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"

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

$x\,y - 1 > 0$

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

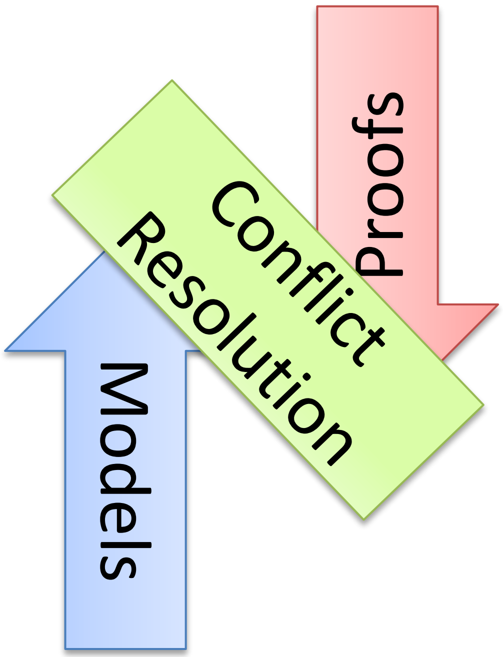
	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

NLSAT: MCSAT for Nonlinear Arithmetic

Static x Dynamic

Optimistic approach

Key ideas



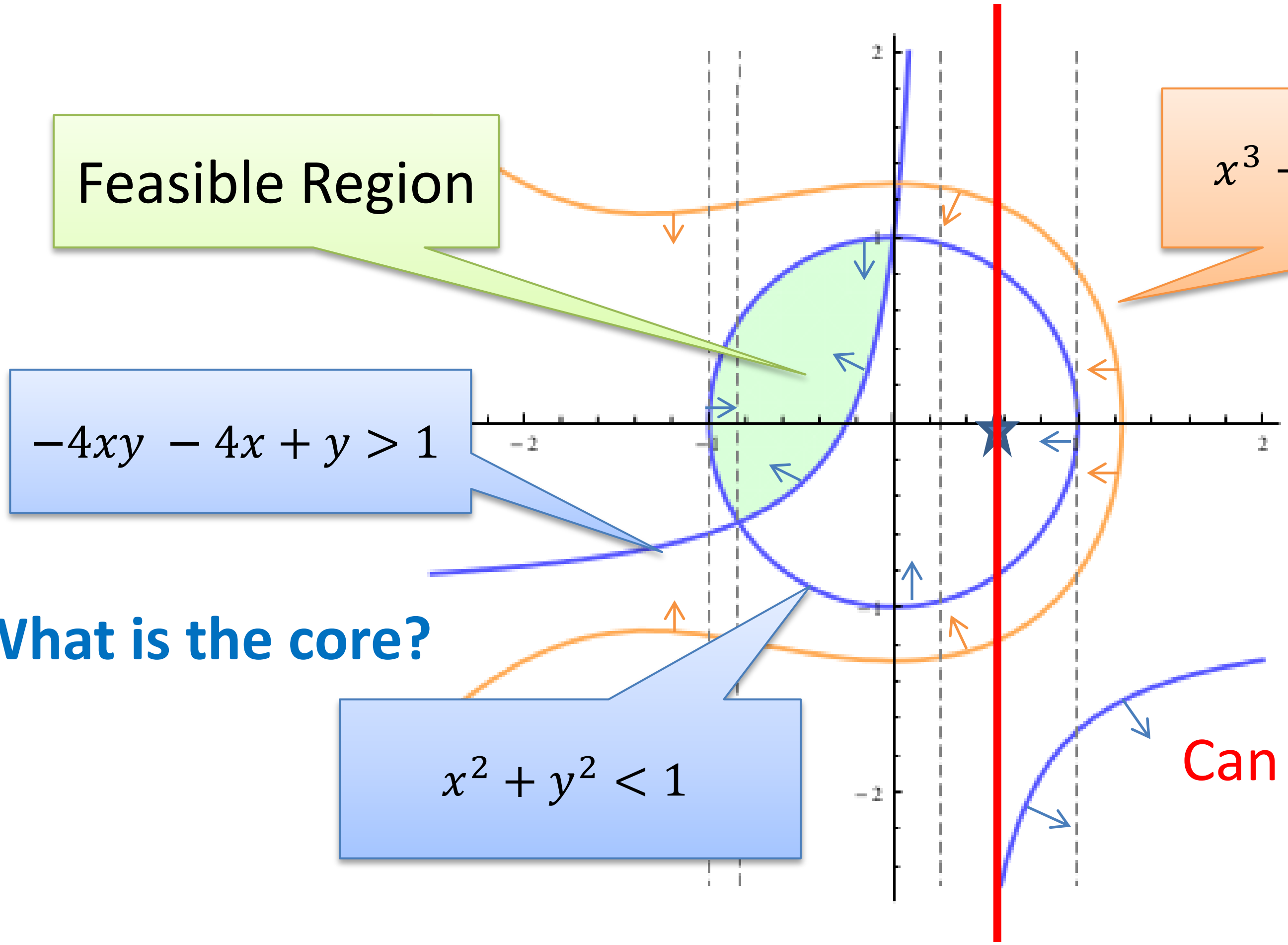
Start the Search before Saturate/Project

