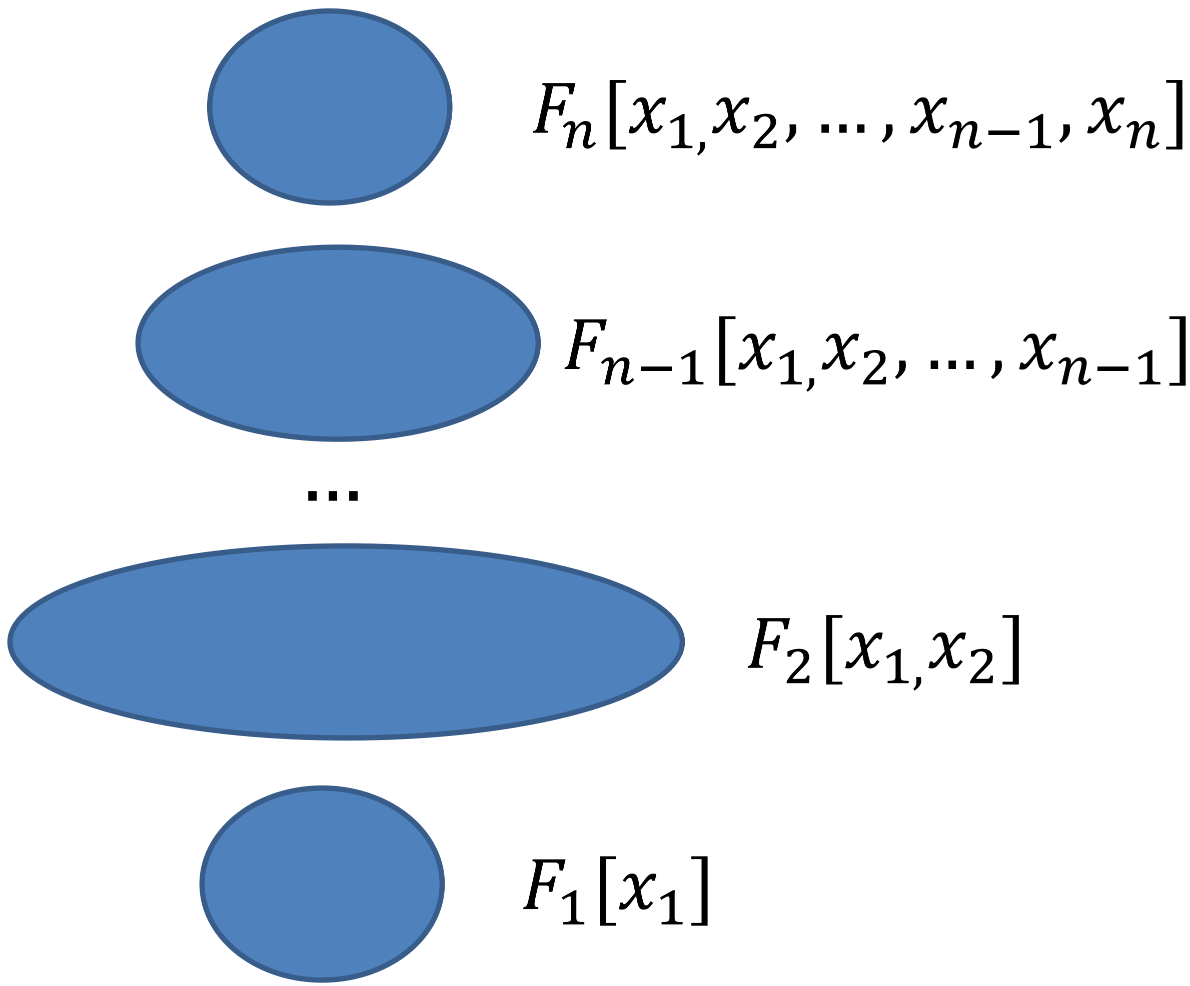
$F_{n-1}[x_1, x_2, \ldots, x_{n-1}]$

…

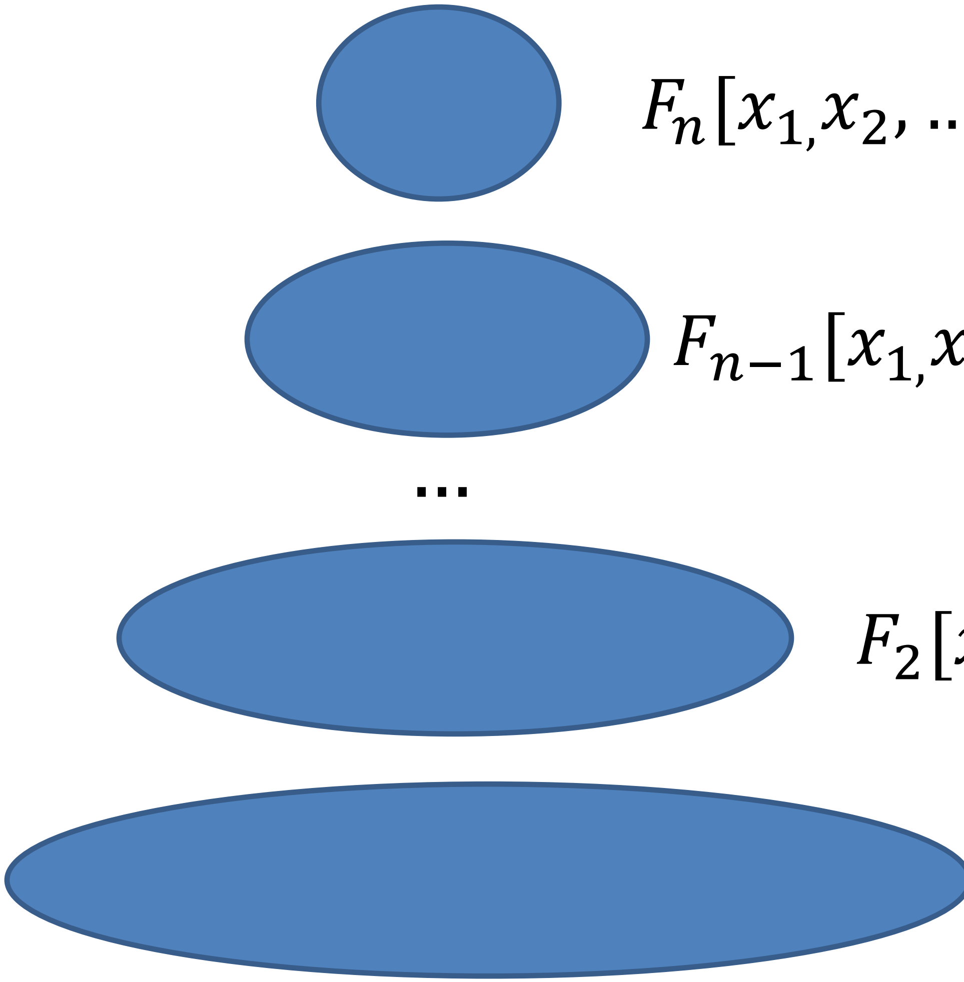
$F_2[x_1, x_2]$

$F_1[x_1]$

NLSAT/MCSAT – Finite Basis



NLSAT/MCSAT – Finite Basis



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

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