We saturate on demand

Model guides the saturation

NLSAT/MCSAT

Key ideas: Use partial solution to guide the search



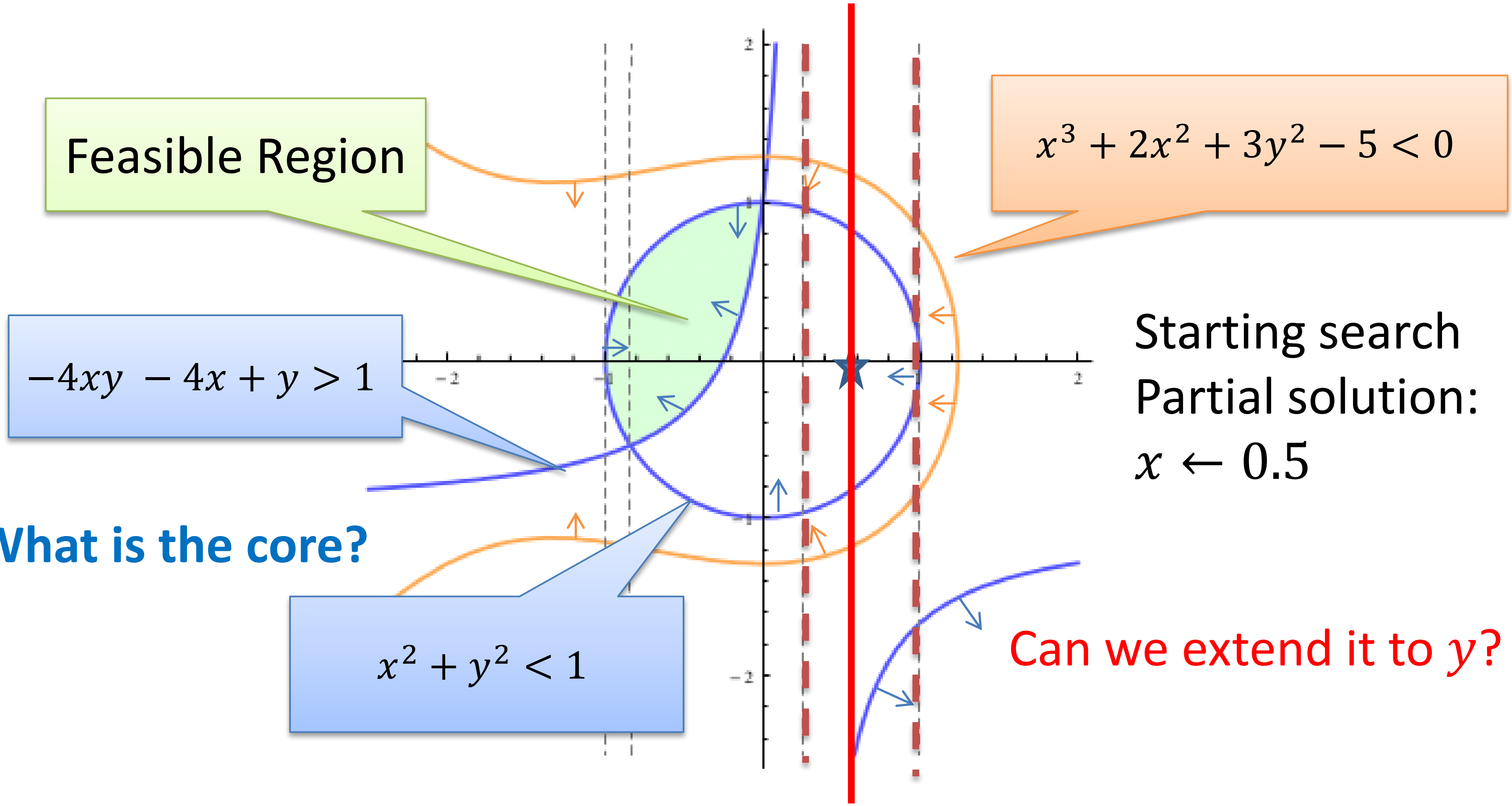
Starting search
Partial solution:
$x \leftarrow 0.5$

What is the core?

Can we extend it to y?

NLSAT/MCSAT

Key ideas: Use partial solution to guide the search



Starting search
Partial solution:
$x \leftarrow 0.5$

What is the core?

Can we extend it to y?

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

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

$x \geq 2$

Propagations

NLSAT/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

NLSAT/MCSAT

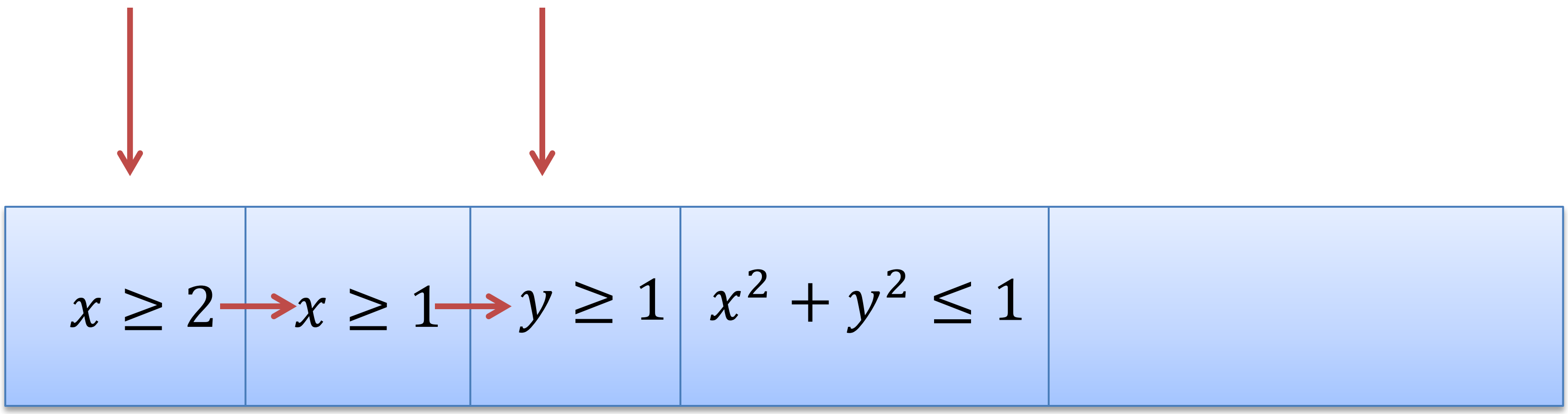
$x \geq 2, \quad (\neg x \geq 1 \vee y \geq 1), \quad (x^2 + y^2 \leq 1 \vee xy > 1)$