…

$$F_2[x_{1,}x_2]$$

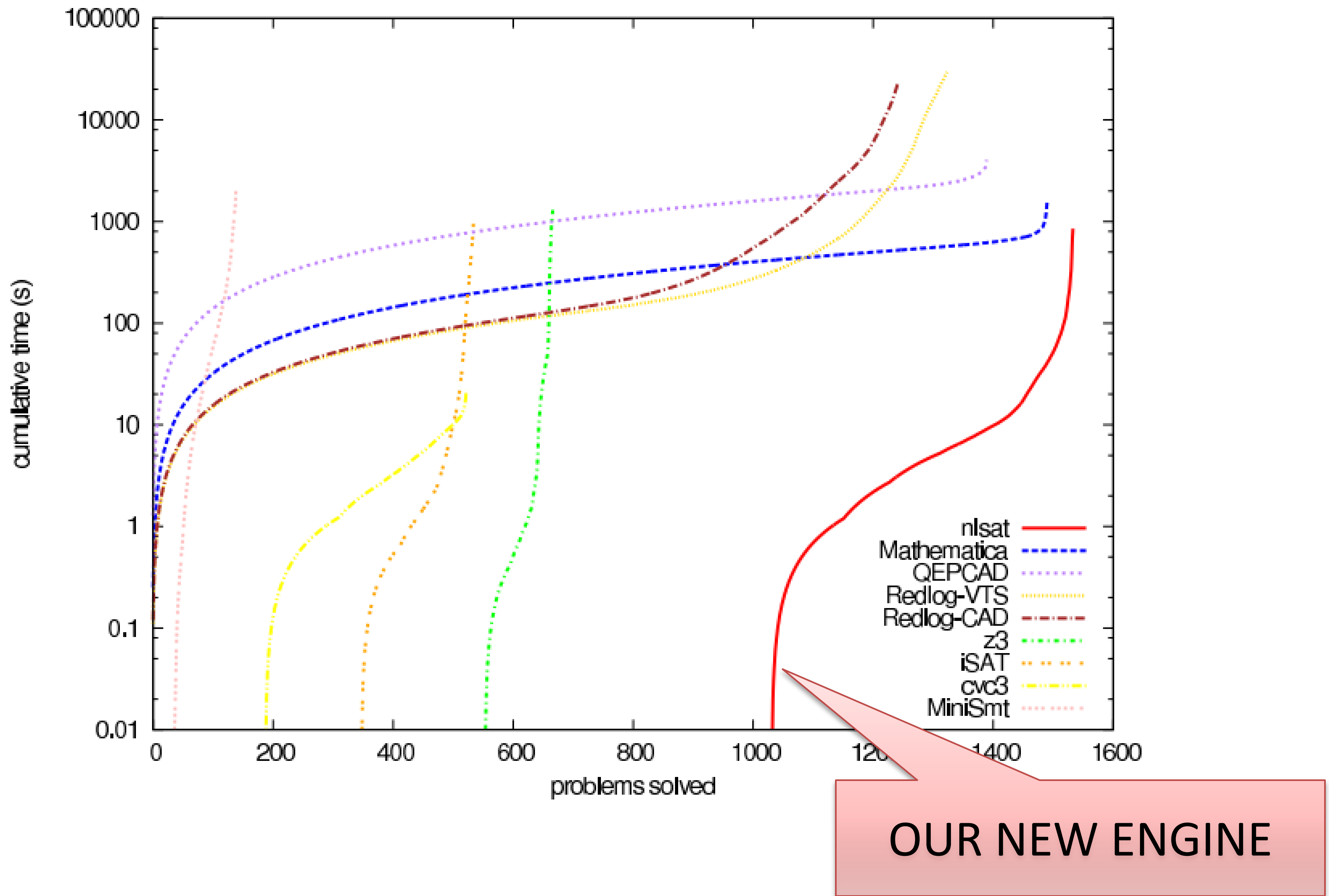
$$F_1[x_1]$$

Experimental Results (1)

OUR NEW ENGINE

solver	meti-tarski (1006) solved	time (s)	keymaera (421) solved	time (s)	zankl (166) solved	time (s)	hong (20) solved	time (s)	kissing (45) solved	time (s)	all (1658) 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)



NLSAT Bootlenecks

Real Algebraic Computations

$$x^5 - x - 1 = 0$$
$$y^3 - x^2 - 1 = 0$$

NLSAT Bootlenecks

Real Algebraic Computations

$$x^5 - x - 1 = 0$$
$$y^3 - x^2 - 1 = 0$$

Partially solved with new data-structure for representing algebraic numbers (CADE-24)