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

Propagations

NLSAT/MCSAT

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



Boolean Decisions

NLSAT/MCSAT

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

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

Semantic Decisions

NLSAT/MCSAT

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

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

Conflict

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

NLSAT/MCSAT

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

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

Conflict

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

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

NLSAT/MCSAT

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

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

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

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

NLSAT/MCSAT

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

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

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

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

NLSAT/MCSAT

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

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

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

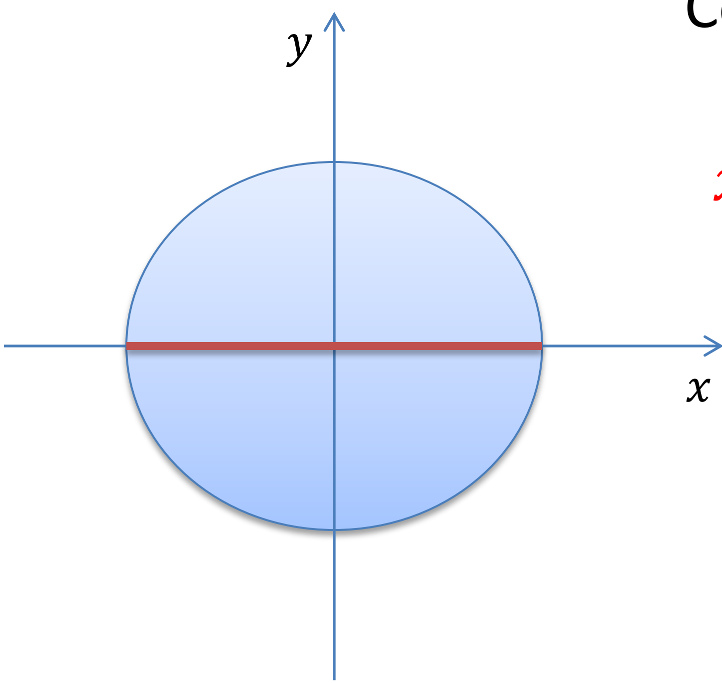
"Same" Conflict

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

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

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



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

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

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

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

NLSAT/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

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

NLSAT/MCSAT

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

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

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

Learned by resolution

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

NLSAT/MCSAT

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

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

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

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

NLSAT/MCSAT – Finite Basis

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

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

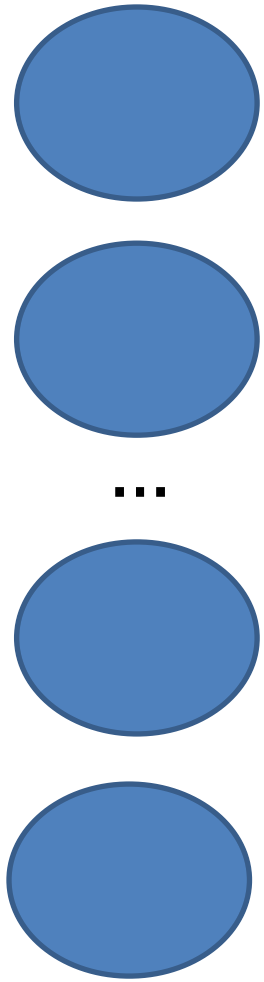
$$y_1 \to \alpha_1, \ldots, y_m \to \alpha_m$$

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

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

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

NLSAT/MCSAT – Finite Basis



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

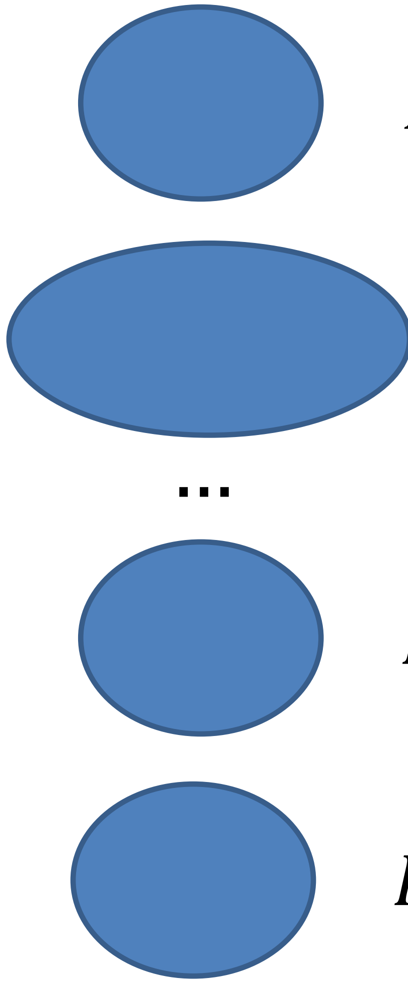
$F_{n-1}[x_{1,}x_2, \dots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

NLSAT/MCSAT – Finite Basis



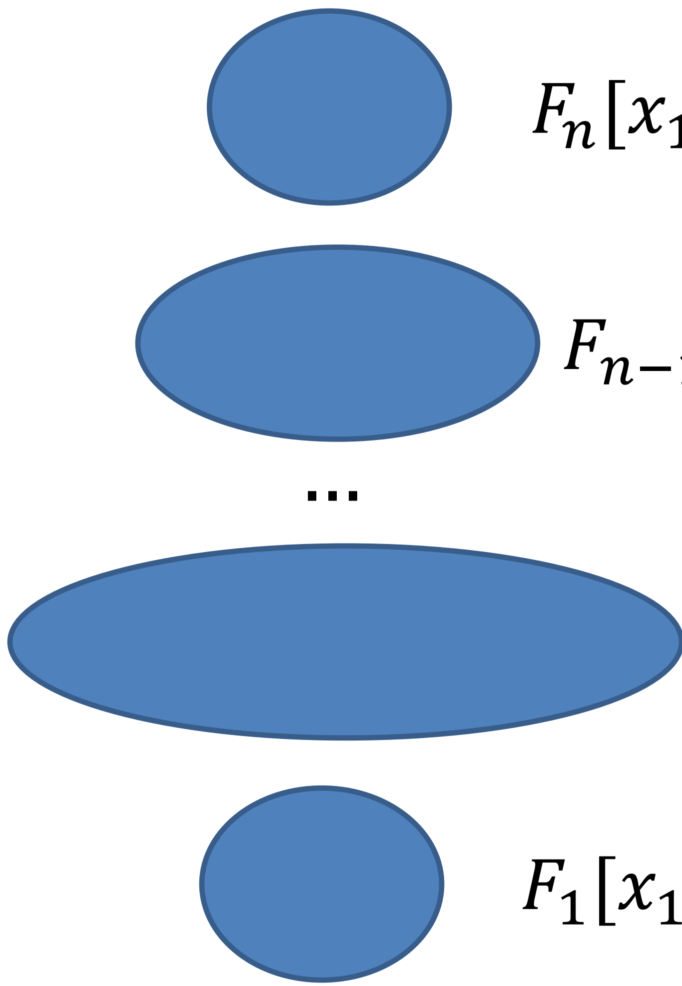
$F_n[x_{1,}x_2, \ldots, x_{n-1}, x_n]$

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

$F_2[x_{1,}x_2]$