NLSAT Bootlenecks

PSCs (aka Subresultants)

used in the projection operation

NLSAT Bootlenecks

17775151118729246135103863388881244617666660995187997666751969361497959600261429526762965024955216280099712289835808749268353553329553408 x^532 +
14473361351917674942786915532863722010517729893029084002260132795724226061515042219666395922056072037155558819647140168198657847446137681117341286 4 x^528 +
72292649983139394997552859023359265193070565975516513811467535116460477381469054150674773988888617112303736934499923798937474384593298066265981583 36 x^524 +
15878482744622230892197972763581705423599198084235302253839649254815362649956536420885372278601947898596949668258188411414058700707614097818551897292 8 x^520 -
44105631689271549593077872808091483730101541566498339782560640363764370015426874290345769336389318155341052758269694167475697507851796021032713422110 72 x^516 +
27598160480965812548892638119998585519355277551514463222302333940057270410103048662363026531125946582051424948578752952138516755724717963410320457623142 4 x^512 +
60054961138517092321591893871554321291861242623870223453740621077995360357001795668079198231252226148014016026754218355851864746123524378206256324254105 60 x^508 +
98685162357640703325166712842507505387177409247052107988201472802589649253510147534662944253897894908984182841953202525358783342487581788772150996579123 20 x^504 -
37802815947438723742578392456237020646480154189917313873828344821455250631048120772292593335477190067155566022331743171410770501741115073710230504517455052 8 x^500 -
17808730106231073191878658236761328920282399007852768768460960004984306031572442483001419105190712931575531169183096099485281417843325729694855759690884710 40 x^496 +
49905604284676548601966045974533248435590879632764816978998632197254465597694923675229896407885432202196615787541140551943997984919108571076077238106204405 76 x^492 +
59251181672059584077424535291209687078232953829881306760118723543670560648034779432845164225459730400245051751104340753741284859922353854611675214692701175808 x^488 +
10920175192087855415206967852478228704629797103599433293030516216268358978224564312639118680739557385035839445302036863220734608250040386232047731519925098905 6 x^484 -
54363547237989392536050512424711049877096158862296431809125136818358221279800439115293008758238362119015368136331920428153565504670619454073127716484861552230 4 x^480 -
31946709568565070381707828048692668027254026452841026790371455013743524367931174064806811987767567310384777847207210311627108016457572329053499948120228631674 88 x^476 -
43895429996166486311768968621404824960251805702041606068686040528519520383832523272244021536948764994713912613843859787948674684859317644987969972972171852513 28 x^472 +
15524463640477929342623012689068443238906921917318414901015667570651210157882543051008270507122059363243821913470981377270906967132756811349600993710391290757120 x^468 +
80230430018834186054096672189233096308237228378515144056129280360834909794336559434803359466411692112541882365896166210172878178922236773486199994866195813629952 x^464 +
13078328343001159299252593768827129174795086403301182349912209762331113931187105546878135777646826440054978653252721693240762541807535237634985301906811947214438 4 x^460 -
60351536353188030534762927297367399984025488595096075263659285538732087664513596914391741526578214246339915348904989182771248594080446910993435975372364947914752 x^456 -
67373718826047549898293242072979140242935660968636456905324857080923272347462487449537284595037209343817403464265968832716855216008309470561344428360488227281305 6 x^452 -
13181175099277935061623802252280239902877419124787200668092459922717124214910091334599692065434897856522317661948776715600480215483989064863394423012906113800601 60 x^448 -
12057729022966243535250644682297312941599524028265024079669572437124740448717568639772208673394456199588827095355421166242689949470950990006014017945438915573841 92 x^444 -
49814754013992786837112112319354479399739079235158415820927050744316622931710296323475805107666498627201262926378938382533380944191959734389155788434248270715289 6 x^440 -
42518316035687815029500437329049753144853170778074503722857356709783483039433964598020662789393811356984055296482888805350497766068131792648011052930362953957376 x^436 +
21679968049931581630011819957832267936351235986717546627273851123744774943756364163016094421113035531298199968978567952479566758150036991833085956605496913108664 32 x^432 +
92401210692670512950454170008516086932167071451068658882221180739360783848126170951033407531855618186464003334694642988790166383198325066394694994965022155818926 08 x^428 +
14142674873965714441086369293263351081598953483434978452220946251634405490570039165341647880486182030947941853112320373639351925117748260464648116616807160519589888 x^424
+ 48043923162171692987972995522805171491415563711011101180797061757498198934560843308342131920171525920336527564651960026449395441317078499149865549560684187966504 96 x^420
- 61343286510477893282975942659113228679831767768284170422045263283528007102104968690274463160634338537081343995842293500958302056275810547934071032142753033680322 56 x^416
+ 36670900530940909453137560731056303335823629761905427539840410525430748330645725252314774541969829641342560219059247637537012592878577214957791121849402625234042 88 x^412
- 47818201981048087677690656309928524155074930628293058520581649509786217971008937734288774242825811509579744418638927275532750783613120642502614045600532841837363 2 x^408 -
50186901855213154855455322673164185696026971617543598141599919460301704348994047769553919666699488469505760925100359426459292729938602691732233804713882945039892480 x^404 -
49783192919360672941965836922796102255831339676036749735719193270699604144117615499151399963603838515014307866633369426721337772113987367017962230781939280563404800 x^400