$F_1[x_1]$

NLSAT/MCSAT – Finite Basis



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

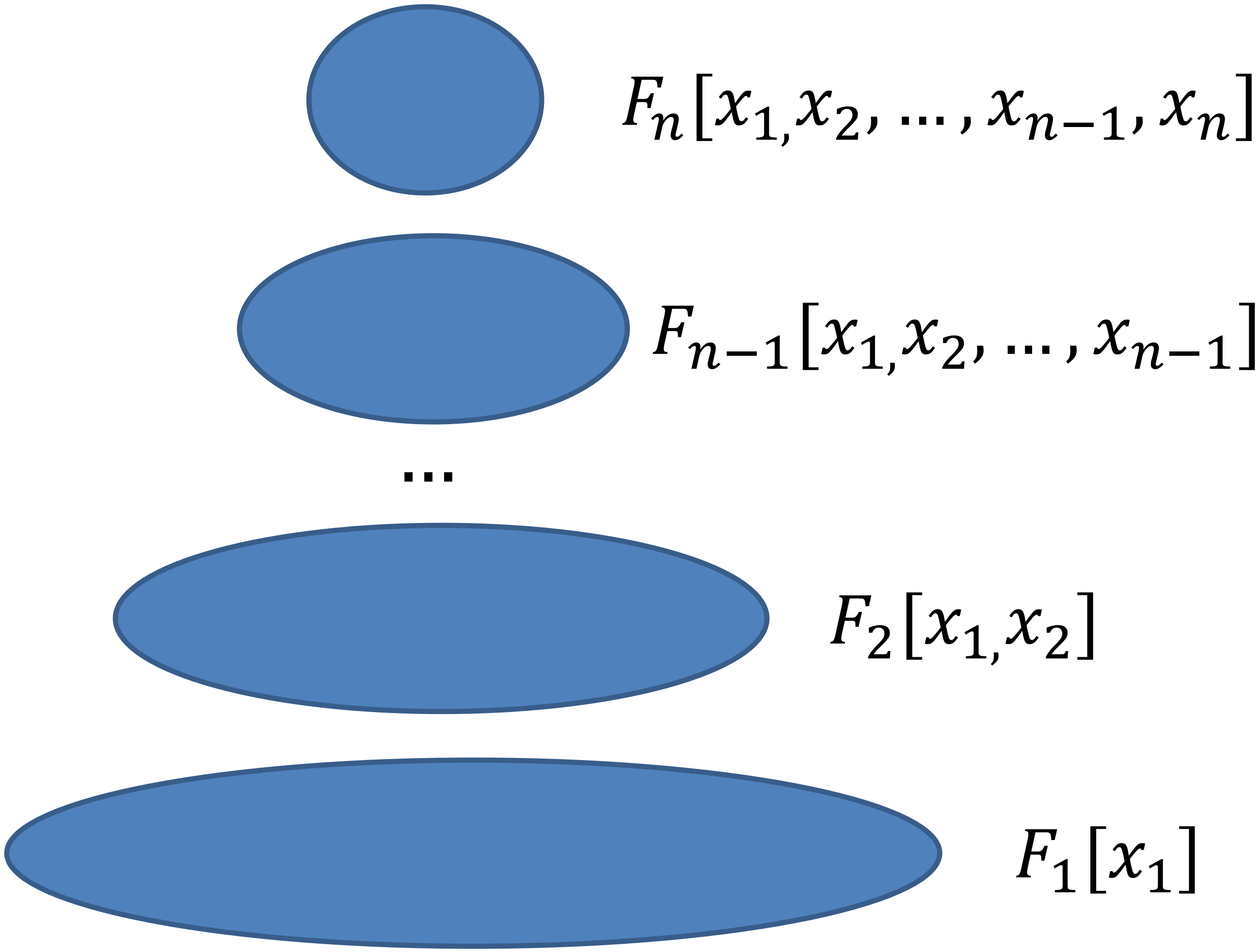
$F_{n-1}[x_{1,}x_2, \dots, x_{n-1}]$

…