....

1389385726272139827600391787516457146404057581084159628129387959867904441533378882732656681024381855322448 x^24 +
620628817761514905811282699618821217759839634640333727965142477866219324574857534794611520948542626504 9 x^20 +
367427074610454070056469795165580196050000194113672530558928364635826090406030636905429257496922636544 x^16 +
70332887417991884658952663143921054160262580168445685617174831300163538633716580995934281038561280 0 x^12 -
689990970469176278891695524203537985554534761096161230088163647222704320520188742855362168750 08 x^8 -
140432623903101758790898107887718053467061472637614549187228994429864721538224739784429911670784 x^4 +
272654874565539049477735920513220412248759995742372057602216372063084536679766701870415872000

PREAMBLE FOR GRANT’S TALK

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, $\{l_1, \dots, l_k\} \subseteq S$ 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

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

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

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

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

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

Extending Check Modulo Assignment for MCSAT

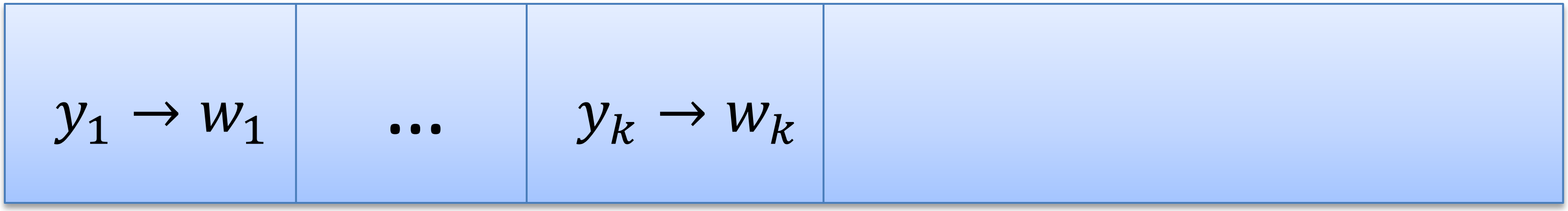
$$F[\bar{x}, \bar{y}] \qquad \bar{y} \rightarrow \bar{v}$$

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

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

NLSAT/MCSAT

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



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

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

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

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

...

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

...

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

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

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

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

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 $\{\bar{x} \to \bar{w}, \bar{y} \to \bar{v}\}$

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

If SAT return SAT

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

Conclusion

Model-Based techniques are very promising

NLSAT source code is available in Z3

http://z3.codeplex.com

Extended Check Modulo Assignment

Grant's talk: nonlinear optimization

New version coming soon