$F_2[x_{1,}x_2]$

$F_1[x_1]$

NLSAT/MCSAT – Finite Basis

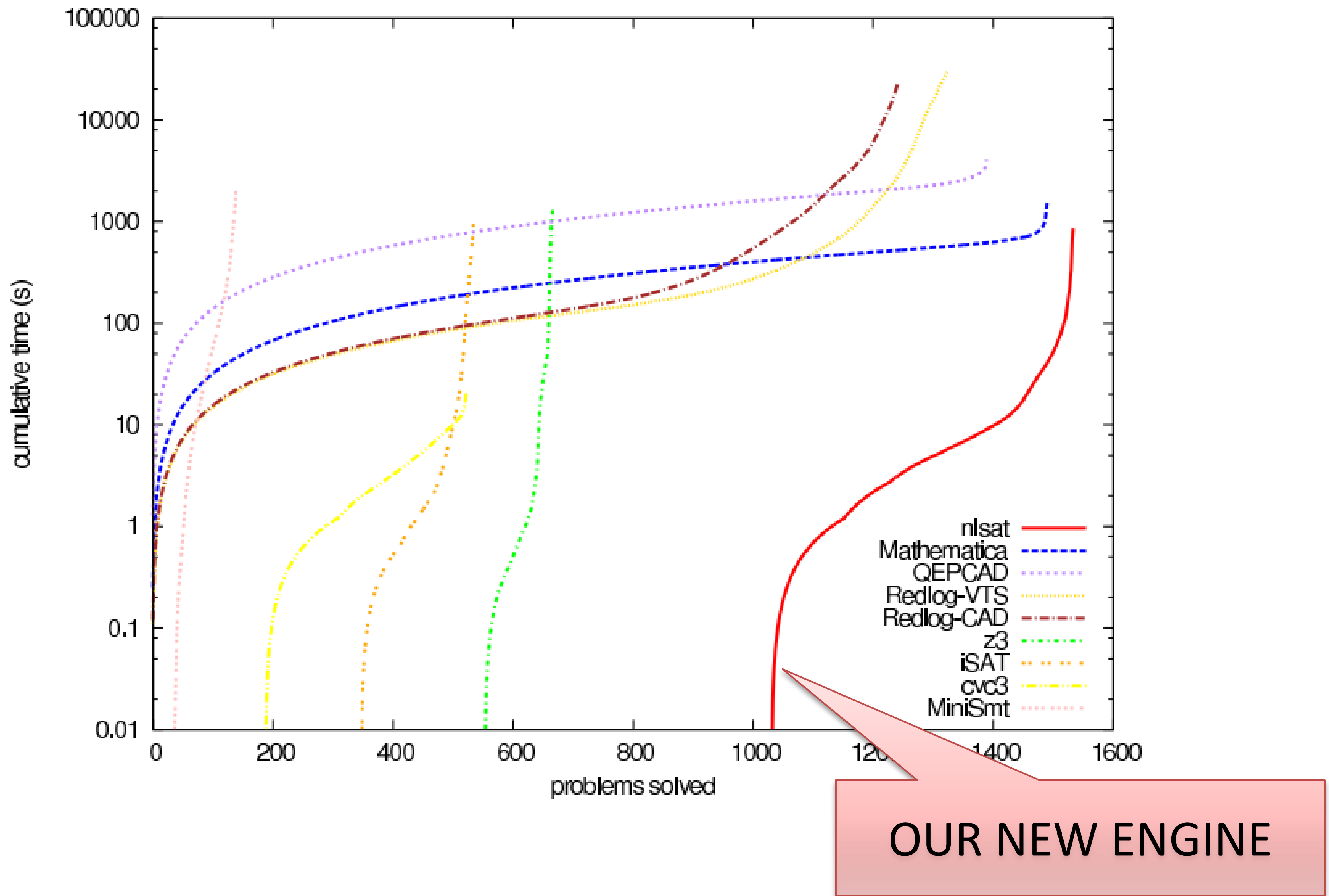


Experimental Results (1)

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)



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 +
144733613519176749427869155328637220105177298930290840022601327957242260615150422196663959220560720371555881964714016819865784744613768111734128 64 x^528 +
722926499831393949975528590233592651930705659755165138114675351164604773814690541506747739888886171123037369344999237989374743845932980662659815833 6 x^524 +
158784827446222308921979727635817054235991980842353022538396492548153626499565364208853722786019478985969496682581884114140587007076140978185518972928 x^520 -
441056316892715495930778728080914837301015415664983397825606403637643700154268742903457693363893181553410527582696941674756975078517960210327134221107 2 x^516 +
275981604809658125488926381199985855193552775515144632223023339400572704101030486623630265311259465820514249485787529521385167557247179634103204576231424 x^512 +
600549611385170923215918938715543212918612426238702234537406210779953603570017956680791982312522261480140160267542183558518647461235243782062563242541056 0 x^508 +
986851623576407033251667128425075053871774092470521079882014728025896492535101475346629442538978949089841828419532025253587833424875817887721509965791232 0 x^504 -
378028159474387237425783924562370206464801541899173138738283448214552506310481207722925933354771900671555660223317431714107705017411150737102305045174550528 x^500 -
178087301062310731918786582367613289202823990078527687684609600049843060315724424830014191051907129315755311691830960994852814178433257296948557596908847104 0 x^496 +
49905604284676548601966045974533248435590879632764816978998632197254465597694923675229896407885432202196615787541140551943997984919108571076077238106204405 76 x^492 +
592511816720595840774245352912096870782329538298813067601187235436705606480347794328451642254597304002450517511043407537412848599223538546116752146927011758 08 x^488 +
109201751920878554152069678524782287046297971035994332930305162162683589782245643126391186807395573850358394453020368632207346082500403862320477315199250989056 x^484 -
543635472379893925360505124247110498770961588622964318091251368183582212798004391152930087582383621190153681363319204281535655046706194540731277164848615522304 x^480 -
319467095685650703817078280486926680272540264528410267903714550137435243679311740648068119877675673103847778472072103116271080164575723290534999481202286316748 8 x^476 -
438954299961664863117689686214048249602518057020416060686860405285195203838325232722440215369487649947139126138438597879486746848593176449879699729721718525132 8 x^472 +
155244636404779293426230126890684432389069219173184149010156675706512101578825430510082705071220593632438219134709813777270906967132756811349600993710391290757120 x^468 +
802304300188341860540966721892330963082372283785151440561292803608349097943365594348033594664116921125418823658961662101728781789222367734861999948661958136299 52 x^464 +
130783283430011592992525937688271291747950864033011823499122097623311139311871055468781357776468264400549786532527216932407625418075352376349853019068119472144384 x^460 -
603515363531880305347629272973673999840254885950960752636592855387320876645135969143917415265782142463399153489049891827712485940804469109934359753723649479147 52 x^456 -
673737188260475498982932420729791402429356609686364569053248570809232723474624874495372845950372093438174034642659688327168552160083094705613444283604882272813056 x^452 -
131811750992779350616238022522802399028774191247872006680924599227171242149100913345996920654348978565223176619487767156004802154839890648633944230129061138006016 0 x^448 -
120577290229662435352506446822973129415995240282650240796695724371247404487175686397722086733944561995888270953554211662426899494709509900060140179454389155738419 2 x^444 -
498147540139927868371121123193544793997390792351584158209270507443166229317102963234758051076664986272012629263789383825333809441919597343891557884342482707152896 x^440 -
425183160356878150295004373290497531448531707780745037228573567097834830394339645980206627893938113569840552964828888053504977660681317926480110529303629539573 76 x^436 +
216799680499315816300118199578322679363512359867175466272738511237447749437563641630160944211130355312981999689785679524795667581500369918330859566054969131086643 2 x^432 +
924012106926705129504541700085160869321670714510686588822211807393607838481261709510334075318556181864640033346946429887901663831983250663946949949650221558189260 8 x^428 +
141426748739657144410863692932633510815989534834349784522209462516344054905700391653416478804861820309479418531123203736393519251177482604646481166168071605195898 88 x^424
+ 480439231621716929879729955228051714914155637110111011807970617574981989345608433083421319201715259203365275646519600264493954413170784991498655495606841879665049 6 x^420
- 613432865104778932829759426591132286798317677682841704220452632835280071021049686902744631606343385370813439958422935009583020562758105479340710321427530336803225 6 x^416
+ 366709005309409094531375607310563033358236297619054275398404105254307483306457252523147745419698296413425602190592476375370125928785772149577911218494026252340428 8 x^412
- 478182019810480876776906563099285241550749306282930585205816495097862179710089377342887742428258115095797444186389272755327507836131206425026140456005328418373632 x^408 -
501869018552131548554553226731641856960269716175435981415999194603017043489940477695539196666994884695057609251003594264592927299386026917322338047138829450398924 80 x^404 -
497831929193606729419658369227961022558313396760367497357191932706996041441176154991513999636038385150143078666333694267213377721139873670179622307819392805634048 00 x^400

....

13893857262721398276003917875164571464040575810841596281293879598679044415333788827326566810243818553224 48 x^24 +
62062881776151490581128269961882121775983963464033372796514247786621932457485753479461152094854262650 49 x^20 +
36742707461045407005646979516558019605000019411367253055892836463582609040603063690542925749692263654 4 x^16 +
70332887417991884658952663143921054160262580168445685617174831300163538633716580995934281038561280 0 x^12 -
68999097046917627889169552420353798555453476109616123008816364722270432052018874285536216875008 x^8 -
14043262390310175879089810788771805346706147263761454918722899442986472153822473978442991167078 4 x^4 +
2726548745655390494777359205132204122487599957423720576022163720630845366797667018704158720 00

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

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

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

Check Modulo Assignment

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

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

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

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

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

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

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

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

$y_1 \to w_1$	…	$y_k \to w_k$	

NLSAT/MCSAT

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

NLSAT/MCSAT

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

UNSAT, $y > 1$

No-good sampling

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

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

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

$\dots$

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

…

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

NLSAT source code is available in Z3

    http://z3.codeplex.com

Extended Check Modulo Assignment

    Grant's talk: nonlinear optimization

New version coming soon